Loopring:
Un Protocolo de Intercambio de Tokens Descentralizado

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

May 15, 2018

Abstracto

Loopring es un protocolo abierto que construye intercambios descentralizados. Loopring opera como un conjunto público de contratos inteligentes (smart contracts) responsables del comercio y la liquidación, con un grupo de agentes fuera-de-cadena (off-chain) que agregan y comunican órdenes. 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 sin-confianza (trustless). Una mejora importante con respecto a los protocolos de intercambios descentralizados actuales es la habilidad para hacer que las órdenes sean mezcladas y combinadas con otras órdenes 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 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 este momento de escribir este documento, Loopring es operable en Ethereum [1] [2] y Qtum [3] con NEO [4] siendo construida.

1 Introducción

Con la proliferación de activos basados en la blockchain, la necesidad de intercambiar estos activos entre las partes interesadas ha crecido considerablemente. A medida que miles de nuevos tokens son introducidas - incluyendo los activos tradicionales de tokenización -esta necesidad se magnifica. Ya sea intercambiando tokens por motivaciones comerciales especulativas, o convirtiéndose en sus tokens de utilidad nativos para acceder a la red específica, la habilidad de intercambiar una cripto a un activo por otro es fundamental para un ecosistema mayor. De hecho, hay una energía potencial en los activos [5], y liberando esta energía - para desbloquear el capital âĂŞ no solo requiere determinar la propiedad, que las blockchains han permitido inmutablemente, sino que también la habilidad de transferir y transformar libremente estos activos.

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

El comercio de tokens descentralizados en los lugares de intercambio o Exchange centralizados no tiene sentido desde el punto de vista filosófico, porque es imposible mantener los valores propugnados por estos proyectos descentralizados. También existen numerosos riesgos prácticos y limitaciones en el uso de exchanges centralizados, que se describirán más adelante. Los Exchanges Descentralizados (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 El panorama actual de las Exchanges

2.1 Insuficiencias de los Exchanges Centralizados

Los tres principales riesgos asociados con los exchanges centralizados son; 1) falta de seguridad, 2) falta de transparencia, y 3) Falta de liquidez.

La falta de seguridad generalmente surge del hecho de 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 los exchanges centralizados sean presa de hackers maliciosos. Los riesgos de seguridad y los ciberataques sufridos por los exchanges son bien conocidos [10] [11], aunque a menudo se aceptan como "table stakesâĂİ" o "mesa de riesgos", en el comercio del intercambio de tokens. Al tener bajo su custodia a más de millones de dólares en fondos de los usuarios, en sus servidores, los exchanges centralizados continúan siendo atractivos para el ataque de los hackers. Además, los desarrolladores de exchanges pueden cometer errores accidentales, honestos, con los fondos de los usuarios. Simplemente, los usuarios no tienen el control de sus tokens cuando los depositan en un exchange centralizado.

La falta de transparencia expone a los usuarios al riesgo de que los exchanges deshonestos actúen injustamente o incorrectamente. La distinción aquí se basa en las intenciones maliciosas de los operadores de los exchanges, ya que los usuarios no están realmente comerciando sus propios activos en estos exchanges centralizados, sino más bien, hacen un "reconocimiento de la deuda" (IOU). Cuando los tokens son enviados a la billetera del exchange, el exchange los pone bajo su custodia y ofrece un reconocimiento de la deuda (IOU) en su lugar. Es así como, todos los intercambios de comercio se realizan entre los pagarés-IOU de los usuarios. Para retirar, los usuarios canjean sus pagarés-IOU con el exchange, y reciben sus tokens en la dirección de su billetera externa. En este proceso hay una falta de transparencia, y el exchange 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, aun así, sin perder el total de fondos, por ejemplo, puede generar tasas de cambio más altas, retrasos en los momentos de mayor demanda, riesgos regulatorios y órdenes siendo âĂIJfront-ranâĂİ (transacciones enviadas a un bloque más rápido que el proveedor de la solución original)

Falta de liquidez. Desde el punto de vista de los operadores del exchange, la liquidez fragmentada impide la entrada de nuevos exchanges debido a la presencia de dos escenarios del "el-ganador-se-lleva-todoâĂİ". En el primero, el exchange con el mayor número de pares de divisas gana, porque a los usuarios les resulta más ventajoso realizar todos sus intercambios comerciales en un solo exchange. En el segundo, el exchange con el mayor registro de órdenes gana, debido al diferencial favorable del bid-ask (oferta-demanda) para cada uno de los pares de 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, es que muchos exchanges controlan una gran parte del mercado a pesar de las quejas de los usuarios y los incidentes sustanciales de ciberataques por hackers informáticos. Es importante subrayar que cuanto los exchanges centralizados más compren y ganen las cuotas del mercado, más expuestos están a los ataques de hackers.

