Abraçando a Web3 através da abstração em cadeia: um caminho para a auto soberania digital.

Sasha | ahsaS.NEAR

(traduzido por: Rodolfo Agustinho) rodobossa.near

8 min read

👍**Tip 2 nL**

Post on X + 4nL

Existem poucas dúvidas sobre o enorme potencial das tecnologias e ecossistemas descentralizados, especialmente quando se trata de capacitar os indivíduos com auto-soberania. No entanto, a enorme complexidade das aplicações descentralizadas (dApps) e o ecossistema

fragmentado de blockchains e rollups limitaram a convocatória do público em geral.

Para aproveitar verdadeiramente o poder transformador da Web3, precisamos simplificar a experiência do usuário através da abstração e promover um ambiente que apoie a auto soberania digital.

O problema de complexidade da Web3.

#1 Gestão de dados.

O estado atual dos dapps revela uma verdade absoluta: a maioria não é verdadeiramente descentralizada e nem fácil de usar. A necessidade dos usuários ao navegar nas exchanges, gerir múltiplas contas e lidar com taxas de gás, sublinha o abismo entre o ideal de aplicações contínuas e a realidade da sua complexidade. Essa complexidade não apenas impede a adoção convencional, mas também confina os dapps a uma base de usuários de nicho distante da web democratizada prevista.

Mas de onde vem essa complexidade? Vamos voltar ao básico e entender como a Web3 lida com os dados. A Web3 muda completamente a forma como os dados são armazenados e gerenciados, passando de bancos de dados centralizados para um ambiente descentralizado onde os dados são protegidos com provas criptográficas.

A forma como os dados da Web3 são abordados, com ênfase na descentralização e na validação criptográfica, apresenta um cenário complexo que desafia as estratégias tradicionais de gestão de dados.

#2 Modularidade

A tendência atual da Web3 rumo à modularidade, que envolve a divisão da funcionalidade da blockchain em camadas distintas, como liquidação, disponibilidade de dados e execução, visa aumentar a escalabilidade. Tecnologias como layer-twos, rollups Optimistic, ZK e Sidechains, exemplificam essa abordagem modular. No entanto, isso complicou inadvertidamente a experiência do usuário e do desenvolvedor, fragmentando o ecossistema em várias blockchains e conduzindo a um cenário disperso de liquidez, aplicações e bases de usuários. Os desenvolvedores enfrentam o dilema de se comprometer com uma blockchain específica, potencialmente restringindo o alcance do seu projeto.

Pode a Abstração consertar isso?

Antes de prosseguir, entendamos o que é abstração. É um conceito fundamental que simplifica a complexidade, ocultando detalhes desnecessários, permitindo que os usuários se concentrem em funcionalidades de nível superior sem ficar presos às complexidades subjacentes. Este princípio, crucial na programação orientada a objetos, vai além do desenvolvimento de software, facilitando a implementação de lógica complexa em vários domínios, fornecendo uma interface simples e fácil de interagir.

A abstração desempenha um papel crucial no desenvolvimento de software, simplificando a complexidade da construção do programa. Ele permite que os programadores se concentrem no alto nível de funcionalidade de seu código, em vez de ficarem atolados em detalhes pouco significativos de implementação. Ao abstrair códigos complexos em componentes mais gerenciáveis, os desenvolvedores podem acelerar seu fluxo de trabalho, aprimorar sua capacidade de solucionar problemas, iterar em seus programas e lidar com projetos mais avançados com maior eficiência.

A abstração não apenas agiliza o processo de desenvolvimento, mas também promove a inovação, dando liberdade aos programadores para

explorar novas ideias e soluções, aproveitando os componentes abstraídos existentes para ampliar os limites de alcance de seu software.

Mas será que essa lógica pode ser estendida às blockchains?

A “abstração de cadeia” refere-se à simplificação da experiência do usuário da blockchain, ocultando seus complexos mecanismos subjacentes. Esta estratégia visa melhorar a acessibilidade e promover uma adoção mais ampla, apresentando assim uma interface mais intuitiva, como ficou evidenciado pelo crescimento significativo de usuários do NEAR, impulsionados pela sua ênfase na abstração desde 2018.

A visão da abstração em cadeia

A abstração de cadeia permite que os usuários possam interagir perfeitamente com os dapps, sem a necessidade de entender as complexidades das redes blockchain ou gerenciar vários ativos de criptomoeda. O objetivo é fazer com que as interações com a blockchain sejam tão intuitivas quanto usar qualquer aplicativo convencional, reduzindo assim as barreiras de entrada e incentivando uma adoção mais ampla das tecnologias Web3.

