

Cardano DÀNH CHO CỘNG ĐỒNG

Một hệ điều hành tài chính cho những người không có

John Greene Cử nhân, ThS, CISSP, C|EH

kindle | direct
publishing

Cardano dành cho cộng đồng: Một hệ điều hành tài chính dành cho những người chưa có
Bởi John Greene

Bản quyền © 2023, Xuất bản bởi Kindle Direct Publishing

Thông báo về Bản quyền:

Đã đăng ký Bản quyền. Không phần nào của cuốn sách này có thể được sao chép, lưu trữ trong hệ thống truy xuất hoặc chuyển giao dưới bất kỳ hình thức nào hoặc bằng bất kỳ phương tiện nào mà không có sự cho phép trước bằng văn bản, ngoại trừ trường hợp trích dẫn ngắn gọn được nhúng trong các bài báo hoặc bài phê bình.

Thông báo về trách nhiệm pháp lý:

Tác giả đã cố gắng hết sức để đảm bảo thông tin trong cuốn sách này là chính xác. Tuy nhiên, thông tin trong cuốn sách này được bán mà không có bảo hành, rõ ràng hay ngụ ý. Tác giả sẽ không chịu trách nhiệm cho bất kỳ thiệt hại nào gây ra trực tiếp hoặc gián tiếp bởi nội dung của cuốn sách này. Lời khuyên trong cuốn sách này có thể không phù hợp với hoàn cảnh của bạn. Bạn nên tham khảo ý kiến với một chuyên gia khi thích hợp. Độc giả nên biết rằng các trang Web được liệt kê trong cuốn sách này có thể đã thay đổi hoặc biến mất giữa thời điểm cuốn sách này được viết và khi nó được đọc.

Che phủ:

tín dụng *Heisenbird* (twitter @EyeOfTheKing1)

Người soát lỗi:

Oussama Benmahmoud

Tiến sĩ Lingling Liu

Diarmuid Buckley

Kevin Pendred

Giới thiệu về tác giả

John Greene có kiến thức cơ bản về cơ sở hạ tầng đám mây và bảo mật với bằng Thạc sĩ về Tiền tệ Kỹ thuật số của Đại học Nicosia. Đây là 'cuốn sách khó thứ hai' của anh ấy sau *AWSoeasy* năm 2015 (hiện đã lỗi thời). Anh ấy sống ở Dublin và tìm hiểu về Cardano, chạy bộ trên núi cho cơ thể và chơi bodhrán cho tâm hồn.

Liên hệ:

twitter.com/CardanoBook ,
john@cardanobook.com

Lời nói đầu

Chương 1: Ban đầu

Nguồn gốc của Blockchain và Crypto

Những ngày đầu của Charles Hoskinson trong lĩnh vực Crypto

Cardano được tạo ra

Dòng thời gian Cardano

Chương 2: Cardano là gì?

Khái niệm cơ bản

Tại sao Cardano lại khác biệt?

Tại sao chọn Cardano?

Lộ trình Cardano

Cardano hoạt động như thế nào?

Quyết định thiết kế Cardano

Đằng sau những cái tên

Chương 3: Bằng chứng cổ phần

Bằng chứng cổ phần là gì?

'Blockchain xanh'

Triết lý của POS

Người vận hành Stake Pool

Thiết lập và vận hành Stake Pool

Mạng Cardano

Cách nghiên cứu Stake Pool

Hiệu suất Stake Pool

Xếp hạng Stake Pool

Các loại địa chỉ trong Cardano

Cam kết

Ủy thác

Cam kết và phần thưởng

Tùy chọn cam kết và ủy thác

Các loại khóa trong Cardano

Cardano RTView

Công cụ theo dõi Cardano

Chương 4: Shelley (Sự đồng thuận)

Thách thức về khả năng mở rộng

Giao thức đồng thuận là gì?

Ouroboros

Các triển khai khác nhau của Ouroboros

Cách lớp đồng thuận hoạt động

Kinh doanh Hardfork

Con đường dẫn đến phi tập trung hoàn toàn

Ouroboros đặt nền móng cho kỷ nguyên Basho

Xác nhận giao dịch Chain v

P2P (ngang hàng)

Cardano Entropy (Tính ngẫu nhiên)

Phí trên Cardano

Ba khía cạnh khác nhau của Phi tập trung hoàn toàn

Chỉ số phi tập trung Edinburgh

Chương 5: Goguen (Hợp đồng thông minh)

UTXO mở rộng

'Không thông minh cũng không hợp đồng'

Siêu dữ liệu trên Cardano

Khóa Token trên Cardano

Token gốc

Hỗ trợ đa tài sản (MAS)

Tạo Token gốc trên Cardano

Vòng đời của Token gốc trên Cardano

Yêu cầu giá trị tối thiểu

Câu hỏi thường gặp về Token gốc

Đa tài sản trên Sàn giao dịch

Triển khai hợp đồng thông minh

Tính đồng thời không vấn đề

Liên minh UTXO

Chương 6: Plutus

Plutus là gì?

Tập lệnh Plutus

Phiên bản Plutus

Các trường hợp sử dụng Plutus điển hình

Công cụ Plutus

Viết giao dịch Plutus

Cơ chế tài sản đảm bảo

Học Plutus

Chương 7: Marlowe

Marlowe là gì?

Cấu trúc ngôn ngữ Marlowe

Marlowe Playground

Sử dụng Blockly với Marlowe

Sử dụng Trình chỉnh sửa cho Haskell hoặc JavaScript

Marlowe Run

Hợp đồng thông minh Actus

Marlowe cho tài chính P2P

Phát triển Marlowe Playground

Câu hỏi thường gặp về Marlowe

Chương 8: Basho (Khả năng mở rộng)

Khả năng mở rộng được xác định

Cải tiến liên tục

Pipelining

Lưu trữ trên đĩa

Tính toán ngoài chuỗi

Mithril

Hydra

Sidechains

Nửa đêm trong Khu vườn Thiện và Ác

Milkomeda

Input Endorsers

Chương 9: Voltaire (Quản trị)

Tiền là xã hội

Đề xuất cải tiến Cardano (CIP)

Dự án Catalyst là gì?

Nguồn quỹ ban đầu của Catalyst

Vòng tròn Catalyst

Catalyst gốc

Quỹ sau này

Quỹ Cardano cFund

dRep

Tạm dừng chiến thuật cho Catalyst

Thời đại Voltaire

Chương 10: RealFi trên Cardano

Cuộc cách mạng DeFi

~~DeFi~~-RealFi cho cộng đồng

ID phi tập trung Atala Prism

Phí Babel

Phí ổn định

Định giá theo cấp độ khi mạng mở rộng

Djed Stablecoin

Câu hỏi thường gặp về Djed

EUTXO đối phó với tổn thất tạm thời như thế nào

Bộ chuyển đổi ERC20

DApp được chứng nhận trên Cardano

Oracle trên Cardano

Cardano ở Châu Phi

Quan điểm

Bảng chú giải

Lời nói đầu

Tôi phát hiện ra Cardano khi đang nghiên cứu một dự án đại học vào năm 2018. Kể từ khi tôi đặt câu hỏi cho Charles Hoskinson, người đồng sáng lập Cardano tại một trong những AMA của anh ấy, 'tôi đã có ý định viết một cuốn sách nào đó. Tôi đã thử những ý tưởng khác nhau, bỏ cuộc và quay lại nhiều lần. Khi nghe nói rằng cuốn sách *Mastering Cardano* rất được mong đợi sẽ bị trì hoãn, tôi cảm thấy có thể có chỗ cho 'cái hộp được mở' trong thời gian chờ đợi.

Viết về Crypto là một thách thức. Hầu hết các cuốn sách về Crypto bán chạy nhất đều có 'Điểm dễ đọc' trong vòng 50 giây. Tôi muốn cuốn sách này bao quát hơn.

Với rất nhiều biệt ngữ trong lĩnh vực Blockchain, tôi quyết định cung cấp cho người đọc những lời giải thích xuyên suốt. Tuy nhiên, tôi cũng không muốn cản trở dòng chảy. Vì Kindle tự động chuyển đổi chủ thích cuối trang thành định dạng Pop-Up, nên người giải thích có thể truy cập được bằng cách nhấp vào chỉ số trên trong văn bản. Những người giải thích cũng tạo thành một bảng thuật ngữ ở cuối cuốn sách. Tôi đã thêm các đoạn trích từ các cập nhật khác nhau của Charles Hoskinson để đan xen quan điểm của anh ấy trong suốt cuốn sách. Tôi cảm thấy họ thêm bối cảnh vào nhiều quyết định công nghệ trong khi vẽ ra tầm nhìn cho toàn bộ dự án và ngành.

Tôi đã cố gắng hết sức để chính xác, tuy nhiên, Cardano đang phát triển nhanh chóng. Có thể đã có một sự thay đổi hoặc cập nhật nào đó khi bạn đọc điều này. Tôi dự định cập nhật cuốn sách thường xuyên với các bản cập nhật Cardano, cải thiện khả năng đọc với mỗi lần xuất bản.

Đối với thiết bị đọc sách điện tử, đồ họa được xem tốt nhất ở chế độ 'ngang'.

Đối tượng dự định

Cuốn sách này chủ yếu dành cho những người mới biết đến Cardano. Nó không tập trung vào các dự án cụ thể được xây dựng trên Cardano. Báo cáo đầu tiên *Hướng dẫn Essential Cardano cho hệ sinh thái*² đề cập đến điều đó. Nó không đi sâu vào nội dung của các tài liệu nghiên cứu kỹ thuật,³ cũng không khám phá các khái niệm một cách chi tiết. Mục tiêu là cung cấp một cái nhìn tổng quan về Cardano. Mỗi chương có thể được đọc riêng, tuy nhiên, tốt nhất bạn nên đọc từ đầu đến cuối nếu bạn chưa quen với Cardano. OG⁴ có thể duyệt và đọc các phần một cách độc lập. Những thông tin được đưa ra không phải là một lời khuyên tài chính.

Chương 1 là tổng quan cấp cao về Blockchain và cách Cardano bắt đầu. Chương 2 đi qua các khái niệm cơ bản. Chương 3 đề cập đến bằng chứng cổ phần và các điểm khác biệt của Cardano. Các chương còn lại đi qua các khía cạnh khác nhau của lộ trình Cardano (roadmap.cardano.org). Chương 10 nói về sản phẩm cuối cùng: RealFi trên Cardano.

IOG và IOHK

Input Output được thành lập tại Hồng Kông nên có tên viết tắt là IOHK. Tuy nhiên, công ty đã chuyển cơ sở sang Wyoming, Hoa Kỳ và đổi thương hiệu thành Input Output Global (IOG). Ở một số giai đoạn, trang Web có thể sẽ chuyển từ iohk.io sang iog.io.

¹AMA Chủ nhật ngày 17/05/2020, youtube.com/watch?v=-CJ5pcullgg &t=690s

²Hướng dẫn Cardano cần thiết cho Hệ sinh thái, services.iohk.io/guide-to-the-ecosystem

³Thư viện IOHK, iohk.io/en/research/library/

⁴OG (crypto Original Gangster) là tiếng lóng của người sáng lập bất kỳ Blockchain Crypto ban đầu nào, chẳng hạn như Vitalik Buterin, người đã phát minh ra Ethereum. Một OG Crypto cũng có thể đề cập đến một nhà đầu tư ban đầu vào Bitcoin hoặc Ethereum.

Sự nhìn nhận

Tốt nhất là nên làm rõ ngay từ đầu và thừa nhận tôi không phải Satoshi Nakamoto, tôi cũng không phát minh ra giao thức đồng thuận *Ouroboros* hay nghĩ ra phí Babel.

Cuốn sách này được lấy cảm hứng từ những bộ óc lỗi lạc tại IOG và hệ sinh thái Cardano. Đối với một số khái niệm và tính năng kỹ thuật vẫn đang trong quá trình nghiên cứu, tôi sẽ không nói quá sâu. Tôi đã cố gắng tham khảo tất cả các nguồn.

Chương 1: Phần mở đầu

'Nhà tiên tri tốt nhất của tương lai là quá khứ'

- Lord Byron

Nguồn gốc của Blockchain và Crypto

Nếu ai nghi ngờ câu ngạn ngữ 'Đôi khi sự thật còn kỳ lạ hơn bất cứ điều gì có thể tưởng tượng được' thì nên nhìn vào lịch sử tiền tệ.⁵Từ những viên đá tròn trên đảo Yap, đến việc người Ireland 'ăn miếng trả miếng' đối với người Đan Mạch, đến hòa bình và thịnh vượng của thời đại Belle Époque, đến việc áp dụng và từ bỏ tiêu chuẩn vàng...Crypto và Blockchain⁶ cũng tiếp tục như vậy, chỉ là bước ngoặt mới nhất trong một câu chuyện dài và đầy màu sắc.

Để hiểu một Blockchain thế hệ thứ ba như Cardano, trước tiên chúng ta phải xem xét những Blockchain thuộc thế hệ trước. Thế hệ đầu tiên là Bitcoin,⁷với mục tiêu là tạo ra tiền phi tập trung. Có thể có một Token khan hiếm, có thể giao dịch được tồn tại trên một số loại Blockchain phi tập trung không duy trì bởi mọi người trên khắp thế giới?

Đây không phải là một sự theo đuổi mới. Bitcoin tinh cở là bước đột phá, nhưng nó được xây dựng dựa trên những nỗ lực trước đó. Ý tưởng về Bitcoin bắt đầu từ những năm 1980, với rất nhiều ý tưởng đến từ phong trào 'Cypherpunk'.⁸ Ecash đi trước DigiCash với công trình tiên phong của Hal Finney và David Chaum. Trong những năm 1990 và đầu những năm 2000, Nick Szabo đã đề xuất hệ thống 'Bitgold'. Có những yếu tố góp phần khác như những tiền bộ công nghệ của chip Arm cung cấp năng lượng cho các thiết bị nhỏ hơn, giúp khả năng xử lý trở nên khả thi.

Vào năm 2008, Bitcoin chỉ là một giấc mơ viễn vông dưới dạng một bản White Paper.⁹ Satoshi Nakamoto là bút danh của người đã viết bài nghiên cứu này. Người sáng lập Bitcoin vẫn ẩn danh, ngay cả sau khi tài khoản Email của họ bị xâm phạm và Email được chia sẻ công khai. Ngay từ đầu, Bitcoin đã bị che giấu trong bí ẩn. Đó là một thử nghiệm được sinh ra từ sự bất mãn với cách mọi thứ đang diễn ra và chủ nghĩa lý tưởng về cách mọi thứ nên diễn ra. Vào ngày 3 tháng 1 năm 2009, Satoshi Nakamoto đã khai thác khối đầu tiên – Genesis Block¹⁰ cho Bitcoin. 100.000 dòng mã C++ bình thường thường¹¹đã thu hút rất nhiều bộ óc thông minh.

Từ những người ủng hộ ban đầu như Hal Finney đến Martti Malmi, nhiều người khác đã đổ xô đến trong nhiều năm khi Bitcoin phát triển từ một vài người theo chủ nghĩa vô chính phủ về Crypto trong danh sách gửi thư, thành một phong trào toàn cầu. Tất cả điều này mặc dù không có ngân sách tiếp thị, với Logo do người dùng diễn đàn có tên Bitboy cung cấp.¹² Bitcoin kể từ đó đã chứng minh khả năng phục hồi của nó. Nó đã bị tuyên bố là đã chết vô số lần và chịu đựng nhiều sự cố. Nhiều người đóng góp ban đầu đã rời đi. Các nhà phát triển như Mike Hearn và Gavin Andresen đã thất bại và rời đi. Satoshi Nakamoto, người sáng lập ẩn danh, cũng đã biến mất. Bất chấp những trở ngại và thất bại như vậy, giấc mơ vẫn tồn tại.

⁵Lịch sử ngắn gọn (và hấp dẫn) về tiền tệ', [britannica.com/story/a-brief-and-fascinating-history-of-money](https://www.britannica.com/story/a-brief-and-fascinating-history-of-money)

⁶Blockchain là một danh sách các bản ghi liên tục phát triển, được gọi là các Block, được liên kết và bảo mật bằng mật mã. Mỗi khối thường chứa một liên kết đến khối trước đó, dấu thời gian và dữ liệu giao dịch. Theo thiết kế, các Blockchain vốn có khả năng chống sửa đổi dữ liệu. Blockchain là 'một sổ cái mở, phân tán có thể ghi lại các giao dịch giữa hai bên một cách hiệu quả và theo cách có thể kiểm chứng và lâu dài.'

⁷ **Bitcoin (BTC)** là một loại Crypto và một hệ thống thanh toán sử dụng sổ cái phân tán công khai được gọi là Blockchain. Được phát minh bởi một người (hoặc có khả năng là một nhóm) dưới bí danh Satoshi Nakamoto. Vào ngày 31 tháng 10 năm 2008, Bitcoin đã được đưa vào danh sách gửi thư mật mã và được phát hành dưới dạng phần mềm nguồn mở vào năm 2009. Đã có nhiều tuyên bố và suy đoán liên quan đến danh tính của Nakamoto, không có tuyên bố nào được xác nhận. Hệ thống này là ngang hàng, vì vậy các giao dịch diễn ra trực tiếp giữa những người dùng mà không cần trung gian. Các giao dịch này được xác minh bởi các Node mạng và được ghi lại trong Blockchain, sử dụng bitcoin làm đơn vị tài khoản.

⁸Một **cypherpunk** là bất kỳ nhà hoạt động nào ủng hộ việc sử dụng rộng rãi các công nghệ mã hóa mạnh và nâng cao quyền riêng tư như một lộ trình dẫn đến thay đổi xã hội và chính trị. Ban đầu giao tiếp thông qua danh sách email của cypherpunks, các nhóm không chính thức nhằm đạt được quyền riêng tư và bảo mật thông qua việc chủ động sử dụng mật mã. Cypherpunks đã tham gia vào một phong trào tích cực từ cuối những năm 1980.

⁹Satoshi Nakamoto (2008) 'Bitcoin: Hệ thống tiền mặt điện tử ngang hàng', bitcoin.org/bitcoin.pdf

¹⁰ Khối **genesis** là khối đầu tiên của Blockchain. Khối genesis hầu như luôn được mã hóa cứng vào phần mềm của các ứng dụng sử dụng Blockchain của nó. Đây là một trường hợp đặc biệt ở chỗ nó không tham chiếu đến một khối trước đó.

¹¹Hướng dẫn mã nguồn bitcoin, drnealagarwal.info/bitcoin-source-code-walkthrough/

¹²Logo của bitcoin, decrypt.co/43923/bitcoins-logo-the-story-of-the-big-orange-b

Trong vòng vài năm, Bitcoin đã có hàng nghìn người dùng có thể gửi và nhận giá trị mà không cần phải tin cậy vào bên thứ ba hoặc bên trung gian nào. Giá Bitcoin đã tăng từ dưới một xu lên 1 đô la vào năm 2011, lên 1.000 đô la vào năm 2013, 17.000 đô la vào năm 2018 và đạt mức cao nhất là 67.000 đô la vào năm 2021. Trong suốt thời gian đó, đã có những sự cố như 'mùa đông Crypto' năm 2017, khi giá bitcoin đã giảm từ khoảng 20.000 đô la xuống còn 6.000 đô la trong vòng vài tuần. Một vụ sụp đổ tương tự đã xảy ra vào đầu năm 2022 khi Bitcoin bị mất 2/3 giá trị.

Chủ nghĩa lý tưởng của Bitcoin là tạo ra tiền tốt hơn, hay 'tiền tốt'¹³ trong thời đại kỹ thuật số' như được mô tả bởi nhà kinh tế Saifedean Ammous trong *Tiêu chuẩn Bitcoin*. Bitcoin xuất hiện sau cuộc khủng hoảng tài chính năm 2008, cuộc khủng hoảng tài chính toàn cầu tồi tệ nhất kể từ cuộc Đại suy thoái. Nhiều người bắt đầu quay trở lại những nguyên tắc đầu tiên, đặt câu hỏi liệu các ngân hàng trung ương có thể được tin cậy để tạo ra 'tiền tốt' hay không? Những người khác có thể tạo ra tiền tốt hơn không? Liệu thế giới có thực sự cần các ngân hàng đóng vai trò trung gian? Tôi có thể là ngân hàng của riêng mình không? Những câu hỏi như thế này cùng với sự ngờ vực của các tổ chức là mầm mống để Bitcoin phát triển.

Các thuộc tính của tiền tốt là gì?

Tiền thường được định nghĩa là có ba thuộc tính cơ bản:

- 1) Đơn vị tài khoản
- 2) Phương tiện trao đổi
- 3) Kho lưu trữ giá trị.

Tiền là một **đơn vị tài khoản** có nghĩa là chúng ta có khả năng đo lường giá cả một cách nhất quán. Chúng ta có thể so sánh hàng hóa và dịch vụ bằng đô la, Euro hoặc bảng Anh. Không có đơn vị tài khoản, nó có thể giống như nhà tù nơi bạn so sánh và đổi thuốc lá lấy bánh mì, sách, thẻ bóng chày hoặc bất cứ thứ gì xung quanh. Rõ ràng là xã hội sẽ rất hỗn loạn, khiến việc khám phá giá¹⁴ gần như là không thể.

Phương tiện trao đổi, có nghĩa là Token phải được chấp nhận rộng rãi. Để một loại tiền được đề xuất hoạt động, nó sẽ có thể được trao đổi để lấy hàng hóa, dịch vụ và hoạt động như một công cụ trung gian. Việc trở thành một phương tiện trao đổi hợp lệ sẽ tránh được những hạn chế của hệ thống trao đổi hàng hóa, trong đó những gì người này muốn phải khớp chính xác với những gì người kia đưa ra.

Cuối cùng, **kho lưu trữ giá trị** là tài sản mà khi bạn nhận được tiền, nó không phai màu, không bốc hơi thành không khí loãng, hư hỏng hoặc thối rữa. Nhiều hàng hóa có một số thuộc tính của tiền. Ví dụ, nếu bạn đang ở trong tù, chuối hoặc thực phẩm đóng hộp có thể là phương tiện trao đổi khả thi. Tuy nhiên, nhìn chung thì thực phẩm không thể được sử dụng như một kho lưu trữ giá trị vì nó sẽ mau hỏng. Để tiền trở thành phương tiện lưu trữ giá trị, nó phải bền về giá trị theo thời gian. Nó cũng phải bền về mặt vật lý. Ngay cả khi bạn quên nó trong túi trước khi giặt quần áo, tiền giấy và tiền kim loại Euro thường có thể sử dụng được sau đó. Có rất nhiều đồng tiền kim loại vẫn còn tồn tại từ thời La Mã trở về trước.

Có nhiều tài sản khác. Liệu nó có thể vận chuyển được không? Vàng thường được cho là một phương tiện trao đổi kém vì nó khó vận chuyển trên một khoảng cách dài. Liệu một kho vàng lớn dưới tầng hầm có giá trị đối với một người chạy trốn chiến tranh không? **Khả năng vận chuyển** của tiền có thể thay thế tất cả các tài sản khác trong một kịch bản như vậy.

Tính có thể thay thế là một thuật ngữ chỉ quen thuộc với các nhà giao dịch hàng hóa cho đến khi cơn sốt NFT (Token không thể thay thế) vào năm 2021 diễn ra.¹⁵ Đó là thước đo của *sự giống nhau*, liệu hai vật giống hệt nhau hay mỗi vật là duy nhất. Nếu có thể thay thế được, thì không có sự khác biệt thực tế giữa hai thứ. Để công việc kinh doanh trôi chảy, phải có sự nhất quán rằng một đô la là một đô la, là một đô la. Điều này có thể ở dạng kỹ thuật số trong thanh toán bằng thẻ tín dụng, khoản vay hoặc ghi chú vật lý được chuyển

¹³ **Tiền lành mạnh** là tiền không có khả năng bị tăng giá đột ngột hoặc giảm giá trị.

¹⁴ **Khám phá giá** là quá trình xác định giá của một tài sản trên thị trường thông qua sự tương tác của người mua và người bán.

¹⁵ **Token không thể thay thế (NFT)**. Token như vậy chứng minh quyền sở hữu đối với một mặt hàng kỹ thuật số giống như cách mọi người sở hữu Crypto. Tuy nhiên, không giống như các loại Crypto giống hệt nhau và có giá trị như nhau, NFT là duy nhất. Một cơn sốt bắt đầu với cuộc đấu giá của Christie's *Mỗi ngày : 5.000 ngày đầu tiên*, một ảnh ghép gồm 5.000 tác phẩm kỹ thuật số vào ngày 11 tháng 3 năm 2021. Mike Winkelmann, được biết đến với cái tên Beeple, đã tạo ra tác phẩm nghệ thuật kỹ thuật số và tạo ra một NFT cho nó. Đầu thầu bắt đầu ở mức 100 đô la. Nó được bán với giá 69,3 triệu USD. Mười ngày sau, người đồng sáng lập Twitter Jack Dorsey đã bán một NFT của tweet đầu tiên với giá 1.630,5 ether (2,9 triệu đô la) và quyền góp số tiền thu được cho tổ chức từ thiện. NFT đã trở thành từ của năm trong Từ điển Collins cho năm 2021. Tuy nhiên, khi người mua NFT của Dorsey cố gắng bán nó một năm sau đó, mức giá cao nhất chỉ là 6.800 đô la. Cuối cùng, giá trị của một NFT chỉ được xác định bởi những gì ai đó sẵn sàng trả cho nó.

giao. Đây là những gì bạn mong đợi với hai đơn vị tiền tệ giống nhau. Tuy nhiên, nếu bạn mua một bức tranh đắt tiền từ một phòng trưng bày, bạn muốn nó không thể thay thế được, một vật thể độc nhất.

Tính có thể chia nhỏ là một tính chất quan trọng khác. Bạn có thể thử, nhưng quán cà phê có thể sẽ không chấp nhận thanh toán bằng vỏ sò. Vì vậy, thật thuận tiện để nhân rộng hệ thống 'tiền vào, tiền ra'. Các loại tiền kỹ thuật số tạo điều kiện thuận lợi cho việc chia nhỏ theo nghĩa toán học rất tốt theo thiết kế. Tuy nhiên, một số thực quan hơn trong thực tế. Ví dụ: thanh toán số tiền tương đương 10 đô la cho cuốn sách này bằng các loại Crypto khác nhau (tháng 7 năm 2022) sẽ diễn ra như sau:

0,00043 Bitcoin (BTC)
0,0063 Ethereum (ETH)
20.01035705 Cardano (ADA)

Một số loại tiền tệ thực đang mất khả năng chia nhỏ và đã có đề xuất loại bỏ đồng xu, một đơn vị tài khoản cơ bản. Làm tròn số đã được giới thiệu cho các giao dịch tiền mặt ở Ireland vào năm 2015, có nghĩa là tổng số tiền của một hóa đơn sẽ được làm tròn lên hoặc xuống đến năm xu gần nhất.

Cách bạn có thể xác định các loại lạm phát khác nhau và chính xác thể nào là 'tiền tốt' xứng đáng là một cuốn sách của riêng nó. Bitcoin có lập trường về cách cung cấp các thuộc tính cần thiết cho một loại tiền. Nó khan hiếm, chỉ có 21 triệu Bitcoin tồn tại. Một Bitcoin có thể chia thành 100.000.000 Satoshi. Bitcoin là kỹ thuật số, vì vậy nó có tính bền vững. Bitcoin có thể di chuyển được như một tài sản tiền tệ. Vào tháng 4 năm 2020, một sàn giao dịch Crypto đã chuyển số tiền trị giá 1,1 tỷ đô la trong một giao dịch chỉ trong vài phút với chi phí giao dịch 0,68 đô la.¹⁶ Bitcoin có thể thay thế được, nhưng không hoàn toàn như vậy, bởi vì bất kỳ ai cũng có thể theo dõi chuyển khoản giữa các ví trên Blockchain.

Ở cấp độ cao, Bitcoin đạt được các thuộc tính trên thông qua tính phi tập trung.¹⁷ Cốt lõi của phi tập trung hóa là loại bỏ hoặc 'Killing' người trung gian nhưng không có định nghĩa nào được ngành công nghiệp đồng ý. Điều này đã gây tranh cãi trong một thời gian, đặc biệt là khi đề xuất luật. Thuật ngữ này cũng đã bị lạm dụng như một từ thông dụng tiếp thị và cay độc hơn như một màn khói cho hành vi sai trái trắng trợn của các thực thể tập trung đóng giả là những người theo chủ nghĩa lý tưởng Web3¹⁸. Điều này dẫn đến việc thành lập EDI 'Chỉ số phi tập trung Edinburgh', đây là một nỗ lực mang lại sự rõ ràng bằng cách phát triển một khuôn khổ để đánh giá sự phi tập trung của Blockchain. Chỉ số do Đại học Edinburgh¹⁹ phát triển, xem xét các biện pháp khách quan như phân phối tiền tệ, kho bạc, phân phối của nhà phát triển, mức độ phi tập trung của cơ chế đồng thuận, v.v. Thông tin thêm về EDI sẽ có ở phần sau.

Có và không có

Nếu chúng ta gặp nhau để uống cà phê ở một nước phát triển, bộ máy và cơ chế sẽ sẵn sàng để thực hiện thanh toán liền mạch. Mặc dù thanh toán bằng thẻ tín dụng là một trải nghiệm tiêu dùng dễ dàng và ngay lập tức, nhưng có rất nhiều hoạt động 'tập trung' đằng sau hậu trường. Chủ thẻ đã nhận được thẻ tín dụng của mình từ một tổ chức phát hành. Tổ chức phát hành này thường là một ngân hàng hoặc một số tổ chức tài chính, phát hành thẻ tín dụng thay mặt cho các mạng lưới lớn (Visa và Mastercard). Quán cà phê là thương gia trong trường hợp này. Sau đó, có một bên thứ tư tham gia, người mua lại. Đây thường là ngân hàng, chẳng hạn như JP Morgan Chase hoặc HSBC, nơi cửa hàng cà phê (người bán) có tài khoản.

Toàn bộ quy trình ủy quyền kể từ khi bạn quét thẻ để thanh toán sẽ mất vài giây. Không thành vấn đề nếu ngân hàng của bạn ở Ireland và ngân hàng của người bán ở Nhật Bản, dữ liệu được truyền nhanh chóng trong thời gian thực. Việc ủy quyền đầy đủ và chuyển giao giá trị giữa các ngân hàng có thể mất vài ngày làm việc phía sau hậu trường. Quá trình giải quyết được quy định chặt chẽ, tốn kém và không bao hàm.

Các ngân hàng sẽ không cung cấp các dịch vụ này nếu nó không mang lại lợi nhuận cho họ. Kết quả là có ba tỷ người 'không có tài khoản ngân hàng', chủ yếu ở các nước đang phát triển, nơi cơ sở hạ tầng như vậy không tồn tại. Những người này không có ngân hàng, không có các dịch vụ đi kèm như tín dụng hay bảo hiểm.

¹⁶Năm giao dịch bitcoin lớn nhất trong lịch sử, cryptovantage.com/news/here-are-the-5-biggest-bitcoin-transactions-in-history/

¹⁷ **Phi tập trung hóa** là quá trình mà các hoạt động của một tổ chức, đặc biệt là những hoạt động liên quan đến lập kế hoạch và ra quyết định, được phân phối hoặc ủy quyền từ một địa điểm hoặc nhóm trung tâm, có thẩm quyền.

¹⁸Web3 (còn được gọi là Web 3.0) là ý tưởng cho một phiên bản mới của World Wide Web kết hợp các khái niệm như phân cấp, công nghệ Blockchain và kinh tế dựa trên Token

¹⁹Chỉ số phi tập trung của Edinburgh, ed.ac.uk/informatics/blockchain/edi

Bất kỳ hình thức tiền nào cũng chỉ tốt khi mọi người tin tưởng vào nó. Niềm tin có thể thay đổi và bị ảnh hưởng bởi các sự kiện kinh tế lớn và nhỏ. Mọi người phải có niềm tin rằng số tiền họ sử dụng có giá trị gì đó, nó chứa đựng những đặc tính và đặc điểm mà họ mong đợi.

Vì vậy, đây là những gì Bitcoin đặt ra để đạt được. Đó đã và đang là một mục tiêu rất tham vọng và lý tưởng để cung cấp một hình thức kiểm tiền trực tuyến không phụ thuộc vào cơ quan trung ương phát hành nó. Mọi người phải có niềm tin vào nó như một hình thức tiền khả thi. Không có Cục Dự trữ Liên bang hoặc ngân hàng trung ương tham gia. Không ai chịu trách nhiệm, nhưng mọi người đều chịu trách nhiệm. Bitcoin đạt được điều này thông qua mật mã (được giải thích trong các chương sau) để duy trì 'trách nhiệm giải trình toàn diện', khái niệm thể hiện mọi người có thể 'kiểm tra bài tập về nhà của nhau'.²⁰ Mọi người có thể thấy và xem xét hồ sơ để đảm bảo (các) giao dịch là hợp lệ và không ai nói dối.

Một động lực khác đằng sau Bitcoin là sự bất mãn và bức tức. Mọi người mất niềm tin vào các tổ chức và cơ chế của họ. Genesis Block của Bitcoin đã nhúng vào trong nó một tham chiếu đến tiêu đề từ tờ báo *The Times* ngày 3 tháng 1 năm 2009, 'Thủ tướng trên bờ vực cứu trợ ngân hàng lần thứ hai', thể hiện sự thất vọng với các sự kiện vào thời điểm đó. Cuộc khủng hoảng tài chính năm 2008 chỉ là sự cố mới nhất trong chuỗi những thất bại của thể chế.

Hầu hết, nếu không muốn nói là tất cả các loại tiền pháp định²¹ cuối cùng sẽ mất giá trị và/hoặc sụp đổ. Quyền lực tham nhũng. Có rất nhiều cảm dỗ về chính trị và đạo đức để làm giảm giá trị đồng tiền vì những lợi ích ngắn hạn, với cái giá phải trả là những lợi ích lâu dài. Bạn không cần phải tìm kiếm các ví dụ trong lịch sử. Cộng hòa Weimar ở Đức, Venezuela, Argentina và Zimbabwe đều bị lạm phát phi mã.²² Những ảnh hưởng của cuộc khủng hoảng tài chính năm 2008 vẫn còn rất lớn và còn trầm trọng hơn bởi chi phí để giữ người có việc làm trong đại dịch Covid-19, với hàng nghìn tỷ đô la Mỹ được in ra từ không khí.

Blockchain là gì?

Bitcoin chạy trên một Blockchain. Tuy nhiên, Crypto chỉ là một ứng dụng của Blockchain. Nếu tạo và giao dịch Token kỹ thuật số thì chúng sẽ nằm trên sổ cái. Sổ cái này thường được so sánh với cơ sở dữ liệu. Một số người hoài nghi về Crypto tuyên bố, 'Đó chỉ là một cơ sở dữ liệu! Vấn đề là gì?' Blockchain có khả năng loại bỏ nhu cầu về cơ quan trung ương trong nhiều tình huống. Đó là một điểm bán hàng khá hấp dẫn. Bạn có thể coi Blockchain như một 'nhà môi giới tin cậy', nơi các bên riêng biệt, những người cần phải không tin tưởng lẫn nhau, cần hợp tác với nhau. Blockchain cũng thường được gọi là công nghệ sổ cái phân tán (DLT).²³

Vì vậy, nó là một loại cơ sở dữ liệu đặc biệt; nó lưu trữ một bản ghi các sự kiện và tất cả các loại siêu dữ liệu (dữ liệu về dữ liệu) liên quan đến các giao dịch. Thông thường, một bên trung gian như Revolut hoặc Ngân hàng Ireland sẽ xác minh và lưu giữ tất cả lịch sử ngân hàng của bạn thay mặt cho Visa hoặc Mastercard. Nếu bạn không còn tin tưởng họ nữa thì sao? Hoặc nếu bạn không muốn trả phí xử lý giao dịch? Đây là sự đổi mới cốt lõi của Bitcoin, nhằm cung cấp một hệ thống thay thế với Blockchain hoạt động như một 'nhà môi giới tin cậy'. Vì vậy, một cách ngắn gọn, Blockchain chỉ đơn giản là một sổ cái, nó lưu trữ các giao dịch và dữ liệu liên quan để bất kỳ ai cũng có thể xác minh khiêu nại.

Blockchain đạt được điều này bằng cách sử dụng các phương pháp mã hóa và giao thức đồng thuận.²⁴ Hãy coi đó là việc sử dụng toán học và khoa học máy tính để tạo một loại cơ sở dữ liệu đám mây. Một khi bản ghi được viết ra, nó không thể thay đổi, đó là sự thật không thể thay đổi. Vì vậy, một khi có một nhà môi giới tin cậy phi tập trung giúp loại bỏ nhu cầu về một cơ quan có thẩm quyền tập

²⁰Giải quyết sự đánh đổi ẩn của Blockchain, [youtube.com/watch?v=FSByg_sdjaM](https://www.youtube.com/watch?v=FSByg_sdjaM)

²¹ **Tiền định danh** đã được định nghĩa khác nhau là:

Bất kỳ khoản tiền nào được chính phủ tuyên bố là hợp pháp

Tiền do nhà nước phát hành không thể chuyển đổi theo luật thành bất kỳ thứ gì khác, cũng như không cố định về giá trị theo bất kỳ tiêu chuẩn khách quan nào

Tiền vô giá trị nội tại được sử dụng làm tiền vì nghị định của chính phủ

Một đối tượng về bản chất vô dụng dùng làm phương tiện trao đổi, còn được gọi là tiền ủy thác.

²²Trong kinh tế học, **siêu lạm phát** nhanh chóng làm xói mòn giá trị thực của đồng nội tệ khi giá của tất cả hàng hóa tăng lên. Điều này khiến mọi người giảm thiểu việc nắm giữ loại tiền đó khi họ chuyển sang các loại ngoại tệ ổn định hơn (tiền tệ cứng).

²³ **Công nghệ sổ cái phân tán (DLT)** là một giao thức hoặc cơ sở dữ liệu được đồng thuận chia sẻ và đồng bộ hóa trên nhiều trang web, tổ chức hoặc khu vực địa lý, được nhiều người truy cập và cho phép hoạt động an toàn của cơ sở dữ liệu kỹ thuật số phi tập trung.

²⁴Một **sự đồng thuận giao thức** là một cơ chế chịu lỗi được sử dụng trong các hệ thống Blockchain để đạt được thỏa thuận cần thiết về một giá trị dữ liệu hoặc một trạng thái mạng duy nhất giữa các quy trình phân tán hoặc hệ thống đa tác nhân, chẳng hạn như với Crypto.

trung thì nó có thể được sử dụng cho nhiều thứ khác. Nếu yếu tố con người có thể được loại bỏ bằng cách tạo ra tiền phi tập trung thì câu hỏi tiếp theo rõ ràng là 'có thể sử dụng các cơ chế tương tự để xác thực phi tập trung và bỏ phiếu phi tập trung không, v.v.?'

Các trường hợp sử dụng Blockchain

Bỏ phiếu có thể được ghi lại trên một Blockchain và không thể thay đổi, minh bạch, chống giả mạo, không tốn kém và thuận tiện (bỏ phiếu bằng ứng dụng dành cho thiết bị di động). Nền dân chủ có an toàn không khi một tỷ lệ cử tri cao như vậy không tin vào kết quả của một cuộc bầu cử? Nhà lãnh đạo của một quốc gia có thể đơn phương quyết định xâm chiếm một quốc gia khác mà không cần bỏ phiếu công khai không? Không cần vượt qua ngưỡng đa số cao?

Quyền tài sản hiện đang được quản lý bởi một số hình thức đăng ký trung tâm. Vì vậy, nếu bạn có quyền sở hữu hoặc chứng thư đối với một ngôi nhà, một tác nhân trung tâm phải duy trì cơ sở dữ liệu đó. Điều gì xảy ra nếu tác nhân đó có thể thao tác hoặc chỉnh sửa cơ sở dữ liệu đó? Điều gì xảy ra nếu có một sự thay đổi của chính phủ? Như khi ISIS đánh chiếm Syria, hay tình trạng hỗn loạn ở Ukraine. Nếu (những) tác nhân trung tâm chỉ có thể quyết định cập nhật lịch sử thì sau khi hòa bình trở lại, sẽ rất khó để quyết định ai thực sự sở hữu cái gì và ở đâu. Hàng triệu người trên khắp thế giới sống trên vùng đất tranh chấp. Một Blockchain có thể cung cấp một hệ thống công bằng hơn mà không cần sự hiện diện của cơ quan trung ương.

Cùng với Ngân hàng, **Xuất bản** là một trong những ngành lâu đời nhất. Mặc dù máy đọc sách điện tử và cửa hàng sách trực tuyến đã phá vỡ mô hình này ở một mức độ nào đó, hầu hết các công ty đều hoạt động theo cách tập trung. Bạn thường mua giấy phép để xem sách điện tử mà không cần sở hữu sản phẩm. *Book* (book.io) là một nền tảng mới sáng tạo nhằm mục đích phá vỡ không gian xuất bản bằng cách đưa sách ('tài sản mã hóa phi tập trung') vào Blockchain. Theo mô hình này, người mua sở hữu tài sản kỹ thuật số, có thể bán lại sách sau khi đọc và nhận phần thưởng 'đọc sách để kiếm tiền' để mua sách khác hoặc tương tác với nền tảng theo những cách khác, chẳng hạn như các buổi AMA (hỏi tôi bất cứ điều gì) với tác giả. Có rất nhiều ý nghĩa đối với độc giả, tác giả và nhà xuất bản được nêu trong White Paper của Book.²⁵

Chuỗi cung ứng là một cách sử dụng lý tưởng khác cho Blockchain. Trong đại dịch Covid-19, chuỗi cung ứng thiết bị bảo hộ cá nhân và vắc xin đóng vai trò quan trọng đối với hàng triệu người. Những hàng hóa này được xử lý bởi nhiều công ty. Mọi người đang đưa ra quyết định sinh tử dựa trên sự ổn định của các chuỗi cung ứng này và độ tin cậy của thông tin trong đó. Với công nghệ Blockchain, bạn không cần phải tin tưởng vào cơ quan trung ương hoặc bên thứ ba để đảm bảo rằng các bản ghi là chính xác.

Danh tính là tài sản cá nhân quan trọng cần thiết để nhiều dịch vụ hoạt động toàn diện cho tất cả mọi người. Theo truyền thống, bạn sẽ cần hộ chiếu hoặc bằng lái xe để kiểm tra nhận biết khách hàng (KYC) hoặc chỉ cần có điểm tín dụng để đủ điều kiện vay. Danh tính của nhiều người đã được liên kết với thông tin nhận dạng cá nhân (PII) trong các hồ sơ trực tuyến do Facebook, Google và những tập đoàn khổng lồ tập trung khác nắm giữ.

Ngày nay, danh tính của bạn phụ thuộc vào các bên thứ ba. Các thông tin sau đó được đưa ra về danh tính đó, một lần nữa bởi các cơ quan tín dụng và dịch vụ của chính phủ. Bạn không thực sự sở hữu danh tính của riêng bạn trực tuyến. Bạn không thể kiểm soát được, danh tính của bạn thường ở dạng danh tính trực tuyến thường được quản lý bởi những người trung gian và bên thứ ba, những người có khả năng thao túng hồ sơ vì lợi ích tốt nhất của họ. Danh tính phi tập trung có thể thực hiện được nhờ ID phi tập trung (DID)²⁶ và tài liệu DID,²⁷ giải quyết nhiều vấn đề trong số này và cung cấp quyền riêng tư cao hơn cho người dùng.

Tài chính phi tập trung (DeFi) nói về việc Blockchain cung cấp các dịch vụ ngân hàng truyền thống. Khách hàng ngân hàng ở các nước phát triển không quá cần đến DeFi. Ở các nước đang phát triển, nơi bạn có thể trả lãi suất lên tới 80% cho khoản vay tài chính vi mô, thật dễ hiểu tại sao DeFi bắt đầu được chấp nhận. Đó là một khía cạnh tiềm năng quan trọng của Blockchain và Crypto để đưa ba tỷ người 'không có tài khoản ngân hàng' vào nền kinh tế, phân phối hàng nghìn tỷ đô la tài sản kém thanh khoản.

Các ví dụ trên chỉ giải quyết một phần nhỏ của vấn đề. Có nhiều nền tảng khác mà chúng tôi sử dụng hàng ngày có thể được cải thiện bằng các giải pháp thay thế phi tập trung. Vì vậy, mục đích của những hệ thống này là tìm cách xây dựng chúng theo cách mà chúng

²⁵BOOK Token : Con đường dẫn đến phân cấp kiến thức,
book-token.medium.com/book-token-the-path-to-decentralize-knowledge-1ee651d657c3

²⁶ **Mã định danh phi tập trung (DID)** là một loại mã định danh cho phép nhận dạng kỹ thuật số phi tập trung, có thể kiểm chứng. DID đề cập đến bất kỳ chủ thể nào (chẳng hạn như người, tổ chức, sự vật, mô hình dữ liệu hoặc thực thể trừu tượng) được xác định bởi bộ điều khiển của DID. Trái ngược với các số nhận dạng liên kết, điện hình, DID đã được thiết kế để chúng có thể được tách rời khỏi các cơ quan đăng ký tập trung, nhà cung cấp danh tính và cơ quan cấp chứng chỉ.

²⁷ **Tài liệu DID** : một bộ dữ liệu mô tả chủ thể DID, bao gồm các cơ chế, chẳng hạn như khóa công khai mật mã, mà chủ thể DID hoặc người được ủy quyền DID có thể sử dụng để xác thực chính nó và chứng minh mối liên hệ của nó với DID. Một tài liệu DID có thể có một hoặc nhiều biểu diễn khác nhau.

làm việc cho những người nhỏ bé ở Châu Phi, giống như cách chúng làm cho chủ ngân hàng giàu có ngồi trong tòa nhà chọc trời ở Manhattan.

Những ngày đầu của Charles Hoskinson trong lĩnh vực Crypto

Charles Hoskinson là một doanh nhân công nghệ và nhà toán học có trụ sở tại Colorado. Ông đã nghiên cứu lý thuyết số giải tích trước khi khám phá ra mật mã. Ông ấy là người ủng hộ chiến dịch tranh cử tổng thống Hoa Kỳ năm 2008 của Ron Paul và thường nói một cách sôi nổi về cách mà ông ấy đã được Paul truyền cảm hứng.²⁸ Charles Hoskinson đã tham gia với Bitcoin từ những ngày đầu tiên.²⁹

Vì vậy, cuộc khủng hoảng tài chính năm 2008 đã xảy ra và sau đó tôi cứ nhìn thấy hết thất bại chính trị này đến thất bại chính trị khác. Tôi đã nói, phải có một cách khác và khi Bitcoin ra đời, đó là sự kết hợp của rất nhiều thứ mà tôi yêu thích. Tôi yêu thích phần mềm nguồn mở³⁰, mật mã và những thứ khoa học thực sự khó. Nhưng đồng thời, có một loại trào lưu chính trị ngấm của chủ nghĩa tư bản vô chính phủ và đạo đức tự do. Những thứ này tồn tại trong không gian Bitcoin và đã có một chính sách tiền tệ hoàn toàn khác. Tôi đã nói, 'ồ thật tuyệt, nó sẽ không bao giờ hoạt động... nhưng nó thực sự rất tuyệt', bởi vì đó là một trong những kiểu hệ sinh thái 'con gà và quả trứng' mà bạn nói, 'Chà, để nó hoạt động, rất nhiều người phải thực hiện nó một cách nghiêm túc, nhưng mọi người chỉ thực hiện nó một cách nghiêm túc nếu nó hoạt động. Làm thế nào để bạn có được khối lượng quan trọng đó?' Mọi người đều nói, 'Ồ, tiền giám phát không hoạt động được... Chúng ta đã thử điều đó vào thế kỷ 19, và đó là một thất bại thảm hại nên, vâng, thậm chí đừng nghĩ đến điều đó.' Tất cả các nhà kinh tế đều nói rằng Bitcoin sẽ chết.

Tôi là một nhà đầu cơ. Tôi đã mua rất nhiều Bitcoin và tôi cũng là một thợ đào. Tôi đã thiết lập AMD CrossFire và tôi đã sử dụng Slush Pool³¹ ... 1,2 Giga Hash sức mạnh khai thác, khá nhiều vào thời đó. Tôi đã kiếm được rất nhiều Bitcoin, nhưng tôi không quá coi trọng lĩnh vực này. Sau đó, vào khoảng năm 2013, tôi nhận thấy một điểm quan trọng; đó là sau cuộc khủng hoảng Síp³² khi chính phủ nói, 'Chúng tôi bắt đầu lấy tiền từ tài khoản ngân hàng của người khác để thanh toán mọi thứ là được.' Điều đó có thể sẽ xảy ra ở đây nếu chúng ta không quá cẩn thận, và lạ thay, Bitcoin đã tăng từ 4 đô la lên khoảng 263 đô la. Đó chỉ là một sự đột biến điên cuồng nên tôi đã nói rằng đây có thể sẽ là một điều lớn. Tôi cần phải lên tàu và nếu tôi không lên tàu, tôi sẽ bỏ lỡ nó.

Tôi có kỹ năng phân tích từ thế giới toán học và cũng đã lập trình rất nhiều. Vậy nên tôi có kỹ năng mã hóa và biết nhiều thứ vì có sự trùng lặp rất lớn giữa lý thuyết số và mã hóa. Sau đó tôi cũng có tất cả kiến thức về chính sách tiền tệ, vì vậy tôi rất hào hứng với lĩnh vực Crypto, nhưng tôi không biết ai cả. Tôi không biết phải làm gì trong lĩnh vực này.

Vì vậy, tôi đã nói chuyện với một vị giáo sư mà tôi biết và xin lời khuyên của ông ấy. Đó là Karl Gustafson ở Đại học Colorado Boulder... Karl nói, 'Charles, những người không thể làm... giảng dạy.' Vì vậy, tôi đã tạo một khóa học miễn phí trên Udemy về Bitcoin. Nó được gọi là 'Bitcoin hoặc cách tôi học cách ngừng lo lắng và yêu thích Crypto'³³ và tôi đã có 70.000 sinh viên, hàng nghìn Email và tôi đã gặp tất cả mọi người. Tôi đã gặp Roger Ver, Erik Voorhees và Andreas Antonopoulos và tất cả những tên tuổi lớn trong lĩnh vực Crypto, trước khi họ trở nên nổi tiếng.

²⁸Charles Hoskinson về Ron Paul đã truyền cảm hứng cho bạn như thế nào, youtube.com/watch?v=jqiLVxSA8w

²⁹Slot Leader Tập 1: Phỏng vấn Charles Hoskinson, youtube.com/watch?v=YT0PXYBEnuE, Charles Hoskinson: Tương lai của Blockchain ở Châu Phi, youtube.com/watch?v=m3eSEPrJ-1A

³⁰

Phần mềm **mã nguồn mở** (OSS) là phần mềm trong đó mã nguồn được phát hành theo giấy phép trong đó người giữ bản quyền cấp cho người dùng quyền nghiên cứu, thay đổi và phân phối phần mềm cho bất kỳ ai và cho bất kỳ mục đích nào.

³¹Hồ bơi bằng bùn, slushpool.com/home/

³²Khủng hoảng tài chính Síp, theatlantic.com/business/archive/2013/03/everything-you-need-to-know-about-the-cyprus-bank-disaster/274096/

³³

Charles Hoskinson và Brian Göss, 'Bitcoin hay cách tôi học cách ngừng lo lắng và yêu Crypto', udemy.com/course/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/

Bitcoin đã đi trước thời đại vào năm 2009. Nó cho phép tạo ra giá trị phi tập trung, được gửi và nhận như một Email. Không lâu sau đó mọi người muốn nhiều hơn nữa. Giống như khi trình duyệt Web phát triển từ trang tĩnh sang trang động, khả năng lập trình³⁴ được yêu cầu để đáp ứng nhu cầu cho nhiều ứng dụng hơn.

Cũng như giá trị di chuyển, cũng có một câu chuyện đằng sau mỗi giao dịch tài chính, bởi vì có các điều khoản và điều kiện. Ví dụ, nếu bạn muốn mua một cuốn sách trực tuyến, sẽ có một kiểm tra để xem bạn có đủ tiền hay không. Nếu bạn thanh toán số tiền cần thiết, sách sẽ được gửi tới Kindle của bạn khi và chỉ khi nhận được khoản thanh toán. Đây là một hợp đồng; đây là câu chuyện về một giao dịch đơn giản. Blockchain thế hệ đầu tiên là Bitcoin không được trang bị cho việc này. Hoskinson và những người khác như Vitalik Buterin, một người đồng sáng lập tương lai khác của Ethereum,³⁵ muốn cải thiện Bitcoin. Nhưng họ đã vấp phải sự phản đối và không dễ để đạt được thỏa thuận về cách tiến hành.

Đổi mới Invictus & BitShares

Hoskinson đã gặp nhiều người thông qua khóa học Udemy của mình. Một trong những học trò của ông là Li Xiaolai, người đã thành lập *Bitfund*.³⁶ Xiaolai đã đề nghị tài trợ để cùng nhau bắt đầu kinh doanh, vì vậy vào tháng 6 năm 2013, Hoskinson đã bắt đầu một chủ đề trên Bitcointalk có tên *Dự án Invictus*,³⁷ được đặt tên theo một bài thơ của [William Ernest] Henley. Bài đăng đã hỏi những gì có thể được thực hiện để khiến Bitcoin trở nên 'bất khả chiến bại' và giải quyết các vấn đề hiện có. Phản hồi tập trung vào hai nhu cầu của ngành. Đầu tiên là nhu cầu về một Stablecoin³⁸ để hạn chế khả năng biến động. Thứ hai là nhu cầu về một sản phẩm giao dịch phi tập trung.³⁹ Đây là khoảng thời gian Mt Gox⁴⁰ sụp đổ, vì vậy các sản phẩm giao dịch tập trung được coi là một điểm thất bại duy nhất. CH đã nói:⁴¹

Tôi nói 'được rồi, có cách nào chúng ta có thể kết hợp cả hai giải pháp lại với nhau không?'. Dan Larimer là người đầu tiên trả lời trên chủ đề này trong số tất cả mọi người. Anh ấy nói, 'Tôi đồng ý!'⁴² ...và anh ấy có bài nghiên cứu về BitShares.⁴³ Vì vậy, tôi đã đọc bài nghiên cứu, chúng tôi cùng nhau viết lại nó, bố của anh ấy (Stan) đã tham gia. Stan, Dan và tôi đã cùng nhau thành lập một công ty tên là Invictus. [...] nó bao gồm hai Larimers và một Hoskinson, vì vậy tôi đã mua lại.

34

Khả năng lập trình là khả năng thay đổi trong phần cứng và phần mềm; để chấp nhận một bộ hướng dẫn mới làm thay đổi hành vi của nó. Khả năng lập trình thường đề cập đến logic chương trình (quy tắc kinh doanh), nhưng nó cũng đề cập đến việc thiết kế giao diện người dùng, bao gồm các lựa chọn menu, Node và hộp thoại.

35

Ethereum là một blockchain mã nguồn mở phi tập trung với chức năng hợp đồng thông minh. Ether là Crypto gốc của nền tảng. Ethereum được hình thành vào năm 2013 bởi lập trình viên Vitalik Buterin. Những người sáng lập Ethereum khác bao gồm Gavin Wood, Charles Hoskinson, Anthony Di Iorio và Joseph Lubin.

³⁶ Bitfund, crunchbase.com/person/xiaolai-li

37

án Invictus, bitcointalk.org/index.php?topic=229315.0

38

Stablecoin là loại Crypto được thiết kế để giảm thiểu sự biến động về giá của nó, so với một số tài sản 'ổn định' hoặc một rổ tài sản. Một stablecoin có thể được chốt vào một loại Crypto khác, tiền định danh hoặc để trao đổi hàng hóa. Stablecoin có thể đổi được bằng tiền tệ, hàng hóa hoặc tiền định danh được cho là được hỗ trợ, trong khi những đồng tiền gắn liền với thuật toán được gọi là kiểu chủ quyền (không được hỗ trợ).

39

Sàn giao dịch phi tập trung (DEX) là dịch vụ trực tuyến ngang hàng (p2p) cho phép giao dịch Crypto trực tiếp giữa các bên quan tâm. ErgoDEX và WingRiders chỉ là hai trong số rất nhiều trên Cardano.

⁴⁰ **Mt Gox** là một sàn giao dịch bitcoin có trụ sở tại Tokyo. Ra mắt vào năm 2010, ba năm sau, nó đã xử lý 70% tất cả các giao dịch bitcoin trên toàn thế giới. Vào tháng 2 năm 2014, Mt Gox đã tạm ngừng giao dịch, đóng trang web và dịch vụ trao đổi, đồng thời nộp đơn xin bảo hộ phá sản từ các chủ nợ. Vào tháng 4 năm 2014, công ty bắt đầu thủ tục thanh lý.

⁴¹ Cardano, độc tính của Crypto và sự sụp đổ của thể chế, youtu.be/5-vsuU-OIhI?t=1405

⁴² Dan Larimer, iq.wiki/wiki/dan-larimer

⁴³ Lịch sử của BitShares, how.bitshares.works/vi/master/technology/history_bitshares.html

Cũng trong khoảng thời gian đó, Buterin trở nên thất vọng khi cố gắng mở rộng chức năng của Bitcoin bằng Colored Coins⁴⁴ và Mastercoin.⁴⁵ Việc cố gắng cải tiến Bitcoin được chứng minh là nỗ lực nhiều hơn giá trị của nó. CH đã nói:⁴⁶

Hãy trung thực ở đây, nó (Bitcoin) là số cái phức tạp nhất, thuật toán đồng thuận kém phức tạp nhất và nó tiêu thụ nhiều năng lượng hơn cả đất nước Thụy Điển hoặc Thụy Sĩ. Nó là ngôn ngữ tập lệnh phức tạp nhất, nó không hữu ích vào lúc này và nó đòi hỏi nỗ lực rất lớn để đổi mới.

Chúng tôi đã tạo ra Ethereum trên nền tảng của Colored Coins và Mastercoin. Chúng tôi không chỉ tạo ra Ethereum. Mọi người trong dự án đó đang cố gắng làm điều gì đó hữu ích với Bitcoin và họ không thể! Họ đã chi hàng triệu đô la, hàng tháng trời để làm những việc cơ bản như phát hành một tài sản, và rồi đột nhiên với Ethereum, bạn có thể làm điều đó với một vài dòng mã Code mà chúng ta có thể đặt trên chiếc áo thun f\$king!

Vì vậy, đây là điểm đối lập của tôi với Bitcoin. Vấn đề chính của tôi với Bitcoin là bản chất hẹp hòi của cộng đồng, đặc biệt là những người theo chủ nghĩa Maximalist,⁴⁷ không có khả năng thích ứng, phát triển và áp dụng công nghệ mới, ngay cả khi rõ ràng là công nghệ đó tốt như NIPoPoWs.⁴⁸ Thực tế là họ tấn công đã man những người đang đổi mới và gọi những người đó là tội phạm và những kẻ lừa đảo vì đã mạnh dạn thử những điều khác biệt.

Thực tế là chính sách tiền tệ không bao giờ có thể được cập nhật hoặc phát triển. Đó vừa là điều may mắn vừa là điều đáng tiếc. Đó là sự thiếu hiểu biết về khoa học, đặc biệt là khi nói đến bằng chứng cổ phần⁴⁹ và niềm tin rằng những gì họ đã làm là hoàn hảo. Đó là việc không bao giờ có thể được thay đổi và sự sùng bái cá nhân xung quanh sự sùng bái Satoshi. Điều đó thể hiện rằng nó là vàng kỹ thuật số, nó là một tiêu chuẩn, tôi nghĩ nó sẽ luôn có giá trị. Nó đã làm được rất nhiều điều tốt đẹp. Bitcoin là lý do tại sao tất cả chúng ta ở đây, đó là lý do tại sao tôi ở đây. Vì vậy, tôi sẽ không bao giờ nói đó là một dự án tồi. Tôi sẽ không bao giờ nói rằng không đáng để giữ BTC.

Nguồn gốc của Ethereum

Hoskinson đã gặp Anthony Di Iorio thông qua một liên hệ của anh ấy. Di Iorio đã điều hành Liên minh Bitcoin của CanADA (BAC)⁵⁰. Anh ấy đã hỏi về việc có thể sử dụng một số tài liệu giáo dục của Hoskinson trên Udemmy không. Hoskinson đồng ý và họ bắt đầu làm việc cùng nhau. Di Iorio đã chia sẻ White Paper của Vitalik Buterin. Hoskinson đã đọc nó và cung cấp phản hồi. White Paper đã trải qua nhiều lần nghiên cứu và điều chỉnh, nhóm hội tụ lại với nhau và kết quả là Ethereum được tạo ra, nó hiện được coi là Blockchain thế hệ thứ hai. Gavin Wood được Hoskinson ghi nhận là người đã xây dựng nó theo cách phù hợp và thực sự hiệu quả. Hoskinson đã giúp thiết lập cơ cấu pháp lý ban đầu. Điểm chính của Ethereum là thêm khả năng lập trình vào Crypto. CH đã nói:⁵¹

Vì vậy, từ năm 2009 đến khoảng năm 2013 là giai đoạn thử nghiệm của Bitcoin. Sau đó vào năm 2013, Bitcoin đã đạt khoảng một tỷ đô la, một ngành công nghiệp ổn định hình thành xung quanh nó. Tôi đã nói: 'Nó sẽ không đi đâu cả.' Bitcoin ở đây để

44

Đồng xu màu là một loại phương pháp để liên kết tài sản trong thế giới thực với địa chỉ trên mạng Bitcoin. Ví dụ có thể là chứng thư mua nhà, cổ phiếu, trái phiếu hoặc hợp đồng tương lai.

45

Omni (trước đây là **Mastercoin**) là một loại tiền kỹ thuật số và giao thức truyền thông được xây dựng trên Blockchain bitcoin. Đây là một trong những nỗ lực nhằm kích hoạt các chức năng tài chính phức tạp trong Crypto.

46

Phỏng vấn Charles Hoskinson 'Ivan on Tech', youtu.be/dWW_RRgAxKI?t=3500

47

Người **theo chủ nghĩa tối đa** là người có quan điểm cực đoan và không sẵn sàng thỏa hiệp.

48

Proof-of-Work không tương tác (NIPoPoWs) là các chuỗi độc lập ngắn mà chương trình máy tính có thể kiểm tra để xác minh rằng một sự kiện đã xảy ra trên Blockchain dựa trên bằng chứng công việc mà không cần kết nối với mạng Blockchain và không cần tải xuống tất cả các tiêu đề khối. Ví dụ: những bằng chứng này có thể minh họa rằng một khoản thanh toán bằng Crypto đã được thực hiện.

⁴⁹ **Bằng chứng cổ phần (PoS)** là một loại thuật toán mà mạng Blockchain Crypto nhằm mục đích đạt được sự đồng thuận. Trong Crypto dựa trên PoS, người tạo Block tiếp theo được chọn thông qua các kết hợp khác nhau giữa lựa chọn ngẫu nhiên và số tiền đã cam kết (tức là **tiền đặt cược**). Ngược lại, thuật toán của Crypto dựa trên **bằng chứng công việc (PoW)** chẳng hạn như bitcoin sử dụng khai thác; nghĩa là giải các câu đố chuyên sâu về tính toán để xác thực các giao dịch và tạo Block.

50

Liên minh Bitcoin CanADA, coindesk.com/bitcoin-alliance-launches-canADA

51

The Erica Show EP9 - Charles Hoskinson, youtu.be/l35h0xW47-Y?t=904

tồn tại. Tuy nhiên, vấn đề với Bitcoin là nó mù, điếc và câm. Ý tôi muốn nói là bạn không thể làm được gì nhiều với nó ngoài việc di chuyển Bitcoin đi khắp nơi. Bạn không thể phát hành tiền tệ của riêng mình; bạn không thể viết ứng dụng.

Nó tương tự như khi JavaScript được đưa vào trình duyệt Web. Trước đó, trình duyệt Web đã hoạt động, nhưng các trang Web rất buồn tẻ và tĩnh. JavaScript cho phép YouTube, Facebook và Google cung cấp nội dung động với Video và thương mại điện tử. Tương tự như vậy, với Bitcoin, bạn có thể gửi, nhận và hiển thị các giao dịch, bạn có thể sử dụng siêu dữ liệu cho những điều thú vị nhưng DApp thì không thể, ICO⁵² thì không thể, bạn không thể phát hành Token tùy chỉnh của riêng mình... tất cả đều thú vị và các tính năng hữu ích hiện đang tạo nên bối cảnh DeFi của ngành.

Trớ trêu thay, Ethereum đã được công bố tại hội nghị Bitcoin Bắc Mỹ vào tháng 1 năm 2014. Bitcoin vừa tăng từ 100 đô la lên 1.000 đô la, vì vậy sự kiện này rất náo nhiệt và ồn ào. Chiếc áo phông Ethereum đầu tiên được sản xuất cho hội nghị có mã nguồn ở mặt sau để phát hành Token của riêng bạn. Thật khó xử khi làm điều đó với Mastercoin và Colored Coins. Trớ trêu thay, Ethereum cũng được sinh ra từ sự chán nản, thất vọng với sự cứng nhắc của Bitcoin và kinh nghiệm kém của nhà phát triển. Bằng cách đưa ngôn ngữ lập trình vào Blockchain, điều này cho phép các hợp đồng thông minh⁵³ được viết để có các giao dịch có thể tùy chỉnh. Vì vậy, bây giờ khi Alice gửi giá trị cho Bob, các điều khoản và điều kiện có thể được đưa vào trong giao dịch, phù hợp với nhu cầu cụ thể của cô ấy.



Hình 1: Áo phông Ethereum khi ra mắt vào tháng 1 năm 2014

Hoskinson muốn thành lập một công ty phù hợp, hoạt động vì lợi nhuận và có các thỏa thuận dành cho người sáng lập.⁵⁴ Sau khi xem xét cấu trúc và phương hướng của dự án, anh ấy lo lắng rằng không ai có động lực để tiếp tục tham gia sau khi dự án được triển khai. Anh ấy muốn 'còng tay vàng', lễ phục và những thứ tiêu chuẩn mà một công ty bình thường sẽ có. Đã có sự bất đồng khi Buterin muốn

⁵²

Cung cấp tiền xu ban đầu (ICO) là một phương tiện gây quỹ cộng đồng thông qua việc sử dụng Crypto, có thể là nguồn vốn cho các công ty mới thành lập và các dự án phần mềm nguồn mở. Trong một ICO, một tỷ lệ phần trăm Crypto mới phát hành được bán cho các nhà đầu tư để đổi lấy đầu thầu hợp pháp hoặc các loại Crypto khác như bitcoin hoặc ether.

⁵³

Hợp đồng thông minh là một giao thức máy tính nhằm tạo điều kiện thuận lợi, xác minh hoặc thực thi việc đàm phán hoặc thực hiện hợp đồng. Hợp đồng thông minh lần đầu tiên được đề xuất bởi Nick Szabo vào năm 1996. Những người ủng hộ hợp đồng thông minh cho rằng nhiều loại điều khoản hợp đồng có thể được thực hiện một phần hoặc toàn bộ tự thực thi hoặc cả hai. Mục đích của hợp đồng thông minh là cung cấp bảo mật vượt trội so với luật hợp đồng truyền thống và giảm các chi phí giao dịch khác liên quan đến hợp đồng.

⁵⁴

Thỏa thuận của những người sáng lập là một hợp đồng mà những người sáng lập công ty ký kết để điều chỉnh các mối quan hệ kinh doanh của họ. Thỏa thuận đưa ra các quyền, trách nhiệm, trách nhiệm pháp lý và nghĩa vụ của mỗi người sáng lập.

nó vẫn là một dự án mã nguồn mở. Hoskinson lập luận rằng nếu tất cả mọi người đều được trả trước thì sẽ không có động lực để cam kết lâu dài. Mọi chuyện không suôn sẻ, Hoskinson rời đi vào tháng 6/2014.

Không có cái tôi, hay những cuốn sách được viết vào thời điểm đó. Nhóm chỉ muốn tạo ra "thứ gì đó thú vị và hay ho" để mở rộng chức năng của Crypto. Ethereum đã đạt được thành công lớn. Thuật ngữ 'The Flipping' thậm chí còn được đặt ra. Nó đề cập đến thời điểm giả định về việc Ethereum vượt qua Bitcoin để trở thành Crypto lớn nhất. Vấn đề chính là khả năng mở rộng, nó không thể xử lý hàng triệu người dùng và hàng tỷ giao dịch. Bitcoin chỉ có thể xử lý 7 giao dịch mỗi giây, đối với Ethereum là 10-20.

Quản trị cũng là một vấn đề. Nó trở thành nạn nhân của sự thành công của chính nó. Mỗi khi có một cuộc tranh luận lớn, thay vì giải quyết nó một cách thân thiện, lại có những Hardfork lộn xộn.⁵⁵ Ethereum chia làm hai, một nửa tạo thành Ethereum Classic. Tương tự như vậy, Bitcoin đã có một phe chia tách hình thành Bitcoin Cash.⁵⁶ Vấn đề về tính bền vững xuất hiện. Sau khi hết tiền ICO cho một dự án, hoặc các quỹ đầu tư mạo hiểm của nó cạn kiệt, ai sẽ tham gia và tài trợ cho mọi thứ? Những lỗ hổng này trong thiết kế của Ethereum sẽ được giải quyết bằng các Blockchain thế hệ thứ ba như Cardano và Polkadot (được thành lập bởi Gavin Wood).

Nền tảng Ethereum được chia thành hai phiên bản: 'Ethereum Classic' (ETC) và 'Ethereum' (ETH). Trước khi phân tách, Token đã được gọi là Ethereum. Sau khi chia tách, các Token mới⁵⁷ giữ tên Ethereum (ETH) và các Token cũ được đổi tên thành Ethereum Classic (ETC). Ethereum Classic được hình thành do sự bất đồng với Ethereum Foundation liên quan đến Hardfork DAO.⁵⁸ Một số người muốn hoàn trả tiền. Những người khác hợp nhất theo triết lý 'mã Code là luật', từ chối Hardfork và tách thành Ethereum Classic. Người dùng đã sở hữu ETH trước đợt Hardfork DAO đã sở hữu một lượng ETC tương đương sau đợt phân tách.

Thời gian tại Ethereum. CH đã nói:⁵⁹

Tôi không tưởng tượng được Vitalik lại đánh giá quá cao về tôi, và nó là như vậy. Thực tế là chúng tôi có những bất đồng triết học rất lớn về cách vận hành mọi thứ. Khi tôi ở đó, tôi đã nói, 'hãy xem nếu chúng tôi đang lấy tiền của người khác, chúng tôi phải đặt số tiền đó vào một cấu trúc tạo ra trách nhiệm giải trình. Hơn nữa, chúng tôi phải "còng tay vàng" cho những người sáng lập và giữ họ trung thành với dự án, bởi vì có quá nhiều người sáng lập. Có tám nhà sáng lập và nếu họ không bị ràng buộc vào một thứ gì đó, thì điều sắp xảy ra là tất cả họ sẽ chạy trốn và tạo ra những dự án kinh doanh của riêng mình.'

Đó là những gì họ đã làm, Anthony Di Iorio đã làm 'Decentral', Gavin Wood đã làm PolkaDot⁶⁰ và Parity, tôi đã làm Cardano. Bấy giờ số tám người đã rời đi. Hơn nữa cơ chế khuyến khích đã thiết lập để chúng tôi được trả tiền thưởng cho người sáng lập trước, mà tôi đã không nhận, bảy người còn lại đã... về cơ bản nếu các dự án thành công, halelujah, nếu nó thất bại, xin chào... nhưng bạn đã nhận được phần thưởng tối đa ngay từ đầu, trong khi ở mô hình tài chính vốn cổ phần, bạn phải xây dựng giá trị theo thời gian và bạn có một nhánh đầu tư mạo hiểm giúp bạn chịu trách nhiệm.

Tôi đã thấy có sự bất đồng cơ bản về chiến lược kinh doanh và tầm nhìn thực hiện. Tôi cảm thấy một mô hình vì lợi nhuận bằng tiền VC, để xây dựng giao thức, sẽ có ý nghĩa hơn rất nhiều và sau đó khi giao thức được hoàn thành, tách nó ra và để một nền tảng quản lý vận hành, đó có lẽ là một cách tiếp cận tốt hơn nhiều.

55

Hard fork : đại tu toàn bộ giao thức của mạng, dẫn đến sự thay đổi luồng hoạt động từ mô hình này sang mô hình khác. Cardano có một cơ chế duy nhất, được gọi là bộ kết hợp hard fork, để thực hiện các hard fork với sự gián đoạn tối thiểu. Xem Chương 4.

56

Bitcoin Cash là một loại Crypto được tạo ra vào giữa năm 2017. Một nhóm các nhà phát triển muốn tăng giới hạn kích thước khối của Bitcoin đã chuẩn bị thay đổi mã. Sự thay đổi, được gọi là hard fork, có hiệu lực vào tháng 8 năm 2017 và Crypto bị chia làm hai. Tại thời điểm chia tách, bất kỳ ai sở hữu bitcoin cũng sở hữu cùng số lượng đơn vị Bitcoin Cash.

57

Token Crypto là tài sản kỹ thuật số được xây dựng trên Blockchain Crypto. Blockchain là một sổ cái kỹ thuật số lưu trữ thông tin trong các Block được liên kết với nhau. Thông tin này có thể là hồ sơ giao dịch hoặc các chương trình chính thức hoạt động trên Blockchain, được gọi là hợp đồng thông minh. 'Xu' của Crypto là một Token. Trên thực tế, đó là mã kỹ thuật số xác định từng phân số, có thể được sở hữu, mua và bán.

⁵⁸DAO là một tổ chức tự trị phi tập trung (DAO) được ra mắt vào năm 2016 trên Ethereum. Sau khi huy động được số ether (ETH) trị giá 150 triệu USD thông qua việc bán Token, The DAO đã bị tấn công do các lỗ hổng trong cơ sở mã của nó.

⁵⁹Charles Hoskinson về việc rời Ethereum, youtube.com/watch?v = AWSI78nh6jc

60

Polkadot là một mạng blockchain được xây dựng để kích hoạt Web3, một mạng internet phi tập trung và công bằng, nơi người dùng kiểm soát dữ liệu cá nhân của họ và thị trường phát triển thịnh vượng nhờ hiệu quả và bảo mật của mạng. Polkadot là dự án hàng đầu của Web3 Foundation.

Đó là một khía cạnh, các khía cạnh khác là lý do giữa các cá nhân. Trong sáu tháng, chúng tôi đã sống như những kẻ lập dị trong ngôi nhà ở Thụy Sĩ và anh ấy đang đi du lịch khắp thế giới, giao tiếp rất kín kẽ, và chứng hoang tưởng và sợ hãi bắt đầu hình thành. Hiện đã có ba cuốn sách viết về vấn đề này. Những cuốn sách đó vẽ nên một bức chân dung rằng có một nhóm người rất thông minh, có hai liều lượng trí tuệ và một nửa kỹ năng xã hội, bao gồm cả tôi. Khi bạn đặt họ vào một tình huống căng thẳng kiểu Hippie, nó sẽ tạo ra rất nhiều thuyết âm mưu, nỗi sợ hãi và những thứ tương tự.

Thành thật mà nói, có quá nhiều người sáng lập. Vì vậy, tại một số thời điểm, bạn phải hợp nhất và thực sự có hai con đường khác nhau mà Vitalik có thể chọn, anh ấy ngồi ở giữa, anh ấy có thể chọn bên kinh doanh, đó là điều tôi, Anthony Di Iorio và Joe Lubin đang ủng hộ hoặc anh ta có thể chọn thế giới công nghệ, Crypto tử hỗn loạn, phi lợi nhuận, bình đẳng, trọng dụng nhân tài, mã nguồn mở.

Cardano ra đời

Bây giờ với tư cách là một doanh nhân Crypto, Hoskinson cảm thấy vỡ mộng, nhưng một cánh cửa khác đang mở ra. CH đã nói:⁶¹

Sau Ethereum, tôi đã nghỉ một thời gian, khoảng sáu tháng và tôi thực sự sẽ rời khỏi ngành. Tôi đã thực hiện TED Talk⁶² và tôi nói 'đây là điểm xuất phát của tôi, tôi sẽ nói cho mọi người biết lĩnh vực này nói về điều gì và sau đó tôi sẽ đi làm việc khác.'

Bài nói chuyện của Hoskinson tập trung vào vấn đề gần gũi nhất với trái tim ông, giúp mọi người có thể tiếp cận tài chính một cách phổ biến. Ông cho rằng điểm chính của công nghệ Blockchain là về danh tính kinh tế. Nó nên hướng tới ba tỷ người trên thế giới không có quyền truy cập vào tài khoản ngân hàng, những người không có hệ thống danh tính cũng như hệ thống tài sản nên họ sống trong cảnh nghèo đói vĩnh viễn với tư cách là nạn nhân của hoàn cảnh địa chính trị.

Cuộc nói chuyện đã được đón nhận nồng nhiệt. Jeremy Wood, người từng quản lý các hoạt động tại Ethereum và giữ liên lạc với Hoskinson, đã mời ông đến Nhật Bản để nói về một liên doanh mới với các doanh nhân địa phương. Các cuộc đàm phán diễn ra trong vài tháng về cấu trúc được đề xuất, cách huy động vốn. Họ đã xem xét lộ trình không được sử dụng của Hoskinson từ Ethereum. Cuối cùng, một thỏa thuận đã đạt được với các nhà đầu tư Nhật Bản để bắt đầu 'Ethereum của Nhật Bản', đó chính là Cardano.

Cardano Foundation (cardanofoundation.org), hiện có trụ sở tại bang Zug của Thụy Sĩ, được thành lập như một cơ quan quản lý và là người giám sát hợp pháp của thương hiệu. Người Nhật đã thành lập một công ty mà sau này trở thành Emurgo (emurgo.io), nhánh thương mại hóa của Cardano. Vào năm 2015, Hoskinson và Wood đã đồng sáng lập Input Output Global (iog.io), trước đây là IOHK (iohk.io). IOG là bộ phận phát triển và khoa học cho Cardano. Phần còn lại của năm 2015 tập trung vào phát triển giao thức và thuê một nhóm các nhà khoa học. Đợt mở bán cho cộng đồng⁶³ của Cardano diễn ra từ cuối năm 2015 đến tháng 1 năm 2017, được quản lý bởi một công ty Nhật Bản có tên là Attain⁶⁴, người đã tổng hợp tất cả các khoản tiền. IOG có hợp đồng 5 năm để xây dựng Cardano.

Ngay từ đầu, sứ mệnh của họ đã rõ ràng: 'sử dụng các đổi mới ngang hàng để cung cấp dịch vụ tài chính cho ba tỷ người chưa có'. IO tin vào nguyên tắc nền tảng của 'sự gián đoạn theo tầng' - ý tưởng là hầu hết các cấu trúc hình thành hệ thống tài chính, quản trị và xã hội của thế giới vốn không ổn định. Do đó, những nhiễu loạn nhỏ có thể gây ra hiệu ứng gợn sóng cấu hình lại toàn bộ hệ thống về cơ bản. Công ty cam kết xác định và phát triển công nghệ để ngăn chặn những nhiễu loạn này nhằm thúc đẩy một trật tự công bằng và minh bạch hơn.

Toàn bộ năm 2016 được dành cho khoa học và nghiên cứu. Nhóm nhỏ ban đầu với những ý tưởng lớn là Charles Hoskinson, Giám đốc điều hành; Jeremy Wood, giám đốc chiến lược; Nikos Benteinis, giám đốc điều hành; Chikara Wakae, giám đốc truyền thông; Richard Wild, giám đốc thiết kế; và Tomas Vrana, nhà phát triển Full Stack.

Ngày 4 tháng 11 năm 2020. IOG là gì? CH đã nói:⁶⁵

⁶¹

Cardano, độc tính của Crypto và sự sụp đổ của thể chế, youtu.be/5-vsuU-OIhI?t=21

⁶²

Tương lai sẽ phi tập trung | Charles Hoskinson | TEDxBermuda, youtube.com/watch?v=97ufCT6lQcY

⁶³

một **đám đông** là một loại gây quỹ cộng đồng phát hành Token được lưu trữ trên thiết bị của người dùng. Các Token có thể hoạt động giống như một phần cổ phiếu và được mua và bán ("Token vốn chủ sở hữu") hoặc chúng có thể thanh toán cho các dịch vụ khi dịch vụ hoạt động ("Token người dùng").

⁶⁴

Cardano CrowdSale, nasdaq.com/articles/iohk-launches-cardano-blockchain-ADA-now-trading-on-bittrex-2017-10-02

⁶⁵

Với Input Output, điều tôi muốn làm là kết hợp hai thứ cùng một lúc. Thứ nhất, tôi muốn có một công ty có triết lý mạnh mẽ về cách xây dựng sản phẩm. Tôi đã nói, 'những sản phẩm này được sinh ra như một phương pháp khoa học và bằng chứng. Chúng ta cần tuân theo các phương pháp chính quy'⁶⁶ và phần mềm dựa trên bằng chứng. Chúng ta cần tuân theo một cách tiếp cận học thuật nghiêm ngặt để phát triển giao thức'.

Đó là một chuyện, còn chuyện khác là loại sản phẩm tôi muốn xây dựng. Những gì tôi tin vào là triết lý của sự gián đoạn theo tầng. Về cơ bản, điều đó có nghĩa là bạn giống như quân Domino đầu tiên, bạn giống như viên sỏi nhỏ trên đỉnh đồi mà khi bạn đẩy nó, nó sẽ tạo ra một trận tuyết lở. Vì vậy, bạn xây dựng một sản phẩm, bạn nhúng vào đó tất cả các quy trình và quy tắc này, rồi sau một thời gian, có thể là vài năm... bạn thực sự có thể rời đi và sản phẩm sẽ tự phát triển.

Quay trở lại năm 2015, IOG đã lùi lại và hỏi một câu hỏi rất đơn giản, đó là 'Vấn đề sau thành công của Ethereum là gì? Nếu nó hoạt động thì điều gì sẽ diễn ra với ngành công nghiệp này?'

Họ đã xác định ba vấn đề không thể tránh khỏi nếu Ethereum thành công.

- 1) **Khả năng mở rộng.** Có vấn đề đối với cách Bitcoin và Ethereum được thiết kế. Vitalik Buterin về cơ bản đã thừa nhận điều này bằng cách xây dựng ETH 2 (Ethereum 2.0),⁶⁷ đó là Ethereum chỉ có thể đạt đến một khả năng nhất định và tại thời điểm đó, nó trở nên không thể kiểm soát được. Các giao dịch trở nên quá đắt đỏ, hệ thống phình to. Cần có một ngăn xếp giao thức khác để khi bạn có được người dùng, mức hiệu suất sẽ nhất quán. Nó cần phải hoạt động tương tự như các hệ thống tập trung như Facebook hay Amazon, nơi nó có thể xử lý hàng triệu đến hàng tỷ người. IOG đã tìm cách tìm ra cách giải quyết vấn đề đó.
- 2) **Khả năng tương tác.** Thế giới được tạo thành từ nhiều tiêu chuẩn, khác nhau đối với các ngành và khu vực pháp lý khác nhau. Có khả năng các hệ thống tài chính truyền thống sẽ không biến mất, vì vậy tốt nhất là hợp tác với chúng để tạo cầu nối nếu có thể. Các tiêu chuẩn Wi-Fi sẽ không bao giờ hoạt động nếu chúng bị ràng buộc bởi các nhà sản xuất. Nếu điện thoại di động Huawei của bạn chỉ có thể nói chuyện với bộ định tuyến Huawei, thì việc chuyển vùng ở bất cứ đâu là không thực tế. Lý do Wi-Fi hoạt động là vì nó hoạt động với tất cả mọi người bất kể nhà sản xuất thiết bị di động của bạn. Tương tự, giống như tiền và danh tính của bạn, cuộc sống sẽ dễ dàng hơn nếu thông tin có thể lưu chuyển liên mạch giữa hàng nghìn loại Crypto và hệ thống kế thừa truyền thống.
- 3) **Quản trị,** đôi khi được gọi là tính bền vững. Bitcoin và Ethereum đều gặp sự cố khi mở rộng quy mô. Không có cơ chế quản trị để thúc đẩy sự thay đổi. Khi chúng tăng lên hàng triệu người dùng, cuối cùng không thể đưa ra các quyết định gây tranh cãi mà không làm hỏng dự án. Ví dụ: Bitcoin đã có cuộc tranh luận về 'Khối lớn so với SegWit' dẫn đến việc nó bị chia thành hai, Bitcoin Cash và Bitcoin. Ethereum cũng có biến động tương tự với vụ Hack "The DAO". Sự chia rẽ này là một trở ngại lớn đối với việc chấp nhận của chính phủ, việc chấp nhận Fortune 500 và việc chấp nhận chính thống bởi vì người dùng hàng ngày. Các tập đoàn sợ đầu đá nội bộ và Hardfork nhiều hơn mỗi khi xảy ra tranh cãi hoặc quyết định khó khăn.

Quản trị không phải là một chủ đề hấp dẫn trên Twitter về Crypto,⁶⁸ nhưng nó được cho là quan trọng nhất đối với khả năng tồn tại lâu dài của dự án. Ai quyết định cách thay đổi hệ thống? Cập nhật nên được thực hiện như thế nào và khi nào? Một Blockchain cần phải có một kính hiển vi tầm ngắn cho những mối nguy hiểm gần và hiện tại, và một kính viễn vọng tầm xa cho những thách thức kỹ thuật ở phía trước. Ví dụ, nếu tất cả đều thất bại khi tranh luận về việc thay đổi tham số, thì điều gì sẽ xảy ra khi máy tính lượng tử xuất hiện? Không thể tránh khỏi ai đó trong vài thập kỷ tới sẽ sản xuất một máy tính lượng tử thương mại hóa có thể phá vỡ mật mã. Chúng tôi biết nó sẽ đến, vậy làm thế nào để một giao thức non trẻ đối phó với điều này? IOG đã lên kế hoạch kháng lượng tử từ những ngày đầu của dự án và sẽ triển khai nó khi thích hợp.

Chương trình Erica EP9 - Charles Hoskinson, CEO của Input Output, youtu.be/l35h0xW47-Y?t=611

⁶⁶

Trong khoa học máy tính, **các phương pháp chính thức** là một loại kỹ thuật dựa trên toán học cụ thể để đặc tả, phát triển và xác minh hệ thống phần mềm và phần cứng. Việc sử dụng các phương pháp chính thức cho thiết kế phần mềm và phần cứng được thúc đẩy bởi kỳ vọng rằng, giống như trong các ngành kỹ thuật khác, việc thực hiện phân tích toán học phù hợp có thể đóng góp vào độ tin cậy và độ bền của thiết kế.

⁶⁷

Ethereum 2.0 là phiên bản mới của Blockchain Ethereum sẽ chuyển sang cơ chế đồng thuận bằng chứng cổ phần, chuyển từ cơ chế bằng chứng công việc ban đầu, hiện có.

⁶⁸

Crypto Twitter là một thuật ngữ để mô tả cộng đồng và tiểu văn hóa Twitter bao quanh các chủ đề về Blockchain và Crypto.

Ngoài ra còn có các vấn đề về tài trợ với Crypto thế hệ thứ nhất và thứ hai. Có một bi kịch về⁶⁹ kịch bản chung khi hầu hết mọi người đồng ý rằng cơ sở hạ tầng thiết yếu hoặc các bản cập nhật quan trọng là bắt buộc nhưng không có cơ chế nào để đăng ký hoặc phê duyệt tài trợ cho phát triển.

Từ năm 2015 đến 2017, IOG đã có một bước lùi lớn, chỉ nghiên cứu học thuật và đặt câu hỏi cơ bản, không quyết định bất cứ điều gì. Họ hỏi, 'Blockchain là gì?' Họ thậm chí còn không quyết định bằng chứng công việc hay bằng chứng cổ phần. Họ chỉ cố gắng tạo ra các định nghĩa, mô hình và hiểu đủ cơ sở để có thể tiếp cận các vấn đề này một cách hợp lý.

Giáo sư Aggelos Kiaysis⁷⁰ đã tham gia vào năm 2016. IOG đã phát minh ra một giao thức bằng chứng cổ phần mới có tên là *Ouroboros* và đã chứng minh rằng nó có thể thực hiện được và an toàn. Họ đã phát minh ra toàn bộ các giao thức có khả năng tương tác như NIPoPoW (Non-Interactive Proofs of Proof-of-Work)⁷¹ và các giao thức Sidechain, cũng như ngăn xếp quản trị. Nhân viên của IOG đã viết và xuất bản hơn 170 bài nghiên cứu học thuật (số lượng mới nhất) được trích dẫn vô số lần trong ngành, thường là của các đối thủ cạnh tranh. Nhân viên của IOG đã xuất hiện tại hầu hết các hội nghị Mật mã học lớn trên thế giới.

Cùng với việc tìm kiếm những học giả giỏi nhất, IOG cũng đã liên hệ với các nhóm kỹ sư giỏi nhất tại các công ty như WellTyped, Tweag và Runtime Verification, dành cho những người như Duncan Coutts và Edsko de Vries, những người có công việc bao gồm bộ tổ hợp Hardfork được thảo luận sau. IOG (IOHK) nổi bật trên Google Scholar, nhiều người trong số họ là giáo sư hoặc có trích dẫn cấp giáo sư, chẳng hạn như Dionysis Zindros, Kevin Hammond và người khác.

IOG sử dụng các phương pháp chính quy để triển khai bảo mật nghiêm ngặt trên lý thuyết và trong quá trình phát triển. Tất cả các tài liệu nghiên cứu của IOG đều trải qua một số hình thức đánh giá ngang hàng. Mục tiêu cuối cùng luôn là triển khai mã Code đảm bảo cao, sử dụng các kỹ thuật tương tự mà người ta sẽ thấy với Shinkansen⁷² hoặc trong động cơ máy bay, nơi lỗi hệ thống dẫn đến cái chết của con người. Những kỹ thuật này được áp dụng cho các giao thức, kỹ thuật và phát triển của IOG, để thu được mức độ tin cậy cao về chất lượng của mã Code nhằm tránh các sự cố như tấn công DAO, Hack Ví Parity hoặc Hack Solana Wormhole.⁷³

IOG đã chọn một trong những ngôn ngữ lập trình theo định hướng khoa học nhất là Haskell,⁷⁴ được sử dụng và kiểm tra kỹ lưỡng từ những năm 1980. Giáo sư Phil Wadler,⁷⁵ một trong những người tạo ra Haskell, đã lãnh đạo quá trình phát triển Plutus⁷⁶ cùng với Giáo sư Manuel Chakravarty, Giáo sư Elias Koutsoupias và Giáo sư Simon Thompson. IOG đã tài trợ cho nghiên cứu và phát triển tại Phòng thí nghiệm Công nghệ Blockchain tại Đại học Edinburgh, Đại học Athens, Viện Công nghệ Tokyo, Đại học Stanford và Đại học Wyoming. Plutus và Marlowe⁷⁷ đã được ra mắt tại PlutusFest vào tháng 12 năm 2018 bởi nhóm nghiên cứu tiên tiến này.

⁶⁹

Bi kịch của tài sản chung là một tình huống trong hệ thống chia sẻ tài nguyên, trong đó những người dùng cá nhân, hành động độc lập theo lợi ích cá nhân của họ, hành xử trái ngược với lợi ích chung của tất cả người dùng, bằng cách làm cạn kiệt hoặc làm hỏng tài nguyên đó thông qua hành động tập thể của họ.

⁷⁰

Giáo sư Aggelos Kiayias, iohk.io/en/team/aggelos-kiayias

⁷¹

Sidechain là một **Blockchain** chạy song song với Blockchain chính. Token có thể được chuyển và đồng bộ hóa giữa chuỗi chính và chuỗi phụ.

⁷²

Shinkansen là tuyến đường sắt cao tốc ở Nhật Bản. Ban đầu, nó được xây dựng để kết nối các vùng xa xôi của Nhật Bản với thủ đô Tokyo, nhằm hỗ trợ tăng trưởng và phát triển kinh tế.

⁷³

Solana's Wormhole Hack Phân tích sau khi chết,
extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13

⁷⁴

Haskell là một ngôn ngữ lập trình thuần chức năng, có mục đích chung, được gõ tĩnh, với suy luận kiểu và đánh giá lười biếng. Được thiết kế cho các ứng dụng giảng dạy, nghiên cứu và công nghiệp, Haskell đã đi tiên phong trong một số tính năng của ngôn ngữ lập trình.

⁷⁵

Giáo sư Phil Wadler, iohk.io/en/team/philip-wadler

⁷⁶

Plutus là bộ công cụ lập trình để tạo hợp đồng thông minh Cardano.

⁷⁷

Marlowe là một ngôn ngữ lập trình được tạo riêng để tạo các hợp đồng thông minh tài chính. Nó bị giới hạn trong các ứng dụng tài chính và dành cho các chuyên gia tài chính hơn là các lập trình viên.

Dòng thời gian Cardano

Tháng 9 năm 2015	Crowdsale tài trợ phát triển và ngân quỹ.
Tháng 8 năm 2017	Nghiên cứu Ouroboros được chấp nhận tại Crypto 17 ⁷⁸
Tháng 9 năm 2017	Khởi chạy Byron
Tháng 12 năm 2018	Ra mắt Plutus và Marlowe tại PlutusFest
Tháng 12 năm 2018	Nghiên cứu Sidechains ⁷⁹ được xuất bản
Tháng 12 năm 2019	Shelley Incentivized Testnet (ITN) ⁸⁰
Tháng 3 năm 2020	Byron Reboot, sự kiện bộ tổ hợp HardFork đầu tiên
Tháng 7 năm 2020	Khởi chạy Shelley (phi tập trung)
Tháng 3 năm 2021	Phi tập trung hoàn toàn (d=0)
Tháng 9 năm 2021	Khởi chạy Goguen (hợp đồng thông minh, Plutus V1)
Tháng 9 năm 2022	Phát hành Vasil (Plutus V2)
Tháng 11 năm 2022	Ra mắt <i>Thời đại Voltaire</i> tại ScotFest
Tháng 2 năm 2023	Nâng cấp SECP

Lưu ý rằng không có White Paper trong suốt thời gian này, thay vào đó IOG tập trung vào việc xây dựng các nguyên tắc. Trong chương tiếp theo, chúng ta sẽ đi sâu vào các chi tiết kỹ thuật hơn và giải thích sơ đồ đặt tên và lộ trình của Cardano.

Hoskinson thường than thở khi được giới thiệu là cựu đồng sáng lập Ethereum. Ông ấy muốn được biết đến với công việc của mình tại IOG.⁸¹

Tôi có sáu năm (vào năm 2021) tại IOG và tôi chỉ có sáu tháng lịch sử tại Ethereum. Điều đáng thất vọng là Ethereum là dự án lớn và Cardano vẫn chưa hoàn thiện, vì vậy Ethereum là thứ mà mọi người biết đến tôi. Vì vậy, họ chỉ có sáu tháng dữ liệu, trong đó tôi có khả năng hạn chế trong việc tác động và kiểm soát mọi thứ. Tôi chỉ là một trong số rất nhiều người. Sau đó tôi là CEO của IOG, vì vậy tôi đã có khả năng tại công ty của mình để chứng minh tầm nhìn sẽ như thế nào..

Rất nhiều người thường hỏi điều gì sẽ xảy ra với Ethereum nếu bạn ở lại? Vì vậy, chúng tôi đã chạy thử nghiệm đó. Nó sẽ trông rất giống Cardano, cách chúng tôi xây dựng Cardano, phương pháp chúng tôi thực hiện, đó chính xác là Ethereum sẽ trông như thế nào. Tương tự, họ hỏi điều gì sẽ xảy ra với Ethereum nếu Gavin Wood đóng góp nhiều hơn. Chúng tôi đã chạy thử nghiệm đó rồi, chúng ta có PolkaDot.

⁷⁸

Crypto 17, iacr.org/conferences/crypto2017/

⁷⁹

Gazi1, Kiayias, Zindros (2018), 'Các chuỗi phụ bằng chứng cổ phần', eprint.iacr.org/2018/1239.pdf

⁸⁰

Dynal Patel, 'Incentivized Testnet : nó là gì và làm thế nào để tham gia', iohk.io/en/blog/posts/2019/10/24/incentivized-testnet-what-is-it-and-how-to-get-có-liên-quan

⁸¹

Charles Hoskinson về việc rời Ethereum, youtube.com/watch?v=AWSI78nh6jc

Chương 2: Cardano là gì?

'Chúng tôi cho bạn biết chúng tôi sẽ làm gì, chúng tôi viết nó ra, chúng tôi bắt tay vào thực hiện và sau đó chúng tôi nói với bạn rằng chúng tôi đã làm điều đó, và chúng tôi cho bạn thấy bằng chứng và bằng chứng... đó là cách làm việc của Paul Halmos'

- Charles Hoskinson



Alex Hammer

@AlHammer



Trả lời @IOHK_Charles

Charles, vui lòng giải thích đề xuất giá trị thiết yếu của Cardano trong một câu.



Charles Hoskinson

@IOHK_Charles



Trả lời @AlHammer

Cardano là một nền tảng mở tìm cách cung cấp danh tính kinh tế cho hàng tỷ người thiếu nó bằng cách cung cấp các ứng dụng phi tập trung để quản lý danh tính, giá trị và quản trị

Cardano là một nền tảng Blockchain bằng chứng cổ phần thuộc thể hệ thứ ba và hoàn toàn phi tập trung. Đây là Blockchain đầu tiên xuất hiện từ đặc điểm khoa học và phương pháp nghiên cứu. ADA (A hoặc ADA là 'mã đánh dấu' được sử dụng trên các sản phẩm giao dịch Crypto) là loại Crypto đầu tiên được xây dựng trên Cardano.

Ngày 12 tháng 12 năm 2020. Làm thế nào để bạn giải thích dự án Cardano và sứ mệnh của nó trong vài phút cho một người không tham gia vào ngành Crypto hoặc thậm chí là lĩnh vực tài chính? CH.⁸²

Cách giải thích đơn giản nhất là thế giới đang trải qua quá trình nâng cấp, nơi chúng ta sẽ chuyển từ một hệ thống phân chia sang một hệ thống thống nhất. Ngay bây giờ, chúng ta có hai hệ thống, hệ thống thế giới phát triển và thế giới đang phát triển. Hệ thống thế giới phát triển có ngân hàng, bảo hiểm, tín dụng; nó có danh tính, bạn có thể kinh doanh trực tuyến. Bạn có thể xây dựng niềm tin với mọi người, quản lý rủi ro và có thể phát triển sự giàu có. Vì vậy, bất kỳ người nào sinh ra ở một quốc gia phát triển trên thế giới, nếu họ làm việc chăm chỉ, đều có cơ hội tốt để đạt được điểm mà họ có thể nghỉ hưu và có một cuộc sống tốt đẹp. Điều đó có nghĩa là một cuộc sống mà họ có thức ăn, nước uống, chỗ ở, v.v. Họ có thể theo đuổi những thứ khiến họ hạnh phúc và còn dư đủ để khi họ trở nên yếu đuối và dễ bị tổn thương, khoản tiết kiệm của họ có thể trang trải cho những lần ốm đau đó.

Khi bạn nhìn vào thế giới đang phát triển, không phải do lỗi của họ, họ sống trong những hệ thống mà việc tạo ra của cải là rất khó khăn. Ngay cả khi bạn có một ít trong số đó, bạn cũng không thể bảo hiểm và phòng ngừa cho nó, vì vậy khi một sự kiện xảy ra, có thể là chiến tranh hoặc sự kiện tự nhiên như bão hoặc sóng thần, chúng sẽ bị xóa sổ. Vì vậy, thế giới đang nâng cấp để chúng ta có một hệ thống thống nhất nơi tất cả 7-8 tỷ người sống dưới một hệ thống điều hành tài chính. Vì vậy, danh tính của bạn có thể tương tác và phổ biến. Bạn có thể nhận được một khoản vay bất kể bạn là ai và đang ở đâu. Bạn có thể nhận được bảo hiểm bất kể bạn đang ở đâu. Bạn có thể kinh doanh với bất kỳ ai trên thế giới một cách thoải mái.

Quan điểm của Cardano là thừa nhận điều này phải được thực hiện theo nguyên tắc. Vì vậy, chúng tôi đang cố gắng đạt được điều gì? Chúng tôi đang cố gắng đẩy quyền lực ra rìa, và đặt bạn chịu trách nhiệm về tiền của chính mình, đặt bạn chịu trách nhiệm về danh tính của chính mình, đặt bạn chịu trách nhiệm về tiếng nói của chính mình và trao cho bạn quyền quản lý. Vì vậy, khi chúng ta đến với hệ thống phổ quát đó, chúng ta sẽ đến với một hệ thống nguyên tắc, cởi mở, phi tập trung không thể đồng chọn. Rất kiên cường trước những người cố gắng đến và can thiệp vào nó, và rồi đột nhiên những người giàu

nhất thế giới, Jeff Bezos của thế giới, sẽ sử dụng cùng một hệ thống như những người nghèo nhất thế giới và cả hai sẽ có một hệ thống tốt hơn hệ thống ra đời trước nó, trong cả hai hệ thống cũ đó. Đó là những gì chúng tôi đang cố gắng hoàn thành.

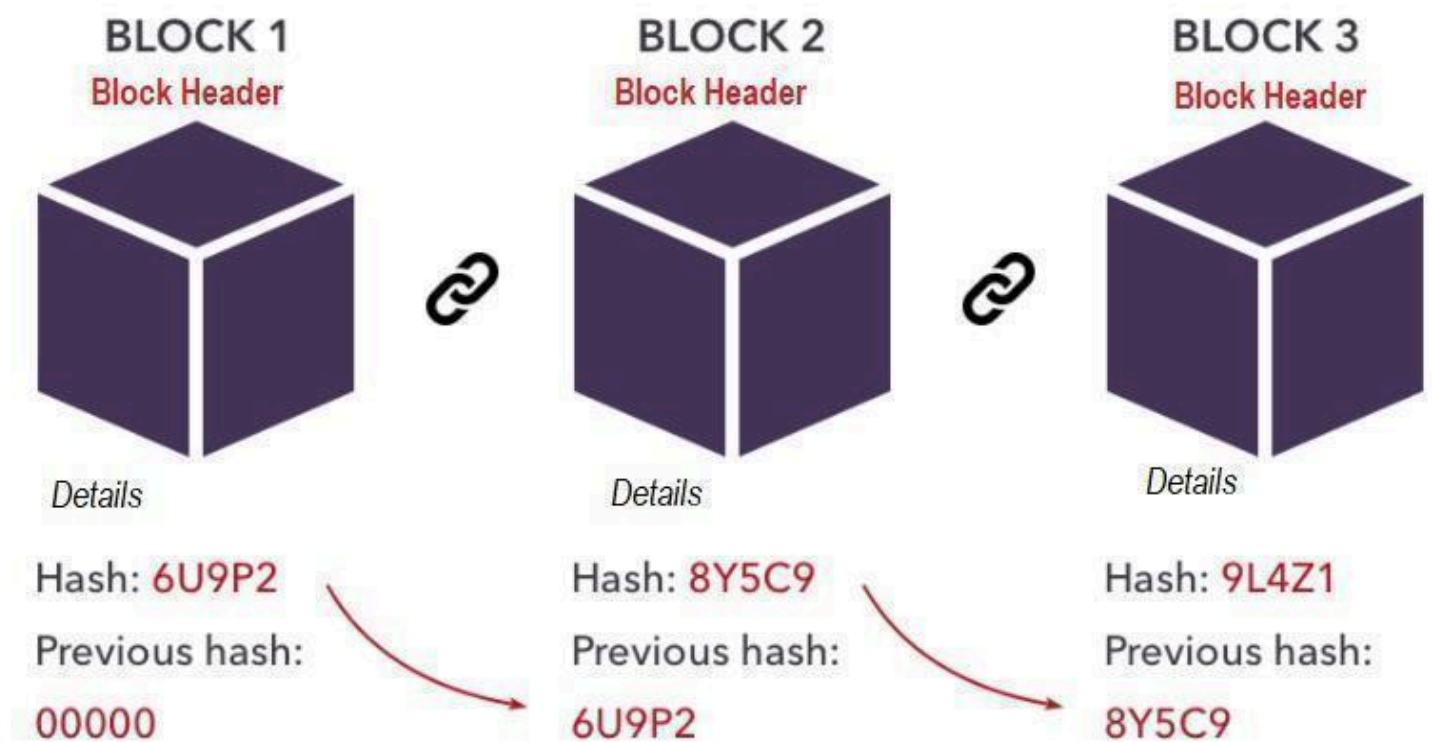
Khái niệm cơ bản

Như đã thảo luận trong Chương 1, Blockchain có một số tính năng của cơ sở dữ liệu, trong trường hợp này là sổ cái kế toán,⁸³ được sao chép và phân phối cho tất cả người dùng Blockchain. Blockchain bao gồm một mạng lưới các Node⁸⁴ được liên kết qua Internet lưu trữ dữ liệu hoặc các tệp kỹ thuật số có giá trị trong các Block.⁸⁵ Các giao dịch xác minh các Block này, sau đó được kết nối thành một chuỗi theo thứ tự thời gian. Chi tiết của các giao dịch này được ghi lại mãi mãi trong Block và không thể thay đổi.

Công nghệ Blockchain còn được gọi là công nghệ sổ cái phân tán (DLT), cung cấp cấu trúc dữ liệu phi tập trung và có thể truy cập cho các tệp và tài liệu kỹ thuật số. Dữ liệu giao dịch và thanh toán tài chính, cũng như các loại thông tin khác như hồ sơ thương mại và thông tin quản lý chuỗi cung ứng, có thể được đưa vào.

Một Blockchain phi tập trung độc lập với các công ty, tổ chức hoặc trung gian kiểm soát tập trung vì nó lưu giữ dữ liệu theo cách phi tập trung. Điều này làm tăng khả năng hiển thị của lưu trữ và quản trị dữ liệu. Một khía cạnh cơ bản của Blockchain là các bản ghi được lưu trữ cố định, có nghĩa là chúng không thể bị sửa đổi, làm sai lệch hoặc phá hủy mà không làm cho chuỗi bản ghi bị phá vỡ.

Một Blockchain có thể được ví như một cuốn sổ ghi chép vĩnh viễn, với mỗi trang đóng vai trò là một thiết bị lưu trữ dữ liệu.



Hình 2: Infographic về các Block Blockchain được liên kết bởi Hash Pointer⁸⁶

⁸³

Sổ cái : sổ cái phân tán (còn được gọi là sổ cái dùng chung hoặc được gọi là công nghệ sổ cái phân tán) là sự đồng thuận của dữ liệu kỹ thuật số được sao chép, chia sẻ và đồng bộ hóa về mặt địa lý trên khắp các trang web, quốc gia hoặc tổ chức. Không có quản trị viên trung tâm hoặc lưu trữ dữ liệu tập trung.

⁸⁴

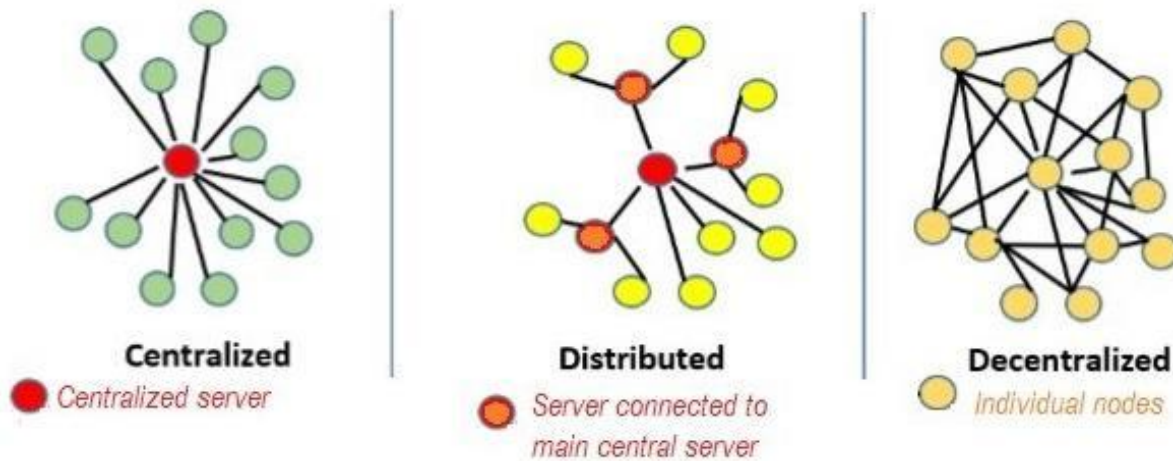
Trong các mạng viễn thông, một Node là điểm phân phối lại hoặc điểm cuối giao tiếp. Định nghĩa của một Node phụ thuộc vào lớp mạng và giao thức được đề cập. Node mạng vật lý là một thiết bị điện tử hoạt động được gắn vào mạng và có khả năng tạo, nhận hoặc truyền thông tin qua kênh liên lạc.

⁸⁵

Chặn : bản ghi các giao dịch mạng gần đây. Mỗi khối cũng bao gồm dữ liệu cần thiết để quản lý Blockchain, chẳng hạn như bản ghi được mã hóa của khối trước đó. Mỗi khối hoàn thành được theo sau bởi việc tạo Block tiếp theo để tiếp tục chuỗi.

⁸⁶

Mạng có thể được cấu hình theo nhiều cách (xem Hình 3):



Hình 3. Ba loại cấu trúc mạng.

Với các Blockchain phi tập trung, người dùng có thể giao dịch trực tiếp ngang hàng với nhau mà không cần phải thông qua một hệ thống kiểm soát trung tâm

- Hệ thống tập trung: trong hầu hết các trường hợp, một máy chủ trung tâm duy nhất quản lý tất cả dữ liệu và hành động. Điều này làm tăng khả năng xảy ra lỗi tại một điểm duy nhất đồng thời thể hiện rằng tổ chức kiểm soát (thường là ngân hàng hoặc cơ quan chính phủ) đưa ra tất cả các quyết định.
- Hệ thống phân tán: những hệ thống này phụ thuộc vào một số Node máy chủ, mỗi Node phục vụ một phần trong tổng số người dùng.
- Hệ thống phi tập trung: tất cả dữ liệu và hồ sơ giao dịch được mã hóa và lưu giữ trên một mạng gồm các Node và thiết bị đầu cuối được liên kết, độc lập, thay vì trên một máy chủ. Điều này đảm bảo tính bảo mật, minh bạch và độc lập với các tổ chức tập trung.

Ngoài việc cung cấp cơ sở dữ liệu an toàn và bất biến, Blockchain còn đóng vai trò là môi trường chức năng để chuyển tiền mặt, tạo tiền kỹ thuật số và xử lý các giao dịch phức tạp, bao gồm hợp đồng thông minh (thỏa thuận kỹ thuật số tự động).

Crypto là gì?

Crypto là một tài sản kỹ thuật số được ghi trên sổ cái và nó thường được dùng làm hình thức thanh toán cho các sản phẩm hoặc dịch vụ.

Trong một môi trường phi tập trung, sổ cái Blockchain đóng vai trò là công nghệ nền tảng cho Crypto. Để cho phép đúc (tạo) Crypto và để bảo vệ cũng như xác thực quyền sở hữu Crypto và hồ sơ chuyển tiền, các hệ thống Blockchain sử dụng các phương pháp mã hóa nghiêm ngặt. Chính phủ hoặc tổ chức tài chính tập trung không có ảnh hưởng đến cấp độ giao thức của Crypto. Họ chắc chắn có thể ảnh hưởng đến giá một cách gián tiếp thông qua tin đồn, đe dọa (ban hành) pháp luật. Giá trị của Crypto, liên kết đến dữ liệu trong thế giới thực, cung và cầu thị trường là những gì định nghĩa nó.

Băm **mật mã** là một thuật toán ánh xạ dữ liệu có kích thước tùy ý (thường được gọi là 'thông báo') thành một chuỗi bit có kích thước cố định ('giá trị băm', 'băm' hoặc 'thông báo tóm tắt'). Đó là một hàm một chiều, nghĩa là một hàm thực tế không thể đảo ngược. Các hàm băm mật mã là một công cụ cơ bản của mật mã hiện đại.

Khi truyền thanh toán bằng Crypto, địa chỉ⁸⁷ được sử dụng. Mỗi địa chỉ là một mã định danh duy nhất được tạo thành từ một chuỗi số và chữ cái lấy từ khóa công khai của mỗi người dùng.

Mỗi số cái Blockchain có Crypto riêng cung cấp 'nguồn nhiên liệu' để vận hành hệ thống. Loại Crypto này là 'tài sản gốc' đối với Blockchain vì nó tương tác trực tiếp với Blockchain. Tài sản gốc sáng lập của Cardano, ADA (A), là đơn vị thanh toán chính của Blockchain. ADA có thể được sử dụng để thanh toán phí, gửi tiền và là loại tiền tệ duy nhất mà phần thưởng⁸⁸ được trao. Điều này sẽ thay đổi với Sidechains (được thảo luận sau trong Chương 8).

Mệnh giá ADA nhỏ nhất là một Lovelace. 1.000.000 Lovelace = 1 ADA. Vì các giao dịch được tính đến sáu chữ số thập phân, nên dễ dàng chia một ADA thành các phân số.

Token gốc là gì?

Cardano cho phép người dùng tạo (đúc) hoặc xóa (đốt) Token. Đây là những tài sản kỹ thuật số, mỗi tài sản được đúc cho một mục đích cụ thể. Trên Cardano, Token là tài sản gốc, chúng tương tác trực tiếp với Blockchain thay vì được tạo bằng hợp đồng thông minh. Điều này nghĩa là người dùng, nhà phát triển và công ty có thể tạo Token phản ánh dấu ấn giá trị trên Blockchain Cardano (như được xác định bởi cộng đồng, trạng thái thị trường hoặc tổ chức tự quản). Token có thể thay thế được (có thể thay thế) hoặc không thể thay thế (duy nhất) và nó có thể được sử dụng làm đơn vị thanh toán, phần thưởng, tài sản giao dịch hoặc người nắm giữ thông tin.

Tại sao Cardano lại khác biệt?

Cardano là một Blockchain bền vững được thiết kế để bảo mật, có thể mở rộng và tương tác.⁸⁹ Điều quan trọng là Ouroboros, giao thức đồng thuận bằng chứng cổ phần của Cardano, đã được chứng minh là cung cấp sự đảm bảo tính bảo mật giống như các Blockchain bằng chứng công việc như Bitcoin.

Cardano được mô tả là một Blockchain 'thể hệ thứ ba':

- thể hệ đầu tiên: Bitcoin, một Blockchain bằng chứng công việc;
- thể hệ thứ hai: Ethereum mang đến khả năng lập trình và hợp đồng thông minh cho Blockchain. Tuy nhiên, đó là thiếu sót bởi vì, giống như Bitcoin, ban đầu nó sử dụng một hệ thống bằng chứng công việc lãng phí một lượng lớn năng lượng để giải các câu đố toán học ngày càng phức tạp không có mục đích nào ngoài việc xác thực các giao dịch. Nó cũng không có khả năng mở rộng, vì vậy càng nhiều giao dịch được thực hiện thì Blockchain càng chậm và chi phí thực hiện giao dịch càng đắt. Vào tháng 9 năm 2022, Ethereum cuối cùng đã chuyển đổi từ bằng chứng công việc sang bằng chứng cổ phần, nhưng đây chỉ là một bước trên lộ trình Ethereum 2.0 dài và phức tạp. Phí giao dịch (phí Gas) vẫn cao và có các tính năng kém hấp dẫn như cơ chế phạt⁹⁰ và sự không chắc chắn xung quanh việc cổ phần của người dùng bị khóa vô thời hạn.⁹¹

⁸⁷

Địa chỉ : một cấu trúc dữ liệu được sử dụng để thể hiện các loại thông tin khác nhau trong đầu ra giao dịch. Để xác định giữa các mạng khác nhau (ví dụ : mạng chính hoặc mạng thử nghiệm), mỗi địa chỉ có thể phân biệt mạng và bằng chứng về quyền sở hữu (người sở hữu đầu ra giao dịch). Các tùy chọn ủy quyền và tham chiếu tập lệnh cũng được bao gồm trong một số địa chỉ .

⁸⁸

Phần thưởng : một số tiền có trong mỗi khối mới được mạng thanh toán cho các bên liên quan.

⁸⁹

Được tạo ra bởi Vitalik Buterin , người dẫn đầu việc tạo ra Ethereum, '**bộ ba bất khả thi về Blockchain** ' đặt ra những thách thức mà các nhà phát triển phải đối mặt trong việc tạo ra một Blockchain có khả năng mở rộng, phi tập trung và an toàn mà không ảnh hưởng đến bất kỳ khía cạnh nào. Các Blockchain buộc phải đánh đổi giữa ba khía cạnh sau:

- phân cấp: tạo ra một hệ thống Blockchain không dựa vào điểm kiểm soát trung tâm.
- khả năng mở rộng: khả năng của một Blockchain để xử lý số lượng giao dịch ngày càng tăng.
- bảo mật: khả năng của một Blockchain hoạt động như mong đợi và tự bảo vệ khỏi các cuộc tấn công, lỗi và các vấn đề không lường trước khác.

⁹⁰ **Chém** là một cơ chế được sử dụng bởi một số giao thức PoS (nhưng không phải Cardano) để ngăn chặn hành vi có hại và khiến người xác nhận có trách nhiệm hơn. Chúng giúp giữ an toàn cho mạng bởi vì, không cắt giảm các hình phạt, trình xác thực có thể sử dụng cùng một Node để xác thực các Block trên nhiều chuỗi hoặc làm như vậy trên chuỗi sai.

⁹¹ những người đặt cược Ethereum sẽ có thể rút ETH của họ, beincrypto.com/nobody-knows-when-ethereum-stakers-will-be-able-to-draw-their-eth/

- thể hệ thứ ba: Cardano sử dụng bằng chứng cổ phần, sử dụng lượng năng lượng nhỏ, để cung cấp tất cả các khả năng của Ethereum. Nó cũng được thiết kế để phát triển, hoạt động với các Blockchain khác và được tích hợp kho bạc cũng như cấu trúc để quản lý thay đổi trong tương lai.

Các kỹ sư đã viết mã nguồn mở cho Cardano quyết định rằng cách tốt nhất để tạo ra các hệ thống phần mềm có độ đảm bảo cao mà người dùng có thể tin tưởng để xử lý các loại tiền kỹ thuật số là sử dụng các phương pháp chính quy như thống số kỹ thuật toán học, kiểm tra dựa trên thuộc tính và bằng chứng. Cardano được thiết kế bằng các phương pháp chính quy để đảm bảo chắc chắn tính chính xác về chức năng của các thành phần cơ bản của hệ thống.

Một trong những nguyên lý trung tâm của Cardano là bảo mật. Haskell, một ngôn ngữ lập trình hàm an toàn, được sử dụng trong quá trình phát triển của nó. Một ngôn ngữ lập trình hàm như Haskell thúc đẩy việc sử dụng các hàm thuần túy⁹² trong thiết kế hệ thống, dẫn đến một kiến trúc dễ dàng được kiểm tra độc lập. Hơn nữa, các khả năng phức tạp của Haskell cung cấp những cách mạnh mẽ để đảm bảo tính chính xác của mã Code, chẳng hạn như dựa trên việc triển khai dựa trên các thông số kỹ thuật chính thức và có thể thực thi được, thử nghiệm kỹ lưỡng dựa trên thuộc tính và thử nghiệm mô phỏng.

Cardano phải có khả năng phát triển và tương tác với các hệ thống tài chính truyền thống để cung cấp cơ sở hạ tầng mạnh mẽ trên quy mô toàn cầu. Mặc dù thực tế là Cardano được xây dựng với lưu ý đến hiệu quả tài nguyên, nhưng quy mô vẫn là một vấn đề, giống như đối với tất cả các giao thức Blockchain. Để giải quyết vấn đề tăng trưởng, các nhà nghiên cứu của IOG đã phát triển Hydra,⁹³ một giao thức có thể chạy trên Cardano⁹⁴. Hydra cho phép xử lý giao dịch và hợp đồng thông minh ngoài chuỗi chính. Hydra và nhiều giải pháp khả năng mở rộng khác được thảo luận trong Chương 8.

Các kỹ thuật hiệu suất đã được sử dụng để kiểm tra lựa chọn thiết kế nào đã giúp IOG đạt được khả năng phục hồi, hiệu suất và khả năng mở rộng. Một mục tiêu quan trọng khác của kiến trúc Cardano là ngăn chặn sự tập trung hóa bằng cách sử dụng các biện pháp khuyến khích kinh tế khuyến khích sự phi tập trung. Stake Pool (Stake Pool)⁹⁵ có động cơ kinh tế để mở rộng ngay khi chúng được tạo ra, vì vậy, điều quan trọng là làm cho nó trở nên kém hấp dẫn hơn đối với Stake Pool trở nên quá lớn. Tuy nhiên, cần phải cân bằng vì một số lượng hạn chế các Pool lớn sẽ tiết kiệm chi phí hơn so với một số lượng lớn các Pool nhỏ.

Một sự cân bằng đã được thực hiện bằng cách thay đổi công thức phần thưởng. Trong một hệ thống cơ bản, tổng số phần thưởng của Pool chỉ đơn giản là tỷ lệ thuận với số cổ phần của nó, do đó cổ phần càng lớn thì càng tốt. Với Cardano, nếu một Pool thu được nhiều cổ phần hơn ngưỡng nhất định ($1/k$, trong đó k là tham số có thể điều chỉnh), khoản thanh toán của nhóm sẽ không tăng nữa. Pool được cho là đã bão hòa⁹⁶ và việc ủy quyền thêm cổ phần sẽ không làm tăng phần thưởng. Kết quả là k Pool có quy mô gần bằng nhau nếu mọi người hành động vì lợi ích cá nhân của họ để tối đa hóa phần thưởng.

Khả năng tương tác, hoặc khả năng giao tiếp với các hệ thống khác, là một thành phần kiến trúc cơ bản của Cardano. Việc sử dụng Sidechain là một trong những đổi mới của Cardano. Thiết kế có nghĩa là hệ thống có thể được chia nhỏ và nó cho phép khả năng tương tác bên trong nền tảng Blockchain. Một Sidechain giữ và thao tác dữ liệu ngoài chuỗi chính. Nhiều Sidechain có thể hoạt động đồng thời và nếu một bên bị lỗi, phần còn lại của hệ thống vẫn hoạt động. Kết quả là Blockchain có độ chắc chắn và đáng tin cậy hơn. Tài sản có thể được di chuyển giữa các Blockchain riêng biệt chạy theo các quy tắc, quy trình hoặc ngôn ngữ riêng biệt, cũng như các phương thức truy cập mạng khác nhau bằng cách sử dụng Sidechain.

⁹²

Một **hàm thuần túy** là một hàm có các thuộc tính sau: thứ nhất, giá trị trả về của nó giống nhau đối với cùng một đối số (không thay đổi với biến tính cục bộ, biến không cục bộ, đối số tham chiếu có thể thay đổi hoặc luồng đầu vào từ thiết bị đầu vào-đầu ra); thứ hai, đánh giá của nó không có tác dụng phụ (không có đột biến của biến tính cục bộ, biến không cục bộ, đối số tham chiếu có thể thay đổi hoặc đầu vào và đầu ra).

⁹³

MMT Chakravarty, S Coretti, M Fitzi, P Gazi, P Kant, A Kiayias và A Russell (2020) 'Hydra: các kênh trạng thái đăng cấu nhanh'. eprint.iacr.org/2020/299.pdf

⁹⁴

Trong hệ sinh thái phi tập trung, **Lớp 1** đề cập đến chính giao thức Blockchain. **Lớp 2** đề cập đến một công nghệ hoạt động trên blockchain để cải thiện khả năng mở rộng và hiệu quả của nó. Ví dụ: Bitcoin là mạng Lớp 1 và Mạng Lightning là Lớp 2 để cải thiện tốc độ giao dịch. Hydra là một giao thức lớp 2 được xây dựng trên Cardano, lớp 1.

⁹⁵

Nhóm cổ phần: một Node máy chủ tạo Block, ổn định, tổng hợp cổ phần của một số bên liên quan (trong trường hợp của Cardano, chủ sở hữu ADA) thành một thực thể hoặc nhóm duy nhất.

⁹⁶

Độ bão hòa: nhóm cổ phần bị bão hòa khi nó có nhiều cổ phần được ủy quyền hơn mức tối ưu cho mạng. Mức độ bão hòa được biểu thị bằng phần trăm. Khi nhóm cổ phần đạt đến mức bão hòa 100%, phần thưởng bắt đầu thu hẹp lại. Cơ chế bão hòa được tạo ra để tránh tập trung hóa bằng cách khuyến khích chủ sở hữu ADA ủy quyền cho một số nhóm cổ phần và các nhà khai thác xây dựng nhiều nhóm hơn để tiếp tục nhận được phần thưởng tối đa. Saturation nhằm mục đích bảo vệ cả lợi ích của những người nắm giữ ADA ủy quyền cổ phần của họ và lợi ích của những người điều hành nhóm cổ phần (SPO).

Kiến trúc của Cardano cũng ưu tiên quản trị⁹⁷ để duy trì tính linh hoạt và khả năng tồn tại lâu dài của hệ thống. Cơ cấu quản trị được phát triển tốt cho phép sự phát triển dài hạn của Cardano được tài trợ một cách hiệu quả và dân chủ. Hệ thống ngân quỹ của Cardano là nguồn tài chính dài hạn cho giao thức và các dự án xây dựng trên đó. Nó sẽ được điều hành bởi cộng đồng và cho phép một cơ chế ra quyết định hợp tác, phi tập trung để đảm bảo sự phát triển và duy trì liên tục của Cardano. Có thể sử dụng nhiều nguồn tài chính khác nhau để nạp vào kho bạc, chẳng hạn như tổng hợp các đồng Coin mới được đúc, một phần phần thưởng Stake Pool, phí giao dịch và quyên góp. Nó sẽ có thể hỗ trợ phát triển dự án và trả tiền cho các khuyến nghị cải tiến bằng cách sử dụng số tiền kiếm được. Ngoài ra, các đề xuất cải tiến Cardano (CIP) được ban hành để kích thích và hệ thống hóa các cuộc trò chuyện của cộng đồng về các tính năng mới và sự phát triển của chúng.

Một hệ thống bỏ phiếu là trung tâm của kho bạc, cho phép chủ sở hữu ADA quyết định các đề xuất tài trợ và xác định cách sử dụng tiền. Điều này sẽ đảm bảo các lựa chọn được thực hiện một cách dân chủ chứ không phải bởi một nhóm người nhỏ. Phương thức bỏ phiếu này sẽ quyết định các lựa chọn như tài trợ cho các dự án, nâng cấp giao thức và thực hiện bất kỳ thay đổi hiến pháp nào, chẳng hạn như sửa đổi quy trình ra quyết định. Dự án Catalyst⁹⁸ đang phát triển thành một cơ chế quản trị dân chủ hoàn toàn trên chuỗi, cho phép dự án mở rộng theo thời gian và tự hỗ trợ một cách bền vững thông qua hệ thống ngân quỹ có tầm nhìn xa.

Ngày 20 tháng 1 năm 2021. Dự án Catalyst là gì? Mọi người có thể tham gia vào các quỹ trong tương lai bằng cách nào? CH.⁹⁹

Chúng tôi đang xây dựng toàn bộ ngăn xếp phiếu bầu cho Cardano. Chúng tôi đã hợp tác với rất nhiều công ty và tổ chức tư vấn lớn. Ví dụ: chúng tôi hợp tác với một công ty quản lý đối mới tên là IdeaScale ... họ đã hoạt động được gần một thập kỷ. Họ làm việc với Pfizer và Boeing... vậy làm thế nào Pfizer nghĩ ra loại vắc xin đó nhanh như vậy? Họ sử dụng IdeaScale . Về cơ bản, chúng tôi đã đưa chúng vào cùng với một số công cụ phi tập trung. Chúng tôi đã tạo ra một hệ thống bỏ phiếu hoàn toàn mới. Chúng tôi đã dành bốn năm để nghiên cứu cách thực hiện một hệ thống bỏ phiếu riêng dựa trên Blockchain ngoài trường đại học Lancaster có thể mở rộng quy mô cho nhiều người dùng.

Về cơ bản, chúng tôi đang tung tiền một cách có hệ thống... kho bạc của Cardano lấy một phần lạm phát mà thông thường bạn sẽ cung cấp cho SPO hoặc thợ đào... nó đưa số tiền đó vào một tài khoản phi tập trung và sau đó mọi người gửi phiếu bầu để được tài trợ. Theo thời gian, mọi người có thể kiểm tra những lá phiếu đó và nó trải qua một quá trình, giống như một cuộc so găng... nếu họ vượt qua, họ có thể bỏ phiếu... nếu có đủ phiếu bầu, bạn sẽ được tài trợ.

Các điểm khác biệt của Cardano

Các khía cạnh sau của Cardano sẽ được trình bày chi tiết trong các chương sau, đây là bản tóm tắt về những đổi mới của Blockchain.

Nghiên cứu học thuật: phương pháp chính quy bao gồm các đặc tả toán học, kiểm tra dựa trên thuộc tính và bằng chứng, là phương tiện hiệu quả nhất để cung cấp các hệ thống phần mềm có độ đảm bảo cao. Họ cũng cung cấp cho người dùng sự tin tưởng trong việc quản lý tài sản kỹ thuật số. Cardano được tạo bằng các phương pháp chính quy để có sự đảm bảo mạnh mẽ về tính chính xác về chức năng của các thành phần chính của hệ thống. Nghiên cứu hỗ trợ Cardano được xuất bản tại các hội nghị học thuật và trên các tạp chí, các bài nghiên cứu được cung cấp cho công chúng và tất cả các hoạt động phát triển Cardano đều được ghi lại trên GitHub.¹⁰⁰

Chi khi thuật toán đồng thuận Ouroboros đã được chứng minh là an toàn về mặt toán học bởi một nhóm học thuật do Giáo sư Aggelos Kiayias đứng đầu tại Đại học Edinburgh đã bắt đầu công việc kỹ thuật phần mềm bằng cách triển khai Blockchain trong mã Code. IOG rất tự hào về sự hiện diện ngày càng tăng của họ trong giới học thuật trên toàn cầu.¹⁰¹ Tầm quan trọng của những quan hệ đối tác và đầu tư này sẽ được đề cập trong Chương 9 (Voltaire).

⁹⁷

Quản trị Blockchain tập hợp các chuẩn mực và văn hóa, luật pháp và mã, con người và các tổ chức cần thiết để vận hành một hệ thống và đảm bảo sự ổn định của nó trong dài hạn. Quản trị, bao gồm bỏ phiếu và ngân quỹ để tài trợ dài hạn, là trọng tâm của giai đoạn Voltaire trong lộ trình Cardano.

⁹⁸

Project Catalyst là một loạt các thử nghiệm nhằm khuyến khích sự đổi mới của cộng đồng ở mức độ cao nhất. Catalyst đang mang lại khả năng quản trị trên chuỗi cho Cardano bằng cách cho phép cộng đồng xác định các ưu tiên cho sự phát triển (xem Chương 9).

⁹⁹

Hãy nói về Cardano - Phỏng vấn Charles Hoskinson, [youtube.com/watch?v=NX3fGKMd004](https://www.youtube.com/watch?v=NX3fGKMd004)

¹⁰⁰

IOG Github : github.com/input-output-hk/

¹⁰¹

Nghiên cứu của IOG mở rộng thế giới học thuật như thế nào,
iohk.io/en/blog/posts/2022/10/25/how-iog-s-research-spans-the-academic-world

Thiết kế hệ thống: Cardano được xây dựng bằng Haskell, một ngôn ngữ lập trình hàm¹⁰² an toàn, tạo điều kiện thuận lợi cho việc tạo các hệ thống sử dụng các chức năng thuần túy, dẫn đến một thiết kế dễ kiểm tra độc lập. Hơn nữa, các khả năng phức tạp của Haskell bao gồm các cách mạnh mẽ để đảm bảo tính chính xác của mã Code, chẳng hạn như dựa trên việc triển khai dựa trên các thông số kỹ thuật chính thức và có thể thực thi được, thử nghiệm kỹ lưỡng dựa trên thuộc tính và thử nghiệm mô phỏng.

Tính bảo mật: Ouroboros¹⁰³ (giao thức bằng chứng cổ phần của Cardano) cung cấp các đảm bảo bảo mật nghiêm ngặt; nó dựa trên các bài nghiên cứu được đánh giá ngang hàng được trình bày tại các hội nghị và ấn phẩm về mật mã và an ninh mạng hàng đầu. Chỉ khoảng một nửa số người dùng đang hoạt động trong mạng được yêu cầu tuân theo giao thức; trên thực tế, mức tăng tạm thời vượt quá ngưỡng 50% có thể được chấp nhận. Do đó, Ouroboros mạnh mẽ và thích ứng hơn nhiều so với các giao thức chịu lỗi truyền thống của Byzantine (BFT),¹⁰⁴ giao thức này phải dự báo mức độ tham gia dự kiến và có thể ngừng hoạt động nếu dự đoán không chính xác.

Giao thức mạng của Cardano sử dụng phương thức giao tiếp kéo. Nếu một Node cố gắng đẩy thông tin, nó sẽ tự động bị ngắt kết nối.

- Khả năng bảo mật tích hợp độc đáo:
 - VRF (chức năng ngẫu nhiên có thể kiểm chứng): được sử dụng để chứng minh rằng một Node có quyền tạo Block trong một Slot¹⁰⁵ nhất định.
 - VRF¹⁰⁶ làm cho cơ chế đồng thuận khó bị tấn công vì không thể dự đoán các Node sản xuất tiếp theo.
 - KES (chữ ký phát triển khóa): các phím được xoay sau một số Epoch¹⁰⁷ nhất định.
- Plutus, ngôn ngữ tập lệnh gốc của Cardano,¹⁰⁸ sử dụng một phương pháp chính quy để mang lại các khả năng hợp đồng thông minh tiên tiến cho Blockchain mà không ảnh hưởng đến bảo mật.
- DApp¹⁰⁹ sẽ được triển khai vào năm 2023.

Theo thông lệ tốt nhất, IOG luân phiên giữa các trình kiểm tra bảo mật khác nhau như Bcryptic, R9B (root9b), Grimm, Rpisec và Kudelski. Các báo cáo có sẵn trên trang IOG GitHub.¹¹⁰

¹⁰²

Lập trình hàm là một phong cách nghiêm ngặt để xây dựng cấu trúc và các thành phần của chương trình máy tính coi tính toán là việc đánh giá các hàm toán học và tránh thay đổi các thuộc tính của dữ liệu đang được xử lý. Đó là một mô hình 'khai báo' trong đó lập trình được thực hiện bằng các biểu thức hoặc khai báo thay vì các câu lệnh. Trong mã chức năng, giá trị đầu ra của một hàm chỉ phụ thuộc vào các đối số của nó, do đó, việc gọi một hàm có cùng giá trị cho một đối số luôn tạo ra cùng một kết quả. Điều này trái ngược với lập trình mệnh lệnh, ngoài các đối số của hàm, trạng thái chung của chương trình có thể ảnh hưởng đến giá trị kết quả của hàm. Việc loại bỏ các hiệu ứng phụ, nghĩa là, những thay đổi về trạng thái không phụ thuộc vào đầu vào hàm, có thể giúp hiểu chương trình dễ dàng hơn, đây là một trong những động lực để phát triển lập trình hàm.

¹⁰³

Giáo sư Aggelos Kiayias, 'Con đường Ouroboros dẫn đến phi tập trung hóa',
iohk.io/en/blog/posts/2020/06/23/the-ouroboros-path-to-centralization/

¹⁰⁴

Khả năng chịu lỗi Byzantine (BFT) : Lỗi Byzantine là tình trạng của một hệ thống máy tính, đặc biệt là các hệ thống máy tính phân tán, trong đó các thành phần có thể bị lỗi và có thông tin không hoàn hảo về việc liệu một thành phần có bị lỗi hay không. Thuật ngữ này lấy tên từ một câu chuyện ngụ ngôn, 'Vấn đề các tướng lĩnh Byzantine', được phát triển để mô tả một tình huống trong đó, để tránh sự thất bại thảm hại của hệ thống, các tác nhân của hệ thống phải đồng ý về một chiến lược phối hợp, nhưng một số tác nhân này không đáng tin cậy.

¹⁰⁵

Khe: Trong một kỷ nguyên, một khoảng thời gian đã đặt. Thời gian được chia thành các khe được đánh số cho mỗi kỷ nguyên. Các vị trí đang hoạt động là những vị trí bị chiếm bởi các Block.

¹⁰⁶

Trong mật mã, **hàm ngẫu nhiên có thể kiểm chứng (VRF)** là một hàm giả ngẫu nhiên cung cấp bằng chứng có thể kiểm chứng công khai về tính đúng đắn của kết quả đầu ra.

¹⁰⁷

Kỷ nguyên: một nhóm các vị trí được thiết lập tạo thành một khoảng thời gian (hiện tại là 5 ngày).

¹⁰⁸

Tập lệnh là một thuật ngữ chung cho một chương trình thực thi được sử dụng trong sổ cái. Trong Blockchain Cardano, chúng được viết trong Plutus Core.

¹⁰⁹

Một ứng dụng phi tập trung (DApp, dApp hoặc Dapp) là một dự án nguồn mở chạy trên mạng Blockchain. Bản chất phân tán của các mạng này cung cấp cho người dùng tính minh bạch, phân cấp và khả năng chống lại các cuộc tấn công.

¹¹⁰

toán IOG, github.com/input-output-hk/external_audits

Ngày 4 tháng 2 năm 2020. Phỏng vấn về tính bảo mật. CH:¹¹¹

Khi chúng tôi bắt đầu dự án Cardano, chúng tôi đã nói, 'hãy viết phần mềm theo cách khác và hãy nghĩ về khoa học khác một chút so với cách ngành của chúng ta nghĩ về nó...trái ngược với việc viết một sổ sách trắng hoặc chỉ viết ra ý tưởng hoặc nói đây là mã Code, hãy tận hưởng nó'. Chúng tôi đã nói rằng chúng tôi sẽ bắt đầu với quy trình khoa học được đánh giá ngang hàng. Vì vậy, điều đầu tiên chúng tôi làm là thuê một nhóm lớn các nhà khoa học. Chúng tôi đã hỏi rất nhiều câu hỏi khó. Họ suy nghĩ sâu sắc về các bằng chứng bảo mật, đối thủ và mô hình bảo mật cũng như tìm hiểu sâu sắc về những gì đã được thực hiện và nơi cần có sự đổi mới ban đầu để tồn tại.

Chỉ riêng điều đó vào thời điểm đó đã là một bước tiến lớn bởi vì nó không chỉ đơn giản được thực hiện ở quy mô thương mại lớn bởi bất kỳ ai trong ngành của chúng tôi. Bây giờ chúng tôi bắt đầu thấy rằng với việc David Chaum và Silvio Micali bước vào lĩnh vực này, và những người khác thực sự thuê các nhà khoa học chất lượng, viết các bài nghiên cứu chất lượng, bao gồm cả Ethereum, đó không còn là sự khác biệt cốt lõi nữa, nhưng chúng tôi không dừng lại ở đó.

Vào năm 2015, chúng tôi cũng mong muốn có khái niệm về các phương pháp chính quy. Đây là điều mà rất ít kỹ sư phần mềm trong ngành hiểu đầy đủ hoặc đánh giá cao giá trị của nó. Về cơ bản, phương pháp chính quy là gì, đó là nơi bạn nói, 'hãy viết ra một cách thật cụ thể, chi tiết, chặt chẽ, toán học những gì chúng ta dự định làm...cái gì là cái gì'.

Chúng tôi có khái niệm về Ouroboros, có nhiều phiên bản của nó, nhưng ý nghĩa thực sự của việc chuyển từ những bài nghiên cứu khô khan mà các học giả của chúng tôi đã viết thành một thứ mà một kỹ sư có thể nhìn vào và biết rõ hoàn toàn rằng những gì họ đã tạo ra phù hợp với ý định của các tác giả của hệ thống. Về cơ bản, bạn phải viết một đặc điểm kỹ thuật cho điều này. Sau đó các đặc điểm kỹ thuật có thể được phân tích một cách nghiêm ngặt về tính chính xác. Bạn có thể sử dụng tất cả các loại kỹ thuật như kiểm tra mô hình và giải SAT¹¹², v.v. để xác minh rằng thông số kỹ thuật của bạn đáp ứng một số loại tập hợp các yêu cầu hoặc kiểm tra thiết kế.

Chúng tôi đã chọn đi theo con đường này. Không may là hầu hết thời gian, khi viết phần mềm theo cách này bạn sẽ cần thêm nhiều năm vào lộ trình. Đó chính xác là những gì đã xảy ra với chúng tôi. Khi chúng tôi đi theo con đường này, ngoài một nhóm các nhà khoa học, chúng tôi còn phải thuê một nhóm các chuyên gia về phương pháp chính quy. Sau đó chúng tôi phải tìm ra cách thực hiện các phương pháp chính quy với Crypto. Vào thời điểm đó, chưa có ai thực sự làm điều đó trước đây.

Tiêu thụ năng lượng: Cardano là một Blockchain bằng chứng cổ phần. Nó đòi hỏi ít năng lượng hơn để hoạt động so với các chuỗi bằng chứng công việc. Mạng Bitcoin phát triển nhờ các máy tính thực hiện các phép tính tốn nhiều năng lượng, một quy trình được gọi là bằng chứng công việc không bền vững về lâu dài. Theo Chỉ số tiêu thụ điện Bitcoin của Cambridge,¹¹³ các máy vận hành Bitcoin sử dụng nhiều năng lượng mỗi năm tương đương với một quốc gia như Na Uy hoặc Thụy Điển. Ouroboros xác định đòn bẩy của người tham gia trong hệ thống bằng cách sử dụng cổ phần làm tài nguyên chính. Bất chấp các cuộc tấn công 'mô phỏng không tồn kém' và 'không có gì bị đe dọa – Nothing at Stake',¹¹⁴ vốn trước đây được coi là rào cản cơ bản đối với sổ cái dựa trên cổ phần, không có tài nguyên vật chất nào được sử dụng trong quá trình bảo trì sổ cái. Điều này phân biệt Ouroboros với các phương pháp bằng chứng công việc, vốn cần mức tiêu thụ năng lượng cao để thiết lập cơ chế đồng thuận.

Nâng cấp liền mạch: trong các Blockchain cũ hơn, việc nâng cấp được thực hiện thông qua các Hardfork. Khi một Hardfork xảy ra, giao thức hiện có bị vô hiệu hóa, các quy tắc và sửa đổi mới được đưa ra và chuỗi được khởi động lại với tất cả lịch sử bị hủy. Các

¹¹¹

Một số nhận xét ngắn gọn về quy trình, [youtube.com/watch?v=T4hjGjredpw](https://www.youtube.com/watch?v=T4hjGjredpw)

¹¹²

Vấn đề thỏa mãn Boolean (viết tắt là **SATISFIABILITY** hoặc **SAT**) là vấn đề xác định xem có tồn tại một diễn giải thỏa mãn một công thức Boolean nhất định hay không. Nó hỏi liệu các biến của một công thức Boolean nhất định có thể được thay thế một cách nhất quán bằng các giá trị TRUE hoặc FALSE theo cách mà công thức đánh giá là TRUE hay không. Nếu đây là trường hợp, công thức được gọi là thỏa mãn. Mặt khác, nếu không tồn tại phép gán như vậy, thì hàm được biểu thị bằng công thức là SAI đối với tất cả các phép gán biến có thể có và công thức không thỏa mãn.

¹¹³

'Xếp hạng quốc gia', [ccaf.io / cbeci / index / comparisons](https://ccaf.io/cbeci/index/comparisons)

¹¹⁴

Oettler (2022), 'Không có gì bị đe dọa / Mô phỏng không tồn kém', blockchain-academy.hs-mittweida.de/courses/game-theory-blockchain/lessons/attacks-on-proof-of-stake-pos/topic/nothing-at-stake-chi-phi-mo-phong/

Hardfork được xử lý khác với Cardano. Thay vì thực hiện những thay đổi mạnh mẽ, bộ tổ hợp Hardfork Cardano (HFC)¹¹⁵ cho phép chuyển đổi liên mạch sang một giao thức mới mà vẫn lưu giữ lịch sử của các Block và gây ra sự bất tiện tối thiểu cho người dùng.

Phi tập trung: Cardano được quản lý thông qua mạng do cộng đồng điều hành gồm hơn 3.000 Stake Pool phân tán. Không dựa vào cơ quan tập trung, các thành viên mạng xác minh tất cả các Block và giao dịch.

Ouroboros bao gồm một hệ thống chia sẻ phần thưởng để khuyến khích người tham gia hình thành các Node hoạt động, được gọi là Stake Pool, có thể cung cấp dịch vụ chất lượng bất kể cổ phần được chia như thế nào cho người dùng. Do đó, tất cả các bên liên quan đều đóng góp vào hoạt động của hệ thống, đảm bảo khả năng phục hồi và đại diện dân chủ, trong khi chi phí duy trì sổ cái được phân bổ hiệu quả trên cộng đồng người dùng. Các tính năng của hệ thống không khuyến khích tập trung hóa. Do đó, Ouroboros vốn đã bao trùm và phi tập trung hơn các giao thức khác, dẫn đến việc chỉ có một số ít tác nhân chịu trách nhiệm duy trì sổ cái hoặc không khuyến khích các bên liên quan tham gia và cung cấp dịch vụ chất lượng.

Ouroboros cũng cung cấp trải nghiệm Staking¹¹⁶ tốt hơn. Cardano không áp dụng các hình phạt như giảm cổ phần hoặc khóa (liên kết). Khi bạn ủy thác ADA cho Stake Pool từ ví của mình, nó sẽ không bị khóa. Phần thưởng được phân phối mỗi Epoch (khoảng 4% ADA đang lưu hành) và bạn có thể truy cập hoặc rút cổ phần bất cứ lúc nào. Ngoài ra, việc Staking trên Cardano không bị giam giữ, điều đó có nghĩa là cũng không có nguy cơ bị phạt. Với tư cách là người ủy quyền, số tiền ủy thác của bạn không bao giờ có nguy cơ bị Stake Pool lấy đi.

- Giao thức Ouroboros có hiệu quả cao, nghĩa là các nhà khai thác Stake Pool có thể chạy các Node của họ trên phần cứng có thông số kỹ thuật thấp, với yêu cầu đầu tư phần cứng ít hơn so với các Blockchain khác.
- Hơn 80% Token được nắm giữ bởi công chúng và hơn 70% ADA được ủy thác từ hàng triệu ví.

Các trang Web như ADAPools (ADApools.org) và PoolTool (pooltool.io) cung cấp thông tin về Stake Pool.

Môi trường chức năng dành cho doanh nghiệp: Cardano đang đặt nền móng cho tài chính phi tập trung toàn cầu bằng cách cho phép các nhà phát triển tạo ứng dụng phi tập trung (DApp) chạy trên hợp đồng thông minh dành riêng cho miền và chức năng, đồng thời cung cấp Token đa tài sản¹¹⁷ cho bất kỳ nhu cầu nào. Hai nền tảng ngôn ngữ hợp đồng thông minh được cung cấp: Plutus,¹¹⁸ là 'Turing Complete',¹¹⁹ có thể được sử dụng cho mọi mục đích; và Marlowe, một ngôn ngữ chuyên biệt cho ngân hàng và dịch vụ tài chính.

Cardano bổ sung khả năng lập trình cho mô hình UTXO¹²⁰ đã được chứng minh của Bitcoin với mô hình sổ cái UTXO mở rộng (eUTXO), cung cấp hợp đồng thông minh với khả năng mở rộng tăng lên và duy trì tính bảo mật. Với eUTXO, siêu dữ liệu¹²¹ và tập lệnh được nhóm lại trong một giao dịch duy nhất để có thông lượng lớn hơn. Xác minh giao dịch đơn giản hơn nên bạn có thể dự đoán

¹¹⁵

Anthony Quinn, 'Combinator làm cho công việc của Shelley trở nên dễ dàng',
iohk.io/en/blog/posts/2020/05/07/combinator-makes-easy-work-of-shelley-hard-fork/

¹¹⁶

Đặt cược liên quan đến việc giữ tiền trong ví Crypto để hỗ trợ bảo mật và hoạt động của mạng Blockchain và đôi lại nhận được phần thưởng đặt cược. Nói cách khác, đặt cược là quá trình tích cực tham gia xác thực giao dịch (tương tự như khai thác) trên Blockchain bằng chứng cổ phần (PoS).

¹¹⁷

Sổ cái đa tài sản (MA) có thể thực hiện việc hạch toán hoặc tương tác với nhiều loại tài sản. Cardano sử dụng Token gốc để cung cấp tính năng này.

¹¹⁸

Plutus: một khung lập trình hoàn chỉnh Turing để xây dựng các hợp đồng thông minh chức năng. Plutus là một ngôn ngữ lập trình dựa trên Haskell.

¹¹⁹

Một hệ thống được gọi là **Turing hoàn chỉnh** nếu nó có thể được sử dụng để mô phỏng bất kỳ máy Turing nào. Điều này có nghĩa là hệ thống này có thể nhận ra hoặc quyết định các bộ quy tắc thao tác dữ liệu khác. Tính đầy đủ của Turing được sử dụng như một cách để thể hiện sức mạnh của bộ quy tắc thao tác dữ liệu như vậy. Hầu như tất cả các ngôn ngữ lập trình ngày nay đều là Turing hoàn chỉnh. Khái niệm này được đặt tên theo nhà toán học và khoa học máy tính người Anh Alan Turing.

¹²⁰

Mô hình **Đầu ra giao dịch chưa chi tiêu (UTXO)** thường được sử dụng trong lĩnh vực Công nghệ sổ cái phân tán (DLT) để chuyển giá trị giữa những người tham gia. UTXO là thuật ngữ kỹ thuật chỉ lượng tiền kỹ thuật số còn lại sau một giao dịch Crypto. Bạn có thể coi đó là tiền lẻ bạn nhận được sau khi mua một món hàng. Nhiều hơn nữa về điều này sau này, Chương 5.

¹²¹

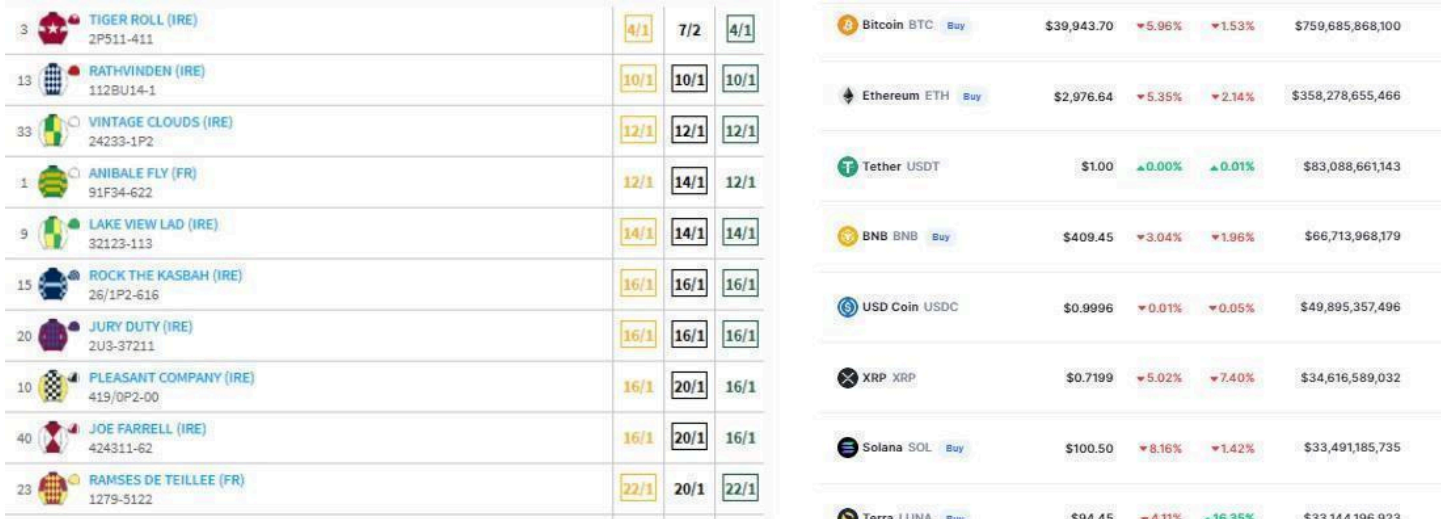
Siêu dữ liệu: tập hợp dữ liệu bổ sung thể hiện các trường hợp giao dịch hoặc thông tin chủ sở hữu. Siêu dữ liệu được sử dụng trong các hợp đồng thông minh để chỉ ra các trường hợp theo đó một giao dịch sẽ diễn ra.

điều gì sẽ xảy ra, bao gồm cả phí giao dịch. Nếu một giao dịch không thành công thì sẽ không bị tính phí. Các tính năng thử nghiệm được cung cấp trong Plutus và Marlowe, các nhà phát triển có thể đảm bảo tập lệnh hợp đồng thông minh hoạt động như dự kiến.

Token có thể thay thế và không thể thay thế (NFT) là Token gốc nên không cần hợp đồng thông minh. Điều này làm giảm độ phức tạp, giúp các nhà phát triển dễ dàng hơn và mở ra những cách sử dụng mới, cũng như trải nghiệm chơi Game và Metaverse vượt trội.

Tại sao lại chọn Cardano?

Với 18.000 Crypto¹²² ngày nay, việc nắm bắt sự khác biệt có thể là quá sức. Crypto có được xếp hạng dựa trên giá trị của chúng không? Làm thế nào mà một thứ tầm thường như Doge¹²³ lọt vào Top 20 trong khi một tuyệt tác kỹ thuật như Ergo¹²⁴ nằm ngoài Top 200? Nếu bạn quan sát nó đủ lâu, CoinMarketCap bắt đầu giống như tỷ lệ cược của một cuộc đua ngựa và không thể dự đoán được.



Hình 4. Tỷ lệ cược đua ngựa so với Coincap.io
Vậy Cardano có gì đặc biệt? Thế hệ Blockchain đầu tiên (Bitcoin) cung cấp khả năng di chuyển Crypto an toàn thông qua sổ cái phi tập trung. Tuy nhiên, các Blockchain như vậy không cung cấp môi trường phù hợp để giải quyết các giao dịch phức tạp hoặc tạo ứng dụng phi tập trung (DApp). Thế hệ Blockchain thứ hai (Ethereum) mang đến các giải pháp tiên tiến hơn để viết và thực hiện hợp đồng thông minh, phát triển ứng dụng và tạo Token khi công nghệ Blockchain phát triển. Tuy nhiên, các Blockchain thế hệ thứ hai cũng được xây dựng bằng cách khai thác bằng chứng công việc tốn năng lượng và đối mặt với những thách thức về khả năng mở rộng.

Cardano được coi là nền tảng Blockchain 'thế hệ thứ ba' vì nó kết hợp các đặc điểm của các thế hệ trước nhưng tránh được những cạm bẫy của chúng và có thể thích ứng để đáp ứng mọi nhu cầu của người dùng. Cardano được xây dựng trên Ouroboros, một giao thức Blockchain bằng chứng cổ phần được đánh giá ngang hàng¹²⁵ đã được xuất bản tại hội nghị nghiên cứu về Crypto hàng đầu thế giới (Hiệp hội Nghiên cứu Mật mã Quốc tế lần thứ 37 – Crypto 2017).

¹²² ADAm Hayes, (2022) ' 10 loại Crypto quan trọng khác ngoài Bitcoin ', Investopedia.com/tech/most-important-cryptocurrency-other-than-bitcoin

¹²³ **Dogecoin** là một loại Crypto có hình giống chú chó Shiba Inu từ meme trên internet 'Doge' làm biểu tượng của nó. Được giới thiệu như một "đồng tiền đùa" vào năm 2013, Dogecoin đã nhanh chóng phát triển cộng đồng trực tuyến của riêng mình và đạt mức vốn hóa 1 tỷ đô la Mỹ vào năm 2018.

¹²⁴ **Ergo** (ergoplatform.org) là một nền tảng hợp đồng thông minh bằng chứng công việc cho phép các mô hình tương tác tài chính mới, được củng cố bởi một ngôn ngữ kịch bản an toàn và phong phú được xây dựng bằng các bằng chứng không kiến thức linh hoạt và mạnh mẽ (giao thức Σ).

¹²⁵ **Đánh giá ngang hàng** là đánh giá công việc của một hoặc nhiều người có năng lực tương tự như những người sản xuất công việc (đồng nghiệp). Nó hoạt động như một hình thức tự điều chỉnh của các thành viên có trình độ chuyên môn trong lĩnh vực liên quan. Các phương pháp đánh giá ngang hàng được sử dụng để duy trì các tiêu chuẩn chất lượng, cải thiện hiệu suất và mang lại sự tin cậy. Trong giới học thuật, bình duyệt ngang hàng mang tính học thuật được sử dụng để xác định tính phù hợp của một bài báo học thuật để xuất bản.

Các bài nghiên cứu của Cardano là truy cập mở, không có bằng sáng chế và cung cấp tất cả thông tin kỹ thuật cần thiết cho bất kỳ ai có kỹ năng kỹ thuật phù hợp để xác minh tính chính xác của các tuyên bố về hiệu suất, bảo mật và chức năng ([iohk.io/research](https://iohk.io/en/research)). Các dự án khác đã vay mượn rất nhiều từ nghiên cứu của IOG, chẳng hạn như giao thức đồng thuận hỗn hợp của Polkadot được lấy cảm hứng từ Ouroboros.¹²⁶ Bạn có thể kiểm tra các trích dẫn trên Google Scholar: một tìm kiếm tạo ra khoảng hơn 1.500 trích dẫn.¹²⁷ Tương tự, bài nghiên cứu 'Giao thức xương sống Bitcoin' (GKL), là nền tảng cho phần lớn Cardano có hơn 1.800 trích dẫn.¹²⁸

Giải pháp lý tưởng phải cung cấp mức độ bảo mật, khả năng mở rộng cao nhất (tốc độ giao dịch, quy mô dữ liệu, dung lượng mạng) và chức năng để xử lý mọi khía cạnh của việc giải quyết thỏa thuận kinh doanh, không chỉ xử lý giao dịch. Hơn nữa, điều quan trọng là đảm bảo công nghệ Blockchain tiếp tục phát triển tính bền vững, khả năng tương tác với các Blockchain và tổ chức tài chính khác.

Để đáp ứng những nhu cầu này, Cardano tập trung vào các nguyên tắc như:

Khả năng mở rộng: đảm bảo rằng sổ cái Cardano có thể xử lý một số lượng lớn giao dịch mà không làm chậm mạng. Khả năng cung cấp bằng chứng cao hơn thông qua khả năng mở rộng, cho phép các giao dịch vận chuyển một lượng lớn dữ liệu hỗ trợ có thể được xử lý đơn giản bên trong mạng. IOG đang dần giới thiệu Hydra cùng với các giải pháp khác như Sidechain. deSpark (công ty phát triển bên thứ ba) đã ra mắt Sidechain Milkomeda. IOG sẽ sớm ra mắt Sidechain của riêng họ. (Tìm hiểu thêm về điều này trong Chương 8).

Khả năng tương tác: đảm bảo một môi trường đa chức năng cho các quy trình tài chính, kinh doanh hoặc thương mại bằng cách cho phép người dùng tương tác với nhiều loại tiền tệ trên nhiều Blockchain. Khả năng tương tác với các cơ quan tài chính tập trung cũng rất quan trọng để đảm bảo tính hợp pháp và dễ sử dụng.

Tính bền vững: việc xây dựng một Blockchain bằng chứng cổ phần đòi hỏi một hệ thống độc lập. Cardano được thiết kế để cộng đồng duy trì sự phát triển bằng cách tham gia, gửi đề xuất và thực hiện đổi mới hệ thống để thúc đẩy tăng trưởng và trưởng thành theo cách hoàn toàn phi tập trung. Để duy trì khả năng tồn tại lâu dài, cộng đồng kiểm soát hệ thống ngân quỹ được cung cấp thường xuyên từ nhiều nguồn khác nhau như lượng Coin mới đúc được giữ lại làm tài chính, một phần phần thưởng Stake Pool và phí giao dịch.

Lộ trình Cardano

Sự phát triển của lộ trình Cardano¹²⁹ đã được chia thành năm kỷ nguyên, mỗi kỷ nguyên tập trung vào một bộ tính năng khác nhau:

- Byron tập trung vào việc thiết lập một nền tảng.
- Shelley tập trung vào phi tập trung mạng lưới.
- Goguen là tất cả về hợp đồng thông minh.
- Basho là động lực để đạt được khả năng mở rộng thực sự.
- Voltaire dựa trên việc thực hiện quản trị phi tập trung.

Mỗi kỷ nguyên được xây dựng xung quanh một tập hợp các tính năng được triển khai và cải thiện qua nhiều bản phát hành mãCode. Mặc dù công việc cho từng luồng phát triển này được phân phối theo thứ tự, nhưng nó thường được thực hiện đồng thời, với việc nghiên cứu, tạo mẫu và phát triển diễn ra đồng thời xuyên suốt.

¹²⁶

'Chăm bít đồng thuận', wiki.polkadot.network/docs/learning-consensus

¹²⁷

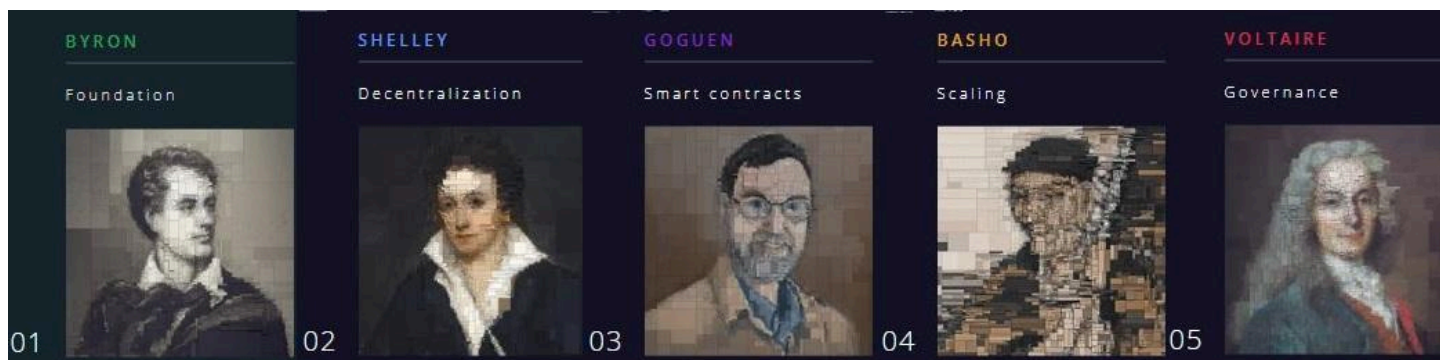
A Kiayias, A Russell, B David, R Oliynykov (2017) Trích dẫn 'Ouroboros: Một giao thức Blockchain bằng chứng cổ phần an toàn có thể chứng minh được', [Scholar.google.com/scholar?cites=9760004817031418890&as_sdt=2005&sciodt=0,5&hl=vi](https://scholar.google.com/scholar?cites=9760004817031418890&as_sdt=2005&sciodt=0,5&hl=vi)

¹²⁸

J Garay, A Kiayias, N Leonardos (2014) 'Giao thức xương sống bitcoin: phân tích và ứng dụng', eprint.iacr.org/2014/765.pdf

¹²⁹

Cardano roadmap, [Mapano.cardano.org/vi/](https://mapano.cardano.org/vi/)



Hình 5. Từ maps.cardano.org

Byron

Byron đã đặt nền móng cho việc tạo ra Cardano. Nó cho phép người dùng mua và giao dịch ADA trên mạng Blockchain bằng chứng cổ phần. Ban đầu, sổ cái Cardano được thiết lập như một mạng liên kết, với các Stake Pool được điều hành bởi Input Output Global, và Emurgo xử lý việc tạo Block và xác thực giao dịch. Byron chứng kiến việc phát hành ví Daedalus và Yoroi,¹³⁰ cũng như trình khám phá Block để kiểm tra Blockchain.¹³¹

Shelley

Kỷ nguyên phát triển Shelley đã cung cấp một sổ cái phi tập trung, dẫn đến một cấu trúc kinh tế mới thúc đẩy sự phát triển và tối ưu hóa mạng lưới. Trong giai đoạn chuẩn bị cho việc phi tập trung, một mạng thử nghiệm được khuyến khích (ITN) đã được thiết lập để chứng minh rằng Cardano sẽ tồn tại lâu dài chỉ với các Pool do cộng đồng quản lý.

Shelley nổi lên từ mạng liên kết của Byron, với cộng đồng SPO (SPO) phân tán tạo ra số lượng Block ngày càng tăng cho đến khi mạng được phi tập trung hoàn toàn vào năm 2021. Về hoạt động của Stake Pool, ưu tiên ủy quyền¹³² và khuyến khích, Shelley tập trung vào các quy trình thiết yếu cung cấp trải nghiệm người dùng được cải thiện.

Goguen

Sự phát triển của Goguen tập trung vào việc tạo ra một hệ thống toàn cầu, tài chính và đa chức năng để tạo ra các ứng dụng phi tập trung (DApp), hỗ trợ hợp đồng thông minh và phát hành Token tùy chỉnh. Goguen là một thành phần cơ bản trong việc thiết lập một nền tảng linh hoạt để phát triển các ứng dụng trong các lĩnh vực như chuỗi cung ứng, theo dõi và truy vết, tài chính, hồ sơ y tế, danh tính bỏ phiếu, đăng ký tài sản và thanh toán ngang hàng.

Basho

Basho tập trung vào việc tối ưu hóa Cardano về khả năng mở rộng và khả năng tương tác của mạng lưới. Trong khi các vòng phát triển trước đây tập trung vào phi tập trung và các tính năng mới, Basho hoàn toàn tập trung vào việc nâng cao hiệu suất cơ bản của mạng Cardano để tạo điều kiện phát triển và tiếp nhận cho các ứng dụng hoạt động.

Voltaire

Voltaire được xây dựng dựa trên quản trị và ra quyết định phi tập trung, cho phép cộng đồng Cardano bỏ phiếu về các bản cập nhật

¹³⁰

Ví **Crypto** lưu trữ khóa công khai và khóa riêng có thể được sử dụng để nhận hoặc chi tiêu Crypto. Một ví có thể chứa nhiều khóa công khai nhưng chỉ có một khóa riêng, khóa này phải được giữ an toàn để không bị mất hoặc bị đánh cắp. Một khi khóa cá nhân bị mất sẽ kết thúc vòng đời của chiếc ví đó. Bản thân Crypto không có trong ví. Crypto được lưu trữ và duy trì một cách phi tập trung trong một sổ cái có sẵn công khai được gọi là Blockchain. Mỗi phần của Crypto đều có khóa riêng. Với khóa riêng tư, có thể ký điện tử một giao dịch và ghi nó vào sổ cái công khai, thực tế là chỉ tiêu Crypto được liên kết.

¹³¹

Trình khám phá Cardano, explorer.cardano.org/ vi

¹³²

Ủy quyền : Bằng cách ủy quyền cổ phần liên quan đến việc nắm giữ ADA của họ cho nhóm cổ phần, chủ sở hữu ADA tham gia vào mạng và thu thập phần thưởng mỗi kỷ nguyên (năm ngày). Người ủy quyền được thưởng tương ứng với số cổ phần được ủy quyền.

phát triển mạng, tiến bộ công nghệ và tài chính dự án. Để thực sự phi tập trung, mạng Cardano không chỉ cần kiến trúc phân tán được phát triển dưới thời Shelley mà còn cần khả năng duy trì và nâng cao theo cách phi tập trung theo thời gian. Dự án Catalyst là về việc đưa ra các cơ chế để mọi người có thể xin tài trợ và bỏ phiếu cho các đề xuất.

Cardano hoạt động như thế nào?

Node Cardano là thành phần cấp cao nhất của mạng cung cấp năng lượng cho Blockchain. Lớp mạng lưới là động lực cung cấp nhu cầu trao đổi thông tin, kết nối các Node mạng với nhau. Đối với luồng dữ liệu nâng cao, điều này cung cấp siêu dữ liệu giao dịch và khuếch tán Block mới. Các Node Cardano giữ liên lạc với nhau bằng phương pháp lựa chọn ngang hàng. Bạn tham gia và đóng góp cho mạng Cardano bằng cách lưu trữ một Node. Như với mọi khía cạnh của Cardano, bảo mật là tối quan trọng. Giao thức mạng sử dụng phương thức giao tiếp kéo, vì vậy nếu một Node cố gắng đẩy thông tin, nó sẽ tự động bị ngắt kết nối.

Stake Pool chịu trách nhiệm xử lý giao dịch và tạo Block và sử dụng Node Cardano để kiểm tra cách Pool tương tác với mạng. Chúng hoạt động như các Node máy chủ an toàn, lưu trữ và duy trì cổ phần gộp của một số bên liên quan trong một thực thể duy nhất.

Sản xuất Block

Mục đích của công nghệ Blockchain là tạo ra một chuỗi hồ sơ (Block) được kết nối bằng mật mã, có thể kiểm chứng độc lập. Một mạng lưới các nhà sản xuất Block hợp tác để nâng cao toàn bộ Blockchain. Một giao thức đồng thuận đảm bảo rằng chuỗi minh bạch và xác định Block ứng cử viên nào sẽ được chọn để mở rộng chuỗi.

Các giao dịch hợp lệ đã được gửi có thể được đưa vào bất kỳ Block mới nào. Nhà sản xuất của một Block ký tên bằng mật mã và liên kết nó với Block trước đó trong chuỗi. Điều này gây khó khăn cho việc xóa các giao dịch khỏi một Block, thay đổi thứ tự của các Block, xóa một Block khỏi chuỗi (nếu nó có nhiều Block khác theo sau nó) hoặc thêm một Block mới vào chuỗi mà không thông báo cho tất cả các thành viên mạng. Điều này bảo vệ tính toàn vẹn và trách nhiệm giải trình của việc mở rộng Blockchain.

Slot và Epoch

Giao thức Ouroboros được sử dụng bởi Blockchain Cardano để hỗ trợ sự đồng thuận của chuỗi. Thời gian được chia thành các Epoch. Một Epoch được tạo thành từ các Slot, mỗi Slot kéo dài một giây. Hiện tại có 432.000 Slot (năm ngày) trong một Epoch Cardano. Các Slot Leader¹³³ được bầu chọn ngẫu nhiên trong số các Stake Pool. Trung bình cứ 20 giây lại có một Node được đề cử, với tổng số 21.600 đề cử mỗi Epoch. Một trong những Slot Leader được rút ngẫu nhiên sẽ được thêm vào chuỗi nếu họ tạo Block. Một Node ngoại tuyến sẽ bỏ lỡ cơ hội và một Node khác sẽ được chọn. Điều này có nghĩa là Stake Pool phải rất đáng tin cậy và luôn trực tuyến. Phần còn lại của các Block ứng cử viên sẽ bị loại bỏ.

Có một số phiên bản của Ouroboros: Classic, Byzantine Fault Tolerance (BFT), Genesis, Praos và Hydra. Thông tin thêm về điều này trong Chương 3.

Bầu chọn Slot Leader

Mạng Cardano được tạo thành từ một số lượng Stake Pool hoặc người được ủy quyền, chi phối tổng số cổ phần của chủ sở hữu và các bên liên quan khác. Các Slot Leader được chọn ngẫu nhiên từ Stake Pool. Cổ phần của nhóm càng lớn thì càng có nhiều khả năng được chọn làm Slot Leader và tạo ra một Block mới được chấp nhận vào Blockchain. Đây là nền tảng của cách tiếp cận bằng chứng cổ phần (PoS) của Cardano. Cardano bao gồm một kế hoạch khuyến khích không khuyến khích ủy quyền cho các Pool đã kiểm soát quá nhiều cổ phần tổng thể, để duy trì một sân chơi bình đẳng và tránh một số lượng nhỏ các Pool cực lớn kiểm soát phần lớn cổ phần.

Xác thực giao dịch

Slot Leader phải xác nhận rằng người gửi đã bao gồm đủ tài nguyên để thanh toán cho giao dịch và các yêu cầu của giao dịch được đáp ứng trong khi xác thực giao dịch. Slot Leader sẽ ghi lại giao dịch như một phần của Block mới, Block này sau đó sẽ được nối với các Block khác trong chuỗi, nếu nó phù hợp với tất cả các điều kiện này.

Làm thế nào để mua ADA?

Hầu hết mọi người mua ADA thông qua các sàn giao dịch tập trung như Kraken, Coinbase hoặc Binance. Các bước được ghi lại trong

133

Người dẫn đầu vị trí : một Node được chọn đã được chọn để xây dựng một khối trong vị trí hiện tại. Một cuộc bầu cử tùy ý diễn ra dựa trên tỷ lệ cổ phần.

Tài liệu Cardano, rất nhiều Blog và video trên YouTube.¹³⁴ Các sàn giao dịch tập trung không còn là một dịch vụ cho phép trao đổi tiền pháp định và Crypto duy nhất có sẵn với các ví như *Eternl* và các nhà cung cấp như Nmkr.io cung cấp cho người dùng khả năng mua ADA bằng nội tệ của họ.

