Tại sao các DAO nên chuyển sang vận hành trên Private Shard?

(Source: https://learnnear.club/why-should-daos-migrate-to-running-a-private-shard/ - ~1100 words)

Giới thiệu về DAO và hợp đồng đa chữ ký

Hầu hết người dùng Web3 đều đã quen thuộc với hai khái niệm là DAO và Multisign smart contract - Hợp đồng đa chữ ký, nhưng đối với những người mới tới với thế giới Web3, tôi cho rằng cần giải thích qua về hai thuật ngữ này.

DAO là gì?

"Tổ chức tự trị phi tập trung" (DAO) là một thực thể được **quản lý bởi cả cộng đồng và không có thực thể tập trung nào kiểm soát**. Hoàn toàn **tự động và minh bạch**: các hợp đồng thông minh được sử dụng để kiểm soát việc ra quyết định và phân bổ quyền sở hữu tài sản. Quá trình bỏ phiếu cho DAO được công khai trên blockchain và người dùng thường phải chọn giữa các tùy chọn loại trừ lẫn nhau. **Quyền biểu quyết thường được phân phối giữa những người dùng dựa trên trọng số biểu quyết** mà họ có trong DAO (trọng số thường được tính tỉ lệ với lượng token quản trị của dự án mà họ nắm giữ). Tất cả các phiếu bầu và hoạt động thông qua DAO được lưu trữ trên blockchain, làm cho tất cả các hành động của người dùng có thể được theo dõi một cách công khai.
Các DAO đưa ra quyết định bằng việc áp dụng ví đa chữ ký (là một smart contract).

Ví đa chữ ký là gì?

Ví đa chữ ký (Multisig) là một loại hợp đồng tiền mã hóa đặc biệt để lưu trữ token một cách an toàn. Nó yêu cầu **hai hoặc nhiều khóa riêng tư** (tương ứng các thành viên trong một DAO) để ký và tạo giao dịch và thường được sử dụng **như một lớp bảo mật bổ sung** cho các giao dịch ví bằng cách đảm bảo rằng nhiều người nắm giữ khóa tham gia phê duyệt giao dịch.
Hợp đồng đa chữ ký cũng có thể được cấu hình để cho phép từng thành viên tạo chữ ký riêng, đây cũng là một lựa chọn tuyệt vời cho những người muốn **lưu trữ tiền điện tử của họ một cách an toàn và không phụ thuộc vào bên thứ ba**.

Các DAO đang áp dụng hợp đồng đa chữ ký như thế nào?

DAO đang sử dụng ví đa chữ ký để **lưu trữ tiền của họ một cách an toàn và quản lý tài sản một cách hiệu quả**. Hợp đồng đa chữ ký cung cấp cho nhiều bên liên quan khả năng ký kết giao dịch, cho phép quản lý tiền và quyết định an toàn và đa dạng. Đa chữ ký cũng tăng thêm một lớp bảo mật bổ sung bằng cách yêu cầu nhiều khóa riêng tư để truy cập tài sản.

Ngoài ra, các DAO có thể sử dụng hợp đồng đa chữ ký để triển khai hệ thống bỏ phiếu và quản trị phức tạp hơn so với hợp đồng nhiều chữ ký thông thường. Điều này cho phép việc ra quyết định được phi tập trung và an toàn.
Các cấu trúc bỏ phiếu DAO phổ biến nhất là bỏ phiếu đại biểu theo trọng số token, bỏ phiếu bậc hai, ủy quyền bỏ phiếu (Liquid Democracy) hoặc khóa phiếu bầu và bỏ phiếu đại biểu dựa trên token.

- **Bỏ phiếu đại biểu theo trọng số token**: Yêu cầu một ngưỡng nhất định để một đề xuất được thông qua. Ví dụ: 60% đại biểu, có nghĩa là 60% số lượng chủ sở hữu của token phải bỏ phiếu ủng hộ đề xuất để nó được thông qua.
- **1 token = 1 phiếu bầu quản trị**: Quyền biểu quyết của một cá nhân tỷ lệ thuận với số lượng token họ nắm giữ.
- **Biểu quyết bậc hai**: Đó là một hệ thống cân bằng lợi ích của các nhóm thiểu số trong khi vẫn ra quyết định dựa trên ý kiến của đa số. Hệ thống này cho phép mọi người ủy thác lá phiếu của họ cho một người đại diện.
- **Khóa phiếu bầu**: một cơ chế cho phép người tham gia xóa phiếu bầu của mình mà không bị phạt.
- **Bỏ phiếu đại biểu dựa trên việc nắm giữ token**: Một hệ thống yêu cầu cử tri nắm giữ một lượng token nhất định để đề xuất được thông qua.

