Loopring:
Giao thức trao đổi Token phân tán

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

Ngày 27 tháng 4 năm 2018

Tóm tắt nội dung

Loopring là một giao thức mở cho việc xây dựng các giao dịch phi tập trung. Loopring hoạt động như một tập hợp công khai của các hợp đồng thông minh có trách nhiệm trao đổi và thanh toán, cùng với một nhóm off-chain tổng hợp và truyền đạt các trao đổi. Giao thức này là miễn phí, có khả năng mở rộng và phục vụ như một khối xây dựng được chuẩn hóa cho các ứng dụng phân cấp (dApps) kết hợp chức năng trao đổi. Các tiêu chuẩn tương thích của nó giúp trao đổi thuận tiện cho giao dịch ẩn danh và không cần đặt niềm tin vào bất kỳ ai. Một cải tiến quan trọng đối với các giao thức trao đổi phân quyền hiện nay là khả năng làm cho các lệnh có thể trộn lẫn và trùng khớp với các lệnh khác, các lệnh không giống nhau, loại bỏ các ràng buộc của các cặp giao dịch hai token và cải thiện đáng kể khả năng thanh khoản. Loopring cũng sử dụng một giải pháp độc đáo và mạnh mẽ để ngăn chặn lỗi front-running: là một nỗ lực không công bằng để gửi các giao dịch thành một khối nhanh hơn nhà cung cấp giải pháp ban đầu. Loopring là một chuỗi khối bất khả tri, và có thể triển khai trên bất kỳ chuỗi khối nào với chức năng hợp đồng thông minh. Vào thời điểm viết, nó hoạt động trên Ethereum [1] [2] và Qtum [3] với NEO [4] đang được xây dựng.

1 Giới thiệu

Với sự gia tăng của các loại hình tài sản trên chuỗi khối blockchain, nhu cầu trao đổi tài sản giữa những cá thể hay tổ chức đã tăng lên đáng kể. Khi hàng ngàn tiền mã hóa mới được giới thiệu - bao gồm cả việc mã hóa các tài sản truyền thống - nhu cầu này được mở rộng. Cho dù trao đổi các loại tiền mã hóa để thúc đẩy đầu cơ thương mại, hay chuyển đổi để truy cập mạng thông qua các các loại tiền mã hóa tiện ích bản địa, khả năng trao đổi một tài sản mã hóa cho khác là nền tảng cho các hệ sinh thái lớn hơn. Thật vậy, có một sức mạnh tiềm năng trong tài sản [5], và nhận thức sức mạnh này - mở vốn - đòi hỏi không chỉ xác nhận quyền sở hữu mà blockchains đã được phép cho phép, mà còn là khả năng tự do chuyển đổi và biến đổi các tài sản này. Như vậy, trao đổi tiền mật mã mà không cần đặt niềm tin vào bất kỳ ai là một điểm khai phá cho công nghệ blockchain. Cho đến bây giờ, những người đam mê Crypto đã giải quyết phần lớn việc giao dịch tiền mã hóa trên các sàn giao dịch tập trung truyền thống. Cần phải có giao thức Loopring bởi vì cũng giống như Bitcoin [6] đã nhấn

mạnh một cách nghiêm túc rằng, đối với tiền điện tử peer-to-peer, "những lợi ích chính sẽ mất nếu một bên thứ ba đáng tin cậy vẫn phải ngăn ngừa việc chi tiêu gấp đôi" cũng là những lợi ích chính của tài sản phi tập trung bị mất nếu họ phải vượt qua các sàn giao dịch tập trung. Giao dịch các loại tiền mã hóa phân quyền trên các sàn giao dịch tập trung không có ý nghĩa từ quan điểm triết học, vì nó không giữ được các phẩm chất mà các dự án phi tập trung này tán thành. Có nhiều rủi ro thực tế và hạn chế trong việc sử dụng các sàn giao dịch tập trung được mô tả dưới đây. Các sàn giao dịch phi tập trung (DEXs) [7] [8] [9] đã tìm cách giải quyết những vấn đề này, và nhiều trường hợp đã thành công trong việc làm giảm các nguy cơ bảo mật bằng việc sử dụng các chuỗi khối để cắt giảm trung gian. Tuy nhiên, khi DEX trở thành cơ sở hạ tầng quan trọng cho nền kinh tế mới, sẽ có nhiều cải thiện hiệu suất. Loopring nhắm tới mục tiêu cung cấp các công cụ mô đun cho cơ sở hạ tầng nói với giao thức mở không đồng thuận dApp của nó.

2 Tổng quan giao dịch hiện nay

2.1 Các bất cập của các sàn giao dịch tập trung

Ba rủi ro chính của các cuộc sàn giao dịch tập trung là; 1) Thiếu bảo mật, 2) Thiếu sự minh bạch, và 3) Thiếu thanh khoản. Thiếu an toàn phát sinh từ việc người dùng thường từ bỏ sự kiểm soát các mã khóa của họ (quỹ) cho một thực thể tập trung. Điều này dẫn tới người dùng có thể bị mất tài sản nếu sàn tập trung đó bị hack. Các rủi ro về an ninh và hack phải đối mặt với tất cả các sàn giao dịch tập trung được biết đến [10] [11], nhưng thường được chấp nhận như là "bảng stakes" cho việc giao dịch tiền mã hóa. Các sàn giao dịch tập trung tiếp tục trở thành cơ chế honeypots cho các hacker tấn công vì các máy chủ của họ có quyền giám sát hàng triệu đô la của các quỹ người dùng. Các nhà phát triển giao dịch cũng có thể đưa ra các lỗi sai số không trung thực, vô tình với các khoản tiền của người sử dụng. Đơn giản là người dùng không kiểm soát các thẻ mã hoá của riêng mình khi gửi vào một sàn giao dịch tập trung. Thiếu Minh bạch sẽ làm cho người dùng gặp nguy cơ giao dịch không trung thực diễn ra một cách không công bằng. Sự khác biệt ở đây là do thiếu minh bạch của các nhà điều hành sàn giao dịch vì người dùng không thực sự buôn bán tài sản của họ trên các sàn giao dịch tập trung, mà là một IOU. Khi các Token được gửi đến ví của sàn, sàn đó sẽ tạm giữ và cung cấp một IOU ở vị trí của nó. Tất cả các giao dịch sau đó sẽ diễn ra giữa các IOU của người dùng. Để rút tiền, người dùng sẽ sử dụng IOU của họ với sàn giao dịch, và nhận Token của họ vào địa chỉ ví ngoại lệ của họ. Trong suốt quá trình này, có thể thiếu sự minh bạch và việc trao đổi có thể hủy, đóng băng tài khoản, phá sản ...; Họ có thể sử dụng tài sản của người dùng cho các mục đích khác trong thời gian lưu ký, như cho vay đối với bên thứ ba. Sự thiếu minh bạch có thể làm tăng chi phí cho người sử dụng, chẳng hạn như chi phí giao dịch cao hơn, sự chậm trễ khi có nhu cầu cao điểm, rủi ro về luật lệ và các lệnh đang chạy phía trước. Thiếu thanh khoản. Từ quan điểm của các nhà quản lý sàn giao dịch, tính thanh khoản bị phân mảnh cản trở việc lối vào bằng các sàn giao dịch mới vì hai kịch bản thắng-lấy-tất cả. Thứ nhất, giao dịch với số lượng lớn nhất của cặp giao dịch chiến thắng, bởi vì người dùng nhận thấy nó mong muốn để thực hiện tất cả các giao dịch của họ trên một sàn giao dịch. Thứ hai, việc trao đổi với bảng đấu giá Order Book lớn nhất sẽ thắng, bởi vì hoạt động trả giá-đặt giá mở rộng cho mỗi cặp giao dịch. Điều này không khuyến khích sự cạnh tranh từ những người mới đến bởi vì họ rất khó khăn trong việc xây dựng thanh khoản ban đầu. Kết quả là nhiều cuộc giao dịch đòi hỏi thị phần cao mặc dù có sự phàn nàn của người dùng và thậm chí các sự cố về hacker. Cần lưu ý rằng khi các sàn tập trung giành chiến thắng về thị phần, chúng trở thành một mục tiêu hacking lớn hơn bao giờ hết. Từ quan điểm của người dùng, tính thanh khoản bị phân mảnh làm giảm đáng kể trải nghiệm người dùng. Trong một sàn giao dịch tập trung, người dùng chỉ có thể giao dịch trong phạm vi tài sản thanh khoản của chính sàn đó, chống lại với bảng đấu giá của mình và giữa các cặp Token được hỗ trợ. Để trao đổi Token A cho token B, người dùng

phải đi đến một sàn giao dịch hỗ trợ cả hai Token hoặc đăng ký tại cácsàn giao dịch khác nhau, dẫn tới tiết lộ thông tin cá nhân. Người dùng thường phải thực hiện các giao dịch sơ bộ hoặc trung gian, thường là sử dụng BTC hoặc ETH, dẫn tới mất phí trả giá hay đặt giá mong muốn bán. Cuối cùng, các bảng đấu giá có thể không đủ sâu để hoàn thành giao dịch mà không có sự trượt giá hữu hình. Ngay cả khi sàn giao dịch có mục đích xử lý khối lượng lớn, không có đảm bảo rằng khối lượng và thanh khoản không phải là giả mạo [12]. Kết quả là tình trạng thanh khoản bị ngắt kết nối và một hệ sinh thái bị phân mảnh tương tự như hệ thống tài chính kế thừa, với khối lượng giao dịch đáng kể được tập trung ở một vài giao dịch. Các cam kết thanh khoản toàn cầu của các chuỗi khối không có giá trị trong các trao đổi tập trung.