Cách ủy quyền và kiếm phần thưởng

Số lượng ADA bạn nắm giữ xác định quy mô cổ phần của bạn. Người dùng Cardano có thể nhận được phần thưởng thụ động để xác minh các Block nếu họ có cổ phần trong giao thức.

Bởi vì không phải ai cũng có thời gian, kỹ năng hoặc tiền bạc để vận hành một Stake Pool, nên những người nắm giữ ADA có thể ủy quyền cổ phần của họ cho một Pool và được một nhà điều hành thay mặt họ quản lý. Điều này cho phép mọi người đóng góp vào sự đồng thuận và nhận phần thưởng mà không cần phải giữ Node trực tuyến mọi lúc. Cổ phần trong một Pool càng lớn, phần thưởng cho chủ sở hữu của nó càng nhiều. Bạn có thể chi tiêu ADA của mình bất cứ khi nào, bất kể nó đã được ủy quyền hay chưa.

Những người nắm giữ ADA ban đầu dựa vào ví *Daedalus* từ IOG (Node đầy đủ, ví máy tính để bàn) hoặc *Yoroi* từ Emurgo (ứng dụng máy trạm nhẹ, di động) để ủy quyền. Nhưng khi Cardano trưởng thành, giờ đây có nhiều lựa chọn hơn. Vào tháng 6 năm 2022, IOG đã công bố ví nhẹ mới, *Lace* sẽ là cửa hàng duy nhất cho mọi thứ trong hệ sinh thái Cardano. Trong khi đó, *Flint* và *Eternl* của dcSpark (dcSpark.io) chỉ là hai trong số nhiều ví có sẵn.¹³⁵ Dưới đây là một số hướng dẫn được đề xuất trong Cardano Docs:

- Làm thế nào để chọn một Stake Pool¹³⁶
- Mức độ an toàn khi ủy quyền cho Stake Pool?¹³⁷
- Cách ủy quyền cho Stake Pool¹³⁸ (Daedalus)
- Staking và ủy quyền cho người mới bắt đầu¹³⁹ (Daedalus)
- Cách ủy quyền từ ví Yoroi¹⁴⁰

Node Cardano ban đầu được phát triển bởi IOG, hiện là một dự án nguồn mở theo đúng nghĩa của nó. IOG đang ngày càng chú trọng vào thông tin xác thực nguồn mở của họ. Bạn có thể xem lại kho lưu trữ trên GitHub¹⁴¹ để hiểu cách bạn có thể đóng góp, quy tắc ứng xử, kết quả đo điểm chuẩn, v.v. và truy cập CardanoUpdates.com để biết chi tiết về lộ trình.

Quyết định thiết kế Cardano

Nhiều người đã phát hiện ra Cardano bằng cách xem bài thuyết trình trên YouTube về Video tám bảng trắng của Charles Hoskinson¹⁴². Tuy nhiên, Cardano đã không bắt đầu với một kế hoạch chi tiết hoặc thậm chí là sách trắng, như nhiều sáng kiến nguồn mở đã làm.

¹³⁴

Làm thế nào để ủy quyền Cardano ADA c Crypto dành cho người mới bắt đầu, youtube.com/watch?v=3MEO-Im6OSg

¹³⁵

Ví cardano, cardanocube.io/collections/wallets

¹³⁶

Cách chọn nhóm cổ phần, iohk.zendesk.com/hc/en-us/articles/900002174303-How-to-choose-a-stake-pool

¹³⁷

Mức độ an toàn khi ủy quyền cho nhóm cổ phần?

iohk.zendesk.com/hc/en-us/articles/900002046123-How-safe-is-it-to-delegate-to-a-stake-pool-

¹³⁸

Cách ủy quyền cho nhóm cổ phần, iohk.zendesk.com/hc/en-us/articles/900005718683-How-to-Delegate-to-a-stake-pool

¹³⁹

Đặt cược và ủy quyền cho người mới bắt đầu, forum.cardano.org/t/staking-and-delegating-for-beginners-a-step-by-step-guide/36681

¹⁴⁰

Cách ủy quyền từ ví Yoroi, forum.cardano.org/t/cardano-shelley-how-to-delegate-from-the-yoroi-wallet/38230

¹⁴¹

cardano -node , github.com/input-output-hk/cardano -node _

¹⁴²

IOHK | Bảng trắng Cardano; tổng quan với Charles Hoskinson, youtube.com/watch?v=Ja9D0kpkxw

IOG đã khám phá bối cảnh Crypto bằng cách áp dụng cách tiếp cận 'các nguyên tắc đầu tiên'.¹⁴³ Dự án Scorex¹⁴⁴ và kho tài liệu nghiên cứu của IOG¹⁴⁵ là sản phẩm của nghiên cứu này.

Không giống các giao thức thành công như TCP/IP,¹⁴⁶ hầu hết các loại Crypto không có phân lớp trong kiến trúc của chúng. Bất kể điều đó có hợp lý hay không, đã có mong muốn duy trì một khái niệm thống nhất duy nhất xung quanh các sự kiện và sự kiện được ghi lại trong một sổ cái duy nhất.

Ví dụ: Ethereum đã tích lũy được sự phức tạp to lớn trong nhiệm vụ trở thành một máy tính thế giới, nhưng nó lại bị cản trở bởi những vấn đề nhỏ có thể gây nguy hiểm cho khả năng hoạt động của hệ thống. Mọi DApp, bất kể giá trị kinh tế, chi phí bảo trì hay ý nghĩa pháp lý, có nên được đối xử như một công dân hạng nhất không?

Kiến trúc phân lớp

Trọng tâm thiết kế của IOG là đáp ứng các tính năng xã hội của Crypto, tạo các lớp bằng cách tách kế toán giá trị khỏi tính toán và đáp ứng nhu cầu của các nhà quản lý trong khi tuân thủ các nguyên tắc sáng lập.¹⁴⁷ IOG cũng đánh giá các giao thức thông qua đánh giá ngang hàng và mã Code được kiểm tra dựa trên các thông số kỹ thuật chính thức¹⁴⁸ bất cứ khi nào có thể.

Ngày 8 tháng 2 năm 2019, Charles Hoskinson: Bảo vệ đánh giá ngang hàng¹⁴⁹

...không giống như các tạp chí, đôi khi phải mất nhiều năm để nghiên cứu thực sự được xuất bản, được bình duyệt đầy đủ và thông qua hệ thống, các hội nghị diễn ra rất thường xuyên. Nếu bạn nhìn vào thế giới mật mã, bạn có Eurocrypt, CCS, Real World Crypto và hàng chục hội nghị khác hàng năm. Hầu như mỗi tháng có một số hình thức hội nghị đang diễn ra. Vì vậy, nó không làm bạn chậm lại để viết một bài nghiên cứu, theo một cách rất có cấu trúc, chu đáo, đưa nó vào một cuộc hội thảo và sau đó nhận được một số đánh giá từ cộng đồng. Đột nhiên, bây giờ bạn có một số người thông minh nhất trên thế giới thức dậy và cố gắng phá hủy lập luận của bạn, bởi vì họ biết rằng điều đó có lợi cho sự nghiệp học tập của họ nếu họ có thể tìm thấy một lỗ hổng trong bài nghiên cứu của bạn.

Cardano là một Crypto thừa nhận rằng 'tiền là xã hội'. Cấu trúc xã hội là một thứ xuất hiện thông qua sự tương tác của con người hơn là thực tế khách quan. Nó tồn tại bởi vì mọi người thừa nhận và tin tưởng vào nó. Quốc gia và tiền tệ là hai ví dụ về cấu trúc xã hội.

Tính linh hoạt và khả năng xử lý sự phức tạp trong bất kỳ giao dịch nào là rất quan trọng. Nếu dự án Cardano thành công trong việc mở rộng quy mô để hàng tỷ người sử dụng, thì các tài nguyên mạng, lưu trữ và điện toán khổng lồ sẽ được yêu cầu để xử lý đồng thời hàng tỷ giao dịch. Kiến trúc của Cardano kế thừa khái niệm tách biệt các mối quan tâm¹⁵⁰ khỏi TCP/IP.

¹⁴³

Tư duy theo nguyên tắc đầu tiên là một trong những cách tốt nhất để thiết kế ngược các vấn đề phức tạp và giải phóng các khả năng sáng tạo. Đôi khi được gọi là 'suy luận từ những nguyên tắc đầu tiên', ý tưởng là chia nhỏ các vấn đề phức tạp thành các yếu tố cơ bản và sau đó tập hợp chúng lại từ đầu.

¹⁴⁴

Dự án Scorex, iohk.io/projects/scorex/

¹⁴⁵

Tài liệu nghiên cứu của IOHK, iohk.io/research/library/

¹⁴⁶

Giao thức điều khiển truyền tải (TCP) là một trong những giao thức chính của **bộ Giao thức Internet (IP)**. Do đó, toàn bộ bộ thường được gọi là TCP/IP. TCP cung cấp khả năng phân phối đáng tin cậy, có thứ tự và được kiểm tra lỗi của một luồng octet (byte) giữa các ứng dụng đang chạy trên các máy chủ giao tiếp qua mạng IP. Các ứng dụng internet chính như World-Wide Web, email và truyền tệp đều dựa trên TCP.

¹⁴⁷

Tại sao lại là Cardano?, tại cardano.org/

¹⁴⁸

Duncan Coutts, 'Crypto cần một biện pháp bảo vệ để ngăn chặn một thảm họa DAO khác', iohk.io/blog/cryptocurrency-need-a-safeguard-to-prevent-another-DAO-disaster/

¹⁴⁹

Để bảo vệ đánh giá ngang hàng, youtube.com/watch?v=3-rbn73cUEk

¹⁵⁰

Tách các mối quan tâm là một nguyên tắc thiết kế để tách một chương trình máy tính thành các phần riêng biệt, sao cho mỗi phần giải quyết một mối quan tâm riêng biệt. Mỗi quan tâm là một tập hợp thông tin ảnh hưởng đến mã của chương trình máy tính.

Về cốt lõi, Blockchain là cơ sở dữ liệu sắp xếp các sự thật và sự kiện dựa trên dấu thời gian và tính bất biến để ghi lại quyền sở hữu tài sản. Sau đó, việc thêm tính toán phức tạp để lưu trữ và thực thi DApp là không hề nhỏ. Chúng ta có cần biết ai đó đang gửi bao nhiêu tiền không? Chúng ta có muốn tham gia vào việc giải mã toàn bộ câu chuyện của giao dịch không?

Để biết điều gì đang xảy ra, một giao thức duy nhất phải có khả năng hiểu các sự kiện tùy ý, viết tập lệnh giao dịch tùy ý, cho phép phân xử gian lận và thậm chí đảo ngược giao dịch khi có thông tin mới.

Sau đó, có vấn đề về việc quyết định thông tin nào cần giữ lại cho mỗi giao dịch, đây là một lựa chọn thiết kế đầy thách thức. Những thành phần nào của một tường thuật giao dịch có liên quan? Chúng có quan trọng trong tương lai không? Khi nào sẽ an toàn để loại bỏ một số dữ liệu? Làm như vậy có bất hợp pháp ở một số khu vực pháp lý nhất định không? Một số tính toán về bản chất là bí mật.¹⁵¹ Luôn luôn tốt để ghi nhớ sự khác biệt giữa tính bảo mật và quyền riêng tư.

Quyền riêng tư và tính bảo mật là hai khái niệm riêng biệt bảo vệ các loại dữ liệu khác nhau. 'Quyền riêng tư' được sử dụng liên quan đến dữ liệu được pháp luật bảo vệ. 'Tính bảo mật' đề cập đến các dữ liệu khác nhau có trong các hợp đồng và thỏa thuận hợp lệ.

Một giao dịch bao gồm hai phần: cơ chế gửi và ghi lại các luồng Token, cũng như lý do và hoàn cảnh chuyển Token. Cái sau có thể rất phức tạp, bao gồm hàng Gigabyte dữ liệu, chữ ký và sự xuất hiện của các tình huống không lường trước được. Với một chữ ký duy nhất di chuyển giá trị đến một địa chỉ khác, nó cũng có thể đơn giản.

Mô hình hóa các động cơ và hoàn cảnh của chuyển động giá trị là khó khăn bởi vì chúng mang tính cá nhân đối với các bên liên quan theo những cách không lường trước được nhất. Luật hợp đồng tạo ra một bức tranh thậm chí còn phức tạp hơn, trong đó các bên tham gia thậm chí có thể không nhận thức được rằng giao dịch không phù hợp với thực tế thương mại.¹⁵² Khái niệm này được gọi là "khoảng cách ngữ nghĩa".¹⁵³

Việc thiếu sự rõ ràng về mặt pháp lý xung quanh các biện pháp bảo vệ pháp lý của những người tham gia giao thức là một vùng xám khác. Không có giới hạn đối với những gì một loại Crypto tinh vi có thể làm. Một Blockchain như Cardano có thể vô tình tạo điều kiện cho tất cả các loại tội phạm và hành vi sai trái. Việc này phức tạp như thế nào trong thực tế đã được thảo luận trong các bài báo học thuật khác nhau, bao gồm *The Ring of Gyges*.¹⁵⁴ *sử dụng hợp đồng thông minh cho tội phạm*.¹⁵⁵

Cardano và Bitcoin có một lợi thế là chúng đã chọn chia thành các lớp. Bitcoin đã cho chúng ta Rootstock (rsk.co),¹⁵⁶ trong khi Lớp tính toán Cardano là đề xuất của Cardano.

¹⁵¹

Hoskinson công bố một hệ thống mới để giải quyết các vấn đề về bảo mật và quyền riêng tư, ambcrypto.com/hoskinson-announces-a-new-system-to-tackle-both-security-privacy-concerns/

¹⁵²

Mã ướt và mã khô, unnumerated.blogspot.com/2006/11/wet-code-and-dry.html

¹⁵³

Khoảng cách ngữ nghĩa đặc trưng cho sự khác biệt giữa hai mô tả về một đối tượng bằng các biểu diễn ngôn ngữ khác nhau, chẳng hạn như ngôn ngữ hoặc ký hiệu. Theo Hein, khoảng cách ngữ nghĩa có thể được định nghĩa là "sự khác biệt về ý nghĩa giữa các cấu trúc được hình thành trong các hệ thống biểu diễn khác nhau". Trong khoa học máy tính, khái niệm này có liên quan bất cứ khi nào các hoạt động, quan sát và nhiệm vụ thông thường của con người được chuyển thành một biểu diễn tính toán.

¹⁵⁴

Ring of Gyges là một cổ vật thần thoại, ma thuật được nhà triết học Plato nhắc đến trong *tác phẩm Republic của ông*. Nó ban cho chủ nhân của nó sức mạnh để trở nên vô hình theo ý muốn. Thông qua câu chuyện về chiếc nhẫn, *Republic* xem xét liệu một người thông minh có công bằng hay không, nếu họ không phải lo sợ bị tổn hại về danh tiếng nếu phạm phải những điều bất công.

¹⁵⁵

Ari Juels, Ahmed Kosba và Elaine Shi, 'The Ring of Gyges: sử dụng hợp đồng thông minh cho tội phạm', arjjuels.com/wp-content/uploads/2013/09/Gyges.pdf

¹⁵⁶

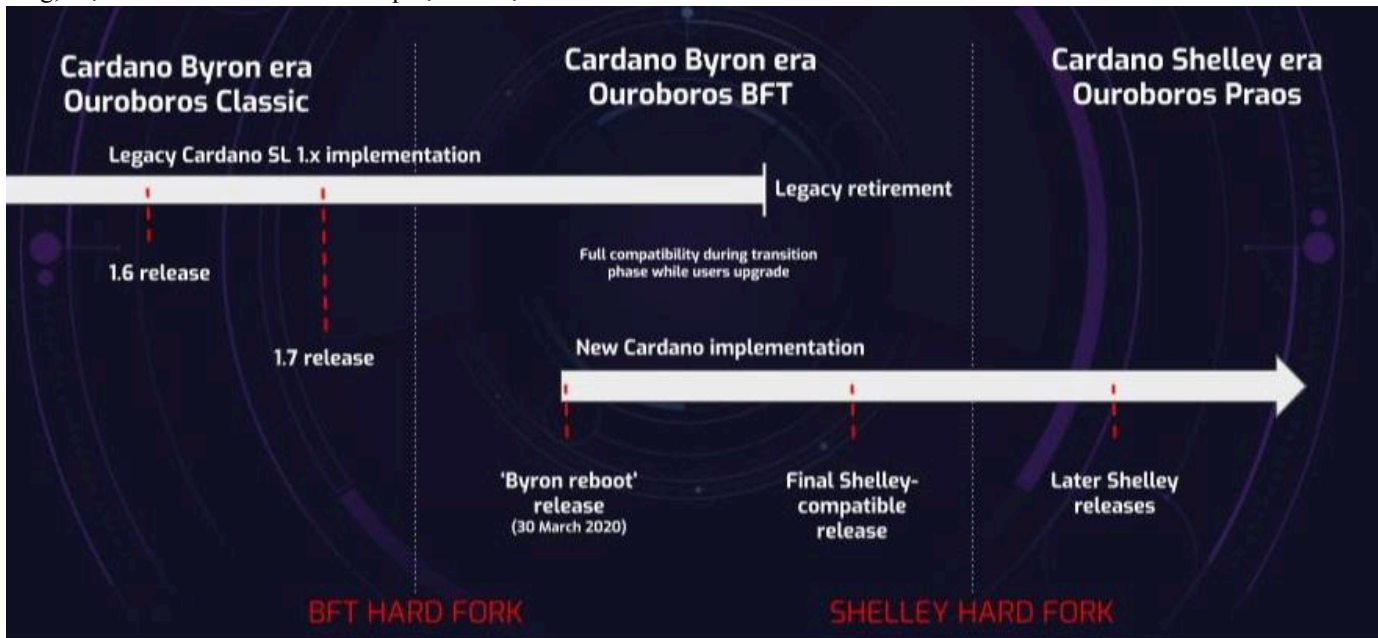
RootStock là một nền tảng ngang hàng hợp đồng thông minh được xây dựng dựa trên Blockchain Bitcoin. Mục tiêu của nó là tăng thêm giá trị và chức năng cho mạng Bitcoin cốt lõi bằng cách triển khai các hợp đồng thông minh dưới dạng Sidechain.

IOG cung cấp một thư viện tham chiếu về mã Code Plutus để các nhà phát triển ứng dụng sử dụng trong các dự án của họ, tương tự như dự án Zeppelin¹⁵⁷ dựa trên Solidity¹⁵⁸. IOG cũng đã tạo một bộ công cụ để xác minh chính thức dựa trên dự án Liquid Haskell.¹⁵⁹

Bài tiểu luận 'Tại sao lại chọn Cardano' từ năm 2017 mô tả tầm nhìn¹⁶⁰ cho Lớp thanh toán Cardano (CSL) so với Lớp tính toán Cardano (CCL). Chức năng tương tự tồn tại ngày nay, nhưng nó được triển khai khác với những gì được phác thảo trước đó.

Cách tiếp cận theo lớp được giữ nguyên nhưng việc tính toán được thực hiện trên chuỗi chính, Lớp 1. Điều này được triển khai rất cẩn thận vì sự phát triển của Plutus dựa trên các phương pháp chính quy và thiết kế an toàn sẽ không gây nguy hiểm cho các tài sản phi tập lệnh 'đơn giản' trên chuỗi.

Cơ sở mã Code đã được viết lại hoàn toàn theo định dạng mô-đun¹⁶¹ để chuẩn bị cho việc triển khai bộ tổ hợp Hardfork (HFC)¹⁶² vào tháng 3 năm 2020. Cách tiếp cận mô-đun giúp thực hiện các thay đổi với HFC dễ dàng hơn rất nhiều. 'Khởi động lại Byron' và HFC vào năm 2020, cùng với việc chuyển sang Ouroboros Praos, là nền tảng trong việc triển khai mã Code hỗ trợ tương lai của Blockchain. Đây là một bước ngoặt trong hiệu quả của dây chuyền và năng suất của IOG. Nó có thể chuyển sang lịch trình cập nhật hàng quý diễn ra ngày hôm nay. Không dự án đã làm bất cứ điều gì giống như HFC trước đây; nó làm cho việc nâng cấp trở nên dễ dàng, một ưu điểm khác của cách tiếp cận thể hệ thứ ba.



Hình 6: Lộ trình từ Mainnet Byron đến Shelley

¹⁵⁷ Jeevak Kasarkod, 'Zeppelin: khung nguồn mở hợp đồng thông minh an toàn cho các ứng dụng Blockchain', infoq.com/news/2016/10/zeppelin-secure-smart-contracts/

¹⁵⁸ Solidity là ngôn ngữ lập trình hướng đối tượng để viết hợp đồng thông minh. Nó được sử dụng để triển khai các hợp đồng thông minh trên các nền tảng Blockchain khác nhau, đáng chú ý nhất là Ethereum.

¹⁵⁹ Haskell lỏng, ucsd-progsys.github.io/liquidhaskell-blog/

¹⁶⁰ Tại sao Cardano? CCL, [tại sao.cardano.org/en/introduction/cardano-computation-layer/](https://cardano.org/en/introduction/cardano-computation-layer/)

¹⁶¹ Nói rộng ra, **tính mô đun** là mức độ mà các thành phần của hệ thống có thể được tách ra và kết hợp lại, thường mang lại lợi ích về tính linh hoạt và đa dạng trong sử dụng. Khái niệm về tính mô đun được sử dụng chủ yếu để giảm độ phức tạp bằng cách chia hệ thống thành các mức độ phụ thuộc và độc lập lẫn nhau khác nhau và 'che giấu sự phức tạp của từng phần đằng sau một giao diện và trừu tượng.'

¹⁶² Bộ kết hợp là một thuật ngữ kỹ thuật được sử dụng để chỉ sự kết hợp của các quy trình hoặc sự vật nhất định. Trong trường hợp của Cardano, một **bộ kết hợp hard fork** kết hợp các giao thức, do đó cho phép quá trình chuyển đổi Byron sang Shelley mà không làm gián đoạn hoặc khởi động lại hệ thống. Nó đảm bảo rằng số cái Byron và Shelley xuất hiện dưới dạng một số cái.

Charles Hoskinson đã giải thích cách tiếp cận theo lớp trong nhiều AMA (hỏi tôi bất cứ điều gì) trên YouTube của ông ấy. Đoạn trích từ một số trong số này được bao gồm dưới đây cho rõ ràng.

Ngày 21 tháng 4 năm 2019. Cardano có phải là một mô hình máy chủ sidechain không? CH:¹⁶³

Cardano luôn là một hệ thống hai lớp, vì vậy khái niệm về hệ thống thanh toán và ý tưởng về lớp kiểm soát... các lớp kiểm soát được phép hoặc không được phép¹⁶⁴ và chúng có thể có độ phức tạp tùy ý. Hệ thống thanh toán về cơ bản có mọi thứ bạn cần cho một loại Crypto dài hạn... về cơ bản, Cardano ở lớp thanh toán, giống như những gì tôi muốn Bitcoin trông như thế nào. [...]

Về mặt thiết kế khái niệm và thực tế là đặc điểm kỹ thuật chính thức, chúng tôi có hiểu biết tổng thể về các số cái cần trông như thế nào, hệ thống kế toán đằng sau chúng... chúng tôi có hiểu biết cực kỳ phức tạp về sự đồng thuận trông như thế nào và sự đánh đổi của sự đồng thuận. Chúng tôi có hiểu biết chi tiết về khả năng tương tác; chúng tôi hiểu cách mở rộng mô hình UTXO để bao gồm nhiều tập lệnh như bạn muốn... nhưng thực hiện điều này theo cách rất an toàn khi bạn có thể dự đoán được chi phí gas

Ngày 9 tháng 7 năm 2020. Suy nghĩ về Giao tiếp Cross-Chain, Sidechain, NiPoPoW và Litecoin¹⁶⁵

Bạn có thể có một mô hình tối đa... nếu họ (Bitcoin) thực sự triển khai công nghệ này, thì nó thực sự sẽ có tính cạnh tranh. Họ đã có từ năm 2014 để làm điều đó nhưng họ đã không làm được. Đây là khái niệm về chuỗi sơ cấp - thứ cấp. Từng được gọi là ông chủ – nô lệ, nhưng ngôn ngữ đó đang nhanh chóng không còn được sử dụng ngay cả trong các ngữ cảnh khác nhau. Về cơ bản, chúng tôi đã làm điều này trong sách trắng ban đầu của mình, chúng tôi đã nói khái niệm SL (lớp thanh toán) và CL (lớp tính toán)... vì vậy, ý tưởng là có một chuỗi chính và đó là nơi tồn tại của Token, ADA. Sau đó, Token ADA đó có thể được sử dụng để cung cấp năng lượng cho các chuỗi khác nhau, có Logic mạng khác nhau, nó có các quy tắc đồng thuận khác nhau, nó có các quy tắc số cái khác nhau, một mô hình tính toán khác và bằng cách nào đó các chuỗi này không có Token gốc của riêng chúng... đúng hơn chúng là dịch vụ của chuỗi chính. Vì vậy, hãy xem xét điều này trong bối cảnh của ITN (mạng thử nghiệm được khuyến khích).

Giả sử rằng chúng tôi sửa đổi Ouroboros.... Ouroboros ngay bây giờ khi bạn là SPO, thay vì chỉ nhận được một Block, bạn nhận được Block Cardano... nhưng sau đó bạn cũng sẽ nhận được Block CL1, Block CL2... Block CLn ... nếu bạn là SPO, khi công việc của bạn bắt đầu là mở rộng trạng thái của chuỗi, bạn sẽ thực sự làm điều đó cho từng mạng trong số này ngoài SL. Vì vậy, bạn sẽ tạo Block Cardano bình thường, giống như tất cả các SPO vẫn làm, nhưng sau đó bạn sẽ tạo Block cho mạng tiếp theo, Block cho mạng tiếp theo... bạn sẽ tra cứu Logic mạng, những sự đồng thuận, quy tắc và Logic số cái. Bạn sẽ tuân theo mô hình tính toán, và tất cả những điều này sẽ khác nhau.

[...] Đây là một loại mô hình được hình dung ra từ Blockstream¹⁶⁶ khi họ đang nói về Sidechain. Họ nói rằng Bitcoin có thể là phiên bản SL đó, và nó có thể rất đơn giản, an toàn và bảo mật. Sau đó bạn có thể có Ethereum như một Sidechain của Bitcoin, gửi Bitcoin của bạn vào Sidechain đó, vận hành và sau đó gửi lại Bitcoin của bạn khi bạn hoàn thành.

Ngày 30 tháng 12 năm 2020. Sự khác biệt giữa lớp tính toán và lớp thanh toán của Cardano có còn phù hợp không? CH:¹⁶⁷

Trên thực tế, các Sidechain mà chúng tôi sẽ chạy là những ví dụ về cái mà tôi gọi là lớp tính toán. Sự khác biệt là chúng không phải là phù du, chúng thực sự ở đó vĩnh viễn... đó chính xác là những gì chúng tôi dự định. Bạn có một hệ thống thanh toán an toàn rất ổn định, đây là mạng chính với các SPO... Bạn có bộ sưu tập các Sidechain này thực hiện những việc khác nhau và có các mô hình tính toán khác với chuỗi chính.

Bối cảnh quy định

¹⁶³

Bản tóm tắt sau hội nghị, suy nghĩ và AMA 21/04/2019, youtu.be/pBXZVrBQ6U8?t=3325

¹⁶⁴

Được phép v không được phép . Ở cấp độ đơn giản nhất, sự khác biệt nằm ở chỗ thiết kế của mạng mở cho bất kỳ ai tham gia – không được phép – hay chỉ giới hạn cho những người tham gia được chỉ định hoặc được phép.

¹⁶⁵

Suy nghĩ về giao tiếp chuỗi chéo, Sidechain, NiPoPoW và Litecoin, youtube.com/watch?v=HvIAGdeUC4o,

¹⁶⁶

Blockstream là một công ty công nghệ Blockchain do người đồng sáng lập ADAM Back lãnh đạo. Blockstream dự định phát triển phần mềm để 'ngắt' các giao dịch khỏi mạng bitcoin và tính một khoản phí cố định hàng tháng để cho phép mọi người sử dụng 'Sidechains' thay thế. Blockstream sử dụng một số lượng lớn các nhà phát triển Bitcoin Core nổi bật.

¹⁶⁷

Phiên bản đặc biệt AMA năm mới 2020, youtu.be/GtWt68kp1dg?t=777

Nếu một hệ thống tài chính phát triển và đạt được sự chấp nhận thì nó sẽ nảy sinh nhu cầu về quy định, hoặc ít nhất là mong muốn về nó. Đây thường là hậu quả của sự đổ vỡ định kỳ của thị trường do sự kém cỏi của những tác nhân.

Ví dụ, cuộc khủng hoảng Knickerbocker năm 1907 đã dẫn đến việc thành lập Hệ thống Dự trữ Liên bang với tư cách là người cho vay cuối cùng vào năm 1913. Một ví dụ khác là sự thái quá của Hoa Kỳ trong những năm 1920, kết thúc bằng cuộc Đại suy thoái, một cuộc khủng hoảng tài chính tàn khốc. Ủy ban Giao dịch Chứng khoán được thành lập vào năm 1934 do sự sụp đổ này nhằm cố gắng tránh lặp lại vụ việc hoặc ít nhất là buộc những kẻ vô đạo đức phải chịu trách nhiệm. Block Genesis của Bitcoin ghi lại nội dung "Thủ tướng trên bờ vực cứu trợ thứ hai cho các ngân hàng"¹⁶⁸ thể hiện một số nguồn cảm hứng từ các sự kiện vào thời điểm đó.

Người ta có thể đặt câu hỏi về sự cần thiết, phạm vi và tính hữu ích của quy định, nhưng người ta không thể phủ nhận rằng nó tồn tại và các chính phủ lớn đã thực hiện nó một cách nhiệt tình, với nhiều người sau đó đã quay đầu lại khi họ nhận ra hậu quả.¹⁶⁹ Cardano, giống như các hệ thống tài chính khác, phải có quan điểm về những gì công bằng và được chấp nhận trong thiết kế của nó. Cardano đã chọn phân biệt giữa quyền cá nhân và quyền thị trường.

Các cá nhân phải luôn có toàn quyền kiểm soát tài chính của mình, không bị cưỡng chế hoặc tịch thu tài sản dân sự. Nguyên tắc này phải được thực thi bởi vì, như các cuộc khủng hoảng ở Venezuela, Zimbabwe và Síp đã cho thấy trước đây, và cuộc chiến đang diễn ra ở Ukraine ngày nay cho thấy, không phải tất cả các chính phủ đều có thể được tin tưởng là không lạm dụng quyền lực tối cao của mình để làm giàu cho cá nhân các nhà lãnh đạo tham nhũng. Crypto phải được thiết kế với mẫu số chung thấp nhất trong tâm trí.

Không bao giờ nên có bất kỳ sự can thiệp nào vào lịch sử. Tính bất biến được hứa hẹn bởi các Blockchain. Việc giới thiệu khả năng viết lại lịch sử hoặc hồ sơ chính thức mang đến quá nhiều cảm dỗ thay đổi quá khứ để có lợi cho những tác nhân nhất định.

Không nên hạn chế sự di chuyển của cải. Nhân quyền bị tổn hại bởi các hạn chế về vốn và các rào cản nhân tạo khác. Bên cạnh việc không thể thực thi chúng, trong một thị trường toàn cầu nơi nhiều cư dân ở các nước đang phát triển di cư ra khỏi khu vực tài phán của họ để tìm kiếm thu nhập đủ sống, việc hạn chế dòng vốn thường gây hại cho những người nghèo nhất thế giới.

Theo những khái niệm này, thị trường tách biệt với con người. Mặc dù Cardano tin vào các quyền cá nhân, nhưng thị trường cũng có quyền thể hiện công khai các điều khoản và điều kiện của nó. Nếu một người quyết định tiến hành kinh doanh bên trong thị trường này, họ phải tuân theo các Điều khoản & Điều kiện đó vì lợi ích của tính toàn vẹn của hệ thống.

Ngày 30 tháng 12 năm 2020. SEC (Ủy ban Chứng khoán & Sàn giao dịch) có phải là kẻ thù của Crypto không? CH:¹⁷⁰

Không...các cơ quan quản lý không phải là kẻ thù của Crypto... thành thật mà nói ngành của chúng tôi đã tạo ra Bitconnect,¹⁷¹ OneCoin,¹⁷² Mt Gox,¹⁷³ Bitmex¹⁷⁴... hàng ngàn vụ lừa đảo đã làm tổn thương mọi người. Theo một cách tốt, các cơ quan quản lý giống như ma cà rồng. Họ đến khi bạn mời họ. Một ma cà rồng đứng ở cửa nói, 'tôi vào được chứ?' ...điều gì đưa cơ quan quản lý vào một ngành? Các ngành hoạt động và mọi thứ đang diễn ra tốt? ... như toán học có bao nhiêu cơ quan quản lý? Có hoa hồng trao đổi toán học không? ...ngồi xuống và nói rằng 'chúng ta có thực sự cần xem xét những nhà cấu trúc liên kết đó không? họ là những kẻ gian manh, chúng tôi rất quan tâm đến số liệu thống kê. Có một số vấn đề ở đó, vấn đề nghiêm trọng, 64% mọi người biết điều đó...'

¹⁶⁸

Thủ tướng sắp có gói cứu trợ thứ hai cho các ngân hàng, coindesk.com/podcasts/the-breakdown-with-nlw/13-years-on-the-meaning-of-chancellor-on-the-brink-of-second-bailout-cho-ngan-hang/

¹⁶⁹

' Giờ đây, Ấn Độ đã rút lại lệnh cấm Crypto, đây là cách họ lên kế hoạch phát triển tiền kỹ thuật số theo cách riêng của mình ', fortune.com/2022/02/02/india-crypto-ban-plans-develop-digital-currency-taxes-quy-dinh-bitcoin/

¹⁷⁰

Phiên bản đặc biệt AMA năm mới 2020, youtu.be/GtWt68kp1dg?t=7282

¹⁷¹

Người sáng lập BitConnect bị truy tố trong Kế hoạch Crypto trị giá 2,4 tỷ đô la toàn cầu, [Justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme](https://justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme)

¹⁷²

Những gì chúng ta có thể học hỏi từ OneCoin , trò lừa đảo lớn nhất của Crypto , crazy.com/the-ascent/cryptocurrency/articles/what-we-can-learn-from-onecoin-cryptos-biggest-scam/

¹⁷³

Các khoản thanh toán cho khoản thanh toán 9 tỷ đô la bitcoin từ sự sụp đổ của Mt. Gox có thể bắt đầu sau vài tháng nữa, market.businessinsider.com/news/currencies/mt-gox-bitcoin-settlement-payouts-9-billion-dollars-early-2022-2021-11

¹⁷⁴

Tòa án Liên bang yêu cầu BitMEX trả 100 triệu đô la cho việc điều hành bất hợp pháp nền tảng giao dịch Crypto và vi phạm chống rửa tiền, cftc.gov/PressRoom/PressReleases/8412-21

KHÔNG! bởi vì nó giống như... những vụ bê bối nào xảy ra trong thế giới toán học? Thịnh vượng chúng tôi có một người từng đoạt huy chương lĩnh vực lớn tuổi tuyên bố rằng ông đã chứng minh giả thuyết Riemann và hóa ra bộ não của ông đã bị tổn thương và nó chỉ là một nghiên cứu rác! Chúng tôi khá giỏi trong việc tự điều chỉnh trong ngành đó. Mặt khác, tại sao ngành công nghiệp được phẩm được quản lý? Bởi vì chúng tạo ra những thử mà bạn đưa vào cơ thể con người. Nếu chúng tạo ra chúng, chúng sẽ làm gãy dương vật của bạn, chúng sẽ làm hỏng não của bạn, chúng sẽ làm hỏng mắt của bạn, bạn sẽ bị điếc.... hơn một người đã bị điếc ngay từ lần đầu tiên phản ứng với thuốc kháng sinh. Có đủ loại điều tồi tệ có thể xảy ra...vì vậy bạn cần quản lý nó! Bởi vì có những động cơ xấu chống lại sức khỏe của bạn!

...

Hãy nhìn vào Crypto, bạn có sự bùng nổ của ICO (Phát hành Token lần đầu), bạn có vô số vụ bê bối và lừa đảo, bạn có giao dịch nội gián tràn lan, bạn có giao dịch rửa trên các sàn giao dịch, bạn có các sàn giao dịch thất bại, những người đứng đầu sàn giao dịch đang ăn cắp tiền và trốn ra nước ngoài, bạn có những lỗ hổng phần mềm được tạo ra với mục đích ăn cắp tiền của mọi người, bạn có những thông tin sai lệch nghiêm trọng... bạn có những hành vi mạo danh... bạn có những người tuyên bố rằng họ đang sử dụng vốn dự án cho một thứ gì đó nhưng thực ra họ đang sử dụng để mua du thuyền và những ngôi nhà ở Miami và gái mại dâm ...

Đó là một bảng hiệu đèn Neon lớn trước cửa nhà bạn.... 'Ma cà rồng vào đi!' ...ngành công nghiệp của chúng tôi đã làm điều đó, chúng tôi đã không tự điều chỉnh, chúng tôi đã không ngăn chặn những thất bại của cơ quan, chúng tôi đã tạo ra một bảng hiệu đèn neon và chào đón một con ma cà rồng, và giờ chúng đang ở đây! ... chúng ta sẽ phản nản rằng họ đang làm những việc... đệ đơn kiện, tham gia như một con bò đực trong một cửa hàng ở Trung Quốc... tất nhiên rồi, và khả năng hành động của họ tỷ lệ thuận với sự phức tạp của các công cụ và sự hiện đại của luật lệ. Bài kiểm tra *Howey*¹⁷⁵ là một sản phẩm của những năm 1940...nó không thể hoạt động trong lĩnh vực tài chính 'tế bào gốc', nơi một tài sản có thể là tất cả... nó có thể đồng thời là tiền tệ, hàng hóa và chứng khoán, có thể là tất cả và không là gì cả ...

Vào tháng 6 năm 2022, Charles Hoskinson đã phát biểu¹⁷⁶ trước Quốc hội về 'Tương lai của quy định về tài sản kỹ thuật số'. Ông ấy không tập trung sự chú ý vào Cardano mà thay vào đó, ông ấy nói thay cho toàn bộ ngành. Thông điệp chính mà ông ấy gửi tới các đại diện là nói chung, Cryot nên được coi là tế bào gốc tài chính thay vì được định nghĩa cứng nhắc là chứng khoán, tiền tệ hoặc hàng hóa. Luật pháp trong tương lai nên dựa trên các nguyên tắc, không tập trung vào các khu vực pháp lý hoặc cơ quan riêng lẻ. Đóng góp của ông ấy đã được đón nhận rộng rãi.¹⁷⁷

Tầm nhìn Cardano

Cardano là một dự án dài hạn được hưởng lợi từ đầu vào của hàng trăm bộ óc thông minh nhất thế giới, cả trong và ngoài lĩnh vực Crypto. Nó đòi hỏi phải lặp đi lặp lại liên tục, đánh giá ngang hàng tích cực và tận dụng những phát hiện của nghiên cứu nguồn mở.

Mặc dù không có dự án nào có thể đáp ứng tất cả các mục tiêu hoặc làm hài lòng tất cả người dùng, nhưng IOG dự định trình bày tầm nhìn về một hệ thống tài chính tự phát triển sẽ như thế nào đối với các quốc gia không có dự án đó. Trên thực tế, Crypto sẽ không thay thế các tổ chức tài chính hiện tại. Các hệ thống tài chính truyền thống luôn có khả năng hấp thụ thay đổi. Thay vào đó, sẽ hiệu quả hơn nếu tập trung vào các khu vực tài phán nơi việc triển khai hệ thống ngân hàng cũ quá tốn kém, nơi nhiều người sống sót với ít hơn vài đô la một ngày, không có giấy tờ tùy thân cố định và khó tiếp cận tín dụng.

Khả năng kết hợp hệ thống thanh toán, quyền sở hữu, danh tính, tín dụng và bảo vệ rủi ro vào một ứng dụng dành cho thiết bị di động không chỉ mang lại lợi ích mà còn thay đổi cuộc sống ở những khu vực này. IOG tin rằng Cardano có thể phát triển dựa trên thành

¹⁷⁵

Phép thử Howey : Ủy ban Chứng khoán và Hối đoái (SEC) v. WJ Howey Co. (1946). Vụ việc dẫn đến một phép thử, được gọi là **phép thử Howey** , để xác định xem một công cụ có đủ điều kiện là 'hợp đồng đầu tư' theo các mục đích của Đạo luật Chứng khoán hay không: 'một hợp đồng, giao dịch hoặc kế hoạch theo đó một người đầu tư tiền của mình vào một doanh nghiệp chung và dẫn đến việc mong đợi lợi nhuận chỉ từ những nỗ lực của người quảng bá hoặc bên thứ ba. Thử nghiệm Howey vẫn là một yếu tố quyết định đáng chú ý đối với sự giám sát theo quy định trong nhiều thập kỷ. Trong vài năm qua, nó đã được đặt câu hỏi, thường xuyên nhất là khi kết hợp với các cuộc thảo luận về Crypto và công nghệ Blockchain '.

¹⁷⁶

Tương lai của quy định về tài sản kỹ thuật số, [youtube.com/watch?v=K4ZM2AIGT-s](https://www.youtube.com/watch?v=K4ZM2AIGT-s)

¹⁷⁷

Nhà sáng lập Cardano thể hiện xuất sắc tại phiên điều trần của Quốc hội về quy định Crypto, cryptoslate.com/cardano-founder-steals-the-show-at-congressional-hearing-on-crypto-regulation/

công của các dự án như M-pesa¹⁷⁸ và Kiva.¹⁷⁹ Nếu Cardano có thể thay đổi cách hình thành, phát triển và cấp vốn cho Crypto, thì chúng ta đang hướng tới 'thế giới tốt nhất trong tất cả các thế giới có thể' của Tiến sĩ Pangloss.¹⁸⁰

Đăng sau những cái tên

Tại sao nó được gọi là Cardano? CH giải thích:¹⁸¹

Girolamo Cardano là một người cuối cùng của thời Phục hưng, ông ấy là bác sĩ, luật sư, nhà toán học, ông ấy cũng là một con bạc, một kẻ hoàn toàn vô lại. Ông ấy là bác sĩ riêng của Giáo hoàng nhưng sau đó phải chịu hình phạt và tuyệt thông nhưng vẫn đi chơi với Giáo hoàng ngay cả sau khi bị phạt, vì Giáo hoàng thích ông ấy. Ông ấy suýt giết một trong những người con trai của mình trong một cuộc đấu kiếm vì họ ngủ với cùng một người phụ nữ. Ông ấy cũng là một tay cờ bạc. Ông ấy cũng đã phát minh ra rất nhiều lý thuyết xác suất chỉ để có thể trở thành một tay cờ bạc giỏi hơn. Vì vậy, Ông ấy đã tạo ra tất cả toán học cao cấp chỉ để có thể đếm bài và tung xúc xắc đúng cách, v.v. Ông ấy có thói quen bị đuổi khỏi các thành phố... Ông ấy cũng là một nhà mật mã vì ở Ý thời Phục hưng, họ có rất nhiều âm mưu giữa các gia đình ngân hàng. Vì vậy, ông ấy đã phát minh ra thiết bị bánh xe để mã hóa tin nhắn, để họ giữ bí mật liên lạc giữa các gia đình. Tôi mới đọc về ông ấy nhiều năm trước và nghĩ rằng ông ấy là một trong những người thú vị nhất mà tôi từng đọc trong đời. Vì vậy, tôi đã nghĩ đến một loại Crypto, nó có thể làm cả điều tốt lẫn điều xấu. Nó cũng làm được một chút của mọi thứ và là một hệ thống thú vị. Tôi nghĩ thật tuyệt khi đặt tên cho nó theo tên Cardano.

Ông ấy là một trong những kẻ sống một cuộc sống giàu có đến khó tin, không tử tế, không xấu xa, ông ấy ở đâu đó ở giữa. Về cơ bản, ông đã xây dựng lý thuyết xác suất hiện đại vì ông muốn trở thành một tay cờ bạc giỏi hơn. Ông ấy cũng vô tình tạo ra quy trình đánh giá ngang hàng của Ý bởi vì vào thời điểm đó, xung quanh ông ấy hầu hết là các nhà khoa học ở Ý, những người sẽ bảo vệ kiến thức của họ và không công bố bất cứ điều gì vì đó là một cách để duy trì việc làm. Vậy làm thế nào để bạn có được chức giáo sư tại một trường đại học ở Ý. Bạn sẽ đi thuyết trình với sinh viên. Nếu họ cảm thấy bạn có kiến thức, họ sẽ đồng ý, người này nên là một phần của hệ thống của chúng tôi, vì vậy mọi người không muốn xuất bản bất cứ thứ gì vì nó sẽ hủy hoại thương hiệu của họ, họ đã giữ bí mật mọi thứ.

Những gì Cardano sẽ làm, ông ấy sẽ chuốc cho mọi người say khướt và tìm hiểu tất cả bí mật của họ. Ông ấy đã viết tất cả chúng ra giấy và xuất bản những cuốn sách về điều này, điều cực kỳ cấm kỵ và bao gồm cả cách tính đa thức bậc bốn...ông ấy đã học được điều đó từ Tartaglia¹⁸²...có nghĩa là người nói lắp. Vì vậy, ông ấy là một người huyền thoại. Tôi nghĩ ông ấy thậm chí còn là người cùng thời với DaVinci. Tôi cho rằng đó sẽ là cái tên hoàn hảo cho một loại Crypto bởi vì Crypto không tốt cũng không xấu, nó là một thứ trung lập, nó tuyệt vời và đầy cảm hứng, đó là một điều hơi phức tạp và mọi người đều có ý kiến về nó. Bạn sẽ không bao giờ hiểu được một cách rõ ràng và ngắn gọn, nhưng nó chắc chắn có tác động rất lớn và đó là con người của thời đại.

Nhưng một điều nữa là khi bạn có Crypto, bạn có tên giao thức, sau đó bạn có tên tiền tệ. Trong Bitcoin, đó là Bitcoin, nó giống nhau, nhưng trong các hệ thống khác thì chúng khác. Vì vậy, những gì tôi quyết định làm với Cardano là tôi đặt tên cho loại tiền này là ADA, theo tên của ADA Lovelace.¹⁸³ Bà ấy là một nhân vật tiên phong trong thế kỷ 19, nữ lập trình viên đầu tiên được chú ý, bạn tốt của Charles Babbage. Bà ấy để lại một di sản vĩ đại và truyền cảm hứng cho các thế hệ phụ nữ. Bà ấy tham gia vào khoa học và trở thành nhà phát triển. Tôi muốn nói rằng người kế thừa tinh thần của ADA Lovelace ở thế

¹⁷⁸

M-Pesa (M cho điện thoại di động, pesa là tiếng Swahili cho tiền) là một dịch vụ chuyển tiền, tài chính và tài chính vi mô dựa trên điện thoại di động, được Vodafone ra mắt vào năm 2007 cho Safaricom và Vodacom, nhà khai thác mạng di động lớn nhất ở Kenya và Tanzania. Kể từ đó, nó đã mở rộng sang Afghanistan, Nam Phi, Ấn Độ và vào năm 2014 đến Romania và năm 2015 đến Albania. M-Pesa cho phép người dùng gửi, rút tiền, chuyển tiền và thanh toán hàng hóa và dịch vụ (Lipa na M-Pesa) một cách dễ dàng bằng thiết bị di động.

¹⁷⁹

Kiva (thường được biết đến với tên miền Kiva.org) là một tổ chức phi lợi nhuận, nền tảng cho vay trực tuyến đầu tiên trên thế giới kết nối những người cho vay trực tuyến với các doanh nhân trên toàn cầu. Sứ mệnh của Kiva là 'mở rộng khả năng tiếp cận tài chính để giúp các cộng đồng chưa được phục vụ phát triển.'

¹⁸⁰

Những thế giới tốt nhất có thể, everipedia.org/wiki/lang_en/Best_of_all_possible_worlds

¹⁸¹

Một số suy nghĩ và cập nhật ngẫu nhiên, youtu.be/ttFptsL5hN0?t=4353

¹⁸²

Tartaglia, everipedia.org/wiki/lang_en/Niccol%25C3%25B2_Fontana_Tartaglia

¹⁸³

Chúc mừng sinh nhật ADA!, youtube.be/hhAOJyi_3lA?t=27

kỷ 20 là Grace Hopper, người tạo ra COBOL (Ngôn ngữ định hướng kinh doanh thông dụng) và cũng là người chịu trách nhiệm về lỗi máy tính, cũng có một di sản tuyệt vời ở đó.

Khi chúng tôi đặt tên cho hệ sinh thái Cardano và suy nghĩ cẩn thận về tên gọi, giao thức cũng như đặt tên cho loại tiền tệ nào, tôi muốn kết nối mọi phần của Cardano với những nhân vật lịch sử, những người đã làm điều gì đó độc đáo và đặc biệt trong cuộc đời họ, không nhất thiết phải là người giỏi nhất. Chẳng hạn, bản thân Cardano là một nhà toán học đa tài và xuất sắc, nhưng đôi khi ông ấy cũng là một kẻ vô lại. Trên thực tế, nếu bạn đọc tiểu sử của ông ấy, tôi sẽ ngạc nhiên khi Hollywood chưa làm một cuốn sách hay một bộ phim nào về Cardano, bởi vì ông ấy là một chàng trai tuyệt vời. Nhưng ADA là một trong những người tốt. Bà ấy đã sống một cuộc đời đáng kinh ngạc và để lại một di sản đáng kinh ngạc.

Sau đó, tôi đặt tên cho mọi bản phát hành chính của Cardano theo tên của một nhà thơ nổi tiếng hoặc nhà khoa học máy tính nổi tiếng hoặc ai đó mà tôi được truyền cảm hứng. Ví dụ, Byron được đặt theo tên Lord Byron. Goguen là một nhà khoa học máy tính nổi tiếng thế giới, người đã làm rất nhiều công việc mà tôi ngưỡng mộ.

Lord Byron là một trong những nhà thơ yêu thích của tôi, ông ấy đã viết *She Walks in Beauty*.¹⁸⁴ Vì vậy, tôi đã nói rằng thật tuyệt nếu có được kết nối Byron và mang nó vào. Tôi cũng muốn có sự cân bằng, nếu tôi đặt tên thứ gì đó theo tên con trai, thì tôi muốn đặt tên thứ gì đó theo tên con gái. Vì vậy, hãy luôn có sự cân bằng tốt đẹp giữa nữ tính và nam tính bên trong hệ thống. Đó là nơi mà nó đến từ.

Kế hoạch đặt tên đến từ đâu trong Cardano? CH giải thích:

Họ chỉ là tất cả những người mà tôi ngưỡng mộ trong đời... Tác phẩm của Voltaire, và tôi đã đọc tác phẩm của Shelley, và một số trong đó là những câu chuyện mang tính cảnh báo, - chẳng hạn như Percy Shelley đã viết *Ozymandias*.¹⁸⁵

Cái tên Shelley thật thú vị, thực ra có hai Shelley nổi tiếng. Có Mary Shelley và Percy Shelley. Nhiều người nghĩ đó là Mary Shelley vì bà ấy nổi tiếng hơn trong hai người. Bà ấy đã viết *Frankenstein* và rất nhiều cuốn sách khác, và chồng của bà ấy Percy là một nhà thơ nổi tiếng, ông ấy cũng là thành viên của Illuminati, ông ấy đã đi khắp thế giới và là một nghệ sĩ. Ông ấy đã làm rất nhiều điều tuyệt vời. Thực ra, tôi đặt tên Shelley theo tên Percy, nhưng tại thời điểm này, rất nhiều người nhầm lẫn nó với Mary. Tôi nói hãy lựa chọn của bạn. Vấn đề là, cho dù một hệ thống tập trung có vĩ đại đến đâu, thì cũng có khái niệm rằng cuối cùng thời gian sẽ thay thế nó và vì vậy Shelley đã viết một bài thơ rất nổi tiếng tên là *Ozymandias* về một du khách đã đến Ai Cập. Ông anh ấy đã nhìn thấy tất cả những di tích đồ sộ này từ lâu lắm rồi và chỉ đang bình luận về thực tế là tất cả chúng đều đang mục nát.

Tôi cũng nhìn nó theo cùng một cách, rằng mọi thứ đều phải thay đổi cho dù ý tưởng ban đầu của bạn có tuyệt vời đến đâu. Thời gian thay thế vị trí của nó, vì vậy đây là một lời nhắc nhở rằng các hệ thống này cần phải thường xuyên cảnh giác, cập nhật và bảo trì để thực sự tự duy trì. Bây giờ nó nằm trong tay không phải của một nhà lãnh đạo, mà là của cộng đồng để làm điều đó với Shelley. Vì vậy, tôi cảm thấy đó là một cách đặt tên thích hợp, nhưng khi tôi nói bản phát hành có tên là Shelley, mọi người chỉ cho rằng đó là Mary và họ đang trích dẫn *Frankenstein* khi nó ra mắt và tôi nói, 'chết tiệt'. Được rồi, đó là Mary nếu bạn muốn, họ đã kết hôn, vì vậy nó cũng ổn.' Dù sao, nó đã được đón nhận nồng nhiệt.¹⁸⁶

Tại sao biểu tượng của ví Daedalus lại là đầu con bò? CH:¹⁸⁷

Đó không phải là đầu của một con bò, đó là đầu của một con Minotaur. Minotaur là một sinh vật thần thoại sống trong mê cung. Chúng tôi đặt tên ví là Daedalus, nhân vật lịch sử, hay nhân vật thần thoại, cha đẻ của Icarus và là người tạo ra mê cung. Mê cung được xây dựng bởi vì không có xiềng xích nào có thể trói được con Minotaur. Về cơ bản bằng cách xây dựng một mê cung khổng lồ và đặt con Minotaur vào đó, nó không thể thoát khỏi mê cung. Vì vậy, Daedalus là tên của ví Cardano. Daedalus là người tạo ra mê cung và Minotaur là sinh vật nổi bật nhất trong mê cung, đó là lý do tại sao lại chọn biểu tượng là Minotaur.

Byron được đặt theo tên của nhà thơ Romantic, bố của ADA Lovelace. Thư viện Anh¹⁸⁸ mô tả ông là 'Tận tụy với tự do suy nghĩ và

¹⁸⁴

¹⁸⁵ *She Walks in Beauty*, thơ ca.org/poems/43844/she-walks-in-beauty

¹⁸⁶

¹⁸⁷ *Ozymandias*, [thorfoundation.org/poems/46565 / ozymandias](https://thorfoundation.org/poems/46565/ozymandias)

¹⁸⁸

Charles Hoskinson - Xây dựng một thế giới tốt đẹp hơn với Blockchain, podcasts.apple.com/us/podcast/charles-hoskinson-building-a-better-world/id1553861681?i=1000517944232

¹⁸⁷

Phiên bản đặc biệt AMA Năm Mới 2020, youtu.be/GtWt68kp1dg?t=8496

¹⁸⁸

hành động, đồng thời vô chính phủ trong quan điểm chính trị và đạo đức cá nhân, nhà thơ và nhà thám hiểm Lord Byron là hiện thân của người anh hùng Romantic.'

Lord Byron là một nhà thơ, đồng nghiệp và chính trị gia người Anh, người đã trở thành một nhà cách mạng trong Chiến tranh giành độc lập của Hy Lạp. Ông được coi là một trong những nhân vật lịch sử hàng đầu của phong trào Romantic trong thời đại của ông. Ông được coi là một trong những nhà thơ người Anh vĩ đại nhất và vẫn được đọc rộng rãi và có ảnh hưởng. Trong số các tác phẩm nổi tiếng nhất của ông là những bài thơ tự sự *Childe Harold's Pilgrimage* và *Don Juan*, một bài thơ châm biếm dài trong đó Byron miêu tả Juan là một người dễ bị phụ nữ quyến rũ, đảo ngược truyền thuyết về Don Juan là một kẻ lãng nhăng thực sự.

Ông ấy đã đi du lịch khắp châu Âu, đặc biệt là ở Ý, nơi ông ấy đã sống bảy năm ở các thành phố Venice, Ravenna và Pisa. Trong thời gian ở Ý, ông ấy thường xuyên đến thăm người bạn và nhà thơ đồng nghiệp của mình, Percy Shelley. Sau này khi lớn lên, Byron tham gia Chiến tranh giành độc lập của Hy Lạp chống lại Đế chế Ottoman và chết vì bệnh khi dẫn đầu một chiến dịch trong cuộc chiến đó, mà người Hy Lạp tôn kính ông như một anh hùng dân tộc. Thường được mô tả là người khoa trương và khét tiếng nhất trong các tác phẩm lãng mạn, Byron được coi là một nhân vật nổi tiếng trong thời đại của ông vì sự thành công của ông với tư cách là một nhà thơ lãng mạn và vì sự thái quá của giới quý tộc, bao gồm những khoản nợ khổng lồ và nhiều vụ bê bối tình dục - nhiều cuộc tình với cả nam và nữ. Một trong những người tình của ông ấy, Lady Caroline Lamb, đã nói tóm tắt ông ấy bằng cụm từ nổi tiếng 'điên rồ, tồi tệ và nguy hiểm'. Đứa con hợp pháp duy nhất của ông là ADA Lovelace, được coi là nhân vật nền tảng trong lĩnh vực lập trình máy tính. Mã của dự án Cardano là ADA, được đặt theo tên của bà ấy và họ Lovelace của bà ấy được sử dụng để mô tả các đơn vị nhỏ hơn của Token ADA. 1 triệu Lovelace = 1ADA

Goguen: Joseph Goguen là một nhà khoa học máy tính người Mỹ. Ông là giáo sư Khoa học Máy tính tại Đại học California và Đại học Oxford, đồng thời giữ các vị trí nghiên cứu tại IBM và SRI International. Công việc của Goguen là một trong những cách tiếp cận sớm nhất đối với đặc tính đại số của các loại dữ liệu trừu tượng. Ông đã khởi xướng và giúp phát triển họ ngôn ngữ lập trình OBJ¹⁸⁹. Goguen nghiên cứu triết lý tính toán, các phương pháp hình thức và lập trình hàm. Ông ấy đã truyền cảm hứng cho Cardano với công việc của mình là xây dựng khung K để xác minh mã Code của các hợp đồng thông minh, để chúng có thể được tự động kiểm tra lỗi. Goguen là cố vấn cho Grigore Rosu¹⁹⁰ khi Grigore học tại Đại học California. Grigore là giám đốc điều hành của Runtime Verification, người tiếp tục phần lớn công việc này¹⁹¹ cho đến ngày nay. CH:¹⁹²

Nhân tiện, tôi thực sự hối tiếc về điều này. Lẽ ra tôi không nên đặt tên nó là Goguen, kỷ nguyên này đáng lẽ phải được gọi là Hopper theo tên của Grace Hopper. Tôi thích Goguen, ông ấy là một người tốt, nhưng không có đủ tên của phụ nữ ở đây (trên lộ trình phát triển).

Basho: Matsuo Basho là nhà thơ nổi tiếng nhất từ thời Edo thế kỷ 17 của Nhật Bản. Ông viết bài thơ ngắn 3 câu. Một trong những bài thơ nổi tiếng nhất của ông có tên là *Old Pond* mô tả cách một con ếch, bằng cách thực hiện những cú nhảy nhỏ, có thể đến được đại dương rộng lớn. Tương tự như vậy, khi Cardano phát triển và có thêm người dùng mới, hệ thống sẽ mở rộng quy mô và phù hợp với 'đại dương'. CH:

Basho đã thực hiện cuộc hành trình điên rồ này trong thời kỳ Edo ở Nhật Bản khi mọi người sống trong các vùng mà họ được phép. Bạn không được phép đi du lịch, nhưng ông ấy là một người đã đi du lịch và bằng cách nào đó không bị giết. Ông ấy đã viết về tất cả những chuyến đi điên rồ đó.

Voltaire: Được đặt theo tên của nhà triết học người Pháp, người đánh giá cao sự phê bình và tranh luận về sự tách biệt giữa nhà thờ và nhà nước. Voltaire, một trong những nhà thơ yêu thích của Charles Hoskinson, là một nhà văn đa năng và có nhiều tác phẩm, viết các tác phẩm ở hầu hết mọi thể loại văn học, bao gồm kịch, thơ, tiểu thuyết, tiểu luận, các tác phẩm lịch sử và khoa học. Ông đã viết hơn 20.000 bức thư, hơn 2.000 cuốn sách và tập sách nhỏ. Ông ấy là một người thẳng thắn ủng hộ các quyền tự do dân sự, bất chấp nguy cơ điều này khiến ông ấy phải tuân theo luật kiểm duyệt nghiêm ngặt vào thời điểm đó. Là một nhà luận chiến châm biếm, ông thường sử dụng các tác phẩm của mình để chỉ trích sự không khoan dung, giáo điều tôn giáo và các thể chế của Pháp vào thời của ông.

Lord Byron, bl.uk/people/lord-byron

¹⁸⁹

Ngôn ngữ lập trình OBJ, everipedia.org/wiki/lang_en/OBJ_%28programming_language%29

¹⁹⁰

Grigore Rosu, runtimeverification.com/blog/author/grigore-rosh/

¹⁹¹

Cardano360 - Tháng 3 năm 2021, youtu.be/ULBLgPgxtN8?t=1571

¹⁹²Bài phát biểu quan trọng của IO ScotFest với Charles Hoskinson, youtu.be/tbtKClr3Y3I?t=356

Yoroi là ví di động 'ứng dụng nhẹ'¹⁹³ cho Cardano. Trong tiếng Nhật, Yoroi có nghĩa là áo giáp. Nó được xây dựng để bảo vệ sự toàn vẹn của các Samurai trong thời Trung Cổ.

Ouroboros là tên của giao thức đồng thuận của mạng Cardano. Ouroboros là một biểu tượng cổ đại ('kẻ nuốt đuôi' trong tiếng Hy Lạp) mô tả một con rắn hoặc rồng đang ăn đuôi của chính nó, một biểu tượng sinh sản cũng đại diện cho sự vĩnh cửu và sự trở lại vô tận.

Jörmungandr¹⁹⁴ là một triển khai Node, được viết bằng Rust,¹⁹⁵ với mục đích ban đầu là hỗ trợ loại giao thức đồng thuận Ouroboros trên mạng thử nghiệm được khuyến khích vào năm 2019, sau đó được tái sử dụng để trở thành một phần của Catalyst. Node sẽ tham gia mạng Blockchain, liên tục tạo, gửi, nhận và xác thực các Block. Mỗi Node chịu trách nhiệm đảm bảo rằng tất cả các quy tắc của giao thức đều được tuân thủ. Jörmungandr đề cập đến Rắn Midgard trong thần thoại Bắc Âu. Đó là một ví dụ về Ouroboros, con rắn Ai Cập cổ đại, ăn đuôi của chính nó, cũng như bài nghiên cứu của IOG¹⁹⁶ về bằng chứng cổ phần.

Plutus là vị thần giàu có của Hy Lạp. Ông ấy bị Zeus làm mù, vì Zeus muốn ông ấy có thể phân tán những món quà của mình mà không có bất kỳ định kiến và phân biệt đối xử nào. Plutus¹⁹⁷ là nền tảng hợp đồng thông minh cho Cardano. Hợp đồng Plutus bao gồm các phần chạy trên Blockchain (mã trên chuỗi¹⁹⁸) và các phần chạy trên máy của người dùng (mã ngoài chuỗi hoặc mã máy trạm). Plutus rút ra từ nghiên cứu ngôn ngữ hiện đại để cung cấp một môi trường lập trình Full-Stack an toàn dựa trên Haskell, ngôn ngữ lập trình hàm hàng đầu.

Marlowe. Được đặt theo tên của Christopher Marlowe, một người thời Elizabeth 'thợ rèn, kẻ cãi lộn, gián điệp, nhưng trên hết là nhà viết kịch, nhà thơ và nhà văn nổi tiếng nhất trong thế hệ của ông',¹⁹⁹ người đã bị giết ở tuổi 29 trong một cuộc ẩu đả say xỉn vì một hóa đơn nhưng có thể đã bị ám sát. Marlowe, còn được gọi là Kit Marlowe, là một nhà viết kịch, nhà thơ và dịch giả người Anh. Ông có ảnh hưởng lớn đến William Shakespeare, người sinh cùng năm với Marlowe. Ông ủng hộ chủ nghĩa chống trí thức, đó là một hình thức thù địch và mất lòng tin đối với trí thức.

Ở Cardano, Marlowe là một ngôn ngữ dành riêng cho miền (DSL)²⁰⁰ mới để mô hình hóa các công cụ tài chính dưới dạng hợp đồng thông minh trên Blockchain. Nó được nhúng trong ngôn ngữ Haskell, ngôn ngữ này có khung kiểm tra và hệ sinh thái được thiết lập riêng. Bạn không cần có kiến thức chuyên môn về lập trình để sử dụng Marlowe. Bạn có thể khám phá các hợp đồng tài chính Marlowe của mình bằng trình giả lập và trình chỉnh sửa hợp đồng dựa trên trình duyệt.

¹⁹³

Ví di động Yoroi, yoroi-wallet.com/

¹⁹⁴

Jormungandr, [everipedia.org/wiki/ lang_en /J%C3%B6rmungandr](https://everipedia.org/wiki/lang_en/J%C3%B6rmungandr)

¹⁹⁵

Rust là một ngôn ngữ lập trình nhẹ, di động của Mozilla, có thể biên dịch cho web, iOS và Android. Rust là một ngôn ngữ đa mô hình, có mục đích chung được thiết kế cho hiệu suất và sự an toàn, đặc biệt là tính đồng thời an toàn.

¹⁹⁶

Kiayias, Russell, David, Oliynykov (2019) 'Ouroboros: Giao thức Blockchain bằng chứng cổ phần an toàn có thể chứng minh được', eprint.iacr.org/2016/889.pdf

¹⁹⁷

Plutus, [developer.cardano.org/ en /programming-languages/ plutus /overview/](https://developer.cardano.org/en/programming-languages/plutus/overview/)

¹⁹⁸

Mã ngoại tuyến : Phần mã của ứng dụng hợp đồng chạy ngoài chuỗi, thường là ứng dụng hợp đồng. **Mã trên chuỗi** : Một phần mã của ứng dụng hợp đồng chạy trên chuỗi (tức là dưới dạng tập lệnh).

¹⁹⁹

Marlowe, bbc.co.uk/ chương trình /p003k9d6

²⁰⁰

Ngôn ngữ dành riêng cho miền (DSL) là ngôn ngữ máy tính dành riêng cho miền ứng dụng cụ thể. Điều này trái ngược với ngôn ngữ có mục đích chung (GPL), được áp dụng rộng rãi trên các miền.

Chương 3: Bằng chứng cổ phần

'Người có lý do để sống có thể chịu đựng hầu như bất cứ điều gì'

- Friedrich Nietzsche

Bằng chứng cổ phần là gì?

Bằng chứng cổ phần (PoS) là một giao thức hoặc phương pháp đồng thuận, xác định sự đồng thuận dựa trên lượng cổ phần (hoặc giá trị) được giữ lại trong hệ thống. Về bản chất, một giao thức đồng thuận là thứ chi phối các luật và tham số điều chỉnh hành vi của các Blockchain, tương tự như một bộ quy tắc mà mỗi thành viên mạng tuân theo. Vì các Blockchain không được kiểm soát bởi một cơ quan trung ương duy nhất, nên một giao thức đồng thuận được sử dụng để cho phép người dùng mạng phân tán đồng ý về lịch sử của mạng như được ghi lại trên Blockchain để đạt được thỏa thuận về những gì đã xảy ra và tiến triển từ một nguồn sự thật duy nhất.

Cardano dựa trên Ouroboros, một hệ thống đồng thuận bằng chứng cổ phần sáng tạo được tạo ra thông qua nghiên cứu đánh giá ngang hàng. Stake Pool, là các Node máy chủ được duy trì bởi SPO (SPO) mà chủ sở hữu ADA có thể ủy quyền cổ phần của họ, là cốt lõi của công nghệ PoS này. Stake Pool được sử dụng để đảm bảo rằng mọi người đều có thể tham gia vào giao thức, bất kể chuyên môn kỹ thuật hay khả năng duy trì một Node. Các Stake Pool này tập trung vào việc bảo trì và giữ cổ phần gộp của một số bên liên quan ở một nơi.

Bằng chứng cổ phần so với bằng chứng công việc

Bằng chứng công việc (PoW) là một hệ thống đồng bộ²⁰¹ khuyến khích các thợ đào cạnh tranh để giải quyết các vấn đề bên trong Block đầu tiên. Việc giải quyết vấn đề này được khen thưởng thông qua một hệ thống khuyến khích. Tuy nhiên, chiến lược này phải trả giá đắt: mức tiêu thụ điện năng cao hơn và thời gian xử lý các sự cố trong chuỗi dài hơn. Những sự cố này có thể khiến mạng chậm đi đáng kể, khiến việc duy trì mạng trở nên tốn kém.

Một trong những yếu tố quan trọng nhất của bằng chứng cổ phần (PoS) là khi tiền của người dùng tăng lên thì khả năng duy trì số cái của họ cũng tăng theo, tức là khả năng tạo các Block mới có thể được đưa vào Blockchain và được đánh dấu thời gian chính xác. Sự kết hợp giữa lựa chọn ngẫu nhiên và xác định cổ phần hoặc tiền của họ sẽ xác định ai sẽ tạo ra một Block mới. Trong chuỗi, một hình thức bầu chọn người lãnh đạo diễn ra. Theo hệ thống bằng chứng cổ phần, người dùng kiểm được phí giao dịch khi họ thực hiện, tăng số dư của họ bằng thu nhập thụ động (Staking). Chiến lược này thúc đẩy sự mở rộng ổn định và nhất quán của Blockchain phù hợp với mục tiêu mạng trở nên mạnh mẽ hơn khi mọi người tham gia.

Lợi ích của bằng chứng cổ phần

Sau đây là một số lợi ích chính của PoS so với PoW:

- Giao thức bằng chứng cổ phần kết hợp các quy trình bảo mật nghiêm ngặt
- Phi tập trung hóa - giảm nguy cơ tập trung hóa bằng cách áp đặt các hình phạt đối với hành vi tư lợi cá nhân bên trong mạng
- Hiệu quả năng lượng - tiêu thụ năng lượng cực kỳ hiệu quả vì Blockchain yêu cầu ít năng lượng và tài nguyên phần cứng hơn để hoạt động. Ví dụ: 'Berry' là Stake Pool Cardano²⁰² chạy trên Raspberry Pi²⁰³. Markus Gufler²⁰⁴ đã chạy một Node Cardano trên Rock Pi (máy tính một bảng do Radxa sản xuất) tại Hội nghị thượng đỉnh IOHK năm 2019. Một Rock Pi sử dụng ít nhất 10W để hoạt động.
- Hiệu quả chi phí - tiền tệ bằng chứng cổ phần tiết kiệm chi phí hơn đáng kể so với tiền tệ bằng chứng công việc.

Mặc dù sử dụng bằng chứng cổ phần cho Crypto là một quyết định thiết kế gây tranh cãi, nhưng IOG đã chọn chấp nhận nó vì nó cung cấp một phương pháp giới thiệu bỏ phiếu an toàn, có khả năng mở rộng quy mô lớn hơn và cho phép các chương trình khuyến khích phức tạp hơn.

²⁰¹

Trong một **hệ thống đồng bộ**, các hoạt động được điều phối bởi một hoặc nhiều tín hiệu đồng hồ tập trung. Ngược lại, một hệ thống kỹ thuật số không đồng bộ không có đồng hồ toàn cầu. Các hệ thống không đồng bộ không phụ thuộc vào thời gian đến nghiêm ngặt của tín hiệu hoặc thông báo để hoạt động đáng tin cậy. Sự phối hợp đạt được thông qua các sự kiện như: gói đến, thay đổi (chuyển đổi) tín hiệu, giao thức bắt tay và các phương pháp khác.

²⁰²

Bê Berry, github.com/alessandrokonrad/Pi-Pool

²⁰³

Raspberry Pi: máy tính trên bảng có kích thước bằng thẻ tín dụng. Ý tưởng được phát triển bởi Eben Upton và những người khác từ Phòng thí nghiệm Máy tính của Đại học Cambridge và được đưa ra bởi Quỹ Raspberry Pi của họ. Lấy cảm hứng từ Dự án Kiến trúc Máy tính của BBC những năm 1980, máy tính bảng đơn chạy Linux với phần mềm nguồn mở đã được ra mắt vào năm 2012 với chi phí £22 để khuyến khích sử dụng máy tính trong trường học và các nước đang phát triển.

²⁰⁴

Cardano on the Rocks: nhóm cổ phần bằng chứng cổ phần tiết kiệm năng lượng, youtube.com/watch?v=kXR1UXkM46s

Giao thức Ouroboros được phát triển bởi một nhóm các nhà mật mã lành nghề từ năm tổ chức học thuật do Giáo sư Aggelos Kiayias của Đại học Edinburgh đứng đầu. Ngoài việc được xác minh an toàn bằng cách sử dụng một mô hình mật mã nghiêm ngặt, sự đổi mới cơ bản mà nó mang lại là một kiến trúc mô-đun và có thể thích ứng, cho phép kết hợp nhiều giao thức để tăng cường chức năng.

Ủy quyền, Sidechain, điểm kiểm tra có thể đăng ký, cấu trúc dữ liệu được cải thiện cho ứng dụng khách nhẹ²⁰⁵, nhiều loại tạo số ngẫu nhiên và thậm chí cả các giả định đồng bộ hóa thay thế đều có thể thực hiện được nhờ tính linh hoạt này. Nhu cầu về thuật toán đồng thuận của mạng sẽ thay đổi khi nó phát triển từ hàng trăm lên hàng triệu và cuối cùng là hàng tỷ thành viên. Do đó, điều quan trọng là phải có đủ tính linh hoạt để xử lý những thay đổi này và đảm bảo cốt lõi của Crypto trong tương lai.

'Blockchain xanh'

Tác động môi trường của việc khai thác bằng chứng công việc đã trở thành một chủ đề nóng vào năm 2021. Yahoo Finance²⁰⁶, EuroNews²⁰⁷ và tờ báo Độc lập²⁰⁸ chỉ là một số trong số đó, họ gọi Cardano là 'Blockchain xanh'. Cơ chế Staking của Cardano tránh tiêu thụ năng lượng khổng lồ và ô nhiễm phần cứng như khi khai thác Bitcoin. Bitcoin đã trở thành chủ đề tranh luận kể từ khi Satoshi Nakamoto phát hành sách trắng Bitcoin²⁰⁹ vào năm 2008. Crypto đã nhiều lần xuất hiện trên các bản tin vì tất cả những lý do sai lầm. Sự phản đối phổ biến nhất là việc khai thác Bitcoin và các loại Crypto khác dựa trên bằng chứng công việc vô ích²¹⁰ có hại cho môi trường.

²⁰⁵

Máy **khách nhẹ** hoặc máy khách mỏng là một máy tính nhẹ đã được tối ưu hóa để thiết lập kết nối từ xa với môi trường điện toán dựa trên máy chủ. Máy chủ thực hiện hầu hết công việc, có thể bao gồm khởi chạy các chương trình phần mềm, thực hiện tính toán và lưu trữ dữ liệu. Điều này trái ngược với một khách hàng béo hoặc một máy tính cá nhân thông thường; cái trước cũng nhằm mục đích hoạt động trong mô hình máy khách-máy chủ nhưng có sức mạnh xử lý cục bộ đáng kể, trong khi cái sau nhằm mục đích thực hiện chức năng của nó chủ yếu là cục bộ.

²⁰⁶

Đưa Blockchain xanh lên một tầm cao mới với Cardano, tài chính.yahoo.com/news/green-blockchain-next-level-cardano-192654597.html

²⁰⁷

Crypto 'xanh' ADA của Cardano có thể tiếp quản Bitcoin và Ethereum không?, euronews.com/next/2021/08/23/could-cardano-s-green-cryptocurrency-ADA-take-over-bitcoin-and-ethereum

²⁰⁸

Cardano là gì? Crypto 'xanh' đã thách thức sự sụp đổ bitcoin của Musk – và hy vọng sẽ vượt qua Facebook và Netflix, độc lập.co.uk/space/cardano-crypto-bitcoin-elon-musk-b1849021.html

²⁰⁹

Satoshi Nakamoto, 'Bitcoin: Hệ thống tiền mặt điện tử ngang hàng', bitcoin.org/bitcoin.pdf

²¹⁰

Dotan và Tochner, ' Bằng chứng về công việc vô ích: Kết quả tích cực và tiêu cực đối với hệ thống khai thác không lãng phí ', arxiv.org/pdf/2007.01046.pdf

BẢNG II: Xếp hạng Bitcoin và Ethereum với các quốc gia về lượng khí thải Carbon hàng năm tính đến tháng 7/2021 [23, 26, 27, 30]

Rank	Country	Population (Millions) [26]	Emission (MtCO ₂)	Share (%)
0	World	7,878.2	37,077.40	100.00
1	China	1,444.9	10,060.00	27.13
2	U.S.A	332.9	5410.00	14.59
3	India	1,336.4	2,300.00	6.2
38	Nigeria	211.3	104.30	0.28
39	Czech Republic	10.7	100.80	0.27
40	Belgium	11.6	91.20	0.24
41	Bitcoin + Ethereum	N.A.	90.31	0.24
42	Kuwait	4.3	87.80	0.23
43	Qatar	2.9	87.00	0.23
49	Oman	5.2	68.80	0.18
50	Bitcoin	N.A.	64.18	0.17
51	Greece	10.3	61.60	0.16
76	Tunisia	11.94	26.20	0.07
77	Ethereum	N.A.	26.13	0.07
78	SAR	17.9	25.80	0.06

Hình 7. Bảng từ bài nghiên cứu của Đại học Cornell

Theo một bài nghiên cứu²¹¹ được xuất bản bởi Đại học Cornell, lượng khí thải Carbon kết hợp của Bitcoin và Ethereum sẽ xếp thứ 41 trên thế giới.

Các thuật toán để khai thác tốn rất nhiều năng lượng. Vấn đề này đã trở nên trầm trọng hơn cho đến gần đây bởi thực tế là 70% hoạt động khai thác diễn ra ở Trung Quốc, nơi năng lượng được tạo ra bằng nhiên liệu hóa thạch, đặc biệt là than đá. Một cuộc đàn áp của chính quyền Trung Quốc đã dẫn đến một cuộc di cư của thợ đào Crypto, điều này chỉ chuyển vấn đề sang các quốc gia khác. Và vấn đề có sự phân nhánh trong các lĩnh vực khác. Ví dụ, những lo ngại về sử dụng năng lượng đã dẫn đến việc cấm khai thác ở Nội Mông.²¹²

Thuật toán bằng chứng công việc của Bitcoin là gót chân Achilles, nhưng nó rất cần thiết cho hoạt động của hệ thống. Các giàn khai thác mạnh mẽ và hiện đại tạo ra năng suất cao hơn, nhưng càng nhanh thì càng sử dụng nhiều năng lượng. Điều này đặt ra vấn đề về khả năng tồn tại lâu dài. Theo một bài báo gần đây trên Blog của Ethereum Foundation²¹³, “Những ngày ngọn năng lượng của Ethereum là có hạn” và việc chuyển đổi được chờ đợi từ lâu sang bằng chứng cổ phần sẽ cần ít hơn 99,95% năng lượng²¹⁴. Sự kiện 'The Merge' cuối cùng đã diễn ra vào tháng 9 năm 2022. Tuy nhiên, việc Ethereum chuyển sang bằng chứng cổ phần không diễn ra suôn sẻ với các cổ phần bị khóa vô thời hạn và những lo ngại về tập trung hóa²¹⁵. Đây cũng chỉ là bước đầu tiên trên lộ trình phức tạp đến ETH 2.0. Vì 'The Merge' đã bị trì hoãn trong vài năm nên rất khó để dự đoán khi nào phần còn lại của lộ trình sẽ diễn ra.

Vì các công cụ khai thác bằng chứng công việc của Ethereum sẽ không thể hoạt động sau khi có 'The Merge', nên một cuộc thảo luận thú vị là 'Khi Ethereum chuyển sang bằng chứng cổ phần, Ergo có khả năng hấp thụ hầu hết sức mạnh Hash không?'²¹⁶

²¹¹

Phân tích về mức tiêu thụ năng lượng và dấu chân carbon của Crypto và các giải pháp khả thi, arxiv.org/pdf/2203.03717.pdf

²¹²

Khu vực khai thác bitcoin lớn ở Trung Quốc đặt ra các hình phạt nghiêm khắc đối với các hoạt động Crypto, cnbc.com/2021/05/26/major-china-bitcoin-mining-hub-lays-out-harsher-crackdown-measures.html

²¹³

của Ethereum sẽ sớm giảm ~99,95%, blog.ethereum.org/2021/05/18/country-power-no-more/

²¹⁴Bước đột phá này có thể làm cho Ethereum thân thiện với môi trường hơn Bitcoin, fortune.com/2021/05/24/ethereum-bitcoin-buterin-carbon-footprint-proof-of-stake/

²¹⁵Hợp nhất Ethereum có ý nghĩa gì đối với Crypto?, buildin.com/blockchain/ethereum-merge

²¹⁶Hội nghị bàn tròn với Charles Hoskinson và Alex Chepurnoy | Ergo Pulse, youtu.be/k9a3SYV6FJA?t=3182

Nhưng điều gì phân biệt bằng chứng cổ phần với các Blockchain khác về tác động môi trường? Vì thợ đào phải giải quyết các vấn đề toán học ngày càng phức tạp để tạo ra các Block, bằng chứng công việc đòi hỏi nhiều tài nguyên. Họ đang tham gia một cuộc chạy đua năng lượng cao trên toàn thế giới để giải quyết các vấn đề vô nghĩa được tạo ra một cách ngẫu nhiên. Lượng điện toán khổng lồ này có thể được sử dụng tốt hơn như lập trình Tua-bin gió hoặc pin mặt trời. Bài nghiên cứu PoUW (Bằng chứng công việc hữu ích)²¹⁷ thảo luận về các giải pháp thay thế cho bằng chứng công việc. Nỗ lực kỹ thuật số lãng phí này có sự phân nhánh trong thế giới thực.

Nhu cầu về phần cứng mạnh mẽ tạo ra một vấn đề khác: rác thải điện tử. Những thợ đào phải liên tục theo kịp các đối thủ cạnh tranh của họ, điều này đòi hỏi phải mua thiết bị khai thác ngày càng mạnh mẽ. Thiết bị 'cũ', thường chỉ phù hợp để khai thác, sẽ sớm trở nên lỗi thời. Nó bị lãng phí và rác thải điện tử của Bitcoin là một vấn đề đang gia tăng. Bởi vì chỉ có 20% rác thải điện tử được tái chế trên toàn thế giới, nhựa của giàn khoan và các nguyên tố nguy hiểm, chẳng hạn như kim loại nặng, có thể kết thúc ở các bãi chôn lấp. Đến năm 2050, Liên Hợp Quốc dự đoán rằng toàn cầu sẽ tạo ra tới 120 triệu tấn rác thải điện tử mỗi năm. Bài viết này 'Vấn đề rác thải điện tử ngày càng tăng của Bitcoin'²¹⁸ đi vào chi tiết hơn.

Vậy tại sao Cardano được mệnh danh là 'Blockchain xanh'? Cardano mang lại hai lợi ích khác biệt khi nói đến tính bền vững và Crypto thân thiện với môi trường: giảm đáng kể việc sử dụng năng lượng và Staking. Người dùng mạng chạy các Node trong bằng chứng cổ phần và chuỗi chọn một Node để thêm Block tiếp theo tùy thuộc vào cổ phần và các thuộc tính khác của Node. Sự khác biệt cơ bản giữa hai thuật toán này (và nhu cầu năng lượng của chúng) là các nhà sản xuất Block bằng chứng cổ phần không cần phải dành nhiều thời gian và sức mạnh tính toán để giải quyết các vấn đề ngẫu nhiên. Mức tiêu thụ năng lượng của Cardano được dự đoán là 0,01% so với Bitcoin.²¹⁹

Trong một cuộc chạy đua vũ trang tốn nhiều năng lượng và vô nghĩa, các loại Crypto bằng chứng công việc cần sức mạnh tính toán để tạo Block. Mặt khác, Node Cardano có thể hoạt động trên CPU công suất thấp như Raspberry Pi. Hơn 40 triệu trong số này đã được tạo ra, nhiều trong số đó được dành cho các trường học ở các quốc gia kém phát triển do chi phí thấp từ 40 đến 70 đô la. Sự đơn giản này cũng cắt giảm rác thải nhựa và rác thải điện tử.

Thời tiết khắc nghiệt và cháy rừng dường như gia tăng hàng năm, với những cảnh báo từ các báo cáo Khí hậu của Liên hợp quốc ngày càng rõ ràng hơn. Báo cáo mới nhất vào tháng 4 năm 2022²²⁰ khẳng định đó là 'bây giờ hoặc không bao giờ'. Xã hội nhận thức được nạn phá rừng, cạn kiệt thêm băng và sự nóng lên toàn cầu. Các đợt nắng nóng đang tàn phá hệ sinh thái ở nhiều khu vực trên toàn cầu và cháy rừng đang tàn phá nhiều nơi. Do đó, mọi thứ góp phần vào vấn đề bền vững đều được xem xét kỹ lưỡng. Điều này bao gồm thị trường Crypto đang mở rộng.

Khi nói đến việc giải quyết các vấn đề môi trường, không có giải pháp đơn giản nào. Cardano là một nền tảng phi tập trung có thể thay thế sự kém hiệu quả của các hệ thống cũ và cũ hơn. Cardano và các giao thức bằng chứng cổ phần khác được coi là đang đóng góp cho giải pháp vì thông tin xác thực về tính bền vững của chúng.

Mặc dù Cardano là một Blockchain bằng chứng cổ phần và là trọng tâm trong phần lớn công việc của IOG, nhưng họ cũng nghiên cứu các giao thức khác và cũng đã xuất bản rộng rãi về Bằng chứng công việc. Bài nghiên cứu mới nhất của họ²²¹ *Ofelimos: Tối ưu hóa tổ hợp thông qua bằng chứng công việc hữu ích: Giao thức Blockchain an toàn có thể chứng minh* được trình bày tại Crypto 2022.

Triết lý của POS

Phi tập trung được cho là mục tiêu cơ bản và quan trọng nhất của Cardano. Cơ sở của mọi Blockchain là các giao thức và tham số. Tuy nhiên, bản thân cộng đồng, cách cộng đồng tự nhận thức, hành động và thiết lập các chuẩn mực chung, có ảnh hưởng lớn đến

217

Một bằng chứng mới về công việc hữu ích cho một Blockchain lưu trữ các giao dịch vận tải, [sciencedirect.com/science/article/pii/S0306457321002302](https://www.sciencedirect.com/science/article/pii/S0306457321002302)

218

Vấn đề rác thải điện tử ngày càng tăng của bitcoin, [Sciencedirect.com/science/article/abs/pii/S0921344921005103](https://www.sciencedirect.com/science/article/abs/pii/S0921344921005103)

219

Cardano là gì? Crypto 'xanh' đã thách thức sự sụp đổ bitcoin của Musk – và hy vọng sẽ vượt qua Facebook và Netflix, [lập.co.uk/life-style/gadgets-and-tech/cardano-crypto-bitcoin-elon-musk-b1849021.html](https://www.theguardian.com/technology/2022/apr/11/cardano-crypto-bitcoin-elon-musk-b1849021.html)

220

Báo cáo khí hậu của Liên Hợp Quốc: 'Bây giờ hoặc không bao giờ' để hạn chế sự nóng lên toàn cầu ở mức 1,5 độ, [news.un.org/en/story/2022/04/1115452](https://www.un.org/en/story/2022/04/1115452)

221

Fitzi, Kiayias, Panagiotakos, Russell (2022), 'Ofelimos: Tối ưu hóa kết hợp thông qua Proof-of-Useful-Work: Giao thức Blockchain an toàn có thể chứng minh được', [iohk.io/en/research/library/papers/ofelimos-combinatorial-optimization-thông-qua-bằng-chứng-về-công-việc-có-hữu-ích-một-giao-thức-blockchain-có-thể-chứng-minh-an-toàn/](https://www.iohk.io/en/research/library/papers/ofelimos-combinatorial-optimization-thông-qua-bằng-chứng-về-công-việc-có-hữu-ích-một-giao-thức-blockchain-có-thể-chứng-minh-an-toàn/)

thành công của dự án. Cardano đã được kiến trúc một cách tỉ mỉ để có 'theo thiết kế' tất cả các phẩm chất cần thiết cho một hệ thống Blockchain thành công. Cardano là một cấu trúc xã hội nên việc tuân thủ, diễn giải và các quy ước xã hội đều góp phần xác định tính bền vững và khả năng tồn tại lâu dài của nó.

Nguyên tắc Staking

Kể từ khi ra mắt Blockchain Bitcoin, dựa trên sự đồng thuận dựa trên *tài nguyên* được phổ biến trên một nhóm người dùng thay vì tham gia dựa trên danh tính đã trở thành đặc điểm nổi bật của hệ sinh thái Blockchain. Các hệ thống bằng chứng cổ phần khác biệt trong ngành này vì chúng sử dụng một *tài nguyên ảo* được gọi là cổ phần được ghi lại trong chính Blockchain.

Tập hợp các nguồn lực để tham gia là không thể tránh khỏi; một số lượng tổng hợp nói chung là thuận lợi về mặt kinh tế; do đó những người nắm giữ tài nguyên sẽ tìm ra phương tiện để biến nó thành hiện thực. Với tính tất yếu này, thách thức lúc đó là tránh sự xuất hiện của một chế độ độc tài, thực thể lớn hoặc đầu sỏ chính trị²²² kiểm soát quá nhiều cổ phần.

Mục tiêu của hệ thống phần thưởng Staking

Không giống như các hệ thống Blockchain trước đây, Cardano sử dụng cơ chế chia sẻ phần thưởng (a) cho phép Staking mà không gây bất tiện không cần thiết và (b) khuyến khích tổng hợp tài nguyên theo cách phi tập trung toàn hệ thống phát triển một cách tự nhiên thông qua sự tham gia hợp lý của chủ sở hữu tài nguyên.

Hai mục tiêu chính của cơ chế như sau:

- Thu hút tất cả các bên liên quan - Càng nhiều người tham gia vào hệ thống, số cái phân tán càng trở nên an toàn hơn. Điều này cũng có nghĩa là hệ thống không được có rào cản tham gia và không được gây ra xích mích bằng cách yêu cầu sự phối hợp ngoài chuỗi giữa các bên liên quan để tham gia vào cơ chế.
- Giữ quyền hạn của từng bên liên quan ở mức tối thiểu - Đối với một số bên liên quan nhất định, việc tập hợp các nguồn lực sẽ làm tăng ảnh hưởng của họ. Quyền lực của SPO trên hệ thống tỷ lệ thuận với các tài nguyên được quản lý bởi Pool của họ chứ không phải của riêng họ. Nếu không gộp chung, tất cả những người nắm giữ tài nguyên đều có đòn bẩy là một. Đòn bẩy của hệ thống càng mạnh thì càng kém an toàn (có nhiều khả năng xảy ra một cuộc tấn công 51%²²³ vào hệ thống).

Kích thước Pool lớn không phải là nguyên nhân duy nhất làm tăng đòn bẩy; các bên liên quan cũng có thể đạt được đòn bẩy bằng cách hình thành một số Pool, công khai hoặc bí mật (được gọi là tấn công Sybil²²⁴). Mức độ phân cấp của hệ thống Blockchain càng lớn thì đòn bẩy của nó càng thấp.

Từ lý thuyết đến thực tiễn

Vậy cơ chế chia sẻ phần thưởng của Cardano đạt được các mục tiêu nói trên như thế nào? Staking với Cardano cho phép có hai tùy chọn: cam kết²²⁵ và ủy quyền. Các SPO sử dụng cổ phần đã cam kết; cổ phần cam kết được cam kết với một Stake Pool và dự kiến sẽ duy trì ở đó trong suốt thời gian hoạt động của Pool. Coi cam kết là một 'cam kết' với mạng. Đó là một cách để 'khóa' một lượng cổ phần cụ thể để giúp bảo vệ và bảo mật giao thức.

Mặt khác, ủy quyền dành cho những cá nhân không muốn thực hành. Thay vào đó, các cá nhân được khuyến khích đánh giá các ưu đãi của SPO và ủy quyền cổ phần của họ cho một hoặc nhiều Pool mà theo đánh giá của họ là phục vụ tốt nhất cho lợi ích của họ và cộng đồng. Không có lý do gì để từ chối Staking vào Cardano vì ủy quyền không liên quan đến việc khóa tiền; tất cả các bên liên quan đều được hoan nghênh làm như vậy. Đây không phải là điều được đưa ra với các Blockchain bằng chứng cổ phần khác.

²²²

Đầu sỏ chính trị, có nghĩa là 'vài', và 'cai trị hoặc chỉ huy', là một dạng cấu trúc quyền lực trong đó quyền lực thuộc về một số ít người.

²²³

Một **cuộc tấn công 51%** là một sự tiếp quản thù địch đối với Crypto được xác thực thông qua Thuật toán bằng chứng công việc thông qua việc mua lại phần lớn sức mạnh băm của mạng.

²²⁴

Trong một **cuộc tấn công Sybil**, kẻ tấn công phá vỡ hệ thống danh tiếng của mạng ngang hàng bằng cách tạo ra một số lượng lớn danh tính giả và sử dụng chúng để đạt được ảnh hưởng lớn không tương xứng. Nó được đặt tên theo chủ đề của cuốn sách *Sybil*, một nghiên cứu trường hợp về một phụ nữ được chẩn đoán mắc chứng rối loạn nhận dạng phân ly.

²²⁵

Cam kết: khi một SPO chỉ định cổ phần ADA của riêng họ để hỗ trợ nhóm cổ phần của họ. Điều này cung cấp khả năng bảo vệ chống lại các cuộc tấn công Sybil bằng cách ngăn chủ sở hữu nhóm tạo ra một số lượng lớn nhóm mà bản thân họ không sở hữu nhiều cổ phần.

Ví dụ: với Polkadot²²⁶, tiền của bạn được 'liên kết' hoặc 'bị khóa'. Phải mất đủ 28 ngày để 'hủy liên kết' hoặc 'mở khóa' tiền của bạn. Điều đó thật hào phóng so với Ethereum, nơi mọi người có thể không rút được Ether đã Staking cho đến khi nâng cấp *Shanghai* diễn ra. Staking trên Cardano không bị giam giữ, vì vậy không có hình phạt²²⁷ nặng nề nào được áp dụng. Với tư cách là người ủy quyền, số tiền Staking của bạn không bao giờ có nguy cơ bị SPO lấy đi, điều này bổ sung đáng kể vào sự tham gia của người ủy quyền.

Mô hình khuyến khích của Cardano dựa trên trạng thái cân bằng Nash²²⁸. Ý tưởng là khi những người điều hành Stake Pool và những người ủy quyền được khuyến khích hợp lý, thì trạng thái cân bằng Nash sẽ đạt được dựa trên hành vi hợp lý và trung thực của họ. Mục tiêu của cơ chế khuyến khích là đạt được mức độ phi tập trung, bảo mật và tham gia cao.

Hai tham số k và $a0$ (*a naught*) rất quan trọng đối với hoạt động của cơ chế. Phần thưởng Pool được giới hạn ở mức $1/k$ số tiền có sẵn nhờ tham số k . Thêm X số tiền cam kết vào Pool sẽ tăng phần thưởng của nó lên tới $a0 * X$, nhờ tùy chọn $a0$. Đây không phải là chi phí của các Pool khác; bất kỳ phần thưởng nào không được nhận do cam kết không đầy đủ sẽ được khôi phục vào nguồn dự trữ của Cardano và được phân phối trong tương lai.

Việc tạo Stake Pool yêu cầu các nhà khai thác (hay còn gọi là SPO - SPO) tuyên bố tỷ suất lợi nhuận²²⁹ và chi phí hoạt động²³⁰ của họ bên cạnh việc đồng ý về số tiền cam kết. Chi phí hoạt động được giữ lại trước tiên khi các khoản thanh toán Pool được phân phối vào cuối mỗi Epoch, đảm bảo rằng Stake Pool luôn bền vững. Sau đó, lợi nhuận của nhà điều hành được xác định và tất cả những người ủy quyền trong Pool nhận được phần phù hợp với khoản đầu tư của họ.

Cách tiếp cận này, khi được kết hợp với đánh giá Stake Pool của người ủy quyền, đưa ra tập hợp các hạn chế chính xác để hệ thống hội tụ thành một cấu hình gồm k nhóm có kích thước bằng nhau với số tiền cam kết lớn nhất.

Kiến trúc Blockchain của Cardano, giống như nhiều kiến trúc khác, có một cơ chế sáng tạo và được nghiên cứu kỹ lưỡng. Hệ thống phần thưởng đã được chứng minh về mặt toán học để cung cấp trạng thái cân bằng phù hợp với mục tiêu của nó. Nhưng, cuối cùng, số học thôi sẽ không đủ; chỉ con người mới có thể làm cho nó diễn ra. Tương lai của Cardano nằm trong tay cộng đồng.

Stake Pool cá nhân

Stake Pool là một Node máy chủ tổng hợp và duy trì cổ phần của một số bên liên quan thành một thực thể duy nhất. Stake Pool giám sát quá trình xử lý giao dịch và sản xuất Block và giám sát các tương tác của họ với mạng thông qua Node Cardano.

Để quản lý Stake Pool một cách hiệu quả, bạn sẽ cần một người điều hành Stake Pool và một hoặc nhiều chủ sở hữu Stake Pool. Có sự khác biệt về khái niệm giữa hai công việc này:

- SPO chịu trách nhiệm thiết lập và quản lý Stake Pool, nghĩa là họ sở hữu hoặc thuê một máy chủ, quản lý và giám sát Node và có quyền truy cập vào Stake Pool. Người điều hành Stake Pool có thể ký các Block, đăng ký, đăng ký lại và hủy bỏ Stake Pool, cũng như tải lên các chứng chỉ được cập nhật bằng cách sử dụng khóa của họ

²²⁶

Đặt cược Polkadot, wiki.polkadot.network/docs/learn-staking

²²⁷

Chém là một cơ chế được sử dụng bởi các giao thức PoS để ngăn chặn các hành vi có hại và khiến người xác nhận có trách nhiệm hơn. Chúng giúp giữ an toàn cho mạng vì không cắt giảm các hình phạt, trình xác thực có thể sử dụng cùng một Node để xác thực các Block trên nhiều chuỗi hoặc làm như vậy trên chuỗi sai.

²²⁸ **Cân bằng Nash** được sử dụng trong lý thuyết trò chơi để lập mô hình và xác định giải pháp trong một trò chơi mà những người chơi không hợp tác với nhau.

²²⁹

Biên lợi nhuận: Người điều hành nhóm cổ phần lấy một phần trong tổng số phần thưởng ADA trước khi chia phần thưởng còn lại cho tất cả những người được ủy quyền của nhóm. Nếu tỷ suất lợi nhuận của nhà điều hành thấp, họ sẽ chấp nhận ít rủi ro hơn, điều đó có nghĩa là những người được ủy quyền nên dự đoán sẽ thu được nhiều phần thưởng hơn cho cổ phần được ủy quyền của họ. Nhóm riêng tư là nhóm có tỷ suất lợi nhuận là 100%, cho biết rằng nhà điều hành nhận được tất cả các phần thưởng và những người được ủy quyền không nhận được gì.

²³⁰

chi phí mỗi kỳ nguyên: SPO khấu trừ một khoản phí xác định trước từ các khoản thanh toán của nhóm mỗi kỳ nguyên để trang trải chi phí duy trì nhóm cổ phần. Trước khi nhà điều hành thu lợi nhuận biên của họ, chi phí cho mỗi kỳ nguyên sẽ bị xóa khỏi tổng số ADA được trao cho một nhóm. Những gì còn lại được chia đều cho những người được ủy quyền.

- Chủ sở hữu Stake Pool là người cung cấp cổ phần của họ cho Pool để tăng khả năng kiếm phần thưởng và sức hấp dẫn của Pool. Các cuộc tấn công Sybil được giảm thiểu nhờ khả năng cầm cổ cổ phần của chủ sở hữu.

Người điều hành Stake Pool và chủ sở hữu Stake Pool thường là cùng một người, mặc dù một Stake Pool có thể có một số chủ sở hữu cam kết chia phần của họ để thiết lập một nhóm lớn hơn và duy trì nó một cách cạnh tranh. Các hoạt động Stake Pool vẫn được quản lý bởi một SPO duy nhất trong trường hợp này.

Người điều hành Stake Pool phải có được sự tin tưởng của tất cả các chủ sở hữu Stake Pool. Tất cả phần thưởng của nhà điều hành và chủ sở hữu được đặt vào một tài khoản phần thưởng được chia sẻ duy nhất được liên kết với địa chỉ phần thưởng của Pool và giao thức phân phối chúng giữa các tài khoản của chủ sở hữu. Lý do cho điều này là bởi vì nếu mọi người có thể trở thành đồng sở hữu của Stake Pool thay vì ủy quyền, quy trình sẽ trở nên lỗi thời.

Bạn nên có một hợp đồng để chỉ định thời điểm và cách thức chia các khoản khuyến khích thu được trong tài khoản dùng chung. Ví dụ: họ có thể đồng ý để nhà điều hành quản lý tài khoản dùng chung hoặc họ có thể sử dụng tài khoản đa chữ ký.²³¹

Cần có mối quan hệ hai chiều và sự tin tưởng để vận hành Pool đúng cách. Nếu niềm tin này bị phản bội, các bên khác có thể bị tổn thất về lợi ích tích lũy hoặc dự kiến, cũng như danh tiếng của nhà điều hành.

Cổ phần được kiểm soát là toàn bộ số cổ phần được nắm giữ bởi một Stake Pool. Nó kết hợp cổ phần của người điều hành nhóm và bất kỳ cổ phần nào đã được những người nắm giữ ADA khác ủy quyền cho Pool. Nó có thể được biểu thị dưới dạng tổng số ADA (ví dụ: 2 triệu ADA) hoặc dưới dạng phần trăm tổng nguồn cung ADA của mạng (ví dụ: 2%).

Thiết lập và vận hành Stake Pool

Stake Pool là một khía cạnh quan trọng của mạng Cardano phi tập trung, vì chúng cho phép các quy trình đảm bảo sức khỏe và khả năng tồn tại lâu dài của mạng. Người điều hành Stake Pool cho phép những người dùng khác tham gia vào hệ thống và kiếm phần thưởng mà không cần phải luôn lưu trữ một Node hoạt động. Phạm vi của cuốn sách này là để giải quyết lý thuyết. Nhiều chi tiết thực tế chuyên sâu khác nằm ngoài phạm vi và được đề cập trong các phần tài liệu Cardano sau:

- Tạo Stake Pool²³²
- Thiết lập kết nối giữa các Node lỗi và Relay²³³
- Chứng chỉ và chìa khóa hoạt động²³⁴
- Stake Pool công khai và quản lý siêu dữ liệu²³⁵
- Quản lý siêu dữ liệu SMASH²³⁶
- Hiệu suất Stake Pool²³⁷
- Xếp hạng Stake Pool²³⁸

²³¹

Đa chữ ký (đa chữ ký) là sơ đồ chữ ký số cho phép một nhóm người dùng ký một tài liệu. Thông thường, một thuật toán đa chữ ký tạo ra một chữ ký chung nhỏ gọn hơn một tập hợp các chữ ký riêng biệt từ tất cả người dùng. Đa chữ ký có thể được coi là khái quát hóa của cả chữ ký nhóm và chữ ký vòng cung cấp bảo mật bổ sung cho các giao dịch Crypto.

²³²

Tạo nhóm cổ phần, docs.cardano.org/getting-started/operating-a-stake-pool/creating-a-stake-pool

²³³

Thiết lập kết nối giữa các Node, docs.cardano.org/getting-started/operating-a-stake-pool/node-connectivity

²³⁴

Chứng chỉ và khóa hoạt động, docs.cardano.org/getting-started/operating-a-stake-pool/creating-keys-and-certificates

²³⁵

Nhóm cổ phần công cộng và quản lý siêu dữ liệu, docs.cardano.org/getting-started/operating-a-stake-pool/public-stake-pools

²³⁶

Quản lý siêu dữ liệu SMASH, docs.cardano.org/getting-started/operating-a-stake-pool/SMASH

²³⁷

Hiệu suất nhóm cổ phần, docs.cardano.org/getting-started/operating-a-stake-pool/performance

²³⁸

Xếp hạng nhóm cổ phần, docs.cardano.org/getting-started/operating-a-stake-pool/running

Mạng Cardano

Các Node liên kết chỉ chịu trách nhiệm sản xuất Block và kết nối mạng trong kỷ nguyên Byron. Mạng Byron được tạo thành từ các Node lỗi được liên kết, là các Node tính toán ra các Block và giữ cho mạng Cardano hoạt động. Với sự ra mắt của Shelley, mạng đã chuyển sang chế độ kết hợp, với các Node được liên kết do IOG vận hành (thiết lập cấu hình kết nối giữa các SPO khác nhau) và các Node do SPO (SPO) vận hành. Tỷ lệ Block được tạo bởi các Node phi tập trung tăng đều đặn, trong khi các Node được liên kết dần dần ngừng hoạt động, phân phối bảo trì mạng một cách công bằng trên tất cả các SPO. Bằng cách sử dụng tính năng khám phá và lựa chọn ngang hàng tự động đang diễn ra, mạng Shelley đã chuyển sang phi tập trung hoàn toàn.

Các Node được liên kết với các Node khác bằng cấu hình tĩnh được thiết lập trong tệp cấu trúc liên kết trong giai đoạn khởi động. Điều quan trọng là phải kết nối với các Node Relay đáng tin cậy để tránh trường hợp các Node Relay ngoại tuyến, khiến các Node tạo Block không thể truy cập được. IOG đã cung cấp cho SPO một danh sách tất cả các Relay đã đăng ký²³⁹ được sắp xếp theo vị trí địa lý vì lý do kết nối. Ngoài ra, các SPO cũng nên tạo một cấu hình bao gồm 20 SPO khác ngang hàng. Nhiều SPO có thể tuyển dụng hơn 20 đồng nghiệp vì lý do kết nối trong thực tế. Danh sách cho phép bạn chọn các đồng nghiệp ở gần và ở xa, đảm bảo kết nối liên vùng.

Lớp mạng của Node đã được thay đổi để sử dụng khám phá tự động liên tục và lựa chọn ngang hàng khi mạng được chuyển từ liên kết sang phi tập trung hoàn toàn. Nâng cấp lên ngăn xếp mạng đã được sử dụng để thực hiện điều này. Ban đầu, điều này cho phép tự động hóa nâng cao kết nối các Relay SPO với nhau, giảm yêu cầu thiết lập tĩnh. Cuối cùng, nó sẽ cho phép tất cả các Node Cardano có kiến trúc ngang hàng (P2P)²⁴⁰ đầy đủ, loại bỏ nhu cầu về Relay do IOG vận hành của mạng.

Bạn có thể tìm thêm thông tin về mạng Cardano, giao tiếp Node và các giao thức nhỏ cho phép khả năng này trong tài liệu.²⁴¹

Kết nối Node lỗi và Node Relay

Với tư cách là SPO, bạn quan tâm đến hai loại Node: Node lỗi và Node Relay. Một hoặc nhiều Node Relay phải đi kèm với mỗi Node lỗi. Node lỗi chịu trách nhiệm tạo các Block, trong khi Node Relay chịu trách nhiệm kết nối với các Relay khác trong mạng cũng như truyền tải các Block. Sự khác biệt này ảnh hưởng đến cách chúng được thiết lập và liên kết với mạng.

Để tạo Block, Node lỗi được thiết lập với một số cặp khóa²⁴² và chứng chỉ hoạt động. Nó chỉ giao tiếp với các Node Relay mà nó đã thiết lập.

Hướng dẫn cấu hình Node và tạo chứng chỉ hoạt động:

- Giới thiệu về tệp cấu hình Node²⁴³
- Định cấu hình các tệp cấu trúc liên kết cho các Node Relay và tạo Block²⁴⁴
- Tạo chứng chỉ hoạt động với chữ ký phát triển chính (KES)²⁴⁵

²³⁹

Danh sách các role đã đăng ký, explorer.cardano-mainnet.iohk.io/relays/topology.json

²⁴⁰

Peer-to-peer (P2P): kiến trúc ứng dụng phân tán phân vùng các nhiệm vụ hoặc khối lượng công việc giữa các đồng nghiệp. Các đồng nghiệp đều có đặc quyền như nhau, những người tham gia bình đẳng trong ứng dụng. Chúng được cho là tạo thành một mạng lưới các Node ngang hàng. Trong Cardano, điều này liên quan đến việc gửi các giao dịch (hoặc tệp) trực tiếp giữa các Node trong một hệ thống phi tập trung mà không cần dựa vào cơ quan tập trung.

²⁴¹

Giới thiệu về mạng Cardano, docs.cardano.org/explore-cardano/cardano-network/about-the-cardano-network

²⁴²

Cặp khóa : Mật mã khóa công khai, hoặc mật mã bất đối xứng, là một hệ thống mật mã sử dụng các cặp khóa: khóa chung có thể được phổ biến rộng rãi và khóa riêng chỉ được biết bởi chủ sở hữu. Việc tạo các khóa như vậy phụ thuộc vào các thuật toán mã hóa dựa trên các vấn đề toán học để tạo ra các hàm một chiều. Bảo mật hiệu quả chỉ yêu cầu giữ khóa riêng tư; khóa công khai có thể được phân phối công khai mà không ảnh hưởng đến bảo mật. Trong Blockchain, các khóa này được sử dụng để xử lý và ủy quyền giao dịch

²⁴³

Giới thiệu về các tệp cấu hình node c , github.com/input-output-hk/cardano-node/blob/master/doc/getting-started/under-configuration-files.md

²⁴⁴

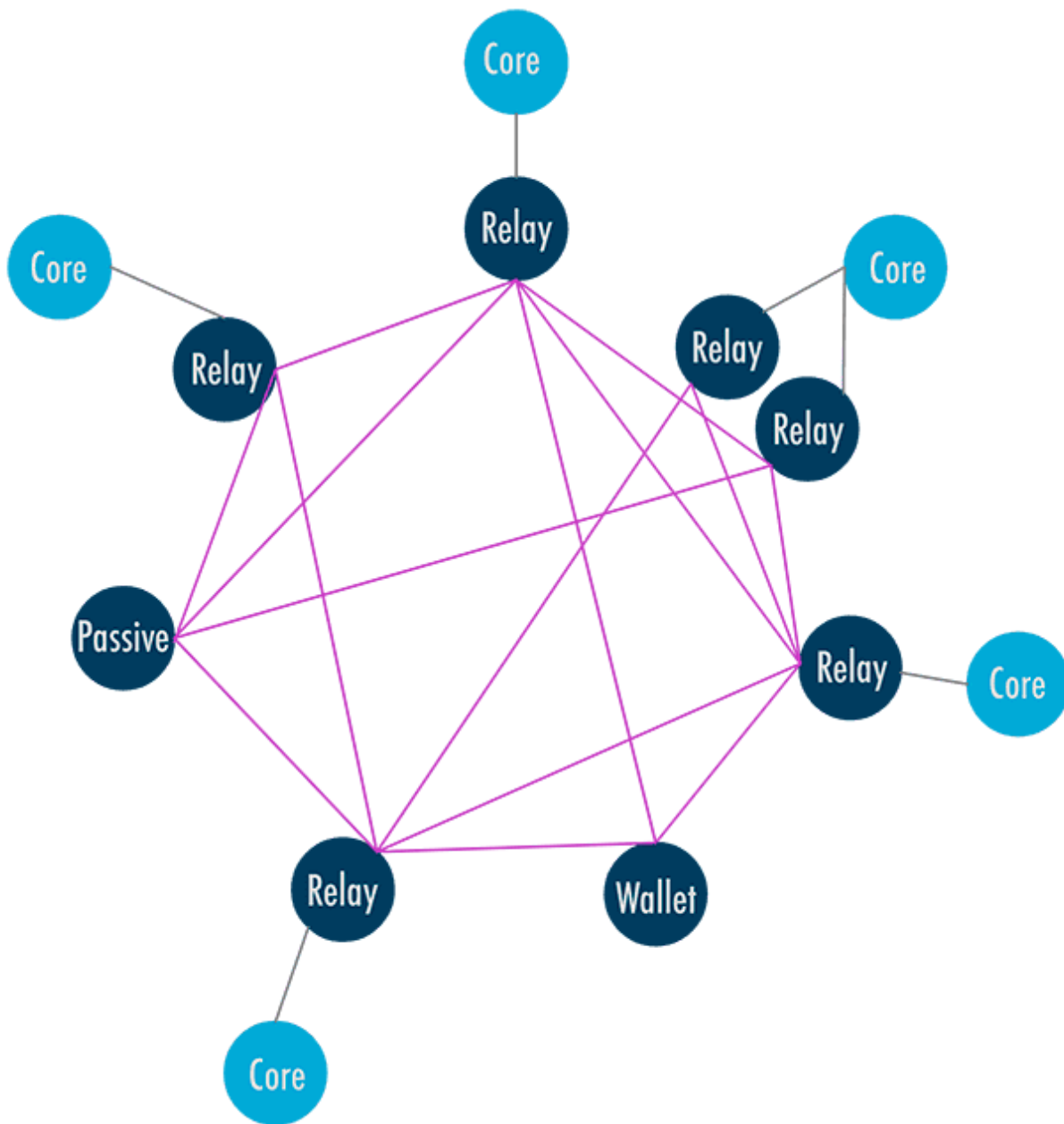
Định cấu hình các tệp cấu trúc liên kết cho các Node chuyển tiếp và tạo Block, github.com/input-output-hk/cardano-node/blob/master/doc/stake-pool-operations/core_relay.md

²⁴⁵

Tạo chứng chỉ hoạt động với chữ ký phát triển khóa (KES), github.com/input-output-hk/cardano-node/blob/master/doc/stake-pool-operations/KES_period.md

Vì một Node Relay không cần bất kỳ khóa nào nên nó không thể tạo Block. Nó giao tiếp với Node lõi, Relay và các Node bên ngoài.

Mỗi Node nên hoạt động trên máy chủ của chính nó, với tường lửa trên máy chủ Node lõi được đặt thành chỉ chấp nhận kết nối từ các Relay của nó.



Hình 8: Các Node lõi và Relay

Cách nghiên cứu Stake Pool

SPO (Người điều hành Stake Pool) có thể quan tâm đến việc nhận thông tin cụ thể về hoạt động của Pool sau khi đăng ký và vận hành Stake Pool thành công. Pooltool.io cung cấp các dữ kiện về Stake Pool đã được xác nhận, có thể được sử dụng để lấy thông tin về những Pool đang hoạt động trên mạng chính.²⁴⁶

²⁴⁶

Mainnet : Blockchain đã được triển khai và hiện đang được sử dụng. Tài sản được lưu trữ trên mạng chính có giá trị, nhưng tài sản được lưu trữ trên testnet thì không.

Đặc biệt, các sản giao dịch và SPO đang tìm kiếm thông tin chi tiết về Pool mạng chính và mạng thử nghiệm của họ trong một số trường hợp nhất định. Bạn nên sử dụng `cardano-node`, `cardano-db-sync`²⁴⁷ và `cardano-graphql`²⁴⁸ để truy cập dữ liệu được lưu trữ trên Blockchain Cardano.

GraphQL là ngôn ngữ thao tác và truy vấn dữ liệu nguồn mở dành cho API và là thời gian chạy để thực hiện các truy vấn với dữ liệu hiện có. GraphQL được Facebook phát triển nội bộ vào năm 2012 trước khi được phát hành công khai vào năm 2015. Vào ngày 7 tháng 11 năm 2018, dự án GraphQL đã được chuyển từ Facebook sang GraphQL Foundation mới thành lập, được tổ chức bởi Linux Foundation phi lợi nhuận. Đây là một đoạn Video ngắn mà tôi đã ghi lại để giải thích về *GraphQL trong 6 phút*.²⁴⁹

Docker²⁵⁰ có thể được sử dụng để cài đặt và triển khai từng thành phần tích hợp được mô tả ở trên.

Một giải pháp thay thế khác là Cardano Explorer công khai (explorer.cardano.org), cũng được xây dựng trên phiên bản `cardano-graphql` và thường được sử dụng bởi các sản giao dịch và các SPO muốn kiểm tra chức năng Stake Pool trên Testnet²⁵¹. Ngày càng có nhiều lựa chọn thay thế của bên thứ ba như *cexplorer.io*.

Hiệu suất của Stake Pool

Việc tạo các Block mới cho mạng Cardano là trách nhiệm của Stake Pool được chỉ định là Slot Leader²⁵². Slot sẽ không được lấp đầy nếu Stake Pool không tạo Block và Blockchain sẽ không được mở rộng. Mặc dù Blockchain Cardano có thể chấp nhận một vài Block bị thiếu, nhưng phần lớn các Block dự kiến (ít nhất 50% + 1) phải được tạo trong một Epoch. Mặc dù các Block bị thiếu không ảnh hưởng đến phần mở rộng tổng thể của Blockchain, nhưng Stake Pool được bầu chọn không phản hồi sẽ làm giảm tốc độ chung của mạng.

Tỷ lệ số lượng Block mà Stake Pool tạo ra trong một Epoch cụ thể so với số Block mà nó có khả năng tạo ra được sử dụng để đo hiệu suất của Stake Pool. Ví dụ: nếu Stake Pool có thể tạo 100 Block trong một Epoch (tùy thuộc vào cổ phần và khả năng được bầu chọn), nhưng chỉ tạo ra 50 Block, thì hiệu suất của nó sẽ là 50%. Hiệu suất Stake Pool kém làm giảm số lượng phần thưởng mà một Pool và các thành viên của nó nhận được, khiến nó trở nên kém hấp dẫn hơn đối với những người ủy quyền. Một Stake Pool phải có kết nối mạng đầy đủ, được chạy trên một hệ thống đáng tin cậy và tham gia vào việc tạo và xác minh Block để tăng hiệu suất của nó.

Hiệu suất của Pool càng mạnh thì càng hấp dẫn đối với những người ủy quyền, vì phần thưởng sẽ được cung cấp cao hơn. Thiết lập và vận hành Stake Pool không quá khó khăn từ góc độ kỹ thuật. Tiếp thị và thu hút những người ủy quyền cho Pool của bạn là một lĩnh vực cạnh tranh.

Xếp hạng Stake Pool

Stake Pool được xếp hạng trong ví Daedalus và Cardano Explorer tùy thuộc vào số lượng phần thưởng mà người dùng sẽ nhận được nếu họ chọn ủy quyền. Bảng xếp hạng cho biết mức độ bão hòa²⁵³ của Pool, giúp việc lựa chọn Pool dễ dàng hơn. Từ quan điểm của

²⁴⁷

`cardano - db -sync` , [github.com/input-output-hk/cardano - db -sync](https://github.com/input-output-hk/cardano-db-sync) _

²⁴⁸

`cardano - graphql` , github.com/input-output-hk/cardano-graphql

²⁴⁹

GraphQL sau 6 phút, [youtube.com/watch?v = Ys-aox3oOD8](https://youtube.com/watch?v=Ys-aox3oOD8)

²⁵⁰

Docker là một công cụ phần mềm giúp triển khai ứng dụng dễ dàng hơn bằng cách sử dụng 'bộ chứa', mỗi bộ chứa chứa tất cả các phần, chẳng hạn như thư viện, mà ứng dụng cần chạy.

²⁵¹

Testnet là một Blockchain thay thế được các nhà phát triển phần mềm sử dụng để kiểm tra xem mã của họ có chạy đúng cách hay không trước khi họ triển khai một mạng chính có thể **tồn kém** . Testnet sử dụng công nghệ và phần mềm giống hệt như blockchain 'mainnet', nói cách khác là một mạng song song, ngoại trừ testnet không thực hiện các giao dịch 'thực tế' với 'giá trị' và được dùng cho mục đích thử nghiệm. Tiền testnet khác với tiền thực tế trên mạng chính, vì tiền testnet không có bất kỳ giá trị tiền tệ nào.

²⁵²

Người dẫn đầu vị trí, developers.cardano.org/docs/stake-pool-course/introduction-to-cardano/

²⁵³

Bão hòa : một từ dùng để chỉ nhóm cổ phần có nhiều cổ phần được ủy quyền cho nó hơn mức tối ưu cho mạng. Mức độ bão hòa được biểu thị bằng phần trăm. Khi nhóm cổ phần đạt đến mức bão hòa 100%, phần thưởng bắt đầu thu hẹp lại. Cơ chế bão hòa được tạo ra để tránh tập trung hóa bằng cách khuyến khích người ủy quyền ủy quyền cho nhiều nhóm cổ phần và người vận hành xây dựng các nhóm thay thế để tiếp tục nhận được phần thưởng tối đa. Saturation nhằm mục đích bảo vệ cả lợi ích của những người nắm giữ ADA ủy quyền cổ phần của họ và lợi ích của những người điều hành nhóm cổ phần.

người ủy quyền, một khi Pool đạt đến ngưỡng bão hòa cụ thể, việc ủy quyền cho Pool đó không còn sinh lãi nữa. Stake Pool mong muốn nhất được hiển thị đầu tiên và chúng được sắp xếp từ trên xuống dưới.

Hệ thống xếp hạng nhằm cho phép người dùng chọn Stake Pool tốt nhất để có lợi tức đầu tư (ROI) cao hơn, để chủ sở hữu Stake Pool đáng tin cậy có thể duy trì hệ thống hoạt động và tối đa hóa khả năng phi tập trung.

Các thông số xếp hạng

Chi phí và tỷ suất lợi nhuận của một Pool, cũng như hiệu suất của Pool và số lượng cổ phần mà Pool đó đã thu hút trước đó, tất cả đều là yếu tố ảnh hưởng đến xếp hạng của Pool đó. Các biến này khuyến khích việc tạo ra các Stake Pool đáng tin cậy chưa bão hòa và cung cấp chi phí và lợi nhuận thấp.

*Tài liệu Cardano bao gồm các hướng dẫn để vận hành Stake Pool lớn.*²⁵⁴

Các loại địa chỉ trong Cardano

Các địa chỉ là Hash blake2b-256 của các khóa xác minh/khóa công khai có liên quan được kết hợp với một số siêu dữ liệu được lưu trữ trên Blockchain Cardano.

Shelley đã giới thiệu bốn loại địa chỉ khác nhau:

- địa chỉ cơ sở
- địa chỉ con trỏ
- địa chỉ doanh nghiệp
- địa chỉ tài khoản thường

Ngoài những địa chỉ đó, các địa chỉ tập lệnh và Bootstrap²⁵⁵ của kỷ nguyên Byron vẫn được Shelley hỗ trợ. Chỉ có địa chỉ cơ sở và con trỏ mới có quyền cổ phần. Các địa chỉ, chẳng hạn như địa chỉ UTXO²⁵⁶, được tạo thành từ dữ liệu được tuần tự hóa được mô tả trong đặc tả sổ cái được lưu trữ trong các Block của Blockchain.

Có hai phần đối với dữ liệu tuần tự hóa (địa chỉ):

- Siêu dữ liệu để giải thích.
- Tải trọng: dữ liệu thô hoặc được mã hóa

Địa chỉ cơ sở

Stake Key sẽ quản lý số lượng cổ phần cho địa chỉ đó được chỉ định rõ ràng trong địa chỉ cơ sở. Chủ sở hữu của Stake Key có thể thực hiện các quyền Staking liên quan đến số tiền được giữ tại địa chỉ này. Nếu không đăng ký Stake Key trước, địa chỉ cơ sở có thể được sử dụng trong các giao dịch. Chỉ bằng cách đăng ký Stake Key và ủy quyền cho Stake Pool²⁵⁷ thì quyền Staking mới có thể được thực hiện. Sau khi Stake Key đã được đăng ký, quyền Staking có thể được thực hiện cho các địa chỉ cơ sở được sử dụng trong các giao dịch trước hoặc sau khi đăng ký khóa.

Địa chỉ con trỏ

Một địa chỉ con trỏ gián tiếp chỉ định Stake Key sẽ kiểm soát số lượng cổ phần cho địa chỉ. Chúng khá nhiều sắc thái và việc sử dụng

²⁵⁴

Nguyên tắc dành cho các SPO lớn,
github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/04-guidelines-for-large-spos.mdx

²⁵⁵

Nói chung, **bootstrapping** thường đề cập đến một quá trình tự bắt đầu được cho là sẽ tiến hành mà không cần đầu vào bên ngoài. Trong công nghệ máy tính, thuật ngữ này (thường được rút ngắn thành khởi động) thường đề cập đến quá trình tải phần mềm cơ bản vào bộ nhớ của máy tính sau khi bật nguồn hoặc thiết lập lại chung, đặc biệt là hệ điều hành sau đó sẽ đảm nhận việc tải phần mềm khác khi cần.

²⁵⁶

Đầu ra giao dịch chưa sử dụng (UTXO) là thuật ngữ kỹ thuật cho lượng tiền kỹ thuật số còn lại sau một giao dịch Crypto.

²⁵⁷

Nhóm cổ phần, docs.cardano.org/core-concepts/stake-pools

thực tế của chúng vẫn còn là một câu hỏi. Chúng không được thảo luận chi tiết ở đây vì chúng không trực quan dễ hiểu, nhưng cũng bởi vì việc xóa địa chỉ con trỏ là một yếu tố phụ thuộc để triển khai phiên bản tương lai của Ouroboros. Để tìm hiểu lý do kỹ thuật, hãy xem cuộc thảo luận đang diễn ra về *Loại bỏ địa chỉ con trỏ CPS-0002*²⁵⁸. CPS là viết tắt của 'Cardano Problem Statement - Tuyên bố Vấn đề Cardano', một cơ chế quản trị để đề xuất thay đổi. Nó sẽ được nhắc đến thêm sau này.

Địa chỉ doanh nghiệp

Vì địa chỉ doanh nghiệp không đi kèm với quyền Staking, nên việc áp dụng chúng có nghĩa là bạn chọn không tham gia giao thức bằng chứng cổ phần. Quyền Staking có thể không được thực hiện bởi các sản phẩm dịch vụ hoặc các thực thể khác thay mặt cho những người dùng khác kiểm soát số lượng ADA đáng kể. Các sản phẩm dịch vụ có thể chỉ ra rằng họ tuân thủ nguyên tắc này bằng cách sử dụng địa chỉ doanh nghiệp. Địa chỉ doanh nghiệp sẽ tự động bị xóa khỏi quy trình xác định lịch trình Slot Leader do chúng không được kết nối với bất kỳ Stake Key nào. Việc sử dụng các địa chỉ không có quyền cổ phần sẽ làm giảm tổng số lượng cổ phần, điều này hỗ trợ cho một cuộc tấn công trong tương lai.

Địa chỉ tài khoản phần thưởng

Địa chỉ phần thưởng²⁵⁹ là Hash mật mã của Stake Key công khai của địa chỉ. Để trả phần thưởng cho việc tham gia vào giao thức bằng chứng cổ phần, địa chỉ tài khoản phần thưởng được sử dụng (trực tiếp hoặc thông qua ủy quyền).

Chúng sở hữu những đặc điểm sau:

- Kế toán kiểu tài khoản được sử dụng thay vì kiểu UTXO
- Giao dịch không thể được sử dụng để nhận tiền. Thay vào đó, khi phần thưởng được trả, số dư của họ²⁶⁰ chỉ tăng lên
- Stake Key đã đăng ký và địa chỉ tài khoản phần thưởng có mối quan hệ một đối một.

Khi tiền được xóa khỏi địa chỉ, khóa này sẽ được sử dụng. Ngoài ra, cổ phần được kết nối với số tiền trong địa chỉ góp phần vào cổ phần của khóa này. Đối tượng Staking cho địa chỉ phần thưởng không cần phải bao gồm bất kỳ thông tin nào, giống như với địa chỉ doanh nghiệp.

Cam kết

Phi tập trung hóa đã trở thành một điểm gây tranh cãi khi Shelley tiếp cận trên mạng chính Cardano. Các loại Crypto bằng chứng công việc như Bitcoin đã ngày càng phát triển tập trung theo thời gian, bất kể mục đích thành lập ban đầu của chúng là gì. Thời của những người đam mê Bitcoin khai thác các Block trên các phiên bản giao ngay AWS EC2²⁶¹ đã qua lâu rồi và các mạng khai thác ngày nay bị chi phối bởi một số ít các công ty khai thác chuyên nghiệp, chuyên biệt.

Bản thân điều này không phải là một điều tiêu cực, nhưng nó sẽ đi ngược lại ý tưởng của Cardano về một hệ thống bằng chứng cổ phần phi tập trung nếu nó xảy ra. Cardano được xây dựng từ dưới lên với lưu ý đến tính phi tập trung, đặc biệt là về hệ thống phần thưởng và ủy quyền cổ phần. Các Pool lớn hơn một kích thước nhất định sẽ không cạnh tranh trên mạng Cardano và phần thưởng ủy quyền cho mọi người sẽ là lý tưởng khi có nhiều Pool cỡ trung bình. Sự đa dạng có lợi cho tất cả các hệ sinh thái. Tương tự như vậy, phương pháp này tạo ra sự kết hợp tối ưu giữa việc thúc đẩy sự tham gia của cơ sở từ các thành viên cộng đồng có kinh nghiệm và hỗ trợ các cá nhân muốn thành lập các công ty cổ phần thương mại.

Cách thức hoạt động của cam kết

Một SPO có thể cam kết đầu tư cá nhân vào nhóm của họ khi đăng ký để làm cho nó hấp dẫn hơn. Số tiền cam kết có thể được sửa đổi theo từng Epoch và sẽ được hoàn trả khi Pool đóng lại.

²⁵⁸Loại bỏ địa chỉ con trỏ CPS-0002, github.com/cardano-foundation/CIPs/pull/374

²⁵⁹

Ví phần thưởng: ví chứa ADA và có thể được sử dụng để ủy thác cổ phần. Một cổ phần chỉ có thể được ủy quyền cho một nhóm cổ phần duy nhất từ một ví Phần thưởng duy nhất. Bạn sẽ cần xây dựng nhiều ví Phần thưởng và chia ADA cho chúng nếu bạn muốn ủy quyền cho nhiều nhóm cổ phần. Việc ủy quyền chia nhóm đã được IOG hứa hẹn một thời gian nhưng đã bị hoãn lại, để cho phép tập trung nguồn lực vào các ưu tiên lộ trình khác.

²⁶⁰

Ví số dư: số dư ADA testnet ban đầu của bạn, được sao chép từ mạng chính thông qua ảnh chụp nhanh số dư, được lưu trữ trong ví này. Cổ phần của ví này không thể chuyển nhượng được, mặc dù nó có thể được chuyển đến và ủy quyền từ ví Phần thưởng.

²⁶¹

Chúng tôi có thể sử dụng phiên bản spot AWS để đảm bảo lợi nhuận khai thác không?, stackoverflow.com/questions/51665962/can-we-use-aws-spot-instances-for-guaranteed-mining-profits

Trên Blockchain Cardano, bất kỳ ai cũng có thể điều hành một Pool. Không có cam kết tối thiểu. Để làm cho Pool của họ hấp dẫn hơn, những người quản lý Pool có thể cam kết một số hoặc toàn bộ cổ phần của họ cho Pool. Càng nhiều ADA cam kết, càng nhiều phần thưởng sẽ được trao cho Pool, điều này sẽ thu hút nhiều người ủy thác hơn.

Cũng cần lưu ý rằng cũng không có cam kết tối đa, do đó, SPO có nhiều ADA để ủy thác có thể tối đa hóa lợi nhuận của chính họ bằng cách lấp đầy Pool bằng các cam kết và tránh thu hút bất kỳ ủy quyền nào. Tất nhiên, chỉ một số SPO có thể làm như vậy; hầu hết sẽ cố gắng thu hút ủy quyền bằng sự kết hợp của cam kết, chi phí rẻ, thu lợi nhuận thấp và hiệu suất mạnh mẽ.

Sự hấp dẫn của một Pool đối với người ủy quyền được xác định bởi bốn yếu tố liên kết với nhau:

- chi phí vận hành (càng thấp càng tốt)
- ký quỹ nhà điều hành (càng thấp càng tốt)
- hiệu suất (càng cao càng tốt)
- cam kết (càng cao càng tốt).

Người điều hành Pool có thể yêu cầu số tiền ký quỹ của người điều hành lớn hơn trong khi vẫn duy trì mong muốn của người ủy quyền bằng cách đưa ra một khoản cam kết lớn hơn.

Phần thưởng cam kết

Với hai Stake Pool tương tự nhau, Pool có cam kết cao hơn sẽ nhận được nhiều phần thưởng hơn và do đó sẽ hấp dẫn hơn đối với những người ủy quyền khác. SPO (Người điều hành Stake Pool) hoặc các chủ sở hữu Pool khác nên làm việc cùng nhau để thực hiện cam kết bằng cách ủy quyền cho chính họ. Điều quan trọng nữa là đảm bảo có đủ tiền trong các tài khoản sử dụng (các) địa chỉ của chủ sở hữu Pool làm tham chiếu cổ phần. Việc không đáp ứng cam kết sẽ dẫn đến việc bất kỳ chủ sở hữu hoặc người ủy quyền nào kiếm được phần thưởng cho Pool. Điều này hầu như luôn dẫn đến việc mất quyền ủy quyền và trong trường hợp xấu nhất là sự sụp đổ của Pool.

Không giống như ủy quyền, SPO chịu trách nhiệm phân phối tất cả phần thưởng cam kết. Điều này có thể được thực hiện theo bất kỳ cách nào được cả hai bên đồng ý và không bị điều chỉnh bởi Blockchain.

Tại sao chúng ta cần cam kết?

Cam kết trên Blockchain Cardano là một kỹ thuật để thúc đẩy một môi trường kinh tế lành mạnh. Cơ chế cam kết cũng được yêu cầu để ngăn chặn cuộc tấn công Sybil²⁶² vào hệ thống. Trong một cuộc tấn công như vậy, một người nào đó có rất ít cổ phần cá nhân thiết lập hàng trăm hoặc hàng nghìn Pool với tỷ suất lợi nhuận nhỏ và cố gắng rút phần lớn cổ phần vào Pool của họ. Họ có thể tác động đến sự đồng thuận và tham gia vào các cuộc tấn công chi tiêu gấp đôi²⁶³, tạo ra các nhánh, Block kiểm duyệt và gây hại hoặc thậm chí làm sập hệ thống nếu điều này thành công. Các cuộc tấn công như vậy bị ngăn chặn bằng cách làm cho các Pool có cam kết lớn hơn trở nên hấp dẫn hơn, vì giờ đây kẻ tấn công phải chia cổ phần của họ cho nhiều Pool, khiến các Pool đó trở nên kém hấp dẫn hơn và làm tăng chi phí vốn có để thực hiện một cuộc tấn công Sybil.

Cách đo lường tác động của Cam kết

Trước khi ra mắt Shelley trên mạng chính Cardano, cần phải đặt tham số ảnh hưởng đến cam kết. Tham số được tạo ra để linh hoạt và thích ứng theo thời gian. Mạng thử nghiệm Shelley Haskell²⁶⁴ là một tài nguyên tuyệt vời để tinh chỉnh tham số này và xác định giá trị

²⁶²

Lars Brünjes, 'Ngăn chặn các cuộc tấn công của bọn khủng bố', iohk.io/en/blog/posts/2018/10/29/preventing-sybil-attacks/

²⁶³

Chi tiêu gấp đôi là một lỗi hỏng tiềm ẩn trong sơ đồ tiền kỹ thuật số trong đó cùng một Token kỹ thuật số duy nhất có thể được chi tiêu nhiều lần. Không giống như tiền mặt vật lý, Token kỹ thuật số bao gồm một tệp kỹ thuật số có thể bị sao chép hoặc làm sai lệch. Đối với tiền giả, chi tiêu gấp đôi như vậy dẫn đến lạm phát bằng cách tạo ra một lượng tiền sao chép mới mà trước đây không tồn tại. Điều này làm giảm giá trị của tiền tệ so với các đơn vị tiền tệ hoặc hàng hóa khác và làm giảm lòng tin của người dùng cũng như việc lưu thông và lưu giữ tiền tệ. Các kỹ thuật mã hóa cơ bản để ngăn chi tiêu gấp đôi, đồng thời duy trì tính ẩn danh trong giao dịch, là chữ ký mù và, đặc biệt là trong các hệ thống ngoại tuyến, chia tách bí mật.

²⁶⁴

Kevin Hammond, 'From Byron to Shelley: Part one, the testnets', iohk.io/en/blog/posts/2020/04/29/from-byron-to-shelley-part-one-the-testnets/

nào hiệu quả và giá trị nào không. IOG cũng đã tạo một máy tính²⁶⁵ để hỗ trợ các SPO ước tính số lượng cam kết thay thế và tìm hiểu xem việc ủy quyền có thể bị ảnh hưởng như thế nào.

Các giá trị hợp lý được xác định bởi nhiều biến số, bao gồm: Người đó sở hữu bao nhiêu phần trăm tiền lãi của SPO? Chi phí để chạy một Node là bao nhiêu? Có bao nhiêu người muốn điều hành một Stake Pool? Trong mạng thử nghiệm được khuyến khích, rất nhiều dữ liệu đã được thu thập.

IOG cam kết thực hiện phương pháp khoa học, kiến trúc của họ sẽ tạo ra một Blockchain phi tập trung, ổn định và an toàn. Tuy nhiên, khoa học và toán học chỉ có thể đưa bạn đi xa. Các giả định về mô hình hóa luôn phải được đưa ra và sẽ không có mô hình nào phức tạp và nhiều màu sắc như những gì xảy ra trong thực tế.

Trên Reddit²⁶⁶ và trong tập 'Hiệu ứng Cardano'²⁶⁷ đã có một cuộc thảo luận sôi nổi về vấn đề này. Các mạng thử nghiệm Shelley Haskell cung cấp môi trường lý tưởng để tiếp tục tranh luận. IOG đã đánh giá, thử nghiệm và hợp tác với các nhà quản lý Stake Pool để xác định điều gì là tốt nhất cho mọi người. IOG đã tranh thủ sự hỗ trợ của cộng đồng để biến những phát hiện của họ thành hiện thực, giống như họ đã làm với mạng thử nghiệm được khuyến khích và thử nghiệm người dùng²⁶⁸ Daedalus Flight²⁶⁹.

Sự uỷ quyền

Thực tiễn chỉ định ADA của các bên liên quan riêng lẻ cho Stake Pool được gọi là ủy quyền cổ phần. Ủy quyền được sử dụng trong sản xuất Block để đảm bảo rằng Block được tạo theo sự đồng thuận bằng chứng cổ phần. Các bên liên quan không chuyển nhượng quyền sở hữu cổ phần, quyền biểu quyết hoặc các quyền khác khi họ ủy quyền.

Để duy trì niềm tin vào Blockchain, các SPO lớn thường sẽ sở hữu một lượng đáng kể cổ phần của bên thứ ba, khiến họ phải chịu trách nhiệm về:

- sản xuất Block
- xử lý giao dịch
- bảo trì mạng Cardano
- đảm bảo chủ sở hữu cam kết
- bảo mật Pool (bảo vệ khóa riêng của nó)
- cập nhật cộng đồng về bất cứ điều gì liên quan đến Pool.

Blockchain xử lý việc phân phối phần thưởng sản xuất Block cho những người ủy quyền, vì vậy các SPO lớn không quan tâm đến nó. SPO cũng không chịu trách nhiệm lấy khóa được ủy quyền hoặc hành động thay mặt cho các bên liên quan về ủy quyền, bỏ phiếu hoặc các hoạt động khác. Các bên liên quan cá nhân phải chịu trách nhiệm cá nhân đối với bảo mật của chính họ và đưa ra đánh giá của riêng họ về ủy quyền, bỏ phiếu và các vấn đề khác.

Bởi vì Cardano là một hệ thống bằng chứng cổ phần, nên việc có ADA mang lại cho bạn quyền và nghĩa vụ tham gia vào giao thức và xây dựng các Block ngoài việc cho phép bạn mua sản phẩm và dịch vụ. Ủy quyền cổ phần là một kỹ thuật được tích hợp trong giao thức bằng chứng cổ phần (PoS) của Cardano cho phép nó phát triển ngay cả khi đối mặt với một nhóm các bên liên quan phân tán rộng rãi.

Bất kỳ ai có ADA đều có thể tham gia vào quy trình ủy quyền cổ phần trong khi vẫn giữ khả năng chỉ tiêu của mình. Lưu ý rằng bất kể bạn đã ủy quyền ADA của mình như thế nào, bạn có thể chỉ tiêu nó ở bất kỳ giai đoạn nào. Trong mỗi Epoch, giao thức cho phép các bên liên quan tham gia vào quá trình bầu chọn Slot Leader.

²⁶⁵

Máy tính Cardano, cardano.org/calculator/?calculator=operator

²⁶⁶

Cardano Mainnet: Phân tích yếu tố ảnh hưởng của cam kết, reddit.com/r/cardano/comments/gfed1l/cardano_mainnet_pledge_influence_factor_analysis/

²⁶⁷

Các yếu tố ảnh hưởng đến cam kết, ảnh hưởng đến người điều hành và người đặt cược, với Umed Saidov | TCE 88, youtube.com/watch?v=ubWlytFZYGE

²⁶⁸

Anthony Quinn, 'Chúng tôi cần bạn cho chương trình thử nghiệm Daedalus!', iohk.io/en/blog/posts/2020/04/01/we-need-you-for-the-daedalus-flight-testing-program/

²⁶⁹

Daedalus Flight là phiên bản 'tiền phát hành' của ví Daedalus.

Ủy quyền cổ phần tạo ra 'Stake Pool', hoạt động tương tự như các Pool đào của giao thức Bitcoin. Khi họ được chọn làm Slot Leader, SPO phải trực tuyến để tạo Block.

Các yêu cầu về ủy quyền cổ phần

Ủy quyền cổ phần liên quan đến việc tải hai chứng chỉ lên chuỗi: đăng ký địa chỉ cổ phần và chứng chỉ ủy quyền. Vì việc đăng chứng chỉ cần có tiền nên người dùng mới bắt đầu sử dụng ví của họ cần có phương pháp khởi động. Cách tiếp cận này dựa trên khả năng của các địa chỉ cơ sở sử dụng Stake Key trước khi xuất bản chứng chỉ đăng ký của khóa. Địa chỉ cổ phần có thể dựa trên một khóa duy nhất hoặc tập lệnh như đa chữ ký.

Sơ đồ ủy quyền

Với khái niệm ủy quyền, bất kỳ bên liên quan nào cũng có thể ủy quyền cho Stake Pool tạo Block cho mạng Cardano và giao thức sau đó sẽ phân phối phần thưởng cho tất cả những người tham gia, bao gồm cả phí của SPO. Một bên liên quan được gán cho một ID Pool cụ thể, là Hash của khóa xác minh của SPO.

Bên liên quan có thể hạn chế không gian thông báo hợp lệ của khóa ký Proxy²⁷⁰ đối với các chuỗi kết thúc bằng số lượng Slot trong một phạm vi giá trị nhất định để giới hạn khả năng tạo Block của đại biểu trong một phạm vi Epoch và Slot cụ thể. Do tính chất có thể kiểm chứng và ngăn ngừa lạm dụng của sơ đồ chữ ký²⁷¹ Proxy, sơ đồ cơ bản này là đáng tin cậy. Điều này đảm bảo rằng mọi bên liên quan đều có thể xác minh rằng khóa ký Proxy đã được cấp cho một đại biểu cụ thể bởi bên liên quan đó và đại biểu đó chỉ có thể sử dụng các khóa này để ký thư bên trong không gian thư hợp lệ của khóa.

Cần có một giao dịch duy nhất với chứng chỉ ủy quyền để gửi tiền thuộc về một Stake Key trong ví của người dùng. Chi phí giao dịch tiêu chuẩn sẽ được áp dụng. Một bên liên quan phải trả một khoản đặt cọc để đăng ký một địa chỉ cổ phần, không phải cho chính ủy quyền cổ phần. Sau khi đăng ký địa chỉ cổ phần, bên liên quan sẽ chỉ phải trả phí cho ủy quyền đã chọn của họ. Trong quá trình trao thưởng, cổ phần của các bên liên quan sẽ được coi là một phần cổ phần của Pool.

Ví dụ về ủy quyền cổ phần

Hãy xem xét một người dùng được thiết lập để nhận ADA đầu tiên của họ, cho dù thông qua quy đổi, giao dịch trao đổi hay một số phương tiện khác. Họ sẽ tạo một ví mới và một địa chỉ để nhận các khoản thanh toán. Địa chỉ này sẽ là địa chỉ cơ sở sẽ được sử dụng với Stake Key được tạo bởi ví nhưng chưa được đăng ký trên Blockchain Cardano.

Sau đó, người dùng có thể tham gia Staking bằng cách đăng chứng chỉ đăng ký Stake Key và chứng chỉ ủy quyền cho Stake Key của họ. Các địa chỉ mới được tạo có thể là địa chỉ con trỏ tới chứng chỉ đăng ký Stake Key sau khi khóa đã được đăng ký.

Cam kết và phần thưởng

Cam kết là một phương pháp quan trọng để thúc đẩy sự phát triển của một hệ sinh thái lành mạnh trên Blockchain Cardano. Bạn có thể cam kết một phần hoặc toàn bộ ADA của mình cho Stake Pool khi bạn đăng ký nó để làm cho nó hấp dẫn hơn đối với những người muốn ủy quyền. Mặc dù việc cam kết không bắt buộc khi tạo Stake Pool, nhưng điều đó có thể khiến người ủy quyền mong muốn hơn vì số lượng ADA được cam kết càng lớn thì phần thưởng được trao càng cao. Tham số giao thức *a0* chỉ định cách cam kết ảnh hưởng đến phần thưởng Pool. Không có số tiền cam kết tối ưu, nó phụ thuộc vào Pool và sở thích cá nhân. Bạn càng cam kết phần thưởng càng cao.

Phân phối phần thưởng

Phần thưởng được cấp cho tất cả các bên liên quan đã ủy quyền cho Stake Pool, Pool của chính họ hoặc Pool khác, vào cuối mỗi Epoch. Giao thức tạo ra những phần thưởng này và không dựa vào các SPO để quản lý chúng. Có hai loại phần thưởng:

- Tất cả phí giao dịch: được tổng hợp từ tập hợp các giao dịch có trong một Block được đúc (được tạo) trong Epoch đó

²⁷⁰

Người sáng lập Cardano chia sẻ ý tưởng khóa proxy để triển khai,
coinregwatch.com/cardano-founder-shares-proxy-keys-idea-to-implement/

²⁷¹

Chữ ký ủy quyền là một loại chữ ký số đặc biệt cho phép một người dùng (người ký ban đầu) ủy quyền ký của mình cho người ký khác (người ký ủy quyền). Sau đó, cái sau có thể đưa ra chữ ký thay mặt cho cái trước.

- Mở rộng tiền tệ đòi hỏi phải xác định sự khác biệt giữa tổng cung và nguồn cung tối đa của ADA. Tất cả ADA hiện đang được lưu hành, cũng như ADA được giữ trong kho bạc, tạo nên tổng nguồn cung. Nguồn cung cấp tối đa đề cập đến nhiều ADA nhất có thể tồn tại (45 tỷ ADA). Dự trữ là sự khác biệt giữa hai khoản tiền này. Một tỷ lệ xác định trước của khoản dự trữ còn lại được rút trong mỗi Epoch và được sử dụng cho phần thưởng Epoch và kho bạc, với số tiền được chuyển đến kho bạc là một tỷ lệ phần trăm đã đặt của số tiền được lấy từ khoản dự trữ.

Nhà khoa học trưởng của IOG, Giáo sư Aggelos Kiayias thảo luận nhiều hơn trong Video *chia sẻ và cam kết Phần thưởng trên Cardano*.²⁷²

Hãy nhớ rằng cam kết được thể hiện (cùng với chi phí và số tiền ký quỹ) trong quá trình đăng ký Pool và phải được thực hiện bởi chủ sở hữu Pool đang ủy quyền cho Pool: Phần thưởng Pool cho Epoch đó sẽ bằng 0 nếu họ cùng nhau ủy quyền ít hơn mức cam kết đã chỉ định. Nếu tỷ suất lợi nhuận của SPO được đặt thành dưới 100%, thì Pool sẽ ở chế độ công khai.

Tùy chọn cam kết và ủy quyền

Trên mạng Cardano, ADA phản ánh cổ phần của người dùng trong giao thức, với số cổ phần tỷ lệ thuận với số lượng ADA sở hữu. Người dùng Cardano có thể nhận được phần thưởng thụ động để xác minh các Block nếu họ có cổ phần trong Crypto. Số lượng ADA mà họ cam kết hoặc ủy thác cho Stake Pool xác định số phần thưởng mà họ có thể nhận được.

Chủ sở hữu ADA có 3 lựa chọn khi ủy thác cổ phần của họ:

1. Họ chịu trách nhiệm về Stake Pool của riêng họ.
2. Dựa vào bên thứ ba để thay mặt họ quản lý Stake Pool tư nhân, chẳng hạn như Kraken²⁷³, một trong những sàn giao dịch Crypto lâu đời nhất.
3. Ủy quyền cho các Stake Pool khác

Xem hướng dẫn tạo giao dịch²⁷⁴ để được tư vấn về cách thiết lập Stake Pool, cam kết, ủy quyền và kiếm phần thưởng ADA.

Các Stake Pool phải duy trì tính sẵn sàng cao, có nghĩa là chúng phải có thể truy cập được để xác minh và tạo các Block mới mọi lúc. Số lượng ADA được cam kết hoặc ủy quyền, cũng như số Block mà một Stake Pool có thể xây dựng trong một Epoch cụ thể, xác định phần thưởng mà một Stake Pool có thể nhận được. Dựa trên các tiêu chí đã nói ở trên, Ouroboros, xương sống của giao thức Cardano, bầu chọn Slot Leader cấp quyền xử lý giao dịch và đúc các Block mới.

Lưu ý: Trước khi triển khai lên mạng chính, tất cả chức năng Stake Pool phải được kiểm tra kỹ lưỡng trên mạng thử nghiệm.

Cam kết

Khi một Stake Pool được khởi chạy, cam kết của SPO là số lượng ADA mà họ 'ủy thác' cho nhóm của chính họ. Cam kết của nhà điều hành để duy trì nhóm của họ và thúc đẩy hoạt động mạng có thể được nhìn thấy trong cam kết. Không cần thiết phải cam kết, tuy nhiên, bạn nên làm như vậy trước khi bắt đầu Stake Pool. Cam kết càng lớn, phần thưởng cho nhóm càng nhiều, tùy thuộc vào thời gian hoạt động và hiệu suất của nhóm.

Ủy quyền

Ủy quyền cho bất kỳ Stake Pool nào có thể truy cập trên mạng có thể mang lại các ưu đãi cho những người nắm giữ ADA không có bí quyết kỹ thuật trong việc vận hành Stake Pool. Ví dụ Daedalus có giao diện người dùng cho phép người dùng bắt đầu ủy quyền cho bất kỳ Stake Pool đã đăng ký nào ngay lập tức. Ví dụ ren *nhẹ* (lace.io) là một lựa chọn thân thiện hơn cho người mới bắt đầu.

Lưu ý: những người nắm giữ ADA và SPO (SPO) cam kết hoặc ủy quyền sẽ luôn có quyền truy cập vào ADA của họ. Phần thưởng giảm tương ứng khi ADA được ủy quyền được sử dụng hoặc rút khỏi nhóm.

²⁷²

Chia sẻ và cam kết phần thưởng trên Cardano, [youtube.com/watch?v=EAzyN3H8MOA](https://www.youtube.com/watch?v=EAzyN3H8MOA)

²⁷³

Kiểm 4-6% Staking Cardano (ADA), có sẵn trên Kraken ngay bây giờ!, blog.kraken.com/post/8891/earn-4-6-staking-cardano-ADA-available-on-kraken-now/

²⁷⁴

Tạo một giao dịch đơn giản, <https://developers.cardano.org/docs/stake-pool-course/handbook/create-simple-transaction/>

Phần thưởng

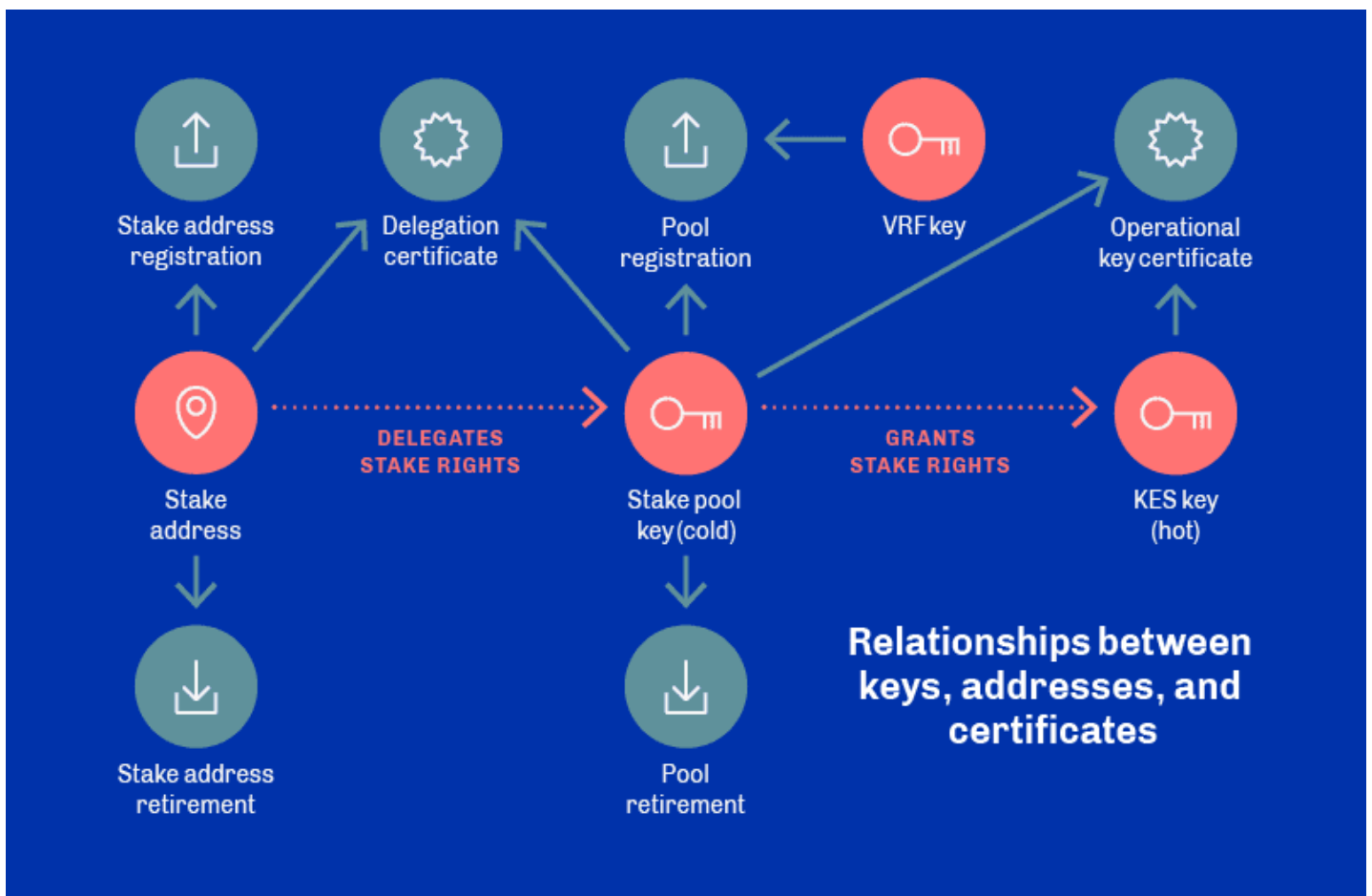
Khi tham gia đặt cược (cam kết hoặc ủy quyền), người ủy quyền kiếm được phần thưởng, phần thưởng này sẽ được chia ngay cho những người tham gia theo kế hoạch phần thưởng. Hệ thống phần thưởng của Cardano được phân cấp, nghĩa là không có một thực thể quản lý nào. Phần thưởng được tính toán theo giao thức Ouroboros và thường là khoảng 4-6% giá định rằng bạn đã ủy quyền cho Stake Pool chưa bão hòa. Nếu số lượng ADA được ủy quyền cho một Stake Pool nhất định vượt quá một lượng đã đặt, thì nhóm đó được coi là quá bão hòa. Tab ủy quyền trong Daedalus sẽ hiển thị các số liệu thống kê hữu ích và thông tin chi tiết về từng ứng cử viên ủy quyền Stake Pool.

Phần thưởng được phân phối mỗi kỳ nguyên cho Stake Pool để xác thực các Block. Vào năm 2022, khoảng 4% số tiền đặt cược sẽ được phân phối. Không nên nhầm lẫn việc đặt cược và phần thưởng với *việc kiếm tiền lãi*. Tiền lãi là một số tiền cố định được hứa cho người nhận, trong khi có một yếu tố ngẫu nhiên trong việc phân phối phần thưởng, với trách nhiệm của người nắm giữ ADA là ủy quyền cho một nhóm chưa bão hòa. Pooltool.io có một cột 'tiền lãi trên cổ phần'; điều này thay đổi từ 0% đến 18% đối với 2.978 nhóm được liệt kê.

Các loại khóa trong Cardano

mã hóa bất đối xứng²⁷⁵ được gọi là khóa được sử dụng cho:

- Bảo đảm các khoản thanh toán và chứng chỉ đặt cược bằng cách ký tên và xác minh chúng
- Xác định và xác định địa chỉ.



²⁷⁵Mật mã khóa công khai, hoặc mật mã bất đối xứng, là một hệ thống mật mã sử dụng các cặp khóa: khóa chung có thể được phổ biến rộng rãi và khóa riêng chỉ được biết bởi chủ sở hữu. Bảo mật hiệu quả chỉ yêu cầu giữ khóa riêng tư; khóa công khai có thể được phân phối công khai mà không ảnh hưởng đến bảo mật.

Hình 9. Liên kết giữa khóa, địa chỉ và chứng chỉ:

Có hai loại khóa chính trong Cardano:

- phím Node
- phím địa chỉ

Khóa Node

Các khóa sau đây tạo nên các khóa Node, cấu thành tính bảo mật của Blockchain.

- Toán tử/phím thao tác
- Cặp khóa KES
- phím VRF

Toán tử/phím thao tác

Đây là các cặp khóa ngoại tuyến dành cho người vận hành bao gồm bộ đếm chứng chỉ cho các chứng chỉ mới. Người điều hành chịu trách nhiệm quản lý cả khóa nóng (trực tuyến) và khóa lạnh (ngoại tuyến) cho nhóm. Khóa lạnh phải được giữ an toàn và không được lưu trữ trên thiết bị có quyền truy cập internet. Sao lưu khóa lạnh nên được giữ ở một số vị trí.

Cặp khóa KES Cần phải có cặp khóa

Chữ ký phát triển khóa ²⁷⁶(KES), xác thực bạn là ai, để thiết lập chứng chỉ hoạt động cho một Node tạo Block.

Khóa KES chỉ có thể phát triển trong một khoảng thời gian nhất định (một số kỷ nguyên nhất định) trước khi trở nên vô giá trị. Điều này quan trọng bởi vì, ngay cả khi kẻ tấn công thỏa hiệp khóa và có quyền truy cập vào khóa ký, anh ta chỉ có thể sử dụng nó để ký các Block trong tương lai, chứ không phải các Block từ các kỷ nguyên trước, ngăn kẻ tấn công viết lại lịch sử.

Người vận hành Node phải tạo cặp khóa KES mới, cấp chứng chỉ Node hoạt động mới với cặp khóa mới và khởi động lại Node bằng chứng chỉ mới khi hết số lượng kỷ nguyên được chỉ định.

Các khóa VRF

Ouroboros Praos (các phiên bản Ouroboros được giải thích sau, trong Chương 4) đã cung cấp một mức độ bảo vệ bổ sung bằng cách sử dụng các khóa Chức năng ngẫu nhiên có thể xác minh (VRF) trong sản xuất Block. VRF làm cho giao thức đồng thuận khó bị tấn công vì không thể dự đoán các Node sản xuất tiếp theo.

Bởi vì lịch trình của người dẫn đầu vị trí được biết đến trong các giao thức Blockchain bằng chứng cổ phần khác (chẳng hạn như Ouroboros Classic hoặc BFT), nên người ta biết ai có quyền tạo Block trong mỗi vị trí. Trong trường hợp này, bạn phải xác định rằng bạn là chính bạn và bất kỳ ai cũng có thể xác minh điều này bằng cách xem lịch trình của người dẫn đầu vị trí công khai. Quá trình này sau đó đã được cải thiện trong bản phát hành tháng 2 năm 2022, ²⁷⁷với một công cụ CLI mới dành cho các SPO để kiểm tra lịch trình dẫn đầu vị trí của chính họ.

Mặt khác, lịch trình của người đứng đầu vị trí của Ouroboros Praos được giữ kín, điều đó có nghĩa là không ai biết trước người đứng đầu vị trí sẽ là ai, nhưng một khi đã có, họ có thể xác minh với những người khác rằng họ đang sử dụng khóa VRF .

Khóa VRF là khóa xác minh chữ ký được ghi trong chứng chỉ vận hành. Nó thiết lập quyền của một Node để tạo một khối trong một vị trí nhất định.

phím địa chỉ

Mục đích của các khóa địa chỉ bắt nguồn từ các khóa để xác định ADA trên Blockchain, bao gồm các khóa sau:

- Khóa thanh toán: một cặp khóa địa chỉ thường được sử dụng để tạo địa chỉ UTxO

²⁷⁶

Tại sao lại sử dụng chữ ký phát triển chính, forum.cardano.org/t/why-use-key-evolving-signatures/11133/4

²⁷⁷

Tim Harrison, 'Từ nâng cao Node đến lãnh đạo khối... Bản phát hành tháng 2 của Cardano', iohk.io/en/blog/posts/2022/02/28/from-node-enhancement-to-block-leadership-cardano-s-february- giải phóng

- Khóa đặt cược: một cặp khóa bao gồm tiền đặt cược và địa chỉ phần thưởng thường được sử dụng để tạo địa chỉ tài khoản và phần thưởng.

Chữ ký

Nếu một loại Crypto sử dụng một sơ đồ chữ ký duy nhất, thì nó phải chấp nhận rủi ro rằng sơ đồ này có thể bị phá vỡ trong tương lai và ít nhất một thực thể sẽ không thể sử dụng Crypto do các ràng buộc pháp lý hoặc ngành. Tuy nhiên, một loại Crypto không thể hỗ trợ tất cả các sơ đồ chữ ký vì mỗi khách hàng sẽ phải hiểu và xác minh từng sơ đồ.

Đối với Cardano, IOG đã chọn bắt đầu bằng mã hóa đường cong elip, cụ thể là đường cong Ed25519.²⁷⁸

Cardano sẽ kích hoạt các hệ thống chữ ký bổ sung sau hard fork 'Vasil'. Chữ ký chống máy tính lượng tử sẽ được đưa vào hệ thống. Cardano được xây dựng với các tính năng cụ thể cho phép phân tách mềm và bổ sung các sơ đồ chữ ký mới. Chúng sẽ được đưa vào khi được yêu cầu và là một phần của các bản phát hành chính của lộ trình.

Ngày 19 tháng 3 năm 2020, để đáp lại dự luật của Thượng viện Hoa Kỳ và tuyên bố mã hóa ngoài vòng pháp luật . CH:²⁷⁹

Tôi nghĩ điều đó tương đương với khả năng đặt ngoài vòng pháp luật lực hấp dẫn hoặc thay đổi Pi thành 3. Ý tôi là mọi người chắc chắn có thể nói điều gì đó và cố gắng làm mọi việc, nhưng bạn không thể thực thi điều gì đó điên rồ như đặt ngoài vòng pháp luật mã hóa... nó giống như cách thức hoạt động của internet? SSL (lớp công bảo mật)²⁸⁰ hiện là bất hợp pháp? Bạn phải có cơ quan cấp chứng chỉ... thực hiện một cuộc tấn công trung gian cho mọi trang web? Chính phủ Hoa Kỳ có thực thi điều đó không? Đó là những người già không biết cách thức hoạt động của internet, hoặc công nghệ, đang chơi và nghịch ngợm mọi thứ... và họ nên quán tử thay vì bỏ phiếu.

Cardano RTView

RTXem²⁸¹ là một ứng dụng giám sát thời gian thực hiển thị trạng thái của các Node Cardano trong thời gian thực. Ngay cả khi các Node nằm trên các máy tính riêng biệt, nó vẫn cung cấp khả năng giám sát nhiều Node.

Các nhà phát triển, người thử nghiệm và người dùng cuối có các Node được kết nối với cụm thực tế có thể sử dụng RTView để xem những gì đang diễn ra và các Node đang hoạt động như thế nào. Nó cho biết lượng bộ nhớ và CPU đang được sử dụng, trạng thái của Blockchain, số khối mà một Node cụ thể đã giả mạo, số lượng giao dịch đã được xử lý, v.v.

Đây là chương trình đa nền tảng hoạt động với Windows, Linux và macOS, đồng thời có giao diện người dùng dựa trên web cho phép bạn sử dụng bất kỳ trình duyệt nào.

Ưu điểm chính của RTView là dễ sử dụng. Thật dễ dàng để thiết lập; về mặt lý thuyết, không cần cài đặt; tất cả những gì bạn phải làm là giải nén kho lưu trữ và chạy tệp thực thi. Việc thiết lập rất đơn giản vì nó có một cửa sổ bật lên thiết lập tương tác cho người dùng biết cần thực hiện những sửa đổi nào trong các tệp cấu hình Node. Nó cũng có thể được sử dụng với bất kỳ trình duyệt nào.

Cách thiết lập RTView

Làm theo hướng dẫn cài đặt để tải xuống, giải nén và khởi chạy RTView . RTView sẽ được khởi chạy và sẵn sàng sử dụng sau khi bạn hoàn thành các bước này.

²⁷⁸

Trong mật mã khóa công khai, Thuật toán chữ ký số đường cong Edwards (**EdDSA**) là lược đồ chữ ký số sử dụng một biến thể của chữ ký Schnorr dựa trên các đường cong Twisted Edwards. Nó được thiết kế để nhanh hơn các sơ đồ chữ ký số hiện có mà không ảnh hưởng đến tính bảo mật.

²⁷⁹

AMA bắt ngày 19/03/2020, youtu.be/9rCIM2pLNmo?t=2406

²⁸⁰

Bảo mật tầng vận chuyển (TLS) và tiền thân của nó, **Tầng công bảo mật (SSL)** , là các giao thức mật mã cung cấp bảo mật liên lạc qua mạng máy tính.

²⁸¹

Cài đặt RTView , github.com/input-output-hk/cardano-rt-view/blob/master/doc/getting-started/install.md/

Công cụ theo dõi Cardano

Bởi vì Cardano là một sổ cái Blockchain công khai, nhiều công cụ có thể được sử dụng để thuận tiện theo dõi tất cả các giao dịch gần đây, thông tin khối và dữ liệu kỹ nguyên.

Khám phá các giao dịch và khối

Cardano Explorer là một ứng dụng thân thiện với người dùng, lấy thông tin từ cơ sở dữ liệu chính và hiển thị thông tin đó trong giao diện trực tuyến dễ sử dụng.

Bằng cách chọn một khối duy nhất, bạn có thể khám phá thêm về khối đó, bao gồm ID, kích thước, kỹ nguyên và dữ liệu khối, cũng như số lượng giao dịch và xác nhận có trong đó. Bạn cũng có thể sử dụng khu vực tìm kiếm để tìm kiếm các kỹ nguyên, giao dịch hoặc khối nhất định bằng cách dán ID của chúng.

Có rất nhiều công cụ như *cardanoscan.io*, *ceexplorer.io* và nhiều công cụ khác được liệt kê trong IOG's Essential Cardano,²⁸² Công thông tin dành cho nhà phát triển Cardano,²⁸³ cũng như các trang web của bên thứ ba như *CardanoCube* (*cardanocube.io*) và *BuildOnCardano* (*buildoncardano.com*).

Khám phá tài sản

Cardano hỗ trợ tạo và quản lý nhiều tài sản. Bạn có thể sử dụng các công cụ như Cardano Assets (*cardanoassets.com*) và Cardanoscan (*cardanoscan.io/tokens*) để xem danh sách tài sản và Token. Mọi người đều có mục yêu thích của họ, của tôi là *taptools.io*

Khám phá Stake Pool

Bạn có thể sử dụng các công cụ này như ADApools (*ADApools.org*) và Pool.pm (*pool.pm/search*) để nhận danh sách tất cả các Stake Pool đang hoạt động, mã đánh dấu, tên nhóm và ID của chúng. IOG đã tạo một máy chủ tổng hợp siêu dữ liệu Stake Pool (SMASH) để cung cấp danh sách các Stake Pool đã được xác thực với thông tin phù hợp cho cộng đồng. Smash được kết nối với ví Daedalus và trong trang trung tâm ủy quyền, người dùng có thể xem danh sách các Stake Pool đủ điều kiện.

²⁸²

Cardano cần thiết, github.com/input-output-hk/essential-cardano/blob/main/essential-cardano-list.md

²⁸³

Công thông tin dành cho nhà phát triển Cardano, developer.cardano.org/showcase

Chương 4: Shelley (Sự đồng thuận)

'Nếu đông tới, xuân có thể lùi xa?'

- Percy Bysshe Shelley

Thách thức về khả năng mở rộng

Các hệ thống phân tán được tạo thành từ một nhóm máy chủ ²⁸⁴(các Node) đã đồng ý thực thi một giao thức hoặc một tập hợp các giao thức để đạt được mục đích chung. Mục tiêu này có thể đơn giản như phân phối tệp bằng giao thức BitTorrent ²⁸⁵ hoặc lưu trữ phi tập trung. ²⁸⁶

Khi có nhiều Node tham gia vào mạng, các giao thức hiệu quả nhất sẽ thu được tài nguyên. Ví dụ: nếu một số đồng nghiệp đang tải xuống đồng thời một tệp phim do BitTorrent cung cấp, thì trung bình, tệp đó có thể được tải xuống nhanh hơn đáng kể. Bởi vì các đồng nghiệp đều đóng góp và sử dụng hết tài nguyên, tốc độ tăng lên. Khi ai đó nói rằng một hệ thống phân tán có quy mô, họ thường đề cập đến tính năng này.

Vấn đề với hầu hết các giao thức Blockchain hiện có là chúng không được xây dựng để có thể mở rộng ngay từ đầu. Ví dụ, các Blockchain thường là một danh sách các Block được liên kết chỉ có thể được thêm vào. Tính bảo mật và tính khả dụng của giao thức Blockchain phụ thuộc vào nhiều Node có một bản sao hoàn chỉnh của dữ liệu Blockchain. Kết quả là N Node phải sao chép một bit dữ liệu. Các Node bổ sung đặt gánh nặng lên các tài nguyên cần thiết.

Điều này đúng cho cả giao thức xử lý giao dịch và giao thức tin đồn ²⁸⁷ trên toàn hệ thống. Việc tăng số lượng Node trong hệ thống đồng thuận không làm tăng sức mạnh xử lý giao dịch. Nó chỉ đơn giản chỉ ra rằng cần nhiều tài nguyên hơn để thực hiện cùng một nhiệm vụ. Nhiều mạng chuyên tiếp hơn có nghĩa là nhiều Node phải gửi cùng một thông báo để giữ cho toàn bộ mạng đồng bộ với khối gần đây nhất.

Crypto không thể phát triển thành một mạng lưới toàn cầu, có thể so sánh với các hệ thống tài chính cũ hơn, do cấu trúc của chúng. Mặt khác, cơ sở hạ tầng kế thừa có khả năng mở rộng và có thể xử lý các đơn đặt hàng có sức mạnh lưu trữ và xử lý lớn hơn. Bitcoin là một mạng tương đối nhỏ so với các đối tác thanh toán của nó như Visa, Mastercard, PayPal, v.v. và nó hiện đang phải vật lộn để xử lý tài hiện tại của mình.

Giao thức đồng thuận Ouroboros tăng cường khả năng mở rộng cho Cardano. Nó cho phép bầu cử phi tập trung một nhóm tối thiểu các Node đồng thuận, sau đó có thể thực thi các giao thức thông thường hơn để đáp ứng nhu cầu của các nhà cung cấp cơ sở hạ tầng không lồ như AWS, Google và Facebook.

Ví dụ: bầu một đại biểu cho một kỷ nguyên ngụ ý rằng có một nhóm Node đáng tin cậy để giữ cho sổ cái được cập nhật trong một khoảng thời gian nhất định. Thật đơn giản để bầu nhiều đại biểu cùng một lúc và phân chia các giao dịch giữa chúng.

Giao thức đồng thuận là gì?

