Loopring:
Un Protocolo Descentralizado de Plataformas de Intercambio de Tokens

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

May 26, 2018

Abstracto

Loopring es un protocolo abierto que permite construir plataformas de intercambio descentralizado. Loopring opera como un conjunto de contratos inteligentes públicos, responsables del comercio y de la liquidación, junto a un grupo de agentes fuera-de-cadena (off-chain) que agregan y comunican pedidos. El protocolo es gratuito, extensible, y sirve como un elemento de soporte estandarizado para la construcción de aplicaciones descentralizadas (dApps), que incorporan la funcionalidad de intercambios. Sus estándares interoperables facilitan un comercio anónimo que no requiere de confianza (trustless). Una mejora importante, con respecto a los protocolos descentralizados de plataformas de intercambio actuales, es la habilidad para hacer que los pedidos sean mezclados y emparejados con otros pedidos diferentes, obviando las restricciones de formar pares de intercambio entre dos-tokens y mejorando drásticamente la liquidez. Además, Loopring emplea una solución única y robusta para la prevención del front-running: el intento injusto de enviar transacciones a un bloque más rápido que el del proveedor de la solución original. Loopring es agnóstica en relación con las cadenas de bloques (blockchains), y puede implantarse en cualquier blockchain con funcionalidad de contrato inteligente. Hasta el momento de escribir este documento, Loopring es operable en Ethereum [1] [2] y Qtum [3] con NEO [4] bajo construcción.

1 Introducción

Con la proliferación de activos basados en la blockchain, la necesidad de intercambiar estos activos entre las contrapartes se ha incrementado considerablemente. A medida que miles de nuevos tokens son introducidos - incluyendo los activos tradicionales de tokenización - está necesidad se magnifica. Ya sea intercambiando tokens, por motivaciones comerciales especulativas, o convirtiéndolos para acceder a la red vía sus tokens de utilidad nativa, la habilidad de intercambiar un activo criptográfico es fundamental para un ecosistema amplio. De hecho, hay una energía potencial en los activos [5]; liberar esta energía - desbloqueando el capital - no solo requiere determinar la propiedad, lo que las blockchains han permitido inmutablemente, sino también la habilidad de transferir y transformar libremente estos activos.

Como tal, el intercambio de tokens (valor) que no requiere una relación de confianza, es un caso convincente de uso para la tecnología de blockchain. Sin embargo, hasta ahora, los entusiastas de la criptografía se han conformado, en gran medida, por comerciar tokens en las tradicionales plataformas de intercambio (exchanges, en inglés) centralizado. El protocolo Loopring es necesario porque, al igual que Bitcoin [6], enfatiza diligentemente que, con respecto al dinero electrónico entre-pares (peer-to-peer), "los mayores beneficios se pierden si un tercero confiable aún requiere prevenir el gasto-doble"; de la misma manera, los principales beneficios de los recursos descentralizados se pierden, si tienen que pasar por las plataformas de intercambio centralizado, cerrado, que requieren de confianza.

El intercambio descentralizado de tokens en las plataformas de intercambio centralizado no tiene sentido desde una perspectiva filosófica, porque es imposible mantener los valores propugnados por estos proyectos descentralizados. También existen numerosos riesgos prácticos y limitaciones en el uso de las plataformas de intercambio centralizado, que se describirán más adelante. Las Plataformas de Intercambio Descentralizado (DEX) [7] [8] [9] han tratado de abordar estos problemas y, en muchos casos, han logrado mitigar los riesgos de seguridad mediante el uso de las blockchains para negociaciones directas. Sin embargo, dado

que la capacidad de DEX se convierte en una infraestructura crucial para la nueva economía, existe un margen considerable para la mejora del rendimiento. Loopring tiene como objetivo proporcionar herramientas modulares para dicha infraestructura, con su protocolo abierto de Aplicaciones Descentralizadas (dApp) agnósticas.

2 Panorama Actual de las Plataformas de Intercambio

2.1 Insuficiencias de las Plataformas de Intercambio Centralizado

Los tres principales riesgos, asociados con las plataformas de intercambio centralizado, son: 1) la falta de seguridad, 2) la falta de transparencia, y 3) la falta de liquidez.

La falta de seguridad surge del hecho en que los usuarios suelen ceder sus llaves privadas (es decir, fondos) a una entidad centralizada. Esto expone a los usuarios, a la posibilidad de que las plataformas de intercambio centralizado sean presa de los hackers maliciosos. Los riesgos de seguridad y los ciberataques sufridos por todas las plataformas de intercambio son bien conocidos [10] [11], aunque a menudo se aceptan como "table stakes" ("mesa de riesgos"), en el comercio del intercambio de los tokens. Al tener bajo su custodia a millones de dólares en fondos de los usuarios, en sus servidores, las plataformas de intercambio centralizado siguen siendo atractivas para el ataque de los hackers. Además, los desarrolladores de plataformas de intercambio también pueden cometer errores accidentales honestos con los fondos de los usuarios. Los usuarios, simplemente, no tienen el control de sus tokens cuando los depositan en una plataforma de intercambio centralizado.

La falta de transparencia expone a los usuarios al riesgo de que las deshonestas plataformas de intercambio actúen injustamente. La distinción aquí se basa en las intenciones maliciosas de los operadores de las plataformas de intercambio, ya que los usuarios no están realmente comerciando sus propios activos en estas plataformas de intercambio centralizado, sino más bien, hacen un reconocimiento de deuda (IOU). Cuando los tokens son enviados a la cartera de la plataforma de intercambio, este los pone bajo su custodia y ofrece un reconocimiento de la deuda en su lugar. Es así, como todos los intercambios se realizan entre los pagarés (IOU) de los usuarios. Para retirarlos, los usuarios canjean sus pagarés con la plataforma de intercambio, y reciben sus tokens en la dirección de su cartera externa. En este proceso hay una falta de transparencia, y la plataforma de intercambio puede cerrar, congelar su cuenta, declararse en quiebra, etc. También existe la posibilidad de que utilicen los activos de los usuarios para otros fines mientras los mantienen bajo su custodia, como prestarlos a terceros. La falta de transparencia puede tener un costo para los usuarios, aún sin perder el total de sus fondos; por ejemplo, puede generarse tasas de cambio más altas, retrasos en los momentos de mayor demanda, riesgos regulatorios y pedidos siendo "front-ran".

Falta de Liquidez Desde el punto de vista de los operadores de las plataformas de intercambio, la liquidez fragmentada impide la entrada de nuevas plataformas de intercambio, debido a la presencia de dos escenarios de "el-ganador-se-lleva-todo". En el primero, la plataforma de intercambio con el mayor número de pares de divisas gana, porque a los usuarios les resulta más ventajoso realizar todos sus intercambios en una sola plataforma de intercambio. En el segundo, la plataforma de intercambio con el mayor registro de pedidos gana, debido al diferencial favorable de la bid-ask (oferta-demanda) para cada uno de los pares del intercambio. Esto desalienta la competencia de las personas nuevas en el mercado de intercambios, porque les resulta difícil acumular la liquidez inicial necesaria. Como resultado, muchas plataformas de intercambio controlan una cuota alta del mercado, a pesar de las quejas de los usuarios y los incidentes sustanciales de ciberataques realizados por los hackers informáticos. Es importante mencionar, que mientras las plataformas de intercambio centralizado más compren y ganen las cuotas del mercado, más expuestos están a los ataques de los hackers.

