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

1 de junio de 2018

Resumen

Loopring es un protocolo abierto para la creación de casas de cambio descentralizadas. Loopring opera como un conjunto público de contratos inteligentes responsables del intercambio y de la liquidación, con un grupo de agentes externos a la cadena de bloques añadiendo y comunicando órdenes. El protocolo es libre, extensible y sirve como un bloque de código estandarizado para aplicaciones descentralizadas (en inglés: *decentralized applications* o *dApps*) que incorporen la función de intercambio. Sus estándares interoperables facilitan el intercambio anónimo y libre de confianza en terceras partes. Una importante mejora frente a los protocolos de intercambio descentralizados actuales es su habilidad para mezclar y combinar diferentes órdenes entre sí, obviando las restricciones de uso de un único par de intercambio entre dos *tokens*, y mejorando considerablemente la liquidez. Loopring también emplea una solución única y robusta para prevenir la inversión ventajista, o *front-running*: el intento de enviar transacciones a un bloque antes que el proveedor de la solución original. Loopring es una tecnología agnóstica, por lo que puede lanzarse en cualquier cadena de bloques que admita contratos inteligentes. En el momento de redactarse este artículo, Loopring ya es operable en Ethereum [1] [2] y Qtum [3], y próximamente lo será en NEO [4].

1. Introducción

Con la proliferación de activos basados en la cadena de bloques, la necesidad de intercambiar estos activos entre contrapartes ha aumentado considerablemente. A medida que miles de *tokens* nuevos se van creando - incluyendo la conversión de activos tradicionales en *tokens* - esta necesidad seguirá aumentando. Ya sea intercambiando *tokens* por motivos especulativos, o bien digitalizando los activos para acceder a las redes mediante el uso de *tokens* de utilidad nativos, la habilidad de intercambiar un criptoactivo por otro es fundamental para el ecosistema. En efecto, hay una energía potencial en los activos [5], y hacer efectiva esta energía - desbloqueando capital - requiere no sólo reivindicar la propiedad, que es lo que las cadenas de bloque han permitido indudablemente, sino también poder transferir y transformar estos activos libremente.

Por ello, el intercambio de *tokens* (o valor) libre de confianza es un ejemplo convincente de la tecnología de la cadena de bloques. Hasta ahora, sin embargo, los entusiastas de las criptomonedas se han conformado mayormente con intercambiar *tokens* en las casas de cambio centralizadas. El protocolo Loopring es necesario porque, tal como Bitcoin enfatizó responsablemente [6] en relación al dinero electrónico entre pares (en inglés: *peer-to-peer*): "las principales ventajas se pierden si la confianza en una tercera parte es aún necesaria para evitar el doble gasto". De la misma manera, las principales ventajas de los activos descentralizados se pierden si deben ser confiados y transferidos a través de casas de cambio centralizadas.

Intercambiar *tokens* descentralizados en casas de cambio centralizadas no tiene sentido desde un punto de vista filosófico, puesto que falla en apoyar las virtudes que estos proyectos de descentralización defienden. Además, el uso de casas de cambio centralizadas presenta numerosos riesgos y limitaciones prácticas que se describen en la siguiente sección. Las casas de cambio descentralizadas (comúnmente referidas como DEX, del inglés: *decentralized exchange*) [7] [8] [9] han intentado hacer frente a estos problemas, consiguiendo en muchos casos disminuir los riesgos de seguridad mediante el uso de cadenas de bloques para la desintermediación. Sin embargo, todavía existe un margen de mejora considerable a medida que las DEX (gracias a sus capacidades) se conviertan en la infraestructura crucial para la nueva economía. Loopring, con su protocolo agnóstico y abierto para *dApps*, pretende proveer a dicha infraestructura de las herramientas modulares necesarias.

2. Panorama actual de las casas de cambio

2.1. Insuficiencias de las casas de cambio centralizadas

Los tres riesgos principales de las casas de cambio centralizadas son: 1) la falta de seguridad, 2) la falta de transparencia y 3) la falta de liquidez.

La **falta de seguridad** surge cuando los usuarios ceden el control de sus claves privadas (y por consiguiente, sus fondos) a una entidad central. Esto expone a los usuarios al riesgo de que las casas de cambio centralizadas caigan en manos de *hackers* maliciosos. Los riesgos de seguridad y *hackeo* a los que toda casa de cambio centralizada se expone son bien conocidos [10] [11], y aun así comúnmente aceptados como un "riesgo implícito" del intercambio de criptomonedas. Las casas de cambio centralizadas continúan siendo una tentación para los *hackers*, ya que sus servidores controlan millones de dólares en fondos de sus usuarios. Los desarrolladores de estas casas de cambio también pueden cometer errores accidentales y sin intencionalidad con dichos fondos. Simplemente, los usuarios no tienen el control de sus propios *tokens* cuando estos son depositados en una casa de cambio centralizada.

La **falta de transparencia** expone a los usuarios al riesgo de que las casas de cambio descentralizadas deshonestas actúen injustamente. La diferencia aquí reside en las intenciones maliciosas de los operadores de estas casas de cambio. En las casas de cambio centralizadas, los usuarios no están intercambiando sus propios activos, sino un IOU (del inglés: *I owe you*), un pagaré o instrumento de deuda informal. Cuando un *token* es enviado a la cartera virtual de una casa de cambio, esta adquiere la custodia del mismo y ofrece un IOU en su lugar. Por tanto, todos los intercambios realizados dentro de la case de cambio son, a todos los efectos, entre los IOU de los usuarios. A la hora de realizar retiros, los usuarios canjean sus IOU con la casa de cambio, y reciben sus *tokens* correspondientes en su dirección pública de monedero. Es a través de este proceso donde hay una falta de transparencia; una casa de cambio puede cerrar, congelar su cuenta, declararse en quiebra, etc. También es posible que usen los activos de los usuarios para otros propósitos mientras están en su custodia, como por ejemplo, para prestarlos a terceras partes. La falta de transparencia puede costar a los usuarios no solo una pérdida total de sus fondos, sino también impuestos de transacción más altos, retrasos durante máxima demanda, riesgo regulatorio y órdenes expuestas a inversión ventajista.

Falta de liquidez. Desde el punto de vista de los operadores de casas de cambio, la liquidez fragmentada impide la entrada de nuevas casas de cambio debido a dos escenarios de "ganador absoluto". En primer lugar, la casa de cambio con el mayor número de pares de intercambio gana, debido a que los usuarios prefieren realizar todas sus operaciones en una sola casa de cambio. En segundo lugar, la casa de cambio con el libro de órdenes más grande gana, debido a que posee una horquilla de precios (comúnmente denominado en inglés como *spread*) favorable para cada par de intercambio. Esto evita la competencia por parte de nuevas casas de cambio, debido a la dificultad para crear una liquidez inicial. Como resultado, muchas casas de cambio siguen poseyendo una cuota de mercado alta, a pesar de las quejas de sus usuarios e incluso de *hackeos* importantes ocurridos en el pasado. Merece la pena apuntar que, a medida que una casa de cambio centralizada gane cuota de mercado, esta se convertirá en un objetivo mayor para los *hackers*.