Giao thức đồng thuận là tập hợp các quy tắc và tham số điều chỉnh hành vi của sổ cái phân tán: một bộ quy tắc mà mỗi thành viên mạng phải tuân theo. Không có một cơ quan trung ương nào chịu trách nhiệm về các Blockchain công khai. Thay vào đó, một cơ chế đồng thuận được sử dụng để cho phép người dùng mạng phân tán đồng ý về lịch sử của mạng như được ghi lại trên Blockchain - để đạt được thỏa thuận về những gì đã xảy ra và tiến hành từ một nguồn sự thật duy nhất.

Một bản ghi duy nhất được cung cấp bởi một nguồn sự thật. Đây là lý do tại sao các Blockchain thường được gọi là 'không tin cậy', vì niềm tin được tích hợp vào giao thức thay vì cần người dùng tin tưởng lẫn nhau. Các tác nhân không xác định có thể liên lạc và giao dịch với nhau mà không yêu cầu sự trung gian của bên thứ ba hoặc chia sẻ dữ liệu cá nhân.

Đồng thuận là phương pháp mà qua đó mọi người tham gia vào hoạt động của Blockchain đi đến một thỏa thuận. Phải có sự nhất trí về việc tạo Block nào, sử dụng chuỗi nào và cách thiết lập trạng thái đơn của mạng. Các Node riêng lẻ kiểm tra trạng thái hiện tại của sổ

²⁸⁴Máy chủ là một chương trình hoặc thiết bị máy tính cung cấp dịch vụ cho một chương trình máy tính khác và người dùng của nó, còn được gọi là máy khách.

²⁸⁵

BitTorrent là một giao thức truyền thông để chia sẻ tệp ngang hàng (P2P) được sử dụng để phân phối dữ liệu và tệp điện tử qua Internet. BitTorrent là một trong những giao thức phổ biến nhất để truyền các tệp lớn, chẳng hạn như các tệp kỹ thuật số chứa phim hoặc nhạc.

²⁸⁶

So sánh 4 dịch vụ lưu trữ dữ liệu phi tập trung, techtarget.com/searchstorage/tip/Comparing-4-decentralized-data-storage-offerings

²⁸⁷

Một **giao thức tin đồn** là một thủ tục hoặc quy trình giao tiếp ngang hàng trên máy tính dựa trên cách thức lây lan của dịch bệnh. Một số hệ thống phân tán sử dụng tin đồn ngang hàng để đảm bảo rằng dữ liệu được định tuyến tới tất cả các thành viên của mạng đặc biệt. Một số mạng ad-hoc không có cơ quan đăng ký trung tâm và cách duy nhất để truyền bá dữ liệu chung là dựa vào từng thành viên để chuyển dữ liệu đó cho hàng xóm của họ.

cái và hình thành sự đồng thuận bằng cách sử dụng giao thức đồng thuận Ouroboros. Nó có ba trách nhiệm chính: thực hiện kiểm tra đầu mối và quyết định xem có nên tạo một khối hay không, xử lý lựa chọn chuỗi và xác minh các Block đã được tạo.

Blockchain đạt được sự đồng thuận bằng cách cho phép người dùng nhóm các giao dịch được gửi tới hệ thống thành các Block và thêm chúng vào chuỗi của riêng họ (chuỗi các Block). Mục tiêu của các giao thức đồng thuận khác nhau là xác định ai được phép tạo Block? Khi? ... và phải làm gì trong trường hợp có bất đồng? Ví dụ: nếu hai người tham gia thêm các Block khác nhau cùng một lúc thì sao? Có nhiều loại giao thức đồng thuận khác nhau,²⁸⁸ hai loại chính là bằng chứng công việc và bằng chứng cổ phần. Ouroboros là một cơ chế đồng thuận dựa trên bằng chứng cổ phần đã được chứng minh là có cùng mức độ bảo mật như bằng chứng công việc.

Ouroboros

Ouroboros là một sinh vật thần thoại được đại diện là một con rắn hoặc rồng, nuốt chửng cái đuôi của chính nó trong một vòng tròn khép kín. Cái tên 'Ouroboros' bắt nguồn từ tiếng Hy Lạp cổ đại và có nghĩa đen là 'kẻ ăn đuôi' hoặc 'kẻ ăn đuôi'.

Ouroboros là biểu tượng cho thời gian vô tận chảy ngược vào chính nó trong một vòng tròn vô tận, như thể bị mắc kẹt trong một vòng lặp không hồi kết. Sự xuất hiện đầu tiên của Ouroboros là ở Ai Cập vào thế kỷ 13 trước Công nguyên. Các nhà giả kim sau đó đã sử dụng Ouroboros trong biểu tượng thần bí của họ. Ouroboros đã được nhiều nền văn minh hiểu và sử dụng theo nhiều cách trong suốt lịch sử. Một trong những cách giải thích phổ biến nhất của biểu tượng là nó biểu thị sự kết nối và vô hạn của Vũ trụ.

Charles Hoskinson đã đặt tên cho sự đồng thuận bằng chứng cổ phần của Cardano là Ouroboros vào năm 2017. Theo nghĩa này, Ouroboros phản ánh tiềm năng của Blockchain đối với khả năng mở rộng và tăng trưởng vô tận. Chủ đề cốt lõi của Ouroboros là cung cấp các khả năng mở rộng cho hành tinh, cũng như bảo tồn nó thông qua việc sử dụng năng lượng giảm đáng kể.²⁸⁹

Ouroboros là hệ thống đồng thuận Blockchain đầu tiên được tạo ra thông qua nghiên cứu được đánh giá ngang hàng như một giải pháp thay thế bền vững và tiết kiệm năng lượng hơn cho bằng chứng công việc, vốn là nền tảng của các loại Crypto trước đây như Bitcoin và cho đến gần đây là Ethereum. Ouroboros và các phiên bản khác nhau của nó tạo ra một nền tảng mới để giải quyết một số vấn đề khó khăn nhất của thế giới một cách an toàn và trên quy mô lớn.

Ouroboros đảm bảo tính bảo mật và tính bền vững của bất kỳ Blockchain nào sử dụng nó bằng cách kết hợp công nghệ độc đáo và các phương pháp được xác thực về mặt toán học (bao gồm tâm lý học hành vi và ý tưởng triết học kinh tế). Ouroboros đã được chứng minh là an toàn và có khả năng tạo điều kiện cho sự lan rộng của các mạng toàn cầu, không cần cấp phép với mức tiêu thụ năng lượng thấp. Cardano là mạng đầu tiên thuộc loại này. Ouroboros cho phép người dùng - trong ví dụ này là Stake Pool²⁹⁰ - thiết lập các Block mới dựa trên số cổ phần mà họ sở hữu trong mạng và do đó cho phép tạo ra một mạng phân tán, không cần cấp phép.

Các triển khai khác nhau của Ouroboros

Ngày 25 tháng 5 năm 2020. re: Ouroboros . CH:²⁹¹

Vì vậy, nếu tôi phải nói ngắn gọn .. 'vậy Ouroboros là gì?' ... Tôi muốn nói rằng đó là một cách thức mới, dựa trên các nguyên tắc đầu tiên để thực hiện sự đồng thuận giúp lưu giữ những thứ mà chúng ta đã biết và yêu thích từ Bitcoin, điều đó rất hữu ích và tuyệt vời, nhưng sau đó thực hiện nó theo cách thân thiện với năng lượng bền vững hơn nhiều, điều đó cũng cho phép bạn tạo ra nhiều tiện ích hơn là chỉ khai thác vào hệ thống. Nó làm như vậy theo cách thu hút nhiều cạnh tranh, nhiều phân cấp và nhiều doanh nghiệp. Khai thác có xu hướng tập trung vào một nhóm nhỏ các tác nhân vì tính kinh tế theo quy mô

Ouroboros **Ouroboros Classic** cổ điển

là triển khai đầu tiên được phát hành vào năm 2017. Nó đã thiết lập giao thức như một giải pháp thay thế tiết kiệm năng lượng cho

²⁸⁸

6 loại cơ chế đồng thuận blockchain, essentialcardano.io/article/6-types-of-blockchain-consensus-mechanisms

²⁸⁹

Fernando Sanchez, 'Tại sao họ gọi Cardano là Blockchain xanh', iohk.io/en/blog/posts/2021/08/17/why-they-re-calling-cardano-the-green-blockchain/

²⁹⁰

Về nhóm cổ phần, docs.cardano.org/getting-started/operating-a-stake-pool/about-stake-pools

²⁹¹

Phỏng vấn Lark Davis, youtu.be/BptZkkNN3tw?t=575

bằng chứng công việc, cung cấp một khung toán học để phân tích bằng chứng cổ phần và đưa ra cơ chế khuyến khích duy nhất cho người dùng bằng chứng cổ phần.

Điều làm nên sự khác biệt của Ouroboros so với các Blockchain trước đó và các giao thức bằng chứng cổ phần khác là khả năng cung cấp tính ngẫu nhiên không thiên vị trong phương thức lựa chọn người dẫn đầu của giao thức, cũng như các đảm bảo an ninh đi kèm với điều đó. Tính ngẫu nhiên ngăn các mẫu hình thành và là một khía cạnh quan trọng trong bảo mật của giao thức. Khi một hành vi có thể được mong đợi, hành vi đó có thể bị thao túng — và mặc dù Ouroboros đảm bảo tính minh bạch, nhưng nó ngăn chặn sự ép buộc. Ouroboros đáng chú ý vì là công nghệ Blockchain đầu tiên trải qua thử nghiệm bảo mật kỹ lưỡng như vậy.

Tài liệu nghiên cứu về Ouroboros có những giải thích sâu sắc về chức năng của nó. Blockchain được Ouroboros chia thành các vị trí và kỷ nguyên. Mỗi vị trí trong Cardano kéo dài 1 giây và mỗi kỷ nguyên (là một tập hợp các vị trí) bao gồm các vị trí có giá trị trong năm ngày.

Nhận thức rằng các cuộc tấn công là không thể tránh khỏi nằm ở trung tâm thiết kế của Ouroboros. Do đó, giao thức bao gồm khả năng chịu đựng để ngăn kẻ tấn công phát tán các bản sao khác của Blockchain và giả định rằng đối thủ có thể truyền thông điệp tùy ý tới bất kỳ thành viên nào vào bất kỳ lúc nào. Trên thực tế, giao thức được đảm bảo an toàn miễn là những người chơi trung thực nắm giữ hơn 51% cổ phần.

Mỗi vị trí có một người đứng đầu vị trí giám sát việc thêm các Block vào chuỗi và chuyển chúng cho người đứng đầu vị trí tiếp theo. Để ngăn chặn các nỗ lực thù địch nhằm phá hoại giao thức, mỗi người dẫn đầu vị trí mới có nghĩa vụ coi một số khối cuối cùng của chuỗi sắp tới là tạm thời, chỉ với chuỗi trước khi số lượng khối tạm thời được xác định trước được coi là đã được giải quyết. Điều này còn được gọi là độ trễ giải quyết. Điều này có nghĩa là, trong số những thứ khác, một bên liên quan có thể ngoại tuyến và vẫn được đồng bộ hóa với Blockchain, miễn là độ trễ không dài hơn độ trễ giải quyết.

Mỗi Node mạng trong giao thức Ouroboros giữ một bản sao của cả mempool giao dịch,²⁹² nơi các giao dịch mới được chèn vào nếu chúng nhất quán với các giao dịch hiện tại và Blockchain. Khi một Node nhận biết được một chuỗi mới hơn, hợp pháp hơn, thì Blockchain được lưu trữ cục bộ sẽ được thay thế.

Nhược điểm của Ouroboros Classic là nó dễ bị tấn công bởi những kẻ tấn công thích ứng — một mối nguy hiểm trong thế giới thực đã được giải quyết trong Ouroboros Praos — và không có phương tiện an toàn nào để thành viên mới khởi động từ Blockchain, vấn đề này được giải quyết bằng Ouroboros Genesis.

Ouroboros BFT²⁹³

Theo sau 'Cổ điển' là bài báo Ouroboros BFT vào năm 2018 (được triển khai vào tháng 5 năm 2020). Cardano đã sử dụng giao thức Ouroboros BFT (Byzantine Fault Tolerance) trong quá trình khởi động lại Byron, đây là quá trình chuyển cơ sở mã Cardano cũ sang cơ sở mã mới. Ouroboros BFT đã hỗ trợ chuẩn bị cho việc phát hành Shelley của Cardano, cùng với đó là tính phi tập trung.

Thay vì cần tất cả các Node luôn sẵn sàng, Ouroboros BFT giả định một mạng máy chủ được liên kết và giao tiếp đồng bộ giữa các máy chủ, cho phép đồng thuận số cái dễ dàng hơn và dễ dự đoán hơn.

Các ưu điểm khác bao gồm bằng chứng thanh toán ngay lập tức, thanh toán giao dịch ở tốc độ mạng (nghĩa là tốc độ kết nối mạng của bạn với Node OBFT xác định việc thanh toán giao dịch) và xác nhận ngay lập tức trong một chuyển liên lạc một vòng. Mỗi trong số này có tác động đáng kể đến hiệu suất.

Ouroboros Praos²⁹⁴ (giao thức hiện tại tại thời điểm viết, tháng 1 năm 2023)

Ouroboros Praos đã ra mắt vào năm 2018 (được triển khai vào tháng 8 năm 2020) và dựa trên Ouroboros Classic, nhưng với các cải tiến đáng kể về bảo mật và khả năng mở rộng. Ouroboros Praos, giống như Ouroboros Classic, chia các Block giao dịch thành các vị trí, sau đó được tổng hợp thành các kỷ nguyên. Mặt khác, Praos được kiểm tra trong bối cảnh bán đồng bộ và an toàn trước những kẻ tấn công thích ứng, không giống như Ouroboros Classic.

²⁹²

Vai trò của mempool trong nhiều giao dịch, docs.cardano.org/core-concepts/multiple-transactions

²⁹³

Kiayias, Russell (2018) 'Ouroboros-BFT: Giao thức đồng thuận chấp nhận lỗi Byzantine đơn giản', eprint.iacr.org/2018/1049.pdf

²⁹⁴

David, Gazi, Kiayias, Russell (2017) 'Ouroboros Praos: Blockchain bằng chứng cổ phần bán đồng bộ, an toàn thích ứng', eprint.iacr.org/2017/573.pdf

Nó giả định trước hai điều: đối thủ có thể truyền thông điệp tùy ý tới bất kỳ người tham gia nào vào bất kỳ lúc nào và những đối thủ đó có thể tri hoãn liên lạc của người tham gia trung thực trong nhiều thời điểm. Praos đảm bảo rằng kẻ tấn công mạnh mẽ không thể đoán được người dẫn đầu vị trí tiếp theo và tiến hành một cuộc tấn công có chủ đích (như tấn công DDoS) để phá hoại giao thức bằng cách sử dụng lựa chọn người dẫn đầu riêng tư và chữ ký phát triển khóa, an toàn chuyển tiếp. Lời khen ngợi cũng có thể chịu đựng được sự chậm trễ gửi tin nhắn do đối thủ kiểm soát và tham nhũng dần dần của từng người tham gia trong nhóm các bên liên quan đang phát triển, điều này rất quan trọng để duy trì an ninh mạng trong môi trường toàn cầu, miễn là phần lớn các bên liên quan trung thực được duy trì.

Nguồn gốc của Ouroboros²⁹⁵ (bài báo năm 2018, không được triển khai tại thời điểm báo chí, nhưng đang trong quá trình phát triển)

Ouroboros Genesis là phiên bản thứ tư của giao thức và được xây dựng trên Ouroboros Praos bằng cách bao gồm một cơ chế lựa chọn chuỗi duy nhất cho phép các bên khởi động từ một khối genesis — mà không cần yêu cầu về điểm kiểm tra đáng tin cậy hoặc giả định về tính khả dụng trước đó. Genesis cũng chứng minh khả năng kết hợp phổ biến của giao thức,²⁹⁶ chứng minh rằng nó có thể được sử dụng với các giao thức khác trong cấu hình thể giới thực mà không làm suy yếu tính trạng bảo mật của nó. Điều này tăng cường bảo mật và khả năng tồn tại lâu dài của nó, cũng như của các mạng sử dụng nó. Genesis đang được phát triển và cuối cùng sẽ cho phép tất cả các role IOG, cùng với việc triển khai ngang hàng, sẽ hoàn thành việc phân cấp mạng vật lý.

Ouroboros Hydra

Hydra là một kiến trúc mở rộng quy mô ngoài chuỗi giải quyết ba vấn đề chính về khả năng mở rộng: sản lượng giao dịch lớn, độ trễ thấp và dung lượng lưu trữ nhẹ trên mỗi Node. Sách trắng của Hydra đề xuất và trình bày chi tiết việc bao gồm các kênh trạng thái đa bên,²⁹⁷ cung cấp khả năng xử lý giao dịch song song để tăng đáng kể sản lượng giao dịch mỗi giây (TPS) của Cardano, cũng như xác nhận giao dịch nhanh chóng. Bài báo đề cập đến các anh chị em sỏ cái ngoài chuỗi — các kênh trạng thái — với tư cách là người đứng đầu, phản ánh tên gọi của việc triển khai. Điều này làm cho sỏ cái có nhiều đầu.

Thay vì mở rộng quy mô theo chiều dọc bằng cách thêm phần cứng mạnh hơn, Ouroboros Hydra cho phép Cardano mở rộng theo chiều ngang, nâng cao hiệu suất bằng cách bao gồm các Node bổ sung. Thử nghiệm ban đầu chỉ ra rằng mỗi đầu có khả năng 1.000 TPS. Hydra đang được phát triển với sự cộng tác của giao thức Ouroboros và sỏ cái Cardano, mặc dù nó có thể được sử dụng với các hệ thống khác miễn là chúng có cùng thuộc tính như Cardano. Hydra sau đó được tách ra khỏi Ouroboros và trở thành một dự án mã nguồn mở²⁹⁸ theo đúng nghĩa của nó. Thông tin thêm về Hydra ở phần sau của Chương 8.

Đồng thuận Redux

Consensus Redux²⁹⁹ được xuất bản vào tháng 8 năm 2020. Bài báo này thảo luận về khái niệm sỏ cái tự phục hồi. Làm thế nào để sỏ cái phục hồi khi nó bị tấn công? Làm thế nào để một mạng phục hồi khi nó bị tấn công? Bài viết phân tích các giải pháp trong cả hai loại.

Ouroboros Khóc

³⁰⁰

²⁹⁵

Badertscher, Gazi, Kiayias, Russell, Zikas (2019), 'Ouroboros Genesis: Blockchain bằng chứng cổ phần có thể kết hợp với tính khả dụng động', eprint.iacr.org/2018/378.pdf

²⁹⁶

Khuôn khổ của **khả năng tổng hợp phổ quát** là một mô hình có mục đích chung để phân tích các giao thức mật mã. Nó đảm bảo tính chất bảo mật rất mạnh. Các giao thức vẫn an toàn ngay cả khi được kết hợp tùy ý với các phiên bản khác của cùng một giao thức hoặc các giao thức khác. Bảo mật được định nghĩa theo nghĩa mô phỏng giao thức. Theo trực giác, một giao thức được cho là mô phỏng một giao thức khác, nếu không có môi trường nào (người quan sát) có thể phân biệt các lần thực thi. Theo nghĩa đen, giao thức này có thể mô phỏng giao thức khác (không có quyền truy cập vào mã). Khái niệm về bảo mật bắt nguồn từ hàm ý.

²⁹⁷

Các kênh trạng thái đề cập đến quá trình trong đó người dùng giao dịch với nhau trực tiếp bên ngoài Blockchain hoặc 'ngoài chuỗi' và giảm thiểu đáng kể việc sử dụng các hoạt động 'trên chuỗi' của họ.

²⁹⁸

Đầu Hydra GitHub, github.com/orgs/input-output-hk/projects/21

²⁹⁹

Badertscher, Gazi, Kiayias, Russell, Zikas (2020), 'Consensus Redux: Distributed Ledgers in Face of Adversarial Supremacy', eprint.iacr.org/2020/1021.pdf

³⁰⁰

Kerber, Kohlweiss, Kiayias, Zikas (2019), 'Ouroboros Cryptosignatures bảo vệ quyền riêng tư bằng chứng cổ phần', eprint.iacr.org/2018/1132.pdf

Bài báo Crypsinous đã được xuất bản vào năm 2019 nhưng vẫn chưa được thực hiện. Crypsinous là giao thức bằng chứng cổ phần bảo vệ quyền riêng tư đầu tiên. Nó tự hào có các tính năng bảo mật được tăng cường để bảo vệ chống lại các cuộc tấn công thích ứng bao gồm kỹ thuật phát triển tiên xu dựa trên SNARKS³⁰¹ và mã hóa bảo mật chuyển tiếp khóa-riêng tư.

Ouroboros Chronos³⁰²(Paper 2021, không được triển khai tại thời điểm viết bài)

Chronos sẽ mang lại khả năng phục hồi mạng và bảo mật cao hơn đối với sự chậm trễ trong giao tiếp bằng cách cung cấp tính năng chấm công toàn cầu chính xác hơn. Để duy trì tính mạnh mẽ của bất kỳ mạng phân tán nào, cần phải đồng bộ hóa thời gian toàn cầu. Đồng bộ hóa thời gian là rất quan trọng trong việc triển khai hợp đồng thông minh, từ việc đảm bảo thông tin cập nhật giữa tất cả những người tham gia để duy trì quá trình xử lý giao dịch chính xác và xây dựng khối.

IOG đã phát hiện ra một phương tiện để đồng bộ hóa đồng hồ trên một Blockchain kết hợp với các chuyên gia từ Đại học Edinburgh, Purdue và Connecticut để tạo ra một nguồn thời gian toàn cầu an toàn hơn và chống giả mạo. Điều này bao gồm đồng bộ hóa thời gian từ các thiết bị kết nối vạn vật (IoT)³⁰³, chẳng hạn như các công cụ giám sát chuỗi cung ứng và các hệ thống phân tán chung, đặc biệt nếu lỗi đồng hồ trung tâm gây ra sự cố bảo mật. Nghiên cứu được thực hiện với tên gọi Ouroboros Chronos (tiếng Hy Lạp có nghĩa là 'Thời gian').

Chronos là một giao thức Blockchain bảo mật bằng mật mã cũng cung cấp nguồn thời gian chính xác nhờ kỹ thuật đồng bộ hóa thời gian sáng tạo giúp tránh các sai sót của đồng hồ được bảo trì bên ngoài. Điều này cũng cho phép Blockchain đánh dấu thời gian chính xác cho các giao dịch, làm cho sổ cái có khả năng chống lại các cuộc tấn công dựa trên thời gian cao hơn.

Bằng cách đồng bộ hóa giờ địa phương với đồng hồ mạng thống nhất mà không có điểm lỗi duy nhất, giao thức mới có thể cải thiện đáng kể khả năng phục hồi của các hệ thống viễn thông, giao thông vận tải, thương mại và cơ sở hạ tầng thiết yếu. Thành tựu khoa học này cũng thể hiện một bước tiến lớn trong việc xây dựng các hệ thống tài chính hoàn toàn có thể kiểm toán được và chống gian lận bằng cách cung cấp thời gian chính xác và do đó có khả năng truy xuất nguồn gốc đầy đủ của tất cả các giao dịch.

Ngày 22 tháng 9 năm 2020, lại: Thời gian. CH:³⁰⁴

Ouroboros Chronos là một tờ báo đặc biệt. Leslie Lamport³⁰⁵ là một trong những người đầu tiên thực hiện công việc quan trọng trong các hệ thống phân tán và ông đã viết bài báo tuyệt vời này về đồng hồ và thời gian trong hệ thống phân tán từ những năm 1960 hoặc 1970. Đó là một trong những bài báo được trích dẫn nhiều nhất mọi thời đại trong thế giới hệ thống... 'Thời gian, đồng hồ và thứ tự các sự kiện trong một hệ thống phân tán'³⁰⁶ và Chronos giống như công việc đang dở về mặt đó. Thật thú vị khi viết những bài báo như vậy và nó có công dụng thực sự. Bạn hoàn toàn có thể tách rời sự phụ thuộc vào NTP³⁰⁷ và những thứ này, có rất nhiều lý thuyết ở đó.

Thời gian là tất cả

Trong các hệ thống và ứng dụng máy tính, ý tưởng về thời gian là rất quan trọng. Bạn sẽ không thể truy cập bất kỳ trang web dựa trên bảo mật tầng vận chuyển (TLS), trao đổi dữ liệu hoặc sử dụng các kỹ thuật mã hóa khác nếu không có khái niệm này.

301

SNARK là viết tắt của 'Lập luận kiến thức không tương tác ngắn gọn'. A (không có kiến thức) zk-SNARK là một bằng chứng mật mã cho phép một bên chứng minh rằng họ sở hữu một số thông tin nhất định mà không tiết lộ thông tin đó. Bằng chứng này được thực hiện bằng cách sử dụng khóa bí mật được tạo trước khi giao dịch diễn ra.

302

Badertscher, Gazi, Kiayias, Russell, Zikas (2019), 'Ouroboros Chronos: Đồng bộ hóa đồng hồ không cần xin phép thông qua Proof-of-Stake', eprint.iacr.org/2019/838.pdf

303

Internet **vạn vật (IoT)** là một hệ thống gồm các thiết bị máy tính, máy cơ khí và kỹ thuật số, vật thể, động vật hoặc con người có liên quan với nhau được cung cấp mã định danh duy nhất (UID) và khả năng truyền dữ liệu qua mạng mà không cần kết nối giữa người với người, hoặc tương tác giữa người với máy tính.

304

Thủ lĩnh máy đánh bạc Tập 1, youtu.be/YT0PXYBenuE?t=2218

305

Leslie Lamport, everipedia.org/wiki/lang_en/Leslie_Lamport

306

Leslie Lamport, 'Thời gian, đồng hồ và thứ tự các sự kiện trong hệ thống phân tán', dl.acm.org/doi/10.1145/359545.359563

307

Giao thức thời gian mạng (NTP) là một giao thức mạng để đồng bộ hóa đồng hồ giữa các hệ thống máy tính qua các mạng dữ liệu có độ trễ thay đổi được chuyển mạch gói. Được vận hành từ trước năm 1985, NTP là một trong những giao thức Internet lâu đời nhất được sử dụng hiện nay.

Mặt khác, theo dõi thời gian là một vấn đề khó giải quyết. Đồng bộ hóa thời gian chính xác yêu cầu truyền dữ liệu trên toàn bộ internet, điều này cũng tốn thời gian. Cũng khó dự báo thời gian truyền dữ liệu cụ thể sẽ mất bao lâu do trạng thái mạng liên tục thay đổi và bị ảnh hưởng bởi các biến số như tắc nghẽn và kích thước dữ liệu, trong số những yếu tố khác. Do đó, sự khác biệt là phổ biến và điều quan trọng là phải cung cấp các công cụ và giải pháp cần thiết để chấm công chính xác.

Thật dễ dàng coi việc chấm công là đương nhiên với các PC cơ bản. Tuy nhiên, đằng sau hậu trường, có một giao thức nghiêm ngặt phải tuân theo. Ví dụ, Giao thức thời gian mạng (NTP) sử dụng hệ thống phân cấp máy chủ trên toàn thế giới để giải quyết vấn đề chấm công.³⁰⁸ Điều này bao gồm tối đa 15 Tầng, mỗi tầng có định tuyến riêng được thiết kế để đồng bộ hóa theo cách hiệu quả nhất có thể. Sự phát triển của cây bao trùm đường dẫn ngắn nhất³⁰⁹ Bellman-Ford, giúp giảm độ trễ và sự không nhất quán về thời gian truyền, cũng có ích.

Đồng bộ hóa thời gian trên Blockchain

Đối với công nghệ sổ cái phân tán, ý tưởng về chấm công là khác nhau. Mạng không thể xác minh rằng giao dịch đang được xử lý là có thật và không đảo ngược giao dịch trước đó nếu không có dấu thời gian chính xác. Các thuật toán đánh dấu thời gian khác nhau được sử dụng trên nhiều loại sổ cái Blockchain; tuy nhiên, chúng không phải lúc nào cũng đáng tin cậy. Ví dụ, Bitcoin sử dụng dấu thời gian để bảo mật đồng thuận nhưng không phải để chấm công.

Chấm công cũng cần thiết để thực hiện hợp đồng thông minh. Các cuộc tấn công hợp đồng thông minh tài chính phi tập trung (DeFi) dễ bị thiếu chính xác. Các lỗ hổng trong hợp đồng thông minh không nhất thiết phải do mã xấu gây ra; sự khác biệt về thời gian nên được khắc phục để ngăn chặn bất kỳ cuộc tấn công tiềm ẩn nào vào sổ cái. Một số Blockchain, chẳng hạn như Solana, đã gặp sự cố nghiêm trọng về 'độ lệch đồng hồ'.³¹⁰

Thời gian để suy ngẫm

Việc xây dựng các nền tảng giao dịch phức tạp, chẳng hạn như Axo (axo.trade), không hề đơn giản khi tính toán thời gian chính xác trên một Blockchain phi tập trung. Chủ đề này đã được tranh luận trên các blog của IOG, trong các tài liệu³¹¹ và sôi nổi hơn trên twitter. Mặc dù thước đo thời gian hiện tại của Cardano có vẻ thỏa đáng để bao gồm nhiều trường hợp sử dụng, nhưng nó không hoàn hảo. Để tìm hiểu sâu hơn về các chi tiết kỹ thuật vụn vặt, tốt nhất bạn nên tham khảo quan điểm của một số chuyên gia. Axo trưởng Jarek Hirniak, một nhà phát triển có kinh nghiệm về phần mềm giao dịch, đã viết *Time on Cardano*,³¹² trong khi Sebastien Guillemot đã đề cập đến 'thời gian' một cách toàn diện trong một số video trên YouTube của anh ấy.³¹³

Ngày 12 tháng 12 năm 2020. Chronos có được triển khai không? CH:³¹⁴

Chúng tôi muốn không phụ thuộc vào bất cứ thứ gì và không có ai, và càng phi tập trung càng tốt. Vì vậy, chúng tôi là những người đầu tiên giải quyết vấn đề này trong bài báo đầu tiên thuộc loại này, với thứ gọi là Ouroboros Chronos, nhưng sẽ là một sự đánh lạc hướng không cần thiết nếu cứ theo đuổi 3 tháng triển khai để kéo Chronos vào, khi chúng tôi không cần nó như một hệ thống ngay bây giờ. [...]

³⁰⁸

Giao thức thời gian mạng, ntp.org/

³⁰⁹

Thuật toán **Bellman-Ford** tính toán các đường đi ngắn nhất từ một đỉnh nguồn duy nhất đến tất cả các đỉnh khác trong một sơ đồ có trọng số. Nó chậm hơn thuật toán Dijkstra cho cùng một vấn đề, nhưng linh hoạt hơn, vì nó có khả năng xử lý các đồ thị trong đó một số trọng số cạnh là số âm. Thuật toán lần đầu tiên được đề xuất bởi Alfonso Shimbel (1955), nhưng thay vào đó được đặt theo tên của Richard Bellman và Lester Ford Jr., người đã xuất bản nó lần lượt vào năm 1958 và 1956.

³¹⁰

Chuỗi thời gian ngừng hoạt động của Solana vẫn tiếp tục, Mạng lại gặp phải các vấn đề nghiêm trọng

³¹¹ thời gian trên Cardano, docs.cardano.org/explore-cardano/time

³¹² Jarek Hirniak về vấn đề thời gian của Cardano, twitter.com/ravanave/status/1589241299667800065?s=20&t=tCzT7srtCJ362-aWyi-jYA

³¹³ MinSwap & Axo : thời gian và các cuộc tấn công bánh sandwich trong Blockchain, youtube.com/watch?v=mGLm0QdVoNc

³¹⁴

AMA bắt đầu! 12/12/2020, youtube.be/GIVU8ZiVUL0?t=3061

Một điều khác là Chronos nên được triển khai với Consensus Redux, nên được triển khai với Genesis và nên được triển khai với thời hạn nhanh chóng. và cải tiến thông lượng cao cho hệ thống, vì vậy Ouroboros 2 (sau đó được đặt tên là Ouroboros Omega) là tổng hợp tất cả các nghiên cứu mà chúng tôi đã thực hiện để làm cho nó tốt hơn đáng kể so với bất kỳ sản phẩm nào trên thị trường. Vì vậy, tên của việc thực thi triển khai đang nói 'hôm nay có vấn đề gì? Một vấn đề lý thuyết nhưng không chắc là gì? So với vấn đề thực tế và chắc chắn có vấn đề cần giải quyết là gì?' ...và hiểu cách cân bằng mọi thứ và tạo ra một lộ trình phù hợp.

Ouroboros Leios

Bài báo ³¹⁵của Leios được xuất bản vào tháng 11 năm 2022 và có thể đọc được một cách đáng ngạc nhiên. Nó đã được xem trước trong video này ³¹⁶bởi Giáo sư Aggelos Kiayaas . Trọng tâm của Leios là Trình xác thực đầu vào, tận dụng chức năng cơ bản của Ouroboros đã nói ở trên cũng như Mithril (Xem Chương 8). Vì những người xác nhận đầu vào khá kỹ thuật và dựa trên các khái niệm chưa được thảo luận, nên chúng được đề cập trong phần cuối của Chương 8, *Basho (Khả năng mở rộng)* . Từ phần 6.2 của bài viết:

Cũng giống như Ouroboros Praos+Genesis là một sự kết hợp hợp lệ, Ouroboros Leios+Genesis cũng có ý nghĩa hoàn hảo và mang lại những lợi ích tương tự. Do đó, theo một nghĩa nào đó, Leios và Genesis là các tính năng độc lập. Trong thực tế, Genesis sẽ được triển khai vào thời điểm Leios khả dụng và do đó, sẽ là một sự thụt lùi nếu không bao gồm tính năng Genesis.

Ouroboros Omega ³¹⁷sẽ là đỉnh cao của tất cả các nghiên cứu về bằng chứng cổ phần mà IOG đã hoàn thành kể từ năm 2016. Sẽ sớm có một bài báo về 'sự hội tụ của tất cả các ý tưởng'.

Ngày 9 tháng 2 năm 2021. Bạn có thể nói về Ouroboros Omega không? CH:³¹⁸

Omega là đỉnh cao của tất cả các nghiên cứu của chúng tôi trong 6 năm qua cho Ouroboros: không phụ thuộc vào đồng hồ bên ngoài, tự phục hồi để có thể phục hồi dần các cuộc tấn công 51%, khả năng khởi động từ Genesis, bán đồng bộ, bảo mật thích ứng, tức thì tài chính... tất cả các loại nội dung...xác thực đa dạng cho mỗi khối...có rất nhiều nội dung.... Những thứ như bài báo Redux đồng thuận, bài báo Ledger Combiners ³¹⁹... bài báo Chronos, bài báo Genesis, bài báo Praos và sau đó là tất cả lý thuyết và sau đó là một số sự nhảy bèn về kỹ thuật, bao gồm cả việc cải thiện khoảng một nghìn TPS (giao dịch mỗi giây).

Cách lớp đồng thuận hoạt động

Tính trừu tượng ³²⁰là một tính năng chính của lớp đồng thuận.

Lớp đồng thuận Cardano chịu trách nhiệm cho hai nhiệm vụ chính:

1. Nó sử dụng cơ chế đồng thuận Blockchain để theo dõi các giao dịch. Sự đồng thuận, hay 'đa số ý kiến', trong ngữ cảnh của Blockchain, ngụ ý rằng mọi người tham gia đều đồng ý về một chuỗi thực sự. Điều này có nghĩa là lớp đồng thuận chịu trách nhiệm chấp nhận các Block, lựa chọn giữa các chuỗi đối thủ nếu có tồn tại và xác định thời điểm tạo các Block của riêng mình.

³¹⁵Coutts, Panagiotakos , Fitz , (2022) 'Ouroboros Leios : mục tiêu và khái niệm thiết kế', iohk.io/en/research/library/papers/ouroboros-leios-design-goals-and-concepts/

³¹⁶

Những tiến bộ trong Ouroboros: Mở rộng quy mô để phát triển trong tương lai, youtube.com/watch?v=xKv94MwSNBw

³¹⁷

Ouroboros Omega, [twitter.com/iohk_charles / status/1357364560504709120](https://twitter.com/iohk_charles/status/1357364560504709120)

³¹⁸

AMA bắt đầu 09/02/2021, youtube.be/K3l3_SAGXEE?t=1350

³¹⁹

Gazi, Kiayias , Russell, Zikas (2020) 'Bộ kết hợp số cái để thanh toán nhanh', eprint.iacr.org/2020/675.pdf

³²⁰

Tính trừu tượng được sử dụng để tạo các mô hình có thể được sử dụng và tái sử dụng mà không cần phải viết lại tất cả mã chương trình cho mỗi ứng dụng mới trên mọi loại máy tính khác nhau. Tính trừu tượng thường đạt được bằng cách viết mã nguồn bằng một số ngôn ngữ máy tính cụ thể , ngôn ngữ này có thể được dịch thành mã máy để các loại máy tính khác nhau thực thi. Trừu tượng hóa cho phép các nhà thiết kế chương trình tách một khung khỏi các trường hợp cụ thể triển khai các chi tiết.

2. Nó chịu trách nhiệm lưu giữ tất cả các thông tin cần thiết để đưa ra những đánh giá này. Giao thức phải xác minh một khối liên quan đến trạng thái của sổ cái trước khi quyết định có chấp nhận nó hay không. Nó phải lưu giữ đủ lịch sử để có thể xây dựng lại trạng thái sổ cái trên một chuỗi khác (một điểm khác của ngã ba trong chuỗi) nếu nó chọn chuyển sang một chuỗi khác. Nó phải duy trì một bản ghi nhớ³²¹ các giao dịch được đặt vào các Block đó để có thể tạo Block.

Lớp đồng thuận nằm giữa lớp mạng bên dưới nó, xử lý các giao thức truyền thông và lựa chọn ngang hàng, và lớp sổ cái phía trên nó, xác định cách sổ cái sẽ được cập nhật với mỗi khối mới và cách cập nhật nó. Lớp sổ cái hoàn toàn không trạng thái³²² và chỉ chứa các chức năng thuần túy. Do đó, lớp đồng thuận không cần thiết phải hiểu bản chất chính xác của trạng thái sổ cái hoặc thậm chí nội dung của các Block (ngoài một số trường tiêu đề cần thiết để chạy giao thức đồng thuận).

Lớp đồng thuận sử dụng rộng rãi tính trừu tượng. Điều này rất quan trọng vì nhiều lý do:

- Khi thực hiện các bài kiểm tra, nó cho phép các lập trình viên **mô phỏng các lỗi**. Ví dụ, IOG có thể trừu tượng hóa hệ thống tệp cơ bản và sử dụng nó để kiểm tra mức độ căng thẳng của lớp lưu trữ trong khi mô phỏng các lỗi đĩa khác nhau. Tương tự, chúng trừu tượng hóa theo thời gian và sử dụng điều này để xem điều gì xảy ra với một Node khi đồng hồ hệ thống của người dùng tăng hoặc giảm.
- Nó cho phép IOG **sử dụng nhiều loại sổ cái** để tạo lớp đồng thuận. Họ đã sử dụng nó để chạy lớp đồng thuận với sổ cái Byron và sổ cái Shelley cho mạng thử nghiệm Shelley Haskell. Họ cũng sử dụng nó để kiểm tra lớp đồng thuận bằng cách sử dụng các loại sổ cái khác nhau được phát triển rõ ràng để thử nghiệm, thường đơn giản hơn sổ cái 'thực', cho phép IOG tập trung kiểm tra của họ vào chính lớp đồng thuận.
- Nó **nâng cao tính tổng hợp**³²³ bằng cách cho phép IOG xây dựng các thành phần lớn hơn từ các thành phần nhỏ hơn. Ví dụ: sổ cái Shelley testnet chỉ bao gồm sổ cái Shelley; nhưng, sau khi Shelley được ra mắt, chuỗi thực tế có cả sổ cái Byron và Shelley cho đến thời điểm hard fork. Điều này đòi hỏi phải tạo ra một lớp sổ cái chuyển đổi giữa hai sổ cái tại một thời điểm xác định trước. Thay vì tạo một sổ cái mới, IOG đã tạo một bộ kết hợp hard fork chỉ thực hiện các tính năng này. Khả năng tái sử dụng mã nâng cao này (không cần triển khai lại chức năng hard fork cho các lần hard fork trong tương lai), cũng như phân tách trách nhiệm (sự phát triển và thử nghiệm của tổ hợp hard fork không phụ thuộc vào chi tiết của các sổ cái mà nó lật giữa).
- Việc sử dụng trừu tượng **làm tăng khả năng kiểm tra**. Bộ kết hợp là các biến thể của phương pháp đồng thuận cho phép IOG tập trung vào các khu vực nhất định. Ví dụ: IOG có một bộ kết hợp chấp nhận một giao thức đồng thuận hiện có và chỉ thay đổi kiểm tra để xem liệu có nên tạo một khối hay không. Sau đó, lớp đồng thuận có thể được sử dụng để thiết lập các kịch bản thử nghiệm trong đó nhiều Node tạo ra một khối trong một vị trí cụ thể hoặc ngược lại, không có Node nào cả và xác minh rằng nó hoạt động bình thường.

Vai trò đồng thuận

Giao thức đồng thuận có ba vai trò chính:

1. Kiểm tra người lãnh đạo (ai nên sản xuất một khối?)
2. lựa chọn chuỗi
3. chặn xác minh

Giao thức được thiết kế độc lập với một khối hoặc sổ cái cụ thể, cho phép một giao thức duy nhất được sử dụng với nhiều khối và/hoặc sổ cái khác nhau. Kết quả là, mỗi vai trò trong số ba vai trò này thiết lập 'bức tranh' dữ liệu của riêng mình.

Mỗi vị trí có một **kiểm tra đầu** để xác định xem Node có nên tạo một khối hay không. Trong thực tế, kiểm tra người lãnh đạo có thể cần trích xuất một số thông tin nhất định từ trạng thái sổ cái. Chẳng hạn, cơ hội để một Node được bầu làm người lãnh đạo (được ủy quyền tạo Block) trong giao thức đồng thuận Ouroboros Praos, phụ thuộc vào cổ phần của nó, cổ phần của Node.

³²¹

Mempool (**nhóm bộ nhớ**) là một cơ sở dữ liệu nhỏ hơn về các giao dịch chưa được xác nhận hoặc đang chờ xử lý mà mỗi Node lưu giữ. Khi một giao dịch được xác nhận bằng cách đưa vào một khối, giao dịch đó sẽ bị xóa khỏi mempool. Bạn có thể coi mempool giống như một 'phòng chờ', nơi một giao dịch nằm trước khi nó được thêm vào một khối.

³²²

Các dịch vụ **trạng thái** theo dõi các phiên hoặc giao dịch và phản ứng khác nhau với cùng một đầu vào dựa trên lịch sử đó. Các dịch vụ **phi trạng thái** dựa vào máy khách để duy trì các phiên và xoay quanh các hoạt động thao túng tài nguyên, thay vì trạng thái.

³²³

Trong toán học, ngữ nghĩa học và triết học ngôn ngữ, nguyên tắc **cấu thành** là nguyên tắc mà ý nghĩa của một biểu thức phức tạp được xác định bởi ý nghĩa của các biểu thức cấu thành nó và các quy tắc được sử dụng để kết hợp chúng.

Quá trình lựa chọn giữa hai chuỗi cạnh tranh được gọi là **lựa chọn chuỗi**. Độ dài chuỗi ³²⁴ là tiêu chí lựa chọn quan trọng nhất ở đây, tuy nhiên các giao thức khác có thể có các yêu cầu bổ sung.

Ví dụ: các Block thường được ký bằng phím 'nóng' tồn tại trên máy chủ và được tạo bằng phím 'lạnh' không bao giờ xuất hiện trên bất kỳ thiết bị nối mạng nào. Nếu phím nóng bị xâm phạm, người điều hành Node có thể tạo một phím mới bằng cách sử dụng phím lạnh và 'ủy quyền' cho nó.

Một giao thức đồng thuận sẽ ưu tiên khóa nóng mới hơn trên hai chuỗi có độ dài tương tự nhau, tức là . Mỗi chuỗi bao gồm một mero ³²⁵ được ký bởi cùng một phím lạnh nhưng một phím nóng khác.

Xác thực khối chủ yếu là một vấn đề về sổ cái; kiểm tra chẳng hạn như đảm bảo tất cả các đầu vào giao dịch có thể truy cập được để ngăn chỉ tiêu hai lần được chỉ định trong lớp sổ cái. Những gì bên trong các Block chủ yếu không được biết đến đối với lớp đồng thuận; trên thực tế, nó thậm chí có thể không phải là một loại Crypto, mà là một cách sử dụng công nghệ Blockchain khác biệt. IOG đã sử dụng ví dụ về sổ cái Pokémon ³²⁶ trên Ouroboros trước đây. Tuy nhiên, các tiêu đề khối bao gồm một số mục được thiết kế rõ ràng để hỗ trợ lớp đồng thuận.

Cấu hình Node

Để thực thi, mỗi giao thức có thể cần một số dữ liệu tĩnh nhất định, chẳng hạn như các khóa để ký các Block, một id duy nhất để kiểm tra đầu mối, v.v. Điều này được gọi là 'cấu hình Node.'

Trạng thái sổ cái

Lớp đồng thuận không chỉ xử lý trạng thái sổ cái mà còn vận hành giao thức đồng thuận. Nó không quan tâm đến giao diện của trạng thái sổ cái; thay vào đó, nó giả định rằng một số dạng trạng thái sổ cái được kết nối với một loại khối.

Nếu một khối không hợp lệ, bạn có thể gặp lỗi khi áp dụng nó vào trạng thái sổ cái. Lớp sổ cái xác định loại lỗi sổ cái chính xác, là loại lỗi sổ cái cụ thể. Ví dụ, sổ cái Shelley sẽ có lỗi đặt cược, nhưng sổ cái Byron thì không vì nó không cho phép đặt cược; và sổ cái không phải là sổ cái Crypto sẽ có các lỗi khá khác nhau.

Lớp đồng thuận Cardano được tạo ra với lưu ý đến Blockchain Cardano, ban đầu chạy Byron và được cập nhật để chạy Shelley. Thật công bằng khi đặt câu hỏi tại sao các nhà phát triển IOG không tạo ra Blockchain cụ thể đó trước? Sau đó khái quát hóa khi sử dụng lớp đồng thuận cho các Blockchain khác? Tuy nhiên, sẽ có những hạn chế đáng kể khi làm như vậy:

- Nó sẽ cản trở khả năng tiến hành các thử nghiệm của IOG. Họ sẽ không thể chọn Node nào tạo Block khi nào, họ sẽ không thể sử dụng sổ cái kép, v.v.
- Nó sẽ làm vướng víu những thứ lẽ ra phải tách biệt về mặt logic. Sổ cái Shelley, theo phương pháp trừu tượng, được tạo thành từ ba phần: chuỗi Byron, chuỗi Shelley và bộ kết hợp hard fork kết nối cả hai. Nếu không có sự trừu tượng hóa, việc phân tách các mối quan tâm như vậy sẽ khó thiết lập hơn, dẫn đến mã phức tạp hơn để hiểu và duy trì
- Mã trừu tượng ít có khả năng bao gồm các sai sót. Ví dụ: vì bộ kết hợp sổ cái kép đa hình ³²⁷ trong hai sổ cái mà nó kết hợp và chúng thuộc các loại khác nhau, nên IOG không thể tạo mã chính xác loại cố gắng áp dụng khối chính cho sổ cái phụ

³²⁴

Chiều cao khối biểu thị số lượng khối đã được xác thực và xác nhận trong toàn bộ lịch sử của một mạng Blockchain cụ thể, từ khối gốc (hoặc khối không) cho đến khối gần đây nhất. Không giống như khối genesis, tất cả các Block khác chứa một tham chiếu hoặc hàm băm cho khối xuất hiện ngay trước nó và chiều cao khối là số lượng của mỗi khối trong chuỗi đó. Vì vậy, chiều cao khối của khối genesis là #0 và chiều cao khối của khối đầu tiên là #1.

³²⁵

lệnh truy vấn cardano -cli (giao diện dòng lệnh) chứa lệnh con, một trong số đó là mero:
mero: lấy mero hiện tại của Node (số vị trí, hàm băm và số khối)

³²⁶

Anthony Quinn, 'Combinator giúp Shelley hard fork hoạt động dễ dàng',
iohk.io/en/blog/posts/2020/05/07/combinator-makes-easy-work-of-shelley-hard-fork

³²⁷ Đa hình: xảy ra ở một số dạng khác nhau. Trong điện toán (tính năng của ngôn ngữ lập trình) cho phép các thói quen sử dụng các biến thuộc các loại khác nhau tại các thời điểm khác nhau.

- Khi chắc chắn đến lúc khởi tạo lớp đồng thuận cho một Blockchain mới, việc viết nó theo cách trừu tượng ngay từ đầu buộc IOG phải suy nghĩ cẩn thận về thiết kế và tránh ghép nối những thứ không nên ghép nối hoặc đưa ra các giả định có thể hoặc có thể. nói chung là không đúng. Có thể khó khắc phục các sự cố như vậy khi thiết kế đã được triển khai.

Để đạt được tất cả những điều này, cần phải có một ngôn ngữ lập trình có khả năng trừu tượng hóa đặc biệt và Haskell được trang bị tốt về mặt này.

Ngày 10 tháng 1 năm 2021. Vui lòng giải thích Cardano được phân cấp gấp 100 lần so với BTC hoặc các loại khác, điều này được tính như thế nào? CH.³²⁸

Nó được tính toán bởi những người tạo ra các Block, vì vậy nếu bạn có gấp trăm lần các thực thể duy nhất tạo ra các Block, thì chúng tôi nói rằng nó phi tập trung hơn gấp trăm lần, nhưng có nhiều phép đo về sự phi tập trung. Bạn có thể xem sự lan truyền của mạng để biết bạn có bao nhiêu Node đầy đủ. Bạn có thể xem các thực thể phát triển duy nhất chịu trách nhiệm về nó... bạn có thể xem các nguồn tài trợ và xem có bao nhiêu nguồn tài trợ duy nhất ở đó. Bạn có thể thấy tổng số người dùng....

Bạn có thể thấy điều đó qua tổng số ứng dụng trên hệ thống nhưng thông thường khi chúng tôi nói phân cấp, chúng tôi thực sự muốn nói đến số lượng Node tham gia vào quy trình đồng thuận và số lượng người duy nhất đang tạo Block. Trong trường hợp của bitcoin, 3 đến 5 thường tạo ra các Block giống nhau lặp đi lặp lại... và chúng tôi luôn có 300 đến 500 Stake Pool liên tục tạo ra các Block duy nhất. Có hơn 1200 người đã đăng ký (hiện tại là hơn 3.000), vì vậy tôi cảm thấy rất thoải mái với tuyên bố 100x, nhưng những người hợp lý có thể có các định nghĩa khác nhau, không có sự đồng thuận nào trong ngành về phân cấp là gì.

Kinh doanh hard fork

Trong ngữ cảnh của Blockchain, một 'phân nhánh cứng' đề cập đến một sự thay đổi đáng kể trong chuỗi, chẳng hạn như chuyển từ giao thức này sang giao thức khác. Một hard fork trong hầu hết các Blockchain biểu thị các sửa đổi khối hoặc thay đổi cách giải thích của chúng. Thông thường, khi một hard fork được thực hiện, giao thức hiện có sẽ bị tắt, các quy tắc và sửa đổi mới được đưa ra và chuỗi được khởi động lại. Một chuỗi hard-fork sẽ khác với phiên bản trước đó và lịch sử của Blockchain pre-fork sẽ không còn truy cập được nữa.

Blockchain Cardano đã hard fork từ mô hình Byron liên kết sang mô hình Shelley phi tập trung. Mặt khác, hard fork này là độc nhất vô nhị. IOG đảm bảo quá trình chuyển đổi liền mạch sang một giao thức mới trong khi vẫn duy trì lịch sử của các Block trước đó, thay vì thực hiện các sửa đổi lớn, chuỗi không thay đổi đáng kể. Thay vào đó, nó bao gồm các Block Byron trước khi thêm các Block Shelley sau một thời gian chuyển tiếp. Không có 'bật và tắt lại'. Toàn bộ lịch sử đã được giữ lại. Không có thời gian ngừng hoạt động hoặc khởi động lại với Cardano, điều này không phải lúc nào cũng xảy ra với các chuỗi khác.³²⁹

Hard Fork Combinator

Trong các tài liệu và blog của Cardano, bạn có thể đã thấy một hard fork được gọi là 'HFC' hoặc 'sự kiện HFC'. Bộ kết hợp là một thuật ngữ kỹ thuật đề cập đến sự kết hợp của hai hoặc nhiều quy trình. Trong ngữ cảnh của Cardano, một bộ kết hợp hard fork kết hợp các giao thức, cho phép hoàn thành quá trình chuyển đổi Byron-to-Shelley mà không cần khởi động lại hệ thống. Nó đảm bảo rằng các số cái của Byron và Shelley hiển thị dưới dạng một số cái duy nhất. Tất cả các Node không cần thiết phải cập nhật cùng lúc khi chuyển từ Ouroboros BFT sang Ouroboros Praos. Thay vào đó, các Node được cập nhật theo từng giai đoạn; một số đang chạy khối Byron, số khác đang chạy khối Shelley.

Bộ kết hợp hard fork nhằm mục đích cho phép tích hợp nhiều giao thức mà không yêu cầu những thay đổi lớn. Các Block Byron và Shelley hiện được kết hợp trong chuỗi Cardano. Đối với các 'sự kiện hard fork' trong tương lai, các Block Basho và Voltaire cũng sẽ được kết hợp - tất cả dưới dạng một tài sản duy nhất. Bằng cách đơn giản hóa quá trình phát triển Byron-to-Shelley trước đó, bộ kết hợp hard fork (HFC) này cũng giúp quá trình chuyển đổi từ Shelley sang Goguen diễn ra liền mạch với các nâng cấp lặp đi lặp lại dần dần được triển khai khi các bản cập nhật *Allegra*, *Mary* và *Alonzo*.

Lịch sử HFC cho đến nay

³²⁸

AMA bắt ngày 10/01/2021, youtube.be/iLq6mRk2dyg?t=3926

³²⁹

Solana Sputters hoạt động trở lại sau thời gian ngừng hoạt động, khởi động lại mạng, decrypt.co/81004/solana-back-online-following-downtime-network-restart

Nền tảng Cardano bước vào giai đoạn phát triển nhanh chóng với sự ra đời của Incentivized Testnet vào năm 2019, đánh dấu sự khởi đầu của kỷ nguyên Shelley. Hệ thống đồng thuận Ouroboros Classic trước đây đã hỗ trợ Byron và ADA, sau đó được chuyển sang Ouroboros Praos. Khi Cardano được phân cấp, đây là phiên bản của giao thức bằng chứng cổ phần (PoS) lần đầu tiên hỗ trợ Shelley. Nó kết hợp phần thưởng bằng tiền vào quy trình đặt cược cho những người nắm giữ ADA và chủ sở hữu Stake Pool.

Vào tháng 2 năm 2020, IOG đã nâng cấp Cardano bằng một đợt hard fork đã chuyển mạng chính từ Ouroboros Classic sang Ouroboros BFT, một phiên bản nâng cao của cơ chế đồng thuận ban đầu. Bản hard fork BFT này đã khởi động giai đoạn chuyển tiếp trong Ouroboros BFT, một phiên bản rút gọn của giao thức nhằm mục đích dễ dàng chuyển sang Praos trong khi vẫn tránh hành vi nguy hiểm. Người dùng dường như không nhận thấy. Nó có nghĩa là một bản cập nhật phần mềm định kỳ cho người dùng ví Daedalus. Các sản phẩm giao dịch được yêu cầu cập nhật thủ công, nhưng họ có nhiều tuần để thực hiện việc này và IOG luôn sẵn sàng hỗ trợ. Tiếp theo là

'khởi động lại Byron'³³⁰ vào tháng 3 năm 2020. Nhiều thành phần Cardano đã nhận được mã hoàn toàn mới, bao gồm một Node mới để xử lý ủy quyền và phân quyền, cũng như các tính năng Shelley trong tương lai. Cơ sở mã mới được thiết kế lại theo mô-đun, nghĩa là nhiều thành phần có thể được cập nhật mà không ảnh hưởng đến các thành phần khác.

Đổi lại, BFT đóng vai trò là bàn đạp cho hard fork Shelley, diễn ra sau khi mạng thử nghiệm Haskell hoàn tất. Đối với các sản phẩm giao dịch, chủ sở hữu ADA và người dùng ví, lần hard fork thứ hai này tương tự như lần đầu tiên, không phải là sự kiện gây gián đoạn cho người dùng. Tuy nhiên, mặc dù bề ngoài mọi thứ có vẻ ổn thỏa, nhưng có rất nhiều hoạt động đang diễn ra đằng sau hậu trường. Các nhà phát triển của IOG đã làm việc chăm chỉ để biến nó thành một trải nghiệm lành tính, liền mạch cho người dùng cuối. Kiến trúc sư trưởng IOG Duncan Coutts³³¹ giải thích vào thời điểm đó:

Các kỹ sư Blockchain của IOG tin tưởng vào các bản cập nhật mã mượt mà. Thay vì cố gắng chuyển từ Ouroboros Classic sang Praos trong một bản cập nhật duy nhất – đây sẽ là một nhiệm vụ cực kỳ phức tạp – đó là cách tiếp cận hai giai đoạn sử dụng Ouroboros BFT làm trung gian. Mã BFT tương thích với cả Node liên kết thời Byron và Node kiểu Shelley được phát hành trong quá trình khởi động lại Byron. Nó giống như một cuộc chạy tiếp sức: một người chạy (trong trường hợp của chúng tôi là chạy một giao thức) đi vào ô bàn giao nơi người chạy kia đang đợi; họ đồng bộ hóa tốc độ của mình (để chúng hoàn toàn tương thích với nhau) và sau đó bàn giao dùi cui (vận hành mạng chính), sau đó người chạy mới với dùi cui tiếp tục từ hộp bàn giao cho vòng tiếp theo.

IOG đã có thể nhanh chóng thiết kế và thử nghiệm một chiếc ví mới bằng cách sử dụng Daedalus *Flight* và khi mọi người đang sử dụng nó trên mạng chính và IOG đã hoàn thành việc thay đổi các Node lỗi, mã cũ đã lỗi thời. *Chuyến bay* là phiên bản IOG của Chrome Canary dành cho Daedalus.

Tóm lại, hard fork thực sự duy nhất dành cho Cardano là chuyển đổi từ Ouroboros Classic sang BFT (tháng 2 năm 2020). Mạng chính Byron đã được khởi chạy lại để chạy giao thức BFT, cho phép chuyển đổi mượt mà hơn sang Ouroboros Praos với ít gián đoạn chuỗi hơn. Giao thức BFT được xây dựng một cách tỉ mỉ để lưu giữ lịch sử Blockchain và làm cho Blockchain trông giống như một thực thể duy nhất.

Như giám đốc điều hành của IOG, Charles Hoskinson đã thảo luận trong video bảng trắng của mình về hard fork,³³² mục tiêu là để có một 'lối vào Shelley một cách duyên dáng'. Bộ kết hợp hard fork rất quan trọng trong việc hoàn thành quá trình chuyển đổi này.

Cập nhật thời đại Goguen

Allegra (Khóa Token)

Khóa Token là một tính năng được giới thiệu cho giao thức Shelley để cho phép nhiều trường hợp sử dụng hợp đồng thông minh, chẳng hạn như tạo và giao dịch bằng Token đa tài sản và thêm hỗ trợ cho cơ chế bỏ phiếu Voltaire. Khóa Token là hành động dự trữ một số lượng tài sản nhất định và đồng ý không bán chúng trong một khoảng thời gian nhất định. Chức năng này đã được kích hoạt trong bản nâng cấp *Allegra*³³³ vào tháng 12 năm 2020. *Allegra* được đặt theo tên của Allegra Byron, con gái của Lord Byron và là em

³³⁰

Tim Harrison, 'Khởi động lại Byron có ý nghĩa gì đối với Cardano', iohk.io/en/blog/posts/2020/03/30/what-the-byron-reboot-means-for-cardano/

³³¹

Duncan Coutts, iohk.io/en/team/duncan-coetts

³³²

Chúng tôi sẽ ra mắt Shelley như thế nào, youtube.com/watch?v=g7uySEgt06c

³³³

gái của ADA Lovelace.

Khóa Token cho phép giải quyết thỏa thuận phức tạp hơn và hạch toán quỹ. Nó được sử dụng trong các tình huống sau:

- **Thỏa thuận hợp đồng** - khi ai đó tham gia vào một thỏa thuận hợp đồng, chẳng hạn như bán một tài sản như bức tranh, điều cần thiết là phải đảm bảo rằng bức tranh sẽ không được bán cho bất kỳ ai khác ngoại trừ người trả tiền. Token có thể đại diện cho cả bức tranh và 'lời hứa', Token thực sự khóa trong ví dụ này. Hợp đồng trở nên vô hiệu nếu bức tranh được bán cho một bên thứ ba khác
- **Đăng ký bỏ phiếu** - Khóa Token cho phép người dùng khóa một số lượng Token nhất định để phản ánh quyền biểu quyết của họ bên trong hệ thống bỏ phiếu Voltaire. Những người nắm giữ Token ADA tham gia vào quá trình bỏ phiếu phải 'khóa' Token của họ. Điều này sẽ phản ánh quyền biểu quyết của họ tương ứng với khoản đầu tư của họ và sẽ ngăn chặn nguy cơ đếm phiếu hai lần, trao nhiều phiếu bầu hơn mức khả thi, phiếu bầu mâu thuẫn hoặc phiếu bầu trùng lặp
- **Token đa tài sản** - Ngoài ADA, Cardano cho phép Token đa tài sản, với số cái hỗ trợ việc tạo và sử dụng một số loại Token riêng. Khóa Token cho phép Token ADA được 'khóa' để tạo ra một tài sản riêng biệt có giá trị tương đương.

Mary (hỗ trợ nhiều tài sản)

Điều này sau đó đã mở đường cho việc nâng cấp *Mary* (hỗ trợ nhiều tài sản) vào tháng 3 năm 2021. Bản nâng cấp này được đặt theo tên của Mary Shelley (tác giả và vợ của Shelley). MAS (hỗ trợ đa tài sản) có nghĩa là bạn có thể ghi lại rằng một Token cụ thể đang được sử dụng cho một mục đích cụ thể. Token có thể đại diện cho bất kỳ đối tượng nào được ghi trên (gốc của) sổ cái Blockchain, chẳng hạn như ADA và các Token tùy chỉnh khác. *Mary* cho phép người dùng tạo Token (tùy chỉnh) với các đặc điểm độc đáo và thực hiện giao dịch với chúng trực tiếp trên Blockchain.

Kiến trúc kế toán của sổ cái hiện không chỉ xử lý các giao dịch ADA mà còn cả các giao dịch chứa nhiều loại tài sản cùng một lúc. Các nhà phát triển được hưởng lợi từ hỗ trợ riêng vì họ không phải viết hợp đồng thông minh để xử lý các giao dịch hoặc quá trình đúc Token riêng. Thay vào đó, sổ cái kế toán theo dõi quyền sở hữu và chuyển nhượng tài sản, giảm thiểu sự phức tạp không cần thiết và rủi ro do lỗi của con người đồng thời đảm bảo tiết kiệm đáng kể chi phí.

Để hoàn thành các mục tiêu thương mại hoặc kinh doanh, nhà phát triển, doanh nghiệp và ứng dụng có thể tạo Token cho mục đích chung (có thể thay thế) hoặc chuyên dụng (không thể thay thế). Token thanh toán tùy chỉnh hoặc phần thưởng cho các ứng dụng phi tập trung, stablecoin được chốt bằng các loại tiền tệ khác và tài sản duy nhất đại diện cho tài sản trí tuệ chỉ là một vài ví dụ. Tất cả những tài sản này sau đó có thể được mua bán, trao đổi hoặc sử dụng để mua hàng hóa và dịch vụ.

Alonzo (hợp đồng thông minh)

Vẫn là một phần của kỷ nguyên Goguen, *Alonzo* là bản cập nhật giao thức tiếp theo vào tháng 9 năm 2021. Để kích hoạt các hợp đồng thông minh chức năng, *Alonzo* đã xây dựng dựa trên siêu dữ liệu giao dịch, khóa Token và chức năng nội dung gốc. Bằng cách cho phép phát triển hợp đồng thông minh và ứng dụng phi tập trung (DApp) cho DeFi (tài chính phi tập trung), bản cập nhật này đã tạo ra một nền tảng đa dạng mở ra các tùy chọn cho doanh nghiệp và nhà phát triển.

Chức năng này khả dụng và được kích hoạt bởi các công cụ và cơ sở hạ tầng tạo nên Nền tảng Plutus. *Alonzo* đã nâng cao ngôn ngữ kịch bản đa chữ ký (multisig) cơ bản của Shelley bằng một phương pháp chặt chẽ dựa trên các phương pháp chính thức và xác minh. Để có khả năng tạo tập lệnh phức tạp và an toàn hơn, Multisig đã được cập nhật thành ngôn ngữ Plutus Core³³⁴. *Alonzo* cho phép điều này thông qua kế toán đầu ra giao dịch chưa chi tiêu (eUTXO) mở rộng. Thêm về điều này sau.

Alonzo được đặt tên theo Nhà thờ Alonzo (1903-95). Church là một nhà logic học và toán học, người đã làm việc về logic và nền tảng của khoa học máy tính lý thuyết ở Hoa Kỳ. Ông cũng được công nhận vì đã thiết lập phép tính lambda,³³⁵ một hệ thống chính thức có

Giải thích về các thay đổi hard fork của Cardano Allegra và Mary, [youtube.com/watch?v=9mJvXjxTks8](https://www.youtube.com/watch?v=9mJvXjxTks8)

³³⁴

Plutus Core là ngôn ngữ lập trình trong đó các tập lệnh trên Blockchain Cardano được viết. Plutus Core là một ngôn ngữ lập trình chức năng nhỏ — có sẵn thông số kỹ thuật chính thức. Plutus Core không được đọc hoặc viết bởi con người; nó là mục tiêu biên dịch cho các ngôn ngữ khác.

³³⁵

Phép tính Lambda (λ -phép tính) là một hệ thống chính thức trong logic toán học để thể hiện tính toán dựa trên trừu tượng hóa hàm và ứng dụng bằng cách sử dụng liên kết và thay thế biến. Nó là một mô hình tính toán phổ quát có thể được sử dụng để mô phỏng bất kỳ máy Turing nào. Nó được giới thiệu bởi nhà toán học Alonzo Church vào những năm 1930 như một phần trong nghiên cứu của ông về nền tảng của toán học.

thể được sử dụng để lập luận rằng Entscheidungsproblem là ³³⁶không thể giải được. Sau đó, khi làm việc với Alan Turing, họ nhận ra rằng phép tính lambda và máy Turing ³³⁷có khả năng tương đương nhau, hiển thị nhiều quy trình tính toán cơ học. Plutus Core (ngôn ngữ hợp đồng thông minh của Cardano) là một biến thể của phép tính lambda, đây là một trong những lý do để đặt tên cho bản nâng cấp hợp đồng thông minh theo tên Church.

Vasil

Được đặt theo tên của nhà toán học người Bulgary Vasil Dabov , người cũng là thành viên cộng đồng Cardano, hard fork *Vasil* vào tháng 9 năm 2022 đã mang đến 5 tính năng chính để tăng hiệu suất. Những điều này chủ yếu tập trung vào Plutus V2 sau khi cộng đồng gửi CIP (Đề xuất cải tiến Cardano). CIP-31 (Đầu vào tham chiếu), CIP-32 (Dữ liệu nội tuyến), CIP-33 (Tập lệnh tham chiếu), CIP-40 (Đầu ra tài sản thể chấp) và đường ống khuếch tán sẽ được thảo luận sau.

Thuật ngữ và việc sử dụng các thuật ngữ giống nhau trong các ngữ cảnh khác nhau có thể khá khó hiểu. Đừng sợ, vì có trang tài liệu ³³⁸giải thích sự khác biệt giữa 'kỷ nguyên' và 'giai đoạn', và 'hard fork' khác với 'hard fork trong thời đại' như thế nào. Bắt đầu với *Alonzo* , 'kỷ nguyên số cái' được đặt theo tên của các nhà toán học và nhà khoa học máy tính, giống như hệ thống đặt tên bảo nhưng theo thứ tự bảng chữ cái. Ngày phát hành được đặt tên để vinh danh các thành viên cộng đồng Cardano.

Date	Phase	Era	Slot Number	Epoch Number	Protocol Version	Ledger Protocol	Consensus Mechanism	Notes
2017/09	Byron	Byron	0	0	0,0	-	Ouroboros Classic	
2020/02	Byron	Byron	3801600	176	1,0	-	Ouroboros BFT	
2020/07	Shelley	Shelley	4492800	208	2,0	TPraos	Ouroboros Praos	
2020/12	Goguen	Allegra	16588800	236	3,0	TPraos	Ouroboros Praos	
2021/03	Goguen	Mary	23068800	251	4,0	TPraos	Ouroboros Praos	
2021/09	Goguen	Alonzo	39916975	290	5,0	TPraos	Ouroboros Praos	
2021/10	Goguen	Alonzo	43372972	298	6,0	TPraos	Ouroboros Praos	intra-era hardfork
2022/09	Goguen	Babbage	72316896	365	7,0	Praos	Ouroboros Praos	Vasil HF

Hình 10: Các giai đoạn, kỷ nguyên và hard fork trong kỷ nguyên Cardano

Bản cập nhật SECP vào tháng 2 năm 2023 đã được thực hiện dưới dạng 'phân nhánh cứng trong thời đại'. Điều này đã mang lại nguyên tắc mật mã mới cho Cardano. Thông tin thêm về bản cập nhật này trong chương 6.

Ngày 5 tháng 6 năm 2020. Mã nào tốt nhất trong Cardano? CH.³³⁹

Mã tổ hợp hard fork là mã thanh lịch thứ hai mà chúng tôi có; mã thanh lịch nhất thuộc về mã mạng. Chúng tôi có rất nhiều thứ diễn rõ ở đó, mã rất thanh lịch, rất học thuật đáng sợ...nhưng đẹp.

³³⁶ Trong toán học và khoa học máy tính, **Entscheidungsproblem** (phát âm tiếng Đức có nghĩa là 'bài toán quyết định') là một thách thức do David Hilbert và Wilhelm Ackermann đặt ra vào năm 1928. Bài toán yêu cầu một thuật toán lấy đầu vào là một mệnh đề đầu tiên. logic thứ tự và câu trả lời 'Có' hoặc 'Không' tùy theo việc tuyên bố đó có giá trị phổ biến hay không, tức là có giá trị trong mọi cấu trúc thỏa mãn các tiên đề. Theo định lý về tính đầy đủ của logic bậc nhất, một mệnh đề có giá trị phổ biến khi và chỉ khi nó có thể được suy ra từ các tiên đề, do đó, bài toán Entscheidungs cũng có thể được xem như yêu cầu một thuật toán để quyết định liệu một mệnh đề đã cho có thể chứng minh được từ các tiên đề hay không. sử dụng các quy tắc logic .

³³⁷ Máy **Turing** là một mô hình tính toán toán học xác định một máy trừu tượng, thao tác các ký hiệu trên một dải băng theo một bảng quy tắc. Bất chấp tính đơn giản của mô hình, với bất kỳ thuật toán máy tính nào, máy Turing có khả năng mô phỏng logic của thuật toán đó có thể được xây dựng.

³³⁸ Các giai đoạn và thời kỳ phát triển trên Cardano , docs.cardano.org/explore-cardano/eras-and-phases

³³⁹ AMA bắt ngày 05/06/2020, youtu.be/6pQzQbVgX7c?t=2449

Đường dẫn đến phân cấp đầy đủ

Cardano đã đạt được một cột mốc quan trọng vào cuối tháng 3 năm 2021 khi d , tham số xác định tỷ lệ giao dịch được xử lý bởi các Node gốc, về 0. Nhiệm vụ tạo Block hoàn toàn phi tập trung vào thời điểm này. Mạng lưới 1.800 nhóm cộng đồng (tháng 3 năm 2021) của Cardano chịu trách nhiệm hoàn toàn cho việc tạo Block.

Ngày d về 0 là một bước ngoặt đối với Cardano. Khi IOG phát hành bản cập nhật Shelley vào tháng 7 năm 2020, họ đã đặt d thành 1.0, có nghĩa là mọi khối được tạo bởi các Node liên kết của IOG. Tất nhiên, điều này trái ngược với phân cấp, nhưng đó là một chiến lược thận trọng (an toàn) trong thời gian ngắn cho đến khi mạng lưới SPO (SPO) được thiết lập và trưởng thành.

IOG giảm dần d với tốc độ 0,02 mỗi kỷ nguyên theo thời gian, tăng hai điểm phần trăm trong sản xuất Block cộng đồng cứ sau 5 ngày. Khi d giảm xuống, cộng đồng đã tạo ra nhiều khối hơn và nhiều Stake Pool hơn có thể tạo Block. Sự đa dạng và phân tán địa lý của mạng tăng lên khi d giảm.

d chạm mốc 0 vào ngày 31 tháng 3 năm 2021, vào cuối kỷ nguyên 257. Ngày hôm đó thật đáng nhớ bởi vì, mặc dù d là một con số khiêm tốn nhưng tầm quan trọng của nó là rất lớn. Số 0 đó là tín hiệu bên ngoài quan trọng nhất của sự phân cấp, một biểu tượng được tham số hóa xác nhận một nguyên tắc chính trong hệ tư tưởng của Cardano là đẩy quyền lực ra rìa.

Điều chỉnh thông số phức tạp hơn

Đặt cài đặt tham số ổn định, trong khi vẫn linh hoạt cho tương lai, là điều tối quan trọng đối với sự phát triển và phân cấp liên tục của Cardano. Mặc dù quá trình chuyển đổi tham số d diễn ra suôn sẻ và có thể dự đoán được, nhưng việc thay đổi các tham số khác đòi hỏi một cách tiếp cận nhiều sắc thái hơn. IOG đã tham khảo ý kiến của cộng đồng trước khi thiết lập các giá trị ban đầu. Khoảng 20 tham số³⁴⁰ điều chỉnh hành vi của mạng và cài đặt phải được chỉ định cho tất cả chúng trước khi mạng chính có thể được khởi chạy. Phần lớn các tham số này đều mang tính chất kỹ thuật, vì vậy mặc dù chúng phải được đặt phù hợp để đảm bảo an toàn cho hệ thống và cải thiện hiệu suất, nhưng các giá trị cụ thể của chúng ít ảnh hưởng đến trải nghiệm người dùng. Bạn có thể xem lại danh sách đầy đủ các cài đặt tham số hiện tại trên ADApools.org.³⁴¹

Tháng Sáu 4, 2019. Re: Thông số Ouroboros. CH:³⁴²

Tại sao cơ chế bảo vệ chống lại quá nhiều Stake Pool? Vì vậy, bạn phải ủy quyền cho Stake Pool... vì vậy chỉ có một lượng ADA hữu hạn và các ưu đãi tài chính về cơ bản được thiết lập theo cách mà bạn sẽ có mức trần của Stake Pool và nếu bạn có nhiều hơn thế, bạn thực sự kiếm ít tiền hơn. Vì vậy, tôi rất khuyến khích bạn đọc bài báo của chúng tôi, chúng tôi đã viết từ Oxford với Alexander Russel.³⁴³ Bài báo đề cập đến cách bạn tham số hóa mô hình đó và đó là lý do tại sao chúng tôi có thể tin rằng sẽ có một nghìn cổ phần ổn định sau một thời gian.

K = số Stake Pool

Một yếu tố quan trọng là số lượng Stake Pool mong muốn hoặc tham số k . k là tham số sơ đồ phần thưởng xác định giới hạn mềm đối với kích thước nhóm. Các ưu đãi của Cardano nhằm mục đích thúc đẩy trạng thái cân bằng với k nhóm bảo hòa hoàn toàn, có nghĩa là khi tất cả cổ phần được phân bổ đều cho k nhóm hấp dẫn nhất, phần thưởng sẽ là tối ưu cho tất cả mọi người. Ở trạng thái cân bằng, giả sử những người tham gia hợp lý và không có ảnh hưởng bên ngoài, cơ chế được xây dựng sao cho hành vi phản ứng tối ưu của các bên liên quan hội tụ thành k nhóm có quy mô bằng nhau, mỗi nhóm mang lại cùng một lượng phần thưởng trên mỗi đơn vị cổ phần cho người đại diện của họ.

k càng lớn, hệ thống càng phi tập trung. Mặt khác, nhiều k hơn dẫn đến một hệ thống kém hiệu quả hơn (chi phí cao hơn, tiêu thụ năng lượng nhiều hơn) và ít lợi nhuận hơn cho cả người ủy quyền và chủ sở hữu Stake Pool. IOG biết rằng cộng đồng sẽ có động lực để xây dựng nhóm dựa trên những gì IOG đã học được từ cả Mạng thử nghiệm được khuyến khích (ITN) và mạng thử nghiệm Haskell Shelley.

Phân cấp diễn ra nhanh nhưng chỉ phân cấp thôi là chưa đủ. Cardano yêu cầu cam kết lâu dài từ các nhà khai thác và các nhà khai thác phải được khen thưởng xứng đáng để tiếp tục duy trì hệ thống. Đề xuất ban đầu là $k = 150$ cho việc triển khai mạng chính của Shelley,

³⁴⁰Tham số Giao thức, cips.cardano.org/cips/cip9/

³⁴¹Cài đặt tham số Cardano hiện tại, [ADApools.org/protocol-parameters](https://adapools.org/protocol-parameters)

³⁴²

Đặc biệt ngày 4 tháng 7 AMA bắt ngờ, youtu.be/1qoeLinJ3rg?t=3278

³⁴³

Alexander Russel, iohk.io/en/research/library/authors/alexander-russel/

sẽ được tăng dần để tạo sự cân bằng giữa phân cấp và phần thưởng cho các nhà quản lý Stake Pool. Đây là một cải tiến nhỏ so với lựa chọn tham số trong mạng thử nghiệm khuyến khích (ITN), là $k=100$. Đây được coi là một cách tiếp cận thận trọng vào thời điểm đó, nhằm mục đích cho phép chuyển đổi liên mạch môi trường ITN sang mạng chính. Điều này đảm bảo rằng hệ thống ban đầu ổn định và hiệu quả và có thể dần dần phát triển theo thời gian để trở nên phi tập trung và an toàn hơn trong tương lai.

Cardano có mức độ phi tập trung cao hơn bất kỳ Blockchain nào khác do k Stake Pool có quy mô gần tương tự nhau. Và đây mới chỉ là khởi đầu. Không thể tăng dần dần, nhỏ trong tham số k (ví dụ, không giống như tham số d phân cấp, vốn tự cho phép giảm dần). Mỗi lần tăng k đòi hỏi phải có hành động từ phía nhóm và người ủy quyền. Đối với các nhà điều hành nhóm, điều này đòi hỏi phải tinh chỉnh cài đặt của họ, đặc biệt là tiền ký quỹ của họ; đối với người ủy quyền, nó đòi hỏi phải chọn các nhóm mới để ủy quyền cho ADA của họ, đặc biệt nếu lựa chọn hiện tại của họ trở nên quá bão hòa.

Kết quả là, phương pháp tối ưu để tăng k là thực hiện nó với số lượng lớn hơn, ít thường xuyên hơn – và nhanh nhất có thể mà động lực học và kinh tế mạng thực tế cho phép. Tùy chọn tối ưu là tùy chọn gây ra ít xáo trộn nhất cho các nhóm thành công và những người được ủy quyền của họ đồng thời tăng cơ hội cho các nhóm trung bình và nhỏ hơn tạo ra các Block và thu hút thêm tiền đặt cược. Điều quan trọng nữa là phải có mục tiêu chiến lược dài hạn với tư cách là một cộng đồng: truyền bá tính phi tập trung càng rộng càng tốt.

Thay đổi $k = 500$

Vào kỷ nguyên 234, một sự điều chỉnh thành $k=500$ đã được thực hiện vào ngày 6 tháng 12 năm 2020. Các pool quy mô vừa và nhỏ gặp khó khăn trong việc thu hút ủy quyền đã được hưởng lợi từ thay đổi thành $k=500$. Nó cũng giới hạn kích thước nhóm ở mức 64 triệu ADA, nghĩa là hơn 100 nhóm lớn nhất sẽ bị quá tải.

Người đại diện luôn luôn là cách tốt nhất để theo dõi các nhóm ưa thích của họ. Bạn nên chuyển hạng lại nếu bạn thấy nhóm đã chọn của mình trở nên quá bão hòa. Điều quan trọng cần nhớ là phần thưởng sẽ vẫn được thanh toán từ các nhóm tương đối bão hòa, nhưng chúng sẽ giảm khi độ bão hòa của nhóm tăng lên. Không ai được ủy quyền cho một nhóm quá bão hòa từng bị mất bất kỳ ADA nào. Chỉ là nếu một người vẫn ở trong một nhóm bão hòa, lợi tức đầu tư sẽ bị giảm đi.

Chính sách tiền tệ

Phí giao dịch và mở rộng tiền tệ được sử dụng để tài trợ cho phần thưởng đặt cược cho cả người ủy quyền và SPO. Mỗi kỷ nguyên, tất cả phí giao dịch từ tất cả các giao dịch từ tất cả các Block được tạo trong kỷ nguyên đó được thu thập và đặt trong một 'bình' ảo. Một tỷ lệ xác định trước của dự trữ ADA còn lại, ρ , cũng được đóng góp vào pot. Sau đó, một phần của pot, τ , được trả cho Kho bạc và phần còn lại được sử dụng làm phần thưởng kỷ nguyên.

Cách tiếp cận này đảm bảo rằng tỷ lệ phần thưởng lấy từ dự trữ là lớn ngay từ đầu, khi số lượng giao dịch vẫn còn tương đối khiêm tốn do người dùng chỉ mới bắt đầu tạo doanh nghiệp của họ trên Cardano. Những người chấp nhận sớm sẽ bị lỗi cuốn hành động nhanh chóng để gặt hái những lợi ích từ khoản thanh toán ban đầu cao. Chi phí cao hơn bù đắp cho dự trữ giảm dần theo thời gian khi khối lượng giao dịch tăng lên.

Kỹ thuật này cũng đảm bảo rằng phần thưởng được cung cấp có thể dự đoán được và phát triển theo thời gian. Sẽ không có "bước nhảy" nào như ³⁴⁴sự kiện giảm một nửa bitcoin xảy ra cứ sau 4 năm. Thay vào đó, sự sụt giảm đều đặn theo cấp số nhân được đảm bảo bởi một tỷ lệ xác định trước được khấu trừ từ dự trữ còn lại mỗi kỷ nguyên.

ρ nên nhận giá trị nào? Bao nhiêu phần trăm ngân sách nên đến Kho bạc? Đây cũng là một sự đánh đổi khác: giá trị lớn hơn của ρ biểu thị phần thưởng lớn hơn cho mọi người lúc đầu, cũng như kho bạc được lấp đầy nhanh hơn. Tuy nhiên, mức ρ cao hơn ngụ ý dự trữ cạn kiệt nhanh hơn. Trả các ưu đãi lớn và khuyến khích những người chấp nhận sớm là rất quan trọng, tuy nhiên, điều quan trọng không kém là cung cấp cho tất cả các bên liên quan một cái nhìn dài hạn.

Cardano sẽ không bao giờ hết dự trữ; thay vào đó, nó sẽ là một sự phân rã theo cấp số nhân. Tính toán 'thời gian bán hủy dự trữ', hoặc thời gian cần thiết để một nửa dự trữ được sử dụng hết, để có được ý nghĩa về tác động của một giá trị nhất định của ρ . Sau khi xem xét cẩn thận, 0,22% là đề xuất cho ρ . Khi các con số được tính toán, 'thời gian bán hủy dự trữ' sẽ vào khoảng 4 đến 5 năm. Nói cách khác, một nửa lượng dự trữ còn lại sẽ bị tiêu hao sau mỗi 4 đến 5 năm. Bởi vì điều này gần với 'thời gian bán hủy bitcoin' 4 năm, nên lượng nắm giữ Cardano sẽ giảm với tốc độ tương tự như lượng dự trữ bitcoin.

Điều đáng nói là Bitcoin đã mất gần tám năm để đạt được mức độ phổ biến và giá cả cao nhất. Do đó, thật hợp lý khi dự đoán khối lượng giao dịch Cardano và tỷ giá hối đoái sẽ tăng đáng kể trong những năm tới để bù đắp cho việc giảm mở rộng tiền tệ.

³⁴⁴Giảm một nửa Bitcoin là khi phần thưởng cho việc khai thác Bitcoin giảm một nửa. Giảm một nửa diễn ra cứ sau 4 năm. Chính sách giảm một nửa đã được viết vào thuật toán khai thác Bitcoin để chống lại lạm phát bằng cách duy trì sự khan hiếm

Tài trợ cho Kho bạc

IOG cũng đề xuất chỉnh sửa con số khởi điểm là 5% cho τ , tỷ lệ phần thưởng được tự động gửi đến Kho bạc vào cuối mỗi kỳ nguyên. Trong 5 năm tới, ít nhất 380 triệu ADA sẽ được chuyển từ kho dự trữ sang Kho bạc.

Số tiền thực tế đến Kho bạc sẽ lớn hơn nhiều. Để bắt đầu, sẽ không thực tế khi dự đoán rằng tất cả ADA sẽ được ủy quyền dựa trên các bài học từ Mạng thử nghiệm được khuyến khích, nhưng cũng dự đoán việc sử dụng ADA trong tương lai. Một số trong số đó sẽ được lưu trữ trên các sàn giao dịch, giao dịch và sử dụng trong các hợp đồng thông minh. Phần thưởng không có người nhận sẽ là kết quả của ADA không được ủy quyền. Kho bạc sẽ trực tiếp vượt những phần thưởng không có người nhận này.

IOG không lường trước được mức cam kết của hầu hết các pool là cực kỳ lớn, chỉ đủ cao để khiến việc phát động một cuộc tấn công Sybil là điều không mong muốn. Sự khác biệt giữa phần thưởng nhóm tiềm năng với mức cam kết rất cao và nhóm có mức cam kết thực tế hơn, cuối cùng cũng nằm trong kho bạc. Trong tương lai gần, tổng số ADA được chuyển đến Kho bạc cho thấy rằng sẽ có đủ tiền để thanh toán cho các tính năng và bản nâng cấp mới.

Yếu tố ảnh hưởng cam kết ($a0$)

ADA được chủ sở hữu nhóm cam kết bảo vệ chống lại các cuộc tấn công của Sybil bằng cách đảm bảo rằng cổ phần được ủy quyền không bị thu hút quá mức vào các nhóm mà chủ sở hữu cố gắng lạm dụng hệ thống bằng cách hình thành nhiều nhóm mà bản thân họ không sở hữu một lượng cổ phần đáng kể. Vào thời điểm đó, đã có một cuộc tranh luận kéo dài về tập này của Hiệu ứng Cardano.

³⁴⁵Cuộc tranh luận đã tiếp tục trong một thời gian về lý do tại sao, bằng cách nào và bởi ai, các thông số nên được điều chỉnh. Umed Saidov (người đã viết bài phân tích này ³⁴⁶vào năm 2020) và 'Big Pey' đã trình bày trường hợp của họ về sự thay đổi trong cuộc thảo luận sôi nổi này ³⁴⁷tại sự kiện *Rare Bloom*.

Yếu tố ảnh hưởng cam kết có tác động trực tiếp đến phần thưởng của nhóm: yếu tố ảnh hưởng càng cao, tác động của cam kết lớn hơn đối với phần thưởng càng lớn. Một yếu tố ảnh hưởng lớn hơn sẽ cải thiện khả năng bảo vệ Sybil và làm cho hệ thống trở nên an toàn và bảo mật hơn, nhưng nó cũng mang lại lợi thế cho các chủ sở hữu Stake Pool có khả năng chi trả cho khoản cam kết lớn hơn.

Giá trị ban đầu là 0,3 nhằm đạt được sự thỏa hiệp giữa mức độ bảo vệ của Sybil và cam kết cần thiết. Tuy nhiên, không có cam kết tối thiểu. Cam kết có thể được thực hiện ở mức thấp hoặc cao tùy theo quyết định của nhà điều hành nhóm. Lựa chọn của họ ảnh hưởng đến phần thưởng, nhưng không có quy tắc 'cứng rắn' nào yêu cầu họ cam kết một số tiền nhất định. Điều này có nghĩa là các cam kết của nhóm cuối cùng sẽ tăng cao khi chủ sở hữu nhóm sẵn sàng thực hiện và cộng đồng sẽ phải đạt được sự cân bằng giữa các mối quan tâm về an ninh, kinh tế và mong muốn công lý và cơ hội bình đẳng.

cập nhật hoàn lại cam

kết tập trung cam kết của họ vào một số nhóm giới hạn sẽ được thưởng bằng tham số $a0$. Điều này đã hoạt động tốt trong việc khuyến khích các nhóm có mức độ cam kết ADA cao kết hợp thành các nhóm riêng lớn (như IOG đã làm), tạo cơ hội tốt hơn cho các nhóm nhỏ hơn để tuyển dụng người ủy quyền. Tuy nhiên, IOG cảm thấy phương pháp hiện tại có thể được cải thiện, do đó, các ý tưởng đã được tranh luận và mô hình hóa để thực hiện cam kết thành công hơn trong việc giải quyết việc chia nhóm cho các mức cam kết thấp hơn.

Mặc dù đã có nhiều cuộc tranh luận nội bộ, nhưng IOG đã đi đến kết luận rằng bất kỳ thay đổi nào trong k chỉ nên được thực hiện sau khi sửa đổi công thức cho $a0$ để đạt được kết quả mong muốn (đặc biệt là khuyến khích chuyển cổ phần sang các nhóm đơn lẻ nhỏ hơn thay vì các nhóm chia nhỏ). Bởi vì đây là một sự thay đổi hoàn toàn về công thức chứ không chỉ là một sự thay đổi về ranh giới kỳ nguyên, nên nó phải được phát hành như một phần của hard fork. IOG đã lên kế hoạch thực hiện điều chỉnh này trong một thời gian nhưng do hệ thống sản phẩm của họ và nhóm của họ tập trung vào việc giới thiệu Goguen, bản cập nhật vẫn chưa diễn ra và hệ số ảnh hưởng cam kết $a0$ vẫn ở mức 0,3.

Khi mọi thứ ổn định (tháng 1 năm 2023)

³⁴⁵Cam kết Cardano, Phần thưởng và An ninh mạng với Kevin, Lars và Duncan | TCE 90, youtube.com/watch?v=X-zilksiPOE

³⁴⁶Cardano Mainnet: Phân tích yếu tố ảnh hưởng của cam kết, reddit.com/r/cardano/comments/gfed1l/cardano_mainnet_pledge_influence_factor_analysis

³⁴⁷Phát trực tiếp Cardano ngày nở hoa hiếm hoi, youtu.be/eBH34WkU_2w?t=16180

Các tham số khác nhau được sử dụng làm đòn bẩy để kiểm soát hành vi giao thức của Cardano. Một số tham số có thể dự đoán được và không được chú ý và phần lớn bị bỏ mặc. Những thứ khác nổi bật hơn vì chúng tác động trực tiếp đến các hoạt động trên chuỗi và cần điều chỉnh thường xuyên khi giao thức rời khỏi mạng thử nghiệm và các hard fork thay đổi điều kiện sân chơi cho những người điều hành và người ủy quyền Stake Pool.

Hai tham số khác nhau tiếp tục gây chia rẽ ý kiến trong cộng đồng SPO vì chúng liên quan đến nguyên tắc cốt lõi của Cardano, tính phi tập trung và chúng ảnh hưởng đến khả năng kiếm sống của họ. Đây là giá trị k (số Stake Pool nhận được phần thưởng) và phí nhóm tối thiểu, là số tiền cố định được trả cho một nhóm trước khi phần thưởng được chia cho người ủy quyền.

k (hiện tại là 500) tác động đến kích thước nhóm tối đa, dựa trên phương trình: $= (45 \text{ tỷ} - \text{trữ lượng}) / k = (35 \text{ tỷ} / 500) = 70m$

IOG đã tiến hành một cuộc khảo sát cộng đồng³⁴⁸ để 'đọc phòng' nhưng không có sự đồng thuận về những thay đổi cần thực hiện hoặc cách thực hiện chúng. IOG trước đây đã đề xuất tăng k lên 1000, nhưng điều này đã bị hoãn lại do cuộc khảo sát không rõ ràng, IOG đang bận rộn với hard fork Vasil và quyết định rằng cần phải lập kế hoạch và thảo luận thêm.

Phí MinPool cũng là một chủ đề gây nhiều cảm xúc. SPO là phòng máy cho Cardano hoạt động. Họ tạo ra các Block mới và đảm bảo mạng lưới phi tập trung phát triển. Họ được trả tiền cho công việc của họ theo hai cách:

- một khoản phí cố định, một số tiền nhất định được thực hiện nếu các Block được tạo ra và
- một khoản phí biến đổi, một tỷ lệ phần trăm của tổng số phần thưởng được trả cho một nhóm.

Các nhóm đặt cược có thể chọn đặt bất kỳ khoản phí biến đổi nào mà họ muốn, nhưng các quy tắc sổ cái có một khoản phí cố định *tối thiểu* được áp dụng. Điều này ban đầu là để bảo vệ chống lại các cuộc tấn công của Sybil (một kẻ thù có thể chiếm quyền điều khiển mạng bằng cách tạo ra nhiều nhóm không tính phí). Nhiều người cảm thấy sự bảo vệ này không còn cần thiết nữa, bao gồm cả IOG, những người thừa nhận rủi ro này có thể mang tính lý thuyết hơn là thực tế ở giai đoạn này vì việc ủy quyền quá phi tập trung.

Một lý do lớn để giảm hoặc loại bỏ nó là nó là một trở ngại cho các nhóm nhỏ mới cạnh tranh với các Stake Pool lớn hơn, lâu đời hơn. Đây có thể là một cú hích gấp đôi vì mức phí tối thiểu cũng có thể khuyến khích các SPO lớn hơn tạo ra các nhóm mới vì có một khoản lợi nhuận được đảm bảo từ việc làm như vậy.

Để hiểu được mức độ xúc động của những vấn đề này, bạn nên lắng nghe Không gian Twitter do Bullish Dumpling tổ chức³⁴⁹ và đọc chủ đề twitter của ADAM Dean.³⁵⁰ *Army of Spies* đã dành riêng một video³⁵¹ cho nó và IOG đã viết một bài đăng trên blog³⁵² vạch ra các hướng hành động tiềm năng. Chúng tôi thậm chí còn chưa đề cập đến CIP 50 (Liesenfelt Shelleys Voltaire Decentralization Update) xứng đáng là một cuốn sách. Tôi nghi ngờ những quyết định này đang được cố tình để lại để thử nghiệm các cơ chế quản trị trên chuỗi mới vào năm 2023. Những đòn bẩy quyền lực mới này được khám phá trong Chương 9. Charles Hoskinson gần như đã xác nhận điều này trên một AMA gần đây:³⁵³

Vấn đề không phải là IOG thay đổi các tham số, hệ thống hiện tại ổn định, thật tuyệt khi lấy tất cả các tham số và điều chỉnh chúng một cách thường xuyên, nhưng đó là toàn bộ quan điểm của CIP 1694. Các bạn nên làm điều đó. Nếu bạn muốn đăng ký và có người giám sát ngôi xuống và suy nghĩ về cách điều chỉnh hệ thống hàng tháng để nó thúc đẩy một số kết quả, tôi nghĩ đó không phải là quan điểm của Cardano, quan điểm của Cardano là cộng đồng Cardano tự điều chỉnh Cardano. Vì vậy, những gì chúng tôi đã làm là đưa hệ thống về trạng thái ổn định, với trạng thái ổn định đó, nó có thể tồn tại và phát triển, bước tiếp theo là khiến cộng đồng sử dụng trạng thái ổn định đó và tạo ra một chính phủ trên đó. Vì vậy, nếu bạn muốn thay đổi các tham số hệ thống, thì hãy tiếp tục và lấy thứ gì đó như CIP 1694. Rõ ràng, sẽ có một số tinh chỉnh trong suốt năm nay, có một số điều cuối cùng cần làm khi mọi thứ thay đổi, như mạng ngang hàng được triển khai đầy đủ và Genesis được triển khai đầy đủ, nhưng nó đánh bại toàn bộ mục đích phân cấp để có một ủy ban điều chỉnh được liên kết

³⁴⁸Cuộc gọi SPO tháng 4 - Theo dõi Giai đoạn Discord, input-output.typeform.com/report/Row2tnqQ/HSCUwpltfMyJ7yp7

³⁴⁹Ngày 25 tháng 10 năm 2022 : Thảo luận về phí MinPool của Cardano , youtube.be/Gz8J5vX1Rnk

³⁵⁰@ADAMKDean, twitter.com/ADAMKDean/status/1612118333603860480?t=mM5focPvmY-GKax-lOkAPA

³⁵¹

Cardano (ADA) & Viên đạn bạc | Tóm tắt tin đồn về Cardano #514, youtube.com/watch?v=yWRwncQd4Vs&t=28s

³⁵²Tham số đặt cược và tối ưu hóa mạng – vị trí tiếp theo cho 'k' và 'phí tối thiểu?', essentialcardano.io/article/staking-parameters-and-network-optimization-where-next-for-k-and-min-fee

³⁵³AMA bắt đầu 07/01/2023, youtube.com/watch?v=djhKk-3rYhU&t=328s

Ouroboros đặt nền móng cho kỷ nguyên Basho

Cardano được xây dựng để phục vụ hàng triệu người dùng trên mạng lưới toàn cầu. Điều này có nghĩa là, giống như bất kỳ Blockchain phi tập trung nào khác, nó phải cung cấp nguồn cung cấp ổn định và có thể dự đoán được cho các Block mới để cùng nhau phát triển chuỗi và ghi lại các giao dịch của người dùng một cách minh bạch. Điều quan trọng là hệ thống sử dụng tài nguyên một cách tiết kiệm để đảm bảo rằng các Block mới được truyền qua mạng một cách hiệu quả và an toàn.

Vì tính linh hoạt là rất quan trọng nên giao thức Cardano được xây dựng với lưu ý đến khả năng mở rộng thực sự. Kỹ thuật được tham số hóa của nó nhằm uốn cong và phản ứng với sự dao động của giá, sự bão hòa của mạng và nhu cầu gia tăng. Có một số tùy chọn giao thức có thể được sử dụng để tinh chỉnh hành vi của hệ thống mà không yêu cầu hard fork. Nhưng ngay cả khi đó, những sửa đổi lớn hơn cần điều này có thể được xử lý gọn gàng bằng cách sử dụng bộ kết hợp hard fork (HFC). Đây là những điểm khác biệt quan trọng đối với Cardano, vì chúng mang lại độ bền và độ tin cậy, cũng như các tùy chọn nâng cấp rất linh hoạt khi mạng phát triển và cơ sở người dùng tăng lên.

Lộ trình của Cardano được thiết kế tương tự trong các thời đại, thực hiện từng bước một để hướng tới mục tiêu cuối cùng. Trong một mạng liên kết, Byron nói về năng lực giao dịch cơ bản. Trong khi làm việc ở giai đoạn tiếp theo, IOG đã có thể bắt đầu thiết lập một cộng đồng và các mối quan hệ. Việc khởi động lại Byron đã đặt nền tảng cho việc tăng khả năng, trong khi Shelley giới thiệu Stake Pool, giúp phát triển cộng đồng và cho phép sản xuất Block phi tập trung 100%.

IOG đã ra mắt một loạt tính năng mới, được nhiều người mong đợi vào năm 2021. Cardano đã kích hoạt tính năng tạo Token đa tài sản và Token không thể thay thế (NFT) ³⁵⁴ trên sổ cái kể từ khi nâng cấp 'Mary'. Đã có sự bùng nổ hoạt động trong lĩnh vực này do phí rẻ và thiếu yêu cầu đối với hợp đồng thông minh.

Hỗ trợ cho các hợp đồng thông minh Plutus đã được thêm vào với bản cập nhật 'Alonzo' vào tháng 9 năm 2021, cho phép xây dựng nhiều loại ứng dụng phi tập trung (DApp). Các hợp đồng thông minh trên Cardano vẫn còn ở giai đoạn sơ khai, nhưng với nhiều dự án hoạt động trên DApps và một số dự án đã được phát hành, động lực đang được xây dựng. Các tính năng bổ sung này có tác động đến cách sổ cái xử lý các tập lệnh và giao dịch mới, cũng như đặt ra các yêu cầu mới đối với tài nguyên của hệ thống. Khi khối lượng hoạt động tăng lên, thiết kế của Cardano sẽ cho phép nó uốn cong và thích ứng khi cần thiết.

Bảng thông mạng

Tất cả các hoạt động của Cardano đều được xây dựng trên mạng. Mạng Cardano phân phối các giao dịch và khối giữa các Node trên toàn cầu để xây dựng và xác thực Blockchain. Điều này được gọi là phổ biến dữ liệu và giao thức đồng thuận cần đưa ra phán đoán bằng cách cung cấp thông tin cần thiết cho các Node. Những lựa chọn này giúp chuỗi tiến lên, vì sự đồng thuận của Node đảm bảo rằng tất cả các giao dịch được xác nhận và phê duyệt, cho phép chúng được đưa vào một khối mới một cách minh bạch.

Tốc độ mà toàn bộ hệ thống hoạt động bị ảnh hưởng bởi hiệu suất mạng. Điều này bao gồm những thứ như:

- *thông lượng* (lượng dữ liệu được truyền)
- *kịp thời* (thời gian áp dụng khối)

Hai nhu cầu này đối lập trực tiếp với nhau. Khi các Block đã tạo được sử dụng hiệu quả nhất có thể, thông lượng có thể tăng lên. Đổi lại, điều này yêu cầu bộ đệm đầy đủ để bù đắp độ trễ, giảm tác động tiêu cực của hệ thống phân tán toàn cầu. Khi hệ thống đã bão hòa, nhiều bộ đệm hơn thường có thể gợi ý mức sử dụng khối (và mạng) lớn hơn, nhưng điều này phải trả giá bằng độ trễ cao hơn (thời gian áp dụng trong chuỗi).

Ngân sách của một khối

Để hiểu các giao dịch và tập lệnh Cardano có thể được hoàn thành nhanh như thế nào, khái niệm về ngân sách khối là chìa khóa. Tổng kích thước của một khối tạo ra sự cân bằng giữa tối đa hóa việc sử dụng mạng và giảm độ trễ giao dịch. Một khối duy nhất có thể bao gồm nhiều loại giao dịch, bao gồm hợp đồng thông minh được viết bằng Plutus, Token gốc, siêu dữ liệu và giao dịch ADA đơn giản (thanh toán).

Vai trò của blockchain là chứng minh tính độc đáo và quyền sở hữu. **NFT** nổi lên vào năm 2017 với trò chơi CryptoKitties, trong đó người chơi mua và 'nhân giống' những chú mèo ảo phiên bản giới hạn. Các nhà phát triển trò chơi sử dụng NFT để cho phép người chơi giành được các công cụ trong trò chơi và đồ sưu tầm. Token của các tài sản đó cho phép chúng được chuyển dưới dạng Token giữa trò chơi và người chơi trong thị trường Blockchain NFT. NFT hiện được sử dụng để bán các đồ sưu tầm như thẻ giao dịch ảo, âm nhạc, hình ảnh và video. NFT phân đoạn cho phép nhiều người nắm giữ (và giao dịch) một phần tài sản, ví dụ như một tác phẩm nghệ thuật.

Một thuộc tính khác là ngân sách thời gian khối, là khoảng thời gian được phép để hoàn thành tất cả các giao dịch trong một khối. Điều này được phân chia giữa lượng thời gian có sẵn để thực thi tập lệnh Plutus và lượng thời gian có sẵn cho các giao dịch khác. Thuộc tính này đảm bảo rằng các giao dịch có chứa tập lệnh Plutus không tiêu tốn quỹ thời gian khả dụng và các khoản thanh toán cơ bản có thể luôn được xử lý trong cùng một khối với tập lệnh Plutus.

Toàn bộ ngân sách thời gian để tạo mỗi khối (bao gồm cả chi phí mạng) được đặt thành 1 giây, với ngân sách thực thi tập lệnh Plutus là khoảng 50 mili giây. Đây là một điều khoản hợp lý; Thử nghiệm của IOG đã chứng minh rằng nhiều tập lệnh trên môi trường thử nghiệm sẽ chạy trong 1 mili giây hoặc ít hơn.

Ngân sách thời gian khối được đặt ban đầu là 1 giây. Do những lo ngại về bảo mật, quy trình đồng thuận của Praos chỉ chọn một tỷ lệ nhỏ (1 trên 20) các Block có thể được thêm vào chuỗi. Rõ ràng, kích thước và tải trọng hiệu quả của các giao dịch khác nhau sẽ thay đổi. Ví dụ: một giao dịch đơn lẻ có thể kết thúc toàn bộ vòng bỏ phiếu của Catalyst, di chuyển hàng triệu đô la giá trị.

Như đã nêu trước đây, mỗi khối chứa một số giao dịch được gửi bởi người dùng cuối thông qua ví, giao diện dòng lệnh (CLI) và các phương tiện khác. Các giao dịch này được lưu trữ trong mempool, một không gian lưu trữ tạm thời trong bộ nhớ, cho đến khi chúng sẵn sàng được xử lý và đưa vào một khối. Khi một khối được đúc, các giao dịch đang chờ xử lý sẽ bị xóa khỏi mempool, cho phép thêm các giao dịch mới. Khả năng các Node bị quá tải trong thời gian có nhu cầu cao đã được loại bỏ bằng cách sử dụng mempool có kích thước cố định, mặc dù điều này có nghĩa là có thể cần phải có ví hoặc ứng dụng để gửi lại giao dịch. Kích thước mempool được xác định bằng mô hình xếp hàng.

Kiểm tra căng thẳng mạng

Ouroboros được xây dựng để quản lý lượng dữ liệu khổng lồ, cũng như các giao dịch và tập lệnh có quy mô và độ phức tạp khác nhau. Với các cài đặt sẵn có, mạng Cardano vẫn chỉ sử dụng trung bình khoảng 25% công suất vào tháng 10 năm 2021. Tất nhiên, tùy chọn hiệu quả nhất là Cardano hoạt động ở mức hoặc gần 100% công suất (độ bão hòa của mạng). Trong khi nhiều hệ thống mạng sẽ bị ảnh hưởng trong những trường hợp như vậy, thì Ouroboros và ngăn xếp mạng Cardano đã được thiết kế để trở nên công bằng và rất bền ngay cả khi đối mặt với tình trạng quá bão hòa.

Dữ liệu điểm chuẩn cho thấy rằng ngay cả ở mức bão hòa 200%, hiệu suất tổng thể vẫn ổn định và không xảy ra lỗi mạng. Ngay cả khi được kiểm tra căng thẳng ở mức 44x, không có vấn đề gì trong toàn bộ dung lượng mạng (mặc dù một số giao dịch có thể bị chậm một chút). Áp suất ngược³⁵⁵ được sử dụng để điều chỉnh tải toàn bộ hệ thống, đó là cách mạng hoạt động.

Mặc dù một số người dùng nhất định tham gia vào đợt giảm giá NFT lớn³⁵⁶ có thể phải chờ đợi lâu hơn cho các giao dịch của họ hoặc có thể cần gửi lại giao dịch hiếm hoi từ một đợt lớn (hoặc trải đều các đợt giảm giá trong một khoảng thời gian dài hơn), điều này không có nghĩa là mạng không ổn định. Nó thực sự biểu thị rằng mạng đang hoạt động bình thường. Nó được gọi là "suy thoái duyên dáng" và bạn có thể hiểu chi tiết hơn bằng cách đọc tài liệu thiết kế mạng.³⁵⁷ Xem 'Mức giảm NFT sắp tới của Cardano.'³⁵⁸

các loại ví

Ví của người dùng cuối thay mặt họ gửi các khoản thanh toán và các giao dịch khác tới Blockchain, cũng như theo dõi tiến trình của Blockchain. Một trong những chức năng quan trọng nhất của ví là thay mặt người dùng gửi các giao dịch, xác thực rằng chúng đã được phê duyệt vào Blockchain và thử lại chúng nếu lần thử đầu tiên không thành công. Nghĩa là, khi mạng bão hòa, ví nên xem xét tác động của áp lực ngược cũng như các hiệu ứng mạng khác (ngắt kết nối tạm thời, có thể phân nhánh chuỗi, v.v.). Ví có thể là một trong hai loại:

- Ví toàn Node (như Daedalus), vận hành một Node kết nối trực tiếp với mạng Cardano bằng tài nguyên mạng và điện toán cục bộ

³⁵⁵

Áp suất ngược : Cardano được thiết kế để tự động xử lý lưu lượng truy cập lớn. Ouroboros và chức năng ngăn xếp mạng ngay cả khi bão hòa. Nếu mạng bão hòa, Cardano có thể sử dụng phương pháp kiểm soát đầu vào để điều chỉnh và khôi phục trạng thái bình thường. Đây là thuật ngữ 'áp lực ngược' được đề cập trong các blog và tài liệu, về cơ bản nó là một chiến lược để quản lý tải mạng.

³⁵⁶

Sự sụt giảm NFT là việc phát hành dự án Token không thể thay thế. Mức giảm đề cập đến ngày, giờ chính xác và nói chung là giá đúc của NFT. Nhiều NFT drop có giới hạn mua áp dụng cho số lượng NFT mà bạn có thể đúc trong một giao dịch.

³⁵⁷

Coutts, Davies, Szamotulski, Thompson (2020) 'Giới thiệu về thiết kế Mạng lưới và Truyền bá Dữ liệu cho Cardano Shelley', hydra.iohk.io/build/7249613/download/1/network-design.pdf

³⁵⁸

Các đợt giảm giá NFT sắp tới của Cardano, nftcalendar.io/b/cardano/

- Mặt khác, các ví nhẹ như Yoroi và Flint tận dụng các tài nguyên mạng và xử lý tổng hợp để phục vụ một số lượng lớn người dùng.

Cả hai loại ví có thể cần thử lại các giao dịch trong thời gian có nhu cầu cao (ví dụ: NFT giảm). Các ví nhẹ có thể cần tạm thời mở rộng quy mô tài nguyên mạng và máy tính có sẵn để đáp ứng nhu cầu của người dùng vì chúng chia sẻ tài nguyên cho nhiều người dùng. Mặt khác, ví đầy đủ Node có thể không bị ảnh hưởng. Các giao dịch có thể bị chậm trễ một chút, nhưng mỗi ví sẽ có các tài nguyên chuyên dụng, bao gồm các kết nối mạng riêng, để thử gửi. Các nhà cung cấp DApp nên tuân theo các nguyên tắc tương tự: nếu các điểm cuối mạng cụ thể được cung cấp, tài nguyên hệ thống phải được điều chỉnh để phù hợp với nhu cầu.

Xác nhận giao dịch Chain v

"TPS của Cardano (giao dịch mỗi giây) là gì?" là một trong những câu hỏi phổ biến nhất trên Crypto Twitter. Cardano yêu cầu bao nhiêu xác nhận mạng trước khi giao dịch được thực hiện? Các giải pháp cho những mối quan tâm này đòi hỏi phải kiểm tra sâu hơn về các nguyên tắc xác nhận chuỗi và xác nhận giao dịch, cũng như mối quan hệ của chúng với giao thức.

xác nhận chuỗi

Đây là ngưỡng mà giao thức đảm bảo rằng chuỗi sẽ không thay đổi thêm nữa do tính ngẫu nhiên hoặc sự cố ngẫu nhiên. Sau khi đủ khối tương lai đã được phát hành, xác nhận chuỗi sẽ xảy ra vào một thời điểm nào đó trong tương lai. Khoảng thời gian ổn định là khoảng thời gian từ bây giờ đến khi xác nhận chuỗi cho một giao dịch nhất định xảy ra (nghĩa là số lượng vị trí cần thiết để một khối trở nên ổn định, trong đó độ ổn định được định nghĩa là một khối không thể khối phục). Công thức tính của số này là:

$3k/f$

- trong đó k là tham số hạn chế sự tăng trưởng của nhóm bằng cách hạ thấp năng suất phần thưởng vượt quá một ngưỡng cụ thể, - f là tham số xác định kích thước tối đa của nhóm

Xác nhận giao dịch

Khi một giao dịch được chấp nhận vào chuỗi, nó sẽ trở nên bất biến vào thời điểm này. Các thuật ngữ 'độ sâu khối' và 'cửa sổ thanh toán' được sử dụng ở đây. Nếu khối chứa giao dịch đủ sâu trong chuỗi, nó được coi là đã xác nhận. Độ sâu là một thuật ngữ tương đối: độ sâu của một khối cho biết có bao nhiêu khối tiếp theo đã được thêm vào chuỗi kể từ khi khối đó được giới thiệu. Bởi vì các Block có độ sâu nên các giao dịch bao gồm trong chúng cũng có độ sâu.

Giao dịch được coi là đã xác minh khi độ sâu của một khối cụ thể vượt quá một ngưỡng nhất định và tài sản trong giao dịch đó có thể được sử dụng 'an toàn' (nghĩa là giao thức có thể đảm bảo giao dịch là bất biến, vì vậy tài sản có thể được mua bán, trao đổi, v.v.).

Khoảng thời gian thanh toán là khoảng thời gian giữa khi giao dịch được xác nhận và khi tài sản của giao dịch có thể được sử dụng để hoán đổi với các tài sản khác. Một giao dịch trở nên bất biến ngay khi độ sâu của nó lớn hơn $3k/f$ vị trí (nghĩa là 129600 vị trí trên mạng chính hiện tại hoặc 36 giờ).

Cơ hội bất biến

Một yếu tố khác cần kiểm tra khi quyết định xem một giao dịch có được xác minh hay không là khả năng không thay đổi của nó. Khả năng giao dịch là bất biến tỷ lệ thuận với số lượng khối được thêm vào chuỗi kể từ khi giao dịch được chấp thuận. Số lượng khối được thêm vào càng lớn thì giao dịch càng có nhiều khả năng trở nên bất biến. Khi độ sâu của giao dịch vượt quá $3k/f$ khe, nó sẽ trở thành bất biến. Giao thức Ouroboros Praos đảm bảo điều này.

Tuy nhiên, trong hầu hết các trường hợp, các vị trí $3k/f$ vượt qua tiêu chí, do đó, một cách thực tế hơn là đánh giá khả năng giao dịch là bất biến. Trong trường hợp này, chúng tôi coi một giao dịch sẽ được xác minh nếu khả năng giao dịch đó là bất biến đủ cao.

Sebastien Guillemot đề cập đến tính hữu hạn của giao dịch, trong số những thứ khác, trong bài viết chuyên sâu đầy thông tin này về *Cardano & Algorand*: *Giải thích về lựa chọn nhà lãnh đạo*³⁵⁹

P2P (ngang hàng)

Lớp **mạng** của Cardano là cơ sở hạ tầng vật lý hợp nhất các Node và tương tác của chúng thành một hệ thống duy nhất. Mạng phổ biến thông tin giao dịch và tạo Block cho tất cả các Node đang hoạt động. Hệ thống xác thực và thêm các Block vào chuỗi theo cách

³⁵⁹ Cardano & Algorand : Giải thích về lựa chọn nhà lãnh đạo, youtu.be/3k3ls7pzlKg

này, cũng như xác minh các giao dịch. Do đó, một mạng phân tán gồm các Node phải có độ trễ giao tiếp tối thiểu và đủ mạnh để đối phó với sự cố ngừng hoạt động, hạn chế về dung lượng và tin tặc.

Nếu cần phải có sự phân cấp hoàn toàn về mặt tạo Block, thì điều quan trọng là cũng phải có sự phân cấp về kết nối mạng. Cardano sẽ làm như vậy bằng cách chuyển sang mạng ngang hàng (P2P).

Trong thời kỳ Byron, P2P chạy dưới dạng một hệ thống liên kết, với các Node được kết nối bởi một cấu hình tĩnh được xác định trong tệp cấu trúc liên kết. Kể từ Shelley, hệ thống đã chuyển sang chế độ kết hợp. Trong quá trình chuyển đổi này, IOG đã bổ sung thêm mạng ngang hàng (P2P) gồm các Node Relay của SPO (SPO) được xây dựng thủ công. Các Node lõi SPO hiện có thể kết nối với cả các Node Relay liên kết và các Node Relay chạy SPO khác. Kết nối này không tự động nhưng vẫn cho phép trao đổi thông tin khối và giao dịch mà không cần dựa vào các Node liên kết. Mục tiêu là tất cả các Node Relay liên kết để các SPO có thể kết nối với các role của nhau.

Làm thế nào nó hoạt động

Mạng của Cardano là một mạng tiên tiến, tự tổ chức. Nó bao gồm các Node tạo Block, các Node Relay kết nối mạng và các Node hỗ trợ như ví Node đầy đủ Daedalus, Node trao đổi, v.v. Mạng liên kết tất cả các Node này lại với nhau. Các SPO chạy các Node tạo Block tự cô lập khỏi mạng bằng cách sử dụng các role, giao tiếp trực tiếp với phần còn lại của mạng. Role đảm nhiệm việc kết nối mạng tổng thể.

Tìm hiểu sâu hơn về những điểm phức tạp xung quanh các kỹ thuật và giao thức nhỏ có liên quan nằm trong tài liệu.³⁶⁰ Một số công cụ cải tiến được IOG sử dụng bao gồm IOSim,³⁶¹ gói Haskell mã nguồn mở cho phép IOG kiểm tra căng thẳng mạng với lưu lượng mạng lớn để giúp họ chạy mô phỏng các sự kiện quy mô lớn hiếm gặp.

Mạng cũng đa hình theo tham số,³⁶² nghĩa là có một mức độ tách biệt giữa lớp mạng với phần còn lại của mã Node Cardano. Điều này cho phép số cái và các lớp đồng thuận được phát triển độc lập với mã Node, vì vậy các cập nhật quan trọng đối với mạng và Node không cần phải xảy ra cùng một lúc.

Tất cả các kết nối đều ghép kênh³⁶³, nghĩa là kết hợp một loạt các giao thức nhỏ vào một kênh kết nối Giao thức Điều khiển Truyền dẫn (TCP) duy nhất. Điều này có ba lợi ích: giao tiếp ngang hàng hai chiều (bất kỳ máy ngang hàng nào cũng có thể bắt đầu giao tiếp mà không bị ràng buộc vì cả hai bên đều có quyền đọc và ghi trong cùng một kênh) và cải thiện giao tiếp giữa các Node mà không ảnh hưởng đến hiệu suất. Nó cũng giúp khắc phục sự cố dễ dàng hơn khi bạn có ít kết nối hơn.

Bộ điều khiển P2P³⁶⁴ theo dõi các kết nối và đồng nghiệp nào đang hoạt động và hoạt động tốt. Nó tối ưu hóa tốc độ mạng và độ tin cậy hàng giờ. Đồng nghiệp được chia thành ba loại:

- **đồng nghiệp lạnh lùng** : đồng nghiệp được biết đến, nhưng không có kết nối được thiết lập
- **các đồng nghiệp ấm áp** : nơi kết nối được thiết lập nhưng nó chỉ được sử dụng cho các phép đo mạng chứ không phải cho bất kỳ giao thức đồng thuận cấp ứng dụng nào
- **các đồng nghiệp nóng** : các đồng nghiệp nơi kết nối đang tích cực sử dụng để cho các giao thức đồng thuận cấp ứng dụng.

Kevin Hammond, Giám đốc Công nghệ của IOG, đã đưa ra một phép loại suy thông minh trong buổi nói chuyện về ScotFest của mình:³⁶⁵

Theo kết nối nóng, ý tôi là tôi và những người trong phòng này là kết nối nóng. Mọi quan hệ thân thiết là những người đang xem tôi trên YouTube, bạn không hoạt động trong phòng này vào thời điểm này nhưng bạn có thể sẽ ở đó rất nhanh nếu bạn

³⁶⁰

Tài liệu về mạng P2P, docs.cardano.org/explore-cardano/cardano-network/p2p-networking

³⁶¹

io-sim, github.com/input-output-hk/io-sim

³⁶² Đa hình là việc cung cấp một giao diện duy nhất cho các thực thể thuộc các loại khác nhau.

³⁶³

Ghép kênh, docs.cardano.org/explore-cardano/cardano-network/networking-protocol/#multiplexing

³⁶⁴

Ouroboros.Network.PeerSelection.Governor, đầu vào-đầu ra-hk.github.io/ouroboros-network/ouroboros-network/Ouroboros-Network-PeerSelection-Governor.html

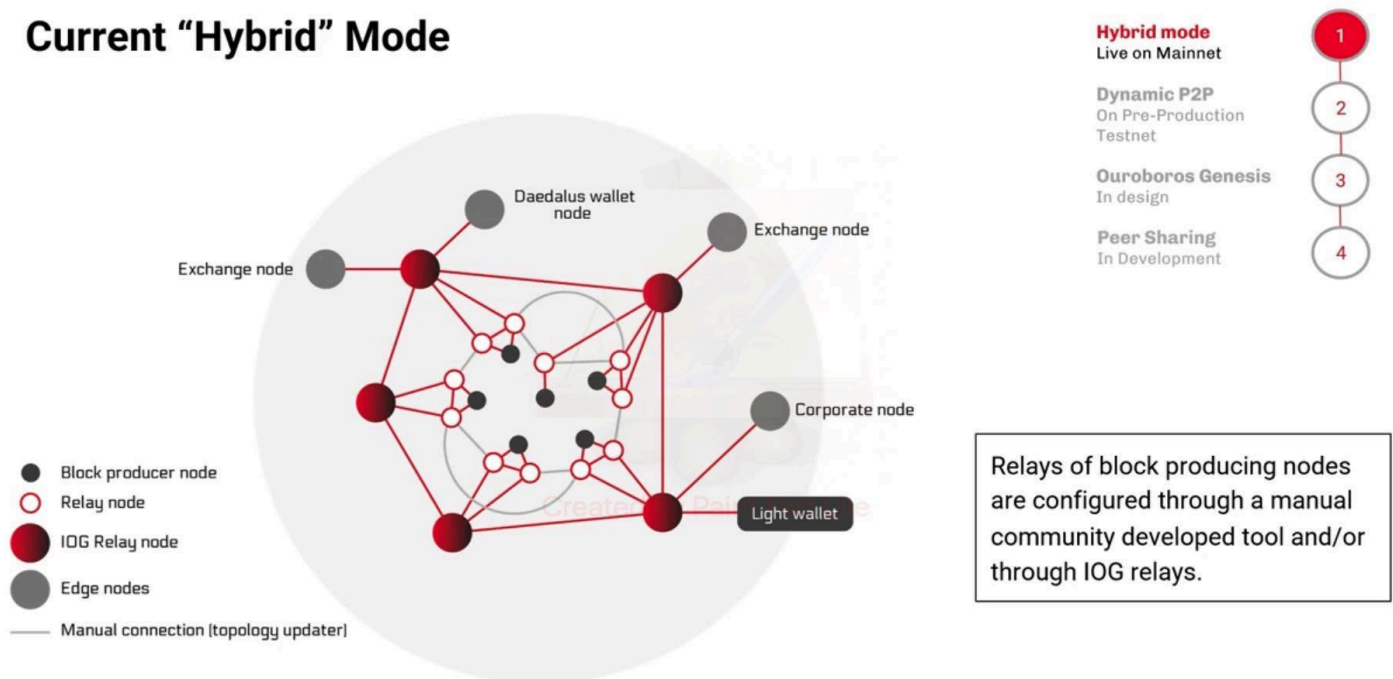
³⁶⁵ Kevin Hammond, Nói chuyện trên mạng P2P @ 2 giờ 30 phút, twitter.com/InputOutputHK/status/1593884394715897858?s=20&t=0mPqLNPBdJ7vFHxTGFw6ew

đến Edinburgh... Những mối quan hệ lạnh lùng, những người chưa được kết nối, nhưng chúng tôi' Tôi biết những người không xem trực tiếp video trên YouTube nhưng sẽ xem sau. Các kết nối lạnh có thể trở thành (được tăng cường) thành các kết nối nóng khi họ xem video YouTube và sau đó có thể (được tăng cường) thành các kết nối nóng vào một thời điểm nào đó trong tương lai...đây là khái niệm cơ bản mà chúng tôi đang sử dụng với hệ thống thống đốc p2p

lộ trình P2P

Để có được mạng P2P tự tổ chức, hoàn toàn tự động, phi tập trung, mạng cần trải qua bốn giai đoạn sau. Chiến lược này không được vạch ra sau lưng bìa mà dựa trên nghiên cứu kỹ thuật chuyên sâu ³⁶⁶ nằm ngoài phạm vi của cuốn sách dành cho người mới bắt đầu này.

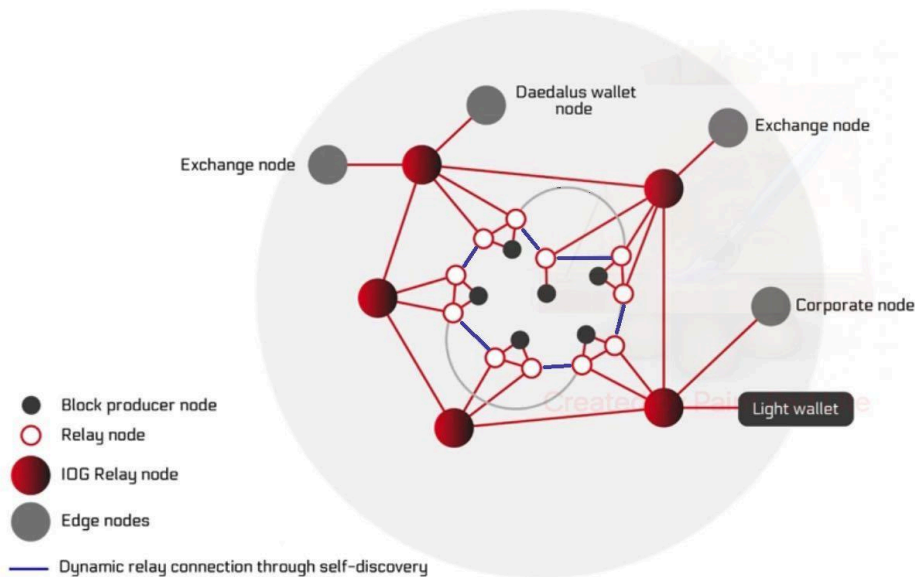
Current "Hybrid" Mode



Hình 11: Chế độ 'Hybrid', từ Kevin Hammond ScotFest talk

Chế độ kết hợp là trạng thái hiện tại của mạng tại thời điểm viết. Trong thiết lập này, các Node màu đen là các Node tạo Block, kết nối thông qua các vòng tròn màu đỏ (role). Cộng đồng đã tạo ra một cấu trúc liên kết thủ công cho phép các role tạo Block kết nối với nhau. Xương sống, vòng ngoài, là tập hợp các role hiện đang được vận hành bởi IOG, mà các sản phẩm giao dịch, ví Daedalus và ví nhẹ kết nối với.

In Development: Dynamic Peer-to-Peer (P2P)



Hybrid Mode
Live on Mainnet

Dynamic P2P
On Pre-Production
Testnet

Ouroboros Genesis
In design

Peer Sharing
In Development



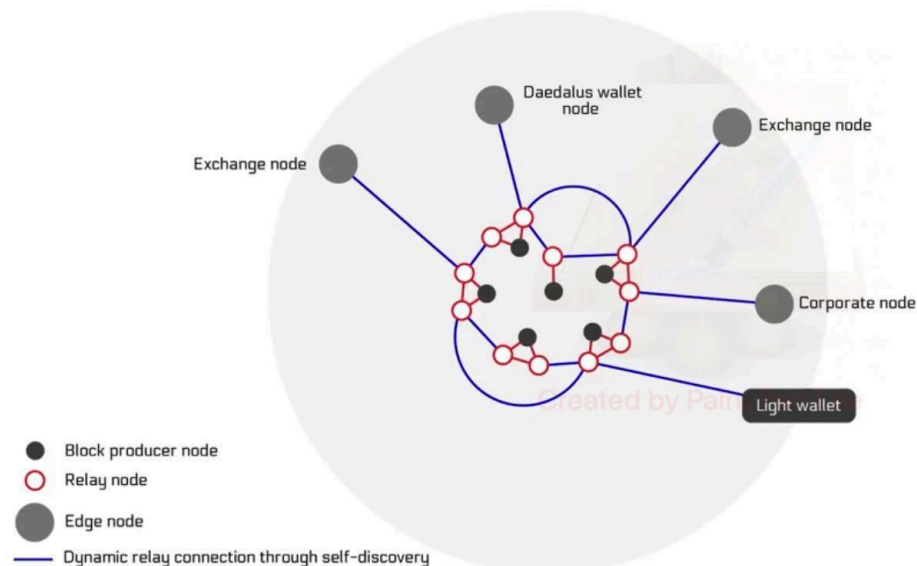
Relays of block-producing nodes will communicate dynamically through self-discovery and optimization

Hình 12: Giai đoạn p2p động, từ Kevin Hammond ScotFest talk

Giai đoạn 2 đang được triển khai dần dần trong giai đoạn 2022-23. Giai đoạn này giới thiệu một lớp tự khám phá động giữa các SPO. Thay vì có một cấu hình thủ công, sẽ có một lớp cấu hình lại tự động cấu hình lại. Các SPO sẽ không phải đi và tải xuống danh sách chuyển tiếp mới nhất, bản thân các Node Relay sẽ tự động định cấu hình lại mạng để giữ cho mạng được tối ưu hóa và bảo mật.

Như mọi khi, tốt nhất bạn nên kiểm tra các bản cập nhật dành cho nhà phát triển hàng tuần của IOG ³⁶⁷ để biết thông tin mới nhất. Đối với những người kỹ thuật hơn, có các bản cập nhật thường xuyên từ các nhóm kỹ thuật trong kho lưu trữ. ³⁶⁸

In Development: Ouroboros Genesis



Hybrid mode
Live on Mainnet

Dynamic P2P
On Pre-Production
Testnet

Ouroboros Genesis
In design

Peer Sharing
In Development



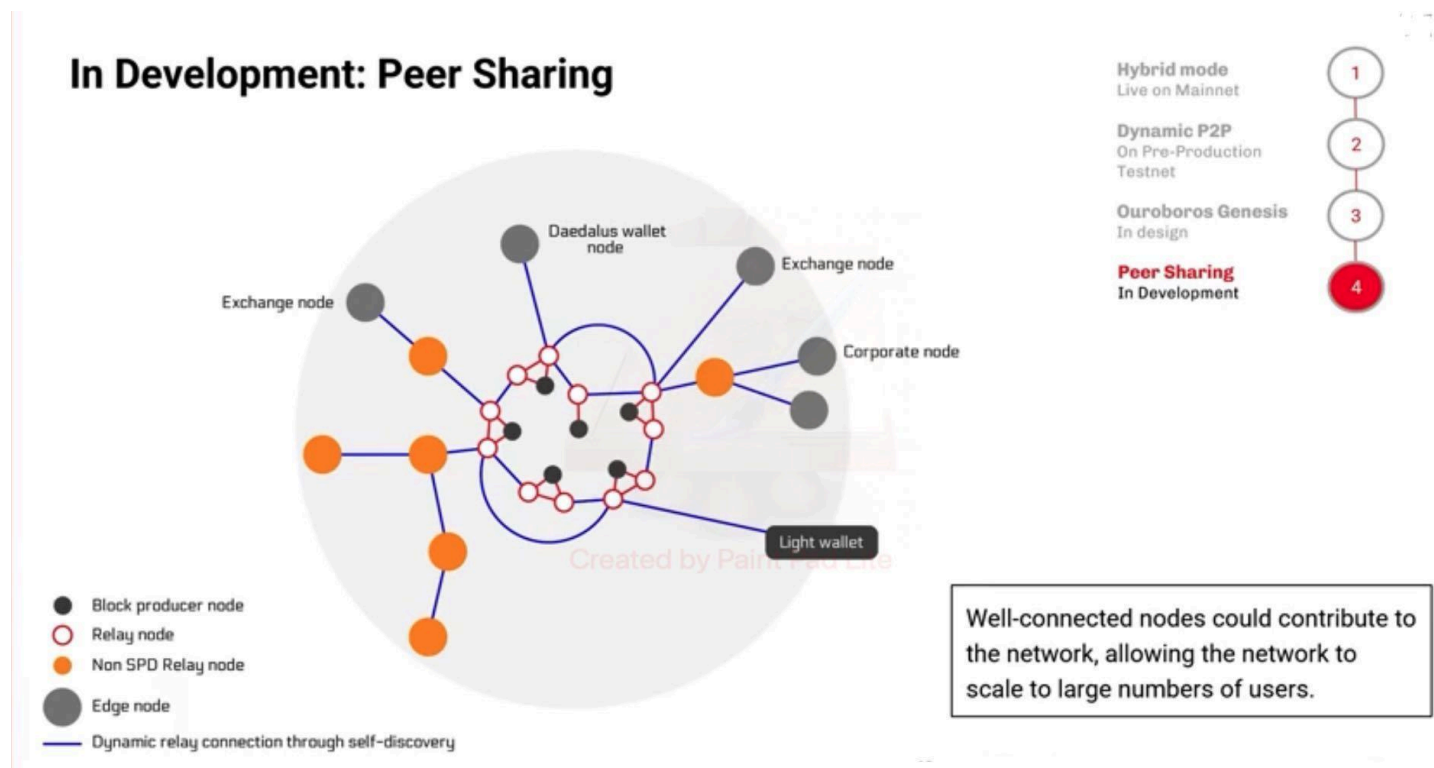
Enables secure node bootstrapping and the removal of trusted IOG relays.

³⁶⁷Cập nhật nhà phát triển Cardano hàng tuần, essentialcardano.io/development-update

³⁶⁸Các bản cập nhật của IOG Engineering, engineering.iog.io/archive/

Hình 13: Giai đoạn 'Sáng thể ký', từ Kevin Hammond ScotFest talk

Giai đoạn thứ ba là Ouroboros Genesis, đang trong quá trình thiết kế và phát triển. Genesis sẽ cho phép khởi động Node an toàn bằng cách loại bỏ nhu cầu về role IOG. Lớp bên ngoài sẽ biến mất, để lại một mạng hoàn toàn được hỗ trợ ngang hàng.



Hình 14: Giai đoạn 'Chia sẻ ngang hàng', từ Kevin Hammond ScotFest talk

Giai đoạn cuối cùng 4 là 'chia sẻ ngang hàng' khi các Node màu cam ở trên sẽ được giới thiệu. Đây sẽ là các Node được kết nối tốt, được điều hành bởi cộng đồng, cộng đồng này sẽ duy trì và thiết lập mạng. Vì vậy, sau đó bạn sẽ không còn phải truy cập các nguồn đáng tin cậy để tải xuống bộ chuyển tiếp ngang hàng đã biết mới nhất, các Node riêng lẻ sẽ tự động định cấu hình lại và mạng sẽ tự tổ chức.

Đọc thêm

Bạn có thể đọc chi tiết hơn nhiều về các chủ đề như Quản lý *kết nối* ³⁶⁹ và ghép kênh trong *Giới thiệu về mạng Cardano* ³⁷⁰ và tổng quan về thiết kế giao thức mạng ³⁷¹ trong Tài liệu Cardano hoặc Truy cập *Mạng Ouroboros* trong repo GitHub.

Entropy Cardano (Tính ngẫu nhiên)

Không thể dự đoán hoặc ảnh hưởng đến các trạng thái Blockchain trong tương lai nếu hệ thống thực sự phi tập trung. Tất cả các sự kiện trên chuỗi trong tương lai phải hoàn toàn ngẫu nhiên. Cardano thực hiện điều này bằng cách bao gồm một cơ chế entropy bổ sung có thể được áp dụng để đảm bảo tính ngẫu nhiên của hệ thống. Bất kỳ hệ thống mật mã phức tạp nào cũng dựa trên tính ngẫu nhiên thực sự. Một nguồn ngẫu nhiên thuần túy, bất ngờ phải tồn tại để một môi trường mật mã, như Blockchain Cardano, hoạt động và

³⁶⁹

Trong mạng viễn thông và máy tính, **ghép kênh** (còn gọi là ghép kênh) là phương pháp kết hợp nhiều tín hiệu tương tự hoặc kỹ thuật số thành một tín hiệu trên một phương tiện dùng chung. Mục đích là để chia sẻ một tài nguyên đắt tiền. Ví dụ, trong viễn thông, một số cuộc gọi điện thoại có thể được thực hiện bằng một dây. Ghép kênh bắt nguồn từ những năm 1870 và hiện được áp dụng rộng rãi trong truyền thông.

³⁷⁰

Giới thiệu về mạng, docs.cardano.org/explore-cardano/cardano-network/about-the-cardano-network#gatsby-focus-wrapper

³⁷¹

Tổng quan về giao thức mạng, docs.cardano.org/explore-cardano/cardano-network/networking-protocol#gatsby-focus-wrapper

được cộng đồng chấp nhận là thực sự phi tập trung và công bằng. Điều này đảm bảo rằng con đường tương lai của chuỗi không thể bị thay đổi bởi bất kỳ ai có kiến thức về quá khứ.

Tham số entropy chỉ định nguồn ngẫu nhiên của Cardano. Bên ngoài hệ sinh thái Cardano, điều này biểu thị một điều gì đó bất ngờ, đảm bảo rằng không ai có thể 'chiếm đoạt' tính ngẫu nhiên của Blockchain. Giá trị của tham số này được tính toán dựa trên các sự kiện không thể dự đoán trước hoặc về những điều mà bất kỳ ai cũng có thể đã biết.

Cơ chế bổ sung entropy

Để đánh giá cao cơ chế bổ sung entropy, trước tiên người ta phải hiểu việc tạo Block hoàn toàn phi tập trung và cách nonce chuyển đổi³⁷² sẽ tác động đến quá trình này.

Giao thức Ouroboros sử dụng một chuỗi các nonce lãnh đạo đang phát triển để quyết định nhóm nào được chọn làm nhà sản xuất Block (hạt mã hóa được sử dụng để tạo chuỗi giá trị bằng thuật toán tạo số ngẫu nhiên có thể lặp lại). Những nonce này xác định lịch trình sản xuất Block. Thời gian biểu này được xác định bởi mỗi nonce của nhà lãnh đạo trong toàn bộ kỳ nguyên 5 ngày, trong đó nonce kiểm soát Stake Pool được sử dụng để hướng dẫn sự phát triển của mỗi khối. Để đạt được các tính năng số cái cơ bản cần thiết, các quyền lãnh đạo và phân phối cổ phần phát triển theo từng bước.

Giá trị nonce

IOG đã thêm nonce chuyển đổi vào nonce lãnh đạo đang chạy ngay sau ngày 3 tháng 3, ngày 1 tháng 3 năm 2022. Khi việc phân phối cổ phần cho kỳ nguyên ngày 10 tháng 4 được quyết định, nonce chuyển đổi sau đó phải phụ thuộc vào các giá trị ngẫu nhiên (được giới thiệu bởi on-chain). giao dịch) không thể lường trước được. Điều này nhấn mạnh các giao dịch xuất hiện trên Blockchain giữa mốc 12 giờ — khi việc phân phối cổ phần được giải quyết — và mốc 42 giờ, khi giá trị băm bị xóa.

Nonce chuyển đổi là sự phản ánh của entropy được tạo ra bởi vô số các yếu tố bên ngoài, không thể kiểm soát được. Tất cả các giao dịch được đăng lên Blockchain trước Thứ Tư, ngày 7 tháng 4 lúc 15:44:51 UTC đóng một vai trò quan trọng trong lịch sử của Cardano: giá trị băm tích lũy của giao dịch (được phản ánh trong 'hàm băm khối trước' từ khối đầu tiên được tạo vào ngày -chain vào hoặc sau thời điểm này) sẽ xác định thời điểm chuyển tiếp không bắt đầu và do đó đóng góp trực tiếp vào chu kỳ tạo ngẫu nhiên vĩnh viễn

của Ouroboros. Người dùng cung cấp nonce cho một giao dịch khi sử dụng giao diện dòng lệnh Cardano (cardano -CLI), tuy nhiên, nonce được truy xuất khi xem chi tiết giao dịch lại khác. Bạn có thể xem thêm chi tiết và các tùy chọn dòng lệnh có liên quan trong tài liệu Cardano tại đây.³⁷³

Ngày 2 tháng 2 năm 2021... Làm thế nào bạn có thể giải thích tính ngẫu nhiên có thể kiểm chứng cho một người bình thường? CH:

Điều đó thật dễ dàng, vì vậy hãy tưởng tượng bạn đánh bạc với máy chủ, bạn biết đấy, chẳng hạn như bạn đang chơi Blackjack. Vì vậy, khi bạn chơi Blackjack trong cuộc sống con người, bạn có người chia bài và người chia bài chơi với bạn và anh ta chia bài cho bạn, bạn muốn tin rằng bộ bài được xáo trộn ngẫu nhiên nhưng không nhất thiết phải như vậy. Điều gì sẽ xảy ra nếu người chia bài đã sắp xếp sẵn các quân bài để anh ta luôn nhận được quân bài tốt và bạn nhận được quân bài xấu? Vì vậy, một đại lý làm gì để cung cấp cho bạn một số niềm tin trong quá trình này? Anh ấy xáo bài trước mặt bạn. Nếu bạn tin rằng xáo bài là một quá trình ngẫu nhiên thì bạn sẽ hài lòng rằng mình đang chơi một trò chơi công bằng, nhưng vấn đề là điều gì sẽ xảy ra nếu bạn không thể nhìn thấy họ xáo bài?

Đây là vấn đề khi bạn đánh bạc với các máy chủ trung tâm, vì vậy bạn đang chơi blackjack với blackjackstarz.com hoặc bất kỳ trang web nào. Chà, làm thế nào để bạn biết rằng đó là một bộ bài công bằng? Chà, họ có một bộ tạo số ngẫu nhiên, nhưng làm sao bạn biết nó không thiên vị để họ thắng nhiều hơn bạn? Chà, bạn tin rằng có thể một cơ quan quản lý đã can thiệp và làm điều đó. Điều gì sẽ xảy ra nếu bạn có một giao thức mật mã, bạn có thể xác minh hoạt động của người đó và bạn tin tưởng giao thức đó tạo ra tính ngẫu nhiên thực sự, thì giao thức đó sẽ đảm bảo rằng họ đang xáo trộn chính xác.

³⁷²

Số **nonce** là một số tùy ý có thể được sử dụng chỉ một lần trong giao tiếp mật mã. Về tinh thần, nó tương tự như một từ nonce, do đó có tên. Nó thường là một số ngẫu nhiên hoặc giả ngẫu nhiên được đưa ra trong một giao thức xác thực để đảm bảo rằng các thông tin liên lạc cũ không thể được sử dụng lại trong các cuộc tấn công lặp lại.

³⁷³

thích về giá trị nonce, docs.cardano.org/explore-cardano/explain-nonce

Điều đó phải được thực hiện đối với một hệ thống bằng chứng cổ phần. Tại sao? Bởi vì chúng tôi đang thay thế bằng chứng công việc truyền thống, nơi mà máy tính của bạn xử lý các phép tính, bằng một số số tổng hợp tỷ lệ thuận với số tiền bạn đặt cược vào hệ thống. Vì vậy, nếu bạn có 25% tổng số cổ phần trong hệ thống, bạn sẽ giành được trung bình 25% thời gian. Nhưng nếu tính ngẫu nhiên bị sai lệch thì sao? Sau đó, điều có thể xảy ra là mặc dù bạn có 25% (số tiền đặt cược), nhưng có thể bạn chỉ thắng được 8% thời gian, bởi vì tôi đã thiên vị các con số theo cách để giảm cơ hội chiến thắng của bạn. Vì vậy, bạn phải tin rằng tính ngẫu nhiên trong hệ thống là an toàn, đó là sự thật.

Phí trên Cardano

Cardano có chương trình phí giao dịch bao gồm chi phí xử lý giao dịch và lưu trữ dài hạn.

Phí không được trả trực tiếp cho người tạo Block trong hệ sinh thái Cardano, điều này làm cho nó trở nên độc nhất. Thay vào đó, chúng được gộp lại và trao cho tất cả các nhóm đã tạo ra các Block trong một kỷ nguyên. Không có chi phí bộ nhớ để theo dõi trạng thái chuỗi tích lũy, cụ thể là UTXO.

Ngừng các cuộc tấn công kinh tế

Hard fork Shelley đã thay đổi Blockchain Cardano từ liên kết thành phi tập trung hoàn toàn, do đó làm tăng động cơ cho những kẻ xấu thực hiện các cuộc tấn công kinh tế.

Khi chi phí do người vận hành hệ thống trả không được bù đắp bằng phí áp dụng cho người dùng hệ thống, một cuộc tấn công kinh tế có thể xảy ra. Những điều kiện này cho phép người dùng tính phí đối với các nhà khai thác mà không phải chịu toàn bộ chi phí, có thể dẫn đến sự suy giảm đáng kể về sự tham gia của nhà điều hành và cuối cùng là sự sụp đổ của hệ thống.

Để tránh tình huống như thế này, điều quan trọng là phải xử lý cả chi phí vận hành chưa tính hiện tại cũng như các chi phí bổ sung.

Cấu trúc phí của Cardano rất đơn giản.

Cấu trúc phí dựa trên hai hằng số (a và b).

- a và b là các tham số giao thức và phương pháp xác định phí tối thiểu cho một giao dịch (tx) là $a * \text{size}(tx) + b$
- $\text{size}(tx)$ là kích thước của giao dịch tính bằng byte.

Thông số giao thức

Hệ thống cập nhật của Cardano có thể điều chỉnh cài đặt giao thức để đáp ứng và thích ứng với những thay đổi về khối lượng giao dịch, giá phần cứng và định giá ADA. Việc thay đổi các cài đặt này được coi là một hard fork vì nó ảnh hưởng đến các giao dịch mà hệ thống chấp nhận.

Thông số một

Chi phí giao dịch phụ thuộc vào quy mô giao dịch, như được chỉ ra bởi tham số a . Các giao dịch lớn hơn yêu cầu nhiều tài nguyên hơn để lưu trữ và hoàn thành giao dịch.

Tham số b

Bất kể quy mô của giao dịch, giá trị của b là phí phải trả. Mục đích của tùy chọn này là để tránh các cuộc tấn công từ chối dịch vụ phân tán (DDoS). b làm cho các cuộc tấn công như vậy trở nên cực kỳ tốn kém và loại bỏ khả năng kẻ tấn công làm ngập hệ thống với hàng triệu giao dịch nhỏ.

Từ Twitter Space, ngày 18 tháng 4 năm 2022, 'Trò chuyện vào Chủ nhật với Charles' **Re: Phần thưởng giảm, được đền bù bằng phí Giao dịch.**³⁷⁴

Chà, có một đường cong chính thức trong thông số kỹ thuật, vì vậy nếu bạn nhìn vào lạm phát, tôi nghĩ đó là một khoảng thời gian 140 năm, vì vậy nó sẽ đi xuống. Nhưng nó có giới hạn và có những công thức chính xác về cách thức hoạt động của nó.

³⁷⁴

Nó không giống như Bitcoin, có chức năng bước giảm một nửa sau mỗi bốn năm. Đây là sự suy giảm phát thải liên tục, do đó, nó là một đường cong giảm dần đều đẹp và khá trơn tru.

Bây giờ Cardano là duy nhất, không giống như Bitcoin, nơi các Sidechains sẽ thực sự thay đổi mọi thứ. Vì vậy, điều mà mọi người dường như không hiểu là khi một Sidechain xuất hiện, Sidechain sẽ thực hiện lấy mẫu đại biểu của nó từ các SPO. Và khi bạn khai thác Sidechain đó, bạn phải trả phần thưởng khối để thu hút những người điều hành Stake Pool quan tâm đến nó, nhưng sau đó khoản tiền đó được trả cho những người điều hành và người ủy quyền, giống như phần thưởng ADA.

Vì vậy, khi một hệ sinh thái Sidechain bắt đầu được xây dựng và chúng tôi có hàng chục và cuối cùng là hàng trăm Sidechains, điều đó có nghĩa là khi bạn giữ ADA, ngoài việc nhận được phần thưởng ADA, bạn còn nhận được Token từ tất cả các Sidechains được hỗ trợ. Vì vậy, cộng với phí giao dịch sẽ thực sự thay đổi phép tính. Một điều khác là ADA là một tài sản rất dễ bay hơi. Vì vậy, vâng, phần thưởng khối có giá trị gì đó, nhưng bạn biết đấy, cách đây chưa đầy 7 tháng, giá trị của nó là 3 đô la. Nó có thể là 5 đô la trong bảy tháng. Nó có thể là 0,05 đô la trong bảy tháng. Vì vậy, tỷ lệ phần trăm chắc chắn quan trọng, nhưng giá trị thực cũng vậy. Và có một số tính đàn hồi ở đó. Vì vậy, tôi nghĩ rằng việc giới thiệu các Sidechains làm tăng khối lượng giao dịch, và sau đó là sự biến động về giá của tài sản cơ bản sẽ thực sự là yếu tố thay đổi cuộc chơi đối với lợi nhuận khi nắm giữ ở khía cạnh đó và đây là điều khiến nó trở nên thú vị.

Bạn biết đấy, một điều nữa là sự đồng thuận đa tài nguyên sẽ đến vào một lúc nào đó. Đó là một trong những đề xuất của chúng tôi cho lộ trình dài hạn và ở đó, bạn sẽ có nhiều cách khác nhau để tạo tài nguyên cho sự đồng thuận và những cách đó có thể được kiểm tiền trực tiếp bằng ADA hoặc chúng có thể được kiểm tiền bằng một nội dung khác. Vì vậy, có rất nhiều ở đó. Điều đó nói rằng, ADA là một tài sản giảm phát. Bitcoin Maxis (những người theo chủ nghĩa tối đa) dường như ghét chúng tôi, nhưng chúng tôi thực sự có chính sách tiền tệ giống nhau về mặt đó.

Nguồn cung cố định 45 tỷ, chúng tôi đang dần dần kiểm được theo cách của mình và nó đang giảm lạm phát một cách đơn điệu. Vì vậy, cốt lõi của nó là tài sản giảm phát, và đó là một trong những lý do tại sao nhiều người thích ADA. Nhưng sẽ có cả một hệ sinh thái các Token, một tập hợp các Token, cùng rất nhiều tiện ích và việc cần làm. DeFi cũng thay đổi phương trình, bởi vì bạn có thể sử dụng ADA của mình và DeFi cùng một lúc, vì vậy bạn cũng có thể tăng lợi nhuận của mình để bù đắp cho sự sụt giảm lợi nhuận. Vì vậy, về cơ bản nó phụ thuộc vào hồ sơ rủi ro của bạn từ khía cạnh đó.

3 khía cạnh khác nhau của Phân quyền đầy đủ

Phân cấp là việc chuyển giao quyền lực từ một cơ quan trung ương cho các thực thể nhỏ hơn. Tuy nhiên, trong bối cảnh của Crypto và Blockchain, định nghĩa này chỉ là bề nổi. Con đường công nghệ của Cardano để hoàn thành việc phân cấp dần được mở ra, với các SPO (SPO) tạo ra các Block ở các mức độ khác nhau, khám phá mạng ngang hàng (P2P) và 'tin đồn' với các đồng nghiệp về thông tin giao dịch giữa họ. Nó đòi hỏi phải triển khai các cơ chế ra quyết định và quản trị tinh vi do cộng đồng lãnh đạo, với kết quả là các thay đổi giao thức và phần mềm hoàn toàn phi tập trung.

Đẩy sức mạnh đến các cạnh

Cán cân quyền lực đã chuyển từ người dân sang các doanh nghiệp như Facebook và Google, dẫn đến tình trạng độc quyền thông tin ảo. Cơ quan tập trung có quyền bá chủ dữ liệu đối với khách hàng của họ do vị trí thị trường không thể có được của họ.

Phi tập trung hóa là liều thuốc giải độc cho sự tập trung quyền lực và những mối nguy hiểm mà nó kéo theo. Phân cấp cho phép các cá nhân đưa ra lựa chọn và quyết định, khôi phục quyền sở hữu thông tin cá nhân cho cá nhân, đẩy quyền hạn ra ngoài lề và trao cho mọi thành viên mạng (hoặc chủ sở hữu ADA) một cổ phần. Tính phi tập trung của Cardano được xây dựng trên ba nguyên tắc: sản xuất Block, kết nối mạng và quản trị. Những điều này gắn bó chặt chẽ với nhau và phối hợp với nhau để tạo ra một kết quả gắn kết: phân cấp hoàn toàn, nằm ở giao điểm của chúng.

1. Sản xuất Block phi tập trung

Để phát triển và thịnh vượng, mọi Blockchain đều phụ thuộc vào việc tạo ra các Block mới. Các Node lõi – được duy trì bởi IOG, Emurgo và Cardano Foundation – chỉ chịu trách nhiệm xây dựng các Block và duy trì mạng trong suốt quá trình triển khai kỷ nguyên Byron. Shelley và Incentivized Testnet, ra mắt vào năm 2019, đóng vai trò là nơi thử nghiệm để sản xuất Block phi tập trung. Thử nghiệm Testnet được khuyến khích đã chứng minh rằng Cardano có thể được hỗ trợ bởi một mạng lưới các Stake Pool do cộng đồng điều hành.

Số lượng Stake Pool tiếp tục phát triển và tăng trưởng, với một số lượng đáng kể trong số đó tạo thành các Block và trao thưởng cho các đại biểu. Các sản phẩm giao dịch kiểm soát một số, trong khi các nhà điều hành cộng đồng nhóm đơn xử lý những người khác. Mọi người đều đóng góp vào giá trị của mạng lưới. Cái trước vì khả năng thu hút những người nắm giữ ADA mới vào hệ sinh thái và cái

sau vì sự đóng góp của họ cho sự phân cấp và sự tham gia của cơ sở. IOG tận tâm thúc đẩy tính phi tập trung và mặc dù họ đã điều chỉnh các tham số trong quá khứ, nhưng các triều đại sẽ dần dần được trao lại cho cộng đồng vào năm 2023 với Thời đại *Voltaire*.

2. Mạng phi tập trung

Việc giới thiệu mạng ngang hàng (P2P) là trụ cột thứ hai trong quá trình phân cấp của Cardano. Mục tiêu là kết nối các pool phân tán về mặt địa lý để tạo ra một nền tảng Blockchain an toàn và đáng tin cậy.

Tính năng này sẽ tận dụng một tập hợp các giao thức nhỏ ³⁷⁵ và phân loại các đồng nghiệp lạnh, ấm và nóng trên mạng chính để cho phép một Node đưa ra lựa chọn kết nối tốt nhất có thể. Về mặt kết nối mạng, đã có một kỷ nguyên hỗn hợp mà các SPO phải sử dụng các phương pháp thủ công để duy trì kết nối mạng. Khi SPO tiếp quản sản xuất Block ở $d = 0$, tất cả các Node cốt lõi đã ngừng hoạt động. IOG tiếp tục duy trì các role, nhưng mạng SPO đang dần đảm nhận nhiệm vụ này. Để tìm hiểu thêm về điều này, hãy xem tập Cardano360 vào tháng 3 năm 2021, ³⁷⁶ trong đó kiến trúc sư chính của IOG là Duncan Coutts đã vạch ra tương lai P2P.

3. Quản trị phi tập trung

Cardano đã có siêu dữ liệu giao dịch và Token gốc nhờ triển khai Goguen. Kể từ khi Shelley ra mắt, đây có lẽ là bằng chứng rõ ràng nhất về sự phát triển và thành công của Cardano.

Đồng thời, một thứ thậm chí còn mạnh mẽ hơn đã xuất hiện với Project Catalyst: một cộng đồng tích cực gồm những người xây dựng, đổi mới và doanh nhân. Cộng đồng Catalyst có các thành viên trên toàn thế giới bao gồm các doanh nhân, chuyên gia và chuyên gia từ nhiều lĩnh vực khác nhau tạo nên nhóm tài năng phi tập trung này, nơi cung cấp một nguồn sáng tạo rộng lớn để đảm bảo những ý tưởng tuyệt vời nhất và sáng giá nhất nhận được nguồn tài chính xứng đáng.

Mục tiêu cuối cùng của Cardano là tạo ra một Blockchain nơi cộng đồng các bên liên quan đưa ra các lựa chọn thực tế liên quan đến giao thức và sự phát triển của chuỗi, được hỗ trợ bởi một lớp quản trị mạnh mẽ. Catalyst là tiền thân của Voltaire, kỷ nguyên phát triển sẽ mở ra mức độ phân cấp thứ ba và cuối cùng bằng cách tích hợp quản trị và ra quyết định/bỏ phiếu trên chuỗi. Chương 9 nói về *Thời đại của Voltaire* và các cơ chế quản trị sẽ được triển khai như thế nào.

³⁷⁵

Marcin Szamotulski, 'Con đường phi tập trung hóa của Cardano',
iohk.io/en/blog/posts/2020/07/09/cardanos-path-to-centralization-by-marcin-szamotulski/

³⁷⁶

Giải nén phi tập trung với Colin Edwards, Duncan Coutts, Lars Brunjes & Shawn McMurdo, youtu.be/mXYIQDUitYI

INITIAL TOKEN ALLOCATIONS FOR PUBLIC BLOCKCHAINS

Let's be honest here, concentrated insider ownership may permanently impair blockchains' ability to become credibly neutral public infrastructure.

Public

Includes all pre-launch sale or "lock drop" allocations that were open to public participation.

Community Allocations

Ecosystem funds or airdrops that will eventually go to the community

Insiders

Includes all team, company and VC purchased tokens

Foundations & More

Tokens allocated to foundations, community-governed grant pools, or other incentives like testnet participation rewards.

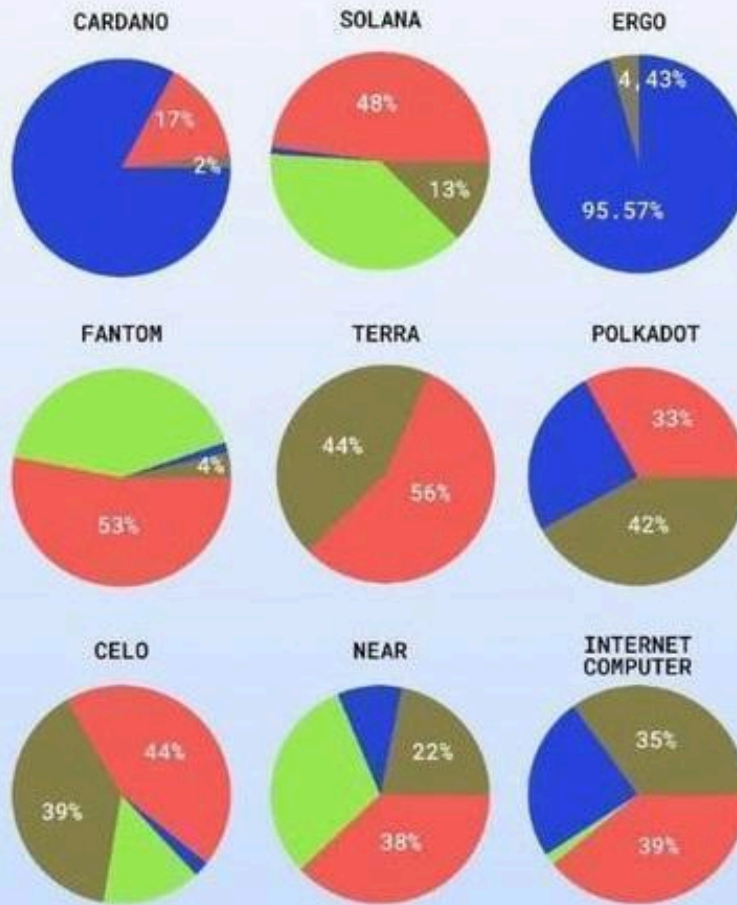


WITHOUT A FAIR LAUNCH, ULTIMATELY, CONTROL & MANIPULATION WILL FOLLOW

Data as of: Aug. 30, 2021

Source: Messari, CoinList, Various Blogs

MESSARI



Hình 15: Biểu đồ phân bổ token ban đầu của Messari

Ngày 8 tháng 9 năm 2021. Re: Chât xúc tác. CH.³⁷⁷

không gian Crypto, nói chung, vẫn chưa nhận thức được điều này, họ vẫn nghĩ rằng tất cả chỉ là tập trung và từ trên xuống, và có một số người nổi xung quanh thực hiện tất cả các cuộc gọi này. Họ không thực sự hiểu rằng chúng tôi đã âm thầm xây dựng một trong những tổ chức phi tập trung lớn nhất thế giới và những cỗ máy ra quyết định phi tập trung, và nó vẫn đang ở giai đoạn sơ khai.

Chúng tôi đã xây dựng bộ não meta này, vận hành cỗ máy meta này trên bầu trời, và tất cả những người này dù ở miền nam nước Pháp, hay một hòn đảo, hay ngay tại Colorado này với một con tôm hùm trên mic... bằng cách nào đó, chúng tôi đến với nhau, với các giá trị khác nhau, ngôn ngữ khác nhau, nhận thức khác nhau về thực tế và chúng tôi hội tụ đến một điểm mà chúng tôi thực sự có thể bỏ phiếu, tiến về phía trước, tạo ra sự thay đổi và nhận tài trợ từ mọi người... cộng đồng sẽ ngày càng nhiều hơn tham gia vào việc quyết định phương hướng và quản trị của Cardano nói chung.

Điều thú vị về điều này là nó hoàn toàn từ dưới lên. Không có nhiều thứ từ trên xuống ở đây, thứ từ trên xuống chỉ là đảm bảo rằng có các phương pháp hay nhất và cơ sở hạ tầng tốt...và đặt câu hỏi về những công cụ nào chúng ta cần xây dựng và

cách chúng ta cải thiện mọi thứ? ...nhưng các giải pháp đang dần đi lên và nó đang phát triển nhanh chóng và ngày càng có nhiều người tham gia mỗi khi chúng tôi gây quỹ, nó chỉ tăng lên ở ạt [...]...chúng tôi thậm chí không có giao diện di động trong chưa, hoặc tích hợp Daedalus trong chưa.

Nửa triệu, hàng triệu người sẽ tham gia câu lạc bộ này vào năm tới, nếu không muốn nói là nhiều hơn. Vì vậy, đây là cơ hội tuyệt vời để chúng tôi giải thích điều này sẽ diễn ra ở đâu và tại sao đây là trái tim của Cardano và điều gì sẽ khiến Cardano thăng tiến không chỉ ở đây mà còn là giao thức thống trị của tất cả các giao thức.

Chỉ số phi tập trung của Edinburgh

'Phi tập trung' đã trở thành một từ thông dụng vô nghĩa đối với nhiều dự án Crypto. Làm thế nào để một người đánh giá tuyên bố với quá nhiều thông tin sai lệch, có ý thiếu hiểu biết, FUD (sợ hãi sự không chắc chắn và nghi ngờ) cũng như lòng tham và tham nhũng kiểu cũ phổ biến? Mô tả lịch sử nhất về nhiều tuyên bố là chúng mang tính chủ quan và cần được xem xét kỹ lưỡng. Blockchain và Crypto rất phức tạp và có nhiều sắc thái đối với hầu hết các nhà đầu tư bình thường, những người có ít thời gian trong cuộc sống bận rộn của họ để thực hiện bất kỳ nghiên cứu sâu nào về các dự án.

Với khoảng trống pháp lý và không có yêu cầu về tính minh bạch, không khó để làm cho một tài sản kỹ thuật số có vẻ ngoài hấp dẫn. Không có định nghĩa thống nhất về phân cấp là gì, ai có thể nói điều gì đó không phân cấp? Ai quyết định các tiêu chí về những gì tất cả chúng ta phải đo lường? Ai có tiền gửi trong một ngành công nghiệp mới và không được phép? Với nhiều Blockchain được phân loại dựa trên các tiêu chí cấp cao, chúng thường rất khác nhau khi bạn xem xét kỹ hơn.

Chỉ xem xét một số phát hiện từ một bài báo được nghiên cứu kỹ lưỡng ³⁷⁸của *Cardanians (cardanians.io)* được xuất bản vào tháng 10 năm 2022:

- Cardano có một thực thể (Binance) với hơn 10% thị phần trong mạng. Ethereum có nhiều thực thể như vậy với lớn nhất có hơn 30% cổ phần
- Vector tấn công tối thiểu (MAV) của Cardano ³⁷⁹là khoảng 24, Ethereum và Bitcoin đều có MAV là 3.
- Bất kỳ ai cũng có thể đặt cược quảng cáo của họ trên Cardano mà không cần ủy thác quảng cáo của bạn cho bên thứ ba. Bạn có thể chi tiêu hoặc rút ADA của mình bất cứ lúc nào. Đặt cược thanh khoản có nghĩa là tiền của bạn không bao giờ bị khóa. Với Ethereum, không có ủy quyền cổ phần cấp giao thức. Nếu bạn có ít hơn 32 ETH, bạn có nghĩa vụ phải tin tưởng người xác thực giao tiền và khóa ký của mình.
- Thật dễ dàng và không tốn kém để điều hành Stake Pool Cardano. Trên Ethereum, bạn được yêu cầu khóa 32 ETH để chạy trình xác thực (tương đương với Stake Pool).

Mặc dù nghiên cứu trên rất hấp dẫn và các con số tự nói lên điều đó, nhưng một nghiên cứu như vậy rất phức tạp và mang nhiều sắc thái vì các cấu hình luôn thay đổi. Định nghĩa của các thuật ngữ khác nhau khác nhau tùy thuộc vào người bạn hỏi. Rõ ràng, cần phải có một phân tích chính thức lâu dài và khách quan hơn. Một viện hàn lâm có thể là ứng cử viên tốt nhất để tổ chức một chương trình nghiên cứu như vậy. Tham gia *Chỉ số phân cấp Edinburgh (EDI)*, một dự án do Tiến sĩ Daniel Woods và Giáo sư Aggelos khởi xướng tại ScotFest ³⁸⁰Mục tiêu là đề xuất một cách tiếp cận có cấu trúc để định lượng tính phi tập trung trong các hệ thống Blockchain.

EDI sẽ là đầu mối cho ngành, là ngôi sao phía bắc cho các nhà đầu tư bán lẻ, cơ quan quản lý và chính phủ. Nghiên cứu tại Edinburgh sẽ là một sáng kiến hợp tác, liên ngành được dẫn đầu bởi một trong những đối tác học thuật lâu đời nhất của IOG, Phòng thí nghiệm Công nghệ Blockchain (BLT) của UoE.

EDI sẽ dựa trên một khuôn khổ thống nhất để đánh giá các khía cạnh khác nhau của phân quyền. Các nhà nghiên cứu sẽ bắt đầu với Bitcoin và cuối cùng bao gồm các chuỗi khác. Chỉ số đo lường các tiêu chí sau:

- Phần cứng
- Phần mềm
- Mạng
- cơ chế đồng thuận

³⁷⁸So sánh tính phi tập trung của Cardano và Ethereum, cexplorer.io/article/comparing-the-centralized-of-cardano-and-ethereum

³⁷⁹Vector tấn công tối thiểu (MAV) là số lượng người tham gia tối thiểu cần thiết để chiếm quyền kiểm soát nhằm tấn công hoặc thao túng mạng.

³⁸⁰Lần đầu tiên thuộc loại này, giới thiệu Chỉ số phân quyền của Edinburgh, youtube.com/watch?v=8GJQDsH854Q

- Tokenomics
- API
- quản trị
- Phân phối địa lý của trình xác nhận

Để tìm hiểu sâu hơn về EDI, hãy nghiên cứu tài liệu nghiên cứu ³⁸¹phác thảo khuôn khổ.

Công việc có liên quan

Tiến sĩ Laura Reder và Sooraj Saju đã đồng viết một tác phẩm đồng hành hữu ích cho EDI. Cuốn sách của họ, *Khung đánh giá cho Blockchain lớp 1*, ³⁸²xem xét kỹ lưỡng tất cả các loại Crypto bằng chứng cổ phần hàng đầu dựa trên cách chúng giải quyết bộ ba bất khả thi của Blockchain.

Mô hình đặt cược của Ethereum, CH³⁸³

Ethereum đã dành 7 năm để cung cấp cho cộng đồng của họ một mô hình đặt cược kém hơn rất nhiều so với mô hình của chúng tôi. Nó có tính lưu ký, không có tính thanh khoản, nó thực sự chỉ là một mớ hỗn độn...và có thể một ngày nào đó bạn sẽ lấy lại được tiền của mình, nhưng hiện tại Ethereum là Khách sạn California của không gian Crypto...và 7 năm nỗ lực với gấp 10 lần tài nguyên chúng tôi có, trong khi đó chúng tôi đã tìm ra tất cả vào năm 2020 và đưa nó ra Thị trường...và bây giờ chúng tôi đang nói về cách đưa nó lên cấp số nhân, trong đó về cơ bản, hệ thống sẽ mở rộng theo tốc độ mạng mãi mãi.

³⁸¹ Karakostas, Kiayias, Ovezik (2022), 'SoK : Cách tiếp cận phân tầng để phân cấp Blockchain', arxiv.org/abs/2211.01291

³⁸²

Khung đánh giá dựa trên số liệu 3 bước cho Blockchain lớp 1, t.co/qW9RRE43v7

³⁸³

Hãy nói về Basho, youtu.be/fhVo-2QUjLM?t=1869

Chương 5: Goguen (Hợp đồng thông minh)

*'Cụm từ tai hại nhất trong ngôn ngữ này là...
nó luôn được thực hiện theo cách này'*

- Phễu ăn sủng



Erik Voorhees 
@ErikVoorhees



Noise: Bitcoin doesn't have smart contracts

Noise: Bitcoin does have smart contracts

Signal: Bitcoin has some smart contract ability, but it's far more limited than other protocols such as Ethereum.

Signal: Ethereum has greater complexity & attack surface due to this.



Charles Hoskinson 
@IOHK_Charles



Signal: Cardano's EUTXO and Plutus have the expressiveness of Ethereum with the attack surface of Bitcoin.

UTXO mở rộng

Mạng Blockchain là cấu trúc dữ liệu phức tạp. Các giao dịch đi qua chuỗi một cách thường xuyên, để lại dấu vân tay kỹ thuật số phải được theo dõi và quản lý cẩn thận để duy trì tính toàn vẹn và độ tin cậy của sổ cái cơ bản. Trong thế giới Blockchain, có hai loại sổ cái kế toán chính: Blockchain dựa trên UTXO (như Bitcoin) và chuỗi Tài khoản/Sổ dư (Ethereum và các loại khác).

Các mô hình kế toán của hai mô hình này khác nhau về nhiều mặt. Mô hình Đầu ra giao dịch chưa sử dụng (UTXO) được sử dụng bởi Bitcoin, Cardano, Zcash, Ergo, Avalanche và những người khác trong khi mô hình Tài khoản/Sổ dư được sử dụng bởi Ethereum, Polkadot, Algorand, v.v.

Cardano nhằm mục đích tạo ra một mô hình kế toán UTXO mở rộng (eUTXO) bằng cách kết hợp mô hình UTXO của Bitcoin với khả năng xử lý các hợp đồng thông minh của Ethereum. Việc áp dụng eUTXO giúp tích hợp hợp đồng thông minh vào mạng Cardano dễ dàng hơn.

Mô hình kế toán hoạt động như thế nào?

Sự tương tự của bảng cân đối kế toán thường được sử dụng để giải thích mô hình tài khoản. Bất kỳ thực thể thương mại nào cũng cần có bảng cân đối kế toán để duy trì hồ sơ chính xác về lãi, lỗ, dòng tiền và các yếu tố khác. Các công ty có thể hình dung tình hình tài chính của họ bất cứ lúc nào bằng cách lưu giữ hồ sơ tỉ mỉ về tất cả các thông tin này. Một lợi ích khác của sổ cái kế toán của công ty là khả năng theo dõi nguồn gốc và quyền sở hữu của các quỹ. Các mạng Blockchain cũng cần một mô hình kế toán để xác định ai sở hữu loại tiền nào, theo dõi nơi những đồng tiền đó di chuyển, những đồng tiền nào đã được sử dụng hết và những đồng tiền nào vẫn có thể truy cập được để chi tiêu.

Mô hình tài khoản/sổ dư so với mô hình UTXO

Kế toán được sử dụng để duy trì hồ sơ chuyển tiền trong sổ cái vật lý với các mục viết tay. Các phiên bản điện tử của cùng một thứ đang được các doanh nghiệp sử dụng. Để giám sát nguồn gốc và quyền sở hữu, các Blockchain sử dụng các giao dịch dưới dạng hồ sơ (giống như các mục trong sổ cái). Các giao dịch này bao gồm rất nhiều thông tin (tiền đến từ đâu, chúng sẽ đi đâu và số tiền lẻ còn lại).

UTXO

Đầu ra giao dịch chưa sử dụng (UTXO) là thuật ngữ chỉ lượng tiền kỹ thuật số còn lại sau một giao dịch Crypto. Luồng tài sản được ghi lại trong mô hình UTXO dưới dạng biểu đồ tuần hoàn³⁸⁵ có hướng với các Node biểu thị các giao dịch và các cạnh biểu thị các đầu ra của giao dịch, với mỗi giao dịch liên tiếp tiêu thụ một số UTXO và thêm các giao dịch mới. Ví của người dùng xác định số dư của người dùng bằng cách theo dõi danh sách các đầu ra chưa sử dụng được kết nối với tất cả các địa chỉ do người dùng nắm giữ.

