Loopring:
Giao Thức Trao Đổi Phân Quyền

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

May 9, 2018

Tóm Tắt

Loopring là một giao thức mở được xây dựng nhằm tạo ra sự trao đổi phi tập trung (phân quyền). Loopring hoạt động giống như một tập hợp các hợp đồng thông minh công khai có khả năng giải quyết các giao dịch và thanh toán, với sự tập trung của các khách hàng bên ngoài chuỗi và kết nối các giao dịch với nhau. Giao thức miễn phí với người dùng, có thể mở rộng, và được sử dụng như một khối chuẩn hóa nhằm xây dựng các ứng dụng phân tán (dApps) kết hợp các chức năng giao dịch. Các tiêu chuẩn tương thích của chúng tôi giúp cho quá trình giao dịch được ẩn danh, không cần có sự tín nhiệm. Một cải tiến quan trọng so với các giao thức trao đổi phân quyền hiện nay là khả năng sắp xếp các lệnh khớp với các đơn đặt hàng khác, không giống nhau, loại bỏ các ràng buộc của hai cặp thẻ khi giao dịch và cải thiện đáng kể tính thanh khoản. Loopring cũng sử dụng một giải pháp độc đáo và mạnh mẽ để ngăn chặn hoạt động gian lận như "chạy trước": hành động trái đạo đức khi chuyển các giao dịch thành khối dữ liệu nhanh hơn người gửi ban đầu. Loopring là chuỗi khối đa nền tảng và có thể triển khai trên bất kỳ chuỗi khối nào với chức năng hợp đồng thông minh. Vào thời điểm viết bài viết này, giao thức đã và đang hoạt động trên các nền tảng Ethereum [1] [2] và Qtum [3] ,đang được xây dựng trên nền tảng NEO [4] .

1 Giới thiệu

Với sự gia tăng của các tài sản số dựa trên công nghệ chuỗi khối (blockchain), nhu cầu trao đổi các tài sản này giữa các bên đã tăng đáng kể. Khi hàng ngàn loại tiền tệ số (tiền điện tử/thẻ) mới được giới thiệu bao gồm cả việc áp dụng số hóa các tài sản truyền thống - nhu cầu sử dụng loại tài sản này ngày càng gia tăng. Mặc dù việc giao dịch các loại tiền tệ số nhằm mục đích đầu cơ hay chuyển đổi để truy cập mạng lưới thông qua việc sử dụng các thẻ tiện ích gốc của họ, nhu cầu chuyển đổi các tài sản số hóa cho tài sản khác là cơ bản cho việc hình thành hệ sinh thái lớn hơn. Thực vậy, các tài sản số này cho thấy một sự tiềm năng to lớn [5], không chỉ yêu cầu mà còn khẳng định quyền sở hữu của người dùng, mà các chuỗi khối đã cho phép bất biến, nhưng đồng thời cũng cung cấp khả năng tự do giao dịch và chuyển đổi các tài sản này.

Như vậy, việc giao dịch các thẻ (giá trị) mà không cần có sự tín nhiệm với các bên là một ví dụ hấp dẫn trong việc sử dụng công nghệ blockchain. Cho đến bây giờ, hầu hết những người sử dụng các tài sản số đã tiến hành giao dịch các loại tiền tệ số trên các sàn giao dịch tập trung truyền thống. Điều này càng cho chúng ta thấy giao thức Loopring là cần thiết bởi vì, giống như Bitcoin [6] đã từng nhấn mạnh rằng, liên quan đến giao dịch ngang hàng (peer-to-peer) tiền điện tử, " lợi ích chính vẫn sẽ bị mất đi nếu như bên thứ ba mà người dùng tin tưởng sử dụng gian lận hai giao dịch khác nhau để cùng chi tiêu số dư của một tài khoản", điều này cũng chính là nguyên nhân chính của sự thất thoát các tài sản tập trung nếu việc giao dịch bắt buộc phải có sự tham gia của bên thứ ba, các cổng giao dịch, các sàn giao dịch tập trung.

