Loopring:
Protocolo para Exchanges Descentralizadas

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

5 de Abril de 2018

Resumo

Loopring é um protocolo aberto para a construção de exchanges descentralizadas. Loopring opera como um conjunto público de contratos inteligentes responsáveis pela negociação (trader) e liquidação, com um grupo de agentes off-chain agregando e comunicando pedidos. O protocolo é gratuito, extensível e serve como um bloco de construção padronizado para aplicativos descentralizados (dApps) que incorporam a funcionalidade de exchange. Seus padrões interoperáveis facilitam a negociação anônimo e sem confiança. Uma melhoria importante em relação aos atuais protocolos de exchanges descentralizadas é a capacidade de os pedidos serem misturados e combinados com outros pedidos diferentes, eliminando as restrições dos pares de negociação de dois tokens e melhorando drasticamente a liquidez. A Loopring também emprega uma solução única e robusta para impedir o front-running: a tentativa injusta de enviar transações para um bloco mais rápido do que o provedor da solução original. Loopring é independente de blockchain e implementável em qualquer blockchain com funcionalidade de contrato inteligente. Nesse momento, é operável na Ethereum[1] [2] e Qtum [3] com NEO [4] em construção.

1 Introdução

Com a proliferação de ativos baseados em 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 motivado por negociações de tokens especulativos, ou convertendo para acessar redes através de seus tokens de utilidade nativos, a capacidade de trocar um cripto por outro é fundamental para o ecossistema maior. De fato, existe uma energia potencial em ativos [5], e a realização desse capital de desbloqueio de energia - requer não apenas a afirmação de propriedade, que as blockchains impediram imensamente, mas a capacidade de transferir e transformar livremente esses ativos.

Assim sendo, a negociação sem confiança de tokens (valor) é um caso de uso atraente para a tecnologia blockchain. Até agora, no entanto, os entusiastas cripto decidiram amplamente fazer negociação de seus tokens em exchanges centralizadas tradicionais. O protocolo Loopring é necessário porque, assim como o Bitcoin [6] respeitosamente enfatizou que, em relação ao dinheiro eletrônico peer-to-peer, "os principais benefícios são perdidos se um terceiro confiável ainda for necessário para evitar gastos duplicados", Da mesma forma, os principais benefícios dos ativos descentralizados são perdidos se eles precisarem passar por exchanges confiáveis, fechadas e centralizadas. Fazer negociação de tokens descentralizados em exchanges centralizadas não faz sentido do ponto de vista filosófico, já que falha em defender as virtudes que esses projetos descentralizados adotam. Há também inúmeros riscos e limitações práticas no uso de exchanges centralizadas, descritas abaixo. Exchanges Descentralizadas (Decentralized Exchanges - DEXs) [7] [8] [9] procuraram abordar essas questões e, em muitos casos, conseguiram aliviar os riscos de segurança usando blockchains para desintermediação. No entanto, como a capacidade do DEX torna-se uma infraestrutura crucial para a nova economia, há espaço substancial para a melhoria do desempenho. O Loopring visa fornecer ferramentas modulares para essa infraestrutura com seu protocolo aberto agnóstico do dApp.

2 Cenário atual das Exchange

2.1 Inadequações das Exchanges Centralizadas

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

Falta de Segurança surge de usuários que entregam o controle de suas chaves privadas (fundos) a uma entidade centralizada. Isso expõe os usuários à possibilidade de que as exchanges centralizadas sejam vítimas de hackers mal-intencionados. Os riscos de segurança e hackers que enfrentam todas as exchanges centralizadas são bem conhecidos [10] [11], ainda são muitas vezes aceitos como "table stakes (mesa de apostas)" para o negociador de tokens. As exchanges centralizadas continuam a ser chamariz para os hackers atacarem, pois seus servidores custodiam milhões de dólares em fundos de usuários. Os desenvolvedores das exchanges também podem cometer erros acidentais e sem más intenções com os fundos do usuário. Simplesmente, os usuários não estão no controle de seus próprios tokens quando depositados em uma exchange centralizada.

Falta de Transparência expõe os usuários ao risco de exchanges desonestas que agem de forma injusta. A distinção aqui é pelas intenções maliciosas da exchange, já que os usuários não estão realmente negociando seus próprios ativos em exchanges centralizadas, mas sim, uma nota promissória. Quando os tokens são enviados para a carteira da exchange, a exchange fica sob custódia e oferece uma nota promissória em seu lugar. Todos os negócios são efetivamente entre as notas promissórias dos usuários. Para retirar seus fundos, os usuários resgatam suas notas promissórias com a exchange e recebem seus tokens em seu endereço de carteira externa. Ao longo deste processo, há uma falta de transparência, e a exchange pode paralisar, congelar sua conta, ir à falência, etc. Também é possível que eles usem ativos dos usuários para outros fins enquanto estão sob custódia, como cedê-los a terceiros. A falta de transparência pode custar muito aos usuários mesmo sem uma perda total de fundos, como taxas de negociação mais altas, atrasos quando houver alta demanda, risco regulatório e pedidos em execução.

Falta de Liquidez. Do ponto de vista dos operadores da exchange, a liquidez fragmentada inibe a entrada de novas exchanges por causa de dois cenários, "o vencedor leva tudo". Primeiro, a exchange com o maior número de pares de negociação ganha, porque os usuários acham mais fácil fazer todas suas negociações em uma única exchange. Em segundo lugar, a exchange com o maior livro de ofertas (order book) vence, devido a spreads favoráveis de compra-venda para cada par de negociação. Isso desencoraja a concorrência dos recém-chegados, porque é difícil para eles acumular liquidez inicial. Como resultado, muitas exchanges geram uma alta participação de mercado, apesar das queixas dos usuários e até mesmo grandes incidentes de hackers. Vale a pena notar que, à medida que as exchanges centralizadas ganham market share, elas se tornam um alvo cada vez maior de hackers.