Desde el punto de vista de los usuarios, la fragmentación de la liquidez reduce considerablemente la experiencia del usuario en su facilidad de uso. En un exchange centralizado, los usuarios solo pueden comerciar dentro de los grupos de liquidez de los exchanges, contra sus propios libros mayores y entre los pares de tokens que soporta. Para intercambiar el token `A` por el token `B`, los usuarios deben ir a un exchange que soporte ambos tokens o registrarse en diferentes exchanges, divulgando su información personal. Los usuarios a menudo necesitan realizar transacciones preliminares o intermedias, generalmente mediante BTC o ETH, pagando las brechas entre la oferta y la demanda en el proceso. Finalmente, los libros mayores pueden no ser lo suficientemente grandes como para completar la transacción sin una desaceleración importante. Incluso si el exchange afirma que puede manejar grandes volúmenes, no hay garantía de que 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, con un volumen significante de transacciones centralizadas en unos pocos exchanges. Las promesas de liquidez global de las blockchains no tienen ningún mérito o valor dentro de los exchanges centralizados.

2.2 Insuficiencias de los Exchanges descentralizados

Los exchanges descentralizados se diferencian de los exchanges centralizados, 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 sin confianza" de las criptomonedas, ellas mismas han mitigado con éxito muchos de los riesgos en torno a la seguridad antes mencionados. 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 las órdenes no son compartidas o propagadas dentro de una red amplia. La liquidez del limite de los libros mayores, y, específicamente, su capacidad de recuperación, cuán rápido las órdenes de

limite ejecutadas son reemplazadas por órdenes nuevas - puede afectar significantemente a las estrategias optimas de intercambio [13]. La ausencia de estos estándares ha resultado no solo 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 en cadena, los DEX heredan las limitaciones de la bloackchain subyacente, nominalmente: escalabilidad, retrasos en la ejecución (proceso de minería) y modificaciones costosas en las órdenes. Por lo tanto, el registro de órdenes de la blockchain no se escala particularmente bien, ya que la ejecución de código en la blockchain genera un costo (gas), lo que hace que las cancelaciones múltiples de órdenes sean excesivamente caras.

Finalmente, dado que los registros de las órdenes de la blockchain son públicos, la transacción para hacer una orden es visible para los mineros de criptomedas, mientras se espera que sea extraída en el bloque siguiente y colocada en libro mayor. Este retraso expone a los usuarios al riesgo de una "ejecución anticipada" (front-run) y también al riesgo de tener el precio o la ejecución en su contra.

2.3 Soluciones Híbridas

Por las razones mencionadas anteriormente, los exchanges puramente basados en blockchain tienen limitaciones que los hacen no competitivos con los exchanges centralizados. Existe un balance entre la falta de confianza característica de la en-cadena (on-chain, en inglés) y la velocidad y flexibilidad de las órdenes de exchanges centralizadas. Protocolos como los de Loopring y 0x [14] proponen una solución de liquidación de transacciones en-cadena con una gestión de órdenes fuera de línea. 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 (off-chain, en inglés) y 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, nuestro enfoque para una solución híbrida se presenta a través de este artículo.

3 El protocolo Loopring

Loopring no es un Exchange descentralizado (DEX), sino un protocolo modular para construir DEXs en múltiples blockchains. Hemos desmontado partes de los componentes principales de una exchange tradicional y hemos ofrecido un conjunto de contractos inteligentes públicos y agentes descentralizados en su lugar. Los roles en la red incluyen billeteras, relés (relays, en inglés), blockchains de consorcio para compartir liquidez, buscadores de registros de órdenes, 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 las órdenes en Loopring.

3.1 Anillo de Órdenes

Las órdenes en Loopring se expresan en lo que llamamos el Modelo de Orden Unidireccional (UDOM)[16]. La UDOM expresa órdenes como solicitudes de intercambio de token, `cantidadS`/`cantidadB`, (cantidad para vender / comprar) en lugar de las órdenes de oferta y demanda. Dado que cada orden es solo un tipo de cambio entre dos tokens, una característica importante del protocolo es la mezcla y coincidencia entre varias órdenes en un intercambio circular. Utilizando hasta 16 órdenes 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.