Desde el punto de vista de los usuarios, la liquidez fragmentada reduce considerablemente la experiencia del usuario. En una casa de cambio centralizada, los usuarios son capaces de comerciar únicamente dentro de los fondos de liquidez de la propia casa de cambio, con su propio libro de órdenes y entre los pares de intercambio a los que se da soporte. Para intercambiar el *token* `A` por el *token* `B`, los usuarios deben, o bien acudir a una casa de cambio que de soporte a ambos *tokens*, o bien registrarse en diferentes casas de cambio, con la consiguiente divulgación adicional de información personal. A menudo, los usuarios necesitan realizar intercambios intermedios o iniciales, normalmente en BTC o ETH, pagando la horquilla correspondiente en el proceso. Además, el libro de órdenes puede no ser lo suficientemente grande como para completar un intercambio sin realizar deslizamiento (en inglés: *slippage*). Incluso si la casa de cambio parece procesar un volumen grande, no hay garantía de que ese volumen y liquidez no sean falsos [12].

El resultado es un conjunto de silos de liquidez desconectados y un ecosistema fragmentado que se asemeja al antiguo sistema financiero, donde los volúmenes de cambio importantes se encuentran centralizados en unas pocas casas de cambio. Las promesas de liquidez global de la cadena de bloques no tienen ninguna virtud en las casas de cambio centralizadas.

2.2. Insuficiencias de las casas de cambio descentralizadas

Una de las diferencias entre las casas de cambio descentralizadas con respecto a las casas de cambio centralizadas es que los usuarios mantienen el control de sus claves privadas, y por tanto de sus activos, al realizarse los intercambios directamente en las cadenas de bloques subyacentes. Mediante el uso de la tecnología libre de confianza de las criptomonedas mismas, estas casas de cambio mitigan muchos de los riesgos de seguridad mencionados anteriormente. Sin embargo, los problemas relacionados con el rendimiento y las limitaciones estructurales todavía existen.

La liquidez sigue siendo un problema frecuente, ya que los usuarios deben buscar contrapartes a través de fondos de liquidez y estándares dispersos. Los efectos de la liquidación fragmentada estarán presentes si la mayoría de las DEX o *dApps* no se valen de estándares consistentes para operar

entre sí, o si las órdenes no se comparten/envían a través de una red lo suficientemente amplia. La liquidez de los libros de órdenes limitadas, y especialmente su resiliencia – cuán rápido se regeneran estas órdenes de precio límite – puede afectar considerablemente a las estrategias de comercio [13]. La ausencia de estos estándares ha resultado no solo en una liquidez reducida, sino también en una exposición a una variedad de contratos inteligentes potencialmente inseguros.

Además, debido a que los intercambios se realizan en la cadena, las DEX heredan las limitaciones de la cadena de bloques subyacente, a saber: escalabilidad, retrasos en la ejecución (minado), y modificaciones de órdenes costosas. Debido a ello, los libros de órdenes en las cadenas de bloques no escalan especialmente bien, ya que la ejecución de código en la cadena de bloques incurre en un coste (gas), el cual hace que el coste de una cancelación múltiple de órdenes sea prohibitivo.

Finalmente, debido a que los libros de órdenes en las cadenas de bloques son públicos, la transacción para crear una orden es visible por los mineros mientras espera a ser minada en el siguiente bloque y añadida al libro de órdenes. Este retraso expone al usuario al riesgo de sufrir una inversión ventajista que mueva el precio en contra suya.

2.3. Soluciones híbridas

Debido a las razones anteriormente expuestas, las casas de cambio basadas estrictamente en la cadena de bloques presentan limitaciones que les impiden competir con las casas de cambio centralizadas. Hay una solución intermedia entre la libre confianza inherente a la cadena de bloques y la velocidad y flexibilidad de órdenes de una casa de cambio centralizada. Protocolos como Loopring y 0x [14] ofrecen una solución intermedia de liquidación de intercambios dentro de la cadena con una gestión de órdenes fuera de la cadena. Estas soluciones giran en torno a contratos inteligentes abiertos, pero sortean ciertas limitaciones de escalabilidad ejecutando varias funciones fuera de la cadena y dando a los nodos flexibilidad en el cumplimiento de roles críticos para la red. Sin embargo, los inconvenientes de un modelo híbrido se mantienen [15]. El protocolo Loopring propone, a través de este artículo, un enfoque de una solución híbrida con mejoras significativas.

3. Protocolo Loopring

Loopring no es una DEX, sino un protocolo modular para la creación de múltiples DEX en sus respectivas cadenas de bloques. Desensamblamos las partes que componen una casa de cambio tradicional para ofrecer, en su lugar, un conjunto público de contratos inteligentes y agentes descentralizados. Sus roles y funciones en la red son diversos, entre los que se incluyen: monederos, relés, una cadena de bloques de consorcio para la compartición de liquidez, exploración del libro de órdenes, mineros de anillos, y servicios de gestión de activos mediante *tokens*. Debemos entender las órdenes de Loopring antes de definir cada uno de ellos.

3.1. Anillo de órdenes

Las órdenes de Loopring se estructuran en lo que definimos como un modelo de orden unidireccional (MOU)[16]. El MOU expresa las órdenes como peticiones de intercambio de *tokens*, a un ratio `amountS/amountB`, (cantidad a vender/comprar) en lugar de de los tradicionales precios de compra y venta (comúnmente referidos en inglés como *bids and asks*). Como cada orden es simplemente un tipo de cambio entre dos *tokens*, una característica potente del protocolo es la mezcla y combinación de múltiples órdenes en un intercambio circular. El uso de hasta 16 órdenes en lugar de un solo par de intercambio permite que haya un aumento drástico de la liquidez y la posibilidad de una mejora del tipo de cambio.

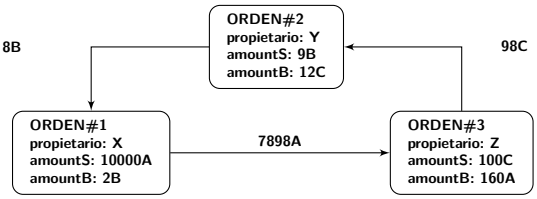

Figura 1: Un anillo compuesto de 3 órdenes

La figura anterior muestra un anillo compuesto de 3 órdenes. Cada orden de venta de `tokenS` es otra orden de compra de `tokenB`. Esto crea un bucle que permite a cada orden intercambiar los *tokens* deseados sin requerir de una orden opuesta para su par de *tokens*. Las órdenes mediante pares de intercambio tradicionales aún pueden ser realizadas en lo que sería un caso especial de anillo de órdenes formado por tan solo 2 órdenes.

Definición 3.1 (anillo de órdenes) *Dados n tokens distintos C_0, C_1, $\cdots$, C_{n-1} y n órdenes distintas $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$. Estas órdenes pueden formar un anillo de órdenes para el siguiente intercambio:*

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

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

Un anillo de órdenes es válido cuando todas las transacciones que la componen pueden realizarse a un tipo de cambio igual o mejor que el valor original especificado implícitamente por el usuario. Para verificar la validez del anillo de órdenes, los contratos inteligentes del protocolo Loopring deben recibir, por parte de los mineros, anillos de órdenes cuyo producto del tipo de cambio original de todas las órdenes sea igual o mayor que 1.