Do ponto de vista dos usuários, a liquidez fragmentada reduz significativamente a experiência do usuário. Em uma exchange centralizada, os usuários só podem negociar dentro das próprias pools de liquidez da exchange, contra seu próprio livro de ofertas e entre seus pares de token suportados. Para negociar o token `A` para o token `B`, os usuários devem ir a uma exchange que suporte os dois tokens ou registrar-se em diferentes exchanges, divulgando informações pessoais. Os usuários geralmente precisam executar negociações preliminares ou intermediárias, normalmente contra o BTC ou ETH, pagando spreads no processo de compra e venda. Finalmente, os livros de ofertas podem não ter liquidez o suficiente para concluir o negócio. Mesmo que a exchange 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 significativamente centralizado em poucas exchanges. As promessas de liquidez global das blockchains não têm mérito dentro de exchanges centralizadas.

2.2 Inadequações das Exchanges Descentralizadas

As exchanges descentralizadas diferem das exchanges centralizadas em parte porque os usuários mantêm o controle de suas chaves privadas (ativos) executando negociações diretamente no blockchain subjacente. Ao alavancar a tecnologia sem confiança das criptomoedas, elas mitigam com sucesso muitos dos riscos acima mencionados relacionados à segurança. No entanto, persistem problemas em relação ao desempenho e limitações estruturais.

A liquidez muitas vezes continua sendo um problema, pois os usuários devem buscar contrapartes em diferentes pools e padrões de liquidez. Os efeitos de liquidez fragmentada estão presentes se os DEXs ou os dApps em geral não empregarem padrões consistentes para interoperar e se os pedidos não forem compartilhados/propagados em uma rede ampla. A liquidez dos livros de ofertas e, especificamente, sua resiliência - a rapidez com que as ordens de limite são regeneradas - podem afetar significativamente as estratégias de negociação ideais [13]. A ausência de tais padrões resultou não apenas em liquidez reduzida, mas também exposição a uma série de contratos inteligentes proprietários potencialmente inseguros.

Além disso, como as negociações são realizados na blockchain, as DEXs herdam as limitações da blockchain subjacente, a saber: escalabilidade, atrasos na execução (mineração) e modificações dispendiosas nas ordens. Assim, os livros de ofertas blockchain não são particularmente adequados, já que a execução de código na blockchain incorre em um custo (gás), tornando a opção de cancelamento de

pedidos muito caras.

Finalmente, como os livros de ofertas blockchain são públicos, a transação para fazer um pedido é visível para os mineiradores enquanto aguarda a mineração para o próximo bloco e colocados em um livro de ofertas. Esse atraso expõe o usuário ao risco de ter o preço ou a execução se movendo contra ele.

2.3 Soluções Híbridas

Pelas razões acima, as exchanges puramente baseadas em blockchain têm limitações que as tornam pouco competitivas em exchanges centralizadas. Existe uma compensação entre a confiabilidade inerente on-chain e a velocidade de uma exchange centralizada e a flexibilidade do pedido. Protocolos, como Loopring e 0x [14] estendem uma solução de liquidação on-chain com o gerenciamento de pedidos off-chain. Essas soluções giram em torno de contratos inteligentes abertos, mas navegam pelas limitações de escalabilidade realizando diversas funções fora da cadeia e proporcionando aos nodes (nós) flexibilidade no cumprimento de funções críticas para a rede. No entanto, as desvantagens permanecem para o modelo híbrido [15]. O protocolo Loopring propõe diferenças significativas em nossa abordagem para uma solução híbrida ao longo deste artigo.

3 Protocolo Loopring

Loopring não é um DEX, mas um protocolo modular para construir DEXs em vários blockchains. Desmontamos em partes os componentes de uma exchange tradicional e oferecemos um conjunto de contratos públicos inteligentes e atores descentralizados em seu lugar. As funções na rede incluem carteiras, relays, 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 comandos Loopring.

3.1 Order Ring

Os comandos Loopring são expressos no que chamamos de ModelRing de Ordem Unidirecional (Unidirectional Order) (UDOM)[16]. UDOM requisita pedidos como solicitações na exchange de tokens, `amountS`/`amountB`, (quantidade de venda/compra) em vez de lances compra e venda. Como cada pedido é apenas uma troca entre dois tokens, um recurso poderoso do protocolo é a mistura e a correspondência de vários pedidos de negociação circular. Utilizando até 16 pedidos em vez de um único par de negociação, há um aumento dramático na liquidez e potencial para melhoria de preço.

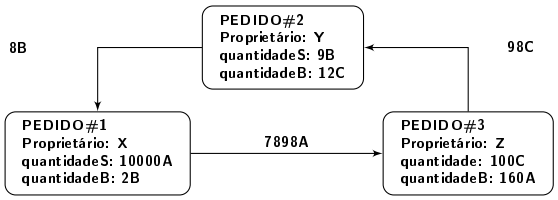

Figura 1: order-ring de 3 pedidos

A figura acima mostra um order-ring de 3 pedidos. O token de cada pedido para vender (`tokenS`) e o token de outro pedido para comprar (`tokenB`). Ele cria um loop que permite que cada pedido troque seus tokens desejados sem exigir uma ordem oposta 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 order-ring.

Definition 3.1 (order-ring) *Sendo* C_0, C_1, $\cdots$, C_{n-1} *com n diferentes tokens,* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ *com n pedidos. Esses pedidos podem formar um order-ring 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 order-ring, e $i \oplus 1 \equiv i + 1 \mod n$.

Um order-ring é válido quando todas as transações de componentes podem ser executadas em uma exchange igual ou melhor que a taxa original especificada implicitamente pelo usuário. Para verificar a validade do order-ring, os contratos inteligentes do protocolo Loopring devem receber order-rings dos ring-miners (mineradores), onde as taxas da exchange de todos os pedidos são igual ou maior que 1.