Ở nhiều khía cạnh, UTXO giống hệt với tiền tệ. 'Cash in cash out' là phép loại suy thường được sử dụng. Giả sử bạn phải thanh toán hóa đơn nhà hàng €15. Bạn quên thẻ tín dụng nên trả bằng tiền mặt. Bạn thanh toán bằng tờ 20 € (đầu vào) và muốn để lại 2 € tiền boa. Người phục vụ đặt €15 vào máy tính tiền (đầu ra 1) và đưa lại cho bạn đồng xu €2 (đầu ra 2) và đồng xu €1 (đầu ra 3). Cô ấy bỏ tiền boa €2 (đầu ra 4) vào hũ đựng tiền boa. Bất kể, nếu bạn quyết định để lại tiền boa hay không, hoặc đưa ra số tiền lẻ chính xác, đầu vào và đầu ra phải khớp nhau.

Điều này cũng đúng với UTXO. Bất kỳ số dư nào bạn có trong ví Blockchain của mình đều có thể được tích lũy bằng cách sử dụng nhiều kết hợp UTXO khác nhau tùy thuộc vào các giao dịch trước đó, nhưng tổng giá trị vẫn giữ nguyên. Nói cách khác, số dư của một địa chỉ ví là tổng của tất cả các UTXO chưa được sử dụng từ các giao dịch trước đó.

Khái niệm 'thay đổi' trong mô hình UTXO

UTXO giới thiệu 'sự thay đổi', giống như các giao dịch tiền tệ tại một cửa hàng. Ví dụ, bạn không thể cắt tờ 50 € thành nhiều mảnh nhỏ hơn để thanh toán cho bất kỳ thứ gì có giá 15 € khi bạn lấy nó ra khỏi túi. Bạn phải giao toàn bộ số tiền €50 và nhân viên bán hàng sẽ đưa tiền lẻ cho bạn. Điều này cũng đúng với UTXO. Một UTXO không thể được 'chia' thành các phần nhỏ hơn. UTXO được sử dụng toàn bộ, phần còn lại được trả về địa chỉ ví của bạn dưới dạng UTXO nhỏ hơn.

Ưu điểm của UTXO

Người ta có thể lấy được thông tin đáng tin cậy về việc sử dụng Blockchain và các hoạt động tài chính bằng cách kiểm tra và theo dõi kích thước, tuổi và số lượng UTXO được di chuyển xung quanh.

Các lợi ích khác của các mô hình UTXO có thể được tìm thấy như khả năng mở rộng tốt hơn, đặc biệt là đối với các kênh trạng thái và giải pháp bảo vệ. Về quyền riêng tư, UTXO khiến kẻ xấu khó liên kết các giao dịch. Người dùng có thể liên tục thay đổi địa chỉ nhận của họ, với các địa chỉ mới không có chủ sở hữu trước đó. Ngoài ra, vì mỗi UTXO chỉ có thể được sử dụng một lần và toàn bộ, logic giao dịch được sắp xếp hợp lý, giúp việc xác minh giao dịch dễ dàng hơn đáng kể.

Để tóm tắt UTXO:

- UTXO là kết quả của một giao dịch trước đó có thể được chi tiêu trong tương lai
- Không có tài khoản nào trong chuỗi UTXO. Thay vào đó, tiền xu được lưu giữ dưới dạng danh sách các UTXO và các giao dịch được thực hiện bằng cách sử dụng các UTXO hiện có và tạo các UTXO mới ở vị trí của chúng
- Số dư là tổng số UTXO được sở hữu bởi một địa chỉ nhất định (UTXO được sử dụng toàn bộ).

Mô hình Tài khoản/Sổ dư là một phương pháp để theo dõi và cân bằng tài chính của bạn. Một tài khoản (có thể được quản lý bằng khóa riêng hoặc hợp đồng thông minh) được sử dụng để giữ số dư tiền xu trong các mô hình Blockchain sử dụng mô hình kế toán Tài

³⁸⁵

Đồ thị tuần hoàn có hướng là đồ thị có hướng không có chu trình có hướng. Nghĩa là, nó bao gồm các đỉnh và các cạnh, với mỗi cạnh hướng từ đỉnh này sang đỉnh khác, sao cho việc đi theo các hướng đó sẽ không bao giờ tạo thành một vòng khép kín.

khoản/Số dư, như tên gọi của nó. Tài sản được thể hiện dưới dạng số dư bên trong tài khoản của người dùng trong kiến trúc này và số dư được lưu dưới dạng trạng thái toàn cầu của tài khoản được duy trì bởi mỗi Node và được cập nhật với mỗi giao dịch.

Chuỗi tài khoản/Số dư (chẳng hạn như Ethereum) hoạt động tương tự như các tài khoản ngân hàng thông thường theo nhiều cách. Khi tiền được gửi, số dư của ví tăng lên và khi tiền được chuyển đi nơi khác, số dư của ví sẽ giảm. Điểm khác biệt chính là, không giống như UTXO, bạn chỉ có thể sử dụng một phần số dư của mình. Vì vậy, nếu bạn có 50 ETH trong tài khoản của mình, bạn có thể chuyển một phần của nó cho người khác (ví dụ: 15 ETH). Do đó, số dư tài khoản của bạn sẽ là 35 ETH và địa chỉ mà bạn đã gửi tiền sẽ tăng thêm 15 ETH. Trong các mô hình kế toán Tài khoản/Số dư, ý tưởng thay đổi không áp dụng như trong các mô hình kế toán UTXO.

Kích thước giao dịch thường nhỏ hơn với mô hình tài khoản, so với UTXO, vì chỉ dữ liệu cơ bản liên quan đến người gửi, người nhận, số tiền và chữ ký được thu thập. Do đó, việc tích hợp các Node mới sẽ dễ dàng hơn vì có ít dữ liệu hơn để đồng bộ hóa.

Để tóm tắt khái niệm Tài khoản/Số dư:

- Cách tiếp cận kế toán này hoạt động tương tự như cách một ngân hàng thực hiện
- Người dùng có tài khoản giữ số dư tiền xu của họ
- Một phần số dư có thể được chi tiêu
- Ý tưởng thay đổi là không liên quan
- Các mô hình tài khoản phù hợp với việc triển khai Lớp 2 vì kích thước/siêu dữ liệu giao dịch nhẹ.

Đầu ra và đầu vào của giao dịch

Từ 'giao dịch' thường gợi lên hình ảnh về tiền. Mặc dù định nghĩa này áp dụng cho Bitcoin (vì Bitcoin được sử dụng để chuyển khoản thanh toán giữa các đồng nghiệp), nhiều Blockchain khác (như Cardano) linh hoạt hơn. Từ 'giao dịch' phức tạp hơn nhiều trong những trường hợp này. Giao dịch có thể được coi là chuyển giao giá trị.

Mỗi giao dịch trong hệ thống Blockchain có thể có một hoặc nhiều đầu vào và một hoặc nhiều đầu ra. Nếu một người muốn nắm bắt cách thức hoạt động của một giao dịch và cách nó kết nối với UTXO, thì trước tiên người đó phải hiểu khái niệm về đầu vào và đầu ra. Hãy coi một giao dịch là hoạt động mở khóa các đầu ra trong quá khứ đồng thời tạo ra các đầu ra mới.

đầu ra giao dịch

Một địa chỉ (mà bạn có thể xem là khóa) và một giá trị được bao gồm trong đầu ra giao dịch.³⁸⁶Theo sự tương tự này, chữ ký của địa chỉ là chìa khóa mở khóa đầu ra. Đầu ra có thể được sử dụng làm đầu vào sau khi đã được mở khóa. Các giao dịch mới sử dụng đầu ra của các giao dịch trước đó đồng thời tạo ra các đầu ra mới có thể được sử dụng bởi các giao dịch tiếp theo. Mỗi UTXO chỉ có thể được sử dụng một lần và nó phải được tiêu thụ hoàn toàn. Chỉ một đầu vào có thể sử dụng mỗi đầu ra.

Đầu vào giao dịch

Đầu ra của một giao dịch trước đó được gọi là đầu vào giao dịch. Một con trỏ và chữ ký mật mã đóng vai trò là chìa khóa mở khóa được bao gồm trong đầu vào giao dịch. Khóa mở khóa đầu ra giao dịch trước đó và con trỏ tham chiếu trở lại giao dịch đó. Blockchain gắn nhãn một đầu ra được mở khóa là 'đã tiêu' khi nó được mở khóa bằng một đầu vào. Sau đó, các đầu vào mới có thể đề cập đến các đầu ra mới được tạo ra bởi một giao dịch nhất định và chuỗi tiếp tục. UTXO là đầu ra mới (chưa được mở khóa, tức là đã sử dụng). Đầu ra chưa sử dụng chỉ là: đầu ra chưa được sử dụng.

Cách thức hoạt động của UTXO

Các giao dịch tiêu thụ các đầu ra chưa sử dụng từ các giao dịch trước đó và tạo ra các đầu ra mới có thể được sử dụng làm đầu vào cho các giao dịch trong tương lai theo mô hình kế toán UTXO.

Các UTXO này được quản lý bởi ví của người dùng, ví này cũng bắt đầu giao dịch bằng cách sử dụng UTXO của người dùng. Tại mọi thời điểm, mỗi Node Blockchain luôn theo dõi một tập hợp con của tất cả các UTXO. Đây được gọi là bộ UTXO. Theo thuật ngữ kỹ thuật, đây là chainstate, được lưu giữ trong thư mục dữ liệu của mỗi Node. Chuỗi trạng thái được thay đổi bất cứ khi nào một khối mới được thêm vào chuỗi. Danh sách các giao dịch gần đây được bao gồm trong khối mới này (tất nhiên bao gồm cả bản ghi các UTXO đã sử dụng và các giao dịch mới được tạo kể từ khi trạng thái chuỗi được cập nhật lần cuối). Mỗi Node giữ một bản sao của chainstate.

³⁸⁶

Đầu ra của giao dịch: Đầu ra được tạo ra bởi các giao dịch. Chúng được tiêu thụ khi chúng được sử dụng bởi một giao dịch khác. Thông thường, cần có một số loại bằng chứng để có thể sử dụng UTXO, chẳng hạn như chữ ký từ khóa công khai hoặc (trong Mô hình UTXO mở rộng) đáp ứng một tập lệnh.

Tại sao Cardano chọn eUTXO

Cơ chế kế toán UTXO của Cardano không giống với Bitcoin, vì Cardano có nghĩa là làm nhiều việc hơn là chỉ quản lý các khoản thanh toán. Sự cần thiết phải tăng tính biểu cảm của chương trình trong tính năng hợp đồng thông minh của kỷ nguyên Alonzo yêu cầu một cách tiếp cận ('Mở rộng') độc đáo.

Khái niệm UTXO 'cơ bản' có khả năng lập trình hạn chế. Với việc thiết lập sổ cái dựa trên tài khoản và các tài khoản hợp đồng liên quan, mô hình kế toán Tài khoản/Số dư của Ethereum giải quyết thách thức cụ thể này. Tuy nhiên, kết quả là ngữ nghĩa của mã hợp đồng trở nên phức tạp hơn đáng kể, điều này dẫn đến hậu quả ngoài ý muốn là buộc người viết hợp đồng phải hiểu đầy đủ ngữ nghĩa để ngăn chặn việc chen các lỗ hổng có khả năng cực kỳ tốn kém vào mã.

Một giải pháp UTXO 'mở rộng' sẽ cần hai tính năng mà mô hình UTXO hiện tại thiếu:

1. Để có thể giữ hợp đồng ở trạng thái hiện tại.
2. Để có thể đảm bảo rằng cùng một mã hợp đồng được sử dụng trong suốt chuỗi giao dịch. Đây là những gì được gọi là tính liên tục.

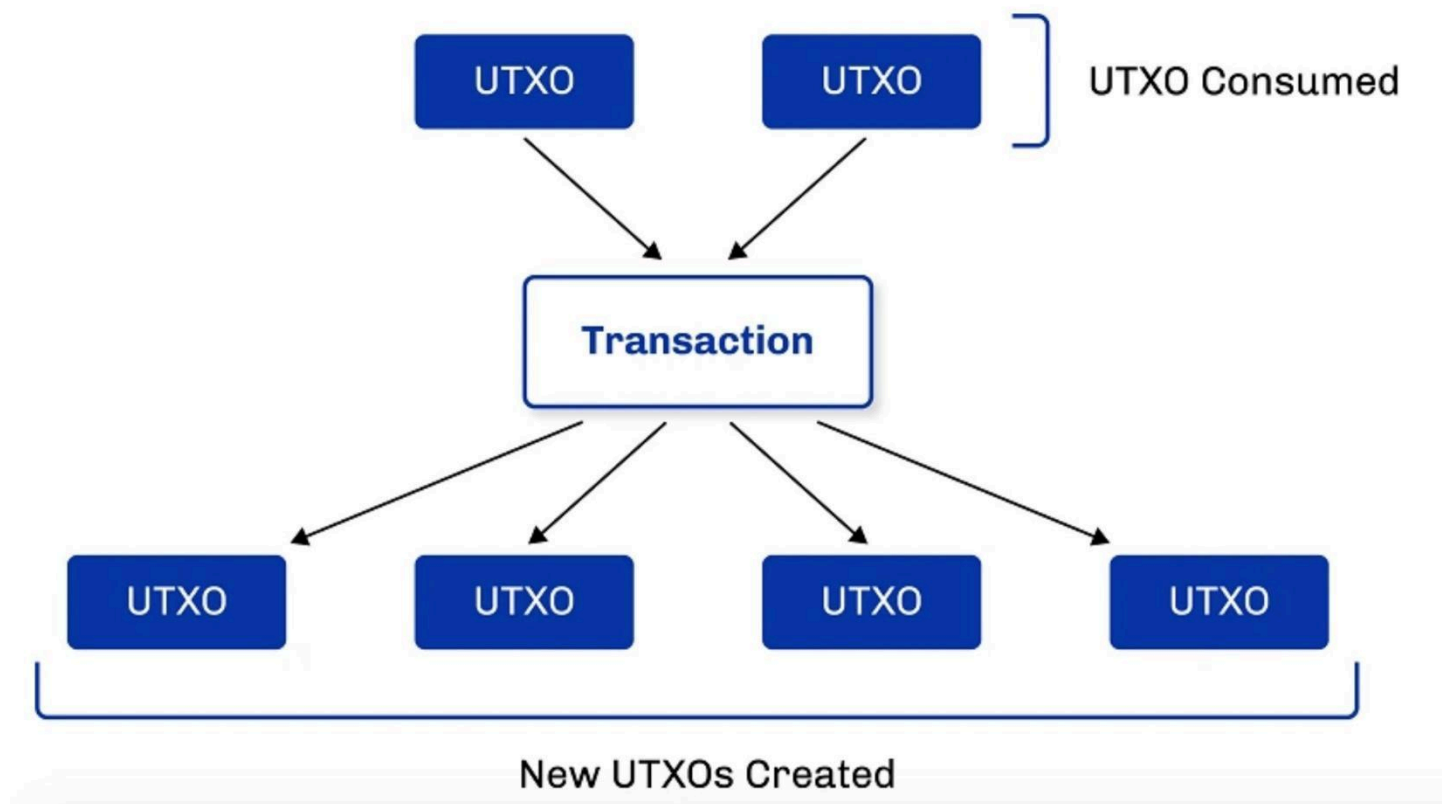
Mô hình eUTXO có lợi thế là có thể dự đoán các khoản phí cần thiết cho một giao dịch thành công trước khi nó được xử lý. Đây là một đặc điểm mà các mô hình dựa trên tài khoản không có.

Tại sao nó được gọi là eUTXO ?

UTXO được 'mở rộng' bằng cách cho phép kiểm soát 'khóa' và 'phím' bổ sung theo các điều kiện mà đầu ra có thể được mở khóa để tiêu thụ bởi một giao dịch (ngoài giá trị) và bằng cách cho phép thêm dữ liệu tùy chỉnh vào đầu ra. Nói cách khác, thay vì có các khóa công khai (bấm) cho khóa và chữ ký đi kèm đóng vai trò là 'khóa', eUTXO cho phép triển khai logic tùy ý bằng cách sử dụng tập lệnh. Logic tùy ý này kiểm tra giao dịch và dữ liệu để xác định xem giao dịch có thể sử dụng đầu vào hay không.

Điều gì tuyệt vời về eUTXO ?

Kiến trúc sổ cái của Cardano mở rộng trên mô hình UTXO để phù hợp với nhiều tài sản và hợp đồng thông minh trong khi vẫn duy trì các lợi ích của mô hình UTXO. Nghiên cứu đột phá cho phép Cardano thực hiện các chức năng mà không sổ cái UTXO nào khác có thể làm được, khiến nó trở thành ứng cử viên duy nhất trong không gian Blockchain.



Hình 16: Mô hình UTXO

Mô hình UTXO mở rộng

Mô hình UTXO được mô hình eUTXO mở rộng theo hai cách :

1. Phép loại suy ổ khóa và chia khóa được sử dụng để mở rộng ý tưởng về một 'địa chỉ'. Địa chỉ trong mô hình eUTXO có thể bao gồm logic tùy ý ở dạng tập lệnh thay vì giới hạn khóa đối với khóa chung và khóa đối với chữ ký. Ví dụ, khi một Node xác minh một giao dịch, nó sẽ đánh giá xem giao dịch đó có thể sử dụng một đầu ra nhất định làm đầu vào hay không. Nếu đầu ra có thể được sử dụng làm đầu vào, giao dịch sẽ tra cứu tập lệnh được cung cấp bởi địa chỉ của đầu ra và chạy nó.
2. Điểm khác biệt thứ hai giữa UTXO và eUTXO là ngoài địa chỉ và giá trị, đầu ra có thể chứa (hầu như) bất kỳ dữ liệu nào. Bằng cách cho phép các tập lệnh mang trạng thái, chúng trở nên mạnh mẽ hơn đáng kể.

Hơn nữa, eUTXO mở rộng khái niệm UTXO bằng cách cho phép các địa chỉ đầu ra bao gồm logic phức tạp để xác định giao dịch nào được phép mở khóa chúng, cũng như bằng cách cho phép thêm dữ liệu tùy chỉnh vào tất cả các đầu ra. Khi xác minh một địa chỉ, tập lệnh sẽ xem xét dữ liệu do đầu ra mang theo, giao dịch đang được kiểm tra và một số dữ liệu bổ sung được gọi là người mua lại mà giao dịch cung cấp cho mỗi đầu vào. Tập lệnh cung cấp đủ ngữ cảnh để đưa ra phản hồi 'có' hoặc 'không', trong những trường hợp có thể rất phức tạp, bằng cách khám phá tất cả thông tin này.

³⁸⁷

Địa chỉ của UTXO cho biết đầu ra đang 'đi' ở đâu. Địa chỉ quy định các điều kiện để mở khóa đầu ra. Đây có thể là hàm băm khóa công khai hoặc (trong mô hình UTXO mở rộng) hàm băm tập lệnh.

³⁸⁸

Đầu ra tập lệnh : UTXO bị khóa bởi tập lệnh.

³⁸⁹

Redeemer : Đối số cho tập lệnh trình xác thực được cung cấp bởi giao dịch sử dụng đầu ra tập lệnh.

³⁹⁰

Tập lệnh trình xác thực là tập lệnh được đính kèm với đầu ra tập lệnh trong mô hình UTXO mở rộng. Phải được chạy và trả lại tích cực để đầu ra được sử dụng. Nó xác định địa chỉ của đầu ra.

³⁹¹

Bối cảnh xác thực : Một cấu trúc dữ liệu chứa bản tóm tắt về giao dịch đang được xác thực và đầu vào hiện tại có trình xác thực đang được chạy.

eUTXO cho phép logic tùy ý được thể hiện dưới dạng tập lệnh. Logic tùy ý này kiểm tra giao dịch và dữ liệu để xác định xem giao dịch có thể sử dụng đầu vào hay không.

Cấu trúc biểu đồ của mô hình UTXO khác đáng kể so với mô hình dựa trên tài khoản được sử dụng bởi một số Blockchain hỗ trợ hợp đồng thông minh hiện tại. Do đó, các mô hình thiết kế cho DApps trên Blockchain dựa trên tài khoản không dễ dàng thích ứng với Cardano. Vì biểu diễn cơ bản của dữ liệu là khác nhau nên cần có các mẫu thiết kế mới.

Kiến trúc trên mỗi nhánh của mô hình UTXO (Bitcoin) được chuyển sang eUTXO, trong đó một nhánh được định nghĩa là một chuỗi các giao dịch yêu cầu xác thực liên tiếp. Xây dựng DApps và các giải pháp khác với nhiều UTXO là rất quan trọng để phân chia chức năng trên các nhánh khác nhau và thực thi tính song song bổ sung.³⁹² Điều này có lợi thế về khả năng mở rộng, giống như việc tạo ra các dịch vụ Bitcoin đòi hỏi phải chia một ví thành các ví phụ.

Ưu điểm eUTXO

So với các mô hình kế toán khác, mô hình eUTXO có một số lợi ích khác biệt. Thành công hay thất bại của giao dịch chỉ được xác định bởi giao dịch và đầu vào của nó, không phải bởi bất kỳ thứ gì khác trên Blockchain. Do đó, trước khi một giao dịch được đăng lên Blockchain, tính hợp pháp của giao dịch có thể được xác nhận ngoài chuỗi. Một giao dịch vẫn có thể thất bại nếu một giao dịch khác sử dụng đầu vào mà giao dịch đang mong đợi cùng một lúc, nhưng nếu tất cả các đầu vào vẫn khả dụng, giao dịch sẽ thành công.

Điều này trái ngược với cách tiếp cận dựa trên tài khoản (chẳng hạn như Ethereum), cho phép một giao dịch thất bại khi đang thực hiện. Trong eUTXO,³⁹³ điều này sẽ không bao giờ xảy ra. Ngoài ra, chi phí thực hiện giao dịch có thể được tính toán ngoài chuỗi trước khi truyền, đây là điều mà Ethereum không cho phép.

eUTXO của Cardano cung cấp một môi trường an toàn và linh hoạt để xử lý nhiều hoạt động mà không gây ra sự cố hệ thống. Kiến trúc này cung cấp khả năng mở rộng và quyền riêng tư vượt trội, cũng như logic giao dịch đơn giản hơn, vì mỗi UTXO chỉ có thể được sử dụng một lần và toàn bộ, giúp việc xác minh giao dịch dễ dàng hơn đáng kể.

Mô hình eUTXO có lợi thế là có thể dự đoán các khoản phí cần thiết cho một giao dịch thành công trước khi nó được đăng. Đây là một tính năng mà các mô hình dựa trên tài khoản không có. Các Blockchain dựa trên tài khoản, chẳng hạn như Ethereum, là không xác định, có nghĩa là tác động của một giao dịch trên chuỗi không thể được đảm bảo. Sự mơ hồ này làm tăng nguy cơ tổn thất tài chính, chi phí đắt đỏ ngoài dự kiến và là phương tiện tấn công rộng lớn hơn để tin tặc khai thác.

Phân tích kỹ thuật chuyên sâu về kiến trúc của sổ cái eUTXO nằm ngoài phạm vi của cuốn sách này, tuy nhiên, bạn có thể 'đi sâu vào tìm hiểu' bằng cách xem lại blog của IOG 'Kiến trúc DApps trên Sổ cái eUTXO' nơi³⁹⁴ họ cung cấp kiến trúc mẫu. SundaeSwap³⁹⁵ và Axo (trước đây là Maladex) cũng viết blog về giải pháp của họ trong khi ERGOdex³⁹⁶ nói về triết lý của họ trên kênh YouTube *Cardano với Paul*³⁹⁷. Ngoài ra còn có một số mẫu mã từ IOG về việc tránh sử dụng đồng thời nhiều chữ ký trong Lobster Challenge.³⁹⁸ IOG phân tích cấu trúc mẫu sổ đặt hàng mẫu³⁹⁹ trong blog của họ. Để tìm hiểu sâu hơn về eUTXO, hãy đọc sổ tay.⁴⁰⁰

³⁹²

Thuật ngữ **Song song** đề cập đến các kỹ thuật để làm cho các chương trình nhanh hơn bằng cách thực hiện một số tính toán cùng một lúc.

³⁹³

Fernando Sanchez, 'Mô hình kế toán UTXO mở rộng của Cardano',
iohk.io/en/blog/posts/2021/03/12/cardanos-extends-utxo-accounting-model-part-2/

³⁹⁴

Jean-Frédéric Etienne, 'Kiến trúc DApps trên sổ cái EUTXO',
iohk.io/en/blog/posts/2021/11/16/architecting-dapps-on-the-eutxo-ledger/

³⁹⁵

Blog SundaeSwap, sundaeswap-finance.medium.com/sundaeswap-labs-presents-the-scooper-model-678d6054318d

³⁹⁶

Giải pháp đồng thời ERGO + ERGOdex cho Cardano là gì, youtube.com/watch?v=xIDINmIFrFM

³⁹⁷

Cardano với Paul, youtube.com/watch?v=xIDINmIFrFM

³⁹⁸

Thử thách tôm hùm IOHK, github.com/input-output-hk/lobster-challenge/tree/concurrency-multisig

³⁹⁹

Mẫu sách đặt hàng, plutus-apps.readthedocs.io/en/latest/plutus/explanations/order-book-pattern.html#what-is-the-order-book-pattern

⁴⁰⁰

Sổ tay EUTXO, ucarecdn.com/3da33f2f-73ac-4c9b-844b-f215dcce0628/EUTXOhandbook_for_EC.pdf

'Không thông minh cũng không hợp đồng'

Trong khi Vitalik Buterin và những người khác ⁴⁰¹ đã cho rằng hợp đồng thông minh không phải là thông minh cũng không phải là hợp đồng, chúng ta đừng khoa trương vì mục đích ngắn gọn. Hợp đồng thông minh là một thỏa thuận kỹ thuật số tự động dựa trên mã ghi lại, xác thực và thực hiện các giao dịch ràng buộc của hợp đồng giữa nhiều người tham gia. Khi các tiêu chí đặt trước được thỏa mãn, mã hợp đồng thông minh sẽ tự động thực hiện các giao dịch của hợp đồng. Hợp đồng thông minh chỉ là một chương trình ngắn gọn có đầu vào và đầu ra là các giao dịch Blockchain.



vitalik.eth
@VitalikButerin

Replying to @CleanApp @cryptoecongames and 4 others

To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts".

6:21 PM · Oct 13, 2018 · Twitter Web Client

Hợp đồng thông minh tự thực hiện và đáng tin cậy, không yêu cầu sự can thiệp hoặc hiện diện của bên thứ ba. Mã hợp đồng thông minh được lưu giữ trên mạng Blockchain phi tập trung và lan truyền khắp mạng, làm cho nó trở nên minh bạch và không thể hủy bỏ.

Hợp đồng thông minh là bất biến vì không thể sửa đổi, có thể phân phối và chống giả mạo, nhanh chóng và tiết kiệm chi phí vì không có người trung gian, tiết kiệm tiền và thời gian, đồng thời an toàn vì được mã hóa.

Tại sao hợp đồng thông minh?

Các bên trung gian tham gia vào nhiều thủ tục thương mại bao gồm trao đổi giá trị (chẳng hạn như tiền, tài sản hoặc cổ phiếu) để đảm bảo rằng các điều kiện của thỏa thuận là toàn diện, rõ ràng và được đáp ứng trước khi trao đổi có thể diễn ra. Chi phí của một giao dịch được tăng lên bởi những người trung gian này. Hợp đồng thông minh đã phát triển như một kỹ thuật giảm thời gian, sự tham gia của bên thứ ba và chi phí thực hiện thỏa thuận một cách đáng tin cậy.

Hợp đồng thông minh là các chương trình phần mềm được lưu trữ trên Blockchain ở định dạng không thay đổi. Chúng chạy trên các máy tính ảo và dữ liệu của chúng được lưu trữ trong cùng một kiến trúc bất biến. Các doanh nghiệp nhằm mục đích cải thiện hoạt động của họ có thể thu được lợi nhuận lớn từ các hợp đồng thông minh. Nhiều lĩnh vực, bao gồm ô tô, chuỗi cung ứng, bất động sản và chăm sóc sức khỏe, đang đầu tư vào nghiên cứu để xem công nghệ này có thể giúp họ cạnh tranh hiệu quả hơn như thế nào.

Siêu dữ liệu trên Cardano

Sự cần thiết của siêu dữ liệu

Hãy nhớ rằng, tiền là một công trình xã hội. Nó chỉ có giá trị nếu mọi người thừa nhận và tin vào nó. Hầu hết các giao dịch đều có bối cảnh cần được ghi lại trong siêu dữ liệu. Bitcoin và những người cùng thời với nó đã từ bỏ yêu cầu về danh tính, thông tin và danh tiếng đáng tin cậy trong các giao dịch thương mại nhằm tìm cách ẩn danh và loại bỏ những người chơi trung gian. Việc áp dụng các phương pháp tập trung để thêm dữ liệu này sẽ làm mất khả năng kiểm tra, tính khả dụng toàn cầu và tính bất biến, đó là toàn bộ ý tưởng sử dụng Blockchain.

Thông tin giao dịch có rất nhiều trong các hệ thống tài chính kế thừa, chẳng hạn như các hệ thống dựa trên SWIFT. Quy định thường liên quan đến việc quy kết các cá nhân tham gia, thông tin tuân thủ, báo cáo hành vi đáng ngờ cũng như các hồ sơ và hoạt động khác

ngoài việc biết giá trị được chuyển giữa các tài khoản. Siêu dữ liệu có thể cần thiết hơn giao dịch trong một số trường hợp nhất định. Siêu dữ liệu là câu chuyện của giao dịch.

Do đó, có vẻ hợp lý khi kết luận rằng việc giả mạo siêu dữ liệu có thể nguy hiểm như làm tiền giả hoặc thay đổi lịch sử giao dịch. Việc không cấp phép cho những người muốn tự do tham gia vào các lĩnh vực này dường như gây bất lợi cho sự chấp nhận phổ biến và bảo vệ người tiêu dùng.

Thêm siêu dữ liệu vào các giao dịch là bước đầu tiên để chuẩn bị Cardano cho DeFi. Cardano đã phát triển thành một nền tảng hợp đồng thông minh với sự ra mắt của Goguen. Điều này bắt đầu bằng cách bao gồm siêu dữ liệu — thông tin về dữ liệu đang được xử lý — trong các giao dịch, được đưa vào Blockchain. Cardano đã phát triển từ một nền tảng tập trung vào giao dịch thành một nền tảng tiện ích dành cho các đối tác, doanh nghiệp và ứng dụng thương mại có thể được sử dụng cho các quy trình phức tạp sẽ đặc trưng cho tương lai tài chính phi tập trung (DeFi).

Với số lượng giao dịch Crypto ngày càng tăng, việc có quyền truy cập vào dữ liệu cố định không thể thay đổi là rất quan trọng, đặc biệt đối với các ứng dụng như quản lý tài sản. Blockchain Cardano lưu giữ hồ sơ vĩnh viễn về các giao dịch đã hoàn thành, đảm bảo lịch sử hoạt động tài chính minh bạch và có thể kiểm tra được. Tuy nhiên, để các hoạt động tài chính có trách nhiệm và khả năng hiển thị cao hơn, bối cảnh phải được đưa ra cho các giao dịch này. Các sự kiện như thông tin người gửi và người nhận, hoàn cảnh xử lý và thời gian xử lý là những ví dụ về thông tin bổ sung. Điều này được thực hiện bằng cách bao gồm siêu dữ liệu giao dịch.

Dữ liệu về dữ liệu

Thuật ngữ 'siêu dữ liệu' đề cập đến thông tin về thông tin. Nói cách khác, nó xác định ngữ cảnh, nội dung và cấu trúc của các bản ghi. Siêu dữ liệu thúc đẩy sự tự tin thông qua chứng thực dữ liệu vĩnh viễn, vì công nghệ Blockchain cung cấp một sổ cái minh bạch để lưu giữ thông tin một cách bất biến và an toàn.

Cho dù đó là giao dịch mua sản phẩm hoặc dịch vụ hay chuyển tiền cho thành viên gia đình, tất cả giao dịch đều có mục đích xác định. Ví dụ: khi thực hiện mua hàng trực tuyến, có rất nhiều thông tin có thể được thu thập về giao dịch. Siêu dữ liệu có thể giúp truyền tải câu chuyện về việc mua sản phẩm bằng cách tiết lộ thông tin về khách hàng và người bán, ngày giao dịch, nhà sản xuất sản phẩm và hoàn cảnh cung ứng.

Ngày 31 tháng 3 năm 2019. Trên siêu dữ liệu. CH:⁴⁰²

Một ví dụ về điều này.... giả sử Bob đi đến một cây ATM và rút \$300 giá trị từ một cây ATM ...bây giờ đó là một giao dịch ...bây giờ hãy nói rằng Bob đã làm điều đó tiếp theo tại một nhà hàng Ý vào ngày sinh nhật của anh ấy và tất cả bạn bè của anh ấy tình cờ có mặt ở đó...bạn sẽ nói 'oh, có vẻ như Bob đang rút tiền để thanh toán séc' hoặc theo một cách nào đó có liên quan đến sự kiện này, anh ấy đang ở một lễ kỷ niệm, có nhiều người ở đó.... nó đắt và giả sử là lúc 12 giờ...giờ là giờ ăn trưa...Sau đó Bob có thể lấy 300 đô la từ máy ATM, vì vậy cùng một loại giao dịch nhưng bây giờ tôi đã thay đổi siêu dữ liệu....

Giả sử bây giờ là 2:00 sáng ngay bên cạnh một nhà thổ nổi tiếng vì vậy về cơ bản là cùng một loại giao dịch...cùng một loại giá trị, cùng một bên tham gia...đây là tài khoản và tiền của anh ta, nhưng bởi vì bạn đã thay đổi siêu dữ liệu nó có ý nghĩa rất khác nhau.... Vì vậy, điều gì sẽ xảy ra nếu bạn có thể hoán đổi các siêu dữ liệu này và đột nhiên giờ đây bạn có thể khiến nhà hàng Ý trông giống như một nhà chứa? bất cứ ai kiểm soát câu chuyện đó có rất nhiều quyền lực.

Với sự ra đời của Bitcoin, các nhà phát triển bắt đầu sử dụng công nghệ Blockchain để thêm một lượng nhỏ dữ liệu mới vào chuỗi, biết rằng dữ liệu sẽ có thể truy cập được trong thời gian còn lại. Vào năm 2015, Đại học Nicosia⁴⁰³ đã trở thành trường đại học đầu tiên cấp chứng chỉ học thuật có thể xác minh tính xác thực thông qua Blockchain Bitcoin. Thêm thông tin vào chuỗi đã trở thành tiêu chuẩn theo thời gian.

siêu dữ liệu giao dịch

Siêu dữ liệu là một công cụ hữu ích để xác nhận và xác thực thông tin. Nó cho phép các tài sản Crypto lưu thông tin về chủ sở hữu, chuyển khoản và giá trị trước đây của chúng. Điều này đặc biệt hữu ích khi xử lý các tài sản không thể thay thế phản ánh giá trị, chẳng hạn như tài sản hoặc tài sản trí tuệ. Khóa công khai cũng có thể được sử dụng để ký và xác nhận nhiều loại tài liệu, chứng minh tính xác thực của tài liệu.

⁴⁰²

AMA bắt ngày 31/03/2019, [youtube.be/sc4D2KrvaNA](https://www.youtube.com/watch?v=sc4D2KrvaNA)?t=2315

⁴⁰³

Chứng chỉ Blockchain (Học thuật & Khác), [unic.ac.cy/ iff /blockchain-certificates/](https://unic.ac.cy/iff/blockchain-certificates/)

Một trong những ứng dụng nổi tiếng nhất của siêu dữ liệu là trong chuỗi cung ứng. Các nhà máy, khách hàng, nhà cung cấp và dịch vụ giao hàng đều là một phần của chuỗi cung ứng. Người tham gia phải cung cấp bằng chứng về các dịch vụ được kết nối với nhau sẵn có cho mọi người để xác minh nhằm cho phép theo dõi dữ liệu hiệu quả. Trong tình huống này, siêu dữ liệu có thể cung cấp cái nhìn đầy đủ về các hoạt động của chuỗi cung ứng bằng cách kết hợp dữ liệu cố định trên sổ cái Blockchain với siêu dữ liệu. Đối với tất cả các bên, điều này đảm bảo tính cởi mở, tính bất biến và sự tự tin.

Atala

IOG, bao gồm các giải pháp Atala PRISM, Atala Trace và Atala Scan, đã chứng kiến quá trình thương mại hóa sớm việc triển khai siêu dữ liệu trên Cardano. Nhóm IOG đang phát triển hỗ trợ siêu dữ liệu trong khi kết nối với sổ cái Cardano để cải thiện toàn bộ chức năng của sản phẩm về tính khả thi của dữ liệu, trách nhiệm giải trình và khả năng truy xuất nguồn gốc.

Lăng kính Atala⁴⁰⁴ là một hệ thống nhận dạng phi tập trung cho phép các cá nhân kiểm soát dữ liệu cá nhân của họ và giao tiếp với các tổ chức một cách liền mạch, riêng tư và an toàn. Trên Cardano, nhóm Atala PRISM đang sử dụng siêu dữ liệu để chứng nhận và lưu trữ DID và tài liệu DID. Nó cũng sẽ có thể hủy các thông tin đăng nhập như chứng chỉ đại học, ngoài việc tạo chúng.

Atala Trace và Atala Scan đang được phát triển để giúp chủ sở hữu thương hiệu hiểu rõ hơn về hoạt động của chuỗi cung ứng đồng thời thiết lập nguồn gốc và khả năng kiểm toán của sản phẩm. Tích hợp siêu dữ liệu sẽ được sử dụng trong những trường hợp này để lưu trữ thông tin chuỗi cung ứng chống giả mạo.

Cả tổ chức và cộng đồng nhà phát triển đều có nhiều cách tiếp cận khác nhau để xử lý siêu dữ liệu. Sử dụng dịch vụ siêu dữ liệu do Nhóm dịch vụ chuyên nghiệp của IOG thành lập là một trong những phương pháp như vậy. IOG đã làm việc tích hợp với một số đối tác và có nhiều kế hoạch hơn. Siêu dữ liệu giao dịch là một thành phần ban đầu của tiện ích Goguen và khả năng hợp đồng thông minh, được mở rộng và phát triển bởi nhiều tính năng bổ sung.

Chiến lược siêu dữ liệu của Cardano

Siêu dữ liệu có nhiều ứng dụng. Với suy nghĩ này, IOG đã cố gắng làm cho việc đưa siêu dữ liệu vào ứng dụng của họ trở nên đơn giản nhất có thể. IOG cũng muốn đảm bảo rằng chủ sở hữu ADA có một phương tiện đơn giản để xem thông tin về các giao dịch của họ.

Bộ phân biệt

Siêu dữ liệu truyền tải tường thuật của một giao dịch và có một số phương pháp để tương tác với nó. Người dùng ADA có thể tìm kiếm thông tin cụ thể trong Cardano Explorer và các nhà phát triển có thể sử dụng siêu dữ liệu bằng cách nhúng chi tiết trực tiếp vào giao dịch. Dữ liệu có thể được đóng gói trực tiếp hoặc⁴⁰⁵ có thể tạo cây Merkle của dữ liệu và hàm băm gốc của cây Merkle được đặt trên Blockchain cho các tập dữ liệu lớn hơn. Khi điều này được hoàn thành, có thể chỉ ra rằng dữ liệu tồn tại tại một thời điểm nhất định và nó được lưu trữ vĩnh viễn trên chuỗi để sử dụng trong tương lai.

Cũng cần lưu ý rằng thông tin giao dịch được ghi lại trên Blockchain và được gửi cùng với mọi giao dịch. Việc nó được giữ trên chuỗi thay vì ở trạng thái sổ cái là thuận lợi vì nó không ảnh hưởng đến việc xác thực giao dịch và không làm giảm hiệu suất của sổ cái.

Dịch vụ siêu dữ liệu

Dịch vụ tư vấn kinh doanh và công nghệ được cung cấp bởi Nhóm dịch vụ chuyên nghiệp của IOG (PSG). PSG cung cấp các dịch vụ hỗ trợ các doanh nghiệp thiết kế và triển khai các giải pháp Blockchain bằng cách kết nối hệ thống của họ với công nghệ sổ cái phân tán một cách đơn giản và dễ dàng. Dịch vụ siêu dữ liệu được tạo ra với nhiều mục đích sử dụng, nhưng đặc biệt là cho các mục đích thương mại.

Giao diện này quản lý các tương tác ví, gửi cảnh báo số dư thấp cho người dùng và gói gọn mọi thứ trong bộ chứa Docker. Điều này loại bỏ sự phức tạp của việc cung cấp thông tin theo cách thủ công trong API phụ trợ của ví. Trước khi một giao dịch được tuyên bố hoàn tất, dịch vụ siêu dữ liệu chỉ cần thông tin được yêu cầu và số khối mà nó sẽ được lưu trữ.

⁴⁰⁴

Lăng kính Atala , atalaprism.io/

⁴⁰⁵

Cây băm hoặc **cây Merkle** là cây trong đó mọi Node lá được gắn nhãn bằng hàm băm của khối dữ liệu và mọi Node không phải là lá được gắn nhãn bằng hàm băm mật mã của nhãn của các Node con của nó. Cây băm cho phép xác minh hiệu quả và an toàn nội dung của cấu trúc dữ liệu lớn. Cây băm là sự tổng quát hóa danh sách băm và chuỗi băm.

Người ta có thể thêm phần sau vào yêu cầu siêu dữ liệu:

- Siêu dữ liệu thực tế, bao gồm danh tính của người gửi và người nhận, cũng như nhận xét và thẻ.
- Độ sâu: số khối trong đó giao dịch chứa siêu dữ liệu sẽ được lưu giữ trước khi được tuyên bố là hoàn tất.
- Ví sẽ được sử dụng được chỉ định bởi nhận dạng khách hàng.
- Nhận dạng giao dịch: trong trường hợp lỗi hoặc khởi động lại, chức năng này rất hữu ích.

Nó cho phép khách hàng kiểm tra lại siêu dữ liệu đã được cung cấp. Dịch vụ siêu dữ liệu lưu trữ một giao dịch trên Blockchain sau khi kết hợp tất cả các chi tiết, cho phép truy cập thông tin giao dịch thông qua Cardano Explorer. Tất cả những gì được yêu cầu là đặc điểm kỹ thuật của một nhận dạng giao dịch.

Dịch vụ siêu dữ liệu PSG cũng có thể được cung cấp qua bộ đệm giao thức ngôn ngữ trung lập. Trình tạo ứng dụng khách hỗ trợ nhiều loại ngôn ngữ lập trình, bao gồm Python, Java và Scala, giúp tăng cường số lượng ứng dụng khả thi. Quá trình tích hợp với Blockchain Cardano được thực hiện dễ dàng hơn nhờ các tùy chọn mở rộng này.

Để đọc thêm về 'Giao diện người dùng tự phục vụ' và các tính năng API, hãy truy cập tài liệu PSG.⁴⁰⁶ Trên GitHub, bạn có thể tìm hiểu thêm về API ví PSG Cardano⁴⁰⁷ và cách nó cho phép khách hàng thực hiện các tác vụ như gửi và liệt kê giao dịch, quản lý ví và giám sát Node.

Ví và Cardano-CLI

Gửi siêu dữ liệu trực tiếp từ ví hoặc giao diện dòng lệnh Cardano (CLI) là tùy chọn. Các quy trình này cần một số kỹ năng mã hóa cũng như sự quen thuộc với Node Cardano và CLI. Bởi vì các nhà phát triển có thể xác minh dữ liệu quan trọng theo cách riêng của họ, nên việc tương tác trực tiếp với siêu dữ liệu sẽ mở ra những cơ hội to lớn để tạo các ứng dụng phi tập trung trên Cardano.

Định dạng của siêu dữ liệu được thiết lập trong ví Cardano và CLI thông qua ánh xạ từ khóa sang giá trị (cặp khóa-giá trị) tích hợp thông tin cho nhiều mục đích sử dụng vào một giao dịch.

- Khóa siêu dữ liệu đóng vai trò là mã định danh lược đồ cho giá trị siêu dữ liệu mà chúng đại diện
- Giá trị siêu dữ liệu là các thuật ngữ đơn giản, bao gồm số nguyên, chuỗi văn bản, chuỗi byte, danh sách và bản đồ; khóa là số nguyên không dấu với kích thước tối đa là 64 bit; Các giá trị cần được cấu trúc để chúng có thể được xem và kiểm soát dễ dàng hơn, đặc biệt là bằng các tập lệnh.

Chi phí bổ sung duy nhất là siêu dữ liệu làm tăng kích thước của giao dịch theo byte và giá xử lý tùy thuộc vào kích thước giao dịch. Các ký hiệu Biểu diễn đối tượng nhị phân ngắn gọn (CBOR)⁴⁰⁸ và Ngôn ngữ định nghĩa dữ liệu ngắn gọn (CDDL)⁴⁰⁹ có thể được sử dụng để tạo siêu dữ liệu. Kiểm tra [Siêu dữ liệu giao dịch](#) của ví Cardano và cách sử dụng các lược đồ siêu dữ liệu giao dịch trong Cardano CLI.⁴¹⁰

Khóa Token trên Cardano

của Cardano đã được hình dung như một hành trình bao gồm năm thời kỳ phát triển chồng chéo, mỗi thời kỳ được hỗ trợ bởi hệ thống đồng thuận Ouroboros. Khi Cardano phát triển, giao thức cũng được điều chỉnh, vì các tính năng và chức năng mới đã được thêm vào nền tảng. Nâng cấp cần sửa đổi liên tục cho giao thức mạng.

⁴⁰⁶Tài liệu về dịch vụ của PSG, [psg-services.readthedocs.io/ vi /latest/](https://psg-services.readthedocs.io/en/latest/)

⁴⁰⁷

API ví PSG Cardano, github.com/input-output-hk/psg-cardano-wallet-api

⁴⁰⁸

CBOR (Biểu diễn đối tượng nhị phân ngắn gọn) là định dạng tuần tự hóa dữ liệu nhị phân dựa trên JSON một cách lỏng lẻo. Giống như JSON, nó cho phép truyền các đối tượng dữ liệu chứa các cặp tên-giá trị, nhưng theo cách ngắn gọn hơn. Điều này làm tăng tốc độ xử lý và truyền tải với cái giá phải trả là khả năng đọc của con người.

⁴⁰⁹

Ngôn ngữ định nghĩa dữ liệu ngắn gọn (CDDL) thể hiện cấu trúc dữ liệu Biểu diễn đối tượng nhị phân ngắn gọn (CBOR). Mục tiêu chính của nó là cung cấp một cách dễ dàng và rõ ràng để thể hiện cấu trúc cho các thông báo giao thức và định dạng dữ liệu sử dụng CBOR hoặc JSON (Ký hiệu đối tượng JavaScript).

⁴¹⁰

Siêu dữ liệu giao dịch, github.com/input-output-hk/cardano-node/blob/master/doc/reference/tx-metadata.md

Việc giới thiệu khóa Token

Khóa Token là tính năng chính của lần nâng cấp giao thức Goguen thứ hai. *Allegra* là tên cho giai đoạn phát triển này. Đây là bản cập nhật lớn tiếp theo cho Goguen, sau khi tích hợp siêu dữ liệu vào mạng.⁴¹¹

Đây là một điều chỉnh kỹ thuật nhỏ đối với quy trình đồng thuận và ít ảnh hưởng đến sổ cái. Tuy nhiên, điều đó rất quan trọng vì nó đã chuẩn bị nền tảng cho các hợp đồng thông minh và sản xuất các tài sản dựa trên Cardano (ngoài ADA). Nó cũng hỗ trợ bỏ phiếu, một phần thiết yếu của chức năng Voltaire (quản trị).

Khóa Token là phương pháp khóa việc sử dụng một Token cho một mục đích xác định (chẳng hạn như bỏ phiếu hoặc chạy hợp đồng thông minh). Các tài sản được kiểm đếm bởi sổ cái Blockchain được gọi là Token. Trước đó mới chỉ có quảng cáo này, nhưng kể từ đó, nhiều Token tùy chỉnh khác đã có thể sử dụng nền tảng Cardano. Trong trường hợp này, khóa có nghĩa là 'đặt trước' một số lượng Token cụ thể trong một khoảng thời gian nhất định để chúng không thể được bán để kiếm lời.

Khóa Token cho phép hợp đồng thông minh

Khóa Token là cần thiết để thực hiện các hợp đồng thông minh tinh vi và một số trường hợp nhất định, chẳng hạn như khi hoàn tất giao dịch mua. Khi ai đó đạt được thỏa thuận hợp đồng để bán một bức tranh cho một phòng trưng bày nghệ thuật, người bán hứa rằng bức tranh sẽ không được bán cho bất kỳ ai khác. Trong trường hợp này, Token có thể đại diện cho bức tranh, trong khi 'lời hứa' đại diện cho việc khóa Token thực sự. Nếu bức tranh được bán cho bên thứ ba, bảo đảm của hợp đồng sẽ bị vi phạm và mọi hình phạt sẽ được áp dụng. Với việc giới thiệu khóa Token và sử dụng tiền ADA làm Token, các nhà cung cấp hợp đồng sẽ có quyền truy cập vào khả năng chính xác này.

Những người nắm giữ ADA đã tham gia vào quá trình bỏ phiếu của Catalyst Fund2 phải 'đóng băng' ADA. Điều này cho thấy các đặc quyền biểu quyết của họ, dựa trên số lượng quảng cáo mà họ đã khóa. Nó chứng tỏ mỗi người có một số phiếu bầu nhất định và tránh khả năng phiếu bầu được kiểm hai lần. Các cá nhân không thể chỉ định nhiều phiếu bầu hơn họ có, bỏ phiếu cho các đề xuất phản đối hoặc bỏ phiếu trùng lặp.

Khóa Token được thực hiện theo cách bí mật.

Nó không ảnh hưởng đến trải nghiệm của chủ sở hữu ADA vì ví Daedalus và Yoroi được cập nhật tự động.

Sau khi triển khai khóa Token trên sổ cái Cardano trên mạng chính, các đợt hard fork trong tương lai bao gồm nhiều tài sản và các tính năng hợp đồng thông minh khác. Các tính năng này cũng tận dụng khóa Token, mang đến cho người dùng Cardano rất nhiều tùy chọn bổ sung. Điều này đã mở đường cho các Token không thể thay thế (duy nhất) được tạo trên Blockchain Cardano.

Cardano có một lộ trình an toàn, liền mạch để thay đổi giao thức thường xuyên, mỗi thay đổi trong số đó sẽ bổ sung giá trị và tính hữu dụng mới cho mạng đồng thời giảm gián đoạn và rủi ro, nhờ bộ kết hợp hard fork của IOG.

Token gốc

Token trên

Giao thức Bitcoin được xây dựng từ rất sớm khi Bitcoin tồn tại để cho phép người dùng phát hành tài sản dựa trên hệ thống kế toán của Bitcoin để theo dõi nhiều loại tiền tệ cùng một lúc. Giao thức Bitcoin không hỗ trợ các giao thức này một cách nguyên bản mà chúng được tạo ra thông qua các vụ hack. Các client nhẹ buộc phải phụ thuộc vào các máy chủ đáng tin cậy trong trường hợp lớp phủ Bitcoin như Colored Coins và Mastercoin (nay là Omni). Phí giao dịch vẫn phải được thanh toán bằng bitcoin. Những đặc điểm này, cùng với thực tế là các giao dịch được phê duyệt thông qua một đường ống duy nhất, khiến Bitcoin không phù hợp để hạch toán nhiều tài sản.

Token trên Ethereum

Vào tháng 7 năm 2015, Ethereum đã được ra mắt. Mặc dù Bitcoin đã tồn tại được sáu năm vào thời điểm đó, nhưng thế giới Crypto là một ngành công nghiệp non trẻ. Khi Ethereum lần đầu tiên xuất hiện, đầu mối của nó là các hợp đồng thông minh. Điều này có nghĩa

411

Alan McSherry, 'Làm quen với siêu dữ liệu trên Cardano',
iohk.io/en/blog/posts/2020/11/03/getting-to-grips-with-metADaTa-on-cardano/

là các nhà phát triển bên thứ ba có thể tạo ứng dụng của riêng họ và chạy chúng trên Blockchain Ethereum theo cách phi tập trung. Ethereum vượt trội so với Bitcoin về khả năng tiếp thị và khả năng thích ứng.

Trên Blockchain Ethereum, các hợp đồng thông minh cho phép tạo Token do người dùng xác định. Tiêu chuẩn ERC20⁴¹² cho phép tạo các Token Ethereum có thể thay thế được, trong khi⁴¹³ khung ERC721 cho phép tạo các Token duy nhất, không thể thay thế. Tuy nhiên, vì chuỗi Ethereum không kích hoạt hỗ trợ Token gốc, Token Ethereum do người dùng xác định (cả có thể thay thế và không thể thay thế) có một sự kém hiệu quả cố hữu: chúng yêu cầu xây dựng và thực thi mã tùy chỉnh.

Token hóa là gì?

Tokenization là quá trình chuyển đổi các đối tượng vật lý thành tài sản kỹ thuật số. Token thay thế phần tử dữ liệu không nhạy cảm bằng phần tử dữ liệu nhạy cảm. Loại tương đương không nhạy cảm này được gọi là Token và nó không có giá trị hoặc ý nghĩa nội tại hoặc có thể khai thác được.

Giảm chi phí giao dịch, minh bạch, thanh khoản cao hơn, phân cấp và tăng hiệu quả chỉ là một số lợi ích của việc này. Tokenization là một tính năng rất linh hoạt có thể được sử dụng để đạt được nhiều mục tiêu khác nhau. Token⁴¹⁴ có thể lập trình được; do đó, chúng có thể được làm độc đáo, điều này làm tăng thêm tính hữu dụng của chúng.

Ví dụ, Token có thể được thiết kế để cung cấp cho chủ sở hữu quyền truy cập vào tài liệu độc đáo, vật phẩm được cá nhân hóa hoặc thậm chí là quyền biểu quyết. Mục đích của quá trình bỏ phiếu là gì không có gì khác biệt. Cuối cùng, Token khả năng bỏ phiếu mang lại cho các cá nhân cảm giác trở thành một phần của điều gì đó lớn hơn chính họ và ý kiến của họ có thể được lắng nghe.

Hàng hóa tài chính và mô hình kinh tế có thể được tạo thông qua token hóa. Đồ sưu tầm, đầu tư thay thế, thẻ quà tặng, cá cược thể thao, tài sản trong trò chơi, hàng hóa, video clip về ngôi sao NBA yêu thích của bạn⁴¹⁵ và nhiều lĩnh vực khác đều là những ví dụ khả thi. Điều này có khả năng liên kết các sản phẩm, dịch vụ và hoạt động vật lý với thế giới ảo.

Token trên Cardano

Goguen đã thêm một kỹ thuật xử lý Token nguyên bản. Thay vì phụ thuộc vào hợp đồng thông minh, logic dựa trên sổ cái Cardano. IOG đã tạo ra một kỹ thuật Token hiệu quả vượt trội so với các tiêu chuẩn ERC20 và ERC721 của Blockchain Ethereum bằng cách làm theo phương pháp này.

Trên Blockchain Ethereum, các Token do người dùng xác định (cả Token ERC20 có thể thay thế và Token ERC721 không thể thay thế) không phải là bản địa, nghĩa là sổ cái cơ bản không hỗ trợ trực tiếp chúng. Các Token ERC20 và ERC721 về cơ bản khác với Ether, đồng tiền gốc của Ethereum.

Cách tiếp cận Token của Cardano cho phép đại diện cho các tài sản tùy chỉnh trên Blockchain mà không cần sử dụng hợp đồng thông minh, cũng như để các tài sản đó hoạt động tương tự như tiền tệ chính, ADA, ngoại trừ:

- Token gốc, không giống như ADA, có thể được đúc và phá hủy; Và
- Hiện tại, ADA là loại tiền tệ duy nhất có thể được sử dụng để thanh toán phí, phần thưởng và tiền gửi. Điều này có thể thay đổi với việc giới thiệu *Phí Babel* và Token dành riêng cho các Sidechain mới khác nhau. Thêm về điều này sau.

Cách nói về Token gốc

Trong ngành công nghiệp Crypto, các cụm từ 'coin' và 'token' thường có thể thay thế cho nhau và đôi khi chúng không. Và, trong các trường hợp khác, từ 'token' được dùng để chỉ tất cả các tài sản kỹ thuật số. Chiến lược Token của Cardano cũng độc đáo như chính Blockchain, do đó, đây là bảng thuật ngữ để giúp bạn nắm bắt kiến trúc Token gốc.

⁴¹²

Hợp đồng Ethereum ERC20 là một tiêu chuẩn để xây dựng Token trên Blockchain Ethereum. Trước Token ERC20, trao đổi Crypto phải xây dựng cầu nối tùy chỉnh giữa các nền tảng để hỗ trợ trao đổi bất kỳ Token nào. Vì lý do này, sáu quy tắc đã được tạo ra bởi một nhà phát triển Ethereum có tên là Fabian Vogelsteller và được đặt dưới tên ERC20, có nghĩa là “ yêu cầu bình luận ethereum ”.

⁴¹³

ERC721 là một tiêu chuẩn mở, miễn phí mô tả cách tạo Token không thể thay thế hoặc Token duy nhất trên Blockchain Ethereum.

⁴¹⁴

Token: Token mật mã phản ánh giá trị như được xác định bởi cộng đồng, trạng thái thị trường hoặc thực thể tự quản. Token có thể thay thế hoặc không thể thay thế có thể được sử dụng làm đơn vị thanh toán, phần thưởng, tài sản giao dịch hoặc người giữ dữ liệu.

⁴¹⁵

Tất cả các trận đấu của NBA có gì hấp dẫn ?, si.com/nba/2021/03/17/nba-top-shot-crypto-daily-cover

- Token được định nghĩa là đại diện của một tài sản được lưu giữ trên Blockchain Cardano
- Một tài sản được định nghĩa là bất cứ thứ gì có thể định lượng được
- Gói Token là đại diện của nhiều Token trong Cardano
- Logic Token chạy trên sổ cái Cardano chứ không phải hợp đồng thông minh được gọi là *gốc*.

Token gốc trên Cardano so với Ethereum

Token cho cả hai tiêu chuẩn (ERC20 và ERC721) được sao chép và sửa đổi, thay vì là một phần của chính hệ thống, do đó Ethereum cần mã tùy chỉnh cho các Token do người dùng xác định để được hỗ trợ trên chuỗi. Điều này thêm một lớp phức tạp, chi phí (*gas* ⁴¹⁶ được yêu cầu để trả cho việc thực thi mã) và kém hiệu quả. Đây là một lỗ hổng cố hữu trong Blockchain Ethereum vì nó cho phép lỗi của con người. Nếu không tuân thủ các phương pháp mã hóa tốt nhất, thì mã tùy chỉnh tinh ranh có thể gây ra các vấn đề có thể dẫn đến tổn thất tài chính đáng kể. Các lỗ hổng phần mềm đã góp phần làm mất lượng ether trị giá 300 triệu đô la trong một ⁴¹⁷sự kiện đặc biệt đáng nhớ. Solana ⁴¹⁸ đã được khởi động lại nhiều lần và bị hack Wormhole đắt tiền. Cardano tìm cách tránh những sự cố như vậy.

Khung Token gốc trong Cardano cho phép Token do người dùng xác định nguyên bản, tức là không yêu cầu lập trình đặc biệt. Token gốc là một loại hệ thống kế toán vốn được cung cấp bởi sổ cái. Điều này giúp loại bỏ các khía cạnh phức tạp, khó đoán và tốn kém của Token trên Ethereum.

Cardano là một loại sổ cái phi tập trung. Thông thường, một sổ cái phân tán chỉ có thể theo dõi một loại tài sản duy nhất khi nó được tạo (thường là Crypto của riêng nó). Tuy nhiên, khi sổ cái được phân cấp nhiều hơn, yêu cầu và khả năng giám sát các loại tài sản khác nhau trên cùng một cơ sở hạ tầng xuất hiện, đó là lý do tại sao các Blockchain cần xử lý nhiều tài sản như stablecoin, Token tiện ích, Token xác thực và Token bảo mật ⁴¹⁹. Token gốc, không giống như ERC20, không cần logic xử lý sự kiện bổ sung hoặc chi phí chuyển cụ thể để giám sát giao dịch.

Cơ sở hạ tầng kế toán được thiết lập trong mô hình sổ cái, ban đầu dự định chỉ xử lý các giao dịch ADA, đã được mở rộng để hỗ trợ các giao dịch sử dụng nhiều loại tài sản cùng một lúc. Token gốc có lợi thế là không yêu cầu hợp đồng thông minh truyền giá trị của chúng và có thể được giao dịch cùng với các loại Token khác.

Bảo mật là một lợi ích khác của tiền gốc so với ERC20. Các Token ERC20 đã được chứng minh là có nhiều vấn đề bảo mật được ghi lại rõ ràng. ⁴²⁰ Điều này là do việc tạo Token ERC20 yêu cầu thay đổi thủ công tiêu chuẩn hợp đồng, điều này có thể dẫn đến sai sót và sai sót. Vì sổ cái quản lý logic Token nên việc tạo và giao dịch Token sẽ loại bỏ rủi ro này một cách tự nhiên. Ngoài ra, các Token gốc không gặp phải các lỗ hổng tràn và tràn giống như Token ERC20 do ngôn ngữ kịch bản của Cardano không sử dụng các số nguyên có kích thước cố định và chính sổ cái (trái ngược với mã người dùng ERC20) giám sát chuyển động của Token.

Bốn điểm khác biệt của Token gốc trên Cardano

Kiến trúc nhẹ

Kiến trúc Token gốc được xây dựng xung quanh các gói Token và dựa trên cấu trúc sổ cái đa tài sản. Gói Token có thể bao gồm hỗn hợp ADA và các Token khác. Thay vì ADA, các cấu trúc chứa Token này được ghi lại dưới dạng đầu ra trên sổ cái. ID nội dung của từng loại Token chứa tham chiếu hàm băm đến chính sách đúc của Token. Chính sách đúc tiền chỉ được xác minh trong quá trình đúc hoặc đốt và nó không được duy trì trên sổ cái, làm cho phương pháp này rất nhẹ.

⁴¹⁶

Gas (Ethereum) đề cập đến phí hoặc giá trị định giá, cần thiết để thực hiện thành công giao dịch hoặc thực hiện hợp đồng thông minh trên nền tảng Blockchain Ethereum. Được định giá bằng một phần nhỏ của ether Crypto, thường được gọi là gwei hoặc đôi khi là nanoeth, gas được sử dụng để phân bổ tài nguyên của Máy ảo Ethereum (EVM) để các ứng dụng phi tập trung như hợp đồng thông minh có thể tự thực thi là một cách bảo mật. Lượng gas tối đa mà bạn sẵn sàng chi tiêu cho một giao dịch cụ thể được gọi là giới hạn gas.

⁴¹⁷

' 300 triệu đô la Crypto ' vô tình bị mất vĩnh viễn do lỗi, theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether

⁴¹⁸

3 lý do Solana không thực sự phi tập trung, makeuseof.com/reasons-solana-not-really-decentralized/

⁴¹⁹

Token tiện ích: một Token kỹ thuật số đại diện cho một dự án hoặc môi trường nhất định và có các khả năng cụ thể. Những Token này có thể được sử dụng làm đơn vị thanh toán, giải thưởng hoặc như một phương tiện để giành được quyền truy cập vào một mạng cụ thể.

⁴²⁰

Lỗ hổng Blockchain: Token ERC20 dễ bị tổn thương và cách tránh viết mã dễ bị tổn thương, apriorit.com/dev-blog/555-erc20-token-vulnerability

ID nội dung cũng nắm bắt được kết nối có thể thay thế theo cách đơn giản: các Token có cùng một ID nội dung có thể thay thế cho nhau, nhưng không phải với các Token có ID nội dung khác nhau. ID nội dung của các Token duy nhất được kết hợp với số lượng chính xác là một.

Trong một gói Token duy nhất và trong toàn bộ sổ cái, ID tài sản xác định từng loại Token. Nó cũng cho biết vị trí của Token bên trong cấu trúc bản đồ hai cấp bên trong của gói Token. Cấu trúc dữ liệu cơ bản này cho phép thể hiện các Token có thể thay thế và không thể thay thế theo cùng một cách. Nó cũng cho phép hệ thống linh hoạt hơn về các loại trường hợp sử dụng tài sản có thể được mã hóa. Chẳng hạn, thật đơn giản để đại diện cho một bộ sưu tập các tác phẩm nghệ thuật có một không hai được bao phủ bởi một chính sách đúc duy nhất do nghệ sĩ đặt ra.

Khi chúng tôi kiểm tra cách ERC20 của Ethereum xử lý việc chuyển tài sản giữa hai hợp đồng, tính đơn giản vốn có của các Token gốc càng được nhấn mạnh nhiều hơn. Mã hợp đồng thông minh là cần thiết trong trường hợp này, điều này làm tăng thêm độ phức tạp, cũng như khả năng xảy ra sai sót và chi phí. Bởi vì một số loại Token có thể được giao dịch trong một giao dịch duy nhất, cấu trúc của gói Token cho phép phương pháp chuyển tài sản nhẹ nhàng hơn.

không tốn kém

Việc chuyển bất kỳ số lượng Token nào giữa hai đồng nghiệp trong hệ sinh thái Token ERC20 yêu cầu thực hiện hợp đồng thông minh, đi kèm với phí thực hiện (gas). Việc chuyển giao tài sản (Token, ADA, tiền tệ tùy chỉnh, v.v.) trong hệ sinh thái đa tài sản gốc của Cardano không cần hợp đồng thông minh và không phát sinh chi phí thực hiện.

Bảo mật hơn, ít mã tùy chỉnh hơn

Các Token gốc có thiết kế nhẹ hơn và ít tốn kém hơn so với các giao thức ERC20 và ERC721 của Ethereum. Tuy nhiên, hai yếu tố này sẽ trở nên vô dụng nếu không có lớp bảo mật đủ mạnh để đảm bảo tính toàn vẹn của hệ thống.

Tính toàn vẹn của hệ thống với Token gốc dựa trên thuộc tính sổ cái bảo toàn giá trị (nghĩa là tổng của tất cả các đầu vào bằng tổng của các đầu ra). Không giống như các hợp đồng thông minh do người dùng xác định, tất cả logic chuyển Token gốc được nhúng trong sổ cái. Điều này đảm bảo rằng hệ thống hoạt động có thể đoán trước và nhất quán, đồng thời loại bỏ nhu cầu người dùng phải nắm vững các hợp đồng thông minh, vốn thường dễ bị tin tặc khai thác.

Mặc dù sổ cái đảm bảo tính chính xác của kế toán, nhưng việc đúc và đốt Token được điều chỉnh bởi các chính sách đúc do người dùng xác định. Chính sách đúc được liên kết chặt chẽ với các Token mà chính sách đó áp dụng vô thời hạn và không có cách nào để sửa đổi chính sách đó. Điều này đảm bảo rằng chính sách của tổ chức phát hành không thể được sửa đổi để cho phép đúc hoặc đốt Token không được phép theo chính sách ban đầu. Chính sách cho từng loại Token được đúc đều được xác minh và phải được đáp ứng bất cứ khi nào một giao dịch đúc được đưa vào sổ cái. Ngoại trừ ADA (Cardano có nguồn cung hạn chế là 45 triệu ADA), mọi Token đang lưu hành phải có chính sách đúc và phải được đúc theo chính sách đó.

Do đó, chính sách này là mã tùy chỉnh duy nhất cần thiết để thay đổi Token trong Cardano. Bởi vì hàm băm chính sách được liên kết với nhận dạng tài sản, nên không cần đăng ký tài sản toàn cầu, giúp việc tạo tài sản trở nên đơn giản và rẻ tiền. Công nghệ này vẫn ở mức cơ bản, nhẹ và dễ vận hành.

Sự đơn giản

Giờ đây, các Token gốc của Goguen đã được triển khai, sổ cái xử lý tất cả các Token theo cùng một cách. Để tránh sự mơ hồ và bất kỳ lỗi hoặc sai sót nào, Token chỉ có thể được đúc theo một phương pháp. Sự hợp lý hóa quá trình phát triển này thông qua việc sử dụng một phương pháp thống nhất dẫn đến sự phát triển nhanh hơn và trải nghiệm phát triển tổng thể tốt hơn.

IOG đã cung cấp thêm chi tiết trên GitHub dưới Token gốc và cách chúng so sánh với ADA và ERC20.⁴²¹ Ngoài ra còn có một video giải thích Token gốc.⁴²² Động lực được xây dựng ổn định sau khi nâng cấp *Mary* và *Alonzo*, với việc các nhà phát triển nhận ra lợi ích

⁴²¹

Token gốc là gì và nó so sánh với ADA và ERC 20 như thế nào?,
github.com/input-output-hk/cardano-ledger-specs/blob/master/doc/explanations/features.rst

⁴²²

Chào mừng bạn đến với Token gốc trên Cardano!, youtube.com/watch?v=PVqsCXh-V5Y

của việc triển khai Token gốc và NFT trên Cardano. Thông tin chi tiết về Blockchain Cardano ⁴²³báo cáo gần 3,3 triệu ví, hơn 4,5 triệu Token gốc, hơn 5.000 NFT và hơn 1.100 dự án triển khai cho Cardano kể từ tháng 1 năm 2023.⁴²⁴

Hỗ trợ đa tài sản (MAS)

Sổ cái tài sản duy nhất

Sổ cái một tài sản là sổ cái Crypto chỉ theo dõi một loại tài sản.

Hỗ trợ

đa tài sản Khi một Blockchain, sổ cái hoặc Crypto cho phép ghi lại việc chuyển nhượng và quyền sở hữu một số loại tài sản trên sổ cái của nó, nó được cho là có hỗ trợ đa tài sản (MA). Tính năng Token gốc trong hệ sinh thái Cardano cung cấp khả năng này.

Tính năng này mở rộng cơ sở hạ tầng kế toán được chỉ định trong mô hình sổ cái, nhằm xử lý các giao dịch chỉ dành cho ADA, cho các giao dịch sử dụng nhiều loại tài sản cùng một lúc. ADA và một loạt các loại Token tùy chỉnh do người dùng xác định nằm trong số những nội dung này.

Bản địa so với không bản địa

Một sổ sổ cái Crypto có các tính năng cho phép bạn giám sát quyền sở hữu và chuyển giao nhiều loại tài sản. Hỗ trợ MA gốc (đa tài sản) là tên được đặt cho loại hỗ trợ MA này. Chức năng MA của Cardano được tích hợp sẵn hoặc 'gốc'.

Có thể giám sát các tài sản không có hỗ trợ kế toán sổ cái nếu nền tảng Crypto có khả năng hợp đồng thông minh đủ tinh vi. Điều này được thực hiện bằng cách sử dụng giải pháp Lớp 2 dựa trên hợp đồng thông minh. Đây là một hình thức hỗ trợ MA không bản địa.

Tài sản

Trên Blockchain, tài sản là một vật thể hiện giá trị. Một tài sản kỹ thuật số như ADA, vị trí, chứng chỉ hoặc một số sản phẩm đều là ví dụ về các mục này.

Từ tài sản có thể đề cập đến một trong hai điều sau:

- mã định danh của một lớp đối tượng, chẳng hạn như ADA hoặc 'johnCoin'; hoặc
- một số tiền chính xác của một điều nhất định, ví dụ. '10 lovelace', '33 johnCoin', 'cuốn sách này' hoặc 'những lọ mứt này'

ID nội dung là sự kết hợp giữa ID chính sách và tên nội dung xác định duy nhất nó. Cần lưu ý rằng mặc dù ADA có thể được sử dụng làm nội dung nhưng nó không có ID chính sách rõ ràng.

Các Token có cùng ID tài sản có thể thay thế lẫn nhau, tuy nhiên chúng không thể thay thế cho các Token có ID tài sản khác nhau. ID nội dung là mã định danh duy nhất của bộ sưu tập Token có thể thay thế được.

PolicyID - ID duy nhất được liên kết với chính sách đúc. ID là một chuỗi các chữ cái và số được tạo bằng cách áp dụng hàm băm trên chính chính sách đó.

Tên nội dung - thuộc tính (bất biến) của nội dung được sử dụng để phân biệt giữa các nội dung trong cùng một chính sách. Tên nội dung, không giống như *policyID*, không tương ứng với bất kỳ mã hoặc bộ quy tắc nào và có thể là bất kỳ thuật ngữ phổ biến nào, chẳng hạn như 'vé' hoặc 'VIPTickets.' Tuy nhiên, tên nội dung hợp lệ có thể bị giới hạn bởi chính sách xác định phạm vi của nội dung.

Đối với các Token riêng biệt, các chính sách khác nhau có thể sử dụng cùng tên nội dung.

Token

⁴²³

Thông tin chi tiết về Blockchain, datastudio.google.com/u/0/reporting/3136c55b-635e-4f46-8e4b-b8ab54f2d460/page/p_wxcw6g0irc
⁴²⁴

Số liệu thống kê cho đến nay (cập nhật hàng tuần), essentialcardano.io/development-update

Token là một từ viết tắt của 'Token tài sản', là đơn vị kế toán và đại diện trên chuỗi của tài sản. Ví dụ, một ADA, một ngôi nhà hoặc một tấn trà có thể được biểu thị bằng một Token.

tiền tệ

Tiền tệ là một thuật ngữ được sử dụng để mô tả một đơn vị tiền tệ phục vụ như một phương tiện trao đổi hàng hóa và dịch vụ. Cardano chấp nhận ADA và Token gốc, cả hai đều hoạt động như nhau trên mạng.

Tuy nhiên, tại thời điểm này, ADA là loại tiền tệ duy nhất được sử dụng để thanh toán phí và gửi tiền, đồng thời đây cũng là loại tiền tệ duy nhất phát hành phần thưởng. Kiến trúc của giao thức đồng thuận cơ bản chịu trách nhiệm về thuộc tính này của ADA (và không có loại tài sản nào khác).

Token gốc là một loại đơn vị kế toán có thể được sử dụng cho các khoản thanh toán và giao dịch, cũng như được chuyển đến một địa chỉ trao đổi. Vì sổ cái kế toán Cardano có chức năng tích hợp để theo dõi quyền sở hữu và chuyển giao một số loại tài sản, các Token này được sổ cái hỗ trợ mà không cần thêm hợp đồng thông minh. Mặc dù cả Token ADA và Token gốc đều có giá trị và có thể được sử dụng để thanh toán và giao dịch, nhưng chỉ Token ADA được sử dụng cho phí và phần thưởng và chỉ Token gốc mới có thể được tùy chỉnh.

Điều kiện khi sử dụng ADA

Đồng tiền chính của Cardano là ADA (₳). Bởi vì mỗi địa chỉ phải có giá trị ADA tối thiểu, nên cần phải có ADA (cùng với các loại tiền tệ khác) để chuyển Token đa tài sản giữa các địa chỉ (giá trị ADA tối thiểu, hiện được đặt ở mức 1 ADA).

Do thiết kế của nó, các điều kiện sau sẽ áp dụng:

1. Không thể tạo đầu ra chỉ bao gồm các Token tùy chỉnh.
2. Số lượng của từng loại Token trong đầu ra không ảnh hưởng đến giá trị tối thiểu của đầu ra, nhưng số lượng loại Token sẽ làm tăng giá trị tối thiểu. (Điều này là do tên và ID chính sách của từng loại Token khác nhau chiếm thêm dung lượng trong đầu ra.)
3. Khi gửi Token tùy chỉnh đến một địa chỉ, giá trị tối thiểu của ADA luôn được gửi cùng với Token tùy chỉnh (bằng cách đưa ADA vào cùng một đầu ra). ADA được cung cấp cùng với Token không còn thuộc về người gửi nếu người gửi Token không thể sử dụng địa chỉ đó.

Người dùng có thể chọn sử dụng đối thoại ngoài chuỗi để thảo luận xem ai sẽ cung cấp ADA để trang trải giá trị tối thiểu trong đầu ra được tạo bởi giao dịch chuyển trước khi chuyển Token tùy chỉnh.

4. Để truy xuất ADA được đặt cùng với Token tùy chỉnh trong đầu ra O , người dùng phải:

- Sử dụng đầu ra O và ghi các Token tùy chỉnh chứa trong đó
- Chỉ tiêu một đầu ra O và một đầu ra O' , sau đó kết hợp các Token trong các đầu ra đó với cùng một bộ Token tùy chỉnh được lưu trữ trong một đầu ra khác (được chỉ tiêu trong cùng một giao dịch).

5. Bởi vì một số ADA phải được cung cấp trong mỗi đầu ra, nên việc chia Token tùy chỉnh thành nhiều đầu ra hơn so với trước khi giao dịch được thực hiện cần tổng số ADA nhiều hơn để trang trải giá trị ADA tối thiểu.

Gói Token là gì?

Gói Token là một tập hợp các Token không đồng nhất (' hỗn hợp '). Bất kỳ loại token nào cũng có thể được đóng gói cùng nhau. Trên Blockchain Cardano, các gói Token là cách tiêu chuẩn để đại diện và lưu trữ tài sản. Token nhóm các Token vào một cấu trúc dữ liệu nhất định, đảm bảo Token nào có thể thay thế được với các Token khác được xác định rõ ràng.

Số tiền đã được nêu trong giao dịch và đầu ra UTXO trong các phiên bản trước của sổ cái Cardano. Số lượng này đã được mở rộng với các gói Token, có thể xác định số lượng ADA với số lượng tài sản khác trong một đầu ra, nhờ vào việc bổ sung chức năng đa tài sản.

Các gói Token được lưu trữ trong đầu ra giao dịch và trường dư tiền, cũng như đầu ra của bộ UTXO, được theo dõi bởi sổ cái. Một số yếu tố của giao dịch, chẳng hạn như trường phí, vẫn phải nêu rõ số tiền ADA.

Lưu trữ gói Token

Gói Token có thể được tìm thấy:

- Là trường đúc của giao dịch, cho biết rằng giao dịch đang tạo Token của gói
- Trong đầu ra của giao dịch hoặc đầu ra trong UTXO hiện tại được sở hữu, bên cạnh địa chỉ của đầu ra, ví dụ: `Multi { MyAddress , value: TB_Example }`

Tách và kết hợp các gói Token

Các gói Token có thể được phân chia và kết hợp tùy ý theo giao dịch.

chính sách khai thác

Chính sách đúc tiền là một tập hợp các quy tắc kiểm soát việc đúc và đốt tài sản nằm trong tầm kiểm soát của chính sách. Chính sách đúc chỉ định các trường hợp theo đó Token được đúc (hoặc đốt). Ví dụ, các quy tắc có thể mô tả ai có thẩm quyền đối với việc cung cấp tài sản thông qua việc đúc và đốt.

Người dùng muốn sản xuất một tài sản mới sẽ thiết lập các chính sách đúc. Ví dụ: người dùng có thể chọn giới hạn bản thân trong việc chỉ đúc một loại Token nhất định. Đây là một cái gì đó sẽ được vạch ra trong chính sách.

Sau đây là các quy tắc đúc tiền:

Là một bộ quy tắc rất đơn giản, nó bao gồm các quy tắc sau (AND và OR):

- Danh sách các chữ ký cần thiết để cho phép đúc hoạt động (ví dụ: thông số kỹ thuật đa chữ ký, trong đó không cần mã)
- Với tập lệnh Plutus Core, thông số kỹ thuật về thời điểm tập lệnh có thể được sử dụng (ví dụ: sau vị trí 10 và trước vị trí 30).

Khi một giao dịch được thực hiện, Node sẽ kiểm tra việc tuân thủ các quy định đúc tiền bằng cách thực thi mã hoặc xác thực các chữ ký thích hợp. Tất cả các chính sách đúc cho tất cả các tài sản mà giao dịch đang tìm cách đúc phải được tuân theo.

Đúc tiền: Điều khoản & Điều kiện

- Một chính sách đúc tiền là bắt buộc đối với tất cả các tài sản. Ví dụ, chính sách đúc tiền của ADA quy định rằng 'không bao giờ được đúc tiền mới'
- Token chỉ có một chính sách đúc được kết nối với nó
- Một chính sách duy nhất mô tả các yêu cầu đối với cả việc đúc và đốt Token nằm trong phạm vi của nó. Sự tuân thủ của nó được giám sát cả trong quá trình đúc và trong quá trình đốt
- Chính sách khai thác liên quan đến nội dung không thể thay đổi bất cứ lúc nào, chính sách này không thể đảo ngược. Không thể liên kết các Token hiện tại với một chính sách mới. Với chính sách đúc mới, người dùng có thể mua lại và ghi tất cả các Token hiện tại trong khi vẫn đúc các mã mới. Đây là do thiết kế, nó không phải là lỗi trong hệ thống
- Một tài sản tồn tại trên sổ cái nằm trong phạm vi của một chính sách nhất định được đảm bảo đã được đúc theo chính sách đó
- Chính sách thực tế không quan trọng cho đến khi Token của chính sách đó được tạo trong một giao dịch. Mục đích duy nhất của nó là phục vụ như một ID duy nhất cho nội dung
- Các tài sản liên quan đến các chính sách đúc tiền khác nhau không bao giờ được hoán đổi cho nhau. Chúng có thể được trao đổi theo cách tương tự như USD có thể được sử dụng để mua Euro: số lượng Euro bạn có thể mua với một lượng USD cụ thể được xác định bởi tỷ giá hối đoái.

Mối quan hệ giữa một nội dung và chính sách khai thác của nó

Vì lý do bảo mật, liên kết giữa nội dung và chính sách đúc của nó là vĩnh viễn. Tính năng này bảo vệ người dùng và hệ thống chống lại các Token giả mạo.

của Token thay đổi, Token đó không còn là cùng một Token nữa và giá trị của nó không thể được so sánh với Token ban đầu. Để xác định các chính sách đảm bảo cao, phương pháp liên kết chính sách tài sản cố định này là rất cần thiết. Kỹ thuật MA (Đa tài sản) của Cardano trở nên dễ bị tấn công nếu nhận dạng này bị nổi lên. Tốt nhất là đảm bảo rằng mọi Token đều được đúc theo chính sách đúc của nó, chứ không phải bất kỳ chính sách nào khác mà nó có thể đã được liên kết trước đó, bằng cách có một liên kết vĩnh viễn giữa chúng.

Các loại chính sách khai thác

Có một số loại chính sách đúc khác để xem xét.

Chính sách một tổ chức phát hành

của một tổ chức phát hành quy định rằng chỉ thực thể có một bộ khóa nhất định mới có thể đúc Token cho một nhóm tài sản cụ thể. Ví dụ: giao dịch đúc tiền phải được ký bởi bộ khóa được cung cấp trong chính sách đúc tiền.

Token đại diện cho thẻ bóng đá Panini là một ví dụ về danh mục tài sản sẽ áp dụng chính sách một nhà phát hành. Công ty sản xuất thẻ của các nhà sưu tập đích thực sẽ cung cấp chìa khóa cần thiết để đúc thẻ bóng đá mới, theo yêu cầu của kịch bản đúc. Điều này có nghĩa là không có thẻ bóng đá mới nào có thể được sản xuất mà không có sự chấp thuận của công ty. Không cần sử dụng hợp đồng thông minh Plutus khi tạo hình thức chính sách này.



Hình 17: Thẻ bóng đá Panini

Chính sách đúc có khóa thời gian

AKA khóa Token. Chính sách này có thể được sử dụng để giới hạn số lượng Token có thể được sử dụng từ một địa chỉ nhất định.

- chỉ trong hoặc sau một khoảng thời gian xác định
- chỉ trước một khoảng thời gian xác định

Thông thường, hình thức chính sách này không được sử dụng riêng. Ví dụ, nó thường được sử dụng kết hợp với chính sách đa chữ ký hoặc chính sách đơn vị phát hành. Chỉ giao dịch được ký bởi khóa 'k' mới có thể sử dụng đầu ra này sau vị trí 's'. Hình thức chính sách này có thể được tạo mà không cần hợp đồng thông minh Plutus.

Chính sách đúc tiền một lần

Trong chính sách đúc một lần, một giao dịch đơn lẻ sẽ đúc toàn bộ Token cho một loại tài sản cụ thể. Điều này cho thấy rằng sẽ không bao giờ có thêm bất kỳ Token nào trong danh mục tài sản đó. Loại chính sách này bắt buộc phải sử dụng hợp đồng thông minh Plutus.

Ví dụ: chính sách đúc tiền một lần có thể được sử dụng để tạo Token vé cho Super Bowl. Vì sức chứa của địa điểm đã được biết trước nên sẽ không cần phát hành thêm vé.

giao dịch đúc tiền

Mỗi giao dịch có một trường đúc tiền có thể được sử dụng để thêm số lượng Token mới vào sổ cái (đúc) hoặc để xóa Token hiện có (đốt). Giao dịch đúc là các giao dịch trong đó trường đúc không trống. Việc sử dụng trường này phải được quy định chặt chẽ để đảm bảo rằng các Token được đúc và đốt theo chính sách đúc của Token.

Các giao dịch đúc tiền phải bao gồm các quy tắc đúc cho các Token mà chúng đang đúc, ngoài trường đúc tiền, để các Token này có thể được kiểm tra trong quá trình xác thực.

Sổ cái sẽ ghi lại các tài sản có trong trường đúc tiền, được bao gồm trong số dư của giao dịch: nếu trường là dương, thì đầu ra của giao dịch phải có nhiều tài sản hơn nguồn cung cấp đầu vào; nếu nó là âm, thì chúng phải chứa ít hơn.

Cần lưu ý rằng một giao dịch đơn lẻ có thể dẫn đến việc tạo ra các Token với nhiều quy tắc đúc. Chẳng hạn, (Policy1, SomeTokens) hoặc (Policy2, SomeOtherTokens). Một giao dịch cũng có thể đúc và đốt các Token cùng một lúc.

Sổ đăng ký siêu dữ liệu

Siêu dữ liệu là mô tả về nội dung gốc mà bất kỳ ai cũng có thể đọc được trong Cardano. Những tài sản này được giữ trên chuỗi bằng cách sử dụng ID mà con người không thể đọc được. Phiên bản có thể đọc được của dữ liệu này được lưu giữ trong các cơ quan đăng ký Token công khai, không phải trên Blockchain. Các cơ quan đăng ký này, đầu tiên sẽ được kiểm soát bởi IOG, cuối cùng sẽ được sở hữu và định cấu hình bởi cộng đồng, cho phép Cardano đạt được một mức độ phân cấp khác. IOG đảm bảo rằng cộng đồng có thể hoàn toàn tin tưởng vào các bộ dữ liệu bằng cách cho phép cộng đồng sở hữu và định cấu hình các cơ quan đăng ký này. Bởi vì người dùng là chủ sở hữu của dữ liệu, nên hành vi trung thực là điều tốt nhất cho họ.

Có một dự thảo *CIP 26 - Siêu dữ liệu ngoài chuỗi của Cardano* đề xuất một tiêu chuẩn cho siêu dữ liệu ngoài chuỗi ánh xạ các số nhận dạng trên chuỗi thành siêu dữ liệu mà con người có thể đọc được.

Tạo Token gốc trên Cardano

Người dùng có thể chọn giữa các công cụ đơn giản và tinh vi để đưa tài sản của họ vào cuộc sống trên Cardano. Token đang trở nên phổ biến hơn cho các giao dịch tài chính. Họ giảm phí đồng thời tăng cường tính minh bạch, tăng tính thanh khoản và tất nhiên là vẫn độc lập với các thực thể tập trung như ngân hàng. Tokenization là quá trình chuyển đổi tài sản thực tế (chẳng hạn như tiền tệ fiat, cổ phiếu, kim loại quý và bất động sản) thành token kỹ thuật số có thể được sử dụng để xây dựng các công cụ tài chính thương mại.

Nhiều tùy chọn Token ⁴²⁵ có sẵn trong Cardano. Kiến trúc kế toán của sổ cái không chỉ xử lý các giao dịch ADA mà còn xử lý các giao dịch chứa nhiều loại tài sản cùng một lúc.

Tính thiết thực

Để hoàn thành các mục tiêu thương mại hoặc kinh doanh, nhà phát triển, doanh nghiệp và ứng dụng có thể tạo ⁴²⁶Token cho mục đích chung (có thể thay thế) hoặc chuyên biệt (không thể thay thế). Token thanh toán tùy chỉnh hoặc phần thưởng cho DApps, stablecoin gắn liền với các loại tiền tệ khác và tài sản độc nhất, như sách điện tử, đại diện cho tài sản trí tuệ chỉ là một vài ví dụ. Tất cả những tài sản này sau đó có thể được mua bán, trao đổi hoặc sử dụng để mua hàng hóa và dịch vụ.

Người dùng sẽ có thể truyền, nhận và ghi Token của họ mà không phải trả phí giao dịch hoặc cài đặt logic xử lý sự kiện để giám sát giao dịch vì Token gốc không cần hợp đồng thông minh để chuyển giá trị của chúng. Người dùng có thể sản xuất, phân phối, giao dịch và lưu trữ Token theo một trong bốn cách, tùy thuộc vào sở thích và chuyên môn kỹ thuật của họ:

1. CLI Cardano

⁴²⁵

Tim Harrison, 'Token gốc trên Cardano', iohk.io/en/blog/posts/2020/12/08/native-tokens-on-cardano/

⁴²⁶

Trong kinh tế học, **tính có thể thay thế được** là thuộc tính của hàng hóa hoặc hàng hóa mà các đơn vị riêng lẻ về cơ bản có thể hoán đổi cho nhau và mỗi bộ phận của nó không thể phân biệt được với bộ phận khác.

Nhà phát triển có thể tạo nội dung (đúc tiền) và gửi giao dịch thử nghiệm đến các địa chỉ khác nhau bằng cách sử dụng môi trường thử nghiệm Token gốc.

Do tính chất làm việc với CLI, giả định rằng bạn cảm thấy thoải mái với việc thiết lập và quản lý Node Cardano, cũng như xử lý các giao dịch và quản lý địa chỉ và giá trị. Để tạo Token gốc sử dụng Cardano CLI, hãy làm theo các bước được nêu trong tài liệu.⁴²⁷ Ở cấp độ cao, các bước như sau:

- Tạo và bắt đầu một Node Cardano
- Tạo khóa xác minh và ký
- Tạo địa chỉ thanh toán, nạp tiền và kiểm tra số dư
- Bắt đầu quá trình đúc, tạo chính sách và đúc một tài sản mới
- Cuối cùng, xây dựng các giao dịch thô, gửi và ký các giao dịch để gửi Token đến địa chỉ mục tiêu.

Trên trang tài liệu Cardano,⁴²⁸ IOG cung cấp các hướng dẫn và bài tập về Token gốc để cho phép các nhà phát triển tạo Token, triển khai các quy tắc tiền tệ và hiểu cách thực hiện các giao dịch đa tài sản.

2. GUI trình tạo Token

CLI yêu cầu một lượng chuyên môn lập trình nhất định. Do đó, IOG đã thiết lập các phương pháp khác cho người dùng ít kỹ thuật hơn để tạo Token. Sau khi khởi chạy mainnet CLI, IOG đã triển khai trình tạo Token để thực hiện việc này.

Trình tạo Token là giao diện người dùng đồ họa giúp đơn giản hóa quá trình tạo Token. Trình tạo Token có thể hỗ trợ bạn xây dựng Token cho ứng dụng phi tập trung của bạn, mã hóa tài sản của bạn, tạo thẻ sưu tập NFT được biểu thị dưới dạng tài sản chuyên dụng hoặc thiết lập một đồng tiền ổn định gắn với giá trị của các loại tiền tệ khác.

Để tạo Token, chỉ cần điền vào các trường sau:

- Tên của Token (ví dụ: CardanoForTheMasses)
- biểu tượng của Token (ví dụ: CFTM)
- biểu tượng của Token (được tạo tự động)
- Số tiền được thực hiện (ví dụ : 10m)
- Vị trí ví Cardano (địa chỉ của bạn để lưu trữ Token mới được tạo).

Chính sách tiền tệ được tạo tự động bởi trình tạo Token, vì vậy bạn sẽ không phải tự mô tả chính sách đó. Điều này tăng tốc và đơn giản hóa quy trình tạo Token cho người dùng không có kỹ thuật.

Sau khi Token đã được đúc, tùy chọn 'Đúc thêm' sẽ cho phép bạn đúc thêm. Điều này có thể được thực hiện bằng cách sử dụng cùng một chính sách để tạo thêm Token cùng loại hoặc sử dụng chính sách mới để tạo Token đại diện cho các giá trị khác nhau. Ví dụ: bạn có thể tạo Token *CardanoForTheMasses* cho mỗi ấn bản của Sách điện tử này. Ban đầu chỉ đúc cho 'Phiên bản Vasil'. Khi sự kiện HFC tiếp theo xảy ra, sẽ không có thêm Token 'phiên bản Vasil' nào được đúc. Các Token mới hiện đã được đúc cho ấn bản mới với ảnh bìa mới và Sách điện tử được cập nhật. Mỗi phiên bản sẽ có một chính sách đúc tiền khác nhau.

Trình tạo Token tìm cách đơn giản hóa việc sản xuất Token đồng thời nhấn mạnh vào việc cải thiện và hiển thị trực quan các quy trình chức năng. Do đó, người dùng muốn có thể xem tất cả các Token đã được tạo, giá trị, số lượng và địa chỉ mà chúng đang được chuyển đến — tất cả ở một nơi.

có nhiều công cụ xây dựng Token của bên thứ 3 chẳng hạn như *cardano-native-token.com*

3. Token trên Daedalus

Người dùng không muốn tạo token của riêng mình mà muốn sử dụng token hiện tại để thanh toán, mua hàng hoặc trao đổi có thể sử dụng Daedalus, Yoroi, Flint,... hầu hết các ví hiện nay đều hỗ trợ chức năng này.

ID chính sách và Tên nội dung là hai số nguyên thập lục phân được ghi trên chuỗi xác định duy nhất các Token gốc. IOG đã tạo dấu vân tay để giúp người dùng dễ dàng xác định Token gốc hơn vì những con số này không 'thân thiện với con người'. Dấu vân tay là chuỗi chữ và số gồm 44 ký tự với tiền tố 'Token' ở đầu.

⁴²⁷Bắt đầu với Token gốc, docs.cardano.org/native-tokens/getting-started

⁴²⁸

Sổ đăng ký Token Cardano, được kiểm soát ban đầu bởi Cardano Foundation, bao gồm dữ liệu Token bổ sung được trình bày trong giao diện người dùng ví (tên, mô tả và từ viết tắt). ADAHandle (\$handle, ADAhandle.com) là một trong những dự án đầu tiên ra mắt sau Goguen với tư cách là 'Giải pháp đặt tên do NFT cung cấp cho địa chỉ ví Cardano của bạn, được bảo mật hoàn toàn trên chuỗi thông qua Tiêu chuẩn xử lý'.

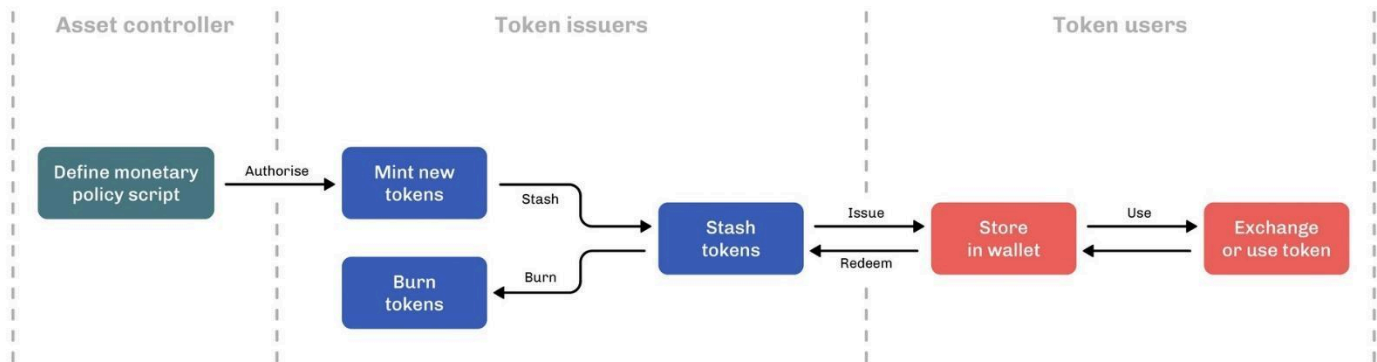
4. Nền tảng của bên thứ ba.

Ví dụ: Dripdropz (dripdropz.io), 'Hệ thống phân phối Token Cardano' đã bổ sung giá trị lớn cho hệ sinh thái.

Vòng đời của Token gốc trên Cardano

Vòng đời Token gốc sẽ hoàn tất sau khi tất cả các thành phần bắt buộc đã được triển khai. Nó được chia thành năm giai đoạn:

- đúc tiền
- phát hành
- sử dụng
- mua chuộc
- Đốt cháy.



Hình 18: Vòng đời của Token gốc trên Cardano

Mỗi quy trình logic này bao gồm các giao dịch Blockchain Cardano, có thể dẫn đến phí ADA. Sau đây là các diễn viên chính:

- Người kiểm soát tài sản, người xác định chính sách của loại tài sản và ủy quyền cho nhà phát hành Token đúc và đốt Token. Họ cũng có thể giữ quyền đồng ký cho bất kỳ Token nào được đúc hoặc đốt
- Người phát hành Token, người tạo Token mới, dự trữ chúng trong lưu thông, phân phối chúng cho chủ sở hữu Token và hủy chúng khi chúng không còn hữu ích
- Chủ sở hữu Token, những người giữ Token, gửi chúng cho những người dùng khác, sử dụng chúng để thanh toán và sau đó đổi chúng với tổ chức phát hành khi chúng không còn cần thiết nữa. Người dùng 'Joe Soap' bình thường, sản giao dịch và các thực thể khác có thể là người dùng Token.

Tuổi thọ của Token đa tài sản bắt đầu bằng quá trình tạo – đúc tiền, đây là quá trình mà một hoặc nhiều tổ chức phát hành Token tạo Token mới phù hợp với tập lệnh chính sách tiền tệ do bộ điều khiển tài sản cung cấp. Trong hầu hết các trường hợp, các Token mới sẽ được phát hành để phục vụ một chức năng cụ thể. Chẳng hạn, các Token có thể thay thế hoặc không thể thay thế (duy nhất) có thể được phát triển cho các yêu cầu thanh toán, mua hoặc trao đổi cụ thể. Khi một Token mới được tạo, nguồn cung cấp Token tổng thể cho Token đó sẽ tăng lên, nhưng nguồn cung cấp ADA vẫn giữ nguyên. Việc đúc tiền và chuyển chúng đến địa chỉ mới có thể yêu cầu thanh toán ADA, có thể tỷ lệ thuận với số lượng Token riêng biệt sở hữu.

Chủ sở hữu Token sẽ lưu trữ Token trong ví của họ và sẽ có thể chuyển chúng cho người dùng khác, trao đổi chúng để lấy các đối

tượng có giá trị (bao gồm cả Token không có nguồn gốc), v.v., giống như họ làm với ADA. Khi Token của người dùng đã được sử dụng hết, họ có thể chọn đổi Token đó. Có nghĩa là Token được trả lại cho nhà phát hành ban đầu của chúng (chẳng hạn như đổi lại sản phẩm, dịch vụ hoặc một số loại tiền tệ khác). Sau đó, Token có thể được cấp lại cho người dùng khác theo yêu cầu sau khi chúng được đổi. Để thanh toán phí giao dịch, chủ sở hữu Token sẽ cần giữ một số ADA trong ví của họ.

Nếu được yêu cầu, các Token có thể bị đốt cháy khi chúng trở nên dư thừa, phù hợp với kịch bản chính sách tiền tệ cơ bản. Hành động đốt các Token này sẽ loại bỏ chúng (loại bỏ chúng khỏi lưu thông), làm giảm nguồn cung cấp Token tổng thể. Tại thời điểm này, mọi khoản đặt cọc sẽ được hoàn trả. Các token có thể thay thế và không thể thay thế đều được đốt cháy theo cùng một cách.

Vòng đời Token đa tài sản có thể cho phép các bên khác mua và phát hành lại Token, chẳng hạn như chủ sở hữu Token đóng vai trò là người phát hành lại. Điều này có thể được thực hiện để tạo điều kiện thuận lợi cho giao dịch giữa các loại tài sản khác nhau, duy trì tính thanh khoản của một hoặc nhiều Token (bằng cách đóng vai trò là nhà môi giới) hoặc giảm nỗ lực/chi phí tạo Token, phát hành hoặc bảo trì máy chủ siêu dữ liệu. Kết quả là, một giao dịch như vậy mang lại lợi ích cho cả người phát hành lại và người phát hành bằng cách giảm chi phí và nỗ lực, duy trì sự tách biệt và tính toàn vẹn, đồng thời truyền giá trị vào loại tài sản.

Yêu cầu giá trị tối thiểu

Trên sổ cái, UTXO có thể chứa một túi hỗn hợp các Token, bao gồm cả ADA. Tổng kích thước tối đa được sử dụng bởi các mục nhập UTXO trên sổ cái tại bất kỳ thời điểm nào bị giới hạn bằng cách yêu cầu một lượng ADA được đưa vào mỗi UTXO (trong đó lượng đó phụ thuộc vào kích thước của UTXO, tính bằng byte).

Bằng cách điều chỉnh cài đặt giá trị tối thiểu, kích thước UTXO tối đa được phép (tổng kích thước của tất cả các mục nhập UTXO) được sửa đổi hoàn toàn. Giới hạn ngăn sổ cái Cardano vượt quá một kích thước cụ thể theo cách này. Sổ cái không có giới hạn về kích thước có xu hướng trở nên quá tải dữ liệu đến mức người dùng sẽ không thể xử lý nó (hoặc vận hành một Node) trên các thiết bị đáp ứng tiêu chí Node bắt buộc.

Có nhiều chi tiết hơn trong Tài liệu Cardano về trường hợp 'chỉ dành cho ADA', tính toán 'giá trị tối thiểu của ADA' và với các ví dụ đã hoạt động.

Kết quả của chiến lược này là

- Bạn không thể tạo đầu ra chỉ chứa Token tùy chỉnh
- Số lượng của mỗi loại Token trong một đầu ra có thể ảnh hưởng một chút đến giá trị tối thiểu của đầu ra. Có một số ảnh hưởng vì giá trị UTXO tối thiểu sẽ tính đến chi phí bộ nhớ khi lưu trữ nó trên máy tính. Chi phí bộ nhớ không bị ảnh hưởng nhiều bởi sự gia tăng ADA nhưng việc thêm nhiều nội dung sẽ có tác động. Điều này là do tên và ID chính sách của từng loại Token chiếm thêm dung lượng trong đầu ra
- Khi gửi Token tùy chỉnh đến một địa chỉ, giá trị tối thiểu của ADA luôn được gửi cùng với Token tùy chỉnh (bằng cách đưa ADA vào cùng một đầu ra). ADA được cung cấp cùng với Token không còn thuộc về người gửi, nếu địa chỉ không thể được sử dụng bởi người gửi Token
- Trước khi chuyển Token tùy chỉnh diễn ra, người dùng có thể sử dụng giao tiếp ngoài chuỗi để xác định ai cung cấp ADA để trang trải giá trị tối thiểu trong đầu ra được tạo bởi giao dịch chuyển
- Để khôi phục ADA được lưu trữ cùng với Token tùy chỉnh trong đầu ra O , người dùng phải:

- a) sử dụng đầu ra O và ghi Token tùy chỉnh trong đó; hoặc
- b) sử dụng một đầu ra O và một đầu ra O' và hợp nhất các Token trong đó với cùng một bộ sưu tập các loại Token tùy chỉnh được lưu trữ trong một đầu ra O khác. (được chi tiêu trong cùng một giao dịch)

Ví dụ: trong một đầu ra mới được tạo bởi giao dịch hợp nhất, (`CryptoBisonPolicy`, `AmericanBison`, 2) trong O có thể được hợp nhất với (`CryptoBisonPolicy`, `AmericanBison`, 4) trong O' , tổng cộng là (`CryptoBisonPolicy`, `AmericanBison`, 6)

- Việc chia Token tùy chỉnh thành nhiều đầu ra hơn so với trước khi giao dịch được thực hiện bắt buộc phải sử dụng tổng cộng nhiều ADA hơn để đáp ứng giá trị ADA tối thiểu, vì ADA được yêu cầu trong các đầu ra bổ sung.

Câu hỏi thường gặp về Token gốc

Hỗ trợ 'đa tài sản (MA)' nghĩa là gì và Cardano có hỗ trợ không?

Hỗ trợ đa tài sản (MA) đề cập đến một tập hợp các tính năng mà một sổ cái (Blockchain/ví tiền/Crypto/nền tảng ngân hàng) có thể cung cấp để cho phép nó tính toán và tương tác với một số loại tài sản.

Token gốc là tính năng hỗ trợ MA của Cardano. Người dùng có thể giao dịch với ADA và vô số Token do người dùng xác định bằng MA. Đây là hỗ trợ gốc, có nghĩa là Token có thể được giao dịch bằng cách sử dụng hệ thống kế toán được thiết lập như một phần khả năng sổ cái của Crypto mà không cần bất kỳ hợp đồng thông minh nào.

Sự khác biệt giữa tài sản gốc và NFT là gì ?

Về mặt kỹ thuật, NFT giống như tài sản gốc. Có những đặc điểm làm cho tài sản gốc trở thành NFT. A) Nó phải không thể thay thế nghĩa là bạn cần phải có các số nhận dạng hoặc thuộc tính duy nhất được đính kèm với một Token để làm cho nó trở nên độc nhất so với những Token khác. Thông thường, NFT tồn tại mãi mãi trên Blockchain, do đó cần phải có một cơ chế để đảm bảo NFT luôn là duy nhất và không thể trùng lặp.

Định nghĩa của Token (tài sản) là gì?

Token hóa một tài sản đòi hỏi phải tạo ra một phiên bản kỹ thuật số của nó trên Blockchain.

Việc 'đúc' một Token có nghĩa là gì?

'Đúc tiền' đề cập đến quá trình tạo hoặc hủy Token mới. Nghĩa là, tổng số lượng lưu thông của loại Token được đúc thay đổi (tức là khi tất cả các địa chỉ trên sổ cái được đặt cùng nhau). Tạo Token là khi một số lượng Token dương được đúc, trong khi việc đốt Token xảy ra khi một số âm được đúc.

'Đốt' Token có nghĩa là gì?

Thuật ngữ 'đốt' dùng để chỉ quá trình hủy Token. Nó giống như 'đúc tiền tiêu cực'.

Đổi Token đòi hỏi gì?

Mua lại Token đòi hỏi phải trả lại Token cho nhà phát hành để bị đốt cháy. Điều này thường được thực hiện khi các Token được đổi không còn phục vụ chức năng trên sổ cái và người dùng hoặc hợp đồng sở hữu chúng không thể ghi Token (theo chính sách đúc tiền). Mặc dù chính sách phát hành/đúc Token có thể không trao bất kỳ phần thưởng nào cho việc đổi Token, tuy nhiên, người dùng có thể chọn làm điều đó để tránh có những Token vô dụng trong ví của họ.

Giao dịch đúc tiền là gì?

Giao dịch đúc tiền là những giao dịch trong đó phần dữ liệu giao dịch này (được gọi là trường đúc tiền) không trống. Ngoài ra, các giao dịch này phải bao gồm các chính sách đúc cho các Token mà chúng đang đúc, để chúng có thể được xác minh trong quá trình xác thực.

Các tài sản có trong trường đúc (đúc) của giao dịch giờ đây sẽ được thêm vào sổ cái do thực hiện giao dịch đúc. Nếu số lượng của một tài sản nhất định trong trường đúc tiền là âm, thì tổng số lượng của tài sản đó trên sổ cái sẽ bị giảm xuống bằng số lượng được chỉ định trong trường đúc tiền khi giao dịch được xử lý.

Lưu ý rằng một giao dịch đơn lẻ có thể đúc Token được liên kết với nhiều chính sách đúc khác nhau. Cũng cần lưu ý rằng một giao dịch có thể đúc và đốt các Token cùng một lúc.

Chính sách đúc tiền là gì?

Chính sách đúc tiền là một tập hợp các quy tắc chi phối việc đúc các tài sản được liên kết với nó. Ví dụ, ai kiểm soát nguồn cung cấp tiền tệ (và trong những trường hợp nào), cũng như việc đúc và đốt tiền tệ đó. Các quy tắc này áp dụng cho nội dung của dữ liệu giao dịch cho giao dịch mà cơ sở đúc tiền đang thực hiện. Ví dụ: chính sách đúc có thể chỉ định rằng giao dịch đúc được ký bởi một bộ khóa nhất định.

Người dùng muốn đúc một nội dung mới sẽ xác định bộ quy tắc này. Ví dụ: người dùng có thể muốn giới hạn bản thân trong việc đúc loại Token này. Điều này sẽ được chỉ định trong chính sách. Khi một giao dịch được thực hiện, Node sẽ kiểm tra sự tuân thủ các quy định đúc tiền bằng cách thực thi mã hoặc xác thực các chữ ký phù hợp. Tất cả các chính sách đúc của tất cả các tài sản mà giao dịch đang tìm cách đúc phải được thỏa mãn bởi dữ liệu giao dịch.

Trình tạo Token là gì và chức năng của nó là gì?

Trình tạo Token là phần mềm cho phép người dùng chỉ định Token sẽ được tạo và đưa chúng vào giao dịch đúc. Nó cũng đảm bảo rằng giao dịch có dữ liệu bổ sung cần thiết để xác minh rằng giao dịch được ủy quyền để thực hiện quá trình đúc.

'multisig' là gì và nó có liên quan gì đến các chính sách đúc tiền?

Ngôn ngữ tập lệnh đa chữ ký đặt số lượng chữ ký tối thiểu cần thiết cho một giao dịch để hoàn thành một hoạt động nhất định, thường sử dụng một mục nhập UTXO.

Các tập lệnh multisig cũng có thể được sử dụng để xác định các quy tắc đúc cơ bản nhất, chẳng hạn như các quy tắc cần một bộ khóa được chỉ định để ký giao dịch đúc. Ví dụ: tập lệnh nhiều chữ ký có thể được sử dụng để chỉ định chính sách đúc tiền của một tổ chức phát hành.

Mối quan hệ giữa hợp đồng thông minh Plutus và Token gốc là gì?

Ngôn ngữ hợp đồng thông minh Plutus có thể được sử dụng để viết các chính sách đúc tiền. Điều này cho phép người dùng chỉ định nhiều loại chính sách hơn nhiều so với chính sách của một nhà phát hành duy nhất mà multisig có thể truyền đạt. Ví dụ, Plutus có thể chỉ định chính sách đúc một lần (nhưng không chỉ là multisig).

Định nghĩa của chính sách đúc tiền của một tổ chức phát hành duy nhất là gì?

Chính sách đúc tiền của một nhà phát hành duy nhất tuyên bố rằng chỉ thực thể có một bộ khóa nhất định mới được phép đúc Token theo chính sách đó. Ví dụ: giao dịch đúc tiền phải được ký bởi bộ khóa được cung cấp trong chính sách đúc tiền. Multisig có thể được sử dụng để cung cấp loại chính sách này.

Token giống như bức tranh của một nghệ sĩ là một ví dụ về trường hợp sử dụng chính sách của một tổ chức phát hành. Điều này sẽ loại trừ việc sản xuất các thẻ tranh mới mà không có chữ ký của nghệ sĩ. Mặt khác, bảo hiểm xác định rằng tất cả các bức tranh hiện có được bảo hiểm theo chính sách đều do nghệ sĩ sản xuất chứ không phải ai khác. Tokhun⁴²⁹ chỉ là một thị trường NFT nơi các nghệ sĩ có thể bán tranh của họ như nghệ sĩ Jonathan Dickson⁴³⁰ đã giải thích trong video này.⁴³¹

Chính sách đúc tiền một lần là gì?

Chính sách đúc một lần sẽ đúc toàn bộ Token được bao phủ bởi nó trong một giao dịch. Điều này có nghĩa là theo chính sách đó, sẽ không có thêm Token nào được đúc. Hợp đồng thông minh là bắt buộc đối với hình thức chính sách này, không thể được thể hiện qua nhiều chữ ký. Đúc Token vé cho Superbowl là một ví dụ về chính sách đúc một lần đang hoạt động. Vì sức chứa của địa điểm đã được biết trước nên sẽ không cần phát hành thêm vé.

Sự khác biệt giữa có thể thay thế và không thể thay thế là gì?

Tính linh hoạt là mối quan hệ tồn tại giữa hai tài sản hoặc Token. Khi hai Token có thể hoán đổi cho nhau, chúng được cho là có thể thay thế được. Ví dụ, tờ 10 € có thể hoán đổi với tất cả các tờ 10 € khác (cũng như tất cả 10 đồng 1 € và tất cả các cặp tờ 5 €). Tài sản không thể thay thế không thể hoán đổi cho nhau. Ví dụ: hai viên ngọc quý hoặc hai Token trên chuỗi đại diện cho hai viên ngọc trong thế giới thực. Nếu một Token không thể thay thế được với các tài sản khác, chẳng hạn như Token đại diện cho một bức tranh, thì nó được coi là duy nhất (không thể thay thế).

Gói Token là gì và nó hoạt động như thế nào?

Một tập hợp Token hỗn hợp tuân theo một hoặc nhiều chính sách đúc. Bất kỳ loại token nào cũng có thể được nhóm lại với nhau.

Sự xuất hiện của Token gốc trong ví của người dùng là gì?

Ví của người dùng lưu trữ cả đầu ra với địa chỉ thuộc về người dùng và số lượng ADA mà những địa chỉ này có trước khi đưa chức năng MA (đa tài sản) vào hệ thống Cardano. (Địa chỉ người dùng l, someADAAmount) là một ví dụ.

Ví của người dùng giờ đây có thể bao gồm nhiều loại tài sản trong một đầu ra duy nhất với hỗ trợ đa tài sản (MA), nghĩa là ví sẽ có thể chứa một gói Token. Điều này có nghĩa là ví có thể bao gồm các mục sau:

- Nội dung được bao phủ bởi nhiều chính sách trong một UTXO duy nhất (bao gồm cả ADA)
- Nội dung được bao phủ bởi một chính sách duy nhất và phân tán trên một số UTXO

Các Token gốc có chứa ID và thông tin khác mà con người có thể đọc được không?

Thay vì chuỗi ID chính sách dài và tên nội dung, tên nội dung mà con người có thể đọc được có thể được đăng ký trên máy chủ siêu dữ liệu. Khi người dùng xem tài sản của họ trong ví được kết nối với máy chủ siêu dữ liệu, họ sẽ có thể thấy tên mà con người có thể đọc được. Người dùng sẽ có thể tải tên Token của họ lên, cũng như bất kỳ thông tin cụ thể nào khác về Token, lên máy chủ siêu dữ liệu. Người dùng sẽ phải chọn (các) máy chủ để tải lên hoặc tải xuống siêu dữ liệu của họ từ đó nếu có nhiều máy chủ siêu dữ liệu

⁴²⁹

Tokhun, tokhun.io/ jonathandickson

⁴³⁰

Twitter Jonathan Dickson, twitter.com/JonathanDickson

⁴³¹

Jonathan Dickson Elements NFT trên Cardano, youtube.com/watch?v = F1DR-39RN28

hoạt động cùng lúc. Người dùng cũng có thể nhập tên và các chi tiết khác trực tiếp vào trường siêu dữ liệu của giao dịch. Chi phí giao dịch sẽ tăng tỷ lệ thuận với lượng siêu dữ liệu được thêm vào.

Phí tạo Token gốc và trao đổi chúng là gì?

Có hai loại chi phí liên quan đến nhiều tài sản:

- **Phí:** Gửi và đúc Token có tác động đến phí mà tác giả của giao dịch phải trả. Phí được xác định tùy thuộc vào toàn bộ số tiền của giao dịch, giống như trong sổ cái chỉ dành cho ADA. Có thể có thêm chi phí để xác minh các chính sách đúc tiền, tuy nhiên, hiện tại chỉ có các chính sách nhiều chữ ký, không phát sinh thêm phí so với các chính sách dựa trên quy mô giao dịch
- **Giá trị ADA tối thiểu:** Đầu ra của mọi giao dịch phải chứa một lượng ADA tối thiểu, được tính tùy thuộc vào kích thước của đầu ra (số lượng loại Token khác nhau trong đó và độ dài tên của chúng).

Giá trị tối thiểu:

Hãy nhớ rằng đầu ra có thể bao gồm một túi hỗn hợp các Token, bao gồm cả ADA, đây là một nguồn tài nguyên khan hiếm. Việc bao gồm một số lượng ADA trong mỗi đầu ra trên sổ cái (trong đó lượng đó phụ thuộc vào kích thước của đầu ra tính bằng byte) ngăn không cho sổ cái Cardano trở nên quá lớn.

Tôi có thể tận dụng loại tài sản nào để thanh toán các chi phí của Token gốc?

Tại thời điểm này, chỉ có thể sử dụng ADA để thanh toán phí hoặc gửi tiền.

Làm thế nào để lựa chọn tiền xu Token gốc bespoke hoạt động?

Nó hoạt động tương tự như lựa chọn tiền xu ADA trong đó người dùng chọn Token và số tiền họ muốn chi tiêu, đồng thời vì chọn đầu vào phù hợp và trả phí.

Có thể gửi Token đến một địa chỉ

không ? Có, việc gửi Token gốc đến một địa chỉ được thực hiện theo cách tương tự như việc gửi ADA được thực hiện, cụ thể là bằng cách gửi giao dịch có đầu ra chứa gói Token mà tác giả giao dịch muốn gửi, cũng như địa chỉ mà chúng được gửi đến. Xem eutxo.org để biết hình ảnh trực tiếp về các giao dịch trong thế giới thực trên Cardano

Người dùng có mức độ kiểm soát nào đối với nội dung Token tùy chỉnh?

Token đa tài sản có thể được sử dụng, gửi, giao dịch và nhận theo cách tương tự như Token ADA. Người dùng có thể đúc và ghi Token gốc, không giống như ADA.

Người dùng có thể chi tiêu Token trong ví của họ hoặc Token trong đầu ra bị khóa bởi tập lệnh cho phép người dùng này chi tiêu đầu ra. Gửi Token cho người dùng khác: Người dùng có thể gửi (chi tiêu) Token trong ví của họ tới bất kỳ địa chỉ nào.

Đúc Token: Người dùng có thể đúc Token tùy chỉnh theo chính sách của nội dung. Các Token này có thể được gửi đến địa chỉ của người dùng hoặc bất kỳ ai khác trong quá trình giao dịch đúc. Chính sách có thể giới hạn địa chỉ đầu ra cụ thể cho Token nếu được yêu cầu.

Lưu ý rằng, tùy thuộc vào các quy tắc chính sách, ngay cả khi người dùng đã chỉ định chính sách, người dùng đó có thể không được phép đúc hoặc đốt tài sản thuộc phạm vi điều chỉnh của chính sách đó. Bất kể danh tính của người dùng đã phát triển chính sách là gì, chính sách đúc sẽ chi phối việc đúc bất kỳ tài sản nào được bảo vệ bởi chính sách đó.

Đốt Token: Chính sách được liên kết với nội dung cũng kiểm soát việc đốt Token. Người dùng phải có khả năng chi tiêu các Token mà họ đang cố gắng đốt ngoài việc có thể đốt chúng (luôn tuân thủ chính sách đúc).

Ngay cả khi chính sách đúc tiền cho phép rõ ràng, người dùng không thể ghi Token mà họ không có quyền kiểm soát, chẳng hạn như Token trong ví của người khác.

Làm thế nào để Token gốc Cardano so sánh với Token tùy chỉnh Ethereum ERC721 và ERC20?

Cách tiếp cận của Cardano đối với việc tạo Token tùy chỉnh thay đổi từ việc triển khai Token tùy chỉnh không có nguồn gốc, chẳng hạn như ERC721 hoặc ERC20, sử dụng các khả năng của hợp đồng thông minh để bắt buộc việc chuyển tài sản tùy chỉnh (tức là hệ thống kế toán sổ cái). Vì kiến trúc sổ cái cho phép kế toán các tài sản gốc không phải của ADA, nên kỹ thuật tạo Token tùy chỉnh của Cardano không cần hợp đồng thông minh. Một điểm khác biệt quan trọng khác là, không giống như ERC721 hoặc ERC20, sổ cái đa tài sản Cardano cho phép cả token có thể thay thế và không thể thay thế mà không cần hợp đồng chuyên biệt và đủ linh hoạt để kết hợp hỗn hợp các token có thể thay thế và không thể thay thế trong một đầu ra duy nhất .

Đa tài sản trên Sàn giao dịch

Nội dung gốc được xác định theo *chính sách đúc của chúng*, do người dùng đặt khi tạo (đúc) (các) nội dung mới. Các chính sách này chỉ định giới hạn tối đa và giới hạn dưới của những gì Token có thể thực hiện, cũng như ai có thể thực hiện và khi nào có thể thực hiện trong suốt vòng đời giao dịch.

Giao thức mạng và các quy tắc do số cái xác định ràng buộc một chính sách đúc tiền. Giá trị UTXO tối thiểu là một trong những nguyên tắc như vậy (số lượng ADA tối thiểu phải được gửi trong một giao dịch). Bởi vì giá trị hiện tại được cố định thành một ADA, tối thiểu một ADA phải được đưa vào và hạch toán trong mỗi giao dịch tài sản gốc trên mạng Cardano.

cardano-graphql hoặc cardano-rosetta có thể được sử dụng để xác thực và định vị các giao dịch nội dung gốc duy nhất này.

quản lý đa tài sản

liệt kê ADA có khả năng gặp phải một trong hai trường hợp:

Tình huống 1: Chi tiêu một UTXO có đính kèm nhiều tài sản

Tình huống này chỉ liên quan đến các sàn giao dịch kiểm soát UTXO của chính họ.

Làm cách nào để khám phá các UTXO có đính kèm nội dung gốc? Trình khám phá khối cục bộ (ví dụ: cardano-graphql hoặc cardano-rosetta) thường được sử dụng bởi các sàn giao dịch và ví của bên thứ ba duy trì UTXO của riêng họ.

cardano-graphql là ngôn ngữ truy vấn và thành phần thời gian chạy cho API Cardano cho phép bạn đáp ứng các truy vấn bằng cách sử dụng dữ liệu từ cơ sở dữ liệu cardano - db -sync PostgreSQL ⁴³². Nó cung cấp cho khách hàng khả năng yêu cầu thông tin họ cần bằng cách cung cấp cho họ mô tả rõ ràng và dễ hiểu về dữ liệu. Do đó, cả sự phát triển của API máy khách và việc triển khai các công cụ dành cho nhà phát triển đều được đơn giản hóa.

Bắt đầu

Sau khi bạn đã thấy cách thức hoạt động của giao dịch tài sản gốc, bạn có thể muốn tạo hoặc ghi một số tài sản hoặc Token gốc trên mạng thử nghiệm . Để bắt đầu khai thác nội dung gốc, hãy xem các yêu cầu này ⁴³³ và làm theo các bước bên dưới:

- Kết nối cardano -node với testnet
- Xây dựng cardano -node và kết nối với testnet
- Tải xuống nhị phân dựng sẵn cardano -cli hoặc sử dụng bản dựng từ nguồn
- Làm theo các bước trong tài liệu

Làm cách nào để tôi chi tiêu UTXO với nội dung gốc được đính kèm?

Điều quan trọng là phải tính đến hai yếu tố khi sử dụng cardano -cli để tạo giao dịch bằng nội dung gốc, như được mô tả trong phần này:

1. Giá trị của ADA bạn muốn gửi
2. Số lượng token

Bất kỳ trao đổi hoặc bên thứ ba nào muốn chi tiêu, hoàn tiền hoặc lưu trữ bất kỳ tài sản đa năng nào đều phải tuân theo các quy tắc tương tự. Nhận một giao dịch nhiều tài sản, theo định nghĩa, giống như nhận bất kỳ giao dịch Cardano nào khác. Điểm khác biệt duy nhất là giao dịch có thể bao gồm dữ liệu bổ sung, chẳng hạn như nhiều tài sản.

Đó là phương pháp hay nhất cho tất cả các sàn giao dịch và ví của bên thứ ba để kiểm tra và xử lý bất kỳ giao dịch đa tài sản nào trong khối. Người dùng quyết định cách xử lý các loại giao dịch này.

Điều gì về Token không mong muốn? Chức năng của bất kỳ tài sản đa năng nào có thể là bất kỳ thứ gì bạn muốn, nhưng điều quan trọng cần nhớ là, giống như ADA, đó là một phần của giao dịch và phải được quản lý và cân đối phù hợp.

⁴³²

PostgreSQL , còn được gọi là Postgres, là một hệ thống quản lý cơ sở dữ liệu quan hệ nguồn mở và miễn phí, nhấn mạnh khả năng mở rộng và tuân thủ SQL. *Xem Phụ lục: Kiến trúc Cardano.*

⁴³³

Bắt đầu với Token gốc, docs.cardano.org/native-tokens/getting-started

Đa tài sản sẽ không gây ra bất kỳ vấn đề gì, cho dù chúng nằm trong ví của tổ chức phát hành hay ví của sản giao dịch. Cho đến khi nó được mua lại, sử dụng hoặc đốt cháy, nó sẽ 'sống'.

Trao đổi hoặc ví của bên thứ ba chịu trách nhiệm cuối cùng trong việc quyết định phải làm gì với nhiều tài sản.

Để xử lý và duy trì UTXO, ví cardano sử dụng một thuật toán UTXO. Trên Blockchain, nhiều tài sản được quản lý thông qua cardano-wallet có thể dễ dàng không bị phát hiện.

Chọn một UTXO có nghĩa là tính đến nội dung được liên kết với UTXO đó. Lỗi mất cân bằng sẽ xảy ra nếu đầu vào bổ sung này không được xử lý thích hợp.

Bạn có toàn quyền kiểm soát nội dung gốc. Bạn có hai tùy chọn: trả lại cho người gửi nếu bạn biết địa chỉ hoặc chuyển nội dung gốc đến một địa chỉ trong ví của bạn trong khi tuân thủ các điều kiện mạng và giá trị UTXO tối thiểu.

Để biết thêm thông tin về cách thiết lập và cân bằng giao dịch với nội dung gốc được đính kèm, hãy xem phần *Token gốc* của Cardano Docs.

Kịch bản 2 – Bắt ngờ nhận được nhiều tài sản trong ví cardano .

Lưu ý: Kịch bản này chỉ áp dụng cho các sản giao dịch sử dụng cardano -wallet .
Xác nhận bạn đã nhận được nhiều tài sản

1. Kiểm tra thông tin ví để xác nhận
2. Để xác nhận thông tin ví, hãy sử dụng lệnh curl bên dưới:

vỏ sò

```
cuộn tròn http://localhost:8090/v2/wallets
```

3. Xác nhận trong phần tài sản:

```
"tài sản": {
  "tổng cộng": [
    {
      "_name tài sản ": "2e7444437f696e",
      "số lượng": 10,
      "chính sách _id ": "f325fdd8f936d76d3d9944358380cff64d0db66e545f99a3cc01ab97"
    }
  ],
  "có sẵn": [
    {
      "_name tài sản ": "6e7466636f696e",
      "số lượng": 10,
      "chính sách _id ": "f125fdd8e336d56d3d9943117380cff64d0db66e545f99a3cc01ab97"
    }
  ]
}
```

Còn về việc đổi Token hoặc loại bỏ nhiều tài sản không mong muốn khỏi ví cardano thì sao ? Token được tạo bằng chính sách đúc tiền tuân thủ một bộ nguyên tắc. Ví dụ: chính sách đúc có thể cho phép chủ sở hữu Token ghi hoặc tạo Token mới. Nếu bạn nhận được các Token không mong muốn, bạn thường phải trả lại chúng cho người phát hành hoặc người gửi hoặc lưu trữ chúng ở một nơi khác để bảo vệ. Để biết thêm thông tin về các chính sách đúc tiền, hãy xem phần tài liệu về chính sách đúc tiền.⁴³⁴

Lưu ý rằng việc truyền bất kỳ số lượng tài sản gốc nào cũng tốn một ADA cộng với phí giao dịch ở mức tối thiểu. Để biết thêm chi tiết về các yêu cầu UTXO tối thiểu, hãy xem phần yêu cầu giá trị ADA tối thiểu trong tài liệu.⁴³⁵

⁴³⁴

Chính sách khai thác và sổ cái đa tài sản, cardano-ledger.readthedocs.io/en/latest/explanations/policies.html

⁴³⁵

Tùy chọn 1 : Trả lại Token cho người gửi hoặc người phát hành:

1. Xác nhận địa chỉ của người gửi /người phát hành .
2. Trong cardano -wallet, hãy tạo một giao dịch JSON với UTXO tối thiểu là một ADA và bao gồm nội dung gốc.

Giao dịch mẫu để gửi nhiều tài sản:

```
curl -XPOST http://localhost:8090/v2/wallets/{wallet_id}/transactions \
H "Loại nội dung: application/ json \; bộ ký tự = utf-8"
d "{
  "thanh toán": [
    {
      "địa chỉ":"{ địa chỉ đích }",
      "số tiền ":{
        "số lượng":5000000,
        "đơn vị":" tình yêu "
      },
      "tài sản": [
        {
          "_id chính sách ":" property_policy_id ",
          "_name tài sản ": "6e7436436f646e",
          "số lượng": 5
        }
      ]
    },
    "cụm mật khẩu":" mylittlepony "
  ]
}
```

Xác nhận rằng giao dịch nhiều tài sản đã hoàn tất và tài sản đã rời khỏi ví.

vỏ sò

cuộn tròn <http://localhost:8090/v2/wallets>

4. Bạn sẽ thấy kết quả sau:

```
"tài sản": {
"tổng cộng": [],
"có sẵn": [ ] }
```

Tùy chọn 2 : Di chuyển Token đến một địa chỉ bên trong ví hiện có:

1. Xác nhận rằng bạn có Token gốc trong ví.
2. Chỉ định một địa chỉ từ ví để gửi Token.
3. Làm theo các bước trong Tùy chọn 1 để gửi Token đến một địa chỉ.
4. Theo dõi địa chỉ chứa nội dung gốc.

Nhiệm ýt tài sản bản địa trên một sàn giao dịch

Nhiều tài sản gốc hiện đang hoạt động trên Cardano và những tài sản mới đang được bổ sung thường xuyên. Một số tài sản bản địa này đã hoạt động tốt trên thị trường, nơi các thành viên cộng đồng và tổ chức tài chính đã thể hiện sự quan tâm và đầu tư. Có một danh sách không đầy đủ các nội dung gốc trên CardanoAssets.com .

Công khai với tài sản bản địa

Người tạo Token có hai tùy chọn để cung cấp Token của họ cho công chúng:

yêu cầu giá trị ADA tối thiểu,
cardano-ledger.readthedocs.io/en/latest/explanations/min-utxo-mary.html?highlight=minimum%20ADA%20value%20requirement

1. Bán nội dung gốc một cách riêng tư trong đợt bán Token hoặc
2. Liệt kê nội dung gốc trên một sàn giao dịch đồng thời tuân thủ các chính sách và nguyên tắc của sàn giao dịch.
3. Các nền tảng của bên thứ ba như Dripdropz , 'Hệ thống phân phối Token Cardano'

Bán Token cá nhân

Các nhà sản xuất tài sản bản địa muốn bán Token của họ một cách riêng tư nên thực hiện nghiên cứu và thẩm định trước khi quyết định cách tốt nhất để thực hiện.

Niêm yết trên thị trường của một sàn giao dịch

Các nhà phát triển nội dung gốc có thể chọn liệt kê và bán Token của họ trên một sàn giao dịch. Khi nói đến việc niêm yết Token, mỗi sàn giao dịch có bộ quy định, tiêu chuẩn và luật riêng.

Từ quan điểm kỹ thuật, IOG có thể hỗ trợ mọi thắc mắc. IOG có thể trợ giúp những việc như tạo, đúc và đốt Token, nhưng mọi thắc mắc về quy trình niêm yết phải được xử lý cho sàn giao dịch thích hợp. Quy trình niêm yết khác nhau tùy theo trao đổi, ví dụ. Kraken,⁴³⁶ Coinbase hoặc Binance .⁴³⁷ Nếu bạn dự định niêm yết một tài sản gốc trên một sàn giao dịch, thì tốt nhất bạn nên nói chuyện trực tiếp với sàn giao dịch đó trước.

Hỗ trợ kỹ thuật: Khi nói đến hỗ trợ kỹ thuật cho các sàn giao dịch, Cardano Foundation là đầu mối liên hệ ban đầu. Nếu bạn gặp bất kỳ sự cố hoặc khó khăn kỹ thuật nào, hãy liên hệ với họ qua các kênh hỗ trợ tiêu chuẩn hoặc gửi yêu cầu hỗ trợ.

Triển khai hợp đồng thông minh

Alonzo đã xây dựng dựa trên các cải tiến Token của Cardano để cung cấp cho các nhà phát triển các công cụ họ cần để tạo DApps thương mại. IOG đã đặt nền móng cho Cardano trở thành nền tảng hợp đồng thông minh hàng đầu bằng cách giới thiệu siêu dữ liệu giao dịch,⁴³⁸ khóa mã hóa⁴³⁹ với *Allegra* vào tháng 12 năm 2020 và phát hành Token gốc.⁴⁴⁰ Ngay sau đó là *Mary* , một bản cập nhật giao thức đa tài sản vào tháng 3 năm 2021 cho phép người dùng tạo Token gốc cho các giao dịch Cardano.

Các tính năng này đã được tích hợp vào Alonzo, bản cập nhật giao thức tiếp theo vào tháng 9 năm 2021. Alonzo đã đóng góp chức năng cho hợp đồng thông minh (thỏa thuận kỹ thuật số) cho Cardano, tận dụng công nghệ kết hợp hard fork của IOG. Bằng cách tạo điều kiện thuận lợi cho việc xây dựng các hợp đồng thông minh và ứng dụng phi tập trung (DApps) cho tài chính phi tập trung (DeFi), nó đã mang đến những khả năng mới cho các nhà phát triển.

Tiến trình của Cardano với tư cách là một sổ cái phân tán toàn cầu tiếp tục với các hợp đồng thông minh. Khi nói đến thương mại thông thường, một Blockchain phải đảm bảo rằng mọi người có thể chuyển tiền của họ và thanh toán hàng hóa một cách an toàn.

Hợp đồng thông minh có thể được sử dụng để giải quyết các giao dịch phức tạp, giữ tiền trong tài khoản ký quỹ và chuyển tiền an toàn theo các tiêu chí được xác định trước. DApps có thể giao tiếp với sổ cái của Cardano để theo dõi các hành động của họ và thực hiện các hợp đồng thông minh. Các thỏa thuận kỹ thuật số này kể câu chuyện về một giao dịch, chỉ định tiền sẽ được chuyển đến đâu và chúng sẽ được chuyển trong những trường hợp nào và chỉ hoàn tất một thỏa thuận nếu tất cả các yêu cầu đã được đáp ứng. Cardano có thể xử lý các ứng dụng như vậy nhờ *Alonzo* .

Alonzo đã trình bày một khuôn khổ linh hoạt để xây dựng các hợp đồng thông minh, trong khi hỗ trợ đa tài sản cho phép người dùng thiết kế các loại tiền tệ độc đáo đáp ứng nhu cầu kinh doanh. Ví dụ: hiện có thể sưu tầm, cung cấp dịch vụ cộng đồng và đấu giá.

⁴³⁶ Quy trình niêm yết Kraken, support.kraken.com/hc/en-us/articles/360001388206-New-coin-listing-requests

⁴³⁷ Quy trình niêm yết Binance , binance.com/en/support/faq/053e4bdc48364343b863d1833618d8ba

⁴³⁸ Alan McSherry, 'Mang lại giá trị và tiện ích mới cho Blockchain Cardano', iohk.io/en/blog/posts/2020/10/29/bring-new-value-and-utility-to-the-cardano-blockchain/

⁴³⁹ Kevin Hammond, 'Goguen mang khóa Token đến Cardano', iohk.io/en/blog/posts/2020/12/02/goguen-brings-token-locking-to-cardano/

⁴⁴⁰ Tim Harrison, 'Xây dựng Token gốc trên Cardano vì niềm vui và lợi nhuận', iohk.io/en/blog/posts/2021/02/18/building-native-tokens-on-cardano-for-pleasure-and-profit/

Có thể khám phá việc triển khai các sàn giao dịch Crypto phi tập trung (DEX) dựa trên ký quỹ hoặc phát triển các ứng dụng phức tạp hỗ trợ các stablecoin tập trung. Người dùng có thể sử dụng khóa Token để tạo Token tiện ích với thời gian trao quyền, nghĩa là Token có thể bị khóa hoặc đóng băng trong một khoảng thời gian nhất định trước khi được phát hành.

Xác thực bằng chữ ký và tập lệnh

Xác thực các hành động đang được thực hiện là một phần quan trọng trong việc thực hiện một giao dịch. Khi dữ liệu trong trường cụ thể cho hành động đó được cung cấp trong một giao dịch, nó được coi là đang thực hiện hành động. Khi một giao dịch có tham chiếu đến 'U' trong trường đầu vào của nó, thì giao dịch đó đang sử dụng UTXO 'U' và khi trường đầu ra của nó chứa 'X', thì nó đang đúc Token 'X'.

Khi một Node xử lý một giao dịch, nó sẽ kiểm tra xem liệu nó có thể thực hiện hành động hay không. Đối với điều này, người tạo giao dịch phải cung cấp dữ liệu cần thiết, chẳng hạn như tập lệnh, người đối quả hoặc chữ ký. Chỉ tiêu UTXO bị khóa bằng khóa công khai là một ví dụ điển hình của hoạt động cần xác thực. Để hoàn thành bước này, giao dịch phải cung cấp chữ ký từ khóa riêng được liên kết.

Cardano xác thực các hành động thông qua tập lệnh. Mã trong các tập lệnh này triển khai các hàm Thuần túy với đầu ra Đúng hoặc Sai. Quá trình gọi trình thông dịch tập lệnh để thực thi một tập lệnh nhất định với các tham số đã cho được gọi là xác thực tập lệnh.

Viết kịch bản Plutus

IOG đã phát triển các công cụ và cơ sở hạ tầng thiết yếu với Alonzo để cho phép phát triển ứng dụng Nền tảng Plutus. Alonzo đã nâng cao ngôn ngữ kịch bản đa chữ ký cơ bản (multisig) của Cardano Shelley bằng một phương pháp nghiêm ngặt dựa trên các phương pháp và xác minh chính thức. Để có khả năng tạo tập lệnh phức tạp và an toàn hơn, Multisig đã được cập nhật thành ngôn ngữ Plutus Core. Số cái Alonzo sử dụng Plutus Core để kích hoạt tập lệnh nâng cao tận dụng mô hình kế toán đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO).

Nền tảng cho hợp đồng thông minh phải vừa an toàn vừa đáng tin cậy. Do đó, Haskell đã được chọn làm ngôn ngữ lập trình cho các hợp đồng thông minh Plutus Core. Haskell là ngôn ngữ lập trình cấp cao được các nhà phát triển sử dụng để viết mã, sau đó được biên dịch thành Plutus Core.⁴⁴¹

Haskell đã xuất hiện từ năm 1987 và nó nổi bật trong số các ngôn ngữ máy tính vì mức độ đáng tin cậy cao. Các hợp đồng thông minh được viết bằng Haskell và Plutus được thiết kế để thực hiện chính xác những gì được mong đợi ở chúng và có thể được kiểm tra tính chính xác trước khi thực hiện. Điều này đảm bảo rằng các hợp đồng thông minh được viết trên Cardano sẽ đơn giản và an toàn, điều này rất quan trọng đối với các ứng dụng quản lý giao dịch tự động hoặc chuyển tiền quy mô lớn.

Công cụ và API

Trên Cardano, các nhà phát triển có thể kiểm tra và điều chỉnh xác thực giao dịch bằng các công cụ chức năng. Mã Plutus Core được triển khai và chạy trên Cardano trong khi giao tiếp với ví và sổ cái, cùng với phần mở rộng của thư viện API.⁴⁴²

Công nghệ hợp đồng thông minh nào hiện đang có sẵn?

Trong số 18.000 ⁴⁴³loại Crypto hiện nay, chỉ có 70 loại có hợp đồng thông minh theo CryptoSlate.⁴⁴⁴ PolkaDot, Solana và Ethereum nằm trong số những người tham gia thị trường hỗ trợ hợp đồng thông minh. Công nghệ đang thay đổi để phù hợp với nhu cầu của thị trường về các hệ thống nhanh chóng, an toàn, chính xác và đáng tin cậy. Nhiều công ty đã cố gắng cài đặt các ứng dụng quy mô lớn

⁴⁴¹

Michael Peyton Jones, 'Plutus Tx: biên dịch Haskell thành Plutus Core',
iohk.io/en/blog/posts/2021/02/02/plutus-tx-compiling-haskell-into-plutus-core/

⁴⁴²

Thư viện API, github.com/input-output-hk/cardano-node/tree/master/cardano-api _

⁴⁴³

ADAm Hayes, '10 loại Crypto quan trọng khác ngoài Bitcoin', investopedia.com/tech/most-important-cryptocurrency-other-than-bitcoin/

⁴⁴⁴

Tiền hợp đồng thông minh CryptoSlate, cryptoslate.com/cryptos/smart-contracts/

trên các nền tảng này và gặp phải ' sự cố '. Ví dụ: vụ hack DAO,⁴⁴⁵ lỗi Parity và vụ hack lỗ sâu Solana tồi tệ⁴⁴⁶ khiến 320 triệu đô la bị mất tích. Bất chấp các vụ hack và kéo thăm tái diễn,⁴⁴⁷ các vấn đề nghiêm trọng nhất trong hợp đồng thông minh vẫn tiếp tục xuất hiện.⁴⁴⁸ Có rất nhiều không gian cho sự đổi mới ở đây và IOG đang nỗ lực để khẳng định mình là người dẫn đầu trong lĩnh vực này.

Đồng thời không vấn đề

đồng thời là gì?

Đồng thời có thể nâng cao hoặc gây hại cho hiệu suất, thông lượng và khả năng đáp ứng của hệ thống. Số lượng hoạt động đồng thời tối đa có thể được thực thi bị giới hạn bởi mức độ đồng thời. Bộ xử lý hoặc các tác nhân khác trong Blockchain dựa trên UTXO sẽ có thể thực hiện một số hoạt động cùng lúc để đạt được lợi ích hiệu suất thực sự. Khả năng song song tối đa có thể đạt được tăng lên khi số lượng đồng thời tăng lên. Kết quả của chiến lược này là hiệu suất và thông lượng tăng lên. Nó cũng có một số lợi ích so với các hệ thống dựa trên tài khoản như Ethereum.

FUD

Ngay sau khi các hợp đồng thông minh được giới thiệu với hard fork Alonzo, đã có một loạt các meme và cáo buộc sai lầm rằng Cardano chỉ có thể xử lý một giao dịch tại một thời điểm do các vấn đề tương tranh.⁴⁴⁹ Một phân tích khách quan chỉ có thể kết luận rằng đây là FUD (sợ hãi, không chắc chắn và nghi ngờ) được lan truyền chủ yếu bởi các đối thủ Cardano.

Giải quyết FUD đồng thời, Charles Hoskinson đã sử dụng sự tương tự giữa bộ xử lý lõi đơn và bộ xử lý đa lõi:⁴⁵⁰

Phép loại suy mà tôi muốn sử dụng ở đây là khi chúng ta chuyển từ bộ xử lý lõi đơn sang bộ xử lý đa lõi. Bạn sẽ thấy tiếp thị lõi kép, lõi tứ, 8 lõi, 16 lõi, điều đó có nghĩa là phần mềm bên trong thực sự phải được viết khác đi một chút để tận dụng tính song song. Nếu bạn không làm điều đó, bạn có thể có 16 lõi, 32 lõi .. nhưng chỉ một lõi thực sự được sử dụng, một luồng sẽ được sử dụng trong ứng dụng đó, trừ khi ứng dụng được viết lại cho nó. Sau đó, hơi thiếu trung thực khi nói, 'ồ, intel' là lừa đảo ... ARM là lừa đảo và AMD là lừa đảo... họ đã nói dối chúng tôi rằng họ nói 16 lõi, nhưng tôi chỉ sử dụng một lõi'. Chà, đó là một thứ tùy thuộc vào phần mềm, chúng ở đó, bạn có thể truy cập chúng, có các mẫu thiết kế để làm điều đó. Ngày nay chúng ta đã trở nên tốt hơn rất nhiều so với khi thế giới lõi kép xuất hiện, nhưng bạn vẫn cần đưa tính song song vào mã của mình để làm được điều đó.

Một hoặc nhiều đầu vào có thể được sử dụng trong một giao dịch Blockchain, cũng như một hoặc nhiều đầu ra. Nếu một người muốn nắm bắt cách thức hoạt động của một giao dịch và cách nó liên quan đến mô hình kế toán Đầu ra giao dịch chưa chi tiêu (UTXO), thì trước tiên người đó phải hiểu ý tưởng về đầu vào và đầu ra. Hãy coi một giao dịch là hoạt động mở khóa các đầu ra trong quá khứ đồng thời tạo ra các đầu ra mới.

đầu ra giao dịch

Một địa chỉ (mà bạn có thể coi là khóa) và một giá trị được bao gồm trong đầu ra giao dịch. Theo sự tương tự này, chữ ký của địa chỉ là chìa khóa mở khóa đầu ra. Đầu ra có thể được sử dụng làm đầu vào sau khi đã được mở khóa. Các giao dịch mới sử dụng đầu ra của

⁴⁴⁵

Giải thích về vụ tấn công DAO: Hợp đồng thông minh không may cất cánh, oguculturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562

⁴⁴⁶

Hơn 320 triệu đô la bị đánh cắp trong vụ hack Crypto rõ ràng mới nhất, cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html

⁴⁴⁷Thâm kéo là một trò lừa đảo Crypto, trong đó những kẻ lừa đảo nói dối công chúng để thu hút vốn và nhanh chóng lấy đi tiền của nhà đầu tư và/hoặc Token kỹ thuật số.

⁴⁴⁸

Nikolic, Kolluri, Sergey, Saxena, Hobor (2018), Tìm kiếm các hợp đồng tham lam, hoang đường và tự sát trên quy mô lớn, arxiv.org/pdf/1802.06038.pdf

⁴⁴⁹

Người sáng lập Cardano giao dịch với FUD đồng thời, Sàn giao dịch thứ hai của Nhật Bản niêm yết \$ADA, cryptoglobe.com/latest/2021/09/cardano-founder-deals-with-concurrency-fud-a-second-japanese-exchange-lists-ADA/

⁴⁵⁰

Thông tin thêm về Đồng thời, youtu.be/OVh-eiACTzY?t=325

các giao dịch trước đó đồng thời tạo ra các đầu ra mới có thể được sử dụng bởi các giao dịch tiếp theo. Mỗi UTXO chỉ có thể được sử dụng một lần và nó phải được tiêu hóa toàn bộ. Chỉ một đầu vào có thể sử dụng mỗi đầu ra.

Đầu vào giao dịch

Đầu ra của một giao dịch trước đó được gọi là đầu vào giao dịch. Một con trỏ và chữ ký mã hóa đóng vai trò là chìa khóa mở khóa được bao gồm trong đầu vào giao dịch. Khóa mở khóa đầu ra giao dịch trước đó và con trỏ tham chiếu trở lại giao dịch đó. Blockchain gắn nhãn một đầu ra được mở khóa là 'đã tiêu' khi nó được mở khóa bằng một đầu vào. Sau đó, các đầu vào mới có thể đề cập đến các đầu ra mới được tạo ra bởi một giao dịch nhất định và chuỗi tiếp tục. UTXO là đầu ra mới (chưa được mở khóa / chi tiêu). Như tên ngụ ý, đầu ra chưa chi tiêu là đầu ra chưa được chi tiêu.

Nhiều giao dịch

Có một số điểm cần lưu ý khi gửi nhiều giao dịch. Khi mempool đầy, những người dùng cần gửi lần lượt nhiều giao dịch có thể gặp sự cố. Điều này được gọi là 'thông lượng cao'. Một số giao dịch có thể không được phê duyệt nếu người dùng tiếp tục gửi giao dịch sau khi mempool đầy. Hệ thống chưa bao giờ đảm bảo một giao dịch có thể được gửi một cách đáng tin cậy. Trong một hệ thống phân tán như Cardano, rất khó để đưa ra một sự đảm bảo như vậy. Logic gửi lại phải được xử lý thích hợp bằng cách gửi các đại lý.

cardano -submit- api là điểm cuối thích hợp để sử dụng. Chủ đề bị tạm dừng khi mempool đầy. Do đó, người dùng API có thể xếp hàng một số giao dịch, các giao dịch này sẽ được xử lý ngay khi có dung lượng mempool. Tuy nhiên, ứng dụng phải tính đến thực tế là số lượng giao dịch trên chuyến bay bị hạn chế bởi số lượng tệp mở tối đa của hệ điều hành. Nếu đạt đến giới hạn này, cardano -submit- api chỉ cần thoát và không có yêu cầu nào được xử lý nữa. Sử dụng *ulimit*⁴⁵¹ để tăng số lượng tệp mở được hệ điều hành cho phép sẽ tăng số lượng giao dịch trên chuyến bay khả dụng, giảm tắc nghẽn UTXO.⁴⁵²

Để tránh yêu cầu quản lý hàng đợi phức tạp, bạn có thể sử dụng cardano -submit- api nối tiếp hoặc với tính đồng thời cực thấp.⁴⁵³

Nguyên tắc chung là sự đơn giản thúc đẩy khả năng phục hồi; nếu trường hợp sử dụng của bạn cho phép, chỉ cần gửi một giao dịch tại một thời điểm và đợi giao dịch đó được xác minh trước khi chuyển sang giao dịch tiếp theo.

Cách eUTXO xử lý đồng thời trên Cardano

Mô hình eUTXO trong Cardano cung cấp một môi trường an toàn và có thể thích ứng để xử lý nhiều hoạt động mà không gặp sự cố hệ thống. Cardano là một Blockchain dựa trên UTXO sử dụng mô hình lập trình khác với các Blockchain dựa trên tài khoản hiện có như Ethereum cho các ứng dụng phi tập trung (DApps). Cardano sử dụng mô hình Đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO), được triển khai với bản cập nhật *Alonzo*. Do đó, eUTXO cung cấp một giải pháp riêng biệt để song song hóa, cho phép tăng cường bảo mật và khả năng dự đoán chi phí (không có những cú sốc khó chịu) trong quá trình thực thi hợp đồng thông minh.

Kiến trúc mỗi nhánh của mô hình UTXO (Bitcoin) được chuyển sang eUTXO, trong đó một nhánh được xác định là một chuỗi các giao dịch yêu cầu xác thực liên tiếp. Xây dựng DApps và các giải pháp khác với nhiều UTXO là rất quan trọng để phân chia chức năng trên các nhánh khác nhau và thực thi tính song song bổ sung. Điều này có lợi thế về khả năng mở rộng, giống như việc tạo ra các dịch vụ Bitcoin bắt buộc phải chia một ví thành các ví phụ.

Cardano DApps không bị giới hạn chỉ một giao dịch trên mỗi khối. Trên thực tế, ngân sách khối (số lượng giao dịch tối đa mà nó có thể thực hiện) cho phép thực hiện đồng thời hàng trăm giao dịch đơn giản và nhiều tập lệnh phức tạp. Mặt khác, phương pháp eUTXO chỉ cho phép chi tiêu đầu ra của giao dịch một lần. Bởi vì người dùng có thể gặp phải tranh chấp khi cố gắng truy cập cùng một UTXO, điều quan trọng là phải sử dụng nhiều loại UTXO. Điều này rất quan trọng trừ khi kiến trúc sẽ đạt được từ một thứ tự nghiêm ngặt của khách hàng. Các mẫu thiết kế liên quan đến semaphores⁴⁵⁴ có thể được triển khai bằng cách sử dụng các bộ UTXO.

⁴⁵¹

ulimit là lệnh shell Linux tích hợp cho phép xem hoặc giới hạn lượng tài nguyên hệ thống mà người dùng cá nhân sử dụng. Hạn chế sử dụng tài nguyên có giá trị trong môi trường có nhiều người dùng và các vấn đề về hiệu suất hệ thống.

⁴⁵²

Tắc nghẽn UTXO: Hiệu ứng của nhiều giao dịch cố gắng sử dụng cùng một đầu ra giao dịch.

⁴⁵³

Đồng thời, thuộc tính của chương trình, thuật toán hoặc phân tách vấn đề thành các đơn vị độc lập theo thứ tự hoặc theo thứ tự một phần.

⁴⁵⁴

Semaphore là một biến hoặc kiểu dữ liệu trừu tượng, được sử dụng để kiểm soát quyền truy cập vào một tài nguyên chung theo nhiều luồng và tránh các sự cố phân quan trọng trong hệ thống đồng thời, chẳng hạn như hệ điều hành đa nhiệm. Semaphores là một loại nguyên thủy đồng bộ hóa. Một semaphore tầm thường là một biến đơn giản được thay đổi tùy thuộc vào các điều kiện do lập trình viên xác định.

Hơn nữa, một số người dùng có thể tương tác với một hợp đồng thông minh duy nhất mà không gây ra sự cố tương tranh. Điều này là do hợp đồng thông minh có thể quản lý nhiều loại UTXO tạo nên trạng thái hiện tại của nó, cũng như siêu dữ liệu ngoài chuỗi cho phép diễn giải các UTXO đó.

song song

Blockchain cung cấp tính bất biến và minh bạch trong xử lý giao dịch. Để giải quyết yêu cầu ngày càng tăng về xử lý hoạt động an toàn nhưng hiệu quả, mọi hệ thống Blockchain nên có các thuộc tính sau:

- **Thông lượng:** số lượng quy trình mà một hệ thống có thể hoàn thành trong một khoảng thời gian nhất định. Điều này đề cập đến số lượng giao dịch hoặc hợp đồng thông minh được hoàn thành trong một giây, ví dụ:
- **Hiệu suất hệ thống:** hệ thống hoạt động nhanh như thế nào. Thời gian thực hiện của một giao dịch hoặc hợp đồng thông minh được đo bằng hiệu suất.
- **Khả năng mở rộng:** khả năng xử lý nhiều quy trình của hệ thống mà không làm quá tải mạng hoặc ảnh hưởng đến hiệu suất.

Thông lượng của hệ thống có thể được nâng lên trong khi vẫn duy trì tốc độ của các hoạt động riêng lẻ bằng cách tăng tính song song, nhưng loại khả năng mở rộng này sẽ luôn bị hạn chế bởi một số mức độ tranh chấp.

Đồng thời, song song và tranh chấp là tất cả các cân nhắc của hệ thống khi nói đến khả năng mở rộng. Đồng thời là cần thiết để một số tác nhân thực hiện một công việc mà không làm phiền lẫn nhau. Tính song song cho phép sự phát triển như vậy được thực hiện đồng thời mà không can thiệp lẫn nhau. Xung đột xảy ra khi các tác nhân khác nhau hoạt động đồng thời hoặc song song và can thiệp lẫn nhau.

Khởi chạy DApps trên sổ cái UTXO

Cách tiếp cận của Cardano đối với việc triển khai DApp là duy nhất, với một đường cong học tập dốc đòi hỏi một cách tiếp cận mới. Việc chọn từ nhiều ngôn ngữ lập trình cũng tương tự như vậy: thường có một mục tiêu cuối cùng duy nhất để triển khai một thứ gì đó, nhưng có rất nhiều ngôn ngữ bạn có thể sử dụng để đạt được mục tiêu này.

Tối ưu hóa đồng thời là một năng lực cần phải thành thạo. Các nhà phát triển phải viết mã theo cách hạn chế sự tranh chấp (ví dụ: tránh các trạng thái được chia sẻ và theo dõi các phụ thuộc ngẫu nhiên). Sự đồng thời này sau đó phải được chuyển thành song song bởi hệ thống. Một số nhà phát triển (chẳng hạn như SundaeSwap⁴⁵⁵) trước đây đã tìm ra cách tiếp cận vấn đề này, trong khi những người khác hiện đang nghiên cứu chúng. Vào tháng 4 năm 2022, DEX sáng tạo của WingRiders (wingriders.com) đã được ra mắt thành công.⁴⁵⁶ Không thể áp dụng trực tiếp các kỹ năng tương tự đã học được trên một Blockchain khác vào các hợp đồng thông minh của Plutus. Đường cong học tập dốc, nhưng lợi ích lớn hơn nỗ lực.

Trong mọi trường hợp, điều quan trọng cần nhớ là nhà phát triển không thể chỉ sử dụng hợp đồng Ethereum được điều chỉnh để xây dựng DApp có thể mở rộng trên Cardano. Cardano sử dụng mô hình UTXO thay vì mô hình dựa trên tài khoản. Do đó, một trạng thái trên chuỗi duy nhất sẽ không đáp ứng thuộc tính đồng thời trên Cardano. Thay vào đó, các DApp nên phân phối trạng thái trên chuỗi của chúng trên một số UTXO. Do đó, tính đồng thời của ứng dụng của họ sẽ phát triển, cho phép thông lượng lớn hơn.

liên minh UTXO

IOG hợp tác với các Blockchain dựa trên UTXO khác để phát triển các giải pháp mới giúp cải thiện khả năng tương tác, khả năng lập trình và khả năng mở rộng. IOG đã công bố hợp tác với Ergo (ergoplatform.org), Nervos (nervos.org) và Topl (topl.co) để thành lập liên minh UTXO trong Hội nghị thượng đỉnh Cardano năm 2021.⁴⁵⁷ Sau đó, họ mời Komodo (komodoplatform.com), Alephium (alephium.org) và DigiByte (digibyte.org) cũng tham gia liên minh.

⁴⁵⁵

Blog SundaeSwap về đồng thời, sundaeswap.finance/posts/concurrency-state-cardano

⁴⁵⁶

WingRiders dựa trên Cardano đạt 44 triệu đô la TVL trong vòng 24 giờ sau khi ra mắt, thecryptobasic.com/2022/04/13/cardano-based-dex-wingriders-hits-44-million-tvl-within-24-hours-of-launch/

⁴⁵⁷

Thông báo liên minh UTXO, Summit.cardano.org/sessions/taking-outputs-as-inputs

Liên minh UTXO sẽ giúp các hoạt động xuyên hệ sinh thái mở rộng khả năng hợp đồng thông minh của UTXO. Mục tiêu chung của việc hợp tác với các sáng kiến khác trong lĩnh vực Blockchain là kích thích và hỗ trợ nghiên cứu, phát triển và giáo dục hơn nữa trong toàn bộ khu vực.

Mục đích của liên minh UTXO là giữ cho mô hình UTXO phát triển về khả năng tương tác, khả năng mở rộng (sharding ,⁴⁵⁸ các kênh trạng thái, v.v.) và các giải pháp hợp đồng thông minh. Cải thiện các giải pháp này và dẫn dắt các dự án lớn để phát triển cầu nối qua các Blockchain cho phép mọi người có quyền truy cập vào tài chính toàn cầu công bằng và dễ tiếp cận. Điều này cũng cung cấp một nỗ lực hợp tác để thúc đẩy số cái dựa trên UTXO trong ngành. Bitcoin rõ ràng là Blockchain UTXO nổi tiếng nhất nhưng các sản phẩm phụ như Bitcoin Cash, Litecoin và Zcash nằm trong số các dự án khác sử dụng phương pháp này.

Xây dựng những cây cầu

Thay vì phụ thuộc vào những người trung gian đắt đỏ, công nghệ Blockchain giải quyết những khó khăn của việc tập trung hóa bằng cách cho phép các giao dịch ngang hàng đáng tin cậy dựa trên xác minh mật mã. Để tạo ra một môi trường an toàn và phi tập trung cho các giao dịch tài chính, một số giải pháp Blockchain đã được phát triển. Mặc dù các sáng kiến này khác nhau về giao thức đồng thuận, mô hình kế toán và cách tiếp cận hợp đồng thông minh, nhưng tất cả chúng đều tập trung vào các trường hợp sử dụng tương tự.

Tăng trưởng DeFi⁴⁵⁹ đã nhất quán và không có dấu hiệu chậm lại. Tuy nhiên, các hệ sinh thái bị phân mảnh, các tiêu chuẩn quản trị khác nhau, các phiên bản công nghệ và hỗ trợ tính năng đã làm chậm quá trình phát triển của môi trường Blockchain. Dự báo của Nasdaq về Tăng trưởng DeFi được chia sẻ bởi Romain Pellerin, giám đốc công nghệ IOG:

Việc áp dụng Blockchain chính thống sẽ chỉ thông qua kết nối mạng, tương tự như cách Internet được xây dựng bằng cách kết nối mạng nội bộ và mạng ngoại vi.

Với suy nghĩ này, điều quan trọng là phải đảm bảo rằng toàn bộ lĩnh vực đang hướng tới khả năng tương tác. Người dùng sẽ có thể tương tác với nhau mà không bị ràng buộc bởi một số cái duy nhất, hợp đồng thông minh sẽ hoạt động trong nhiều bối cảnh khác nhau và các ứng dụng phi tập trung (DApp) phải tương thích đa nền tảng. Chỉ theo cách này, lĩnh vực Blockchain mới có thể phát huy hết tiềm năng của nó, dẫn đến việc tăng cường áp dụng.

Không có một kích cỡ phù hợp với tất cả

Liên minh UTXO cũng quan tâm đến khả năng lập trình Blockchain cho phép phát triển DApps và hợp đồng thông minh. Trên thực tế, các ngôn ngữ mới phải được tạo để thích ứng với quản lý lưu trữ dữ liệu và giao dịch cụ thể của mô hình UTXO (ví dụ: eUTXO của Ergo⁴⁶⁰ và Cardano). Antara, CKB-VM, ErgoScript và Plutus là các ngôn ngữ hợp đồng thông minh do các thành viên sáng lập của liên minh tạo ra. Để nhanh chóng mở rộng số lượng các trường hợp sử dụng có thể được thực thi trên các Blockchain dựa trên UTXO, các thành viên liên minh đang tập hợp chuyên môn và hợp tác trong việc phát triển các công nghệ đó.

Hơn nữa, các ngôn ngữ như vậy được xây dựng dưới dạng ngôn ngữ dành riêng cho miền (DSL) trên các ngôn ngữ lập trình được sử dụng rộng rãi như Scala, Haskell, C, JavaScript, Go, Rust và các ngôn ngữ khác. Tuy nhiên, những ngôn ngữ chính thống đó có thể không phải lúc nào cũng cung cấp tính bảo mật hoặc sự tiện lợi khi sử dụng mà các nhà phát triển hợp đồng thông minh tìm kiếm.

IOG đã chọn Haskell làm ngôn ngữ lập trình cho các hợp đồng thông minh Plutus để đảm bảo tăng cường bảo mật và khả năng xác minh mã. Để phát triển ứng dụng, nó là ngôn ngữ lập trình chức năng được sử dụng rộng rãi nhất. Haskell là một ngôn ngữ lập trình an toàn và đã được kiểm chứng chính thức. Về mặt chấp nhận, nó phù hợp với nhiều trường hợp sử dụng tài chính khác nhau, cung cấp khả năng chuyển khoản thanh toán nhanh chóng, kết quả chính xác và khả năng mở rộng. Về phân phối trạng thái và song song hóa để tăng khả năng mở rộng, phương pháp lập trình này hoạt động tốt bên trong mô hình UTXO.

Liên minh UTXO sẽ điều tra các tình huống tốt nhất để tạo ra một bối cảnh hợp đồng thông minh thống nhất, nơi một loạt ngôn ngữ lập trình có thể được xây dựng và sử dụng trên các nền tảng Blockchain khác nhau, có tính đến các sáng kiến phát triển khác nhau. Điều này sẽ rất quan trọng trong việc cho phép khả năng tương tác Blockchain nhiều hơn.

Khả năng mở rộng thực sự

⁴⁵⁸

Sharding chia toàn bộ mạng của công ty Blockchain thành các phân vùng nhỏ hơn, được gọi là 'phân đoạn'. Mỗi phân đoạn bao gồm dữ liệu riêng của nó, làm cho nó khác biệt và độc lập khi so sánh với các phân đoạn khác.

⁴⁵⁹

Tại sao quyền riêng tư và khả năng tương tác sẽ thúc đẩy tăng trưởng theo cấp số nhân trong DeFi, nasdaq.com/articles/why-privacy-and-interoperability-will-fuel-exponential-growth-in-defi-2021-03-04

⁴⁶⁰

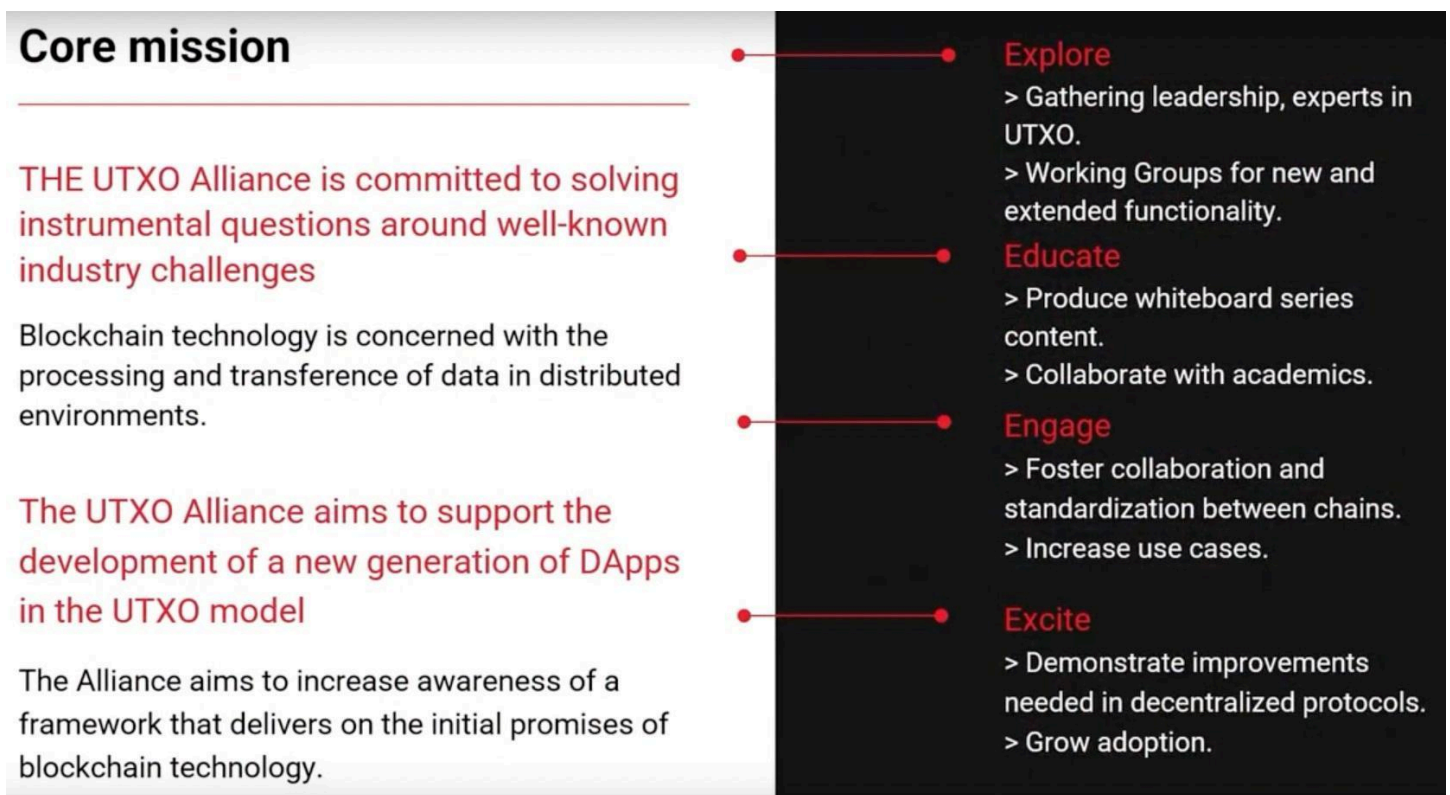
Học Ergo 101: giải thích eUTXO cho con người, dav009.medium.com/learning-ergo-101-blockchain-paradigm-eutxo-c90b0274cf5e

Điều quan trọng nữa là phải xem xét khả năng mở rộng tiềm năng của mạng về mặt xử lý giao dịch và thông lượng khi mạng mở rộng. Do mô hình UTXO dựa trên trạng thái cục bộ nên nó khác với mô hình dựa trên tài khoản và do đó cần một mô hình lập trình riêng biệt.

Hai mô hình này có các tính năng đa dạng và cung cấp sự đánh đổi khác nhau, những lợi ích và hạn chế khác nhau. Mô hình tài khoản thúc đẩy việc tạo các trường hợp sử dụng phụ thuộc vào trạng thái toàn cầu, nhưng mô hình UTXO đảm bảo tính xác định, khả năng dự đoán và khả năng mở rộng bằng cách quản lý các trạng thái cục bộ, nghĩa là các phần nhỏ của biểu đồ giao dịch tổng thể. Điều này làm mọi thứ chậm lại vì toàn bộ biểu đồ giao dịch cần được xử lý trước khi xác thực.

Do đó, kiến trúc UTXO có lợi thế là đảm bảo việc thực hiện các giao dịch và hợp đồng trước khi chúng được gửi tới Blockchain mà không có bất ngờ về phí hoặc xác thực. Ngoài ra, vì việc phân mảnh biểu đồ giao dịch dễ dàng hơn bằng cách chia nó thành một tập hợp các biểu đồ con, nên mô hình UTXO sẽ cho phép khả năng mở rộng cao hơn.

Việc tách một giao dịch cụ thể hoặc tập hợp các giao dịch (chuyển dữ liệu, tập lệnh và tài sản) và tiếp tục hoạt động ngoài chuỗi trước khi quay lại chuỗi chính với kết quả cũng đơn giản hơn, đảm bảo khả năng mở rộng bằng cách giảm tải các hoạt động ra khỏi chuỗi chính. Ví dụ, IOG đã tạo ra các giải pháp kênh trạng thái Hydra giúp tăng hiệu suất hệ thống đồng thời cho phép một số tác vụ diễn ra song song mà không làm giảm khả năng mở rộng. Để tìm hiểu thêm, hãy đọc về đồng thời ⁴⁶¹ trên Cardano. Hydra ⁴⁶² và các giải pháp khả năng mở rộng khác được đề cập trong Chương 8.



Hình 19: Slide từ bài nói chuyện 'Liên minh UTXO' của James Aman tại ScotFest

Cùng nhau là tốt hơn

Liên minh UTXO làm việc cùng nhau để cải thiện mô hình UTXO và thiết lập một tiêu chuẩn UTXO chung. Mục tiêu của nó là cung cấp nhiều tùy chọn cho chủ sở hữu ADA, người dùng Crypto, doanh nghiệp và cộng đồng phát triển không bị ràng buộc với một tiêu

⁴⁶¹

Olga Hryniuk , ' Đồng thời và tất cả những thứ đó: Hợp đồng thông minh Cardano và mô hình EUTXO ' ,
iohk.io/en/blog/posts/2021/09/10/concurrency-and-all-that-cardano-smart-contracts-and-the-eutxo-model/

⁴⁶²

Sebastian Nagel , ' Giải pháp của Hydra – Cardano cho khả năng mở rộng Lớp 2 cuối cùng ' ,
iohk.io/en/blog/posts/2021/09/17/hydra-cardano-s-solution-for-ultimate-scalability/

chuẩn cụ thể. Đối với điều này, liên minh sẽ thực hiện nghiên cứu học thuật và xuất bản một số bài báo hỗ trợ việc tạo ra các hợp đồng thông minh an toàn và có thể mở rộng bằng cách sử dụng kiến trúc UTXO.

Mặc dù khả năng tương tác là quan trọng, nhưng các giải pháp Blockchain cũng cần thiết để bảo mật tài chính tốt hơn, khả năng mở rộng quy trình xử lý giao dịch và tất nhiên là khả năng hợp đồng thông minh. Để cho phép sử dụng các chức năng đa dạng theo cách không liên quan đến Blockchain, liên minh được dành riêng để giải quyết các mối quan tâm quan trọng như:

- Cách truyền dữ liệu qua nhiều Blockchain một cách trơn tru
- Kích thước dữ liệu thích hợp cho các giao dịch là gì?
- Tốc độ xử lý dữ liệu nên là bao nhiêu?
- Phí giao dịch nên là bao nhiêu?

Do đó, liên minh đang tập trung vào việc phát triển một hệ thống cho phép các giao dịch trơn tru và an toàn trên nhiều Blockchain nhằm khuyến khích sử dụng rộng rãi hơn công nghệ Blockchain. Điều này cũng sẽ khuyến khích tạo ra các giải pháp DApps và DeFi đáng tin cậy. Đây mới chỉ là bước khởi đầu, vì Cardano đang xem xét hợp tác với các hệ sinh thái khác để nâng cao chế độ UTXO 1 và đóng góp cho nghiên cứu nguồn mở.

Chương 6: Sao Diêm Vương

'Không có người đàn ông trung thực! không ai có thể cưỡng lại sức hút của vàng!'