Desde la perspectiva de los usuarios, la fragmentación de la liquidez reduce significativamente la Experiencia de Usuario. En una plataforma de intercambio centralizado, los usuarios solo pueden intercambiar dentro de los grupos de liquidez de su misma plataforma de intercambio, contra sus propios libros de pedidos y entre los pares de tokens que soporta. Para intercambiar el token `A` por el token `B`, los usuarios deben ir a una plataforma de intercambio que soporte ambos tokens o registrarse en diferentes plataformas de intercambio, divulgando así su información personal. Los usuarios a menudo necesitan realizar transacciones preliminares o intermedias, generalmente mediante BTC o ETH, lo que lleva a pagar las brechas entre la oferta y la demanda en el proceso. Finalmente, los libros de pedidos pueden no ser lo suficientemente grandes, como para completar la transacción sin una desaceleración importante. Incluso si la plataforma de intercambio afirma que puede manejar grandes volúmenes, no hay garantía de que el manejo de este volumen y liquidez no sean falsos [12].

Los resultados son silos de liquidez desconectados y un ecosistema fragmentado que se asemeja al antiguo sistema financiero, que tiene un volumen significante de transacciones centralizadas en unas pocas plataformas de intercambio. Las promesas de la liquidez global de las blockchains no tienen ningún mérito o valor dentro de las plataformas de intercambio centralizado.

2.2 Insuficiencia de las Plataformas de Intercambio Descentralizado

Las plataformas de intercambio descentralizado se diferencian de las plataformas de intercambio centralizado, en parte porque los usuarios mantienen el control de sus llaves-

privadas (activos), mediante la ejecución directa de intercambios en la blockchain subyacente. Aprovechando la *tecnología que no requiere de confianza* de las criptomonedas, ellas mismas han mitigado con éxito muchos de los riesgos, antes mencionados, en torno a la seguridad. Sin embargo, los problemas persisten en relación con el rendimiento y las limitaciones estructurales.

La liquidez a menudo sigue siendo un problema, ya que los usuarios deben buscar contrapartes, a través de grupos de liquidez y estándares dispares. Los efectos de la liquidez fragmentada están presentes si los DEXs o dApps no utilizan estándares consistentes para interoperar, y si los pedidos no son compartidos o propagados dentro de una red amplia. La liquidez de los libros de pedidos limitados y, específicamente su resiliencia - cuán rápido los pedidos de limite ejecutados son reemplazados por pedidos nuevos - puede afectar significativamente las estrategias optimas del intercambio [13]. La ausencia de estos estándares ha resultado no sólo en la reducción de la liquidez, sino también en la exposición a una variedad de contratos inteligentes patentados potencialmente inseguros.

Además, dado que los intercambios se realizan dentro de la cadena, los DEXs heredan las limitaciones de la blockchain subyacente; nominalmente: escalabilidad, retrasos en la ejecución (proceso de minería) y modificaciones costosas en los pedidos. Por lo tanto, el registro de pedidos de la blockchain no es particularmente bien escalado, ya que la ejecución del código en la blockchain genera un costo (gas), lo que hace que las cancelaciones de pedidos múltiples sean excesivamente caras.

Finalmente, dado que los registros de los pedidos de la blockchain son públicos, la transacción para hacer un pedido es visible para los mineros de criptomonedas, mientras se espera que esta sea extraída en el bloque siguiente y colocada en el libro de pedidos. Este retraso expone a los usuarios al riesgo de una "ejecución anticipada" (front-run) y también al riesgo de que el precio o la ejecución sean cambiados en su contra.

2.3 Soluciones Híbridas

Por las razones mencionadas anteriormente, las plataformas de intercambio únicamente basados en la blockchain tienen limitaciones que las hacen no competitivas con las plataformas de intercambio centralizado. Existe un balance entre la falta de confianza característica de la on-chain (dentro-de-cadena) y la velocidad y flexibilidad de los pedidos de las plataformas de intercambio centralizado. Protocolos como los de Loopring y 0x [14] proponen una solución de liquidación de transacciones dentro-de-cadena, con una gestión de pedidos fuera-de-cadena. Estas soluciones giran en torno a los contratos inteligentes abiertos; pero superan las limitaciones de escalabilidad mediante la ejecución de muchas funciones fuera de la cadena, dejando a los nodos flexibilidad para completar diferentes roles críticos para la red. Sin embargo, las desventajas también permanecen para los modelos híbridos [15]. El protocolo Loopring propone diferencias significativas, en nuestro enfoque para una solución híbrida a través del desarrollo del presente artículo.

3 El protocolo Loopring

Loopring no es una Plataforma de Intercambio Descentralizado (DEX), sino un protocolo modular para construir DEXs en múltiples blockchains. Hemos desmontado partes de los componentes principales de una plataforma de intercambio tradicional y ofrecido un conjunto de contratos inteligentes públicos y agentes descentralizados en su lugar. Los roles en la red incluyen carteras, relés (relays, en inglés), blockchains de consorcio para compartir liquidez, buscadores de registros de pedidos, Mineros-de-Anillo (Ring-Miners, en inglés) y servicios de tokenización de activos. Antes de definir cada uno de estos elementos, primero debemos entender cuáles son los pedidos en Loopring.

3.1 Anillo de Pedidos

Los pedidos en Loopring se expresan en lo que llamamos un Modelo de Pedidos Unidireccional (UDOM, por sus siglas en inglés)[16]. UDOM formula pedidos como solicitudes de intercambio de token, `cantidadS`/`cantidadB`, (cantidad a vender/comprar) en lugar de los pedidos de oferta y demanda. Dado que cada pedido es solo un tipo de cambio entre dos tokens, una característica importante del protocolo es la mezcla y coincidencia entre varios pedidos en un intercambio circular. Utilizando hasta 16 pedidos simultáneamente, en lugar de un solo par de intercambio, se genera un aumento drástico en la liquidez y un potencial para la mejora del precio.

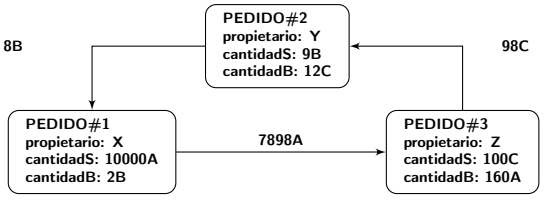

Figura 1: Un anillo de pedidos de 3 órdenes

La Figura de arriba muestra un anillo de 3 pedidos. El token de cada pedido a vender (`tokenS`) es el token de otro pedido a comprar (`tokenB`). Esto crea un bucle que permite que cada pedido intercambie sus tokens deseados, sin necesitar un pedido opuesto a su par. Los pares de pedidos de intercambios tradicionales pueden, por supuesto, seguir ejecutándose, en lo que es esencialmente un caso especial de un anillo de pedidos.

Definition 3.1 (anillo-de-pedidos) *Deje* C_0, C_1, $\cdots$, C_{n-1} *ser n diferentes tokens,* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$,

$O_{n-1\to 0}$ ser n pedidos. Estos pedidos pueden formar un anillo-de-pedidos para intercambiar:

$$O_{0\to 1} \to \cdots \to O_{i\to i\oplus 1} \to \cdots \to O_{n-1\to 0},$$

donde n es la longitud del anillo de pedidos, y $i \oplus 1 \equiv i + 1 \mod n$.

