Loopring:
Um Protocolo de Câmbio de Tokens Descentralizado

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

6 de abril de 2018

Resumo

O Loopring é um protocolo aberto para a construção de câmbios descentralizados. O Loopring opera como um conjunto público de contratos inteligentes responsáveis pelo comércio e liquidez, com um grupo de agentes em cadeia que agregam e comunicam pedidos. O protocolo é gratuito, extensível e serve como um módulo estrutural padronizado para aplicativos descentralizados (dApps) que incorporam a funcionalidade de câmbio. Seus padrões interfuncionais facilitam a negociação ainda que ela seja anônima e não seja digna de confiança. Uma importante melhoria em relação aos atuais protocolos de câmbio descentralizado é a capacidade de que os pedidos sejam misturados e combinados com outros diferentes pedidos, eliminando assim as restrições dos pares de comercialização de dois tokens e melhorando consideravelmente a liquidez. O Loopring também utiliza uma solução única e sólida para evitar o front running: a tentativa desleal de enviar transações para um bloco mais rapidamente do que o provedor original da solução. O Loopring é independente do blockchain, além de ser aplicável em qualquer blockchain com a funcionalidade de contrato inteligente. No momento da escrita, ele é operável em Ethereum [1] [2] e Qtum [3] com NEO [4] em construção.

1 Introdução

Com a multiplicação de ativos baseados no blockchain, a necessidade de trocar esses ativos entre as contrapartes aumentou significativamente. À medida que milhares de novos tokens são introduzidos – incluindo a tokenização de ativos tradicionais – essa necessidade é ampliada. Seja o câmbio de tokens por motivações especulativas de negociação, ou conversão para o acesso de redes através de seus tokens de utilidade nativos, a capacidade de trocar um ativo cripto por outro é fundamental para um ecossistema maior.

De fato, existe uma energia potencial em ativos [5], e a compreensão dessa energia - de capital de desbloqueio - requer não apenas a propriedade, que os blockchains permitiram invariavelmente, mas também a capacidade de transferir e transformar gratuitamente esses ativos.

Como tal, o câmbio de tokens sem confiança (valor) é um caso de uso convincente para a tecnologia blockchain. Até agora, no entanto, os entusiastas da criptografia decidiram maioritariamente por tokens de negociação em câmbios centralizados tradicionais. O protocolo Loopring é necessário uma vez que, assim como o Bitcoin [6] destacou enfaticamente isso, em relação ao dinheiro eletrônico peer-to-peer, "os principais benefícios são perdidos se um terceiro de confiança ainda for necessário para evitar o gasto duplo", e assim também são os principais benefícios dos ativos descentralizados perdidos, caso eles precisem passar por trocas confiáveis, fechadas e centralizadas.Negociar tokens descentralizados em câmbios centralizados não faz sentido do ponto de vista filosófico, uma vez que essa negociação não consegue sustentar as virtudes adotadas por esses projetos descentralizados. Existem também inúmeros riscos práticos e limitações no uso de câmbios centralizados, descritos abaixo. Os câmbios descentralizados (DEXs) [7] [8] [9] procuraram abordar tais questões e, em muitos casos, conseguiram aliviar os riscos de segurança utilizando os blockchains para a desintermediação. No entanto, na medida em que a capacidade do DEX torna-se uma infraestrutura fundamental para a nova economia, há espaço substancial para a melhoria do desempenho. O Loopring tem como objetivo fornecer ferramentas modulares para essa infraestrutura com seu protocolo aberto independente do dApp.

2 Panorama de Câmbio Vigente

2.1 Inadequações dos Câmbios Centralizados

Os três principais riscos das câmbios centralizados são; 1) Falta de segurança, 2) Falta de transparência e 3) Falta de liquidez.

A falta de segurança: é proveniente do fato de que usuários geralmente entregam o controle de suas chaves privadas (fundos) a uma entidade centralizada. Isso expõe os usuários à possibilidade de que os câmbios centralizados sejam vítimas de invasores (hackers) mal-intencionados. Os riscos de segurança e invasão que defrontam todos os câmbios centralizados são bem conhecidos [10] [11], mas muitas vezes são aceitos como "Estacas da Tabela" para negociação de token. Os câmbios centralizados continuam a ser alvos fáceis para os ataque de hackers, uma vez que seus servidores custodiam milhões de dólares em fundos de usuários. Os desenvolvedores do câmbio também podem cometer erros acidentais, mas sem más intenções, com os fundos do usuário. De maneira simples, os usuários não estão no controle de seus próprios tokens quando depositados em um câmbio centralizado. .

A falta de transparência: expõe os usuários ao risco de câmbios desleais que atuam de forma injusta. A distinção aqui é pelas más intenções do operador de câmbio, já que os usuários não estão realmente negociando seus próprios ativos em câmbios centralizados, mas sim um IOU. Quando os tokens são enviados para a carteira do câmbio, esse câmbio fica sob custódia e oferece um IOU em seu lugar. Todos os negócios são, de forma efetiva, entre os IOUs dos usuários. Para retirar, os usuários resgatam seus IOUs com o câmbio e recebem seus tokens em seu endereço da carteira externa. Ao longo desse processo, existe uma falta de transparência, e o câmbio pode ser interrompido, congelar sua conta, ir à falência, etc. Também é possível que eles usem ativos de usuário para outros fins enquanto estão sob custódia, como emprestá-los a terceiros. A falta de transparência não quer dizer que os usuários perderá todos os seus fundos, mas pode acarretar em altas taxas de negociação, atrasos quando houver alta demanda, riscos com regulamentações e pedidos em execução.

Falta de Liquidez: Do ponto de vista dos operadores de câmbio, a liquidez fragmentada inibe a entrada de novas trocas por causa de dois cenários de "o vencedor-leva-tudo". Primeiro, o câmbio com o maior número de pares negociáveis ganha, tendo em vista que os usuários acham isso necessário para conduzir todos os seus negócios em um intercâmbio. Em segundo lugar, o intercâmbio com o maior registro de pedidos vence, devido a spreads de oferta-procura favoráveis para cada par de negociação. Isso desencoraja a concorrência dos iniciantes, uma vez que é difícil para eles acumularem liquidez inicial. Como resultado, muitas trocas geram uma alta participação de mercado, apesar das reclamações dos usuários e até mesmo das grandes incidências de hackers.

Vale a pena notar que, à medida que as centrais ganham quota de mercado, elas se tornam um alvo cada vez maior dos invasores

Do ponto de vista dos usuários, a liquidez fragmentada reduz significativamente a experiência do usuário. Em um câmbio centralizado, os usuários só podem negociar dentro dos próprios conjuntos de liquidez do câmbio, mediante seu próprio registro de pedidos e entre seus pares de token suportados. Para trocar o token `A` pelo token `B`, os usuários devem ir para um câmbio que ofereça suporte para ambos os tokens, ou devem se registrar em diferentes trocas, divulgando informações pessoais. Os usuários geralmente precisam executar negociações preliminares ou intermediárias, normalmente mediante ao BTC ou a ETH, pagando spreads de oferta-procura no processo. Finalmente, os registros de pedidos podem não ser suficientemente profundos para concluir o negócio sem um deslize relevante. Mesmo que o câmbio pretenda processar grandes volumes, não há garantia de que esse volume e liquidez não sejam falsos.[12].

O resultado são silos de liquidez desconexos e um ecossistema fragmentado que se assemelha ao legado sistema financeiro, com volume de negociação significativo centralizado em poucas trocas. As promessas de liquidez global de blockchains não têm mérito dentro de câmbios centralizados.

2.2 Inadequações dos Antigos Câmbios Descentralizados

Os câmbios descentralizados diferem dos câmbios centralizados em parte porque os usuários mantêm o controle de suas chaves privadas (ativos) executando negociações diretamente no blockchain subjacente. Aproveitando a tecnologia confiável de criptomoedas, eles por si só mitigam com sucesso muitos dos riscos acima mencionados relacionados à segurança. No entanto, problemas em relação ao desempenho e limitações estruturais persistem.