- Aristophanes

Chương này chỉ là tổng quan về Plutus. Để trở thành một chuyên gia, bạn chỉ cần biết một trang này: *Tài nguyên Plutus*⁴⁶³ kết nối bạn với mọi thứ đang diễn ra trong hệ sinh thái Plutus. Tài liệu hơi phân tán và thay đổi liên tục, chính xác là nó phải như thế nào đối với một ngôn ngữ lập trình đang phát triển. IOG phân loại hợp đồng thông minh và giao dịch tài chính thành hai kịch bản:

Trong một kịch bản, bạn muốn truyền đạt cảm giác chuyển giao giá trị từ tác nhân này sang tác nhân khác. (Các) hợp đồng tài chính phải thể hiện giá trị đó, cũng như các quy tắc và hoàn cảnh kiểm soát giá trị đó, cũng như sự kiện kích hoạt. Hợp đồng tài chính được triển khai tốt nhất với ngôn ngữ dành riêng cho miền.

Trong các tình huống khác, bạn muốn viết các chương trình, có thể nhằm phá vỡ một ngành công nghiệp, thay thế một tập đoàn lớn hoặc giải quyết một vấn đề nhỏ hơn.

Các ứng dụng này thường bao gồm ba điều:

- Máy khách là một phần của chương trình đang chạy trên máy tính của bạn
- Máy chủ là một máy tính (hoặc Node) hoạt động trên máy tính của người dùng khác (hoặc có thể là nhiều máy chủ)
- Hợp đồng thông minh là mã cho phép một hệ thống phi tập trung hoạt động.

Hai ngôn ngữ lập trình chính cho Cardano là:

- Plutus - nền tảng chính để viết mã DApps tương tác với Blockchain Cardano
- Marlowe - một ngôn ngữ dành riêng cho miền để xây dựng các hợp đồng tài chính, sẽ được thảo luận trong chương tiếp theo.

Sao Diêm Vương là gì?

Plutus là một nền tảng cung cấp ngôn ngữ hợp đồng thông minh bản địa cũng như cơ sở hạ tầng và công cụ hỗ trợ để thực hiện các hợp đồng thông minh trên Cardano.

Nền tảng Plutus cho phép các nhà phát triển tạo *DApp* tương tác với *số cái phân tán* có khả năng *tạo tập lệnh*. Đây là lý do tại sao nó là toàn bộ nền tảng, không chỉ là một ngôn ngữ. Nó không chỉ cung cấp một vài công cụ để thực hiện ở mức tối thiểu nhất có thể, nó hỗ trợ toàn bộ quá trình phát triển DApp, từ đầu đến cuối từ viết tập lệnh, đến thử nghiệm, hỗ trợ thời gian chạy và xác minh.

Để thành thạo Plutus, người ta phải nắm được ba khái niệm:

- Đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO)
- Mã trên chuỗi, Plutus Core, chạy trên Blockchain và được biên dịch bởi trình biên dịch Plutus
- Mã ngoại tuyến chạy trên thiết bị của người dùng. Khung ứng dụng Plutus (PAF) có thể được sử dụng để viết mã ngoài chuỗi, sau đó được biên dịch bởi GHC (Trình biên dịch Haskell của Glasgow)

Hợp đồng thông minh Plutus về cơ bản là các chương trình Haskell hoàn chỉnh Turing, với cả mã trên chuỗi và mã ngoài chuỗi được viết bằng Haskell. Bạn có thể chắc chắn rằng các hợp đồng thông minh của mình sẽ được thực hiện chính xác nếu bạn tuân theo phương pháp hay nhất với Plutus. Haskell là ngôn ngữ lập trình chức năng thuần túy hàng đầu và được xây dựng dựa trên nghiên cứu ngôn ngữ gần đây để tạo ra một môi trường phát triển toàn ngăn xếp an toàn.

Để hỗ trợ bạn bắt đầu, Plutus Playground⁴⁶⁴ bao gồm các hướng dẫn và hướng dẫn 'cách thực hiện'. Để hiểu thêm về ngôn ngữ Plutus, bạn nên đọc phần giải thích của Plutus.⁴⁶⁵ Nếu bạn muốn được hỗ trợ khi sử dụng Plutus, hãy tạo một vấn đề trong Kho Plutus⁴⁶⁶ bao gồm càng nhiều thông tin càng tốt.

⁴⁶³

Tài nguyên Plutus docs.cardano.org/plutus/ plutus-resources

⁴⁶⁴

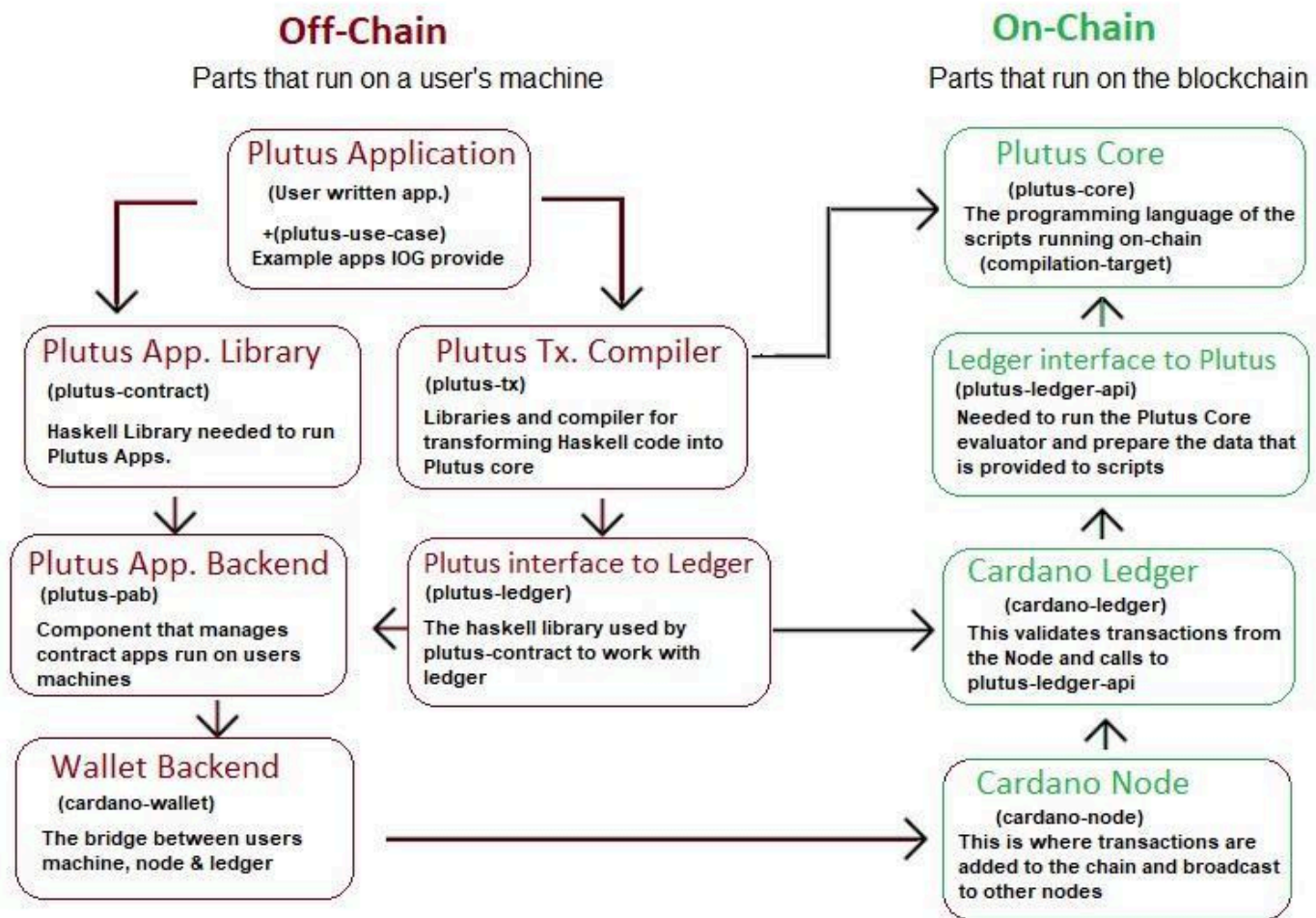
Sân chơi Plutus, [sân chơi.plutus.iohkdev.io/](https://plutus.iohkdev.io/)

⁴⁶⁵

Giải thích về Plutus, plutus-apps.readthedocs.io/en/latest/plutus/explanations/index.html

⁴⁶⁶

lưu trữ github của Plutus , github.com/input-output-hk/plutus



Hình 20: Plutus off-chain và on-chain

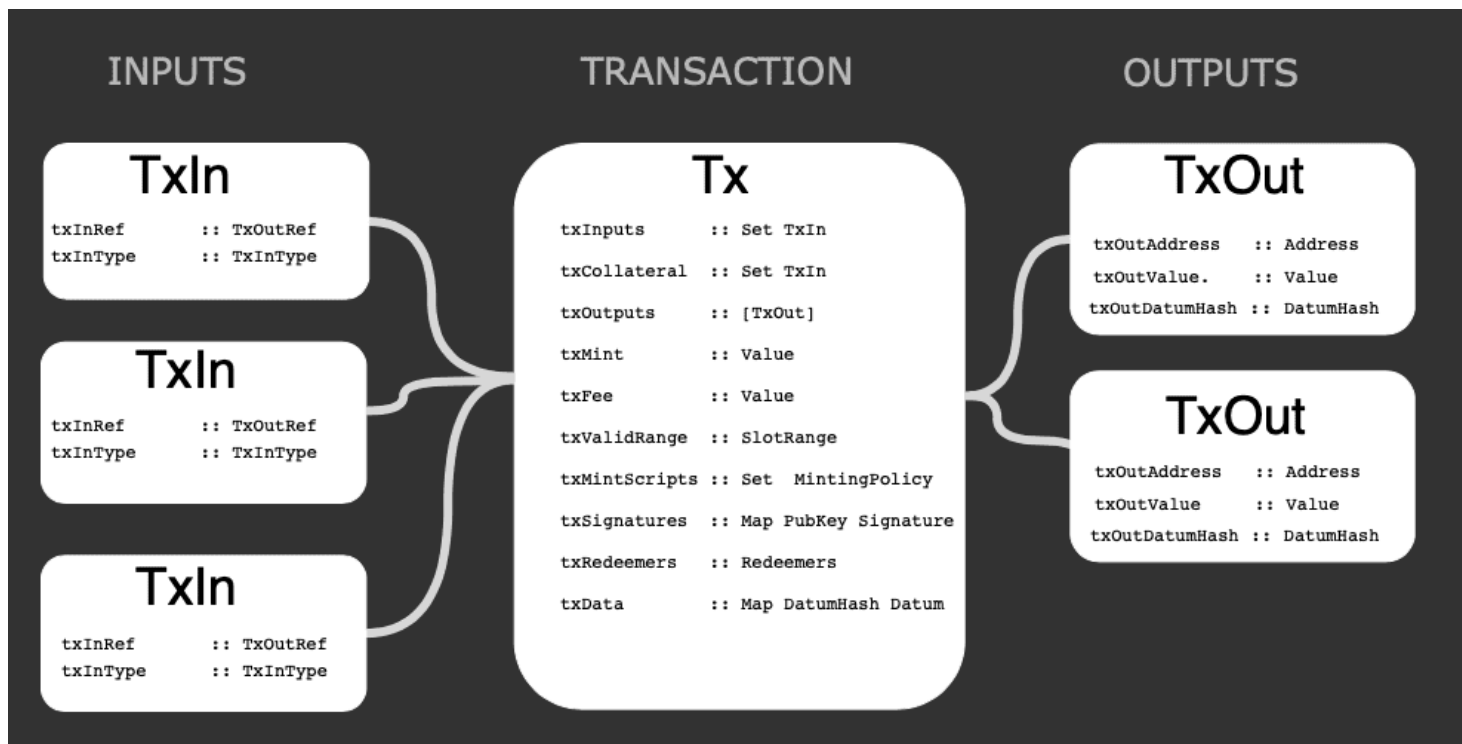
Plutus sử dụng UTXO mở rộng (eUTXO)

Cardano sử dụng mô hình kế toán UTXO mở rộng (eUTXO), mở rộng mô hình kế toán đầu ra (O) giao dịch (U) chưa chi tiêu (TX) của mô hình UTXO (được sử dụng bởi Bitcoin). Một giao dịch trong mô hình UTXO chứa đầu vào và đầu ra, với đầu vào là đầu ra chưa sử dụng từ các giao dịch trước đó. Khi một đầu ra được sử dụng làm đầu vào trong một giao dịch, nó được coi là đã sử dụng và không thể sử dụng lại. Một địa chỉ (khóa công khai hoặc hàm băm khóa công khai) và một giá trị được sử dụng để chỉ định đầu ra (bao gồm số lượng ADA và số lượng Token gốc bổ sung, tùy chọn).

eUTXO cải thiện kiến trúc UTXO bằng cách cho phép các địa chỉ đầu ra bao gồm logic phức tạp xác định giao dịch nào được phép mở khóa chúng, cũng như bằng cách thêm dữ liệu tùy chỉnh vào tất cả các đầu ra. So với các mô hình kế toán khác, mô hình này có những lợi ích khác biệt nhất định. Thành công hay thất bại của giao dịch chỉ được xác định bởi giao dịch và đầu vào của nó, không phải bởi bất kỳ thứ gì khác trên Blockchain. Do đó, trước khi một giao dịch được truyền đến Blockchain, giao dịch đó có thể được xác thực về tính hợp pháp ngoài chuỗi. Mặt khác, giao dịch được đảm bảo thành công nếu tất cả các yếu tố đầu vào vẫn còn.

Hoạt động của một giao dịch Plutus

Giao dịch là một phần dữ liệu có cả đầu vào và đầu ra và chúng có thể kết hợp các tập lệnh Plutus. Đầu ra chưa sử dụng từ các giao dịch trước đó (UTXO) được gọi là đầu vào. Một UTXO được sử dụng ngay khi nó được sử dụng làm đầu vào trong giao dịch và không thể sử dụng lại. Một địa chỉ (khóa công khai hoặc hàm băm khóa công khai) và một giá trị được sử dụng để chỉ định đầu ra (bao gồm số lượng ADA và số lượng Token gốc bổ sung tùy chọn). Sơ đồ luồng này giúp hiểu rõ hơn về các thành phần kỹ thuật của giao dịch:



Hình 21: Đầu vào và đầu ra của giao dịch

Tóm lại, đầu vào là tham chiếu đến các UTXO được giới thiệu bởi các giao dịch trước đó và đầu ra là các UTXO mới do giao dịch này tạo ra. Vì dữ liệu mới có thể được lưu trữ trong các đầu ra được tạo, điều này cho phép sửa đổi trạng thái của hợp đồng thông minh.

Plutus Tx đề cập đến các phần của chương trình Haskell được sử dụng để biên dịch thành phần trên chuỗi của ứng dụng hợp đồng thành Plutus Core (mã được biên dịch này sau đó được sử dụng để xác thực giao dịch, do đó có tên là 'Tx'). Biểu thức Plutus Core mà kết quả có thể được bao gồm trong dữ liệu giao dịch hoặc được lưu trong sổ cái. Tập lệnh Plutus đề cập đến một số đoạn mã nhất định cần xử lý cụ thể trên Blockchain. Bạn có thể quản lý luồng thực thi tập lệnh Plutus bằng cách sử dụng các giao dịch. Do đó, một giao dịch có thể được coi là một loạt các tin nhắn được gửi đến hợp đồng thông minh.

Trong khi đánh giá mã ngoài chuỗi, ví sẽ bắt đầu giao dịch. Sau khi giao dịch được gửi, nó sẽ được xác minh và một Node xác thực sẽ phân tích mã Plutus. Giao dịch sẽ được coi là hợp lệ nếu tập lệnh đánh giá chính xác. Nếu không thì giao dịch sẽ bị từ chối.

PAF có thể được sử dụng để viết mã ngoài chuỗi, sau đó được biên dịch bởi GHC (Trình biên dịch Glasgow Haskell), trong khi trình biên dịch Plutus biên dịch mã trên chuỗi (được viết trong Plutus Core). Điều quan trọng là phải nắm bắt được mối liên hệ giữa các nguyên tắc Plutus này và chức năng của Token gốc để nhận ra cách cái sau trở thành một tính năng mạnh mẽ hơn do sự tương tác của chúng.

lỗi Plutus

Ngôn ngữ lập trình của Cardano, Plutus Core, được sử dụng để xây dựng mô hình eUTXO. Các tập lệnh Plutus Core có thể được viết bằng một ngôn ngữ chức năng, súc tích có thể so sánh được với Haskell và một phần đáng kể của Haskell có thể được tận dụng. Bạn không viết Plutus Core với tư cách là một lập trình viên hợp đồng thông minh; Trên thực tế, bạn sẽ tạo tập lệnh trình xác thực trong Haskell, tập lệnh này sẽ được tự động biên dịch vào Plutus Core bằng trình cấm GHC (Trình biên dịch Haskell của Glasgow) có tên là Plutus Tx.⁴⁶⁷ Các tập lệnh này sẽ được chạy 'trực tiếp' trên chuỗi bởi các Node trong quá trình xác thực giao dịch. Họ sẽ sử dụng tập lệnh xác thực⁴⁶⁸ để mở khóa UTXO hoặc chính sách đúc để điều chỉnh việc đúc và đốt Token gốc.

Trong dấu hiệu của một hệ sinh thái trưởng thành, hiện có nhiều lựa chọn thay thế của bên thứ ba cho Plutus Tx. Chỉ một số trong danh sách đang phát triển là:

⁴⁶⁷

Plutus Tx : Thư viện và trình biên dịch để biên dịch Haskell thành Plutus Core để tạo thành phần trực tuyến của ứng dụng hợp đồng.

⁴⁶⁸của trình xác thực, docs.cardano.org/plutus/Plutus-validator-scripts

- **plu-ts**⁴⁶⁹ là thư viện cho phép phần mềm liên quan đến Cardano được viết hoàn toàn bằng TypeScript
- **Aiken**⁴⁷⁰ không phải là ngôn ngữ có mục đích chung. Nó được thiết kế riêng cho Cardano, cung cấp các công cụ dành cho nhà phát triển chất lượng cao.
- **Helios**⁴⁷¹ là một giải pháp thay thế không phải Haskell cho Plutus. Đó là Ngôn ngữ dành riêng cho miền (DSL) biên dịch thành Plutus-Core. Tất cả những gì bạn cần là thư viện Helios, được viết bằng Javascript, để biên dịch các tập lệnh Helios và xây dựng các giao dịch Cardano.
- **Sao Diêm Vương**⁴⁷² về cơ bản là Untyped Plutus Core (UPLC)⁴⁷³ với một chút đường cú pháp
- **Imperator**⁴⁷⁴ là một bằng chứng về ngôn ngữ mệnh lệnh khái niệm biến ngôn ngữ mệnh lệnh nhẹ thành Pluto
- **Plutarch**⁴⁷⁵ là một eDSL đã nhập (ngôn ngữ dành riêng cho miền nhúng) trong Haskell để viết các trình xác thực Plutus Core hiệu quả.
- **eopsin**⁴⁷⁶ là một triển khai của các hợp đồng thông minh Cardano được viết bằng một tập hợp con nghiêm ngặt của Python hợp lệ.
- **Cardano Multiplatform lib**⁴⁷⁷ là một dạng thư viện dcSpark, được viết bằng Rust, có thể được triển khai cho nhiều nền tảng (Rust crate, JS, TypeScript, WASM, v.v.)

dcSpark được thành lập bởi các nhà phát triển Emurgo và IOG trước đây và trong một khoảng thời gian ngắn, đã có những đóng góp đáng kể như ví *Flint* và Sidechain *Milkomeda*. dcSpark là những người tiên phong cho Cardano, thu hút các nhà phát triển tham gia vào không gian và đảm bảo có sự đa dạng trong hệ sinh thái chứ không phải là sự phụ thuộc quá mức vào IOG. Người dẫn chương trình và nhà giáo dục không gian Twitter, Bullish Dimpling, nhận xét:⁴⁷⁸

Tôi nghĩ sẽ tạo ra một câu hỏi đồ vui và khó như vậy để hỏi mọi người 'Vui lòng kể tên tất cả các sản phẩm mà dcSpark đã phát triển và đang phát triển...', họ đang làm rất nhiều thứ, rất nhiều thứ

Khung ứng dụng Plutus (PAF)

Trạng thái trên chuỗi của tập lệnh xác thực chỉ có thể được thay đổi bởi các giao dịch chi tiêu và tạo đầu ra tập lệnh. Khi thiết kế một ứng dụng Plutus, cả hai thành phần trên chuỗi (tập lệnh Plutus Core) và ngoài chuỗi (xây dựng và gửi giao dịch) đều phải được tính đến.

Không giống như Ethereum, nơi mã trên chuỗi được viết bằng Solidity trong khi mã ngoài chuỗi được viết bằng JavaScript, mã ngoài chuỗi của Cardano được viết bằng Haskell, giống hệt như mã trên chuỗi. Logic nghiệp vụ⁴⁷⁹ sẽ chỉ phải được viết một lần theo cách này. Sau đó, tập lệnh trình xác thực và mã tạo giao dịch thực thi tập lệnh trình xác thực có thể sử dụng lý do này.

Nhiều ứng dụng cần theo dõi bộ UTXO⁴⁸⁰ để biết các thay đổi đối với một số địa chỉ nhất định, vì vậy nếu hợp đồng được viết dưới

⁴⁶⁹

plu-ts, [github.com/ HarmonicLabs / plu-ts](https://github.com/HarmonicLabs/plu-ts)

⁴⁷⁰

Aiken, github.com/txpipe/aiken/ __

⁴⁷¹

Helios, github.com/hyperion-bt/helios __

⁴⁷²

Sao Diêm Vương, [github.com/Plutonomicon/sao Diêm Vương](https://github.com/Plutonomicon/sao-Diem-Vuong)

⁴⁷³

Plutus Tx: biên dịch Haskell thành Plutus Core, iohk.io/en/blog/posts/2021/02/02/plutus-tx-compiling-haskell-into-plutus-core/

⁴⁷⁴

Đế chế, [github.com/ ImperatorLang /imperator](https://github.com/ImperatorLang/imperator)

⁴⁷⁵

Plutarch, github.com/Plutonomicon/plutarch __

⁴⁷⁶Hợp đồng thông minh Cardano bằng Python, [github.com/ ImperatorLang / eopsin](https://github.com/ImperatorLang/eopsin)

⁴⁷⁷Multiplatform lib (CML), [github.com/dcSpark/cardano -multiplatform - lib](https://github.com/dcSpark/cardano-multiplatform-lib)

⁴⁷⁸

Ngày 28 tháng 12 năm 2022 : Tóm tắt về các dự án Cardano 2022, youtu.be/hx5TNM5U958?t=673

⁴⁷⁹

Logic nghiệp vụ hoặc logic miền là một phần của chương trình mã hóa các quy tắc nghiệp vụ trong thế giới thực xác định cách dữ liệu có thể được tạo, lưu trữ và thay đổi. Nó tương phản với phần còn lại của phần mềm có thể liên quan đến các chi tiết cấp thấp hơn.

⁴⁸⁰

Bộ **UTXO** là tập hợp toàn diện của tất cả các UTXO hiện có tại một thời điểm nhất định. Tổng số lượng của mỗi UTXO trong tập hợp này là tổng nguồn cung tiền tệ hiện có tại thời điểm đó. Bất kỳ ai cũng có thể xác minh tổng nguồn cung bất cứ lúc nào một cách không tin cậy.

dạng máy trạng thái, ⁴⁸¹bạn cần theo dõi đầu ra chưa sử dụng, phản ánh trạng thái hiện tại của máy và cập nhật trạng thái cục bộ của bạn nếu bất -chain thay đổi trạng thái. Nhiều ứng dụng cần giao tiếp với phần phụ trợ của ví để truy cập vào các quỹ Crypto mà chúng đang sử dụng cho các giao dịch. Plutus Application Framework (PAF) giúp việc truy cập các dịch vụ thường được các ứng dụng Plutus sử dụng trở nên đơn giản.

Chương trình phụ trợ ứng dụng Plutus (PAB)

Chương trình phụ trợ ứng dụng Plutus, cung cấp hỗ trợ thời gian chạy để truy cập vào Blockchain cũng như các mối quan tâm bổ sung như tính bền vững, ghi nhật ký và giám sát, có thể được sử dụng để thực thi các ứng dụng được xây dựng bằng thư viện của khung. Các ứng dụng được xây dựng trên PAF cung cấp ⁴⁸²giao diện HTTP và WebSocket cho phép người dùng tương tác với ứng dụng từ trình duyệt web.

Thành phần ngoại tuyến của Plutus được thực thi bởi PAB, được lặp lại liên tục sau mỗi lần phát hành. Nó xử lý các yêu cầu ứng dụng Node và phụ trợ ví, lưu trạng thái ứng dụng và cung cấp API HTTP để quản lý các phiên bản ứng dụng.

Token gốc và Plutus

Với Mary hard fork vào tháng 2 năm 2021, các Token gốc có thể truy cập được trên Cardano. Các Token, như ADA, có thể được tạo bởi bất kỳ ai và chúng có thể được chuyển và nhận một cách tự do.

Mỗi Token gốc có riêng chính sách đúc, ⁴⁸³chỉ định các trường hợp theo đó Token có thể được đúc và đốt. Người dùng tạo các chính sách đúc tiền trong Haskell và biên dịch chúng thành Plutus Core sau khi Plutus được triển khai. Trong quá trình đúc hoặc ghi, tập lệnh chính sách Plutus Core sẽ được chạy trong ngữ cảnh của giao dịch và nó sẽ phải phê duyệt hoặc từ chối hành động. Tính năng này đã thúc đẩy việc áp dụng Token không thể thay thế (CNFT) của Cardano bằng cách cho phép sử dụng các chính sách đúc tiền phức tạp hơn đáng kể và phát hành NFT không đáng tin cậy.

Chính sách đúc tiền được tạo thành từ một loạt các quy tắc cơ bản xác định chữ ký và khóa thời gian. Ví dụ: một chính sách có thể tuyên bố rằng các giao dịch chỉ có thể đúc hoặc đốt Token nếu chúng được ký bởi hai trong số năm chữ ký tiềm năng. Một chính sách khác chỉ có thể cho phép đúc tiền trước hoặc sau một thời gian nhất định.

Thế mạnh của Plutus

Plutus cung cấp các lợi ích bảo mật đáng kể. Nó cung cấp một phương pháp đơn giản hơn, đáng tin cậy hơn để chứng minh rằng các hợp đồng thông minh của bạn là chính xác và sẽ không gặp phải các vấn đề đã cản trở các thiết kế ngôn ngữ hợp đồng thông minh trước đây.

Plutus cho phép một cách tiếp cận tích hợp mới đối với hợp đồng thông minh và phát triển ứng dụng phân tán, dễ dàng và an toàn hơn so với các tùy chọn trước đó. Cùng một ngôn ngữ được sử dụng cho cả lập trình on-chain và off-chain. Bạn sử dụng một cơ sở mã chung, mà chuỗi công cụ Plutus ⁴⁸⁴phân chia thành các gói và mã trên chuỗi và ngoài chuỗi để triển khai. Plutus cũng cho phép Token do người dùng xác định (cả có thể thay thế và không thể thay thế) vốn cần ít mã hơn nhiều so với Ethereum.

⁴⁸¹

Máy trạng thái hữu hạn (FSM) hay đơn giản là **máy trạng thái**, là một mô hình tính toán toán học. Nó là một cỗ máy trừu tượng có thể ở chính xác một trong số hữu hạn trạng thái tại bất kỳ thời điểm nào. FSM có thể thay đổi từ trạng thái này sang trạng thái khác để đáp ứng với một số đầu vào bên ngoài và/hoặc một điều kiện được thỏa mãn; sự thay đổi từ trạng thái này sang trạng thái khác được gọi là quá trình chuyển đổi. Một FSM được xác định bởi một danh sách các trạng thái của nó, trạng thái ban đầu và các điều kiện cho mỗi lần chuyển đổi.

⁴⁸²

WebSocket là một giao thức truyền thông, cung cấp các kênh truyền thông song công hoàn toàn qua một kết nối TCP. Giao thức Điều khiển Truyền dẫn (TCP) là một trong những giao thức chính của bộ giao thức Internet. Nó bắt nguồn từ việc triển khai mạng ban đầu trong đó nó bổ sung cho Giao thức Internet (IP). Do đó, toàn bộ bộ thường được gọi là TCP/IP.

⁴⁸³

Chính sách đúc tiền,
github.com/input-output-hk/cardano-documentation/blob/staging/content/07-native-tokens/01-learn.mdx#minting-policy

⁴⁸⁴

Chuỗi **công cụ** là một tập hợp các công cụ lập trình được sử dụng để thực hiện một tác vụ phát triển phần mềm phức tạp hoặc để tạo ra một sản phẩm phần mềm, thường là một chương trình máy tính khác hoặc một tập hợp các chương trình liên quan.

Điểm khác biệt chính của eUTXO và Plutus là khả năng dự đoán của nó, thường được gọi là thuyết tất định. Tại ScotFest, ⁴⁸⁵James Aman (CTO của Topl) đã đặt ra cụm từ:

'Không phải đầu ra của bạn, không phải kết quả của bạn' bởi vì nếu bạn muốn một điều gì đó xảy ra trên thế giới, bạn cần đầu ra, điều thực tế đi vào trạng thái, để phản ánh mong muốn của bạn... bởi vì những kết quả đầu ra đó sẽ giúp bạn đạt được kết quả mong muốn

Tập lệnh Plutus

Cardano xác thực hoạt động thông qua tập lệnh. Các hàm thuần túy có đầu ra Đúng hoặc Sai được triển khai trong các tập lệnh này. Quá trình gọi trình thông dịch tập lệnh để chạy tập lệnh với các đối số có liên quan được gọi là xác thực tập lệnh. Tập lệnh là mã xác định xem giao dịch chi tiêu đầu ra có được chấp thuận hay không. Loại tập lệnh này được gọi là tập lệnh trình xác thực vì nó kiểm tra xem giao dịch có được phép hay không. Một tập lệnh trình xác thực đơn giản sẽ xác minh xem giao dịch chi tiêu có được ký bởi một khóa nhất định hay không, giống như các đầu ra trả tiền cho pubkey cơ bản. Các tập lệnh có thể được sử dụng để thể hiện logic có ý nghĩa trên chuỗi. Siêu dữ liệu và tập lệnh được nhóm lại với nhau trong một giao dịch để có thông lượng lớn hơn.

Mô hình eUTXO hoạt động bằng cách chuyển ba tham số cho tập lệnh trình xác thực:

- Dữ liệu: Đây là một phần dữ liệu được liên kết với đầu ra và bị khóa bởi tập lệnh (chỉ có hàm băm). Điều này thường được sử dụng để thực hiện trạng thái.
- Người chuộc lỗi: một phần thông tin liên quan đến đầu vào chi tiêu. Điều này thường được sử dụng để cung cấp thông tin đầu vào của người chi tiêu cho tập lệnh
- Bối cảnh: đây là siêu dữ liệu liên quan đến giao dịch chi tiêu. Điều này được sử dụng để đưa ra các xác nhận về cách gửi đầu ra (ví dụ: 'John đã ký cái này'). Bối cảnh có thể được tạo thành từ đầu vào (đầu ra từ các giao dịch trước đó sẽ được chi tiêu), đầu vào tham chiếu (chỉ dành cho giới thiệu, không được chi tiêu), đầu ra mới, phí, giá trị đúc, chứng chỉ, rút tiền thưởng, phạm vi ngày, chữ ký giao dịch, người mua lại, bản đồ băm dữ liệu, ID giao dịch).

ví dụ đơn giản

Một khách hàng 'John' muốn mua 'Cardano cho Masses' có giá A10. Phải có xác nhận rằng họ có đủ A trong ví trước khi có thể mua.

```
nếu ĐủADA ( book= CardanoForTheMasse , khách hàng=john) :
    muaSách ( )

def ĐủADA ( sách, khách hàng ) :
    trả lại khách hàng["số dư"] >= sách[" giá sách "]

def buyBook ( ) :
    print ("Bạn có đủ ADA để mua cuốn sách")

CardanoForTheMasses = {" giá sách ":A 10}
john = {"số dư ":A 11}
```

Trong ví dụ trên:

- Dữ kiện là thông tin về giao dịch này: *john.balance*
- Bối cảnh là trạng thái của thế giới, tại thời điểm đó có nghĩa là: *CardanoForTheMasses.bookPrice*
- Người mua lại, là hành động để thực hiện: *buyBook ()*

Tập lệnh trình xác thực là chức năng sử dụng tất cả thông tin đó, trong ví dụ này là *EnoughADA*

IOG's GitHub chứa các ví dụ về tập lệnh xác thực trên mọi hợp đồng thông minh:

⁴⁸⁵

- Hướng dẫn giao dịch Plutus⁴⁸⁶
- Plutus Xin Chào Thế Giới⁴⁸⁷
- Tiên phong Plutus English Auction⁴⁸⁸

Thông số mô hình chi phí

Một số tham số trong mô hình chi phí cho tập lệnh Plutus Core cũng được bao gồm trong tham số giao thức Cardano. Cài đặt cá nhân có thể được điều chỉnh bởi các nhà phát triển.

Xem phần sau để biết thêm chi tiết:

- Danh sách các tham số mô hình chi phí và mô tả ngắn gọn của chúng⁴⁸⁹
- Các nguồn để tìm hiểu thêm về ý nghĩa của các tham số⁴⁹⁰

Phiên bản Plutus

Cardano, giống như bất kỳ Blockchain nào khác, là một sổ cái hoặc cơ sở dữ liệu phi tập trung theo dõi tất cả các giao dịch và khối được tạo trên mạng. Cơ sở dữ liệu này phân phối hồ sơ với tất cả những người tham gia và đồng bộ hóa với hoạt động Blockchain một cách thường xuyên để cung cấp dữ liệu minh bạch và cập nhật cho bất kỳ ai. Theo thuật ngữ của giáo dân, sổ cái chỉ là một hệ thống theo dõi ai sở hữu cái gì.

Cardano DB Sync⁴⁹¹ truy xuất thông tin Blockchain đó và cho phép người dùng chạy các lệnh CLI để truy cập chi tiết giao dịch và khối. Bạn có thể sử dụng Cardano Explorer – giao diện người dùng đồ họa hiển thị thông tin một cách đơn giản – để phân tích dữ liệu dễ dàng và thân thiện với người dùng hơn.

Trước khi một giao dịch được gửi đến một khối,⁴⁹² nó sẽ được xác thực bởi nhà sản xuất Block. Để tránh chi tiêu gấp đôi, người gửi phải có đủ tiền và tất cả các Node trên sổ cái phải thiết lập sự đồng thuận. Hãy xem cách điều này hoạt động trong sổ cái Shelley và cách các tập lệnh Plutus thay đổi nó để kích hoạt các giao dịch đa tài sản và hợp đồng thông minh.

Xác thực giao dịch trước Goguen

Khi một đầu ra được sử dụng làm đầu vào trong một giao dịch, nó được coi là đã sử dụng và không thể sử dụng lại. Sau đây là các tham số cho đầu ra:

- một địa chỉ chứa thông tin xác thực thanh toán và thông tin xác thực cổ phần tùy chọn, có thể là hàm băm khóa công khai/xác minh hoặc hàm băm tập lệnh. Ngoài ra, chúng chỉ cổ phần có thể là một liên kết đến giấy chứng nhận đăng ký.
- một giá trị: đây là số lượng ADA có thể được chi tiêu.

⁴⁸⁶

Mô hình giao dịch Plutus,

github.com/input-output-hk/Alonzo-testnet/blob/main/Alonzo-tutorials/Plutus_transactions_tutorial.md#transaction-to-lock-funds

⁴⁸⁷

Plutus HelloWorld,

github.com/input-output-hk/Alonzo-testnet/blob/e27563ec0c3723376f4d12881cd003a7a7157f/resources/plutus-sources/plutus-hello-world/src/Cardano/PlutusExample/HelloWorld.hs#L47

⁴⁸⁸

EnglishAuction.hs ,

github.com/input-output-hk/plutus-pioneer-program/blob/024ebd367bf6c4003b482bfb4c6db7d745ec85aa/code/week01/src/Week01/EnglishAuction.hs#L103

⁴⁸⁹

Tham số mô hình chi phí, plutus.readthedocs.io/en/latest/reference/cost-model-parameters.html

⁴⁹⁰

Thư mục Plutus, plutus.readthedocs.io/en/latest/reference/bibliography.html#id13

⁴⁹¹

Mục đích của **DB Sync** là theo dõi chuỗi Cardano và lấy thông tin từ chuỗi cũng như một bản sao trạng thái sổ cái được duy trì nội bộ. Dữ liệu sau đó được trích xuất từ chuỗi và chèn vào cơ sở dữ liệu PostgreSQL. Các truy vấn SQL sau đó có thể được viết trực tiếp vào lược đồ cơ sở dữ liệu.

⁴⁹²

Node Cardano , docs.cardano.org/new-to-cardano/cardano-nodes_

Chủ sở hữu khóa riêng tư (còn được gọi là khóa chữ ký), tương ứng với thông tin xác thực thanh toán được cung cấp trong địa chỉ, phải ký một giao dịch. Cardano Shelley chỉ hỗ trợ các giao dịch ADA. Đặc tả hình thức Shelley giới thiệu ý tưởng về tập lệnh đa chữ ký (multisig),⁴⁹³ được ghi lại hoàn toàn theo quy tắc sổ cái. Nếu một tổ hợp chữ ký được xác định trước được cung cấp, phương pháp đa chữ ký này cho phép sử dụng đầu ra giao dịch chưa sử dụng làm đầu vào cho một giao dịch mới.

Ví dụ: nếu hai người phải ký giao dịch cùng một lúc thì hai trong số ba chìa khóa phải được cung cấp, v.v. Multisig là một ngôn ngữ rất đơn giản cho phép bạn tương tác với RequireSignature, RequireAllOf, RequireAnyOf và RequireMOF, trong số các hàm tạo khác. Các tập lệnh nên được thiết kế để cho phép nhiều cụm từ hơn thể hiện nhiều điều kiện khác nhau khi chức năng của sổ cái phát triển.

Alonzo (Plutus V1)

Với việc giới thiệu hỗ trợ đa tài sản và hợp đồng thông minh trên Cardano, việc nâng cấp ngôn ngữ tập lệnh đa chữ ký cơ bản với các tùy chọn phức tạp hơn là bắt buộc. Là một phần của quá trình nâng cấp Alonzo, IOG đã triển khai các công cụ và cơ sở hạ tầng cần thiết, cũng như hỗ trợ ngôn ngữ lập trình mới có tên là Plutus Core.

Sổ cái Alonzo sử dụng mô hình đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO) để nâng cấp multisig lên Plutus Core nhằm cung cấp các tính năng tập lệnh mạnh mẽ.

Alonzo đã thực hiện các điều chỉnh sau đối với dữ liệu sổ cái:

1. Tập lệnh Plutus có thể khóa UTXO.
2. Chức năng giống như trạng thái tập lệnh đã được bật thông qua một thành phần mới được thêm vào nội dung của các phần đầu ra của UTXO. Một UTXO bị khóa bởi các tập lệnh Plutus bao gồm dữ liệu ngoài tài sản và địa chỉ. Dữ liệu chuẩn là một phần thông tin đại diện cho việc giải thích trạng thái tập lệnh.
3. Một số tham số giao thức mới đã được thêm vào để thực thi các yêu cầu xác thực giao dịch bổ sung. Chúng bao gồm các hạn chế cao hơn về mức độ xử lý tập lệnh có thể sử dụng.

Các giao dịch đã được cập nhật để hỗ trợ tập lệnh Plutus như sau:

1. Giao dịch hiện có một người mua lại, là thông số do người dùng chỉ định cho từng hoạt động của nó. Người chuộc lỗi có thể thực hiện nhiều chức năng khác nhau tùy thuộc vào tập lệnh. Ví dụ: nó có thể đóng vai trò là quyết định của người dùng để 'đánh' hoặc 'đứng' trong trò chơi xì dách hoặc 'thích' hoặc 'chia sẻ' trong một số DApp truyền thông xã hội phi tập trung không tưởng.
2. Giao dịch xác định ngân sách thực thi tính toán của mỗi tập lệnh.
3. Alonzo tận dụng tài sản thế chấp để xác minh rằng một giao dịch có thể thanh toán chi phí thực hiện của nó.
4. Các giao dịch bao gồm một hàm băm toàn vẹn, được sử dụng để xác nhận rằng nó không bị giả mạo, chưa hết hạn, v.v.

Node chạy các thử nghiệm dành riêng cho Alonzo để đảm bảo rằng giao dịch được tạo thành công. Ví dụ, nó không được vượt quá ngân sách tài nguyên thực thi tối đa. Nó cũng chạy các tập lệnh bằng cách sử dụng trình thông dịch tập lệnh Plutus.

Mô hình 'gas' không xác định của Ethereum có khả năng tính phí cao ngất ngưỡng cho người tiêu dùng. Hình thức không xác định này được giải quyết trong các tập lệnh Cardano bằng cách yêu cầu cả ngân sách tài nguyên và phí cần thiết để trang trải nó phải được đưa vào giao dịch. Khi thiết kế một giao dịch trong Alonzo, người dùng có thể dự đoán cả cục bộ. Quá trình thực thi tập lệnh sẽ luôn trả về một trong hai giá trị: Đúng hoặc Sai và sẽ không lặp lại vô tận. Điều này là do mọi hành động mà tập lệnh thực hiện đều yêu cầu một lượng tài nguyên khác không mà trình thông dịch sẽ theo dõi. Nếu vượt quá ngân sách của giao dịch, tập lệnh sẽ bị chấm dứt và Sai được trả về.

Các tính năng quan trọng sau đây giúp dự báo kết quả xác thực tập lệnh và giao dịch:

- Khi được áp dụng với các tham số giống nhau, trình thông dịch tập lệnh sẽ luôn kết thúc và cung cấp cùng một kết quả xác thực
- Trong quá trình xác thực, một giao dịch phải sửa tất cả các biến được cung cấp cho trình thông dịch tập lệnh
- Một giao dịch liệt kê tất cả các hoạt động mà nó thực hiện cần xác thực tập lệnh
- chữ ký bắt buộc của một giao dịch đảm bảo rằng nó không thể bị giả mạo bởi kẻ tấn công theo cách khiến các tập lệnh không thành công.

Trong mô hình sổ cái eUTXO, việc thực hiện một giao dịch mang tính quyết định.

⁴⁹³

Vasil (Plutus V2)

Có ba Đề xuất cải tiến Cardano được triển khai với hard fork Vasil để nâng cao cách thức hoạt động của Plutus, giúp mọi thứ dễ dàng hơn cho các nhà phát triển. Cả ba đều ăn khớp với nhau và bổ sung cho nhau.



Sebastien Guillemot
@SebastienGllmt

...

Pretty cool: 50% of the Cardano ledger changes for the upcoming Vasil upgrade were CIPs (Cardano Improvement Proposals)

Đầu vào tham chiếu đã xác định CIP31⁴⁹⁴, một bước tiến quan trọng về cách các nhà phát triển tương tác với UTXO. Đầu vào tham chiếu là đầu vào giao dịch được liên kết với một đầu ra giao dịch cụ thể, tuy nhiên, thay vì sử dụng đầu ra, nó chỉ tham chiếu đầu ra đó.

Một dữ liệu có thể được coi là dữ liệu cho tập lệnh của bạn, các bit dữ liệu được đính kèm với đầu ra, nơi bạn có thể lưu trữ dữ liệu như tên người dùng hoặc hình đại diện, v.v. Trước Vasil, nếu bạn muốn đọc tay cầm của mình hoặc tỷ số của một trận bóng đá match, v.v., trong DApp của bạn, bạn phải sử dụng UTXO và sau đó tạo lại nó sau khi bạn đã đọc dữ liệu.

Đầu vào tham chiếu cho phép bạn đọc dữ liệu chuẩn hoặc dữ liệu được lưu trữ tại UTXO mà không cần sử dụng và tạo lại dữ liệu đó. Điều này có nghĩa là nhiều DApp có thể đọc đồng thời từ cùng một dữ liệu. Điều này làm tăng tính đồng thời và thông lượng một cách đáng kể.

Ergo, những người tiên phong trong không gian UTXO, đã giới thiệu một khái niệm tương tự gọi là 'đầu vào dữ liệu'⁴⁹⁵ vào năm 2020.

CIP 32 xác định **dữ liệu nội tuyến**. Trước Vasil, điểm số cao này hoặc dữ liệu khác từ mốc thời gian không được lưu trữ trên chuỗi. Hàm băm (dấu vân tay) của nó được lưu trữ trên chuỗi và nhà phát triển có thể đưa nó vào khi họ tương tác với tập lệnh hay không. Kể từ Vasil, dữ liệu có thể được lưu trữ trên chuỗi, loại bỏ nhu cầu băm và tiến gần hơn đến một kiến trúc phi tập trung thực sự.

CIP 33 là về **kịch bản tham khảo**. Các tham chiếu tập lệnh Plutus có thể được liên kết với các đầu ra của giao dịch, cho phép chúng được lưu trữ trên chuỗi và sử dụng lại sau này. Điều đó có nghĩa là bạn không còn bắt buộc phải cung cấp một bản sao của tập lệnh với mỗi giao dịch, do đó giảm bớt trở ngại cho nhà phát triển. Sử dụng cùng một tập lệnh trong một số giao dịch sẽ giảm quy mô giao dịch, tăng thông lượng và giảm chi phí thực thi tập lệnh.

Trước Vasil, các nhà phát triển phải chia sẻ ngoại tuyến các tập lệnh để chúng có thể được đưa vào các giao dịch. Tuy nhiên, việc chia sẻ các tập lệnh đó với những người khác nhau để họ có thể tương tác với DApp của họ trở nên khó khăn hơn.

Các tập lệnh tham chiếu cho phép các nhà phát triển đưa các tập lệnh Plutus vào chuỗi và sau đó, thay vì đưa chúng vào một giao dịch, thay vào đó, họ có thể đưa một con trỏ vào giao dịch chỉ tham chiếu tập lệnh đó trên chuỗi hiện có. Điều đó có nghĩa là người dùng không cần phải có bản sao của tập lệnh này để tương tác với nó. Bạn chỉ cần cho mọi người biết địa chỉ của nó, sau đó người dùng ở bất cứ đâu có thể sử dụng cùng một tập lệnh và trỏ đến nó.

Điều này cho phép trường hợp sử dụng trong đó nhà phát triển có thể đặt các tập lệnh tham chiếu trên chuỗi và cho phép những người khác sử dụng chúng làm thư viện. Có thể có một số thư viện được coi là cốt lõi của Plutus và IOG sẽ đặt chúng ở nơi mọi người có thể sử dụng và sau đó công bố địa chỉ. Điều này cho phép bất kỳ ai trong hệ sinh thái lấy thư viện và cung cấp chúng cho công chúng rộng rãi hơn, một cải tiến mạnh mẽ.

⁴⁹⁴

CIP (Đề xuất cải tiến Cardano), cips.cardano.org/

⁴⁹⁵Đầu vào dữ liệu Ergo, docs.ergoplatform.com/dev/scs/data-inputs/

Nhìn vào cả ba CIP một cách tổng thể, những cải tiến này đã thúc đẩy Plutus tiến lên và giúp cuộc sống của các nhà phát triển trở nên dễ dàng hơn. IOG đang đưa nhiều hơn vào chuỗi, giải phóng các nhà phát triển khỏi nhu cầu giám sát tập lệnh và chia sẻ tập lệnh cũng như dữ liệu và tăng tính đồng thời bằng cách cho phép người dùng tương tác với UTXO.

CIP 49: Chữ ký ECDSA và Schnorr trong Plutus Core⁴⁹⁶

Được biết đến trong nội bộ là bản cập nhật 'SEC P', CIP 49 đã được triển khai dưới dạng một hard fork Intra-era⁴⁹⁷ vào tháng 2 năm 2023.

Nguyên tắc mã hóa giống như các Block Lego được sử dụng để tạo giao dịch an toàn và phát triển thuật toán khi xây dựng DApps. Chúng có thể là bộ tạo số ngẫu nhiên, nguồn entropy (tính ngẫu nhiên), bộ nhớ cơ bản hoặc các phép toán được thuật toán mã hóa yêu cầu.

Trước khi tiếp tục, chúng ta hãy sắp xếp lại một số thuật ngữ:

Thuật toán Chữ ký số Đường cong Elliptic hoặc *ECDSA* là một sơ đồ mật mã để tạo chữ ký bằng cách sử dụng khóa công khai và khóa riêng. Nó sử dụng một biến thể của chữ ký Schnorr dựa trên các đường cong Edwards xoắn. Vậy chữ ký Schnorr là gì?

Chữ ký *Schnorr* là chữ ký điện tử được tạo bởi thuật toán chữ ký Schnorr được mô tả bởi Claus Schnorr. Nó được biết đến với tính đơn giản, hiệu quả và tạo chữ ký ngắn.

Secp256k1 là tên của đường cong elip được sử dụng bởi Bitcoin, Ethereum và các loại khác để triển khai mật mã khóa công khai của nó. Trong khi Cardano, Monero, Ripple và những người khác sử dụng đường cong elip *edwards25519* làm cơ sở cho việc tạo cặp khóa của họ. Đường cong đến từ *Ed25519* sơ đồ chữ ký.

Ban đầu, hard fork Vasil là để thêm hỗ trợ tích hợp cho *secp256k1* trên Cardano, cho phép các nhà phát triển tương tác với chữ ký từ các Blockchain khác đó. Tuy nhiên, sau khi thử nghiệm rộng rãi, Vasil đã quyết định loại bỏ cải tiến này. Vì bản nâng cấp này ảnh hưởng đến trình thông dịch Plutus nên nó cần được triển khai dưới dạng một bản hard fork. Sau Vasil, người ta đã quyết định rằng các bản cập nhật trong tương lai sẽ chỉ được lên lịch nếu các chỉ số khối lượng quan trọng nhất định được đáp ứng. Một tỷ lệ phần trăm SPO đã đặt sẽ cần chạy Node mới. Trao đổi sẽ cần phải được tư vấn. Tác động đến các thành phần Cardano khác sẽ cần được đánh giá. *Cexplorer.io/versions* là một trang tốt để theo dõi 'sự sẵn sàng của hard fork'.

Như Nigel Hemsley (Trưởng bộ phận giao hàng của IOG) đã giải thích trong một tập Cardano350,⁴⁹⁸ lần này cộng đồng tham gia nhiều hơn vào chu kỳ phát hành. Các phiên bản gốc đã trải qua quá trình thử nghiệm rộng rãi trên môi trường devnet, xem trước và tiền sản xuất trước khi được đẩy lên mạng chính dưới dạng sự kiện kết hợp hard fork.

Những thay đổi, được nêu trong CIP 49, cho phép các nhà phát triển DApp xây dựng hiệu quả các ứng dụng chuỗi chéo với cầu nối, Sidechain và tài sản được bao bọc. Chức năng mới rất quan trọng đối với các cầu nối với Sidechains và các giải pháp tương tác khác như *Wanchain*.⁴⁹⁹ Các nguyên mẫu này được hỗ trợ dưới dạng các chức năng tích hợp sẵn có trong Cardano, được triển khai và kiểm tra bởi các chuyên gia bảo mật. Điều này mang lại cho nhà phát triển Plutus nhiều lựa chọn hơn. Ví dụ: các thiết kế dựa trên Schnorr đã được thiết lập tốt và được cộng đồng DApp rộng lớn hơn chấp nhận.

Như thường thấy với Cardano, phép loại suy giúp hiểu rõ hơn. Emmanuel (@thepizzaknight)⁵⁰⁰ đã tặng món quà ngày đầu năm mới này:

Đối với mục đích của chủ đề này, coi Crypto Primitives là họ ngôn ngữ trong thế giới thực, hãy sử dụng họ ngôn ngữ Ấn-Âu. Cardano sử dụng Curve25519, nghĩ tiếng Đức (tiếng Anh, Deutsche, v.v.) Ethereum, Bitcoin, v.v. sử dụng SECP256k1, nghĩ về ngôn ngữ Lãng mạn (tiếng Pháp, tiếng Tây Ban Nha, v.v.). Như bạn có thể tưởng tượng, việc kinh doanh giữa một người nói tiếng Anh với một người nói tiếng Tây Ban Nha có thể khó khăn. Bạn phải thuê người phiên dịch và trải qua rất nhiều công việc chỉ để hoàn thành công việc. Đây là những gì nó giống như bây giờ đối với những người xây dựng dApp (và

⁴⁹⁶CIP 49: Chữ ký ECDSA và Schnorr trong Plutus Core,
github.com/mlabs-haskell/CIPs/blob/c5bdd66fe49c19c341499f86cebaa2eef9e90b74/CIP-0049/README.md

⁴⁹⁷

Hard fork trong thời đại là một thay đổi ngữ nghĩa nhỏ và tập trung đối với số cái yêu cầu một hard fork.

⁴⁹⁸Nigel Hemsley (Cardano 360 tháng 10 năm 2022), youtube.com/watch?v=hZRwLWKNNfQ&t=257s

⁴⁹⁹Wanchain, chuỗi Mạng diện rộng, là một giải pháp về khả năng tương tác với sứ mệnh thúc đẩy việc áp dụng Blockchain thông qua khả năng tương tác giữa các chuỗi bằng cách xây dựng các cầu nối phi tập trung hoàn toàn kết nối các mạng Blockchain bị cô lập

⁵⁰⁰ thepizzaknight _ phép loại suy nguyên thủy ,
twitter.com/thepizzaknight_/status/1609373418759012353?s=20&t=2BonGRIWcKofrMSWJe4qYg

Bridge) trên Cardano đang cố gắng chuyển sang chuỗi chéo. Rất may, Sự kiện nâng cấp chuỗi tiếp theo đã khắc phục điều này bằng cách thêm hỗ trợ cho SECP256k1 dưới dạng chức năng Tích hợp trên Cardano (hãy coi đó là việc thêm một chuỗi DNA mới). Điều này sẽ cho phép Cardano (tiếng Anh) hiểu một cách tự nhiên các chuỗi khác (tiếng Tây Ban Nha). Điều này có ý nghĩa gì đối với bạn với tư cách là người dùng hoặc người xây dựng? Cơ hội chuỗi chéo mới với câu nói tốt hơn và quyền truy cập vào Token và dApp mới từ các chuỗi khác. Với chiến lược Sidechain, Cardano cần cải tiến này để tầm nhìn Khả năng tương tác của nó trở nên khả thi và thực tế.

Tương thích ngược

Sổ cái Cardano gắn thẻ tập lệnh bằng ngôn ngữ (V1 cho Alonzo, V2 là Vasil). Điều này chỉ ra cách sổ cái xử lý tập lệnh. Plutus V1 phải giữ nguyên như cũ mãi mãi, nếu không, bất kỳ ai cũng có thể thao túng các tập lệnh hiện có, có khả năng khiến đầu ra không thể sử dụng được và phá vỡ các giả định của người dùng. Vì lý do này, nếu Plutus cần cập nhật quan trọng, thì cần phải có ngôn ngữ 'mới' trong sổ cái.

Nói chung, mỗi hard fork sẽ tạo ra một 'phiên bản ngôn ngữ Plutus' mới với chức năng bổ sung. Từ quan điểm của sổ cái, chúng hoàn toàn không liên quan và không có yêu cầu rằng chúng phải giống nhau theo bất kỳ cách nào. Các tập lệnh cũ của bạn vẫn hợp lệ và sẽ hoạt động như trước. Bạn không bắt buộc phải sử dụng phiên bản ngôn ngữ mới, là phiên bản thay thế của phiên bản trước. Rõ ràng là bạn cần gắn thẻ tập lệnh của mình với phiên bản chính xác để tận dụng các tính năng mới, hãy xem 'phiên bản ngôn ngữ' trong tài liệu để biết thêm chi tiết.

Để hiểu những loại thay đổi nào yêu cầu phiên bản ngôn ngữ mới, hãy xem CIP 35–Plutus Core Evolution.⁵⁰¹

Các trường hợp sử dụng Plutus điển hình

Plutus thường được sử dụng cho các trường hợp sử dụng cấp cao sau đây, trong số các trường hợp khác:

- Nhà tiên tri — nhà tiên tri hoạt động đầy đủ tương tác và cung cấp hợp đồng thông minh bằng cách đưa dữ liệu ngoài chuỗi vào chuỗi. Oracles cũng cung cấp cho các ứng dụng Plutus nguồn cấp dữ liệu ngoài chuỗi tập trung và đáng tin cậy (ví dụ: nguồn cấp giá từ các sàn giao dịch tập trung khác nhau)
- Hoán đổi Token DEX — xây dựng một hệ thống trao đổi phi tập trung cho phép người dùng hoán đổi các Token được hỗ trợ. Người dùng có thể hình thành nhóm thanh khoản (hoặc đóng góp tiền cho những nhóm hiện có), sẽ cung cấp tiền để giao dịch. Họ có thể kiếm được phí cho bất kỳ giao dịch nào sử dụng tiền của họ để đổi lấy điều này. Người dùng cũng có thể quyên góp cho nhóm thanh khoản cho bất kỳ Token được hỗ trợ nào và kiếm tiền hoa hồng dưới dạng phí trao đổi để đổi lấy những nỗ lực của họ. Khi người dùng cung cấp thanh khoản cho một nhóm, người dùng sẽ được cấp một Token thanh khoản đại diện cho khoản tiền gửi. Phí phải được tính toán theo hợp đồng và sau đó được phân phối cho các nhà cung cấp thanh khoản dựa trên phần của mỗi nhà cung cấp trong nhóm thanh khoản
- Cho vay và vay - phát triển một giao thức cho vay cho phép người dùng cho vay và vay Crypto một cách an toàn và bảo mật, với lãi suất thay đổi và ổn định. Người dùng có thể tham gia với tư cách là người gửi tiền hoặc người đi vay. Người cho vay phải gửi tiền vào các nhóm thanh khoản để giao dịch và người đi vay phải vay từ các nhóm thanh khoản này. Người gửi tiền được thưởng bằng các Token có lãi suất. Để bảo vệ chống lại sự biến động, mỗi nhóm có một nhóm dự trữ
- NFT — phát triển chức năng cốt lõi để đúc, gửi và nhận NFT vào ví, cũng như các trường hợp sử dụng bổ sung
- Các công cụ tài chính phi tập trung (DeFi) — xây dựng bảng điều khiển đa chức năng (dựa trên web hoặc thiết bị di động) giao tiếp với các hợp đồng thông minh để cung cấp giá trị cho các nhà giao dịch Token gốc. Các giải pháp này có thể có nhiều bảng điều khiển chức năng hiển thị số dư Token và nhóm thanh khoản, trong số những thứ khác. Họ cũng có thể kết hợp nhiều dịch vụ vào một giao dịch duy nhất, chẳng hạn như hoán đổi và cung cấp thanh khoản, giúp việc áp dụng DeFi trở nên đơn giản hơn
- Đồng tiền ổn định được hỗ trợ bằng Crypto — tận dụng hệ thống ID phi tập trung Atala PRISM của Cardano để tạo ra một triển khai đồng tiền ổn định mới dựa trên tài sản thế chấp trên chuỗi. Các hạn chế chuyển giao, đóng băng tài sản và các biện pháp khác có thể được thực hiện.

⁵⁰¹

- Đồng tiền ổn định được thể chấp quá mức — nhóm COTI đã hợp tác chặt chẽ với nhóm Plutus của IOG khi triển khai đồng tiền ổn định Djed.

Công cụ Plutus

Các nhà phát triển có thể tận dụng nhiều công cụ khác nhau để đánh giá và thực hiện các hợp đồng thông minh trên Cardano.

Sân chơi Plutus

Các Plutus Playground là nơi các hợp đồng thông minh có thể được viết và thử nghiệm trước khi đưa vào Blockchain Cardano. Đó là một nền tảng dựa trên web để phát triển Plutus với mức tiêu thụ tài nguyên khiêm tốn. Plutus Playground cung cấp một trình mô phỏng dựa trên web để xây dựng và thực hiện các hợp đồng thông minh, cũng như quyền truy cập vào các hợp đồng thông minh phổ biến đã được phát triển.

Không cần cài đặt bất kỳ thứ gì để sử dụng Plutus Playground, có thể truy cập từ trình duyệt web. Giao diện người dùng được chia thành ba phần:

- biên tập viên
- giả lập
- giao dịch

Trình giả lập hiển thị cách một hợp đồng sẽ hoạt động trên Cardano. Một trong những phần quan trọng của điều này là nó có thể được sử dụng như một công cụ giảng dạy cho người mới bắt đầu. Các ví tương tác với hợp đồng, cũng như các hành động ảnh hưởng đến kết quả, có thể được xác định và cập nhật bởi người dùng. Sau đó, các kết quả có thể được phân tích để xác định điều gì xảy ra trên Blockchain và cách các giao dịch diễn ra. Tham quan Kho lưu trữ github của Plutus hoặc xem hướng dẫn biên dịch và thử nghiệm ứng dụng Plutus⁵⁰² để biết thêm chi tiết.

Phụ trợ ứng dụng Plutus

Khung ứng dụng Plutus (PAF) bao gồm Phần cuối ứng dụng Plutus (PAB), là cơ sở hạ tầng ngoài chuỗi trong mô hình UTXO tạo ra các giao dịch cung cấp năng lượng cho các DApp. Bởi vì nó phải xem xét trạng thái sổ cái, lấy một số thông tin từ sổ cái và kết hợp tất cả lại với nhau để tạo ra một giao dịch với các bit dữ liệu thích hợp ở đúng vị trí, kiến trúc ngoài chuỗi này hơi phức tạp. PAB là một thư viện Haskell giúp đơn giản hóa việc phát triển cả cơ sở hạ tầng ngoài chuỗi và tập lệnh trên chuỗi.

PAB hỗ trợ xây dựng các giao dịch UTXO theo hai cách:

- Đường dẫn đọc đòi hỏi phải truy xuất dữ liệu từ Blockchain và phản hồi các sự kiện xảy ra ở đó
- Đường dẫn ghi - Đây là nơi các giao dịch thực thi tập lệnh Plutus được xây dựng.

Plutus Application Backend (PAB) cung cấp các thành phần và môi trường cho phép các nhà phát triển giao tiếp với các hợp đồng thông minh, đồng thời thiết kế và thử nghiệm các DApp trước khi triển khai chúng vào môi trường sản xuất trực tiếp. Đó là một môi trường hộp cát, tương tự như Plutus Playground và Marlowe Playground,⁵⁰³ nơi các nhà phát triển có thể kiểm tra các tính năng DApp trước khi cam kết triển khai Cardano đầy đủ.

PAB giúp các nhà phát triển không cần phải xây dựng cơ sở hạ tầng của riêng họ từ đầu (bao gồm cả chỉ mục chuỗi,⁵⁰⁴ v.v.), cắt giảm thời gian phát triển. Nó cho phép các nhà phát triển mô hình hóa cách một ứng dụng sẽ hoạt động trên chuỗi để thử nghiệm và giảm lỗi trước khi khởi chạy, đảm bảo quá trình chuyển đổi diễn ra suôn sẻ.

Đó là một dịch vụ phụ trợ ngoài chuỗi quản lý và xử lý các yêu cầu của phiên bản ứng dụng trong suốt vòng đời của nó. Điều này liên quan đến việc tương tác với các ứng dụng khách bên thứ ba (chẳng hạn như giao diện người dùng của ví) và đóng vai trò là liên kết giữa các ứng dụng Plutus, Node, phần phụ trợ của ví và người dùng cuối. Các lệnh PAB và các thành phần giả cho phép dễ dàng mô phỏng và tích hợp DApps.

⁵⁰²

Plutus Playground - Video Hướng dẫn: Biên dịch và thử nghiệm Ứng dụng Plutus, youtube.com/watch?v=DhRS-JvoCw8

⁵⁰³

Sân chơi Marlowe, alpha.marlowe.iohkdev.io/#/

⁵⁰⁴

Chỉ số chuỗi là cơ sở dữ liệu thông tin thu được từ các giao dịch Cardano.

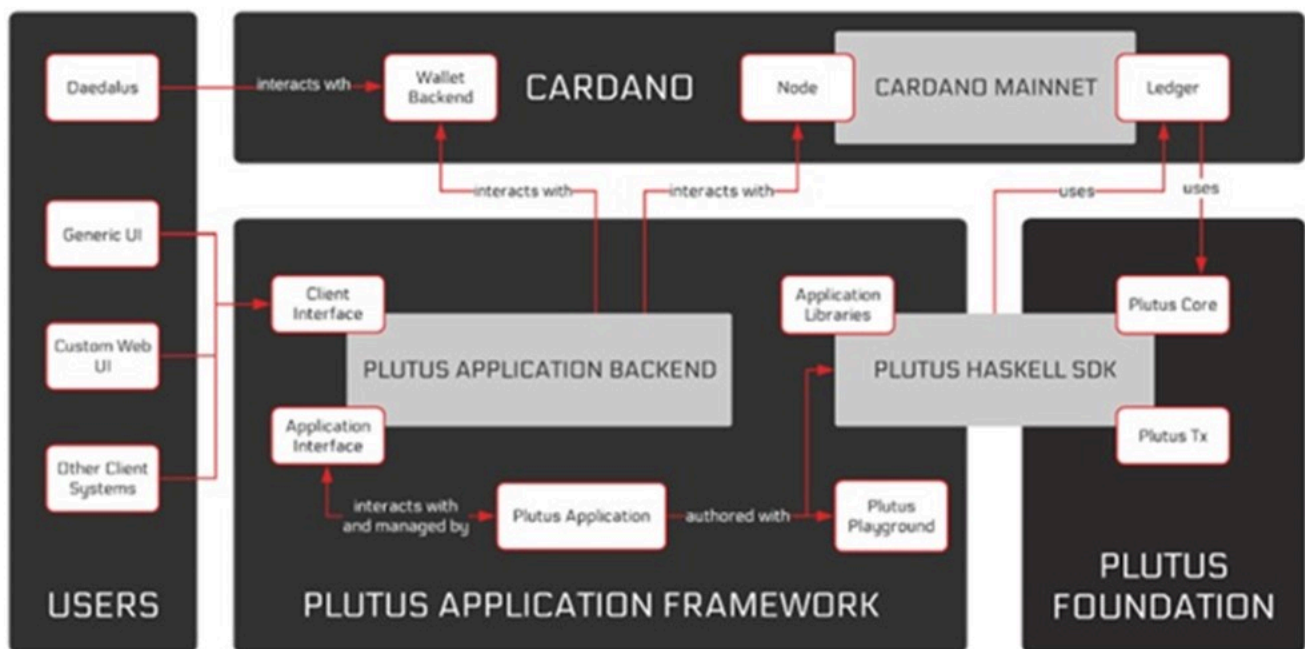
Nó hỗ trợ xây dựng các giao dịch UTXO cho cả tuyến đọc và ghi bằng cách lấy thông tin từ chuỗi, phản hồi các sự kiện và tạo các giao dịch thực thi các tập lệnh Plutus.

Mục tiêu chính của PAB là:

- cung cấp một môi trường tiêu chuẩn cho các ứng dụng Plutus chạy trong đó
- đề nghị quản lý nhà nước kỹ luật
- cung cấp cho khách hàng bên ngoài các giao diện có thể khám phá
- theo dõi dữ liệu trên chuỗi cho các ứng dụng hợp đồng thông minh
- giúp các nhà phát triển có thể hoạt động trong môi trường mô phỏng hoặc không mô phỏng
- xử lý các yêu cầu như bắt đầu các phiên bản hợp đồng, chuyển thông tin đầu vào của người dùng đến các phiên bản này và thông báo cho các phiên bản này về các thay đổi trạng thái sổ cái.

PAB có thể dễ dàng chuyển đổi giữa bối cảnh mô phỏng và không mô phỏng (mạng thực). Điều này làm cho việc viết các loại bài kiểm tra khác nhau - bài kiểm tra đơn vị, bài kiểm tra tích hợp, bài kiểm tra dựa trên thuộc tính, v.v. - đơn giản hơn nhiều. Vì phần phụ trợ của PAB có thể nhận và gửi tin nhắn nên các DApp có thể dễ dàng giao tiếp với nó. Do đó, DApp có thể đưa ra các yêu cầu tiêu chuẩn đối với các điểm cuối do PAB cung cấp, tương ứng với các hành động và hoạt động mà mỗi hợp đồng thông minh có thể xử lý.

PAB, cung cấp hỗ trợ thời gian chạy để truy cập vào Blockchain nhằm tiếp tục thực hiện các hoạt động hợp đồng thông minh kích hoạt giao dịch dựa trên mô hình eUTXO, có thể chạy các ứng dụng được xây dựng bằng thư viện của khung. PAB cũng bao gồm các khả năng như kiểm tra, ghi nhật ký và giám sát.



Hình 22: Kiến trúc cấp cao của Nền tảng Plutus, nhấn mạnh vào các ứng dụng. Từ CardanoDocs.com

Trong sơ đồ này, Nền tảng bị hỏng dựa trên phần nào của hệ thống mà chúng tôi quan tâm:

- Plutus Foundation⁵⁰⁵ có mặt để hỗ trợ viết mã nhân đáng tin cậy và thực thi nó trên chuỗi
- Khung ứng dụng Plutus dành cho việc viết Plutus DApps

Các thành phần sau phải có mặt ngoài PAB:

- Chỉ số chuỗi: cơ sở dữ liệu thông tin thu được từ các giao dịch Cardano. Nó phải được đặt cùng vị trí với một Node Cardano và sử dụng giao thức đồng bộ hóa chuỗi của Node Cardano. Chỉ mục chuỗi của PAB là thành phần chỉ đọc. Do đó, một phiên bản duy nhất của chỉ mục chuỗi có thể được chia sẻ bởi một số phiên bản của PAB. API HTTP được sử dụng để phục vụ tất cả các yêu cầu chỉ mục chuỗi
- Node Cardano: PAB tận dụng giao thức ổ cắm để đăng ký các thay đổi sổ cái từ Node.

Mặc dù không bắt buộc đối với việc tạo hoặc triển khai DApp, nhưng PAB là một công cụ Cardano hữu ích giúp phát triển DApp dễ dàng hơn, an toàn hơn và tiết kiệm chi phí hơn. Nó giải phóng các nhà phát triển các nhiệm vụ trần tục bằng cách cung cấp thông tin từ các nguồn có liên quan theo phong cách dễ tiếp cận. Khi hệ sinh thái trưởng thành, cộng đồng đang phát triển các giải pháp thay thế dựa trên API và công cụ của riêng họ.⁵⁰⁶

Các nền tảng mới sáng tạo như Genius Yield (geniusyield.co) là những nền tảng tiên phong cho Plutus, tạo ra các lựa chọn thay thế PAB tùy chỉnh là nguồn mở, có sẵn cho các nhà xây dựng khác. Tiên sĩ Lars Brünjes, Giám đốc Công nghệ (Giám đốc Giáo dục IOG và CTO Genius Yield) đã nói về đặc tính nguồn mở trong một cuộc phỏng vấn của *Learn Cardano*:⁵⁰⁷

Đó là một trong những sở thích thú cưng của tôi, tôi không thể hiểu làm thế nào bạn có thể không biến nó thành nguồn mở. Ý tôi là, toàn bộ quan điểm của hợp đồng thông minh...khi tôi giải thích cho ai đó hợp đồng thông minh là gì...bạn luôn nói rằng 'với các hợp đồng bình thường của con người, luôn có sự mơ hồ và các vấn đề pháp lý và bạn thay thế điều đó bằng toán học và mã, và vì vậy nó rõ ràng đó là gì'...nhưng toàn bộ vấn đề này sẽ bị tắt tiếng nếu bạn không công khai hợp đồng thông minh của mình, bởi vì khi đó không ai có thể kiểm tra logic thực tế. Ý tôi là sau đó bạn cũng có thể quên Blockchain đi và tập trung hóa nó. Vì vậy, theo ý kiến của tôi, ít nhất bạn phải công khai các hợp đồng thông minh... và sự thay thế PAB này mà chúng tôi đã đề cập một vài lần bây giờ, chúng tôi chắc chắn cũng muốn biến nó thành nguồn mở để mọi người đều có thể thu lợi từ nó chứ không phải mọi người. dự án phải phát minh lại điều đó nhiều lần.

Công cụ ước tính phí Plutus

Các chuyên gia về hiệu suất của IOG đã tạo ra công cụ tính phí Plutus như một công cụ nội bộ để đo điểm chuẩn và so sánh giá. Nó dự đoán các khoản phí sẽ được tính cho một giao dịch bằng cách sử dụng dữ liệu từ các giao dịch Plutus trong thế giới thực. Công cụ ước tính có thể được sử dụng để ước tính chi phí cho các giao dịch tập lệnh riêng lẻ hoặc toàn bộ DApps trước hoặc trong quá trình phát triển, cũng như để tính phí cho các giao dịch hiện có (ví dụ: để đánh giá các khoản phí sẽ được tính nếu tham số mạng thay đổi).

Các nguyên tắc thiết kế của sổ cái Cardano mang lại hiệu suất tuyệt vời trong khi vẫn duy trì các tiêu chuẩn bảo mật nghiêm ngặt. Mô hình kế toán Đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO) cho phép kiểm tra các giao dịch và tập lệnh Cardano cục bộ (ngoài chuỗi), cho phép người dùng xem liệu một giao dịch có hợp pháp hay không trước khi thực hiện giao dịch đó trên chuỗi và phát sinh phí. Hơn nữa, phí giao dịch được cố định không có gì bất ngờ. Để so sánh, chi phí thực hiện hợp đồng thông minh trên Ethereum thay đổi tùy theo lưu lượng mạng, từ 5 đô la đến hàng trăm đô la.⁵⁰⁸ của đô la. Ngay cả các giao dịch Ethereum không thành công cũng có thể phát sinh phí, làm tăng thêm sự khó đoán về giá.

Mặt khác, người dùng trên Cardano có thể đánh giá trước phí xử lý giao dịch tiềm năng. Không cần phải trả tiền cho một giao dịch có thể thất bại vì người dùng biết trước liệu giao dịch đó có hợp pháp hay không. Điều này ngăn tiền bị lãng phí và loại bỏ các lỗi trên chuỗi. Phí thực thi ADA của Cardano luôn nhất quán vì nó dựa trên các tham số giao thức mạng được xác định trước thay vì, ví dụ, thay đổi các biến tắc nghẽn mạng.

Chiến lược định giá của Cardano chủ yếu dựa trên nhu cầu thị trường hơn là nguồn cung thực. Với chức năng hợp đồng thông minh của Cardano, nhiều loại nhu cầu hiện đang cạnh tranh để có được cùng một nguồn cung. Do đó, giá cả tương đối và tuyệt đối⁵⁰⁹ phải được xem xét. Một phương tiện để thực hiện điều này là kiểm tra ý nghĩa của việc định giá hợp đồng thông minh, các hoạt động của Token không thể thay thế (NFT) và các yếu tố khác liên quan đến một giá trị chung — trong ví dụ này là việc sử dụng sức mạnh xử lý của Cardano.

Định giá hợp đồng thông minh trong Cardano dựa trên chi phí cố định, được xác định bởi giá của các tài nguyên đã sử dụng (kích thước UTXO hoặc tính toán/bộ nhớ được tiêu thụ trong khi thực thi). Lao động và tài nguyên của các SPO (SPO) xác minh các giao dịch mạng phải được đền bù thỏa đáng bằng các khoản phí. Hơn nữa, đảm bảo rằng bất kỳ phương pháp áp dụng Cardano nào không rẻ hơn đáng kể so với phương pháp khác sẽ giúp ngăn chặn một loạt các cuộc tấn công bất lợi (ví dụ: tấn công DDoS).

⁵⁰⁶

Các lựa chọn thay thế API, youtu.be/W2R3zl91U24?t=357

⁵⁰⁷Tim hiểu Phỏng vấn Cardano w/ Genius Yield, youtube.com/watch?v=7KBhfe6GVAA&t=1763s

⁵⁰⁸

Phí gas Ethereum tiếp tục tăng e, analyticsinsight.net/ethereum-gas-fees-Continue-to-rise-while-bitgert-zero-gas-fee-blockchain-is-booming/

⁵⁰⁹

Giá tuyệt đối so với giá tương đối : Giá tuyệt đối là số đô la có thể được trao đổi cho một số lượng nhất định của một hàng hóa nhất định. Giá tương đối là số lượng của một số hàng hóa khác có thể được trao đổi với một số lượng cụ thể của một hàng hóa nhất định. Giả sử chúng ta có hai hàng hóa A và B. Giá tuyệt đối của hàng hóa A là số đô la cần thiết để mua một đơn vị hàng hóa A. Giá tương đối của hàng hóa A tính theo B là số lượng hàng hóa B cần thiết để mua một đơn vị hàng hóa đó của tốt A.

Tính linh hoạt cũng là một đặc điểm quan trọng của giao thức Cardano, vì nó cho phép người dùng điều chỉnh cài đặt của họ và phản ứng với sự dao động của giá. Nếu giá trị của ADA tăng đáng kể, cài đặt giao thức có thể được sửa đổi nếu cần thiết để tránh người dùng chi tiêu quá mức cho việc thực hiện hợp đồng thông minh.

IOG đã tạo công cụ ước tính phí Plutus để định giá và so sánh. Công cụ ước tính có thể được sử dụng để ước tính chi phí cho các giao dịch tập lệnh riêng lẻ hoặc toàn bộ DApps trước hoặc trong quá trình phát triển, cũng như để dự đoán phí cho các giao dịch hiện tại. Nó cũng có thể được sử dụng để xem các bản cập nhật hoặc tối ưu hóa tập lệnh ảnh hưởng đến chi phí như thế nào.

Công thức tính phí được sử dụng bởi công cụ ước tính giống như công thức được sử dụng bởi Node Cardano. Nó có thể cung cấp một ước tính chính xác về phí yêu cầu nếu đầu vào đủ chính xác. Người dùng có thể chỉ cần dự đoán chi phí của một DApp bằng cách cộng các khoản phí từ nhiều giao dịch. Công cụ ước tính chứa một số ví dụ trong thế giới thực đã được kiểm tra chéo so với phí thực tế.

Cần có ba thông tin để tính phí:

- Kích thước của các giao dịch trên chuỗi tính bằng byte: một giao dịch cơ bản là khoảng 300 byte, một giao dịch chứa siêu dữ liệu là khoảng 650 byte và các tập lệnh Plutus thường là 4.000-8.000 byte (việc tối ưu hóa liên tục sẽ cải thiện những điều này)
- Số bước tính toán (CPU) được tập lệnh sử dụng: mỗi bước trên hệ thống điểm chuẩn bằng 1 pico giây thời gian thực hiện. Trung bình, các tập lệnh nên sử dụng ít hơn 1.000.000.000 đơn vị CPU (1 mili giây)
- Số đơn vị bộ nhớ được sử dụng bởi tập lệnh: đây là số byte được phân bổ bởi tập lệnh. Trong hầu hết các trường hợp, tập lệnh nên sử dụng ít hơn 1.000.000 đơn vị bộ nhớ (1 MB cấp phát bộ nhớ).

Người dùng chỉ cần nhập thông tin tương đối để sử dụng công cụ ước tính, công cụ này có thể được truy xuất từ trình biên dịch Plutus sau khi tạo tập lệnh trong đó. Cũng không cần phải chạy một Node cho việc này, điều này làm cho quy trình dễ dàng hơn nhiều đối với những người không chuyên về công nghệ.

Lái thử công cụ ước tính phí Plutus⁵¹⁰ và xem việc ước tính phí xử lý dễ dàng như thế nào mà không phải tạm biệt số tiền của bạn nếu giao dịch không thành công.

trình xác thực nấu chín

Với thư viện *cook-validators*, bạn có thể viết mã ngoài chuỗi và nhận thử nghiệm dựa trên thuộc tính miễn phí. Là nhà phát triển Haskell sử dụng các phương pháp chính thức, bạn nên tận tâm sử dụng các công cụ và quy trình để đảm bảo tính an toàn và lành mạnh của các ứng dụng phi tập trung (DApp). Viết và triển khai một DApp là không đủ; tất cả mã trên chuỗi và tập lệnh Plutus phải được kiểm tra cẩn thận trước nhiều tác nhân xấu khác nhau.

Với suy nghĩ này, *Tweag* đã giới thiệu *trình xác thực đã chuẩn bị*,⁵¹¹ một tập hợp các công cụ sẵn sàng sử dụng để làm việc với các tập lệnh trình xác thực Plutus. Thư viện này hỗ trợ triển khai lớp mã ngoài chuỗi trong cùng, chịu trách nhiệm tạo và gửi giao dịch. Bạn nhận được thử nghiệm dựa trên tài sản ở cấp độ giao dịch miễn phí bằng cách sử dụng thư viện này.

Bạn có thể xác minh các khía cạnh an toàn và chính xác khác nhau của mã trên chuỗi của mình bằng cách sử dụng trình xác thực đã chuẩn bị sẵn để tạo mã ngoài chuỗi của mình, điều này có thể nâng cao đáng kể niềm tin của bạn vào tính chính xác của mã. Trong quá trình kiểm toán, điều này có thể tiết kiệm thời gian và tiền bạc. Bước đầu tiên trong quá trình kiểm tra Tweag là tận dụng các trình xác thực đã nấu chín để viết mã tạo giao dịch, cho phép chúng tương tác với cơ sở hạ tầng của khách hàng.

Viết giao dịch Plutus

Viết một giao dịch Plutus được thực hiện theo thứ tự sau:

1. Viết mã trên chuỗi Plutus của bạn.

⁵¹⁰

Công cụ ước tính phí Plutus, [docs.cardano.org/ cardano-testnet / tools/ plutus -fee-estimator](https://docs.cardano.org/cardano-testnet/tools/plutus-fee-estimator)

⁵¹¹

Trình xác thực đã chuẩn bị, [github.com/ tweag / plutus -libs/tree/main/cooked-validators](https://github.com/tweag/plutus-lib/tree/main/cooked-validators)

2. Chuyển đổi mã Plutus của bạn sang định dạng phong bì văn bản (đây là định dạng mà giao diện dòng lệnh cardano -cli . tức là . mong đợi).
3. Sử dụng (các) tập lệnh Plutus có sẵn, tạo giao dịch của bạn.
4. Thực thi tập lệnh Plutus bằng cách gửi giao dịch.

Chuyện hoang đường

Điều quan trọng cần lưu ý là Plutus Tx là ngôn ngữ cấp cao để viết kịch bản logic xác thực của hợp đồng thông minh. Logic này xác định liệu một giao dịch có được phép chi tiêu UTXO hay không. Plutus Tx là một tập hợp con của Haskell, sau đó nó được biên dịch thành Plutus Core, một ngôn ngữ cấp thấp dựa trên phép tính lambda. Plutus Core là mã chạy trên chuỗi và thường được gọi là tập lệnh Plutus hoặc trình xác thực Plutus.

Để triển khai hợp đồng thông minh, bạn cũng sẽ yêu cầu mã ngoại tuyến để xây dựng và gửi giao dịch, triển khai hợp đồng thông minh, truy vấn các UTXO có sẵn trên chuỗi, v.v. Bạn cũng có thể sẽ cần một giao diện người dùng mặt trước để giúp người dùng dễ dàng thực hiện .

Sau một khởi đầu gập ghềnh, điều được mong đợi với một ngôn ngữ hoàn toàn mới , các nhà phát triển và trải nghiệm người dùng đã được cải thiện trong suốt năm 2022 và sẽ tiếp tục phát triển với công cụ tốt hơn. Tại buổi nói chuyện *Vượt qua những thách thức và con đường áp dụng hàng loạt* tại Hội nghị thượng đỉnh năm 2022, các nhà phát triển Cardano giàu kinh nghiệm nhất đã nói về tiến trình kể từ những ngày đầu. Tất cả họ đều đồng ý rằng hầu hết mã được yêu cầu là ngoại tuyến và có thể được viết bằng bất kỳ ngôn ngữ nào bạn muốn.

Andrew Westberg, CTO của NEWM⁵¹²

Hoàn toàn sai lầm khi cho rằng bạn phải là nhà phát triển Haskell mới có thể làm việc trên Cardano, hầu hết các nhà phát triển Cardano mà tôi biết dành nhiều thời gian hơn cho các ngôn ngữ khác. Có rất nhiều Rust, có rất nhiều Kotlin, có rất nhiều JavaScript... mọi người đang sử dụng ngôn ngữ của riêng họ và bạn thực sự có thể mang ngôn ngữ của riêng mình mà bạn đã quen thuộc và cảm thấy thoải mái với Cardano.

Bỏ qua FUD 'đồng thời'

Tính đồng thời có thể làm tăng hoặc giảm hiệu suất, thông lượng và khả năng đáp ứng của hệ thống. Số lượng hoạt động đồng thời có thể được thực hiện bị giới hạn bởi mức độ đồng thời.⁵¹³

Bộ xử lý trong Blockchain dựa trên UTXO sẽ có thể thực hiện nhiều hành động cùng một lúc để đạt được hiệu quả thực sự. Khả năng song song tối đa có thể tăng lên khi số lượng đồng thời tăng lên. Kết quả của chiến lược này là hiệu suất và thông lượng tăng lên. Nó cũng có một số lợi ích so với các hệ thống dựa trên tài khoản (như Ethereum).

Tính bất định, tính song song và tính đồng thời

Những tính năng này là điểm khác biệt của Plutus. Có một cấu trúc được gọi là đồ thị tuần hoàn có hướng đã đề cập trước đây, đôi khi có thể được coi như một mạng nhện gồm các Node nhỏ, các vòng tròn nhỏ và chúng có các đường nối với Node tiếp theo và các đường nối với Node tiếp theo khi mạng phát triển, đặc biệt nếu nó đi theo một chiều.

Sở cái Cardano tạo thành biểu đồ giao dịch và biểu đồ rất phù hợp để xử lý song song. Theo định nghĩa, Cardano cho phép xử lý song song với cách hoạt động của UTXO. Điều này có nghĩa là vì lõi Plutus mang tính quyết định và vì các tập lệnh chỉ có quyền truy cập vào thông tin cục bộ nên có thể xử lý song song nhiều thứ trong cả quá trình xác thực tập lệnh Plutus và xác thực sổ cái.

Khi bạn đang xây dựng trên Cardano, có thể đạt được đồng thời tốt hơn bằng cách sử dụng nhiều UTXO và khai thác tính song song và bạn có thể xây dựng với phong cách này một kiến trúc mở rộng song song ồ ạt và cho phép bạn phục vụ tất cả người dùng của mình cùng một lúc.

Triển khai DApps trên sổ cái UTXO là khác

⁵¹²

Xây dựng trên Cardano: vượt qua thách thức và con đường áp dụng hàng loạt, youtu.be/bASyKD2dnys?t=715

⁵¹³ **Đồng thời**, thuộc tính của chương trình, thuật toán hoặc phân tích vấn đề thành các đơn vị độc lập theo thứ tự hoặc được sắp xếp một phần.

Tóm lại từ trước đó, hãy nhớ rằng cách tiếp cận của Cardano đối với việc triển khai DApp là khác. Nó đòi hỏi phải mở rộng một đường cong học tập dốc và sử dụng một chiến lược cẩn thận.

Tối ưu hóa đồng thời là một nguyên tắc phải được nghiên cứu: các nhà phát triển phải tạo mã theo cách hạn chế sự tranh chấp (ví dụ: bằng cách tránh các trạng thái chia sẻ và phụ thuộc ngẫu nhiên). Sự đồng thời này sau đó phải được hệ thống dịch thành song song. Một số nhà phát triển trước đây đã tìm ra các cách tiếp cận thành công, trong khi những người khác hiện đang nghiên cứu chúng. Không thể đơn giản chuyển các kỹ năng đã học trên một Blockchain này sang Blockchain khác; mặc dù có một đường cong học tập, nhưng lợi ích lớn hơn nỗ lực.

Trong mọi trường hợp, điều quan trọng cần nhớ là nhà phát triển không thể chỉ sử dụng hợp đồng Ethereum được điều chỉnh để xây dựng DApp có thể mở rộng trên Cardano. Cardano được xây dựng trên mô hình UTXO thay vì cách tiếp cận dựa trên tài khoản; do đó, một trạng thái trên chuỗi duy nhất sẽ không đáp ứng điều kiện đồng thời của Cardano. Thay vào đó, các DApp nên phân phối trạng thái trên chuỗi của chúng trên một số UTXO. Do đó, tính đồng thời của ứng dụng của họ sẽ tăng lên, cho phép thông lượng nhanh hơn. Đọc cách thiết kế ứng dụng Plutus có thể mở rộng⁵¹⁴ để tìm hiểu thêm về khả năng mở rộng và mẫu số đặt hàng⁵¹⁵ để tìm hiểu thêm về cách tổ chức DApps trên Cardano bằng các mẫu.

Sở cái Cardano được xây dựng với tính chắc chắn cao, bảo mật và xác minh chính thức. Theo triết lý này, điều quan trọng là phải đảm bảo quá trình xử lý giao dịch mang tính quyết định, nghĩa là người dùng có thể dự đoán tác động và kết quả của giao dịch trước khi nó xảy ra.

Với việc bổ sung các khả năng của hợp đồng thông minh, khả năng đảm bảo chi phí thực hiện giao dịch và cách giao dịch hoạt động trên sổ cái trước khi nó được gửi trở nên quan trọng hơn. Thiết kế xác định của Cardano và tập lệnh Plutus⁵¹⁶ đảm bảo khả năng này.

Datums và Redeemers

Dữ liệu và người đổi quà là hai tính năng quan trọng trong Plutus; điều quan trọng là phải biết chúng là gì và cách sử dụng chúng khi gửi giao dịch. Dữ liệu chuẩn là một phần dữ liệu có thể liên quan đến UTXO và được sử dụng để chứa thông tin trạng thái tập lệnh như chủ sở hữu của tập lệnh hoặc siêu dữ liệu thời gian (có thể xác định thời điểm có thể sử dụng UTXO). Nó thường được sử dụng cùng với một công cụ đổi quà, là dữ liệu tùy ý được cung cấp trong một giao dịch được sử dụng làm đầu vào tập lệnh.

Xác thực giao dịch qua hai giai đoạn

Các đầu ra chưa sử dụng từ các giao dịch trước đó được gọi là đầu vào. Hàm băm dữ liệu và một giá trị (bao gồm một lượng ADA và Token gốc bổ sung, tùy chọn) được lưu giữ trong một UTXO tại một địa chỉ (khóa công khai hoặc hàm băm khóa công khai). Tập lệnh quyết định có 'mở khóa' tiền hay không khi UTXO tại địa chỉ tập lệnh là đầu vào cho một giao dịch hợp lệ. Điều này có thể được triển khai nếu các yêu cầu của tập lệnh được đáp ứng (sự kết hợp tùy ý của các yếu tố bao gồm dữ liệu, trình đổi mã và ngữ cảnh tập lệnh). Giao dịch phải được ký bởi chủ sở hữu khóa riêng được liên kết với địa chỉ trong bước xác thực đầu tiên.

Từ quan điểm của một giao dịch mua lại, điều quan trọng là phải nắm bắt các khái niệm sau:

1. Địa chỉ tập lệnh: địa chỉ Cardano lưu trữ tiền được bảo vệ bởi tập lệnh Plutus có thể được mở khóa thêm. Nó là một hàm băm của tập lệnh Plutus.
2. Hàm băm dữ liệu: hàm băm dữ liệu phải được liên kết với UTXO tại một địa chỉ tập lệnh trong Cardano. Điều này được thực hiện để tiết kiệm bộ nhớ và cho phép truy cập nhanh khi xác minh giao dịch.
3. Tập lệnh Plutus là một ứng dụng thực thi dựa trên sổ cái thực hiện xác thực giao dịch (giai đoạn hai) tiếp theo.
4. Giá trị dữ liệu: bạn cần cung cấp giá trị dữ liệu khớp với hàm băm dữ liệu được cung cấp trong giao dịch khóa khi gửi giao dịch để đổi tiền.
5. Giá trị quy đổi: định dạng dữ liệu tùy ý giống như dữ liệu được sử dụng. Giá trị quy đổi được tập lệnh sử dụng để xác minh giao dịch và được gắn với giao dịch đầu vào để giải phóng tiền từ tập lệnh.
6. Ngữ cảnh tập lệnh: một bản tóm tắt giao dịch cũng được yêu cầu bởi tập lệnh Plutus để xác minh giao dịch đó.

⁵¹⁴ Viết một ứng dụng có thể mở rộng, plutus.readthedocs.io/en/latest/plutus/howtos/writing-a-scalable-app.html

⁵¹⁵ Mẫu số lệnh là gì? sân chơi, plutus.iohkdev.io/doc/plutus/explanations/order-book-potYPE.html

⁵¹⁶ Tập lệnh trình xác thực Plutus, docs.cardano.org/plutus/Plutus-validator-scripts

Quá trình làm việc với dữ liệu và người mua lại nằm ngoài phạm vi của cuốn sách này, nhưng bạn có thể nghiên cứu các ví dụ đã được thực hiện trong Chương trình Tiên phong Plutus⁵¹⁷ và Tài liệu Cardano.⁵¹⁸

Ngày 12 tháng 3 năm 2019. Giao dịch đơn giản khác với chạy hợp đồng thông minh như thế nào? CH:⁵¹⁹

Vì vậy, mục tiêu của Plutus là thực sự biến tất cả các giao dịch thành một hợp đồng thông minh theo một cách nào đó. Vì vậy, về cơ bản, nếu bạn nhìn vào sự khác biệt giữa những gì Ethereum làm và những gì một hệ thống UTXO như Cardano làm... thì chúng là những cấu trúc dữ liệu khác nhau. Vì vậy, một loại sổ cái có thể thay đổi được và bạn gửi tin nhắn đến nó để đánh thức nó, sau đó bạn sẽ có tất cả quản lý nhà nước mà bạn phải đối mặt... và điều đó thực sự khó khăn, đặc biệt là khi hệ thống phát triển và đặc biệt là khi bạn muốn phân mảnh hệ thống để theo dõi mọi thứ... vì vậy bạn phải thêm rất nhiều độ phức tạp vào mô hình của mình.

Khi bạn nhìn vào hệ thống UTXO, nó được gọi là biểu đồ luồng dữ liệu... và về cơ bản, nó chỉ nói rằng bạn có tất cả các luồng này... và bạn có đầu ra và tất cả những gì bạn phải làm để đánh thức một trong số chúng chỉ là tuyên bố rằng bạn có quyền để chi tiêu... và sau đó nếu bạn có bằng chứng rằng nó hợp lệ, nó sẽ chi tiêu...

... vì vậy những gì chúng tôi đã làm là lấy mô hình đó và chúng tôi đã mở rộng nó để bao gồm một số thông tin trạng thái và bao gồm giá trị và bao gồm một số dữ liệu... và chúng tôi gọi đây là mô hình UTXO mở rộng... vì vậy bạn giữ nguyên ngữ nghĩa của trình xác nhận Người chuộc lỗi⁵²⁰ (tập lệnh btc) mà Bitcoin đã giới thiệu hơn 10 năm trước... nhưng giờ đây bạn đã thêm khả năng có đủ thông tin trong đó, rằng bạn thực sự có thể chạy mã, đây là những gì về cơ bản của Plutus...

Giờ đây, lợi thế của loại hệ thống này là giờ đây tất cả các giao dịch có thể đơn giản như giá trị chảy từ Alice sang Bob... hoặc chúng có thể phức tạp như một hợp đồng thông minh mà bạn sẽ thấy giống như tạo ra một loại tiền tệ hoặc thứ gì đó tương tự... vì vậy có cả một phạm vi phức tạp ở đó... và bạn có thể xâu chuỗi những thứ này lại với nhau.. và bạn cũng có thể dễ dàng tương tác hơn với giao dịch trực tuyến đó bằng mã ngoại tuyến... bởi vì khi bạn thực sự xem xét các hợp đồng thông minh này một cách tổng quát, chúng chúng có phức tạp với những thứ sống bên ngoài hệ thống không... vì vậy bạn sẽ có một số mã JavaScript và một số hành động web3 đang diễn ra và đang chạy trên máy chủ hoặc máy khách... và sau đó, đó là nói chuyện với thứ gì đó sống trên chuỗi... đó là mô hình Ethereum

...với Cardano, nó sẽ chỉ là Plutus... mẫu Haskell... Haskell và sau đó chạy và nó chạy như một đơn vị duy nhất... và bạn có thể viết tất cả mã cùng nhau và rất dễ dàng để xác thực rằng chuỗi ngoại tuyến và mã trên chuỗi thực sự hoạt động chính xác cùng nhau

[...] Vì vậy, chúng tôi có một khung làm việc tốt ở đó và bạn có thể thực hiện nhiều thử nghiệm dựa trên thuộc tính và nhiều xác nhận thủ vị... và nói rằng mọi thứ đang hoạt động chính xác... bởi vì nó đang chạy mô hình luồng dữ liệu không thay đổi này... điều thực sự tuyệt vời về điều đó là việc phân tách các loại giao dịch này dễ dàng hơn nhiều... Vì vậy, về cơ bản, câu trả lời ngắn gọn cho câu hỏi của bạn là tất cả các giao dịch đều là hợp đồng thông minh về mặt kỹ thuật trong mô hình trình xác thực Redeemer này... chỉ là độ phức tạp của chúng tùy thuộc vào người dùng và cách họ chạy những thứ này

cơ chế tài sản đảm bảo

Cơ chế tài sản thế chấp là một thành phần quan trọng đảm bảo các hợp đồng thông minh được chạy thành công.

Cardano sử dụng cơ chế xác thực hai giai đoạn, dựa trên sự đảm bảo được cung cấp bởi kiến trúc xác định của sổ cái. Mục tiêu chính của việc triển khai xác thực hai giai đoạn là giảm số lượng nỗ lực xác thực không bù đắp được thực hiện bởi các Node. Mỗi giai đoạn có một vai trò cụ thể để đạt được mục tiêu này:

- Giai đoạn đầu tiên xác minh rằng giao dịch đã được cấu trúc chính xác và phí xử lý có thể được thanh toán

⁵¹⁷

Plutus Pioneers Chào mừng & Giới thiệu,
[youtube.com/watch?v=X80uNXenWF4&list=PLK8ah7DzglhgK0bEyELK8EzbW0mn6xavC](https://www.youtube.com/watch?v=X80uNXenWF4&list=PLK8ah7DzglhgK0bEyELK8EzbW0mn6xavC)

⁵¹⁸

Dữ liệu và người đổi quà,
github.com/input-output-hk/cardano-documentation/blob/staging/content/10-plutus/07-datums-redeemers.mdx

⁵¹⁹

AMA bắt đầu 12/03/2019, [youtube.be/f-rqaTLwWgs?t=1575](https://www.youtube.be/f-rqaTLwWgs?t=1575)

⁵²⁰

Trình xác thực người đổi quà, bitcoinmagazine.com/articles/thinking-transactions-1401650873

- Các tập lệnh của giao dịch được thực hiện trong giai đoạn thứ hai.

Tập lệnh giai đoạn 2 được thực thi nếu giao dịch tuân thủ giai đoạn 1. Nếu giai đoạn 1 không thành công, không có tập lệnh nào được thực thi và giao dịch bị từ chối ngay lập tức. Nếu xác minh giai đoạn 2 không thành công, tài sản thế chấp sẽ được sử dụng để đảm bảo rằng các Node được khen thưởng cho những nỗ lực của họ. Do đó, tài sản thế chấp là khi người dùng đưa ra sự đảm bảo bằng tiền rằng hợp đồng đã được xây dựng đúng cách và được kiểm tra nghiêm ngặt. Số lượng đầu vào tài sản thế chấp được đặt và bao gồm khi giao dịch được tạo. Số tiền ký quỹ của giao dịch là toàn bộ số dư trong UTXO tương ứng với các đầu vào được gắn thẻ cụ thể này. Tài sản thế chấp được bảo đảm nếu người dùng đáp ứng các yêu cầu của bảo lãnh và hợp đồng được thực hiện.

Vấn đề

Nếu hợp đồng thông minh không thành công mà không có tài sản thế chấp, người dùng sẽ không bị phạt. Tuy nhiên, vào thời điểm giao dịch không thành công, mạng đã thanh toán cho giao dịch được bắt đầu và xác thực. Một đối thủ thù địch có thể gửi thư rác trên mạng bằng các giao dịch giả, do đó tước đi dịch vụ của những người dùng khác với chi phí rất thấp.

Làm thế nào tài sản thế chấp giải quyết điều này

Khi người dùng bắt đầu giao dịch, họ cam kết đủ ADA để đáp ứng chi phí thực hiện giao dịch. Các giao dịch sử dụng hợp đồng thông minh không bản địa (còn được gọi là hợp đồng giai đoạn 2) cần có tài sản thế chấp đầy đủ để trang trải chi phí cho bất kỳ lỗi giao dịch nào. Số tiền này có vẻ không đáng kể, nhưng nó đủ để ngăn chặn một cuộc tấn công từ chối dịch vụ (DoS). Chỉ khi một giao dịch không xác thực được thì chi phí thế chấp mới được thu thập. Chi phí giao dịch được thanh toán nếu hợp đồng vượt qua xác nhận, nhưng tài sản thế chấp thì không. Tài sản thế chấp của một người dùng trung thực không bao giờ có nguy cơ bị mất.

Chi phí giao dịch trên Blockchain Cardano có thể dự đoán được vì chúng chỉ bị ảnh hưởng bởi các giá trị và trạng thái địa phương. Người dùng có thể dự đoán chi phí thực hiện giao dịch (tính bằng ADA) trước khi bắt đầu giao dịch. Các Blockchain khác, chẳng hạn như Ethereum, có thiết kế cho phép các hoạt động mạng khác tác động đến chi phí gas. Số lượng tài sản thế chấp cần thiết chỉ được xác định bởi chi phí thực hiện.

Các Mạng thử nghiệm ⁵²¹Cardano cung cấp một môi trường an toàn với ADA thử nghiệm miễn phí (tADA), cho phép các nhà phát triển DApp kiểm tra căng thẳng các hợp đồng thông minh của họ trước khi xuất bản chúng lên mạng chính. Nếu các giao dịch diễn ra suôn sẻ trên mạng thử nghiệm, nhà phát triển có thể chắc chắn rằng tất cả các tập lệnh cũng sẽ chạy trơn tru.

Nếu hoàn cảnh trên chuỗi đã thay đổi sau khi giao dịch được tạo, giao dịch sẽ bị từ chối hoàn toàn mà không thu được phí. Chẳng hạn, sẽ không có tài sản thế chấp nào bị tính phí nếu không có chữ ký.

Trong thực tế

Tổng số ADA có trong UTXO được tham chiếu bởi đầu vào tài sản thế chấp được gọi là tài sản thế chấp. Nếu tập lệnh giai đoạn 2 không thành công, giao dịch sẽ sử dụng đầu vào tài sản thế chấp để thanh toán phí.

Ý tưởng về các tập lệnh 'đa chữ ký' đã được giới thiệu bởi đặc điểm kỹ thuật chính thức của Shelley. Các quy tắc sổ cái nắm bắt hoàn toàn các tập lệnh Giai đoạn 1 như thế này. Do đó, chi phí thực thi có thể được ước tính dễ dàng trước khi chạy triển khai và bất kỳ khoản phí nào cũng có thể được xác định trực tiếp trong quá trình triển khai quy tắc sổ cái tùy thuộc vào quy mô của giao dịch chứa tập lệnh.

Mặt khác, các tập lệnh Giai đoạn 2 có thể thực hiện bất kỳ tính toán Turing-đầy đủ nào về mặt lý thuyết. Chúng tôi muốn có ngân sách dưới dạng một số *ExUnits* trừu tượng cho các giao dịch tận dụng tập lệnh giai đoạn 2. Ngân sách này thiết lập một giới hạn định lượng về mức tiêu thụ tài nguyên theo nhiều biện pháp khác nhau, chẳng hạn như sử dụng bộ nhớ hoặc các bước thực thi trừu tượng. Ngân sách sau đó được sử dụng để tính phí giao dịch.

Từ Báo cáo kỹ thuật của Plutus,⁵²²

*Tài nguyên được theo dõi theo hai đơn vị trừu tượng: thời gian trừu tượng và bộ nhớ trừu tượng (cao điểm). Cùng nhau, chúng tôi gọi đây là **những người xuất gia**. Tại sao các đơn vị ở đây là 'trừu tượng'? Chúng phải như vậy, bởi vì chúng ta cần có khả năng giữ cho mọi thứ trở nên xác định và vì vậy chúng ta không thể sử dụng thời gian thực hoặc mức sử dụng bộ nhớ. Thay vào đó, chúng tôi phải xác định một số biện pháp trừu tượng mà chúng tôi cố gắng điều chỉnh phù hợp với việc sử dụng.*

⁵²¹

Mạng thử nghiệm Cardano, testnets.cardano.org/vi/testnets/cardano/overview/

⁵²²

Peyton Jones, Kireev, 'Nền tảng Plutus', hydra.iohk.io/build/12983030/download/1/plutus.pdf

Để biết thêm thông tin, hãy đọc đặc tả sổ cái Cardano cho Plutus Core.⁵²³

CIP 40 - Đầu ra tài sản thể chấp rõ ràng đã cải thiện hơn nữa trải nghiệm người dùng. Một số mã tình ranh trong một số ví nhất định có nghĩa là có quá nhiều tài sản thể chấp đã được thực hiện do nhầm lẫn. Trong một kịch bản như vậy, sẽ không có gì quá thảm khốc xảy ra, nhưng cuối cùng tài sản thể chấp đã bị lấy đi, vì vậy người dùng mất tài sản thể chấp. Nó tương tự như việc tính phí quá cao.

IOG muốn cải thiện trải nghiệm người dùng, vì vậy họ đã tìm ra cách có thể gửi giao dịch nhưng tài sản thể chấp đi kèm chỉ đủ trang trải. Nếu bạn thêm một số '0' do một ngón tay béo vô tình hoặc bất cứ điều gì, chẳng hạn như một triệu ADA, bạn sẽ nhận lại mọi thứ không cần thiết. Một sự điều chỉnh đáng hoan nghênh. Đây là một phần trong hành trình đưa Plutus trở thành một trải nghiệm người dùng tuyệt vời. Nếu mọi người mắc lỗi vô tội, chẳng hạn như lỗi chính tả, họ sẽ không bị phạt nặng.

Học Plutus

Vì Plutus dựa trên Haskell, nên một điểm khởi đầu tốt là cuốn sách nổi tiếng *Learn You a Haskell for Great Good* của Miran Lipovača (learnyouahaskell.com) là bước đột phá đầu tiên của nhiều người vào Haskell.

Bạn có thể nghiên cứu Hướng dẫn ban đầu của Plutus⁵²⁴ từ tài liệu. Nhóm giáo dục IOG đã viết sách điện tử Plutus giới thiệu, có sẵn trên Amazon⁵²⁵ và LeanPub. *Plutus: Việc viết các hợp đồng thông minh đáng tin cậy* nhằm vào các nhà phát triển Haskell ở cấp độ mới bắt đầu tập trung vào các nguyên tắc cơ bản với các ví dụ thực tế. Gần đây, họ cũng đã phát hành Khóa học Haskell 'không có gì' trên GitHub.⁵²⁶

Chương trình tiên phong Plutus

IOG đã tạo ra Chương trình tiên phong Plutus với dự đoán về hard fork Alonzo. Chương trình này không dành cho người mới bắt đầu, vì vậy tốt nhất bạn nên học khóa học trực tuyến Haskell trước tiên và Crypto Mông Cổ vào tháng 9 năm 2020⁵²⁷ có sẵn trên YouTube, do Andres Löh, người đồng sáng lập công ty tư vấn Well-Typed và Tiến sĩ Lars Brünjes, Giám đốc Giáo dục tại IOHK, trình bày.

Có rất nhiều sự giúp đỡ từ cộng đồng. Người tiên phong Plutus và Atala Prism Oussama Benmahmoud đã viết *Cách chuẩn bị cho Chương trình Người tiên phong Plutus*.⁵²⁸ Chris Moreton (@PoolChess⁵²⁹) đã chép lại các bài giảng của Chương trình Tiên phong Plutus. Truy cập trang web 'readthedocs' của anh ấy⁵³⁰, nơi bạn cũng có thể tải xuống phiên bản pdf hoặc epub.

Bây giờ bạn đã sẵn sàng để đăng ký⁵³¹ cho nhóm tiếp theo. Bạn cũng có thể tương tác trực tiếp với cộng đồng về Plutus trên Diễn đàn Cardano⁵³² hoặc trên IOG Technical Discord.⁵³³

⁵²³

Thông số kỹ thuật chính thức của Sổ cái Cardano tích hợp Plutus Core, hydra.iohk.io/build/7172824/download/1/alonzo-changes.pdf
⁵²⁴

Hướng dẫn Plutus, plutus.readthedocs.io/en/latest/plutus/tutorials/index.html
⁵²⁵

cây, amazon.com/Plutus-Writing-reliable-smart-contracts-ebook/dp/B07V46LWTW/ref=sr_1_1, leanpub.com/plutus-smart-contracts

⁵²⁶Khóa học Haskell, github.com/input-output-hk/haskell-course
⁵²⁷

Haskell và Crypto Mông Cổ, youtube.com/watch?v=ctfZ6DwFiPg&list=PLJ3w5xyG4JWmBVligNBytJhvSSfZZzfTm&index=4
⁵²⁸

Cách chuẩn bị cho Chương trình Plutus Pioneer, essentialcardano.io/article/how-to-prepare-for-the-plutus-pioneer-program
⁵²⁹

PoolChess trên Twitter, twitter.com/PoolChess
⁵³⁰

PoolChess PP Ghi chú bài giảng, plutus-pioneer-program.readthedocs.io/en/latest/plutus_pioneer_program.html
⁵³¹

Đăng ký Chương trình Tiên phong Plutus, testnets.cardano.org/en/plutus-pioneer-program/
⁵³²

Plutus trên Diễn đàn Cardano, forum.cardano.org/c/developers/cardano-plutus/148
⁵³³

IOG Tech Discord, discord.com/invite/w6TwW9bGA6

Nhà phát triển áp dụng

IOG đã thành lập bộ phận Trải nghiệm dành cho nhà phát triển (DevX) mới do ⁵³⁴Moritz Angermann chỉ đạo để đảm bảo rằng các nhà phát triển tại IOG không bị cản trở bởi các công cụ họ sử dụng hàng ngày . Bộ phận làm việc chặt chẽ với tất cả các nhóm kỹ thuật và chịu trách nhiệm tối đa hóa sức mạnh tổng hợp của nhóm và đơn giản hóa các quy trình phát triển. Là phần mở rộng hợp lý của nhóm 'công cụ' hiện là một phần của DevX , một ưu tiên khác của DevX là phát triển công cụ Haskell.

Nhóm DevX đang làm việc để phát triển công nghệ cho phép cập nhật và cải tiến sổ cái liên tục. Bộ công cụ này đáp ứng nhu cầu của các nhà phát triển và cung cấp cho việc sử dụng hiệu quả hơn các thư viện tòa nhà đa dạng. Sau đây là một số điều có thể được thực hiện để làm cho trải nghiệm phát triển Haskell hiệu quả hơn:

- Những cải tiến đáng kể đối với khả năng biên dịch chéo
- Hỗ trợ plugin được cải thiện
- Khả năng tương tác với ngôn ngữ lập trình Rust và các ngôn ngữ khác.

Những cải tiến này cho phép các nhà phát triển không chỉ sử dụng các thư viện Haskell được viết bằng các ngôn ngữ khác mà còn tận dụng các thư viện Haskell được viết bằng các ngôn ngữ khác. Ngoài ra, bộ phận tập trung vào việc cải thiện quy trình công việc liên quan đến việc sử dụng Nix, ⁵³⁵Trình biên dịch Haskell của Glasgow (GHC) và GHCJS (trình biên dịch Haskell sang Javascript).

IOG dự đoán rằng khi Cardano phát triển thành một mô hình cơ sở hạ tầng mở hoàn toàn vào năm 2023, những cải tiến này sẽ trao quyền cho cộng đồng nhà phát triển lớn hơn với các khả năng được cải thiện để làm việc trên các dự án khác nhau và triển khai chúng trên Cardano. Công cụ của bên thứ ba phổ biến hơn cũng như *các công cụ Plutus của IOG đang được phát triển* .⁵³⁶

Charles Hoskinson đã vạch ra ⁵³⁷mong muốn của mình để Cardano phản ánh OSS (hệ thống nguồn mở) khác như Linux. ⁵³⁸Vào tháng 6 năm 2022, Cardano Foundation đã tham gia *The Linux Foundation* với tư cách là thành viên Vàng, trở thành tổ chức phi lợi nhuận duy nhất hoạt động ở cấp độ này. Thông tin thêm về cuộc đại tu quản trị trên chuỗi được công bố tại ScotFest trong Chương 9.

Trao đổi ngăn xếp Cardano

IOG khuyến khích các nhà phát triển tham gia tại một địa điểm — Cardano Stack Exchange ⁵³⁹— để trao đổi ý tưởng, hỏi và trả lời các câu hỏi liên quan đến tất cả các khía cạnh của hoạt động và phát triển Cardano cũng như tài nguyên nhóm. Trang web này do các thành viên cộng đồng Cardano điều hành, là một trong những công cụ để tìm hiểu cách tạo DApps và hợp đồng thông minh hoặc nếu bạn chỉ muốn biết 'Lớp 0 là gì?'⁵⁴⁰

Cardano Stack Exchange có nguồn gốc từ Stack Overflow.⁵⁴¹ Đây là trang web Hỏi & Đáp do cộng đồng kiểm duyệt, nơi tất cả các nhà phát triển Cardano, bao gồm cả những người tiên phong của Plutus, có thể nhận được câu trả lời cho nhiều loại câu hỏi, từ câu hỏi cài đặt đến cấu hình và triển khai cụ thể. Tâm lý phi tập trung, hướng đến cộng đồng của Stack Overflow kết hợp đặc biệt tốt với triết lý phi tập trung, mã nguồn mở của Cardano.

⁵³⁴

Moritz Angermann , iohk.io/team/moritz-angermann/ _
⁵³⁵

Nix là trình quản lý gói đa nền tảng sử dụng mô hình triển khai chức năng thuần túy. Phần mềm được cài đặt vào các thư mục duy nhất được tạo thông qua các hàm băm mật mã. Nó cũng là tên của ngôn ngữ lập trình của công cụ, dành riêng cho cấu hình và triển khai phần mềm.

⁵³⁶

Công cụ Plutus đang được phát triển,
plutus-apps.readthedocs.io/en/latest/plutus/explanations/plutus-tools-component-descriptions.html#
⁵³⁷

Tầm nhìn năm 2022 của Cardano: Hoskinson cuối cùng có thể có ngày phát hành cho ' Mamba',
ambcrypto.com/cardanos-2022-vision-hoskinson-may-finally-have-a-release-date-for-mamba/
⁵³⁸

Người sáng lập Cardano Charles Hoskinson đưa ra kế hoạch năm 2022,
coindesk.com/tech/2021/12/27/cardano-founder-charles-hoskinson-lays-out-2022-plans/
⁵³⁹

Trao đổi ngăn xếp Cardano, cardano.stackexchange.com/
⁵⁴⁰

'Lớp 0 là gì?', cardano.stackexchange.com/questions/8244/what-is-layer-0
⁵⁴¹

Stack Overflow là trang web hỏi đáp dành cho các lập trình viên chuyên nghiệp và đam mê lập trình. Đây là một trang web tư nhân, trang web hàng đầu của Mạng trao đổi ngăn xếp, được tạo ra vào năm 2008 bởi Jeff Atwood và Joel Spolsky .

Ngày 10 tháng 4 năm 2020. Bạn có hối hận khi sử dụng Haskell không? CH:⁵⁴²

Có lẽ chúng tôi đã có thể bỏ qua F# hoặc Scala thay vì Haskell và nhận được rất nhiều lợi ích từ Haskell. Tôi đã không nhận ra rằng Haskell sẽ yêu cầu nhiều như nó đã làm... và tôi đã không chuẩn bị cho điều đó, chúng tôi đã không thiết lập cơ cấu tổ chức mà chúng tôi cần ngay từ đầu cho điều đó và tôi đã chuẩn bị tốt hơn trong ban đầu, chúng tôi có lẽ đã có thể tránh được một số nỗi đau ngày càng tăng mà chúng tôi đã mắc phải. Mặt khác, chúng tôi đã có thể thu hút một số bộ óc thông minh nhất trên thế giới và làm việc với những bộ óc đó để giải quyết vấn đề theo những cách sáng tạo hoàn toàn nguyên bản và vì vậy Cardano cuối cùng là một sản phẩm tốt hơn cho nó nhưng thời gian đưa ra thị trường của chúng tôi bị ảnh hưởng. Đó có phải là quyết định đúng đắn hay không... Ai mà biết được?!

Bởi vì chúng tôi phải xem xét dự án vào năm 2022 và 2023 và nếu chúng tôi có quy mô, phạm vi và quy mô của Ethereum và chúng tôi có một hệ sinh thái mạnh mẽ có khả năng phục hồi thì đó là quyết định đúng đắn... nếu chúng tôi không ở đó, đó là quyết định sai lầm quyết định... nhưng chúng ta sẽ không biết. Chúng tôi đã thực sự quan tâm đến Scala; trên thực tế, chúng tôi đã viết một sản phẩm bằng Scala... và chúng tôi đã viết Mantis⁵⁴³, một ứng dụng khách Ethereum Classic trong Scala. Đó là một trải nghiệm tuyệt vời, tôi thích nó... Tôi đã rất vui vì chúng tôi không bị chậm trễ, dễ dàng thoát ra, nó giống như vẽ theo số... vì vậy tôi rất thích Scala, đó là một trong những ngôn ngữ yêu thích của tôi và Tôi nghĩ rằng có rất nhiều lợi thế trong hệ sinh thái đó. Các cạnh sắc nét hầu hết đã bị tắt tiếng.

Điều đó nói rằng, vì công việc chúng tôi đã làm với Haskell và những cải tiến mà chúng tôi đã thực hiện, đặc biệt là với GHCJS⁵⁴⁴ và những cải tiến⁵⁴⁵ chúng tôi đã thực hiện trên Windows và những cải tiến ở cấp độ thư viện mà chúng tôi đã thực hiện... nếu ai đó chọn Haskell hôm nay cho một dự án, với những thứ mà chúng tôi đã làm và hệ sinh thái đã làm, tôi nghĩ việc xây dựng một sản phẩm trong Haskell sẽ dễ dàng hơn rất nhiều. Chúng tôi đã để lại một mẫu để làm điều đó và các dự án trong tương lai sẽ không gặp phải những khó khăn ngày càng tăng mà chúng tôi đã gặp phải.

Tại một thời điểm, tôi thực sự đã cân nhắc việc viết Cardano bằng JavaScript... Tôi thực sự nghĩ về điều đó, tôi đã nói rằng chúng tôi có ngữ nghĩa chính thức thông qua chương trình JSCert, ngoài Imperial College London,⁵⁴⁶ và có một số chức năng mà chúng tôi có thể làm... và chúng tôi có thể làm chính thức xác minh một số mã JavaScript... vì vậy đây là một ý nghĩ điên rồ... tại sao chúng ta không thực sự thuê một số lập trình viên lỗi cứng Haskell và sau đó buộc họ thực sự viết JavaScript? ... và xây dựng toàn bộ hệ sinh thái xung quanh nó, viết một loạt công cụ JavaScript tuyệt đẹp cho QuickCheck⁵⁴⁷ và cho tất cả những thứ khác và thực sự tạo một⁵⁴⁸ công TLA... để chúng tôi có thể thực hiện TLA+ và kết nối nó với mã JavaScript.

⁵⁴²

TRỰC TIẾP với Charles Hoskinson của Cardano, youtu.be/x6TZSBmDWMw?t=5107

⁵⁴³

Niamh Ahern, 'The new Mantis: Mang lại tính bảo mật và ổn định cho hệ sinh thái Ethereum Classic', iohk.io/en/blog/posts/2020/12/09/the-new-mantis-bringing-security-and-stability-to-the-ethereum-classic-ecosystem-1/

⁵⁴⁴

Luite Stegeman, 'Hướng tới tương lai của Haskell và JavaScript cho Plutus', iohk.io/en/blog/posts/2020/06/04/looking-to-the-future-of-haskell-and-javascript-for-plutus/

⁵⁴⁵

Sylvain Henry, 'Cải thiện hỗ trợ số lớn của Haskell', iohk.io/en/blog/posts/2020/07/28/improving-haskells-big-numbers-support/

⁵⁴⁶

JSCert : Chính thức hóa ngôn ngữ lập trình JavaScript, wp.doc.ic.ac.uk/fswp/project/jscert-formalization-of-the-javascript-programming-language/

⁵⁴⁷

Kiểm tra nhanh, hackage.haskell.org/package/QuickCheck

⁵⁴⁸

TLA⁺ là một ngôn ngữ đặc tả chính thức được phát triển bởi Leslie Lamport. Nó được sử dụng để thiết kế, mô hình hóa, lập tài liệu và xác minh các chương trình, đặc biệt là các hệ thống đồng thời và hệ thống phân tán

Chương 7: Marlowe

'Địa ngục chỉ là một khung cửa tâm trí'

- Christopher Marlowe, Tiến sĩ Faustus

Marlowe là gì?

Marlowe là một ngôn ngữ lập trình đơn giản để viết các hợp đồng thông minh tài chính cho Cardano. Nó được đặt theo tên của nhà thơ, nhà soạn kịch và điệp viên thời Elizabeth, Christopher Marlowe. Marlowe bị giới hạn trong các ứng dụng tài chính và không phải là Turing-đầy đủ. Nó dành cho những người là chuyên gia về tài chính hơn là có kiến thức về lập trình.

Marlowe dựa trên nghiên cứu được đánh giá ngang hàng được thực hiện bởi một nhóm do Giáo sư Simon Thompson đứng đầu, đầu tiên tại Đại học Kent với sự trợ giúp của khoản tài trợ nghiên cứu IOG, sau đó là một nhóm IOG nội bộ phối hợp với Blockchain nâng cao của Đại học Wyoming Phòng thí nghiệm R&D. Nghiên cứu đã dẫn đến một số bài báo được xuất bản.⁵⁴⁹

Bối cảnh cho Marlowe

'Mã máy' đã được sử dụng để lập trình những chiếc máy tính đầu tiên. Mỗi hệ thống có mã riêng của nó, cấp độ thấp và không biểu cảm: các chương trình là những chuỗi dài các lệnh cực kỳ đơn giản mà bất kỳ ai không tạo ra chúng đều không thể hiểu được. Các ngôn ngữ cấp cao hơn như C, Java và Haskell hiện có thể được sử dụng để lập trình hệ thống. Cấu trúc của các chương trình phản ánh những gì chúng thực hiện và các ngôn ngữ giống nhau có thể được sử dụng trên nhiều loại thiết bị. Các ngôn ngữ như Plutus, Solidity và Simplicity là các đối tác của Blockchain. Những ngôn ngữ cấp cao hơn này có mục đích chung ở chỗ chúng có thể được sử dụng để giải quyết nhiều vấn đề khác nhau; tuy nhiên, các giải pháp mà chúng đại diện vẫn là các chương trình và việc sử dụng chúng thành công đòi hỏi chuyên môn về lập trình.

Mặt khác, Marlowe cung cấp các hợp đồng tài chính Blockchain mà bất kỳ ai cũng có thể viết. Đó là ngôn ngữ dành riêng cho miền (DSL) để tạo và thực hiện các hợp đồng tài chính cho phép người dùng sử dụng kiến thức về miền của họ để nhanh chóng tạo và quản lý hợp đồng mà không cần quá trình học tập phức tạp đi kèm với phát triển phần mềm, Blockchain và hợp đồng thông minh.

Marlowe là ngôn ngữ lập trình thân thiện với người dùng có thể được sử dụng để bắt chước các sản phẩm tài chính. Đó là một nền tảng tài chính phi tập trung (DeFi) cho phép cho vay ngang hàng trực tiếp, hợp đồng chênh lệch (CFD)⁵⁵⁰ và các sản phẩm liên quan khác. Các hợp đồng Marlowe được điều chỉnh cho các giao dịch tài chính, nền tảng phát triển và theo dõi nhanh các nhà cung cấp dịch vụ tài chính để thiết lập năng lực trong các hợp đồng thông minh và công nghệ Blockchain.

Hợp đồng Marlowe dễ đọc, viết và hiểu hơn vì chúng được viết bằng một ngôn ngữ có mục đích đặc biệt. Nó cũng an toàn hơn: không thể tạo ra một số lỗi nhất định và IOG có thể phân tích đầy đủ hành vi của hợp đồng mà không cần chạy hợp đồng. Marlowe có một số lợi thế so với ngôn ngữ hoàn chỉnh Turing. Nó an toàn hơn, có thể dự đoán được và giải quyết vấn đề tạm dừng⁵⁵¹ bằng cách đảm bảo chấm dứt.

Các tính năng thiết kế của Marlowe:

- Không có đệ quy⁵⁵² hoặc vòng lặp vì hợp đồng là hữu hạn
- Có thời gian chờ trên tất cả các hành động, đảm bảo chấm dứt
- Các cam kết và thời gian chờ là trung tâm của cách Marlowe hoạt động trong bối cảnh Blockchain
- Tất cả các hợp đồng đều có thời hạn xác định
- Không có tài sản nào được giữ lại khi đóng
- Giá trị được bảo tồn.

Đối tượng mục tiêu của Marlowe là ai?

⁵⁴⁹ Giấy tờ Marlowe, play.marlowe-finance.io/doc/marlowe/tutorials/introducing-marlowe.html#research-based

⁵⁵⁰ Trong tài chính, **hợp đồng chênh lệch (CFD)** là hợp đồng giữa hai bên, thường được mô tả là 'người mua' và 'người bán', quy định rằng người bán sẽ trả cho người mua khoản chênh lệch giữa giá trị hiện tại của một tài sản và giá trị của nó tại thời điểm hiện tại. thời gian hợp đồng (nếu chênh lệch âm thì bên mua thanh toán thay cho bên bán).

⁵⁵¹ Trong lý thuyết tính toán, **vấn đề tạm dừng** là vấn đề xác định, từ mô tả của một chương trình máy tính tùy ý và đầu vào, liệu chương trình sẽ chạy xong hay tiếp tục chạy mãi mãi.

⁵⁵² **Đệ quy** xảy ra khi một cái gì đó được định nghĩa theo chính nó hoặc theo kiểu của nó. Đệ quy được sử dụng trong nhiều lĩnh vực khác nhau, từ ngôn ngữ học đến logic. Ứng dụng phổ biến nhất của đệ quy là trong toán học và khoa học máy tính, trong đó một hàm được định nghĩa được áp dụng theo định nghĩa của chính nó. Mặc dù điều này rõ ràng xác định một số lượng vô hạn các thể hiện (giá trị hàm), nhưng nó thường được thực hiện theo cách mà không có vòng lặp vô hạn nào có thể xảy ra.

Bởi vì Marlowe cho phép bạn viết hợp đồng bằng đồ họa cũng như bằng mã thông thường hơn, nó có thể được sử dụng bởi một người là chuyên gia về chủ đề hợp đồng tài chính hoặc kinh doanh nhưng thiếu khả năng và kiến thức chuyên môn về lập trình. Nó có thể được các tổ chức tài chính sử dụng để tạo và triển khai các công cụ độc đáo cho khách hàng và khách hàng của họ.

Ngôn ngữ Marlowe được nhúng trong cả JavaScript và Haskell, cung cấp cho bạn nhiều trình chỉnh sửa để lựa chọn, tùy thuộc vào sở thích và trình độ kỹ năng của bạn. Bạn có thể viết hợp đồng bằng các ngôn ngữ này và sau đó chuyển đổi ('biên dịch') chúng thành Marlowe trong Sân chơi Marlowe. Haskell là ngôn ngữ lập trình chức năng với hệ sinh thái được thiết lập riêng và môi trường thử nghiệm mạnh mẽ, nhưng JavaScript cung cấp tính linh hoạt và tốc độ sử dụng với một cộng đồng sôi động.

Marlowe có thể tương tác với dữ liệu trong thế giới thực, chẳng hạn như lời tiên tri và những người tham gia hợp đồng có thể chọn những gì xảy ra trên và ngoài chuỗi, chẳng hạn như trong ví, bằng cách đưa ra quyết định bên trong quy trình hợp đồng. Marlowe là Blockchain-agnostic, cho phép các liên hệ thông minh được thể hiện trên các mô hình dựa trên tài khoản như Ethereum cũng như mô hình đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO) của Cardano. Marlowe là một giải pháp quy mô ngành kết hợp các ví dụ từ ACTUS⁵⁵³ (actusfrf.org) tiêu chuẩn phân loại và hợp đồng tài chính.

Cấu trúc ngôn ngữ Marlowe

Marlowe dựa trên các ngôn ngữ hợp đồng tài chính dành cho mục đích đặc biệt được các học giả và công ty như Lexifi (lexifi.com) áp dụng, chuyên sản xuất phần mềm hợp đồng tài chính. IOG đã tùy chỉnh các ngôn ngữ này để hoạt động trên Blockchain trong khi tạo Marlowe. Marlowe là một ngôn ngữ đơn giản với một vài cấu trúc riêng biệt xác định hành vi với một số vai trò cố định, hạn chế cho mỗi hợp đồng. Các trách nhiệm này do các bên trong hợp đồng thực hiện.

Các hợp đồng có thể được xây dựng bằng cách kết hợp một số lượng hạn chế các cấu trúc này, có thể được sử dụng để mô tả và đại diện cho một loạt các hợp đồng tài chính. Một hợp đồng đang chạy có thể thực hiện thanh toán cho một vai trò hoặc khóa công khai, một hợp đồng có thể chờ hành động của một trong các vai trò, chẳng hạn như tiền gửi hoặc quyết định từ một tập hợp các tùy chọn chỉ là một vài ví dụ. Điều quan trọng là hợp đồng không thể đợi mãi để thực hiện một hành động: nếu không có hành động nào được thực hiện trong một khoảng thời gian nhất định (thời gian chờ), hợp đồng sẽ tiếp tục theo một lộ trình khác, chẳng hạn như thực hiện hành động khác phục chẳng hạn như hoàn trả bất kỳ khoản tiền nào trong hợp đồng. hợp đồng.

Một hợp đồng có thể lựa chọn giữa hai hướng hành động khác nhau trong tương lai, mỗi hướng là một hợp đồng, tùy thuộc vào điều kiện hiện tại của nó. Hợp đồng sẽ chấm dứt khi không còn hoạt động nào cần thiết nữa và mọi khoản tiền còn lại trong hợp đồng sẽ được hoàn trả. Khi một hợp đồng được thực hiện, các nhiệm vụ mà nó đòi hỏi sẽ được hoàn thành bởi những người tham gia (danh tính Blockchain). Mỗi vị trí trên Blockchain được đại diện bởi một Token và các vai trò có thể được trao đổi trong quá trình thực hiện hợp đồng, do đó cho phép chúng được giao dịch.

Marlowe là ngôn ngữ dành riêng cho miền cho DeFi

Có nhiều lợi ích khi dành riêng cho miền thay vì mục đích chung. Hợp đồng được viết bằng ngôn ngữ định hướng tài chính thay vì ngôn ngữ dành riêng cho Blockchain. Do đó, một số loại sai lầm không thể viết được, và một số loại hợp đồng không phù hợp bị loại bỏ. Ví dụ, mọi hợp đồng Marlowe sẽ có thời hạn cố định, sau đó nó sẽ ngừng thực hiện các hành vi và mọi khoản tiền đính kèm trong hợp đồng sẽ được trả lại cho những người tham gia, nghĩa là tiền trong hợp đồng không bao giờ có thể bị khóa vĩnh viễn.

Không cần thực hiện hợp đồng, có thể tự động phân tích cách hợp đồng sẽ phản ứng trong mọi tình huống. Ví dụ: bạn có thể đánh giá liệu một hợp đồng có thể không thanh toán được trong một số trường hợp nhất định hay không hoặc liệu nó có được đảm bảo thanh toán đầy đủ trong mọi trường hợp hay không.

Hành vi hợp đồng có thể được sao chép trong trình duyệt, cho phép người dùng thử nghiệm các tình huống khác nhau trước khi cam kết tiền mặt và thực hiện hợp đồng thực sự. Người dùng có thể xây dựng hợp đồng DeFi theo nhiều phương pháp khác nhau, bao gồm viết chúng dưới dạng văn bản hoặc sử dụng lập trình trực quan để tạo hợp đồng thông minh bằng cách kết nối các Block đại diện cho các thành phần khác nhau. Người dùng cũng có thể chọn và chọn từ nhiều mẫu khác nhau, sau đó họ có thể tùy chỉnh theo yêu cầu.

bộ phân biệt Marlowe

Cách Marlowe đảm bảo rằng hợp đồng được tuân thủ là điểm khác biệt giữa Marlowe với các lựa chọn thay thế không phải Blockchain. Điều này không chỉ giả định rằng các hướng dẫn của hợp đồng được tuân theo mà còn là những người tham gia cam kết và không dễ dàng bị khóa trong hợp đồng vô thời hạn. Thời gian chờ được sử dụng để thực hiện điều này.

553

ACTUS (Tiêu chuẩn thống nhất cho các loại hợp đồng thuật toán) Các loại hợp đồng được xác định dựa trên các mẫu thuật toán hợp đồng cơ bản tương ứng bao gồm các loại sản phẩm tài chính khác nhau mà mỗi mẫu Loại hợp đồng có thể thể hiện.

Một hợp đồng có thể yêu cầu một người đặt cọc một số tiền nhất định, nhưng nó không thể bắt buộc người đó làm như vậy. Thay vào đó, hợp đồng có thể đợi họ cam kết với hợp đồng trong một khoảng thời gian nhất định, sau đó hợp đồng sẽ tiếp tục thực hiện theo một số hướng dẫn thay thế. Điều này cấm một bên hủy bỏ hợp đồng bằng cách từ chối tham gia, đảm bảo rằng không có bế tắc.

Thời gian chờ bảo vệ tất cả các cấu trúc của Marlowe cần đầu vào của người dùng, chẳng hạn như tiền gửi của người dùng và lựa chọn của người dùng. Do đó, thật dễ dàng để nhận thấy rằng cam kết của người dùng đối với hợp đồng là hữu hạn: Marlowe có thể thấy trước khi nào hợp đồng sẽ được hoàn thành - khi nào hợp đồng có thể được đóng lại. Bất kỳ tài sản chưa sử dụng nào trong hợp đồng đều được hoàn trả cho người tham gia vào thời điểm này và hợp đồng sẽ kết thúc. Do đó, bất kỳ tài sản nào được gửi vào hợp đồng bởi người tham gia đều không thể bị khóa vô thời hạn: cam kết về cơ bản chấm dứt tại thời điểm này.

Hơn nữa, thật đơn giản để chúng ta đọc từ hợp đồng khi nào nó sẽ kết thúc, mà Marlowe gọi là thời hạn của hợp đồng: tất cả các bên sẽ có thể xác định thời hạn này trước khi ký kết bất kỳ hợp đồng nào .

Hợp đồng đang chạy ở Marlowe không thể yêu cầu đặt cọc hoặc lựa chọn; nó chỉ có thể tìm kiếm một khoản tiền gửi hoặc một lựa chọn từ người dùng. Nó không thể 'đẩy' những hành động này, nhưng nó có thể 'kéo' chúng. Tuy nhiên, nó có thể thực hiện thanh toán tự động, do đó, một số tính năng của hợp đồng Marlowe có thể 'thúc đẩy' một số sự kiện nhất định xảy ra, chẳng hạn như đảm bảo rằng khoản thanh toán được gửi tới người tham gia bằng cách tạo đầu ra giao dịch phù hợp.

Vì Marlowe là một DSL nên nó có thể dự đoán cách hợp đồng Marlowe sẽ hoạt động mà không cần phải thực hiện chúng: nghĩa là bạn có thể tận dụng phân tích tĩnh⁵⁵⁴ để đưa ra chẩn đoán quan trọng cho người dùng trước khi họ ký hợp đồng. Marlowe cũng có thể tận dụng các công cụ logic để thiết lập rõ ràng các thuộc tính của hợp đồng Marlowe, cung cấp cho người dùng mức độ chắc chắn tối đa rằng hợp đồng của họ sẽ thực hiện như dự định.

lộ trình Marlowe

IOG sẽ hoàn thành việc triển khai Marlowe trên Cardano như một phần của triển khai Goguen, cho phép các cá nhân và tổ chức thực hiện các hợp đồng DeFi mà họ tự viết hoặc nhận được từ kho lưu trữ hợp đồng, chuyển tài sản Crypto theo các điều kiện của hợp đồng. Ban đầu, Marlowe sẽ hoạt động trên Blockchain Cardano, nhưng cuối cùng nó sẽ không liên quan đến Blockchain và có thể hoạt động trên các Blockchain khác trong tương lai.

Thông qua các nhà tiên tri, các hợp đồng thông minh Cardano sẽ có thể truy xuất các giá trị dữ liệu bên ngoài như tỷ giá hối đoái giữa ADA và Bitcoin. Ở một số khía cạnh, một nhà tiên tri tương tự như một người tham gia đưa ra quyết định và là một phần của việc triển khai, IOG muốn cung cấp các giá trị của nhà tiên tri, cho phép các hợp đồng nhận được các giá trị trực tiếp từ 'mã đánh dấu' trên thị trường chứng khoán hoặc nguồn cấp dữ liệu như CoinMarketCap .

Tùy thuộc vào khả năng lập trình của họ, các chuyên gia tài chính và nhà phát triển giờ đây có thể bắt đầu viết các hợp đồng tài chính thông minh trực tiếp trong Haskell hoặc Marlowe thuần túy hoặc bằng đồ họa bằng Marlowe Playground. Sau này vào kỷ nguyên Goguen, bạn có thể mô phỏng và phân tích các hợp đồng bạn xây dựng trong Sân chơi để đảm bảo rằng chúng hoạt động chính xác và sẵn sàng được phát hành vào thế giới tiền phi tập trung. Khi IOG chuẩn bị hoàn thành việc triển khai Marlowe trên Cardano và giới thiệu các hợp đồng thông minh tài chính cho chính Blockchain, nhóm IOG Marlowe sẽ tiếp tục triển khai các ví dụ từ tiêu chuẩn Actus.

Cấu trúc ngôn ngữ Marlowe

các loại Haskell

Các thành phần khác nhau của hợp đồng, chẳng hạn như tài khoản, giá trị, quan sát và hành động, được thể hiện bằng các loại Haskell. Các thành phần Marlowe này được sử dụng để quản lý cách một hợp đồng đang chạy phát triển bằng cách cung cấp thông tin và đầu vào bên ngoài. Các phần cơ bản của Marlowe được lập mô hình bằng cách sử dụng kết hợp các loại dữ liệu Haskell, phát triển các loại mới và các từ đồng nghĩa của loại, cung cấp cho loại hiện có một tên mới.

Bạn có thể sử dụng một trong các môi trường lập trình trực quan sau đây ngoài việc phát triển các hợp đồng trong phiên bản văn bản của Marlowe:

Sử dụng Blockly⁵⁵⁵

⁵⁵⁴

Phân tích tĩnh , phép chiếu tĩnh hoặc tính điểm tĩnh là một phân tích đơn giản hóa trong đó tác động của một thay đổi tức thời đối với hệ thống được tính toán mà không tính đến phản ứng dài hạn của hệ thống đối với thay đổi đó.

⁵⁵⁵

hợp đồng Marlowe

Ở Marlowe, một hợp đồng được tạo thành từ một tập hợp nhỏ các Block xây dựng có thể được sử dụng để thể hiện nhiều giao dịch tài chính khác nhau, chẳng hạn như thanh toán, thực hiện quan sát, chờ đợi cho đến khi một điều kiện cụ thể trở thành sự thật, v.v. Sau đó, hợp đồng được thực hiện trên một Blockchain, chẳng hạn như Cardano và nó tương tác với thế giới bên ngoài.

Marlowe được viết bằng Haskell và nó được biểu diễn dưới dạng một tập hợp các kiểu dữ liệu đại số, với các hợp đồng được chỉ định bởi loại Hợp đồng:

```
Hợp đồng dữ liệu = Đóng
| Hợp đồng giá trị Token của bên thanh toán
| Nếu Quan sát Hợp đồng Hợp đồng
| Khi [Trường hợp] Hợp đồng hết hạn
| Hãy để hợp đồng giá trị ValueId
| Khẳng định hợp đồng quan sát
```

Marlowe đưa ra sáu cách khác nhau để xây dựng hợp đồng. Năm trong số các phương thức này – Thanh toán, Cho phép, Nếu, Khi nào và Khẳng định – kết hợp các hợp đồng nhỏ hơn để tạo ra một hợp đồng phức tạp hơn, trong khi phương thức thứ sáu, Đóng, là một hợp đồng cơ bản. Hiệu ứng – thanh toán – và cảnh báo có thể được tạo ở mỗi giai đoạn thực hiện, ngoài việc tạo ra một trạng thái mới và hợp đồng tiếp tục.

Chi trả

Hợp đồng thanh toán **Pay aptv cont** sẽ chuyển giá trị **v** của token **t** từ tài khoản **a** sang người được thanh toán **p**, đây sẽ là một trong những người tham gia hợp đồng hoặc một tài khoản khác trong hợp đồng. Nếu giá trị **v** không dương hoặc nếu số dư tài khoản không đủ để chi trả toàn bộ khoản thanh toán, cảnh báo sẽ được đưa ra (ngay cả khi có số dư dương của các Token khác trong tài khoản). Một phần thanh toán (của tất cả các khoản tiền có sẵn) được thực hiện trong tình huống sau. Hợp đồng tiếp tục, **cont**, được đưa ra trong hợp đồng.

Đóng

Hợp đồng **Đóng** biểu thị việc đóng (hoặc chấm dứt) hợp đồng. Chức năng duy nhất của nó là cung cấp tiền hoàn lại cho chủ sở hữu tài khoản có số dư dương. Việc này được thực hiện cho từng tài khoản, tuy nhiên, tất cả các tài khoản đều được hoàn tiền cùng một lúc.

Trước tiên, chúng ta phải xác định các giá trị, quan sát và hành động trước khi chuyển sang các loại hợp đồng bổ sung:

- Giá trị - bao gồm các đại lượng thay đổi theo thời gian, chẳng hạn như 'khoảng thời gian đặt cược hiện tại', 'số dư hiện tại của một số Token trong tài khoản' và bất kỳ quyết định nào trước đó. Đây là những 'giá trị dễ bay hơi'. Các giá trị cũng có thể có điều kiện dựa trên một quan sát và được hợp nhất bằng cách sử dụng phép cộng, phép trừ và phép phủ định
- Quan sát - là các giá trị Boolean có thể được nối bằng cách sử dụng các toán tử Boolean điển hình và thu được bằng cách so sánh các giá trị. Cũng có thể xem liệu có bất kỳ quyết định nào đã được đưa ra hay không (đối với một lựa chọn đã xác định cụ thể). Các quan sát sẽ hữu ích ở mọi giai đoạn thực hiện
- Hành động - xảy ra tại những thời điểm nhất định trong suốt quá trình thực hiện, chẳng hạn như:
 - gửi tiền
 - chọn từ nhiều tùy chọn, bao gồm một giá trị tiên tri
 - cảnh báo hợp đồng về một quan sát hóa ra là đúng
- Tiên tri - Các tiên tri như Carli3 (charli3.io) và Ergo Pools đang được xây dựng cho Blockchain Cardano và sẽ có thể sử dụng được trong Marlowe trên Cardano. Cho đến thời điểm đó, có một nguyên mẫu tiên tri trong Sân chơi Marlowe. Oracles được thể hiện dưới dạng các quyết định được đưa ra bởi một người tham gia với vai trò Oracle chuyên dụng.

Nếu như

Viết Marlowe với Blockly, docs.cardano.org/ marlowe /writing- marlowe -with- blockly

⁵⁵⁶

Marlowe: Sử dụng JS Editor, docs.cardano.org/ marlowe /using- javascript -editor

⁵⁵⁷

Sử dụng trình soạn thảo Haskell, docs.cardano.org/ marlowe /using-the- haskell -editor

Vị từ **if obs cont1 cont2** sẽ dẫn đến **cont1** hoặc **cont2** , dựa trên quan sát giá trị Boolean của **obs** **mỗi** khi cấu trúc này được thực thi.

Khi

Với dạng **When cases timeout cont** , đây là hàm tạo hợp đồng phức tạp nhất. Đó là một hợp đồng được kích hoạt bởi các sự kiện có thể xảy ra hoặc không xảy ra tại bất kỳ thời điểm cụ thể nào: các trường hợp của hợp đồng xác định điều gì sẽ xảy ra khi một số sự kiện nhất định xảy ra.

Trong hợp đồng **Khi các trường hợp hết thời gian tiếp** , danh sách **các trường hợp** nắm giữ một bộ sưu tập các trường hợp. Mỗi trường hợp có dạng **Case ac co** trong đó **ac** là một hành động và **co** là sự tiếp tục (một hợp đồng khác). Ví dụ: khi một hành động nhất định xảy ra **ac** , trạng thái được cập nhật và hợp đồng sẽ tiếp tục dưới dạng tiếp tục tương ứng **co** .

Để đảm bảo hợp đồng cuối cùng hoàn thành, hợp đồng **Khi các trường hợp hết thời gian tiếp** **tục** sẽ tiếp tục như **một cont sau** khi đạt đến **thời gian chờ** , **một số vị trí**.

Cho phép

Hợp đồng **let id val cont** cho phép một hợp đồng ghi lại một giá trị, tại một thời điểm cụ thể và đặt tên cho nó bằng cách sử dụng mã định danh. Trong ví dụ này, biểu thức **val** được ước tính và được lưu trữ với tên **id** . Hợp đồng sau đó tiếp tục như **cont** .

Cách tiếp cận này không chỉ cho phép chúng tôi tận dụng các chữ viết tắt mà còn cho phép chúng tôi nắm bắt và lưu giữ dữ liệu không ổn định có thể thay đổi theo thời gian, chẳng hạn như giá gas hiện tại hoặc số vị trí hiện tại, tại một thời điểm cụ thể trong quá trình thực hiện hợp đồng, để được sử dụng sau này trong quá trình thực hiện hợp đồng.

khẳng định

Một hợp đồng xác nhận **Assert obs cont** không ảnh hưởng đến trạng thái của hợp đồng, nó tiếp tục ngay lập tức dưới dạng **cont** , nhưng nó đưa ra cảnh báo khi Observation **trả** về false. Nó có thể được sử dụng để đảm bảo rằng một tài sản được giữ ở bất kỳ giai đoạn nào của hợp đồng, vì phân tích tĩnh ⁵⁵⁸sẽ không thành công nếu bất kỳ việc thực thi nào buộc một **Khẳng định** dẫn đến sai.

Có một hợp đồng ký quỹ mẫu ⁵⁵⁹trong Cardano Docs.

Ký quỹ ở Marlowe

Các cấu trúc bổ sung được bao gồm trong hợp đồng Marlowe để đảm bảo rằng chúng tiến triển phù hợp. Khi chúng ta quan sát **When** , chúng ta cũng phải cung cấp thêm hai chi tiết:

- Giá trị thời gian chờ mà sau đó hợp đồng sẽ tiếp tục
- Hợp đồng tiếp tục mà nó ứng trước

Tài khoản Marlowe và việc sử dụng Token

Tài khoản Marlowe có thể lưu trữ nhiều loại tiền tệ cũng như Token có thể thay thế và không thể thay thế. Số tiền đã đặt được lập chỉ mục bởi **Token** , là một cặp **CurrencySymbol** và **TokenName** . Coi Tài khoản là Số nguyên Token bản đồ, trong đó:

dữ liệu Token = Token Tên tệSymbol Tên Token

Token ADA của Cardano được ký hiệu là **Token ADASymbol ADAToken**

⁵⁵⁸

Phân tích tĩnh là một phân tích đơn giản hóa trong đó tác động của một thay đổi tức thì đối với một hệ thống được tính toán mà không tính đến phản ứng dài hạn của hệ thống đối với thay đổi đó. Nếu tác động ngắn hạn sau đó được ngoại suy sang dài hạn, thì phép ngoại suy như vậy là không phù hợp.

⁵⁵⁹

Hợp đồng ký quỹ mẫu, github.com/cardano-foundation/docs-cardano-org/blob/main/marlowe/marlowe-lang-guide.md

Sân chơi Marlowe

Lý tưởng nhất là người dùng muốn hiểu các hợp đồng sẽ hoạt động như thế nào sau khi được triển khai vào Blockchain, nhưng không có rủi ro khi triển khai thực sự. Marlowe có thể trợ giúp ở đây vì nó sao chép hành vi hợp đồng ngoài chuỗi trong Sân chơi Marlowe.

Sân chơi Marlowe là một môi trường hợp cát trực tuyến, nơi bạn có thể xây dựng, lập mô hình, mô phỏng và thử nghiệm quá trình phát triển hợp đồng thông minh mà không cần phải cài đặt bất kỳ thứ gì. Mục tiêu của nó là trao quyền cho tất cả các loại nhà phát triển để tạo ra các sản phẩm tài chính trên Cardano, ngay cả khi họ không có kiến thức về Haskell hoặc JavaScript trước đó. Có một số hướng dẫn⁵⁶⁰ có sẵn trình bày chi tiết các hợp đồng mẫu cũng như thông tin chung về Marlowe và cách hợp đồng nên được lập mô hình.

Sân chơi Marlowe là một nền tảng để tạo các hợp đồng thông minh tài chính từ đầu đến cuối. Các nhà phát triển có thể sử dụng nó để không chỉ xây dựng mã hợp đồng thông minh mà còn để thực hiện thiết kế lặp lại ban đầu bằng cách sử dụng mô phỏng, chính thức xác thực hợp đồng thông minh và thử nghiệm chúng. Những đặc điểm này, cùng với DSL (ngôn ngữ dành riêng cho miền) dành riêng cho tài chính, đảm bảo rằng các hợp đồng dễ tạo, an toàn, có thể kiểm chứng và được thử nghiệm tốt.

Marlowe được viết trong Sân chơi có thể được lưu dưới dạng ý chính GitHub.⁵⁶¹ Sau đó, các dự án có thể được tải lại hoặc sao chép. Dự án được lưu trữ trong các phiên ngay cả khi bạn không sử dụng GitHub, tuy nhiên, hãy cẩn thận vì xóa bộ nhớ cache của trình duyệt có thể xóa công việc của bạn.

Bắt đầu

Khi sử dụng Sân chơi Marlowe, bạn có ba lựa chọn để chọn. Bạn có thể viết trực tiếp bằng văn bản Marlowe, nhưng bạn cũng có thể sử dụng hình ảnh. Blockly là một công cụ lập trình trực quan cho phép bạn thiết kế hợp đồng bằng cách kết nối các Block đại diện cho các thành phần khác nhau.

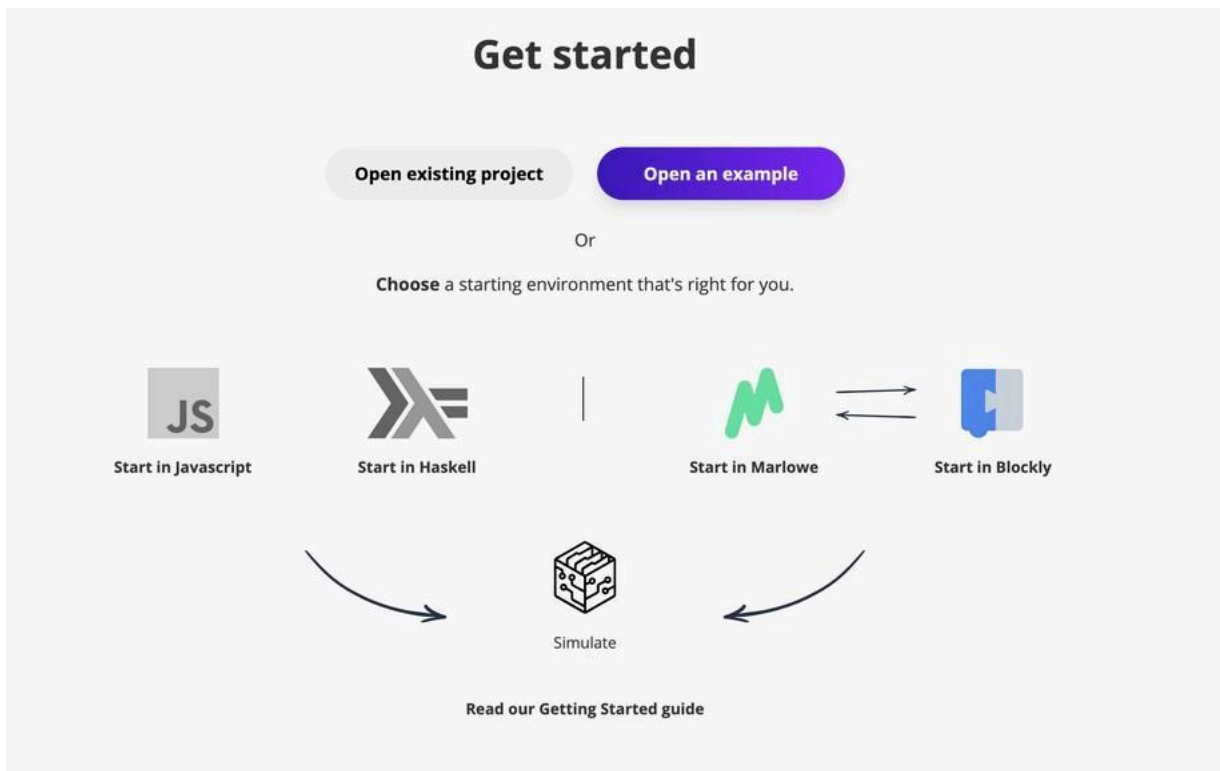
Bạn cũng có thể sử dụng trình soạn thảo Haskell hoặc JavaScript có sẵn để giúp bạn viết các hợp đồng Marlowe ngắn gọn và dễ đọc hơn. Sau khi hợp đồng được tạo, bạn có thể kiểm tra hành vi của nó, chẳng hạn như xác định xem có bất kỳ khoản thanh toán nào của hợp đồng có thể không thành công hay không. Bạn cũng có thể mô phỏng hoạt động của các bên để xem hợp đồng sẽ hoạt động như thế nào.

⁵⁶⁰

Hướng dẫn về Marlowe, alpha.marlowe.iohkdev.io/doc/marlowe/tutorials/index.html

⁵⁶¹

GitHub Gist cho phép các nhà phát triển chia sẻ mã, ghi chú và đoạn mã ngay lập tức. Mỗi ý chính là một kho lưu trữ Git, có nghĩa là nó có thể được rẽ nhánh và sao chép.



Hình 23: Marlowe bắt đầu

Sử dụng Blockly với Marlowe

Bạn có thể sử dụng giao diện trực quan của Blockly để liên kết các phần của hợp đồng với nhau hoặc viết mã Marlowe trực tiếp dưới dạng văn bản Marlowe. Đây là một công cụ tuyệt vời cho những người không cảm thấy thoải mái với trình soạn thảo lập trình và thích viết hợp đồng bằng hình ảnh. Blockly được sử dụng bởi hàng trăm dự án khác, chẳng hạn như MIT App Inventor ⁵⁶²mà chính tôi đã sử dụng, nhiều tháng trước, để tạo các ứng dụng dành cho kỳ thi này. ⁵⁶³Tôi không có trải nghiệm người dùng liền mạch khi thực hiện những điều này với Blockly .

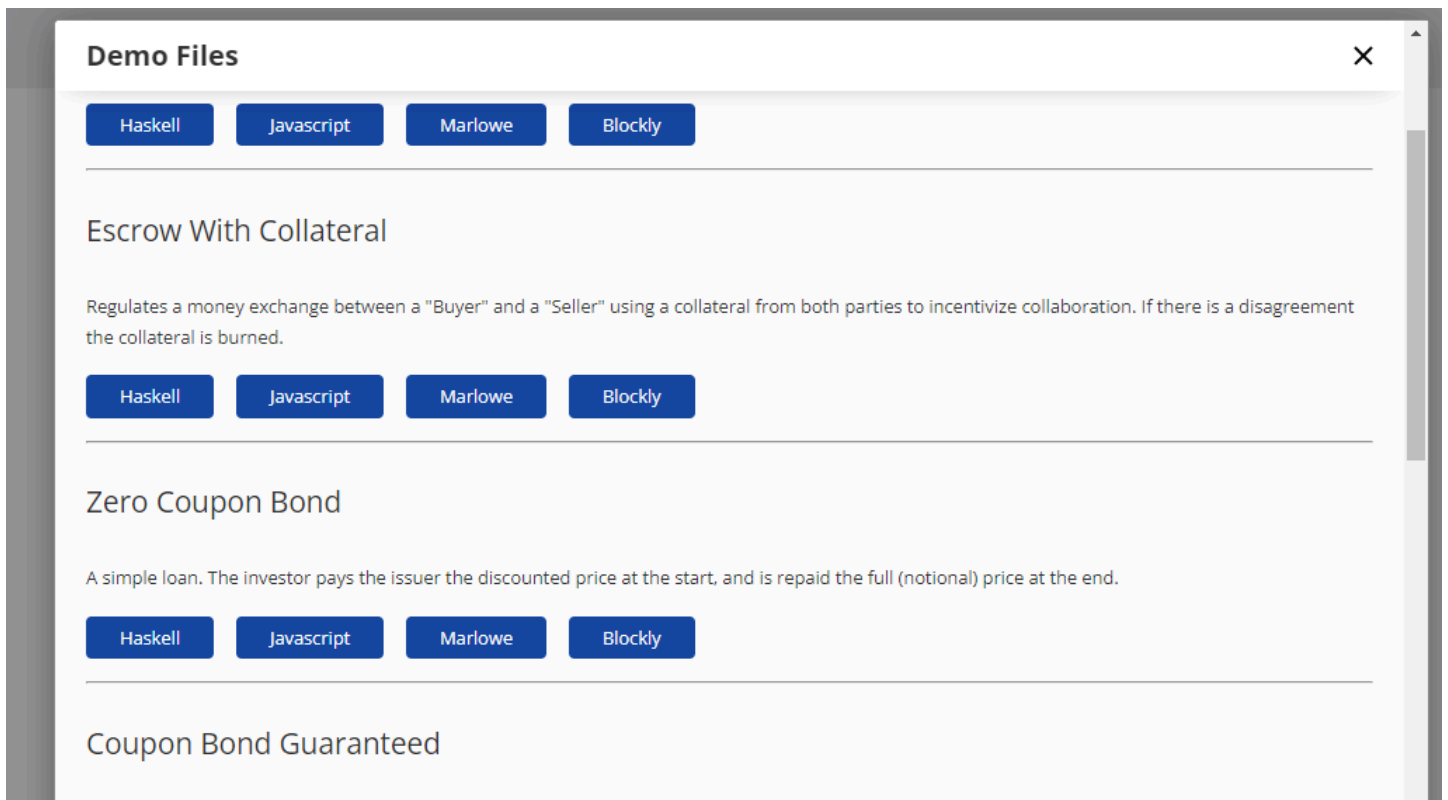
Chỉ với một vài cú nhấp chuột, thật dễ dàng để tạo hợp đồng trong Blockly bằng cách sử dụng tệp demo 'Zero Coupon Bond'. Hợp đồng 'Cho mượn sách của John' mất khoảng 10 phút để tạo. Tôi chỉ cần cập nhật một vài trình giữ chỗ trước khi có thể xem hợp đồng dưới dạng khối hoặc dưới dạng mã Marlowe. Trình chỉnh sửa Blockly cũng cung cấp cho bạn quyền truy cập vào trình chỉnh sửa siêu dữ liệu và phân tích tĩnh.

⁵⁶²

MIT AppInventor , appinventor.mit.edu/

⁵⁶³

Ứng dụng Greenelight ,
androidblip.com/dev/greenelight___a55fdd36512db0ebd6faad85f5a7e76687f8b28592819d76d5f18ec86f3b1cde.html



Hình 24: Các tập tin Demo Blockly

Hợp đồng được xây dựng bằng cách kéo và thả các thành phần vào các lỗ trong khối. Các Block được chọn bằng cách chỉ cần nhấp vào chúng, khối hoạt động hiện tại bạn đang sử dụng sẽ có đường viền màu vàng.

Play

Loan to buy John's book *

New ProjectOpenOpen ExampleRenameSaveSave As...

Contracts

Observations

Actions

Values

Payee

Party

Token

Bounds

by

the amount of

currency

into account of

continue as

Pay

payee

the amount of

of currency

from account of

continue as

Role Lender

ConstantParam Amount

ada

Role Lender

Party Role Borrower

ConstantParam Amount

ada

Role Lender

MetadataStatic AnalysisWarnings

Contract type:

Zero Coupon Bond

Contract name:

Loan to buy John's book

Contract short description:

A simple loan: the ****borrower**** borrows the `_amount_` from the ****lender****, and at the `_payback deadline_`

Contract long description:

This is a high risk/high reward contract. There is no guarantee that the ****borrower**** will pay back the loan

Role descriptions

Role "Borrower":

The party that borrows the `_amount_`.

Role "Lender":

The party that lends the `_amount_`.

Slot parameter descriptions

Slot parameter "Loan deadline":

The ****lender**** needs to deposit the `_amount_` by this time.

Slot parameter "Payback deadline":

The ****borrower**** needs to deposit the repayment (`_amount_` plus `_interest_`) by this time.

Value parameter descriptions

Hình 25: . Tab khởi

MetadataStatic AnalysisWarnings

Role descriptions

Role "Borrower":

The party that borrows the `_amount_`.

Role "Lender":

The party that lends the `_amount_`.

Slot parameter descriptions

Slot parameter "Loan deadline":

The ****lender**** needs to deposit the `_amount_` by this time.

Slot parameter "Payback deadline":

The ****borrower**** needs to deposit the repayment (`_amount_` plus `_interest_`) by this time.

Value parameter descriptions

Value parameter "Interest":

Fixed point amount

1

The interest paid by

Value parameter "Amount":

Fixed point amount

8

The amount borrow

Hình 26: Siêu dữ liệu dạng khối

into account of

continue as

Pay

payee

the amount of

of currency

from account of

continue as

Close

Role Borrower

Party

Role Lender

ConstantParam Interest + ConstantParam Amount

ada

Role Borrower

Metadata

Static Analysis

Warnings

Warning Analysis Result: Pass

Static analysis could not find any execution that results in any warning.

Analyse for warnings

Analyse reachability

Analyse for refunds on Close

Clear

cardano.org iohk.io

Hình 27: Cảnh báo

tác nghiên

Metadata

Static Analysis

Warnings

Timeout template parameters

Slot for **Loan deadline:**

340

Slot for **Payback deadline:**

500

Value template parameters

Constant for **Interest:**

₹ 1.0

Constant for **Amount:**

₹ 8.00000000

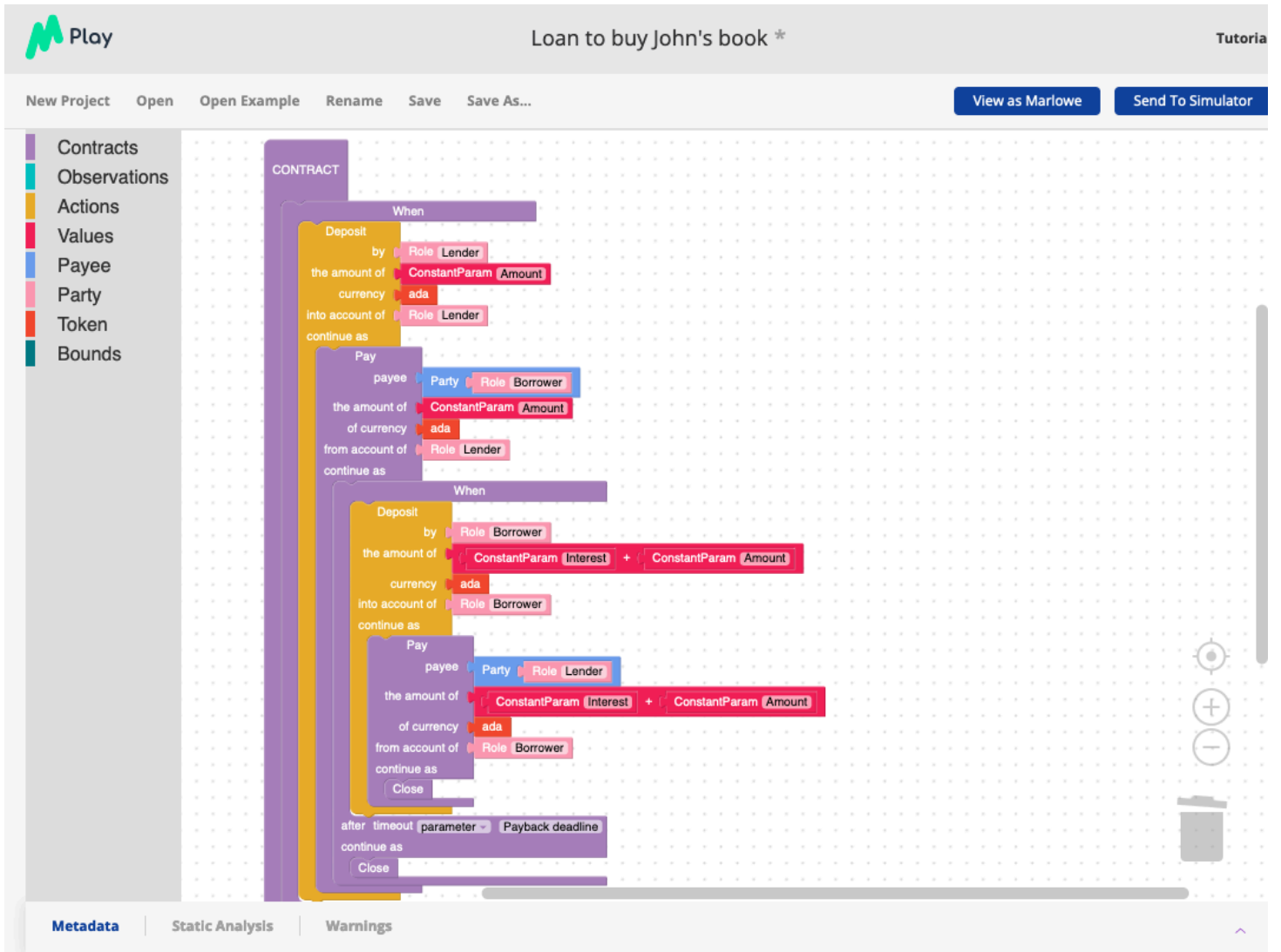
Analyse for warnings

Analyse reachability

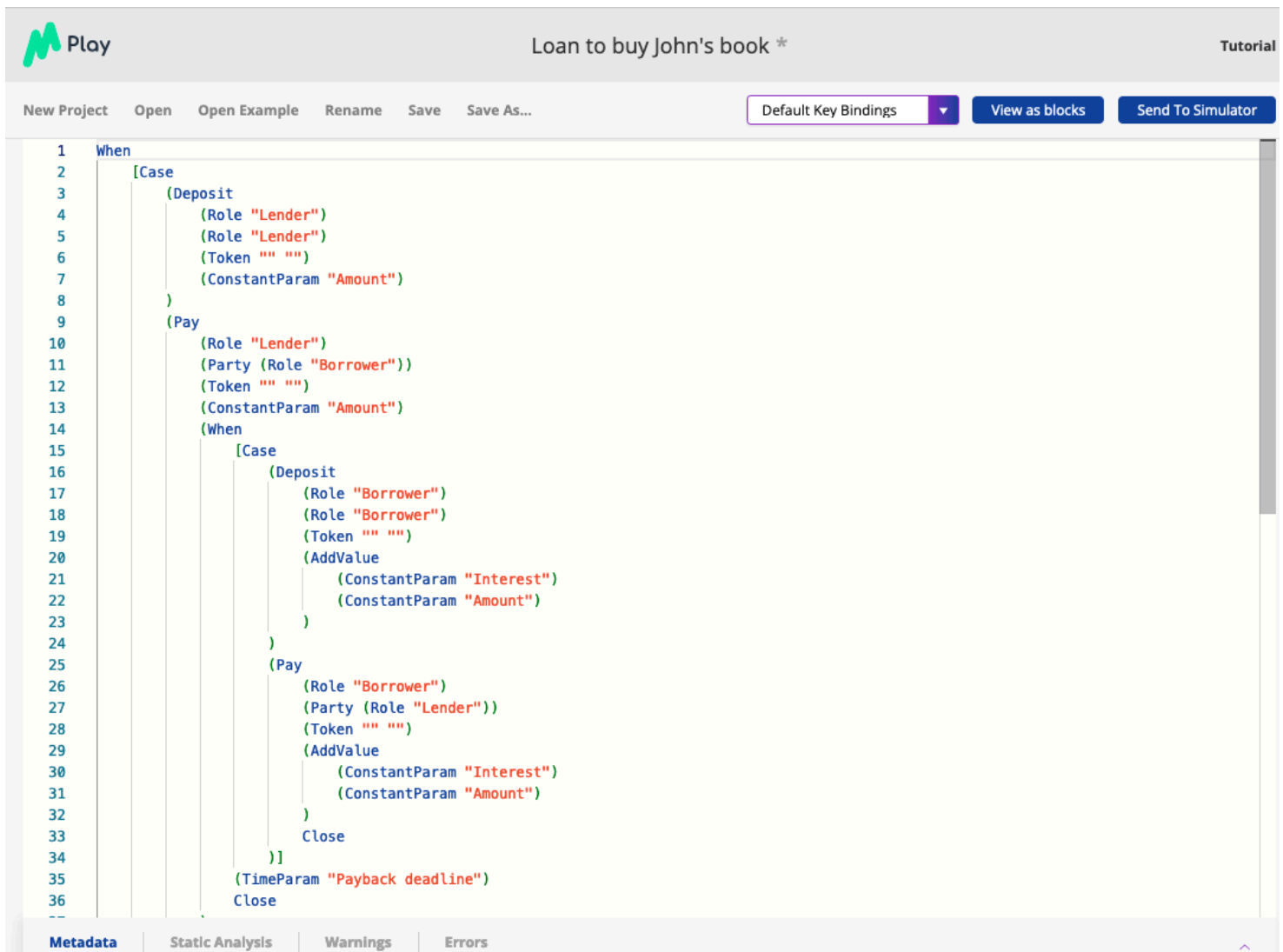
Analyse for refunds on Close

Clear

Hình 2 8: Phân tích tĩnh khối



Hình 29: Ví dụ khối



Hình 30: Marlowe Haskell

Sử dụng Trình chỉnh sửa cho Haskell hoặc JavaScript

Bạn có thể sử dụng trình soạn thảo Haskell để tạo mã Marlowe nếu bạn là nhà phát triển Haskell dày dạn kinh nghiệm. Vì Marlowe được xây dựng dưới dạng kiểu dữ liệu Haskell nên việc tạo hợp đồng thông minh Marlowe bằng Haskell rất dễ dàng. Chỉ cần chọn 'Haskell' trong 'Demo files' mẫu. Bạn có thể sử dụng Haskell để làm cho các định nghĩa hợp đồng dễ đọc hơn bằng cách sử dụng các định nghĩa Haskell cho các thành phần phụ, chữ viết tắt và các hàm mẫu đơn giản. Trình chỉnh sửa sẽ hỗ trợ bạn tự động hoàn thành, kiểm tra lỗi trong quá trình chỉnh sửa và liên kết các mẹo khi di chuột qua..

Zero Coupon Bond

A simple loan. The investor pays the issuer the discounted price at the start, and is repaid the full (notional) price at the end.