Un anillo de pedidos es válido, cuando todas las transacciones que lo componen pueden realizar a un tipo de cambio igual o superior a la tasa original especificada por el usuario. Para verificar la validez del anillo de pedidos, los contratos inteligentes del protocolo Loopring deben recibir los anillos de pedidos de los mineros, y verificar que el producto de las tasas de cambio originales de todos los pedidos sea mayor o igual a 1.

Supongamos que Alice y Bob quieren intercambiar sus tokens `A` y `B`. Alice tiene 15 token `A` y quiere 4 token `B`; Bob tiene 10 token `B` y quiere 30 tokens `A` a cambio.

¿Quién está comprando y quién está vendiendo? Esto depende solo en los activos que necesitamos fijar para dar las cotizaciones de precios. Si token `A` es la referencia, entonces Alice está comprando token `B` por el precio de $\frac{15}{4} = 3.75$`A`, mientras que Bob vende 10 token `B` por el precio de $\frac{30}{10} = 3.00$`A`. En el caso de la fijación de token `B` como referencia, decimos que Alice está vendiendo 15 token `A` por el precio de $\frac{4}{15} = 0.26666667$`B` y Bob está comprando 10 token `A` por el precio de $\frac{10}{30} = 0.33333334$`B`. Por lo tanto, quién es el comprador o el vendedor es arbitrario.

En la primera situación, Alice está dispuesta a pagar un precio más alto (3.75`A`) que el precio por el que Bob está vendiendo sus token (3.00`A`), mientras que en la segunda situación Bob está dispuesto a pagar un precio más alto (0.33333334`B`) que el precio por el que Alice está vendiendo sus tokens (0.26666667`B`). Está claro que un intercambio es posible siempre que el comprador esté dispuesto a pagar un precio igual o superior al precio del vendedor.

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

Por lo tanto, para que un conjunto de n pedidos pueda llenarse y ejecutarse, total o parcialmente, necesitamos saber si el producto entre cada una de las tasas de cambio de los pedidos de compra resulta en un número mayor o igual a 1. Si es así, todas los pedidos n pueden ser parcialmente, o totalmente ejecutados [17].

Si presentamos a una tercera contraparte, Charlie, así que si Alice quiere dar x_1 token `A` y recibe y_1 token `B`, Bob quiere dar x_2 token `B` y recibe y_2 token `C`, y Charlie quiere dar x_3 token `C` y recibir y_3 token `A`. Los tokens necesarios están presentes, y el intercambio es posible si:

$$\frac{x_1 \cdot x_2 \cdot x_3}{y_1 \cdot y_2 \cdot y_3} \geq 1 \tag{2}$$

Ver la sección 7.1 para más detalles referentes a los pedidos de Loopring.

4 Participantes del Ecosistema

Los siguientes participantes del ecosistema, proporcionan conjuntamente todas las funcionalidades que una plataforma de intercambio centralizado ofrece.

- **Carteras**: Un servicio o interfaz de la cartera permite a los usuarios acceder a sus tokens y enviar pedidos a la red de Loopring. Las carteras son incentivadas a producir pedidos, al compartir pagos dentro del anillo de pedidos (ver sección 8). Con la creencia de que el futuro de los intercambios se llevara a cabo de manera segura dentro de las carteras de los usuarios, la conexión de estos fondos de liquidez a través de nuestro protocolo es primordial.

- **Blockchain de Consorcio de Intercambio de Liquidez /Malla-Relé**: Una red de malla de relé (relay mesh network, en inglés) para el intercambio de pedidos & liquidez. Cuando los nodos ejecutan el software de relé de Loopring, ellos pueden unirse a una red existente y compartir liquidez con otros relés, a través de una blockchain de consorcio. La blockchain de este tipo, que estamos construyendo como primera implementación, tiene un tiempo casi real de intercambio de pedidos (bloques de 1-2 segundos), y reduce el historial antiguo para permitir una descarga más rápida a los nuevos nodos. Notablemente, los relés no necesitan unirse a este consorcio; pueden actuar solos y no compartir liquidez con otros, o pueden comenzar y administrar su propia red de intercambios de liquidez.

- **Relés / Mineros-de-anillos**: Los relés son nodos que reciben pedidos de las carteras o de la malla de relés; mantienen un registro público de pedidos y uno de intercambios, y opcionalmente emiten pedidos a otros relés (a través de cualquier medio fuera de la cadena arbitrario) y/o nodos de malla de relé. La minería de anillo es una característica – no un requisito – de los relés. Es computacionalmente intensa y se realiza completamente fuera de la cadena (off-chain). Llamamos a los relés con la función activada de minería de anillo "Ring-Miners", que produce anillos de pedidos al unir pedidos dispares. Los relés son libres de elegir (1) cómo comunicarse entre ellos, (2) cómo construir sus libros pedidos, y (3) cómo extraer anillos de pedidos (algoritmos de minería).

- **Contratos inteligentes del protocolo Loopring (LPSC)**: Un conjunto de contratos inteligentes públicos y gratuitos, que verifican los anillos de pedidos recibidos de los mineros de anillo (ring-miners), transfieren los tokens a nombre de los usuarios de manera segura, incentivan las operaciones de las carteras y de los mineros con comisiones, y crean eventos. Los relés/navegadores de pedidos escuchan estos eventos, para mantener actualizados a sus libros de pedidos y su historial comercial. Ver apéndice para más detalles.

- **Servicios de tokenización de activos (ATS)**: Referente a un puente entre activos, que no pueden intercambiarse directamente en Loopring. Estos servicios son administrados centralmente por empresas y organizaciones acreditadas. Los usuarios depositan activos (activos reales, fiat o tokens de otras blockchains) y obtienen tokens que pueden ser redimidos para sus depósitos en el futuro. Looping no es un protocolo de intercambio de cadena-cruzada (hasta que se encuentre una solución adecuada), pero los servicios de tokenización de activos (ATS) permiten el intercambio entre tokens ERC20 [18] y recursos físicos, así como con los recursos presentes en otras blockchains.

5 Proceso de Intercambio

1. **Autorización del protocolo**: En la Figura 2, el usuario `Y`, quiere intercambiar tokens y autoriza a los LPSC a administrar una `cantidadS` del token `B` que el usuario quiere vender. Esta operación no bloquea los tokens del usuario, quien puede transferirlos libremente mientras se procesa el pedido.

2. **Creación del pedido**: El tipo de cambio actual y el registro de pedidos del token `B` vs el token `C`, son proporcionados por los relés o por otros agentes conectados a la red, como los buscadores de pedidos. El usuario `Y` hace un pedido (pedido límite), especificando la `cantidadS` y `cantidadB` y otros parámetros a través de cualquier interface de cartera integrada. Cierta cantidad de LRx se puede agregar al pedido, como una comisión para los mineros de anillo (ring-miners); cuán mayor sea la comisión de LRx, mayor será la probabilidad de que un minero procese rápidamente el pedido. El hash del pedido se firma con la llave privada del usuario `Y`.

3. **Transmisión de pedidos**:La cartera envía el pedido y su firma a uno o más relés. Luego los relés actualizan su libro de pedidos público. El protocolo no requiere que los libros de pedidos sean construidos de una manera específica, como por ejemplo con la regla de "el primero en llegar es el primero en ser atendido". En cambio, los relés tienen el poder de tomar sus propias decisiones de diseño, mediante la construcción de sus libros de pedidos.