Theo quan điểm triết học, việc giao dịch các tài sản số phi tập trung trên các sàn giao dịch là không hề có ý nghĩa, vì các sàn giao dịch tập trung không thể đáp ứng được các đặc tính mà các dự án phi tập trung hóa mong muốn thực hiện. Ngoài ra còn có nhiều rủi ro và hạn chế thực tế trong việc sử dụng các sàn giao dịch tập trung được mô tả ở phần dưới đây. Trao đổi phi tập trung (DEXs) [7] [8] [9] đã đưa cách giải quyết những vấn đề này, và trong nhiều trường hợp đã thành công trong việc giảm bớt rủi ro an ninh bằng cách sử dụng công nghệ chuỗi khối (blockchain) cho việc loại bỏ các bước trung gian. Tuy nhiên, trong thời gian sắp tới khả năng DEX trở thành cơ sở hạ tầng quan trọng đối với việc tạo nên nền kinh tế mới là khả thi, do đó có cần cung cấp một không gian đáng kể để cải thiện hiệu suất. Loopring hướng đến mục tiêu cung cấp các công cụ khuôn mẫu cho

cơ sở hạ tầng của các dApp bằng giao thức mở bất khả tri.

2 Bức Tranh Toàn Cảnh của Thị Trường Giao Dịch Hiện Nay

2.1 Những Bất Cập của Giao Dịch Tập Trung

Ba rủi ro chính của các giao dịch tập trung là: 1) Bảo mật thấp, 2) Thiếu minh bạch, và 3) Tính thanh khoản không cao.

Sự thiếu bảo mật phát sinh đến từ những người tham gia, họ không kiểm soát được những mật mã (quỹ tiền) của mình. Chính điều này đã làm cho họ dễ dàng trở thành con mồi của các tin tặc trong các giao dịch của họ. Các rủi ro về an ninh và bảo mật mà các giao dịch tập trung đang phải đối mặt khá phổ biến [10] [11], nhưng nó thường được xem như là "những khoản đặt cọc" trong giao dịch tiền tệ số. Các giao dịch này tiếp tục là những miếng mồi béo bở cho các tin tặc, bởi các tin tặc có thể dễ dàng truy cập vào các máy chủ đang quản lý hàng triệu đô-la của khách hàng. Đồng thời thì các nhà phát triển cũng có thể tạo ra các lỗi ngẫu nhiên có chủ đích lên các tài khoản của khách hàng. Tóm lại thì khách hàng dường như không có khả năng kiểm soát được tài khoản của mình khi đã gửi chúng vào các sàn giao dịch.

Sự thiếu minh bạch sẽ làm các nhà đầu tư vướng phải nguy cơ bị lừa đảo và thiệt thòi trong chính các giao dịch của mình. Sự khác biệt ở đây là nhà đầu tư giao dịch bằng tài sản của họ có trên sàn mà là giao dịch bằng 1 IOU, điều này là một trong những mục đích không tốt của những nhà điều hành. Khi các đồng tiền được gửi vào ví, thì sàn giao dịch sẽ giữ chúng và thay thế chúng bằng IOU. Tất cả các giao dịch sẽ có hiệu lực trên các IOU của nhà đầu tư. Để thu hồi lại thì nhà đầu tư chỉ cần chuyển từ IOU sang đồng tiền, và các đồng tiền này sẽ được chuyển đến ví riêng của họ trên sàn giao dịch. Sự thiếu minh bạch trong suốt quá trình này sẽ dẫn đến hậu quả sau: giao dịch có thể bị hủy bỏ, tài khoản bị đóng băng, hoặc dẫn đến phá sản, vv … Trong khi họ cũng có thể sử dụng tài sản của nhà đầu tư với các mục đích khác, chẳng hạn như cho một bên thứ ba vay. Mặc khác, sự thiếu minh bạch có thể giúp nhà đầu tư giảm tổng chi phí trong các giao dịch như là phí giao dịch cao, chậm trễ lúc cao điểm, rủi ro về qui định và kẹt các đơn hàng trước.