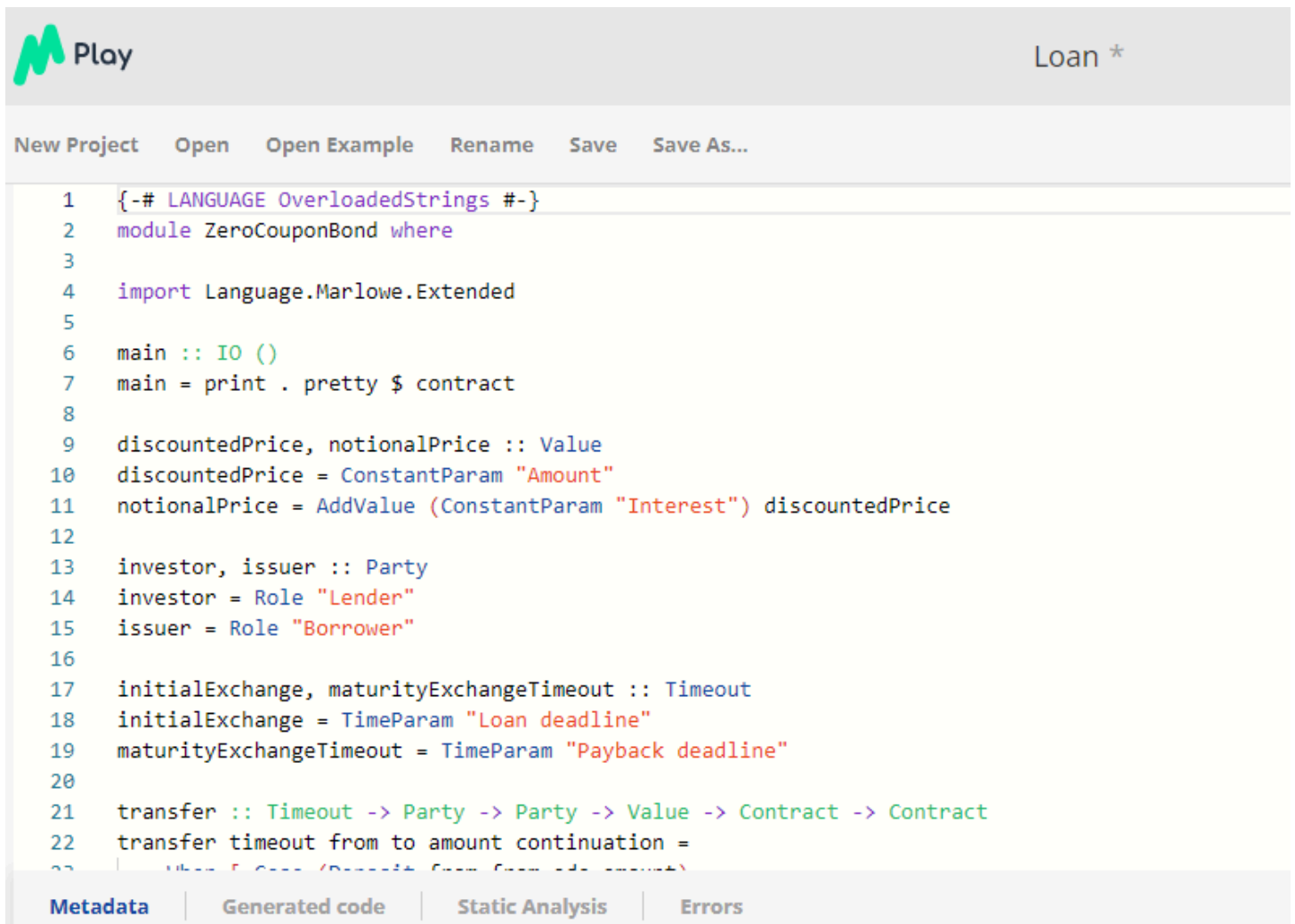
Haskell

Javascript

Marlowe

Blockly

Hình 31: Trái phiếu không lãi suất



```
1 {-# LANGUAGE OverloadedStrings #-}
2 module ZeroCouponBond where
3
4 import Language.Marlowe.Extended
5
6 main :: IO ()
7 main = print . pretty $ contract
8
9 discountedPrice, notionalPrice :: Value
10 discountedPrice = ConstantParam "Amount"
11 notionalPrice = AddValue (ConstantParam "Interest") discountedPrice
12
13 investor, issuer :: Party
14 investor = Role "Lender"
15 issuer = Role "Borrower"
16
17 initialExchange, maturityExchangeTimeout :: Timeout
18 initialExchange = TimeParam "Loan deadline"
19 maturityExchangeTimeout = TimeParam "Payback deadline"
20
21 transfer :: Timeout -> Party -> Party -> Value -> Contract -> Contract
22 transfer timeout from to amount continuation =
23   let f = Case (Deposit from from ada amount)
24   in f
```

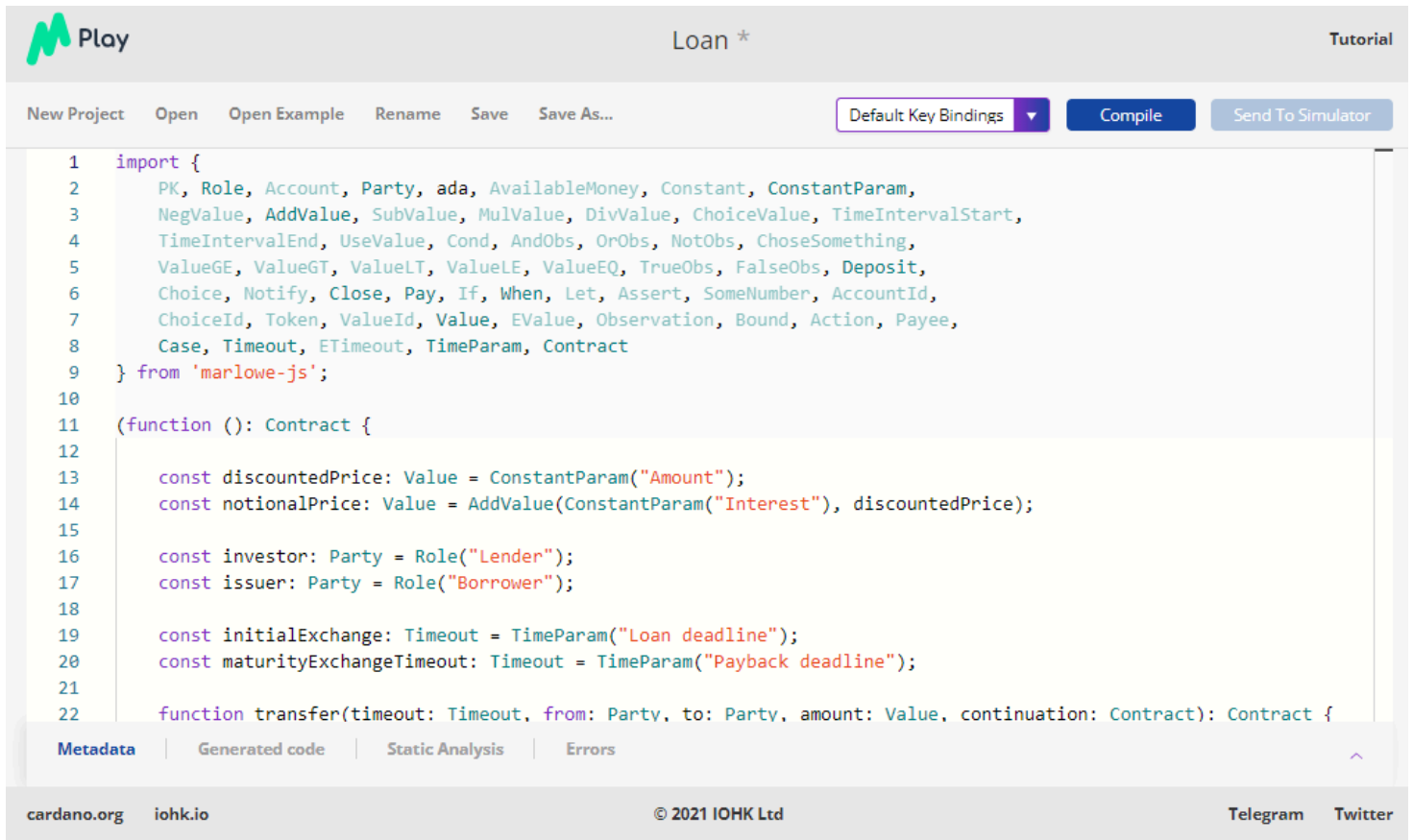
Hình 32: Marlowe JavaScript

Sau khi biên dịch thành công, bạn có thể gửi kết quả tới trình mô phỏng hoặc tới Blockly . Chỉ cần nhấp vào Node 'Gửi tới Trình mô phỏng' và 'Gửi tới Blockly ' ở góc trên cùng bên phải.

Vì Marlowe được mã hóa dưới dạng kiểu dữ liệu Haskell nên việc mô tả hợp đồng thông minh Marlowe trong Haskell rất đơn giản. Tuy nhiên, vì các hợp đồng Marlowe chỉ là dữ liệu nên bạn có thể diễn đạt chúng bằng các ngôn ngữ khác như TypeScript (một siêu bộ JavaScript), như đã nêu trong tài liệu.⁵⁶⁴

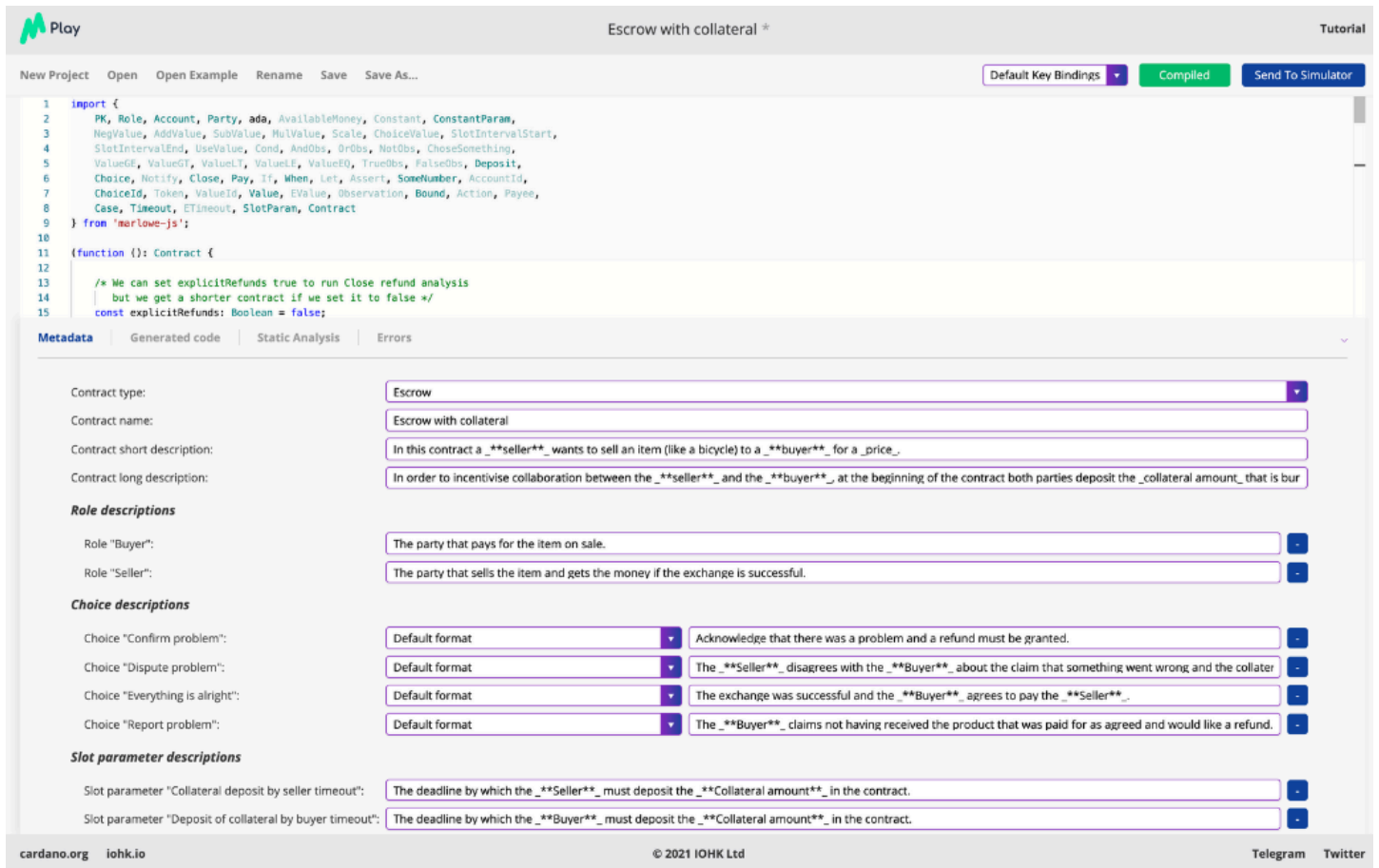
Mã Marlowe có thể được viết bằng trình chỉnh sửa JavaScript tích hợp. Bạn có thể viết mã JavaScript để làm cho các định nghĩa hợp đồng dễ đọc hơn bằng cách sử dụng các định nghĩa JS cho các thành phần phụ, chữ viết tắt và các hàm mẫu đơn giản. Trình chỉnh sửa thân thiện với người dùng với tính năng tự động hoàn thành, kiểm tra lỗi trong khi chỉnh sửa và di chuột qua các mẹo về liên kết. Tùy chọn Biên dịch ở trên cùng bên phải sẽ thực thi mã trong trình chỉnh sửa và đối tượng JSON do hàm trả về được phân tích cú pháp thành hợp đồng Marlowe thực; sau đó bạn có thể nhấn 'Gửi tới trình giả lập' để bắt đầu mô phỏng hợp đồng. Nếu quá trình biên dịch thành công, mã đã tạo có thể được xem bằng cách chọn 'Mã đã tạo' ở cuối trang; nó cũng có thể được giảm thiểu.

⁵⁶⁴



Hình 33: Trình soạn thảo mã Marlowe

Bạn có thể mở rộng phần chân trang và xem lại các tab khác nhau nơi bạn có thể kiểm tra và chỉnh sửa Siêu dữ liệu hợp đồng và xem lại kết quả của Phân tích tĩnh, v.v.



Hình 34: Trò chơi Marlowe

Chạy Marlowe

Marlowe Run ⁵⁶⁵ là ứng dụng khách dành cho người dùng cuối để tải xuống và chạy các hợp đồng Marlowe trên Blockchain Cardano. Chỉ trong vài phút, bạn có thể thiết lập và chạy các hợp đồng thông minh của mình. Để bạn thực hiện các thỏa thuận tài chính với bạn bè, đồng nghiệp hoặc khách hàng của mình trên Blockchain, Marlowe Run cung cấp một giao diện dễ dàng, rõ ràng và mượt mà. Nó cung cấp cho bạn quyền truy cập vào các mẫu hợp đồng thông minh an toàn, được chuẩn bị cẩn thận cho mọi loại thỏa thuận.

Marlowe Run là một phương pháp đơn giản và nhanh chóng để sử dụng và chạy các hợp đồng Cardano. Bạn sẽ khám phá nhiều mẫu hợp đồng tài chính để giúp bạn chọn hợp đồng thông minh tốt nhất cho nhu cầu của mình. Sau khi bạn đã chọn một mẫu, tất cả những gì bạn phải làm bây giờ là điền vào các vai trò và điều kiện, sau đó chạy hợp đồng của bạn.

Chạy UTXO và Marlowe

Các UTXO, được bảo mật bằng mật mã bằng khóa riêng do chủ sở hữu kiểm soát, là nguồn giá trị trên Blockchain. Các khóa này có thể được sử dụng để đổi đầu ra và do đó làm đầu vào cho các giao dịch tiếp theo, do đó chi tiêu giá trị trong đầu vào. Trong ví bảo mật bằng mật mã, người dùng theo dõi các khóa riêng tư của họ và các giá trị được liên kết với chúng.

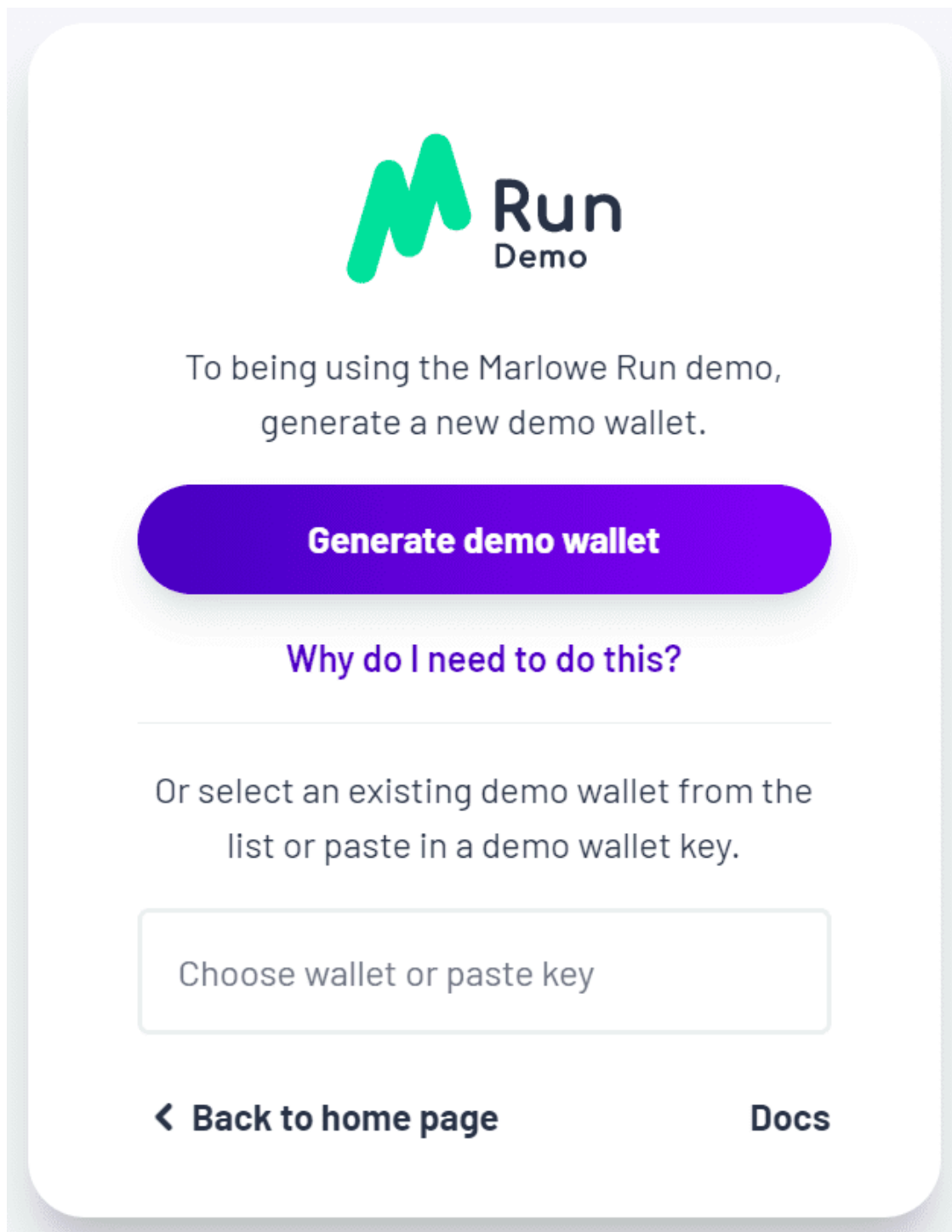
Người dùng sẽ cần tận dụng ứng dụng khách Marlowe Run để tham gia vào hợp đồng Blockchain. Vì tiền gửi được thực hiện từ ví của người dùng và họ nhận được khoản thanh toán, Marlowe Run tương tác với ví để xác thực các giao dịch chi tiêu tài sản Crypto. Lưu ý rằng đây là những hoạt động ngoài chuỗi phải được bắt đầu bằng mã chạy ngoài chuỗi, thường được tìm thấy trong ứng dụng Marlowe Run: chúng không thể được khởi động bằng hợp đồng chạy trên chuỗi.

Lưu ý: Các ảnh chụp màn hình sau đây là từ phiên bản demo của Marlowe Run sử dụng quỹ giả và hợp đồng thử nghiệm.

Chạy thử Marlowe

Để truy cập và xem trang tổng quan, hãy làm theo các bước sau:

1. Truy cập trang web Marlowe ⁵⁶⁶và nhấp vào **Marlowe Run** trên menu chính.
2. Nhấp vào **Thử bản demo**.
3. Bản demo Marlowe Run ra mắt:



 **Run Demo**

To begin using the Marlowe Run demo,
generate a new demo wallet.

Generate demo wallet

Why do I need to do this?

Or select an existing demo wallet from the
list or paste in a demo wallet key.

Choose wallet or paste key

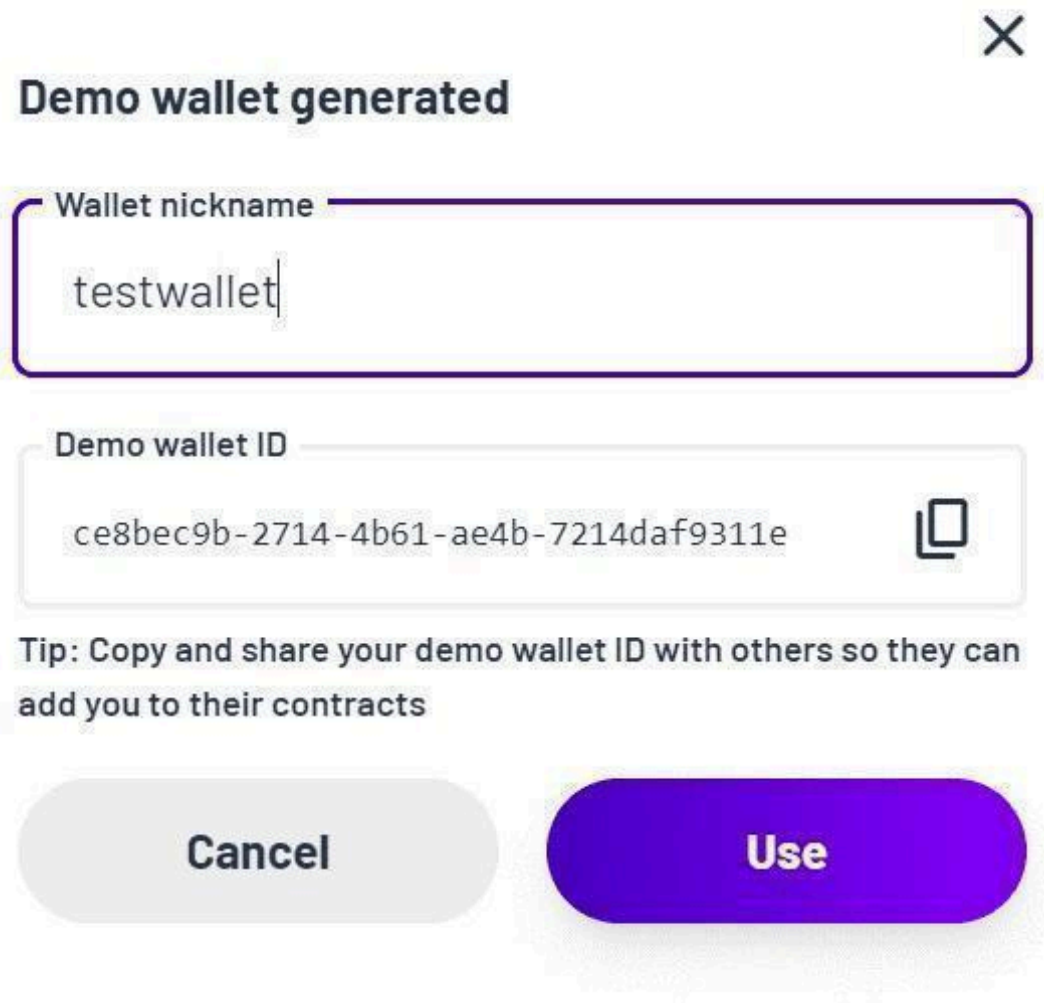
[← Back to home page](#) [Docs](#)

⁵⁶⁶

Hình 35: Chạy Marlowe

Đối với phiên bản demo này, bạn tạo ví thử nghiệm để có thể dùng thử. Bạn có thể sử dụng bất kỳ ví nào trên Marlowe Run bằng 'ID ví demo'. Điều này sẽ trở thành điểm tích hợp với ví thực trong phiên bản phát hành đầy đủ của Marlowe Run.

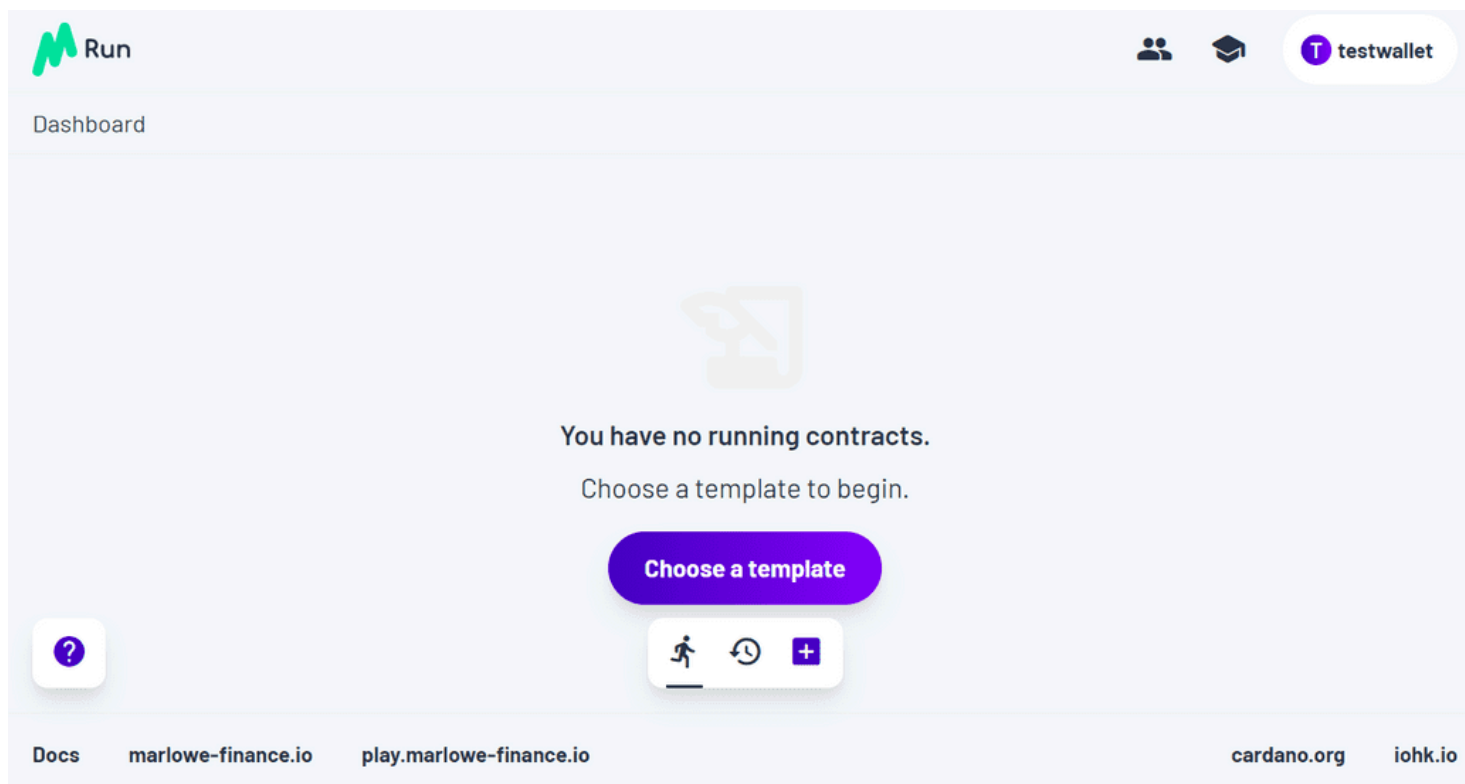
4. Nhấp vào **Tạo ví demo** để sử dụng ví demo.
5. Nhập biệt hiệu chẳng hạn như 'testwallet'.



Hình 36: Ví demo Marlowe

- ## 6. Nhấp vào Sử dụng .

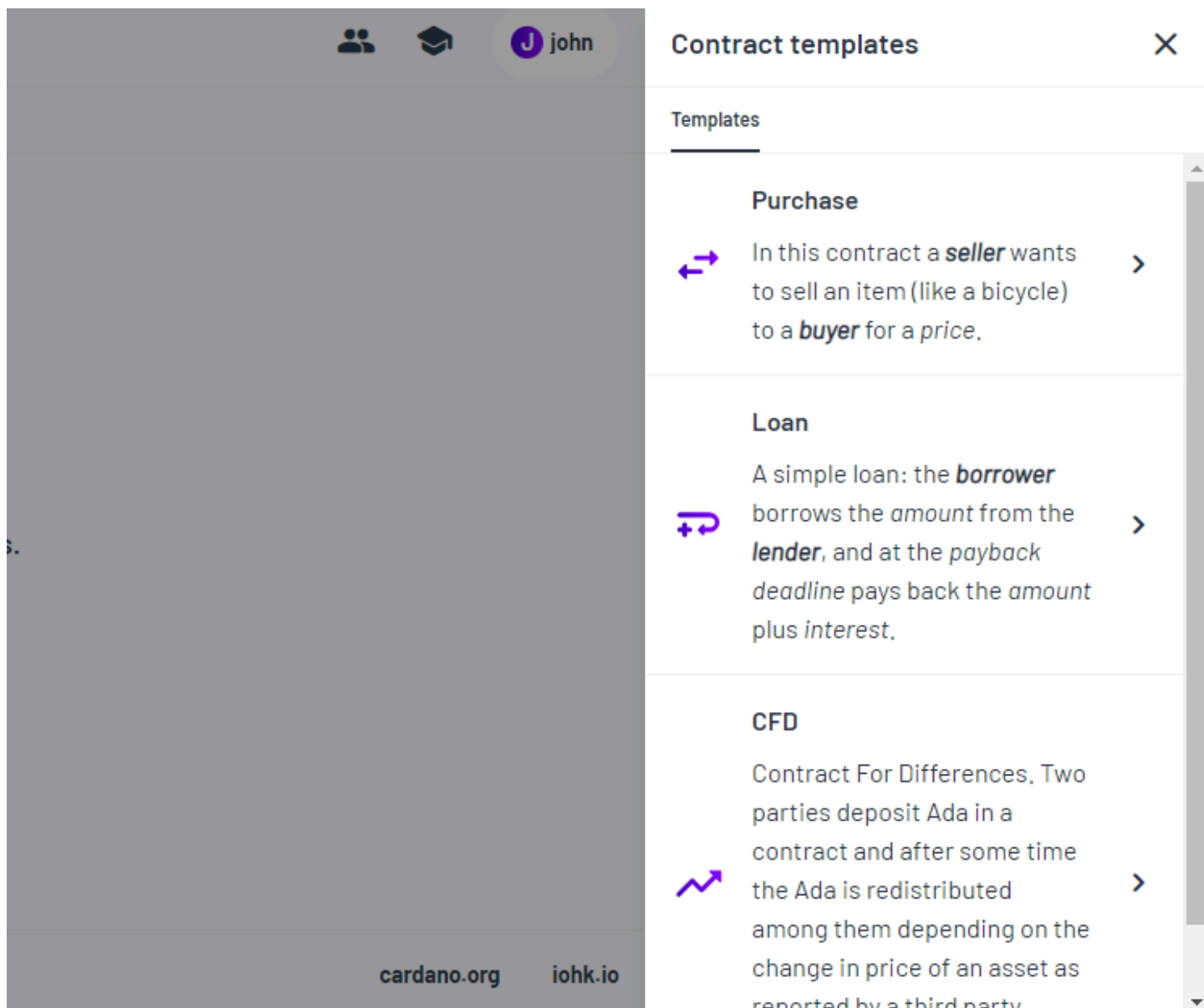
Sau khi bạn đã chọn ví của mình, màn hình sau sẽ hiển thị:



Hình 37: Mẫu Marlowe

7. Nhấp vào **Chọn mẫu** để tạo hợp đồng của bạn.

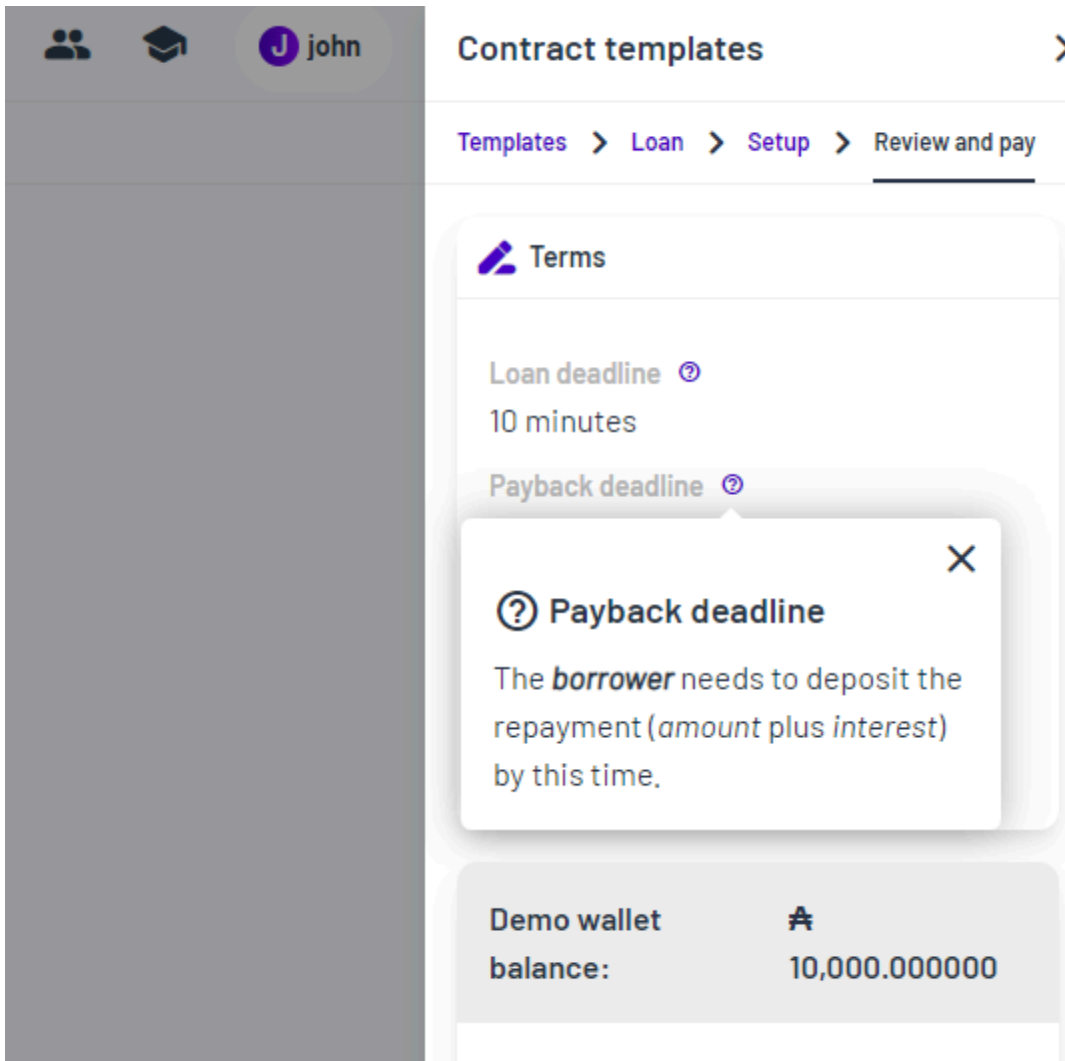
Thẻ lựa chọn Mẫu hợp đồng được hiển thị với ba tùy chọn:



Hình 38: Các mẫu hợp đồng Marlowe

8. Nhấp vào mẫu hợp đồng mà bạn muốn sử dụng, ví dụ này là Khoản vay.

Trình hướng dẫn đối thoại sẽ hướng dẫn bạn qua các bước dễ hiểu như sau:



Hình 39: Giao diện người dùng Marlowe



john

cardano.orgiohk.io

Contract templates

Templates

>

Loan

>

Setup

Lender

john



Terms

Interest

₳ 0.100000

Amount

₳ 8.000000

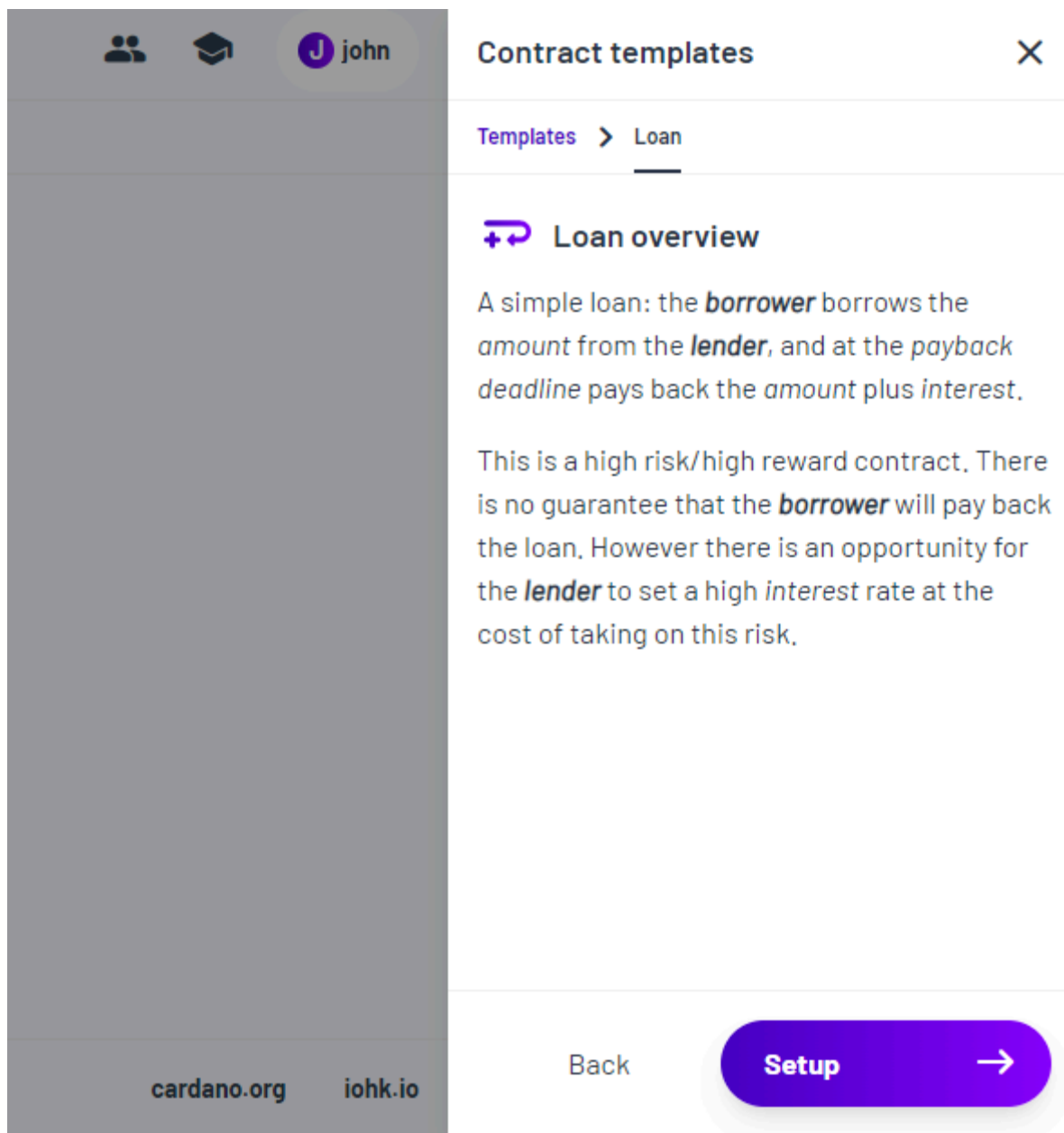
Loan deadline

10minutes

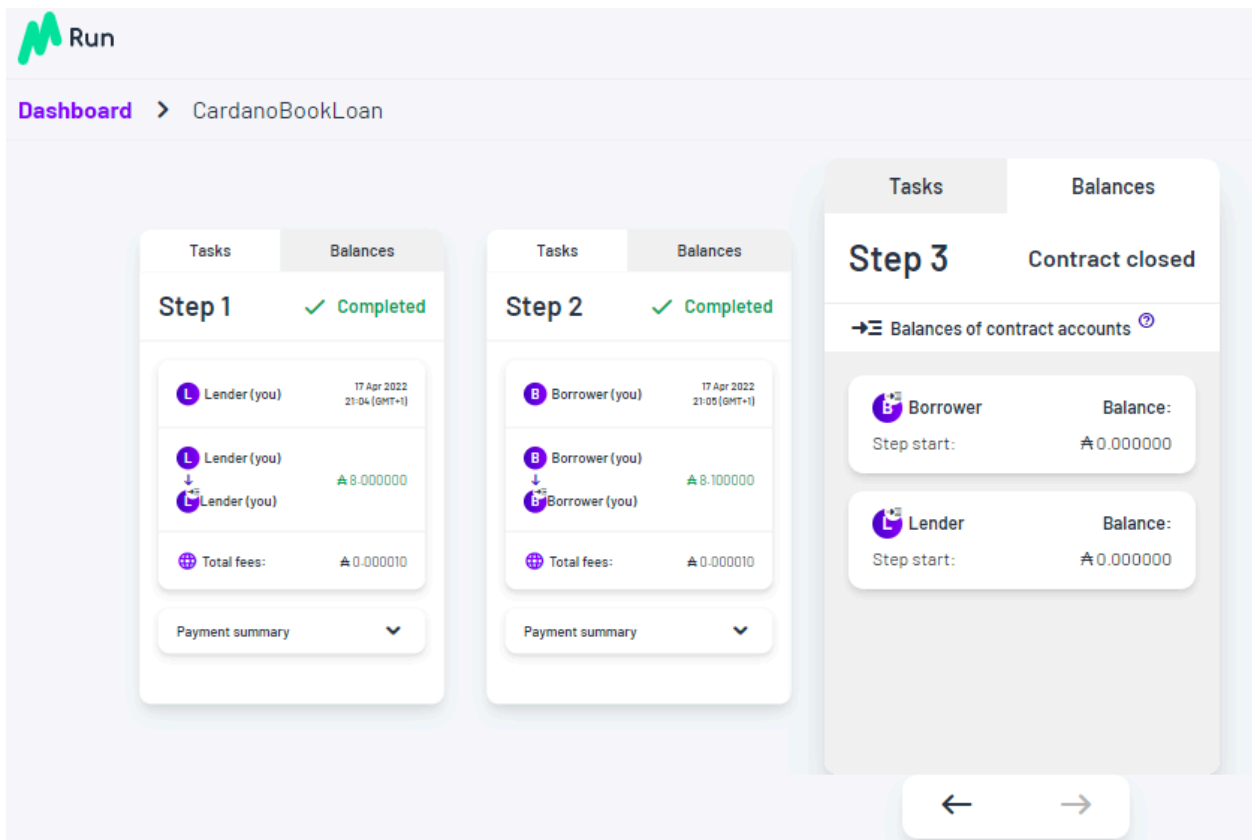
Back

Review

Hình 40: Hộp thoại mẫu Hợp đồng Marlowe.



Hình 41: Luồng UI mẫu hợp đồng



Hình 42: Marlowe CardanoBookLoan

Mô phỏng

Marlowe Playground hỗ trợ mô phỏng hợp đồng *toàn diện*, trong đó người dùng có thể thực hiện bất kỳ hành động nào cho bất kỳ vai trò nào và do đó xem xét việc thực hiện đồng thời từ quan điểm của tất cả người dùng.

Marlowe Run khác ở chỗ mỗi người tham gia chỉ có thể xem xét hợp đồng theo quan điểm của riêng họ. Những người tham gia chỉ có thể tương tác với một hợp đồng đang chạy đang chờ đầu vào của họ. Nếu không phải như vậy, thì họ sẽ thấy rằng việc thực hiện hợp đồng đang chờ ý kiến của người khác.

Hợp đồng thông minh Actus

Khi thế giới chuyển sang kỷ nguyên tài chính phi tập trung, thật đáng để xem xét các sắc thái của ngôn ngữ và nhiều phương pháp xây dựng hợp đồng thông minh Marlowe. Tiêu chuẩn thống nhất về các loại hợp đồng thuật toán (Actus) cho các hợp đồng tài chính đã được IOG triển khai ở Marlowe với cách tiếp cận của họ đối với các nhà tiên tri, vốn nhập thông tin 'thế giới thực' vào một hợp đồng đang chạy.

IOG cố tình giữ ngôn ngữ ở mức tối thiểu nhất có thể để dễ thực hiện. Marlowe chỉ định chuyển động của Crypto giữa những người tham gia và để làm như vậy trên Blockchain Cardano, mã phải được thực hiện cả trên chuỗi và ngoài chuỗi; tuy nhiên, chỉ một hợp đồng Marlowe bao gồm cả hai phần.

Phần trên chuỗi chấp nhận và xác minh các giao dịch đáp ứng các yêu cầu của hợp đồng thông minh: phần này được xây dựng dưới dạng một tập lệnh Plutus duy nhất cho tất cả các hợp đồng Marlowe, với mỗi hợp đồng Marlowe có một dữ liệu được cung cấp thông qua các giao dịch. Ngoài chuỗi, hợp đồng Marlowe sẽ có thể truy cập được thông qua giao diện người dùng và ví, cho phép người dùng gửi tiền và đưa ra quyết định, cũng như nhận các khoản thanh toán bitcoin.

Hành vi của hợp đồng có thể được bắt chước trong Sân chơi, cho phép người dùng tiềm năng xem qua các kịch bản hợp đồng khác nhau dựa trên các hoạt động khác nhau được thực hiện bởi các bên. Người dùng có quan điểm toàn tri trong mô phỏng chính và có thể thực hiện các hoạt động của bất kỳ người tham gia nào, với khả năng đảo ngược các hành vi đã thực hiện bất kỳ lúc nào và sau đó chọn một khóa học thay thế.

Sự đơn giản này cũng cho phép bạn biểu diễn các hợp đồng Marlowe trong bộ giải SMT,⁵⁶⁷ một công cụ logic tự động kiểm tra các đặc tính của hệ thống. IOG có thể kiểm tra xem một hợp đồng có không thực hiện được khoản thanh toán hay không bằng cách sử dụng mô hình này mà họ gọi là phân tích tĩnh và nếu đúng như vậy, họ có thể thu thập bằng chứng về việc nó sẽ không thực hiện được như thế nào, cho phép tác giả thay đổi hợp đồng nếu họ muốn.

IOG có thể sử dụng một trợ lý bằng chứng để tạo một mô hình triển khai chính thức, từ đó họ có thể tạo ra các bằng chứng được kiểm tra bằng máy về cách thức hoạt động của ngôn ngữ. Trong khi bộ giải SMT hoạt động trên các hợp đồng riêng lẻ, trợ lý bằng chứng có thể chứng minh các đặc điểm của mẫu hợp đồng và toàn bộ hệ thống: ví dụ: IOG có thể chứng minh rằng các tài khoản được tham chiếu trong bất kỳ hợp đồng đang hoạt động nào không bao giờ được ghi nợ. Mô phỏng, phân tích tĩnh và bằng chứng là ba lớp đảm bảo cho một hợp đồng mà người dùng sẽ cam kết tài sản để đảm bảo rằng nó hoạt động như bình thường.

nhà tiên tri

Một trong những câu hỏi phổ biến nhất với Marlowe là về các nhà tiên tri tài chính hoặc làm thế nào để có được một hợp đồng tính đến các giá trị dữ liệu bên ngoài như tỷ giá hối đoái giữa ADA và bitcoin. Bởi vì một nhà tiên tri về cơ bản giống như một người tham gia đưa ra quyết định, nên ngữ nghĩa của Marlowe đã có thể xử lý các giá trị bên ngoài. Tuy nhiên, như một phần của quá trình triển khai, mục đích là cung cấp các giá trị tiên tri, cho phép các hợp đồng nhận giá trị trực tiếp từ mã đánh dấu thị trường chứng khoán hoặc nguồn cấp dữ liệu như Coinbase hoặc Binance. Đồng thời, nhóm Plutus đang nghiên cứu phương pháp tốt nhất để đối phó với lời tiên tri nói chung và sẽ có sự hỗ trợ cho phương pháp này trong tương lai.

Tại sao Actus?

Blockchain đảm bảo rằng hợp đồng được thực hiện, do đó Marlowe có khả năng cho phép các cá nhân thiết lập các cam kết tài chính và trao đổi mà không cần bên thứ ba hỗ trợ họ. IOG đang phát triển triển khai Marlowe các hợp đồng không trung gian cho người dùng cuối muốn thực hiện các giao dịch tài chính ngang hàng mà không có sự tham gia của bên thứ ba. Các hợp đồng tài chính được Tổ chức nghiên cứu tài chính Actus phân loại bằng cách sử dụng phân loại⁵⁶⁸ được nêu trong thông số kỹ thuật.⁵⁶⁹

Theo Actus, hợp đồng tài chính là thỏa thuận pháp lý giữa hai (hoặc nhiều) đối tác về việc trao đổi dòng tiền trong tương lai. Các thỏa thuận pháp lý như vậy luôn được thể hiện bằng ngôn ngữ tự nhiên, dẫn đến sự mơ hồ. Do đó, Actus sử dụng một tập hợp các từ trong hợp đồng và các chức năng xác định để dịch các điều khoản này thành nghĩa vụ thanh toán trong tương lai để xây dựng hợp đồng. Do đó, hầu hết các công cụ tài chính có thể được mô tả bằng cách sử dụng 31 loại hợp đồng hoặc mẫu mô-đun.

Actus trông như thế nào ở Marlowe?

Các sản phẩm trong phân loại Actus, chẳng hạn như hợp đồng gốc khi đáo hạn, có thể được trình bày trong Marlowe theo nhiều cách khác nhau, tùy thuộc vào mức độ sẵn sàng chấp nhận các sửa đổi trong các điều khoản của họ trong suốt quá trình tồn tại của hợp đồng.

Trong kịch bản cơ bản nhất, tất cả các dòng tiền được thiết lập hoặc đóng băng khi bắt đầu hợp đồng, đảm bảo rằng hoạt động của hợp đồng hoàn toàn có thể dự đoán được, với điều kiện là tất cả những người tham gia tiếp tục tham gia với nó trong suốt thời gian tồn tại của nó. Hợp đồng Actus-F là một hợp đồng như vậy (F là cố định hoặc đóng băng).

Tính năng động, hoặc thay đổi trong quá trình phát triển hợp đồng, có thể có hai dạng. Những người tham gia có thể thực hiện các khoản thanh toán ngoài kế hoạch, điều này sẽ yêu cầu tính toán lại các dòng tiền còn lại, cũng như sửa đổi các dòng tiền bằng cách tính đến các biến rủi ro bên ngoài. Actus-M mô hình hóa toàn bộ phạm vi hợp đồng thực hiện cả hai (M cho Marlowe).

Các giai đoạn trung gian cũng có sẵn: Hợp đồng Actus-FS (lịch trình cố định) đã thiết lập lịch trình, cho phép xem xét các yếu tố rủi ro nhưng không có khoản thanh toán đột xuất; Mặt khác, các hợp đồng Actus-FR cho phép thanh toán được thực hiện bất cứ lúc nào nhưng không tính đến các yếu tố rủi ro.

⁵⁶⁷

Lý thuyết modulo thỏa mãn (SMT) là vấn đề xác định xem một công thức toán học có thỏa mãn hay không. Nó khái quát hóa vấn đề thỏa mãn Boolean (SAT) thành các công thức phức tạp hơn liên quan đến số thực, số nguyên và/hoặc các cấu trúc dữ liệu khác nhau như danh sách, mảng, vectơ bit và chuỗi. Cái tên này bắt nguồn từ thực tế là các biểu thức này được diễn giải bên trong ("modulo") một lý thuyết hình thức nhất định theo logic bậc nhất có đẳng thức (thường không cho phép các bộ định lượng). **Bộ giải SMT** là các công cụ nhằm giải quyết vấn đề SMT cho một tập hợp con đầu vào thực tế.

⁵⁶⁸

Phân loại ACTUS, actusfrf.org/taxonomy

⁵⁶⁹

Thông số kỹ thuật ACTUS, actusfrf.org/techspecs

các mô hình Actus-H (H cho Haskell) hợp đồng trực tiếp dưới dạng các chương trình Plutus hoặc Haskell, với Marlowe được sử dụng để xác thực từng giao dịch trong suốt thời gian tồn tại của hợp đồng bằng cách tạo mã Plutus từ mô tả logic hợp đồng của Marlowe.

Tại sao có rất nhiều mô hình hợp đồng Actus riêng biệt?

Lý do cho điều này là vì có sự đánh đổi giữa bản chất linh hoạt của hợp đồng và sự chắc chắn mà IOG có thể cung cấp cho khách hàng về cách chúng sẽ hoạt động trước khi chúng được thực thi.

- Các hợp đồng Actus-F (cố định hoặc đóng băng) có lịch thanh toán được thiết lập hoàn chỉnh mà các bên có thể xem xét trực tiếp, giúp dễ dàng xác định, chẳng hạn như tất cả các khoản thanh toán từ hợp đồng đó sẽ thành công
- Các hợp đồng trong sê-ri Actus-FS và -FR có tính năng động cao hơn, nhưng chúng dễ đọc và dễ kiểm tra. Hơn nữa, chúng có thể được phân tích tĩnh để đảm bảo rằng tất cả các khoản thanh toán, ví dụ, sẽ thành công
- Vì các hợp đồng Actus-M (M cho Marlowe) được viết bằng Marlowe nên chúng có thể được phân tích. Tuy nhiên, do không thể đoán trước được các hoạt động mà hợp đồng sẽ thực hiện tại bất kỳ thời điểm nào, nên việc phân tích mất nhiều thời gian hơn. Cần lưu ý rằng sự đảm bảo có thể được cung cấp cho các hợp đồng thu nhỏ có cùng nội dung tính toán nhưng phát triển trong một khoảng thời gian ngắn hơn, dẫn đến ít tương tác hơn
- Bởi vì các hợp đồng Actus-H (H cho Haskell) được viết bằng sự pha trộn giữa Plutus và Marlowe, nên chúng không dễ kiểm tra tĩnh như các hợp đồng khác. Mặt khác, nền tảng này cung cấp tiện ích mở rộng và tùy chỉnh hoàn chỉnh việc triển khai tiêu chuẩn Actus cho khách hàng doanh nghiệp.

Người dùng có thể xây dựng các hợp đồng Actus-F (cố định hoặc cố định) và -FS từ các điều khoản của hợp đồng bằng cách sử dụng bản trình bày trực quan về dữ liệu cần thiết trong quá trình triển khai Actus của IOG, có thể truy cập dưới dạng phiên bản trước khi phát hành trong tab Phòng thí nghiệm của Sân chơi.

Marlowe là một DSL (ngôn ngữ dành riêng cho miền) chỉ xác định các hợp đồng tài chính chứ không phải hợp đồng thông minh nói chung. Nó thay đổi từ các ngôn ngữ Blockchain có mục đích chung như Solidity và Bitcoin Script ⁵⁷⁰vì điều này.

Marlowe là một dự án quy mô lớn. IOG đã tạo các hợp đồng Marlowe bằng cách sử dụng các ví dụ từ khung Tiêu chuẩn thống nhất các loại hợp đồng thuật toán (Actus), đây là một trong những dự án phổ biến nhất cho các hợp đồng thông minh tài chính. Những ví dụ này và nhiều ví dụ khác có sẵn trong Marlowe Playground.

Marlowe cho tài chính P2P

Nếu bạn đã từng cố gắng bán Bitcoin hoặc ADA của mình và rút tiền từ Binance một cách vội vàng, rất có thể bạn sẽ bị chặn làm như vậy. Binance thường tạm dừng rút tiền do tổn động ⁵⁷¹hoặc bạn có thể buộc phải rút tiền thông qua một tùy chọn đắt tiền thay vì chuyển khoản ngân hàng tương đối rẻ. ⁵⁷²Phí trao đổi tập trung ⁵⁷³có ít tổng tiền hơn phí ngân hàng cũ không? Hầu hết mọi người sẽ nghĩ rằng trong không gian Crypto, họ sẽ luôn có thể truy cập vào tài sản của mình, thực hiện giao dịch và rút tiền mà không có bên thứ ba chặn bạn hoặc tính 'phí xử lý' quá đắt.

Có bao giờ đúng là bạn có thể kiểm soát hoàn toàn tài chính của chúng tôi không? Hầu hết mọi người không có lựa chọn nào khác ngoài việc ủy thác việc quản lý tiền của họ cho bên thứ ba, để họ quyết định xem và khi nào những khoản tiền đó có thể được truy cập, sử dụng hoặc thậm chí được nhìn thấy. Điểm kiểm soát chính là điểm chung của tất cả các ngân hàng và nhà môi giới bên thứ ba này. Một tác nhân tư lợi bên ngoài có thể gây ảnh hưởng, tấn công hoặc thao túng điểm kiểm soát chính, khiến nó trở nên trái ngược với tài chính dân chủ hóa.

⁵⁷⁰

Bitcoin Script là một ngôn ngữ lập trình đơn giản, dựa trên ngăn xếp cho phép xử lý các giao dịch trên Blockchain Bitcoin

⁵⁷¹

Binance bị đình chỉ rút Crypto, fnlondon.com/articles/binance-hit-by-crypto-rút-tiền-đình-chỉ-20211101

⁵⁷²

Binance tạm dừng chuyển khoản SEPA cho các nhà đầu tư Ireland, businesspost.ie/investing/binance-suspends-sepa-transfers-for-irish-investors-1ac95e7c

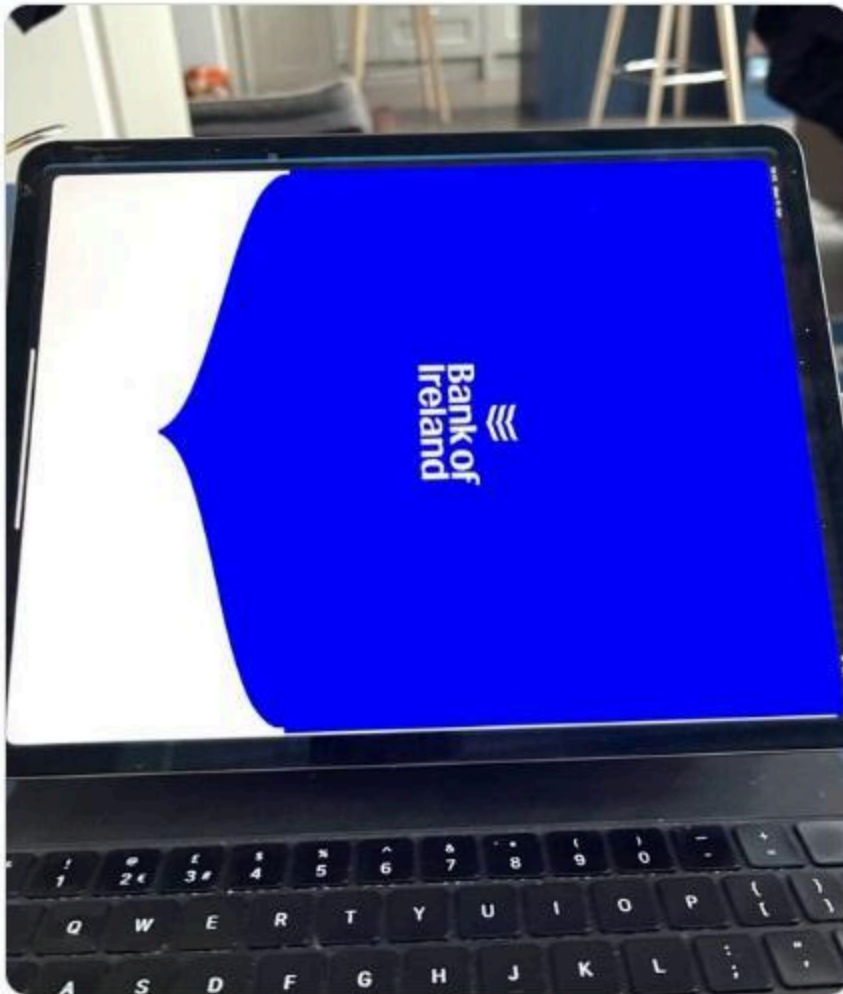
⁵⁷³

Phí trao đổi Crypto là một mớ hỗn độn. Liệu họ có cải thiện được không?, forbes.com/sites/kenrapoza/2021/10/17/cryptocurrency-exchange-fees-are-a-mess-when-will-they-ever-improve/?sh=477a74be2f4c



Adrian Weckler ✓
@adrianweckler

Bank Of Ireland, 2022



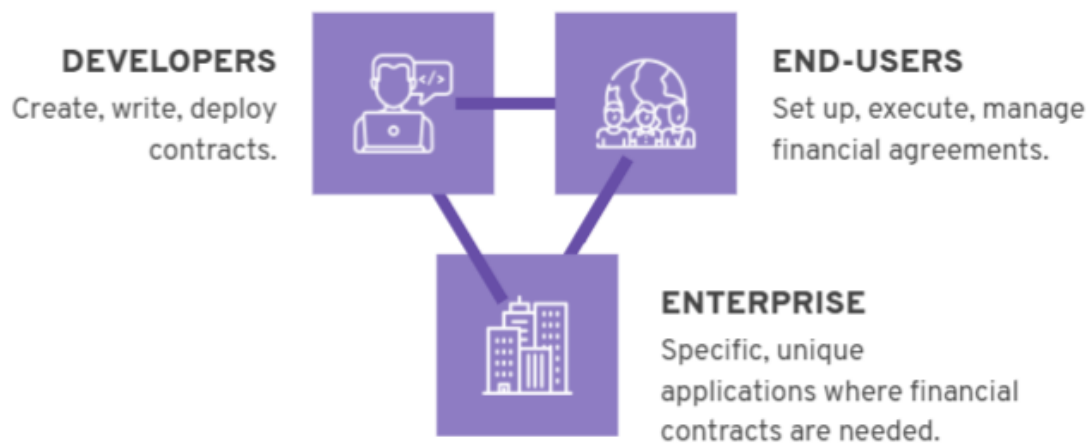
Biểu đồ 43: Ngân hàng trực tuyến năm 2022

Đây là động lực đằng sau tài chính phi tập trung, thường được gọi là DeFi. Cho vay, ký quỹ, phái sinh, hoán đổi và chứng khoán là một trong những công cụ tài chính do DeFi cung cấp, có thể so sánh với các công cụ do Phố Wall cung cấp. Các nền tảng DeFi tự phân biệt bằng cách có thể cung cấp các sản phẩm tài chính khác nhau mà không cần đến các nhà tạo lập thị trường trung tâm, ngân hàng hoặc nhà môi giới. Mỗi thỏa thuận tài chính được ghi lại trên Blockchain dưới dạng hợp đồng thông minh được giải quyết theo thuật toán. Do đặc tính phi tập trung của chúng, chúng có khả năng chống thao túng thị trường và lỗi hệ thống tập trung cao hơn đáng kể.

IOG đang nghiên cứu một bộ sản phẩm Marlowe để giúp dân chủ hóa tiền và làm cho các thỏa thuận tài chính dễ tiếp cận hơn. Điều này bao gồm Marlowe Run, một công cụ cho phép người dùng thực hiện các thỏa thuận tài chính có sẵn một cách an toàn và độc lập với bạn bè hoặc doanh nghiệp. Hệ thống ngang hàng này sẽ tiết kiệm chi phí và quan trọng hơn là dân chủ hóa, với khả năng tự động hóa gia tăng và không cần đến bên thứ ba.

bộ Marlowe

IOG muốn dân chủ hóa tài chính với Marlowe bằng cách cho phép các thỏa thuận ngang hàng hoạt động trên một Blockchain. Chúng nhằm mục đích cung cấp cho các cá nhân khả năng xây dựng các công cụ tài chính của riêng họ và thỏa thuận với bất kỳ ai mà họ chọn để giao dịch. Marlowe sẽ cung cấp một số sản phẩm riêng biệt, mỗi sản phẩm sẽ phục vụ cho một nhóm người tiêu dùng và chức năng cụ thể. Chiến lược sản phẩm của Marlowe được chia thành ba loại: Marlowe dành cho nhà phát triển, Marlowe dành cho người dùng cuối và Marlowe dành cho doanh nghiệp.



Hình 44: Nhóm người dùng Marlowe

Nhà phát triển

Các nhà phát triển có thể sử dụng Marlowe Build và Marlowe Play (còn được gọi là Sân chơi Marlowe) và cũng là đầu vào của Thư viện Marlowe. Sự kết hợp giữa Marlowe Build và Marlowe Play cho phép tạo hợp đồng thông minh tài chính từ đầu đến cuối.

Marlowe Build cho phép các nhà phát triển viết mã hợp đồng thông minh. Sau đó, họ có thể sử dụng các mô phỏng để thực hiện thiết kế lặp lại cơ bản và chính thức xác minh và thử nghiệm các hợp đồng thông minh trên Marlowe Play. Những đặc điểm này, khi được kết hợp với ngôn ngữ dành riêng cho miền dành riêng cho tài chính (DSL), đảm bảo rằng hợp đồng dễ tạo, cũng như an toàn, có thể xác minh và được thử nghiệm tốt. Các nhà phát triển có thể tặng các mẫu hợp đồng thông minh của họ cho Thư viện Marlowe, một thư viện mẫu hợp đồng thông minh mã nguồn mở, sau khi chúng được phát triển và thử nghiệm.

Người dùng cuối

Marlowe dành cho người dùng cuối sẽ cung cấp giao diện đơn giản, trực quan và liền mạch để người dùng ký các thỏa thuận tài chính trên Blockchain với bạn bè, đồng nghiệp hoặc khách hàng của họ. Điều này chứa Marlowe Run và cung cấp cho bạn quyền truy cập vào các mẫu công cụ tài chính của Thư viện Marlowe. Những sản phẩm này được IOG thiết kế có tính đến người dùng. Người dùng không cần phải là chuyên gia Blockchain hoặc biết cách phát triển hợp đồng thông minh để hình thành các thỏa thuận tài chính trên Marlowe Run.

Mỗi bước của hợp đồng được giải thích theo các điều khoản của giáo dân và mỗi hành động chỉ được thực hiện với sự cho phép rõ ràng của người dùng. IOG đã thiết kế một bộ cơ chế tài chính đã được kiểm tra và xác nhận cẩn thận như ký quỹ, chứng khoán nợ và hoán đổi có thể được sử dụng trên Marlowe Run. Thư viện Marlowe làm cho các hợp đồng này và nhiều hợp đồng nguồn mở được xác thực khác có thể truy cập được.

doanh nghiệp

Marlowe for Enterprise tìm cách đưa DeFi vượt ra ngoài người dùng cá nhân, cho phép các doanh nghiệp gặt hái những lợi thế của hợp đồng thông minh một cách thiết thực. Điều này sẽ có một tập hợp các khả năng và thỏa thuận tài chính tùy chỉnh, có thể định cấu hình hướng đến một trường hợp sử dụng kinh doanh cụ thể, cũng như các mẫu hợp đồng thông minh dựa trên Tiêu chuẩn thống nhất các loại hợp đồng thuật toán (Actus) cho các hợp đồng tài chính.

Marlowe trên Cardano

IOG đã phát hành Marlowe Playground Alpha⁵⁷⁴ vào năm 2020. Điều này cho phép các hợp đồng được viết bằng JavaScript bên cạnh Haskell hoặc trực tiếp bằng Marlowe. Các nhà tiên tri chứng minh khái niệm cũng đã được thêm vào, với khả năng truy xuất dữ liệu bên ngoài, chẳng hạn như giá trực tiếp từ 'mã đánh dấu' trên thị trường chứng khoán hoặc, trong tương lai, các nguồn cấp dữ liệu như

⁵⁷⁴

Kraken.⁵⁷⁵ IOG đã tạo các hướng dẫn để giúp các nhà phát triển triển khai, sau đó mở rộng nỗ lực này bằng cách cải thiện trải nghiệm người dùng và phát triển, thử nghiệm và xác minh một ngân hàng các mẫu hợp đồng thông minh đang phát triển.

IOG đang hoàn thiện việc triển khai Marlowe trên Cardano như một phần của quá trình triển khai kỷ nguyên Goguen, cho phép các cá nhân và tổ chức thực hiện các hợp đồng DeFi mà họ tự tạo hoặc lấy từ kho lưu trữ hợp đồng. Marlowe ban đầu sẽ hoạt động trên Blockchain Cardano, nhưng nó là Blockchain bất khả tri và có thể chạy trên các Blockchain khác trong tương lai để tiếp cận nhiều đối tượng hơn.

Marlowe sẽ được cung cấp cho người dùng cuối theo từng giai đoạn. Đầu tiên là nguyên mẫu Marlowe Run, cho phép người dùng giới thiệu và kiểm tra các thỏa thuận tài chính của chính họ. Người dùng có thể sửa đổi một tập hợp các mẫu hợp đồng thông minh tài chính để đáp ứng các yêu cầu cụ thể của họ. Nguyên mẫu này cho phép người dùng thử nghiệm hình thành các thỏa thuận tài chính phi tập trung trong môi trường ngang hàng mà không cần bên thứ ba khai thác giá trị. Người dùng không cần Token thực tế để sử dụng nguyên mẫu Marlowe Run, vì vậy họ có thể kiểm tra nó trước khi cam kết.

Các nhà phát triển của IOG đã tạo một bộ công cụ tài chính mẫu cho việc triển khai này. Trên Marlowe Run, các mẫu này có thể được sử dụng để chạy các thỏa thuận thử nghiệm. IOG đã chia sẻ một số bản demo của Marlowe Run, chẳng hạn như bản này⁵⁷⁶ trên kênh YouTube 'IOHK' của họ. Kiểm tra marlowe-finance.io / để biết chi tiết về hội thảo trên web, sự kiện, v.v.

Sân chơi Marlowe phát triển

Bạn có thể tạo các mẫu của riêng mình từ hợp đồng Marlowe và sử dụng siêu dữ liệu duy nhất để cung cấp đề xuất cho người dùng. Cài đặt hộp cát của Sân chơi Marlowe là nơi bạn có thể thử nghiệm soạn thảo các hợp đồng tài chính. Sân chơi này cho phép bạn làm việc trực tiếp bằng nhiều ngôn ngữ khác nhau, bao gồm Marlowe, JavaScript, Haskell⁵⁷⁷ hoặc Blockly, tùy theo sở thích của bạn. Các công cụ mới để tạo và sửa đổi mẫu và tùy chỉnh thông tin, cũng như tùy chọn tải xuống JSON mới cho chính các hợp đồng, đã được giới thiệu cho Marlowe Playground.

hỗ trợ mẫu

Với việc phát hành Marlowe Run, IOG đã mở rộng Sân chơi Marlowe để bao gồm hỗ trợ mẫu. Phiên bản nâng cao của Marlowe (còn gọi là Marlowe mở rộng, có sẵn trong Marlowe Playground) được sử dụng để tạo các mẫu này. Người dùng sẽ có thể dễ dàng sử dụng lại và tái sử dụng các hợp đồng bằng cách sử dụng các mẫu mới này cho nhiều tình huống và bối cảnh khác nhau.

Marlowe mở rộng linh hoạt hơn so với Marlowe thông thường (hoặc Core Marlowe). Hợp đồng khá cụ thể và thời gian chờ được chỉ định theo giá trị tuyệt đối, đầu tiên thông qua số vị trí và sau đó sử dụng⁵⁷⁸ đầu thời gian POSIX được tiêu chuẩn hóa.

Giá trị Marlowe thường được mã hóa cứng trong Marlowe, ngoại trừ những giá trị được cung cấp dưới dạng Đầu vào. Ví dụ: bạn có thể sử dụng **cấu trúc Lựa chọn** trong **Khi** để tạo khoản vay với giá $\mathbb{A}$ 100 hoặc cấu trúc hỏi người dùng cho vay bao nhiêu, nhưng trước đó bạn không thể có hợp đồng Marlowe có thể tái sử dụng có thể được triển khai bất kỳ lúc nào và với bất kỳ tham số được cung cấp. Khả năng kết hợp các tham số hợp đồng trong Extended Marlowe giải quyết các ràng buộc này. Hiện tại, Marlowe mở rộng hầu như giống với Marlowe đơn giản, ngoại trừ hai hàm tạo bổ sung đại diện cho các tham số mẫu:

- **SlotParam** — Trong cấu trúc **Khi**, nó có thể được sử dụng thay vì thời gian chờ.
- **ConstantParam** - một loại cấu trúc **Giá trị**
- Cả hai hàm tạo đều chấp nhận một tham số duy nhất, đó là một chuỗi hoạt động như một mã định danh tham số, chẳng hạn như:
 - **SlotParam** "**Thời hạn thanh toán**"
 - **ConstantParam** "**Giá**"

Ngay cả khi chúng tồn tại ở các vị trí riêng biệt, hai tham số cùng loại (**SlotParam** hoặc **ConstantParam**) và có cùng mã định danh

⁵⁷⁵

Nguồn cấp dữ liệu Kraken, api.cryptowat.ch/markets/kraken

⁵⁷⁶

Bản trình diễn: Marlowe Run của Cardano, youtube.com/watch?v=sfLLoIEhSGU

⁵⁷⁷

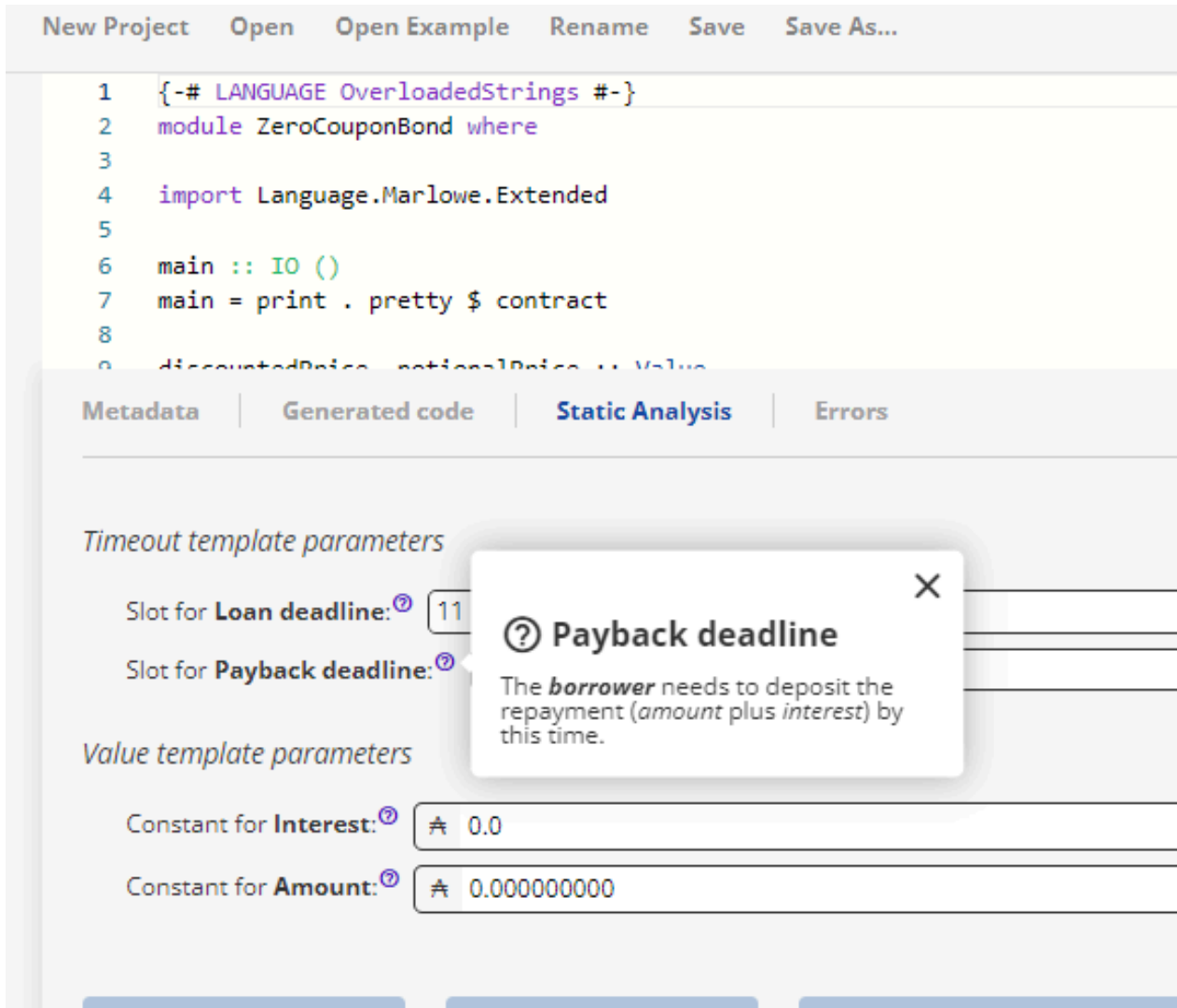
Marlowe nhúng trong Haskell, play.marlowe-finance.io/doc/marlowe/tutorials/embedded-marlowe.html

⁵⁷⁸

Giao diện hệ điều hành di động (POSIX) là một nhóm các tiêu chuẩn do Hiệp hội máy tính IEEE chỉ định để duy trì khả năng tương thích giữa các hệ điều hành. POSIX xác định giao diện lập trình ứng dụng (API), cùng với trình bao dòng lệnh và giao diện tiện ích, để phần mềm tương thích với các biến thể của Unix và các hệ điều hành khác.

được coi là cùng một tham số. Nếu hợp đồng có tham số (nếu đó là mẫu), người dùng sẽ được nhắc cung cấp giá trị cho các tham số đó trước khi bắt đầu mô phỏng hoặc triển khai hợp đồng trong Marlowe Run.

Cần lưu ý rằng trường nhập tham số mẫu giá trị không chỉ là một trường số nguyên. Thay vào đó, nó mong đợi một số thập phân có ký hiệu tiền tệ trên nhãn để cho biết rằng giá trị được dự đoán phản ánh một lượng ADA. Ngoài ra, số lượng ADA không nhất thiết phải được biểu thị bằng các lựa chọn, chúng có thể được sử dụng để biểu thị bất kỳ thứ gì, chẳng hạn như tỷ lệ. Mỗi tham số có một bộ mặt riêng, có thể được truy cập bằng cách nhấp vào dấu chấm hỏi màu tím bên cạnh mỗi hộp. Văn bản đề xuất ('mẹo công cụ') là duy nhất cho mỗi hợp đồng.



Hình 45: Phân tích tĩnh Marlowe

Tùy chỉnh siêu dữ liệu

Siêu dữ liệu có thể được sử dụng để thay đổi các yếu tố trong hợp đồng do người dùng xác định. Mỗi trình chỉnh sửa trong Marlowe Playground đều có tab Siêu dữ liệu ở dưới cùng. Người dùng có thể thay đổi siêu dữ liệu cho phù hợp với nhu cầu của họ. Mỗi hợp đồng được yêu cầu cung cấp một số siêu dữ liệu cơ bản, chẳng hạn như loại hợp đồng, tên hợp đồng và mô tả. Tab siêu dữ liệu cũng cho phép bạn định dạng các lựa chọn và tham số giá trị.

Trong tab Siêu dữ liệu, mỗi tham số vai trò, lựa chọn, vị trí hoặc giá trị mới được thêm vào hợp đồng sẽ được đánh dấu bằng màu đỏ. Có thể phải biên dịch mã thành công trước trong trường hợp trình soạn thảo Haskell và JavaScript.

Bằng cách nhấn Node '+' màu đỏ, một mục nhập siêu dữ liệu mới cho đối tượng đã chọn sẽ được tạo. Tương tự, nếu một tham số vai trò, lựa chọn, vị trí hoặc giá trị không còn được sử dụng trong hợp đồng, thì siêu dữ liệu hiện tại sẽ được đánh dấu bằng màu đỏ và người dùng phải xóa mục siêu dữ liệu khỏi hợp đồng bằng cách sử dụng Node '-'.

Thứ tự siêu dữ liệu

Trình tự trong đó các tham số được thiết lập là rất quan trọng. Người dùng cuối có thể chọn từ một số tham số vị trí để trình bày các tham số đó theo thứ tự xuất hiện sẽ hợp lý hơn. Giờ đây, người dùng có thể kéo các mục vào thứ tự thích hợp để sắp xếp siêu dữ liệu, ví dụ:

Slot parameter descriptions		
Slot parameter "Payment deadline":	The __buyer__ must pay the _price_ of the item by this time, otherwise the contract is cancelled.	
Slot parameter "Complaint deadline":	The __buyer__ can only complain until this deadline, otherwise the contract will assume the transaction went smoothly.	
Slot parameter "Complaint response deadline":	If the __buyer__ complained, the __seller__ must respond before this deadline, otherwise the contract will assume the transaction went smoothly.	
Slot parameter "Mediation deadline":	If the __buyer__ and the __seller__ disagree, the __mediator__ must weigh in before this deadline, otherwise the contract will assume the transaction went smoothly.	

Hình 46: Kéo và thả Marlowe

Thứ tự của các tham số trong siêu dữ liệu sẽ được sử dụng để tạo biểu mẫu sẽ được hiển thị khi bắt đầu mô phỏng hoặc thực hiện hợp đồng.

Vào tháng 4 năm 2022, IOG đã giới thiệu công cụ Marlowe CLI (giao diện dòng lệnh).⁵⁷⁹ Đối với những người dùng muốn quản lý hợp đồng từ dòng lệnh, công cụ mới này cung cấp một cách tiếp cận đơn giản. Nó cho phép bạn tập trung vào hợp đồng Marlowe trong khi công cụ xử lý các chi tiết cụ thể về đầu vào và trạng thái của hợp đồng. Nó cũng tự động hóa một số phần của Plutus, cũng như các tương tác với chính Node Cardano, để giúp người dùng giảm bớt một số công việc nặng nhọc.

Công cụ CLI mới này sẽ hữu ích cho việc hướng dẫn người dùng cách bắt kịp tốc độ với Marlowe. Nó được sử dụng rất nhiều trong Chương trình Tiên phong Marlowe khai mạc. Cuối năm 2022 chứng kiến sự ra mắt của *Marlowe Runtime*,⁵⁸⁰ một phụ trợ ứng dụng để xử lý hợp đồng Marlowe. Các nhà phát triển có thể sử dụng API và chương trình phụ trợ của Marlowe Runtime để xây dựng và triển khai các DApps Web3 của Marlowe. Điều này giúp họ tránh được rắc rối khi phải sắp xếp thủ công quy trình công việc phụ trợ. Để giúp bạn bắt đầu, có ứng dụng khách Marlowe Runtime dành cho AWS Lambda⁵⁸¹ trên repo GitHub với một số video demo của Brian Bush.⁵⁸²

Câu hỏi thường gặp về Marlowe

H: Tôi có thể tìm hiểu thêm về Marlowe ở đâu?

A: Chương này chỉ là tổng quan về Marlowe. Để tìm hiểu thêm, hãy đăng ký kênh YouTube của Giáo sư Simon Thompson⁵⁸³ và xem lại các video của ông. Vào tháng 5 năm 2022, Niamh Ahern (Giám đốc Giáo dục của IOG) đã công bố chương trình Marlowe Pioneer đầu tiên.⁵⁸⁴ Nhóm thuần tập đầu tiên tốt nghiệp vào tháng 7 năm 2022, tất cả các bài giảng đều có trên kênh YouTube 'IOGAcademy'.⁵⁸⁵ Đọc tài liệu⁵⁸⁶ và đăng ký tham gia nhóm tiếp theo tại *Pioneers.marlowe-finance.io*

⁵⁷⁹

Công cụ Marlowe CLI, github.com/input-output-hk/marlowe-cardano/blob/cli-blog-april2022/marlowe-cli/ReadMe.md

⁵⁸⁰Thời gian chạy Marlowe, github.com/input-output-hk/marlowe-cardano/tree/main/marlowe-runtime

⁵⁸¹gian chạy Marlowe cho AWS Lambda, github.com/input-output-hk/marlowe-lambda

⁵⁸²

Brian Bush, iohk.io/en/team/brian-bush

⁵⁸³

Giáo sư Simon Thompson trên YouTube, youtube.com/user/simonjohnthompson/videos

⁵⁸⁴

Niamh Ahern, 'Tìm hiểu cách tạo hợp đồng thông minh tài chính chi phí thấp, mã thấp trong Chương trình Tiên phong Marlowe', [iohk.io/en/blog/posts/2022/05/11/learn-how-to-create-low](https://iohk.io/en/blog/posts/2022/05/11/learn-how-to-create-low-mã-chi-phí-thấp-tài-chính-hợp-đồng-thông-minh-trong-chương-trình-người-tiên-hào/)

[-mã-chi-phí-thấp-tài-chính-hợp-đồng-thông-minh-trong-chương-trình-người-tiên-hào/](https://iohk.io/en/blog/posts/2022/05/11/learn-how-to-create-low-mã-chi-phí-thấp-tài-chính-hợp-đồng-thông-minh-trong-chương-trình-người-tiên-hào/)

⁵⁸⁵

Nhóm tiên phong Marlowe đầu tiên, youtube.com/channel/UCX9j_vYOJu00iqBrCzecVw/playlists?view=50&sort=dd&shelf_id=2

⁵⁸⁶

Tài liệu Marlowe, play.marlowe-finance.io/doc/marlowe/tutorials/introducing-marlowe.html

H: Có bất kỳ hợp đồng thông minh bổ sung mới nào trên Marlowe Run không?

Trả lời: Bạn có tùy chọn sử dụng Marlowe Build để tạo hợp đồng của riêng mình. IOG đang tạo các mẫu hợp đồng mới để người dùng thử nghiệm, mẫu này sẽ sớm được tải lên danh mục hợp đồng.

H: Tôi có thể chỉnh sửa hợp đồng sau khi hợp đồng được tạo không?

Trả lời: Bạn có thể sửa đổi hợp đồng của mình trước khi hợp đồng bắt đầu hoạt động. Bạn chỉ có thể sửa đổi các trường Vai trò và Điều khoản. Tất cả các điều kiện được thiết lập khi nó bắt đầu chạy, chính xác như với một hợp đồng pháp lý điển hình.

Q: Bạn có đang sử dụng tiền thật với Marlowe Run không?

Trả lời: Không, khi bạn sử dụng Marlowe Run, bạn đang chạy và thực hiện các hợp đồng của mình bằng tiền thử nghiệm.

Hỏi: Có giới hạn cứng nào đối với số lượng hợp đồng mà tôi có thể thực hiện song song không?

Đ: IOG không đặt bất kỳ giới hạn cứng nào dành riêng cho người dùng đối với nguyên mẫu nhưng có thể làm như vậy trong Marlowe Run. Hãy nhớ rằng các máy chủ IOG có giới hạn về số lượng hợp đồng và giao dịch mà chúng có thể xử lý tại bất kỳ thời điểm nào, mặc dù điều này không dành riêng cho người dùng tại thời điểm này.

H: Tôi có thể tạo hợp đồng với người dùng từ một Blockchain khác, tức là . không Cardano?

Trả lời: Bởi vì tất cả các thỏa thuận tài chính ban đầu được thiết lập giữa các địa chỉ ví Cardano, nên tất cả các thỏa thuận phải được thực hiện với người sở hữu ví Cardano. IOG có thể cho phép các thỏa thuận trên các chuỗi khác trong các phiên bản trong tương lai, vì Marlowe về cơ bản là không liên quan đến Blockchain.

H: Tôi có thể tạo hợp đồng thông minh mới trên Marlowe Run không?

Trả lời: Bạn có thể tạo các thỏa thuận tài chính ngay bây giờ bằng cách sử dụng nhiều mẫu khác nhau từ Marlowe Marketplace, một thư viện mẫu hợp đồng thông minh. Bạn thậm chí có thể tạo các hợp đồng tài chính của riêng mình trên Marlowe Playground nếu muốn. Sau đó, bạn có thể gửi chúng đến Chợ Marlowe và chạy chúng qua Marlowe Run.

Hỏi: Marlowe Run bắt đầu từ đâu và Marlowe Playground kết thúc ở đâu?

Trả lời: Marlowe Run là sản phẩm hướng tới đối tượng lớn hơn là người dùng cuối không phải nhà phát triển. Sân chơi Marlowe được thiết kế cho các nhà phát triển kỹ thuật và các hợp đồng có thể được tạo ở đó và sau đó được sử dụng trên Marlowe Run.

H: Tôi có thể nhận trợ giúp về Marlowe Run ở đâu?

Đ: Nếu bạn gặp bất kỳ vấn đề nào, hãy sử dụng biểu mẫu email 'Gửi phản hồi' trên trang Phản hồi của trang web Marlowe, Đăng ký Chương trình Người tiên phong Marlowe để cộng tác với IOG và giúp IOG kiểm tra mức độ căng thẳng của Marlowe hơn nữa.

H: Các trường hợp sử dụng của Marlowe là gì?

Trả lời: Hợp đồng Marlowe có thể được tận dụng theo nhiều cách khác nhau, chẳng hạn như tự động hóa hoạt động của hợp đồng tài chính giao dịch Crypto trên Blockchain bằng phần mềm Marlowe. Nó cũng có thể được sử dụng vì lý do kiểm toán để theo dõi sự tuân thủ của người dùng với hợp đồng đang được thực hiện trong thế giới thực.

Marlowe chỉ đơn giản là một ví dụ về DSL hoạt động trên Blockchain. Nó đóng vai trò là một ví dụ về cách DSL mới có thể được xây dựng để bao gồm quản lý chuỗi cung ứng, luật, bảo hiểm, kế toán và các lĩnh vực khác.

Hỏi: Khi nào tôi không nên dùng Marlowe?

A: Mặc dù Marlowe là một DSL tài chính, nhưng nếu bạn cần xây dựng các loại hợp đồng khác thì sao? Cardano sử dụng Plutus, một ngôn ngữ có mục đích chung dựa trên Blockchain, để tạo ra chúng. Hợp đồng Plutus có thể quản lý nhiều loại tài sản Crypto và không có các giới hạn của hợp đồng Marlowe, chẳng hạn như thời gian chúng có thể hoạt động và số lượng cá nhân mà chúng có thể bao gồm. Mỗi hợp đồng Marlowe được quản lý bởi trình thông dịch Marlowe, một ứng dụng Plutus duy nhất.

Q: Tất cả điều này nghe có vẻ quá dễ dàng, có thực sự chỉ là vấn đề kéo và thả các Block xung quanh không?

Trả lời: Không, bạn nên nghiên cứu nội dung và trở thành Người tiên phong của Marlowe trước khi phát triển DApps sử dụng tiền của người khác. Bắt đầu bằng cách xem xét các phương pháp hay nhất, 'mùi hôi' và 'Các vấn đề tiềm ẩn với hợp đồng' trong tài liệu.⁵⁸⁷

Chương 8: Basho (Khả năng mở rộng)

'Hành trình chính là nhà của tôi'

– Matsuo Basho

Có hai thời đại còn lại trên lộ trình Cardano và chúng ta sẽ thấy trong hai chương tiếp theo chúng liên kết với nhau như thế nào. Chúng đang được làm việc song song.

Khả năng mở rộng được xác định

Lộ trình của Cardano ban đầu tập trung vào việc thiết lập một mạng lưới an toàn, phi tập trung. Mô hình bằng chứng cổ phần sáng tạo cần thời gian để ổn định và trưởng thành. Hiện có hơn 3.000 Stake Pool xác nhận giao dịch, thống nhất về trạng thái mạng. Điều này mang đến những thách thức trong việc mở rộng quy mô một hệ thống phân tán không có Node trung tâm, đáng tin cậy. Hệ thống phải đạt được sự đồng thuận để chuyển tài sản, bản ghi trạng thái và bằng chứng mật mã trên toàn cầu với các ràng buộc như tốc độ mạng, thiết lập phần cứng khác nhau, v.v.

khả năng xử lý việc sử dụng hoặc áp dụng của Blockchain . Đo khả năng mở rộng không chỉ đơn giản là đo TPS (giao dịch mỗi giây) trong bất kỳ tình huống ngẫu nhiên nào. Khả năng mở rộng có nhiều sắc thái hơn thế.

'Có, nhưng nó có thể thực hiện một triệu TPS không?' là một điệp khúc quen thuộc thường được sử dụng mà không có bất kỳ ngữ cảnh nào trên twitter Crypto. TPS (giao dịch trên giây) có lẽ là thước đo thô sơ nhất để so sánh trong số tất cả những thước đo có sẵn. Các giao dịch diễn ra ở nhiều quy mô và định dạng khác nhau. Mặc dù điều này đúng với Cardano, nhưng điều quan trọng hơn nhiều là khi so sánh hai hệ thống quá khác biệt. Các câu hỏi thích hợp hơn là... nó có thể đáp ứng nhu cầu ngày nay không? Nó có một lộ trình thực tế để xử lý hàng tỷ người dùng trong tương lai không?

Mở rộng quy mô Blockchain có nghĩa là cải thiện thiết kế Blockchain bằng cách sử dụng các kỹ thuật và tính năng khác nhau được nêu trong chương này. Nhiều người trong số họ là bổ sung và phụ thuộc lẫn nhau. Mục tiêu tổng thể là tăng thông lượng. Tìm hiểu sâu hơn, điều này có nghĩa là cải thiện hiệu suất dựa trên các số liệu sau:

- Thông lượng: lượng dữ liệu mà một hệ thống có thể xử lý trong một khoảng thời gian nhất định. Được đo bằng Byte trên giây (kilobyte trên giây, kB/s)
- CPU giây (mili giây) ms /s trên mỗi đồng hồ treo tường cho **thời gian thực thi tập lệnh**, tức là . CPU bận trong bao lâu.
- Finality : lượng thời gian cần thiết để hậu quả của một hành động trở nên bất biến và đúng với mọi người trong hệ thống
- Đồng thời: khối lượng công việc mà các tác nhân khác nhau có thể thực hiện mà không can thiệp lẫn nhau.
- Quy mô giao dịch

Kể từ tháng 11 năm 2022, các Block trên mạng chính Cardano được tạo khoảng 20 giây một lần, với kích thước khối tối đa là 88kB. Do đó, thông lượng dữ liệu là ~ 4,4kB/s.

Bất kỳ Blockchain nào cũng có thể xuất hiện nhanh chóng và hấp dẫn bằng cách sử dụng các kích thước giao dịch nhỏ và không có tập lệnh. Một số Blockchain cấu hình cao có các đặc điểm tập trung, chẳng hạn như một số ít trình xác thực kiểm soát số lượng cổ phần không tương xứng. Thật dễ dàng để một Blockchain thỏa hiệp về tính phi tập trung sau đó khoe khoang các số liệu TPS thiên văn, nhưng nếu nó cần phải dừng và khởi động lại thường xuyên, thì đó sẽ là manh mối cho thấy nó không thực sự như vẻ ngoài của nó.

TPS trên Cardano còn nhiều sắc thái hơn do tiêu chuẩn tài sản gốc của nó. eUTXO cho phép chuyển hàng trăm, thậm chí hàng nghìn tài sản gốc trong một giao dịch. Một số liệu chính xác hơn ⁵⁸⁸ là TPT (số giao dịch trên mỗi giây). eUTxO.org là một trình khám phá Blockchain được tạo bởi Peter Oravec . Đây là một công cụ học tập tuyệt vời để hiểu và hình dung cách thức hoạt động của các giao dịch trên Cardano.



Peter Oravec - eUTxO.org @oravecpeter · Oct 4

There are two #Cardano transactions on this picture...
#eutxo #cardano



Hình 47: @oravecpeter tweets về eUTxO.org ' Có 923 đầu ra của hai giao dịch này, mỗi đầu ra có thể là những người nhận khác nhau nên 923 TX... đây là siêu năng lực của UTxO ... mọi người sẽ sử dụng cái này vì nó siêu rẻ để làm tất cả những thứ này trong một TX... '

Không giống như nhiều Blockchain áp dụng cách tiếp cận 'di chuyển nhanh và phá vỡ mọi thứ', Cardano luôn tuân theo một chiến lược có chủ ý, cẩn thận và có phương pháp. Bất chấp sự bảo thủ tương đối này, Cardano là dự án Crypto phát triển nhất trên GitHub vào năm 2021⁵⁸⁹ và một lần nữa vào năm 2022.⁵⁹⁰

⁵⁸⁹Cardano trở thành dự án Crypto phát triển nhất trên GitHub vào năm 2021, cointelegraph.com/news/cardano-became-the-most-develop-crypto-on-github-in-2021-santiment

⁵⁹⁰Cardano vượt qua Ethereum trong Hoạt động phát triển hàng ngày của GitHub, invest.com/news/cryptocurrency-news/cardano-surpasses-ethereum-in-github-daily-Development-activity-2956870

IOG đã vạch ra chiến lược Basho của họ trong một bài đăng trên blog vào năm 2022.⁵⁹¹

Không có 'viên đạn ma thuật' nào để mở rộng quy mô Blockchain, nó được thực hiện bằng cách điều chỉnh các tham số và kết hợp các giải pháp khác nhau thường thuộc hai loại:

- Giải pháp lớp 1: nâng cấp được áp dụng cho giao thức chuỗi chính, cardano -node, v.v.
- Giải pháp lớp 2: giảm tải khối lượng công việc, mở rộng chức năng và tích hợp các Blockchain khác với Sidechain, cuộn ZK và các kênh trạng thái như Hydra.

Cho đến nay, Cardano đã mở rộng quy mô để đáp ứng nhu cầu, với mục tiêu đầy tham vọng và nhiều hạn chế. Những thay đổi kể từ khi hard fork Vasil đã đem hoa kết trái, tuy nhiên DeFi và RealFi sẽ bắt đầu hoạt động một cách nghiêm túc vào năm 2023. Có một số stablecoin đang ra mắt, Oracles như Charli3 sẽ trưởng thành, hơn 1.000 dự án đã sẵn sàng tham gia vào ~100 dự án hiện có.

IOG sẽ tiếp tục triển khai nghiên cứu của họ trong suốt năm 2023. **Các giải pháp trên chuỗi** bao gồm tăng kích thước khối, tạo đường ống dẫn, xác nhận đầu vào, điều chỉnh tham số, cải tiến tập lệnh Plutus, cải tiến Node và cải tiến lưu trữ trên đĩa. **Các giải pháp ngoài chuỗi** bao gồm Sidechains, Hydra, điện toán ngoài chuỗi và Mithril.

cải tiến liên tục

Là một phần của giai đoạn phát triển Basho, IOG sẽ tiếp tục cập nhật các thông số. Một cơ sở hạ tầng linh hoạt có thể uốn cong nhưng không bị gãy là chìa khóa khi các điều kiện thay đổi. Một số cân nhắc là:

- **Tăng kích thước khối:** cho phép nhiều giao dịch hơn được trang bị trong một khối. Trong thời gian bão hòa mạng, sẽ giảm thời gian chờ đợi để các giao dịch được chấp nhận bởi một khối, đây là một điều tích cực. Tuy nhiên, có một chi phí. Mất nhiều thời gian hơn để các Block lớn hơn lan truyền khắp mạng. Do đó, các Node cũng sẽ cần thêm thời gian để xác thực các giao dịch. Mặc dù việc tăng kích thước khối có thể cải thiện tốc độ mạng, nhưng những điều chỉnh như vậy nên được thực hiện cẩn thận. IOG dần dần thay đổi cài đặt và theo dõi kết quả trong thời gian bão hòa cao để đảm bảo rằng mức tăng không ảnh hưởng đến thời gian áp dụng khối.
- **Giới hạn mức khối:** tăng số lượng đơn vị bộ nhớ (đơn vị bộ nhớ trừu tượng) có sẵn cho mỗi tập lệnh trong khối. Các tập lệnh thể hiện nhiều loại logic khác nhau để sử dụng UTXO.
- **Kích thước mempool:** Kích thước của mempool được điều chỉnh liên tục. Khi thêm các giao dịch vào một khối, mempool hoạt động như một bộ đệm mạng và có thể gây ra một chút chậm trễ. Tuy nhiên, việc tăng kích thước của mempool sẽ không tăng thông lượng mạng do hàng đợi giao dịch sẽ không thay đổi. Mempool cho phép áp dụng công bằng các giao dịch mới đến một cách ngẫu nhiên.
- **Plutus yêu cầu tài nguyên,** cả đơn vị tính toán (CPU) và đơn vị bộ nhớ, để thực hiện những việc hữu ích với tập lệnh Plutus. Các giới hạn bộ nhớ của Plutus đã được mở rộng, cho phép họ tạo các tập lệnh Plutus phức tạp hơn hoặc cho phép các tập lệnh hiện tại xử lý nhiều mục dữ liệu hơn, nâng cao tính đồng thời hoặc mở rộng khả năng của chúng.
- Vì tham số d (phân quyền) là '0' trong hơn một năm, nên nó đã bị xóa hoàn toàn khỏi giao thức như một phần của hard fork Vasil.

Cân nhắc tính kịp thời khi tăng thông lượng:

- **Tính kịp thời:** thời gian cần thiết để áp dụng một khối. Toàn bộ 'ngân sách' cho việc áp dụng khối được đặt ở mức 5 giây để một khối lan truyền qua 95% mạng, với các tập lệnh Plutus có ngân sách tính bằng mili giây. Điều này được thực hiện để tránh độc quyền bằng cách cho phép khối chứa cả tập lệnh và giao dịch đơn giản.
- **Thông lượng:** Người dùng sẽ trải qua thời gian chấp nhận khối lâu hơn nếu số lượng khối được tăng lên đáng kể cùng một lúc. Đó là bởi vì thông lượng và tính kịp thời trái ngược nhau: tăng thông lượng có nghĩa là hiệu suất mạng cao hơn, nhưng nó có thể phải trả giá bằng sự chậm trễ khi hệ thống bị quá tải.

⁵⁹¹Tim Harrison, 'Cách chúng tôi mở rộng quy mô Cardano vào năm 2022', iohk.io/en/blog/posts/2022/01/14/how-we-re-scaling-cardano-in-2022/

Sự tắc nghẽn được giảm thiểu bởi các hệ thống hiệu quả. Mạng của Cardano sử dụng 'áp lực ngược' để kiểm soát áp lực tổng thể của hệ thống. Mặc dù một số người dùng cá nhân nhất định có thể báo cáo thời gian chờ giao dịch cao hơn trong đợt sụt giảm NFT lớn, nhưng điều này không có nghĩa là mạng đang 'gặp khó khăn'. Nó thực sự biểu thị rằng mạng đang hoạt động bình thường, trong cái được gọi là sự xuống cấp duyên dáng.

Ouroboros (**Praos**) có các tiêu chí chính xác phải được đáp ứng để đạt được **các mục tiêu bảo mật của mình** , trong đó thời gian lan truyền khối là ưu tiên hàng đầu. Thời gian lan truyền khối đề cập đến khoảng thời gian cần thiết để một khối mới đúc được lan truyền qua 95% các Node ADA đã đặt cọc trên mạng. Để Praos luôn an toàn, các Block mới phải được truyền đi cứ sau 5 giây.

Ví dụ, giới hạn 5 giây này được IOG coi là "ngân sách" mà họ có thể sử dụng để tăng kích thước khối. Kích thước khối tăng lên sẽ tự động kéo dài thời gian truyền khối; do đó, họ phải giám sát cẩn thận mọi sửa đổi mà họ thực hiện để cải thiện tốc độ mà không gây nguy hiểm cho an ninh của mạng. Ngân sách này sẽ được mở rộng trong các lần lặp lại Ouroboros trong tương lai. Trong khi đó, IOG sẽ tập trung vào việc bảo vệ an ninh đồng thời mở rộng mạng để đáp ứng nhu cầu ngày càng tăng.

Node (cardano -node)

Node là trung tâm của mọi thứ trong Cardano. Nó lưu trữ một bản sao đầy đủ của Blockchain, xử lý quy tắc sổ cái và tập lệnh plutus , tạo giao dịch và chứng chỉ, phân phối (phân tán) giao dịch và khối trên toàn mạng. Nó tính toán và phân phối trực tiếp phần thưởng đặt cược cho những người được ủy quyền cũng như cho Stake Pool. Node đảm bảo tính phi tập trung khi có hơn 3.000 SPO chạy Node. Khi bạn sử dụng ví của mình, bạn đang sử dụng Node. Vì vậy, rất nhiều thứ đang diễn ra bên trong để làm cho dây chuyền hoạt động. Do đó, điều hợp lý là cải thiện hiệu suất của Node nếu có thể.

Key 2022 Enhancements

Network parameters

Steadily increased block size and script execution budget to meet increasing demand from network utilization.

Diffusion pipelining

Faster diffusion times allow the network to handle more transactions per second.

Reference scripts

10x transaction size reduction when executing Plutus scripts with Plutus V2 with a consequent fee reduction.

Dynamic P2P

Self-organized network based on connection speed will implement the last mile of network decentralization.

Other honorable mentions

- Inline datums
- Reference inputs
- Collateral change address
- New Plutus built-ins
- Incremental transaction signing
- Local transaction monitoring

Hình 48: Các cải tiến Node chính, từ bài nói chuyện của Kevin Hammond tại ScotFest.

Một số thay đổi và cải tiến quan trọng từ năm 2022 là:

- Khả năng tạo các giao dịch tuân thủ Ngôn ngữ định nghĩa dữ liệu ngắn gọn (CDDL) bằng cách sử dụng các công cụ gốc CLI của Node, thay vì dựa vào các công cụ của bên thứ ba.

Cách máy tính lưu trữ dữ liệu khi chúng đang thực thi không nhất thiết là cách tuyệt vời để lưu trữ dữ liệu khi bạn đang cố gửi dữ liệu qua mạng. Khi dữ liệu được lấy ra khỏi bộ nhớ của máy tính và được chuyển sang một máy ngang hàng khác để truyền một khối, điều quan trọng là một biểu diễn được lấy ra khỏi bộ nhớ của máy tính và đưa vào một quy trình được gọi là tuần tự hóa. Tuần tự hóa ⁵⁹²lấy đối tượng dữ liệu và biểu diễn nó theo cách hiệu quả để vận chuyển.

Trong ngữ cảnh lưu trữ dữ liệu, **tuần tự hóa** là quá trình dịch cấu trúc dữ liệu hoặc trạng thái đối tượng sang định dạng có thể được lưu trữ (ví dụ: trong tệp hoặc bộ nhớ đệm) hoặc được truyền (ví dụ: qua mạng) và được xây dựng lại sau đó (có thể trên một máy tính

- IOG sử dụng Biểu diễn đối tượng nhị phân ngắn gọn (CBOR) để tuần tự hóa. Nó dựa trên JSON,⁵⁹³ được sử dụng rộng rãi trong phát triển web. Thay đổi mà IOG đã thực hiện là CDDL. CDDL (Ngôn ngữ định nghĩa dữ liệu ngắn gọn) giống như một lược đồ cho CBOR. IOG đã cố gắng nâng cao lược đồ này cho biểu diễn tuần tự hóa cơ bản của họ. Do đó, việc gửi dữ liệu qua mạng hiện đã được thực hiện hiệu quả hơn.
- Hỗ trợ cho các giao dịch có nhiều chữ ký trong các giai đoạn gia tăng. Mặc dù đã có thể có một giao dịch Cardano được ký bởi nhiều thực thể bằng cách sử dụng khóa riêng của họ (tương đương với tài khoản ngân hàng chung), bản cập nhật này cho phép ký giao dịch gia tăng. Thay vì cần phải ký giao dịch đồng thời, giờ đây một bên có thể ký trước rồi gửi cho bên kia
- Giờ đây, các SPO có thể kiểm tra lịch trình lãnh đạo bằng công cụ CLI mới. Công cụ này cho phép các SPO kiểm tra các vị trí mà SPO gửi lệnh sẽ đúc một khối cho kỳ nguyên tiếp theo. Một số người lo ngại rằng khả năng này gây lo ngại về bảo mật, tuy nhiên, công cụ này được cấu trúc sao cho mỗi SPO chỉ có thể kiểm tra lịch trình sắp tới của chính họ. Họ không thể xác minh lịch trình của bất kỳ SPO nào khác
- Một công cụ CLI để kiểm tra các mempool cục bộ. Đây là một công cụ dành cho nhà phát triển cho phép bạn xem mempool cục bộ, là nơi các giao dịch được lưu trữ trước khi được đưa vào một khối. Tính năng này cho phép các nhà phát triển theo dõi trạng thái của một giao dịch trước khi nó bị chặn
- Một công cụ dòng lệnh để ước tính chi phí tập lệnh. Giờ đây, người dùng Node có thể ước tính chi phí thực thi tập lệnh Plutus với độ chính xác cao hơn. Điều này rất hữu ích vì nó cho phép các nhà phát triển xem họ đang sử dụng tài nguyên nào (giới hạn bộ nhớ/CPU, v.v.) khi xây dựng hợp đồng thông minh hoặc tập lệnh xác thực, điều này đặc biệt có giá trị để tạo giao dịch Plutus. Giờ đây, các nhà phát triển có thể xem tập lệnh của họ sẽ cần bao nhiêu tài nguyên khi chạy trên chuỗi.
- Ngang hàng động cho các Node: dần dần triển khai các cơ chế để kích hoạt mạng tự tổ chức dựa trên tốc độ kết nối và chất lượng kết nối giữa các Node khác nhau trong hệ thống.

Các cải tiến cho phép phân phối đồng đều hơn các tính toán tiền cược và phần thưởng qua các kỳ nguyên, cho phép kích thước khối lớn hơn. Việc sử dụng bộ nhớ cũng hiệu quả hơn về tổng thể. Nén bộ nhớ giảm thiểu dấu vết RSS⁵⁹⁴, trong khi chia sẻ bộ nhớ làm giảm lượng dữ liệu cần khởi tạo.

Nhóm Node đã tham dự các hội thảo xung quanh việc nâng cấp Voltaire được nêu trong CIP 1694 (đề xuất về cách Voltaire nên được triển khai). Sẽ có các nâng cấp dần dần, lặp đi lặp lại đối với Node để phù hợp với những thay đổi đối với cấu trúc quản trị trên chuỗi. Node sẽ tạo điều kiện bỏ phiếu trực tuyến, bao gồm các cơ chế lan can được nêu trong hiến pháp. Bản thân hiến pháp sẽ được ghi lại dưới dạng hàm băm trên chuỗi. Phần lớn chi tiết cho CIP 1694 vẫn cần được loại bỏ nhưng cardano-node đương nhiên sẽ là trung tâm của mọi thứ.

Khi các bản cập nhật đang diễn ra, tốt nhất bạn nên kiểm tra các ghi chú phát hành⁵⁹⁵ để biết bản mới nhất.

Các cải tiến của Plutus V2

Tại ScotFest ở Edinburgh, Andrew Sutherland (Trưởng nhóm Trình biên dịch Plutus), đã đánh giá năm kể từ khi PlutusV1 được ra mắt và sau đó được cải tiến với V2 vào tháng 9 năm 2022. Trong năm, nhóm của anh ấy đã chạy trung bình nửa triệu tập lệnh Plutus mỗi tháng vào mỗi đêm hệ thống kiểm thử hồi quy⁵⁹⁶. Việc tập trung vào chất lượng như vậy đã mang lại kết quả với việc tối ưu hóa trình biên dịch Plutus và tăng 30% hiệu quả của tập lệnh. Nhiều cải tiến khác nhau được thực hiện với hard fork Vasil đã dẫn đến trình thông dịch lỗi nhanh hơn, thực thi Plutus Core không định kiểu nhanh hơn và phí giao dịch thấp hơn. Sutherland ghi nhận quy trình CIP là động lực thúc đẩy tiến độ.

khác). Khi chuỗi bit kết quả được đọc lại theo định dạng tuần tự hóa, nó có thể được sử dụng để tạo một bản sao giống hệt về mặt ngữ nghĩa của đối tượng ban đầu.

⁵⁹³

Ký hiệu đối tượng JavaScript (JSON) là một định dạng tệp tiêu chuẩn mở sử dụng văn bản mà con người có thể đọc được để truyền các đối tượng dữ liệu bao gồm các cặp giá trị thuộc tính và kiểu dữ liệu mảng (hoặc bất kỳ giá trị có thể tuần tự hóa nào khác).

⁵⁹⁴

Kích thước cài đặt thường trú (RSS) là phần bộ nhớ bị chiếm bởi một tiến trình được giữ trong bộ nhớ chính (RAM).

⁵⁹⁵

phát hành Node Cardano, github.com/input-output-hk/cardano-node/releases

⁵⁹⁶

Kiểm thử hồi quy là chạy lại các kiểm thử để đảm bảo rằng phần mềm đã phát triển và kiểm thử trước đó đang hoạt động như mong đợi sau khi thay đổi.

MuesliSwap (muesliswap.com), DEX gốc đầu tiên trên Cardano, đã tham gia vào một nghiên cứu điển hình về điểm chuẩn cho các tập lệnh Plutus V2. Kết quả là giảm 90% quy mô giao dịch và tiết kiệm 50% phí giao dịch.

Bản cập nhật CIP 49 'SEC P' (hard fork trong thời đại) vào tháng 2 năm 2023 đã mở ra một thế giới mới về các tùy chọn khả năng tương tác. Đây là những khối xây dựng quan trọng cho bảo mật cầu, trong số các trường hợp sử dụng khác. Vì chúng đã được cộng đồng thử nghiệm từ tháng 11 năm 2022, nên chúng ta sẽ sớm thấy chúng được áp dụng trong DApps.

The best is yet to come

What's in store for Plutus

New language extensions for cryptography

- Additional elliptic curve primitives
- More arithmetic operators

Plutus compiler

- 30% to 50% performance improvement
- Plutus compiler ready for multiple front end languages

Developer experience improvements

- Much better debugging support
- Example projects

Open Plutus initiative

- Collaborating with the community on Plutus roadmap
- Developer experience working group

Hình 49: từ bài nói chuyện ScotFest của Andrew Sutherland 'Scaling Cardano với Plutus V2'

đường ống dẫn

Trước khi Pipelining được giới thiệu, một khối đã được đúc bởi một SPO, đó là một khối mới trong Blockchain phải được xác thực và gửi lên một máy ngang hàng. Vấn đề là các đồng nghiệp cũng phải xác thực nó và sau đó gửi nó cho đồng nghiệp của họ và đó là cách các Block lan truyền trên mạng.

Bằng cách kết hợp xác thực với lan truyền, thời gian cần thiết để một khối lan truyền sẽ giảm xuống. Bằng cách giảm thiểu 'thời gian chết' giữa các Block, mục tiêu là để các Block được lan truyền tới ít nhất 95% đồng nghiệp trong vòng 5 giây (chỉ phí lan truyền khối). Điều này cho phép linh hoạt thực hiện các điều chỉnh tỷ lệ khác, chẳng hạn như tăng kích thước khối hoặc các giới hạn tham số khác của Plutus.

Hệ thống đường ống là một tiến trình tự nhiên của 'hệ thống ống nước' của Cardano. Đây là một phần quan trọng của chiến lược mở rộng quy mô và là một trong chuỗi các giai đoạn phức tạp cách tiếp cận hợp lý của IOG để tăng cường năng lực của Cardano khi hệ sinh thái mở rộng. IOG theo dõi và xem xét cẩn thận từng bản cập nhật trong ít nhất một kỳ nguyên (5 ngày) trước khi tiến hành các thay đổi tiếp theo. Kiến trúc mạng phi tập trung phải được mở rộng tùy thuộc vào việc sử dụng trong thế giới thực, bất chấp nỗ lực nghiên cứu và kỹ thuật đáng kể đã được tạo ra và cài đặt hệ thống.

đường ống khuếch tán

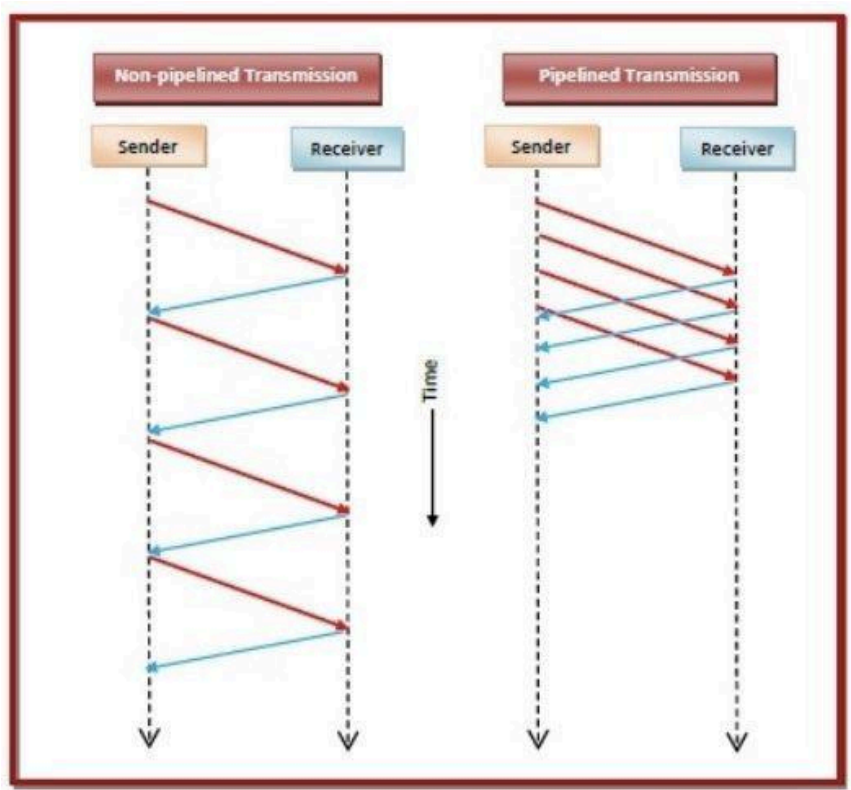
Đường ống, hay cụ thể hơn, đường ống khuếch tán, là một cải tiến của lớp đồng thuận cho phép truyền khối nhanh hơn. Nó cho phép có nhiều khoảng trống hơn, cho phép cải thiện hiệu suất và khả năng cạnh tranh của Cardano hơn nữa. Điều quan trọng là phải hiểu hành vi của hệ thống về cách các Block lan truyền, để xem chiến lược này hoàn thành mục đích của nó như thế nào.

Khi nó đi qua chuỗi, một khối trải qua 6 giai đoạn:

1. Chặn tiêu đề⁵⁹⁷truyền

2. Xác thực tiêu đề khối
3. Khởi yêu cầu cơ thể và truyền
4. Xác thực nội dung khối và mở rộng chuỗi cục bộ
5. Chặn truyền tiêu đề đến các Node hạ lưu
6. Khởi truyền nội dung đến các Node hạ lưu

Đường dẫn của một khối có tính tuần tự cao. Tại mỗi Node, tất cả các bước diễn ra theo cùng một thứ tự mỗi lần. Việc truyền khối mất nhiều thời gian do số lượng lớn các Node và số lượng khối ngày càng tăng. Các lớp đường ống khuếch tán chồng lên nhau một số giai đoạn trên, cho phép chúng xảy ra đồng thời. Điều này mất ít thời gian hơn và tăng thông lượng.



Hình 50: Đường ống (được phép của tweet @jJosjuaThreatt)

Tiết kiệm thời gian do kỹ thuật này mang lại sẽ cho phép Cardano mở rộng hơn nữa, bao gồm các điều chỉnh đối với:

- Kích thước khối – khối càng lớn thì càng có nhiều giao dịch và tập lệnh có thể chứa được
- Giới hạn bộ nhớ Plutus - lượng bộ nhớ tối đa mà tập lệnh Plutus có thể sử dụng
- Giới hạn CPU của Plutus - một tập lệnh có thể được cung cấp thêm tài nguyên máy tính để thực thi hiệu quả hơn.

Pipelining đảm bảo rằng tiêu đề khối tham chiếu hàm băm của khối trước đó được lan truyền chính xác. Siêu dữ liệu được bao gồm trong khối tiếp theo chứa nội dung của khối trước đó. Đây là một biện pháp bảo vệ để ngăn chặn các cuộc tấn công DDoS (từ chối dịch vụ phân tán) ngay cả khi không có xác nhận chặn đầy đủ.

Từ lý thuyết đến thực hành

Đường ống khuếch tán được tạo ra với mục tiêu đạt được sự lan truyền khối nhanh hơn trong khi tránh những thay đổi 'phá hoại' đối với chuỗi. Vì các Node phụ thuộc vào các phương pháp hiện tại nên IOG không muốn loại bỏ bất kỳ giao thức, giao thức nguyên thủy hoặc tương tác nào hiện đang được sử dụng trong Cardano. Thay vì sửa đổi cách thức hoạt động của mọi thứ hiện tại, họ đang thiết lập một giao thức mới với mục đích là thông báo trước cho các thực thể đăng ký khi một khối mong muốn mới được phát hiện, trước khi xác thực đầy đủ. Việc triển khai Pipelining không yêu cầu hard fork và có thể được triển khai với bản phát hành Node tiêu chuẩn. Nó được giới thiệu không phô trương cùng lúc với hard fork Vasil.

Tiêu đề khối : Phần của khối chứa thông tin về chính khối đó (siêu dữ liệu khối), thường bao gồm dấu thời gian, biểu diễn hàm băm của dữ liệu khối, hàm băm của tiêu đề khối trước đó và nonce mật mã (nếu cần).

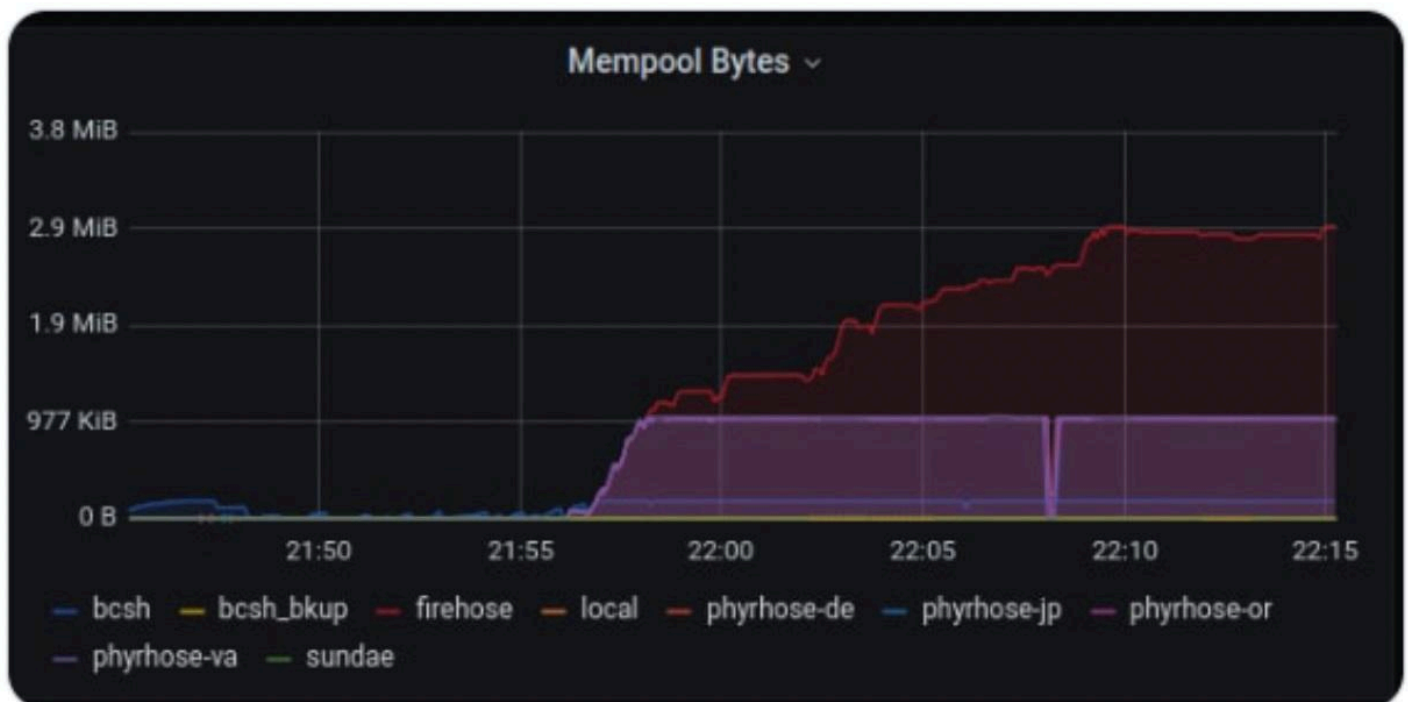
Khả năng thông báo trước cho các đồng nghiệp và cung cấp cho họ một khối trước khi nó được xác minh, cho phép đồng nghiệp xuôi dòng tìm nạp trước phần thân khối mới, là tính năng quan trọng nhất do đường ống mang lại. Điều này tiết kiệm rất nhiều thời gian vì thời gian cần thiết để xác minh một khối qua nhiều bước nhảy được giảm đáng kể. Mạng đã được kiểm tra căng thẳng sau Vasil và kết quả ban đầu rất khả quan. Node hiện đang chạy nhanh hơn, với nhiều thông lượng hơn.



Rick McCracken DIGI
@RichardMcCrackn

...

Hey @IOHK_Charles we are trying our hardest over here to break #Cardano but we have failed. We cannot break it. Your did it! ★ #Cardano #Vasil



Hình 51: Tweet từ Rick McCracken sau Vasil... 'Chúng tôi đang tấn công chuỗi mạnh mẽ nhất có thể từ DripDropz Biểu đồ hiển thị mempool màu đỏ trên đường phyrhose trên công suất chuỗi Cardano và chuỗi đang chạy hoàn hảo khỏe.'

Lưu trữ trên đĩa

IOG nhận thức sâu sắc rằng Node Cardano cần RAM⁵⁹⁸ khi chạy. Họ muốn bắt đầu chuyển mọi thứ ra khỏi RAM, ra khỏi bộ nhớ dễ bay hơi đắt tiền đó sang bộ lưu trữ trên đĩa. Đây là một thực tế phổ biến trong khoa học máy tính. Lưu trữ trên đĩa sẽ cải thiện trải nghiệm người dùng cho các nhà phát triển trên Cardano.

Bằng cách lưu trữ các thành phần của trạng thái giao thức trên đĩa, các Node sẽ sử dụng ít bộ nhớ hơn, cho phép các hệ thống thiếu RAM vận hành các Node miễn là chúng có đủ dung lượng lưu trữ và bộ nhớ sẽ không còn là hạn chế về quy mô. Trạng thái Blockchain sẽ có thể tăng đáng kể do điều này.

⁵⁹⁸

RAM (bộ nhớ truy cập ngẫu nhiên) là một dạng bộ nhớ máy tính có thể đọc và thay đổi theo bất kỳ thứ tự nào, thường được sử dụng để lưu trữ dữ liệu đang hoạt động và mã máy. Thiết bị bộ nhớ truy cập ngẫu nhiên cho phép các mục dữ liệu được đọc hoặc ghi trong khoảng thời gian gần như giống nhau bất kể vị trí vật lý của dữ liệu bên trong bộ nhớ.

Có một dự án 'UtxO HD' đang diễn ra để chuyển trạng thái sổ cái của Cardano từ trạng thái hoàn toàn trong bộ nhớ sang được lưu trữ nhiều hơn trên đĩa. Điều này là cần thiết để có thể mở rộng sang các trạng thái sổ cái lớn hơn. Nó cũng sẽ giảm bớt các yêu cầu về RAM cho các Node một cách tự nhiên. Tính năng này sẽ kích hoạt các mục lộ trình khác, chẳng hạn như các phần của Ouroboros *Leios*.

Có một tài liệu trực tiếp ⁵⁹⁹trên GitHub đi sâu vào các chi tiết kỹ thuật hơn.

Điện toán ngoài chuỗi

Giảm tải một phần của máy tính, chẳng hạn như thông qua Thực thi hợp đồng không đồng bộ ⁶⁰⁰(ACE), có thể cải thiện hiệu quả của mạng lưới. Các giao dịch diễn ra bên ngoài Blockchain, nhưng mô hình tin cậy cho phép các giao dịch nhanh chóng và không tốn kém. Khái niệm này vẫn đang trong chế độ nghiên cứu và có thể sẽ được triển khai trong bản cập nhật trong tương lai.

Bí ngân

Mithril cho phép người dùng có được trạng thái hiện tại của Blockchain mà không cần khôi phục toàn bộ lịch sử của nó. Nhẹ, nhanh, hiệu quả và an toàn ... Mithril được đặt tên theo kim loại hư cấu được tìm thấy trong các tác phẩm về Trung Địa của JRR Tolkien. Nó nhẹ nhưng *'được rèn bằng bạc nguyên chất với sức mạnh và độ bền của thép ba lớp'*.

Tại Hội nghị thượng đỉnh Cardano 2021, ⁶⁰¹các nhà nghiên cứu của IOG, Pyrros Chaidos và Roman Oliynykov đã trình bày Mithril – một giao thức và mạng mới dựa trên tài liệu nghiên cứu ⁶⁰²của Chaidos và Giáo sư Aggelos Kiayaas. Mithril sử dụng sơ đồ đa chữ ký ngưỡng (STM) dựa trên cổ phần để giải quyết các vấn đề về đồng bộ hóa chuỗi, khởi động trạng thái và tin cậy trong DApps. Mithril đã phát triển thành một dự án mã nguồn mở với tần suất phát hành hai tuần một lần. Quá trình phát hành ⁶⁰³liên tục được tinh chỉnh để mang lại trải nghiệm mượt mà cho nhà phát triển.

Bài báo gốc và blog có liên quan ⁶⁰⁴của Olga Hryniuk, kỹ thuật và phân tích tầm nhìn dài hạn cho giao thức. Giống như tất cả các dự án mã nguồn mở, linh hoạt, việc triển khai cuối cùng có thể khác nhau. Điều rõ ràng là nhu cầu cấp thiết về một giải pháp như thế này để cho phép đồng bộ hóa nhanh hơn với Blockchain.

Dựa trên tính bảo mật của hệ thống đặt cược của Cardano, Mithril cho phép các bên liên quan xác nhận một số thực tế, với trọng số tỷ lệ thuận với số tiền đặt cược của họ. Bằng chứng ban đầu về khái niệm của Mithril là khởi động một Node Cardano đầy đủ, tuy nhiên, nó rất linh hoạt để áp dụng cho các giao thức khác. Ví dụ: tính năng chính của việc xác thực ảnh chụp nhanh trạng thái có thể được áp dụng để trao đổi dữ liệu giữa các Sidechain, cuộn lên, bỏ phiếu trên chuỗi... bất kỳ kịch bản nhiều đối tượng nào cũng là một trường hợp sử dụng tiềm năng.

Mithril là lớp phủ nằm trên chuỗi chính Lớp 1 của Cardano, cho phép người dùng tạo chứng chỉ bằng chứng. Các chứng chỉ do Mithril tạo ra có cùng thuộc tính bảo mật mà Ouroboros có. Điều này có lợi ích sâu sắc. Ví dụ: hàng triệu phiếu bầu có thể diễn ra ngoài chuỗi và sau đó được tổng hợp lại với nhau dưới dạng chữ ký ngưỡng. Cuối cùng, nó sẽ chỉ là một giao dịch duy nhất trên chuỗi. Một Node đầy đủ như Daedalus có thể đồng bộ hóa nhanh hơn nhiều và ví nhẹ như *Lace* hiện có bảo mật Node đầy đủ, mặc dù đó là ứng dụng khách nhẹ.

Làm thế nào nó hoạt động

⁵⁹⁹dự thảo tài liệu thiết kế UTxO HD để xem xét,

github.com/input-output-hk/ouroboros-network/commit/f4f9be4f73a4f4cc31e98ec6a0511d9c7e9a4601

⁶⁰⁰

Wust, et al, (2019), 'ACE: Thực thi đồng thời và không đồng bộ của Hợp đồng thông minh phức tạp', eprint.iacr.org/2019/835.pdf

⁶⁰¹

Hội nghị thượng đỉnh Cardano 2021, youtube.com/watch?v=rmknjCvRH-Y

⁶⁰²

Chaidos, Kiayias (2021), 'Mithril: Đa chữ ký dựa trên ngưỡng cổ phần', eprint.iacr.org/2021/916.pdf

⁶⁰³

Quy trình phát hành Mithril, mithril.network/doc/dev-blog/2022/12/05/release-process

⁶⁰⁴

Mithril: một Blockchain mạnh hơn và nhẹ hơn để mang lại hiệu quả tốt hơn,

iohk.io/en/blog/posts/2021/10/29/mithril-a-stronger-and-lighter-blockchain-for-better-efficiency/

Lược đồ STM được mô tả trong tài liệu nghiên cứu ban đầu hiện có sẵn dưới dạng thư viện lỗi độc lập trên GitHub. Nó chứa tập hợp đầy đủ các nguyên mẫu của giao thức Mithril và độc lập ở chỗ nó là Blockchain bất khả tri, nó có khả năng chạy trên bất kỳ Blockchain PoS nào.

Mạng Mithril nằm trên thư viện Mithril Core. Có ba loại Node trong thiết lập bằng chứng về khái niệm hiện tại.

- **Mithril Signer** được điều hành bởi SPO (SPO), song song với Node Cardano. Nó ký trạng thái sổ cái, tức là . tạo chữ ký cá nhân.
- **Bộ tổng hợp Mithril** thu thập chữ ký của Người ký và tạo nhiều chữ ký, sau đó nhúng chúng vào chứng chỉ. Trình tổng hợp cũng tạo và lưu trữ kho lưu trữ ảnh chụp trạng thái sổ cái. Chúng có thể lớn, tính bằng hàng chục GB và sẽ phát triển khi một Blockchain phát triển.
- **dụng khách Mithril** khôi phục (bootstraps) một Node Cardano đầy đủ bằng cách chụp nhanh và chuỗi chứng chỉ của nó từ Node Trình tổng hợp và xác minh tính hợp lệ của chúng bằng các nguyên hàm mật mã Mithril.

Tương tự xổ số

Kiến trúc sư IOG Arnaud Bailly phát biểu trên Cardano360 tháng 5 năm 2022⁶⁰⁵

Một phép loại suy mà bạn có thể sử dụng để nghĩ về nó là xổ số. Như vậy tùy theo số tiền đặt cược mà bạn rút vé số, và tùy theo số tiền đặt cược mà bạn rút ra, tùy theo số lượng vé bạn mua mà khả năng bạn có vé trúng thưởng cao hơn. Và điều này cũng tương tự đối với Mithril...bạn có thể có nhiều vé trúng thưởng. Sau khi đã rút đủ số vé chiến thắng, đối với tất cả các chủ sở hữu Stake Pool, thì chứng chỉ có thể được phát hành cung cấp chữ ký được chứng nhận về trạng thái hiện tại của chuỗi từ một cổ phần, một số cổ phần của chủ sở hữu Stake Pool, từ một số cổ phần được xác định trước. ... và đây là cái mà chúng tôi gọi là ảnh chụp nhanh.

Giờ đây, ảnh chụp nhanh được cung cấp cho khách hàng và khách hàng có thể xác minh nó, họ có thể xác minh những ảnh chụp nhanh này bằng cách kiểm tra chữ ký tổng hợp từ tất cả những người trúng xổ số, có thể nói như vậy, v.v. từ tất cả những người ký tên.... và kiểm tra xem họ thực sự hợp pháp và việc kiểm tra này cũng dựa trên việc kiểm tra xem việc phân phối cổ phần có hợp pháp hay không và điều này được thực hiện thông qua việc kiểm tra chứng chỉ chuỗi cho đến một số chứng chỉ chung...và khi họ đã xác minh tính hợp lệ của chứng chỉ, bây giờ họ chỉ cần tải xuống tự chụp nhanh, khởi động Node mà không cần phải trải qua quá trình xác minh mọi thứ rắc rối.

Tiến tới ngày

Ban đầu, Mạng Mithril đã được thử nghiệm dưới dạng phiên bản tập trung (Bộ tổng hợp Mithril do IOG vận hành). Điều này đã mở đường cho một phiên bản phi tập trung trên mạng thử nghiệm Cardano nơi các SPO chạy Mithril Aggregators. Tại ScotFest,⁶⁰⁶ bản trình diễn của Jean-Philippe Raynaud đã cho thấy ví Daedalus được đồng bộ hóa nhanh hơn 15 lần với Mithril, so với cách khởi động cổ điển. Mithril rất quan trọng đối với các ví nhẹ không đáng tin cậy như *Lace* vì nếu không chúng sẽ cần một bên thứ ba để đồng bộ hóa lịch sử Blockchain. Mithril sẽ cho phép thời gian đồng bộ hóa nhanh nhưng cũng được hưởng lợi từ các thuộc tính bảo mật của chuỗi chính. Việc bỏ phiếu trực tuyến sắp tới được lên kế hoạch cho *Thời đại Voltaire* cũng phụ thuộc vào Mithril.

Mithril sẽ được triển khai trên mạng chính vào năm 2023.

định hướng cộng đồng

Theo dõi mithril.network để có các bản cập nhật mới nhất và đóng góp cho kho lưu trữ Mithril trên GitHub⁶⁰⁷

Cách tốt nhất để đóng góp là thiết lập và thử nghiệm Mithril trong các bối cảnh bằng chứng cổ phần khác nhau. Tài liệu Mithril cung cấp hướng dẫn từng bước để khởi động Node Cardano, chạy Node người ký hoặc chạy mạng Mithril riêng.

Ren

Tại Consensus 2022, diễn ra ở Austin, Texas, IOG đã thông báo rằng ví nhẹ mới của họ là *Lace* (lace.io) đang được phát triển. Charles

⁶⁰⁵

Cardano360 tháng 5 năm 2022, youtube.be/Ar_8Lo0nV1s?t=228

⁶⁰⁶

Nhẹ, nhanh, hiệu quả và an toàn - Mithril, youtube.com/watch?v = VyxsqwNWZt4

⁶⁰⁷

GitHub , github.com/input-output-hk/mithril

Hoskinson chạy qua một bản demo ⁶⁰⁸giải thích rằng *Lace* sẽ không chỉ là một chiếc ví mà còn là một nền tảng cho phép người dùng kết hợp danh tính, bỏ phiếu và trải nghiệm DApp Store với nhau. Rõ ràng ren sẽ là mấu chốt cho việc áp dụng Cardano.

Việc triển khai Node đầy đủ của IOG là ví *Daedalus*, là ứng dụng khách trên máy tính để bàn được đồng bộ hóa hoàn toàn với lịch sử Blockchain. Vì đầy đủ Node là một giải pháp thay thế tuyệt vời cho những người dùng cao cấp hơn, nhưng vì chúng chứa một bản sao đầy đủ của Blockchain nên chúng sử dụng nhiều tài nguyên và mất nhiều thời gian để đồng bộ hóa. Do đó, ví đầy đủ Node có thể không phù hợp với người dùng muốn truy cập ngay vào tiền của họ. Khi Cardano mở rộng sang nhiều quốc gia chính thống hơn, đặc biệt là ở các quốc gia mới nổi, một giải pháp thay thế khả thi là cần thiết. Lace sẽ tập trung vào việc thúc đẩy việc áp dụng bằng cách cung cấp trải nghiệm người dùng tuyệt vời.

Ban đầu nó sẽ hỗ trợ những điều cơ bản: lưu trữ ADA của bạn, gửi/nhận ADA, lưu trữ NFT và ủy thác ADA của bạn. Về lâu dài, nó sẽ tích hợp với Atala Prism (giải pháp Nhận dạng phi tập trung của IOG) và DApp Store, cho phép bỏ phiếu Catalyst và có thể tương tác với các Blockchain khác.

Trong một cuộc phỏng vấn ⁶⁰⁹với Eleanor Terrett cho FoxBusiness, Charles Hoskinson đã nói nhiều hơn về Ren :

Vì vậy, những gì chúng tôi muốn làm là xây dựng một nền tảng rất thân thiện với người tiêu dùng và phát triển rất nhanh. Vì vậy, cứ sau 6 đến 9 tuần, các tính năng và chức năng mới sẽ ra mắt. Nó cung cấp cho bạn một loại dao mật mã của quân đội Thụy Sĩ, vì vậy bạn có thể thực hiện một số việc rất phức tạp theo thời gian như giao dịch nhiều chữ ký, ủy quyền một phần và khóa proxy ⁶¹⁰... nhưng cuối cùng bạn sẽ sử dụng đa chuỗi, đa tài sản. Đó là nơi lưu trữ cuộc sống số của bạn ở khía cạnh đó. Vì vậy, đó là nơi bạn có thể tương tác với mọi người, nơi bạn có thể chia sẻ danh tính, nhiều danh tính mà bạn có thể chia sẻ. Danh tính cho GameFi, một cho tuân thủ, một cho bạn bè, một cho NFT... tất cả những thứ này.

[...] Vì vậy, thật tuyệt khi có một nền tảng, nơi chúng tôi không chỉ có thể tạo ra những đổi mới về công nghệ, tích hợp những đổi mới và kiểu như mang mọi người lại với nhau và thống nhất... mà còn cả những đổi mới về giao diện người dùng để cuối cùng giúp mọi người sử dụng Crypto dễ dàng hơn... bởi vì nếu bạn muốn tăng từ 10 triệu lên một tỷ người, đồng bằng đó là khả năng sử dụng chứ không phải chức năng. Thông thường, chức năng của bạn tuyệt vời ở mức 10 triệu nhưng đó là 'bí mật được giữ kín nhất'. Tỷ chỉ là khi bạn có khả năng sử dụng tuyệt vời trong khía cạnh đó.

thủy

Hydra giới thiệu ⁶¹¹các kênh trạng thái đẳng cấu để tăng thông lượng, giảm độ trễ, tiết kiệm tiền nhờ giảm phí giao dịch và nhu cầu lưu trữ. IOG đã phát triển Hydra như một giải pháp cho Cardano và các mạng liên quan bằng phương pháp dựa trên bằng chứng, nguyên tắc. Hydra là kết quả của quá trình nghiên cứu đáng kể và là một bước quan trọng hướng tới việc cho phép các mạng phi tập trung phát triển một cách an toàn để đáp ứng nhu cầu toàn cầu. Hydra giúp thực hiện các giao dịch ngoài chuỗi dễ dàng hơn trong khi vẫn sử dụng sổ cái chuỗi chính để thanh toán an toàn.

Hydra nghe có vẻ rất phức tạp và đôi khi bị nhầm lẫn với các giải pháp tương tự. Hãy bắt đầu bằng cách làm rõ "các kênh trạng thái đẳng cấu" là gì. 'Iso' là một tiền tố có nghĩa là bằng nhau, ví dụ, isometric có nghĩa là các phép đo bằng nhau. 'morphic' có nghĩa là liên quan đến hình dạng hoặc hình thức. Vì vậy, đẳng cấu có nghĩa là có cùng cấu trúc và tính chất.

'Các kênh trạng thái' mở rộng khái niệm về các kênh thanh toán để hỗ trợ các hợp đồng thông minh trên các kênh ngoại tuyến. Những người tham gia trong kênh giờ đây, ngoài các khoản thanh toán giao dịch truyền thống, có thể thực thi các tập lệnh để xử lý logic phức tạp, ngoại tuyến, trước khi đưa kết quả trở lại lớp 1 sau đó.

Những người tham gia khóa tiền vào một hợp đồng thông minh. Sau đó, họ có thể giao dịch với những người khác trong kênh trạng thái, ngoại tuyến, theo bất kỳ cách nào đáp ứng trường hợp sử dụng của họ. Sau đó, kết quả được giải quyết trên chuỗi mà không yêu cầu lịch sử giao dịch đầy đủ về những gì đã xảy ra ngoài chuỗi trong thời gian chờ đợi.

⁶⁰⁸

Ren: nền tảng lightwallet, youtube.com/watch?v=Q4Z83TSdEfg

⁶⁰⁹

Phỏng vấn Charles Hoskinson, twitter.com/i/broadcasts/1eaKbNQkpBqKX

⁶¹⁰

Về: Khóa proxy. AMA bắt ngày 21/11/2021, youtu.be/NJcVEJ1a6eg?t=2114

⁶¹¹

Đăng thức: tương ứng hoặc giống nhau về hình thức và quan hệ.

Các nhà phát triển có thể tận dụng cơ sở hạ tầng đã được chứng minh của Cardano để phát triển ví và DApp giao tiếp với hệ thống lớp 2, giảm đáng kể thời gian học tập cho Hydra. Một Hydra Head cũng có thể được hình thành mà không cần bất kỳ khoản tiền ban đầu nào từ bên nhận, đảm bảo trải nghiệm người dùng liền mạch.

giao thức hydrat

Hydra là một giải pháp mở rộng quy mô sổ cái phân tán đáp ứng cả ba thách thức về khả năng mở rộng đã nói ở trên : thông lượng giao dịch cao, độ trễ thấp và dung lượng lưu trữ tối thiểu trên mỗi Node. Mặc dù Hydra đang được phát triển với sự cộng tác của giao thức Ouroboros và sổ cái Cardano, nhưng nó cũng có thể được sử dụng với các hệ thống khác có cùng thuộc tính như Cardano.

Mục tiêu tổng thể của Hydra là cung cấp giải pháp mở rộng quy mô lớp 2 tiên tiến cho Cardano. Hydra sẽ tiết kiệm chi phí trong khi tăng thông lượng và đảm bảo an ninh. Hydra sao chép chức năng của chuỗi chính đồng thời giảm thiểu trở ngại cho người dùng, nhưng vẫn cho phép tính linh hoạt khi có cấu trúc phí khác và các ràng buộc về thời gian trên lớp 2.

Hydra là một hệ thống được tạo thành từ nhiều giao thức con hoạt động cùng nhau để giải quyết một vấn đề duy nhất: khả năng mở rộng. Hệ sinh thái của Cardano rất đa dạng, với nhiều tổ chức có khả năng công nghệ đa dạng: hệ thống cân hỗ trợ Stake Pool, ví nhẹ, DEX và những người dùng cuối khác với nhiều đặc điểm hiệu suất và tính khả dụng của máy tính. Thật vô lý khi mong đợi một phương pháp duy nhất, một kích thước phù hợp với tất cả để cung cấp khả năng mở rộng tổng thể cho một nhóm tác nhân mạng đa dạng như vậy.

Trong một blog đầu tiên, ⁶¹²kiến trúc Hydra được chia thành bốn thành phần: giao thức đầu, giao thức đuôi, giao thức liên lạc giữa đầu và đuôi, cũng như một bộ giao thức hỗ trợ để định tuyến, cấu hình lại và ảo hóa. Mặc dù ban đầu nó được phát triển như một phần của chương trình nghiên cứu Ouroboros, nhưng nó đã đi theo con đường riêng của mình và hiện là một dự án nguồn mở linh hoạt với nhịp phát hành kéo dài hàng tuần.

Đầu thủy lực

Giao thức 'đầu' của Hydra là phần đầu tiên của kiến trúc Hydra được phát hành. Giao thức Head bắt đầu hình thành trong 2020 , đặc biệt là trong giai đoạn triển khai sớm và bằng chứng về khái niệm này⁶¹³ sâu sắc. Sự hiểu biết của IOG đã phát triển kể từ đó và năm 2022 đã chứng kiến việc chính thức hóa và triển khai một biến thể trên giao thức 'Head' trong bài báo gốc.

Hydra đóng vai trò là phần mềm nhúng DApp dành cho các nhà phát triển đang tìm kiếm khả năng mở rộng. Nó được thực hiện trong hai phần:

- Các tập lệnh trên chuỗi thực thi giao thức Hydra Head
- Node Hydra, một ngăn xếp phần mềm cung cấp giao diện cấp cao sử dụng các công nghệ web tiêu chuẩn như WebSocket và JSON.

Để vận hành Hydra Head, một Node Cardano đang hoạt động là điều kiện tiên quyết. Sau đó, bạn chạy một Node Hydra, được kết nối với các Node Hydra khác và một Node Cardano. Mỗi Đầu Hydra có thể bao gồm một số Node Hydra. Nhóm Hydra tuyên bố trong các tài liệu rằng mục tiêu hiện tại của họ là bất cứ thứ gì lên tới 100 Node trên mỗi đầu. Mã trên chuỗi sẽ giống nhau giữa Cardano và đầu hydra. Đây là một trong những điểm bán hàng chính của thiết kế hydra.

Các cấu trúc liên kết tiềm năng của Hydra Head và các trường hợp sử dụng được liệt kê chi tiết trên trang web được đặt tên phù hợp <https://hydra.family>. Cộng đồng được khuyến khích tích cực đưa ra phản hồi về lộ trình.⁶¹⁴

Tương tự 'Trò chơi poker' của Hydra Head

Giao thức Hydra Head được sử dụng tốt nhất khi những người tham gia, quen biết với nhau, đồng ý thành lập một mạng lưới nhưng không tin tưởng lẫn nhau về số tiền. Hydra Head cho phép họ làm như vậy bằng các cách để bảo đảm tài sản của họ, được hỗ trợ bởi khả năng giải quyết tranh chấp ở lớp 1.

⁶¹²

Giáo sư Aggelos Kiayias , ' Enter the Hydra: mở rộng quy mô sổ cái phân tán, cách dựa trên bằng chứng, ' iohk.io/en/blog/posts/2020/03/26/enter-the-hydra-scaling-distributed-ledgers-the-evidence- dựa trên cách /

⁶¹³

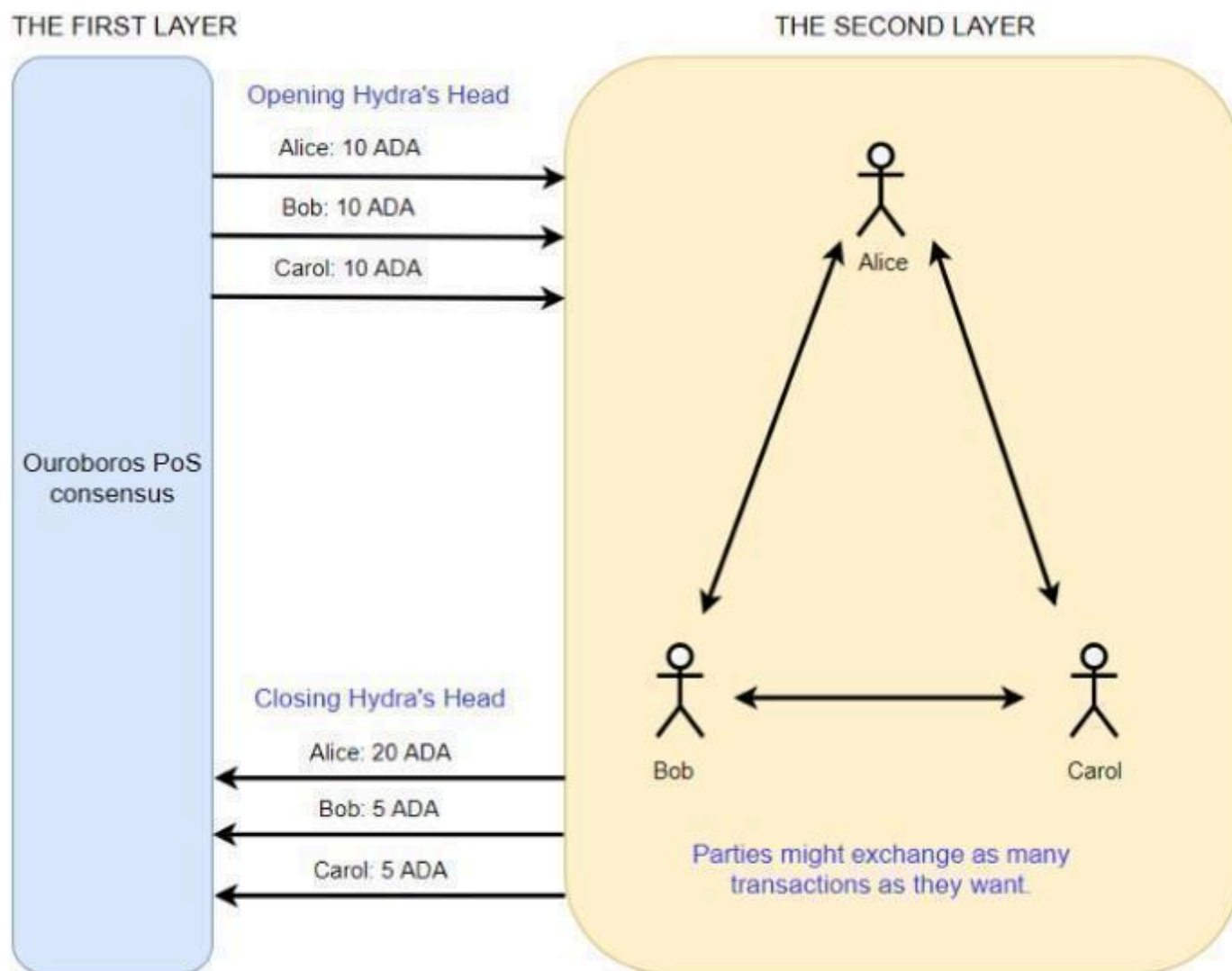
Sebastian N agel, ' Giải pháp của Hydra – Cardano cho khả năng mở rộng Lớp 2 cuối cùng ' , iohk.io/en/blog/posts/2021/09/17/hydra-cardano-s-solution-for-ultimate-scalability/

⁶¹⁴của Hydra Head, github.com/orgs/input-output-hk/projects/21/views/7

Có một số trường hợp sử dụng được giải thích trên trang Hydra, nhưng trò chơi bài xì phé có lẽ là sự tương tự trực quan nhất để giải thích về Hydra Heads. Hãy coi Đầu bài là một 'bàn chơi bài xì phé riêng', nơi người chơi mang theo quân bài của mình để chơi. Trò chơi có thể được chơi bao lâu tùy thích của những người tham gia. Nếu không có ai tham gia, trò chơi sẽ không tiến lên. Tuy nhiên, những người tham gia có thể rời đi với chip của họ. Trò chơi sẽ kết thúc với số tiền hiện có được phân phối nếu họ làm như vậy.

Kênh là một liên kết giao tiếp giữa hai hoặc nhiều đồng nghiệp. Để trở thành một phần của Head, bạn phải là một trong những người ngang hàng. Các kênh thiết lập các mạng biệt lập có thể phát triển độc lập với mạng chính. Những người tham gia trên các mạng thay thế này sử dụng một thuật toán đồng thuận khác, đơn giản hơn: mọi người phải đồng ý về tất cả các giao dịch đi qua. Là một người tham gia, tôi không thể để mất số tiền mà tôi đã không quyết định cụ thể để mất. Tại sao? Bởi vì mọi giao dịch ràng buộc đều cần sự cho phép rõ ràng của tôi.

Những người tham gia có thể thực hiện các cam kết tài chính với Người đứng đầu trong khi tạo ra nó. Điều này đòi hỏi phải chuyển tiền ngoài chuỗi đến một địa chỉ tập lệnh liên kết chúng với một bộ quy tắc. Tập lệnh đảm bảo rằng giao thức được thực thi an toàn trên chuỗi và những người tham gia không thể lừa gạt lẫn nhau. Tuy nhiên, bất kỳ người tham gia nào cũng có thể chọn rời khỏi Đầu bất cứ lúc nào bằng cách đóng nó. Trong tình huống này, mọi người đều nhận được trạng thái gần đây nhất mà họ đã đồng ý ngoại tuyến, trên mạng song song của họ.



Hình 52: Được phép đăng trên phương tiện truyền thông của Cardanians ' Hydra: Giải pháp mở rộng Cardano⁶¹⁵

Người chia bài trên bàn của tập lệnh on-chain đảm bảo rằng mọi người đều tuân theo các quy tắc và không gian lận. Tóm lại, có cùng số lượng chip như trước khi trò chơi bắt đầu, mặc dù chúng có thể đã được sắp xếp lại trong suốt trò chơi. Mặc dù kết quả cuối cùng được biết bên ngoài bàn, nhưng người chơi là những người duy nhất biết lịch sử của tất cả các cuộc được thực hiện trong suốt trò chơi. Tiền, hoặc tiền cược trên bàn hiện có, được mở khóa dựa trên ảnh chụp nhanh được thỏa thuận gần đây nhất.



Payments

- Tipping
- Pay-per-use APIs
- In-app purchases
- E-commerce integrations
- Machine-to-machine
- Royalties
- Prepaid
- Loyalty points



Smart Contracts

- Auctions
- NFT drops
- Voting
- DEX protocols (swaps, OBM)
- Decentralized oracle feeds

Hình 53: Các trường hợp sử dụng Hydra Head, từ ScotFest talk của Giám đốc sản phẩm Hydra, Nebojša Vojvodić

Đánh giá giao thức đầu Hydra

Các Đầu Hydra được biết đến với khả năng đạt được mức độ cuối cùng gần như ngay lập tức bên trong một Đầu. Việc thiết lập và đóng Đầu có thể mất một vài khối. Các mô phỏng đã chỉ ra rằng một đầu Hydra duy nhất có thể đạt tới 1.000 TPS (Giao dịch mỗi giây), vì vậy nếu 1.000 đầu được chạy song song, thì nó sẽ có thể đạt được một triệu TPS. Điều đó thật ấn tượng và nó đưa Cardano vượt xa đối thủ, nhưng nó có thể được đẩy mạnh hơn nữa. Điều gì sẽ xảy ra nếu mỗi nhóm trong số hơn 3.000 Stake Pool hiện tại đều có mặt ngửa? Đó là 3 phút TPS. Hơn nữa, các cải tiến triển khai khác nhau có thể tăng phép đo đầu đơn 1.000 TPS, tăng hiệu suất có thể có của giao thức hơn nữa.

Vì vậy, Hydra có thể gọi bất kỳ số TPS nào mà nó muốn không? Về nguyên tắc, câu trả lời là có, điều này làm nổi bật một lỗ hổng trong việc ⁶¹⁶sử dụng phổ biến TPS như một biện pháp so sánh hệ thống. Mặc dù có thể dễ dàng đơn giản hóa sự phức tạp của việc đánh giá hiệu suất giao thức thành một con số duy nhất, nhưng yêu cầu TPS cao cả gần như vô giá trị nếu không có thêm thông tin.

Rõ ràng, một tiêu chuẩn cao hơn là cần thiết. Giao thức đầu Hydra có phải là giao thức tốt để sử dụng không? Liệu nó có đạt được các giới hạn thực tế của mạng, không chỉ là một con số TPS? Để đảm bảo rằng dữ liệu IOG hiện tại là đáng tin cậy, họ đã áp dụng kỹ thuật sau:

- IOG mô tả rõ ràng tất cả các biến số ảnh hưởng đến quá trình mô phỏng: kích thước giao dịch, thời gian xác minh một giao dịch đơn lẻ, thời gian cần thiết cho các thủ tục mã hóa, băng thông được phân bổ cho mỗi Node, kích thước cụm và phân phối địa lý cũng như các giới hạn song song của giao dịch. Sẽ rất khó để sao chép những con số này nếu không có cài đặt được kiểm soát này
- IOG đã đánh giá hiệu suất của giao thức trên các đường cơ sở xác định giới hạn chính xác và tuyệt đối của cơ sở hạ tầng phần cứng và mạng bên dưới. IOG tiếp cận các ranh giới như vậy hiệu quả như thế nào cho biết có bao nhiêu không gian cho sự tiến bộ.

ngiên cứu giấy⁶¹⁷ (Phần 7: Mô phỏng) có thêm thông tin và đồ họa. Nhóm Hydra thường xuyên đăng kết quả thử nghiệm trên trang web⁶¹⁸ và hoan nghênh nhiều kịch bản thử nghiệm trong thế giới thực hơn. Hydra đang bắt đầu đơm hoa kết trái. Obsidian Systems và IOG đã công bố *Hydra cho các khoản thanh toán*⁶¹⁹, đây là triển vọng thú vị cho các khoản thanh toán vi mô trên Cardano. Tại sự kiện cộng đồng Rare Bloom ở Denver, SundaeSwap đã trình diễn cách giao thức của họ có thể hoạt động như một Hydra Head.⁶²⁰

Làm rõ thủy lực

- Đã có một số cuộc thảo luận quảng bá Hydra là chiến lược khả năng mở rộng Cardano 'cuối cùng' và cuối cùng. Hydra Heads cung cấp cơ sở vững chắc để phát triển lớp khả năng mở rộng của Cardano. Chúng là một phần xây dựng quan trọng cho phép xây dựng các giải pháp phức tạp hơn dựa trên kiến trúc Đầu ra giao dịch chưa chi tiêu mở rộng (eUTXO). Chúng là một phần quan trọng trong hành trình mở rộng quy mô, nhưng chúng không phải là mục tiêu cuối cùng.

Quá trình phát triển của Mithril gắn liền với quá trình phát triển của Hydra, với các đội chồng chéo lên nhau. Một số thành phần của Mithril có thể kết nối và hoạt động tốt với Hydra. Các trang web của họ, mithril.network và hydra.family , có chung định dạng với các hướng dẫn bắt đầu nhanh, bảng chú giải thuật ngữ, v.v. Vì cả hai đều là dự án mã nguồn mở nên bất kỳ ai cũng có thể đóng góp cho các trang này trên GitHub.

- Hydra Head thường là một mạng lưới quy mô tương đối nhỏ được tạo ra bởi một số ít người. Bởi vì ban đầu các nhóm này sẽ độc lập, nên việc nhìn vào tổng số chỉ số riêng biệt của chúng là dễ đánh lừa. Mặc dù lần lặp lại ban đầu của giao thức Hydra Head sẽ cho phép các nhóm nhỏ người tham gia tăng quy mô lưu lượng truy cập của họ với chi phí hợp lý, nhưng nó sẽ không cung cấp giải pháp cho thanh toán giữa người tiêu dùng với người tiêu dùng (vi mô) trên toàn thế giới hoặc bán NFT ngay lập tức.

Tại sao? Bởi vì sự đồng thuận bên trong Head yêu cầu phản hồi của mỗi người tham gia đối với từng giao dịch, nên mọi người cần phải đồng ý về từng giao dịch. Mặc dù điều này đảm bảo an ninh cho những người tham gia Hydra Head, nhưng nó giới hạn tổng số người tham gia trong thực tế. IOG và số lượng ngày càng tăng của những người đóng góp cho dự án, tiếp tục nghiên cứu các cách để mở rộng khả năng của giao thức Hydra Head. Vào năm 2021, có một bài báo được phát hành từ Viện Công nghệ Tokyo với tựa đề *Interhead Hydra: Hai cái đầu tốt hơn một cái* .⁶²¹Nó là một sự lặp lại trên đầu Hydra Head đề xuất một cơ chế liên kết hai Hydra Head với nhau, cho phép hình thành một mạng lưới các Hydra Head được liên kết trong thời gian dài.

- Sẽ có **rủi ro đối với những người không tham gia** vì tiền của bạn nằm trong tay những người tham gia điều hành Hydra Head.
- Giao thức Hydra Head **không phải là Sidechain** . Không có khối nào được tạo trong Hydra Head, cũng như không có bất kỳ lịch sử giao dịch nào bên ngoài Head. Những người tham gia mới không thể tham gia một Head hiện có. Họ cần phải có mặt ngay từ đầu vì Người đứng đầu điều hành là một kênh riêng, biệt lập.

Tương lai của Hydra

Trưởng nhóm của Hydra, Sebastian Nagel, đã trình bày tại Hội nghị thượng đỉnh Cardano năm 2022 ở Lausanne.⁶²²Sau đó, nhóm đã ngồi lại để hoàn thiện chiến lược cho năm tới. Mục tiêu bây giờ là để Hydra trở thành DApp số một trên Cardano, bất kể điều này được đo lường như thế nào.

⁶¹⁷

MMT Chakravarty, S Coretti , M Fitzi , P Gazi, P Kant, A Kiayias và A Russell (2020) 'Hydra: các kênh trạng thái đăng cấu nhanh ' (Phần 7 – Mô phỏng), eprint.iacr.org/2020/299.pdf

⁶¹⁸Điểm chuẩn Hydra Head, hydra.family /head-protocol/benchmarks

⁶¹⁹Hydra cho Thanh toán,
/en/blog/posts/2022/11/10/hydra-for-payments-introducing-developer-tooling-to-unlock-micropayments-on-cardano/

⁶²⁰ Bản demo của SundaeSwap Labs Hydra, twitter.com/ sundaeswap /status/1580969361892085762?lang= vi

⁶²¹

Jourenko , Larangeira , Tanaka Interhead Hydra Hai cái đầu tốt hơn một, eprint.iacr.org/2021/1188

⁶²²Bài nói chuyện của Sebastian Nagel Hydra, Summit.cardano.org/agenda-day-2/cardano-ballot-loa-winner-presentation-6/

Những người quen thuộc với các bản cập nhật dành cho nhà phát triển hàng tuần của Cardano sẽ biết rằng năm 2022 là năm xây dựng chức năng của Hydra Heads và ổn định hiệu suất để những người tiên phong ban đầu có thể thử nghiệm. Năm 2023 sẽ tập trung vào việc áp dụng và khám phá các trường hợp sử dụng mới. Ví dụ: TxPipe đang làm việc trên *Hydra Head như một dịch vụ* thông qua nền tảng của họ Demeter (demeter.run)

Hydra Head dự kiến phát hành V1 vào đầu năm 2023 nhưng chỉ là phần đầu tiên của nhóm giao thức lớn hơn như được mô tả trong Chakravarty và đồng *Hydra: Kênh trạng thái đẳng cấu nhanh* . Khi Hydra trưởng thành và việc áp dụng tăng lên, một số cấu trúc liên kết sẽ được triển khai. Tốt nhất bạn nên kiểm tra hydra.network để biết lộ trình mới nhất. Các kế hoạch hiện tại bao gồm 'Node được ủy quyền', 'Đầu Hydra được quản lý' (còn gọi là Hydra dưới dạng Dịch vụ) và 'Mạng hình sao'.

IOG đã hợp tác với Mlabs (mlabs.city) để sản xuất *Dự án đấu giá triển khai sử dụng giấy Hydra* ⁶²³. Nghiên cứu khám phá nhiều cách khác nhau để thực hiện đấu giá tài sản kỹ thuật số bằng giao thức Hydra Head. Đây là trọng tâm của cách DEX và NFT sẽ hoạt động trên Cardano. Bài báo đề cập đến các nhu cầu và cân nhắc hiện tại của dự án một cách chi tiết. Các cuộc thảo luận đang diễn ra trên Discord và GitHub.

Ngày 21 tháng 9 năm 2022. Re: Hydra: CH⁶²⁴

Khi bạn nhìn vào những thứ như Mithril, Hydra... đây là những phần mở rộng của các khái niệm đã biết, chẳng hạn như Mithril là ý tưởng về chữ ký ngưỡng, và chúng xây dựng các chứng chỉ bằng chứng này, sau đó khi bạn thực hiện giao dịch, chúng được ghép nối với các chứng chỉ bằng chứng, và nó mang lại bạn có trách nhiệm giải trình toàn diện...đó không phải là một ý tưởng mới, nó giống như 10 năm nói về vấn đề này. Chúng tôi chỉ thực hiện nó. Có rất nhiều mật mã khó thực hiện, nhưng một khi đã hoàn thành thì nó đã hoàn thành và vấn đề quan trọng hơn là bạn phân phối chứng chỉ và xây dựng chúng như thế nào?

Hydra là tất cả những gì mà Lightning ⁶²⁵ muốn trở thành khi nó lớn lên. Vấn đề với Lightning là nó không phải là một giao thức cứng... kênh thanh toán và kênh trạng thái. Phần khó khăn là Bitcoin không thể lập trình được. Vì vậy, 95% nỗ lực của bạn là cố gắng tìm ra cách để bạn có được một mô hình, không được thiết kế cho việc này, để hoạt động với điều này.

Nó gần giống như khi họ đang nâng cấp kính viễn vọng Hubble trong không gian, bạn biết đấy, sau khi bạn phóng kính viễn vọng vào không gian, nó không thể nâng cấp được nữa, nhưng NASA lại nói rằng 'chúng tôi cần phải sửa nó' . Vì vậy, họ đã cử các phi hành gia ra ngoài đó, và họ đặt chiếc kính áp tròng khổng lồ này lên đó, và họ phải tìm ra cách mở những thứ mà bạn thực sự chỉ có thể mở trên Trái đất, trong không gian. Vì vậy, bạn có anh chàng này về cơ bản giống như đeo găng tay lò nung, với một chiếc tuốc nơ vít rất nhỏ lơ lửng trong không gian, cố gắng tháo một băng điều khiển và dần dần nâng cấp mạch điện cũ, đồng thời làm cho nó tốt hơn mà không bị giết. Tóm lại, đó là Bitcoin, khi bạn cố gắng áp dụng Lightning. Chà, với Cardano, chúng ta đang ở trên Trái đất, được rồi , điều đó có thể lập trình được nghĩa là chúng ta luôn có thể kéo một mô-đun ra, đặt một mô-đun mới vào và làm những việc này. Vì vậy, với UTXO và Plutus mở rộng, bạn có thể xây dựng các kênh trạng thái đẳng cấu phong phú ở đó. Vì vậy, về cơ bản, bạn có thể lấy trạng thái và tài sản, đồng thời bạn có thể nhóm và gộp chúng lại với nhau, đưa chúng vào giải pháp lớp 2... và sau đó bạn có thể sử dụng nó cho các giao dịch vi mô, bạn có thể sử dụng nó cho các hợp đồng thông minh, nhưng sau đó bạn có thể xây dựng các mô-đun trên nó để thực hiện các ứng dụng cụ thể như DEX, bỏ phiếu... những loại việc này. Đặc biệt, một lĩnh vực mà tôi rất muốn sử dụng Hydra vào năm 2023, đó là tái sử dụng công nghệ đó để thực hiện tất cả những việc chúng tôi đang làm hiện tại với Catalyst và bỏ phiếu.

Ngày 3 tháng 10 năm 2022. Re: Hydra, Hãy nói chuyện với Basho. CH⁶²⁶

Vì vậy, cách chúng tôi thiết kế Plutus là bạn có một thành phần trên chuỗi và đó là tập lệnh Plutus của bạn... và sau đó bạn có ý tưởng về cơ sở hạ tầng ngoài chuỗi phối hợp với DApp để chạy mọi thứ... và điều này rất phổ biến trong Mô hình Ethereum cũng vậy và họ có tất cả những thứ này để kết hợp cả hai, và sau đó cơ sở hạ tầng ngoài chuỗi đôi khi được tập trung, đôi khi không tập trung, nó phụ thuộc vào DApp cụ thể. Ý tưởng về Hydra là nó sẽ là một phần của bộ công cụ ngoài

⁶²³Triển khai các dự án đấu giá bằng Hydra, iohk.io/en/blog/posts/2023/01/20/implementing-auction-projects-using-hydra/

⁶²⁴Phỏng vấn Charles Hoskinson: Các câu hỏi về Cardano của bạn đã được giải đáp, youtu.be/PV_C17noXIA?t=3276

⁶²⁵

Lightning **Network** là một giao thức thanh toán lớp 2 hoạt động trên một Blockchain. Về mặt lý thuyết, nó cho phép giao dịch nhanh giữa các Node tham gia và đã được quảng cáo là giải pháp cho vấn đề về khả năng mở rộng bitcoin.

⁶²⁶Hãy nói về Basho, youtu.be/fhVo-2QUjLM?t=460

chuỗi đó, do đó, nó sẽ được nhúng vào các DApp đòi hỏi nhiều quy mô và về cơ bản, nó sẽ làm điều gì đó tương tự như những gì đang xảy ra với Mithril, nơi bạn truy cập nhiều -một hoặc một số

Sidechains

Sidechain là một Blockchain được liên kết với một Blockchain chính (chuỗi chính hoặc chuỗi mẹ) thông qua cơ chế hai chiều ('cầu nối') cho phép Token và các tài sản kỹ thuật số khác từ một chuỗi được sử dụng trong chuỗi khác và kết quả được chia sẻ qua lại. Nhiều Sidechain có thể tương tác có thể được nối với một chuỗi gốc duy nhất, mỗi chuỗi có thể hoạt động theo một kiểu khác nhau.

Một Sidechain là khái niệm chính xác giống như một Blockchain. Sự khác biệt là triết học, không kỹ thuật. Sidechain thường phù hợp với chuỗi chính, nhưng một Sidechain có thể có logic kinh doanh, Crypto, chính sách tiền tệ, quy tắc đồng thuận, ngôn ngữ lập trình, miền ứng dụng, tập hợp con người dùng, khả năng hợp đồng thông minh, stablecoin, các trường hợp sử dụng như NFT, điểm trung thành của riêng nó, v.v. Sidechain về mặt kỹ thuật giống như một Blockchain độc lập, trong đó các Block được tạo bởi trình xác thực.

Không giống như các kênh trạng thái như Hydra, họ cung cấp dữ liệu sẵn có và sự tham gia cho người dùng mới. Trong kênh trạng thái, thông thường chỉ những người tham gia kênh mới có thể xem những gì đang diễn ra trong kênh và họ phải được quyết định trước. Tham gia một Sidechain thường được thực hiện bằng cách đốt hoặc khóa tài sản trên chuỗi chính, để đổi lấy một số tiền tương đương trên Sidechain.

eUTXO của Cardano có nghĩa là trạng thái được phân đoạn sẵn trên chuỗi chính, do đó, việc chuyển trạng thái sang Sidechain sẽ dễ dàng hơn. Sidechains lý tưởng cho các giao thức có rủi ro từ trung bình đến thấp. Chúng lý tưởng cho các hệ sinh thái mới hoặc đang phát triển vì Sidechain có thể tận dụng tính bảo mật, tính thanh khoản, ví và sự tham gia của người dùng của một chuỗi chính đã được thiết lập. Sidechains giảm tải cho mạng chính lớp 1, đồng thời tận hưởng tính xác thực được cung cấp bởi chuỗi mẹ của nó.

Mặc dù sẽ có khối lượng giao dịch lớn chạy song song trên các Sidechain, nhưng các giao dịch này không đối chiếu trên chuỗi chính, vì vậy các tài nguyên trên chuỗi chính Lớp 1 không bị các Sidechain sử dụng.

Rất nhiều suy nghĩ sâu sắc và sự nghiêm túc trong học thuật đã được đưa vào cấu trúc của Cardano. Rõ ràng là phần thưởng khuyến khích quan hệ đối tác Sidechain như thế nào. Những người nắm giữ ADA theo truyền thống sẽ nhận được phần thưởng đặt cược trong ADA. Các SPO tương tự cung cấp năng lượng cho chuỗi chính, cũng sẽ cung cấp tính thanh khoản đặt cọc cho các Sidechain. Vì vậy, bây giờ, nếu SPO mà bạn ủy quyền cũng là một phần của tập hợp con SPO Sidechain, thì bạn sẽ nhận được phần thưởng trong tài sản gốc của Sidechain đó ngoài phần thưởng ADA thông thường của bạn.