A liquidez muitas vezes continua sendo um problema, visto que os usuários devem buscar contrapartes em diferentes conjuntos e padrões de liquidez. Os efeitos de liquidez fragmentada estão presentes se os DEXs ou os dApps de forma geral não empregarem padrões consistentes para interoperar, e se os pedidos não forem compartilhados/propagados em uma rede ampla. A liquidez dos registros de pedidos limitados e, especificamente, sua resiliência – a rapidez com que os pedidos limitados são regeneradas – podem afetar significativamente as devidas estratégias de negociação[13].A ausência de tais padrões resultou não apenas na redução da liquidez, mas também em exposição a uma série de contratos inteligentes de propriedade potencialmente incertos.

Além disso, como as negociações são realizadas na cadeia, os DEXs herdam limitações do blockchain subjacente, a saber: escalabilidade, atrasos na execução (mineração) e modificações de custos elevados para pedidos. Assim, os registros de pedidos de blockchain não são particularmente adequados, já que a execução de código no blockchain

incorre em um custo (gás), tornando as cadências de cancelamento de pedidos múltiplas inviavelmente caras.

Finalmente, considerando que os registros de pedidos de blockchain sejam públicos, a transação para fazer um pedido é visível pelos mineradores na medida em que aguarda ser extraída para o próximo bloco e colocada em um registro de pedidos. Esse atraso expõe o usuário ao risco de estar na frente e ter o preço ou a execução se movendo contra ele.

2.3 Soluções Híbridas

Pelas razões acima, câmbios totalmente baseados em blockchain têm limitações que os tornam pouco competitivos com câmbios centralizados. Há uma troca entre a confiabilidade inerente em cadeia e a velocidade do intercâmbio centralizado e a flexibilidade do pedido. Protocolos como Loopring e 0x [14] estendem uma solução de estabelecimento em cadeia (on-chain) com o gerenciamento de pedidos fora da cadeia (off-chain). Essas soluções giram em torno de contratos inteligentes abertos, mas navegam nas limitações de escalabilidade, executando várias funções off-chain e dando aos nós flexibilidade no cumprimento de funções críticas para a rede. No entanto, os contras permanecem também para o modelo híbrido [15]. O protocolo Loopring propõe diferenças significativas em nossa abordagem para uma solução híbrida ao longo deste artigo.

3 Protocolo de Loopring

O Loopring não é um DEX, mas um protocolo modular para construir DEXs em vários blockchains. Desmontamos as partes componentes de um câmbio tradicional e oferecemos um conjunto de contratos públicos inteligentes e agentes descentralizados em seu lugar. As funções na rede incluem carteiras, relés, blockchains de consórcio de compartilhamento de liquidez, navegadores de pedidos de compras, Ring-Miners e serviços de tokenização de ativos. Antes de definir cada um, devemos primeiro entender os pedidos de Loopring.

3.1 Anel de Pedido (Order ring)

Os pedidos de loopring são expressos no que chamamos de Modelo de Pedido Unidirecional (UDOM) [16]. A UDOM expressa pedidos como solicitações de troca de tokens, `montanteS`/`montanteB`, (valor para vender/comprar) em vez de licitações e pedidos. Como cada pedido é apenas uma taxa cambial entre dois tokens, um recurso poderoso do protocolo é a mistura e correspondência de vários pedidos no comércio circular. Utilizando até 16 pedidos em vez de um único par de negociação, há um aumento significativo na liquidez e potencial para melhoria de preço.

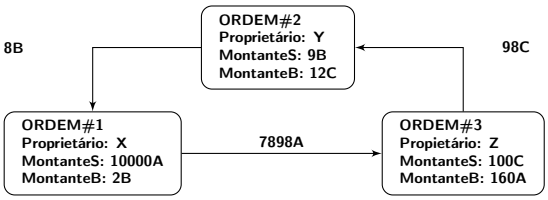

Figura 1: Um anel de pedidos de 3 Pedidos

A figura acima mostra um anel de pedidos de 3 pedidos. O token de cada pedido para vender (`tokenS`) é o token de outro pedido para comprar (`tokenB`).Ele cria um loop que permite que cada pedido troque seus tokens desejados sem exigir um pedido oposto para seu par. As negociações tradicionais de pares de pedidos podem, é claro, ainda ser executadas, no que é essencialmente um caso especial de um anel de pedidos.

Definition 3.1 (anel de pedido) *permitir* C_0, C_1, $\cdots$, C_{n-1} *ser* n *diferentes pedidos,* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ *ser* n *Esses pedidos podem formar um anel de pedidos para negociação:*

$$O_{0\to1} \to \cdots \to O_{i\to i\oplus1} \to \cdots \to O_{n-1\to0},$$

onde n *é o comprimento do anel de pedidos, e* $i \oplus 1 \equiv i + 1 \mod n$.

Um anel de pedidos é válido assim que todas as transações de componentes puderem ser executadas em uma taxa cambial igual ou melhor que a taxa original especificada implicitamente pelo usuário. Para verificar a validade do anel de pedidos, os contratos inteligentes do protocolo de Loopring devem receber anéis de pedido dos mineradores de anel, onde o produto das taxas de câmbio originais de todas os pedidos é igual ou maior que 1.

Vamos supor que Alice e Bob querem trocar suas fichas `A` e `B`. Alice tem 15 fichas `A` e ela quer 4 fichas `B` para eles; Bob tem 10 token `B` e ele quer 30 token `A` para eles.

Quem está comprando e quem está vendendo? Isso depende apenas do ativo que fixamos para dar cotações de preço. Se o token `A` é a referência, então Alice está comprando o token `B` pelo preço de $\frac{15}{4} = 3.75$ `A`, enquanto Bob está vendendo 10 tokens `B` pelo preço de $\frac{30}{10} = 3.00$ `A`. No caso de fixar o token `B` como referência, dizemos que Alice está vendendo 15 token `A` pelo preço de $\frac{4}{15} = 0.26666667$ `B` e Bob está comprando 10 token `A` pelo preço de $\frac{10}{30} = 0.33333334$ `B`. Portanto, quem é o comprador ou vendedor é arbitrário.

Na primeira situação, Alice está disposta a pagar um preço mais alto (3.75`A`) do que o preço que Bob está vendendo seus tokens por (3.00`A`), enquanto na segunda situação Bob está disposto a pagar um preço mais alto (0.33333334`B`) do que o preço que Alice está vendendo seus tokens por (0.26666667`B`). Fica evidente que uma negociação é possível sempre que o comprador esteja disposto a pagar um preço igual ou superior ao preço do vendedor.

$$\frac{\frac{15}{4}}{\frac{30}{10}} = \frac{\frac{10}{30}}{\frac{4}{15}} = \frac{15}{4} \cdot \frac{10}{30} = 1.25 > 1 \quad (1)$$

Assim, para que um conjunto de pedidos n possa ser concluído, total ou parcialmente, precisamos saber se o produto de cada uma das taxas de câmbio como pedidos de compra resulta em um número maior ou igual a 1. Se assim for, todas os pedidos n podem ser parcial ou totalmente concluídos [17].

Se introduzirmos uma terceira contraparte, Charlie, de modo que Alice queira dar Token x_1 `A` e receber o y_1 `B`, Bob quer dar Token x_2 `B` e receber y_2 `C`, e Charlie quer dar o Token x_3 `C` e receber y_3 `A`. Os tokens necessários estão presentes e o comércio é possível se:

$$\frac{x_1 \cdot x_2 \cdot x_3}{y_1 \cdot y_2 \cdot y_3} \geq 1 \quad (2)$$

Veja a seção 7.1 para mais detalhes sobre os pedidos de Loopring.

4 Participantes do Ecossistema

Os seguintes participantes do ecossistema fornecem conjuntamente todas as funcionalidades que um câmbio centralizado tem a oferecer.