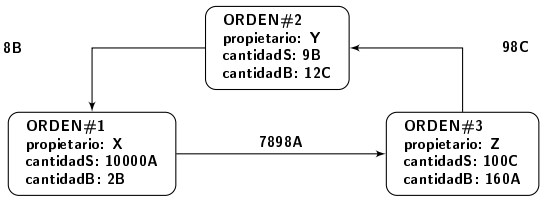

Figure 1: Un anillo de orden de 3 órdenes

La figura de arriba muestra un anillo de órdenes de 3 órdenes. El token de cada orden para vender (`tokenS`) es el token de otra orden para comprar (`tokenB`). Esto crea un bucle que permite que cada orden intercambie sus tokens deseados sin necesidad de una orden opuesta a su par. Los pares de órdenes comerciales tradicionales pueden, por supuesto, seguir ejecutándose, en lo que es esencialmente un caso especial de un anillo de órdenes.

Definition 3.1 (anillo-de-órdenes) *Deje C_0, C_1, $\cdots$, C_{n-1} ser n diferentes tokens, $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ ser n órdenes. Estas órdenes pueden formar un anillo-de-órdenes para intercambiar:*

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

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

Un anillo de órdenes es válido cuando todas las transacciones que lo componen se 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 órdenes, los contratos inteligentes del protocolo Loopring deben recibir los anillos de órdenes de los mineros y verificar que el producto de las tasas de cambio originales de todas las órdenes sea mayor o igual a 1.

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

¿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 (3.75A) que el precio por el que Bob está vendiendo sus token (3.00A), mientras que en la segunda situación Bob está dispuesto a pagar un precio más alto (0.33333334B) que el precio por el que Alice está vendiendo sus tokens (0.26666667B). 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 órdenes puedan ser llenadas y ejecutadas, total o parcialmente, necesitamos saber si el producto de cada una de las tasas de cambio como órdenes de compra resulta en un número mayor o igual a 1. Si es así, todas las órdenes n pueden estar parcialmente, o totalmente ejecutadas [17].

Si presentamos a un tercer participante, 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 las órdenes de Loopring.

4 Participantes del Ecosistema

Los siguientes participantes del ecosistema proporcionan conjuntamente todas las funcionalidades que un exchange centralizado ofrece.

- **Billeteras**: Un servicio o interfaz de la billetera que permite a los usuarios acceder a sus tokens y a enviar órdenes a la red de Loopring. Las billeteras serán incentivadas a producir órdenes al compartir pagos dentro del anillo de órdenes (ver sección 8). Con la creencia de que el futuro de la negociación tendrá lugar dentro de la seguridad de las billeteras de los usuarios individuales, la conexión de estos fondos de liquidez a través de nuestro protocolo es primordial.

- **Blockchain de consorcio para intercambio de liquidez /Malla-Relé**: una red de malla de relé (relay mesh network, en inglés) para el intercambio de órdenes & 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 consorcio que estamos construyendo como primera implementación tiene un tiempo casi real de intercambio de órdenes (bloques de 1-2 segundos), y reduce el historial antiguo para permitir a los nuevos nodos una descarga más rápida. 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 órdenes de las billeteras o de la malla de relés, mantienen un registro público de órdenes y uno de comercio, y opcionalmente emiten órdenes a otros relés (a través de cualquier medio de fuera-de-cadena arbitraria) y/o nodos de malla de retransmisión. La minería de anillo es una característica – no un requisito – de los relés. Es computacionalmente intensa y se realiza completamente fuera-de-cadena (off-chain). Llamamos a los relés con la función activada de minería de anillo "Ring-Miners", que producen anillos de órdenes al unir órdenes dispares. Los relés son libres de (1) cómo elegir comunicarse entre ellos, (2) cómo construir sus libros mayores, y (3) cómo extraer anillos de órdenes (algoritmos de minerá).

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

- **Servicios de tokenización de activos (ATS)**: 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 token 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/cross-chain (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 Exchange/Intercambio

1. **Autorización del protocolo**: En la figura 2, el usuario `Y`, quien quiere intercambiar tokens, 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 la orden.