Vamos supor que Alice e Bob querem trocar seus tokens `A` e `B`. Alice tem 15 tokens `A` e ela quer 4 tokens `B` por eles; Bob tem 10 tokens `B` e ele quer 30 tokens `A` por eles.

Quem está comprando e quem está vendendo? Isso depende apenas do ativo que fixamos para dar cotações de preço. Se token `A` é a referência, então Alice está comprando token `B` para o preço de $\frac{15}{4} = 3.75$`A`, enquanto Bob esta vendendo 10 tokens `B` pelo preço de $\frac{30}{10} = 3.00$`A`. No caso de fixação de token `B` como referência, dizemos que Alice está vendendo 15 tokens `A` pelo preço de $\frac{4}{15} = 0.26666667$`B` e Bob está comprando 10 tokens `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, (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 (0.26666667`B`). É claro que uma negociação é possível sempre que o comprador esteja disposto a pagar um preço igual ou superior ao preço do vendedor.

$$\frac{\frac{15}{4}}{\frac{30}{10}} = \frac{\frac{10}{30}}{\frac{4}{15}} = \frac{15}{4} \cdot \frac{10}{30} = 1.25 > 1 \tag{1}$$

Assim, para que um conjunto de n pedidos possam ser preenchidos, total ou parcialmente, precisamos saber se o produto de cada uma das taxas da exchange como ordens de compra resulta em um número maior ou igual a 1. Se assim for, todao os n pedidos possam ser parcial ou totalmente preenchidos [17].

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

$$\frac{x1 \cdot x_2 \cdot x_3}{y_1 \cdot y_2 \cdot y_3} \geq 1 \tag{2}$$

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

4 Participantes do Ecossistema

Os seguintes participantes do ecossistema fornecem conjuntamente todas as funcionalidades que uma exchange centralizada tem a oferecer.

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

- **Consórcio de Liquidez compartilhado do Blockchain/Relay-Mesh**: Uma rede relay-mesh para compartilhamento de pedidos & liquidez. Quando os nodes executam o software de retransmissão do Loopring, eles podem ingressar em uma rede existente e compartilhar a liquidez com outros relays em uma blockchain do consórcio. O blockchain do 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 nodes. Notavelmente, os relays 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**: Os relays são nodes que recebem pedidos de carteiras ou da relay-mesh, mantêm registros de pedidos públicos e histórico de transações e, opcionalmente, transmitem pedidos para outros relays (por meio de qualquer meio arbitrário off-chain) e/ou nodes relay-mesh. A Ring-mining é um recurso - não um requisito - de relays. É computacionalmente pesado e é feito completamente off-chain. Nós chamamos relays com o recurso de ring-mining ativado "Ring-Miners", que produzem order-rings juntando pedidos diferentes. Os Relays são livres em (1) como eles escolhem se comunicar uns com os outros, (2) como eles constroem suas carteiras de pedidos, e (3) como os order-rings minam os pedidos (algoritmos de mineração).

- **Contratos Inteligêntes do Protocolo Loopring (LPSC)**: Um conjunto de contratos inteligentes públicos e livres que verificam os order-rings recebidos dos ring-miners, depositam e transferem tokens sem confiança em nome dos usuários, incentivam os ring-miners e carteiras com taxas e emitem eventos. Os Relays/navegadores de pedidos recebem esses pedidos para manter seus livros de pedidos e seu histórico de transações atualizados. Veja o apendice 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 blockchain) e recebem tokens emitidos, que podem ser resgatados para o depósito no futuro. Loopring não é um protocolo de exchange cross-chain (até que exista uma solução adequada), mas o ATS permite negociação de tokens ERC20 [18] com ativos físicos, bem como ativos em outras blockchains.

5 Processo de Exchange

1. **Autorização do Protocolo**: Na figura 2, o usuário `Y` que deseja trocar seus tokens, autoriza o LPSC a lidar com a quantidade - `quantidadeS` de token `B` que o usuário quer 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 livro de oferta para token `B` vs token `C`, são fornecidos por relays ou outros agentes conectados à rede, como navegadores de pedidos. O Usuário `Y` coloca um pedido (ordem limite) especificando `quantidadeS` e `quantidadeB` e outros parâmetros através de qualquer interface de carteira integrada. Uma quantidade de LRx pode ser adicionada ao pedido como uma taxa para os ring-miners; Uma taxa mais alta de LRx significa uma chance maior de ser processada mais rápido pelos ring-miners. O hash do pedido é assinado com a chave privada do usuário `Y`.

3. **Transmissão do Pedido**: A carteira envia o pedido e sua assinatura para um ou mais relays. Os relays atualizam seu livro de ofertas público. O protocolo não exige que os livros de ofertas sejam criados de uma determinada maneira, como o primeiro a chegar, primeiro a ser executado. Em vez disso, os relays têm o poder de tomar suas próprias decisões em criar seus livros de ofertas.

4. **Compartilhamento de Liquidez**: Relays transmitem a pedido para outros relays através de qualquer meio de comunicação arbitrário. Mais uma vez, há flexibilidade como/se os nodes interagem. Para facilitar um certo nível de conectividade de rede, existe um relay- mesh de compartilhamento de liquidez embutida usando um blockchain de consórcio. Conforme mencionado na seção anterior, esse relay-mesh é otimizado para velocidade e inclusividade.