- **Carteiras**: Um serviço de carteira comum ou interface que dá aos usuários acesso aos seus tokens e uma forma de enviar pedidos para a rede Loopring. As carteiras serão incentivadas a produzir pedidos compartilhando as taxas com os mineradores (veja seção 8). Com a crença de que o futuro da negociação ocorrerá dentro da segurança das carteiras de usuários individuais, a conexão desses conjuntos de liquidez através de nosso protocolo é fundamental.

- **Blockchain/Relay-Mesh da Partilha de Liquidez do Consórcio**: Uma rede mesh de relé (relay-mesh) para compartilhamento de pedidos e liquidez. Quando os nós executam o software de retransmissão do Loopring, eles podem ingressar em uma rede existente e compartilhar a liquidez com outros relés em um blockchain de consórcio. O blockchain de consórcio que estamos construindo como uma primeira implementação tem um compartilhamento de pedidos quase em tempo real (blocos de 1-2 segundos), e reduz o histórico antigo para permitir um download mais rápido por novos nós. Notavelmente, os relés não precisam ingressar nesse consórcio; eles podem agir sozinhos e não compartilhar a liquidez com outros, ou podem iniciar e administrar sua própria rede de compartilhamento de liquidez.

- **Relays/Ring-Miners - Mineradores de Anel**: Os relés são nós que recebem pedidos de carteiras ou da malha de relés 0, mantêm registros de pedidos públicos e histórico de transações e, opcionalmente, transmitem pedidos para outros relés (por meio de qualquer meio arbitrário fora de cadeia) e/ou nós de malha de retransmissão.Ringmining (mineração de anel) é um recurso – não um requisito – de relés.Ele é computacionalmente pesado e feito totalmente fora da cadeia. Chamamos relés com o recurso de mineração de anel ativado "Mineradores de Anéis (Ring-Miners)", que produzem anéis de pedidos juntando diferentes pedidos.Os relés são gratuitos em (1) como eles escolhem se comunicar uns com os outros, (2) como eles constroem suas registros de pedido e (3) como eles minam anéis de pedidos (algoritmos de mineração).

- **Contratos Inteligentes do Protocolo Loopring (LPSC):** Um conjunto de contratos inteligentes públicos e gratuitos que verificam os anéis de pedidos recebidos dos mineradores de anéis, depositam e transferem tokens sem garantia em nome dos usuários, incentivam mineradores de anéis e carteiras com taxas e emitem eventos. Os relés/navegadores de pedidos ouvem esses eventos para manterem seus registros de pedidos e seu histórico de transações atualizados. Veja o apêndices. A para mais detalhes.

- **Serviços de Tokenização de Ativos (ATS)**: Uma ponte entre ativos que não podem ser negociados diretamente no Loopring. Eles são serviços centralizados administrados por empresas ou organizações confiáveis. Os usuários depositam ativos (reais, fiat ou tokens de outras cadeias) e recebem tokens emitidos, que podem ser resgatados para o depósito no futuro. Loopring não é um protocolo de câmbio de cadeia cruzada (até que exista uma solução adequada), mas o ATS permite o câmbio de tokens ERC20 [18] por ativos físicos, bem como ativos em outros blockchains.

5 Processo de Intercâmbio

1. **Autorização do Protocolo**: Na figura 2, o usuário `Y` que deseja trocar tokens, autoriza o LPSC a manipular o `montanteS` de token `B` que o usuário deseja vender. Isso não bloqueia os tokens do usuário, que permanecem livres para movê-los enquanto o pedido é processado.

2. **Criação de Pedidos**: A taxa atual e o registro de pedidos do token `B` vs o token `C`, são fornecidos por relés ou outros agentes conectados à rede, como os navegadores de pedidos. O usuário `Y` coloca um pedido (pedido de limite) especificando `montanteS` e `montanteB` e outros parâmetros por meio de qualquer interface de carteira integrada. Um montante de LRx pode ser adicionado ao pedido como uma taxa para os mineradores; uma taxa mais alta de LRx significa uma chance melhor de ser processada mais cedo pelos

anulares. O hash do pedido é assinado com a chave privada do usuário `Y`.

3. **Pedido Emitido**: A carteira envia o pedido e sua assinatura para um ou mais relés. Os relés atualizam seu registro de pedidos público. O protocolo não exige que os registros de pedidos sejam construídos de uma determinada maneira, como o primeiro a chegar, primeiro a servir. Em vez disso, os relés têm o poder de tomar suas próprias decisões de projeto ao criar seus pedidos.

4. **Compartilhamento de Liquidez**: Retransmissores transmitem o pedido para outros relés através de qualquer meio de comunicação arbitrário. Mais uma vez, há flexibilidade sobre como/se os nós interagem. Para facilitar um certo nível de conectividade de rede, existe um relaymesh de compartilhamento de liquidez embutido usando um blockchain de consórcio. Conforme mencionado na seção anterior, essa malha de retransmissão é otimizada para velocidade e inclusividade.

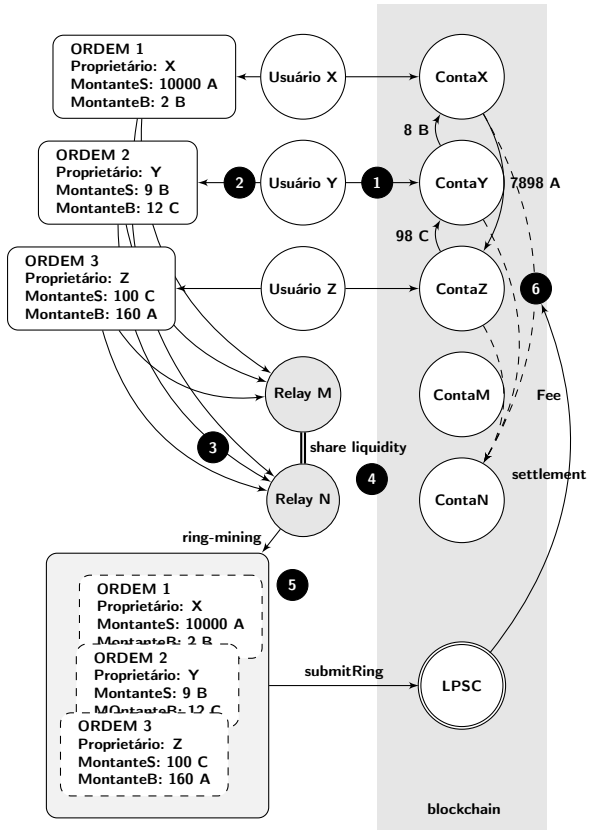

Figura 2: Processo de Câmbio do Loopring

5. **Ring-Mining (Mineração de Anel)**: Os Ring-miners (mineradores de anel) tentam concluir o pedido de forma parcial ou totalmente na taxa de câmbio determinada, ou melhor, combinando isso com vários outros pedidos. A mineração de anel é a principal razão pela qual o protocolo é capaz de fornecer alta liquidez sobre qualquer par. Se a taxa executada for melhor do que a especificada pelo usuário Y, a margem será compartilhada entre todos os pedidos no anel de pedidos. Como recompensa, a mineradora de anel (ring-miner) escolhe entre reivindicar parte da margem (Divisão de Margem, e devolver o LRx ao usuário), ou simplesmente manter a taxa LRx.

6. **Verificação e Liquidez**: O anel de pedidos é recebido pelo LPSC. Ele faz várias verificações para verificar os dados fornecidos pela mineradora de anel e determina se o anel de pedidos pode ser liquidado total ou parcialmente (dependendo da taxa de preenchimento de pedidos in-ring e tokens nas carteiras dos usuários). Se todas as verificações forem bem-sucedidas, o contrato transferirá a nível atômico os tokens aos usuários e pagará as taxas da carteira e da mineradora de anel ao mesmo tempo. Se o saldo do usuário `Y`, conforme determinado pelo LPSC, for insuficiente, ele será considerado reduzido: um pedido reduzido automaticamente aumentará para seu tamanho original se fundos suficientes forem depositados em seu endereço, ao contrário de um cancelamento, que é um maneira manual de operação e não pode ser revertido.