4. **Distribución de liquidez**: Los relés transmiten un pedido a los otros relés, a través del método que consideren más adecuado. De nuevo, hay flexibilidad sobre cómo los nodos interactúan. Para facilitar el logro de un cierto nivel de conectividad, se ha implementado un mecanismo incorporado para compartir la liquidez entre las mallas de relés (relay-mesh), utilizando un consorcio de blockchains. Como se mencionó en la sección anterior, esta malla de relé está optimizada para la velocidad y la inclusión.

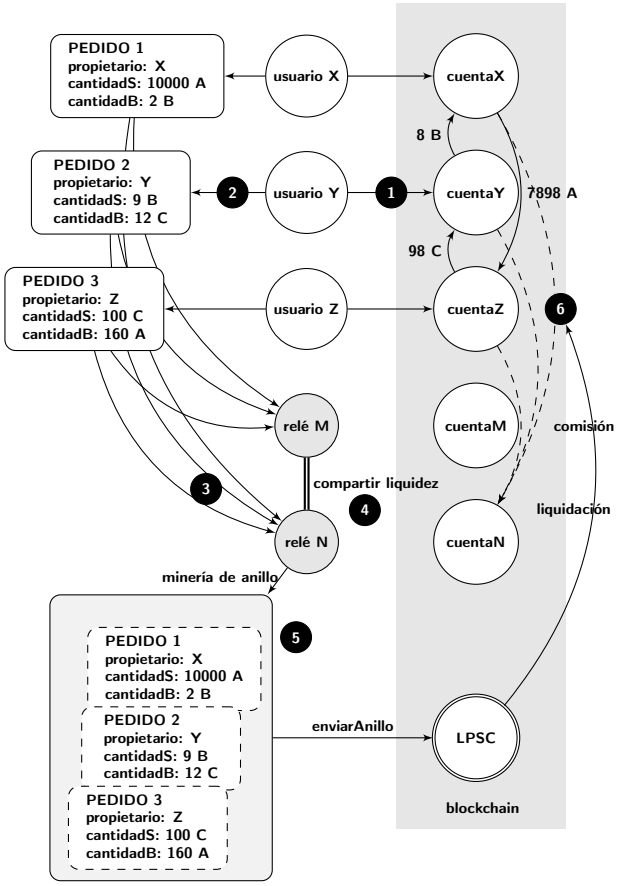

Figura 2: Proceso de Intercambio EN Loopring

5. **Minería de anillo (Coincidencia de Pedidos)**: Los mineros de anillo intentan ejecutar el pedido total o parcialmente a un tipo de tasa de intercambio o mejor, emparejándolo con varios otros pedidos. La minería de anillo es la razón principal por la cual el protocolo puede proporcionar alta liquidez sobre cualquier otro par. Si la velocidad en la que se ejecuta el pedido es mejor que la especificada por el usuario `Y`, el margen se comparte entre todos los pedidos que forman el anillo. Como recompensa, el minero puede elegir entre reclamar una parte del margen (División de Margen, y devolver a los usuarios el LRx), o simplemente quedarse con la comisión en LRx.

6. **Verificación & Transacción**: Los LPSC reciben el anillo de pedidos. Se necesitan varios controles para verificar los datos proporcionados por el minero del anillo, y para determinar si el ciclo de pedidos puede desarrollarse completa o parcialmente (dependiendo de la tasa de ejecución de los pedidos en el anillo y los tokens en las carteras de los usuarios). Si todos los controles son exitosos, el contrato automáticamente transfiere los tokens a los usuarios y paga a los mineros de anillo y a las carteras al mismo tiempo. Si los LPSC detectan la falta de fondos necesarios para el intercambio en la cartera del usuario `Y`, el pedido será reducido: un pedido de escala reducida volverá

automáticamente a su tamaño original, si se deposita una cantidad suficiente de fondos a la dirección del usuario; lo que lo hace diferente de una cancelación, que es una operación manual en un solo sentido, que no se puede revocar.

6 Flexibilidad operacional

Es importante, tener en cuenta que los estándares abiertos de Loopring permiten a los participantes operar con gran flexibilidad. Los participantes son libres de implementar nuevos modelos de negocio y generar un valor para los usuarios, ganando comisiones en LRx, en volúmenes de negociación u otras métricas definidas en el proceso (si así lo deciden). El ecosistema es modular y está diseñado para fomentar la participación de una multitud de aplicaciones.

6.1 Registro de pedidos

Los relés pueden diseñar sus libros de pedidos en cualquier número de maneras, para mostrar y hacer coincidir los pedidos de los usuarios. Una primera implementación de nuestro libro de pedidos sigue un modelo de venta-libre (OTC, en inglés), donde el límite de los pedidos se basa solo en el precio. En otras palabras, la marca del tiempo en los pedidos no tiene un impacto en la formación del libro de pedidos. Sin embargo, un relé es libre de diseñar su propio libro de pedidos, en tal manera de emular y competir con el funcionamiento típico de las plataformas de intercambio centralizado, donde los pedidos se clasifican por precio, mientras también se respeta el momento de creación del pedido. Si un relé está más inclinado a ofrecer este tipo de libro de pedidos, ellos pueden apropiarse/integrarse con una cartera, y hacer que los pedidos desde ella se envíen únicamente a un solo relé, quien luego podrá emparejar esos pedidos en base al tiempo. Cualquier tipo de configuración es posible. Mientras que otros protocolos DEX a veces requieren de Relés para tener recursos - saldos de tokens iniciales, para colocar "pedidos del comprador" (taker orders, en inglés) - Los Relés de Loopring solo necesitan encontrar pedidos que correspondan a otros, para realizar un intercambio, y pueden hacerlo sin tokens iniciales.

6.2 Compartir la liquidez

Los relés son libres de diseñar cómo compartir la liquidez (pedidos) entre ellos. Nuestro consorcio de blockchain es solo una de las soluciones para lograr este objetivo, y el ecosistema es libre de conectarse y comunicarse como lo desee. Además de unirse al consorcio de blockchain, pueden construir y administrar lo suyo, creando reglas/incentivos tal como lo deseen. Los relés también pueden funcionar en forma autónoma, como se ve en el caso de la implementación de la cartera que toma en cuenta el tiempo. Ciertamente, existen claras ventajas de comunicarse con otros relés en busca de obtener efectos de la red; sin embargo, los diferentes modelos comerciales podrían merecer su propio diseño de intercambio de liquidez y las divisiones de comisiones de muchas maneras.

7 Especificación del protocolo

7.1 Anatomía de un Pedido

Un pedido es un paquete de datos que describe la intención del usuario de intercambiar. Un pedido de Loopring se define utilizando el Modelo de Pedidos UniDireccional, o UDOM por sus siglas en inglés, de la siguiente manera:

```
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;
  // Dual-Authoring address
  address authAddr;
  // v, r, s son parte de la firma
  uint8   v;
  bytes32 r;
  bytes32 s;
  // llave-privada de Dual_authoring
  // no utilizada para calcular el hash
  //del pedido,
  // por lo tanto, NO es firmada.
  string  authKey;
  uint256 nonce;
}
```

Para garantizar el origen del pedido, se firma contra el hash de sus parámetros, excluyendo la `authAddr`, con la llave privada del usuario. El parámetro de `authAddr` se utiliza para firmar los anillos de pedidos de los que forma parte este pedido, lo que impide el front-running. Por favor refiérase a la sección 9.1 para más detalles. La firma está representada por los campos `v`, `r`, y `s`, y se envía con los parámetros del pedido a la red. Esto asegura que el pedido permanezca inmutable a lo largo de su toda existencia. Incluso si este pedido nunca cambia, el protocolo aún puede calcular su estado actual en función del balance de su dirección y otras variables.