Sự thiếu tính thanh khoản. Từ cái nhìn của những nhà điều hành, thì tính thanh khoản bị phân mảnh, nó gây ức chế lên việc tiếp cận các giao dịch mới bởi vì kịch bản là "được ăn cả, ngã về không". Đầu tiên, giao dịch với 1 lượng tiền khổng lồ để đôi bên cùng có lợi, do vậy nhà đầu tư muốn đặt cược tất cả trong một lần giao dịch. Tiếp đó, cho đặt lệnh mua bán hàng loạt, để nhà đầu tư kiếm được lợi nhuận từ khoảng chênh lệch giữa các giao dịch. Điều này làm giảm tính cạnh tranh cho những người mới tham gia vì rất khó để họ thanh khoản chi phí ban đầu. Kết quả là nhiều giao dịch đòi hỏi thị phần cao, mặc dù đã có sự phàn nàn từ phía nhà đầu tư và thậm chí có những cuộc tấn công lớn từ tin tặc. Cần lưu ý rằng, thị trường càng béo bở thì nó càng dễ trở thành mục tiêu đáng chú ý cho tin tặc.

Từ quan điểm của nhà đầu tư, tính thanh khoản bị phân mảnh làm giảm đáng kể trải nghiệm của nhà đầu tư. Trong một giao dịch đơn cử, nhà đầu tư chỉ giao dịch được với các đồng mà sàn giao dịch này cung cấp, với các lệnh mua bán và những đồng có tính thanh khoản hỗ trợ cho các đồng của sàn giao dịch đó. Để mà chuyển đổi từ đồng `A` sang đồng `B`, nhà đầu tư phải tìm đến một sàn giao dịch trung gian có hỗ trợ 2 đồng đó và nhà đầu tư phải đăng kí thông tin tại sàn trung gian đó đồng nghĩa với lại việc tiết lộ các thông tin cá nhân của mình. Nhà đầu tư thường phải thực hiện các bước cơ bản hoặc trung gian, thông qua các đồng BTC hoặc ETH và phải trả phí cho quá trình đó. Cuối cùng thì, những lệnh đặt trước thường không đủ mạnh để có thể giao dịch thành công mà không có sự hao tổn. Ngay cả khi có sự hỗ trợ cho một lượng giao dịch khổng lồ thì cũng không có gì đảm bảo rằng khối lượng và tính thanh khoản đó không phải là giả [12].

Kết quả là tính thanh khoản bị phá vỡ và một hệ sinh thái bị phân mảnh tương tự như một hệ thống tài chính dư thừa, với một khối lượng đáng kể tập trung tại một số giao dịch. Các cam kết thanh khoản của chuỗi khối không có giá trị trong các giao dịch này.

2.2 Những Hạn Chế Trong Việc Giao Dịch Phi Tập Trung

Các giao dịch phi tập trung khác với các giao dịch tập trung một phần, bởi vì nhà đầu tư duy trì sự kiểm soát của mình lên các mã cá nhân (tài sản) bằng cách thực hiện các giao dịch trực tiếp trên qua mạng lưới chuỗi khối. Bằng việc giảm tin tưởng vào các công nghệ của các đồng tiền điện tử, họ đã giảm thiểu nhiều rủi ro về các vấn đề bảo mật. Tuy nhiên, sự hiệu quả và cơ cấu hạn chế vẫn còn tồn tại nhiều vấn đề.

Thanh khoản vẫn là vấn đề vì nhà đầu tư phải tìm kiếm các đối tác chấp nhận các khoản thanh khoản và tiêu chuẩn thanh khoản tương đối. Các hiệu ứng thanh khoản vẫn tồn tại nếu như DEXs hoặc dApps không sử dụng các tiêu chuẩn chung để tương tác và nếu các đơn hàng không được chia sẻ hoặc tuyên truyền rộng rãi trên một mạng lưới. Tính thanh khoản của các lệnh đặt trước và cụ thể là khả năng phục hồi của chúng – có thể ảnh hưởng lớn tới các chiến lược kinh doanh tối ưu [13]. Không có các tiêu chuẩn rõ ràng không chỉ dẫn đến việc giảm thanh khoản mà còn liên quan đến hàng loạt các hợp đồng thông minh không an toàn.