2. **Creación de la orden**: El tipo de cambio actual y el registro de órdenes del token `B` vs token `C`, son proporcionados por relés o por otros agentes conectados a la red, como los buscadores de órdenes. El usuario `Y` hace una orden (orden con límite de precio) especificando `cantidadS` y `cantidadB` y otros parámetros a través de cualquier interface de billetera integrada. Cierta cantidad de LRx se puede agregar a la orden 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 la orden. El hash de la orden se firma con la clave privada del usuario `Y`.

3. **Transmisión de órdenes**: la billetera envía la orden y su firma a uno o más relés (relays, en inglés). Luego los relés actualizan su libro mayor público. El protocolo no requiere que los libros mayores sean construidos de una manera específica, como por ejemplo con la regla de *por orden de llegada*, 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 mayores.

4. **Distribución de liquidez**: los relés transmiten una orden a los otros relés a través del método que consideren más adecuado. De nuevo, hay flexibilidad sobre cómo interactúan los nodos. 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.

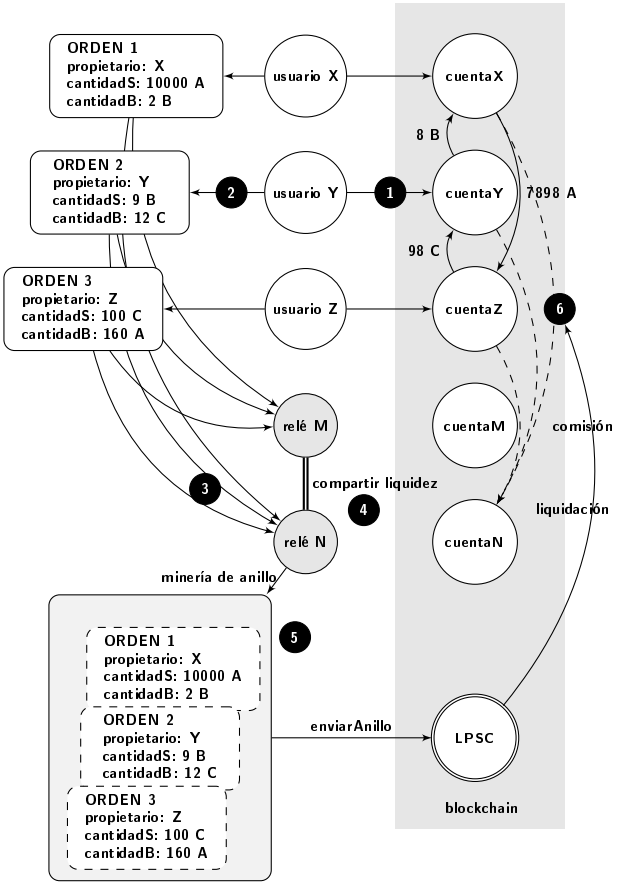

Figure 2: Proceso de Intercambio de Loopring

5. **Minería de anillo (emparejando órdenes)**: los mineros de anillo intentan ejecutar la orden total o parcialmente a un tipo de tasa de intercambio o mejor, emparejándolo con otras órdenes múltiples. La minería de anillo es la razón principal por la cual el protocolo puede proporcionar alta liquidez sobre cualquier otro par. Si la velocidad a la que se ejecuta la orden es mejor que la especificada por el usuario `Y`, el margen se comparte entre todas las órdenes 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 órdenes. Se necesitan varios controles para verificar los datos proporcionados por el minero de anillo y para determinar si el ciclo de órdenes puede completarse completamente o parcialmente (dependiendo en la tasa de ejecución de las órdenes en el anillo y los tokens en las billeteras 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 billeteras al mismo tiempo. Si los LPSC detectan la falta de fondos necesarios para el intercambio en la billetera del usuario `Y`, la orden

será reducida: una orden de escala reducida volverá automáticamente a su tamaño original si se deposita una cantidad suficiente de fondos a la dirección del usuario, a diferencia de una cancelación, que es una operación manual en un solo sentido que no se puede cancelar.