En el siguiente ejemplo supondremos que Alicia y Bob quieren intercambiar sus *tokens* `A` y `B`. Alicia tiene 15 *tokens* `A` y quiere 4 *tokens* `B` por ellos; Bob tiene 10 *tokens* `B` y quiere 30 *tokens* `A` por ellos.

¿Quién de los dos está comprando y quién está vendiendo? Esto depende únicamente del activo en que nos basemos para determinar el precio. Si el *token* `A` es la referencia, entonces Alicia está comprando el *token* `B` a un precio de $\frac{15}{4} = 3.75$`A`, mientras que Bob está vendiendo 10 *tokens* `B` a un precio de $\frac{30}{10} = 3.00$`A`. En el caso de que escojamos el *token* `B` como referencia, diremos entonces que Alicia está vendiendo 15 *tokens* `A` a un precio de $\frac{4}{15} = 0.26666667$`B` y Bob está comprando 10 *tokens* `A` a un precio de $\frac{10}{30} = 0.33333334$`B`. Distinguir entre el comprador y el vendedor es algo puramente arbitrario.

En el primer escenario, Alicia está dispuesta a pagar un precio más alto (3.75`A`) que el precio de venta de los *tokens* de Bob (3.00`A`), mientras que en el segundo escenario Bob está dispuesto a pagar un precio más alto (0.33333334`B`) que el precio de venta de los *tokens* de Alicia (0.26666667`B`). Queda claro que un intercambio es posible cuando el comprador está dispuesto a pagar un precio igual o más alto que el 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 consiguiente, para que un conjunto de n órdenes pueda ejecutarse, de manera parcial o completa, es necesario saber si el producto de cada uno de los tipos de cambio de las órdenes de compra es mayor que 1. De ser así, todas las n órdenes pueden ser ejecutadas parcial o completamente [17].

Si introducimos una tercera parte, Charlie, tal que ahora Alicia quiere dar x_1 *tokens* `A` y recibir y_1 *tokens* `B`, Bob quiere dar x_2 *tokens* `B` y recibir y_2 *tokens* `C`, y Charlie quiere dar x_3 *tokens* `C` y recibir y_3 *tokens* `A`. Existen los *tokens* necesarios, y el intercambio es posible si:

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

Véase la sección 7.1 para más detalles sobre las órdenes de Loopring.

4. Participantes del ecosistema

Los siguientes participantes del ecosistema ofrecen de manera conjunta todas las funcionalidades que una casa de cambio centralizada puede ofrecer:

- **Monederos**: Un servicio o interfaz común de monedero que permite a sus usuarios acceder a sus *tokens* y enviar órdenes a la red de Loopring. Los monederos serán incentivados por crear órdenes mediante la compartición de comisiones con los mineros de anillos (véase la sección 8). Con la creencia de que el futuro del intercambio tendrá lugar dentro de la seguridad de los monederos individuales de los usuarios, es crucial conectar estos fondos de liquidez a través de nuestro protocolo.

- **Cadena de bloques de consorcio para la compartición de liquidez/malla de relés**: Una malla de relés para la compartición de órdenes y liquidez. Cuando los nodos ejecutan el código de relé de Loopring, estos pueden unirse a redes existentes y compartir la liquidez con otros relés a través de una cadena de bloques de consorcio. Esta primera versión de la cadena de bloques de consorcio que estamos construyendo permite la compartición de órdenes casi en tiempo real (bloques de 1-2 segundos), y reduce el historial antiguo, permitiendo descargas más rápidas por parte de los nodos nuevos. Cabe destacar que los relés no necesitan unirse a este consorcio: pueden actuar de forma individual y no compartir liquidez, o bien crear y gestionar su propia red de compartición de liquidez.

- **Relés/mineros de anillos**: Los relés son nodos que reciben órdenes de los monederos o de la malla de relés, mantienen públicos los libros de órdenes e historial de intercambios, y, de manera opcional, transmiten órdenes a otros relés (vía un medio externo arbitrario) y/o mallas de relés. El minado de anillos de órdenes es una característica – no un requisito – de los relés. Esta es una aplicación computacionalmente intensiva y se realiza completamente fuera de la cadena. A los relés con la capacidad de minar estos anillos se les denomina "mineros de anillos", los cuales crean anillos mediante la unión de órdenes dispersas. Los relés tienen libertad para (1) escoger cómo comunicarse entre ellos, (2) cómo crear los libros de órdenes y (3) qué algoritmo de minado usar para minar los anillos de órdenes.

- **Contratos inteligentes del protocolo Loopring (CIPL)**: Un conjunto público y abierto de contratos inteligentes que comprueba los anillos de órdenes recibidos por los mineros, liquida las órdenes y transfiere los *tokens* en nombre de los usuarios, recompensa a los mineros y monederos con las comisiones de transacción y transmite eventos. Los relés y exploradores de órdenes prestan atención a estos eventos para mantener sus libros de órdenes e historial de intercambios actualizados.

- **Servicios de gestión de activos mediante *tokens* (SGAT)**: Una solución para aquellos activos que no pueden ser intercambiados directamente en Loopring. Estos son servicios centralizados gestionados por compañías u organizaciones de confianza. Los usuarios depositan activos (reales, dinero fíat o *tokens* de otras cadenas) y a cambio reciben *tokens* que pueden ser canjeados por su depósito original en el futuro. Loopring no es un protocolo de intercambio entre cadenas (mientras no exista una solución adecuada para ello), pero el SGAT permite el intercambio de *tokens* ERC20 (del inglés: *Ethereum Request for Comments*) [18] por activos físicos o activos digitales de otras cadenas de bloques.

5. Proceso de intercambio

1. **Autorización del protocolo**: En la figura 2, el usuario `Y`, quien quiere cambiar sus *tokens*, autoriza a los CIPL a gestionar una cantidad `amountS` de *tokens* `B` para su venta. Esta autorización no congela los *tokens* del usuario, quien sigue siendo libre de moverlos mientras la orden no se ejecute.

2. **Creación de la orden**: El tipo de cambio y el libro de órdenes para el par *token*`B`/*token*`C` es ofrecido por los relés u otros agentes conectados a la red (p. ej., los exploradores de libros de órdenes). El usuario `Y` crea una orden (de precio límite) especificando el número de *tokens* a intercambiar (`amountS` y `amountB`) junto con otros parámetros a través de la interfaz de monedero integrada. El usuario puede también añadir una cantidad de *tokens* LRx como comisión para los mineros de anillos; una comisión mayor en LRx implica una mayor probabilidad de que los mineros procesen la orden más rápidamente. El *hash* de la orden se firma con la clave privada del usuario `Y`.

3. **Envío de la orden**: El monedero envía la orden y su firma a uno o más relés, quienes actualizan su libro de órdenes público. El protocolo no requiere que estos libros estén estructurados de una manera específica, como por ejemplo, en orden de llegada. Todo lo contrario: los relés tienen el poder de tomar sus propias decisiones al construir sus libros de órdenes.