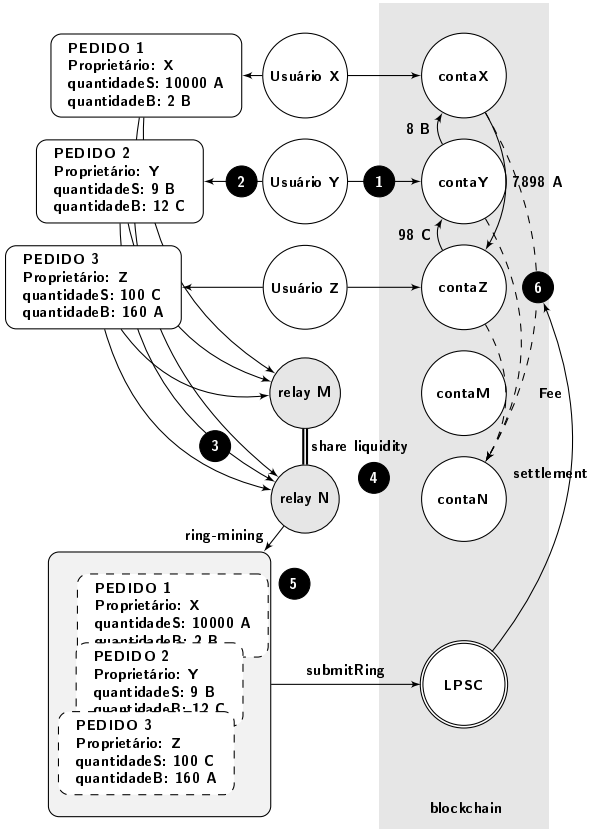

Figura 2: Loopring Exchange Process

5. **Ring-Mining (Order Matching)**: Os ring-miners tentam preencher o pedido total ou parcialmente à taxa da exchange, ou melhor, tenta combiná-lo com vários outros pedidos. O ring-miners 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 diferença será compartilhada entre todos os pedidos no ring-miners. Como recompensa, os ring-miners escolhem entre reivindicar parte da diferença (MarginSplit, e devolver o LRx ao usuário), ou simplesmente manter a taxa de LRx.

6. **Verificação & Liquidação**: O order-ring é recebido pelo LPSC. Ele faz várias verificações para verificar os dados fornecidos pelo order-ring e determina se ele 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 automicamente os tokens aos usuários e pagará as taxas de minerador e de wallet ao mesmo tempo. Se o saldo do usuário `Y`, conforme determinado pelo LPSC, for insuficiente, ele será considerado reduzido: uma ordem reduzida automaticamente aumentará até seu tamanho original, se fundos suficientes forem depositados em seu endereço, ao contrário de um cancelamento, que é uma maneira manual de operação e não pode ser revertida.

6 Flexibilidade Operacional

É importante notar que o padrão aberto pela Loopring permite aos participantes uma flexibilidade significativa na forma como eles operam. Os atores são livres para implementar novos modelos de negócios e fornecer valor para os usuários, ganhando 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 aplicativos.

6.1 Livro de Ofertas (Order Book)

Os relays podem projetar seus livros de ofertas de várias maneiras para exibir e corresponder aos pedidos dos usuários. A primeira implementação de nosso próprio livro de ofertas segue um modelo OTC, no qual as ofertas são posicionadas com base apenas no preço. Os registros de data e hora dos pedidos, em outras palavras, não têm relação com o livro de ofertas. No entanto, um revezamento é livre para projetar seu livro de ofertas de modo a emular um mecanismo de comparação típico de exchange centralizada, em que os pedidos são classificados por preço, respeitando também a data e hora. Se um relay estiver disposto a oferecer este tipo de livro de ofertas ele pode possuir/integrar com uma carteira e fazer com que os pedidos da carteira sejam enviados apenas para o relay único, que então seria capaz de combinar pedidos com base no tempo. Qualquer configuração desse tipo é possível.

Enquanto outros protocolos DEX às vezes exigem que os Relays tenham recursos - saldos iniciais de tokens para fazer pedidos de compradores - os Relays Loopring precisam somente encontrar pedidos que possam ser convertidos para realizar uma negociação, e podem fazê-lo sem os tokens iniciais.

6.2 Compartilhamento de Liquidez

Os relays são livres para projetar como eles compartilham a liquidez (pedidos) uns com os outros. Nosso consórcio blockchain é apenas uma solução para conseguir isso, e o ecossistema está livre para se conectar e comunicar como quiser. Além de aderir a um blockchain de consórcio, eles podem construir e gerenciar os seus próprios, criando regras/incentivos como eles quiserem. Os relays também podem funcionar sozinhos, como visto na implementação de carteira sensível ao tempo. É claro que há claras vantagens na comunicação com outros Relays na busca de efeitos de rede, no entanto, diferentes modelos de negócios podem necessitar de projetos de compartilhamento peculiares e dividir as taxas de diversas maneiras.

7 Especificação do protocolo

7.1 Anatomia de um Pedido

Um pedido é um pacote de dados que descreve a intenção de negociação do usuário. Um pedido Loopring é definida usando o Modelo de Unidade Unidirecional ou UDOM, da seguinte maneira:

```
message Order {
  address protocol;
  address owner;
  address tokenS;
  address tokenB;
  uint256 amountS;
  uint256 amountB;
  unit256 lrcFee
  unit256 validSince; // Seconds since epoch
  unit256 validUntil; // Seconds since epoch
  uint8   marginSplitPercentage;  // [1-100]
  bool    buyNoMoreThanAmountB;
  uint256 walletId;
  // Endereço Dual-Authoring
  address authAddr;
  // v, r, s são partes da assinatura
  uint8   v;
  bytes32 r;
  bytes32 s;
  // Chave privada Dual-Authoring,
  // não é usado para calcular o hash do pedido,
  // assim NÃO é assinado.
  string  authKey;
}
```

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 order-rings dos quais esse pedido faz parte, o que impede o front-running. Por favor, consulte a seção 9.1 para mais detalhes. A assinatura é representada pelos campos `v`, `r`, e `s` e 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 flutuante por natureza), mas, em vez disso, usa o termo `rate` ou r, que é expresso como `amountS`/`amountB`. 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 a precisão do cálculo.

7.1.1 Comprando Quantidades

Quando um ring-miner encontra os pedidos, é possível que uma taxa melhor seja executável, permitindo que os usuários obtenham mais `tokenB` do que o `amountB` especificado. No entanto, se `buyNoMoreThanAmountB` estiver definido como `True`, o protocolo garante que os usuários recebam não mais que `amountB` de `tokenB`. Assim, o parâmetro `buyNoMoreThantokenB` do UDOM determina quando um pedido é considerado completamente preenchido. O `buyNoMoreThantokenB` aplica um limite tanto no `amountS` ou `amountB`, e permite que os usuários expressem intenções comerciais mais granulares do que os pedidos tradicionais de compra/venda.