El Modelo de Pedidos UniDireccional (UDOM) no incluye un precio (que debe ser un número de coma flotante por naturaleza), sino más bien usa el término de `tasa` o r, que se expresa en `cantidadS`/`cantidadB`. La tasa no es un número de coma flotante, sino una expresión que solo

se evaluará con otros números enteros no firmados cuando se solicite, para mantener todos los resultados intermedios como números enteros no firmados y para aumentar la precisión del cálculo.

7.1.1 Importes de compra

Cuando un minero de anillo consigue coincidir los anillos de pedidos, es posible que una mejor tasa sea ejecutable, lo que permitirá a los usuarios obtener 5 veces más del `tokenB` de la `amountB` (cantidadB) que ellos especificaron. Sin embargo, si el parámetro de `buyNoMoreThanAmountB` se establece en `True` (verdad), el protocolo garantiza que los usuarios reciban no más de la `amountB` (cantidad B) del `tokenB`. Asi, el parámetro de UDOM `buyNoMoreThantokenB` determina cuándo se debe considerar que un pedido se ha cumplido por completo. `buyNoMoreThantokenB` aplica un valor máximo a `amountS` o `amountB`, y permite a los usuarios expresar sus intenciones de intercambio de forma más detallada que los pedidos de venta y compra tradicionales.

Por ejemplo: con `amountS` = 10 y `amountB` = 2, la tasa r = 10/2 = 5. Por lo tanto, el usuario está dispuesto a vender 5 `tokenS` por cada `tokenB`. El minero empareja y encuentra una tasa de 4 al usuario, lo que le permite recibir 2.5 `tokenB` en lugar de 2. No obstante, si el usuario solo quiere 2 `tokenB` y establece el parámetro `buyNoMoreThanAmountB` a `True`, los LPSC ejecutan la transacción a una tasa de 4, y el usuario vende 4 `tokenS` por cada `tokenB`, con un ahorro efectivo de 2 `tokenS`. Considerar que las comisiones no se consideran aquí. (Ver la sección 8.1).

De hecho, si usamos

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

para representar un pedido en una forma simplificada, para los mercados ETH/USD, en una plataforma de intercambio tradicional, el modelo tradicional de compra-venta puede expresar el primer y el tercer pedido de abajo, pero no los otros dos:

1. Vende 10 ETH al precio de 300 USD/ETH. Este pedido también puede expresarse como: `Order(10, ETH, 3000, USD, Falso)`.

2. Vende ETH al precio de 300 USD/ETH para obtener 3000 USD. Este pedido puede expresarse como: `Orden(10, ETH, 3000, USD, Verdadero)`.

3. Compre 10 ETH al precio de 300 USD/ETH. Este pedido también puede expresarse como: `Orden(3000, USD, 10, ETH, Verdadero)`.

4. Gaste 3000 USD para comprar la mayor cantidad de ETH posible a un precio de 300 USD/ETH. Este pedido puede expresarse como: `Orden(3000, USD, 10, ETH, Falso)`.

7.2 Verificación de anillo

Los contratos inteligentes del protocolo Loopring no calculan la tasa de cambio o las cantidades, pero deben recibir y verificar lo que los mineros de anillo proporcionan para estos valores. Estos cálculos son realizados por los mineros de anillo, por dos razones principales: (1) el lenguaje de programación usado para los contratos inteligentes, como la Solidity [19] en Ethereum, no es compatible con el proceso matemático de la coma flotante, especialmente pow (x, 1/n) (calculando la raíz n-ésima de un número de coma flotante), y (2) es deseable que dicho cálculo se realice fuera de la cadena para reducir las operaciones y el costo del uso de la blockchain.

7.2.1 Verificación de anillo secundario/Sub-Ring

Este paso impide a los arbitrajistas la posibilidad de obtener injustamente el margen completo de un anillo de pedidos mediante la implementación de nuevos pedidos dentro de él. Básicamente, una vez que un minero identifica un anillo de pedidos válido, podría caer en la tentación de agregar más pedidos al mismo anillo de pedidos, de modo que se absorba completamente el margen del usuario (tasa de descuento). Como se muestra en la siguiente Figura 3, al calcular cuidadosamente $x1$, $y1$, $x2$ and $y2$ será posible hacer que el producto de todas las tasas de pedidos sea igual a 1, para cancelar cualquier tipo de cambio.

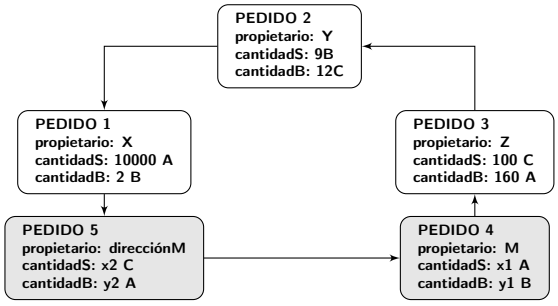

Figura 3: Un anillo de pedidos con un sub-anillo

Esto es de cero-riesgo, cero-valor añadido a la red, y se considera una conducta injusta por parte del minero de anillos. Para prevenir esto, Loopring requiere que un bucle válido no contenga ningún sub-ring. Para verificar esto, los LPSC aseguran que un token no pueda estar en una posición de compra o venta dos veces. En el diagrama anterior, podemos ver que el token `A` es un token de venta dos veces y un token de compra dos veces, lo que no sería permitido.

7.2.2 Verificación de la tasa de ejecución

El cálculo de la tasa de cambio en el anillo de pedidos es realizado por los mineros, por las razones explicadas anteriormente. Son los LPSC los que deben verificar que esta operación sea correcta. Primero, verifica que la tasa de compra que el minero de anillo puede ejecutar por cada pedido, sea menor o igual a la tasa de compra original

impuesta por el usuario. Esto asegura que el usuario obtenga al menos el tipo de cambio que solicitó, o algo mejor en la transacción.

Luego de la confirmación de las tasas de cambio, los LPSC se aseguran de que cada pedido que compone el anillo se beneficie del mismo descuento. Por ejemplo, si la tasa de descuento es γ el precio de cada pedido será

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

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

por lo tanto:

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

Si la transacción agrega n pedidos, el `descuento` es:

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

donde r^i representa la tasa de rotación de la i-ésimo pedido. Obviamente, solo cuando el descuento es $\gamma \geq 0$, estos pedidos pueden ser completados; y la tasa de cambio real del pedido i-ésimo (O^i) es: $\hat{r^i} = r^i\cdot(1-\gamma)$, $\hat{r^i} \leq r^i$.

Recuerde nuestro ejemplo anterior en el que Alice tiene 15 token `A` y quiere cambiarlos por 4 token `B` y Bob tiene 10 token `B` y quiere 30 token `A`. Si tomamos al token `A` como referencia, entonces Alice esta comprando token `B` por un valor de $\frac{15}{4} = 3.75$`A`, mientras que Bob está vendiendo token `B` por $\frac{30}{10} = 3.00$`A`. Para calcular este descuento: $\frac{150}{120} = 1.25$ por lo tanto $\frac{1}{1.25} = 0.8 = (1-\gamma)^2$. Así, la tasa de cambio que ejecuta el intercambio equitativo para ambas partes es $\sqrt{0.8}\cdot 3.75 \approx 3.3541$ token `A` por token `B`.