2.2 Các bất cập của các sàn giao dịch phi tập trung

Các sàn giao dịch phi tập trung khác với các sàn giao dịch tập trung một phần bởi vì người dùng duy trì quyền kiểm soát các mã khóa cá nhân Prive-key (tài sản) bằng cách thực hiện giao dịch trực tiếp trên nền tảng blockchain. Bằng cách tận dụng công nghệ Trustless (không cần đặt tin tưởng vào bất kỳ ai) của chính mình, họ thành công trong việc giảm thiểu nhiều rủi ro về bảo mật. Tuy nhiên, vẫn tồn tại vấn đề liên quan đến hiệu suất và những hạn chế cơ cấu. Tính thanh khoản thường là một vấn đề vì người dùng phải tìm kiếm các đối tác thông qua các nguồn và tiêu chuẩn thanh khoản khác nhau. Các hiệu ứng thanh khoản bị phân mảnh hiện diện nếu DEXs hoặc dApps nói chung không sử dụng các tiêu chuẩn nhất quán để tương tác, và nếu các lệnh không được chia sẻ / tuyên truyền qua một mạng lưới rộng. Tính thanh khoản của các sổ cái giới hạn, và cụ thể là khả năng phục hồi của chúng - các lệnh giới hạn đã được làm mới nhanh chóng - có thể ảnh hưởng lớn đến các chiến lược kinh doanh tối ưu [13]. Sự vắng mặt của các tiêu chuẩn như vậy đã không chỉ dẫn đến việc giảm thanh khoản, mà còn liên quan đến một loạt hợp đồng thông minh độc quyền không an toàn. Hơn nữa, kể từ khi các giao dịch được thực hiện trên chuỗi, DEX thừa kế các hạn chế của nền tảng blockchain, cụ thể là: khả năng mở rộng, sự chậm trễ trong thực hiện (khai thác mỏ), và các sửa đổi tốn kém cho các lệnh. Do đó, bảng đấu giá chuỗi khối không tỷ lệ tốt, vì thực hiện mã trên chuỗi khối phải chịu một chi phí (gas), làm cho việc hủy các lệnh dẫn tới nhiều tốn kém. Cuối cùng, bởi vì các lệnh mua bán là công khai, việc giao dịch để đặt một lệnh mua bán có thể được nhìn thấy bởi các thợ mỏ vì nó đang chờ được khai thác vào khối kế tiếp và được đặt vào một bảng đấu giá. Sự chậm trễ này làm cho người sử dụng gặp nguy cơ chạy trước và các bước thực thi hay giá chống lại anh ta.

2.3 Giải pháp Lai

Vì những lý do trên, các sàn giao dịch thuần túy dựa trên blockchain có những hạn chế làm cho chúng không cạnh tranh với các sàn tập trung. Có một sự cân bằng giữa sự on-chain thuộc về tính không cần đặt tin tưởng vào ai, và tốc độ trao đổi tập trung và sự linh hoạt của lệnh. Các giao thức như Loopring và 0x [14] mở rộng một giải pháp giải quyết on-chain với quản lý các lệnh bằng off-chain: giải pháp mở rộng không trực tiếp trên blockchain. Các giải pháp này xoay quanh các hợp đồng thông minh mở, nhưng điều chỉnh các hạn chế về khả năng mở rộng bằng cách thực hiện một số chức năng off-chain và cho phép các nút linh hoạt trong việc thực hiện các vai trò quan trọng cho mạng. Tuy nhiên, vẫn còn những hạn chế đối với mô hình lai [15]. Giao thức Loopring đề xuất những khác biệt có ý nghĩa trong cách tiếp cận của chúng ta đối với một giải pháp lai trong trang này.

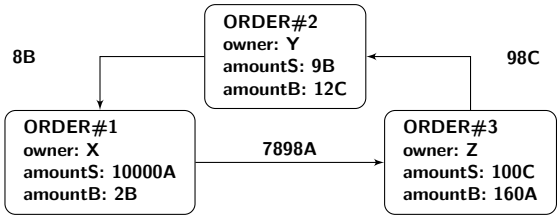
3 Giao thức Loopring

Loopring không phải là một sàn giao dịch phân tán, nhưng là một giao thức mô đun để xây dựng các sàn giao dịch phân tán trên nhiều nền tảng blockchains. Chúng tôi tháo rời các bộ phận cấu thành của một sàn giao dịch truyền thống và đưa ra một bộ hợp đồng thông minh công khai và các bên phân quyền ở vị trí của nó. Các vai trò trong mạng bao gồm ví, rơle, chuỗi khối hiệp hội chia sẻ thanh khoản, các trình duyệt bảng đấu giá, Vòng Thợ đào Ring-

Miners, và các dịch vụ mã hóa tài sản. Trước khi xác định mỗi vai trò, trước tiên cần hiểu các lệnh Loopring.

3.1 Vòng lệnh

Các lệnh của Loopring được thể hiện trong những gì chúng tôi gọi là Mô hình lệnh một hướng (UDOM) [16]. UDOM thể hiện các lệnh như các yêu cầu trao đổi Token, số lượng S / số lượng B, (sô lượng để bán / mua) thay vì đặt giá và đấu giá. Vì mỗi lệnh mua bán chỉ là một tỷ giá hối đoái giữa hai token, một tính năng mạnh mẽ của giao thức là việc trộn và kết hợp nhiều lệnh mua bán trong giao dịch tròn. Bằng cách sử dụng tối đa 16 lệnh thay vì một cặp giao dịch đơn, sẽ có sự gia tăng về tính thanh khoản và sự cải thiện về giá.



Hình 1: Một Vòng lệnh của 3 lệnh

Hình trên cho thấy một vòng lệnh gồm 3 lệnh mua bán. Mỗi token của lệnh bán (tokenS) là token của lệnh khác để mua (tokenB). Nó tạo ra một vòng lặp cho phép mỗi thứ tự để trao đổi các token mong muốn của họ mà không cần một lệnh đối lập cho cặp của nó. Các giao dịch cặp lệnh truyền thống có thể thực hiện được, chủ yếu là một trường hợp đặc biệt của một vòng lệnh.

Định nghĩa 3.1 (vòng lệnh) *để* C_0, C_1, $\cdots$, C_{n-1} *thành n token khác nhau,* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ *thành n lệnh. Các lệnh đó có thể biểu diễn một vòng lệnh cho giao dịch.*

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

với n là độ dài của vòng lệnh, và $i \oplus 1 \equiv i + 1 \mod n$.

Một vòng lệnh có giá trị khi tất cả các giao dịch thành phần có thể được thực hiện với tỷ giá hối đoái bằng hoặc tốt hơn so với tỷ lệ ban đầu được ngầm định bởi người sử dụng. Để xác minh tính hiệu lực của vòng lệnh, các hợp đồng thông minh với giao thức Loopring phải nhận được các vòng lệnh từ người khai thác vòng, nơi sản phẩm của tỷ giá hối đoái ban đầu của tất cả các lệnh bằng hoặc lớn hơn 1.

Giả sử Alice và Bob muốn trao đổi token A và B. Alice có 15 token A và cô ấy muốn 4 token B ; Bob có 10 mã B và anh ta muốn 30 token A. Ai đang mua và ai đang bán? Điều này chỉ phụ thuộc vào tài sản mà chúng tôi sửa chữa để báo giá. Nếu token A là tham chiếu, thì Alice mua token B với giá $\frac{15}{4} = 3.75$A, trong khi Bob bán 10 token B với giá $\frac{30}{10} = 3.00$A. Trong trường hợp lấy token B làm tham chiếu, chúng tôi nói rằng Alice đang bán 15 token A với giá $\frac{4}{15} = 0.26666667$B và Bob mua 10 token A với giá $\frac{10}{30} = 0.33333334$B. Do đó, ai là người mua hoặc người bán là tùy ý.