Express quiz +2 nLEARNs

Qual é o objetivo principal da abstração em cadeia no ecossistema Web3?

- Aumentar a complexidade dos dApps para usuários avançados
- **(X) Simplificar a experiência do usuário, ocultando as complexidades da blockchain**
- Centralizar o gerenciamento de dados em redes blockchain
- Eliminar a necessidade de provas criptográficas nas transações de dados

O Protocolo Near exemplifica a implementação bem-sucedida da abstração em cadeia, demonstrando seu potencial para aumentar significativamente o envolvimento do usuário. Ao abstrair a camada blockchain, o NEAR permitiu que os usuários realizassem transações e participassem da economia digital em diferentes redes por meio de uma interface simples e unificada. Isto não só melhora a usabilidade, mas também abre o espaço Web3 a um público mais amplo, contribuindo para o crescimento e a diversidade do ecossistema.

A abstração de cadeia também facilita o desenvolvimento de aplicações multi-chain, permitindo que os desenvolvedores se concentrem na criação de experiências de usuário de alta qualidade, em vez de ficar presos às limitações técnicas de uma determinada blockchain. Essa abordagem incentiva a inovação e a colaboração dentro da comunidade Web3, avançando rumo a um futuro onde as identidades e os ativos digitais possam ser gerenciados e transacionados de maneira transparente em várias plataformas blockchain, unificando assim o cenário fragmentado do atual ecossistema Web3.

Exemplo de abstração de cadeia

As provas de zero conhecimento ou ZKPs (Zero-knowledge proofs) podem ser uma ótima maneira de permitir a abstração de cadeia. As provas ZKPs introduzem um mecanismo onde é possível verificar a veracidade das informações sem revelar a própria informação. Imagine que você está entrando em uma boate e, para provar que tem idade legal para beber, basta mostrar seu ano de nascimento em vez de outras informações confidenciais (como nome, endereço, número do seguro social, etc.). Esse é um exemplo real de ZKPs. Agora vamos estendê-lo às redes blockchain.

Tradicionalmente, a segurança e a integridade das transações blockchain dependiam de uma rede descentralizada de validadores. Isto exigia um mecanismo de consenso, onde múltiplas partes validaram as transações,

garantindo a sua legitimidade e mantendo assim a confiança da rede. No entanto, este método exige inerentemente um certo nível de confiança nos validadores coletivos e muitas vezes resulta num consumo significativo de recursos devido ao esforço computacional necessário para o consenso.

Os ZKPs podem permitir que um único computador afirme que certas regras ou condições foram cumpridas sem divulgar os dados subjacentes ou exigir um consenso de vários validadores. Esta mudança reduz significativamente a dependência de uma rede distribuída de validadores, permitindo que os processos de validação sejam mais simples e eficientes.

Express quiz

+2 nLEARNs

Como as provas de conhecimento zero (ZK) contribuem para a segurança das transações blockchain?

- Exigindo uma rede descentralizada de validadores para cada transação.
- Divulgando detalhes da transação para maior transparência.
- **(X) Permitindo que um único computador verifique as regras sem revelar os dados subjacentes.**
- Aumentando a necessidade de armazenamento centralizado de dados

Consequentemente, os desenvolvedores ganham flexibilidade para lançar novas blockchains com requisitos de recursos muito menores, já que não precisam mais estabelecer e manter uma grande rede de validadores. À medida que as blockchains adotam cada vez mais segurança comprovável por ZK, a publicação de uma prova ZK em uma cadeia pode verificar transações em múltiplas cadeias, tornando praticamente impossível alterar o estado de uma cadeia sem afetar as outras interligadas por essas provas.

Como o protocolo NEAR permite a abstração de cadeia

O protocolo NEAR está avançando na abstração de cadeia ao desenvolver um ecossistema centrado no usuário que simplifica as interações entre várias blockchains. Desde 2018, a NEAR priorizou a usabilidade, a escalabilidade e um modelo de conta flexível, com o objetivo de acomodar aplicações convencionais com potencial para atrair bilhões de usuários. A plataforma evoluiu para suportar totalmente a abstração de cadeia, permitindo uma operação perfeita em várias blockchains e aplicações.

Os principais componentes da abordagem da NEAR incluem uma infraestrutura de blockchain escalável capaz de suportar mais de um bilhão de contas ativas e uma barreira de segurança robusta. Esta barreira apresenta soluções de disponibilidade de dados (DA) da NEAR, zkWASM (provador de dados ZK) em colaboração com a Polygon Labs para provas eficientes de conhecimento zero e EigenLayer (protocolo de restaking) para finalidade aprimorada. Coletivamente, esses elementos garantem um ambiente seguro e escalável para aplicações descentralizadas.