Hơn nữa, kể từ khi các giao dịch được thực hiện ở dạng chuỗi, DEXs đã kế thừa những hạn chế của blockchain, cụ thể là: sự chậm trễ trong việc thực hiện (đào coin), và tốn kém chi phí trong việc thay đổi đặt lệnh mua bán. Do đó, việc đặt lệnh trước vào chuỗi khối không thực sự tốt, vì khi thực hiện các lệnh trên blockchain bạn phải chịu một chi phí (chi phí hoạt động), làm cho các lệnh hủy trở nên phức

tạp và rất tốn kém.

Cuối cùng do các lệnh đặt trước ở blockchain được công khai nên các thợ đào có thể nhìn thấy các đơn hàng thì điều đó có nghĩa là các thợ mỏ sẽ khai thác ở lần tiếp theo để cung cấp cho đơn hàng đó. Sự chậm trễ này có thể làm cho nhà đầu tư chịu rủi ro bị hớt tay trên và phải chịu những cái giá hoặc giao dịch bất lợi về phía mình.

2.3 Các Giải Pháp Lai

Vì những lý do nêu trên, nên những sàn giao dịch dựa trên công nghệ chuỗi khối có những hạn chế mà làm cho chúng không cạnh tranh được với các sàn tập trung. Có một sự đánh đổi giữa việc không cần có sự tín nhiệm vào bất kì người nào trong chuỗi và việc tốc độ và độ linh hoạt của sàn tập trung. Những giao thức như Loopring và 0x [14] mở rộng giải pháp giải quyết trên chuỗi và quản lý lệnh ngoài chuỗi. Các giải pháp này xoay quanh hợp đồng thông minh mở, nhưng thông qua sự giới hạn mở rộng bằng cách thực hiện một số chức năng ngoài chuỗi và cho thêm nodes sự linh hoạt trong hoàn thành vai trò quan trọng đối với mạng lưới. Tuy nhiên, mô hình Lai vẫn còn một số nhược điểm [15]. Giao thức Loopring đề xuất những khác biệt có ý nghĩa đáng kể trong cách tiếp cận giải pháp lai được mô tả trong bài viết này.

3 Giao Thức Loopring

Loopring không phải là sàn giao dịch phi tập trung (DEX), nhưng là một giao thức khuôn mẫu để xây dựng các giao dịch phi tập trung trên nhiều chuỗi khối. Chúng tôi loại bỏ các thành phần không cần thiết trong các giao dịch truyền thống và đưa ra một bộ hợp đồng thông minh công khai và . Các thành phần đóng vai trò trong mạng lưới bao gồm ví, rơ-le, chia sẻ thanh khoản, các trình duyệt hỗ trợ việc đặt lệnh, các thợ đào trong chu trình và các dịch vụ số hóa (thẻ) tài sản. Nhưng trước khi định nghĩa từng thành phần, chúng ta nên hiểu được việc đặt lệnh trong Loopring là như thế nào.

3.1 Chu Trình Giao Dịch

Các trao đổi trong Loopring được thể hiện dựa trên mô hình chúng tôi gọi là "mô hình giao dịch một chiều" (UDOM)[16]. UDOM thể hiện lệnh như yêu cầu trao đổi thẻ, `lượngS`/`lượngB`, (lượng thẻ bán ra/mua vào) thay vì đặt tỷ giá và đấu giá. Vì mỗi lệnh mua bán chỉ là một tỷ giá hối đoái giữa hai thẻ do đó một tính năng mạnh mẽ mới của giao thức là sự pha trộn và kết hợp của nhiều đơn đặt hàng trong một vòng giao dịch. Bằng cách sử dụng lên đến 16 đơn đặt hàng thay vì một cặp giao dịch duy nhất, đó là một sự gia tăng đáng kể trong tính thanh khoản và khả năng để cải thiện giá.