Trong trường hợp đầu Alice sẵn sàng mua với giá cao hơn (3.75A) hơn mà giá Bob đang bán token của anh ta (3.00A), trong trường hợp thứ hai Bob sẵn sàng mua với giá (0.33333334B) cao hơn mà giá Alice đang bán (0.26666667B). Rõ ràng rằng cuộc giao dịch có thể diễn ra bất cứ khi nào người mua sẵn sàng mua với giá cao hơn hoặc bằng với giá của người bán đang bán.

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

Do đó, để có thể được lấp đầy một bộ n lệnh, toàn bộ hoặc một phần, chúng ta cần phải biết liệu sản phẩm của từng tỷ giá hối đoái như là lệnh mua có dẫn đến một số lớn hơn hay bằng 1. Nếu có, tất cả n các lệnh có thể là một phần, hoặc hoàn toàn được lấp đầy [17]. Nếu chúng tôi giới thiệu một bên thứ ba, Charlie, như vậy Alice muốn bán cho x_1 token A và nhận được y_1 token B, Bob muốn bán x_2 token B và nhận y_2 token C, và Charlie muốn bán x_3 token C và nhận y_3 token A. Các token cần thiết đã có, giao dịch có thể xảy ra nếu:

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

Xem phần 7.1 để biết thêm chi tiết về các lệnh của Loopring.

4 Các thành phần hệ sinh thái

Những thành phần hệ sinh thái sau đây cùng nhau cung cấp tất cả các chức năng mà một cuộc trao đổi tập trung sẽ cung cấp.

- **Ví:**Một dịch vụ ví thông thường hay giao diện cho phép người dùng truy cập vào token của họ và cách gửi các lệnh tới mạng Loopring. Ví tiền sẽ được khuyến khích tạo lệnh bằng cách chia sẻ lệ phí với những người khai tác vòng (xem phần 8). Với niềm tin rằng tương lai của giao dịch sẽ diễn ra trong sự an toàn của ví cá nhân của người dùng, kết nối các khoản thanh khoản này thông qua giao thức của chúng tôi là việc quan trọng nhất.

- **Hiệp hội Chia sẻ thanh khoản Blockchain / Relay-Mesh:** Một mạng lưới Relay-mesh cho việc chia sẻ thanh khoản và lệnh. Khi các nốt chạy phần mềm chuyển tiếp Loopring, họ có thể tham gia vào một mạng hiện có và chia sẻ thanh khoản với các chuyển tiếp khác qua một blockchain của hiệp hội. Blockchain của hiệp hội mà chúng tôi đang xây dựng như là một sự thực hiện đầu tiên với việc chia sẻ lệnh thời gian thực (1-2 giây khối), và giảm bớt lịch sử cũ để cho phép tải nhanh hơn bởi các nốt mới. Đáng chú ý, các chuyển tiếp không cần phải tham gia vào hiệp hội này; họ có thể hành động một mình và không chia sẻ thanh khoản với người khác, hoặc họ có thể bắt đầu và quản lý mạng lưới chia sẻ thanh khoản của chính họ.

- **Chuyển tiếp / các thợ khai thác vòng:**các chuyển tiếp là các nút nhận các lệnh từ ví hoặc mạng relay- mesh, duy trì các bảng đấu giá và lịch sử giao dịch, và tùy chọn phát các đơn lệnh cho các Chuyển tiếp khác (thông qua bất kỳ off-chain nào) và / hoặc các nút mạng relay-mesh. Khai thác mỏ là một tính năng - không phải là yêu cầu - của các chuyển tiếp. Đó là việc tính toán nặng và được thực hiện hoàn toàn bằng phương thức off-chain. Chúng tôi gọi các chuyển tiếp với tính năng khai thác vòng được kích hoạt bởi "Những người khai thác vòng", người sản xuất các vòng bằng cách ghép các lệnh khác nhau. Các chuyển tiếp được miễn phí trong (1) làm thế nào họ chọn để giao tiếp với nhau, (2) cách họ xây dựng bảng đấu giá của họ, và (3) làm thế nào họ khai thác các vòng lệnh (thuật toán khai thác mỏ).

- **Hợp đồng Thông minh Giao thức Loopring (LPTC):** Một bộ hợp đồng thông minh và miễn phí để kiểm tra các mệnh lệnh nhận được từ người khai thác mỏ, thay mặt người dùng tin tưởng và chuyển giao các khoản tiền, khuyến khích những người khai thác mỏ và ví có phí và phát các sự kiện. Các chuyển tiếp / lệnh các trình duyệt lắng nghe những sự kiện này để giữ cho bảng đấu giá của họ và lịch sử giao dịch được cập nhật. Xem phụ lục A để biết chi tiết.

- **Dịch vụ mã hóa Tài sản (ATS):** Một cầu nối giữa các tài sản không thể được giao dịch trực tiếp trên Loopring. Đây là các dịch vụ tập trung do các công ty hoặc tổ chức đáng tin cậy điều hành. Người dùng gửi tài sản (thực, Fiat hay token từ các chuỗi khác) và nhận token được phát hành, có thể được sử dụng để đặt cọc trong tương lai. Loopring không phải là giao thức trao đổi chéo (cho đến khi có giải pháp phù hợp), nhưng ATS cho phép thương mại các token ERC20 với tài sản vật lý cũng như tài sản trên các blockchains khác.

5 Quy tình trao đổi

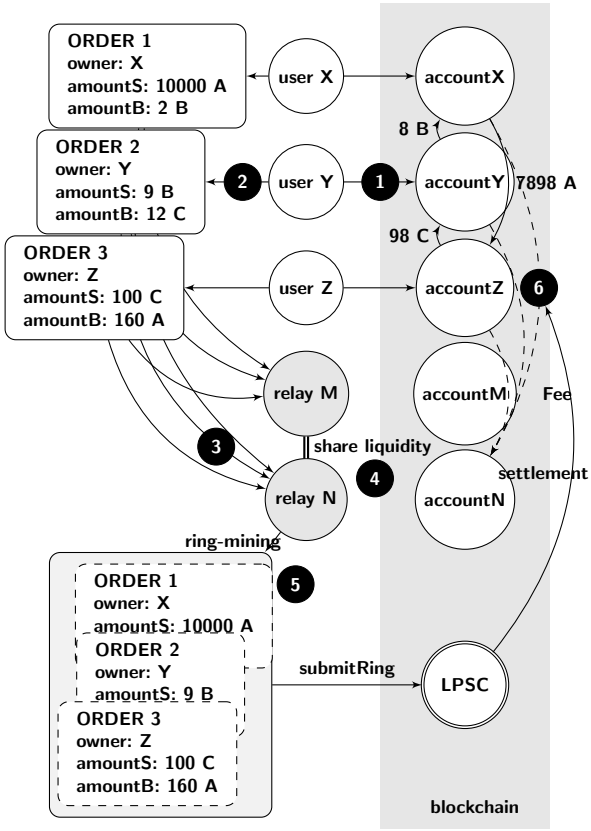
1. **Ủy quyền Giao thức:** Trong hình 2, người dùng Y muốn trao đổi token và ủy quyền cho LPSC xử lý token B với dố lượng S mà người dùng muốn bán. Điều này không khóa token của người dùng, vẫn có thể tự do di chuyển chúng trong khi đơn đặt hàng được xử lý.

2. **Tạo lệnh:** Mức giá hiện tại và bảng đấu giá cho token B và token C được cung cấp bởi các chuyển tiếp hoặc các đại lý khác được kết nối

với mạng, chẳng hạn như trình duyệt bảng đấu giá. Người dùng Y đặt lệnh (đặt lệnh giới hạn) xác định số lượng S và số lượng B và các thông số khác thông qua bất kỳ giao diện ví điện tử nào. Một lượng LRx có thể được bổ sung vào các lệnh như một khoản phí cho người khai thác vòng; lệ phí LRx cao hơn có nghĩa là cơ hội tốt hơn để được xử lý sớm hơn bởi những người khai thác mỏ. Hash của lệnh được liên kết với mã khóa cá nhân của người dùng Y.

3. **Truyền phát lệnh:** Ví gửi các lệnh và chữ ký của nó cho một hoặc nhiều chuyển tiếp. Các chuyển tiếp bảng đấu giá công khai của chúng. Giao thức này không yêu cầu các bảng đấu giá xây dựng trong một cách thức nhất định, ví dụ như các thức người nào đến trước sẽ được phục vụ trước. Thay vào đó, các chuyển tiếp có quyền đưa ra các quyết định đã được thiết kế trong việc xây dựng bảng đấu giá của chúng.