O NEAR permite ainda a abstração da cadeia por meio da agregação de contas, permitindo que os usuários gerenciem suas interações em diferentes cadeias através de uma única conta. Esta simplificação estende-se à camada de dados, suportando uma ampla gama de arquiteturas blockchain e garantindo acesso consistente aos dados. Além

disso, os retransmissores de intenção na infraestrutura do NEAR facilitam operações complexas em múltiplas cadeias, melhorando a interoperabilidade e a experiência do usuário.

Os Frontends descentralizados no NEAR oferecem uma interface unificada para descobrir e interagir com aplicações em todo o espectro Web3, apoiadas por super carteiras que simplificam a experiência do usuário, eliminando a necessidade de trocar de rede ou gerenciar taxas de gás.

Capacitando os usuários com auto soberania.

Além de simplificar a experiência do usuário, a abstração em cadeia se alinha ao objetivo mais amplo da auto soberania digital. Num mundo onde os dados pessoais e os ativos digitais são cada vez mais valiosos, a capacidade de controlar e gerir a identidade e os ativos digitais de uma pessoa torna-se fundamental. A Web3, com a sua natureza descentralizada, oferece uma estrutura para os usuários atingirem este nível de controle, livres das restrições e riscos dos sistemas centralizados.

A auto-soberania garante que os indivíduos controlem os seus dados, ativos e identidades, salvaguardando a privacidade e a autonomia da exploração centralizada da autoridade. Este conceito é crucial para prevenir violações de privacidade e promover interações digitais seguras em seus próprios termos. Isto transforma a economia digital num espaço mais equitativo, diminuindo os desequilíbrios de poder e promovendo um ambiente democrático onde os usuários interagem e fazem suas transações livremente sem se preocupar com a vigilância.

Como o NEAR permite a auto soberania.

O Protocolo NEAR facilita a auto soberania por meio de sua plataforma descentralizada, projetada para dar controle aos usuários sobre suas

interações digitais. Ao abstrair as complexidades da tecnologia blockchain, o NEAR facilita o envolvimento dos usuários com dApps sem a necessidade de conhecimento profundo da infraestrutura subjacente. Esta abordagem não só melhora a usabilidade, mas também garante que os usuários possam gerenciar seus ativos e identidades digitais de forma integrada em vários aplicativos e plataformas.

O compromisso da NEAR com software de código aberto e o desenvolvimento de ferramentas fáceis de usar, como super carteiras e front-ends descentralizados, capacita ainda mais aos usuários, permitindo assim uma experiência digital auto soberana que se alinha ao espírito da Web3 e a visão mais ampla de uma Internet descentralizada.

Express quiz +2 nLEARNs

Qual recurso do protocolo NEAR oferece suporte à operação contínua em vários blockchains e aplicativos?

- Sua dependência de estratégias tradicionais de gerenciamento de dados
- Sua escalabilidade limitada e modelo de conta rígido
- **(X) Sua infraestrutura blockchain escalável é capaz de suportar mais de um bilhão de contas ativas.**
- Seu foco na centralização de identidades e ativos de usuários

A estrada à frente

O caminho para a adoção generalizada da Web3 e a realização da auto soberania digital não é isento de desafios. Requer um esforço conjunto de desenvolvedores, usuários e partes interessadas em todo o ecossistema para adotar os princípios de abstração e simplicidade. Ao nos concentrarmos em aplicativos fáceis de usar que abstraem as complexidades da tecnologia blockchain, podemos abrir as portas da Web3 para um público global.

A jornada caminho a uma Internet descentralizada e capacitada para o usuário, já está em andamento. Através dos princípios da abstração em cadeia e do foco na simplificação da experiência do usuário, podemos acelerar essa transição para a Web3 e capacitar os indivíduos com uma verdadeira auto soberania digital. À medida que navegamos nesta transição, a visão de uma Internet mais aberta, segura e centrada no usuário permanece ao nosso alcance, prometendo um futuro onde todos terão o controle sobre as suas vidas digitais.

Este guia ajudou você a entender a abstração de cadeia?*(Required)*

Sim

Não

Voto quadrático com nLEARNs*(Required)*

1 nLEARN (ONE vote) 4 nLEARNs (TWO votes) 16 nLEARNs (FOUR votes)

7

—----------

(words 2054)