4. **Compartición de la liquidez**: Los relés transmiten la orden a otros relés a través de un medio de comunicación arbitrario. Una vez más, hay una flexibilidad en la manera de definir cómo interactúan los nodos entre sí. Existe una malla de relés fija para la compartición de liquidez dentro de la cadena de bloques de consorcio con el fin de facilitar un cierto nivel de conectividad de la red. Esta malla de relés ha sido optimizada para ser inclusiva y rápida.

5. **Minado del anillo (combinación de órdenes)**: Los mineros de anillos intentan ejecutar las órdenes (parcial o completamente) igualando o mejorando el tipo de cambio mediante la mezcla y combinación de unas órdenes con otras. El minado de anillos es la principal razón por la que el protocolo es capaz de ofrecer alta liquidez en cualquier par de intercambio. Si el tipo de cambio al que la orden se ejecuta es mejor que la que especificó el usuario `Y`, el margen es compartido entre todas las órdenes del anillo. Como recompensa, el minero del anillo puede elegir entre adjudicarse parte de ese margen y devolver la comisión por transacción en LRx al usuario, o sencillamente conservar dicha comisión en LRx.

6. **Verificación y liquidación**: El anillo de órdenes es recibido por los CIPL. Estos realizan múltiples comprobaciones para verificar los datos proporcionados por el minero del anillo y determinan si el anillo puede ser liquidado de manera parcial o completa, en función del ratio de liquidación de órdenes internas y los *tokens* disponibles en los monederos de los usuarios. Si todas las comprobaciones tienen éxito, el contrato transfiere automáticamente los *tokens* a los usuarios, cobra las comisiones a los monederos y paga al minero simultáneamente. Si el saldo del usuario `Y` calculado por los CIPL es insuficiente, la orden será catalogada como reducida: una orden reducida volverá a su estado normal cuando se depositen fondos suficientes en la dirección correspondiente, a diferencia de una cancelación, que supone una operación manual y unilateral irreversible.

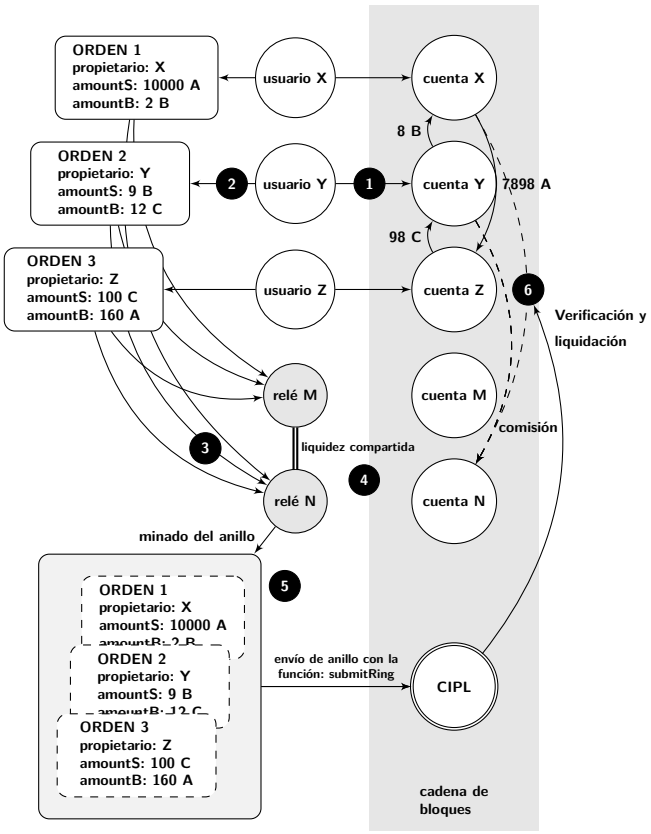

Figura 2: Proceso de intercambio con Loopring

6. Flexibilidad operacional

Cabe destacar de nuevo que el estándar abierto de Loopring ofrece a sus participantes flexibilidad a la hora de decidir cómo operar. Los agentes son libres de implementar nuevos modelos de negocios que ofrezcan valor añadido a sus usuarios, generando ingresos mediante comisiones de LRx con el volumen de cambio u otros sistemas a su elección. El ecosistema es modular, y ha sido diseñado para apoyar la participación de múltiples aplicaciones.

6.1. Libro de órdenes

Los relés pueden elegir de qué manera los libros de órdenes muestran y emparejan las órdenes de los usuarios. La primera implementación de nuestro propio libro de órdenes sigue un modelo extrabursátil u OTC (siglas del inglés *over-the-counter*), donde las órdenes de precio límite son clasificadas únicamente en función de su precio. La antigüedad de dichas órdenes (la fecha y hora de envío) no tiene ninguna relevancia en el libro de órdenes. Sin embargo, un relé tiene libertad para diseñar su libro de órdenes de una manera que imite el sistema de emparejamiento de una casa de cambio centralizada tradicional, en la cual las órdenes son clasificadas en función de su precio, pero respetando también su antigüedad. Si un relé quiere ofrecer este formato de libro de órdenes, puede colaborar/integrarse con un monedero para que envíe las órdenes únicamente a este relé, quien será capaz de emparejar las órdenes en función de la antigüedad. Cualquier configuración es posible.

Mientras que otros protocolos de DEX a veces necesitan que los relés tengan sus propios fondos - por ejemplo saldos de *tokens* iniciales para poder aceptar órdenes - los relés de Loopring únicamente necesitan encontrar órdenes que puedan combinarse o emparejarse entre sí para realizar un intercambio, y sin el requisito previo de disponer de algún *token*.

6.2. Compartición de liquidez

Los relés también tienen libertad de elegir cómo compartir la liquidez (u órdenes) unos con otros. Nuestra cadena de bloques de consorcio no es más que una de las soluciones para conseguirlo, y el ecosistema es libre de conectarse y comunicarse como desee. Además de unirse a una cadena de bloques de consorcio, los relés pueden crear y gestionar la suya propia, creando las reglas y/o recompensas que crean oportunas. También pueden optar por trabajar solos, como se ha descrito anteriormente en la implementación de monederos con funciones de antigüedad. Aunque la comunicación con otros relés y la conexión en red ofrecen ventajas evidentes, diferentes modelos de negocio con diseños interesantes de compartición de comisiones pueden presentar también sus propios méritos.

7. Especificación del protocolo

7.1. Anatomía de una orden

Una orden es un conjunto de datos que describen la intención del intercambio que el usuario quiere realizar. Una orden de Loopring se define mediante el modelo de orden unidireccional, o MOU, tal que así:

```
message Order {
  address protocol;
  address owner;
  address tokenS;
  address tokenB;
  uint256 amountS;
  uint256 amountB;
  unit256 lrcFee
  unit256 validSince; // tiempo en UNIX
  unit256 validUntil; // tiempo en UNIX
  uint8   marginSplitPercentage;  // [1-100]
  bool    buyNoMoreThanAmountB;
  uint256 walletId;
  // dirección de la autoría doble
  address authAddr;
  // v, r y s son partes de la firma
  uint8   v;
  bytes32 r;
  bytes32 s;
  // clave privada de la autoría doble,
  // no se usa para calcular el "hash" de la orden,
  // y por ello NO está firmada.
  string  authKey;
  uint256 nonce;
}
```

Para asegurar el origen de la orden, esta se firma con la clave privada del usuario y usando el *hash* de sus parámetros, excluyendo la dirección `authAddr`. El parámetro `authAddr` es utilizado para firmar los anillos que incluyan dicha orden, previniendo así una posible inversión ventajista o *front-running* (véase la sección 9.1 para más detalles). La firma está representada por los campos `v`, `r` y `s`, y es enviada junto con el resto parámetros de la órden a través de la red. Esto garantiza que la orden permanezca inmutable durante su vida. Incluso si la orden nunca es modificada, el protocolo puede todavía calcular su estado actual basado en el saldo de su dirección, junto con otras variables.