Re: Sidechains, Hãy nói về Basho. CH:

Về cơ bản nó giống như siêu Hydra. Hydra dành riêng cho DApp, Sidechains dành riêng cho hệ sinh thái

Thường có sự đánh đổi để chạy một Sidechain. Thông lượng tăng có thể có nghĩa là bảo mật ít hơn. Bảo mật cầu nối là một thách thức trong thực tế và đã có nhiều vụ hack vào năm 2022.⁶²⁷Tuy nhiên, Cardano cung cấp một chuỗi chính lớp 1 rất an toàn. Tiền trong hợp đồng bắc cầu được bảo vệ tốt và tài sản được chuyển giao an toàn giữa các Sidechains dựa trên định nghĩa chính thức được nêu trong bài viết về *Proof-of-Stake Sidechains năm 2019 của IOG*.⁶²⁸

Nghiên cứu mô tả cách thuộc tính bảo mật 'tường lửa' mới bảo vệ một chuỗi chính khỏi các Sidechain của nó. Các lỗi tiềm ẩn trên Sidechain sẽ không ảnh hưởng đến chuỗi gốc. Ví dụ, Project Catalyst được vận hành như một Sidechain của Cardano. Ngay cả khi sự an toàn của nó bị xâm phạm, thì không có khoản tiền nào bị mất trên Cardano. Bài báo cũng phác thảo một kế hoạch chi tiết mô tả việc đặt cược hợp nhất, chứng nhận chuỗi chéo và đa chữ ký cho các Sidechain bằng chứng cổ phần.

Dựa trên nghiên cứu này, IOG đã phát triển Sidechain Cardano EVM (Ethereum Virtual Machine), Mamba, theo một cách tiếp cận có chủ ý và lặp đi lặp lại. Nó là một giao thức Sidechain mã nguồn mở với một ứng dụng khách được viết bằng Scala. Mamba tương thích với các công cụ và thư viện của Ethereum cho phép các nhà phát triển viết hợp đồng thông minh Solidity, DApps và Token ERC20 trên Cardano. Hợp đồng thông minh Ethereum có thể chạy không thay đổi trên Mamba, với phí *gas thấp hơn nhiều*.

⁶²⁷Tin tức đã đánh cắp 1,4 tỷ đô la trong năm nay bằng cách sử dụng cầu nối Crypto, cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html

⁶²⁸Gazi, Kiayias, Zindors (2019), 'Các Sidechain bằng chứng cổ phần', iohk.io/en/research/library/papers/proof-of-stake-Sidechains/

Giao thức đồng thuận được sử dụng trên Mamba là Ouroboros BFT. Đây là phiên bản trước đó của Ouroboros được sử dụng trên mạng chính Cardano. Nó là một giao thức đơn giản, mang tính quyết định cho sự đồng thuận của số cái có thể chấp nhận các lỗi của Byzantine.⁶²⁹Có nhiều phiên bản khác nhau của bằng chứng cổ phần (PoS), phù hợp với các trường hợp sử dụng khác nhau trên chuỗi phụ và chuỗi chính. Sebastien Guillemot đã phân tích xuất sắc về sự đánh đổi trong video của anh ấy *Cardano & Algorand : Giải thích về lựa chọn nhà lãnh đạo*.

Trong một ⁶³⁰tập Carano360, Kathryn Stacy, Giám đốc sản phẩm của Sidechains, đã giải thích cách IOG lên kế hoạch cho phép nhiều khả năng lập trình hơn bằng cách giúp các nhà phát triển dễ dàng đóng góp. IOG đang cấp quyền truy cập vào mã nguồn EVM để các nhà phát triển có thể sử dụng mã này làm khung để tạo Sidechain EVM của riêng họ. Tầm nhìn là tạo ra một 'hệ sinh thái của các hệ sinh thái'.

Sidechains Toolkit components

Main chain scripts

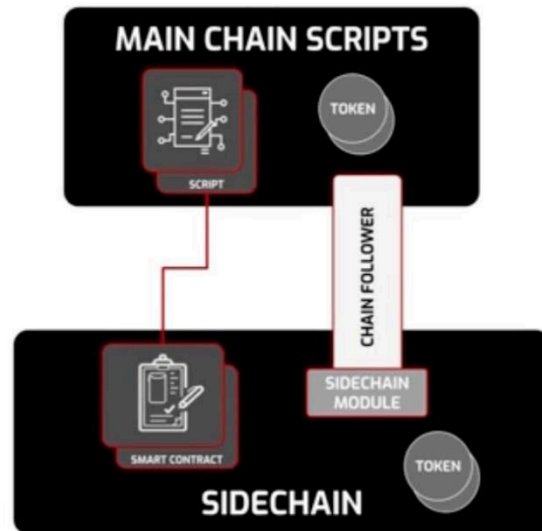
- Allow main chain expansion without modifications to Cardano
- Enable secure cross-chain transactions

Chain follower

- Tracks data on main chain

Sidechain module

- Interprets main chain data and implements the necessary ledger adaptations



Hình 54: slide từ bài nói chuyện của Dominik Zajkowski tại ScotFest

Dominik Zajkowski, Kiến trúc sư kỹ thuật của IOG, đã mở rộng tầm nhìn này tại ScotFest. Anh ấy giải thích rằng các tập lệnh Plutus để duy trì Sidechain EVM Mamba sẽ được cung cấp dưới dạng bộ công cụ được sử dụng làm mẫu tham chiếu, một loại SDK cho các Sidechain trong tương lai với Cardano là nền tảng cốt lõi của sự tin cậy. Zajkowski giải thích rằng bộ công cụ này chưa hoàn thiện một cách có chủ ý và mời cộng đồng phản hồi về các tính năng mà họ muốn xem. Tất cả những lĩnh vực này sẽ được làm việc với cộng đồng khi chúng tôi đi. Tài liệu ⁶³¹hiện đang hoạt động và bao gồm thông số kỹ thuật.

Khi các trường hợp sử dụng được mở rộng phạm vi và các trình giữ chỗ đã được lấp đầy, có lẽ một Sidechain hấp dẫn hàng đầu có thể bắt đầu hoạt động và đó là lúc *Midnight* xuất hiện...

Nửa đêm trong Khu vườn Thiện và Ác

Tại ScotFest, Charles Hoskinson tiết lộ nhóm của ông đã nghiên cứu một loại Crypto khác trong bốn năm qua. Nó được gọi là *Midnight* và sẽ là một Sidechain Cardano với Token gốc có tên là *bụi*. Như đã đề cập trước đây, cách thức hoạt động của Sidechains trên Cardano là quan hệ đối tác. Midnight nhận được sự phân cấp, bảo mật, cơ sở hạ tầng, tính thanh khoản và một hệ sinh thái thịnh vượng từ Cardano. Đổi lại, Midnight trả tiền thuê dưới dạng phần thưởng *bụi* cho các SPO và người được ủy quyền.

⁶²⁹Lỗi Byzantine là bất kỳ lỗi nào biểu hiện các triệu chứng khác nhau đối với những người quan sát khác nhau. Lỗi Byzantine là mất dịch vụ hệ thống do lỗi Byzantine trong các hệ thống yêu cầu sự đồng thuận giữa các Node phân tán.

⁶³⁰

Tháng 6 năm 2022 Clip Sidechains Cardano360, youtube.be/ShBFTaD8nss?t=381

⁶³¹Tài liệu SDK Sidechain, docs.cardano.org/cardano-Sidechains/Sidechain-toolkit/introduction

IOG đã xem xét các giải pháp bảo mật hiện có như Monero và Zcash và cảm thấy họ có thể làm tốt hơn. Nghiên cứu về các yêu cầu bảo mật đối với hợp đồng thông minh đã được tiến hành trong một thời gian. *Kachina-Foundations of Private Smart Contracts* ⁶³² là một bài báo được Charles Hoskinson xếp hạng là "một trong những ấn phẩm có tư duy tiên bộ nhất của chúng tôi". ⁶³³

Lực đẩy bộ não của IOG (giống như chuyên gia kiến thức bằng không, Tiến sĩ Markulf Kohlweiss) đã làm việc và xem xét các giải pháp khác như Zexe ⁶³⁴ và kết luận rằng ba thuộc tính 'phải có' không có trong không gian Blockchain ngày nay. Được viết tắt là 'ACE', chúng là: tự do của Hiệp hội A, tự do thương mại C và tự do biểu diễn E.

Những quyền cơ bản này của con người không phải lúc nào cũng có ở một số khu vực pháp lý vì nhiều lý do. Midnight sẽ cung cấp tính bảo mật và quyền riêng tư với khả năng tự do liên kết với mọi người và tham gia vào các giao dịch thương mại hợp pháp.

Ngoài ra còn có phía quy định. Tìm kiếm sự bảo mật và quyền riêng tư trong hầu hết các trường hợp không phải là bất hợp pháp. Vì nhiều người tin rằng Crypto được che giấu bí mật và chỉ được sử dụng cho hoạt động bất chính, các DApp mới cần bảo vệ quyền và mong muốn của người dùng, nhưng cũng cho phép họ tuân thủ các yêu cầu quy định. DApps trên Midnight cho phép người dùng bảo vệ dữ liệu của chính họ, để giữ dữ liệu của họ trong hệ thống của riêng họ. Họ không phải chia sẻ mọi thứ nhưng có thể chia sẻ các xác nhận về dữ liệu cá nhân của họ dựa trên những thứ như KYC và AML và cơ quan ở phía bên kia của giao dịch có thể tin tưởng rằng những xác nhận đó là chính xác. Tiết lộ có chọn lọc không giống như 'cửa sau', tin tức giả mạo ⁶³⁵ và FUD đã bị chỉ ra và sửa chữa về vấn đề này.

Midnight vượt xa các giao dịch riêng tư và cố gắng hỗ trợ bảo mật thực sự với các hợp đồng thông minh riêng tư. Để thực hiện khái niệm giữ một cái gì đó riêng tư cho công chúng, nhưng vẫn cho phép tiết lộ tự nguyện hoặc không tự nguyện. Một trường hợp sử dụng rõ ràng cho điều này là quy định. Nếu bạn chuyển đến một khu phố độc quyền hoặc nâng cấp ô tô của mình lên một chiếc Ferrari, bạn bè của bạn sẽ không thể tra cứu số dư ngân hàng của bạn. Tuy nhiên, ngân hàng của bạn có nghĩa vụ hỏi bạn đã lấy tiền từ đâu khi bạn vượt quá một giới hạn nhất định tùy thuộc vào khu vực tài phán.

Làm thế nào điều này sẽ đạt được? Atala Prism sẽ được tích hợp chặt chẽ với Midnight, liên kết danh tính và quyền riêng tư. Vì ren *nhẹ* sẽ cung cấp khả năng truy cập dễ dàng vào các tính năng sáng tạo như *công tắc người chết* ⁶³⁶ để lập kế hoạch bất động sản và các tính năng tính toán đa bên ⁶³⁷. Monero và Zcash là những giải pháp đã được chứng minh để giữ các giao dịch và Token của bạn ở chế độ riêng tư, nhưng cũng cần có khả năng lập trình. Bài báo Kachina khám phá cách viết các hợp đồng thông minh riêng tư và IOG đã bạn rộn đưa lý thuyết này vào cuộc sống.

⁶³²

Kerber, Kiayias, Kohlweiss (2021) 'Kachina - Nền tảng của Hợp đồng Thông minh Riêng tư', eprint.iacr.org/2020/543.pdf

⁶³³

Charles Hoskinson Kachina tweet, [twitter.com/iohk_charles / status/1261328840023961602?lang= vi](https://twitter.com/iohk_charles/status/1261328840023961602?lang=vi)

⁶³⁴

Zexe: Kích hoạt tính toán riêng phi tập trung, eprint.iacr.org/2018/962.pdf

⁶³⁵

Cardano Midnight: Monero rút lại các tuyên bố tiêu cực, [u.today / cardano -midnight- monero -retracts-negative-statements](https://u.today/cardano-midnight-monero-retracts-negative-statements)

⁶³⁶

Công tắc của người chết là công tắc được thiết kế để kích hoạt hoặc hủy kích hoạt nếu người vận hành là người mất khả năng lao động hoặc chết. Thông thường, tiền có thể được gửi đến một địa chỉ đặt trước sau khi hết thời gian đã đặt.

⁶³⁷ MPC (tính toán nhiều bên) cho phép nhiều bên – mỗi bên nắm giữ dữ liệu riêng tư của mình – đánh giá một phép tính mà không bao giờ tiết lộ bất kỳ dữ liệu riêng tư nào do mỗi bên nắm giữ.



Hình 55: Tại sao *Midnight* nổi bật, từ Giám đốc chiến lược của IOG, Rob ADAMs nói chuyện tại ScotFest

Sau nhiều năm nghiên cứu và phát triển, họ đã tạo ra một máy ảo trong Typescript. Điều này rất có ý nghĩa về mặt chấp nhận của nhà phát triển. Typescript (~35%), một siêu bộ JavaScript (65%), là một trong những ngôn ngữ lập trình phổ biến nhất trên thế giới.⁶³⁸ Đối với quan điểm, việc áp dụng Haskell suy yếu ở đâu đó trong khoảng (1-2%). IOG đang áp dụng cách tiếp cận ưu tiên nhà phát triển với Midnight, trái ngược với Plutus, ra mắt vài năm sau khi Cardano ra mắt.

Với quy định về ngưỡng cửa của ngành, Midnight có vẻ như là một bước đi chiến lược sắc sảo của IOG. Các cơ quan quản lý có một nhiệm vụ khó khăn là cố gắng lập pháp cho một ngành công nghiệp non trẻ với công nghệ mới nổi đôi khi chưa được sản xuất. Midnight cung cấp một nền tảng trung gian tiềm năng, nơi các nguyên tắc cốt lõi của Crypto có thể được duy trì, nhưng cũng cho phép DApps đáp ứng các yêu cầu tuân thủ ở các địa phương khác nhau.

Chỉ một ví dụ là khi một doanh nghiệp lớn trên toàn cầu cần tuân thủ các yêu cầu GDPR ở Châu Âu, nhưng vẫn có một phiên bản khác của Hoa Kỳ để tuân thủ các yêu cầu trong Đạo luật Bảo mật Ngân hàng. Hầu hết các công ty phải đối mặt với các hình phạt lớn nếu họ không giữ dữ liệu người dùng ở chế độ riêng tư. Có nhiều trường hợp sử dụng rõ ràng khác từ việc làm cho dữ liệu y tế có thể truy cập được, cho đến việc cho phép các tờ báo ngâm trong các xã hội đầy biến động hoạt động.

Charles Hoskinson đã đề cập trong đêm giao thừa trên twitter không gian của anh ấy,⁶³⁹ các Sidechains không gian sẽ được triển khai dựa trên khái niệm võ thuật *Shuhari của Nhật Bản* ... bạn học, bạn làm, sau đó bạn dạy. IOG đã 'học' với bằng chứng khái niệm Mamba, bây giờ họ sẽ 'làm' với Midnight và 'dạy' bằng nhiều bộ công cụ, blog và bài báo chính thức.

Điều gì sẽ xảy ra là bạn lấy một tập hợp con của các nhà khai thác Stake Pool, những người hiện đang vận hành Cardano, họ báo hiệu rằng họ muốn tạo các Block trong chuỗi mới này và sau đó về cơ bản bạn có một thuật toán lựa chọn để đưa chúng vào giao thức BFT và sau đó họ tạo thành đại biểu đó cho một kỳ nguyên. Giờ đây, lợi thế của giao thức đó, với kiểu cấu trúc đó là bạn có được giao thức BFT, tốc độ cao được tối ưu hóa rất cao này và việc lấy mẫu đại biểu của bạn được thực hiện từ chuỗi chính... và do đó, bạn có thể khôi phục bảo mật về mức độ tham gia, và tập hợp các SPO mà bạn có... và cách thức hoạt động của nó nói chung, sẽ được viết ra trong một bài báo nghiên cứu, giống như chúng ta viết tất cả những thứ khác nhau này. Đó sẽ là một mô hình chia khóa trao tay và sau đó mục tiêu là triển khai thuật toán đó trên Cosmos và có lẽ ScoreX và (Hyperledger) Fabric sẽ là ba thứ mà tôi muốn thấy nó được triển khai thông qua. Vì vậy, Vài 3, ScoreX và Cosmos.

⁶³⁸Các ngôn ngữ lập trình hàng đầu, statista.com/statistics/793628/worldwide-developer-survey-most-used-languages/

⁶³⁹

đêm giao thừa với Charles, twitter.com/IOHK_Charles/status/1609417098396323840?t=42JFCPU8bk_mbwlix8wG1w&s=19

Sau đó, bạn có các bộ công cụ xây dựng Sidechain này. Fabric sẽ là một bộ, Cosmos và ScoreX sẽ là một bộ... và đó mới là sơ khai, và tất cả cơ sở hạ tầng đã có sẵn, vì vậy bạn chỉ cần tham số hóa logic mạng, quy tắc sổ cái và logic giao dịch trong hệ thống... nhưng bạn sẽ Tôi không phải lo lắng quá nhiều về việc làm cách nào để tạo một Sidechain? Làm cách nào để tôi nhận được các giao dịch di chuyển qua lại? ...và làm cách nào để nó hoạt động với ví?.. và tất cả những thứ khác...nó gần giống như khởi chạy ERC20.

Nếu bạn đã đọc "Tại sao lại là Cardano?" năm 2016 giấy, những gì được mô tả ở trên nghe có vẻ quen thuộc. Đề xuất ban đầu là dành cho CSL (Lớp thanh toán Cardano) và CCL (Lớp tính toán Cardano). Tầm nhìn này đã thể hiện hơi khác một chút trong mô hình Sidechains. Khung đa tính toán này được thiết kế để đáp ứng nhiều yêu cầu từ các chuỗi đối tác. Vì vậy, trên thực tế, sẽ có nhiều CCL... Midnight và có khả năng là World Mobile, Hyperledger Fabric và Cosmos là những ứng cử viên ban đầu để tạo thành một thư viện gồm các mẫu khác nhau có sẵn để đặt các Sidechain khác nhau vào vị trí.

Truy cập vào *nửa đêm.iohk.io* để đăng ký để biết thêm thông tin

Milkomeda

Không phải ai cũng say mê với kiến trúc hiện tại của Cardano. CTO và đồng sáng lập của dcSpark, Sebastien Guillemot, đã đặt câu hỏi về ⁶⁴⁰cấu trúc nguyên khối của Cardano và tại sao nó lại đi chệch khỏi tầm nhìn ban đầu trong "Tại sao lại là Cardano?". Đã làm việc trên giao thức kể từ những ngày testnet được khuyến khích, quan điểm của anh ấy nên được coi trọng. Phải nói rằng, có sự đánh đổi trong bất kỳ quyết định Blockchain nào.

Cardano là một hệ sinh thái mở và mọi người có thể tự do khởi chạy các Sidechain bằng các mô hình khác nhau. Sidechain Cardano đầu tiên đã được ra mắt dcSpark. *Milkomeda* mang đến khả năng tương thích EVM và là cầu nối cho các nhà phát triển với hệ sinh thái Ethereum. Milkomeda là một từ ghép, được đặt tên theo các thiên hà *Milky Way* và *Andromeda* sẽ hợp nhất trong vài tỷ năm nữa. Milkomeda cũng mang lại khả năng tương thích EVM cho Algorand, hợp nhất nhiều hệ sinh thái. Điều thú vị là Milkomeda hiện được triển khai khác nhau trên cả hai Blockchain. Nó là một Sidechain Cardano với số lượng DApp ngày càng tăng, ⁶⁴¹nhưng là giải pháp Lớp 2 trên Algorand.

Guillemot đã giải thích sự khác biệt và lý do tại sự kiện Rare Bloom. ⁶⁴²Như đã thảo luận trước đây, Sidechain là một Blockchain phù hợp về mặt kỹ thuật với chuỗi gốc nhưng khác về mặt triết học ở các tính năng chính. Ví dụ: Milkomeda C1 là Sidechain Cardano nơi họ chọn giữ cùng một tài sản cơ sở (ADA) nhưng có thời gian tạo Block nhanh hơn (4 giây) với tính hữu hạn tức thời. Không thể triển khai Milkomeda dưới dạng giải pháp Lớp 2 trên Cardano vào thời điểm này do một số trở ngại kỹ thuật, vấn đề này có thể sẽ được giải quyết khi các tính năng như Mithril hoàn thiện.

Với sự tài trợ từ Catalyst,⁶⁴³ dcSpark sẽ sớm thêm các hợp đồng thông minh được bao bọc để mở rộng khả năng tương tác hơn nữa. Các nhà phát triển sẽ sớm có thể gọi các hợp đồng thông minh EVM từ mạng chính Cardano. UX sẽ mượt mà, với người dùng cuối không biết rằng họ đang sử dụng EVM bên dưới. Các hợp đồng thông minh được bao bọc cũng cho phép Oracles được bao bọc cung cấp dữ liệu ngoài chuỗi. Tính năng này sẽ tích hợp quyền truy cập vào các Oracles dựa trên EVM hiện có vào mạng chính Cardano.

Milkomeda A1 là Lớp 2 trên Algorand. Mặc dù Sidechain mang lại cho bạn tính linh hoạt cao hơn nhưng bảo mật kém hơn, Lớp 2 cung cấp cho bạn bảo mật đầy đủ với các bằng chứng toán học, nhưng kém linh hoạt hơn khi bạn cần lập trình mọi thứ trong các mạch không kiến thức (ZK).

Giải pháp mở rộng lớp 2 là gì?

Đây thường là 3 loại giải pháp Lớp 2.

- Kênh trạng thái (như Hydra hoặc Lightning Network trên bitcoin)
- Tổng hợp ZK

⁶⁴⁰

Cardano: vấn đề & sách trắng để khắc phục, [youtube.com/watch?v=LIEM6qbc-x8](https://www.youtube.com/watch?v=LIEM6qbc-x8)

⁶⁴¹Milkomeda dApps, milkomeda.com/dapp-store

⁶⁴²

Bản cập nhật Sebastien Guillemot Milkomeda, [youtube.com/watch?v=LlxTmDPw_cs](https://www.youtube.com/watch?v=LlxTmDPw_cs)

⁶⁴³

Milkomeda Oracle, cardano.ideascale.com/c/idea/369192

- Tổng hợp lạc quan

Cả ZK và các bản tổng hợp lạc quan đều thu thập các giao dịch ngoài chuỗi thành một đợt, sau đó gửi chúng tới Blockchain Lớp 1 dưới dạng một giao dịch.

Bản **tổng hợp Không có kiến thức (ZK)** được xây dựng dựa trên Blockchain Lớp 1 hiện có để thực hiện các giao dịch nhanh hơn, rẻ hơn, có thể mở rộng, an toàn và riêng tư bằng cách không tiết lộ mọi thứ trong khi giao dịch với người xác minh. Vấn đề với nhiều giải pháp Lớp 2 khác là chúng không đủ an toàn. Có một sự đánh đổi khi họ tập trung nhiều hơn vào khả năng mở rộng, điều này có thể khiến họ bị khai thác. Bản tổng hợp ZK rất mạnh mẽ vì việc chứng minh bạn biết câu trả lời sẽ nhanh hơn nhiều so với việc tính toán để có câu trả lời.

Tổng số lạc quan kém an toàn hơn so với Tổng số ZK nhưng cung cấp tính linh hoạt cao hơn vì chúng không yêu cầu mọi thứ phải được mã hóa trong mạch ZK. Trái ngược với các bản tổng hợp ZK trong đó bạn chứng minh mọi thứ đều đúng, bạn chỉ đang chứng minh sự không trung thực (có bằng chứng Gian lận) theo yêu cầu. Như tên gợi ý, bạn cho rằng giao dịch là hợp lệ hoặc sử dụng bằng chứng gian lận để chứng minh giao dịch sai trong vòng 7 ngày.

Các bản tổng hợp ZK có khả năng mở rộng hơn vì chúng tiêu thụ ít tài nguyên Blockchain hơn so với các bản tổng hợp Lạc quan. Các bản tổng hợp ZK ngày nay rất khó triển khai, chủ yếu là do chúng mất thời gian để biên dịch và có thể làm chậm DApp của bạn. Tuy nhiên, điều này đang được cải thiện hàng năm và đó là không gian nghiên cứu hấp dẫn.

Ethereum tập trung rất nhiều vào ZK roll-up với nhiều dự án đang cố gắng thống trị. @StakeWithPride⁶⁴⁴ đã chỉ ra một số nguyên tắc cơ bản và giá trị thiết kế đáng ngờ đến từ cộng đồng Ethereum. Trong một video từ một nhà phát triển cốt lõi, có một sự thừa nhận rằng có khả năng xảy ra một vụ hack nghiêm trọng với các đợt triển khai ZK trên Ethereum. Giải pháp được đề xuất là tận dụng các vỏ bọc đáng tin cậy của Intel SGX⁶⁴⁵ để đảm bảo an ninh.

Trên Cardano, đã có dự án Orbis ZK không thành công do Catalyst tài trợ.⁶⁴⁶ Tiến sĩ Markulf Kohlweiss đã công bố Phòng thí nghiệm ZK tại Đại học Edinburgh và deSpark đã ưu tiên nghiên cứu ZK vào năm 2023.

Ngày 20 tháng 4 năm 2022, 'Hangout 20/4 với không gian Twitter của Charles',⁶⁴⁷

Re: Giải pháp chia tỷ lệ L2, cuộn ZK... CH:

Tại sao chúng ta quan tâm đến công nghệ này? Tại sao điều này hữu ích cho tôi với tư cách là người tiêu dùng? Được rồi, giả sử bạn đến một quán bar và bị phạt thẻ. Khi bạn xuất trình bằng lái xe của mình cho nhân viên pha chế, bạn không chỉ tiết lộ tuổi của mình. Bạn tiết lộ tuổi chính xác của bạn. Thông thường, giấy phép lái xe có địa chỉ trên đó. Cho dù bạn có phải là người hiến tặng nội tạng hay không, một bức ảnh của bạn, giới tính của bạn, bạn sẽ tiết lộ một số điều trong số đó... Tôi nghĩ họ đã ghi số An sinh xã hội trên bằng lái xe, thẻ quân nhân, và hơn thế nữa, trên hộ chiếu. Bạn nhận được tất cả những thứ mà nhân viên pha chế không nên biết.

Nhân viên pha chế đang tìm kiếm một điều kiện ngưỡng. Bạn đang ở trên hay dưới độ tuổi uống rượu? Đó là tất cả những gì họ cần, đó là một Boolean có hoặc không. Bạn trên 21 tuổi?... bằng hoặc hơn 21 tuổi? Vì vậy, điều mà bằng chứng không có kiến thức có thể làm là, đối với một hệ thống nhận dạng có ID kỹ thuật số, bạn có thể chứng minh với nhân viên pha chế rằng bạn đã trên 21 tuổi nhưng không tiết lộ gì khác về bạn. Không có siêu dữ liệu nào khác và một bản tóm tắt mà bạn có thể làm điều đó cho bất kỳ giao thức phản hồi thách thức nào. Bạn có phải là công dân Hoa Kỳ hay không? Số tiền mà tôi nhận được có bị đánh thuế hay không? Bạn có hoàn toàn tuân thủ luật pháp ở bang Colorado không? hay không? Có hay không. Những loại điều này. Bạn có đủ điều kiện để xem thông tin này? Có hay không. Bạn loại bỏ phản xét đó về mặt đó.

Bây giờ ứng dụng còn lại là bạn có sở hữu số tiền này hay không? Bằng chứng kiến thức bằng không là hoàn hảo cho ứng dụng này, bởi vì về cơ bản, bạn đang chứng minh rằng số tiền tồn tại và bạn có quyền chi tiêu nó, nhưng bạn không tiết lộ số tiền đó là gì và bạn không tiết lộ bạn là ai. Vì vậy, đó là lý do tại sao chúng được sử dụng trong các hệ thống bảo mật.

⁶⁴⁴

StakeWithPride lại: Tổng hợp Ethereum zk , [twitter.com/StakeWithPride /status/1607511445549514752](https://twitter.com/StakeWithPride/status/1607511445549514752)

⁶⁴⁵Ý tưởng cốt lõi của SGX là tạo ra một 'vùng chứa' phần mềm. Enclave về cơ bản là một khu vực riêng biệt và được mã hóa cho mã và dữ liệu.

⁶⁴⁶

Quỹ đạo: Tổng hợp ZK lớp 2 <https://cardano.ideascale.com/c/idea/396617>

⁶⁴⁷

20 tháng 4 năm 2022, ' 4/20 Hangout với Charles ' Không gian Twitter, [twitter.com/ i /spaces/11DGLLABeBkGm](https://twitter.com/i/spaces/11DGLLABeBkGm)

Các giải pháp tương tác khác

Ngày càng có nhiều nhà xây dựng trên Cardano. Ví dụ: Wanchain ⁶⁴⁸ là một cầu nối xuyên chuỗi phi tập trung, phi giám sát hai chiều liên kết Cardano với các Blockchain cấp 1 khác. Ngoài việc là một giải pháp tương tác phi tập trung, Wanchain còn là Blockchain bằng chứng cổ phần (PoS) lớp 1 với hệ sinh thái giống Ethereum hỗ trợ các công cụ, DApp và giao thức Ethereum tiêu chuẩn ngành. Nó có những điểm tương đồng nhất định với Cardano. Wanchain sử dụng phương pháp đồng thuận Galaxy Consensus PoS, sử dụng một số phương pháp mã hóa, chẳng hạn như chia sẻ bí mật phân tán và chữ ký ngưỡng, để tăng cường quá trình tạo sổ và tạo Block ngẫu nhiên. Galaxy Consensus là sự tiếp nối của giao thức Ouroboros của chính Cardano.

Để hiểu thêm, hãy xem *Rollup trên Cardano Discussion*. ⁶⁴⁹IOG đã đóng góp cho không gian này với bài viết của họ về Sonic: Zero Knowledge SNARKS. ⁶⁵⁰

Người ủng hộ đầu vào

Bằng cách tách các giao dịch thành các Block được xây dựng trước, những người xác nhận đầu vào sẽ tăng tốc độ lan truyền khối và thông lượng (lượng dữ liệu được truyền). Điều này làm tăng tính nhất quán lan truyền khối và cho phép tăng tỷ lệ giao dịch.

Những người ủng hộ đầu vào đã được John Woods (trước đây là IOG, hiện là CTO của Algorand) mô tả là một "giải pháp trò chơi gắn kết thúc" cho quy mô Lớp 1 sẽ đưa Cardano lên hàng đầu khi nói đến thông lượng cho Lớp 1.

Quy trình hiện tại là lấy các giao dịch ra khỏi mempool, giả mạo một khối, sau đó gửi nó cho các đồng nghiệp. Với những người xác nhận đầu vào, các Block sẽ được tạo trên cơ sở đặc biệt, được ký và phân ký, và sẽ bay quanh mạng trên cơ sở gần như từng giây.

Mạng hiện có Ouroboros Praos, nơi một khối được tạo cứ sau 20 giây, đang đáp ứng đầy đủ nhu cầu của người dùng. Tuy nhiên, những Người ủng hộ đầu vào sẽ giúp Cardano vượt lên dẫn trước các nhu cầu đang diễn ra với ngày càng nhiều doanh nghiệp triển khai trên Cardano, khi Plutus và Marlowe trưởng thành.

Hiện tại, các Block chịu trách nhiệm cho cả sự đồng thuận và nắm giữ dữ liệu giao dịch. Người xác nhận đầu vào chia mỗi khối thành hai. Một trong các Block chịu trách nhiệm về sự đồng thuận, khối còn lại nhanh hơn được chỉ định để lưu trữ dữ liệu giao dịch.

Khối đồng thuận về cơ bản sẽ được giải phóng khỏi nhiệm vụ quản lý dữ liệu giao dịch. Bây giờ nó sẽ có một con trỏ (sử dụng 'ngữ nghĩa tham chiếu') tới khối chứa dữ liệu giao dịch. Điều này sẽ giảm tắc nghẽn và thời gian chờ 20 giây, cho phép các Block được truyền phát liên tục.

Người xác nhận đầu vào đã bị tắt tiếng kể từ bài báo gốc của Ouroboros vào năm 2016. Tương tự như nhà sản xuất Block (BP), người xác nhận đầu vào (IE) được mô tả là một thực thể bên liên quan, theo nghĩa là số lượng cổ phần được ủy quyền cho họ ảnh hưởng đến khả năng của họ trong việc chức năng.

Theo Mục 8.1 của bài báo:

Người xác nhận đầu vào tạo lớp xác nhận giao dịch thứ hai trước khi đưa vào khối. [...] Lưu ý rằng người xác nhận đầu vào được gán cho các vị trí giống như cách của người dẫn đầu vị trí và đầu vào được bao gồm trong các Block chỉ được chấp nhận nếu chúng được xác nhận bởi người xác nhận đầu vào đủ điều kiện.

Mà còn

Lưu ý rằng các Block và đầu vào được xác nhận được phổ biến độc lập với mỗi khối chứa từ 0 đến d đầu vào được xác nhận.

⁶⁴⁸

Temujin Louie, 'Guest blog: cộng tác về khả năng tương tác của Cardano', iohk.io/en/blog/posts/2022/04/27/guest-blog-collaborating-on-cardano-interoperability/

⁶⁴⁹

Tổng hợp về Thảo luận Cardano | Trực tiếp Cardano #48, youtube.com/watch?v=4DslvkLop04

⁶⁵⁰

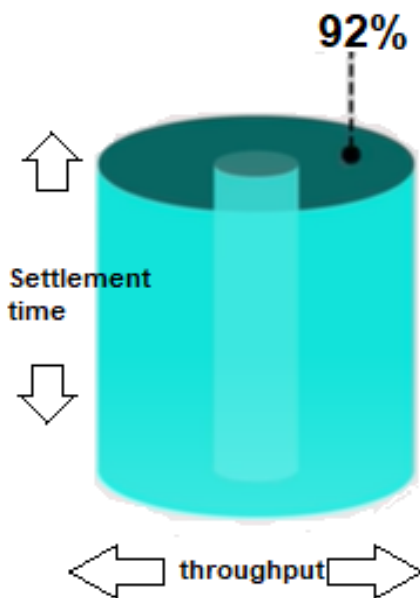
Maller, Bowe, Kohlweiss, Meiklejohn (2019), 'Sonic: SNARK không có kiến thức từ các chuỗi tham chiếu có cấu trúc có thể cập nhật và phổ quát kích thước tuyến tính', eprint.iacr.org/2019/099.pdf

Nhà nghiên cứu của IOG, Peter Gaži, đã giải thích khái niệm người xác nhận đầu vào ⁶⁵¹tại Hội nghị thượng đỉnh Cardano 2021. Người xác nhận đầu vào lặp lại một số khái niệm được thảo luận trong bài báo có tên *Prism: Nhân rộng Bitcoin lên 10.000 lần* ⁶⁵², được bổ sung bằng một video trình bày ⁶⁵³về Prism (đừng nhầm với *Lăng kính Atala của IOG* giải pháp Nhận dạng phi tập trung).

Giáo sư Aggelos Kiayias đã đưa ra lời giải thích chi tiết hơn trong video của mình ⁶⁵⁴, những công thức và toán học nằm ngoài phạm vi của cuốn sách này. Tuy nhiên, rõ ràng là những người xác nhận đầu vào là một tuyến tập những điều tốt nhất của Cardano khi họ tận dụng sức mạnh của Mithril, mô hình UTXO mở rộng, nghiên cứu trước đây về bộ kết hợp sổ cái và nền tảng được thành lập bởi Ouroboros.

Trong video, Giáo sư Kiayias giải thích Ouroboros sử dụng giao thức 'chuỗi dài nhất' ⁶⁵⁵ tương tự như Bitcoin, ngoại trừ nó dựa trên bằng chứng cổ phần. ⁶⁵⁶Vì vậy, nó thừa hưởng tất cả các lợi ích bảo mật và phi tập trung của Bitcoin, nhưng với mức tiêu hao năng lượng ít hơn nhiều. Các giao thức 'chuỗi dài nhất' có những hạn chế nghiêm trọng về hiệu suất về thông lượng. Nếu một đường ống đại diện cho một giao thức đồng thuận, trong đó chiều rộng là thông lượng và chiều dài là thời gian giải quyết, thì chúng tôi muốn có một đường ống ngắn, rộng đẹp.

Dựa trên nghiên cứu ⁶⁵⁷IOG được công bố tại *Hội nghị chuyên đề về bảo mật truyền thông và máy tính ACM* vào năm 2021, có thể xác định giới hạn trên cho thông lượng trong một giao thức chuỗi dài nhất. Con số này chỉ đạt 8%, còn lại 92% công suất thông lượng chưa được khai thác. Ouroboros *Leios*, và cụ thể là người xác nhận đầu vào, sẽ giải quyết thiếu sót nghiêm trọng này.



⁶⁵¹

Gia đình Ouroboros (Người ủng hộ đầu vào), youtu.be/PF1SW7e137A?t=1760

⁶⁵²

Prism: Nhân rộng Bitcoin lên gấp 10.000 lần, arxiv.org/abs/1909.11261

⁶⁵³

Bản trình bày, Prism: Mở rộng quy mô Bitcoin, youtube.com/watch?v=gTJyDtuWvUQ

⁶⁵⁴

Những tiến bộ trong Ouroboros: Mở rộng quy mô để phát triển trong tương lai, youtube.com/watch?v=xKv94MwSNBw

⁶⁵⁵

Chuỗi **dài nhất** là những gì các Node riêng lẻ chấp nhận là phiên bản hợp lệ của Blockchain. Quy tắc các Node chấp nhận Blockchain dài nhất cho phép mọi Node trên mạng đồng ý về giao diện của Blockchain và do đó đồng ý về cùng một lịch sử giao dịch. Quy tắc chuỗi dài nhất đảm bảo rằng mạng sẽ nhận ra 'chuỗi có nhiều công việc nhất' là chuỗi chính. Chuỗi có nhiều công việc nhất thường (không phải luôn luôn) là chuỗi dài nhất trong số các nhánh.

⁶⁵⁶

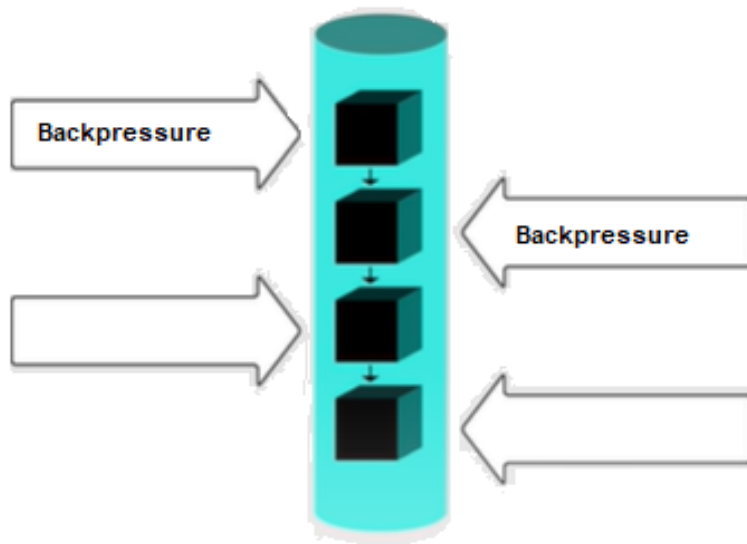
Giao thức chuỗi dài nhất bằng chứng cổ phần: Bảo mật so với khả năng dự đoán, tselab.stanford.edu/downloads/PoS_LC_SBC2020.pdf

⁶⁵⁷

Gaži, Kiayias, Russell (2020), 'Giới hạn nhất quán chặt chẽ cho Bitcoin', eprint.iacr.org/2020/661.pdf

Hình 56: Giao thức chuỗi dài nhất được biểu diễn dưới dạng đường ống

Như đã đề cập trước đây, Ouroboros sử dụng chiến lược mạng áp dụng *áp lực ngược* để đối phó với những thời điểm có nhu cầu xử lý giao dịch cao nhất. Hệ thống xử lý những khối nào nó có thể, trong khi các giao dịch xếp hàng chờ được kéo vào để xử lý. Trong điều kiện lưu lượng truy cập cao điểm, các giao dịch sẽ vẫn được xử lý, nhưng họ phải chờ đến lượt mình.



Hình 57: Khái niệm mạng ngược áp

Người xác nhận đầu vào giải phóng các phân đoạn của mempool (hoặc 'mempool dự phòng với các đặc quyền' khi người dùng trên Stack Exchange ⁶⁵⁸ gọi họ) để trôi nổi xung quanh trước khi chúng được xem xét để xử lý trong khối chuỗi chính. Các phân đoạn nổi này của mempool được gọi là 'khối đầu vào'. Điều này cho phép các nhà sản xuất Block giải phóng không gian trong mempool của họ để họ có thêm khả năng kéo các giao dịch vào. Việc phân đoạn mempool cần phải được đồng thời trên tất cả các nhà sản xuất Block.

IOG có kế hoạch áp dụng các thực tiễn từ truyền thông trái phổ ⁶⁵⁹ để đảm bảo có sự chòng chéo tối thiểu giữa các Block đầu vào. Các Block đầu vào hợp lệ được kiểm tra như với các Block chuỗi dài nhất, nhưng ngoài ra, chúng còn được chứng thực thông qua việc cấp chứng chỉ Mithril. Điều này có nghĩa là các Block đầu vào được chuyển đổi thành các lô giao dịch đã được xác minh để được đưa vào chuỗi chính chỉ bằng cách tham chiếu. Các giao dịch và tập lệnh của khối đầu vào được xử lý bên ngoài từ quá trình xác thực khối chuỗi chính. Chuỗi dài nhất 'khối xếp hạng' được sử dụng để sắp xếp hoặc 'xếp hạng' các Block đầu vào nổi này.

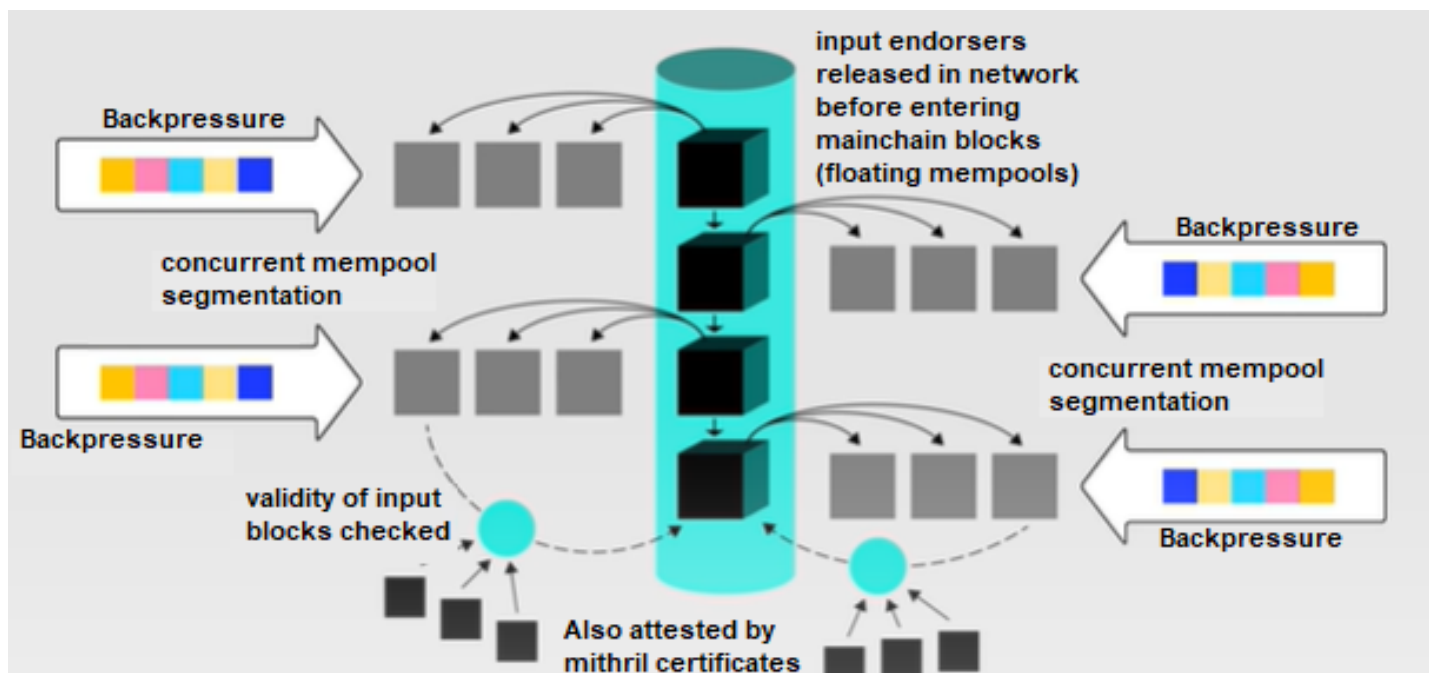
Bản chất tuần tự hóa của giao thức chuỗi dài nhất giải quyết tình trạng 'chỉ tiêu gấp đôi' trong các Block đầu vào. Chiến lược này cũng tận dụng các điểm mạnh của mô hình UTXO mở rộng khi việc thực thi và xác thực tập lệnh diễn ra ngoài quá trình xác thực chuỗi chính. Mục tiêu về thông lượng cao hơn hiện có thể thực hiện được vì 92% công suất nhân rồi hiện có thể được sử dụng. Đồ họa bên dưới ghi lại tất cả các phân chuyển động cho người xác nhận đầu vào.

⁶⁵⁸

Người xác nhận đầu vào khi trao đổi ngắn xếp,
cardano.stackexchange.com/questions/4626/what-are-input-endorsers-and-how-do-they-make-cardano-more-scalable

⁶⁵⁹

Trong truyền thông viễn thông và vô tuyến, **kỹ thuật trái phổ** là các phương pháp mà tín hiệu được tạo ra với một băng thông cụ thể được trải rộng một cách có chủ ý trong miền tần số, dẫn đến tín hiệu có băng thông rộng hơn.



Hình 58: Hình ảnh Người ủng hộ đầu vào phòng theo video giải thích của Giáo sư Kiayias

Nghiên cứu học thuật đột phá này sẽ đi từ lý thuyết đến triển khai thực tế như thế nào sẽ trở nên rõ ràng hơn một chút vào tháng 11 năm 2022. Những người ủng hộ đầu vào sẽ là thành phần chính của *Ouroboros Leios* và sẽ được đề xuất, cộng đồng xem xét và hoàn thiện thông qua CIP 79. Như chúng tôi đang làm bây giờ trong 'thời đại của Voltaire', mọi thứ đều là nguồn mở, khuyến khích phản hồi và tham gia. *Leios* sẽ là một 'phần mở rộng đáng kể' của giao thức Ouroboros. Nó được mô tả sâu hơn trong một bài báo dài hơn⁶⁶⁰ được đưa vào như một phần của CIP này.

Bài báo cũng có sẵn trên GitHub⁶⁶¹ và có thể đọc được một cách đáng ngạc nhiên. Điều này có lẽ là do thiết kế để thu hút càng nhiều thảo luận và tương tác càng tốt trong giai đoạn đầu. Nó được viết bởi kiến trúc sư trưởng của IOG, Duncan Coutts, thường được Charles Hoskinson mô tả là 'phù thủy ngoài đời thực'. Bạn có thể nhìn vào tâm trí của anh ấy và theo dõi cuộc tranh luận với những nhà tư tưởng sâu sắc khác như nhà vật lý hạt nhân Michael Lisenfelt tại đây.⁶⁶²

Bài viết nêu chi tiết chính xác cách thức hoạt động của những người xác nhận đầu vào. Ở cấp độ cao, nghiên cứu đề xuất chuyển từ Blockchain tuần tự sang Blockchain song song. *Leios* sẽ tách rời sự đồng thuận khỏi việc xác thực các Block, nghĩa là các Block sẽ được xác thực liên tục.

Với Ouroboros hiện tại tại Giao thức Praos, thời gian mà một khối được giả mạo và phân tán trên mạng chỉ là một phần nhỏ so với tổng thời gian trung bình giữa các Block. Hiện tại trên mạng chính Cardano: các Block được tạo ra trung bình cứ sau 20 giây, nhưng thời gian để gửi các Block qua mạng là trong vòng 5 giây (đây là tham số Δ).

Trước khi khối đến một Node, Node đó không hoạt động và sau khi nó đã tải xuống, xác thực và chuyển tiếp khối thì nó sẽ trở lại trạng thái không hoạt động. *Leios* đề xuất nhiều cách khác nhau để tận dụng tốt hơn các nguồn tài nguyên nhân rỗi.

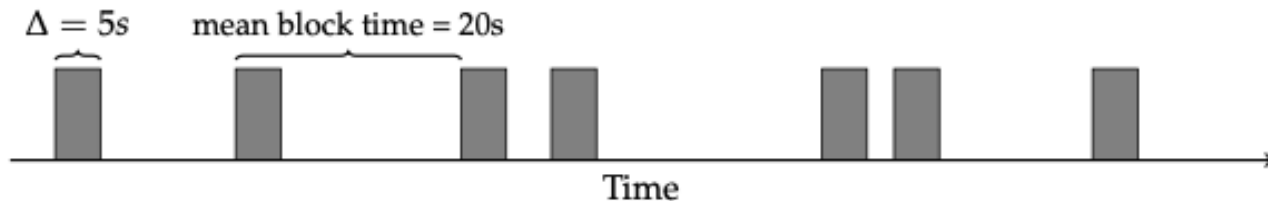
⁶⁶⁰

Coutts, Panagiotakos, Fitzi (2022), 'Ouroboros Leios: mục tiêu và khái niệm thiết kế', iohk.io/en/research/library/papers/ouroboros-leios-design-goals-and-concepts/

⁶⁶¹CIP/CIP-0079/README.md, github.com/cardano-foundation/CIPs/blob/ouroboros-leios/CIP-0079/README.md

⁶⁶²CIP-0079? | Triển khai Ouroboros Leios để tăng thông lượng Cardano, github.com/cardano-foundation/CIPs/pull/379

Example random Praos block production schedule



Hình 59: Thời gian khuếch tán khối của Ouroboros Praos (Δ) là một phần thời gian giữa các Block

Một hệ thống các Node phân tán là một hệ thống song song, nhưng *Ouroboros Praos* là một thuật toán tuần tự. Bất kỳ thuật toán tuần tự nào như vậy chạy trên một hệ thống song song sẽ khiến các tài nguyên không được sử dụng. Thuật toán là tuần tự vì cấu trúc của Blockchain là tuyến tính.

Ouroboros *Leios* sẽ cố gắng triển khai một 'Blockchain đồng thời' để đạt được thuật toán phân tán song song để xây dựng chuỗi. Bằng cách kiểm soát mức độ đồng thời và song song trong thuật toán, điều này sẽ cho phép khối lượng công việc lớn hơn khi các tài nguyên nhân rồi hiện chưa sử dụng được đưa vào hoạt động. Bài báo làm rõ các điều khoản:

Chúng tôi phân biệt đồng thời và song song: đồng thời là dữ liệu hoặc sự kiện không được sắp xếp theo trình tự đối với nhau, trong khi song song là sử dụng nhiều phần cứng máy tính hơn để tính toán nhanh hơn.

Bài báo đi vào chi tiết hơn về cách đạt được điều này với các loại đối tượng mới như khối đầu vào, khối xác nhận, báo cáo xác nhận, chứng chỉ xác nhận và khối xếp hạng. Bài báo và CIP được liên kết ở trên phân tích nhiều cân nhắc và rủi ro với một giải pháp phức tạp như vậy và chắc chắn sẽ phát triển và cập nhật khi quá trình tạo mẫu và mô phỏng tiếp theo cuối cùng đạt được thiết kế tốt nhất. Mô phỏng công khai đầu tiên như vậy được trình bày bởi Benjamin Beckmann (Giám đốc Kiến trúc & Cơ sở hạ tầng của IOG) tại ScotFest.⁶⁶³

Quá trình toàn diện sẽ tuân theo lộ trình quen thuộc của phân tích bảo mật, đánh giá ngang hàng, kiểm toán, chính thức hóa mô tả chính xác về các hành vi dự kiến để làm rõ thiết kế cho kỹ thuật, thử nghiệm hiệu suất, tạo mẫu, cập nhật số cái... và tất cả điều này phụ thuộc vào tiến độ với các tính năng khác như 'Trạng thái sổ cái lưu trữ trên đĩa', triển khai thành công *Ouroboros Genesis*, tăng cường sử dụng ví nhẹ, v.v.

Chỉ sau đó, một hard fork cho *Leios* mới có thể thực hiện được. Đó là một tầm nhìn đầy tham vọng, nhưng IOG và cộng đồng Cardano đang xây dựng trên đá granit, gạt hái những phần thưởng khi làm mọi thứ đúng cách ngay từ đầu. Tất cả các tính năng và khái niệm được mô tả trong cuốn sách này đều dựa trên nghiên cứu học thuật chuyên sâu, được đánh giá ngang hàng bởi những bộ óc thông minh nhất trong lĩnh vực mật mã và được triển khai dựa trên các thông số kỹ thuật chính thức.

Ngày 3 tháng 10 năm 2022. Re: Người ủng hộ đầu vào, Hãy nói chuyện với Basho. CH⁶⁶⁴

Vì vậy, điều xảy ra là bạn đi từ quy trình tiêu chuẩn này của một chuỗi các Block, và chỉ có một chế độ xem chuẩn, về cơ bản, thực hiện nhiều việc này một cách không đồng bộ và song song, và chúng gần như được nhóm lại với nhau, và sau đó không đồng bộ và song song, rất nhiều thứ xảy ra và sau đó chúng được gộp lại với nhau... Vì vậy, khái niệm về khối đầu vào và khối chính, như đã thảo luận trong bài viết về chuỗi song song của chúng tôi.⁶⁶⁵

Giờ đây, quá trình tạo Block này...bạn nghĩ về chứng chỉ Mithril nơi bạn nói về việc tạo Block các giao dịch, sự kiện cùng nhau...bạn cũng có thể sử dụng lại công nghệ này trong mô hình UTXO mở rộng để các Block lại với nhau. Vì vậy, nó cung cấp cho bạn một cách để tìm ra lịch sử không có xung đột và điều này có thể có nghĩa là bạn có quá trình xử lý song song không đồng bộ đối với một lượng lớn sự kiện. Vì vậy, mức tăng thông lượng, giả sử cấu trúc dữ liệu mới và giả định

⁶⁶³Tiếp tục thúc đẩy tiến bộ công nghệ thông qua Người xác nhận đầu vào, youtube.com/watch?v=IGu_1bl6UHQ

⁶⁶⁴Hãy nói về Basho, youtu.be/fhVo-2QUjLM?t=780

⁶⁶⁵ Fitzi, Gaži, Kiayias, Russell (2018), 'Chuỗi song song: Cải thiện thông lượng và độ trễ của các giao thức Blockchain thông qua thành phần song song', iohk.io/en/research/library/papers/parallel-chains-improving-throughput-and-latency-of-blockchain-giao-thuc-thong-qua-song-song-thanh-phan

thiết kế mới, là rất lớn đối với điều này vì về cơ bản bạn có thể là thời gian thực, liên tục chạy các tính toán. Ngay bây giờ, trong thiết kế hiện tại, chỉ 0,25% ngân sách thời gian khối của bạn là dành cho tính toán.

Vì vậy, việc chạy thực thi tập lệnh... do đó, điều đó cực kỳ hạn chế...0,25%, không phải 25%, mà là 0,25% thời gian khối của bạn dành cho thực thi tập lệnh, vì vậy đây là một nguồn tài nguyên rất khan hiếm. Ở đây nó không đồng bộ, vì vậy nó thực thi liên tục. Vì vậy, chúng tôi hy vọng sẽ thấy không chỉ 10x, mà còn rất rất tăng rất đáng kể về tốc độ và giảm chi phí...

Chương 9: Voltaire (Quản trị)

'Không có vấn đề nào có thể chịu được sự tấn công của tư duy bền vững.'
- Voltaire

Tiền là xã hội

Với một vài trường hợp ngoại lệ đáng chú ý, hầu hết các loại Crypto không cung cấp khả năng nâng cấp trong tương lai. Khả năng thúc đẩy một hard fork hoặc soft fork một cách hiệu quả là rất quan trọng đối với khả năng tồn tại lâu dài của Crypto. Do đó, những kẻ hám tiền khó có thể đầu tư hàng triệu đô la vào các giao thức có lộ trình và những người tham gia chỉ là phù du, nhỏ nhen hoặc cực đoan. Phải có một quy trình hiệu quả để hình thành thỏa thuận về tầm nhìn cho sự phát triển của giao thức cơ bản. Sự phân mảnh có thể chia tách nhóm nếu quá trình này khó khăn.

Crypto là một minh họa tuyệt vời về thành phần xã hội của tiền tệ. Khi so sánh Bitcoin và Litecoin chỉ đơn thuần trên cơ sở công nghệ, có rất ít sự khác biệt giữa hai loại này và thậm chí còn ít hơn giữa Ethereum và Ethereum Classic. Mặc dù vậy, cả Litecoin và Ethereum Classic đều có vốn hóa thị trường khổng lồ, cộng đồng tích cực và các chương trình xã hội của riêng họ.

Có thể khẳng định rằng một phần đáng kể giá trị của Crypto được tạo ra từ cộng đồng của nó, cách họ sử dụng tiền của mình và mức độ liên quan của nó đối với tiến trình của tiền tệ. Thêm vào ý tưởng này, các loại tiền tệ khác, chẳng hạn như Dash⁶⁶⁶ hoặc Tezos⁶⁶⁷ đã xây dựng các phương thức trực tiếp vào giao thức để cho phép người dùng bỏ phiếu về những gì nên được ưu tiên phát triển và tài trợ.

Sự đa dạng của các loại Crypto cũng thể hiện các khía cạnh xã hội của chúng. Sự phân mảnh và phân nhánh là kết quả của những bất đồng về triết lý, chính sách tiền tệ hoặc thậm chí là những tranh cãi nhỏ giữa các nhà phát triển cốt lõi. CH tại ScotFest:

Mọi người rơi vào giá trị, không phải sự thật

Tuy nhiên, không giống như những người anh em kỹ thuật số của chúng, tiền tệ fiat có xu hướng vượt qua những biến động chính trị và tranh chấp địa phương mà không xảy ra khủng hoảng tiền tệ. Có vẻ như một số khía cạnh của các hệ thống cũ không có trong lĩnh vực Crypto. IOG tin rằng người dùng giao thức cần được khuyến khích để hiểu hợp đồng xã hội làm nền tảng cho hệ thống của họ và cơ hội đề xuất sửa đổi theo cách mang tính xây dựng. Sự độc lập này áp dụng cho mọi khía cạnh của hệ thống trao đổi giá trị, từ quy định thị trường đến tài trợ dự án. Tuy nhiên, nó không thể được trung gian bởi các tác nhân trung tâm, cũng như không cần bất kỳ thông tin xác thực nào có thể được đồng chọn bởi một số ít đặc quyền.

Nguồn vốn luôn cạn kiệt, bất kể sự thành công của đợt bán hàng cộng đồng⁶⁶⁸ để phát triển bootstrap. Do đó, Cardano chứa một niềm tin phi tập trung giúp giảm lạm phát và phí giao dịch theo thời gian. Thông qua cơ chế bỏ phiếu, bất kỳ người dùng nào cũng có thể tìm kiếm tiền từ quỹ ủy thác và các bên liên quan nên bỏ phiếu xem ai sẽ trở thành người thụ hưởng. Bằng cách tạo ra một cuộc thảo luận về việc ai nên được tài trợ, quá trình này tạo ra một vòng phản hồi tích cực giống như vòng phản hồi được tìm thấy trong các loại Crypto khác có hệ thống quản trị, chẳng hạn như Dash. Đối thoại lành mạnh đảm bảo rằng cộng đồng luôn đánh giá và tranh luận quan điểm của mình trước các quyết định quan trọng.

Trong một thời gian dài và trong nhiều trường hợp, những bất đồng chưa được giải quyết về định hướng kỹ thuật và đạo đức của cơ sở mã đã gây khó khăn cho Bitcoin với cuộc tranh luận về kích thước khối của nó, Ethereum với sự phân chia DAO và một loạt các loại Crypto khác. Nhiều xung đột trong số này, cũng như sự chia rẽ cộng đồng xảy ra khi hành động được thực hiện, có thể là do không có bất kỳ cơ chế nào để thực hiện thay đổi.

Nhìn vào những bài học từ quá khứ, việc áp dụng (SegWit) Segregated Witness của Bitcoin⁶⁶⁹ có thể đã được xử lý tốt hơn rất nhiều.

⁶⁶⁶

Dash là một loại Crypto mã nguồn mở và là một dạng tổ chức tự trị phi tập trung (DAO) được điều hành bởi một nhóm nhỏ người dùng, được gọi là 'masternodes'. Nó là một altcoin được tách ra từ giao thức Bitcoin. Tiền tệ cho phép các giao dịch nhanh chóng không thể theo dõi được.

⁶⁶⁷

Tezos (mã: XTZ) là một Blockchain phi tập trung được thành lập bởi Arthur Breitman và Kathleen Breitman. Breitmans cũng thành lập Dynamic Ledger Solutions (DLS), một công ty chủ yếu tập trung vào phát triển công nghệ Tezos và sở hữu tài sản Trí tuệ Tezos. Đồng tiền này đã được ra mắt trong đợt chào bán tiền xu ban đầu (ICO) vào ngày 1 tháng 7 năm 2017.

⁶⁶⁸

Crowdsales là một cách sử dụng phổ biến cho Ethereum; chúng cho phép bạn phân bổ Token cho những người tham gia mạng theo nhiều cách khác nhau, chủ yếu để đổi lấy Ether. Chúng có nhiều hình dạng và hương vị khác nhau.

⁶⁶⁹

Segregated Witness, hay SegWit, là tên được sử dụng cho một thay đổi ngã ba mềm được triển khai trong định dạng giao dịch của bitcoin.

⁶⁷⁰Có phải cuộc tấn công DAO ⁶⁷¹thực sự dẫn đến hard fork trên Ethereum? Nó có thể được quản lý tốt hơn để không xảy ra sự cố cộng đồng nghiêm trọng như vậy không?⁶⁷²

Trong trường hợp xấu nhất, thẩm quyền đạo đức để hành động có thể chỉ đơn giản là dành cho bất kỳ ai có nhà phát triển, liên kết cơ sở hạ tầng và tiền, thay vì phần lớn lợi ích tốt nhất của cộng đồng. Thật khó để đánh giá liệu các hành động có hợp lệ hay không nếu một bộ phận lớn của cộng đồng không có mặt hoặc không tham gia do các biện pháp khuyến khích kém.⁶⁷³

Một số loại Crypto như Tezos có một mô hình trong đó giao thức Crypto được xử lý như một hiến pháp, với ba phần (Giao dịch, Đồng thuận và Mạng) và một bộ quy tắc và thủ tục rõ ràng để cập nhật hiến pháp. Tuy nhiên, vẫn còn rất nhiều việc phải làm đối với các ưu đãi cũng như cách thể hiện và cập nhật giao thức Crypto bằng ngôn ngữ chính thức.

IOG đã nghiên cứu quản trị Crypto trong nhiều năm. Họ đã viết các bài báo từ năm 2017 về việc đề xuất quỹ cho Ethereum Classic.⁶⁷⁴ Một bài báo khác, của Đại học Lancaster,⁶⁷⁵ tập trung vào khái niệm hệ thống kho bạc và một phương pháp dân chủ, khả thi để tài trợ phát triển dài hạn cho Cardano.

Các phương pháp chính thức, thông số kỹ thuật dễ hiểu của máy và kết hợp kho bạc với quy trình này để khuyến khích tài chính chỉ là một số giải pháp mà IOG theo đuổi. Bây giờ nhìn lại, rõ ràng là họ đang đặt quân cờ vào vị trí, để tạo ra bộ máy cần thiết cho tầm nhìn *Thời đại Voltaire* được trình bày tại ScotFest⁶⁷⁶ vào tháng 11 năm 2022. Thông tin thêm về điều này sau.

Đề xuất cải tiến Cardano (CIP)

Một trong những phần quản trị ban đầu được triển khai vào tháng 11 năm 2020 là CIP 0001,⁶⁷⁷ giải thích CIP là gì. Bất kỳ ai có ý tưởng cải tiến Cardano đều có thể trình bày chúng dưới dạng CIP (đề xuất cải tiến Cardano). CIP là một phương tiện đề xuất chính thức các cải tiến theo cách dựa trên sự đồng thuận. Chúng là một thành phần thiết yếu của quản trị Cardano, mặc dù chúng không ràng buộc, cũng không phải là yêu cầu đối với sửa đổi giao thức hoặc kho bạc. Trước khi bỏ phiếu, ai đó phải gửi đề xuất để những người khác xem xét.

CIP tuân theo một định dạng tiêu chuẩn: cấu trúc đề xuất được tạo khuôn mẫu để giúp cho việc tranh luận và đánh giá dễ dàng hơn. Điều này cho phép các thành viên khác của cộng đồng cân nhắc về các đề xuất cải tiến hoặc các vấn đề trong một đề xuất. CIP được lưu giữ dưới dạng tệp văn bản trong repo⁶⁷⁸ Github được phiên bản và lịch sử sửa đổi của chúng cung cấp hồ sơ lịch sử của đề xuất. Đối với những người không có trên GitHub, cips.cardano.org là một trang web chị em được tạo tự động.

Có ba loại CIP khác nhau:

⁶⁷⁰

câu chuyện của SegWit : Tranh cãi, Nội chiến & Nhận con nuôi, blog.btse.com/segwit/

⁶⁷¹

Tìm hiểu về cuộc tấn công DAO, coindesk.com/learn/2016/06/25/undering-the-dao-attack/

⁶⁷²

Ethereum sụp đổ, fortune.com/2016/09/04/ethereum-fall-out/

⁶⁷³

Khuyến khích : một phương pháp khuyến khích các thành viên tham gia vào mạng bằng cách cung cấp cho họ lợi nhuận tương xứng với nỗ lực của họ. Bằng cách thúc đẩy sự tham gia liên tục, tích cực và mạnh mẽ, các biện pháp khuyến khích cố gắng duy trì sự bình đẳng và công bằng trong một mạng lưới người tham gia phân tán. Các ưu đãi cần thiết trong mô hình khuyến khích của Cardano được tính toán bằng lý thuyết trò chơi.

⁶⁷⁴ Kaidalov , Kovalchuk, Nastenکو , Rodinko , Shevtzov , Oliynykov (2017), 'Đề xuất cho Hệ thống Kho bạc Ethereum Classic', iohk.io/en/research/library/papers/a-proposal-for-an-ethereum-classic- hệ thống ngân quỹ/

⁶⁷⁵Zhang, Oliynykov và Balogun (2019), 'Hệ thống ngân quỹ cho Crypto: Kích hoạt trí thông minh cộng tác tốt hơn', eprint.iacr.org/2018/435.pdf

⁶⁷⁶IO Scotfest : Thời đại của Voltaire, youtube.com/playlist?list=PLnPTB0CuBOBxjKB8DdMhy57MriBCHT1RM

⁶⁷⁷CIP-0001: Đề xuất cải tiến Cardano, github.com/cardano-foundation/CIPs/tree/master/CIP-0001

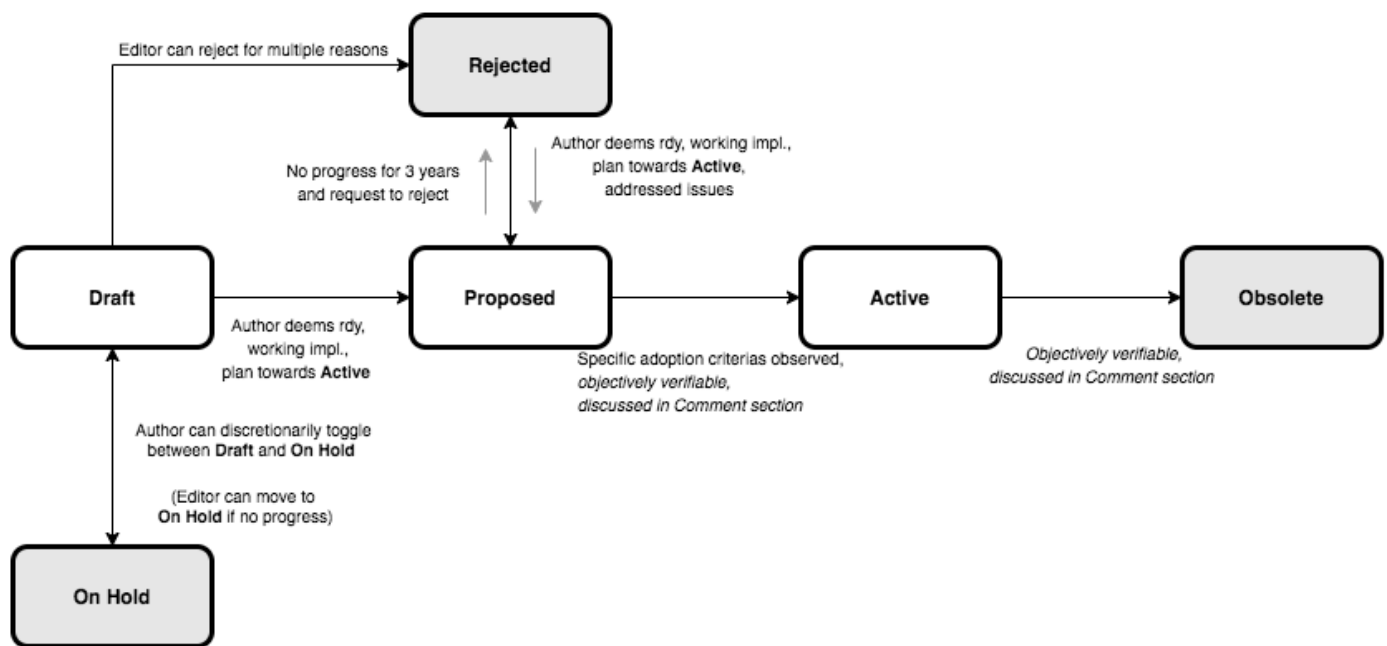
⁶⁷⁸

Kho lưu trữ CIP, github.com/cardano-foundation/CIPs

1. **CIP theo dõi tiêu chuẩn** là một sửa đổi ảnh hưởng đến việc triển khai Cardano. Ví dụ: cập nhật giao thức mạng hoặc về cơ bản là bất kỳ thay đổi nào khác ảnh hưởng đến khả năng tương thích của các ứng dụng Cardano. CIP trên Đường mòn tiêu chuẩn có hai phần: tài liệu thiết kế và triển khai tham chiếu.
2. **CIP quy trình** phác thảo một quy trình liên quan đến Cardano hoặc đề xuất sửa đổi một quy trình. CIP xử lý tương tự như CIP theo dõi tiêu chuẩn, tuy nhiên chúng được sử dụng cho các chủ đề khác ngoài giao thức Cardano. Họ thường cần sự chấp thuận của cộng đồng; do đó, không giống như CIP thông tin, chúng không chỉ là những đề xuất mà người dùng không được phép bỏ qua.
3. **CIP thông tin** thảo luận về vấn đề thiết kế Cardano hoặc cung cấp thông tin hoặc tiêu chuẩn cộng đồng Cardano rộng rãi, nhưng nó không đề xuất bất kỳ điều gì mới. Người dùng và người triển khai có quyền bỏ qua CIP thông tin hoặc làm theo lời khuyên của họ vì chúng không nhất thiết phản ánh sự đồng thuận hoặc đề xuất của cộng đồng Cardano.

Mỗi CIP có định dạng sau: Lời mở đầu, Tóm tắt, Động lực, Thông số kỹ thuật, Cơ sở lý luận, Khả năng tương thích ngược, Đường dẫn đến Lưu trữ, Bản quyền.

Khái niệm này được phát triển dưới dạng một đề xuất bằng văn bản phù hợp và được gửi dưới dạng yêu cầu kéo ⁶⁷⁹ tới kho lưu trữ CIP sau khi thảo luận và phản hồi ban đầu. Dự thảo CIP cập nhật sau đó được xử lý công khai theo cách sau:



Hình 60: Quy trình công việc CIP từ CIP0001

Các CIP được xử lý theo phương thức bán chính thức: Những người biên tập các đề xuất CIP gặp nhau thường xuyên để thảo luận và đánh giá các ý tưởng. Biên bản cuộc họp có sẵn cho công chúng ⁶⁸⁰ và các cuộc họp được tổ chức hai tuần một lần. Các tác giả được khuyến khích đóng góp và đưa ra nhận xét, đồng thời các cuộc thảo luận thường diễn ra đồng thời trong phần CIP của diễn đàn Cardano ⁶⁸¹ và/hoặc trong các yêu cầu kéo GitHub.

Hãy coi kho lưu trữ CIP là một tập hợp các công cụ hữu ích - một số có thể hoạt động tốt cùng nhau, trong khi những công cụ khác thì

⁶⁷⁹

Yêu cầu kéo là một tính năng dành riêng cho GitHub. Chúng cung cấp một cách đơn giản, dựa trên web để gửi tác phẩm của bạn (thường được gọi là “các bản vá lỗi”) cho một dự án. Nó được gọi là yêu cầu kéo vì bạn đang yêu cầu dự án lấy các thay đổi từ ngã ba của bạn.

⁶⁸⁰

Các cuộc họp CIP hai tuần một lần, [github.com/ cardano -foundation/CIPs/tree/master/ BiweeklyMeetings](https://github.com/cardano-foundation/CIPs/tree/master/BiweeklyMeetings)

⁶⁸¹

Diễn đàn Cardano Phần CIP , forum.cardano.org/c/english/cips/122

không. Bạn có toàn quyền kiểm soát việc triển khai của mình tuân theo CIP nào. Cộng đồng sẽ nghiêng về một số hơn những cộng đồng khác, những cái mới sẽ được gửi khi Cardano phát triển.

CIP đáng chú ý:

- CIP 1 - Quy trình CIP

'Đề xuất cải tiến Cardano (CIP) là một tài liệu thiết kế chính thức cho cộng đồng Cardano, cung cấp thông tin hoặc mô tả một tính năng mới cho mạng Cardano, các quy trình hoặc môi trường của nó một cách ngắn gọn và hiệu quả về mặt kỹ thuật .;

- CIP 9 - Thông số giao thức

'CIP này là một CIP thông tin mô tả cài đặt tham số giao thức ban đầu cho kỷ nguyên Shelley của Blockchain Cardano, cộng với những thay đổi đã được thực hiện. Nó nhằm phục vụ như một bản ghi lịch sử, cho phép các thay đổi tham số giao thức được theo dõi trở lại cài đặt ban đầu.'

- CIP 25 - Tiêu chuẩn siêu dữ liệu NFT

Đề xuất này xác định Tiêu chuẩn siêu dữ liệu NFT cho Token gốc.

- CIP 27 - Tiêu chuẩn tiền bản quyền cộng đồng CNFT

Một tiêu chuẩn cộng đồng cho chức năng của tiền bản quyền, không yêu cầu thực hiện hợp đồng thông minh.

- CIP 30 - Cardano DApp-Wallet Web Bridge

CIP này mô tả cầu nối giao tiếp cho phép DApp giao tiếp với ví Cardano.

- CIP 31 - Đầu vào tham chiếu

'Chúng tôi giới thiệu một loại đầu vào mới, đầu vào tham chiếu, cho phép xem xét đầu ra mà không tốn chi phí. Điều này sẽ tạo điều kiện truy cập vào thông tin được lưu trữ trên Blockchain mà không có sự xáo trộn liên quan đến chi tiêu và tạo UTXO.'

- CIP 32 - Dữ liệu nội tuyến

'Chúng tôi đề xuất cho phép bản thân dữ liệu được gắn vào đầu ra thay vì hàm băm dữ liệu. Điều này sẽ cho phép giao tiếp các giá trị chuẩn đơn giản hơn nhiều giữa những người dùng.'

- CIP 33 - Tập lệnh tham khảo

'Chúng tôi đề xuất cho phép đính kèm tập lệnh ("tập lệnh tham chiếu") vào đầu ra và cho phép sử dụng tập lệnh tham chiếu để đáp ứng các yêu cầu về tập lệnh trong quá trình xác thực, thay vì yêu cầu giao dịch chi tiêu phải làm như vậy. Điều này sẽ cho phép các giao dịch sử dụng tập lệnh phổ biến nhỏ hơn nhiều.'

- CIP 50 - Liesenfelt Bản cập nhật phân cấp Shelleys Voltaire

do Tiến sĩ Michael Liesenfelt đề xuất , CIP này thảo luận về sự biện minh, phương pháp, số liệu và lịch trình triển khai để tăng cường phân cấp của Cardano.

- CIP 79 - Triển khai Ouroboros Leois để tăng thông lượng Cardano

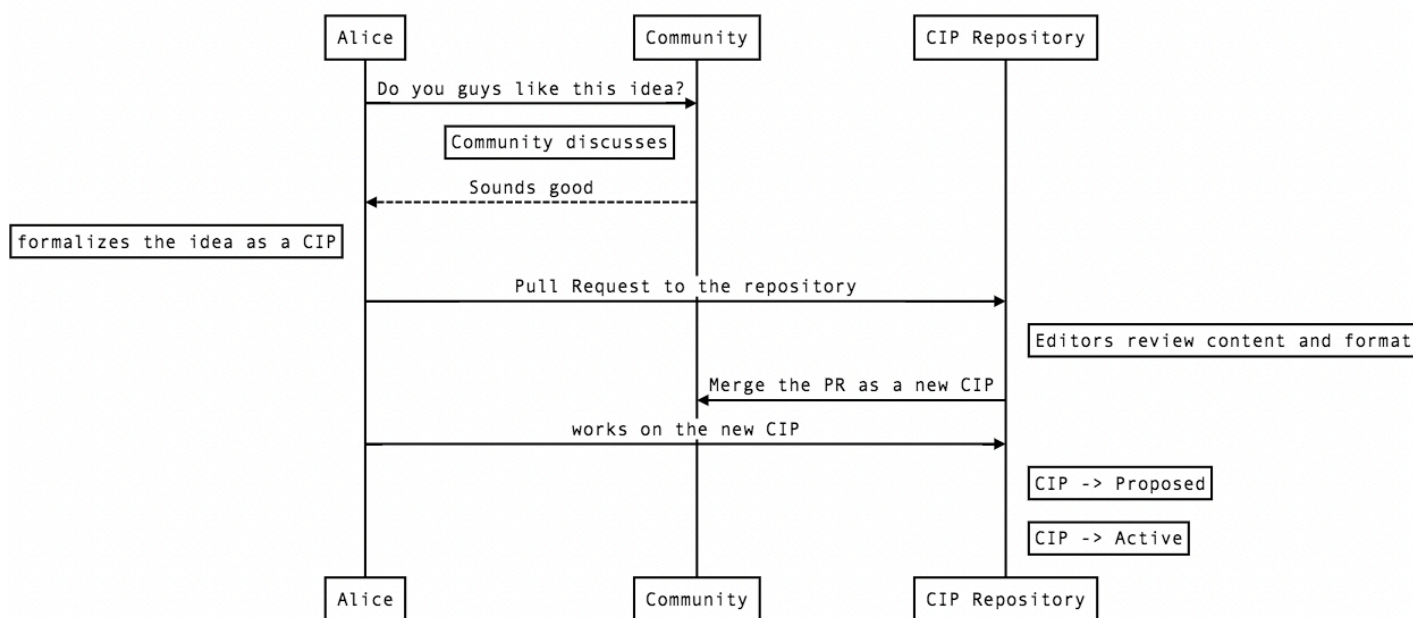
CIP này thảo luận về việc triển khai *Ouroboros Leios* .

- CIP1694 - Đề xuất bước vào giai đoạn Voltaire

- CIP999 (đọc là 'CIP trừ 1') - Báo cáo vấn đề Cardano (CPS)

CPS bổ sung cho CIP. CIP999 giải thích nhu cầu về CPS, cấu trúc, trạng thái và tiêu chí thành công của họ. CPS được giới thiệu để đơn giản hóa quy trình khi giải thích tuyên bố vấn đề của các CIP phức tạp, thay thế phần '*động lực' phức tạp hơn* .

Chúng cũng có thể tồn tại dưới dạng 'yêu cầu đề xuất từ các tác nhân hệ sinh thái, những người đã xác định được vấn đề nhưng vẫn chưa tìm ra giải pháp phù hợp nào'.



Hình 61: Quy trình làm việc CIP từ góc nhìn của biên tập viên

chương trình đại sứ

Cộng đồng Cardano không thiếu các thành viên cam kết sẵn sàng tham gia Chương trình Đại sứ của Quỹ Cardano, ⁶⁸²được thành lập vào năm 2018.

Mục tiêu của chương trình là:

- Tăng cường áp dụng Cardano
- Thúc đẩy nhận thức
- Giáo dục cộng đồng

Để đăng ký trở thành đại sứ, hãy gửi email cho Cardano Foundation: community@cardanofoundation.org

Dự án Catalyst là gì?

Một phần quản trị khác được giới thiệu vào năm 2020 là Project Catalyst. Catalyst là một hệ thống ngân quỹ nguyên mẫu kết hợp các quy trình đề xuất và bỏ phiếu. Việc thiết lập một tương lai lâu dài cho sự phát triển của Cardano bắt đầu bằng kho bạc và bỏ phiếu dân chủ trong dự án Catalyst. Nó trước đây được lưu trữ trên IdeaScale ⁶⁸³nhưng hiện đã được chuyển đến trang web dành riêng cho nó, projectcatalyst.io

Khi tạo một Blockchain bằng chứng cổ phần, điều quan trọng là phải đảm bảo hệ thống tự duy trì. Nó phải có khả năng phát triển và trưởng thành một cách phi tập trung và hữu cơ. Voltaire ⁶⁸⁴là cách tiếp cận của IOG để tạo ra khả năng này, cho phép cộng đồng Cardano duy trì Blockchain đồng thời đề xuất và triển khai các cải tiến hệ thống. Điều này đặt quyền ra quyết định vào tay những người nắm giữ ADA.

⁶⁸²

Chương trình Đại sứ Cardano, cardano.org/ambassadors/

⁶⁸³

Cardano IdeaScale, cardano.ideascale.com/

⁶⁸⁴

Lộ trình Voltaire, [Mapano.cardano.org/en/Voltaire/](https://mapano.cardano.org/en/Voltaire/)



Hình 62: Màn hình mở đầu cho mỗi cuộc họp Catalyst Town Hall, (crowdcast.io/iohk)

Nền tảng của một Blockchain mạnh mẽ là một lĩnh vực nghiên cứu và tranh luận không tầm thường. Một cuộc nói chuyện ⁶⁸⁵về sự cần thiết của việc tài trợ cho sự phát triển của Cardano đã được đưa ra trong hội nghị Shelley vào tháng 7 năm 2021. Dự án Catalyst, kết hợp nghiên cứu, thử nghiệm xã hội và sự đồng ý của cộng đồng để phát triển một nền văn hóa dân chủ, cởi mở trong cộng đồng Cardano, sử dụng các khả năng của cơ chế ngân quỹ của IOG .

Được xây dựng trên nền dân chủ

Sự bền vững và phát triển Blockchain dài hạn cần sự tiến bộ và trưởng thành về công nghệ. Tăng trưởng và cải tiến hệ thống phải được hỗ trợ và tài trợ bởi ai đó. Bởi vì nó cho phép các lựa chọn hợp tác, bền vững mà không phụ thuộc vào một tổ chức quản lý duy nhất, nên cách tiếp cận dân chủ là một khía cạnh quan trọng của hệ sinh thái Blockchain. Kết quả là, quản trị và ra quyết định phải được thực hiện tập thể. Người dùng sẽ có thể xem các cải tiến được thực hiện như thế nào, ai đưa ra quyết định và tiền đến từ đâu.

Sự bền vững

Có nhiều lựa chọn khác nhau để huy động vốn cho phát triển. Các phương pháp phổ biến nhất bao gồm quyên góp, đầu tư mạo hiểm và cung cấp tiền xu ban đầu (ICO). Mặc dù các mô hình như vậy có thể hiệu quả để tạo ra tiền mặt ban đầu, nhưng chúng tiềm ẩn khi đảm bảo nguồn tài chính dài hạn hoặc cung cấp vốn cần thiết để phát triển và duy trì. Hơn nữa, các mô hình này chịu sự kiểm soát tập trung nên khó đạt được sự đồng thuận đáp ứng nhu cầu và nguyện vọng của mọi người.

Một số dự án Crypto sử dụng thuế để tạo nguồn tài chính dài hạn cho sự phát triển Blockchain, thu một phần phí hoặc ưu đãi và gửi chúng vào một nhóm riêng gọi là kho bạc. Các quỹ trong Kho bạc sau đó có thể được sử dụng để phát triển và bảo trì hệ thống. Ngoài ra, khi giá trị của Crypto tăng lên, thì giá trị dự trữ của chính phủ cũng tăng theo. Điều này mở ra một nguồn doanh thu tiềm năng mới.

Tuy nhiên, khi phải đưa ra những đánh giá về cách hướng dẫn sự phát triển, các hệ thống tài chính thường có nguy cơ bị tập trung hóa. Chỉ một vài người trong tổ chức hoặc công ty được phép đưa ra lựa chọn về cách chi tiêu tiền mặt có sẵn trong các hệ thống này. Do tính chất phi tập trung của Blockchain khiến việc quản lý quỹ tập trung trở nên khó khăn, nên có thể xảy ra bất đồng giữa các thành viên trong tổ chức, dẫn đến xung đột.

Kho bạc của Cardano

⁶⁸⁵

Để giải quyết các vấn đề, một loạt các hệ thống kho bạc đã xuất hiện. Các hệ thống này có thể bao gồm các giai đoạn ngân quỹ lặp đi lặp lại khi các yêu cầu tài trợ dự án được trình bày, tranh luận và biểu quyết. Quyền riêng tư của cử tri kém và bảo mật gửi phiếu bầu là hai nhược điểm điển hình. Hơn nữa, nếu các Node chính bị ép buộc, tính hợp lệ của các lựa chọn tài trợ có thể bị nguy hiểm và việc thiếu đầu vào của chuyên gia có thể thúc đẩy các khoản đóng góp không mong muốn.

Cardano được thành lập như một nền tảng Crypto thế hệ thứ ba để giải quyết các vấn đề mà các nền tảng trước đó gặp phải. Cardano muốn làm cho quy trình trở nên dân chủ hơn bằng cách trao cho mọi người ảnh hưởng và đảm bảo rằng các lựa chọn được đưa ra một cách công bằng. Điều quan trọng là phải có các cơ chế bỏ phiếu và tài chính minh bạch để đạt được điều này. Đây là nơi Voltaire bước vào bức tranh.

Bài báo nói trên (Đại học Lancaster) về hệ thống kho bạc cho Crypto đề xuất một phương pháp ra quyết định hợp tác, phi tập trung, do cộng đồng kiểm soát để tài trợ cho việc phát triển và bảo trì Blockchain dài hạn. Loại trí tuệ hợp tác này dựa trên nền dân chủ lỏng, ⁶⁸⁶là sự kết hợp giữa dân chủ trực tiếp và dân chủ đại diện, kết hợp những ưu điểm của cả hai.

Phương pháp này cho phép Hệ thống Kho bạc sử dụng kiến thức chuyên môn trong quá trình bỏ phiếu đồng thời đảm bảo rằng tất cả những người nắm giữ ADA đều có cơ hội bỏ phiếu. Do đó, đối với mỗi dự án, một cử tri có thể bỏ phiếu cá nhân hoặc ủy quyền bỏ phiếu của họ cho một thành viên cộng đồng am hiểu về chủ đề này.

Để duy trì khả năng tồn tại lâu dài, cộng đồng kiểm soát hệ thống kho bạc, thường xuyên được bổ sung từ các nguồn như:

- một phần của phần thưởng Stake Pool và chi phí giao dịch
- đóng góp hoặc từ thiện
- những đồng tiền mới đúc được giữ lại để làm nguồn tài chính.

Nó sẽ có thể tài trợ cho các sáng kiến và trả tiền cho các đề xuất cải tiến vì ADA luôn được tích lũy. Kết quả là, quá trình cấp vốn có thể được chia thành 'thời kỳ ngân quỹ', mỗi giai đoạn được chia thành các giai đoạn sau:

- bỏ phiếu trước
- biểu quyết
- hậu bầu cử.

Các ý tưởng dự án có thể được trình bày bất cứ lúc nào trong suốt nhiệm kỳ, được các chuyên gia và cử tri tranh luận, sau đó được bỏ phiếu để tài trợ cho các sáng kiến quan trọng nhất. Mặc dù thực tế là bất kỳ ai cũng có thể gửi đề xuất, nhưng chỉ một số ít được chọn sẽ được tài trợ, dựa trên phiếu bầu của cộng đồng.

Quy trình ra quyết định

Các nhà khoa học (kể cả các nhà vật lý hạt nhân ⁶⁸⁷), nhà phát triển, loại điều hành, nhà đầu tư và công chúng nói chung nằm trong số những người nắm giữ ADA bỏ phiếu. Với lĩnh vực tham gia đa dạng như vậy, với các chương trình nghị sự và động cơ khác nhau, cần phải có các cơ chế phù hợp để duy trì tính toàn diện, đồng thời đảm bảo diễn ra các cuộc đánh giá và bỏ phiếu công bằng.

Quyền biểu quyết của một người tỷ lệ thuận với số lượng ADA mà họ nắm giữ; họ càng sở hữu nhiều ADA, phiếu bầu của họ càng có trọng lượng. Cùng với việc bỏ phiếu đồng ý/không trực tiếp, một người có thể chuyển quyền biểu quyết của mình cho một chuyên gia mà họ tin tưởng như một phần của khái niệm dân chủ lỏng. Trong trường hợp này, chuyên gia sẽ có thể bỏ phiếu trực tiếp cho ý tưởng mà họ tin là quan trọng nhất.

Sau khi bỏ phiếu, ý tưởng dự án có thể được đánh giá và xếp hạng tùy thuộc vào số phiếu đồng ý/không; các đề xuất dự án kém nhất sẽ bị loại bỏ. Các ý tưởng được xếp hạng cao nhất sẽ lần lượt được tài trợ cho đến khi ngân quỹ cạn kiệt, sau đó các đề xuất lọt vào danh sách rút gọn sẽ được xếp hạng theo điểm số của chúng. Việc chia nhỏ quá trình ra quyết định thành các giai đoạn đảm bảo mỗi đề xuất đều được phê bình nghiêm túc và công bằng.

Nhóm nghiên cứu của IOG đã tận dụng bằng chứng ZK để bảo vệ quyền riêng tư của cử tri. Phương pháp tiếp cận không kiến thức (ZK) là các phương pháp toán học để xác minh thông tin mà không để lộ bất kỳ sự thật cơ bản nào. Bằng chứng không có kiến thức

⁶⁸⁶

Nền dân chủ lỏng là một hình thức của nền dân chủ ủy quyền trong đó một cử tri tham gia vào quá trình ra quyết định tập thể thông qua sự tham gia trực tiếp và đại diện năng động. Hệ thống dân chủ này tận dụng các bộ phận của cả dân chủ trực tiếp và dân chủ đại diện.

⁶⁸⁷

trong tình huống này chỉ ra rằng một người nào đó có thể bỏ phiếu mà không cần cung cấp bất kỳ thông tin cá nhân nào ngoài việc họ đủ tư cách bỏ phiếu. Do đó, mọi khả năng ép buộc cử tri đều bị loại bỏ.

Project Catalyst là một hệ thống ngân quỹ kết hợp các đề xuất và quy trình bỏ phiếu, với mục tiêu thúc đẩy văn hóa dân chủ trong cộng đồng Cardano. Kho bạc của Cardano ban đầu sẽ được bổ sung bằng một tỷ lệ các khoản thanh toán Stake Pool, đảm bảo nguồn cung cấp kho bạc dài hạn. Các Blockchain khác có hệ thống ngân quỹ, nhưng IOG kết hợp tính ẩn danh hoàn hảo nhờ bằng chứng không có kiến thức, nền dân chủ linh hoạt nhờ sự tham gia của chuyên gia và ủy quyền bỏ phiếu cũng như sự tham gia của cộng đồng.

Cũng cần lưu ý rằng kỹ thuật hệ thống ngân quỹ này có thể được sử dụng trên một số Blockchain khác ngoài Cardano. Trước đây, người ta đã đề xuất rằng nó nên được triển khai cho Ethereum Classic ⁶⁸⁸ và sau này chúng ta sẽ xem COTI tận dụng tính năng Catalyst Natives như thế nào. Các hệ thống kho bạc có thể hỗ trợ quá trình này bằng cách cho phép mọi người xem mạng sẽ phát triển như thế nào.

Sau khi thử nghiệm nhóm người dùng hạn chế thành công, Project Catalyst đã có thể truy cập được cho công chúng. Mặc dù quản trị trên chuỗi của Cardano vẫn còn ở giai đoạn sơ khai, nhưng tất cả các số liệu và chỉ số đều chỉ ra một tương lai tươi sáng với cộng đồng dẫn đầu.



Hình 63: Tổng quan về chất xúc tác

Có rất nhiều bộ phận chuyển động đến Catalyst. Hình ảnh này từ bài đăng trên blog của IOG *Project Catalyst - Một chu trình phát triển hệ sinh thái Cardano hiệu quả*⁶⁸⁹ là một bản tóm tắt tốt về các bước liên quan và mục tiêu cuối cùng.

Quỹ đầu tư của Catalyst

Vào tháng 9 năm 2020, IOG đã công bố thành lập quỹ công khai đầu tiên của Project Catalyst, một cột mốc quan trọng đối với Cardano về quản trị on-chain, ngân quỹ và đổi mới cộng đồng.

Quỹ đại chúng đã được ra mắt sau năm tháng hoạt động tích cực trên hai quỹ thí điểm trước đó. Thử nghiệm đầu tiên, có tên là 'Quỹ 0 đồng', được thực hiện với sự trợ giúp của một nhóm tập trung vào IOG. Fund1 là lần đầu tiên khái niệm này được chia sẻ với cộng đồng Cardano, tranh thủ sự trợ giúp của hơn 50 người để giúp IOG xây dựng nền tảng và quy trình. Mặc dù vòng bỏ phiếu này không cung cấp tài chính 'thực sự', nhưng đây là cơ hội quan trọng để nhóm IOG và cộng đồng Cardano thử nghiệm và nâng cao quy trình mới.

Có một chặng đường dài để đi. Tuy nhiên, với sự giúp đỡ của cộng đồng, IOG đã duy trì tốc độ thăng tiến ổn định. Nếu Fund1 là buổi thử trang phục, thì Fund0 là buổi chạy kỹ thuật. Fund2, được công bố vào tháng 9 năm 2020, là đêm khai mạc khi những người hoạt động hiệu quả nhất trong cộng đồng tranh giành tài chính để biến ý tưởng của họ thành hiện thực.

Tài trợ cho các đề xuất tuyệt vời

Nhóm tiên phong của IOG gồm 50 thành viên cộng đồng đã hỗ trợ họ xác định các lĩnh vực cần cải thiện để họ có thể xây dựng và nâng cao quy trình trước khi phổ biến rộng rãi hơn. Việc làm rõ các tài liệu và tiêu chuẩn đã khuyến khích các thành viên cộng đồng tham gia nhiều hơn và gửi đề xuất.

Để đạt được mục tiêu đó, IOG đã xây dựng một hướng dẫn để hỗ trợ bất kỳ ai tạo đề xuất tốt nhất có thể cho Fund2 và hơn thế nữa. Cộng đồng có thể truy cập ADA trị giá tới 250 nghìn đô la trong quỹ công khai đầu tiên.

IOG bắt đầu với quy mô nhỏ, yêu cầu cộng đồng trả lời tuyên bố thách thức: 'Làm cách nào chúng tôi có thể khuyến khích các nhà phát triển và doanh nhân tạo DApps và doanh nghiệp trên Cardano trong sáu tháng tới?' Các đề xuất tài trợ có thể giải quyết vấn đề này bằng nhiều khái niệm, bao gồm các chiến dịch tiếp thị và phát triển cơ sở hạ tầng, cũng như lập kế hoạch kinh doanh và sản xuất nội dung.

Bước đầu tiên là 'kiểm tra vấn đề', bao gồm hỏi các thành viên của cộng đồng về ý kiến đóng góp của họ. Sau đó, thông qua một cuộc trò chuyện Telegram đặc biệt kênh,⁶⁹⁰ IOG kêu gọi mọi người gửi ý tưởng của họ đến nền tảng đổi mới, nơi họ có thể hợp tác và tranh luận.

Công chúng bỏ phiếu

IOG đưa mọi thứ ra biểu quyết sau các giai đoạn động não, hợp tác và đề xuất. Các đề xuất được đánh giá trên IdeaScale hoặc thông qua ứng dụng bỏ phiếu trên thiết bị di động. Khi đến thời điểm bỏ phiếu, mọi người đã đăng ký bỏ phiếu bằng ứng dụng bỏ phiếu. 'Quyền' bỏ phiếu của mỗi người tham gia được kết nối với cổ phần ADA của họ và việc bỏ phiếu sẽ mang lại cho họ thêm phần thưởng ADA. Bỏ phiếu hoạt động tương tự như một 'giao dịch', cho phép tất cả những người tham gia bỏ phiếu để nói 'có' hoặc 'không'.

Cho đến Fund10, Catalyst đã được triển khai như một sự kết hợp của các thành phần on-chain và off-chain. Các đề xuất tồn tại trên IdeaScale, có một trung tâm bỏ phiếu trong ví Daedalus, ứng dụng bỏ phiếu trên android và iphone và sự phụ thuộc vào Node Jormungandr⁶⁹¹ được tái sử dụng (trước đây được sử dụng cho Mạng thử nghiệm được khuyến khích). Khi kỷ nguyên Voltaire mở ra, trải nghiệm bỏ phiếu sẽ chuyển sang ví nhẹ mới của IOG là Lace (lace.io), được bổ sung bởi một trang web mới, projectcatalyst.io.

Làm thế nào nó hoạt động

⁶⁸⁹

Tim Richmond, 'Project Catalyst - Một chu trình phát triển hệ sinh thái Cardano hoàn hảo', iohk.io/en/blog/posts/2022/05/10/project-catalyst-a-virtuous-cycle-of-cardano-ecosystem-development- đầu tư vào những ý tưởng tuyệt vời để tạo ra những thay đổi tích cực trong thế giới thực/
⁶⁹⁰

Kênh Telegram của Catalyst, [t.me/ cardanocatalyst](https://t.me/cardanocatalyst)

⁶⁹¹ Node Jormungandr, github.com/input-output-hk/jormungandr/blob/master/CHANGELOG.md

Voltaire là một thành phần quan trọng của hệ sinh thái Cardano vì nó cho phép mọi chủ sở hữu ADA tham gia vào các lựa chọn về sự phát triển trong tương lai của nền tảng và đóng góp vào sự phát triển của hệ sinh thái. Project Catalyst là bước quan trọng đầu tiên để đạt được năng lực như vậy.

Chương trình khởi nghiệp đầu tiên do Catalyst tài trợ, có tên là *BoostCamp*,⁶⁹² đã sử dụng Entrepreneurdy (entrepreneurdy.com) nền tảng cho phép các doanh nghiệp tham gia vào các phiên nhằm phát triển chiến lược công ty của họ.



Hình 64: Chất xúc tác 'đây là cách nó hoạt động'

Vào tháng 9 năm 2020, Catalyst lần đầu tiên bắt đầu hành động với Fund2.⁶⁹³ Hàng nghìn cá nhân đã tham gia cùng nhau để sản xuất, tinh chỉnh và ưu tiên tài trợ cho các ý tưởng để đưa Cardano tiến lên. Fund3 bắt đầu hoạt động vào tháng 1 năm 2021 và với mỗi quỹ, IOG muốn phát triển cộng đồng Catalyst bằng cách khuyến khích nhiều cá nhân tham gia hơn.

Mỗi vòng tài trợ bắt đầu với một loạt các mục tiêu. Mỗi thử thách tượng trưng cho 'ý định' của cộng đồng Cardano, một mục tiêu chung cần hoàn thành. IOG thích nói về 'hoàn vốn theo ý định' như một phương tiện để theo dõi sự thành công của dự án. Mỗi thử thách được thiết kế đủ rộng để gọi ra cả ý tưởng kỹ thuật và ý tưởng chung trong khi vẫn tập trung.

Fund2 có quỹ ADA trị giá 250.000 đô la, trong khi Fund3 tăng gấp đôi số đó, trao 500.000 đô la ADA cho những người đề xuất, cử tri và cố vấn cộng đồng. Quy mô, số tiền và sự tham gia của cộng đồng đều tăng lên theo mỗi chu kỳ cấp vốn. Trên nền tảng đổi mới IdeaScale vào tháng 2 năm 2021, đã có 7.000 thành viên và 1.800 cử tri tích cực. Việc áp dụng đã tăng 10% mỗi tuần.

Fund4 là vòng tham vọng và dễ tiếp cận nhất, cũng như vòng đầu tiên trị giá hàng triệu đô la — quỹ ADA được sử dụng để tài trợ cho các sáng kiến phát triển Cardano. Khoản tài trợ được các nhóm đề xuất sử dụng để tạo công cụ, xây dựng DApps, thiết lập các nỗ lực đào tạo và giáo dục nhà phát triển, v.v.

IOG tiếp tục cung cấp dự án nhiều hơn cho cộng đồng Cardano trong năm 2021 để thúc đẩy sự tham gia. Đăng ký cử tri tăng lên đáng kể. Trong một trung tâm đăng ký được thiết kế lại, việc đăng ký hiện đã được kết nối hoàn toàn với ví Daedalus.

Người dùng ví Yoroi lite có thể dễ dàng đăng ký thông qua plugin trình duyệt. Sau đó, cử tri có thể hoàn tất quy trình bằng ứng dụng bỏ phiếu trên thiết bị di động cụ thể, có thể tải xuống ứng dụng này trên iOS hoặc Android. Người dùng cũng có thể đăng ký và bỏ phiếu từ ví của họ trong Daedalus. Project Catalyst đã vươn lên trở thành tổ chức tự trị phi tập trung (DAO) lớn nhất thế giới trong vòng chưa đầy sáu tháng.

⁶⁹²

Project Catalyst Fund6 tòa thị chính hàng tuần và Q&A #13 tháng 11 năm 2021, youtube.com/watch?v=x8134D_Ip9o&t=418s

⁶⁹³

Tiến sĩ Dor Rác rười, 'Chất xúc tác dự án; giới thiệu quỹ công khai đầu tiên của chúng tôi cho đổi mới cộng đồng Cardano', iohk.io/en/blog/posts/2020/09/16/project-catalyst-introducing-our-first-public-fund-for-cardano-community-innovation/

vòng xúc tác

Khi Fund4 kết thúc vào tháng 7 năm 2021, Catalyst đã chứng tỏ mình là trung tâm một cửa cho tinh thần đồng đội và đổi mới phi tập trung. Tuy nhiên, sự mở rộng nhanh chóng này kéo theo những trở ngại mới.

Dự án Catalyst đã thu được sự đóng góp từ các nhóm chức năng ngày càng khác nhau, những người đang giúp đưa trí tuệ tập thể phát triển. Cụ thể, cố vấn cộng đồng, người đề xuất được tài trợ, SPO (SPO), nhà sản xuất công cụ & người bảo trì, tất cả những người đóng góp vào sự thành công và mở rộng của Catalyst, cũng như thành công của Cardano.

Project Catalyst thu được lợi ích từ sự đa dạng mở rộng này vì nó cho phép hình thành nhiều ý tưởng và đề xuất hơn nữa. Nó cũng làm cho việc giao tiếp giữa tất cả các nhóm này trở nên khó khăn hơn. Mọi nhóm đều muốn được lắng nghe, những suy nghĩ và mối quan tâm của họ cần được đưa ra ở cấp độ dự án.

Những nhóm này cần đại diện và lãnh đạo đáng tin cậy để biện hộ cho họ. Ảnh hưởng của Project Catalyst sẽ bị suy giảm nghiêm trọng nếu sự đại diện đó không đầy đủ hoặc không tồn tại. Đây là lý do tại sao Catalyst Circle được tạo ra.

'Mạng cảm biến con người'

IOG mô tả Catalyst Circle là một "mạng cảm biến con người" đóng vai trò là cơ quan đại diện cho tất cả những người tham gia Project Catalyst. Circle theo dõi trạng thái hiện tại của Catalyst và các ý định quản trị trong tương lai. Trong hệ sinh thái Catalyst, nó xác định và thảo luận các vấn đề, phản đối và khả năng. Ví dụ: Vòng kết nối có thể tranh luận về số tiền được phân phối cho quỹ, các điều chỉnh hoặc điều kiện đối với các thông số khuyến khích, API Catalyst, v.v.

Hoạt động này sẽ cung cấp thông tin chi tiết về những hy vọng, mong muốn, nhu cầu và lo lắng của cộng đồng bên trong Project Catalyst bằng cách ghi lại các cuộc họp và thu thập các hoạt động trong hồ sơ tồn đọng dành cho mọi người.⁶⁹⁴ Circle cũng chịu trách nhiệm lựa chọn hình thức tương lai của riêng mình và thiết kế các thủ tục bầu chọn Circle.

Circle tồn tại để đạt được bốn mục tiêu chính:

- Để giúp các nhóm chức năng khác nhau giao tiếp với nhau dễ dàng hơn.
- Để cung cấp cho mọi người thông báo khi dòng được vượt qua
- Đề xuất cải tiến cho các kế hoạch và quy trình của Project Catalyst
- Xác định quy trình bầu chọn Vòng kết nối.

thành viên được bầu

Circle, giống như Project Catalyst, sẽ phát triển và thay đổi theo thời gian. Ban đầu, các thành viên được bầu sẽ phục vụ nhiệm kỳ ba tháng, với các cuộc bầu cử tiếp theo để cải thiện và lặp lại quy trình. Các nhiệm vụ và nghĩa vụ cơ bản này đã được cụ thể hóa cho các thành viên được bầu. Mỗi thành viên nên:

- Đại diện cho những người đã chọn họ
- Sử dụng phán đoán tốt nhất của họ khi nói đến các chủ đề trước Vòng tròn
- Giáo dục các thành viên khác về các sáng kiến, hoạt động, mục tiêu, ước mơ và mối quan tâm của cộng đồng họ
- Tận dụng các cơ hội để kết hợp các khuyến nghị chính sách vào chương trình nghị sự của Circle để thảo luận một cách thường xuyên
- Thông báo cho cộng đồng của họ về những nỗ lực của Circle.

Mỗi thành viên trong nhóm dự kiến sẽ:

- Tham dự các cuộc họp định kỳ hai tuần một lần
- Giữ một hồ sơ tồn đọng nhanh nhẹn để theo dõi các mối quan tâm giữa các phiên
- Xem xét và nhận xét về các mục trong chương trình nghị sự trước thời hạn
- Vẫn được thông báo về lợi ích và mối quan tâm của cộng đồng của họ
- Phân phối kết quả đầu ra của Circle một cách rõ ràng và dễ tiếp cận
- Học tập và thực hành quy trình cuộc họp tốt
- Tạo một giấy giao thức cho các cuộc bầu cử tiếp theo
- Tham gia các hội thảo đào tạo về lãnh đạo khởi nghiệp toàn diện và tinh gọn
- Cung cấp nhận xét về hiệu quả của Circle.

⁶⁹⁴

khai mạc bầu cử

IOG đã tổ chức cuộc bầu chọn đầu tiên vào tháng 7 năm 2021 cho các thành viên Catalyst Circle trên toàn cầu. Các thành viên sẽ có thể thiết lập chương trình nghị sự cho mỗi cuộc họp và gửi các khuyến nghị chính sách cho Catalyst Circle để xem xét một cách thường xuyên. Phiên bản khởi động là "nhóm chức năng tối thiểu", dựa trên các cuộc trò chuyện với các nhà lãnh đạo cộng đồng Catalyst và Governance Alive (governancealive.com), một nhóm chuyên gia trong lĩnh vực cấu trúc quản trị mới.

Vòng kết nối có thể mở rộng và phân chia khi các phương pháp hay nhất được thiết lập. Cuối cùng, các thành viên sẽ giúp IOG đạt được mục tiêu hợp pháp hóa chính phủ phi tập trung, mở đường cho một giải pháp thay thế khả thi cho hiện trạng và tạo ra bước đột phá mới trong việc phát triển quản trị Blockchain.

Vào tháng 12 năm 2022, Catalyst Circle V3.5 đã yêu cầu DripDropz (dripdropz.io) thực hiện một cuộc bỏ phiếu trực tuyến cho năm đại diện mới của Vòng kết nối V4. Ba mươi ứng viên đã nộp đơn. Bạn có thể theo dõi những tin tức mới nhất trên blog của họ.⁶⁹⁵

Chất xúc tác bản địa

Như là một phần của chất xúc tác dự án,⁶⁹⁶ chương trình thử nghiệm Catalyst Natives đầu tiên đã được ra mắt vào cuối năm 2021. Catalyst Natives cho phép mọi dự án khai thác trí tuệ tập thể của cộng đồng để giải quyết các thách thức kinh doanh và thuê ngoài dự án. Catalyst Natives cung cấp dịch vụ quản lý quỹ đối mới phi tập trung cho các đối tác, một số bên ngoài Cardano, nhằm mục đích phát triển hệ sinh thái của họ bằng cách khuyến khích các nhà đổi mới hỗ trợ tìm giải pháp cho các vấn đề.

COTI, Catalyst Native đầu tiên

Catalyst Natives mở rộng quyền truy cập vào Project Catalyst cho các tổ chức bên ngoài hệ sinh thái Cardano giờ đây có thể đưa ra các thách thức, đồng thời đưa ra các khuyến khích và phần thưởng cho những cá nhân đáp ứng thành công thách thức với những đổi mới được đề xuất của họ.

COTI đã mang đến cho cộng đồng một thách thức công nghệ mới trong thí điểm này. Bằng cách thêm một trình cắm vào trang web của họ, bất kỳ doanh nghiệp vừa và nhỏ nào sử dụng các nền tảng như Shopify và WooCommerce đều có thể tận dụng các phương pháp mới và sáng tạo để chấp nhận thanh toán ADA với tích hợp liền mạch.

Sau quá trình thử nghiệm, IOG cho phép Catalyst Native chấp nhận nhiều thử thách hơn từ các thực thể khác; tuy nhiên, những thách thức này được IOG lựa chọn, trong giai đoạn đầu tiên, để đảm bảo chúng mang lại giá trị cho hệ sinh thái Cardano. Các tổ chức đề xuất các thách thức thông qua Người bản địa sẽ tài trợ cho những ý tưởng đó, do đó Người bản xứ Catalyst sẽ không sử dụng quỹ Kho bạc Cardano để thanh toán cho các sáng kiến đã được bình chọn thành công. COTI đã phân phối 100 nghìn đô la dưới dạng Token COTI cộng với phí trong Fund7, số tiền này ngoài quỹ 8 triệu đô la ADA.

Catalyst Natives là cơ hội để các doanh nghiệp thuộc mọi quy mô tiếp cận với kho ý tưởng và những người có thể giúp họ hiện thực hóa chúng. Catalyst Natives hiện đang hướng tới việc hỗ trợ các đối tác trong hệ sinh thái Cardano và các dự án Token nội dung gốc, xử lý các điểm khó khăn cụ thể mà họ không có tài nguyên hoặc đơn giản là không có giải pháp và thuê ngoài chúng như những thách thức của Catalyst để những người đề xuất giải quyết.

Dan Friedman, cố vấn chiến lược⁶⁹⁷ của IOG 'OG' và Ergo đã thông báo về bản cập nhật Ergo⁶⁹⁸ rằng Ergo đang lên kế hoạch trở thành Catalyst 'Native' tiếp theo. Bất kỳ ai quan tâm đến Catalyst Natives đều có thể đăng ký tại đây.⁶⁹⁹

quỹ sau này

Mỗi chu kỳ quỹ Catalyst đều mang lại những thành tựu mới, đáng chú ý. Fund7 cũng không khác.

⁶⁹⁵

Bỏ phiếu Catalyst Circle v4, news.dripdropz.io/catalyst-circle-v4-voting-c8863e5697d6

⁶⁹⁶

Đưa con triệu đô của chúng tôi: Project Catalyst, iohk.io/en/blog/posts/2021/02/12/our-million-dollar-baby-project-catalyst/

⁶⁹⁷

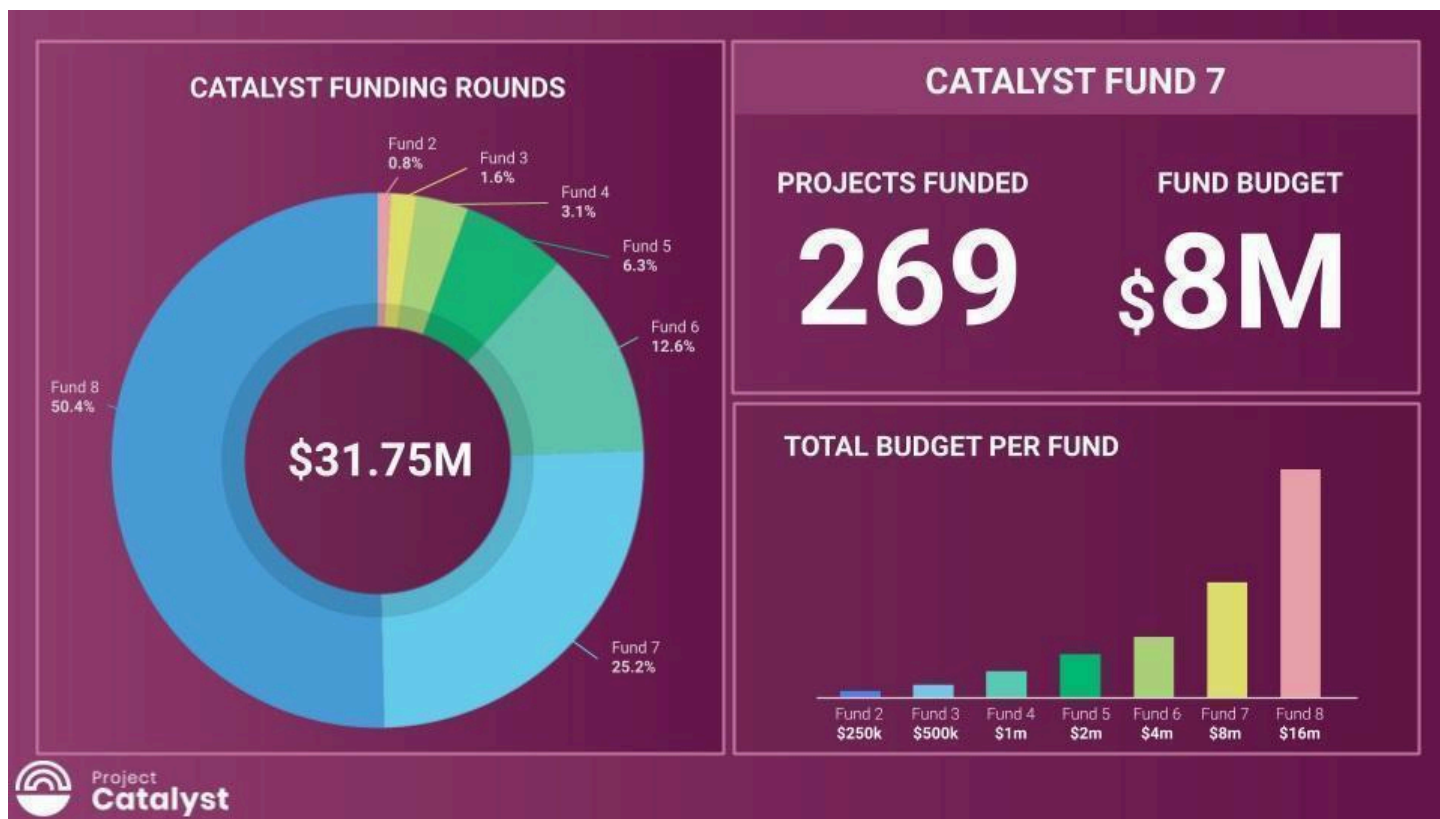
Daniel Friedman, iohk.io/en/team/daniel-friedman

⁶⁹⁸

Cập nhật hàng tuần & AMA - ngày 22 tháng 4 năm 2022, youtube.com/watch?v=rPBZwEPk5Q8

⁶⁹⁹

Ứng dụng Catalyst Natives, Forms.gle/BA8LmtrAWWmHHcY59



Hình 65: Số liệu thống kê của Fund7

Sau khi các phiếu bầu được lập bảng và đếm trong Fund7, 269 sáng kiến bổ sung⁷⁰⁰ đã được chọn để nhận được ADA. Cho rằng mỗi dự án này được tạo ra để giải quyết 24 vấn đề trong thế giới thực do cộng đồng Cardano cung cấp, cũng như một nhiệm vụ bổ sung do COTI, nhà tiên phong Catalyst Native đầu tiên của Cardano đưa ra, đây là những con số ấn tượng.

Khoảng thời gian này, hơn 52.500 ví đã đăng ký bỏ phiếu và các cổ vấn cộng đồng đã xem xét hơn 900 đề xuất để giúp cử tri đưa ra những đánh giá sáng suốt. Số lượng ý tưởng được tài trợ bởi Kho bạc Cardano đã tăng gần gấp bốn lần trong một khoảng thời gian ngắn, đạt 575 dự án.

Kho bạc Cardano hiện chứa khoảng 800 triệu ADA để duy trì và xây dựng hệ sinh thái. Nhiều dự án được tài trợ trong các vòng trước hiện đã được hoàn thành và các sản phẩm cuối cùng của họ đang được trưng bày.⁷⁰¹

quỹ8

Ba tháng một lần, một chiến dịch quỹ đổi mới Project Catalyst mới sẽ khởi động, mang đến cơ hội nhận tài nguyên từ Kho bạc Cardano y . Fund8 đã cung cấp khoản tài trợ 16 triệu đô la trong ADA.

Cộng đồng Catalyst đã thành lập và thống nhất về từng nhiệm vụ trong Fund8. Mục tiêu là gì? Trong kiến trúc nguồn mở của Cardano, để tăng tốc hệ sinh thái DApp và nhà phát triển. Nền tảng & Phát triển Hệ sinh thái Cardano, Phát triển Cộng đồng, Tiếp cận & Áp dụng, Nhận dạng & Khả năng tương tác, và Cải tiến Chất xúc tác Dự án nằm trong số 23 thách thức.

Các đề xuất bao gồm các ứng dụng tài chính phi tập trung (DeFi) sáng tạo nhằm giảm bất bình đẳng tài chính và RealFi , giúp loại bỏ các rào cản khỏi hoạt động kinh tế trong thế giới thực và cung cấp cho mọi người các sản phẩm tài chính rẻ hơn. Ví dụ, các dự án sản xuất tập thể (wayacollective.com) được điều hành bởi các doanh nhân và nhân viên châu Phi.

⁷⁰⁰

Tài trợ cho 7 sáng kiến, drive.google.com/file/d/193GZulHuk0zhpTrMiLhcNC4OeEMoRyIa/view

⁷⁰¹

Kết quả của Fund8⁷⁰² xác nhận động lực không ngừng tăng lên khi tỷ lệ bỏ phiếu tăng lên và một loạt các dự án đã được tài trợ. Một trong những số tiền nhỏ nhất được yêu cầu và tài trợ, cũng là một trong những số tiền quan trọng nhất. Đề xuất thành công của Sebastien Guillemot⁷⁰³ có nghĩa là anh ấy là biên tập viên CIP đầu tiên được trả tiền cho thời gian của mình. Nhiều biên tập viên khác theo sau, đóng vai trò là người quản lý quy trình CIP.

Catalyst cũng hợp tác với Financial Times và Seedstars (seedstars.com) để khởi động *Thử thách Blockchain FT x Cardano* nơi các công ty khởi nghiệp được chọn tham gia Bootcamp 3 ngày và kết nối với mạng lưới cố vấn của Seedstars. 24 công ty khởi nghiệp đã được chọn để tham gia Chương trình tăng tốc kéo dài 3 tháng.⁷⁰⁴ Thông tin chi tiết có trên trang web của Seedstar.

Ngày 21 tháng 4 năm 2019... Ai trả tiền? Ai quyết định? CH:⁷⁰⁵

Đây là lý do tại sao việc bạn có một hệ thống ngân quỹ... và hệ thống bỏ phiếu lại cực kỳ quan trọng bởi vì hiện tại đây là cách không gian Crypto hoạt động và đây là lý do tại sao mọi thứ trở nên độc hại như vậy.... bạn có một nhóm rất nhỏ những người là nhà phát triển, nhà đầu tư, những người lớn đang thực sự xây dựng công cụ trong không gian, tầng lớp doanh nhân, tầng lớp nhà phát triển, tầng lớp cơ sở hạ tầng... sau đó bạn có những nhà đầu cơ là tất cả những người khác... và họ nắm giữ tiền tệ, họ hâm mộ nó, thậm chí có thể phù hợp với nó về mặt triết học ...nhưng họ không có tiếng nói, họ không thể làm gì... họ chỉ ngồi đó và chỉ mong mọi thứ thành hiện thực.

....và sau đó một nhóm nhỏ trong số họ có thể chuyển sang lớp khác khi họ có hợp đồng thông minh hoặc bất cứ thứ gì... nhưng phần lớn trong số họ vẫn ở đó nhưng họ có ý kiến về việc mọi thứ nên đi về đâu... họ nên làm gì... và vì vậy điều quan trọng là cung cấp cho họ công cụ để tổ chức... công cụ để bầu cử... công cụ để thảo luận về triết lý và phương hướng ...có ý thức, không chỉ 'đây là ý kiến của tôi', mà còn khi ý kiến của tôi được thể hiện và nhận được sự đồng thuận dân chủ đằng sau nó ...thì ý kiến đó sẽ biến thành tiền... mà sau đó tầng lớp kia có thể sử dụng.

Đột nhiên, mọi người đều có quyền lực và thực sự có tiếng nói ..và một ý kiến và bạn không chỉ nói về việc khi nào nó sẽ ra mắt, hoặc nó sắp ra mắt là gì... bạn thực sự đang nói về việc chúng ta sẽ ở đâu muốn đi, và chúng ta sẽ đến đó bằng cách nào và những việc chúng ta cần làm để đến đó... ai là người lãnh đạo tốt nhất để đến đó... bạn không thể rẽ nhánh như vậy.... bạn có thể phân nhánh mã và có một hệ thống Kho bạc khác ...nhưng nó giống như nói tốt rằng nhóm gặp gỡ lớn ở đằng kia... Tôi sẽ tổ chức nhóm gặp mặt của riêng mình và tôi sẽ sao chép mọi thứ... cùng các biểu ngữ và cùng một dịch vụ ăn uống và mọi thứ giống nhau... không có nghĩa là những người khác sẽ xuất hiện

Quỹ Cardano

cFund, lần đầu tiên được công bố tại hội nghị thượng đỉnh Shelley năm 2020, là một quỹ đầu tư giai đoạn đầu tập trung vào các công ty sáng tạo trên Cardano. Wave Financial, phối hợp với IOG, quản lý cFund, một quỹ phòng hộ dựa trên Crypto. Quỹ sử dụng phương pháp tiếp cận mạo hiểm giai đoạn đầu để đầu tư vào các công ty công nghệ sáng tạo đang xây dựng các ứng dụng, dịch vụ và sản phẩm dựa trên Cardano, cũng như các dự án R&D khác mà IOG đang thực hiện.

Chữ 'c' trong quỹ c

Chữ 'c' trong tên liên quan đến từ toán học 'hệ số', dùng để chỉ hệ số nhân của một biến. cFund được định vị để mang lại hiệu ứng cấp số nhân về mặt tăng trưởng và khả năng tiếp cận cho các công ty trong danh mục đầu tư của mình bằng cách sử dụng kiến thức chủ đề của IOG và Wave Financial cũng như các mối quan hệ trong ngành.

Dịch vụ cung cấp

cFund đóng vai trò là nhà cung cấp vốn, cố vấn và đối tác cho các công ty danh mục đầu tư của mình và hệ sinh thái Cardano lớn hơn. cFund cung cấp quyền truy cập và định hướng cho danh mục đầu tư của mình bằng cách sử dụng các tài nguyên, danh tiếng, kiến thức và mạng của IOG và Wave Financial. cFund rất tin tưởng vào việc gia tăng giá trị cho các khoản đầu tư của mình và cố gắng trở thành bên đỡ đầu tiên cho các nhóm quản lý.

⁷⁰²

Kết quả quỹ 8, drive.google.com/file/d/1s3jCE7pmoUjy3ASMia-UhFl2KLi_hnf/view

⁷⁰³

Biên tập viên CIP được tài trợ, twitter.com/SebastienGillmt/status/1525139808926191618

⁷⁰⁴

'Thử thách Blockchain FT x Cardano', seedstars.com/community/entrepreneurs/programs/ft-cardano-blockchain-challenge/

⁷⁰⁵

Bản tóm tắt sau hội nghị, suy nghĩ và AMA 21/04/2019, youtu.be/pBXZVrBQ6U8?t=5003

Theo triết lý nền tảng của IOG về 'sự gián đoạn theo tầng', ⁷⁰⁶ hầu hết các cấu trúc tạo nên các hệ thống tài chính, quản trị và xã hội toàn cầu vốn đã không ổn định và những xáo trộn nhỏ có thể tạo ra hiệu ứng gợn làm cấu hình lại hệ thống một cách triệt để. Mục đích của cFund là tìm kiếm và tài trợ cho các giải pháp mang lại sự khác biệt này một cách công bằng và minh bạch cho tất cả những người tham gia. Trong khi các loại Crypto khác ⁷⁰⁷ có mối quan hệ chặt chẽ với Thung lũng Silicon, Cardano đang đổi mới với Catalyst đóng vai trò là Quỹ VC 'được tích hợp sẵn' của riêng mình.

COTI, mạng thanh toán phi tập trung và có thể mở rộng cho lĩnh vực thương mại điện tử, là khoản đầu tư đầu tiên của cFund vào lĩnh vực này.

Một ví dụ khác là Occam.Fi, một bộ giải pháp DeFi được tối ưu hóa cho Cardano. Sản phẩm ban đầu của họ là một nền tảng tài chính phi tập trung. Thế hệ ứng dụng DeFi tiếp theo sẽ có thể huy động vốn bằng cách sử dụng Blockchain Cardano nhờ bộ phóng này.

Ngày 16 tháng 10 năm 2020. Có rất nhiều quỹ khác nhau, vậy bạn có thể giải thích cho chúng tôi biết quỹ DC, cFund và quỹ Cardano Foundation là gì không? CH.⁷⁰⁸

Vì vậy, quỹ DC là cái mà chúng tôi gọi là quỹ đến từ Catalyst... và đó là những mô hình tài trợ... Cardano không có đại lý, vì vậy chúng tôi không thể sở hữu đất đai, nó không thể có tài sản trí tuệ... nó không thể có vốn chủ sở hữu, những thứ như thế này... vì vậy khi nó tài trợ... Giống như khi Quỹ khoa học quốc gia (NSF) tài trợ, hoặc DARPA tài trợ... nơi nó tài trợ cho sự phát triển của một thứ gì đó bởi vì chúng tôi, với tư cách là ⁷⁰⁹ một xã hội, đã xác định rằng đó là một ý tưởng tốt.

Vì vậy, ví dụ khi NSF đưa ra nghiên cứu về vật lý lý thuyết... nó nói rằng chúng ta, với tư cách là một xã hội, muốn nhà vật lý lỗi lạc của chúng ta được tài trợ tốt để họ có thể tìm ra cách thức hoạt động của thời gian và lực hấp dẫn, v.v... nhưng không có tiền mà ra khỏi đó... hoặc những thứ này nhưng có lợi ích xã hội, có khả năng được tận dụng theo thời gian để làm cho đất nước tốt đẹp hơn... Có lẽ chúng ta phát minh ra phân trọng lực vào một lúc nào đó.... nhưng nó không phải là mục tiêu chính.

Vì vậy, chúng tôi nhìn vào quỹ DC như thế.... nơi chúng tôi nói đó là 'hoàn vốn theo ý định'. Các khoản tài trợ đang được thông qua và mục tiêu là làm cho Cardano trở nên tốt hơn.... nhưng không phải để biến Bob thành triệu phú, hay đại loại như thế...

cFund là một nhánh đầu tư mạo hiểm của công ty tôi và Waves ⁷¹⁰... chúng tôi đang làm việc cùng nhau và thiết lập tất cả những thứ đó và về cơ bản, đó sẽ là nơi bạn điều hành một dự án và bạn đến gặp Charles và những người khác có liên quan đến dự án đó... bạn nói, 'Tôi muốn bạn đầu tư vào công ty của tôi... và cung cấp cho tôi những nguồn lực tôi cần để đưa nó lên một tầm cao mới.... và sau đó chúng tôi sẽ nhìn bạn giống như bất kỳ nhà đầu tư mạo hiểm nào sẽ nhìn bạn.... hỏi bạn những câu tương tự Andreessen Horowitz (a16z.com) sẽ hỏi bạn, hoặc Kleiner Perkins (kleinerperkins.com) sẽ hỏi bạn, v.v... và nếu chúng tôi xác định đó là một khoản đầu tư tốt, tôi sẽ mở sổ séc và cắt một tấm séc và gửi theo cách của bạn và chúng tôi sẽ nhận lại vốn chủ sở hữu cho khoản đó, bởi vì đó là một khoản đầu tư tư nhân.

Sau đó, Cardano Foundation, họ có một thứ gọi là CCCI, Cơ sở hạ tầng quan trọng về mặt thương mại của Cardano... và điều đó nói rằng cần phải có một số xác nhận và khởi động sản phẩm, Cardano thực sự có khả năng cạnh tranh hoặc có khả năng làm những việc mà Ethereum, EOS, Tezos và Algorand làm.

Vì vậy, chúng tôi sẽ đưa ra một số khoản tài trợ rất cụ thể được nhắm mục tiêu để giúp hệ sinh thái phát triển... được rồi Quỹ DC, cộng đồng chịu trách nhiệm về điều đó... các khoản tài trợ từ Quỹ (Cardano), Quỹ chịu trách nhiệm về điều đó và họ rất hướng tới việc bắt kịp chúng tôi và đưa chúng tôi đến nơi chúng tôi cần đến để cạnh tranh với Ethereum và phần còn lại của nhóm... và cFund là một khoản đầu tư cổ điển tốt cho những thứ mà tôi nghĩ chúng tôi nên có trong hệ sinh thái của mình.

⁷⁰⁶

Cardano | Quân domino đầu tiên, youtube.com/watch?v=W7gGO058rtU

⁷⁰⁷

Công ty khởi nghiệp Crypto Solana huy động được 314 triệu đô la để phát triển Blockchain nhanh hơn, wsj.com/articles/crypto-startup-solana-raises-314-million-to-develop-faster-blockchain-11623240001

⁷⁰⁸

Giám đốc điều hành Entrevista IOG Charles Hoskinson e Maria Carmo #Cardano #ADA Delegate với CARDS hoặc @cardanistas,youtu.be/rHu6oLTZ7kI?t=3061

⁷⁰⁹

DARPA : The Defense Advanced Research Projects Agency là cơ quan nghiên cứu và phát triển của Bộ Quốc phòng Hoa Kỳ chịu trách nhiệm phát triển các công nghệ mới nổi để quân đội sử dụng

⁷¹⁰

Waves, everipedia.org/wiki/ lang_en /waves-cryptocurrency

dRep

IOG đã giới thiệu khái niệm ủy quyền quyền biểu quyết của bạn cho Đại diện được ủy quyền (dReps) và kêu gọi những người quan tâm đăng ký tại Tòa thị chính Catalyst Dự án Fund8.⁷¹¹

Sự phát triển liên tục này của hệ sinh thái Cardano là một tin tuyệt vời nhưng mặt khác, lại gây ra một vấn đề. Cộng đồng có nghĩa vụ kiểm tra và bỏ phiếu cho các ý tưởng tăng lên khi số lượng đề xuất tăng lên. Cần có một cách tiếp cận mới để đảm bảo rằng tất cả các ý tưởng đều nhận được sự quan tâm xứng đáng, cũng như để hỗ trợ sự phát triển hơn nữa.

Chủ sở hữu ADA có thể bỏ phiếu cho một hoặc nhiều dRep thông qua ủy quyền. Điều này mang lại cho cử tri thụ động hơn cơ hội được lắng nghe tiếng nói của họ, nhưng giờ đây, số lượng đề xuất lớn hơn mức họ có thể đọc và đánh giá cá nhân.

Các dRep này sẽ bỏ phiếu cho hầu hết các đề xuất của Project Catalyst, cải thiện chất lượng của việc ra quyết định trong mỗi Quỹ. dReps sẽ cộng tác để phát triển chính sách, thu thập và đánh giá dữ liệu, tham khảo ý kiến của các chuyên gia và cuối cùng là bỏ phiếu cho nhiều sáng kiến và vấn đề do cộng đồng đề xuất. IOG đang thu hút sự quan tâm đến việc tham gia nhóm dRep đầu tiên để thúc đẩy sự hòa nhập và đa dạng. Nếu muốn tham gia, bạn có thể tham gia cùng những người tiên phong dRep tại đây.⁷¹²

quỹ9

Động lực không ngừng giống như Borg của Catalyst tiếp tục với việc khai trương Fund9 vào tháng 6 năm 2022. Thường có điều gì đó mới mẻ và sáng tạo với sự xuất hiện của mỗi quỹ và lần này Cardashift⁷¹³ đã tham gia chương trình Catalyst Natives.⁷¹⁴ Thách thức của họ dựa trên việc tạo ra giá trị thông qua các dự án định hướng tác động tích cực. Cardashift liệt kê thông tin đăng nhập 'xanh' của Cardano, nó tập trung vào Châu Phi và bản chất quyết định của nó trong số các lý do họ hợp tác với Catalyst trong bài đăng trên blog trung bình của họ.⁷¹⁵ Như với mọi quỹ hàng quý, phần thưởng cho các đề xuất thành công tăng lên. Hướng dẫn ra mắt Fund9⁷¹⁶ đã phác thảo cách phân bổ 16 triệu ADA.

Tạm dừng chiến thuật cho Catalyst

Mặc dù Catalyst đã thành công rực rỡ về nhiều mặt, nhưng nó không hoàn hảo. Cũng có những câu hỏi⁷¹⁷ được đặt ra cho người chiến thắng Fund6 Cardax DEX sau khi ra mắt trên Milkomeda (dcSpark's Cardano Sidechain) thay vì chuỗi chính Cardano như đề xuất ban đầu.

Đã có những lời bất mãn âm ỉ khi một trong số 205 người chiến thắng của Fund9 là một đề xuất gây tranh cãi có tên là *Daedalus Turbo* . Tuyên bố vấn đề của đề xuất đọc:

Daedalus, ví Cardano phi tập trung, rất chậm, mất cả ngày để đồng bộ hóa ban đầu và hàng giờ để đồng bộ hóa lại khi chỉ thỉnh thoảng được sử dụng—một ấn tượng không tốt về Cardano đối với người dùng mới.

⁷¹¹ Ra mắt Project Catalyst Fund8 - Town Hall #1 tháng 2 năm 2022, youtube.com/watch?v=rNZJvzjgduM

⁷¹² Catalyst dRep , bit.ly/3rSyHvP

⁷¹³ **Cardashift** là bộ phóng do cộng đồng điều hành nhằm gây quỹ, xây dựng và thúc đẩy các công ty khởi nghiệp đang giải quyết các vấn đề xã hội và môi trường.

⁷¹⁴ Fernando Sanchez, 'Giới thiệu chất xúc tác bản địa - Cách mọi doanh nghiệp có thể tận dụng công cụ đổi mới Cardano', iohk.io/en/blog/posts/2021/11/10/introducing-catalyst-natives-how-any-business-can-leverage-the-cardano-innovation-engine

⁷¹⁵ 3 lý do tại sao chúng tôi chọn Cardano để tối đa hóa tác động của mình, cardashift.medium.com/the-3-reasons-why-we-choose-cardano-to-maximize-our-impact-28b2e914e894

⁷¹⁶ Hướng dẫn ra mắt Fund9, drive.google.com/file/d/1kJ8F6doXUIJQRiA5pmSMxXc9feVfF21y/view

⁷¹⁷@ câu hỏi cwpaulm CardaxDEX , twitter.com/cwpaulm/status/1597666144059432960?s=20&t=HBr5f_ZkSoMQ4rzv0eIdOA



Rick McCracken DIGI ✓
@RichardMcCrackn

wtf is Daedalus Turbo?

3:49 PM · Sep 27, 2022

Hầu hết người dùng Cardano cảm thấy buồn vì số tiền được thưởng quá lớn, trong khi các dự án khác lại bị bỏ lỡ. Bất kỳ ai tiến hành 'phân tích lỗ hổng' cơ bản, như SPO Rick McCracken đã tweet, ⁷¹⁸có thể sẽ đi đến cùng một kết luận rằng dự án không kịp thời vì nhiều năm nghiên cứu và phát triển sản phẩm đã được dành cho Mithril. Đối với bất kỳ ai theo dõi Cardano, ví dụ *Lace* (lace.io) của IOG đã được ưu tiên hơn Daedalus trong một thời gian.

Từ góc độ trải nghiệm người dùng, nhiều người cảm thấy choáng ngợp khi cố gắng theo dõi hơn một nghìn đề xuất cho một quỹ nhất định trên IdeaScale. Nhiều dự án hứa hẹn đã không được tài trợ. Nó thường được cộng đồng hoan nghênh khi IOG thông báo 'hết thời gian chờ' cho Catalyst trong một bài đăng trên blog vào tháng 11 năm 2022.⁷¹⁹

Chẳng hạn, không phải tất cả điều tiêu cực, chu kỳ phát hành nhanh chóng ⁷²⁰của dcSpark được tài trợ bởi nguồn vốn thường xuyên thông qua nhiều đề xuất của Catalyst. Harris Warren đã phác thảo những thành tựu của Catalyst kể từ năm 2020 trong bài thuyết trình của ông tại ScotFest.⁷²¹

- Gần 48 triệu đô la tài trợ và phần thưởng đổi mới
- Hơn 60.000 người tham gia
- Hơn 58.000 cử tri đã đăng ký
- Hơn 1,7 triệu phiếu bầu.
- 4.700 đề xuất
- Hơn 1.200 đề xuất được tài trợ
- Hơn 91 quốc gia khác nhau đạt được

Một trang web mới projectcatalyst.io và tích hợp với ren ví dụ (lace.io) sẽ là mấu chốt của Catalyst vào năm 2023. Tuy nhiên, như chúng ta đã biết trong các bài thuyết trình tiếp theo của ScotFest, Catalyst chỉ đơn thuần là một công cụ quan sát Thời đại Voltaire.

Tham gia Catalyst

Có một số cách để tham gia Project Catalyst. Gửi đề xuất, bỏ phiếu, đánh giá, nhận xét hoặc trở thành người cố vấn. Đăng ký tài khoản trên nền tảng cộng tác là bước đầu tiên. Một tùy chọn khác là tham gia cộng đồng Project Catalyst tại TownHall vào Thứ Tư hàng tuần, được phát trực tiếp trên Kênh YouTube của IOG. ⁷²²Bạn có thể theo dõi từng quỹ và kiểm tra các đề xuất đã được phê duyệt trước đây tại đây.⁷²³

Thời đại của Voltaire

⁷¹⁸Phân tích khoảng cách Daedalus Turbo, twitter.com/RichardMcCrackn/status/1575057817181966337?s=20&t=XXfR1C0qB9jx6InYxgpQEA

⁷¹⁹Tái định vị Project Catalyst trước vòng cấp vốn tiếp theo, iohk.io/en/blog/posts/2022/11/01/repositioning-project-catalyst-ahead-of-the-next-funding-round/

⁷²⁰blog dcSpark, medium.com/dcspark

⁷²¹Chất xúc tác dự án (ScotFest), youtube.com/watch?v=NAfwj1lukvc

⁷²²Kênh youtube IOHK, youtube.com/c/IohkIo

⁷²³Trình theo dõi chất xúc tác, bit.ly/FundedProjectsReporting

CIP 1694 ⁷²⁴được đặt tên theo năm sinh của Voltaire. Nó được cho là CIP quan trọng nhất cho đến nay vì nó là một đề xuất để khởi động *Thời đại của Voltaire*. Được đồng tác giả bởi Charles Hoskinson, đây là CIP đầu tiên mà anh ấy trực tiếp tham gia. Rõ ràng là rất nhiều suy nghĩ đã được đưa vào nó, và nó được viết một cách có chủ ý như một tài liệu sống, chuyên tiếp.

Khi Cardano được thành lập, có một cấu trúc ba bên với Emurgo, Cardano Foundation (CF) và IOG với các khoản tiền gửi cho sự phát triển, quản trị và kỹ thuật của hệ sinh thái tương ứng. Luôn có ý định chuyển sang một tổ chức dựa trên thành viên (MBO) sẽ quản lý bộ máy quan liêu của quản trị giao thức. Ban đầu, người ta hy vọng rằng CF có trụ sở tại Thụy Sĩ sẽ là thực thể này nhưng do những hạn chế với cấu trúc stiftung ⁷²⁵nên nó không khả thi.

CIP 1694 là kết quả của nhiều năm nghiên cứu. IOG đã nghiên cứu ý tưởng về một hệ thống cập nhật phi tập trung trong một thời gian. Ví dụ: họ đã viết một bài báo về *Blockchain có thể cập nhật* ⁷²⁶với Liên minh Châu Âu, với khoản trợ cấp Horizon 2020, để khám phá các cách thực hiện tầm nhìn này.

Đầu năm 2022, IOG và CF đã tổ chức các hội thảo để tìm ra con đường phía trước cho kỷ nguyên Voltaire. Dirk Hohndel danh tiếng được bổ nhiệm làm Giám đốc Nguồn mở. ⁷²⁷Dưới sự hướng dẫn của Hohndel, một nhóm được thành lập do Johnny Nguyễn đứng đầu với tư cách là Giám đốc của cái được gọi là *Dự án Chòm sao nội bộ*.

Câu hỏi đầu tiên là 'Quản trị tốt là gì?'. Charles Hoskinson đã giải thích trong bài phát biểu quan trọng về ScotFest của mình rằng câu trả lời dựa trên ba loại khác nhau:

1. **Ý tưởng về sự đại diện** ... bạn có đồng ý với điều gì đó không? Có đại diện trực tiếp khi bạn đích thân bỏ phiếu cho một điều gì đó và **được ủy quyền** khi bạn trao phiếu bầu của mình cho người khác. Trong CIP 1694, vai trò này được gọi là **DRep, đại diện được ủy quyền**. Khái niệm này đã được giới thiệu ở dạng tương tự trong dự án Catalyst. IOG thích gieo hạt giống và điện báo các tính năng sắp tới. Trí tuệ đến từ việc thử nghiệm và thử nghiệm các ý tưởng trong môi trường sống. IOG đã học được rất nhiều điều sau 2 năm tham gia vòng tài trợ của Catalyst.
2. Quản trị cần một số khái niệm về quy tắc, thường được gọi là **hiến pháp**. Đây là những lan can cung cấp một số mức độ ổn định. Điều thú vị về hiến pháp, trong bối cảnh Blockchain, là nó có thể hiểu được bằng máy. Thông số kỹ thuật chính thức có thể là bản thiết kế cho Cardano mà máy tính có thể hiểu được ở mức độ có thể tích hợp với hệ thống cập nhật. Sau khi có hệ thống bỏ phiếu, hiến pháp có thể được phê chuẩn, bấm nhỏ và nhúng vào một giao dịch. Giờ đây, bạn có tùy chọn ký một loại 'thỏa thuận người dùng cuối' bằng cách ký một giao dịch.
3. **Các thể chế** nói chung là một mục tiêu của phân quyền. Nếu chúng ta đang 'giết người trung gian', tại sao các thể chế lại quan trọng? Các tổ chức, với khả năng tốt nhất của họ, đặt ra các tiêu chuẩn và cung cấp quy trình đánh giá từ các chuyên gia trong lĩnh vực. Các thể chế rất cần thiết để quản trị tốt vì chúng là những người lưu giữ kiên thức và các thông lệ tốt nhất. Mọi người có thể thiên vị, đôi khi chúng ta cần các cơ quan trung lập khách quan để cung cấp hướng dẫn. Sau nhiều cân nhắc, người ta đã quyết định viện 'mỏ neo' quan trọng nhất sẽ là một **tổ chức dựa trên thành viên (MBO)** sẽ hoạt động tương tự như các sáng kiến nguồn mở khác như Linux Foundation hoặc Cloud Native Computing Foundation (CNCF).

Vì vậy, năm 2023 là tất cả về việc thực hiện ba điều này thông qua CIP 1674. CIP được cố ý ở cấp độ cao, để khuyến khích thảo luận và phản hồi.

Ai, hoặc MBO là gì?

MBO là một điểm tổng hợp để tập hợp tất cả các nhóm khác nhau: hơn 3.000 SPO, Đại sứ Cardano, hơn 1.200 dự án xây dựng trên Cardano, các dự án nguồn mở chạy trên Cardano (Node, Mithril, Hydra, dcSpark, TxPipe.io, ogmios.dev, v.v.), IOG, CF, Emurgo, tất cả những người nắm giữ ADA, v.v. Các thành viên sẽ sở hữu và điều hành MBO, bố trí nhân sự cho các ban chỉ đạo. Mục tiêu của Voltaire là mang các bộ phận chuyên động này lại với nhau. Như Charles Hoskinson đã nói trong bài phát biểu quan trọng của mình: "IO không chạy chương trình, chúng tôi đã không chạy trong một thời gian dài..."

⁷²⁴CIP 1694, github.com/JaredCorduan/CIPs/blob/voltaire-v1/CIP-1694/README.md

⁷²⁵Một stiftung là nền tảng tồn tại để thực hiện các mong muốn đã nêu, phi thương mại của người sáng lập, như được nêu trong chứng thư thành lập và các điều khoản của hiệp hội (quy chế).

⁷²⁶

Ciampi, Karayannidis, Kiayias và Zindros (2020), 'Các Blockchain có thể cập nhật', iohk.io/en/research/library/papers/updatable-blockchains/

⁷²⁷Dirk Hohndel gia nhập Cardano Foundation với tư cách là Giám đốc nguồn mở, cardanofoundation.org/en/news/dirk-hohndel-joins-cardano-foundation-as-chief-open-source-officer/

Tầm nhìn cho MBO, được Johnny Nguyễn vạch ra tại ScotFest:

Đóng vai trò là điểm tổng hợp của toàn bộ cộng đồng Cardano và các thành viên của nó. Tổ chức dựa trên các thành viên nhằm mục đích khám phá những nỗi đau và mong muốn của cộng đồng, tạo điều kiện phát triển các chiến lược để giải quyết chúng, đồng thời thu hút các công ty và cá nhân có năng lực và khả năng để làm như vậy.



Hình 66: dựa trên slide từ ScotFest

MBO là tổ chức mô neo cho Voltaire, nhưng không phải là tổ chức duy nhất. IOG đã liên tục xây dựng sự hiện diện của mình trong các trường đại học trên toàn cầu, cũng như mở Trung tâm toán học chính thức Hoskinson,⁷²⁸ Phòng thí nghiệm tri thức không⁷²⁹ cũng như công bố Chỉ số phân cấp Edinburgh (EDI).⁷³⁰

⁷²⁸Carnegie Mellon nhận 20 triệu đô la để thành lập Trung tâm toán học chính quy Hoskinson, cmu.edu/news/stories/archives/2021/september/hoskinson-center-for-formal-mathematics.html

⁷²⁹Nhà xây dựng Cardano IOG và Đại học Edinburgh ra mắt Zero-Knowledge Lab để thúc đẩy khả năng mở rộng và bảo mật Blockchain lớn hơn, iohk.io/en/blog/posts/2022/11/18/cardano-builder-iog-and-university-of-edinburgh- khởi chạy-zero-kiến thức-phòng thí nghiệm-to-drive-đại-blockchain-khả năng mở rộng-và-bảo mật/

⁷³⁰Nhà xây dựng Cardano IOG và Đại học Edinburgh để tạo chỉ mục đầu tiên cung cấp số liệu tiêu chuẩn ngành cho phân cấp Crypto, iohk.io/en/blog/posts/2022/11/18/cardano-builder-iog-and-university-of-edinburgh -to-create-first-ever-index-to-cung cấp-ngành-tiêu chuẩn-số liệu-cho-Crypto-phân quyền/

Governance actions follow a process of on-chain and off-chain steps to update the Cardano protocol



Hình 67: Slide từ bài nói chuyện của Michael Madoff (Giám đốc sản phẩm của Voltaire) tại ScotFest

Mọi người nên đọc CIP và hình thành quan điểm của riêng mình, vì quản trị mang tính chủ quan cao. CIP xứng đáng là một cuốn sách theo đúng nghĩa của nó và Hoskinson thường tuyên bố rằng ông muốn viết một cuốn sách về quản trị.⁷³¹

CIP 1694 là một tài liệu sống và sẽ cập nhật và phát triển với các cuộc hội thảo và thảo luận sắp tới. Mặc dù các hiến pháp đã được viết trước đó, nhưng chúng tôi đang bước vào vùng nước không thông minh vì tôi không nghĩ rằng bất cứ điều gì ở quy mô này đã được thử trong không gian Crypto. Nền dân chủ lỏng không phải là một khái niệm mới, nhưng có rất ít ví dụ về việc thực hiện thành công. Sau đây là ý kiến của tôi về CIP 1694, kể từ tháng 2 năm 2023.

Động lực của CIP 1694 là khởi động kỷ nguyên Voltaire, tích hợp các thành phần on-chain và off-chain mới và hiện có để tự quản lý hệ sinh thái. Mục tiêu cuối cùng là có một lớp quản trị trên Cardano hoàn chỉnh, từ đầu đến cuối, trên chuỗi.

Chúng tôi đang ở đâu – 5 trên 7 hệ thống

Tại thời điểm viết bài, các giao dịch quản trị (ví dụ: Hard fork, thay đổi tham số, v.v.) yêu cầu chữ ký từ ít nhất năm trong số bảy khóa quản trị Cardano, hiện do ba tổ chức sáng lập nắm giữ. Quá trình này luôn được dự định là một hình thức quản trị phù du khi chúng ta trải qua các thời kỳ đầu tiên của lộ trình trước Voltaire.

Thuật ngữ & Khái niệm

CIP giới thiệu một số thuật ngữ mới. Đầu tiên, có một **hành động quản trị** mà bất kỳ chủ sở hữu ADA nào cũng có thể gửi. Ba nhóm cá nhân sau đó bỏ phiếu phê chuẩn hoặc hủy bỏ hành động quản trị.

Ba nhóm hình thành nên ⁷³²cơ quan lập pháp ba viện này:

- Một ủy ban hiến pháp,
- DReps (cùng tên nhưng khác vai trò với Catalyst dReps).

⁷³¹Charles Hoskinson - Sách về Quản trị phi tập trung, youtube.com/watch?v=kutZ41J-tTU

⁷³² Chế độ ba viện là thực tiễn có ba viện lập pháp hoặc nghị viện. Nó tương phản với chủ nghĩa đơn viện và chủ nghĩa lưỡng viện, cả hai đều phổ biến hơn nhiều

- Người điều hành Stake Pool (SPO)

Ủy **ban hiến pháp** sẽ có vai trò tương tự như thượng viện. Tiếp tục tương tự, DReps sẽ tạo nên hạ viện. DRep hoặc **đại diện được ủy quyền** có thể là bất kỳ chủ sở hữu ADA nào đại diện cho chính họ hoặc những chủ sở hữu ADA khác đã ủy quyền biểu quyết cho họ. **Người điều hành Stake Pool** là cùng một nhóm được giới thiệu trước đó, những người điều hành các Node cung cấp năng lượng cho mạng.

Ouroboros đã là một câu chuyện thành công lớn, với ~75% số tiền đặt cược của ADA khiến Cardano trở thành một trong những mạng phi tập trung nhất. Bằng cách tận dụng mạng SPO, quy trình này thu hút được một nhóm người dùng Cardano đam mê, những người được giáo dục và đủ điều kiện để bỏ phiếu cho các quyết định quan trọng.

Hiến pháp Cardano sẽ được soạn thảo vào năm 2023 với càng nhiều ý kiến đóng góp từ cộng đồng càng tốt. Hiến pháp này sẽ bao gồm các lan can bảo vệ, các giá trị được chia sẻ, các nguyên lý cốt lõi và các nguyên tắc hướng dẫn đã được các bên liên quan nhất trí. Trong những ngày đầu tiên này, nó sẽ chỉ là một tài liệu văn bản với hàm băm được ghi lại trên chuỗi. Giám đốc pháp lý của IOG Joel Telpner đã cùng Charles Hoskinson trò chuyện bên lề ⁷³³tại ScotFest để thảo luận về những thách thức trong việc soạn thảo hiến pháp mới. Telpner đã mô tả hiến pháp là gì:

Tôi nghĩ rằng bạn thực sự có thể đơn giản hóa hiến pháp và nói rằng đó là một bộ quy tắc, nhưng đó là một bộ quy tắc để làm gì? Nó làm ba điều. Nó thiết lập cách bạn lập pháp; nó thiết lập cách bạn quản lý và thiết lập cách bạn phân xử. Nó tạo ra khung này cho ba chức năng đó.

Mỗi cơ quan trong số ba cơ quan đóng vai trò của họ trong việc phê chuẩn các hành động quản trị. Vai trò có thể khác nhau đối với mỗi cơ thể trong những hoàn cảnh khác nhau. Ví dụ, ủy ban hiến pháp sẽ luôn ở một trong hai trạng thái, hoặc là **trạng thái bình thường**, hoặc trạng thái **bất tín nhiệm**. Như bạn có thể mong đợi, nếu nó ở trạng thái không tin tưởng, nó không thể tham gia vào các hành động quản trị. Nó phải được thay thế trước khi bất kỳ hành động quản trị nào có thể được ban hành.

Thành phần của ủy ban hiến pháp ban đầu không được xác nhận, nhưng có khả năng là các thành viên cốt lõi của tổ chức dựa trên thành viên. Một trong những nhiệm vụ đầu tiên sẽ là đổi tên MBO. Đề xuất của tôi là GaaS (Quản trị như một dịch vụ).

Có hai cách để thay thế ủy ban hiến pháp. Nếu nó ở trạng thái bình thường, thì chính ủy ban đó, cùng với DReps, đều có thể phê chuẩn một đề nghị thay thế ủy ban hiến pháp. Các SPO không bắt buộc trong trường hợp này.

Nếu ủy ban hiến pháp ở trạng thái không tin tưởng, các SPO và DRep có thể bỏ phiếu để thay thế nó. Nếu nó đã ở trong tình trạng không tin tưởng, giả định là đa số muốn thay thế ủy ban hiến pháp.

Thượng viện thường có ít thành viên hơn hạ viện, tuy nhiên, không có số lượng cố định (đại biểu) cho ủy ban hiến pháp trong CIP 1694. Nó có thể thay đổi mỗi khi ủy ban được thành lập. Kích thước đại biểu là ngưỡng chữ ký, có bao nhiêu thành viên ủy ban cần ký để phê chuẩn điều gì đó.

Có sáu loại hành động quản trị khác nhau :

- Một kiến nghị bất tín nhiệm trong ủy ban hiến pháp.
- Thay đổi thành viên (và/hoặc số đại biểu cần thiết) của ủy ban hiến pháp.
- cập nhật hiến pháp
- Bắt đầu HardFork
- Thay đổi tham số giao thức
- Rút tiền từ kho bạc (nhỏ, vừa hoặc lớn)

Vì bất kỳ ai cũng có thể gửi hành động quản trị, nên cần có **khoản tiền gửi quản trị** để ngăn gửi thư rác. Khoản tiền gửi này được trả lại sau khi hành động quản trị được phê chuẩn, hủy bỏ hoặc hết hạn.

Các hành động quản trị sẽ được phê chuẩn bằng cách bỏ phiếu trực tuyến, với mỗi loại trong số sáu loại hành động quản trị có các yêu cầu phê chuẩn khác nhau dựa trên một số hoặc tất cả những điều sau:

- một số phiếu đại biểu quy định của ủy ban Hiến pháp
- đặt ngưỡng kiểm soát cổ phần của DReps
- đặt ngưỡng kiểm soát cổ phần của SPO

⁷³³Trò chuyện bên lề ScotFest với Joel Telpner, youtube.com/watch?v=YvTfSx6pv9Y

Biểu đồ dưới đây từ CIP 1694 chứa các tiêu chí khác nhau cho các hành động quản trị khác nhau được ban hành. Tại thời điểm viết bài này, có nhiều trình giữ chỗ cho các giới hạn ngưỡng, v.v. Chúng có thể sẽ được thiết lập sau nhiều cuộc tranh luận, hội thảo và đóng góp từ các bên quan tâm.

199	+						
200	+	Governance Action Type	Constitutional Committee	DReps	AVST	SPOs	
201	+	---	:---	---	---	---	
202	+	1. Motion of no-confidence	:x:	\$P_1\$	:x:	\$R_1\$	
203	+	2(a). New Committee/quorum (_normal state_)	:heavy_check_mark:	\$P_{2a}\$	\$Q_{2a}\$	\$R_{2a}\$	
204	+	2(b). New Committee/quorum (_state of no-confidence_)	:x:	\$P_{2b}\$	:x:	\$R_{2b}\$	
205	+	3. Update to the Constitution	:heavy_check_mark:	\$P_3\$	\$Q_3\$	\$R_3\$	
206	+	4. Hard-Fork initiation	:heavy_check_mark:	\$P_4\$	:x:	\$R_4\$	
redCorduan marked this conversation as resolved. Show resolved							
207	+	5. Protocol parameter changes	:heavy_check_mark:	\$P_5\$	\$Q_5\$	\$R_5\$	
208	+	6(a). Treasury withdrawal, \$[T_0, T_1]\$	:heavy_check_mark:	\$P_{6a}\$	\$Q_{6a}\$	\$R_{6a}\$	
209	+	6(b). Treasury withdrawal, \$[T_1, T_2]\$	:heavy_check_mark:	\$P_{6b}\$	\$Q_{6b}\$	\$R_{6b}\$	
210	+	6(c). Treasury withdrawal, \$[T_2, T_3]\$	:heavy_check_mark:	\$P_{6c}\$	\$Q_{6c}\$	\$R_{6c}\$	

Hình 68: Biểu đồ từ CIP 1694

Ngưỡng **cổ phần biểu quyết đang hoạt động** (AVST) là tỷ lệ phần trăm được sử dụng để xác định xem có đủ cổ phần biểu quyết hay không. Không đi sâu vào chi tiết, AVST được sử dụng để xác định các yêu cầu nhất định. Ví dụ: nếu có đủ AVST, thì không cần phê duyệt SPO cho một hành động quản trị nhất định. Nếu không, cần phải có sự chấp thuận của cử tri SPO.

Các hành động quản trị sẽ được kiểm tra để phê chuẩn trên các ranh giới kỷ nguyên. Chỉ một hành động quản trị của mỗi loại có thể được tổ chức để ban hành, trong bất kỳ thời kỳ nhất định nào. Phiếu bầu có thể là **đồng ý**, không hoặc **bỏ phiếu trắng**. Một phiếu trắng sẽ không được tính cho cổ phần bỏ phiếu đang hoạt động nhưng nếu bạn muốn thay đổi phiếu bầu của mình, bạn chỉ cần bỏ phiếu lại và nó sẽ thay thế phiếu bầu 'bỏ phiếu trắng' sớm của bạn. Tiến trình của một hành động quản trị có thể được theo dõi trên chuỗi.

quan sát

Một câu hỏi xuất hiện trong đầu là làm thế nào để đảm bảo quyền biểu quyết được phân bổ công bằng nếu ủy ban hiến pháp bỏ phiếu cho mỗi người, trong khi các DRep và SPO bỏ phiếu theo cổ phần? Ngoài ra, ba viện không phải lúc nào cũng bỏ phiếu cho các hành động. DReps dường như là những cử tri tích cực nhất. Hầu hết thời gian, ủy ban hiến pháp bỏ phiếu, nhưng không bỏ phiếu cho kiến nghị bất tín nhiệm, hoặc nếu đó là một ủy ban mới hoặc bỏ phiếu theo số đại biểu cần thiết. Thượng viện thường có quyền lực cao nhất, trong khi các SPO đôi khi chỉ bỏ phiếu nếu không đáp ứng ngưỡng cổ phần bỏ phiếu có hiệu lực. Bạn có thể thấy các SPO có vị trí yếu nhất trong cơ quan ba viện nếu họ bỏ phiếu ít thường xuyên nhất. Tuy nhiên, nó mang nhiều sắc thái hơn thế vì DReps và SPO có thể loại bỏ ủy ban hiến pháp.

Ngoài ra, hãy nhớ rằng các SPO đã thể hiện một khía cạnh khác trong phân cấp của Cardano khi họ phủ quyết hiệu quả ngày ban đầu cho hard fork Vasil. ⁷³⁴CIP 1694 có bất kỳ biện pháp nào để ngăn chặn các SPO trì hoãn một hard fork trong tương lai bằng cách không nâng cấp lên Node mới nhất không?

CIP dường như ủng hộ bỏ phiếu theo cổ phần hơn là phiếu bầu cho mỗi người. Bỏ phiếu cho mỗi người yêu cầu một số khái niệm xác minh danh tính, vì vậy có bằng chứng ai đó là người mà họ tuyên bố. CIP giải thích rằng hiện tại không thể có một giải pháp phi tập trung hoàn toàn cho việc này. Với quy định dường như sắp xảy ra, cần thận trọng tránh xa bất kỳ cơ chế nào có thể được hiểu là 'tập trung hóa' bởi các bên có tính không biết gì. Điều đó nói rằng, CIP sẽ sẵn sàng thay đổi trong tương lai khi ID phi tập trung (DID) phát triển. World Wide Web Consortium (W3C) đã thông báo rằng Mã định danh phi tập trung (DID) hiện là tiêu chuẩn web chính thức vào mùa hè năm 2022. Nhà khoa học trưởng của IOG Aggelos Kiayias cho rằng họ chắc chắn sẽ là một phần của thể hệ Blockchain ^{thứ 4}. ⁷³⁵

CIP cho biết thành phần và vai trò của DReps có thể thay đổi. Sẽ rất thú vị để xem cộng đồng coi ai là người đủ điều kiện và mức độ chuyên môn về miền được yêu cầu, nếu có. Xung đột đặt tên với Catalyst dReps roel gây nhầm lẫn, đặc biệt là đối với những người

⁷³⁴@KtorZ 'chậm trễ là tốt', twitter.com/_KtorZ_/status/1538101313564811265?s=20&t=Kygsq-InxS6AO0XhjFfr8g

⁷³⁵Nguyên tắc đầu tiên: Nghiên cứu cho tương lai, youtube.be/MVuweoiXPI?t=2280

mới sử dụng Cardano. Vì một trong những mục chương trình nghị sự đầu tiên là tìm một cái tên phù hợp hơn cho MBO, có lẽ một cái tên tốt hơn cho DRep cũng có thể được bình chọn.

DRep ban đầu và ủy quyền cho họ, sẽ bắt buộc hệ thống chứng chỉ hiện được sử dụng cho Stake Pool. Điều này có dẫn đến số lượng SPO không cân xứng cũng hoạt động như DRep không? Vì vai trò ban đầu của ủy ban hiến pháp là khởi động khuôn khổ, họ có thể thúc đẩy một chương trình nghị sự nếu lợi ích của cộng đồng quá ít hoặc quá nhiều không? Cuộc bỏ phiếu cần tỷ lệ tham gia cao để hệ thống trở nên hợp pháp, nhưng ai là người quyết định các ngưỡng này?

CIP 1674 đang ở giai đoạn sơ khai, thật khó để chắc chắn tất cả lý thuyết này sẽ hoạt động như thế nào trong thực tế. Ví dụ: một trong những lợi ích của hệ thống (5 trên 7 phím) hiện tại là nó tương đối nhanh. Điều gì xảy ra nếu có một sự kiện thiên nga đen và cần phải có một bản cập nhật lớn gấp? Bộ máy gồm các bộ phận chuyển động này có thể tác động đến sự thay đổi kịp thời không? Nếu 'Cập nhật hiến pháp' là một trong sáu hành động quản trị, phần nào của hiến pháp có thể được cập nhật?

Một bên độc hại có thể làm chậm nó xuống không? Nếu chỉ có hai trong số ba viện sẽ bỏ phiếu trong một số tình huống nhất định, thì liệu có xảy ra bế tắc lập pháp như khi đa số kiểm soát của thượng viện Hoa Kỳ chặn hạ viện không? Có những biện pháp nào để ngăn chặn filibuster?

Đây chỉ là một số suy nghĩ và bạn có thể thấy từ cuộc thảo luận đang diễn ra trên GitHub,⁷³⁶ rằng việc đưa điều này vào hiệu quả sẽ không hề tầm thường. Đó là để được mong đợi. Sẽ không đáng nghi ngờ nếu một sự thay đổi mạnh mẽ như vậy được thực thi nhanh chóng mà không có ý kiến đóng góp của cộng đồng? CIP đi vào chi tiết hơn về các kế hoạch triển khai dần dần điều này trong các giai đoạn khác nhau. Ví ren *nhẹ* không được đề cập trong CIP, nhưng rõ ràng là ví di động mới của IOG và các ví Cardano khác sẽ đóng vai trò then chốt trong việc người dùng tham gia và mua vào.

Chúng ta đang đi đâu

Công tác chuẩn bị thực hiện CIP 1694 đang được tiến hành. Đề xuất hiện tại bao gồm hai kỳ nguyên sổ cái mới. Kỳ nguyên đầu tiên sẽ được gọi là *Conway*, theo tên nhà toán học nổi tiếng người Anh John Horton Conway. Kế hoạch hiện tại cho kỳ nguyên sổ cái Conway là:

- giới thiệu bỏ phiếu SPO cho hard fork
- cung cấp một cơ chế trên chuỗi để luân phiên các khóa quản trị
- sắp xếp lại các quy tắc sổ cái liên quan đến quản trị như đã nêu trong CIP-1694

Theo dõi các bản cập nhật mới nhất từ các nhóm kỹ thuật khác nhau trên GitHub.⁷³⁷

Nếu CIP 1694 thành công, thì chúng ta nên hiện thực hóa tầm nhìn được đặt ra trong *Đường đến Hệ sinh thái Đa ngôn ngữ cho Cardano* video băng trắng.⁷³⁸ Các cơ chế quản trị được nêu ở trên sẽ cho phép nhiều khách hàng, với các nhóm nhà phát triển khác nhau, các cách tiếp cận, ngôn ngữ lập trình và USP thương mại khác nhau. Sẽ không có ứng dụng khách hoặc ví chuẩn cho Cardano, chỉ được chứng nhận hoặc chưa được chứng nhận. IOG đã nghiên cứu vấn đề này một thời gian, viết báo và xây dựng kiến thức chuyên môn về các phương pháp chính thức, cụ thể là với Agda.⁷⁴⁰

Ý tưởng là các bên quan tâm, chẳng hạn như dcSpark, sẽ làm việc với MBO để thành lập một nhóm *các Nghiên cứu sinh kỹ thuật Cardano* (CTF), những người duy trì kiến trúc tham chiếu. Mã phi sản xuất này sẽ được đưa qua quy trình CIP, trước khi thông số kỹ thuật chính thức, trong Agda, được soạn thảo. Thông số kỹ thuật 'lỗi Agda' này cho phép trích xuất mã để làm tài liệu tham khảo cho thử nghiệm. Các CTF có thể chứng minh các thuộc tính về thông số kỹ thuật và cũng duy trì chứng nhận ví, cũng như mật mã cốt lõi của hệ thống.

⁷³⁶Cuộc trò chuyện đang diễn ra về CIP 1694, github.com/cardano-foundation/CIPs/pull/380

⁷³⁷Cập nhật nhóm sổ cái, input-output-hk.github.io/cardano-updates/2023-01-19-ledger

⁷³⁸Đường đến Hệ sinh thái Đa ngôn ngữ cho Cardano, youtube.com/watch?v=skcCglWaedA

⁷³⁹Canonical, trong khoa học máy tính, là trạng thái hoặc hành vi tiêu chuẩn của một thuộc tính. Thuật ngữ này được vay mượn từ toán học, nơi nó được dùng để chỉ các khái niệm độc nhất và/hoặc tự nhiên.

⁷⁴⁰Agda là một ngôn ngữ lập trình chức năng được gõ phụ thuộc. Charles Hoskinson gọi nó là 'Super Haskell'

Sẽ không còn ứng dụng khách chuẩn của Cardano nữa, chỉ có các ứng dụng khách cạnh tranh được viết bằng Rust, Typescript, Python và Haskell. Người dùng sẽ chỉ quan tâm đến việc nó có được chứng nhận hay không. Điều này tạo ra một thị trường lành mạnh 'sống còn của kẻ mạnh nhất', nơi bảo mật được đảm bảo và có nhiều sự lựa chọn hơn cho người dùng cuối.

CH tại bài phát biểu quan trọng của ScotFest.⁷⁴¹

Vì vậy, đó là Voltaire... nó mang tính triết học sâu sắc, đó là điều khó khăn nhất mà tôi từng làm trong đời, đó là điều khó khăn nhất mà bạn từng làm trong đời và chúng ta sẽ hoàn thành nó, bởi vì nó cần phải hoàn thành đã xong và tôi quá mệt mỏi với việc ngành của chúng ta thất bại, và đã đến lúc chúng ta có thể chỉ ra điều gì đó và nói rằng 'bạn biết những gì chúng tôi đã làm đúng cách'. Chúng ta phải chăm sóc khu vườn của mình trước. Đó là một bài học của Candide. Vì vậy, chúng tôi phải khắc phục sự quản trị của Cardano trước khi chúng tôi có quyền khiếu nại về bất kỳ sự quản trị nào của người khác.

Để tham gia vào Thời đại Voltaire, bạn cung cấp phản hồi trên GitHub và tham gia MBO bằng cách đăng ký tại cardanombo.org

Sự kiện bỏ phiếu đặc biệt

Không rõ khi nào Catalyst sẽ tiếp tục với Fund10 và mất bao lâu để CIP 1694 được phê duyệt và triển khai. Tại Tòa thị chính đầu tiên của năm 2023, nhóm Catalyst đã giới thiệu một khái niệm mới gọi là *Sự kiện bỏ phiếu đặc biệt* (SVE) sẽ diễn ra bằng cách sử dụng công cụ Catalyst. SVE là một phiếu bầu được tổ chức không liên quan đến các chu kỳ quỹ của Catalyst. Đây là biện pháp dự phòng để đạt được sự đồng ý của cộng đồng đối với các quyết định quan trọng trước khi CIP-1694 hoạt động.

⁷⁴¹Bài phát biểu quan trọng của IO ScotFest với Charles Hoskinson, youtu.be/tbtkClr3Y3I

Chương 10: RealFi trên Cardano

'Giàu có không phải là có nhiều tài sản, mà là có ít mong muốn.'

- Epictetus

Cuộc cách mạng DeFi

Số lượng người dùng ADA và nhà phát triển phần mềm làm việc trên Cardano đang tăng đều đặn. Các trang web như *CardanoCube* , *Build on Cardano* , *Building On Cardano* và *Essential Cardano* đang bận rộn lập bản đồ một hệ sinh thái hấp dẫn với ~110 dự án đã khởi chạy và ~1.100 dự án sắp triển khai.

Cardano được thiết kế để trở thành một nền tảng an toàn và đáng tin cậy để phát triển các tài sản, dịch vụ và hệ thống dựa trên Blockchain. Tài chính phi tập trung, hay DeFi, đã trở nên phổ biến trong những năm gần đây, giới thiệu một loạt sản phẩm tài chính mới, từ thực tế đến đáng ngờ. Mục đích cuối cùng của DeFi , khi thị trường phát triển, là hỗ trợ mọi người và doanh nghiệp thực hiện các giao dịch tài chính mà không cần trung gian trung gian tốn kém như ngân hàng hoặc đạt được lợi nhuận cao hơn từ tài sản của họ trong thời đại lạm phát và lãi suất âm .

Cardano đã mở rộng điều này hơn nữa. Mục tiêu là cung cấp các dịch vụ ngân hàng và bảo hiểm chi phí thấp cho hàng triệu cá nhân trên toàn cầu, những người không có quyền truy cập vào các dịch vụ đó. Điều này sẽ giúp tháo dỡ các rào cản giữa các nước phát triển và nước nghèo. Khái niệm này được IOG ⁷⁴² đặt tên là ' RealFi '.

Mặc dù mức độ phổ biến của Cardano tăng đột biến, nhận thức và sự chấp nhận về Blockchain nói chung vẫn còn thấp. Ít nhất, do hàng loạt thuật ngữ mà bất kỳ cá nhân tò mò về Crypto nào cũng phải lướt qua. TradFi , DeFi, RealFi, DApp, DEX, tính thanh khoản và các thuật ngữ khác đồng nghĩa với các sản phẩm Blockchain gần đây nhất.

Tại sao chúng ta cần DeFi?