6 Flexibilidade Operacional

É importante observar que o padrão aberto de Loopring permite que os participantes tenham uma grande flexibilidade sobre como eles operam. Os agentes são livres para implementar novos modelos de negócios e fornecer valor para os usuários, obtendo taxas de LRx em volume ou outras métricas no processo (se assim o desejarem). O ecossistema é modular e destinado a apoiar a participação de uma infinidade de aplicações.

6.1 Livro de Pedidos

Os relés podem elaborar seus registros de pedidos de várias maneiras para exibir e corresponder aos pedidos dos usuários. Uma primeira implementação de nosso próprio registro de pedido segue um modelo OTC, no qual os pedidos limitados são posicionados com base apenas no preço. Os registros de data e hora das encomendas, em outras palavras, não têm relação com o registro de pedidos.

No entanto, uma retransmissão é livre para elaborar seu registro de pedidos de modo a emular um mecanismo de comparação de câmbio centralizado típico, em que os pedidos são classificados por preço, respeitando também os timestamps. Se um revendedor estiver inclinado a oferecer esse tipo de carteira de encomendas, ele pode ser proprietário/integrado com uma carteira e receber esses pedidos de carteira enviados exclusivamente ao único revendedor, que poderá então corresponder aos pedidos com base no tempo. Qualquer configuração desse tipo é possível.

Enquanto outros protocolos DEX às vezes exigem que os Relays tenham recursos - saldos de token inicial para fazer pedidos de compradores - os Relés de Loopring só precisam encontrar pedidos que possam ser convertidos para consumar um negócio, e podem fazê-lo sem os tokens iniciais.

6.2 Compartilhamento de Liquidez

Os relés têm a liberdade de projetar a maneira como eles compartilham a liquidez (pedidos) uns com os outros. Nosso blockchain de consórcio consiste apenas em uma solução para realizar isso, e o ecossistema é livre para conectar e se comunicar como quiser. Além de se juntar a um blockchain de consórcio, eles podem construir e gerenciar os seus próprios, criando regras/incentivos na medida em que eles vêem isso. Os relés também podem funcionar sozinhos, como visto na implementação de carteira sensível ao tempo. Naturalmente, há claras vantagens na comunicação com outros Relays na busca de efeitos de rede, no entanto, diferentes modelos de negócios podem merecer desenhos de compartilhamento peculiares e taxas divididas de diversas maneiras.

7 Especificação de Protocolo

7.1 Anatomia de um Pedido

Um pedido é um pacote de dados que descreve a intenção da troca do usuário. Um pedido de Looping é definido por meio do Modelo de Pedido Unidirecional ou UDOM, da seguinte maneira:

```
Pedido de mensagem {
  protocolo de endereço;
  proprietário de endereço;
  tokenS de endereço;
  endereço tokenB;
  montanteS de unidade256;
  montanteB de unidade256;
  unidade256 lrcFee
  unidade256 validSince; // Segundos anterior
  unidade256 validUntil; // Segundos anterior
  unidade8 marginSplitPercentage; // [1-100]
  bool buyNoMoreThanAmountB;
  Unit 256 walletId;
  // Endereço de autoria dupla
  endereço authAddr;
  // v, r, s são partes da assinatura
  unidade8 v;
  bytes32 r;
  bytes32
  // Chave privada de autoria dupla,
  // não usado para calcular o hash do pedido
  // assim, isso NÃO é assinado.
  string authKey;
  uint256 nonce;
}
```

Para garantir a origem do pedido, ele é assinado com o hash de seus parâmetros, excluindo `authAddr`,com a chave privada do usuário. O parâmetro `authAddr` é usado para assinar os anéis de pedidos dos quais esse pedido faz parte, o que impede o funcionamento antecipado. Por favor, consulte a seção 9.1 para mais detalhes..

A assinatura é representada pelos campos `v`, e `r`, e `s` é enviada juntamente com os parâmetros do pedido pela rede. Isso garante que o pedido permaneça imutável durante toda a sua vida útil. Mesmo que o pedido nunca mude, o protocolo ainda pode calcular seu estado atual com base no saldo de seu endereço junto com outras variáveis.

O UDOM não inclui um preço (que deve ser um número de ponto de marcação por natureza), mas, em vez disso, usa o termo `rate` ou r, que é expresso como `montanteS`/`montanteB`. A taxa não é um número de ponto flutuante, mas uma expressão que será avaliada somente com outros números inteiros não assinados sob demanda, para manter todos os resultados intermediários como números inteiros sem sinal e aumentar precisão do cálculo.

7.1.1 Comprar Montantes

Quando uma mineradora de anel faz correspondência com pedidos, é possível que uma melhor taxa seja executável, permitindo aos usuários obterem mais 5 `tokenB` do que o `montanteB` No entanto, se o `buyNoMoreThanAmountB` estiver definido como `True`, o protocolo garante que os usuários recebam não mais que `montanteB` de `tokenB`. Assim o parâmetro `buyNoMoreThantokenB` do UDOM determina quando um pedido é considerado integralmente preenchido. `buyNoMoreThantokenB` aplica um limite a `montanteS` ou `montanteB`, e permite que os usuários expressem intenções comerciais mais granulares do que os pedidos de compra/venda tradicionais.

Por exemplo: com `montanteS` = 10 e `montanteB` = 2, a taxar $r = 10/2 = 5$. Assim, o usuário está disposto a vender 5 `tokenS` para cada `tokenB`. A mineradora de anel corresponde e encontra no usuário uma taxa, permitindo que o usuário receba 2,5 `tokenB` em vez de 2. No entanto, se o usuário desejar apenas 2 `tokenB` e definir o marcador `buyNoMoreThanAmountB` como `True`, o LPSC executará a transação a uma taxa de 4 e o usuário venderá 4 `tokenS` para `tokenB`, economizando, de forma efetiva, 2 `tokenS`. Lembre-se de que isso não leva em conta as taxas de mineração (Consulte a seção 8.1).

De fato, se usarmos

```
Ordem(montanteS,tokenS,
      montanteB,tokenB,
      buyNoMoreThantokenB)
```

para representar um pedido de forma simplificada, para os mercados ETH/USD em um intercâmbio tradicional, a modelagem tradicional de compra e venda poderá expressar o 1º e o 3º pedido abaixo, mas os outros dois:

1. Vender 10 ETH pelo preço de 300 USD/ETH. pedido expresso como: `Pedido (10,ETH,3000,USD,Falso)`.

2. Vender ETH pelo preço de 300 USD/ETH para obter 3000 USD. Esse pedido pode ser expresso como: `Pedido (10,ETH,3000,USD,Verdadeiro)`.

3. Comprar 10 ETH pelo preço de 300 USD/ETH, Esse pedido pode ser expresso como `Pedido (3000,USD,10,ETH,Verdadeiro)`.

4. Gastar 3000 USD para comprar o maior número possível de ETH pelo preço de 300 USD/ETH, esse pedido pode ser expresso como: `Pedido(3000,USD,10,ETH,Falso)`.

7.2 Verificação de Anel

Os contratos inteligentes Loopring não realizam cálculos de taxa de câmbio ou de valor, mas devem receber e verificar o que os mineradores de anel fornecem para esses valores. Estes cálculos são feitos por mineradores por duas razões principais: (1)a linguagem de programação para contratos inteligentes, como SOLID [19] em Ethereum, não tem suporte para matemática de ponto flutuante, principalmente $pow(x, 1/n)$ (calculando a n-ésima raiz de um número de ponto flutuante), e (2) é desejável que o cálculo seja efetuado em cadeia para reduzir o cálculo e o custo no blockchain.