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 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 órdenes

Los relés pueden diseñar sus libros mayores en cualquier número de maneras para mostrar y hacer coincidir las órdenes de los usuarios. Una primera implementación de nuestro libro mayor sigue un modelo de venta-libre (Over The Counter - OTC, en inglés), donde las órdenes limitas se basan solo en el precio. El momento en el que se generaron las órdenes, en otras palabras, no tiene un impacto en la formación del libro mayor. Sin embargo, un relé es libre de diseñar su propio libro mayor en la manera que se pueda imitar y competir con el funcionamiento típico de los exchanges centralizados, donde las órdenes se clasifican por precio, mientras también se respeta el momento de creación de la orden. Si un relé está más inclinado a ofrecer este tipo de libro mayor, ellos pueden apropiarse/ integrarse con una billetera, y hacer que las órdenes desde esa billetera se envíen únicamente a un solo relé, que luego podrá ordenarlos 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 "órdenes tomadoras" (taker orders, en inglés) - Los relés de Looping solo necesitan encontrar órdenes que correspondan con otras 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 (órdenes) 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 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 billetera 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 una Orden

Un orden es un paquete de datos que describe la intención del usuario de intercambiar. Una orden de Loopring se define utilizando el Modelo de Orden UniDireccional, o UDOM, de la siguiente manera:

```
message Order {
  address protocol;
  address owner;
  address tokenS;
  address tokenB;
  uint256 amountS;
  uint256 amountB;
  unit256 lrcFee
  unit256 validSince; // Segundos despuÃ¯s de la Ã¯poc
  unit256 validUntil; // Segundos despuÃ¯s de la Ã¯poc
  uint8   marginSplitPercentage;  // [1-100]
  bool    buyNoMoreThanAmountB;
  uint256 walletId;
  // DirecciÃşn de Doble-AutorÃıa
  address authAddr;
  // v, r, s son parte de la firma
  uint8   v;
  bytes32 r;
  bytes32 s;
  // llave-privada de Doble-AutorÃıa
  // no utilizada para calcular el hash de la orden,
  // por lo tanto, NO estÃą firmada.
  string  authKey;
  uint256 nonce;
}
```

Para garantizar el origen de la orden, se firma contra el hash de sus parámetros, excluyendo `authAddr`, con la llave privada del usuario. El parámetro `authAddr` se utiliza para firmar los anillos de orden de los que forma parte esta orden, 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 de la orden a la red. Esto asegura que la orden permanezca inmutable a lo largo de su toda existencia. Incluso si la orden nunca cambia, el protocolo aún puede calcular su estado actual en función del balance de su dirección y otras variables.

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

un número de coma flotante, sino una expresión que será evaluada solo con otros números enteros a demanda sin firma, para mantener todos los resultados intermedios como números enteros sin firmar y para aumentar la precisión del cálculo.

7.1.1 Importes de compra

Cuando un minero de anillo coincide con un anillo de órdenes, es posible que una mejor tasa sea ejecutable, lo que permitirá a los usuarios obtener 5 veces más del `tokenB` que la `cantidadB` que ellos especificaron. Sin embargo, si el parámetro `buyNoMoreThanAmountB` se establece en `True`, el protocolo garantiza que los usuarios reciban no más de la `cantidadB` del `tokenB`. Asi, el parámetro de UDOM `buyNoMoreThantokenB` determina cuándo se debe considerar que una orden se ha cumplido por completo. `buyNoMoreThantokenB` aplica un valor máximo a la `cantidadS` o `cantidadB`, y permite a los usuarios expresar sus intenciones de intercambio de forma más detallada que las órdenes de venta y compra tradicionales.

Por ejemplo: con la `cantidadS` $= 10$ y `cantidadB` $= 2$, 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 orden en una forma simplificada, para los mercados ETH/USD en una exchange tradicional, el modelo tradicional de compra-venta puede expresar el primer y el tercer orden a continuación, pero no los otros dos:

1. Vende 10 ETH al precio de 300 USD/ETH. Esta orden de venta se expresa como: `Order(10, ETH, 3000, USD, Falso)`.
2. Vende ETH al precio de 300 USD/ETH para obtener 3000 USD. Esta orden de venta puede expresarse como: `Orden(10, ETH, 3000, USD, Verdadero)`.
3. Compre 10 ETH al precio de 300 USD/ETH. Esta de compra orden 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. Esta orden 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 hechos por los mineros de anillo esencialmente por dos razones principales: (1) el lenguaje de programación para los contratos inteligentes, como la solidez[19] en Ethereum, dno es compatible con la computación de 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 Verificacón de anillo secundario/sub-anillo

Este paso impide a los arbitrajistas la posibilidad de obtener injustamente el margen completo de un anillo de órdenes, implementando nuevas órdenes dentro de el. Básicamente, una vez que un minero identifica una orden-anillo válida, podría caer en la tentación de agregar más órdenes al mismo anillo de órdenes, 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 $y2$ ser'a posible hacer que el producto de todas las tasas de orden sea igual a 1, para cancelar cualquier tipo de cambio.