Bob da 4 tokens `B` y recibe 13.4164 token `A`, más de los 12 tokens que esperaba por sus 4 tokens. Alice recibe los 4 token `B` que esperaba, pero paga solo 13.4164 token `A` a cambio, menos de los 15 que estaba dispuesta a pagar. Tenga en cuenta que una fracción de este margen se utilizará para pagar las comisiones utilizadas para incentivar a los mineros (y carteras). (Ver la sección 8.1).

7.2.3 Seguimiento de finalización & cancelación

Un usuario puede cancelar parcial o totalmente un pedido enviando una transacción específica a los LPSC, que contiene los detalles del pedido y el importe que se cancelará. Los LPSC toman nota de ello, registran la cantidad que se cancelará y emiten un evento de `OrderCancelled` a la red. Los LPSC mantienen y rastrean las cantidades ejecutadas y eliminadas a través de un registro que usa el hash del pedido como un identificador. Esta información es de acceso público y los eventos de la `OrderCancelled` / `OrderFilled` se emiten con cada cambio. El seguimiento o rastreo de estos valores es crítico para los LPSCs durante el paso de la liquidación de anillos de pedidos.

Los LPSC también permiten la cancelación de un pedido por cualquier par de cambio mediante el evento de `OrdersCancelled` y cancelación de todos los pedidos relacionados con una dirección a través del evento `AllOrdersCancelled`.

7.2.4 Escala de pedidos

Los pedidos son escalados y actualizados en base al historial de importes ejecutados y a los importes cancelados, así como el saldo actual de la cuenta del remitente. En base a estas características, el proceso identifica el pedido con la cantidad más baja que se ejecutará, y utiliza esas características como referencia para escalar todas las transacciones del anillo de pedidos.

La identificación del pedido con el valor más bajo puede ayudar a facilitar la estimación del volumen de ejecución de cada pedido. Por ejemplo, suponiendo que el pedido i–énesimo es el que tiene el valor más bajo, el número de tokens vendidos por cada pedido $\hat{s}$ y el número de tokens comprados $\hat{b}$ por cada pedido se puede calcular como:

$$\begin{aligned}
&\hat{s}^i = \overline{s}_i,\ \hat{b}^i = \hat{s}^i/\hat{r}^i,\ ;\\
&\hat{s}^{i\oplus1} = \hat{b}^i,\ \hat{b}^{i\oplus1} = \hat{s}^{i\oplus1}/\hat{r}^{i\oplus1};\\
&\hat{s}^{i\oplus2} = \hat{b}^{i\oplus1},\ \hat{b}^{i\oplus2} = \hat{s}^{i\oplus2}/\hat{r}^{i\oplus2};\\
&\ldots
\end{aligned}$$

donde $\overline{s}_i$ es el saldo restante después que los pedidos se han ejecutado parcialmente.

En la fase de implementación, podemos suponer con seguridad que cualquier pedido del anillo tiene el valor más bajo, y luego iterar a través del anillo de pedidos, como mucho dos veces, para calcular el volumen de ejecución de cada pedido.

Ejemplo: si la cantidad más baja que debe ejecutarse representa el 5% del pedido original, todas las transacciones en el anillo de pedidos se reducirán en un 5%. Una vez que las transacciones se completen, el pedido que se consideró que tiene la cantidad más pequeña restante para ser llenada, tendrá que ejecutarse por completo.

7.3 Liquidación del anillo

Si el anillo de pedidos satisface todos los puntos anteriores, el anillo de pedidos puede ser cerrado para permitir la ejecución de las transacciones. Esto significa que todos los pedidos n formarán un ciclo cerrado, conectados como en la Figura 4:

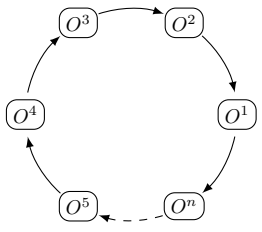

Figura 4: Liquidación del anillo

Para realizar transacciones, los LPSC usan el contrato inteligente `TokenTransferDelegate`. La introducción de ese sistema hace que sea más fácil actualizar cualquier contrato inteligente del protocolo; ya que todos los pedidos solo tendrán que autorizar a este delegado, en lugar de las diferentes versiones del protocolo. Por cada pedido en el anillo de pedidos, un pago de `tokenS` es hecho al pedido siguiente o anterior, dependiendo de la implementación. Luego, la comisión del minero se paga de acuerdo con el modelo de comisiones elegido por el propio minero. Finalmente, una vez que se realizan todas las transacciones, se emite el evento `RingMined`.

7.3.1 Eventos emitidos

El protocolo emite eventos que permiten que los relés y otros participantes involucrados reciban actualizaciones del libro de pedidos, de la manera más eficiente posible. Estos eventos son:

- **OrderCancelled**: Un pedido específico ha sido cancelado.
- **OrdersCancelled**: Todos los pedidos de un par de intercambio especifico de una sola dirección, han sido cancelados.
- **AllOrdersCancelled**: Todos los pedidos de una sola dirección han sido cancelados.
- **RingMined**: Un anillo de pedidos se ha establecido con éxito. Este evento contiene datos relacionados con las transferencias de cada token del anillo-interior.

8 Token LRx

LRx es nuestra forma genérica de nombrar tokens. LRC es el token de Loopring en Ethereum, LRQ en Qtum, LRN en NEO, etc. Se introducirán otros tipos de LRx en el futuro, ya que Loopring se extenderá a otras cadenas de bloques públicas.

8.1 Modelo de Comisiones

Cuando los usuarios crean un pedido, especifican una cantidad de LRx a pagar al minero como comisión, en conjunto con un porcentaje del margen (`marginSplitPercentage`), que el minero puede solicitar. A esto se llama margen dividido. Depende del minero de anillos decidir qué opción escogerá entre una comisión o un margen dividido. Aquí una representación del margen dividido:

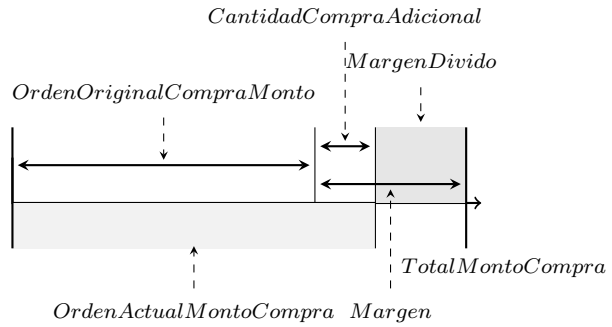

Figura 5: Un 60% de Margen Dividido

Si el margen en el anillo de pedidos es demasiado bajo, el minero de anillo escogerá la comisión en LRx. Si, por lo contrario, el margen es lo suficientemente sustancial para que la división del margen resultante valga mucho más que la tarifa en LRx, un minero de anillo escogerá la división del margen. Sin embargo, hay una condición adicional: cuando el minero de anillo elige la división de margen, debe pagarle al usuario (creador del pedido) una tarifa, que es igual al LRx que el usuario habría pagado al minero de anillo como tarifa. Esto aumenta el umbral de donde el minero de anillo elegirá compartir el margen para doblar la tarifa de LRx del pedido, aumentando así la propensión hacia la adopción de la comisión en LRx. Esto permite a los mineros de anillo obtener un ingreso constante en anillos de bajo margen, a cambio de recibir menos ingresos en pedidos con márgenes más altos. Nuestro modelo de comisión está basado en la expectativa de que, a medida que el mercado crezca y madure, habrá un número cada vez menor de anillos de pedidos de margen alto, de ahí la necesidad de incentivar una comisión fija en LRX.