7.2.1 Verificação de Sub-Ring

Essa etapa impede que os arbitragistas realizem de forma desonesta toda a margem em um pedido, implementando novos pedidos dentro dela. Essencialmente, uma vez que um anel de pedido válido é encontrado por uma mineradora de anel, pode ser tentador adicionar outros pedidos ao anel de pedidos para absorver totalmente a margem dos usuários (descontos de taxa). Como ilustrado na figura 3 abaixo, cuidadosamente calculados $x1$, $y1$, $x2$ and $y2$ farão com que o produto de todos pedidos seja exatamente 1, portanto não haverá desconto de taxa.

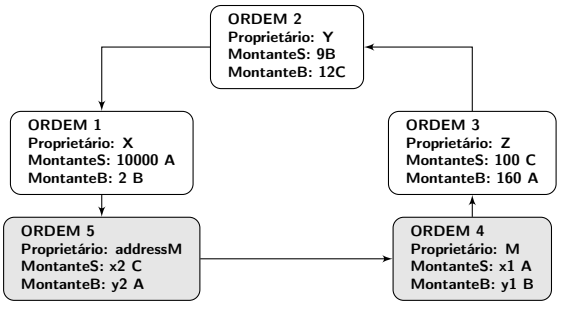

Figura 3: Figura 3: Um anel de pedidos com Sub-Rin

Isso é risco zero, adicionar valor zero à rede é considerado uma conduta injusta pelo minerador. Para evitar isso, o Loopring exige que um loop válido não contendo nenhum sub-token. Para verificar isso, o LPSC garante que um token não pode estar em uma posição de compra ou venda duas vezes. No diagrama acima, podemos ver que o token `A` é um token de venda duas vezes e um token de compra duas vezes, o que não seria permitido.

7.2.2 Verificando a Taxa de Preenchimento

Os cálculos da taxa de intercâmbio no anel de pedidos são feitos por operadores de mineração por razões declaradas acima. É o LPSC que deve verificar se está correto. Primeiro, ele verifica se a taxa de compra que o minerador de anel pode executar para cada pedido é igual ou menor que a taxa de compra original definida pelo usuário. Isso garante que o usuário receba pelo menos a taxa de câmbio solicitada ou melhor na transação. Uma vez que as taxas de câmbio são confirmadas, o LPSC garante que cada pedido no anel de pedidos compartilhe o mesmo desconto de taxa. Por exemplo, se a taxa de desconto for γ, então o preço para cada pedido será:

$r_{0\to1} \cdot (1-\gamma)$, $r_{1\to2} \cdot (1-\gamma)$, $r_{2\to0} \cdot (1-\gamma)$, e satisfazer:

$$r_{0\to1} \cdot (1-\gamma) \cdot r_{1\to2} \cdot (1-\gamma) \cdot r_{2\to0} \cdot (1-\gamma) = 1 \qquad (3)$$

Consequentemente:

$$\gamma = 1 - \frac{1}{\sqrt[3]{r_{0\to1} \cdot r_{1\to2} \cdot r_{2\to0}}}. \qquad (4)$$

Se a transação cruzar n pedidos, o `desconto` é:

$$\gamma = 1 - \frac{1}{\sqrt[n]{\prod_{i=0}^{n-1} r^i}}, \qquad (5)$$

onde r^i é a taxa de rotatividade do pedido do i-ésimo. Obviamente, somente quando a taxa de desconto é $\gamma \geq 0$, esses pedidos podem ser pagos i-ésimo- pedido: (O^i) e a taxa de câmbio real é $\hat{r^i} = r^i \cdot (1-\gamma)$, $\hat{r^i} \leq r^i$.

Lembra de nosso exemplo anterior onde aline tem 15 Tokens `A` e quer 4 tokens `B` para ela, Bob tem 10 tokens `B` e quer 30 token `A` para ele. se token `A` é a referência, então alice está comprando Token `B` por $\frac{15}{4} = 3.75$`A`, enquanto BOB está vendendo token `B` por $\frac{30}{10} = 3.00$,rb|A|. Para calcular o desconto: $\frac{150}{120} = 1.25$ portanto $\frac{1}{1.25} = 0.8 = (1 - -\gamma)^2$. Assim, a taxa de câmbio que torna o comércio equitativo para ambas as partes é de: $\sqrt{0.8} \cdot 3.75 \approx 3.3541$ token `A` por token `B`.

Bob transferi 4 token `B` e recebe 13.4164 token `A`, mais do que os 12 que ele estava esperando por aqueles 4 tokens. Alice recebe 4 token `B` como pretendido, mas dá apenas 13.4164 token `A` em troca, menos do que os 15 que ela estava disposta a dar para aqueles 4 tokens Note: Observe que uma parte dessa margem vai para o pagamento de taxas para incentivar os mineiros (e Carteiras). (Veja a seção 8.1).

7.2.3 Cancelamento & Monitoramento de Cumprimento

Um usuário pode cancelar um pedido de forma parcial ou integralmente enviando uma transação especial ao LPSC, contendo os detalhes sobre o pedido e os valores a serem cancelados. O LPSC leva isso em consideração, armazena os valores para cancelar, e emite um evento de `PedidoCancelado (OrderCancelled)` para a rede. O LPSC controla os valores preenchidos e cancelados armazenando seus valores usando o hash do pedido como um identificador. Esses dados são acessíveis publicamente e os eventos `PedidoCancelado (OrderCancelled)` / `PedidoConcluido (OrderFilled)` são emitidos quando são alterados. O rastreamento desses valores é fundamental para o LPSC durante a etapa de liquidez do anel de pedidos.

O LPSC também apoia o cancelamento de todos os pedidos para qualquer par de negociação com o evento `PedidoCancelado (OrderCancelled)` e o cancelamento de todos os pedidos para um endereço com o evento `TodosPedidosCancelados (AllOrdersCancelled)`.

7.2.4 Escala de Pedidos

Os pedidos são escalonadas de acordo com o histórico de valores preenchidos e cancelados e o saldo atual das contas dos remetentes. O processo define o pedido com o menor valor a ser preenchido de acordo com as características acima e a utiliza como referência para escalonar todas as transações no anel de pedidos.

Encontrar o pedido de menor valor pode ajudar a descobrir o volume de preenchimento para cada pedido. Por exemplo se o i-ésimo pedido for a mais baixo, então o número de tokens vendidos de cada pedido $\hat{s}$ e o número de tokens $\hat{b}$ adquiridas de cada pedido podem ser calculados como:

$$\begin{aligned}
&\hat{s}^i = \overline{s}_i,\ \hat{b}^i = \hat{s}^i / \hat{r}^i,\ ; \\
&\hat{s}^{i\oplus 1} = \hat{b}^i,\ \hat{b}^{i\oplus 1} = \hat{s}^{i\oplus 1} / \hat{r}^{i\oplus 1}; \\
&\hat{s}^{i\oplus 2} = \hat{b}^{i\oplus 1},\ \hat{b}^{i\oplus 2} = \hat{s}^{i\oplus 2} / \hat{r}^{i\oplus 2}; \\
&...
\end{aligned}$$

Onde $\overline{s}_i$ é o saldo restante depois que os pedidos são parcialmente concluídos.

Durante a implementação, podemos assumir com segurança qualquer pedido no anel de pedidos para ter o valor mais baixo e, em seguida, iterar por meio do anel de pedidos no máximo duas vezes para calcular o volume de preenchimento de cada pedido.

Exemplo: Se o menor valor a ser preenchido em comparação com o pedido original for de 5%, todas as transações no anel de pedidos serão reduzidas para 5%. Depois que as transações forem concluídas, o pedido considerado com a menor quantidade restante a ser preenchida, deve ser totalmente preenchido.

7.3 Liquidez do Anel

Se o anel de pedidos preencher todas as verificações anteriores, o anel de pedidos poderá ser fechado e as transações poderão ser feitas. Isto significa que todos os n pedidos formam um anel de pedido fechado, conectado como na figura 4:

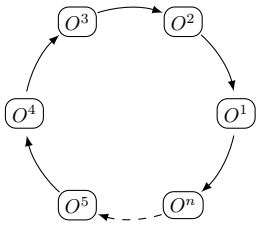

Figura 4: Liquidez do Anel

Para fazer as transações, o LPSC usa o contrato inteligente `TokenTransferDelegate`. A introdução de tal delegatário facilita a atualização do contrato inteligente de protocolo, pois todos os pedidos precisam apenas autorizar esse delegatário em vez de versões diferentes do protocolo.