4. **Chia sẻ thanh khoản:** : các chuyển tiếp truyền cho các chuyển tiếp khác thông qua bất kỳ phương tiện truyền thông tùy ý nào. Một lần nữa, có sự linh hoạt như thế nào của các nút tương tác. Để tạo điều kiện thuận lợi cho một mức độ kết nối mạng nhất định, có một mạng lưới chia sẻ thanh khoản được tích hợp sẵn bằng cách sử dụng một blockchain của hiệp hội. Như đã đề cập trong phần trước, mạng relay-mesh này được tối ưu hóa cho tốc độ và độ bao phủ.



Hình 2: Quy trình thương mại Loopring

5. **Khai thác vòng (Order Matching):** Những người khai thác vòng cố gắng lấp đầy các lệnh hoặc một phần theo tỷ giá nhất định hoặc tốt hơn bằng cách kết hợp nó với nhiều lệnh. Khai thác vòng là lý do chính tại sao giao thức có thể cung cấp tính thanh khoản cao cho bất kỳ cặp nào. Nếu tỷ lệ thực hiện tốt hơn so với người dùng Y đã chỉ định, số dư được chia sẻ giữa tất cả các lệnh mua bán trong vòng lệnh. Như là một phần thưởng, người khai thác mỏ chọn giữa phần số dư (Margin-Split, và trả lại LRx cho người dùng), hoặc chỉ đơn giản là giữ lệ phí LRx.

6. **Sự xác thực và Giải quyết:** Vòng lệnh được nhận bởi LPSC. Nó kiểm tra nhiều lần để xác minh dữ liệu được cung cấp bởi các thợ khai thác vòng và xác định xem có thể giải quyết toàn bộ hay một phần vòng lệnh (phụ

thuộc vào tỷ lệ lấp đầy của các lệnh trong vòng và token trong ví của người dùng). Nếu tất cả các kiểm tra đều thành công, hợp đồng sẽ tự động chuyển các token cho người dùng và đồng thời trả phí cho người khai thác mỏ và lệ phí ví. Nếu số dư của người sử dụng Y được xác định bởi LPSC là không đủ, sẽ được coi là thu nhỏ lại: lệnh mà được thu nhỏ sẽ tự động tăng lên kích thước ban đầu nếu tiền được gửi đến địa chỉ của nó đủ, không giống như hủy bỏ, đó là một chiều và không thể đảo ngược.

6 Vận hành linh hoạt

Điều quan trọng cần lưu ý là tiêu chuẩn mở của Loopring cho phép các thành phần có sự linh hoạt đáng kể trong cách hoạt động của chúng. Các thành phần hoạt động được tự do triển khai các mô hình kinh doanh mới và cung cấp giá trị cho người dùng nếu họ chọn. Hệ sinh thái là mô đun và được thiết kế để hỗ trợ sự tham gia của rất nhiều ứng dụng.

6.1 Bảng đấu giá

Các chuyển tiếp có thể thiết kế các bảng đấu giá của chúng bằng bất kỳ cách nào để hiển thị và so khớp các lệnh của người dùng. Đây là lần đầu tiên nó được thiết kế trên mô hình OTC, trong đó lệnh mua bán giới hạn chỉ dựa trên giá. Các dãy Timestamp của lệnh, nói cách khác, không có ảnh hưởng đến bảng đấu giá. Tuy nhiên, một chuyển tiếp là miễn phí để thiết kế các bảng đấu giá của chúng theo cách để tính toán một động cơ phù hợp sàn giao dịch tập trung, nơi mà các lệnh được xếp hạng bằng giá, trong khi vẫn tôn trọng dãy timestamp. Nếu một chuyển tiếpcó thể làm được điều này với bảng đấu giá, chúng có thể sở hữu hay tích hợp một ví, có các lệnh của những ví đó được chuyển riêng lẻ cho từng chuyển tiếp, cái mà có khả năng sẽ phù hợp với lệnh sau này tùy thuộc vào thời gian. Bất cứ cấu hình nào như vậy đều khả thi. Trong khi Các giao thức sàn giao dịch phân tán DEX vào các thời điểm yêu cầu chuyển tiếp phải có các tài nguyên - token khởi tạo cân bằng để đặt các lệnh -Các chuyển tiếp Loopring cần tìm một lệnh thích hợp để giao dịch, và có thể làm như vậy mà không cần token khởi tạo.

6.2 Chia sẽ tài nguyên

Các chuyển tiếp được tự do thiết kế cách họ chia sẻ thanh khoản (đơn đặt hàng) với nhau. Hiệp hội Blockchain của chúng tôi chỉ là một giải pháp cho vấn đề này, và hệ sinh thái được tự do để kết nối và liên lạc. Bên cạnh việc tham gia vào một liên minh blockchain, họ có thể xây dựng và quản lý riêng của mình, tạo ra các quy tắc / ưu đãi khi họ thấy phù hợp. Các chuyển tiếp cũng có thể hoạt động một mình, như trong thực hiện ví nhạy cảm-thời gian. Tất nhiên, có nhiều lợi thế rõ ràng trong việc giao tiếp với các chuyển tiếp khi theo đuổi các tác động của mạng lưới, tuy nhiên các mô hình kinh doanh khác nhau có thể xứng đáng chia sẽ các thiết kế và chia sẽ phí trong nhiều cách.

7 Chi tiết của giao thức

7.1 Sự mổ xẻ của một lệnh

Một lệnh là một gói dữ liệu mô tả mục đích thương mại của người dùng. Lệnh Loopring được định nghĩa bởi Mô hình lệnh một hướng hay còn gọi là UDOM, như sau:

```
message Order {
    address protocol;
    address owner;
    address tokenS;
    address tokenB;
    uint256 amountS;
    uint256 amountB;
    unit256 lrcFee
    unit256 validSince; // Seconds since epoch
    unit256 validUntil; // Seconds since epoch
    uint8   marginSplitPercentage;  // [1-100]
    bool    buyNoMoreThanAmountB;
    uint256 walletId;
    // Dual-Authoring address
    address authAddr;
    // v, r, s are parts of the signature
    uint8   v;
    bytes32 r;
    bytes32 s;
```

```
    // Dual-Authoring private-key,
    // not used for calculating order's hash,
    // thus it is NOT signed.
    string  authKey;
}
```

Để đảm bảo nguồn gốc của các lệnh, nó được ký kết chống lại các hash của các tham số của nó, không bao gồm authAddr, với mã khóa riêng của người dùng. Tham số authAddr được sử dụng cho việc ký các vòng lệnh mà lệnh đó là một phần trong đó, ngăn chặn lỗi chạy trước. Vui lòng tham khảo mục 9.1 để biết thêm chi tiết. Chữ ký được biểu diễn bởi các trường v, r, và các s, được bao gồm trong các tham số lệnh thông qua mạng. Điều này đảm bảo lệnh đó vẫn không thay đổi trong suốt cả thời gian. Mặc dù lệnh không bao giờ thay đổi, giao thức này vẫn có thể được tính trạng thái hiện tại của nó dựa vào sự cân bằng của địa chỉ của nó theo với các biến khác. UDOM không bao gồm một giá (mà phải là một số điểm nổi theo tự nhiên), nhưng thay vào đó sử dụng tỷ giá hoặc r, được thể hiện bằng số lượng S / số lượng B. Giá đó không phải là một số điểm nổi, nhưng nó biểu hiện sẽ chỉ có thể thực hiện với các số nguyên chưa được ký khác trên mệnh lệnh, để giữ tất cả các kết quả trung gian như các số nguyên chưa được ký và làm tăng độ chính xác tính toán.

7.1.1 Khối lượng mua

Khi một vòng thợ khai thác vòng trùng khớp với các lệnh, có khả năng một giá tốt hơn sẽ được thực thi, cho phép người sử dụng nhận được nhiều token B hơn là họ xác định. Tuy nhiên, nếu Mua không quá số lượng B buyNoMoreThanAmountB được đặt thành True, giao thức đảm bảo nhượgười dùng nhận được không nhiều hơn số lượng B của tokenB. Do đó, tham số Mua không quá số lượng B của UDOM xác định khi một lệnh hoàn toàn được lấp đầy. Mua không quá số lượng B áp dụng giới hạn về số lượng S hoặc số lượng B, và cho phép người dùng thể hiện các ý định thương mại chi tiết hơn các lệnh mua / bán truyền thống. Ví dụ: với amountS = 10 và amountB = 2, tỷ lệ r = 10/2 = 5. Do đó người dùng sẵn sàng bán 5 token S cho mỗi token B. Vòng khai thác trùng khớp và tìm tỷ lệ người dùng là 4, cho phép người dùng nhận được 2,5 tokenB thay vì 2. Tuy nhiên, nếu người dùng chỉ muốn 2 tokenB và đặt cờ Mua không quá số lượng B thành hiện thực, LPSC sẽ thực hiện giao dịch với tỷ lệ của 4 và người dùng bán 4 tokenS cho mỗi tokenB, tiết kiệm hiệu quả 2 tokenS. Lưu ý rằng điều này không tính đến chi phí khai thác tài khoản (Xem phần 8.1).

