

Como funciona a ponte Rainbow do NEAR

A NEAR Rainbow Bridge (ponte) é única em criptografia, é a única ponte sem permissão e Trustless (sem confiança necessária) para Ethereum. Neste artigo, vamos demonstrar como funciona!

rodobossa.near

7 min read

2 nL 4 nL 8 nL [Tip](#)



Para compartilhar e +4 nLEARNs

Artigo de Matt Henderson de [Aurora](#)

A NEAR Rainbow Bridge é única em criptografia, é a única ponte sem permissão e Trustless (que não precisa confiança) para Ethereum. Neste artigo, vamos demonstrar como funciona!

O protocolo NEAR criou a [Rainbow Bridge](#), algo que é único e valioso no espaço criptográfico, uma ponte totalmente "Trustless" para transferir tokens entre Ethereum e NEAR - e, finalmente, Aurora. Embora existam descrições técnicas da ponte por aí, este artigo explicará como ela funciona de uma maneira que esperamos que seja compreensível por qualquer pessoa com familiaridade básica com criptografia.

O conceito

Vamos começar imaginando que eu quero transferir 20 DAI desde [Ethereum até NEAR](#). Como a transferência *física* de tokens não é possível entre redes, isso significa que precisamos tirar 20 DAI de circulação no Ethereum e colocar 20 DAI em circulação na NEAR, para que a oferta global de DAI não mude.

Veja como eu poderia fazer isso sem necessidade de confiança e sem permissão:

1. Digo à rede Ethereum que quero transferir 20 DAI para outro lugar.

2. A rede Ethereum bloqueia meus 20 DAI em um cofre (um contrato inteligente), para que sejam retirados de circulação.
3. Quando tenho a certeza de que esses 20 DAI foram bloqueados no Ethereum, digo ao NEAR para criar 20 novos DAI para mim lá.
4. Logicamente o NEAR não confia em mim, portanto me pede provas que bloqueei 20 DAI no Ethereum.
5. Forneço ao NEAR a prova de que bloqueei esses DAI no Ethereum.
6. NEAR verifica minha prova de maneira independente e, em seguida, cria 20 novos DAI para eu usar no NEAR.

Mais tarde, se e quando eu desejar mover meu DAI de NEAR de volta para Ethereum, simplesmente inverte o procedimento acima. Legal, hein?

Os atores

Então agora vamos ver como tudo isso acontece na prática, usando o Rainbow Bridge. A história vai envolver uma série de componentes técnicos que compõem a ponte:

A Rainbow Bridge UI — Este é [o site](#) onde você, como usuário, interage com a ponte para transferir seus ativos entre as redes.

O LiteNode — Isso é como um nó na blockchain, exceto que ele armazena apenas cabeçalhos de bloco, reduzindo drasticamente o espaço de armazenamento necessário. O LiteNode é implementado como um contrato inteligente e temos dois deles - um implantado na rede Ethereum, que armazena cabeçalhos de bloco NEAR, e outro implantado em NEAR, que armazena cabeçalhos de bloco Ethereum.

(Para a sua informação, o LiteNode é realmente referido, em outros artigos, como o “cliente leve”, por razões históricas. Se você me perguntar: “O que é que armazena dados de blockchain?”, meu primeiro pensamento é “um nó” e, portanto, neste artigo, para ajudar com modelos mentais, eu o chamo de LiteNode).

Relayers (Retransmissores) — Como os LiteNodes são contratos inteligentes, eles não podem ser executados e atualizados sozinhos. Relayers são scripts rodando em servidores tradicionais, que periodicamente leem blocos de uma blockchain, e os comunicam ao LiteNode rodando em outra. Assim, os retransmissores mantêm os LiteNodes atualizados.

Como há um custo de transação - ou seja, taxas de gás - cada vez que um retransmissor atualiza um LiteNode, o que está em NEAR (contendo os blocos Ethereum) é atualizado em cada bloco Ethereum (já que as taxas de gás NEAR são baratas), enquanto a frequência de atualização no Ethereum (contendo os blocos NEAR) é configurável e determinada por um orçamento econômico (atualmente cerca de 12 a 16 horas).

Connectors (conectores)— **Connectors** são contratos inteligentes responsáveis por toda a lógica associada ao gerenciamento de cadeia cruzada (cross-chain) de um determinado tipo de ativo. Como os LiteNodes, eles existem em pares - um funcionando na Ethereum e outro funcionando na NEAR. Por exemplo, existe um par de “ETH Connectors” responsáveis pela transferência de ETH entre as duas redes. E há um par “ERC-20 Connector” responsável

por transferir tokens ERC-20. Alguém poderia escrever um Conector “NFT”, um Conector “Resultados do Mercado de Previsão” ou um Conector “Resultados da Votação DAO” se assim o desejasse. Qualquer ativo ou dados podem ser transferidos através do Rainbow Bridge, se existirem os conectores pertinentes!