El MOU no incluye un precio (el cual debe ser representado en coma flotante por definición): en su lugar usa la variable `rate` o r, expresada como un ratio o tipo de cambio `amountS`/`amountB`. Este ratio no es un número en coma flotante, sino una expresión que solo será evaluada con otros números enteros sin firmar bajo demanda, con la finalidad de mantener todos los resultados intermedios sin firmar y así aumentar la precisión del cálculo.

7.1.1. Cantidades de compra

Cuando un minero de anillo combina las órdenes para crear un anillo, es posible que estas se puedan ejecutar a un ratio mejor, permitiendo a los usuarios obtener más `tokenB` que la cantidad `amountB` especificada. Sin embargo, si la variable `buyNoMoreThanAmountB` es fijada como `True` (verdadero en *booleano*), el protocolo se asegura de que los usuarios reciban como máximo la cantidad `amountB` de `tokenB`. De este modo, el parámetro `buyNoMoreThantokenB` del MOU establece cuándo una orden debe considerarse como ejecutada. El parámetro `buyNoMoreThantokenB` fija un límite bien en la cantidad `amountS` o la cantidad `amountB`,

y permite a los usuarios establecer intercambios más granulares que con las órdenes de compra/venta tradicionales.

Por ejemplo, con unas cantidades `amountS` = 10 y `amountB` = 2, el tipo de cambio se define como $r = 10/2 = 5$. Así, el usuario está dispuesto a vender 5 `tokenS` por cada `tokenB`. El minero del anillo consigue un tipo de cambio igual a 4 para el usuario, permitiéndole recibir 2.5 `tokenB` en lugar de 2. Sin embargo, si el usuario solo quiere 2 `tokenB` y establece el valor del parámetro `buyNoMoreThanAmountB` como `True`, los CIPL realizan el intercambio a un tipo de cambio de 4: el usuario vende 4 `tokenS` por cada `tokenB`, ahorrando así 2 `tokenS`. Este ejemplo no tiene en cuenta las comisiones por minado (véase la sección 8.1).

En efecto, si usamos

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

para representar una orden de manera simplificada, y tomando como ejemplo el par ETH/USD en las casas de cambio tradicionales; un modelo de compra/venta tradicional puede representar la primera y tercera orden que se muestran a continuación, pero no las otras dos:

1. Vender 10 ETH a un ratio de 300 USD/ETH. Esta orden puede expresarse como: `Order(10, ETH, 3000, USD, False)`.

2. Vender ETH a un ratio de 300 USD/ETH para obtener 3000 USD. Esta orden puede expresarse como: `Order(10, ETH, 3000, USD, True)`.

3. Comprar 10 ETH a un ratio de 300 USD/ETH, Esta orden puede expresarse como: `Order(3000, USD, 10, ETH, True)`.

4. Gastar 3000 USD para comprar tantos ETH como sea posible a un ratio de 300 USD/ETH, Esta orden puede expresarse como: `Order(3000, USD, 10, ETH, False)`.

7.2. Verificación del anillo

Los contratos inteligentes del protocolo Loopring no realizan cálculos de tipos de cambio o cantidades, pero deben recibir y verificar los resultados enviados por los mineros de anillos. Dichos cálculos los realizan los mineros fundamentalmente por dos razones: (1) el lenguaje de programación para los contratos inteligentes (p. ej., solidity [19] en Ethereum) no soporta matemáticas de números en coma flotante, en concreto $pow(x, 1/n)$ (calcular la raíz n de un número en coma flotante), y (2) es preferible que la computación se realice fuera de la cadena para reducir el coste computacional de la cadena de bloques.

7.2.1. Comprobación de subanillos

Este paso previene que los arbitrajistas obtengan injustamente todo el margen de un anillo de órdenes mediante la inserción de nuevas órdenes en él. Cuando un anillo de órdenes válido es encontrado por un minero de anillos, puede ser tentador añadir órdenes al anillo para absorber completamente el margen del usuario (descuento en los tipos de cambio). Tal como se ilustra a continuación en la figura 3, un cálculo meticuloso de $x1$, $y1$, $x2$ y $y2$ hará que el producto del tipo de cambio de todas las órdenes sea exactamente 1, eliminando así el descuento.

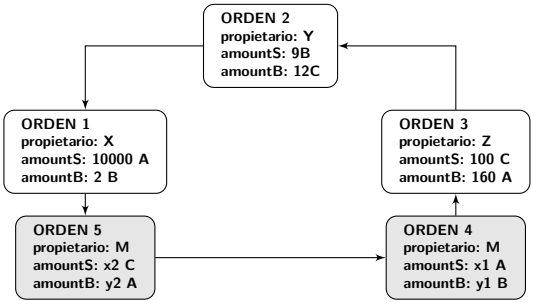

Figura 3: Un anillo de órdenes con un subanillo

Esto es una adición a la red de cero riesgo y cero valor, y se considera una conducta injusta por parte del minero del anillo. Con el fin de evitar esto, Loopring requiere que un bucle válido no contenga ningún subanillo. Para comprobar esto, los CIPL se aseguran de que un *token* no puede estar en una posición de venta o de compra dos veces. En el diagrama superior se observa que el *token* `A` está definido como *token* de compra y venta dos veces, lo cual no estaría permitido.

7.2.2. Comprobación del ratio de compleción

Los cálculos de tipo de cambio en el anillo de órdenes son realizados por los mineros debido a las razones previamente expuestas. Son los CIPL los que deben verificar que sean correctos. Primero, se verifica que el ratio de compra por el que el minero del anillo puede realizar cada orden sea igual o menor que el ratio original establecido por el usuario. Esto asegura que dicho usuario obtiene un tipo de cambio igual o mejor que el que solicitó al realizar la transacción. Una vez los tipos de cambio se han confirmado, los CIPL se aseguran de que cada orden en el anillo de órdenes comparta el mismo descuento o ahorro del tipo de cambio. Por ejemplo, si el descuento sobre el tipo de cambio es γ, entonces el precio de cada orden será:

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

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

y por tanto:

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

Si la transacción se realiza a través de n órdenes, el `discount` será:

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

donde r^i es el ratio de facturación de la i-ésima orden. Las órdenes pueden realizarse únicamente cuando el descuento es $\gamma \geq 0$; y el tipo de cambio actual de la la i-ésima orden (O^i) es $\hat{r^i} = r^i \cdot (1-\gamma)$, $\hat{r^i} \leq r^i$.