Para cada pedido no anel de pedidos, um pagamento de `tokenS` é feito para o pedido seguinte ou anterior, dependendo da implementação. Então a taxa da mineradora de anel é paga dependendo do modelo de taxa escolhido pela mineradora de anel, Finalmente após todas transações serem feitas, um evento `RingMined` é emitido.

7.3.1 Eventos Emitidos

O protocolo emite eventos que permitem que os relés, os navegadores de pedidos e outros agentes recebam atualizações de pedidos com a maior eficiência possível. Os eventos emitidos são:

- **OrderCancelled**: PedidoCancelado: Um pedido específico foi cancelado.
- **OrdersCancelled**: PedidosCancelados: Todas os pedidos de um par de negociação de um endereço de propriedade foram cancelados.
- **AllOrdersCancelled**: TodosOsPedidosCancelados: Todos os pedidos de todos os pares de negociação de um endereço de propriedade foram cancelados.
- **RingMined**: Um pedido de anel foi liquidado com sucesso.

  Esse evento contém dados relacionados a cada transferência de anel interno do token.

8 Token LRx

LRx é nossa notação generalizada de token. LRC é o token de Loopring no Ethereum, LRQ no Qtum e LRN no NEO, etc. Outros tipos de LRx serão introduzidos no futuro, à medida em que o Loopring for implantado em outros blockchains públicos.

8.1 Modelo de Taxas

Quando um usuário elabora um pedido, ele especifica uma quantia de LRx a ser paga à mineradora de anel como uma taxa, em conjunto com uma porcentagem da margem (`marginSplitPercentage`) feita no pedido cujo a mineradora possa solicitar. Isso é chamado de divisão de margem. A decisão de qual escolher (taxa ou margem dividida) é deixada para a mineradora.

Uma representação da divisão de margem:

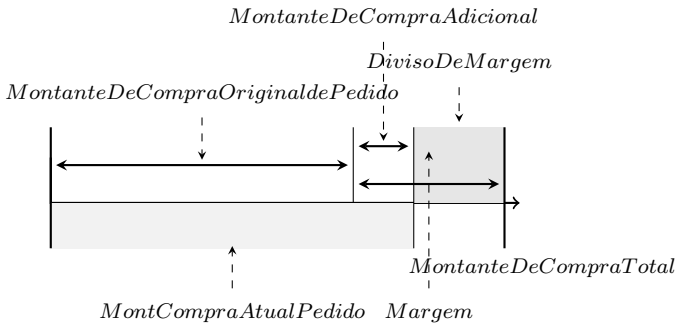

Figura 5: Uma Divisão de Margem de 60%

Se a margem no anel de pedidos for muito pequena, a mineradora escolherá a taxa LRx. Se, ao contrário, a margem for substancial o suficiente para a divisão de margem resultante de modo a valer muito mais do que a taxa de LRx, uma mineradora irá escolher a divisão de margem. Há outra condição, no entanto: quando a mineradora de anel escolhe a divisão de margem, ela deve pagar ao usuário (criador do pedido) uma taxa, que é igual ao LRx que o usuário teria pago à minerador como uma taxa. Isso aumenta o patamar de onde a mineradora escolherá a divisão da margem para o dobro da taxa LRx do pedido, aumentando a propensão da escolha da taxa LRx. Isso permite que as mineradoras recebam uma renda constante em anéis de pedidos de margem baixa para a comercialização de recebimento de menos receita em pedidos de maior margem. Nosso modelo de taxas baseia-se na expectativa de que, à medida em que o mercado cresce e amadurece, haverá menos pedidos de margem alta, necessitando, portanto, de incentivos para as taxas LRx

Concluímos com o seguinte gráfico:

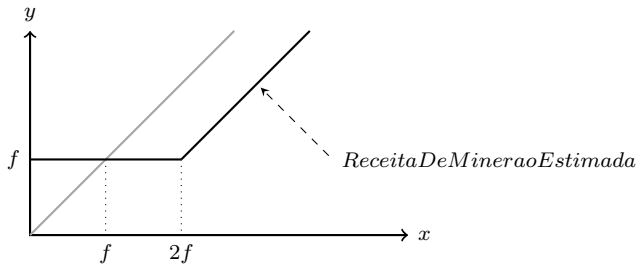

Figura 6: Modelo de Taxa de Loopring

Onde f é a taxa LRx, x é a divisão de margem, y é a receita de mineração. $y = max(f, x - f)$ como indicado pela linha contínua; se a taxa LRx para o pedido for 0, a equação será $y = max(0, x - 0)$ que simplifica para $y = x$ conforme indicado pela linha cinza.

As consequências são:

1. Se a divisão de margem for 0, os mineradores escolherão a taxa de LRx e ainda serão incentivados.

2. Se a taxa LRx for 0, a linha cinza será gerada e a receita será baseada em um modelo linear geral.

3. Quando a margem dividida é maior que 2x (taxa LRx), os mineradores escolhem a divisão de margem e pagam LRx para o usuário.

Deve-se notar que, se a taxa LRx for diferente de zero, independentemente da opção escolhida pela mineradora, sempre haverá uma transferência de LRx entre a mineradora e o emissor do pedido.

A mineradora obtém a taxa LRx ou paga a taxa LRx de volta ao emissor para obter a divisão da margem. As mineradoras de anel irão dividir uma certa porcentagem de taxas com carteiras. Quando um usuário faz um pedido por meio de uma carteira e este é concluído, a carteira é recompensada com uma parte das taxas ou divisão de margem. Embora isso seja modular, e modelos ou implementações de negócios exclusivos sejam possíveis, nossa tendência é que as carteiras recebam aproximadamente 20%-25% das taxas obtidas. As carteiras representam um alvo principal para a integração do protocolo Loopring, visto que elas têm a base de usuários, mas pouca ou nenhuma fonte de renda.

8.2 Governança Descentralizada

Desde o inicio, o protocolo Loopring é um protocolo social no sentido em que ele se baseia na coordenação entre os membros para operar efetivamente em direção a um objetivo. Isso não é diferente dos protocolos criptoeonômicos em geral e, de fato, sua utilidade é amplamente protegida pelos mesmos mecanismos de problemas de coordenação [20], equilíbrio implacável de gatilhos e racionalidade limitada. Para esse fim, os tokens LRx não são usados apenas para pagar taxas, mas também para alinhar os apoios financeiros dos vários participantes da rede. Esse alinhamento é necessário para a ampla adoção de qualquer protocolo, mas é particularmente intenso para os protocolos de troca, uma vez que o sucesso depende, em grande parte, da melhoria da liquidez em um ecossistema robusto e descentralizado.

Os tokens LRx serão usados para efetuar atualizações de protocolo por meio de governança descentralizada. As atualizações e contratos inteligentes e serão regidas pelos titulares dos tokens para garantir a continuidade e a segurança, sendo assim atenuando os riscos de liquidez desviada por meio de incompatibilidade. Como os contratos inteligentes não podem ser alterados depois de implantados, há um risco de que os dApps ou os usuários finais continuem interagindo com versões obsoletas e se excluam de contratos

atualizados. A atualização é fundamental para o sucesso do protocolo, uma vez que ela deve se adaptar às demandas do mercado e aos blockchains subjacentes. A governança descentralizada das partes interessadas do LRx permitirá atualizações de contratos inteligentes de protocolo sem interromper os dApps ou os usuários finais, ou confiar demais na abstração de contrato inteligente. Os tokens LRx têm um fornecimento fixo e, no caso do LRC, determinamos uma porcentagem que serão congeladas pela Fundação Loopring e alocados a fundos destinados à comunidade [21].