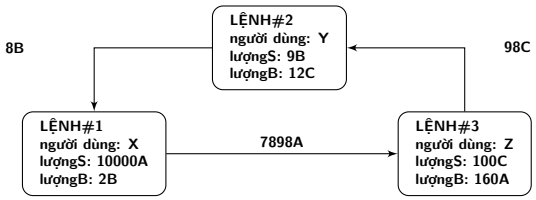

Figure 1: Một chu trình trao đổi của 3 lệnh khác nhau

Hình trên cho thấy một chu trình mua bán gồm 3 lệnh được đưa ra. Mã thông báo của mỗi đơn đặt hàng để bán (`thẻS`) là mã thông báo của một đơn đặt hàng khác để mua (`thẻB`). Điều này tạo ra một vòng lặp cho phép các lệnh đưa ra có thể trao đổi các thẻ mong muốn mà không đòi hỏi cần có sự xuất hiện của một lệnh đối lập với nó. Các cặp lệnh giao dịch truyền thống vẫn có thể, dĩ nhiên, vẫn được thực hiện, về cơ bản, nó chỉ là 1 trường hợp đặc biệt trong chu trình lệnh.

Định nghĩa 3.1 (Chu trình lệnh) *Gọi* C_0, C_1, $\cdots$, C_{n-1} *là n thẻ khác nhau,* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ *là n lệnh. Các lệnh này sẽ được biểu diễn thành 1 chu trình lệnh để trao đổi như sau:*

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

trong đó n là độ dài của chu trình lệnh, và $i \oplus 1 \equiv i + 1 \mod n$.

Một chu trình mua bán có giá trị (hiệu lực) khi tất cả các thành phần giao dịch được thực hiện với tỷ giá hối đoái bằng hoặc cao hơn giá gốc ban đầu được xác định ngầm định bởi người dùng. Để xác minh tính hiệu lực của lệnh được đưa ra, các hợp đồng thông minh sử dụng giao thức Loopring phải nhận được các lệnh mua bán được gửi từ các thợ đào trong chính chu trình nơi mà 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 giao dịch các thẻ của họ là thẻ `A` và thẻ `B`. Alice có 15 thẻ `A` và cô ấy muốn đổi chúng lấy 4 thẻ `B`; Bob có 10 thẻ `B` và anh ta muốn có được 30 thẻ `A` từ số thẻ trên.

Ai là người mua và ai là người bán? Điều này chỉ phụ thuộc vào số tài sản mà chúng tôi dùng để cố định giá trị trên bảng báo giá. Nếu sử dụng thẻ `A` là số liệu tham chiếu, thì Alice đang mua thẻ `B` với giá là $\frac{15}{4} = 3.75$`A`, trong khi đó Bob đang bán 10 thẻ `B` với giá $\frac{30}{10} = 3.00$`A`. Trong trường hợp lấy thẻ B là số liệu tham chiếu, chúng tôi nói rằng Alice đang bán 15 thẻ `A` cho giá là $\frac{4}{15} = 0.26666667$`B` và Bob đang mua 10 thẻ `A` với giá là $\frac{10}{30} = 0.33333334$`B`. Do đó, ai là người mua hoặc người bán vẫn còn phải tùy thuộc vào từng trường hợp.