Por exemplo: com `amountS` = 10 e `amountB` = 2, a taxa $r = 10/2 = 5$. Assim, o usuário está disposto a vender 5 `tokenS` por cada `tokenB`. O ring-miner corresponde e considera o usuário uma taxa de 4, permitindo que o usuário receba 2.5 `tokenB` ao invés de 2. No entanto, se o usuário desejar apenas 2 `tokenB` e definir o`buyNoMoreThanAmountB` como `True`, o LPSC executará a transação a uma taxa de 4 e o usuário vende 4 `tokenS` por cada `tokenB`, economizando efetivamente 2 `tokenS`. Tenha em mente que isso não leva em conta as taxas de mineração (veja a seção 8.1).

De fato, se usarmos

```
Order(amountS,tokenS,
      amountB,tokenB,
      buyNoMoreThantokenB)
```

Para representar um pedido de forma simplificada, para os mercados ETH/USD em uma exchange tradicional, a modelagem tradicional de compra e venda pode expressar a 1ª e a 3ª ordem abaixo, mas não as outras duas:

1. Vender 10 ETH ao preço de 300 USD/ETH. Este pedido pode ser expresso como: `Order(10, ETH, 3000, USD, F`
2. Vender ETH ao preço de 300 USD/ETH para obter 3000 USD. Este pedido pode ser expresso como: `Order(10, ETH, 3000, USD, True)`.
3. Comprar 10 ETH ao preço de 300 USD/ETH, Este pedido pode ser expresso como: `Order(3000, USD, 10, ETH, T`

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

7.2 Ring de Verificação

Os contratos inteligentes Loopring não realizam cálculos de exchange ou de valor, mas devem receber e verificar o que os ring-miners fornecem para esses valores. Estes cálculos são feitos pelo ring-miners por duas razões principais: (1) a linguagem de programação para contratos inteligentes, como a solidez [19] no Ethereum, não tem suporte para matemática de floating point, especialmente $pow(x, 1/n)$ (calculando a n-th root de um número de ponto flutuante), e (2) é desejável que o cálculo seja feito off-chain para reduzir o cálculo computacional e o custo do blockchain.

7.2.1 Verificação de Sub-Ring

Essa etapa impede que os arbitradores realizem injustamente todo o spread em um order-ring, implementando novos pedidos dentro dele. Essencialmente, uma vez que um order-ring válido é encontrado por um ring-miner, pode ser tentador adicionar outros pedidos ao order-ring para absorver totalmente o spread dos usuários (descontos de taxa). Como ilustrado pela figura 3 abaixo, cuidadosamente calculado $x1$, $y1$, $x2$ e $y2$ fará com que o produto de todas as encomendas seja exatamente 1, portanto não haverá desconto de taxa.

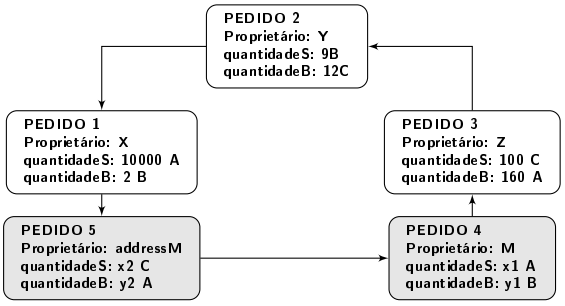

Figura 3: Um order-ring com sub-ring

Não é possível adicionar valor zero à rede e é considerado uma conduta injusta pelo ring-miner. Para evitar isso, o protocolo Loopring requer que um loop válido não possa conter 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 Verificador de Taxas

Os cálculos da exchange no order-ring são feitos por operadores de ring-miners por razões declaradas acima. É o LPSC que deve verificar se está correto. Primeiro, ele verifica se a taxa de compra que o ring-miner 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 da exchange solicitada ou melhor na transação. Uma vez que as taxas da exchange são confirmadas, o LPSC garante que cada pedido do order-ring compartilhe o mesmo desconto de taxa. Por exemplo, se a taxa de desconto for γ, o preço de cada pedido será:

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

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

consequentemente:

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

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

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

onde r^i é a taxa de rotatividade do pedido de i^o ordem. Obviamente, somente quando a taxa de desconto é $\gamma \geq 0$, esses pedidos podem ser preenchidas i^o pedido (O^i) a taxa da exchange é $\hat{r^i} = r^i \cdot (1-\gamma)$, $\hat{r^i} \leq r^i$.

Lembre-se do nosso exemplo anterior, em que Alice tem 15 tokens `A` e quer 4 tokens `B`, Bob tem 10 tokens `B` e quer 30 tokens `A`. Se token `A` é a referência, então Alice está comprando token `B` por $\frac{15}{4} = 3.75$`A`, enquanto Bob esta vendendo token `B` por $\frac{30}{10} = 3.00$`A`. Para calcular o desconto: $\frac{150}{120} = 1.25$ portanto $\frac{1}{1.25} = 0.8 = (1 - -\gamma)^2$. Assim, a taxa da exchange que torna a negociação equitativo para ambas as partes é $\sqrt{0.8} \cdot 3.75 \approx 3.3541$ token `A` por token `B`.

Bob transfere 4 tokens `B` e recebe 13.4164 tokens `A`, mais do que os 12 que ele estava esperando por aqueles 4 tokens. Alice recebe 4 tokens `B` como pretendido, mas dá apenas 13.4164 tokens `A` na troca, menos do que os 15 que ela estava disposta a dar por aqueles 4 tokens. Observe que uma parte dessa margem será destinada ao pagamento de taxas para incentivar os mineiros (e carteiras). (Veja a seção 8.1).