Juntando as peças

Para entender como todos esses elementos funcionam juntos para suportar que eu transfira tokens sem permissão e sem confiança entre Ethereum e NEAR, vamos repassar nosso exemplo original mais uma vez:

1. Usando a **IU da Rainbow Bridge**, dou início a uma transferência de 20 DAI do Ethereum para o NEAR.
2. Quando confirmo a primeira das duas transações em [MetaMask](#), a Rainbow Bridge se comunica com o **conector ERC-20** no Ethereum (já que DAI é um token ERC-20), que transfere e bloqueia 20 DAI em seu cofre. Esses DAI já não irão estar mais em circulação na rede Ethereum.
3. Com base nos dados do cabeçalho no meu bloco de transação, a **IU de Rainbow Bridge** calcula uma “**prova**” **criptográfica** de que eu realmente tenha bloqueado 20 DAI.
4. Como vamos pedir à rede NEAR para criar algum DAI com base no que acabou de acontecer no Ethereum, primeiro esperamos que o **Relayer** envie cerca de 20 cabeçalhos de bloco Ethereum para o **LiteNode** em execução no NEAR. Isso é para mais segurança, da mesma forma que sua troca de criptografia faz você esperar por algumas confirmações antes de usar seus fundos depositados.
5. Após essa espera, a **interface do usuário do Rainbow Bridge** nos permite dar o passo número dois no processo - solicitar ao **conector ERC-20** no NEAR para criar 20 novos DAI para nós na rede NEAR.
6. Quando fazemos essa solicitação do conector ERC-20, fornecemos nossa **prova criptográfica** que recebemos anteriormente, “provando” que bloqueamos 20 DAI no Ethereum.
7. O **conector ERC-20** no NEAR procurará nosso cabeçalho de bloco Ethereum no **LiteNode** em execução no NEAR e fará seu próprio cálculo independente da prova criptográfica.
8. Se a **prova que fornecemos coincide** com a prova que o conector ERC-20 calculou, então estará comprovado que esses 20 DAI estão trancados com segurança no Ethereum - e que fui eu quem bloqueou! então serão criados (mint) 20 novos DAI em NEAR e entregues na minha carteira.

Quando queremos transferir DAI de NEAR de volta para Ethereum, o processo ocorre ao contrário, ou seja, em vez de bloquear 20 DAI em NEAR, nós os destruímos – operação conhecida como “burning” – e então fornecemos a “prova” dessa destruição para o Conector operando no Ethereum. Tendo acesso aos blocos NEAR no LiteNode que funciona no Ethereum, ele valida nossa prova, libera 20 DAI de seu cofre e envia para nossa carteira!

E é assim, em poucas palavras, que funciona a Rainbow Bridge! É a única ponte Ethereum em criptografia que funciona dessa maneira, atualmente - deixando que você transfira ativos

sem permissão entre Ethereum, NEAR e em breve, Aurora **sem ter que confiar em terceiros**. Muito legal!

Miscelâneos:

Aqui estão algumas notas interessantes para acompanhar essa visão geral:

- Como o [NEAR-to-Ethereum](#) Relayer envia apenas cabeçalhos de bloco NEAR para o Ethereum LiteNode a cada 16 horas, há um atraso de 16 horas entre as etapas um e dois ao mover os tokens nessa direção. (Lembre-se, isso ocorre porque as taxas de gás Ethereum tornam proibitivamente caro para o Relayer atualizar o LiteNode em cada bloco.) Existem várias formas de abordagens que nos permitiriam reduzir esse atraso, e a equipe está trabalhando ativamente nisso.
- No NEAR, o LiteNode armazena todos os cabeçalhos de bloco Ethereum anteriores. Para que o espaço de armazenamento não fique fora de controle, o LiteNode “remove” (exclui) blocos com mais de duas semanas. Isso significa que se você iniciar uma transferência de Ethereum para NEAR e sair de férias por três semanas entre as etapas um e dois, não poderá concluir sua transferência, porque os dados Ethereum armazenados NEAR necessários para verificar sua “prova” já estariam excluídos!
- Uma propriedade interessante do design do cabeçalho do bloco NEAR é que, com um único cabeçalho de bloco, podemos calcular o histórico de blocos anteriores por um período bastante longo. Então, em teoria, o LiteNode no Ethereum só precisa de um único bloco NEAR; no entanto, nós os mantemos porque os custos de gás necessários para realizar a remoção seria basicamente um desperdício de recursos.
- A equipe que criou a Rainbow Bridge é a mesma que criou a Aurora - o NEAR EVM. Como essa equipe se transformou em sua própria entidade, a Rainbow Bridge ficará sob sua própria administração para operações, manutenção e evolução futura.
- A equipe do Aurora está trabalhando na “finalização automática” para a Rainbow Bridge, para que você não precise mais iniciar manualmente a etapa número dois dessas transferências. Isso será muito conveniente para os usuários (o que significa que você pode iniciar sua transferência Ethereum para NEAR e depois sair de férias!).
- As transferências entre Ethereum e Aurora são realizadas pela Aurora Bridge, que usa a mesma tecnologia central da Rainbow Bridge, mas aprimorada para lidar com a etapa oculta NEAR/Aurora nas transferências.
- A interface do usuário e a experiência do Aurora Bridge são diferentes da Rainbow Bridge e, em algum momento no futuro, eles serão compatibilizados.

Embora alguns detalhes técnicos tenham sido simplificados, agora você tem uma compreensão fundamental de como funciona a Rainbow Bridge!

Para uma descrição mais aprofundada da Rainbow Bridge, você pode [ler este artigo](#), e também para ficar por dentro de tudo relacionado a Aurora, não deixe de [seguir Aurora no Twitter](#)