Trong tình huống đầu tiên, Alice sẵn sàng trả giá cao hơn (3.75`A`) so với giá mà Bob đang bán thẻ của mình (3.00`A`), trong khi trong trường hợp thứ hai Bob sẵn sàng trả giá cao hơn (0.33333334`B`) so với giá Alice đang bán thẻ của cô ấy (0.26666667`B`). Rõ ràng là việc trao đổi mua bán có thể xảy ra bất cứ khi nào người mua sẵn sàng trả giá bằng hoặc cao hơn giá của người bán.

$$\frac{\frac{15}{4}}{\frac{30}{10}} = \frac{\frac{10}{30}}{\frac{4}{15}} = \frac{15}{4} \cdot \frac{10}{30} = 1.25 > 1 \quad (1)$$

Do đó, để xác định việc đưa ra tập hợp n lệnh đưa ra có được giải quyết hoàn toàn hay một một phần, chúng ta cần phải biết liệu tỷ giá hối đoái cho từng sản phẩm giống như giá trị mà lệnh mua đưa ra có lớn hơn hay bằng 1 hay không. Nếu có, tất cả n lệnh giao dịch đưa ra có thể được giải quyết một phần hoặc hoàn toàn giải quyết [17].

Nếu chúng ta giới thiệu thêm một đối tác thứ ba là Charlie, như vậy Alice muốn bán ra một lượng x_1 thẻ `A` và nhận được một lượng y_1 thẻ `B`, Bob muốn bán ra một lượng x_2 thẻ `B` và muốn có được lượng y_2 thẻ `C`, và Charlie muốn trao đổi số lượng x_3 thẻ `C` để đổi lấy lượng y_3 thẻ `A`. Điều cần thiết ở đây là lượng thẻ bán ra của các bên đều là có thật, và giao dịch có thể được thực hiện nếu:

$$\frac{x_1 \cdot x_2 \cdot x_3}{y_1 \cdot y_2 \cdot y_3} \geq 1 \quad (2)$$

Xem phần 7.1 để biết thêm chi tiết về các lệnh mua bán trong Loopring.

4 Những Người Tham Gia Hệ Sinh Thái

Tất cả mọi người tham gia hệ sinh thái của Loopring đều được cung cấp đầy đủ các công cụ giống như một sàn trao đổi tập trung đã đưa ra.

- **Ví tiền**: Một dịch vụ ví hoặc giao diện thông thường có khả năng cho phép người dùng truy cập các thẻ của họ và cách gửi lệnh mua bán/trao đổi tới mạng lưới Loopring. Ví tiền sẽ được khuyến khích sử dụng để đưa ra các lệnh trao đổi bằng cách chia sẻ các khoản phí với các thợ đào trong chu trình(xem phần8). Với niềm tin rằng tương lai của việc giao dịch sẽ an toàn khi người dùng sử dụng ví cá nhân của họ, việc kết nối các nhà cung cấp thanh khoản này thông qua giao thức của chúng tôi là vô cùng quan trọng.

- **Chia Sẻ Thanh Khoản Trong Liên Kết Chuỗi Khối/ Rơ-le Vô Tuyến**: Một mạng lưới chuyển tiếp vô tuyến và khả năng chia sẻ tính thanh khoản. Khi các nút chạy phần mềm chuyển tiếp Loopring, chúng có thể tham gia vào một mạng lưới hiện có và chia sẻ thanh khoản với các rơ-le (nút chuyển tiếp) khác qua sự liên kết giữa các chuỗi khối. Sự liên kết trong chuỗi khối mà chúng tôi đang xây dựng như là một sự hoàn thành đầu tiên có khả năng chia sẻ lệnh gần với thời gian thực (1-2 giây khối), và loại bỏ các lịch sử cũ để cho phép tải nhanh hơn bởi các nút mới. Điều đáng chú ý ở đây, các nút chuyển tiếp không cần phải tham gia vào sự liên kết này; chúng có thể hoạt động riêng rẽ và không cần chia sẻ tính thanh khoản với các nút khác hoặc có thể tự tạo ra và quản lý mạng lưới chia sẻ thanh khoản của chính chúng.