Thật vậy, nếu chúng ta sử dụng

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

Để thể hiện một lệnh ở dạng đơn giản, sau đó cho thị trường ETH / USD trên một sàn giao dịch truyền thống, mô hình mua bán truyền thống có thể thể hiện thứ tự 1 và thứ 3 dưới đây, nhưng không phải là hai:

1. Bán 10 ETH với giá 300 USD / ETH. Lệnh này có thể được biểu diễn bằng: `Order(10, ETH, 3000, USD, False)`.
2. Bán ETH với giá 300 USD / ETH để được 3000 USD. Lệnh này có thể được biểu diễn như sau: `Order(10, ETH, 3000, USD, True)`.
3. Mua 10 ETH với giá 300 USD / ETH, lệnh này có thể được thể hiện bằng: `Order(3000, USD, 10, ETH, True)`.
4. Chi tiêu 3000 USD để mua càng nhiều ETH càng tốt ở mức 300 USD / ETH: `Order(3000, USD, 10, ETH, False)`.

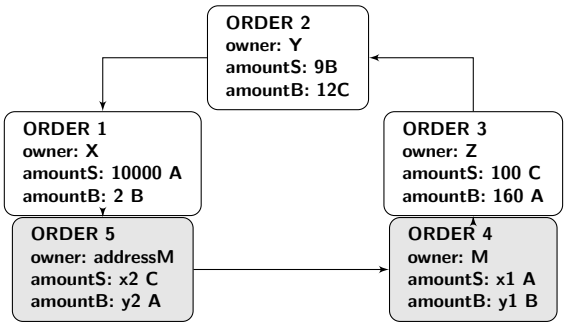
7.2 Xác thực vòng

Hợp đồng Thông minh Loopring không phải được thể hiện tính toán tỷ giá giao dịch và số lượng, nhưng phải nhận và xác minh những gì những người khai thác vòng cung cấp cho các giá trị này. Các tính toán này được thực hiện bởi những người khai thác vòng vì hai lý do chính: (1) ngôn ngữ lập trình cho các hợp đồng thông minh, chẳng hạn như tính vững chắc [19] trên Ethereum, không có hỗ trợ cho toán học điểm nổi, đặc biệt là pow (x, 1 / n) (tính

gốc rễ thứ n của một số điểm nổi), và (2) nó là mong muốn cho việc tính toán được thực hiện off-line để giảm bớt tính toán và chi phí blockchain.

7.2.1 Kiểm tra vòng phụ

Bước này ngăn cản các đầu cơ hưởng chênh lệch bất hợp pháp thực hiện tất cả các giao dịch ký quỹ trong một vòng lệnh bằng cách thực hiện các lệnh mới mới bên trong nó. Về cơ bản, một khi vòng lệnh hợp lệ được tìm thấy bởi một người khai thác vòng, có thể sẽ bị cám dỗ để thêm các lệnh vào vòng lệnh để thu đầy đủ giao dịch ký quỹ của người dùng (đánh giá mức chiết khấu). Theo tính toán của hình 3, cẩn thận tính x1, y1, x2 và y2 sẽ làm cho sản phẩm của tất cả các lệnh sẽ được chính xác những gì bạn cần.



Hình 3: Một vòng lệnh với một vòng phụ

Đây là Rủi ro không, giá trị không được thêm vào mạng, và được coi là sự điều khiển không công bằng cho người khai thác vòng. Để ngăn chặn điều này, Loopring yêu cầu một vòng lặp hợp lệ không thể chứa bất kỳ vòng phụ. Để kiểm tra điều này, LPSC đảm bảo một token không thể đặt ở một vị trí mua hay bán hai lần. Trong sơ đồ trên, chúng ta có thể thấy rằng token A là một token bán hai lần và mua hai lần, điều mà sẽ không được phép.

7.2.2 Kiểm tra tỷ lệ lấp đầy

Việc tính tỷ giá hối đoái trong vòng lệnh được thực hiện bởi người khai thác vòngvì lý do nêu trên. Đó là LPSC phải xác minh là đúng. Thứ nhất, nó xác nhận rằng tỷ lệ mua mà người khai thác vòng có thể thực hiện cho từng lệnh là bằng hoặc ít hơn tỷ giá mua ban đầu được đặt bởi người dùng. Điều này đảm bảo rằng người dùng được tỷ giá giao dịch tối thiểu mà họ yêu cầu hoặc tốt hơn. Một khi các tỷ giá hối đoái được xác nhận, LPSC đảm bảo rằng mỗi tỷ giá hối đoái trong vòng lệnh chia sẽ chiết khấu tỷ giá tương tự. Ví dụ, nếu tỷ lệ chiết khấu là γ, thì giá cho mỗi lệnh sẽ là:

$r_{0\to1}\cdot(1-\gamma)$, $r_{1\to2}\cdot(1-\gamma)$, $r_{2\to0}\cdot(1-\gamma)$, và thõa mản:

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

Do đó:

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

Nếu giao dịch với qua n lệnh, chiết khấu sẽ là:

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

Khi r^i là tỷ lệ doanh số đặt lệnh mua bán của lệnh thứ i. Rõ ràng, chỉ khi tỷ lệ chiết khấu là $\gamma \geq 0$,những lệnh này có thể được lấp đầy; và tỷ giá hối đoái thực tế của lệnh thứ $\hat{r^i} = r^i\cdot(1-\gamma)$, $\hat{r^i} \leq r^i$.

Trở lại ví dụ lúc nãy, khi mà Alice có 15 token A và muốn 4 token B, Bob có 10 token B và muốn 30 token A. Nếu lấy token A làm tham chiếu, sau đó Alice mua token B với giá $\frac{15}{4} = 3.75$A, trong khi Bob bán token B với giá 3.00A. Để tính toán chiết khấu: $\frac{150}{120} = 1.25$ do vậy $\frac{1}{1.25} = 0.8 = (1-\gamma)^2$. Do đó, tỷ giá trao đổi hoàn lại giao dịch công bằng cho cả 2 bên là: $\sqrt{0.8}\cdot 3.75 \approx 3.3541$ token A cho mỗi token B. Bob cho 4 token B và nhận được 13.4164 token A, nhiều hơn con số 12 mà anh ta mong đợi cho 4 token này. Alice nhận 4 token B như dự định nhưng chỉ cho 13.4164 A, ít hơn con số 15 token mà cô đã sẵn sàng cung cấp 4 token B. Lưu ý, một phần lợi nhuận này sẽ được áp dụng để thanh toán các khoản phí để khuyến khích các thợ mỏ (và ví).8.1).

7.2.3 Theo dõi và hủy lấp đầy

Một người dùng có thể hủy hoàn toàn hoặc một phần của một lệnh bằng cách gửi một giao dịch đặc biệt đến LPSC, chứa các chi tiết về lệnh đó và số lượng cần hủy. LPSC đưa nó vào tài khoản, lưu trữ số lượng cần dừng và tạo ra một dữ kiện OrderCancelled đến mạng. LPSC giữ theo dõi các số lượng đã được lấp đầy hay đã hủy bằng việc lưu

trữ các giá trị của chúng sử dụng hash của lệnh như một định danh. Dữ liệu này có thể truy cập công khai và sự kiện OrderCancelled/ OrderFilled được phát khi nó thay đổi. Theo dõi các giá trị này là rất quan trọng đối với LPSC trong suốt các bước giải quyết vòng lệnh. LPSC cũng hỗ trợ hủy tất cả các lệnh cho bất kỳ cặp giao dịch nào với sự kiện hủy lệnh OrderCancelled và hủy tất cả các lệnh cho một địa chỉ với sự kiện AllOrdersCancelled.

7.2.4 Thước đo lệnh

Các lệnh được tỷ lệ theo lịch sử của các tài khoản đã được lấp đầy hoặc đã hủy và số dư tài khoản hiện tại. Quá trình tìm ra lệnh với số lượng nhỏ nhất có thể được lấp đầy dựa vào các đặc tính và sử dụng nó như một tham khảo để chia tỷ lệ cho tất cả các giao dịch trong vòng lệnh.