Por lo tanto, obtenemos el siguiente gráfico:

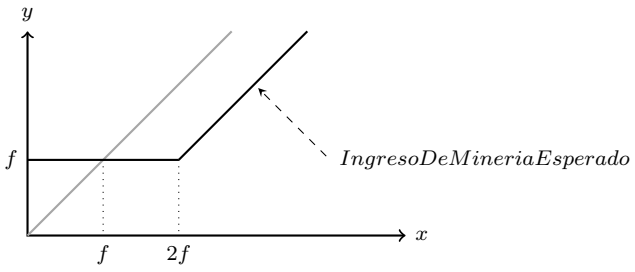

Figura 6: Loopring's Fee Model

donde f es la comisión en LRx, x es el margen dividido, y es la comisión de los mineros. $y = max(f, x - f)$ como lo indica la línea solida; la comisión en LRx para el pedido es 0, la ecuación es $y = max(0, x - 0)$ que se simplifica a $y = x$ como se indica en la línea gris.

Las consecuencias son:

1. Sí el margen se divide en 0, los mineros de anillos escogerán la comisión fija en LRx y aún son incentivados
2. Si la comisión en LRx es 0, el resultado es un modelo lineal genérico representado por la línea gris.

3. Cuando el beneficio de la división del margen es mayor a 2x (tarifa en LRx), los mineros elegirán la división del margen, pagando la comisión en LRx al usuario.

Cabe señalar que, si la comisión en LRx es diferente de cero, no importa la opción que el minero escoja, siempre habrá una transferencia de LRx entre el minero y el creador del pedido. O el minero gana la comisión en LRx o paga la comisión en LRx al remitente, para dividirse el margen.

Los mineros de anillo compartirán un cierto porcentaje de las tarifas con las carteras. Cuando un usuario realiza un pedido a través de una cartera y esta se ejecuta, el administrador de esta es compensado con una parte de la comisión o la división del margen. Aunque esto es modular, y los modelos e implementaciones de negocios únicos sean posibles, consideramos que el porcentaje de comisiones que se debe compartir con las carteras es de aproximadamente un 20% - 25%. Las carteras son un objetivo clave para la implementación del protocolo de Loopring, ya que tienen su propia base de usuarios, pero poco o nada de fuentes de ingresos.

8.2 Gobernanza Descentralizada

En su esencia, el protocolo de Loopring se basa en un protocolo social, en el sentido de que depende de la coordinación de diferentes miembros, para permitirles colaborar de manera eficiente hacia un objetivo en común. Esto no difiere de otros protocolos que caracterizan la criptoeconomía en el sentido más amplio, cuya utilidad está regulada en gran parte por los mismos mecanismos de problemas de coordinación [20], equilibrio de activación (grim trigger equilibrium) y racionalidad limitada. Con este fin, los tokens LRx no solo están destinados al pago de tarifas, sino también a alinear los incentivos financieros de los diversos participantes en la red. Esta alineación es una condición fundamental para la adopción de cualquier protocolo, pero aún más para los protocolos de intercambio; considerando que el éxito de este último está determinado por la capacidad de mejorar la liquidez en un ecosistema descentralizado.

Los tokens LRx se usarán para efectuar actualizaciones de protocolo a través de una gobernanza descentralizada. Las actualizaciones de los contratos inteligentes, en parte, se regirán por los propietarios de los tokens (holders) para garantizar la continuidad y la seguridad, y para mitigar los riesgos de liquidez excesiva/sifonada causadas por los problemas de incompatibilidad. Dado que los contratos inteligentes no pueden ser modificados después de la implementación, existe el riesgo de que las dApps o los usuarios continúen interactuando con las versiones desactualizadas, excluyéndose del uso de contratos inteligentes actualizados. La capacidad de actualización es crucial para el éxito del protocolo, ya que se debe adaptar a las demandas del mercado y las blockchains subyacentes. Una gobernanza descentralizada de los titulares de LRx permitirá las actualizaciones de contratos inteligentes de protocolo, sin interrumpir a los dApps ni a los usuarios finales, o depender demasiado de la abstracción de contratos inteligentes. Los tokens LRx existen en cantidades limitadas; y, en el caso de los LRC, un porcentaje de estos se mantienen congelados por la Fundación Loopring y son asignados como fondos para la comunidad [21].

Sin embargo, los propietarios de los tokens LRx no son los únicos interesados a considerar en dirigir la dirección del protocolo: los relés/mineros de anillo, carteras, desarrolladores y otros son una parte integral del ecosistema y su voz debe ser escuchada. De hecho, dado que estos agentes no tienen la necesidad de poseer ningún LRx, para llevar a cabo su trabajo respectivo (dado que los creadores/tomadores y creadores de mercado tradicionales son inexistentes, las reservas de token iniciales no son obligatorias), tenemos que permitir métodos alternativos para respetar sus intereses. Además, la votación "simple" basada en los tokens, tanto en cadena como fuera de ella, es un bálsamo imperfecto para el desacuerdo; ya que la baja participación de votantes y la concentración de propiedad de token representan riesgos. Por lo tanto, el objetivo es implementar un modelo de gobernanza que sea construido en capas y se base en un conocimiento compartido, de que un conjunto de procesos de toma de decisiones es la norma. Esto puede ser facilitado por instituciones de coordinación que ofrecen señales de un conjunto diverso de participantes y, quizás, de puntos focales de protocolo preestablecidos. Cuando esto llegue a buen término de realización, la Fundación de Loopring inevitablemente evolucionará de desarrolladores de protocolos a administradores de protocolo.

9 Protecciones Contra Ataques y Fraudes

9.1 Prevención del front-running

En las plataformas de intercambio descentralizado, la ejecución anticipada/front-running se produce cuando alguien intenta copiar la solución de intercambio de otro nodo, y la extrae en el bloque correspondiente antes de la transacción original, que está en el grupo de transacciones pendientes (mempool). Esta acción se puede lograr ofreciendo una tarifa de transacción más alta (precio de gas). El principal esquema de "ejecución anticipada" o front-running en Loopring (y en cualquier protocolo de coincidencia-de-pedidos) es el robo de pedidos (order-filch): cuando un front-runner se roba uno o más pedidos de una transacción pendiente de liquidación del anillo de pedidos; y en específico para Loopring, cuando un front-runner se roba el anillo completo de una transacción pendiente.

Cuando una transacción de tipo submittRing no ha sido confirmada y todavía está en el grupo de transacciones pendientes, cualquiera puede localizar fácilmente estas transacciones y reemplazar la dirección del minero (`minerAddress`) con su propia "dirección de ladrón" (`filcherAddress`); de esta manera, ellos pueden volver a firmar el paquete de datos

con su `filcherAddress`, para reemplazar la firma del anillo del pedido. El ladrón puede establecer un precio de gas más alto y enviar una nueva transacción, con la esperanza de que los mineros de bloques escojan su nueva transacción dentro del siguiente bloque, en lugar de la transacción original de submitRing.