7.2.3 Monitoramento & Cancelamento

Um usuário pode cancelar parcial ou totalmente um pedido enviando uma transação especial para o LPSC, contendo os detalhes sobre o pedido e os valores a serem cancelados. O LPSC leva isso em conta, armazena os valores para cancelar e emite um evento `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 publicamente acessíveis em `OrderCancelled` / `OrderFilled` esses eventos são emitidos quando são alterados. O rastreamento desses valores é crítico para o LPSC durante a etapa de liquidação do order-ring.

O LPSC também suporta o cancelamento de todos os pedidos para qualquer par de negociação com o

`OrdersCancelled` e cancelamento de todos os pedidos para um endereço com o `AllOrdersCancelled`.

7.2.4 Escala de Pedidos

Os pedidos são escalonados de acordo com o histórico de valores preenchidos e cancelados e o saldo atual das contas dos remetentes. O processo encontra o pedido com a menor quantidade a ser preenchida de acordo com as características acima e o utiliza como referência para escalonar todas as transações no order-ring.

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

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

onde $\overline{s}_i$ é o saldo deixado após os pedidos estarem parcialmente preenchidos.

Durante a implementação, podemos assumir com segurança qualquer pedido no order-ring para ter o valor mais baixo e, em seguida, iterar no order-ring 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 5%, todas as transações no order-ring serão reduzidas para 5%. Depois que as transações forem concluídas, o pedido considerada como a menor quantidade restante a ser preenchida deve ser totalmente preenchida.

7.3 Liquidez do Ring

Se o order-ring atender a todas as verificações anteriores, o order-ring poderá ser fechado e as transações poderão ser feitas. Isso significa que todos os pedidos de n formam um order-ring fechado de pedidos, conectado como na figura 4:

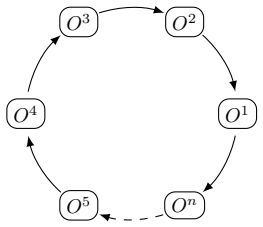

Figura 4: Liquidação do Ring

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

Para cada pedido no order-ring, um pagamento de `tokenS` é feito para o pedido seguinte ou anterior, dependendo da implementação. Então a taxa do ring-miner é paga dependendo do modelo de taxa escolhido pelo ring-miner. Finalmente, uma vez que todas as transações são feitas, um evento `RingMined` é emitido.

7.3.1 Emissão de Eventos

O protocolo emite eventos que permitem que os relays, order browsers e outros atores recebam atualizações do livro de ofertas com a maior eficiência possível. Os eventos emitidos são:

- **OrderCancelled**: Um pedido específico foi cancelado.
- **OrdersCancelled**: Todos os pedidos de um par de negociação de um endereço foram cancelados.
- **AllOrdersCancelled**: Todos os pedidos de todos os pares de negociação de um endereço foram cancelados.
- **RingMined**: Um order-ring foi liquidado com sucesso. Este evento contém dados relacionados a cada transferência de token do inner-ring.

8 LRx Token

LRx é nossa notação de token generalizado. LRC é o token da Loopring no Ethereum, LRQ no Qtum e LRN no NEO, etc. Outros tipos de LRx serão introduzidos no futuro conforme o Loopring for implantado em outras blockchains públicas.

8.1 Modelo de Taxas

Quando um usuário cria um pedido, ele especifica uma quantia de LRx a ser paga ao ring-miner como uma taxa, em conjunto com uma porcentagem da margem (`marginSplitPercentage`) feito no pedido que o ring-miner pode reivindicar. Isso é chamado de divisão de margem. A decisão de qual escolher (taxa ou margem dividida) é deixada para o ring-miner.

Uma representação da divisão de margem:

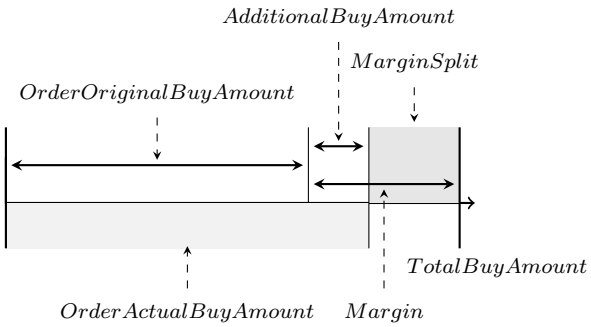

Figura 5: Uma divisão de margem de 60%

Se a margem no order-ring for muito pequena, o ring-miner vai escolher a taxa LRx. Se, pelo contrário, a margem for substancial o suficiente para que a margem de lucro resultante valha muito mais do que a taxa LRx, um ring-miner escolherá a divisão de margem. Há outra condição, no entanto: quando o ring-miner escolhe a divisão de margem, ele deve pagar ao usuário (criador do pedido) uma taxa, que é igual ao LRx que o usuário teria pago ao ring-miner como uma taxa. Isso aumenta o limiar de onde o ring-miner escolherá a divisão da margem para o dobro da taxa LRx do pedido, aumentando a propensão da escolha da taxa LRx. Isso permite que os ring-miner recebam uma renda constante de pedidos de margem baixa para a compensação de receber menos receita em order-rings de margem mais alta. Nosso modelo de taxas baseia-se na expectativa de que, à medida que o mercado cresce e amadurece, haverá menos pedidos de margem alta, necessitando, assim, de taxas fixas de LRx como incentivo.

Acabamos com o seguinte gráfico:

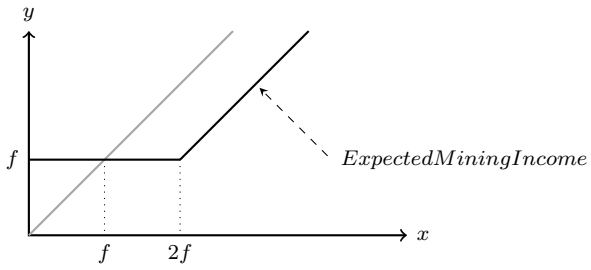

Figura 6: Modelo de Taxa Loopring

onde f é a taxa LRx, x é a divisão de margem, y é a renda de mineração. $y = max(f, x - f)$ conforme 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 ring-miners escolherão a taxa fixa 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 ring-miners 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 pelo ring-miner, sempre haverá uma transferência de LRx entre o ring-miner e o remetente da ordem. O ring-miner ganha a taxa LRx ou paga a taxa LRx de volta ao remetente para obter a divisão da margem.