Làm thế nào chúng ta có thể sử dụng Blockchain trong cuộc sống hàng ngày? Tại sao nó lại quan trọng? Blockchain là tất cả về giao dịch hoặc trao đổi tiền trong những trường hợp nhất định cho nhiều mục đích sử dụng gần như vô hạn. Công nghệ Blockchain đã được sử dụng bởi các công ty trên tất cả các ngành dọc.

	Traditional Finance	DeFi
Custody	Held by institution or custody provider	Held directly by users in non-custodial accounts or via smart contract
Unit of Account	Fiat Currency	Denominated in digital asset or stable coin
Execution	Facilitated via intermediaries	Facilitated via smart contract
Settlement	~3-5 business days depending on transaction, during M-F business hours.	Seconds to minutes depending on blockchain, 24/7 operating times.
Clearing	Facilitated via clearinghouses	Facilitated via blockchain transaction
Governance	Specified by exchanges & regulators	Governed by the protocol developers & users
Auditability	Authorized third-party audits	Open source code & public ledger, can be audited by anyone
Collateral	Transactions may involve no collateral, intermediates take on risk	Over-collateral generally required.
Risks	Vulnerable to hacks and data breaches	Vulnerable to hacks and data breaches of smart contracts

Hình 69: Tài chính truyền thống v DeFi, được phép của CoinYuppie⁷⁴³

DeFi là gì?

Tài chính phi tập trung, thường được gọi là DeFi, là một loại tài chính dựa trên Blockchain phục vụ các chức năng giống như tài chính thông thường (TradFi). Bạn có thể sử dụng Crypto để thực hiện và nhận thanh toán, thanh toán hàng hóa và dịch vụ cũng như đầu tư vào các dự án thay vì trái phiếu hoặc cổ phiếu. Mặt khác, DeFi không dựa vào người trung gian mà thay vào đó dựa vào các hợp đồng thông minh để giải quyết các giao dịch một cách công bằng. RealFi được tạo bằng cách kết hợp một lớp nhận dạng, chẳng hạn như Atala PRISM, ⁷⁴⁴với một 'cầu nối' với thế giới thực.

⁷⁴²

John O'Connor, 'Chào mừng đến với thời đại của RealFi', iohk.io/en/blog/posts/2021/11/25/welcome-to-the-age-of-realfi/

⁷⁴³

DeFi đang đổi mới với tốc độ gấp 10 lần so với tài chính truyền thống?, coinyuppie.com/defi-is-innovating-at-10-times-the-rate-of-traditional-finance/

⁷⁴⁴

Phương tiện trao đổi

Theo truyền thống, chúng ta thanh toán hàng hóa và dịch vụ bằng tiền. Hình thức phổ biến nhất của phương tiện thương mại này là tiền xu hoặc tiền giấy do ngân hàng trung ương phát hành. Từ fiat đã trở nên phổ biến đối với những người dùng Crypto để biểu thị tiền trong thế giới thực. Tiền Fiat bao gồm đồng đô la Mỹ, bảng Anh và đồng yên Nhật. Vì các chính phủ không còn phải hỗ trợ tiền tệ của họ bằng vàng, nên thuật ngữ này đã được thông qua. Thay vào đó, họ chỉ định tiền tệ của mình được đầu thầu hợp pháp bằng một nghị định chính thức được gọi là fiat.

Trên Blockchain, tài sản Crypto được sử dụng thay vì tiền tệ fiat.

Tất cả hoạt động cùng nhau như thế nào

Trước khi chúng ta tìm hiểu chi tiết về danh pháp DeFi, chúng ta hãy xem cách hoạt động của tất cả. Hợp đồng thông minh là động lực đằng sau các thỏa thuận an ninh và công bằng. Giả sử bạn đã tải xuống một DApp và muốn cho Bob mượn 10 ADA. Chúng tôi cần biết rằng Bob sẽ trả lại số tiền đó và chúng tôi muốn có thể thu được một số tiền lãi nếu anh ấy làm như vậy muộn hơn dự kiến. Theo truyền thống, người dùng ký hợp đồng bao gồm các điều khoản đó. Điều này cũng được thực hiện trên Blockchain nhưng sử dụng hợp đồng thông minh.

Hợp đồng thông minh: một thỏa thuận kỹ thuật số tự động dựa trên mã giám sát, xác thực và thực hiện các phần ràng buộc về mặt pháp lý của giao dịch giữa hai hoặc nhiều bên. Khi các tiêu chí đặt trước được thỏa mãn, thuật toán hợp đồng thông minh sẽ tự động thực hiện các bước hợp đồng.

Hợp đồng thông minh không tự truy cập dữ liệu cụ thể. Ví dụ: giả sử chúng tôi đồng ý với Bob rằng anh ấy sẽ trả nợ cho chúng tôi trước ngày 23 tháng 2. Ngày, liệu Bob có hoàn thành giao dịch hay không và liệu số tiền được cung cấp có bằng số tiền đến hạn hay không, tất cả đều cần thiết để hợp đồng thông minh thực thi. Hợp đồng thông minh sử dụng lời tiên tri để làm việc này.

Oracle là một công cụ để tương tác với dữ liệu trong thế giới thực. Oracles liên kết với các nguồn dữ liệu bên ngoài đáng tin cậy, cho phép các hợp đồng thông minh chạy theo thông tin tham chiếu như thời gian chính xác, thời tiết, kết quả bầu cử, thống kê thể thao và thị trường Crypto. Nhà tiên tri đảm bảo rằng dữ liệu là chính xác, kịp thời và không bị thay đổi.

Hệ sinh thái DeFi rộng hơn

Người dùng tận dụng nhiều hệ thống và ứng dụng DeFi vì nhiều lý do. Ví dụ: các giải pháp quản lý tài sản (hoặc đơn giản là ví) cho phép khách hàng lưu trữ, truyền và nhận Crypto. Có rất nhiều ứng dụng phi tập trung (DApps) có sẵn:

Với hệ sinh thái Cardano đang phát triển nhanh chóng, ngày càng có nhiều hàng hóa DeFi đến với Cardano. Đối với các yêu cầu tài chính của họ, giờ đây người dùng có thể sử dụng DApps và nền tảng mới. Do đó, IOG đang tập trung vào những điều sau để đảm bảo rằng người dùng và cộng đồng nhà phát triển có thể cung cấp và sử dụng các sản phẩm chất lượng cao:

- DApp Store là một cửa hàng thân thiện với người dùng, nơi có thể tìm thấy tất cả các DApp Cardano. Nó sẽ có sẵn thông qua ví ảnh sáng Lace, cũng như tiện ích mở rộng trình duyệt trên máy tính để bàn. Nó sẽ là một đoạn đường nối liền mạch so với trải nghiệm hiện tại.
- Chứng nhận DApp: chứng nhận và đảm bảo đảm bảo các mặt hàng đáp ứng các tiêu chuẩn chất lượng. Mặc dù chứng nhận là tùy chọn (Cardano là mã nguồn mở và phi tập trung), nhưng nó giúp ích cho cả nhà phát triển và người tiêu dùng vì nó chứa các kiểm tra bảo mật hỗ trợ kiểm tra hợp đồng thông minh. Có ba cấp độ chứng nhận, mỗi cấp độ đều hữu ích khi kết hợp với các cấp độ khác.

Các hệ thống DeFi và DApps chủ yếu được sử dụng cho các giao dịch tài chính. Chúng có thể được sử dụng để đầu tư, cho vay và vay ngoài việc chuyển tiền. Trên thực tế, trên Blockchain, người dùng có thể vay Crypto mà không phải trả lãi:

- Khoản vay chớp nhoáng: hoạt động như một khoản vay nhanh không có tài sản thế chấp (số tiền cần thiết để đảm bảo khoản vay bằng các loại Crypto hoặc Token khác) hoặc kiểm tra thông tin khách hàng (KYC). Mặt khác, khoản vay chớp nhoáng yêu cầu hoàn vốn trong cùng một khối mà nó được cung cấp cho người vay. Giao dịch ban đầu bị từ chối nếu khoản vay không được hoàn trả và người cho vay giữ tiền.

Atala PRISM là một giải pháp nhận dạng phi tập trung được xây dựng trên Blockchain Cardano. Nó tạo ra một cách tiếp cận mới để quản lý danh tính, trong đó người dùng sở hữu danh tính của họ và có toàn quyền kiểm soát cách dữ liệu cá nhân của họ được sử dụng và truy cập.

Chúng ta hãy xem thêm một vài cụm từ thường được sử dụng nhất trong DeFi:

Trao đổi: trao đổi Crypto cho phép người dùng mua và bán Crypto. Có hai loại trao đổi khác nhau. CEX (sàn giao dịch tập trung) được điều hành bởi một công ty hoặc cấu trúc riêng biệt được điều chỉnh bởi các quy tắc và quy định. Người dùng có thể mua và bán tài sản của họ một cách an toàn, ngang hàng trên DEX (sàn giao dịch phi tập trung) không có người trung gian.

Một từ thông dụng khác mà bạn sẽ bắt gặp là tính thanh khoản. Nó theo dõi lượng cung lưu thông và các hoạt động giao dịch trên một DEX hoặc CEX cụ thể. Nhu cầu giao dịch của người dùng cần sự luân chuyển của vật tư. Đây là những gì thanh khoản đề cập đến: có đủ số lượng tiền xu hoặc Token để đáp ứng nhu cầu của người dùng.

Tính thanh khoản bao gồm các hành động và khái niệm sau đây đi cùng với chúng:

- **Khai thác thanh khoản** đề cập đến việc sản xuất hoặc thêm các loại tiền tệ hoặc Token mới để đáp ứng nhu cầu giao dịch. Công cụ khai thác thanh khoản (nhà cung cấp) thường được bồi thường để duy trì cơ sở người dùng và tạo nhóm thanh khoản. Năng suất canh tác là tên gọi khác của khai thác thanh khoản
- **Nhóm thanh khoản** : một tập hợp các loại Crypto được ký gửi đóng vai trò là nguồn thanh khoản cho mạng khi tiền tệ có nhu cầu cao
- **AMM** (nhà tạo lập thị trường tự động): một nhóm Crypto hoạt động như một nhà cung cấp thanh khoản giữa 'các cặp giao dịch'. Một cặp giao dịch là một trận đấu giữa hai bên, chẳng hạn như Fred muốn bán bitcoin của mình và Barney muốn mua nó. AMM được phân cấp và dựa vào tính thanh khoản mà người dùng của họ cung cấp.

Trao đổi phi tập trung không chỉ là nền tảng giao dịch tiện dụng cho Crypto. Chúng cũng có thể được sử dụng để tạo doanh thu.

Một số thuật ngữ chính:

- **Lợi tức đầu tư (ROI)**: lãi hoặc lỗ trên một khoản đầu tư, thường được biểu thị bằng tỷ lệ phần trăm
- **Canh tác năng suất** đôi khi được gọi là khai thác thanh khoản. Canh tác là một thuật ngữ được sử dụng để mô tả một quá trình trong đó phần thưởng được trao đổi để tạo ra tiền
- **Yield** : số phần thưởng kiếm được bằng cách đặt cược Crypto hoặc thanh khoản khai thác
- **Đòn bẩy** : hành động vay mượn với kỳ vọng kiếm được lợi nhuận cao hơn lãi suất phải trả.

Trong thời điểm mà một số ngân hàng đang đưa ra mức lãi suất âm, cách rủi ro thấp để kiếm lãi từ tiền gốc của bạn chỉ bằng cách đặt cược hoặc ủy thác số tiền đặt cược của bạn trên Cardano.

Mỗi chủ sở hữu ADA có một cổ phần tỷ lệ thuận với số lượng ADA mà họ nắm giữ. Một cá nhân am hiểu công nghệ có thể tạo Stake Pool và vận hành nó để hỗ trợ xác minh các giao dịch Cardano để đổi lấy phần thưởng. Để nhận được một phần của những phần thưởng này, bất kỳ ai cũng có thể ủy thác ADA của họ cho Stake Pool. Không có gì nguy hiểm với điều này vì không có ADA nào rời khỏi ví của bạn. ADA có thể được ủy quyền hoặc chi tiêu tại bất kỳ thời điểm nào từ ví của bạn.

30/08/2020, 'hiệu ứng mạng' DeFi. CH.⁷⁴⁵

Thực tế là lợi thế của người đi trước thực sự là một bất lợi trong DeFi. Những hiệu ứng mạng đó là phù du và thường được bao phủ bởi những sai lầm, vết sẹo và vụ nổ. Bạn thực sự muốn trở thành người bắt chước, danh mục người dẫn đầu thứ hai cho DeFi và tôi nghĩ chúng ta sẽ gặp nhiều may mắn hơn những người dẫn đầu đã làm trong lĩnh vực này và sẽ có một cuộc di cư hàng loạt vì những kiến trúc và thiết kế của người dẫn đầu đó quá không linh hoạt và Cardano phù hợp hơn nhiều với tư cách là một nền tảng.

DeFi-RealFi cho số đông

Thuật ngữ *RealFi* ban đầu được đặt ra bởi giám đốc hoạt động của IOG ở Châu Phi, John O'Connor, trong blog của anh ấy vào năm 2021.⁷⁴⁶ Hiện tượng DeFi (tài chính phi tập trung) là tâm điểm của nhiều người ngoài cuộc khi nhìn vào ngành công nghiệp Crypto. Các nghiên cứu như bài báo *SoK : Tài chính phi tập trung*⁷⁴⁷ từ Đại học Hoàng gia Luân Đôn đưa ra các khái niệm cốt lõi.

RealFi là siêu bộ của DeFi, đề xuất một khung pháp lý bao gồm bốn tính năng bổ sung:

- danh tính,
- metADaTa,
- quản trị,
- tiêu chuẩn và chứng nhận

Danh tính là khái niệm cho rằng bản thân một DApp sẽ có một số đại lý. Nó sẽ có ID và người dùng của nó sẽ có ID... không phải ID truyền thống như chúng ta biết trong Web 2,⁷⁴⁸ nhưng có lẽ ID phi tập trung (DID) vẫn cho phép họ chứng minh khách hàng của bạn (KYC) và tuân thủ chống tiền rửa tiền (AML), v.v. Người dùng có thể giữ lại một số ẩn danh nhưng vẫn có thể tiết lộ dữ liệu có chọn lọc khi cần thiết.

Siêu dữ liệu đang đặt bối cảnh cho các giao dịch và tác nhân trong một hệ thống. Đó là câu chuyện rộng hơn về lý do tại sao quá trình chuyển tiền diễn ra, tại sao một số dữ liệu nhất định được cung cấp hoặc không được cung cấp. Nó có thể là các điều khoản và điều kiện, thỏa thuận người dùng cuối, được ký trước khi sử dụng DEX, v.v.

Quản trị là cách hệ thống được duy trì. Làm thế nào để một cộng đồng phi tập trung nâng cấp, cập nhật và thay đổi các tham số trong DeFi? Ai, và bằng cách nào, thực hiện thay đổi? Ngưỡng cho một số hành động là gì? Tại sao ngưỡng được đặt khác nhau cho một số bản cập nhật nhất định? Ai quyết định bản cập nhật quan trọng là gì? Những cơ chế nào đang được áp dụng? Chúng nên được tự động hóa như thế nào?

Các tiêu chuẩn và chứng nhận trong RealFi vẫn đang phát triển và cần được thống nhất. Đây là những biện pháp mà các DApp và dự án có thể được đánh giá trên thị trường. Trong một hệ sinh thái mở, phi tập trung, chúng có thể là tùy chọn nhưng cho phép người dùng biết thêm về sản phẩm hoặc nhà cung cấp dịch vụ.

Bốn tính năng này có thể được sử dụng để thực hiện một số dạng cấu trúc quy định có thể được điều chỉnh cho phù hợp với bất kỳ khu vực tài phán nào. Giờ đây, quy định không thể tránh khỏi sẽ đến với ngành công nghiệp Crypto sau hàng loạt sự cố vào năm 2022.

⁷⁴⁹Khuôn khổ này theo một cách nào đó sẽ đáp ứng nửa chừng cơ quan quản lý và hình thành quy định phi tập trung, hay còn gọi là dReg, hay còn gọi là 'công nghệ đăng ký'. Cần phải có một số hình thức lớp phủ cho các biện pháp quản lý tiêu chuẩn như đảo ngược giao dịch, đóng băng tài sản, v.v.

Động cơ đằng sau DeFi thường là các kế hoạch 'làm giàu nhanh chóng', với những kẻ xấu sử dụng tiền của khách hàng để trả tiền cho các quảng cáo của người nổi tiếng hoặc quyền đặt tên phù phiếm cho các sản phẩm vận động thể thao.

Hiếm khi có ý định cung cấp các khoản vay thực sự cho những người cần chúng ở các khu vực bị áp bức, không được tiếp cận với hệ thống tín dụng hoặc tiền tệ cơ bản. Lý do nó được gọi là *RealFi*, ngoài thực tế là bạn có bốn tính năng trên, bạn còn có quyền sử dụng thực sự và áp dụng một giải pháp thay thế cho hệ điều hành tài chính truyền thống. Một ngân xếp tài chính dựa trên Blockchain, dựa

⁷⁴⁶Chào mừng đến với thời đại của RealFi, iohk.io/en/blog/posts/2021/11/25/welcome-to-the-age-of-realfi

⁷⁴⁷ SoK : Tài chính phi tập trung (DeFi), berkeley-defi.github.io/assets/material/defi-sok-ariah-2101.08778.pdf

⁷⁴⁸Web 2.0 cho phép mọi người tạo nội dung nhưng tập trung các cơ quan có thẩm quyền và người gác cổng, chẳng hạn như các công cụ tìm kiếm chính và các nền tảng truyền thông xã hội. Web3 cho phép tương tác ngang hàng mà không cần nền tảng tập trung và trung gian.

⁷⁴⁹10 vụ lừa đảo và hack Crypto hàng đầu năm 2022, u.today/top-10-crypto-scams-and-hacks-of-2022

trên Crypto được xây dựng trên các giao thức và chủ nghĩa bình đẳng, thay vì các thực thể tập trung liên tục sụp đổ do lòng tham, sự kém cỏi và tham nhũng của con người.

Phần còn lại của chương này phác thảo một số nền tảng cho RealFi. Bạn sẽ nhận thấy rằng không có gì được kiểm soát bởi một chính phủ hoặc tổ chức liên kết.

Ngày 24 tháng 11 năm 2020. Re: động lực đằng sau Cardano. CH.⁷⁵⁰

Vậy tại sao Cardano tồn tại? Tôi đã nói chuyện trên TED vào năm 2014 và tôi đã không đi lệch hướng kể từ khi tôi làm điều đó. Tôi nói tôi quan tâm đến bản sắc kinh tế. Mỗi ngày chúng ta thức dậy, có ba tỷ người không có bản sắc kinh tế. Họ không có ngân hàng, họ ở bên ngoài nền kinh tế toàn cầu. Họ bị lừa... họ phải trả 85% lãi suất cho các khoản vay. Khi con cái của họ đến London và làm người giúp việc và chuyển tiền về, họ sẽ phải trả 15% phí cho việc đó. Khi họ có tiền, họ không thể giữ nó. Họ không có bảo hiểm, vì vậy khi thảm họa xảy ra, họ không có gì để trang trải. Vì vậy, một sự kiện tồi tệ, một cơn gió mùa, một cơn bão... tất cả đã xong. Đó là thực tế cho ba tỷ người.

... Vì vậy, giải pháp là gì? Bạn có thể là một người có trái tim phóng khoáng và đi khắp nơi quyên góp... điện thoại không hoạt động. Bạn cần một giải pháp kinh tế và cách duy nhất để có một giải pháp như vậy là cung cấp cho mọi người bản sắc kinh tế. Bạn phải cung cấp cho họ danh tính, hệ thống ngân hàng, bảo hiểm và hệ thống cho vay của riêng họ. Chúng ta đang làm gì? Chúng tôi đang mang đến cho mọi người stablecoin, sản giao dịch, khả năng chứng khoán hóa lợi ích kinh doanh của họ, cho vay ngang hàng, khả năng định lượng kiến thức bằng lời tiên tri, các mô hình kinh doanh mới như phương tiện phi tập trung, chia sẻ nội dung phi tập trung, mô hình đầu tư mạo hiểm mới... đó là những gì ngành công nghiệp của chúng tôi là về cốt lõi của nó.

ID phi tập trung Atala Prism

Atala PRISM là một nền tảng nhận dạng kỹ thuật số được xây dựng trên các nguyên tắc cốt lõi của SSI (nhận dạng tự chủ). Đây là bộ dịch vụ của IOG dành cho dữ liệu có thể kiểm chứng và nhận dạng kỹ thuật số.

Để xác định danh tính kỹ thuật số, trước tiên chúng ta phải hiểu tất cả những gì mà danh tính đòi hỏi. Danh tính kỹ thuật số là dữ liệu được máy tính sử dụng để đại diện cho một tác nhân bên ngoài. Đây có thể là một người, tổ chức, ứng dụng hoặc thiết bị. Thông tin xác thực có thể kiểm chứng là một tập hợp các xác nhận quyền sở hữu và siêu dữ liệu chứng minh bằng mật mã ai đã cấp thông tin đó. Chúng tương tự như các tài liệu vật lý mà bạn sử dụng như bằng lái xe hoặc hộ chiếu.

Một thực thể kỹ thuật số có thể sử dụng thông tin xác thực có thể kiểm chứng để chia sẻ thông tin trực tuyến. Tuy nhiên, việc trao đổi thông tin này gây ra một số lo ngại về bảo mật, chẳng hạn như mức độ an toàn của dữ liệu bạn chia sẻ sau khi dữ liệu được công khai. Ai thực sự kiểm soát dữ liệu? Nó có thực sự phi tập trung không?

Với việc phương tiện truyền thông xã hội yêu cầu rất nhiều thông tin cá nhân và các sản phẩm giao dịch Crypto tập trung hoạt động giống như ngân hàng, việc bảo vệ danh tính của chính bạn chưa bao giờ quan trọng hơn thế. **Danh tính tự chủ (SSI)** và ID phi tập trung (DID) nhằm giải quyết vấn đề này.

Danh tính tự chủ là một cách tiếp cận danh tính kỹ thuật số, dựa trên một bộ nguyên tắc,⁷⁵¹ cho phép các cá nhân kiểm soát thông tin họ sử dụng để chứng minh họ là ai trên mạng.

Mã định danh phi tập trung (DID) là một loại mã định danh cho phép nhận dạng kỹ thuật số phi tập trung, có thể kiểm chứng. Một DID có thể được gắn với bất kỳ chủ đề nào (ví dụ: một người, tổ chức, sự vật, mô hình dữ liệu, thực thể trừu tượng, v.v.) do bộ điều khiển của DID xác định. Nhóm làm việc về DID của World Wide Web Consortium (W3C) định nghĩa một DID trong đặc tả cốt lõi của nó:

- DID được kiểm soát bởi các thực thể nắm giữ chúng,
- Chúng cho phép xác thực bằng mật mã của chủ sở hữu DID,
- Chúng mô tả việc khám phá thông tin cần thiết để khởi chạy các phương thức liên lạc bảo mật và bảo mật.
- Cấp quyền truy cập vào tính di động của dữ liệu độc lập với dịch vụ.

⁷⁵⁰

CROW.. Trực tiếp với Charles Hoskinson của Cardano ADA 24/11/20, [youtube.com/watch?v=z3s6olBfbfA](https://www.youtube.com/watch?v=z3s6olBfbfA)

⁷⁵¹

Nguyên tắc SSI, github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

Vào tháng 6 năm 2022, World Wide Web Consortium (W3C) đã phê duyệt việc nâng cấp thông số kỹ thuật lõi DID lên giai đoạn *Đề xuất W3C*. Đây là một cột mốc quan trọng vì nó xác nhận việc nghiên cứu liên tục về nhận dạng kỹ thuật số và mở đường cho các nền tảng nhận dạng như Atala PRISM. Sự chấp thuận của thông số kỹ thuật, bị phản đối bởi một số gã khổng lồ công nghệ lớn (Google, Apple, et al), mang lại cho DID sự tin cậy và động lực để áp dụng rộng rãi hơn.

Atala PRISM V2: A suite of identity infrastructure products

PRISM V2 is Atala’s next-generation SSI offering, based on the learnings of Atala PRISM V1.x

- Supports **global identity standards** that make Atala solutions more widely applicable across different ecosystems and use cases
- Improved architectural model to increase **maintainability** and **scalability**
- **Differentiates** through values and approach (privacy preservation, ease of integration into ecosystems, performance)
- Targeted towards two key stakeholders in the new data economy:
 - **Individuals** – by making verifiable data work in the form of seamless, trustworthy interactions
 - **Service providers** that need to meet compliance needs

Atala PRISM V2 Suite of Infrastructure Products	
Onboard	Identity enrollment
Issue	Credential creation and issuance
Verify	Online credential verification
Connect	Secure P2P interactions
Authenticate	Authentication using DIDs/VCs
Manage	System management & integration

Hình 70: Atala Prism V2, từ Denitsa Bài nói chuyện của Bogoeva tại ScotFest.

Nhóm Atala Prism đã làm việc với DID được một thời gian. Họ đã triển khai các giải pháp quy mô lớn như DISH (dish.com) ở Hoa Kỳ và Bộ Giáo dục Ethiopia. Họ cũng có một chương trình tiên phong , với hai chương trình đã hoàn thành vào năm 2022 và hơn 200 nhà phát triển đang xây dựng trên Atala.

Atala Prism V2 được xây dựng dựa trên các bài học trong vài năm qua và giải quyết các vấn đề như tuân thủ các tiêu chuẩn và tuân thủ luật chẳng hạn như Quy tắc đi lại. ⁷⁵²Nó được xây dựng để tích hợp liền mạch với các đối tác như ví nhẹ *Lace* .

Phí Babel

Cardano đang giới thiệu một cơ chế mới cho phép thanh toán phí giao dịch bằng Token do người dùng xác định trên Cardano. Phí Babel được đặt tên theo Cá Babel, ⁷⁵³một sinh vật trong cuốn sách *The Hitchhiker's Guide to the Galaxy của Douglas ADAm* cho phép bạn nghe bất kỳ ngôn ngữ nào được dịch sang ngôn ngữ của riêng bạn. Bất chấp nhiều ngôn ngữ đa dạng của thiên hà, tầm nhìn dịch thuật toàn cầu này mang lại khả năng giao tiếp có ý nghĩa.

Hợp đồng thông minh cho phép tạo ra nhiều loại Token độc đáo trong lĩnh vực Crypto. Phí Babel dựa trên ý tưởng sử dụng Token ưa thích của bạn để tương tác với nền tảng. Tương tự như cách bạn sẽ tương tác với các hệ thống tài chính cũ, nơi bạn sẽ sử dụng nội tệ của mình bằng cách chỉ cần thực hiện lựa chọn trong danh sách thả xuống. 'Phí Babel' chuyển đổi Token bạn đang sử dụng thành Token mà nền tảng yêu cầu cho các giao dịch hoặc bất kỳ giao dịch nào bạn muốn thực hiện trên nền tảng. Nhà khoa học trưởng của IOG, Giáo sư Aggelos Kiavias , ⁷⁵⁴đã đi trước đón đầu khi giới thiệu khái niệm này vào đầu năm 2021. IOG cũng đã sản xuất một

⁷⁵²Quy tắc Di chuyển yêu cầu các bên lấy và trao đổi thông tin người thụ hưởng và người khởi tạo với việc chuyển tài sản ảo qua một ngưỡng nhất định.
⁷⁵³

Cá Babel, quá giang.fandom.com/wiki/ Babel_Fish .
⁷⁵⁴

video hướng dẫn về bảng trắng⁷⁵⁵ trên kênh YouTube 'IOHK' của họ vào thời điểm đó. Bài báo 'Phí Babel thông qua trách nhiệm hữu hạn' sau đó đã được xuất bản vào tháng 4 năm 2022.⁷⁵⁶

Trong hầu hết các Blockchain, thông thường người gửi phải trả phí cho một giao dịch hợp pháp. Nếu không có giới hạn như vậy, bất kỳ ai cũng có thể áp đảo hệ thống bằng các giao dịch nhỏ, làm vượt quá khả năng của nó và khiến nó trở nên vô giá trị. Trên cơ sở đó, một ngụ ý chung là đối với bất kỳ Blockchain nào hỗ trợ tiền tệ do người dùng xác định, việc thanh toán phí giao dịch bằng các Token đó sẽ bị cấm. Thay vào đó, các giao dịch phải được tính phí bằng Token gốc của nền tảng, được coi là có giá trị đối với tất cả những người nắm giữ Token (hodlers⁷⁵⁷). Người ta cho rằng giới hạn như vậy là không tốt cho việc áp dụng và khả năng tương tác với các Blockchain và hệ thống kế thừa khác. IOG dự định khắc phục thiếu sót này như thế nào?

eUTXO cho phép đổi mới

Mật mã học và lý thuyết trò chơi⁷⁵⁸ có lịch sử biến những điều dường như không thể thành hiện thực. Kiến trúc UTXO mở rộng (eUTXO) của Cardano cho phép một giải pháp nhờ vào cách thức hoạt động của các tài sản gốc trên nền tảng.

Các Token có thể được tạo bằng cách sử dụng chính sách đúc tiền và chúng được coi là tương tự như ADA trên sổ cái. Tạo một giao dịch hợp lệ yêu cầu sử dụng một hoặc nhiều UTXO. Trên Cardano, một UTXO có thể chứa nhiều thứ hơn là chỉ đơn giản là ADA; nó cũng có thể xử lý một gói Token chứa nhiều Token riêng biệt, cả có thể thay thế và không thể thay thế. Do đó, có thể sử dụng một UTXO duy nhất để xây dựng các giao dịch chuyển nhiều Token riêng biệt. Vì vậy, những người tiên phong bị đánh giá thấp trong không gian Crypto, đã phân phối 15 nghìn đầu ra cho mỗi giao dịch bằng cách sử dụng EUTXO và các bản tổng hợp.⁷⁵⁹

Phí giao dịch của sổ cái được định giá bằng ADA, sử dụng một chức năng cố định làm tham số sổ cái. Các chi phí cần thiết cho một giao dịch thành công có thể được dự đoán chính xác trước khi thực hiện, đây là điểm mạnh chính của kiến trúc EUTXO của Cardano. Đây là một thuộc tính duy nhất mà các cấu hình sổ cái khác không có.

Phí Babel sẽ hoạt động như thế nào?

Phí babel cho phép một giao dịch thông báo một khoản nợ bằng mệnh giá ADA bằng với số phí mà người phát hành giao dịch phải trả. Một giao dịch như thế này sẽ bị sổ cái từ chối. Tuy nhiên, nó có thể được coi là một đề nghị mở trong đó khoản nợ được thực hiện. Tại sao ai đó sẽ chấp nhận một gánh nặng như vậy? Để làm cho điều này trở nên hấp dẫn, giao dịch có thể cung cấp một số lượng (các) Token cho bất kỳ ai trả nợ. Giá định là gói Token đã tồn tại trong Cardano. Đây sẽ là giao dịch một đổi một giữa ADA và (các) Token nhất định với tỷ lệ cố định.

Hãy xem xét một nhà sản xuất Block nhận thấy một giao dịch như thế này. Nhà sản xuất Block có thể tạo ra một giao dịch phù hợp và yêu cầu các Token được cung cấp bằng cách hấp thụ khoản nợ và trang trải nó bằng ADA. Giao dịch với khoản nợ, cũng như giao dịch phù hợp của nó, được chấp nhận vào sổ cái dưới dạng một nhóm. Tập hợp hai giao dịch được định giá theo tổng thể ADA do hấp thụ nợ và do đó, nó không vi phạm các yêu cầu kế toán của sổ cái về phí ADA. Do đó, giao dịch với khoản nợ được giải quyết.

Người dùng có thể đề xuất các giao dịch được định giá bằng bất kỳ (các) Token nào họ sở hữu và để chúng thanh toán trong sổ cái như các giao dịch thông thường nếu một nhà sản xuất Block sẵn sàng tiếp nhận chúng trong giao dịch giao ngay.⁷⁶⁰ Điều này cho thấy cách

Phí Babel, iohk.io/en/blog/posts/2021/02/25/babel-fees/

⁷⁵⁵ Cardano360 - Tháng 2 năm 2021, youtu.be/YXaK0cvgoFQ?t=2184

⁷⁵⁶Chakravarty, Karayannidis, Kiayias, Peyton Jones, Vinogradova (2022), 'Phí Babel thông qua trách nhiệm hữu hạn', iohk.io/en/research/library/papers/babel-fees-via-limited-liabilities/

⁷⁵⁷

HODL là tiếng lóng trong cộng đồng Crypto để chỉ việc nắm giữ Crypto thay vì bán nó. HODL cũng có thể có nghĩa là 'Giữ lấy cuộc sống thân yêu' và đề cập đến việc không bán, ngay cả khi thị trường biến động mạnh và hoạt động thị trường kém.

⁷⁵⁸

Lý thuyết trò chơi là nghiên cứu về các mô hình toán học về tương tác chiến lược giữa những người ra quyết định hợp lý. Nó có ứng dụng trong tất cả các lĩnh vực khoa học xã hội, cũng như logic và khoa học máy tính. Ban đầu, nó giải quyết các trò chơi có tổng bằng không, trong đó lợi nhuận hoặc thua lỗ của mỗi người tham gia được cân bằng chính xác với lợi ích của những người tham gia khác. Ngày nay, lý thuyết trò chơi áp dụng cho một loạt các mối quan hệ hành vi và hiện là một thuật ngữ chung cho khoa học về việc ra quyết định hợp lý ở người, động vật và máy tính.

⁷⁵⁹

Hội nghị bàn tròn với Charles Hoskinson và Alex Chepunoy | Ergo Pulse, youtube.com/watch?v=k9a3SYV6FJA

⁷⁶⁰

Giao dịch giao ngay là một quá trình liên tục mua và bán Token và tiền xu ở mức giá giao ngay để thanh toán ngay lập tức. Nhà giao dịch thường có ý định kiếm lợi nhuận từ những biến động của thị trường.

tài sản gốc, kiến trúc EUTXO và thay đổi nhỏ nhưng mạnh mẽ trong việc bổ sung các khoản nợ dưới dạng giá trị âm trong gói Token có thể xử lý phí Babel, cho phép người dùng định giá giao dịch bằng bất kỳ Token nào mà hệ thống hỗ trợ nguyên bản.

Để khái niệm trên hoạt động, Cardano phải có các nhà cung cấp thanh khoản có ADA và sẵn sàng phát hành các giao dịch phù hợp. Hệ sinh thái gồm hàng nghìn nhà khai thác Stake Pool (SPO) rõ ràng là những ứng cử viên ban đầu để tạo ra thị trường bằng cách quảng cáo tỷ giá hối đoái cho các Token ưa thích của họ, v.v.

Sau khi giới thiệu tài sản gốc với *Mary* hard fork, khả năng số tiền âm trong các gói Token có thể được đưa vào các quy tắc sổ cái của Cardano. Ngoài phí Babel, điều này mở ra các trường hợp sử dụng khác như hoán đổi nguyên tử⁷⁶¹ cho các giao dịch giao ngay. Đó chỉ là một ví dụ khác về cách Cardano đổi mới thay vì rẽ nhánh và sao chép các Blockchain thế hệ thứ nhất và thứ hai.

Một ví dụ làm việc

Dưới đây là một giao dịch ví dụ ở định dạng con người có thể đọc được. Đây là về Bill, Ted và Barney trao đổi ADA và một Token gốc mới, JohnCoin (JCN).

Giao dịch:

< **Nhận** 20 ADA từ Bill

> **Gửi** 10 ADA cho Ted

> **Gửi** 9,66 ADA tới Bill

–Sử dụng 0,34 ADA làm phí giao dịch

Bill đã nhận được 20 ADA trong quá khứ, do đó, có một UTXO trị giá 20 ADA ở Daedalus. Anh ta lấy UTXO đó, gửi 10 ADA cho Ted, 9,66 ADA trả lại cho chính mình và sử dụng 0,34 còn lại làm phí giao dịch. Để nó trở thành một giao dịch hợp pháp, đầu vào và đầu ra phải bằng nhau, nghĩa là $20 = 10 + 9,66 + 0,34$

Bây giờ, hãy xem xét một giao dịch sử dụng JohnCoin, JCN cũng như ADA.

Giao dịch:

< **Nhận** 20 JCN từ hóa đơn

< **Nhận** 4 ADA từ Bill

> **Gửi** 10 JCN cho Ted

> **Gửi** 10 JCN đến hóa đơn

> **Gửi** 3,66 ADA tới Bill

–Sử dụng 0,34 ADA làm phí giao dịch

Lần này Bill muốn gửi 10 JCN cho Ted. Anh ấy cũng phải thêm một số khoản 'phụ trội' để trang trải phí giao dịch. Nó hoạt động tốt, nhưng nó bất tiện và không thực sự bền vững nếu chúng tôi xử lý hàng trăm, hoặc hàng nghìn giao dịch.

Đây là cách giao dịch tương tự này sẽ hoạt động với phí Babel.

Giao dịch:

< **Nhận** 20 JCN từ hóa đơn

> **Gửi** 10 JCN cho Ted

> **Gửi** 8 JCN đến hóa đơn

> **Gửi** -0,34 ADA và 2 JCN cho bất kỳ ai nhận khoản nợ

–Sử dụng 0,34 ADA làm phí giao dịch

Điều này đặt ra một số câu hỏi:

Làm thế nào Bill có thể trả khoản phí 0,34 ADA nếu ngay từ đầu anh ấy không có bất kỳ ADA nào trong Daedalus? Với phí babel, đây không phải là vấn đề. Miễn là đầu vào bằng với đầu ra, giao dịch là hợp pháp. ADA âm và dương trong các đầu ra triệt tiêu lẫn nhau.

761

Hoán đổi nguyên tử là trao đổi Crypto từ các Blockchain riêng biệt. Việc hoán đổi được tiến hành giữa hai thực thể mà không có sự tham gia của bên thứ ba. Ý tưởng là loại bỏ các trung gian tập trung như sàn giao dịch được quy định và cung cấp cho chủ sở hữu Token toàn quyền kiểm soát.

Làm cách nào Bill có thể gửi một lượng ADA âm cho bất kỳ ai, như một giao dịch hợp lệ? Nó không phải là một giao dịch hợp lệ cho đến khi ai đó 'tình nguyện' nhận nợ. Nó phải là tự nguyện vì không ai có thể gửi ADA tiêu cực mà không có sự cho phép của họ. Tại sao ai cũng 'tình nguyện' nhận nợ? Họ sẽ không chỉ nhận nợ, tức là . ADA phủ định, họ cũng sẽ nhận được thêm 2 JCN.

Vì vậy, người dùng đầu tiên 'tình nguyện' nhận nợ, Barney trong ví dụ này, sẽ thực hiện một giao dịch như sau:

Giao dịch:

<Nhận 4 ADA từ Barney

<Nhận -0,34 ADA và 2 JCN từ giao dịch của Bill

>Gửi 3,32 ADA tới Barney

>Gửi 2 JCN cho Barney

-Sử dụng 0,34 ADA làm phí giao dịch

Barney đã tình nguyện nhận khoản nợ -0,34, để làm như vậy xác thực giao dịch của Bill. Về mặt kỹ thuật, tất cả các khoản phí đều được thanh toán bằng ADA, tuy nhiên, theo cách nhìn của Bill, anh ấy chỉ thanh toán bằng JCN.

Nếu Barney muốn 2 JCN, anh ấy cũng phải chấp nhận -0,34 ADA. Chúng không thể tách rời nhau. Lưu ý rằng vì cần có hai giao dịch để quy trình này hoạt động nên tổng số phí phải trả cao gấp đôi so với bình thường, 0,68 ADA.

Điều này có nghĩa là số tiền JCN mà Bill trả phải lớn hơn hoặc bằng 0,68 ADA thì số tiền đó mới xứng đáng với Barney. Vì phí trên Cardano tương đối nhỏ so với các chuỗi khác, nên việc tăng gấp đôi chúng không phải là vấn đề lớn.

Hệ thống này hoạt động miễn là có những người dùng coi tài sản 'JohnCoin' JCN có giá trị. Họ sẽ cạnh tranh trong một thị trường công bằng và cò mồi để đưa ra tỷ giá hối đoái tốt nhất cho các khoản phí. Các Token không được coi là có giá trị sẽ vô dụng trong hệ thống này và không thể được sử dụng để thanh toán phí, nhưng đó là cách nó nên diễn ra.

Nghiên cứu đi vào cuộc sống

Phí Babel chỉ là một lĩnh vực mà IOG đang đưa nghiên cứu vào thực tế. Kỹ sư nghiên cứu của IOG, Paulina Vinogradova, đã trình bày các giải pháp tính toán đang được xem xét, phân tích tính cạnh tranh của các giải pháp của các chuỗi khác, cũng như một số thách thức còn lại trong bài thuyết trình này.⁷⁶²

Ngày 27 tháng 2 năm 2021. Re: Phí Babel. CH:⁷⁶³

...về cơ bản, những gì nó làm là cung cấp cho mọi Token được phát hành trên Cardano khả năng thanh toán bằng tài sản gốc, nếu có thị trường cho nó. Vì vậy, nó giải quyết tất cả các vấn đề cùng một lúc và bạn, với tư cách là người phát hành Token, hiện có mạng của riêng bạn. Trước đây, bạn phải mượn một mạng khác và trả phí của mạng đó, hoặc bạn phải khởi chạy mạng của riêng mình và xây dựng hiệu ứng mạng đằng sau nó. Đây là lựa chọn thứ ba. Không gian hiện tại không cho phép điều đó tồn tại. Có một số cách hack thông minh ở đây và ở đó, nhưng phần lớn, đó là một điều mới. Đó là một thứ tạo nhả và là một thứ được mang đến một cách độc đáo nhờ Extended UTXO.

Và đó là điều kỳ diệu của việc làm mọi thứ một cách chính xác. Khi bạn làm mọi thứ một cách chính xác, sẽ rất dễ dàng để đổi mới và chỉ cần thêm vào và nói, 'bạn bắt đầu'. Điều đó có nghĩa là chúng tôi có thể sẽ trở thành nền tảng stablecoin cuối cùng cho tất cả các stablecoin vì bạn phải trả phí giao dịch bằng stablecoin. Bạn không phải trả 100 ETH để gửi một đô la Tether.⁷⁶⁴ bạn biết đó chính là điểm mấu chốt, và đó là điều chúng tôi đang tìm kiếm và đó chỉ là một trong nhiều điều đã đến.

phí ổn định

Cardano có một kỹ thuật mới để làm cho phí công bằng hơn, ổn định hơn và có thể dự đoán được theo thời gian. Việc cho phép giao dịch trên nền tảng Crypto vì phạm mục đích kép của tài sản cơ bản của nền tảng. Một mặt, người dùng có thể giữ và giao dịch nó như một phần trong danh mục đầu tư của họ. Mặt khác, nó cung cấp 'khí' cần thiết để xử lý giao dịch. Do tính hai mặt này, hệ thống nên có

⁷⁶²Phí Babel thông qua trách nhiệm hữu hạn, [youtube.com/watch?v=iJEmRZ6leXE](https://www.youtube.com/watch?v=iJEmRZ6leXE)

⁷⁶³

AMA bắt đầu ngày 26/02/2021, [youtube.be/6eD_mII3ms?t=42](https://www.youtube.be/6eD_mII3ms?t=42)

⁷⁶⁴

Tether (mã USDT) là một loại Crypto được lưu trữ trên các Blockchain Ethereum và Bitcoin, cùng với các Blockchain khác. Token của nó được phát hành bởi công ty Tether Limited của Hồng Kông, do đó được kiểm soát bởi các chủ sở hữu của Bitfinex. Tether được gọi là stablecoin vì ban đầu nó được thiết kế để luôn có giá trị US\$1,00, duy trì dự trữ \$1,00 cho mỗi Tether được phát hành.

một quy trình thay đổi giá giao dịch để chúng luôn cạnh tranh và được chấp nhận. Hệ thống cũng sẽ cho phép người dùng xác định mức phí tối ưu để xử lý giao dịch nhanh chóng, dựa trên nhu cầu cụ thể của họ .

Phí giao dịch được yêu cầu vì ba lý do: Đối với người mới bắt đầu, quá trình xử lý giao dịch sẽ tiêu tốn hệ thống về mặt hoặc tài nguyên tiêu thụ. Việc cho phép các bộ xử lý giao dịch, SPO, bù đắp chi phí của họ là điều công bằng. Thứ hai, ngay cả với khả năng vô hạn về mặt lý thuyết, các nhà phát hành giao dịch phải được ngăn chặn làm tràn mạng với các giao dịch vô giá trị trong một cuộc tấn công DDoS. Thứ ba, khuyến khích các bộ xử lý giao dịch cung cấp dịch vụ chất lượng cao là một thông lệ tốt.

Các vấn đề trên có thể được giải quyết bằng cách tính phí giao dịch.

Học hỏi từ quá khứ

Hệ thống định giá giao dịch đầu tiên trên sổ cái phân tán được giới thiệu bởi Bitcoin. Hệ thống này hoạt động theo cách tương tự như đấu giá theo giá đầu tiên: giao dịch đặt giá thầu cho một vị trí trong khối với phần thưởng nhất định và nhà sản xuất Block chọn giao dịch nào sẽ được đưa vào. Các nhà sản xuất Block cũng được trao quyền đúc tiền mới, nghĩa là hoạt động của họ được tài trợ bởi toàn bộ cộng đồng thông qua việc tăng nguồn cung tiền tệ tổng thể. Theo thời gian, lạm phát giảm tuyến tính và phí giao dịch trở nên nổi bật hơn trong phần thưởng. Quá trình này đã bị thách thức vì sự kém hiệu quả của nó, mặc dù thực tế là nó đã cho phép Bitcoin hoạt động tốt trong hơn một thập kỷ. Theo thời gian, phí giao dịch cũng tăng lên.

Vào mùa hè năm 2021, IOG đã giới thiệu một cơ chế mới khen ngợi ⁷⁶⁵ ý tưởng về phí Babel và mở rộng cách tiếp cận của Cardano đối với các quy tắc sổ cái và tài sản hệ thống. Mục tiêu là làm cho phí công bằng, nhất quán và có thể dự đoán được theo thời gian. Cơ chế này được mô tả trong ngữ cảnh của Cardano nhưng nó có thể được áp dụng cho bất kỳ loại Crypto nào khác có thuộc tính tương đương.

Phí ổn định là gì?

Khái niệm trung tâm của Stablefees là cung cấp giá cơ bản cho các giao dịch bằng cách ràng buộc chúng với một rổ hàng hóa hoặc tiền tệ. Phí ổn định bao gồm hợp đồng 'dự trữ phi tập trung' gốc tạo ra và quản lý một loại tiền ổn định được gắn vào giỏ.

Ý tưởng này phản ánh hoạt động của SDR (Quyền rút vốn đặc biệt) của Quỹ Tiền tệ Quốc tế, ⁷⁶⁶ là một loại tiền tệ fiat được đánh giá dựa trên một rổ gồm năm loại tiền tệ: đô la Mỹ, đồng euro, đồng nhân dân tệ Trung Quốc, đồng yên Nhật và bảng Anh đồng bảng Anh. Stablecoin, hay 'Tiền xu tương đương trong rổ' (BEC), là loại tiền được sử dụng để thanh toán phí giao dịch (và các nhu cầu định giá khác của nền tảng như chi phí vận hành Stake Pool).

ADA có một mục đích kép trong hệ thống này: nó phục vụ như một tài sản dự trữ cho dự trữ phi tập trung và như một đơn vị phần thưởng cho việc đặt cược. Trong những trường hợp nghiêm trọng khi tính thanh khoản của hợp đồng dự trữ cạn kiệt, nó cũng có thể được sử dụng làm tiền tệ dự phòng. Tổ chức phát hành sẽ cần nhận BEC trước khi hoàn tất giao dịch, thông qua bên thứ ba hoặc trực tiếp bằng cách chuyển ADA sang hợp đồng dự trữ phi tập trung.

Dự trữ sẽ sử dụng tiêu chí nào để phân phối BEC? Đổi lại, hợp đồng dự trữ cũng sẽ phát hành cổ phiếu vốn, được gọi là tiền vốn cổ phần phi tập trung (DEC). Dự trữ phi tập trung thường sẽ thay đổi giá trị của BEC để gắn với rổ hàng hóa cơ bản bằng cách tận dụng giá trị của DEC. DEC sẽ hấp thụ ADA so với biến động của rổ để giữ giá trị thực của BEC nhất quán. Đồng tiền ổn định AgeUSD ⁷⁶⁷ đã được triển khai trên Ergo (sigmusd.io). Ergo (ergoplatform.org) là một Blockchain bằng chứng công việc sáng tạo (cũng dựa trên EUTXO) được đồng sáng lập bởi Alex Chepurinov phi thường ⁷⁶⁸.

Ba đồng xu này, được phát hành bởi hệ thống nguyên bản, sẽ thu hút các nhóm khác nhau. Tính bảo mật và tính thanh khoản của BEC (Đồng xu tương đương trong rổ) có thể thu hút các nhà đầu tư ưa thích rủi ro, giao dịch nhiều. DEC (đồng tiền cổ phần phi tập trung) sẽ nhận được nhiều lợi ích nhất nếu ADA tăng nhưng sẽ chịu tổn thất lớn nhất nếu ADA giảm. DEC có thể hấp dẫn hơn đối với các nhà đầu tư dài hạn. Hơn nữa, vì dự trữ phi tập trung định giá các loại tiền này theo ADA, nên cả BEC và DEC đều có thể giúp việc đặt cược và quản trị dễ dàng hơn. Lợi nhuận có thể được cung cấp ở các mức giá khác nhau, tùy thuộc vào loại xu. Cuối cùng, tất cả các phần thưởng sẽ được định giá và thanh toán bằng ADA, đây sẽ tiếp tục là loại tiền dễ thích ứng nhất trong ba loại tiền tệ.

⁷⁶⁵

Phí Babel - chi phí giao dịch bằng token gốc, iohk.io/en/blog/posts/2021/02/25/babel-fees/

⁷⁶⁶

Quyền rút vốn đặc biệt (SDR), imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR

⁷⁶⁷

Giao thức AgeUSD Stablecoin, github.com/Emurgo/age-usd

⁷⁶⁸

Alexander Chepurinov , ergoplatform.org/vi/hall_of_fame/

nhà tiên tri

Một nhà tiên tri trên chuỗi là trung tâm của hệ thống này, xác định giá của giỏ trong ADA. Tiên tri này có thể được thực hiện bằng cách sử dụng các SPO (SPO) theo cách phi tập trung. Từ các khoản phí nhận được trong quá trình phát hành BEC/DEC, quỹ dự trữ có thể trao thêm phần thưởng cho tất cả những người đóng góp cho tiên tri. Điều này sẽ đảm bảo hai điều: hàng nghìn người đóng góp từ khắp nơi trên thế giới và các quy tắc sổ cái tính toán tỷ giá hối đoái tổng hợp theo cách chuẩn mực. Ví dụ: thông qua giá trị trung bình có trọng số trên tất cả các lần gửi giá trong một kỳ nguyên. Nếu những người đóng góp cho Oracle lạm dụng đóng góp của họ, danh tiếng và hiệu suất của họ trên chuỗi có thể được theo dõi và họ có thể phải chịu trách nhiệm.

Giá cả hoạt động như thế nào?

Các giao dịch nên được định giá như thế nào và các nhà sản xuất Block được thưởng như thế nào? Sử dụng cách tiếp cận hiện có trên Cardano, mỗi giao dịch sẽ được chuyển đổi một cách xác định thành một giá trị cụ thể có mệnh giá bằng BEC, sử dụng công thức được xác định bởi các quy tắc sổ cái. Công thức sẽ xem xét quy mô giao dịch cũng như nhu cầu xử lý và có thể bao gồm các chỉ số thời gian chạy như tải hệ thống trung bình. Phí cơ sở sẽ là kết quả, đảm bảo rằng giao dịch sẽ được thực hiện bởi hệ thống. Người dùng cuối sẽ có thể tăng phí bằng cách áp dụng hệ số nhân cho phí cơ bản và tăng tốc độ xử lý. Điều này sẽ rất quan trọng trong thời kỳ nhu cầu cao.

Ngược lại với mô hình đầu giá theo giá đầu tiên, chiến lược này có một lợi thế: cơ chế định giá liên tục được ổn định theo giá trị mặc định hợp lý. Nếu cần, người dùng thực hiện khám phá giá chỉ theo một hướng để tăng tốc độ xử lý. Hơn nữa, các tổ chức phát hành giao dịch có thể tích trữ BEC để bảo vệ khả năng phát hành giao dịch trong tương lai của họ đồng thời tránh biến động giá ADA.

Phí ổn định so với phí Babel

Cơ chế Phí ổn định có thể được coi là phần mở rộng của phí Babel và cả hai cơ chế đều hoạt động tốt và bổ sung cho nhau. Phí Babel có thể được sử dụng song song với Stablefees với một lưu ý: thay vì ADA, BEC có thể được sử dụng để thanh toán phí Babel. Điều này có nghĩa là tất cả các chi phí sẽ được thanh toán bằng ADA (thông qua trách nhiệm pháp lý về phí Babel có thể chuyển đổi thành ADA ngay tại chỗ). Do đó, toàn bộ quá trình tương thích ngược ở chỗ nó sẽ không ảnh hưởng đến những người dùng bình thường chỉ có ADA và không muốn nhận BEC.

Về tính đa dạng, trong khi kịch bản trên mô tả một BEC toàn cầu duy nhất, kỹ thuật tương tự có thể được sử dụng để phát hành các BEC khu vực được chốt vào nhiều giỏ hàng hóa với trọng số khác nhau. Các BEC 'khu vực' như vậy sẽ có thể tăng cường tính toàn diện của hệ thống đồng thời cho phép các SPO có các chính sách bao gồm giao dịch chi tiết hơn.

Stablefees thay thế 'nhẹ'

Cách tiếp cận trên đòi hỏi phải sử dụng hợp đồng dự trữ phi tập trung và hợp đồng phát hành BEC và DEC (đồng tiền cổ phần phi tập trung) cho người mua. Một phiên bản 'lite' bỏ qua hợp đồng dự trữ và thay vào đó sửa đổi công thức tính phí trực tiếp bằng cách sử dụng tiên tri giá để chốt nó vào rổ hàng hóa đã thỏa thuận. Cơ chế dẫn đến biểu thị chi phí giao dịch trong BEC và ngay lập tức chuyển đổi chúng thành ADA. Số tiền đến hạn thay đổi dựa trên giá trị của BEC. Quá trình này có thể so sánh được với hệ số nhân cho phép khám phá giá một chiều.

Hạn chế chính là nhà phát hành giao dịch tiềm năng không có quyền truy cập vào Token gốc cho phép xử lý giao dịch có thể dự đoán được; thay vào đó, người phát hành giao dịch phải trả phí bằng ADA. Tuy nhiên, phí sẽ thích ứng và giữ ổn định so với rổ do cơ chế chốt. Do đó, một nhà phát hành giao dịch sẽ có thể cấu trúc đúng danh mục tài sản ngoài chuỗi của họ để phù hợp với yêu cầu giao dịch của họ.

Phương pháp tiếp cận dựa trên nghiên cứu

Các khía cạnh chi tiết của cơ chế Stablefees đang được IOG nghiên cứu. Charles Hoskinson đã đề cập trong một bản cập nhật gần đây⁷⁶⁹ rằng Định giá theo Bạc và Phí Babel là những kết quả thấp cần sớm được triển khai. Có khả năng Stablefees cũng sẽ tuân theo khung thời gian đó. Nhà tiên tri định giá và BEC toàn cầu rất có thể sẽ tìm thấy nhiều cách sử dụng hơn ngoài việc chỉ trả phí giao dịch, mở rộng tiềm năng của Cardano DApps.

⁷⁶⁹ AMA bắt ngày 01/07/2023, youtube.be/djhKk-3rYhU?t=875

Định giá theo cấp độ khi mạng mở rộng

Việc áp dụng Cardano sẽ tiếp tục phát triển khi nhu cầu về tài chính phi tập trung tăng lên. Nhóm nghiên cứu của IOG đang liên tục xem xét các phương pháp để đảm bảo rằng tất cả người dùng đều có quyền truy cập và thông lượng như nhau. Mạng Cardano sẽ mở rộng và phát triển để đáp ứng nhu cầu về hợp đồng thông minh và DeFi. Tương tự, mô hình phí giao dịch được sử dụng bởi Cardano sẽ cần được nâng cấp.

Cách tiếp cận hiện tại rất đơn giản và công bằng: mọi giao dịch đều được xử lý như nhau và người dùng không thể thay đổi mức độ ưu tiên của họ bằng cách trả phí cao hơn. Chiến lược này hoạt động hiệu quả miễn là khả năng thông qua tương tự như nhu cầu.

Tuy nhiên, có những nhược điểm nhất định. Với nhiều người sử dụng Cardano hơn, sẽ đến lúc không phải tất cả các giao dịch đều có thể được đưa vào Blockchain, ngay cả khi các tham số được điều chỉnh. Mặc dù việc tăng cường năng lực của chuỗi chính và định tuyến các giao dịch tới Hydra sẽ giúp giải quyết vấn đề này, nhưng hệ thống cốt lõi phải luôn duy trì khả năng thích ứng trong mọi tình huống tiềm ẩn.

Trong trường hợp bị tấn công từ chối dịch vụ (DoS), điều này rất quan trọng. Với hệ thống như hiện tại, kẻ tấn công có thể lợi dụng tính công bằng của hệ thống và chuyển thư rác có hại của chúng dưới dạng các giao dịch hợp pháp, khiến những người khác phải chờ đợi lâu hơn. Có những biện pháp bảo vệ tại chỗ khiến một cuộc tấn công như thế này trở nên không thực tế. Tuy nhiên, để bảo mật hơn nữa, mạng sẽ có thể tăng chi phí cho các cuộc tấn công như vậy mà không gây nguy hiểm cho tính công bằng và hiệu quả về giá của hệ thống.

Vào năm 2022, các thành viên trong nhóm nghiên cứu của IOG đã bắt đầu nghiên cứu vấn đề này. Giải pháp được trình bày bảo tồn các nền tảng của quá trình xử lý giao dịch Cardano (khả năng dự đoán, công bằng và quyền truy cập giá rẻ) đồng thời giải quyết các thách thức có thể phát triển khi nhu cầu tăng lên. Đối với các Blockchain, phương pháp của IOG đề xuất một cấu trúc phí giao dịch sáng tạo. Tính năng chính của thiết kế là chia mỗi khối thành ba 'bậc' tùy thuộc vào trường hợp sử dụng. Mỗi tầng dành cho các loại giao dịch khác nhau và chiếm một tỷ lệ nhất định trong kích thước khối tối đa. Các bậc, cũng như cách phân chia được đề xuất mà IOG đã xem xét, như sau:

- công bằng (50%)
- cân bằng (30%)
- ngay lập tức (20%)



Hình 71: Định giá theo tầng: một khối có thể được chia thành ba tầng.

Đi từ phải sang trái từ hình trên... Chức năng 'Ngay lập tức' và 'Cân bằng' bằng cách có 'ngưỡng phí' riêng biệt cho mỗi loại. Người phát hành giao dịch sẽ xác định cấp độ dịch vụ mà họ cần để được đưa vào một khối. Điều này có thể được thực hiện bằng cách áp đặt mức trần phí giao dịch. Sau đó, bắt đầu với cấp 'ngay lập tức', cấp 'cân bằng' và cuối cùng là cấp 'công bằng', mỗi khối sẽ được lấp đầy. Trong cùng một hạng, các giao dịch tương tự sẽ được tính cùng một tỷ lệ. Để đưa ra quyết định này dễ dàng hơn, mỗi giao dịch sẽ chỉ được trả một khoản phí nhỏ nhất để đảm bảo việc đưa nó vào khối. Phí cho các bậc 'ngay lập tức' và 'cân bằng' sẽ được điều chỉnh linh

hoạt và xác định sau mỗi khối (sử dụng các mức nhu cầu trong các Block trước đó) để đảm bảo rằng mỗi bậc tiêu thụ phần trăm khối mong muốn của nó.

Sự khác biệt giữa các bậc 'ngay lập tức' và 'cân bằng' là cách thay đổi phí, đáng chú ý là 'tốc độ' mà chúng thay đổi theo tài hiện tại. Ngưỡng dịch vụ 'ngay lập tức' sẽ luôn lớn hơn ngưỡng 'cân bằng', phản ứng nhanh hơn với nhu cầu và đảm bảo rằng giao dịch yêu cầu nó sẽ được phục vụ nhanh nhất có thể. Ngưỡng 'cân bằng' sẽ chậm thích ứng hơn và ổn định hơn, khiến nó không phù hợp với các giao dịch nhạy cảm với thời gian, nhưng nó sẽ cung cấp mức giá thấp hơn, nhất quán hơn để đổi lấy thời gian chờ đợi lâu hơn, nhiều biến động hơn.

Các cấp 'cân bằng' và 'ngay lập tức' được thiết kế để quản lý các giao dịch với mức độ khẩn cấp khác nhau, trong khi cấp 'công bằng' được thiết kế để xử lý các giao dịch hàng ngày. Cấp độ 'công bằng' có nghĩa là một cải tiến trong cách tiếp cận hiện tại của Cardano, giữ mức phí thấp (hoặc thậm chí ổn định, bằng cách neo vào một rô hàng hóa/tiền pháp định, như đã thảo luận trong blog của IOG về phí ổn định) và loại bỏ bất kỳ sự không chắc chắn nào cho người dùng⁷⁷⁰. Cấp này sẽ hoạt động tương tự như Cardano hiện tại (tháng 1 năm 2023), miễn là nhu cầu ở mức tối thiểu và các giao dịch nằm gọn trong một nửa khối.

Tuy nhiên, nếu nhu cầu tăng lên, một cơ chế duy nhất cho các giao dịch cấp 'công bằng' sẽ được kích hoạt. Cách tiếp cận sẽ sử dụng chức năng ưu tiên để lọc các giao dịch theo cách không phụ thuộc vào phí. Ưu tiên cho các giao dịch dựa trên tuổi và số lượng UTXO của họ là một ví dụ về điều này. Tổng số lượng của mỗi đầu vào nhân với tuổi của nó, sau đó chia cho tổng kích thước của các giao dịch tính bằng byte, sẽ là mức độ ưu tiên của một giao dịch nhất định. Mức độ ưu tiên này có thể được sử dụng với một ngưỡng (được cập nhật động sau mỗi khối) để từ chối các giao dịch có mức độ ưu tiên quá thấp. Bằng cách liên tục cung cấp một cách rẽ tiền vào từng khối, phương pháp như vậy đảm bảo **tính sống động** cho mỗi giao dịch ở mức giá thấp và có thể dự đoán được, hạn chế tác động của kẻ tấn công độc hại hoặc nhu cầu vội vàng đối với giá cả.

Khái niệm về hệ số nhân, mà IOG đã thiết lập trong khái niệm phí ổn định, cũng được mở rộng và làm rõ bằng phương pháp định giá theo cấp bậc. Kết quả là, mỗi trong ba tầng có một hệ số nhân được tính toán xác định, giá trị của nó được xác định bởi sự tắc nghẽn của tầng thích hợp trong các Block trước đó. Bậc 'công bằng' luôn có hệ số nhân là 1.

Kỹ thuật này khác với các phương pháp định giá hiện tại, chẳng hạn như các phương pháp được sử dụng bởi Bitcoin hoặc Ethereum (thậm chí cho phép Đề xuất cải tiến Ethereum EIP-1559),⁷⁷¹ trong đó mỗi giao dịch phải vượt qua một khoản phí biến đổi để được đưa vào một khối. Nhược điểm của chiến lược này là mức phí mà mọi người phải trả được xác định bởi những khách hàng 'giàu nhất'. Tệ hơn nữa, đây là khoản phí mà những người dùng giàu có nhất phải trả để biến nó thành một khối 'ngay lập tức'. Hơn nữa, vì chiến lược đặt giá thầu lý tưởng không rõ ràng đối với người dùng nên các loại cơ chế phí giao dịch này có thể vô tình 'định hình' nhu cầu hoặc vô tình tăng giá, ngay cả khi phí chủ yếu là một chức năng của cung và cầu.

Chiến lược nhiều tầng bóng bẩy hơn. Nó nhận ra rằng không phải mọi giao dịch đều có các yêu cầu giống nhau, cho phép một số trường hợp sử dụng diễn ra cùng một lúc và cho phép người dùng dễ dàng chọn dịch vụ họ muốn. Định giá theo cấp cho phép các khoản phí hợp lý và có thể dự đoán được đồng thời giảm tắc nghẽn trên chuỗi chính theo cách này. Định giá theo tầng, khi kết hợp với các thay đổi thiết kế tập trung vào việc cải thiện năng lực xử lý và thông lượng thô của chuỗi chính, cho thấy Cardano sẽ có thể xử lý mọi nhu cầu xử lý giao dịch như thế nào.

Djed stablecoin

Stablecoin chính của Cardano được đặt theo tên của *Djed*, biểu tượng của 'sự ổn định' ở Ai Cập cổ đại và là biểu tượng xương sống của thần *Osiris*, vị thần của thế giới bên kia và sự phục sinh. Djed là stablecoin đầu tiên loại bỏ biến động giá thông qua xác minh chính thức. Một trong những rào cản chính đối với việc chấp nhận Crypto là tính không ổn định của nó. Tính minh bạch, tính bất biến của dữ liệu và tính bảo mật đã được chứng minh của các giao dịch tài chính là tất cả những lợi thế của công nghệ Blockchain. Tuy nhiên, việc dự báo biến động thị trường Crypto khó khăn hơn so với tiền tệ fiat. Điều này gây khó khăn cho việc sử dụng Crypto trong cuộc sống hàng ngày.

Một stablecoin là một loại Crypto được chốt⁷⁷² vào một rô tiền tệ fiat hoặc một loại tiền tệ fiat duy nhất; hàng hóa như vàng hoặc bạc; cổ phiếu; hoặc các loại Crypto khác. Stablecoin có các quy trình tích hợp giúp duy trì mức biến động giá tối thiểu so với giá mục tiêu, khiến chúng trở nên phù hợp để lưu trữ hoặc trao đổi giá trị do sự biến động bị loại bỏ.

⁷⁷⁰

Giáo sư Aggelos Kiayias, 'Phí ổn định và Hệ thống dự trữ phi tập trung', iohk.io/en/blog/posts/2021/06/10/stablefees-and-the-decentralized-reserve-system/

⁷⁷¹

EIP 1559, cnbc.com/2021/08/04/what-to-know-about-the-ethereum-london-hard-fork-eip-1559-upgrade.html

⁷⁷²

Pegging có nghĩa là gắn hoặc ràng buộc tỷ giá hối đoái của một loại tiền tệ với một loại tiền tệ khác

Có ba loại stablecoin chính:

- Stablecoin được thế chấp quá mức được hỗ trợ bởi rô các loại Crypto khác
- Thuật toán – dự trữ (thường được tạo thành từ một hoặc nhiều loại Crypto) được kiểm soát bởi một thuật toán
- Được hỗ trợ bởi Fiat – dự trữ tiền tệ fiat được sử dụng làm tài sản thế chấp

	 Overcollateralized (Djed)	 Algorithmic	 Fiat backed
Centralization	Decentralized	Decentralized	Centralized
Collateral	Exogenous collateral (\$ADA)	Endogenous collateral	Exogenous collateral (fiat)
Collateralization	Overcollateralized - up to 1:8	Partially collateralized	Collateralized 1:1
Reimbursements	\$DJED is always redeemable for the collateral (\$ADA)	Algorithmic stablecoins depend on the value of the governance token	Fiat backed stablecoins depend on trust in the issuer
Stability	Djed stability is based on overcollateralization	Algorithmic stablecoins stability is based on trust on a governance token	Fiat backed stablecoins stability is based on trust in the issuer

Hình 72: Phân loại Stablecoin

Sự ổn định về giá của một số stablecoin nhất định đang bị đe dọa do thiếu tính minh bạch và tính thanh khoản trong dự trữ của chúng. Để giải quyết những vấn đề này, IOG đã hợp tác với Emurgo (một trong ba đối tác sáng lập khác của Cardano) và Blockchain Ergo, giống như Cardano, sử dụng mô hình kế toán dựa trên UTXO, để phát triển Djed, một hợp đồng stablecoin. Việc triển khai dựa trên bài báo nghiên cứu của Djed.⁷⁷³

Cách thức hoạt động của stablecoin bên dưới mũ xe

Các quy trình khác nhau góp phần ổn định giá trị của đồng xu và giúp giảm thiểu biến động giá. Các khái niệm kinh tế về cung và cầu làm cơ sở cho các hệ thống này. Một kỹ thuật phổ biến là hỗ trợ stablecoin bằng một khoản dự trữ tiền tệ được chốt. Nếu nhu cầu đối với các lệnh 'mua' hoặc 'bán' vượt quá nguồn cung, nguồn cung sẽ được tăng lên để giảm thiểu biến động giá.

Dự trữ stablecoin thường không được giữ bằng tiền mặt. Chúng thường được đầu tư vào các tài sản tài chính mang lại lãi suất, chẳng hạn như trái phiếu. Nhà điều hành gây quỹ từ tiền lãi của các khoản đầu tư này. Sự ổn định về giá được duy trì miễn là stablecoin được hỗ trợ hoàn toàn bởi nguồn dự trữ bằng loại tiền mà nó được liên kết — và nhà điều hành có thể phản ứng nhanh chóng với những biến động về nhu cầu.

Djed stablecoin được dự định là một tài sản được chốt bằng tiền tệ fiat với thuật toán quản lý. Phương pháp này đảm bảo dòng tiền ổn định. Djed không chỉ là một loại tiền tệ bằng đô la. Nó có thể hoạt động với bất kỳ loại tiền tệ nào nếu có sẵn các nhà tiên tri để cung cấp hợp đồng với chỉ số giá thích hợp.

của Djed được gọi là **Shen**, tiếp tục với chủ đề Ai Cập cổ đại. Shen được cho là biểu tượng của cả hoàng gia và tính đối xứng với mối liên hệ sâu sắc với sự vô hạn và trường tồn.

rủi ro

Các khoản đầu tư thường được kết nối với dự trữ stablecoin. Do thiếu tính thanh khoản trong các khoản đầu tư này, nhà điều hành có thể không đáp ứng nhanh nhu cầu. Trong ngắn hạn, điều này làm suy yếu sự ổn định. Các stablecoin được hỗ trợ bởi Fiat có nhược điểm là đòi hỏi niềm tin vào các bên nắm giữ dự trữ. Tether stablecoin (USDT) đã giảm xuống mức thấp nhất là 0,92 đô la vào năm 2017⁷⁷⁴ do thiếu tính minh bạch về dự trữ và yêu cầu 'hoàn toàn ủng hộ', cũng như các biện pháp bảo vệ ổn định không hiệu quả.

Khi tài sản nền tảng là một loại Crypto trên một Blockchain công khai, sẽ không có mối lo ngại nào về tính minh bạch. Hơn nữa, do các quy trình tự động và an toàn, việc áp dụng các hợp đồng thông minh cho phép thực hiện nhanh chóng và đáng tin cậy các bước ổn định.

Djed thuộc loại stablecoin nào?

Djed được phân loại là một stablecoin được thế chấp quá mức. Ngữ nghĩa rất quan trọng bởi vì mặc dù Djed sử dụng thuật toán, nhưng bản thân việc sử dụng thuật toán không phải là lý do để được gọi là đồng tiền ổn định thuật toán. Djed sử dụng tài sản thế chấp bên ngoài (ADA) không liên quan đến giao thức. Các stablecoin thuật toán sử dụng tài sản thế chấp nội bộ, như trong trường hợp của Luna và UST. Djed được thế chấp quá mức từ 4 đến 8 lần, trong khi các đồng tiền ổn định theo thuật toán thường chỉ được thế chấp một phần. Các đồng tiền ổn định được thế chấp quá mức theo truyền thống thường kém hiệu quả về vốn hơn, tuy nhiên, djed thì khác và thực sự khắc phục điều đó bằng mô hình Shen với mối quan hệ cộng sinh của nó. Vì vậy, djed rất hiệu quả về vốn... một đô la của ADA luôn bằng một đô la của djed.

Một điểm khác biệt nữa là djed luôn có thể đổi thành tài sản thế chấp, đó là ADA. Tiền ổn định thuật toán không phải lúc nào cũng có thể đổi được. Chúng phụ thuộc vào giá trị của Token quản trị. Sự ổn định của Djed dựa trên thế chấp hóa quá mức chứ không phải dựa trên sự tin tưởng vào Token quản trị, đây là điều bạn cần phải có nếu đang sử dụng một đồng tiền ổn định theo thuật toán.

Djed là một hợp đồng stablecoin được thuật toán hỗ trợ bằng Crypto có chức năng như một ngân hàng tự trị. Nó hoạt động bằng cách đúc và đốt tiền ổn định và tiền dự trữ, cũng như giữ một lượng dự trữ tiền cơ sở. Hợp đồng sử dụng khoản dự trữ để mua và bán stablecoin và tính phí tích lũy trong khoản dự trữ để giữ giá của stablecoin được chốt ở mức giá mục tiêu. Những người nắm giữ tiền dự trữ, những người đóng góp tiền vào dự trữ trong khi chấp nhận rủi ro biến động giá, là những người hưởng lợi từ nguồn doanh thu này.

Xác minh chính thức – lý thuyết đằng sau Djed

Djed là giao thức stablecoin đầu tiên đã được xác minh chính thức. Các tính năng ổn định và thiết kế của Djed được tăng cường đáng kể bằng cách sử dụng các phương pháp chính thức⁷⁷⁵ trong quy trình lập trình. Các định lý toán học được sử dụng để chứng minh các tính chất bằng các phương pháp hình thức:

- Duy trì giới hạn trên và dưới: giá sẽ không di chuyển trên hoặc dưới mức giá nhất định. Mua và bán không bị hạn chế trong phạm vi tỷ lệ dự trữ thông thường và người dùng không có động cơ giao dịch stablecoin trên thị trường thứ cấp ngoài phạm vi cố định
- Sự ổn định của chốt trong thời gian thị trường sụp đổ: chốt được duy trì đến một giới hạn nhất định, được đặt theo tỷ lệ dự trữ, ngay cả khi giá của đồng tiền cơ sở giảm mạnh
- Không mất khả năng thanh toán vì không có ngân hàng tham gia, không có hợp đồng ngân hàng để phá sản
- Không có ngân hàng nào hoạt động vì tất cả người dùng đều được đối xử bình đẳng và trung thực, không có lý do gì để người dùng tranh giành để đổi lấy stablecoin của họ

⁷⁷⁴

Lịch sử giá Tether và mọi thứ bạn cần biết, rain.bh/learn/tether-price-history-and-information-you-need-for-tether-trading

⁷⁷⁵

Xác minh hình thức là hành động chứng minh hoặc bác bỏ tính đúng đắn của các thuật toán dự định làm cơ sở cho một hệ thống đối với một đặc điểm kỹ thuật hoặc thuộc tính hình thức nhất định, sử dụng các phương pháp toán học hình thức. Xác minh chính thức có thể hữu ích trong việc chứng minh tính đúng đắn của các hệ thống như: giao thức mật mã, mạch tổ hợp, mạch kỹ thuật số có Bộ nhớ trong và phần mềm được biểu thị dưới dạng mã nguồn.

- Vốn chủ sở hữu tăng đơn điệu trên mỗi đồng dự trữ: phần dự trữ vượt quá trên mỗi đồng dự trữ được đảm bảo tăng khi người dùng tham gia hợp đồng trong một số trường hợp nhất định. Những người nắm giữ tiền dự trữ chắc chắn sẽ kiếm được trong những trường hợp này
- Không rút dự trữ: trong một số trường hợp nhất định, người dùng giả mạo không thể thực hiện một loạt hành vi làm cạn kiệt dự trữ của ngân hàng
- Pha loãng có giới hạn : có giới hạn đối với những người nắm giữ tiền dự trữ và lợi nhuận của họ có thể bị pha loãng do phát hành thêm tiền dự trữ.

phiên bản

Djed có sẵn trong hai phiên bản:

- Minimal Djed: Phiên bản này nhằm mục đích tối giản, trực quan và đơn giản nhất có thể trong khi vẫn duy trì sự ổn định
- Extended Djed: phiên bản tinh vi hơn này mang lại sự ổn định cao hơn. Việc áp dụng mô hình định giá liên tục và phí động để khuyến khích hơn nữa việc duy trì tỷ lệ dự trữ thích hợp là những điểm khác biệt chính.

Triển khai

IOG, Ergo và Emurgo đã thử nghiệm nhiều kỹ thuật khác nhau bằng cách triển khai hợp đồng stablecoin Djed.

SigmaUSD trên Ergo là hợp đồng Djed stablecoin đầu tiên được triển khai. Vào quý 1 năm 2021, đây là stablecoin đầu tiên được triển khai trên sổ cái dựa trên UTXO. Nó chứa khoản phí 1% cho các giao dịch mua và bán, cũng như cập nhật tỷ giá hối đoái hàng giờ từ một nhà tiên tri. Một người dùng không xác định có số lượng lớn ERG (đơn vị tiền tệ bản địa của Ergo) đã phát động một cuộc tấn công rút cạn dự trữ đối với phiên bản đầu tiên nhưng nỗ lực này đã không thành công và thủ phạm được cho là đã mất 100 nghìn đô la.

Để ngăn chặn các cuộc tấn công tương tự, phiên bản đầu tiên của Minimal Djed đã được thay thế bằng phiên bản trong đó phí được đặt thành 2%, tiên tri cập nhật 12 phút một lần và mỗi bản cập nhật tiên tri chỉ có thể ảnh hưởng đến giá 0,49% trừ khi chênh lệch giá là lớn hơn 50%. Điều này làm tăng khả năng chống lại các cuộc tấn công tiêu hao dự trữ.

Nhóm IOG cũng đã triển khai Djed trong Solidity. Một phiên bản sử dụng ether tiền tệ gốc của Blockchain Ethereum làm đồng tiền cơ sở, trong khi phiên bản kia có thể sử dụng bất kỳ Token tuân thủ ERC20 nào làm đồng tiền cơ sở. Cho đến nay, những triển khai này đã được triển khai cho các mạng thử nghiệm cho Binance Smart Chain, Avalanche Fuji, Polygon Mumbai, Ethereum Kovan ,⁷⁷⁶Ethereum Rinkeby và RSK .

Ngoài ra, còn có một triển khai OpenStar . OpenStar là một khung dựa trên Scala⁷⁷⁷ cho các Blockchain được phép riêng tư. Việc triển khai của Djed với OpenStar dựa trên khái niệm thực thi hợp đồng thông minh ngoài chuỗi để tạo ra một stablecoin trên Cardano không phụ thuộc vào các hợp đồng thông minh trên chuỗi.

Triển khai Djed trên Cardano

Bản nâng cấp Alonzo của Cardano đã biến các hợp đồng thông minh Plutus trở nên khả thi. Plutus chạy trên Haskell, đảm bảo môi trường phát triển toàn ngăn xếp an toàn. Quá trình triển khai của Djed đã chạy song song và hỗ trợ cho quá trình phát triển của Plutus V2.

Stablecoin và tiền dự trữ là tài sản gốc trong quá trình triển khai này được công nhận duy nhất bởi hàm băm của chính sách tiền tệ điều chỉnh việc đúc và đốt chúng thông qua giao thức Djed. Cách tiếp cận này cũng hy vọng rằng dữ liệu tiên tri, chẳng hạn như tỷ giá hối đoái, được gửi đến các giao dịch dưới dạng dữ liệu đã ký thay vì được đăng trên Blockchain.

⁷⁷⁶

Kovan là một Blockchain có thể truy cập công khai Proof of Authority (PoA) cho Ethereum; được tạo ra và duy trì bởi một nhóm các nhà phát triển Ethereum.

⁷⁷⁷

Scala là ngôn ngữ lập trình đa năng cung cấp hỗ trợ cho lập trình chức năng và hệ thống kiểu tĩnh mạnh . Được thiết kế ngắn gọn, nhiều quyết định thiết kế của Scala nhằm giải quyết những lời chỉ trích về Java.

Xem bài báo của Djed hoặc bài nói chuyện của Bruno Woltzenlogel Paleo tại Ergo Summit 2021 ⁷⁷⁸ để biết thêm thông tin về Djed stablecoin.

COTI (đơn vị tiền tệ của Internet)

COTI là đối tác lâu năm của IOG. Quỹ cFund ⁷⁷⁹ for Cardano Developments đã thực hiện khoản đầu tư vốn cổ phần đầu tiên vào COTI. Nó hoạt động như một cầu nối giữa các ứng dụng DeFi và Blockchain Cardano. COTI cung cấp một giải pháp gọi là ADA Pay (ADApay.finance), một cổng thanh toán cho phép các nhà bán lẻ chấp nhận thanh toán ADA với khả năng thanh toán gần như ngay lập tức. Không giống như nhiều sản phẩm tài chính trên thị trường, kho bạc của Coti luôn có bằng chứng minh bạch về dự trữ.

Charles Hoskinson và giám đốc điều hành COTI, Shahaf Bar-Geffen đã tiết lộ tại Hội nghị thượng đỉnh Cardano năm 2021 rằng nền tảng COTI (coti.io) sẽ là nhà phát hành chính thức của Djed. ⁷⁸⁰ Stablecoin , theo nhóm phát triển COTI, là một 'ứng dụng sát thủ' sẽ được một số lượng lớn người dùng Crypto sử dụng để giải quyết các khoản thanh toán và trang trải chi phí.

Terra UST 2022 sụp đổ

Đồng tiền ổn định theo thuật toán UST của Terra ⁷⁸¹ đã mất giá ⁷⁸² so với đồng đô la Mỹ vào đầu tháng 5 năm 2022. UST giảm mạnh xuống 9c buộc Terra phải đào sâu vào nguồn dự trữ Bitcoin (~1,3 tỷ đô la) từ địa chỉ Bitcoin đã được xác nhận trong một nỗ lực tuyệt vọng để ổn định con tàu ⁷⁸³. Sự sụp đổ kịch tính đã được Coin Bureau tổng kết rất tốt. ⁷⁸⁴

Tether (USDT), một trong những stablecoin lâu đời nhất trong ngành, trước đây đã bị chỉ trích vì thiếu minh bạch ⁷⁸⁵ và miễn cưỡng được kiểm toán. Sự sụp đổ đột ngột của Terra đã làm dấy lên sự hoài nghi về khả năng tồn tại của các stablecoin hiện có và khiến nhiều người ⁷⁸⁶ đánh giá lại quan điểm của họ về Djed và cách nó được thiết kế để có khả năng phục hồi tốt hơn trước các mối nguy hiểm tương tự. Shahaf Bar-Geffen đã xác nhận trong bản cập nhật tiếp theo ⁷⁸⁷ rằng Djed vẫn sống sót bình an vô sự sau cùng một ngày cuối tuần đầy biến động đối với thị trường Crypto.

Djed ra mắt

COTI đã ký 40 quan hệ đối tác với DEX để chuẩn bị cho việc ra mắt Djed được chờ đợi từ lâu. Các vấn đề về khả năng mở rộng testnet riêng tư đã được giải quyết. Mạng thử nghiệm công khai đã được ra mắt vào tháng 5 năm 2022 và sau đó là một cuộc kiểm toán hồi quy đầy đủ. Hai cuộc kiểm toán bảo mật đã được tiến hành, đó là sự thăm định đối với một Token tài chính như vậy. Mạng chính công cộng đã được ra mắt vào tháng 1 năm 2023. Để biết thông tin mới nhất, hãy truy cập trang web Djed (djed.xyz).

Các Stablecoin khác trên Cardano

⁷⁷⁸

Ergo Summit 2021 - Bước vào kỷ nguyên mới - Công bố AgeUSD & Quá trình nâng cấp mạnh mẽ, youtube.com/watch?v = zG-rxMCDIa0&t=8366s

⁷⁷⁹

Tìm hiểu kỹ hơn về cFund, iohk.io/ en /blog/posts/2021/07/28/a-closer-look-at-the- cfund /

⁷⁸⁰

Cập nhật Djed, medium.com/ cotinetwork /djed-Development-update-421cea2c610b

⁷⁸¹

Terra (LUNA) là một hệ thống Phi tập trung tập trung vào việc nâng cao không gian DeFi thông qua các khoản thanh toán có thể lập trình để thúc đẩy việc áp dụng. Giao thức có Token gốc, LUNA và được hỗ trợ bởi một loạt Stablecoin được chốt bằng tiền pháp định . Bằng cách sử dụng Stablecoin, Terra thể hiện một cơ sở hạ tầng thanh toán không có những thiếu sót của các phương thức thanh toán truyền thống như Thẻ tín dụng và các hệ thống thanh toán dựa trên Blockchain cũ.

⁷⁸²

Terra UST sụp đổ, coindesk.com/business/2022/05/09/ust-stablecoin-falls-below-dollar-peg-for- second-time -in-48-hours/

⁷⁸³

Địa chỉ Terra BTC, bitaps.com/2c2daf15ff549f84faf3dde74da288727f4a63724c957bf83a2d263a97779f65/bc1q9d4ywgfnd8h43da5tpcxn6ajv590cg6d3tg6axemvlt2k76zs50tv4q

⁷⁸⁴

KHẨN CẤP THỊ TRƯỜNG CRYPTO: UST, LUNA & BTC - Mang lại điều gì?!, youtube.com/watch?v = x5v67Larlx8

⁷⁸⁵

Tranh cãi về dây buộc, giải thích, theverge.com/22620464/tether-backing-cryptocurrency-stablecoin

⁷⁸⁶

Cardana ADA : Tôi đã sai, youtube.com/watch?v=ew-qrNFKWtA

⁷⁸⁷

Cập nhật COTI của Shahaf Bar-Geffen, Giám đốc điều hành của COTI , youtube.com/watch?v=453M7PjkIbc

Vào tháng 4 năm 2022, WingRiders đã ra mắt cùng với DEX của họ, đồng thời mang đến các đồng tiền ổn định được gói ⁷⁸⁸(USDC và USDT) và thanh khoản thông qua cầu Milkomeda.

Tại Hội nghị thượng đỉnh Cardano năm 2022, James Wager của Indigo Labs đã công bố iUSD. iUSD được gắn với giá trị trung bình của USDC (USD Coin), TUSD (TrueUSD) và USDT (Tether); thiết kế này cho phép iUSD duy trì tỷ giá cố định của nó ngay cả khi một trong ba loại tiền ổn định này giảm giá.

Cũng tại Lausanne, Vineeth Bhuvanagiri (Giám đốc Emurgo Fintech) đã công bố *Anzens*, một bộ sản phẩm giúp thu hẹp khoảng cách giữa DeFi, RealFi và TradFi (tài chính truyền thống). Sản phẩm đầu tiên sẽ là một loại tiền ổn định được hỗ trợ bằng đô la, USDA, ra mắt vào đầu năm 2023. Theo thời gian, Emurgo sẽ mở rộng ra ngoài việc mã hóa đô la sang các loại tiền tệ và tài sản trong thế giới thực khác.

Trong bài nói chuyện của mình, ⁷⁸⁹ Bhuvanagiri nhấn mạnh khoản tiết kiệm phí khi sử dụng tiêu chuẩn tài sản gốc của Cardano. Ngược lại, mô hình dựa trên hợp đồng thông minh của Ethereum yêu cầu nhiều tiền hơn cho phí gas (giao dịch) khi chuyển tiền bằng USDC và USDT. USDC (USD Coin) và USDT (Tether) là các stablecoin tập trung, được phát hành bởi các tổ chức tư nhân thu phí cao, chủ yếu dựa trên Ethereum.

Câu hỏi thường gặp về Djed

Tại sao chúng ta cần Djed?

Sự hỗn loạn của thị trường Crypto vào năm 2022 là minh chứng cho lý do tại sao chúng ta cần sự ổn định và tin tưởng từ các giao thức chứ không phải con người. Djed sẽ cung cấp một nơi trú ẩn an toàn cho phép người dùng giữ tiền trực tuyến trong thời điểm biến động và chuyển tài sản trong RealFi DApps và các giao thức cho vay. Stablecoin mang lại rất nhiều TVL (tổng giá trị bị khóa) cho hệ sinh thái. Chúng giống như một nơi trú ẩn an toàn cho các tài sản giúp hệ thống hoạt động trơn tru. Sự sụp đổ của sàn giao dịch FTX, câu chuyện lớn về Crypto thu hút sự chú ý lớn vào năm 2022, là một trong những vấn đề về lòng tham và sự thổi nạt của con người. Djed là một stablecoin hoàn toàn phi tập trung, tự trị, không có người trung gian tham gia. Nó sẽ được thúc đẩy bởi cộng đồng mà không có tổ chức nào tham gia.

Trong cuộc trò chuyện bên lề với Shahaf Bar-Geffen tại Scotfest, ⁷⁹⁰ Charles Hoskinson đã đề xuất các quốc gia như El Salvador nên xem Djed là cách duy nhất để thực hiện một CBDC ổn định không được hỗ trợ bởi Fiat. Nếu các chính phủ muốn có một stablecoin được hỗ trợ bởi dự trữ Crypto và tồn tại 100% trong không gian Crypto, thì hiện tại không có cơ chế nào khác như Djed.

Những đồng tiền liên quan đến Djed là gì và mục đích của chúng là gì?

\$DJED được chốt bằng đồng đô la Mỹ, được hỗ trợ bởi ADA làm đồng tiền cơ sở của nó. Đồng tiền dự trữ của nó là Shen (\$SHEN). Shen giữ một tỷ lệ dự trữ lành mạnh trong hợp đồng thông minh. Shen ở đó để khuyến khích người dùng đưa ADA vào hợp đồng thông minh.

⁷⁸⁸

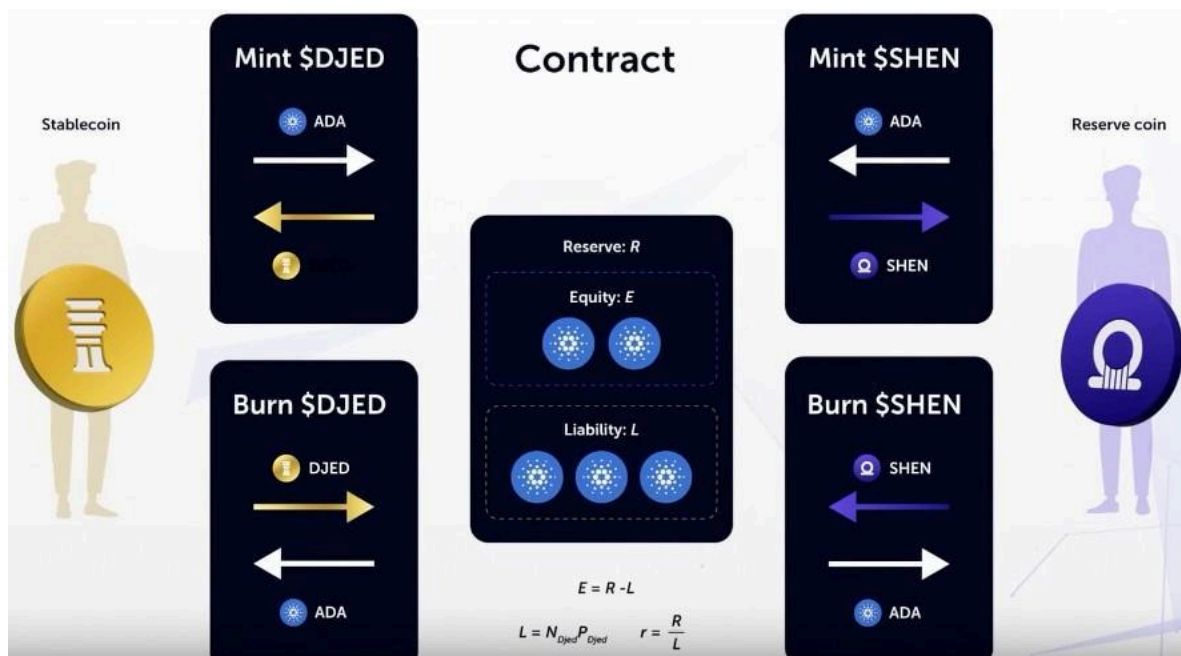
\$ADA: DEX WingRiders ra mắt, đưa Stablecoin USDC và USDT lên Cardano Mainnet, cryptoglobe.com/latest/2022/04/ADA-dex-wingriders-launches-bringing-usdc-and-usdt-stablecoins-to-cardano-mainnet/

⁷⁸⁹

Stablecoin: Cardano cần gì để thu hẹp khoảng cách giữa tài chính truyền thống và DeFi, youtube.com/watch?v=XGAH-TYl600

⁷⁹⁰

COTI Keynote & Fireside Chat, youtu.be/vyyUiT8NvaI?t=911



Hình 73: Djed hoạt động như thế nào

Thế chấp quá mức có nghĩa là gì?

Tỷ lệ giữa dự phòng và nợ phải trả luôn được duy trì trong khoảng 400-800%. Đối với mỗi yêu cầu đô la, sẽ có một khoản dự trữ trị giá từ 4 đến 8 đô la. Các stablecoin được thế chấp quá mức an toàn hơn và hoàn toàn minh bạch để kiểm tra. Không có sự tham gia của con người như với Luna khi mạng bị tạm dừng khi giá bắt đầu giảm.



Hình 74: Tỷ lệ dự trữ bắt buộc Djed.

Djed hoạt động như thế nào?

Ở cấp độ cao, ADA đang ủng hộ Djed stablecoin. Những người có Djed là những người đầu tiên nhận được từ nhóm trách nhiệm pháp lý. Họ sẽ luôn nhận lại một đô la cho Djed của họ. Đây là cơ chế an toàn trong hệ thống, nó được thể chấp quá mức, vì vậy những người nắm giữ Djed được ưu tiên. Trên hết, có một nhóm vốn chủ sở hữu được tạo ra bởi những người cung cấp tính thanh khoản và nhận lại Shen.

Tôi gửi ADA đến hợp đồng thông minh, đổi lại tôi nhận được Djed. Nếu tôi muốn lấy lại ADA của mình, tôi có thể gửi Djed trở lại hợp đồng thông minh và lấy lại ADA. Nếu tôi muốn tận hưởng một số lợi ích trong khi chấp nhận nhiều rủi ro hơn, tôi đúc Shen bằng cách gửi ADA đến hợp đồng thông minh và đốt nó khi tôi muốn rút tiền lãi của mình. Quá trình này là tự trị, tự quản lý mà không có bất kỳ sự tham gia nào của con người.

400-800%

Trong tỷ lệ 400-800%, tức là . Tỷ lệ ADA/đô la có giá trị gấp 4 – 8 lần, đây là phạm vi tối ưu. Bạn có thể đúc và đốt Djed, bạn có thể đúc và đốt Shen...

Trên 800%

Trên 800% (8x), bạn có thể đúc và đốt Djed bao nhiêu tùy thích, tuy nhiên, bạn không thể đúc Shen nữa. Ví dụ, những người nắm giữ Shen được thưởng cho những rủi ro mà họ chấp nhận ngay từ đầu. Họ đang cung cấp thanh khoản khi cần thiết. Nếu không, mọi người có thể đợi cho đến khi tỷ lệ vượt quá 800% để đúc Shen. Thực tế là bạn không thể đúc Shen trên 800% để bảo vệ hiệu quả những người nắm giữ Shen đã đúc nó trước đó.

Dưới 400%

Bạn không thể đúc Djed vì không có đủ tài sản thế chấp. Bạn chỉ có thể ghi Djed, và khi làm như vậy, hãy tăng tỷ lệ. Trong phạm vi này, bạn có thể gửi ADA đến hợp đồng thông minh để lấy lại Shen. Dưới 400% (4x), bạn đúc Shen nhưng bạn không thể đốt nó. Đây là rủi ro mà những người nắm giữ Shen phải gánh chịu, họ không thể đốt (rút) nó dưới 400%. Những người nắm giữ Shen phải đợi cho đến khi có nhiều điều chỉnh hơn trong hợp đồng thông minh và tỷ lệ dự trữ tăng lên trên 400% (4x).

Lộ trình cho Djed là gì?

Coti đã cân nhắc và có phương pháp với việc thực hiện Djed . Ngày này đã bị lùi lại một vài lần do quá trình kiểm toán diễn ra quá mức và một số vấn đề nhỏ đã được khắc phục. Đây là cách tiếp cận thận trọng với rất nhiều thất bại trong ngành cho đến nay và thành công của Djed là mấu chốt cho việc áp dụng RealFi và DeFi trên Cardano.

Phiên bản 1.1.1 là bản phát hành đầu tiên vào tháng 1 năm 2023. Phiên bản này có phiên bản Djed tối thiểu. Nó tương thích với hard fork Vasil, nhưng nó không tận hưởng hết khả năng của Vasil. Nó sẽ có một tiên tri nâng cấp với 6 nguồn bên ngoài. Có hai cuộc kiểm tra, trong đó có một cuộc kiểm tra của Tweag (tweag.io). Sẽ có rất nhiều sự chấp nhận ngay lập tức với hơn 40 quan hệ đối tác với tất cả các DEX chính, thị trường NFT, ví, dịch vụ cho vay và cho vay, v.v.

Phiên bản tiếp theo của Djed, V1.2 sẽ sử dụng đầy đủ Vasil, tức là . Plutus V2. Nó sẽ nhanh hơn, khoảng 4 giao dịch mỗi phút.

Djed v1.3 sẽ có 'Djed mở rộng' với phí và giá động và quan trọng là nó sẽ có hỗ trợ đặt cược. Bạn sẽ không hy sinh phần thưởng đặt cược bằng cách sử dụng Djed. Có nhiều chi tiết hơn trong giấy trắng.

Djed sẽ là một phần của Kho bạc Coti . Kho bạc của Coti là một hệ thống lưu trữ Coti trị giá khoảng 450 triệu và một phiên bản Djed được bọc có thể được cung cấp cho kho bạc này để nhận phần thưởng. Các tài sản được bao bọc khác cũng sẽ được hỗ trợ, vì vậy Bitcoin, Ethereum, v.v.

Sắp ra mắt vào năm 2023 cũng là 'Djed pay', một ứng dụng và cổng Crypto sẽ cho phép người bán, nền tảng thương mại điện tử, tổ chức phi lợi nhuận và về cơ bản là bất kỳ ai muốn gửi và nhận Djed dưới dạng hình thức thanh toán một cách dễ dàng.

Có rủi ro khi cầm Shen không?

Mục đích của Shen là duy trì tỷ lệ dự trữ trong hợp đồng thông minh, hay nói cách khác là mang lại sự ổn định cho Djed. Shen được cho là không ổn định và bạn không thể đốt Shen (rút) dưới mức 400% nhất định (4x). Shen là đồng tiền dự trữ cho Djed, và tiền dự trữ có trách nhiệm pháp lý. Đô la cần được thanh toán cho những người nắm giữ Djed theo yêu cầu. Những người nắm giữ Shen có lợi thế lớn hơn, vì họ đủ điều kiện nhận phần thưởng đúc/đốt. Có mức độ tiếp xúc với ADA lớn hơn, nhưng bạn sẽ nhận được thêm ADA khi giá ADA tăng lên. Trong một bản phát hành trong tương lai, những người nắm giữ Shen cũng sẽ nhận được phần thưởng đặt cược.

Có những loại phần thưởng nào dành cho người nắm giữ Shen?

Vì Shen rất dễ bay hơi và những người nắm giữ Shen cung cấp tính thanh khoản nên phải có động lực để chấp nhận rủi ro bổ sung. Người nắm giữ Shen sẽ tự động nhận được phần thưởng dưới dạng phí đúc và đốt từ hệ thống. Điều này tùy thuộc vào nhu cầu và việc áp dụng, tuy nhiên, ước tính ban đầu của Coti dự đoán sẽ có khoảng. phần thưởng 10%.

Sau khi Coti kích hoạt đặt cược (trên lộ trình), những người nắm giữ Shen cũng có thể nhận được phần thưởng đặt cược (3-5% bổ sung). Nhiều DEX hợp tác với Coti sẽ cung cấp phần thưởng cạnh tranh năng suất hấp dẫn. Họ cần khuyến khích người dùng khởi động tính thanh khoản trên các nền tảng khác nhau của họ. Những người nắm giữ Shen có thể nhận được phần thưởng lên tới 15%. Vì vậy, về tổng thể, có khả năng mang lại lợi nhuận ~30%.

Có nhiều lợi ích tiềm năng hơn. Nếu bạn đang lạc quan về dài hạn, tức là . bạn đang nắm giữ một vị thế mua, thì việc nắm giữ Shen có thể mang lại lợi nhuận tiềm năng. Ví dụ: nếu ADA trị giá 1 đô la khi người dùng gửi ADA đến hợp đồng thông minh, họ sẽ nhận lại một Djed. Theo thời gian, giá ADA tăng lên 3 đô la. Vì vậy, chủ sở hữu Djed đốt một Djed của họ và nhận lại \$1. Câu hỏi rõ ràng là 2 đô la bổ sung sẽ đi đâu? \$2 này sẽ tự động chuyển đến những người nắm giữ Shen. Nó có thể tăng lên theo bất kỳ số lượng nào. Nếu ADA tăng lên chút nào, những người nắm giữ Shen sẽ nhận được phần thừa.

Có trung gian không?

Không có người trung gian, hoặc tổ chức liên quan. Hệ thống tự trị, tự động điều chỉnh các điều kiện 'mua' và 'bán' cho Djed và Shen dựa trên khẩu phần dự trữ. Bất kỳ ai cũng có thể tìm hiểu thêm từ bài báo trên djed.xyz và xem lại hợp đồng thông minh.

Tại sao Djed tốt hơn Terra Luna?

Năm 2022 là một năm tồi tệ đối với các vụ hack và lừa đảo nhưng hai vụ sụp đổ lớn, FTX và Luna, là do lòng tham và sự thối nát của con người. Việc thiếu tự điều chỉnh trong ngành công nghiệp Crypto cũng là một yếu tố. Giống như ngành công nghiệp Crypto bị hoen ố bởi sự sụp đổ của FTX, một số người đang cố gắng bôi nhọ Djed là có tội bởi hiệp hội . Luna cũng là một stablecoin có thuật toán, Djed cũng có một thuật toán nhưng đó là điểm tương đồng kết thúc. Djed được phân loại là một stablecoin được thể chấp quá mức.

Đã có nhiều năm nghiên cứu học thuật đằng sau thuật toán của Djed . Nó bắt đầu như là sản phẩm của các phương pháp chính thức và đã được thử nghiệm thực tế trong các mô phỏng. Ergo cũng đã triển khai phiên bản của họ, SigmaUSD , đã chịu được sự biến động lớn của thị trường (giảm 90%) và duy trì mức cố định của nó. Lý thuyết đằng sau các stablecoin được thể chấp quá mức đã nhiều lần cho thấy khả năng phục hồi của nó trong các điều kiện thị trường bất lợi.

Luna không được thể chấp quá mức, Djed được thể chấp quá mức theo tỷ lệ 4-8x lành mạnh. Luna được hỗ trợ bởi một tài sản, UST, có mối tương quan trực tiếp. 'Vòng xoáy tử thần' của Luna xảy ra do UST mất chốt, ⁷⁹¹giải pháp là bán Luna. Vì vậy, giá của Luna chắc chắn sẽ giảm xuống tạo ra sự phụ thuộc vòng tròn. Khi sự cố diễn ra, thực thể tập trung đằng sau Luna thậm chí đã cố gắng ngăn chặn mạng và thêm Bitcoin làm tài sản hỗ trợ không tương quan.

Djed được hỗ trợ bởi ADA, điều này không tương quan với Djed. Không có sự phụ thuộc, ADA có thể tồn tại mà không cần Djed. ADA có tiện ích và hệ sinh thái riêng với nhiều thanh khoản. Djed tự trị và phi tập trung chạy trên hợp đồng thông minh của riêng mình. Không có sự tham gia của con người, không có cơ quan trung ương nào điều chỉnh tỷ lệ dự trữ bắt buộc. Tất cả các điều kiện động 'mua' và 'bán' đều được đặt tự động. Phí dành cho những người nắm giữ Shen, không dành cho nhà phát hành tập trung.

Làm thế nào để Djed so sánh với các stablecoin khác?

Hầu hết các stablecoin ngày nay đều được *hỗ trợ bởi fiat* . Thường có một sự tin tưởng cần thiết trong một thực thể tập trung. Bạn phải tin họ khi họ hứa sẽ thể chấp theo tỷ lệ dự trữ một đối một. Bạn có trách nhiệm xác minh, đọc các báo cáo kiểm tra, v.v.

Thường có rất nhiều FUD (sợ hãi, không chắc chắn và nghi ngờ) ⁷⁹²xoay quanh các stablecoin như vậy từ các nhóm lợi ích được đầu tư khác nhau. Một nhược điểm quan trọng khác của việc nắm giữ một stablecoin tập trung, chẳng hạn như USDC, là tài khoản của bạn có thể bị cơ quan tập trung đóng băng hoặc tịch thu. Với stablecoin tập trung, được hỗ trợ bởi fiat, cộng đồng không được hưởng lợi từ giao thức. Nó có thể cực kỳ sinh lợi cho tổ chức phát hành, đặc biệt nếu lãi suất cho vay fiat thấp.

⁷⁹¹Vòng xoáy tử thần: Stablecoin thuật toán của Terra sụp đổ như thế nào, forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down/?sh=2e4307f371a2

⁷⁹² Crypto Biz: Bạn không thể dừng Tether FUD, cointelegraph.com/news/crypto-biz-you-can-t-stop-the-tether-fud

được hỗ trợ bằng Crypto có sự phụ thuộc vào tài sản dự trữ Crypto cơ bản. Một cái nhìn nhanh về *coincap.io* sẽ cho thấy mức độ biến động của thị trường. Rủi ro tăng lên khi stablecoin không được thể chấp quá mức.

Cấu trúc phí cho Djed là gì?

Để xem lại các khoản phí mới nhất, hãy truy cập *djed.xyz*

EUTXO đối phó với mất mát vô thường như thế nào

Mất tạm thời ⁷⁹³ là một nhược điểm đối với những người cung cấp thanh khoản cho DEX. Nó có thể là một thuật ngữ khó hiểu cho người mới.

Trình tạo thị trường tự động (AMM) và sổ đặt hàng là những kiến trúc phổ biến nhất được sử dụng để chạy DEX (sàn giao dịch phi tập trung). AMM rất dễ xây dựng và kiến trúc này sau đó đã trở thành tiêu chuẩn cho các chuỗi dựa trên tài khoản. Tuy nhiên, có một số nhược điểm với thiết kế này, 'sự mất mát vô thường' là một trong số đó.

Cardano sử dụng mô hình EUTXO, mang tính quyết định, khiến nó dễ dự đoán hơn so với mô hình dựa trên tài khoản về tổn thất tạm thời. Thuật ngữ 'vô thường' hơi gây hiểu lầm vì việc giảm giá Token có thể chỉ là tạm thời và giá có thể tăng trở lại tùy thuộc vào điều kiện thị trường. Bởi vì giá điều chỉnh tăng lên, tổn thất sẽ là nhất thời (vô thường). Tất cả những gì quan trọng là giá đô la khi bạn rút tiền. Nếu nó thấp hơn giá bạn đã mua, thì rõ ràng là 'lỗ' sẽ trở thành vĩnh viễn. ADA đạt đỉnh ở mức 1,2 đô la trong đợt tăng giá năm 2018. ⁷⁹⁴ Nó giảm mạnh sau đó tăng lên mức cao nhất mọi thời đại là 3,1 đô la vào tháng 9 năm 2021. Sự biến động có thể xảy ra trong một ngành chưa trưởng thành, định giá công nghệ mới nổi.

Với quy định nhẹ nhàng, có thể cho rằng 'tổn thất tạm thời' là rủi ro không thể tránh khỏi đối với các nhà cung cấp thanh khoản ⁷⁹⁵ ở 'miền tây hoang dã' của các sàn giao dịch Crypto. Nếu khoản lỗ vượt quá phí giao dịch thu được, nhà cung cấp thanh khoản sẽ chịu khoản lỗ, điều này có thể tránh được nếu họ giữ Token của mình. Cũng phổ biến là mặc dù các nhà cung cấp thanh khoản có thể không mất tiền, nhưng thu nhập của họ có thể thấp hơn so với việc bạn chỉ giữ lại các Token.

AMM

Kiến trúc DEX của Nhà tạo lập thị trường tự động (AMM) cung cấp giao dịch tự động dựa trên hợp đồng thông minh cho các cặp Crypto. Với việc Ethereum là nền tảng hợp đồng thông minh thông trị cho đến nay, đương nhiên hầu hết các cặp nằm giữa token Ethereum và stablecoin.

Nhóm thanh khoản cho phép người dùng gộp tài sản của họ vào các hợp đồng thông minh, giúp cung cấp năng lượng hiệu quả cho AMM. Thanh khoản trong nhóm càng nhiều thì môi trường giao dịch cho các nhà giao dịch trên DEX mà nhóm liên kết với đó càng đáng tin cậy và đương nhiên, các nhà cung cấp thanh khoản kiếm được càng nhiều phí giao dịch. Nhóm thanh khoản cung cấp tính thanh khoản trên cả hai mặt của giao dịch. Nhóm sử dụng một thuật toán để xác định giá của một nội dung dựa trên tính sẵn có của nó trong nhóm.

Vì vậy, các AMM hoàn toàn phụ thuộc vào các nhà cung cấp thanh khoản của họ để cung cấp đủ quy mô nhóm nhằm đảm bảo giao dịch công bằng và đáng tin cậy. Các nhà cung cấp thanh khoản thường được gọi là 'nhà tạo lập thị trường' trong tài chính truyền thống.

⁷⁹³

Trong DeFi, **tổn thất tạm thời** đề cập đến sự mất mát về giá trị khi đầu tư thanh khoản vào nhóm thanh khoản so với việc chỉ nắm giữ Token. Sự kiện này xảy ra khi giá của Token của người dùng thay đổi so với khi họ gửi chúng vào nhóm thanh khoản. Thay đổi càng lớn thì tổn thất càng lớn.

⁷⁹⁴

Thị trường tăng giá hay **thị trường tăng giá** là một trạng thái của thị trường tài chính nơi giá cả đang tăng lên. Thuật ngữ thị trường giá lên thường được sử dụng trong bối cảnh thị trường chứng khoán. Tuy nhiên, nó có thể được sử dụng trong bất kỳ thị trường tài chính nào, kể cả Crypto.

⁷⁹⁵

Nhà **tạo lập thị trường** hoặc **nhà cung cấp thanh khoản** báo giá cả giá mua và giá bán của một công cụ tài chính hoặc hàng hóa được giữ trong kho, với hy vọng kiếm được lợi nhuận từ chênh lệch giá mua-giá bán hoặc chuyển hướng. Ủy ban Chứng khoán và Giao dịch Hoa Kỳ định nghĩa 'nhà tạo lập thị trường' là một công ty sẵn sàng mua và bán cổ phiếu một cách thường xuyên và liên tục với mức giá niêm yết công khai.

IOG có một số bài báo ⁷⁹⁶về tầm quan trọng của các ưu đãi phù hợp ⁷⁹⁷trong không gian Crypto. Các ưu đãi là điều cần thiết để thúc đẩy các nhà cung cấp thanh khoản cho DEX hoạt động một cách đáng tin cậy và công bằng. Các nhà cung cấp thanh khoản được khuyến khích bằng cách cạnh tranh năng suất ⁷⁹⁸trong trường hợp này.

Quyền sở đặc Mua hàng

Cơ chế của kiến trúc sổ đặt hàng nên quen thuộc với bất kỳ ai làm việc trong thế giới kinh tế. Đó là một mô hình đơn giản để hiểu. Sổ lệnh về cơ bản lưu trữ tất cả các lệnh mua/bán (yêu cầu/đặt giá thầu) và sắp xếp chúng theo giá của tài sản khi các nhà giao dịch đặt lệnh. Tài sản có thể được trao đổi nếu có đủ cung và cầu.

Kiến trúc sổ lệnh phù hợp hơn nhiều với các sổ cái dựa trên EUTXO, chẳng hạn như Cardano và Ergo, vì thiết kế của nó, cùng với các tính năng của EUTXO, giảm thiểu tác động của tổn thất tạm thời.

Số lượng Token trong nhóm thanh khoản và số lượng nhà cung cấp thanh khoản đóng góp vào đó là các biến số khi dự đoán và tránh tổn thất tạm thời. Nếu có tổn thất tạm thời thường xuyên xảy ra, thì nhóm không khả thi và các nhà cung cấp thanh khoản sẽ tự nhiên chuyển sang (các) nhóm đối thủ có lợi hơn. Nó có thể là một vòng luẩn quẩn, vì có thể đã quá muộn để cứu vãn một khi 'ngân hàng Crypto tháo chạy' xảy ra giống như những gì đã xảy ra với sự cố Terra Luna.⁷⁹⁹

Để tóm tắt từ trước đó,

- Các Blockchain dựa trên UTXO không có tài khoản giữ sổ dư. Ví của người dùng theo dõi danh sách các đầu ra chưa sử dụng tương ứng với tất cả các địa chỉ của người dùng và xác định số dư của người dùng. Hãy nhớ rằng các giao dịch UTXO tương tự như 'rút tiền mặt'. Mô hình EUTXO bao gồm một mốc thời gian, là siêu dữ liệu dành riêng cho hợp đồng. Điều này rất quan trọng vì nó cho phép Cardano cung cấp nhiều tài sản và hợp đồng thông minh.
- Mô hình dựa trên tài khoản giữ sổ dư tiền trong tài khoản (được bảo vệ bằng khóa riêng hoặc hợp đồng thông minh). Nội dung được thể hiện dưới dạng sổ dư bên trong tài khoản của người dùng, với sổ dư được lưu dưới dạng trạng thái chung của tài khoản. Mỗi Node duy trì trạng thái riêng của nó, được cập nhật với mỗi giao dịch.

Có nhiều sự khác biệt lớn giữa các mô hình trên, nhưng có một điểm nổi bật. Các AMM hoạt động trên các chuỗi dựa trên Tài khoản có nhiều khả năng sử dụng công thức định giá của Nhà tạo lập Thị trường Công thức Không đổi (CFMM), đây là một trong những thuật toán AMM được sử dụng rộng rãi nhất. Có những điểm không hiệu quả trong công thức này, chẳng hạn như nó cung cấp cho người dùng rất ít hoặc không có quyền riêng tư.⁸⁰⁰

Ngoài ra, Tổng giá trị bị khóa (TVL)⁸⁰¹ được phân tán trong toàn bộ phạm vi giá, ngụ ý rằng giá của một tài sản có thể là 1 đô la hoặc 100.000 đô la. Định giá CFMM là không hợp lý theo tiền đề này và không đại diện cho thực tế thị trường thực tế. Hơn nữa, các giao dịch có khối lượng Token thấp có xu hướng trượt giá nhiều.⁸⁰² Mặc dù CFMM là một tính năng phổ biến đối với AMM, nhưng những

⁷⁹⁶

Kiayias, Koutsoupias, Stouka (2021) 'Các biện pháp khuyến khích chống lại việc nắm quyền hoặc cách tạo ra cuộc cách mạng trong hệ thống bằng chứng cổ phần gộp', arxiv.org/pdf/2111.08562.pdf

⁷⁹⁷

Judmayer, Stifter, Zamyatin, Tsabary, Eyal, Gaži, Meiklejohn, Weippl (2021), 'SoK: Các cuộc tấn công thao túng khuyến khích thuật toán vào Crypto PoW không cần cấp phép', eprint.iacr.org/2020/1614.pdf

⁷⁹⁸

Canh tác năng suất là một thuật ngữ DeFi để tận dụng các giao thức và sản phẩm DeFi để tạo ra lợi nhuận cao, đôi khi đạt trên 100% lợi suất hàng năm 'khi bao thanh toán tiền lãi, phần thưởng Token, tiền thưởng 'hoàn lại tiền' và các ưu đãi khác.' Canh tác năng suất là một cách để những người đam mê Crypto tối đa hóa lợi nhuận của họ. Nó thường liên quan đến việc người dùng cho vay hoặc khóa tiền của họ bằng hợp đồng thông minh. Đổi lại, người dùng kiếm được phí dưới dạng Crypto.

⁷⁹⁹

Do Kwon có bị bắt sau khi giá LUNA của Terra sụp đổ không?, fxstreet.com/cryptocurrency/news/is-do-kwon-going-to-get-arrested-after-terra-luna-price-collapse-202205191033

⁸⁰⁰

Chitra, Angeris, Evans (2021), 'Quyền riêng tư khác biệt trong các nhà tạo lập thị trường chức năng không đổi', eprint.iacr.org/2021/1101.pdf

⁸⁰¹

Tổng giá trị (TVL) được khóa trong hợp đồng thông minh hoặc bộ hợp đồng thông minh có thể được triển khai hoặc lưu trữ tại một hoặc nhiều sàn giao dịch hoặc thị trường. Điều này được sử dụng như một phép đo tiền gửi của nhà đầu tư. Đó là giá trị đồng đô la của tất cả các đồng xu hoặc Token được khóa trong một nền tảng, giao thức, chương trình cho vay, chương trình canh tác năng suất hoặc nhóm thanh khoản bảo hiểm.

⁸⁰²

sự thiếu hiệu quả này có thể khiến thu nhập của nhà cung cấp thanh khoản bị ảnh hưởng. Hơn nữa, thanh khoản này dễ bị mất tạm thời.

EUTXO và sổ đặt hàng DEX giảm thiểu tổn thất tạm thời

Những ưu điểm chính của kiến trúc EUTXO về bảo mật, tính xác định, tính song song và khả năng mở rộng đã được thảo luận trước đó. Các tính năng của EUTXO làm cho Cardano trở thành một nền tảng phù hợp cho các DEX sử dụng kiến trúc sổ đặt hàng, vì nó cung cấp khả năng chống mất mát tạm thời cao hơn. Thiết kế này có một số ưu điểm, một trong số đó là mức độ tập trung của thanh khoản được phân bổ trong một phạm vi giá tùy chỉnh. Tính năng này cải thiện hiệu quả thanh khoản đồng thời giảm thiểu tổn thất tạm thời.

Trạng thái toàn cầu và cục bộ

Không giống như các Blockchain dựa trên tài khoản, trong đó mỗi kết quả giao dịch thay đổi trạng thái toàn cầu, các Blockchain dựa trên EUTXO xác minh tính hợp pháp của giao dịch ở cấp độ giao dịch, với số dư bằng tổng số UTXO còn lại. EUTXO hoạt động ở cấp địa phương.

Đây không phải là trường hợp với các Blockchain dựa trên tài khoản. Hợp đồng thông minh và các tác nhân khác liên tục tương tác và tác động đến trạng thái toàn cầu, dẫn đến việc sử dụng tài sản và tài nguyên, cũng như sự biến động mạnh của giá khí đốt. Do đó, phí giao dịch có thể rất khó dự đoán, thậm chí tăng đột biến giữa thời điểm giao dịch được gửi và thời điểm giao dịch được xác minh. Do đó, chuỗi có thể từ chối một giao dịch như vậy, tuy nhiên, chi phí gas vẫn được thu thập, có khả năng dẫn đến việc ví của người dùng bị ảnh hưởng. Khi khối lượng giao dịch tăng lên và khách hàng doanh nghiệp cân nhắc sử dụng nền tảng này, đây là một lỗ hổng nghiêm trọng đối với Ethereum.

Phí 'gas' quá cao không phải là vấn đề với mô hình EUTXO của Cardano, vì các giao dịch được xác minh và thực hiện tại tiểu bang địa phương. Điều này có thể thực hiện được bằng cách thêm mốc thời gian (siêu dữ liệu bổ sung dành riêng cho hợp đồng) vào giao dịch. Dữ liệu chuẩn được chuyển đến logic xác thực của giao dịch, đảm bảo rằng EUTXO vẫn mang tính quyết định. Điều này về cơ bản đảm bảo rằng chi phí giao dịch là cố định và sẽ không thay đổi trong tương lai. Một ưu điểm khác của EUTXO và chủ nghĩa tất định là các tác nhân xấu không thể cải tổ lại các giao dịch, đây là mối nguy hiểm với các mô hình dựa trên Tài khoản.

Lợi ích chính của việc xác thực giao dịch cục bộ là nó cho phép mức độ song song cao. Chuỗi dựa trên tài khoản không thể thực hiện việc này vì các giao dịch phải được xử lý tuần tự.

Cardano đã vấp phải một số lời chỉ trích vì quá bảo thủ trước các đối thủ cạnh tranh.⁸⁰³ Thay vì 'di chuyển nhanh và phá vỡ mọi thứ', Cardano đã được triển khai cẩn thận với khả năng mở rộng và hiệu suất chỉ được giải quyết sau khi một mạng an toàn và các giao thức đồng thuận được thiết lập. Khi các cải tiến được giới thiệu tại Vasil có hiệu lực, hy vọng sẽ thấy một loạt các DEX phát triển mạnh mẽ trên Cardano, chẳng hạn như ErgoDEX và Axo cùng nhiều loại khác.⁸⁰⁴ Genius DEX là một người khác đã phác thảo chiến lược của họ trong blog và video trung bình của họ.⁸⁰⁵

Bộ chuyển đổi ERC20

Mạng bằng chứng cổ phần của Cardano có thể chứa các Token Ethereum như SingularityNet AGI⁸⁰⁶ nhờ bộ chuyển đổi ERC20. Việc kết nối các giao thức Blockchain và hợp tác trên các ứng dụng là rất quan trọng để hiện thực hóa lời hứa về tài chính phi tập trung (DeFi) như một giải pháp thay thế khả thi cho ngân hàng thông thường.

Đầu năm 2021, DeFi Pulse, một trang web giám sát, đã tuyên bố rằng bitcoin trị giá hơn '75 tỷ đô la hiện đã bị khóa' trong DeFi. Cuối

Trượt giá đề cập đến sự khác biệt giữa giá kỳ vọng của một giao dịch và giá mà giao dịch được thực hiện. Sự trượt giá có thể xảy ra bất cứ lúc nào nhưng phổ biến nhất trong thời kỳ biến động cao hơn khi các lệnh thị trường được sử dụng.

⁸⁰³

Lời chỉ trích từ người sáng lập Solana,
twitter.com/IOHK_Charles/status/1532360549857693697?s=20&t=YIDNMde_QXHGEURpgZj8UA

⁸⁰⁴

CardanoCube DEX, cardanocube.io/collections/exchanges-dex

⁸⁰⁵

vô thường là gì ?, [Geniusyield.medium.com/what-is-im-Permanent-loss-2f03a90a8bcb](https://geniusyield.medium.com/what-is-im-Permanent-loss-2f03a90a8bcb)

⁸⁰⁶

Điểm kỳ dị NET (ký hiệu đánh dấu: AGI) là một thị trường phi tập trung dành cho Trí tuệ nhân tạo.

năm đó, Cision đã báo cáo "Tổng giá trị khóa của DeFi đạt mức cao nhất mọi thời đại là 236 tỷ đô la"⁸⁰⁷ và đạt mức cao nhất mọi thời đại hiện có là 256 tỷ đô la⁸⁰⁸ vào tháng 12 năm 2021. Phần lớn của cái này ở dạng Crypto dựa trên Token ERC20 -tài sản.

Ngay cả kể từ khi chuyển sang bằng chứng cổ phần, phí Ethereum vẫn cao và không thể đoán trước. Cardano tạo điều kiện thuận lợi cho việc chuyển Token ERC20 sang nền tảng của nó để mở rộng phạm vi trường hợp sử dụng cho các nhà phát triển ứng dụng và doanh nghiệp. Người dùng Token Ethereum được hỗ trợ có thể di chuyển chúng từ mạng quá tải của Ethereum sang Cardano và hưởng lợi từ khả năng giao dịch tăng lên và phí thấp hơn, cũng như bảo mật được cải thiện và khả năng tương tác.

Tại sao Token ERC20 lại phổ biến như vậy?

Vào năm 2015, Ethereum đã giới thiệu Blockchain với khái niệm hợp đồng thông minh và 'tiền có thể lập trình'. Do giá trị của nó trong các giao dịch kinh doanh thông thường, Token hóa và Token ERC20 đã trở nên phổ biến kể từ đó. Token được tạo bởi các ứng dụng dựa trên Blockchain có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm:

- thanh toán tài chính
- đơn vị giao dịch
- phương tiện truy cập vào các dịch vụ kỹ thuật số
- phần thưởng/khuyến khích
- quyền biểu quyết
- phương tiện đầu tư

Các Token ERC20 được thiết kế tốt có thể đáp ứng nhiều yêu cầu khác nhau và chúng càng trở nên hữu ích thì nhu cầu về chúng càng phát triển và giá trị của chúng cũng tăng theo. Đó là lý do tại sao các Token này rất phổ biến và được hỗ trợ bởi rất nhiều ví và sàn giao dịch.

Eth v ADA

Tiêu chuẩn Token ERC20 đã được tạo cho Ethereum và hiện có hơn 750.000 hợp đồng (etherscan.io/tokens) dựa trên nó, bao gồm Binance coin (BNB), Tether (USDT) và Uniswap (UNI)⁸⁰⁹.

Ethereum là một Blockchain nổi tiếng và hữu ích, nhưng nó đang bị đình trệ và ngày càng tốn kém hơn. Phí 'gas' được tính để xác thực các giao dịch đang tăng lên nhanh chóng khi có nhiều người dùng tương tác với các ứng dụng phi tập trung hơn. Một nghiên cứu của Cointelegraph được giới thiệu trong *DeFi Adoption 2020*⁸¹⁰ cũng nêu ra các vấn đề mà người dùng Ethereum đang gặp phải. Phát hiện này đã được chứng thực bởi báo cáo của Morgan Stanley vào năm 2022.⁸¹¹ Ethereum vẫn chưa vượt qua được những trở ngại này và khó có thể làm được điều đó sớm. Nhiều công ty sẽ muốn xem xét các khả năng khác.

Trọng tâm của IOG là đưa ra một đề xuất giá trị khai thác lợi thế của Cardano so với Ethereum bằng cách tạo điều kiện thuận lợi cho việc chuyển Token ERC20 sang Cardano. Cardano tự hào về khả năng xử lý giao dịch lớn hơn và phí rẻ hơn, trái ngược với chi phí cao và lưu lượng truy cập thường bị tắc nghẽn của Ethereum.

Bộ chuyển đổi ERC20 làm gì?

⁸⁰⁷

Tổng giá trị khóa của DeFi đạt mức cao nhất mọi thời đại là 236 tỷ đô la,
pnewswire.com/news-releases/defi-total-value-locked-hits-all-time-high-of-236-billion-301412901.html

⁸⁰⁸

Tổng giá trị được khóa trong Defi gần đạt mức cao nhất trong đời, TVL của Ethereum chiếm ưu thế 54%,
news.bitcoin.com/total-value-locked-in-defi-gains-lifetime-high-ethereums-tvl-dominates-by-54

⁸⁰⁹

Uniswap là một Sàn giao dịch phi tập trung (DEX) được xây dựng trên Ethereum, sử dụng hệ thống tạo thị trường tự động thay vì sổ đặt hàng truyền thống. Nó được lấy cảm hứng từ một bài đăng Reddit từ Vitalik Buterin và được thành lập bởi Hayden Adams vào năm 2017.

⁸¹⁰

Việc áp dụng DeFi 2020: Hướng dẫn cơ bản để gia nhập ngành,
s3.cointelegraph.com/storage/uploads/view/48c6c4e03f85bc722d76f88c2676478b.pdf?_ga=2.42938214.270418488.1602500005-1231871228.15935

⁸¹¹

Morgan Stanley cảnh báo Ethereum có thể mất vị thế trước Binance, Solana và Cardano, khiến việc chuyển sang 'bằng chứng cổ phần' thậm chí còn cấp bách hơn, fortune.com/2022/02/18/ethereum-smart-contracts-proof-of-stake-binance-solana-cardano-morgan-stanley

Cardano hiện hỗ trợ ADA và Token gốc, hàng triệu trong số đó đã được đúc.⁸¹² IOG đã giới thiệu bộ chuyển đổi ERC20 vào cuối năm 2021 để đảm bảo khả năng tương thích trong tương lai và xây dựng nền tảng cho tiềm năng thương mại mở rộng.

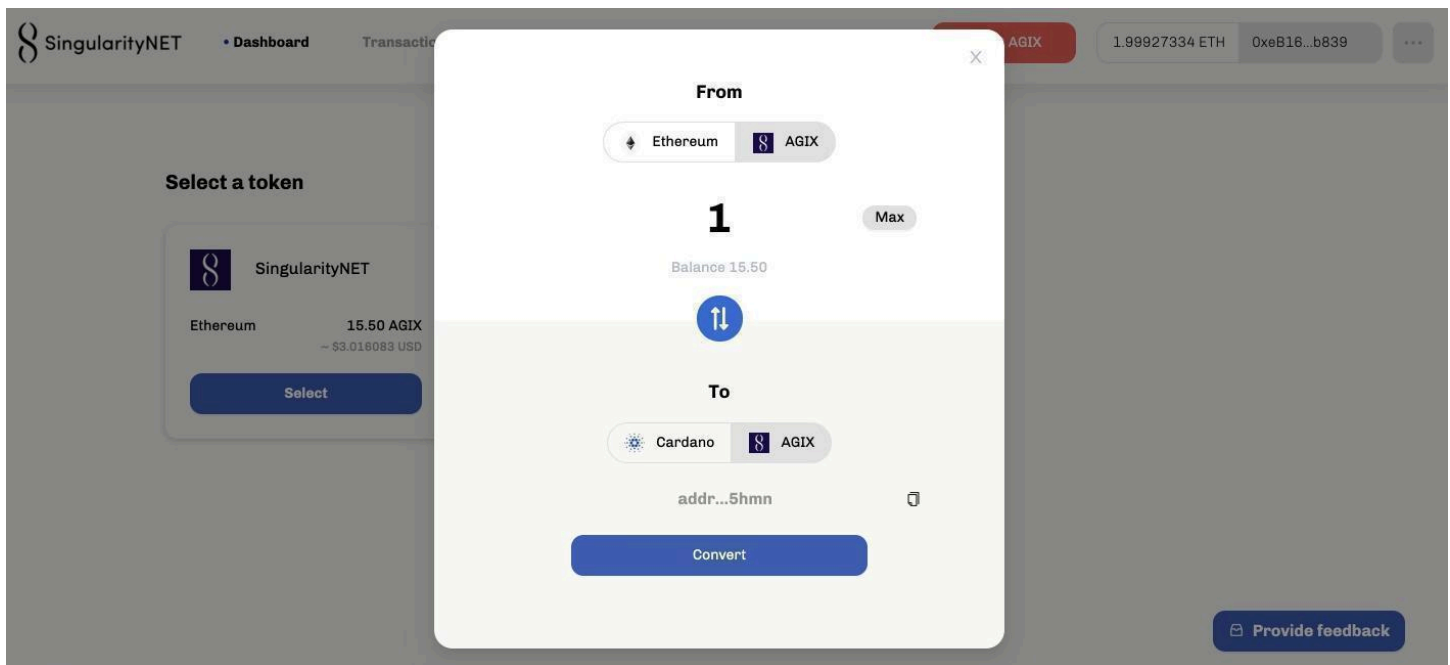
Bộ chuyển đổi ERC20 là một tiện ích sẽ cho phép các nhà phát hành Token ERC20 và người dùng của họ di chuyển Token của họ sang Cardano. Nó dành cho các nhà phát hành Token (tổ chức muốn chuyển Token của họ sang Cardano) và người dùng của họ (người nắm giữ Token) khi chuyển Token ERC20 của họ sang mạng Cardano.

Người dùng chỉ cần chuyển đổi Token Ethereum của họ bằng một vài cú nhấp chuột và những Token này sẽ được 'dịch' thành Token gốc trên Cardano có cùng giá trị và hoạt động tương tự như Token ERC20 khi được chuyển qua. Ngoài ra, nếu người dùng quyết định làm như vậy sau đó, họ có thể ghi Token của mình trên Cardano và trả lại cho mạng nguồn. Khả năng chuyển đổi theo cả hai hướng được tích hợp sẵn.

SingularityNET (singularitynet.io) là những người đầu tiên chuyển sang Cardano. Các Token SingularityNET AGIX⁸¹³ đã được khởi chạy thông qua bộ chuyển đổi ERC20 và việc phát hành nó thể hiện bước đầu tiên trong chiến lược di chuyển SingularityNET sang Cardano. Mạng thử nghiệm đầu tiên cho phép người dùng đánh giá quá trình di chuyển trong khi sử dụng Token AGIX trên Cardano và Ethereum Kovan mạng thử nghiệm.

Metamask (một plugin trình duyệt Chrome) đã được sử dụng để xác minh tài khoản và sau đó là chức năng bổ sung. Người dùng phải cung cấp địa chỉ mạng thử nghiệm Daedalus của họ để chuyển Token của họ sang Cardano và theo dõi số dư cũng như giao dịch của họ.

Người dùng có thể xem các đồng tiền SingularityNET được liệt kê và có sẵn để di chuyển trong tài khoản chuyển đổi ERC20 của họ, cũng như dữ liệu như số dư Token, bằng cách nhấp vào Token. Họ chỉ cần chọn Token, xác định số lượng họ muốn chuyển đổi, sau đó di chuyển chúng sang địa chỉ Cardano. Khi Token được gửi đến địa chỉ, chúng có thể được sử dụng cho các giao dịch và thanh toán ví Daedalus. Cả Etherscan (etherscan.io) và Cardano Explorer đều hiển thị tất cả các hành động.



Hình 75: Bộ chuyển đổi ERC20

Người dùng sẽ thấy nhiều Token khác nhau trên bảng điều khiển khi thời gian trôi qua. Các Token đủ điều kiện để di chuyển sẽ được hiển thị đầu tiên và nếu các Token chưa được liệt kê, người dùng có thể đăng ký nhận thông báo về bất kỳ thay đổi nào.

⁸¹²

Hệ sinh thái CardanoCube, cardanocube.io/ cardano -ecosystem-interactive-map

⁸¹³

Trình tự khởi chạy SingularityNET Giai đoạn II được kích hoạt: Token AGI sẽ được hard-fork thành AGIX tương thích với Cardano, blog.singularitynet.io/singularitynet-phase-ii-launch-sequence-activated-agi-token-to-be-hard-forked-to-10ede4b6c89

Mục đích của IOG là hỗ trợ nhiều Token để tạo thuận lợi cho các giao dịch thương mại. Vì vậy, trong tương lai, bộ chuyển đổi ERC20 sẽ hoạt động như một cầu nối giữa các Blockchain, cho phép giao tiếp giữa các chuỗi thành công với nhiều loại Token.

Bộ chuyển đổi AGIX ERC20

mạng thử nghiệm bộ chuyển đổi AGIX ERC20 đã trực tuyến và sẵn sàng để cộng đồng đánh giá.

Đối tác đầu tiên của sáng kiến này là SingularityNET và bộ chuyển đổi là một bước quan trọng trong mối quan hệ đối tác mới chớm nở của IOG với cộng đồng SingularityNET. Người dùng đã tận dụng một cầu nối được phép để vận chuyển Token AGIX của SingularityNET từ Ethereum sang Cardano và quay lại phiên bản testnet đầu tiên trên. Đây là một bước tiến lớn trong việc thúc đẩy khả năng tương tác của Blockchain nhằm tạo ra một hệ sinh thái hoạt động cho tài chính phi tập trung (DeFi). Người dùng đã đánh giá khả năng của mạng thử nghiệm và thử nghiệm việc chuyển Token AGIX để tận dụng khả năng giao dịch lớn hơn của Cardano, chi phí rẻ hơn và lợi thế bảo mật đã được chứng minh.

Cầu nối với khả năng tương tác

Khả năng tương tác là rất quan trọng để tăng cường áp dụng và tăng trưởng Blockchain trên toàn diện. Cùng với chiến lược mã nguồn mở toàn diện của IOG, việc cung cấp các giải pháp Blockchain cho mọi người, bất kể giao thức nào, luôn là một trong những mục tiêu hàng đầu của họ. IOG đang làm việc để có thể di chuyển các Token từ các Blockchain và Sidechain khác sang Cardano một cách an toàn và dễ dàng.

Cầu chuyển đổi AGIX ERC20 đã hoạt động trên mạng chính vào ngày 18 tháng 4 năm 2022. Xem bridge.singularitynet.io

DApps được chứng nhận trên Cardano

Với sự gia tăng của các ứng dụng mới của bên thứ ba, khả năng có thông tin không phù hợp hoặc có hại, cũng như nội dung không đạt tiêu chuẩn. Do đó, việc giải quyết các thách thức như khám phá và đảm bảo chất lượng là rất quan trọng đối với sự phát triển hệ sinh thái ban đầu. Tại Hội nghị thượng đỉnh Cardano năm 2021, IOG đã cung cấp một cái nhìn sâu sắc hơn⁸¹⁴ về vấn đề quan trọng này bằng cách giới thiệu một chương trình chứng nhận để kiểm tra các ứng dụng được xây dựng trên Cardano. Điều này sẽ không thể thiếu đối với DApp Store trên Lace.

khám phá DApp

Cửa hàng DApp, một nguyên mẫu⁸¹⁵ đã được trưng bày tại Hội nghị thượng đỉnh, sẽ cho phép các nhà phát triển gửi các DApp dựa trên Cardano của họ và giúp phần còn lại của cộng đồng có thể truy cập chúng. Các nhà phát triển sẽ có thể xuất bản DApp của họ mà không sợ bị kiểm duyệt nhờ vào môi trường dân chủ và đáng tin cậy của cửa hàng.

Plutus DApp Store giải quyết hai rào cản gia nhập cụ thể:

- Hiện tại không có cơ chế khám phá DApp chính thức. Hầu như tất cả các sản phẩm mới được phát hiện một cách tự nhiên hoặc truyền miệng hoặc thông qua các chương trình khuyến mãi trên mạng xã hội.
- Không có bức tranh tổng hợp nào về tất cả các DApp có thể truy cập được trong một hệ sinh thái nhất định cho người dùng cuối.

Thông qua kiểm tra logic tự động, kiểm tra hợp đồng thông minh của con người và xác minh chính thức, chương trình chứng nhận cung cấp cho người tiêu dùng sự chắc chắn về hành vi của bất kỳ ứng dụng nào họ sử dụng.

Bất kỳ DApp nào, được chứng nhận hoặc chưa được chứng nhận, đều có thể được tìm thấy trong cửa hàng, nhưng Lace sẽ cung cấp cho người dùng thông tin rõ ràng về trạng thái chứng nhận của DApp. Mục tiêu của DApp Store là phục vụ như một nền tảng để đánh giá người dùng minh bạch thay vì đóng vai trò là người gác cổng hoặc thẩm phán.

Tầm quan trọng của chứng nhận

⁸¹⁴

Phiên họp cấp cao của Cardano 2021 về Chứng nhận, Summit.cardano.org/sessions/smart-contract-certification-the-why-and-how

⁸¹⁵

của Cardano 2021 Summit D App Store, Summit.cardano.org/sessions/redefining-dapp-Discovery-bringing-dapps-to-the-mass-market

DApp Store là một cửa hàng dành cho DApps. Tuy nhiên, nó không cung cấp bất kỳ bảo đảm 'tích hợp sẵn' nào ngoại trừ xác thực cộng đồng. Đây là khi thành phần thứ hai đi vào hình ảnh. Quy trình chứng nhận của IOG chịu trách nhiệm ngăn chặn các lỗi bảo mật cấp mã, đạt được bằng cách triển khai một số cấp độ 'phòng thủ'.

Sẽ có nhiều cấp độ để lựa chọn. Kiểm tra logic tự động, ở mức cơ bản nhất, sẽ giúp xác định một số dạng mã có hại. Ví dụ, những điều này sẽ có thể xác định xem hợp đồng có cơ chế thu hồi tiền đã bị khóa hay không. Các khoản tiền bị khóa phải được lấy lại theo một hợp đồng được viết rõ ràng.

Hơn nữa, kiểm tra hợp đồng thông minh thủ công sẽ hỗ trợ IOG xác minh tính toàn vẹn của bất kỳ DApp nào. Cuối cùng, việc xác minh chính thức kỹ lưỡng sẽ kiểm tra mô hình toán học để xác định rằng hành vi của hợp đồng thông minh phù hợp với đặc điểm kỹ thuật chính thức.

Tất nhiên, bất kỳ chương trình chứng nhận nào cũng chỉ tốt khi những người kết hợp và vận hành nó. Do đó, IOG đã hợp tác với một số người chơi nổi tiếng nhất trong lĩnh vực lập trình chức năng.

Chứng nhận và đảm bảo

IOG đã trình diễn ⁸¹⁶thử nghiệm tự động các hợp đồng thông minh, là các thành phần của DApp chứ không phải toàn bộ DApp, trong Hội nghị thượng đỉnh Cardano năm 2021. Về lâu dài, IOG hy vọng sẽ thấy các công cụ do người dùng thiết kế, việc triển khai chúng tới cửa hàng và mở rộng Plutus DApp Store để kết hợp các tính năng bổ sung như nâng cấp, đánh giá và tích hợp Atala PRISM cho phép người dùng cung cấp phản hồi về DApp của cửa hàng.

Khi nói đến việc xây dựng và xử lý các hợp đồng thông minh, sự đảm bảo cao là điều cần thiết. Bạn muốn biết rằng mã nguồn có chất lượng tuyệt vời, hợp đồng được bảo mật và sẽ hoạt động như mong đợi, đồng thời mã nguồn sử dụng các thuộc tính và hành vi tốt. Chứng nhận đảm bảo rằng các bài kiểm tra bảo mật được thực hiện trước bất kỳ triển khai nào và các hợp đồng thông minh có thể được kiểm tra khi chúng phát triển. Nó hỗ trợ cả nhà phát triển hợp đồng thông minh và người dùng cuối bằng cách hỗ trợ bảo vệ tài sản và danh tiếng của người dùng khỏi lỗi mã hoặc khai thác.

IOG đã công bố ý định cung cấp các cấp chứng nhận cao hơn cho các ứng dụng phi tập trung (DApp) tại Hội nghị thượng đỉnh Cardano 2021. Chương trình chứng nhận này sẽ thiết lập các tiêu chuẩn chất lượng cho DApp và các liên hệ thông minh có liên quan.

Ba cấp độ chứng nhận

Giáo sư Simon Thompson, ⁸¹⁷giám đốc dự án kỹ thuật tại IOG và Shruti Appiah, ⁸¹⁸trưởng bộ phận sản phẩm tại IOG, đang dẫn đầu nỗ lực này. Nó sẽ hỗ trợ IOG tuân thủ các phương pháp hay nhất được thấy trong ngành. Họ đang hợp tác với các công ty như Runtime Verification (runtimeverification.com), Tweag (tweag.io), Well-typed (well-typed.com), Certik (certik.io) và các công ty khác để triển khai chương trình chứng nhận mới này, được tích hợp vào DAppStore mới. Điều này sẽ khả dụng trên ví nhẹ mới của IOG, *Lace*, ⁸¹⁹được ra mắt ở Texas tại Consensus 2022. ⁸²⁰

Các cấp độ chứng nhận khác nhau là gì?

Về mặt đảm bảo và kiểm toán, có ba cấp độ chứng nhận, mỗi cấp độ này bổ sung cho các cấp độ khác chứ không phải cấp tiền.

⁸¹⁶

Chứng nhận hợp đồng thông minh, Summit.cardano.org/sessions/smart-contract-certification-the-why-and-how

⁸¹⁷

Giáo sư Simon Thompson, iohk.io/en/team/simon-thompson

⁸¹⁸

Shruti Appiah, iohk.io/en/team/shruti-appiah

⁸¹⁹

Ví ren nhẹ, ren.io

⁸²⁰

Đồng thuận 2022, coindesk.com/consensus2022/

LEVEL ONE Automated tooling	LEVEL TWO In-depth audit	LEVEL THREE Formal verification
This level gives continual assurance about a range of properties for smart contracts. - It covers the discovery of different types of issues or bugs and is characterized as low cost, low effort, accessible to everyone while providing a substantial level of assurance. - It can be applied repeatedly and automatically, so each time there is a release or a sub-release of an application, we can test to ensure that the application still has the properties that we expect.	This level involves looking at the technology and processes that led to it being produced. - It is characterized by the fact that it involves a manual audit and verification of smart contracts within the DApp itself. - The audit is performed at a much more in-depth level and involves more manual effort that can address a DApp in its entirety, even if it is written in a variety of languages.	This level is more specialized. - We aim to provide full assurance of critical aspects of applications through formal verification of smart contracts. - Formal verification involves ensuring that a smart contract serves the specific business or technical requirements defined at the outset.

Hình 76: Các cấp chứng chỉ

Lợi ích của sự đảm bảo

Cả nhà phát triển ứng dụng và kiểm toán viên sẽ có thể xác minh tính hợp lệ, tuân thủ và nhất quán của các yêu cầu thông qua chứng nhận. Nó cũng sẽ đảm bảo rằng các DApp được khởi chạy trên Cardano không có các lỗi bảo mật điển hình và cung cấp một mức độ khả năng phục hồi, ổn định và bảo trì. Mặc dù chứng nhận sẽ được khuyến khích mạnh mẽ và DApp Store sẽ được quản lý, nhưng nó sẽ không bắt buộc hoặc hoạt động như một 'người gác cổng', đảm bảo sự cân bằng giữa đảm bảo người dùng và các nguyên tắc phi tập trung.

Bạn có thể đảm bảo với cộng đồng và đảm bảo rằng mọi thứ sẽ hoạt động theo kế hoạch bằng cách kiểm tra các giai đoạn thông số kỹ thuật, thiết kế và ý tưởng. Bảng chứng này cung cấp tài liệu mở rộng về các yêu cầu, sẽ đóng vai trò là điểm tham chiếu trong tương lai.

Chứng nhận và Cửa hàng DApp

IOG dự định liên kết chứng nhận này với Cửa hàng DApp mới của họ để tạo ra các Token không thể thay thế (NFT) bảo mật bằng mật mã để làm bằng chứng về các mức chứng nhận mà họ sẽ đảm bảo. Cửa hàng DApp sẽ là một phần của ví ánh sáng *Lace*, nơi người dùng có thể kiểm tra trạng thái chứng nhận của từng DApp khi họ duyệt qua các danh mục và DApp riêng lẻ. Người dùng sẽ tin tưởng hơn vào chất lượng và sự an toàn của DApps nếu trạng thái chứng nhận bắt buộc được thể hiện rõ ràng trong suốt quá trình lựa chọn.

Tại ScotFest ⁸²¹ năm 2022, Simon Thompson đã cung cấp thông tin cập nhật về tiến trình của nhóm. Làm việc với cộng đồng, *Nhóm công tác chứng nhận Cardano Dapp* hiện đã được triển khai cùng với các biện pháp bảo vệ được nêu trong *CIP-52 - Hướng dẫn thực hành tốt nhất về kiểm toán Cardano*.

Cũng tại ScotFest, Giám đốc Dịch vụ & Ví của IOG, Alex Apeldoorn, người đã xem trước ⁸²²những gì sắp ra mắt với Lace. Ví hàng đầu của IOG sẽ tiếp cận mọi khía cạnh của trải nghiệm người dùng trong tương lai:

- sử dụng ví phần cứng để bảo mật khóa của bạn trong ứng dụng di động Lace và plugin trình duyệt
- tận dụng chức năng trình kết nối DApp sẵn có để dễ sử dụng với các DApp khác, dựa trên các tiêu chuẩn CIP
- gửi nhiều tài sản đến nhiều ví trong một giao dịch
- Đối tác đầu tiên của Lace là đội ngũ quản trị. Các đề xuất và biểu quyết của Catalyst sẽ chuyển đến đó từ IdeaScale.

⁸²¹

Chương trình chứng nhận DApp, youtu.be/kSvfj1YZ1Oo

⁸²²Nền tảng ví nhẹ của IOG, Lace, youtu.be/KWulFbCSXus

- ủy quyền nhóm đa cổ phần sẽ mở rộng để ủy quyền cho nhiều DReps
- các tính năng kiểm toán dựa trên sự tích hợp với Atala Prism DID và thông tin đăng nhập có thể kiểm chứng
- Hợp tác với Pezesha trên Trung tâm RealFi của họ

Tiên tri trên Cardano

Sử dụng Plutus và Marlowe để phát triển các ứng dụng tài chính minh bạch và đáng tin cậy bằng cách sử dụng lời tiên tri và hợp đồng thông minh là cốt lõi trong lời hứa của DeFi và RealFi. IOG đã công bố mối quan hệ chiến lược đối mới với Chainlink Labs tại Hội nghị thượng đỉnh Cardano năm 2021,⁸²³ điều này sẽ hỗ trợ các nhà phát triển tạo hợp đồng thông minh cho các ứng dụng Cardano DeFi.

'Mạng tiên tri phi tập trung' của Chainlink sẽ cho phép truy cập vào cơ sở dữ liệu trong thế giới thực, cho phép 'hợp đồng thông minh' thực thi xung quanh dữ liệu như kết quả bầu cử, tỷ số thể thao và giá Crypto. Một ví dụ khác mà điều này có thể có lợi là việc cung cấp dữ liệu thời tiết. Chainlink Labs hợp tác với một số công ty FinTech ở Châu Phi cận Sahara đang cố gắng biến bảo hiểm tham số thành hiện thực. Dữ liệu thời tiết an toàn, đáng tin cậy và linh hoạt là đầu vào quan trọng cho⁸²⁵ các hợp đồng bảo hiểm tham số.

Trên nhiều Blockchain, nhưng chủ yếu là Ethereum, Chainlink cung cấp các dịch vụ tiên tri để thúc đẩy các hợp đồng thông minh lại. Hợp đồng thông minh có thể kết nối với bất kỳ API bên ngoài nào thông qua mạng tiên tri Chainlink, cho phép họ sử dụng các tính toán ngoại tuyến an toàn cho các ứng dụng giàu tính năng. Chainlink hiện bảo đảm hàng chục tỷ đô la trên DeFi, bảo hiểm, trò chơi và các lĩnh vực quan trọng khác, cung cấp một công cụ chung cho tất cả các Blockchain cho các tổ chức toàn cầu và nhà cung cấp dữ liệu nổi bật.

Các nhà phát triển sử dụng Blockchain sẽ có thể đưa dữ liệu cấp tổ chức của Chainlink vào hợp đồng thông minh của họ. Hỗ trợ cho các dịch vụ phi tập trung bổ sung của Chainlink sẽ xuất hiện sau nguồn cấp giá thị trường: dữ liệu thể thao cho thị trường cá cược, bộ dữ liệu thời tiết cho các sản phẩm bảo hiểm tham số và tính ngẫu nhiên có thể kiểm chứng đối với trò chơi và Token không thể thay thế (NFT). Sự hợp tác này giữa IOG và Chainlink Labs sẽ cung cấp quyền truy cập vào rất nhiều dữ liệu an toàn, hỗ trợ DeFi hiện thực hóa mục tiêu tạo ra một hệ thống kinh tế toàn cầu công bằng và tiết kiệm chi phí hơn.

IOG state Chainlink là tùy chọn tiên tri ưa thích của họ dành cho Cardano, tuy nhiên, có những lựa chọn thay thế xứng đáng như được liệt kê trên Essential Cardano⁸²⁶ và các trang web của bên thứ ba như CardanoCube.⁸²⁷ Charli3 đã ra mắt tiên tri bản địa Cardano đầu tiên tại *Rare Bloom* ở Denver.⁸²⁸ Một tùy chọn dựa trên EUTXO khác là Oracle Pools⁸²⁹ của Ergo, người đã tuyên bố trên blog của họ:

Thiết kế của nhóm tiên tri của Ergo hiệu quả và có thể lập trình hơn so với việc sử dụng nhiều điểm dữ liệu tiên tri đơn lẻ, chẳng hạn như trong thiết kế tiên tri của Chainlink. Chúng tôi xây dựng hệ thống phân cấp độ tin cậy bằng cách sử dụng nhóm tiên tri và nhóm của nhóm tiên tri, trong Ergo. Nó nhanh hơn, rẻ hơn và có lợi hơn cho người dùng cuối.

của Ergo nên được xem xét một cách nghiêm túc, vì họ đã thể hiện năng lực kỹ thuật của mình khi cung cấp 15 nghìn đầu ra cho mỗi giao dịch bằng cách sử dụng EUTXO và các bản tổng hợp.

⁸²³

Chainlink (mã: LINK) là một mạng tiên tri phi tập trung đưa dữ liệu ngoài chuỗi sang định dạng trên chuỗi, thu hẹp khoảng cách giữa các Blockchain bị cô lập và dữ liệu trong thế giới thực.

⁸²⁴

Cardano công bố sự hợp tác chiến lược để tích hợp các Oracle của Chainlink, chainlinktoday.com/cardano-announces-strategic-collaboration-to-integrate-chainlinks-oracles/

⁸²⁵

Bảo hiểm tham số là loại bảo hiểm không bồi thường tổn thất thuần túy, nhưng ex-ante (tiếng Latinh nghĩa là 'trước sự kiện') đồng ý thanh toán khi xảy ra sự kiện kích hoạt. Sự kiện kích hoạt thường là một sự kiện tự nhiên thảm khốc thường có thể dẫn đến một hoặc một loạt các tổn thất. Nhưng các nguyên tắc bảo hiểm tham số cũng được áp dụng cho bảo hiểm mùa màng Nông nghiệp và các rủi ro thông thường khác không mang tính chất thiên tai, nếu kết quả của rủi ro có tương quan với một tham số hoặc một chỉ số của các tham số.

⁸²⁶

Tiên tri Cardano cần thiết, github.com/input-output-hk/essential-cardano/blob/main/essential-cardano-list.md#oracles

⁸²⁷

CardanoCube Oracles, cardanocube.io/collections/oracle

⁸²⁸Charli3 Cardano Native Oracle ra mắt tại Rare Bloom, youtu.be/bGFMMs0oDZo

⁸²⁹

Ergo Oracle Pools, ergoplatform.org/en/blog/2021-04-27-chainlink-oracles-vs-ergo-oracle-pools/

Cardano ở Châu Phi

Cardano đã được giới thiệu ở đầu cuốn sách này bằng cách trích dẫn sứ mệnh của nó:

Cardano là một nền tảng mở tìm cách cung cấp danh tính kinh tế cho hàng tỷ người thiếu nó bằng cách cung cấp các ứng dụng phi tập trung để quản lý danh tính, giá trị và quản trị

Bất chấp những tiến bộ công nghệ, con người vẫn sống ở hai thế giới khác nhau, một thế giới dành cho những nước phát triển và một thế giới dành cho những nước đang phát triển. Hàng tỷ người thiếu bản sắc kinh tế hiện không ở trong thế giới phát triển. Nhu cầu về Cardano rõ rệt nhất ở các khu vực như Châu Phi, Đông Nam Á, tiểu lục địa Ấn Độ, Mông Cổ, Châu Mỹ Latinh, trong số những nơi khác, nơi tác động của toàn cầu hóa không được thuận lợi cho lắm.

Cardano không chỉ là một loại Crypto; nó là một nền tảng để quản trị, nhận dạng và mã hóa tài sản kỹ thuật số. Các quốc gia không có cơ sở hạ tầng và hệ thống hoạt động đã chín muồi cho sự gián đoạn. Có nhiều khả năng hơn để cài đặt hoặc thay thế các hệ thống bỏ phiếu, đăng ký quyền sở hữu đất đai, cơ chế thanh toán và quy trình chuỗi cung ứng.

Đã có tiền lệ cho chiến lược này. Khi Estonia rời Khối Xô Viết, họ có một phương tiện trống để bắt đầu lại. Sự chuyển đổi kỹ thuật số tiếp theo của họ ⁸³⁰được các quốc gia khác coi là một ví dụ về cách đại tu cơ sở hạ tầng của bạn.

Châu Phi không phải là trọng tâm duy nhất của Cardano, nhưng nó là bộ phóng lý tưởng cho công nghệ của họ. Tất cả các dự án và sáng kiến được thảo luận trong chương này có thể được sao chép ở các khu vực pháp lý khác, bao gồm cả thế giới phát triển. Nếu một hệ thống có thể hoạt động với 5 triệu sinh viên Ethiopia, thì nó cũng có thể hoạt động tương tự với 107 triệu công dân của đất nước. Nếu một hệ thống có thể kết nối những thứ chưa được kết nối ở Tanzania, thì mô hình của nó có thể được triển khai sang các nước láng giềng.

Câu chuyện thành công về M-Pesa (thanh toán bằng tiền di động) của Kenya là bằng chứng cho thấy 'sự cần thiết là mẹ của mọi phát minh'. ⁸³¹Kể từ khi ra mắt vào năm 2007, M-Pesa hiện đang phát triển mạnh mẽ trên khắp châu Phi với hàng triệu người dùng và giao dịch mỗi tháng, thường là trên điện thoại di động cũ bị người dùng ở các nước phát triển vứt bỏ.

Các nền tảng cho vay vì mô như Kiva (kiva.org) cung cấp một mô hình kinh doanh có lợi nhuận rất phù hợp với nền kinh tế đang mở rộng của Châu Phi. Các khoản vay nhỏ có thể thay đổi cuộc sống của nông dân, doanh nhân và bất kỳ ai có ý chí sáng tạo và phát triển trong môi trường này.

Việc đưa người dùng trực tuyến trở nên dễ dàng hơn và rẻ hơn và xu hướng tiếp tục này là chìa khóa cho các dự án cơ sở hạ tầng như Thế Giới Di Động. Mặc dù có những thách thức cũ như tham nhũng và bất ổn dân sự ở Châu Phi, nhưng thường không có hệ thống cũ nào có thể thay thế, vì vậy những người ra quyết định cởi mở hơn và hướng tới tương lai.

Nhân khẩu học là một cân nhắc lớn khác. Châu Phi là lục địa trẻ nhất thế giới, với độ tuổi trung bình là 20 và 60% dân số dưới 25 tuổi. Một trong những lý do khiến Trung Quốc đầu tư hơn 20 tỷ USD vào cơ sở hạ tầng của Châu Phi là vì họ coi đây là cơ hội để định hình địa chính trị và kinh tế thế giới ở châu Phi. những thập kỷ tới.

Trong quá khứ, những nơi như Thung lũng Silicon là động lực chính của sự đổi mới. Điều này đã thay đổi với Blockchain vì nó không cần xin phép, dễ tiếp cận hơn và được xây dựng để cho phép đưa vào tài chính xã hội trên quy mô toàn cầu. Mô hình đang trở nên phẳng hơn, với ít thứ bậc hơn, vì vậy giờ đây, bất kỳ ai ở bất kỳ đâu có ý tưởng và động lực đều có thể sử dụng nền tảng Blockchain.

Nguồn gốc của IOG ở Châu Phi rất sâu xa như đã được giới thiệu trong chương trình 'Đặc biệt Châu Phi' của họ vào năm 2021. John O'Connor, Giám đốc Điều hành Châu Phi tại IOG, đã cung cấp thông tin cập nhật về tiến độ tại ScotFest. ⁸³²Hiện có 60 dự án được tài trợ trên 12 quốc gia khác nhau trên khắp lục địa. Vào năm 2021, chỉ có hai dự án ở hai quốc gia, cả hai đều có sự tham gia của IOG. Hiện có nhiều dự án được tài trợ bởi Catalyst, Emurgo Châu Phi và *ariob*, (ariob.io) một chương trình vườn ươm IOG hợp tác với iceaddis (iceaddis.com).

⁸³⁰

8 bài học từ quá trình chuyển đổi kỹ thuật số của Estonia cho Châu Mỹ Latinh và Caribe, blogs.iadb.org/administracion-publica/en/8-lessons-from-estonias-digital-transformation-for-latin-america-and-the-caribbean/

⁸³¹

M-Pesa: Câu chuyện thành công về tiền di động của Kenya kỷ niệm 15 năm, africa.businessinsider.com/local/markets/m-pesa-kenyas-mobile-money-success-story-celebrates-15-years/srp9gne

⁸³²IOG & Châu Phi, youtube.be/THC80NFj4lo

Bộ Giáo dục Ethiopia

Đây là quan hệ đối tác hàng đầu của IOG được công bố vào năm 2021. Dự án nhằm triển khai SSI, tận dụng hệ thống Atala Prism cho phép 5 triệu sinh viên và 750.000 giáo viên chuyển từ hệ thống trên giấy sang giải pháp dựa trên DID. Theo dõi điểm số, trình độ học vấn và điểm danh là một trường hợp sử dụng lý tưởng để mở đường cho các đối tác trong tương lai. Thông tin đăng nhập được xác minh sau đó có thể cho phép sinh viên tốt nghiệp chứng minh thành tích học tập của họ và thành công trong thị trường việc làm. Cuộc nội chiến *Tigray* (ngừng bắn 2020-2022) không giúp được gì, nhưng quá trình phát triển hiện đã hoàn tất và sẽ sớm được triển khai trực tiếp tại các trường học.

Chuỗi Thẻ Giới Di Động (WMC)

Dưới sự lãnh đạo lôi cuốn của Mickey Watkins, World Mobile là những người tiên phong trong việc mang lại kết nối cho thế giới đang phát triển. World Mobile chạy trên mạng lưới⁸³³ tận dụng Cardano để cung cấp kết nối chằng cuối cho những người không được kết nối hoặc những người đang bị tính phí quá cao cho nó. Tận dụng công nghệ tiên tiến và máy điều hòa không khí,⁸³⁴ mục tiêu của WMC là cung cấp khả năng truy cập internet với mức giá bằng 50% so với các mạng đối thủ. Thẻ Giới Di Động đã đạt được tiến bộ nhanh chóng⁸³⁵ khi phát triển từ 'thành phố thông minh' sang 'quốc gia thông minh' và hiện đang triển khai 'công nghệ mạng động' của họ đến các khu vực của Hoa Kỳ chưa phủ sóng di động

empowa

Empowa giống như 'RealFi'. Nền tảng tài trợ phi tập trung này cung cấp nhà ở giá cả phải chăng trên khắp Mozambique và hơn thế nữa. Empowa sử dụng thanh khoản dựa trên Crypto trên Cardano để cung cấp tài chính cho các nhà phát triển nhà ở nhằm cung cấp mô hình 'cho thuê để sở hữu'. Có một nhu cầu rất lớn đối với một dự án như vậy, với sự vắng mặt của bất kỳ thị trường thế chấp thực sự nào trên khắp lục địa. Empowa đã có một tác động lớn, mở rộng từ 1% khả năng tiếp cận nhà ở, lên 60% ở Mozambique.

Pezesha

Pezesha là một công ty công nghệ tài chính có trụ sở tại Kenya chuyên cung cấp vốn lưu động giá cả phải chăng cho các doanh nghiệp vừa và nhỏ (SME) ở Châu Phi. Ra mắt vào năm 2016, sứ mệnh của nó là dân chủ hóa các dịch vụ tài chính cho những người không có tài khoản ngân hàng trên khắp Châu Phi. Người sáng lập Pezesha, Hilda Moraa, đã đi vào chi tiết hơn trong bài nói chuyện của cô ấy tại ScotFest.⁸³⁶ IOG trước đây đã đầu tư vào giấc mơ của Moraa và họ sẽ hợp tác với ví ánh sáng *Lace* và *Atala Prism* để làm cho các khoản vay của họ có thể tiếp cận được với nhiều đối tượng hơn. RealFi on *Lace* sẽ ở dạng 'thị trường của các thị trường' và một trong những thị trường đó sẽ là Pezesha.

Charles Hoskinson thường tuyên bố rằng thước đo thành công của anh ấy là nếu thứ gì đó giống như Pezesha có thể chạy trên Cardano⁸³⁷ vì nó sẽ hỗ trợ tầm nhìn của anh ấy được đưa ra trong Ted Talk⁸³⁸ ở Bermuda vào năm 2014. Tôi nghi ngờ có thể có một bản demo vào năm 2023 với Hoskinson cho vay trên Pezesha sử dụng Lăng kính *ren* và Atala.

⁸³³

Mạng lưới là mạng cục bộ (LAN) trong đó các Node kết nối trực tiếp, linh hoạt và không phân cấp với càng nhiều Node khác càng tốt. Các Node hợp tác với nhau để định tuyến dữ liệu đến và từ máy khách một cách hiệu quả.

⁸³⁴ Máy điều hòa không khí của Thẻ Giới Di Động hoạt động như thế nào, worldmobile.io/blog/post/how-aerostats-work

⁸³⁵

Động : Xây dựng thành phố thông minh, xây dựng quốc gia thông minh, youtube.com/watch?v=5ijAOa6VjzA

⁸³⁶ Powerubg vốn lưu động phải chăng, youtube.com/watch?v=2ZgOAduls7Q

⁸³⁷

Charles Hoskinson e giải thích tại sao bây giờ anh ấy sẽ biết rằng Cardano là một 'Thành công' đã đạt được , cardanofeed.com/charles-hoskinson-explains-how-he-will-know-that-cardano-has-achieved-success-356.html

⁸³⁸

Tương lai sẽ phi tập trung | Charles Hoskinson | TEDxBermuda , www.youtube.com/watch?v=97ufCT6lQcY



Hình 77: Tín dụng hình ảnh Pezesha

Quan điểm

Cardano đã đi một chặng đường dài trong một khoảng thời gian ngắn. Kỷ nguyên Byron diễn ra chậm chạp và khó chịu, nhưng nó đã dẫn đến việc tạo ra bộ kết hợp hard fork và nhịp phát hành ổn định mà chúng ta đã thấy kể từ đó. Cách đây không lâu, ý tưởng về bằng chứng cổ phần bị chế nhạo, giờ đây nó đã trở nên hiển nhiên. Nghiên cứu sâu rộng và triển khai ổn định các thời đại trước có nghĩa là các nhà phát triển đang xây dựng trên đá granit.

Cardano luôn trung thành với các nguyên tắc của nó, ngay cả khi điều đó không thuận tiện. Testnet được khuyến khích (ITN) có thể là một loại Crypto theo đúng nghĩa của nó, nhưng nó chỉ là một *đơn đặt hàng* trước Shelley mainnet. Cardano đã tiếp cận sự phát triển từ một góc độ khác với các Blockchain 'xây dựng trước, sửa chữa sau' khác. Với các vụ hack và lừa đảo hiện là tin tức hàng tuần trong ngành, cách tiếp cận có phương pháp và hợp lý này là một luồng gió mới.

Đã có sự bùng nổ ngoài mong đợi của CNFT, kết quả của các tính năng phù hợp và trải nghiệm người dùng dễ dàng. Khi tôi đang học thạc sĩ (2018), tôi nhớ rằng vào thời điểm đó, tôi đã nghĩ rằng một thuật ngữ như Token không thể thay thế (NFT) sẽ không bao giờ phổ biến. Giờ đây, NFT đang trên đà trở thành xu hướng chủ đạo. Nhiều ngôn ngữ lập trình hơn đang được cung cấp, công cụ dành cho nhà phát triển đang phát triển nhanh chóng và ví nhẹ *Lace* sẽ sớm phục vụ cho việc bỏ phiếu trực tuyến và ủy quyền một phần. Nhưng đó chỉ là một chiếc ví cạnh tranh trong một hệ sinh thái thịnh vượng.

Chúng ta hiện đang ở trong Thời đại của Voltaire, quá trình triển khai quản trị trên chuỗi đầy thách thức và tham vọng nhất từ trước đến nay. Không ai khác đang cố gắng bắt cứ điều gì như thế này. Một điểm khác biệt nữa là Midnight Sidechain, giải pháp duy nhất cung cấp các hợp đồng thông minh dựa trên quyền riêng tư.

Như bạn có thể thấy trong vài chương trước, có rất nhiều phân chuyển động trong giai đoạn sơ khai. Tuy nhiên, khi các tính năng như Mamba được phát hành, các phần trước của lộ trình dường như có ý nghĩa hơn khi nhìn lại. Mặc dù chuỗi chính đã ưu tiên tính bảo mật và độ tin cậy, nhưng các chuỗi phụ cho phép các nhà phát triển có các mô hình lập trình linh hoạt hơn và các giao thức đồng thuận nhanh hơn. Việc áp dụng cần có thời gian, Ethereum đã phải đợi hơn hai năm trước khi *CryptoKitties*⁸³⁹ thu hút được sự chấp nhận đáng kể của người dùng.

Cho dù Cardano có thể ẩn tượng đến đâu, thì vẫn có những đám mây pháp lý đen tối hình thành do hậu quả của các vụ lừa đảo và hack vào năm 2022 vẫn đang diễn ra. Thật bức bối khi một thứ nguyên tắc và tỉ mỉ như Cardano lại được nhắc đến cùng lúc với một số diễn viên hiện đang rời sân khấu. Hãy hy vọng đó chỉ là thứ rác rưởi tự đổ ra ngoài.

Quy định có thể đang được thực hiện, nhưng không rõ nó sẽ ở dạng nào hoặc sẽ được thực thi như thế nào. Hầu hết các quốc gia hiện đang triển khai CBDC (tiền kỹ thuật số của ngân hàng trung ương),⁸⁴⁰ trước đó thường là một cuộc đàn áp theo quy định đối với bất kỳ thứ gì giống như cạnh tranh. Một nghiên cứu điển hình đáng chú ý là Nigeria, nơi một phần ba dân số trưởng thành sử dụng Crypto, tỷ lệ chấp nhận cao nhất ở bất kỳ đâu. Khi chính phủ cấm Crypto vào tháng 2 năm 2021, giả định là công dân sẽ nắm lấy eNaira (CBDC của Nigeria).

⁸³⁹

Hướng dẫn về Ethereum, medium.com/coinmonks/pauls-guide-to-ethereum-280be582653

⁸⁴⁰CBDC theo quốc gia, cbctracker.org/

Thực tế là Crypto không thể bị cấm và không bao giờ biến mất. Vào tháng 10 năm 2022, một báo cáo của Bloomberg cho thấy tỷ lệ sử dụng eNaira chỉ ở mức 0,5% dân số cả nước. Trong tháng trước (tháng 1 năm 2023), chính phủ Nigeria đã đặt giới hạn rút tiền mặt qua ATM, dường như để buộc áp dụng CBDC, chỉ để thực hiện một cú quay đầu hoàn toàn thông qua dự luật hợp pháp hóa Crypto. *Kế hoạch tổng thể thị trường vốn Nigeria*⁸⁴¹ tuyên bố họ chỉ quan tâm đến việc tạo ra một "thị trường vốn sôi động". Dù động cơ là gì thì nó cũng cho thấy những cơn gió ngược quy định có thể chuyển thành những cơn gió thuận chiều rất nhanh.

Trong mọi trường hợp, Cardano tiếp tục điều hành theo tiếng trống của chính nó, với những kỷ nguyên cuối cùng của lộ trình sắp thành hiện thực. Trong khi một số đối thủ cạnh tranh đang cố gắng khắc phục cơ sở hạ tầng bị lỗi và những đối thủ khác chỉ phát nổ, thì Cardano đã hướng tới các công nghệ 'thế hệ thứ 4'⁸⁴² như sự đồng thuận đa tài nguyên, hợp đồng thông minh dựa trên quyền riêng tư, v.v. *Midnight* ban đầu là một bằng chứng riêng biệt Blockchain hoạt động nhưng có khả năng là *Minotaur* và *Ofelimos* các tài liệu nghiên cứu sẽ xuất hiện trở lại ở đâu đó trong tương lai của Cardano.

Cuốn sách này bắt đầu bằng việc giải thích nguồn gốc của Bitcoin. Thật trớ trêu khi Cardano hiện đang dẫn đầu trong việc hiện thực hóa tầm nhìn do Satoshi Nakamoto vạch ra trong sách trắng Bitcoin năm 2009. CH:⁸⁴³

Chúng tôi đã nhận ra tầm nhìn về Bitcoin. Đối với tiền màu, (chúng tôi có) tài sản gốc Cardano. Lightning về cơ bản là những gì Hydra đã đạt được. Trách nhiệm giải trình toàn diện có nghĩa là mọi người đều có một bản sao của Blockchain, ngay cả khi không có bản sao của Blockchain. Vì vậy, bạn là Node của riêng bạn, bạn là ngân hàng của chính mình. Khi bạn nhìn vào những người ủng hộ đầu vào, nó sẽ tạo ra một mạng có thể mở rộng quy mô cho hàng tỷ người dùng, và rất nhiều thứ đang diễn ra mà không phải hy sinh tính phi tập trung, hệ thống sẽ trở nên phi tập trung hơn theo thời gian... và sau đó là Voltaire, khái niệm một CPU-một phiếu bầu đó ... ý tưởng rằng mọi người đều có thể đóng góp trong quản trị, tôi nghĩ chúng ta sẽ ở đó. Vì vậy, tất cả những điều mà Satoshi đã vạch ra, cuối cùng chúng tôi đã nhận ra, bằng cách này hay cách khác, trong dự án này với cộng đồng này và chúng tôi chỉ mới bắt đầu ở khía cạnh đó.

Dù điều gì xảy ra tiếp theo, thì có một điều chắc chắn là sẽ có rất nhiều điều để viết trong ấn bản tiếp theo của *Cardano dành cho Thánh lễ*.

⁸⁴¹vốn của Nigeria , sec.gov.ng/wp-content/uploads/2015/10/Opportunities-in-the-Nigerian-Capital-Market.pdf

⁸⁴²

Nguyên tắc đầu tiên: Nghiên cứu cho tương lai, youtube.com/watch?v=MVuweooiXPI

⁸⁴³

Hãy nói về Basho, youtu.be/fhVo-2QUjLM?t=1938

Bảng chú giải