Las soluciones anteriores para este problema tenían desventajas considerables: requerían más transacciones y, por lo tanto, aumentaban los costos de gas para los mineros; tomando al menos dos veces la cantidad de bloques requeridos para asegurar un anillo de pedidos. Nuestra nueva solución, "Doble autoría" (Dual Authoring) [22], que se compone de la adopción de un mecanismo, que desarrolla dos niveles de autorización para los pedidos: una para la regulación y otra para la minería de anillo.

Proceso de Dual Authoring:

1. Para cada pedido, el software de la cartera generará un par de llaves, llave pública/llave privada escogidas al azar, y colocará ese par de llaves en una parte de JavaScript Object Notation (JSON) del pedido. (Una alternativa es usar la dirección derivada de la llave pública en lugar de la llave pública misma para reducir el número de bytes requeridos. Usamos la `authAddr` (dirección de autorización) para representar esta dirección y `authKey` (llave de autorización) para presentar la llave privada correspondiente a `authAddr`).

2. Calcula el hash del pedido con todos los campos en el mismo pedido, excepto `r`, `v`, `s` y `authKey`, y firme el hash usando la llave privada del propietario (no la llave de autorización `authKey`).

3. La cartera envía el pedido junto a la llave de `authKey` a los relés para ser extraídos. Los mineros de los anillos verificarán que la llave de autentificación (`authKey`) y la dirección de autorización (`authAddr`) coincidan, y que la firma del pedido sea válida en relación a la dirección del `propietario`.

4. Cuando un anillo de pedidos es identificado, el minero del anillo usa cada llave de autentificación `authKey` de los pedidos para firmar el hash del anillo, dirección del minero `minerAddress`, y todos los parámetros de la minería. Si el anillo de pedidos contiene n pedidos, habrán n firmas para n llaves de autentificación `authKeys`. Llamamos a estas firmas, `authSignature` (firmas de autorización). El minero de anillos también puede necesitar firmar el hash del anillo junto a todos los parámetros de la minería usando la llave privada de la dirección del minero `minerAddress`.

5. The ring-miner llama a la función submitRing con todos sus parámetros, así también como a las firmas de autentificación `authSignature` adicionales. Tenga en cuenta que las llaves de autentificación `authKey` NO son parte de la transacción en la cadena y, por lo tanto, siguen siendo desconocidas para los participantes que no sean mineros de anillos (ring-miners).

6. El Protocolo de Loopring, ahora, verificará cada firma de autentificación `authSignature` con la dirección de autentificación `authAddr` correspondiente, y rechazará al anillo de pedidos si faltan cualquiera de sus firmas de `authSignature` o si es que estas son invalidas.

El resultado ahora es:

- La firma del pedido (a través de la llave privada de la dirección del `propietario`) garantiza que dicho pedido no pueda ser modificado, incluyendo la `authAddr`.

- La firma del *minero del anillo/* ring-miner (a través de la llave privada de la dirección del minero `minerAddress`), si es proporcionada, garantiza que nadie pueda usar su identidad para extraer un anillo de pedidos.

- La firma `authSignature` garantiza que no se pueda cambiar todo el anillo de pedidos, incluyendo la dirección del minero `minerAddress`, así commo ningún pedido puede ser robado.

La Doble Autoría (Dual Authoring, en inglés) previene el robo de anillos y pedidos, y al mismo tiempo garantiza que la liquidación de los anillos de pedidos se pueda realizar en una sola transacción. Además, Dual Authoring brinda la oportunidad para que los relés compartan pedidos de dos maneras: compartición no compatible y compartición compatible. De manera predeterminada, Loopring opera siguiendo un modelo de OTC y solo permite pedidos con límite de precio; lo que significa que la hora y la fecha del pedido son ignoradas. Esto implica que la front-running no tiene impacto en el precio registrado, pero si tiene impacto en decidir si el pedido es o no es ejecutado.

10 Otros ataques

10.1 Ataque de tipo Sybil o Denial of Service (DOS)

Los usuarios malintencionados – actuando como ellos mismos o usando una identidad falsa – podrían enviar una gran cantidad de pedidos pequeños, para atacar y tratar de saturar los nodos de Loopring. Pero dado que el protocolo permite que los nodos acepten o rechacen pedidos, de acuerdo con su propio criterio – criterio que puede ser escondido o revelado –, la mayoría de estas serían rechazadas por falta de ganancia cuando sean emparejadas. Al permitir que los relés administren pedidos como mejor les parezca, un ataque de este tipo no se considera una amenaza para el Protocolo de Loopring.

10.2 Saldo insuficiente

Los usuarios malintencionados podrían armar y propagar pedidos cuyo valor no sea cero, pero cuyas direcciones tengan un saldo de cero. Los nodos podrían monitorear y darse

cuenta de que los saldos de estos pedidos son de cero, y simplemente actualizar el estado de estos, para deshacerse de ellos. Los nodos deben de dedicar algo de tiempo en actualizar el estado de un pedido, pero también pueden elegir minimizar el esfuerzo de, por ejemplo, crear una lista direcciones negras e ignorar todos los pedidos asociados.

11 Sumario

El protocolo Loopring se propone ser una capa fundamental para las plataformas de intercambio descentralizado. Al hacerlo, el protocolo tiene un impacto profundo en cómo las personas intercambian sus activos y valores. El dinero, como un producto intermedio, facilita el intercambio tipo trueque y soluciona los problemas de la doble coincidencia de necesidades [23], donde dos contrapartes deben necesitar mutuamente los bienes o servicios que la otra parte ofrece. De forma similar, el protocolo Loopring tiene como propósito eliminar nuestras dependencias de coincidencia de necesidades de los pares de intercambios comerciales, usando el anillo de coincidencia para realizar operaciones de intercambio con más facilidad. Esto es importante para la forma en la que la sociedad y los mercados intercambian tokens, activos tradicionales y otros. De hecho, como las criptomonedas descentralizadas amenazan el control que una nación ejerce sobre el dinero, un protocolo combinatorio que puede conectar a las partes que desean intercambiar (consumidores/productores) a gran escala, es teóricamente una amenaza para el concepto mismo del dinero.

Los principales beneficios del protocolo son:

- Una gestión de pedidos fuera de cadena y liquidación en cadena; significa que no se sacrificara el rendimiento por la seguridad..
- Una mejora de la liquidez mediante la extracción de anillos y el intercambio de pedidos.
- Una Dual Authoring, que consta de dos niveles de autorización para los pedidos, resuelve el problema dañino de la front-running; problema que es afrontado hoy en día por todas las Plataformas de Intercambio Descentralizado (DEXs) y sus usuarios.
- Unos contratos inteligentes públicos gratuitos, que permiten a cualquier App descentralizada (dApp) construir o interactuar con el protocolo.
- Una estandarización entre operadores permite efectos de red y una mejor experiencia para el usuario final.
- Una red mantenida con flexibilidad en la ejecución de los libros de pedido y comunicación.
- Unas barreras de entrada reducidas significan costos más bajos para los nodos que se unen a la red y para los usuarios finales.
- Un intercambio anónimo hecho directamente desde las carteras de los usuarios.

12 Reconocimientos

Nos gustaría expresar nuestra gratitud a nuestros mentores, asesores y a muchas personas de la comunidad que han sido tan acogedoras y generosas con su conocimiento. En particular, nos gustaría agradecer a Shuo Bai (de ChinaLedger); al Profesor 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, y a Encephalo Path por examinar y aconsejarnos en este proyecto mediante sus comentarios.

Referencias

[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, bitcoinâĂŹs 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 GenÃğay. 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 âĂŤ loopringâĂŹs 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.