No entanto, os proprietários de tokens LRx não são os únicos interessados Em direcionar o andamento do protocolo, mas sim os relés / ringminers, carteiras, desenvolvedores e outros são parte integrante do ecossistema, e suas vozes devem ser ouvidas. Fica claro, que esses agentes não precisam ter nenhum Token LRx para executar seus respectivos papéis (desde os tradicionais criadores do protocolo, e até seus compradores e marketmakers não tem um poder total sobre as decisões e não é necesspario reservas obrigatória) devemos permitir métodos alternativos para que o interesse de todos sejam respeitados. Além disso, a votação "simples"baseada em tokens, tanto on-chain e off, é uma dose imperfeita para desacordo, com baixa taxa de participação dos eleitores com concentração de posse de tokens . Assim, o objetivo é implementar um modelo de governança que é construído em camadas, e baseado em conhecimento compartilhado com conjuntos de processos de tomada de decisão. Esta pode ser facilitada por instituições de coordenação que ofereçam sinais de um conjunto diversificado de participantes e, talvez, a partir de pontos pré-estabelecidos do protocolo. Como isso deve funcionar, a Fundação Loopring inevitavelmente crescerá em desenvolvedores e administradores de protocolo.

9 Proteções contra Fraudes e Ataques

9.1 Prevenção de front-running

Em câmbios descentralizados, front-running é quando alguém tenta copiar a solução de negociação de outro nó, conseguindo extrai-la antes da transação original que está no conjunto de transações pendente (mempool). Isso pode ser alcançado por meio de uma especificação de uma taxa de transação mais alta (preço do gás). O principal esquema de front-running em Loopring (e qualquer protocolo para correspondência de pedido) é o roubo de pedido: quando um front-runner rouba um ou mais pedidos de uma transação de liquidez de pedidos pendentes; e, específico para Loopring: quando um front-runner rouba todo o anel de pedidos de uma transação pendente.

Quando uma transação submitRing não é confirmada e ainda está no conjunto pendente de transações, qualquer um pode facilmente identificar essa transação e substituir `minerAddress` pelo seu próprio endereço (the `filcherAddress`), então eles podem renunciar a carga com `filcherAddress` e substituir a assinatura do pedido. O fincher pode definir um preço de gás mais alto e enviar uma nova transação esperando que os mineradores de bloco selecionem sua nova transação no próximo bloco, em vez da transação submitRing original.

As soluções anteriores para esse problema tinham reversos importantes: exigir mais transações e, assim, custando mais gás dos mineradores; e tendo pelo menos o dobro dos blocos para acertar um anel de pedido. Nossa nova solução, Autoria Dupla (Dual Authoring)[22], envolve o mecanismo de estabelecer dois níveis de autorização para pedidos - um para liquidez e outro para mineração de anel.

Processo de Autoria Dupla:

1. Para cada pedido, o software da carteira gera um par de chave pública/chave privada aleatório e coloca o par de chaves no snippet JSON do pedido. (Uma alternativa é utilizar o endereço derivado da chave pública em vez da chave pública por si só de forma a reduzir o tamanho dos bytes. Usamos `authAddr` para representar tal endereço, e `authKey` para representar a chave privada de correspondência de `authAddr`).

2. Calcule o hash do pedido com todos os domínios no pedido, exceto `r`, `v`, `s`, e `authKey`), e assine o hash utilizando a chave privada do `proprietário` (não `authKey`).

3. carteira enviará o pedido juntamente com o `authKey` os relés para mineração de anel. Os ring-miners verificarão se `authKey` e `authAddr` estão emparelhados corretamente e se a assinatura do pedido é válida com relação ao endereço do `proprietário`.

4. usando um anel de pedidos é identificado, a mineradora de anel usará o `authKey` cada pedido para assinar o hash do anel, `minerAddress`, e todos os parâmetros de mineração. Se um anel de pedidos contiver n pedidos, haverá n assinaturas feitas pelos n `authKeys`. WNós chamamos essas assinaturas de `authSignature`s. A mineradora também pode precisar assinar o hash do anel junto com todos os parâmetros de mineração usando a chave privada do `minerAddress`'s.

5. A mineradora chama a função submitRing com todos os parâmetros, assim como todas as `authSignature`s. adicionais `authKey`s NÃO fazem parte da transação em cadeia e, portanto, permanecem desconhecidos para outras partes que não sejam a própria mineradora

6. O Protocolo de Loopring irá agora verificar cada `authSignature` contra o `authAddr` ocorrespondente de cada pedido, e rejeitar o anel de pedido se qualquer `authSignature` estiver em falta ou inválida.

O resultado é que agora:

- Assinatura do pedido (pela chave privada do endereço do `proprietário` address) garante que o pedido não pode ser modificado, incluindo o `authAddr`.
- A assinatura da mineradora de anel (pela chave privada do `minerAddress`), se fornecida, garante que ninguém pode usar sua identidade para minerar um anel de pedidos.
- O `authSignature`arante que todo o anel de pedidos não pode ser modificado, incluindo `minerAddress`, e que nenhum pedido possa ser roubado.

Autoria Dupla previne o roubo do anel e roubo de pedido ao mesmo tempo. Ainda que garante que a liquidação de anéis de pedidos possa ser feita em uma única transação. Além disso, a Autoria Dupla abre as portas para que os relés possam compartilhar pedidos de duas maneiras: compartilhamento não tangível e compartilhamento maturável. Por padrão, o Loopring opera um modelo OTC e suporta apenas pedidos com preços limite, o que significa que os timestamps dos pedidos são ignorados. Isso sugere que o front-running de uma troca não tem impacto sobre o preço real dessa troca, mas afeta se ela é executada ou não.

10 Outros Ataques

10.1 Ataque Sybil ou DDOS

Os usuários mal-intencionados - agindo por conta própria ou por meio de falsas identidades - podem enviar uma grande quantidade de pedidos pequenos para atacar os nós do Loopring. No entanto, como permitimos que os nós rejeitem pedidos com base em seus próprios critérios - que podem ser ocultados ou revelados - a maioria desses pedidos será rejeitada por não gerar lucros satisfatórios quando combinados. Ao capacitar os revendedores para ditar como eles gerenciam os pedidos, não vemos um ataque massivo de pedido ínfimo como uma ameaça.

10.2 Equilíbrio Insuficiente

Os usuários mal-intencionados podem assinar e distribuir pedidos cujo valor do pedido é diferente de zero, mas cujo endereço de fato tem saldo zero. Os nós podem monitorar e perceber que o saldo real de alguns pedidos é zero, atualizar esses status de pedido de acordo e, então, descartá-los. Os nós devem gastar tempo para atualizar o status de um pedido, mas também podem optar por reduzir o esforço, por exemplo, por meio de endereços de listas negras e descartando pedidos relacionados.

11 Resumo

O protocolo Loopring se propõe a ser uma camada fundamental para o câmbio descentralizado. Ao fazê-lo, ele tem profundas repercussões em como as pessoas trocam ativos e valor. O dinheiro, como um bem intermediário, facilita ou substitui o intercâmbio de troca e resolve a dupla coincidência do problema de querer, [23], pelo qual duas contrapartes devem desejar o bem ou serviço distinto um do outro. Da mesma forma, o protocolo Loopring pretende dispensar nossas dependências da coincidência de desejos em pares de negociação, usando ring matching (correspondência de anel) para negociações facilmente consumadas. Isso é significativo sobre a forma que a sociedade e os mercados trocam tokens, ativos tradicionais e outros. De fato, assim como as criptomoedas descentralizadas representam uma ameaça ao controle de uma nação sobre o dinheiro, um protocolo combinatório que pode igualar os comerciantes (consumidores/produtores) em escala é uma ameaça teórica ao conceito de dinheiro em si.