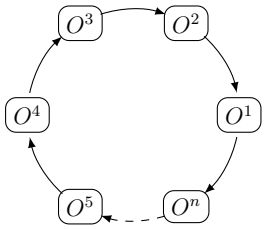
Tìm lệnh có giá trị thấp nhất có thể giúp bạn tìm ra khối lượng cho mỗi lệnh. Ví dụ, nếu lệnh thứ i là lệnh có giá trị thấp nhất, thì số lượng của token đã được bán từ mỗi lệnh s^ và số lượng token đã được mua ^b từ mỗi lệnh có thể tính toán:

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

Với si là số dư còn lại khi lệnh đã được lấp đầy một nửa. Trong quá trình thực hiện chúng ta có thể giả định một cách an toàn bất kỳ lệnh nào trong vòng lệnh cógiá trị thấp nhất, sau đó lặp qua vòng lệnh nhiều nhất hai lần để tính toán khối lượng lấp đầy của mỗi lệnh. Ví dụ: Nếu số tiền nhỏ nhất được so sánh với lệnh ban đầu là 5%, tất cả các giao dịch trong vòng lệnh được thu nhỏ xuống 5%. Một khi các giao dịch được hoàn thành thì lệnh đó được xem là có số lượng nhỏ nhất còn lại để được lấp đầy.

7.3 Thỏa thuận vòng

Nếu vòng lệnh hoàn thành tất cả các kiểm tra trước đó, vòng lệnh có thể đóng và có thể thực hiện các giao dịch. Điều này có nghĩa là tất cả n lệnh đều được đóng vòng lệnh, kết nối như trong hình 4:



Hình 4: thỏa thuận vòng

Để thực hiện giao dịch, LPSC sử dụng hợp đồng thông minh TokenTransferDelegate, làm cho giao thức trở nên dễ nâng cấp hơn vì tất cả các lệnh chỉ cần ủy quyền cho đại diện này khác với các phiên bản khác của giao thức. Đối với mỗi lệnh trong vòng lệnh, một thanh toán của token S được thực thi đến lệnh trước hay kế tiếp tùy thuộc vào việc thực thi. Sau đó, phí khai thác vòng được thanh toán tùy thuộc vào mô hình tính phí do người khai thác vòng chọn. Cuối cùng, tất cả các giao dịch được thực hiện, một sự kiện RingMined được phát ra.

7.3.1 Các sự kiện được phát

Giao thức này phát ra các sự kiện cho phép chuyển tiếp, các trình duyệt lệnh và các tác nhân khác nhận lệnh càng sớm càng tốt. Các sự kiện được phát ra là:

- **OrderCancelled**: Một lệnh cụ thể bị hủy.
- **OOrdersCancelled**: Tất cả các lệnh của một cặp giao dịch từ một địa chỉ sỡ hữu bị hủy. cancelled.
- **AllOrdersCancelled**: Tất cả các lệnh của các cặp giao dịch từ một địa chỉ sỡ hữu bị hủy.
- **RingMined**: Một vòng lệnh đã được thiết lập thành công. Sự kiện này chứa dữ liệu liên quan tới mỗi giao dịch token vòng trong.

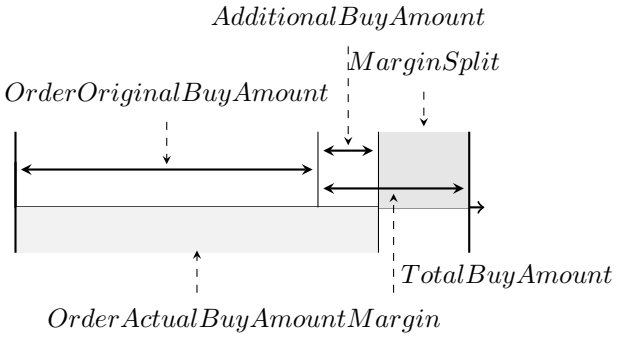
8 LRx Token

LRx là ký hiệu dấu hiệu tổng quát của chúng tôi. LRC là mã thông báo Loopring trên Ethereum, LRQ trên Qtum và LRN trên NEO, v.v. Các loại LRx khác sẽ được giới thiệu trong tương lai.

8.1 Mô hình phí

Khi người dùng tạo ra một lệnh, họ chỉ định số tiền thanh toán cho người khai thác vòng như là phí, cùng với tỷ lệ phần trăm của lợi nhuận (marginSplitPercentage) theo lệnh mà người khai thác vòng có thể yêu cầu bồi thường. Đây được gọi là phân chia lợi nhuận. Quyết định lựa chọn phí hay tỷ lệ phần trăm lợi nhuận là do người khai thác vòng chọn.

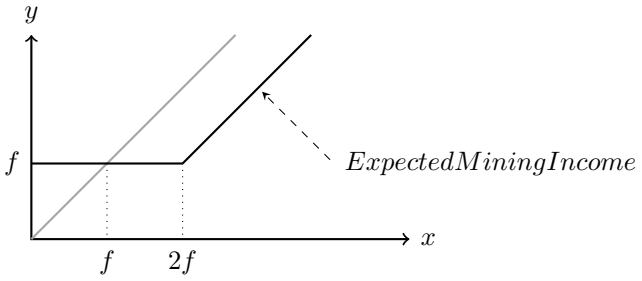
Một ví dụ của sự phân chia lợi nhuận:



Hình 5: chia 60% giao dịch ký quỹ

Nếu ký quỹ là quá nhỏ, một thợ khai thác vòng sẽ chọn lệ phí LRx. Nếu ngược lại, giao dịch ký quỹ đủ lớn để phân chia mà thu được nhiều hơn phí LRx, thì một nhà người khai thác vòng sẽ chọn phân chia ký quỹ. Tuy nhiên, có một điều kiện khác: khi người khai thác vòng chọn phân chia ký quỹ, họ phải trả cho người sử dụng (người đặt lệnh) một khoản phí, bằng LRx mà người sử dụng sẽ phải trả cho người khai thác vòng như một khoản phí bằng với phí LRx người dùng sẽ phải trả cho người khai thác vòng như là phí giao dịch. Điều này làm tăng ngưỡng của người khai thác vòng sẽ chọn phân chia ký quỹ Để gấp đôi phí LRx của lệnh, tăng khuynh hướng chọn lựa phí LRx. Điều này cho phép những người khai thác vòng thu được thu nhập liên tục trên các lệnh có tỷ suất ký quỹ thấp để đánh đổi thu nhập ít hơn trên vòng lệnh ký quỹ cao hơn. Mô hình tính phí của chúng tôi kỳ vọng rằng khi thị trường tăng trưởng và chín muồi, sẽ có ít hơn các vòng lệnh ký quỹ cao, do đó cần phải có phí LRx cố định để khuyến khích.

Chúng tôi kết luận với biểu đồ bên dưới:



Hình 6: Mô hình phí của Loorping

Với f là phí LRx, x là chia ký quỹ, y là thu nhập từ việc khai thác. $y = max(f, x - f)$ như được chỉ thị bởi đường tô đậm; Nếu phí LRx cho một lệnh là 0, phương trình là $y = max(0, x - 0)$ đơn giản hóa đến $y = x$ như được chỉ ra bởi dòng màu xám.

Kết quả là:

1. Nếu phân chia ký quỹ là 0, người khai thác vòng sẽ chọn mức phí trần LRx mà vẫn được khuyến khích.

2. Nếu phí LRx là 0, kết quả dòng màu xám và thu nhập được dựa trên một mô hình tuyến tính chung.

3. Khi thu nhập từ chia ký quỹ lớn hơn 2 lần phí LRx thì người khai thác vòng sẽ chọn chia ký quỹ và trả phí LRx cho người dùng.

Cần lưu ý rằng nếu phí LRx là khác không, cho dù các thợ khai thác vòng chọn lựa chọn nào thì sẽ luôn luôn có một chuyển đổi phí LRx giữa người khai thác vòng và người gửi lệnh.Một là người khai thác vòng thu được phí LRx hoặc trả phí LRx cho người gửi nếu lấy phí chia ký quỹ.

Những người khai thác vòng sẽ chia sẻ một tỷ lệ nhất định lệ phí với các ví. Khi người dùng đặt một lệnh thông qua một ví và được lấp đầy, ví sẽ được nhận một phần của lệ phí LRx hay chia ký quỹ. Mặc dù đây là mô đun, và mô hình kinh doanh độc đáo hay sự thực hiện được là điều có thể, ý định của chúng tôi là dành cho ví để nhận khoảng 20% -25% lệ phí thu được. Ví là một mục tiêu ưu tiên cho liên hợp giao thức Loorping vì họ có cơ sở người dùng nhưng nhỏ hoặc không có nguồn thu nhập.