Os Ring-miners dividirão uma certa porcentagem de taxas com carteiras. Quando um usuário faz um pedido através de uma carteira e é preenchido, a carteira é recompensada com uma parte das taxas ou divisão de margem. Embora isso seja modular, e modelos ou implementações de negócios exclusivos são possíveis, nossa tendência é que as carteiras recebam aproximadamente 20%-25% de taxas ganhas. As carteiras representam um alvo primário para a integração do protocolo Loopring, já que elas têm a base de usuários, mas pouca ou nenhuma fonte de renda.

8.2 Governança Descentralizada

Em sua raiz, o protocolo Loopring é um protocolo social no sentido de que se baseia na coordenação entre os membros para operar efetivamente em direção a um objetivo. Isso não é diferente dos protocolos criptoeconômicos 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 incentivos financeiros dos vários participantes da rede. Esse alinhamento é necessário para a ampla adoção de qualquer protocolo, mas é particularmente agudo para os protocolos de exchange, 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. Atualizações inteligentes de contratos serão, em parte, regidas por portadores de tokens (token holders) para garantir continuidade e segurança, e para atenuar os riscos de liquidez desviados 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 não se atualizem com os contratos atualizados. A atualização é crucial para o sucesso do protocolo, pois ele deve se adaptar às demandas do mercado e às 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, determinados percentuais são congelados da Fundação Loopring e alocados a fundos destinados à comunidade. [21].

No entanto, os proprietários de tokens LRx não são os únicos interessados a serem considerados na orientação do protocolo: relays/ring-miners, carteiras, desenvolvedores e outros são parte integrante do ecossistema e sua voz deve ser ouvida. De fato, dado que esses agentes não precisam deter nenhum LRx para desempenhar suas respectivas funções (já que vendedores/compradores tradicionais e criadores de mercado são inexistentes, as reservas simbólicas iniciais não são obrigatórias) devemos permitir que métodos alternativos para que seus interesses sejam respeitados. Além disso, a votação "simples"baseada em tokens, tanto on-chain quanto off, é uma solução imperfeita para desacordo, já que o baixo número de eleitores e a concentração de propriedade de token representam riscos. Assim, o objetivo é implementar um modelo de governança que é construído em camadas e repousa sobre um conhecimento compartilhado de que o conjunto de processos de tomada de decisão é a norma. Isso pode ser facilitado por instituições de coordenação que oferecem sinais de um conjunto diversificado de participantes e, talvez, de pontos focais do protocolo pré-estabelecido. À medida que isso se concretizar, a Fundação Loopring inevitavelmente evoluirá de desenvolvedores de protocolo para administradores de protocolos.

9 Fraude e Proteções a Ataques

9.1 Prevenção de Front-running

Em exchanges descentralizadas, o front-running é quando alguém tenta copiar a solução de negociação de outro node e tenta minerá-lo antes da transação original que está na pool de transações pendente (mempool). Isso pode ser alcançado especificando 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 order-filch: quando um dos principais concorrentes rouba um ou mais pedidos de uma transação de liquidação de order-ring pendente; e, específico para Loopring: quando um dos principais favoritos rouba todo o order-ring de uma transação pendente.

Quando uma transação submitRing não é confirmada e ainda está no pool de transações pendente, qualquer pessoa pode identificar facilmente essa transação e substituir `minerAddress` com o seu próprio endereço (o `filcherAddress`), então eles podem assinar novamente o payload com`filcherAddress` para substituir a assinatura do order-ring. O fincher pode definir um preço de gás mais alto e enviar uma nova transação esperando que os block-miners selecionem sua nova transação no próximo bloco, em vez da transação submitRing original.

As soluções anteriores para esse problema tinham importantes desvantagens: exigir mais transações e, assim, custar aos ring-miners mais gás; e gastar mais pelo menos duas vezes aos blocos para resolver um order-ring. Nossa nova solução, Dual Authoring[22], envolve o mecanismo de configuração de dois níveis de autorização para pedidos - um para liquidação e outro para ring-mining.

Processo de Dual Authoring:

1. Para cada pedido, o software da carteira gerará um par de chave pública/chave privada aleatória e colocará o par de chaves no snippet JSON do pedido. (Uma alternativa é usar o endereço derivado da chave pública em vez da própria chave pública para reduzir o tamanho do byte. Nós usamos `authAddr` para representar tal endereço e `authKey` para representar `authAddr` a chave privada correspondente).

2. Calcule o hash do pedido com todos os campos na ordem, exceto `r`, `v`, `s`, e `authKey`), e assine o hash usando a `owner` chave privada do proprietário (não `authKey`).

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

4. Quando um order-ring é identificado, o ring-miner usará o `authKey` de cada pedido para assinar o hash do ring, `minerAddress`, e todos os parâmetros de mineração. Se um order-ring conter n ordens, haverá n assinaturas pelas n `authKey`. Nós chamamos essas assinaturas de `authSignature`. O ring-miner também pode precisar assinar o hash do ring junto com todos os parâmetros de mineração usando a chave privada do `minerAddress`.

5. O ring-miner chama a função submitRing com todos os parâmetros, bem como todas as `authSignature`. Observe que os `authKey` não fazem parte da transação on-chain e, portanto, permanecem desconhecidos para outras partes que não o próprio ring-miner.