Volviendo al ejemplo anterior donde Alicia tiene 15 *tokens* `A` y quiere 4 *tokens* `B` por ellos, Bob tiene 10 *tokens* `B` y quiere 30 *tokens* `A` por ellos. Si tomamos el *token* `A` como referencia, entonces Alicia está comprando los *tokens* `B` a un precio de $\frac{15}{4} = 3.75$`A`, mientras que Bob está vendiendo los *tokens* `B` a un precio de $\frac{30}{10} = 3.00$`A`. El descuento se calcula como: $\frac{150}{120} = 1.25$, por tanto $\frac{1}{1.25} = 0.8 = (1-\gamma)^2$. Como resultado, el tipo de cambio que hace que el intercambio sea equitativo para ambas partas es $\sqrt{0.8} \cdot 3.75 \approx 3.3541$ *tokens* `A` por cada *token* `B`.

Bob da 4 *tokens* `B` y recibe 13.4164 *tokens* `A`, más de los 12 que esperaba por sus 4 *tokens*. Alice recibe 4 *tokens* `B` como estaba previsto, pero da únicamente 13.4164 *token* `A` a cambio, menos de los 15 que estaba dispuesta a dar pos esos 4 *tokens*. Cabe destacar que una porción de este margen se destinará al pago de las comisiones para incentivar a los mineros y monederos (véase la sección 8.1).

7.2.3. Seguimiento de la ejecución y cancelación

Un usuario puede cancelar parcial o completamente una orden mediante el envío de una transacción especial a los CIPL, con detalles acerca de la orden y las cantidades a cancelar. Los CIPL reciben la información, almacenan las cantidades a cancelar y transmiten un evento de cancelación (`OrderCancelled`) a la red. Los CIPL realizan un seguimiento de las cantidades completadas y canceladas mediante el almacenamiento de dichos valores usando el *hash* de la orden como identificador. Estos datos son de acceso público y los eventos `OrderCancelled` / `OrderFilled` son transmitidos cuando se produce un cambio. El seguimiento de estos valores es crítico para los CIPL durante el proceso de liquidación de un anillo de órdenes.

Los CIPL también permiten cancelar todas las órdenes para cualquier par de *tokens* con el evento `OrdersCancelled` así como la cancelación de todas las órdenes para una dirección específica con el evento `AllOrdersCancelled`.

7.2.4. Escalado de órdenes

Las órdenes son escaladas de acuerdo con el historial de cantidades canceladas y completadas y con el saldo actual de las cuentas emisoras. El proceso encuentra la orden con la menor cantidad pendiente para completar, según las características mencionadas previamente, y la usa como referencia para el escalado del resto de transacciones en el anillo de órdenes.

Encontrar la orden de menor valor puede ayudar a averiguar el volumen de ejecución para cada orden. Por ejemplo, si la i-ésima orden es la de menor valor, entonces el número de *tokens* vendidos por cada orden $\hat{s}$ y el número de *tokens* adquiridos por cada orden $\hat{b}$ puede calcularse como:

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

donde $\overline{s}_i$ es el balance restante tras la ejecución parcial de las órdenes.

Durante la implementación, podemos asumir con seguridad que, sin importar cuál es la orden en el anillo de valor más bajo, solo se debería iterar un máximo de dos veces para calcular el volumen de ejecución de cada orden.

Por ejemplo: si la cantidad más pequeña de ejecución comparada con la orden original es de un 5 %, todas las transacciones en el anillo de órdenes serán reducidas a un 5 %. Una vez las transacciones se han completado, la orden que fue definida como la de menor cantidad de ejecución pendiente debería haber sido completada.

7.3. Liquidación de un anillo

Si un anillo de órdenes pasa todas las comprobaciones previamente descritas, dicho anillo puede completar sus transacciones y ser cerrado. Esto significa que todas las n órdenes forman un anillo de órdenes cerrado, conectado como se muestra en la figura 4:

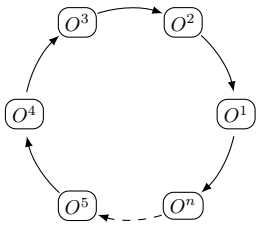

Figura 4: Liquidación de un anillo de órdenes

El contrato inteligente `TokenTransferDelegate` es usado por los CIPL para realizar las transacciones. La introducción de este delegado facilita la actualización del contrato inteligente del protocolo ya que ahora las órdenes solo necesitan autorizar a este delegado en lugar de a las diferentes versiones del protocolo.

Por cada orden en el anillo de órdenes se realiza un pago de `tokenS` bien a la orden siguiente o a la orden previa, dependiendo de la implementación. Después se paga la comisión al minero del anillo en función del modelo de comisión escogido por dicho minero. Finalmente, se transmite el evento `RingMined` una vez que todas las transacciones se han realizado.

7.3.1. Eventos transmitidos

El protocolo transmite eventos que permiten que los relés, los exploradores de órdenes y otros agentes reciban las actualizaciones del libro de órdenes de la manera más eficiente posible. Estos eventos transmitidos son:

- **OrderCancelled**: Una orden en particular ha sido cancelada.
- **OrdersCancelled**: Todas las órdenes de un par de intercambio procedentes de una dirección de propietario han sido canceladas.
- **AllOrdersCancelled**: Todas las órdenes de todos los pares de intercambio procedentes de una dirección de propietario han sido canceladas.
- **RingMined**: Un anillo de órdenes ha sido liquidado con éxito. Este evento contiene datos relacionados con cada una de las transferencia internas del anillo.

8. El *token* LRx

LRx es nuestra notación de *token* generalizada. Por consiguiente, LRC es el *token* de Loopring en Ethereum, LRQ en Qtum, LRN en NEO, etc. Otros tipos de *token* LRx serán introducidos en el futuro a medida que el protocolo Loopring sea lanzado en otras cadenas de bloques públicas.

8.1. Modelo de comisión

Cuando un usuario crea una orden, este especifica la comisión en LRx a pagar al minero del anillo, junto con el porcentaje del posible margen (`marginSplitPercentage`) que el minero puede reclamar. Esto se conoce como reparto del margen. La decisión de cuál escoger (comisión o parte del margen) corresponde al minero.

Una representación del reparto del margen sería:

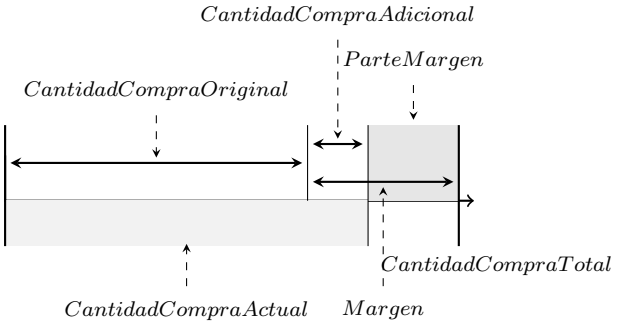

Figura 5: Un reparto del margen del 60 %

Si el margen en el anillo de órdenes es muy pequeño, el minero del anillo escogerá la comisión en LRx. Ahora bien, si el margen es lo suficientemente sustancial como para que el reparto merezca más la pena que la comisión en LRx, el minero escogerá el reparto del margen. Sin embargo, existe otra condición: cuando el minero del anillo escoge el reparto del margen, este debe pagar al usuario (creador de la orden) una comisión equivalente a los LRx que el usuario habría pagado al minero como comisión. Esto aumenta el umbral del precio por el que un minero aceptaría el reparto del margen al doble de la comisión en LRx de la orden, aumentando la tendencia a la elección de la comisión. Esto permite a los mineros de anillos recibir un ingreso constante en los anillos de órdenes con márgenes pequeños a cambio de recibir menos ingresos en los anillos de órdenes con márgenes altos. Nuestro modelo de comisiones está basado en la previsión de que a medida que el mercado crezca y madure, habrán cada vez menos anillos de órdenes con márgenes altos, y por tanto una necesidad de comisiones fijas en LRx como incentivo.