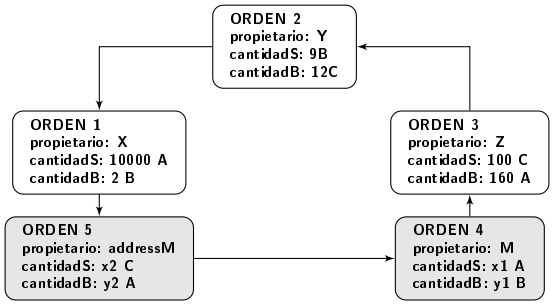

Figure 3: Una orden-anillo con un sub-anillo

Esto es de cero-riesgo, cero-valor añadido a la red, y se considera una conducta injusta para el anillo-minero. Para prevenir esto, Loopring requiere que un bucle válido no pueda contener ningún sub-anillo. 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 se permite.

7.2.2 Verificación de la tasa de ejecución

El cálculo de la tasa de cambio en la orden-anillo son realizadas por los mineros por las razones explicadas anteriormente. LPSC debe verificar que sea correcta. Primeramente, esto verifica que la tasa de compra que el minero de anillo puede realizar por cada orden que sea menor o igual a la tasa de compra original impuesta por el usuario.

Esto asegura que el usuario obtenga en la transacción al menos el tipo de cambio requerido, o algo mejor. Luego de la confirmación de las tasas de cambio, LPSC se asegura de que cada orden que compone el anillo se beneficie del mismo descuento. Por ejemplo, si la tasa de descuento es γ, el precio de cada orden 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 órdenes, 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-ésima orden. Obviamente, solo cuando el descuento es $\gamma \geq 0$, estas órdenes pueden ser completadas; y la tasa de cambio real de la orden i-ésima (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` aque 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 billeteras). (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 contienen los detalles de la orden 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 de la orden 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 orden.

Los LPSC también permiten la cancelación de una orden por cualquier par de cambio mediante el evento de `OrdersCancelled` y cancelación de todas las órdenes relacionadas con una dirección a través del evento `AllOrdersCancelled`.

7.2.4 Escalado de órdenes

Las órdenes son escaladas y actualizadas en base al historial de importes llenados/ejecutados y a los importes cancelados, así como el saldo actual de la cuenta del remitente. En base a estas características, el proceso identifica la orden con la cantidad más baja que se ejecutará y utiliza esas características como referencia para escalar todas las transacciones de la orden-anillo.

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

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

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

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

Ejemplo: si la cantidad más baja que debe ejecutarse representa el 5% de la orden original, todas las transacciones el anillo de ordenes se reducirán en un 5%. Una vez que las transacciones se completen, la orden 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 órdenes satisface todos los puntos anteriores, la orden de anillos puede ser cerrada para permitir la ejecución de las transacciones. Esto significa que todas las órdenes n formarán un ciclo cerrado, conectadas como en la figura 4:

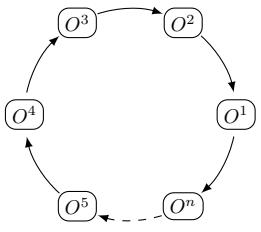

Figure 4: Liquidación del anillo

Para realizar transacciones, los LPSC usan el contrato inteligente `TokenTransferDelegate`. La introducción de un delegado de este tipo hace que sea más fácil actualizar cualquier contrato inteligente de protocolo, ya que todas las órdenes solo tendrán que autorizar a este delegado en lugar de las diferentes versiones del protocolo.

Para cada orden del anillo, el pago de `tokenS` se lleva a cabo con la orden 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 mayor de la manera más eficiente posible. Estos eventos son:

- **OrderCancelled**:Una orden específica ha sido cancelada.
- **OrdersCancelled**: Todas las órdenes de un par de intercambio de una dirección de un propietario han sido canceladas.
- **AllOrdersCancelled**: Todas las órdenes de una sola dirección han sido canceladas.
- **RingMined**: un anillo de orden ha sido resuelto con éxito. Este evento contiene datos relacionados con cada transferencia de token único dentro del anillo.

8 Token LRx

LRx es nuestra notación de token generalizada. 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 una orden, especifican una cantidad de LRx a pagar al minero como comisión, o un porcentaje del margen obtenido a través de la orden (`marginSplitPercentage`) que el minero puede solicitar. A esto se llama margen dividido. Depende del minero decidir qué opción escogerá entre comisión o margen dividido.