Những thách thức hiện tại của các DAO

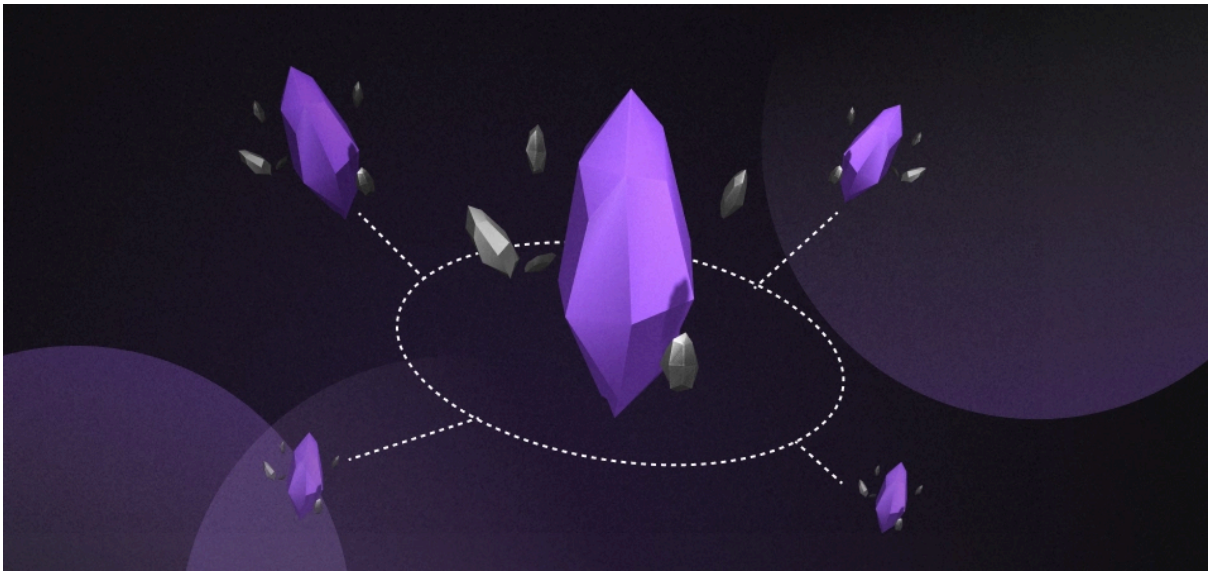
Các vấn đề chính mà DAO đang phải đối mặt bao gồm: **thiếu tư cách pháp nhân được công nhận và khả năng chịu trách nhiệm vô hạn của các thành viên, thiếu quy định và các biện pháp bảo mật không đầy đủ**. Ngoài ra, DAO **dễ bị tấn công quản trị, cấu hình không tốt hoặc có thể bị spam**. Những vấn đề này có thể tạo ra một số rủi ro như dễ lộ dữ liệu cá nhân, hợp đồng thông minh dễ bị tấn công và truy cập trái phép vào quỹ.
Phần lớn các vấn đề này có thể được giải quyết hoặc giảm thiểu bằng cách sử dụng Private Shard (Phân đoạn riêng tư), nhưng trước hết chúng ta cùng khám phá Private Shard là gì.

[Express Quiz] Cách bỏ phiếu nào sau đây có thể được sử dụng khi DAO triển khai private shard?