Os benefícios do protocolo incluem:

- Gerenciamento de pedidos fora da cadeia e liquidação em cadeia significa que não há sacrifício no desempenho por segurança.
- Maior liquidez devido à mineração em anel e compartilhamento de pedidos.
- Autoria Dupla soluciona o problema pernicioso de front-running defrontado por todos os DEXs e seus usuários hoje.
- FContratos públicos inteligentes e gratuitos permitem que qualquer dApp construa ou interaja com o protocolo.
- A padronização entre operadores permite efeitos de rede e uma melhor experiência do usuário final.
- Rede mantida com flexibilidade na execução de pedidos e comunicação.
- Redução de barreiras à entrada significa menores custos para os nós que se conectam à rede e aos usuários finais.
- Negociação anônima diretamente das carteiras dos usuários.

12 Agradecimentos

Gostaríamos de expressar nossa gratidão aos nossos mentores, conselheiros e às muitas pessoas da comunidade que foram tão receptivas e generosas com seus conhecimentos. Em particular, gostaríamos de agradecer a Shuo Bai (da ChinaLedger); Professor Haibin Kan; Alex Cheng, Hongfei Da; Yin Cao; Xiaochuan Wu; Zhen Wang, Wei Yu, Nian Duan, Jun Xiao, Jiang Qian, Jiangxu Xiang, Yipeng Guo, Dahai Li, Kelvin Long, Huaxia Xia, Jun Ma e Encephalo Path por revisar e fornecer feedback sobre este projeto.

Referências

[1] Vitalik Buterin. Ethereum: a next generation smart contract and decentralized application platform (2013). *URL {http://ethereum. org/ethereum. html}*, 2017.

[2] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151, 2014.

[3] Patrick Dai, Neil Mahi, Jordan Earls, and Alex Norta. Smart-contract value-transfer protocols on a distributed mobile application platform. *URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf*, 2017.

[4] Viktor Atterlönn. A distributed ledger for gamification of pro-bono time, 2018.

[5] Hernando de Soto. *The Mystery Of Capital*. Basic Books, 2000.

[6] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[7] Fabian Schuh and Daniel Larimer. Bitshares 2.0: Financial smart contract platform, 2015.

[8] Bancor protocol. *URL https://bancor.network/*, 2017.

[9] Yaron Velner Loi Luu. Kybernetwork: A trustless decentralized exchange and payment service. `https://kr.kyber.network/assets/KyberNetworkWhitepaper.pdf`, Accessed: 2018-03-05.

[10] Fortune. How to steal $500 million in cryptocurrency. `http://fortune.com/2018/01/31/coincheck-hack-how`, Accessed: 2018-03-30.

[11] Robert McMillan. The inside story of mt. gox, bitcoin's 460 dollar million disaster. 2014.

[12] Sylvain Ribes. Chasing fake volume: a crypto-plague. `https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e`, Accessed: 2018-03-10.

[13] Rossella Agliardi and Ramazan Gençay. Hedging through a limit order book with varying liquidity. 2014.

[14] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain, 2017.

[15] Iddo Bentov and Lorenz Breidenbach. The cost of decentralization. `http://hackingdistributed.com/2017/08/13/cost-of-decent/`, Accessed: 2018-03-05.

[16] Daniel Wang. Coinport's implemenation of udom. `https://github.com/dong77/backcore/blob/master/coinex/coinex-backend/src/main/scala/com/coinport/coinex/markets/MarketManager.scala`, Accessed: 2018-03-05.

[17] Supersymmetry. Remarks on loopring. `https://docs.loopring.org/pdf/supersimmetry-loopring-remark.pdf`, Accessed: 2018-03-05.

[18] Fabian Vogelsteller. Erc: Token standard. *URL https://github.com /ethereum /EIPs /issues /20*, 2015.

[19] Chris Dannen. *Introducing Ethereum and Solidity*. Springer, 2017.

[20] Vitalik Buterin. Notes on blockchain governance. `https://vitalik.ca/general/2017/12/17/voting.html`, Accessed: 2018-03-05.

[21] Loopring Foundation. Lrc token documents. `https://docs.loopring.org/English/token/`, Accessed: 2018-03-05.

[22] Daniel Wang. Dual authoring — loopring's solution to front-running. *URL https://medium.com/loopring-protocol/dual-authoring-looprings-solution-to-front-running-d0fc9c348ef1*, 2018.

[23] Nick Szabo. Menger on money: right and wrong. `http://unenumerated.blogspot.ca/2006/06/menger-on-money-right-and-wrong.html`, Accessed: 2018-03-05.

Appendices

Apêndice A Loopring Implementado no Ethereum (EVM)

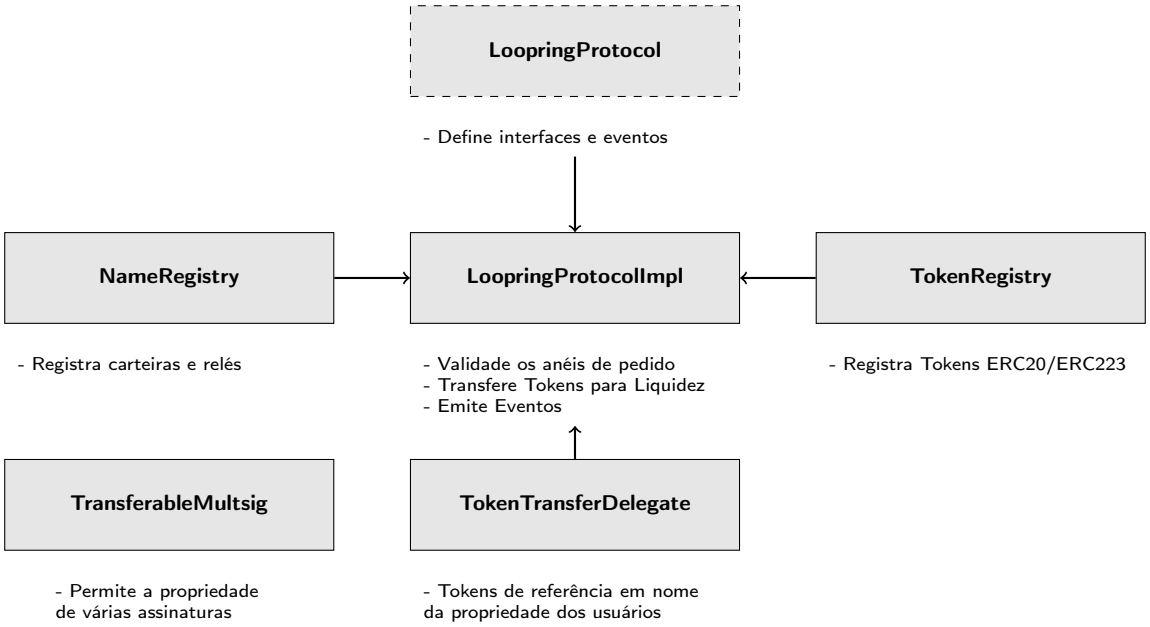

Figura 7: Contratos Inteligentes

Apêndice B Implementações

B.1 Ethereum

Os seguintes contratos inteligentes foram implantados na mainnet da Ethereum:

- LRC: `0xEF68e7C694F40c8202821eDF525dE3782458639f`
- TokenRegistry: `0xa21c1f2AE7f721aE77b1204A4f0811c642638da9`
- TokenTransferDelegate: `0x7b126ab811f278f288bf1d62d47334351dA20d1d`
- NameRegistry: `0xd181c1808e3f010F0F0aABc6Fe1bcE2025DB7Bb7`
- LoopringProtocolImpl: `0x0B48b747436f10c846696e889e66425e05CD740f`

B.2 Qtum

Os seguintes contratos inteligentes foram implantados na mainnet do Qtum:

- LRQ: `2eb2a66afd4e465fb06d8b71f30fb1b93e18788d`
- TokenRegistry: `c89ea34360258917daf3655f8bec5550923509b3`
- TokenTransferDelegate: `60b3fa7f461664e4dafb621a36ac2722cc680f10`
- NameRegistry: `e26a27d92181069b25bc7283e03722f6ce7678bb`
- LoopringProtocolImpl: `5180bb56b696d16635abd8dc235e0ee432abf25d`