8.2 Quản trị phân cấp

Tại vấn đề cốt lõi, giao thức Loopring là một giao thức xã hội theo nghĩa nó dựa vào sự phối hợp giữa các thành viên để hoạt động hiệu quả theo hướng mục tiêu. Điều này giống với các giao thức cryptoeconomic lớn, và thực tế, tính hữu ích của nó phần lớn được bảo vệ bởi cùng một cơ chế của các vấn đề phối hợp [20], cân bằng kích hoạt mạnh mẽ và tính hợp lý bị giới hạn. Để kết thúc điều này, các token LRx không chỉ được sử dụng để trả phí, mà còn để sắp xếp các ưu đãi tài chính của các thành viên mạng khác nhau. Sự liên kết như vậy là cần thiết để áp dụng rộng rãi cho bất kỳ giao thức nào, nhưng đặc biệt cấp tính đối với các giao thức trao đổi, vì thành công đó chủ yếu dựa vào việc cải thiện tính thanh khoản trong một hệ sinh thái phân tán mạnh mẽ. Các token LRx sẽ được sử dụng để thực hiện cập nhật các giao thức thông qua sự quản lý phân quyền. Việc cập nhật hợp đồng thông minh sẽ được quản lý bởi các chủ sở hữu token để đảm bảo tính liên tục và an toàn, đồng thời giảm thiểu rủi ro của thanh khoản bị siết lại thông qua sự không tương thích. Do các hợp đồng thông minh không thể bị thay đổi khi triển khai, có nguy cơ dApps hoặc người dùng cuối tiếp tục tương tác với các phiên bản không dùng nữa và không cho phép họ cập nhật hợp đồng. Khả năng nâng cấp là rất quan trọng đối với thành công của giao thức vì nó phải thích ứng với nhu cầu của thị trường và các blockchains bên dưới. Quản lý phân quyền bởi các bên liên quan của LRx sẽ cho phép cập nhật hợp đồng thông minh hợp đồng mà không làm gián đoạn dApps hoặc người dùng cuối hoặc dựa quá nhiều vào việc trừu tượng hợp đồng thông minh. Số lượng token LRx là cố định , và trong trường hợp của LRC, một phần trăm nhất định bị đóng băng từ quỹ của Loopring và được phân bổ cho các quỹ dự định của cộng đồng

Tuy nhiên, người người sở hữu LRx không phải là các bên liên quan duy nhất để xem xét trong việc định hướng giao thức: các chuyển tiếp / người khai thác vòng, ví, nhà phát triển, và những người khác là một phần không thể tách rời của hệ sinh thái và tiếng nói của họ phải được lắng nghe. Trong thực tế, cho rằng các thành phần này không cần phải giữ bất kỳ LRx để thực hiện vai trò của họ (vì các nhà hoạch định truyền thống / nhà hoạch định thị trường không tồn tại, dự trữ token ban đầu là không bắt buộc) chúng ta phải cho phép các phương pháp thay thế cho lợi ích cần được tôn trọng. Hơn nữa, "đơn giản" bỏ phiếu tokenbased, cả trên on chain và off chain, là một sự giải quyết không hoàn hảo cho việc không đồng ý, như những người bỏ phiếu thấp và quyền sở hữu token tập trung đặt ra những rủi ro. Như vậy, mục đích là để thực hiện một mô hình quản trị được xây dựng theo các lớp, và dựa trên một chia sẻ kiến thức rằng một số quy trình ra quyết định là tiêu chuẩn. Điều này có thể được tạo điều kiện bởi các tổ chức phối hợp cung cấp tín hiệu từ một tập hợp đa dạng của người tham gia, và có lẽ, từ các đầu mối giao thức được thiết lập trước. Do vậy, Loopring sẽ không tránh khỏi việc từ các nhà phát triển giao thức thành người quản lý giao thức.

9 Phòng chống gian lận và tấn công

9.1 Ngăn ngừa lỗi chạy trước Front-running

Trong các sàn giao dịch phi tập trung, lỗi chạy trước là khi ai đó cố gắng sao chép giải pháp giao dịch của một nút khác và khai thác nó trước khi giao dịch ban đầu đang nằm trong vùng giao dịch đang chờ xử lý (mempool). Điều này có thể đạt được bằng cách chỉ định mức phí giao dịch cao hơn (giá gas). Vấn đề chính của lỗi chạy trước trong Loopring (và bất kỳ giao thức nào đối với khớp lệnh) là lệnh-filch: khi một người chạy trước đánh cắp một hoặc nhiều lệnh từ một giao dịch vòng lệnh đang chờ xử lý; và, cụ thể cho Loopring: khi một người chạy trước đánh cắp toàn bộ vòng lệnh từ một giao dịch đang chờ xử lý.

Khi một giao dịch vòng không được xác nhận và vẫn ở trong vùng giao dịch đang chờ xử lý, bất kỳ ai cũng có thể dễ dàng phát hiện ra một giao dịch như vậy và thay thế địa chỉ người khai thác minerAddress bằng địa chỉ riêng của họ (filcherAddress), sau đó họ có thể ký lại payload với filcherAddress để thay thế lệnh- dấu hiệu của vòng. Họ có thể đặt

giá gas cao hơn và gửi một giao dịch mới với hy vọng rằng người khai thác vòng sẽ chọn giao dịch mới của mình vào khối tiếp theo thay vì giao dịch gốc.

Các giải pháp trước đây cho vấn đề này có những nhược điểm quan trọng: yêu cầu nhiều giao dịch hơn và vì vậy gây tốn nhiều phí cho các thợ khai thác mỏ; và lấy ít nhất hai lần khối để giải quyết một đlệnh. Giải pháp mới của chúng tôi, Dual Authoring [21], bao gồm cơ chế thiết lập hai lần ủy quyền cho các lệnh mua bán - một cho giải quyết, và một cho khai thác vòng.

Quy trình Uỷ quyền hai lần:

1. Đối với mỗi lệnh, phần mềm ví sẽ tạo ra một mã khóa công khai / mã khóa cá nhân ngẫu nhiên và đặt cặp khóa vào đoạn mã JSON của lệnh. (Một thay thế sử dụng địa chỉ có được chia ra từ khoá công khai thay vì bản thân khoá đó để giảm kích thước byte. Chúng tôi sử dụng authAddr để biểu diễn một địa chỉ như vậy, và authKey đại diện cho mã khóa riêng của authAddr).

2. Tính toán hash của lệnh với tất cả các trường trong lệnh đó ngoại trừ r, v, s, và authKey, và ký hash sử dụng mã khóa cá nhân của người sở hữu (không phải authKey).

3. Ví sẽ gửi lệnh với authKey để chuyển tiếp cho việc khai thác vòng. Những người khai thác vòn sẽ xác thực rằng authKey và authAddr là được ghép cặp chính xác và chữ ký của lệnh là có giá trị với theo địa chỉ người sỡ hữu.

4. Khi một vòng lệnh được xác định, người khai thác vòng sẽ sử dụng một authKey của mỗi lệnh để đánh dấu hash của vòng, minerAddress, và tất cả các thông số khai thác. Nếu một vòng lệnh chứa n lệnh, sẽ có n chữ ký bởi n authKeys. Chúng tôi gọi các chữ ký này là authSignatures. Người khai thác vòng có thể cần ký hash của vòng cùng nhau với tất cả các thông số đào sử dụng mã khóa riêng của địa chỉ người khai thác minerAddress.

5. Người khai thác vòng gọi hàm submitRing với tất cả các tham số, cũng như tất cả các authSignatures phụ. Lưu ý rằng authKeys KHÔNG phải là một phần của giao dịch On-chain và do đó vẫn chưa được biết đối với các bên khác với chính bản thân người khai thác vòng.

6. Giao thức Loopring bây giờ sẽ xác minh mỗi authSignature với authAddr tương ứng đối với mỗi lệnh và từ chối vòng lệnh nếu bất kỳ authSignature nào bị thiếu hoặc không hợp lệ.

Kết quả là:

- Chữ ký của lệnh (bằng mã khóa riêng của địa chỉ người sỡ hữu) đảm bảo rằng lệnh không thể sửa đổi, bao gồm địa chỉ authAddr.

- Chữ ký Người khai thác vòng (bằng mã khóa riêng của địa chỉ người khai thác minerAddress) nếu được cung cấp, đảm bảo không ai có thể sử dụng danh tính của anh ta để khai thác một vòng lệnh.

- Các chữ ký ủy quyền authSignatures đảm bảo toàn bộ vòng lệnh không thể được sửa đổi bao gồm địa chỉ người khai khác minerAddress, và không có lệnh nào bị đánh cắp.