Aquí una representación del margen dividido:

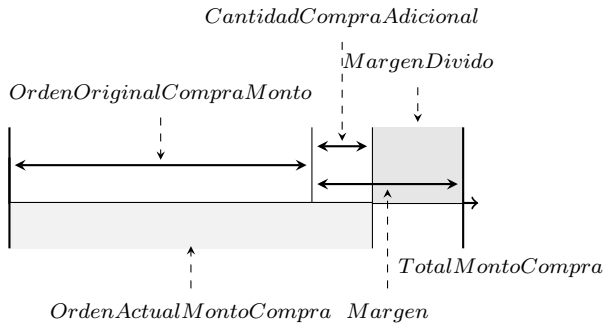

Figure 5: Un 60% de Margen Dividido

Si el margen en el anillo de la orden es demasiado bajo, el minero del anillo escogerá la comisión LRx. Si, por lo contrario, el margen es lo suficientemente sustancial para que la división del margen resultante valga mucho más que la tarifa 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 de la orden) 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 el margen dividido en dos veces la tarifa LRx de la orden, 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 órdenes de margen alto, de ahí la necesidad de incentivar una comisión fija en LRX.

Por lo tanto, obtenemos el siguiente gráfico:

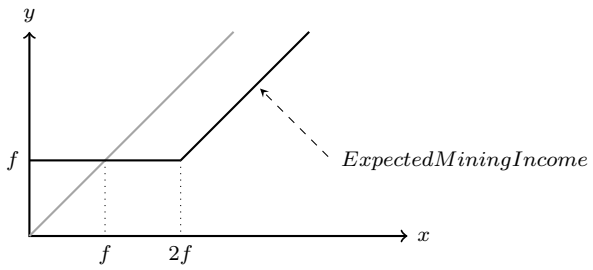

Figure 6: Loopring's Fee Model

donde f 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 la orden 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. Si el margen se divide 0, los mineros de anillos escogen la comisión fija en LRx y aún siguen siendo 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 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 de la orden. 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 los administradores de billeteras. Cuando un usuario realiza una orden a través de una billetera y esta se ejecuta, el administrador de la billetera es compensado con una parte de la comisión o la división del margen. Aunque esto es modular, y es los modelos de negocios únicos o implementación son posibles, consideramos que el porcentaje de comisiones que se debe compartir con las billeteras aproximadamente, es de 20% - 25%. Las billeteras son un objetivo clave para la implementación del protocolo Loopring, ya que tienen su propia base de usuarios, pero poco o nada de fuentes de ingresos.

8.2 Gobierno descentralizado

En su raíz, el protocolo Loopring se basa en un protocolo social, en el sentido de que depende de la coordinación de diferentes participantes para permitirles colaborar de manera eficiente hacia un objetivo 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 que 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 liquide en un ecosistema descentralizado. Los tokens LRx se usarán para efectuar actualizaciones de protocolo a través de un gobierno descentralizado. Las actualizaciones de contratos inteligentes, en parte, se regirán por propietarios de tokens (token holders) para garantizar la continuidad y la seguridad, y para mitigar los riesgos de liquidez excesiva/sifonada a través de la incompatibilidad. La capacidad de actualización es crucial para el éxito del protocolo, ya que debe adaptarse a las demandas del mercado y las blockchains subyacentes. El gobierno descentralizado de las partes interesadas de LRx permitirá 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 Fundaci'on Loopring y son asignados como fondos para la comunidad [21].

Sin embargo, los propietarios de tokens LRx no son los únicos interesados a considerar en la dirigir la dirección del protocolo: los relés/mineros de anillo, billeteras, 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 son inexistentes, las reservas de token iniciales no son obligatorias) tenemos que permitir métodos alternativos para respetar sus intereses.