- Cơ chế 1 token = 1 phiếu bầu
- Biểu quyết bậc hai

- Bỏ phiếu theo trọng số token
- **Tất cả các cách trên**

Private Shard dành cho DAO: sự nâng cấp của ví đa chữ ký



Private Shard là một sidechain có thể tùy chỉnh (sidechain là mạng blockchain chạy song song với blockchain công khai có khả năng chuyển tài sản và thực hiện các lệnh gọi hợp đồng chéo) cho phép bạn bảo vệ dữ liệu của mình trong khi vẫn tận dụng được tất cả các lợi ích của blockchain chính. Nó cho phép các chủ sở hữu Private Shard có **toàn quyền kiểm soát blockchain của họ trong khi vẫn giữ thông tin riêng tư** giữa họ và chỉ cho phép một số bên công khai truy cập thông tin này.
Các thành viên DAO điều hành blockchain riêng dựa trên nhu cầu của họ. Private Shard có thể được tùy chỉnh theo các cấu trúc biểu quyết được giới thiệu ở trên, nơi **các trình xác thực** (các nút xác thực các khối của blockchain) **thuộc sở hữu của các thành viên DAO**, tương tự như cách hoạt động của một ví đa chữ ký, họ sẽ sở hữu một khóa riêng với quyền biểu quyết nhất định. Hãy nghĩ về nó như một **phiên bản nâng cấp của ví đa chữ ký, vì tất cả các thuộc tính của ví multisign cơ bản là giống nhau, trong khi vẫn đảm bảo tính riêng tư cho tất cả thông tin lưu trữ bên trong private shard.**
Trên hết, các thành viên DAO có thể **triển khai các hợp đồng thông minh tùy chỉnh bên trong Shard với "khả năng mở rộng vô hạn"** cung cấp những khả năng:

- Bỏ phiếu kín
- Kế toán và tính lương
- Triển khai các cơ chế thiên về giao dịch như đấu giá (có thể quá đắt nếu thực hiện trên public blockchain)
- Tạo ra các bộ phận quản lý ngân quỹ bên trong DAO
- Và còn nhiều khả năng khác nữa

[Express Quiz] Private shard là gì?

- Một hệ thống Web2 bí mật được lưu trữ trên một hệ sinh thái đóng
- **Một sidechain có thể tùy chỉnh (blockchain chạy song song với blockchain công khai có khả năng chuyển tài sản và thực hiện các lệnh gọi hợp đồng chéo)**

- Một DAO công khai được triển khai trên một shard của blockchain NEAR và được vận hành bởi các trình xác thực của NEAR

Cầu nối Private Shards có smart contract cho phép thiết lập các quy tắc về hợp đồng/tài khoản công khai có thể tương tác và cấu hình phù hợp. Điều này cung cấp khả năng giới hạn quyền truy cập cho một số bên hoặc hợp đồng nhất định để di chuyển tài sản đến các private shard, ngoài ra nó còn cung cấp quyền truy cập vào một số hợp đồng thông minh nhất định để thực hiện các lệnh gọi hợp đồng từ shard hoặc từ mạng chính.
Ví dụ: Một DAO có thể có **hợp đồng bỏ phiếu riêng tư bên trong private shard**, hợp đồng này sẽ bắt đầu lệnh gọi khi cuộc bỏ phiếu kết thúc và **chỉ kết quả bỏ phiếu mới được công bố trên mạng chính mà không tiết lộ phiếu bầu cụ thể của từng thành viên**. Cuộc gọi này chỉ có thể được thực hiện từ bên trong shard đó và không bên nào khác có thể thực hiện nó ngoại trừ hợp đồng cụ thể này. Điều này giúp các thành viên DAO **đảm bảo tính bí mật của phiếu bầu** giống như cách họ sử dụng multisign, trong khi **phiếu bầu thực tế được giữ bí mật**.

[Express quiz] Private shard cung cấp khả năng nào mới cho DAO?
- Bỏ phiếu bí mật
- Kế toán và tính lương nhà thầu
- Triển khai các cơ chế thiên về giao dịch như đấu giá
- **Tất cả các khả năng trên**

Trên hết, Calimero Gateway cung cấp khả năng quản lý quyền bổ sung cho các thành viên DAO để chỉ định các chính sách mà người dùng/ví công khai có thể tương tác với private shard. Trong khi các thành viên DAO chạy trình xác thực và có quyền truy cập quản trị vào shard, họ có thể mời các thành viên/ví bên ngoài đọc một số dữ liệu nhất định hoặc tương tác với các hợp đồng được chỉ định.
Ví dụ: Một DAO có thể có **một hợp đồng riêng bên private shard của mình để các bên bên ngoài gửi đề xuất mà DAO có thể bỏ phiếu**. **Chỉ những người gửi và thành viên DAO** có thể xem thông tin về trạng thái của đề xuất đó.
Khả năng gửi đề xuất có thể được giới hạn trong danh sách các ví được whitelist do DAO thêm, hoặc cũng có thể cấu hình cho phép bất cứ ai cũng có thể thực hiện tạo đề xuất.

Chúng tôi tin rằng Private Shard là sự phát triển tự nhiên tiếp theo của DAO và đang tìm cách làm việc với nhiều DAO hơn cho quá trình chuyển đổi của Web3 này.
Vui lòng liên hệ với chúng tôi nếu bạn có bất kỳ câu hỏi nào hoặc đang muốn dùng thử dịch vụ.