Esto lleva al siguiente gráfico:

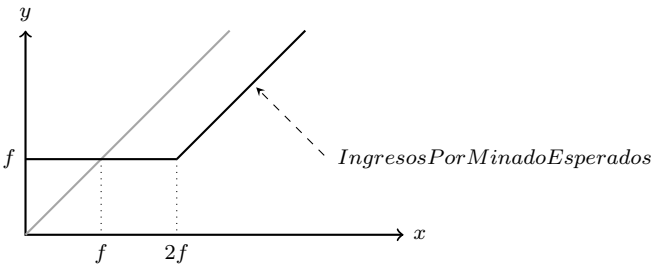

Figura 6: Modelo de comisiones de Loopring

donde f es la comisión en LRx, x es el reparto del margen e y representa los ingresos por minado. La función $y = max(f, x - f)$ está indicada con una línea continua; si la comisión en LRx para esta orden es 0, la función se convierte en $y = max(0, x - 0)$ que se reduce a $y = x$, tal como se indica en la línea gris.

Las consecuencias son:

1. Si el reparto del margen es 0, los mineros de anillos escogerán la comisión fija en LRx para seguir siendo incentivados.
2. Si la comisión fija en LRx es 0, la línea gris se cumple y los ingresos de los mineros de anillos estarán basados en un modelo lineal.
3. Cuando el ingreso por reparto del margen sea mayor que *2x(comisión en LRx)*, los mineros de anillos escogerán el reparto del margen y pagarán al usuario en LRx.

Cabe mencionar que si la comisión en LRx no es nula, siempre habrá una transferencia de LRx entre el minero del anillo y el emisor de la orden, independientemente de la opción que escoja el minero del anillo. O bien el minero obtiene su comisión en LRx, o bien paga la comisión en LRx de vuelta al emisor para obtener el reparto del margen en su lugar.

Los mineros de anillos compartirán cierto porcentaje de las comisiones con los monederos. Cuando un usuario coloca

una orden a través de un monedero y esta se completa, el monedero es recompensado con una porción de las comisiones o del reparto del margen. Aunque esto es modular, y otros modelos de negocio o implementaciones únicas son posibles, nos decantamos por que los monederos reciban aproximadamente entre un 20 %-25 % de las comisiones obtenidas. Los monederos representan un objetivo primordial para la integración del protocolo Loopring, ya que son la base de los usuarios, pero tienen poca o ninguna fuente de ingresos.

8.2. Gobernanza descentralizada

En su esencia, el protocolo Loopring es un protocolo social en el sentido de que necesita de la cooperación y coordinación de sus miembros para operar efectivamente hacia un objetivo. Esto no es diferente de los protocolos criptoeconómicos en su conjunto, ya que su utilidad está protegida mayormente por los mismos mecanismos de coordinación de problemas [20], equilibrio de la estrategia del gatillo y racionalidad limitada. Con este fin, los *tokens* LRx no se usan únicamente para pagar comisiones, sino también para alinear los incentivos financieros de los diferentes participantes de la red. Dicho alineamiento es necesario para que cualquier protocolo consiga una mayor adopción, pero es particularmente crucial para un protocolo de intercambio, dado que su éxito depende mayormente de que se mejore la liquidez en un ecosistema descentralizado robusto.

Los *tokens* LRx serán usados para realizar actualizaciones del protocolo a través de la gobernanza descentralizada. Los contratos inteligentes serán, en parte, gobernados por los poseedores de *tokens* para ofrecer continuidad y seguridad, y atenuar los riesgos de desvío de liquidez a causa de incompatibilidades. Debido a que los contratos inteligentes no pueden ser alterados una vez han sido lanzados, hay un riesgo de que las *dApps* o los usuarios finales continúen interactuando con versiones obsoletas y se excluyan a sí mismos de los contratos actualizados. La mejorabilidad es crucial para el éxito del protocolo, ya que debe adaptarse a las demandas del mercado y a las cadenas de bloques subyacentes. La gobernanza descentralizada por parte de los depositarios de LRx permitirá las actualizaciones de los contratos inteligentes sin perturbar a las *dApps* o a los usuarios finales, o sin confiar excesivamente en la abstracción de los contratos inteligentes. Los *tokens* LRx tendrán un suministro fijo, y en el caso de LRC, un porcentaje está congelado por parte de la fundación Loopring para fondos orientados a la comunidad [21].

Sin embargo, los poseedores de *tokens* LRx no son los únicos a considerar para manejar la dirección del protocolo: relés/mineros de anillos, monederos, desarrolladores y demás son una parte integral del ecosistema, y su voz debe ser oída. De hecho, dado que estos agentes no necesitan conservar ningún LRx para realizar sus respectivas funciones (las reservas iniciales de *tokens* no son obligatorias, debido a que los creadores o sostenedores de mercado tradicionales no existen) debemos permitir métodos alternativos para que sus intereses también puedan ser respetados. Es más, un sistema de voto "simple" basado en *tokens*, fuera y dentro de la cadena, es un bálsamo imperfecto para el desacuerdo, ya que una baja participación de votantes o una baja concentración de depositarios presenta riesgos. Por consiguiente, el objetivo es implementar un modelo de gobernanza que esté construido en capas, y descanse en un convencimiento común de que la norma ha de ser un proceso de toma de decisiones. Esto puede ser facilitado por instituciones de coordinación que ofrezcan avisos de distintos tipos de participantes, y quizá de puntos principales del protocolo ya preestablecidos. A medida que esto florezca, la función de la fundación Loopring como tal evolucionará de desarrolladora del protocolo a delegada del protocolo.

9. Protecciones contra fraude y ataque

9.1. Prevención de la inversión ventajista

En las casas de cambio descentralizadas, la inversión ventajista ocurre cuando alguien intenta copiar la solución de intercambio de otro nodo y que esta sea minada antes que la transacción original que se encuentra pendiente en el fondo de transacciones o *mempool*). Esto se puede conseguir especificando una comisión de transacción mayor (precio del gas). El método principal de inversión ventajista en Loopring (y cualquier otro protocolo que realiza emparejamiento de órdenes) es el hurto de órdenes (del inglés: *order-filch*): cuando un inversor ventajista roba una o más órdenes de un anillo de órdenes pendiente de liquidación; en particular para Loopring: cuando un inversor ventajista roba un anillo de órdenes entero de una transacción pendiente.

Cuando una transacción `submitRing` no está confirmada y se encuentra todavía en el fondo de transacciones pendientes, cualquiera puede identificarla fácilmente y reemplazar la dirección `minerAddress` con su propia dirección (definida como `filcherAddress`), para entonces firmar de nuevo el contenido de la transacción con `filcherAddress`, reemplazando así la firma del anillo de órdenes. El ladrón puede fijar un precio de gas mayor y enviar una nueva transacción a la espera de que los mineros de anillos escojan su transacción para el siguiente bloque en lugar de la transacción `submitRing` original.