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

O resultado é que agora:

- A assinatura do pedido (pelo endereço da chave privada do `owner`) garante que o pedido não pode ser modificado, incluindo o `authAddr`.
- A assinatura do ring-miner (pela chave privada do `minerAddress`), se fornecido, garante que ninguém pode usar sua identidade para minerar um order-ring.
- A `authSignature` garante que todo o order-ring não pode ser modificado, incluindo `minerAddress`, e nenhuma ordem pode ser roubada.

A Dual Authoring (Autoria Dupla) evita ring-filch e order-filch, ao mesmo tempo em que garante a liquidação dos order-rings em uma única transação. Além disso, a Dual

Authoring abre as portas para os relays compartilharem pedidos de duas maneiras: compartilhamento não-conversível e compartilhamento que pode ser compartilhado. Por padrão, o Loopring opera um modelo OTC e suporta apenas ordens de preço limitado, o que significa que os timestamps dos pedidos são ignorados. Isto implica que o front-running de uma negociação não tem impacto sobre o preço real da mesma, mas afeta se ela é executada ou não.

10 Outros ataques

10.1 Ataque Sybil ou DOS

Usuários mal-intencionados - agindo por conta própria ou falsificando identidades - podem enviar uma grande quantidade de pequenos pedidos para atacar os nodes Loopring. No entanto, como permitimos que os nodes rejeitem pedidos com base em seus próprios critérios - que podem ser ocultados ou revelados - a maioria desses pedidos serão rejeitados por não gerar lucros satisfatórios quando combinados. Ao capacitar os revezamentos para ditar como eles gerenciam os pedidos, não vemos um ataque massivo de pedidos mínimo como uma ameaça.

10.2 Saldo insuficiente

Os usuários mal-intencionados podem assinar e distribuir pedidos cujo valor do pedido é diferente de zero, mas cujo endereço realmente tem saldo zero. Os nodes podem monitorar e perceber que o saldo real de alguns pedidos são zero, atualizar esses status de pedido de acordo e, em seguida, descartá-los. Os nodes devem gastar tempo para atualizar o status de um pedido, mas também podem optar por minimizar 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 uma exchange descentralizada. Ao fazê-lo, tem profundas repercussões em como as pessoas negociam ativos e valor. O dinheiro, como um produto intermediário, facilita ou substitui a negociação na exchange e resolve a dupla coincidência do problema [23], pelo qual duas contrapartes devem desejar o bem ou serviço distinto um do outro. Da mesma forma, o protocolo Loopring pretende dispensar a necessidade da nossa estrutura de negociações em pares que se completem, usando ring matching para negociações mais facilmente consumadas. Isso é significativo para como a sociedade e os mercados negociam 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 combinar os comerciantes (compradores/vendedores) em escala, é uma ameaça teórica ao conceito de dinheiro em si.

Os benefícios do protocolo incluem:

- O gerenciamento de pedidos off-chain e a liquidação on-chain não significam nenhum sacrifício no desempenho por segurança.
- Maior liquidez devido ao ring-mining e compartilhamento de pedidos.
- O Dual Authoring resolve o problema pernicioso do front running enfrentado por todos os DEXs e seus usuários hoje.
- Contratos públicos livres e gratuitos permitem que qualquer dApp crie ou interaja com o protocolo.
- A padronização entre os operadores permite efeitos de rede e uma melhor experiência ao usuário final.
- Rede mantida com flexibilidade na execução de pedidos e comunicação.
- Redução de barreiras na entrada significam menores custos para os nodes que se unem 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 rever 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 EVM

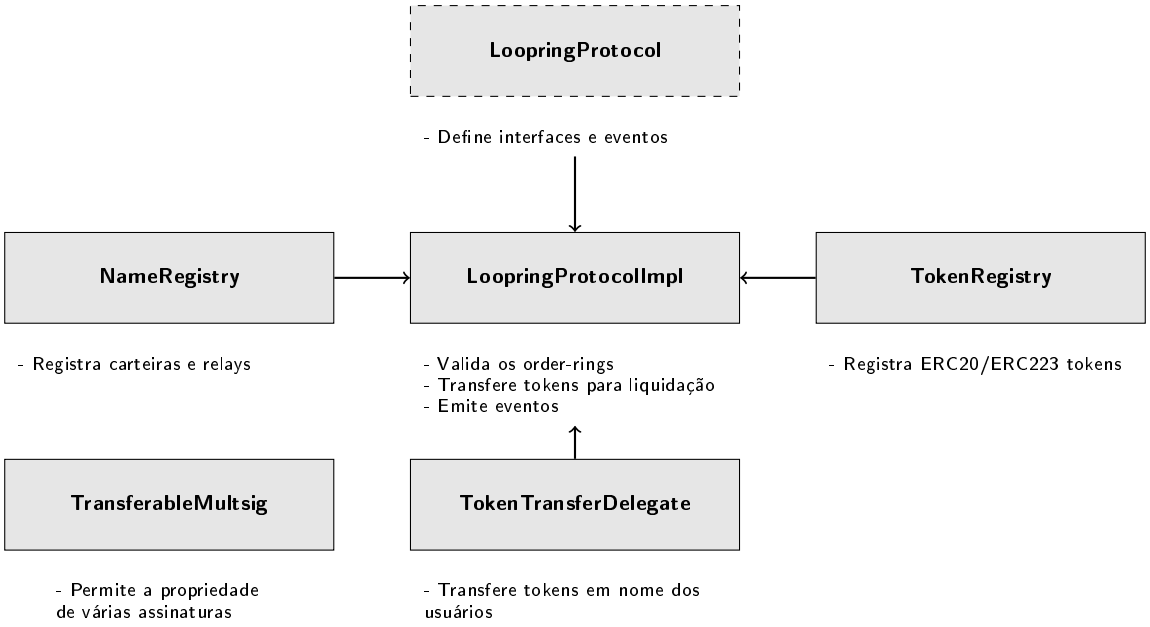

Figura 7: Contratos Inteligentes

Apêndice B Desdobramentos

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 da Qtum:

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