Uỷ quyền hai lần ngăn chặn việc ăn cắp vòng và ăn cắp lệnh ring-filch và order-filch trong khi vẫn đảm bảo việc giải quyết các vòng lệnh có thể được thực hiện trong một giao dịch duy nhất. Ngoài ra, Uỷ quyền hai lần mở ra cánh cửa cho các chuyển tiếp để chia sẻ đcác lệnh theo hai cách: chia sẻ không phù hợp và chia sẻ phù hợp. Theo mặc định, Loopring vận hành mô hình OTC và chỉ hỗ trợ các lệnh có giá giới hạn, có nghĩa là các dấu thời gian của lệnh bị bỏ qua. Điều này ngụ ý rằng lỗi chạy trước của một giao dịch không ảnh hưởng đến giá thực tế của giao dịchđó, nhưng có ảnh hưởng đến việc nó được thực hiện hay không.

10 Các tấn công khác

10.1 Tấn công Sybil hay DOS

Những người dùng có ý phá hoại - hoạt động như chính họ hoặc giả mạo nhân dạng - có thể gửi một

số lượng lớn lệnh nhỏ để tấn công các nút Loopring. Tuy nhiên, vì chúng tôi cho phép các nút từ chối các lệnh như vậy dựa trên các tiêu chí của riêng mình - mà chúng có thể ẩn hoặc tiết lộ - hầu hết các lệnh này sẽ bị từ chối do không mang lại lợi nhuận khi ăn khớp. Bằng cách trao quyền cho các chuyển tiếp để giải thích cách họ quản lý các lệnh, chúng ta không xem một cuộc tấn công lệnh nhỏ như là một mối đe dọa.

10.2 Tài khoản thiếu

Những người sử dụng có ý phá hoại có thể ký và phát ra các lệnh có giá trị khác không nhưng địa chỉ thực lại là tài khoản bằng không. Các nốt có thể điều chỉnh và để ý rằng một vài tài khoản tạo lệnh có số dư là không, cập nhật trạng thái của một lệnh, nhưng có thể chọn tối thiểu hóa các ý định như vậy. ví dụ như đưa ra danh sách đen địa chỉ và thả lệnh liên quan.

11 Tóm lược

Giao thức Loopring được thiết lập để trở thành một lớp cơ sở cho giao dịch phân tán. Trong quá trình đó, nó có những lần lặp lại sâu về cách mọi người trao đổi tài sản và giá trị. Tiền, như là một loại hàng hoá trung gian, tạo điều kiện hoặc thay thế trao đổi trao đổi và giải quyết vấn đề trùng lặp gấp đôi trong vấn đề [22], nhờ đó hai người giao dịch mong muốn những lợi ích riêng biệt hoặc dịch vụ của nhau. Tương tự như vậy, giao thức Loopring nhằm mục đích mang lại sự tin tưởng phù hợp với các mong muốn của các cặp giao dịch, bằng cách sử dụng sự trùng khớp vòng để dễ dàng hoàn thành giao dịch. Điều này có ý nghĩa đối với xã hội và thị trường trao đổi token, các tài sản truyền thống, và hơn thế nữa. Thực tế, giống như các thuật toán mật mã phi tập trung tạo ra mối đe dọa đối với việc kiểm soát tiền tệ của một quốc gia, một giao thức tổ hợp có thể khớp với các nhà giao dịch (người tiêu dùng / nhà sản xuất), là một mối đe dọa về mặt lý thuyết đối với khái niệm tiền.

Lợi ích của giao thức bao gồm:

- Quản lý lệnh trên Off-chain và giải quyết on-chain có nghĩa không cần tốn tài nghuyên cho việc bảo mật.
- Tính thanh khoản tốt hơn do khai thác vòng và chia sẽ lệnh.
- Uỷ quyền hai lần giải quyết các vấn đề nguy hiểm của lỗi phía chạy trước đối với tất cả các sàn giao dịch phi tập trung và người dùng trên các sàn giao dịch đó.
- Miễn phí, các hợp đồng thông minh công khai cho phép bất cứ dApp nào xây dựng hay tích hợp với giao thức.
- Tiêu chuẩn giữa các nhà khai thác cho phép các hiệu ứng mạng và trải nghiệm người dùng cuối được cải thiện.
- Mạng được duy trì với tính linh hoạt trong việc chạy các bảng đấu giá và giao tiếp.
- Giảm rào cản đối với lối vào có nghĩa là chi phí thấp hơn khi tham gia vào các nốt mạng và người dùng cuối.
- Giao dịch ẩn danh trực tiếp từ ví người sử dụng.

12 Kiến thức

Chúng tôi xin bày tỏ lòng biết ơn đối với các cố vấn và nhiều người trong cộng đồng đã chào đón và chia sẻ kiến thức của họ. Đặc biệt, chúng tôi xin cảm ơn Shuo Bai (từ ChinaLedger); Giáo sư Haibin Kan; Alex Cheng, Hongfei Da; Yin Cao; Tiểu Xuyên; Zhen Wang, Wei Yu, Nian Duan, Jun Xiao, Jiang Qian, Jiangxu Xiang, Yipeng Guo, Dahai Li, Kelvin Long, Huaxia Xia, Jun Ma và Encephalo Path về việc xem xét và cung cấp phản hồi về dự án này.

Tài liệu

[1] Bancor protocol. https://bancor.network/, 2017.

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

[3] Viktor Atterlonn. *A distributed ledger for gamification of pro-bono time, 2018. [5] Hernando de Soto. The Mystery Of Capital.* 2000.

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

[5] Vitalik Buterin. Ethereum: a next generation smart contract and decentralized application platform (2013). 2017.

[6] Vitalik Buterin. Notes on blockchain governance, Accessed: 2018-03-05.

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

[8] Yaron Velner Loi Luu. Kybernetwork: A trustless decentralized exchange and payment service. https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-central, Accessed: 2018-03-05.

[9] Robert McMillan. The inside story of mt. gox, bitcoins 460 dollar million disaster. 2014.

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

[11] Jordan Earls Patrick Dai, Neil Mahi and Alex Norta. Smart-contract value- transfer protocols on a distributed mobile application platform. 2017.

[12] Reuters. Coincheck. https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-central, Accessed: 2018-03-05.

[13] Sylvain Ribes. Chasing fake volume: a crypto-plague, Accessed: 2018-03-10.

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

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

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

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

[18] Daniel Wang. Dual authoringlooprings solution to front-running. https://medium.com/loopring-protocol/dual-authoring-looprings-solution-to-front-runningd0fc9c348ef1, 2018.

[19] 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.

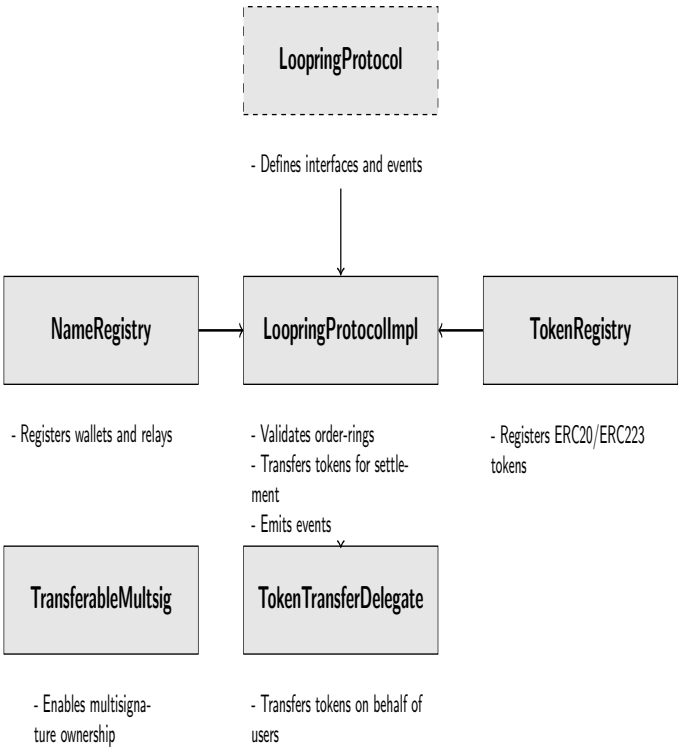
[20] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain. 2017.

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

Phụ lục

Phụ lục A Loopring trên nền tảng Ethereum

A.1 Các hợp đồng thông minh



Hình 7: Smart Contracts

A.2 Triển khai

Các hợp đồng thông minh sau đây đã được triển khai trên mạng chính thức Ethereum:

- LRC:

  `0xEF68e7C694F40c8202821eDF525dE3782458639f`

- TokenRegistry:

  `0xa21c1f2AE7f721aE77b1204A4f0811c642638da9`

- TokenTransferDelegate:

  `0xc787aE8D6560FB77B82F42CED8eD39f94961e304`

- NameRegistry:

  `0x0f3Dce8560a6010DE119396af005552B7983b7e7`

- LoopringProtocolImpl:

  `0xc80BbAb86cED62CF795619A357581FaF0cB46511`

- TransferableMultsig:

  `0x7421ad9C880eDF007a122f119AD12dEd5f7C123B`