Las soluciones usadas hasta ahora presentaban importantes desventajas: requerían de más transacciones y por consiguiente costaban más gas a los mineros de anillos; costando también el doble de tiempo liquidar un anillo de órdenes. Nuestra nueva solución, la autoría doble [22], supone configurar dos niveles de autorización para las órdenes - una para su liquidación y otra para el minado del anillo.

El proceso de autoría doble se describe a continuación:

1. El programa del monedero generará una pareja de clave pública/privada aleatoria para cada orden, y añadirá esta pareja al *snippet* JSON de la orden. Un método

alternativo consiste en reemplazar la clave pública con una dirección derivada de la misma para reducir el número de bits. En este caso, usamos `authAddr` para representar dicha dirección, y `authKey` para representar la correspondiente clave privada `authAddr`.

2. Se calcula el *hash* de la orden con todos sus campos (exceptuando `r`, `v`, `s`, y `authKey`), y se firma el *hash* usando la clave privada del propietario (`owner`) y no la clave `authKey`.

3. El monedero enviará la orden junto con la clave `authKey` a los relés para el minado del anillo. Los mineros verificarán que `authKey` y `authAddr` están correctamente emparejadas y que la firma de la orden es válida con respecto a la dirección del `owner`.

4. Cuando un anillo de órdenes es identificado, el minero del anillo usará las claves `authKey` de cada una de las órdenes para firmar el *hash* del anillo, la dirección `minerAddress` y todos los parámetros de minado. Si un anillo de órdenes contiene n órdenes, habrán n firmas con sus respectivas n claves `authKey`. Estas firmas son denominadas `authSignature`. El minero del anillo también puede necesitar firmar el *hash* del anillo junto con todos los parámetros de minado usando la clave privada de su dirección `minerAddress`.

5. El minero del anillo invoca la función `submitRing` con todos sus parámetros, así como las firmas `authSignature` extras. Fíjese que las claves `authKey` NO son parte de la transacción interna de la cadena y por tanto permanecen desconocidas para el resto de las partes a excepción del minero del anillo.

6. El protocolo Loopring ahora comparará cada firma `authSignature` con su correspondiente dirección `authAddr` para cada orden, y rechazará el anillo de órdenes si falta cualquiera de estas firmas `authSignature` o alguna de ellas es inválida.

El resultado ahora es que:

- La firma de la orden (con la clave privada de la dirección del `owner`) garantiza que la orden no pueda ser modificada, incluyendo la dirección `authAddr`.

- La firma del minero del anillo (con la clave privada de la dirección `minerAddress`), de ser proporcionada, garantiza que nadie pueda usar su identidad para minar un anillo de órdenes.

- La firma `authSignature` garantiza que el anillo de órdenes no pueda ser modificado, incluyendo la dirección `minerAddress`, y que ninguna orden pueda ser robada.

La autoría doble previene el hurto de anillos y órdenes a la vez que asegura que la liquidación de anillos de órdenes pueda hacerse en una sola transacción. Además, la autoría doble ofrece la posibilidad de que los relés puedan compartir órdenes de dos maneras: mediante compartición equitativa o inicua. Por defecto, Loopring opera como un modelo extrabursátil y únicamente soporta órdenes de precio límite, lo que significa que la antigüedad de las órdenes es ignorada. Esto implica que realizar una inversión ventajista a una orden no tendrá un impacto en el precio real de la misma, pero sí que influirá en su ejecución.

10. Otros ataques

10.1. Ataque Sybil o DOS

Los usuarios maliciosos – actuando como ellos mismos o con identidades falsas – podrían enviar una gran cantidad de órdenes pequeñas con el fin de atacar a los nodos de Loopring. Sin embargo, ya que se permite a los nodos rechazar órdenes según su propio criterio – el cual pueden ocultar o revelar – la mayoría de estas órdenes serían rechazadas por no dar suficiente beneficio cuando sean emparejadas. No apreciamos una amenaza en este tipo de ataques facultando a los relés para decidir como manejan sus órdenes.

10.2. Saldo insuficiente

Los usuarios maliciosos podrían firmar y difundir órdenes cuyo valor no sea nulo, pero cuyo saldo en la dirección de monedero sí sea cero. Los nodos podrían observar y darse cuenta de que el balance actual de algunas órdenes es cero, actualizar el estado de dichas órdenes y descartarlas. Los nodos han de gastar tiempo para actualizar el estado de una orden, pero también pueden minimizar el esfuerzo, por ejemplo, con la creación de listas negras de direcciones, cancelando órdenes vinculadas a estas.

11. Conclusiones

El protocolo Loopring tiene la intención de ser una capa fundamental para el intercambio descentralizado. Conseguir esto tendrá unas repercusiones profundas en la manera que las personas intercambiarán activos y valores. El dinero, como una mercancía intermedia, facilita o reemplaza las casas de trueque y resuelve la doble coincidencia de deseos [23] (del inglés: *double coincidence of wants*), donde dos contrapartes deben desear exactamente el bien o servicio del otro. De manera similar, el protocolo Loopring pretende eliminar nuestra dependencia de la coincidencia de deseos en los pares de intercambio mediante el uso de los anillos de órdenes para consumar los intercambios de manera más fácil. Esto es significativo por cómo la sociedad y los mercados intercambian *tokens*, activos tradicionales y más. De hecho, de la misma manera que las criptomonedas descentralizadas suponen una amenaza para el control de una nación sobre el dinero, un protocolo combinatorio que pueda emparejar

agentes (consumidores/productores) a escala es una amenaza teórica para el concepto de dinero en sí mismo.

Entre las ventajas del protocolo se incluyen:

- No se sacrifica rendimiento a costa de seguridad, ya que las órdenes se gestionan fuera de la cadena y la liquidación se realiza dentro de la misma.
- Mayor liquidez debido al minado de anillos y a la compartición de órdenes.
- La autoría doble resuelve el problema dañino de la inversión ventajista al que se enfrentan hoy en día las DEX y sus usuarios.
- Contratos inteligentes libres y públicos, que permiten a cualquier *dApp* construir o interactuar con el protocolo.
- La estandarización entre operadores, lo cual permite mejoras en la red y la experiencia final de usuario
- Mantenimiento de una red flexible con respecto a la creación de libros de órdenes y a la comunicación.
- Barreras reducidas de entrada, que suponen menores costes de acceso a la red para los nodos y los usuarios finales.
- Intercambio anónimo directo desde los monederos de los usuarios.

12. Agradecimientos

Nos gustaría expresar nuestra gratitud a nuestros mentores, consejeros y a todas aquellas personas de la comunidad que han sido enormemente acogedoras y generosas a la hora de compartir sus conocimientos. En particular nos gustaría agradecer a: Shuo Bai (de ChinaLedger), el 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 Encephalo Path por revisar y aportar sus valoraciones a este proyecto.

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, bitcoin's 460 dollar million disaster. 2014.

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

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

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

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

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

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

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

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

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

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

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

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