Además, el voto "simple" basado en tokens, tanto en cadena como fuera de cadena, es un ungüento imperfecto para el desacuerdo, ya que la baja participación de votantes y la concentración de propiedad de tokens representan riesgos. Por lo tanto, el objetivo es implementar un modelo de gobernanza que se construido en capas y se basa 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 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 exchanges descentralizadas, la ejecución anticipada/front-running se produce cuando alguien intenta copiar la solución de intercambio de otro nodo, y la extrae (minar) en el bloque correspondiente antes de la transacción original que está esperando en el grupo de transacciones pendientes(mempool). Esta acción se puede lograr especificando una tarifa de transacción más alta (precio de gas). El principal esquema de "ejecución-frontal" (o front-running) en Loopring (y en cualquier protocolo de "(coincidencia-de-órdenesâĂİ)" es el robo de órdenes (order-filch): cuando un âĂIJcandidato favoritoâĂİ (front-runner) se roba una o más órdenes de una transacción pendiente de liquidación del anillo de órdenes; y, específica a Loopring: cuando un front-runner se roba un anillo completo de una transacción pendiente. Cuando una transacción de tipo submittRing (envío de anillo) 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 de

la orden. 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 antes encontradas para este problema tenían desventajas considerables: requerían más transacciones y, por lo tanto, aumentaban los costos de gas para los mineros; y así tomando al menos dos veces la cantidad de bloques requeridos para asegurar un anillo de órdenes. Nuestra nueva solución, "Doble autoría" (Dual Authoring) [22], está compuesta en la adopción de un mecanismo que desarrolla dos niveles de autorización para órdenes: uno para regulación y otra para minería de anillo. (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 (autorización de llave) para presentar la clave privada correspondiente a authAddr).

Proceso de doble autoría:

1. Para cada orden, el software de la billetera generará un par de llaves, llave pública/llave privada escogidas al azar, y colocará ese par de llaves en una parte de JSON de la orden (JSON, acrónimo de JavaScript Object Notation, sirve para el intercambio de datos). (Una alternativa es usar la direccinó 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` (autorización de llave) para presentar la clave privada correspondiente a `authAddr`).

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

3. La billetera envía la orden 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 de la orden sea válida con respecto a la dirección del `propietario`.

4. Cuando un anillo de orden es identificado, el minero del anillo usa cada llave de autentificación `authKey` de las órdenes para firmar el hash del anillo, dirección del minero `minerAddress`, y todos los parámetros de la minería. Si el anillo de orden contiene n órdenes, 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 órdenes si faltan cualquiera de sus firmas de `authSignature` o si es que estas son invalidas.

El resultado ahora es:

- La firma de la orden (a través de la llave privada de la dirección del `propietario`) garantiza que la orden no pueda ser modificada, 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 órdenes.

- La firma `authSignature` garantiza que no se pueda cambiar todo el anillo de órdenes, incluyendo la dirección del minero `minerAddress`, así commo ninguna orden pueda ser robada.

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

10 Otros ataques

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

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

10.2 Saldo insuficiente

Los usuarios malintencionados podrían firmar y propagar órdenes cuyo valor no sea cero, pero en caso de que la dirección de la orden tenga un saldo de cero. Los nodos podrían monitorear y darse cuenta de que el saldo de estas órdenes es cero, y simplemente actualizar el estado de estas órdenes para deshacerse de ellas. Los nodos deben de dedicar algo de tiempo en actualizar el estado de una orden, pero también pueden elegir minimizar el esfuerzo de, por ejemplo, crear una lista direcciones negras e ignorar todas las órdenes asociadas.

11 Sumario

El protocolo Loopring se propone a ser una capa fundamental para los mercados de intercambio descentralizado (descentralized Exchange). Al hacerlo, el protocolo tiene un impacto profundo en como 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 partes 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 emparejamiento de anillos 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 otras cosas. 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 de dinero.

Los principales beneficios del protocolo son:

- La gestión de órdenes fuera de cadena (off-chain) y regulaciones en cadena (on-chain), significa que no se sacrificara el rendimiento por la seguridad.
- La mejora de la liquidez mediante la extracción de anillos y el intercambio de órdenes.
- La Dual Authoring, que consta de dos niveles de autorización para las órdenes, resuelve el problema dañino de la front-running, problema que es afrontado hoy en día por todas las Exchanges Descentralizadas (DEXs) y sus usuarios.
- El precio, gratis, los contratos inteligentes públicos permiten a cualquier App descentralizada (dApp)construir o interactuar con el protocolo.
- La estandarización entre operadores permite efectos de red y una mejor experiencia para el usuario final.
- La red mantenida con flexibilidad en la ejecución de libros mayores y comunicación.
- Las barreras de entrada reducidas significan costos más bajos para los nodos que se unen a la red y para los usuarios finales.
- El comercio anónimo directamente desde las billeteras de 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. Gracias.

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.