- **Rơ-le/Thợ Đào Trong Chu Trình**: Rơle (nút chuyển tiếp) là các nút nhận các lệnh từ ví hoặc các nút chuyển tiếp vô tuyến, có nhiệm vụ duy trì đơn lệnh mua bán công khai đã được đưa ra và lịch sử giao dịch, và tùy chọn gửi các lệnh mua bán cho các rơ-le khác (thông qua bất kỳ các kênh ngoại tuyến nào) và / hoặc nút chuyển tiếp vô tuyến. Việc khai thác (đào) trong chu trình là một tính năng – không phải là điều bắt buộc đối với các nút chuyển tiếp. Đây là một việc thiên về tính toán và được thực hiện hoàn toàn ngoài chuỗi. Chúng tôi gọi những người có thể kích hoạt các tính năng đào trong chu trình đối các rơ-le là "Thợ đào trong chu trình", người thực hiện các lệnh mua bán trong chu trình bằng cách ghép các đơn đặt hàng khác nhau. Các nút chuyển tiếp được tự do trong việc (1) làm thế nào chúng có thể kết nối với nhau, (2) cách chúng xây dựng các lệnh mua bán được đưa ra, và (3) làm thế nào chúng khai thác được những lệnh mua bán trong chu trình (thuật toán khai thác mỏ).

- **Giao Thức Hợp Đồng Thông Minh Loopring (LPSC)**: Một nhóm các hợp đồng thông minh được công khai và sử dụng miễn phí nhằm kiểm tra các lệnh trong chu trình từ các thợ đào, giúp giải quyết các giao dịch không cần có sự tín nhiệm và chuyển giao thẻ (token) trên danh nghĩa người dùng, khuyến khích các thợ đào cũng như các dịch vụ ví điện tử bằng cách trả phí và tạo ra nhiều sự kiện. Rơle hay các trình duyệt mua bán luôn theo dõi những các hoạt động này để cập nhật kịp thời các lệnh mua bán được đưa ra cũng như lịch sử giao dịch. Xem phụ lục **??** để biết chi tiết.

- **Dịch Vụ Số (thẻ) Hóa Tài Sản (ATS)**: Đây là một cầu nối cho các loại tài sản không thể giao dịch trực tiếp trên mạng lưới của Loopring và 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 hoặc mã thông báo từ các chuỗi khác) và nhận lại các thẻ (token) có giá trị tương đương, có thể được sử dụng để đặt cọc trong tương lai. Loopring không phải là giao thức có thể trao đổi chéo (cho đến khi có giải pháp phù hợp), nhưng dịch vụ ATS cho pép người dùng trao đổi các thẻ chạy trên nền tảng ERC20 [18] với tài sản mang ý nghĩa vật chất cũng như tài sản được tạo ra từ các công nghệ chuỗi khối khác.

5 Quy Trình Trao Đổi

1. **Ủy Quyền Giao Thức**: Trong hình 2, người dùng `Y` muốn giao dịch số thẻ thông qua việc ủy quyền cho LPSC xử lý một `lượngS` của thẻ `B` mà người dùng muốn bán. Việc ủy quyền cho giao thức này số lượng thẻ mà người dùng muốn bán sẽ không bị khóa, người dùng vẫn có thể tự do di chuyển chúng trong khi lệnh trao đổi vẫn đang được thực hiện.

2. **Tạo Lệnh**: Tỉ giá hiện tại và việc tiến hành đặt lệnh mua bán cho hai loại thẻ `B` và `C` được cung cấp bởi các rơ-le hoặc các các đại lý được kết nối với mạng lưới, chẳng hạn như các trình duyệt dùng để đặt lệnh trao đổi. Người dùng `Y` có thể đưa ra lệnh trao đổi (lệnh có giới hạn) với `lượngS` và `lượngB` cụ thể cũng như các yếu tố khác thông qua bất kì ví điện tử có tích hợp. Một lượng thẻ LRx có thể được thêm vào và được dùng để làm chi phí chi trả cho các thợ đào trong chu trình; lượng phí LRx người dùng trả càng cao thì cơ hội để lệnh mua bán được xử lí càng nhanh hơn. Mã băm (hash) của lệnh được xác nhận với mã cá nhân của người dùng `Y`.

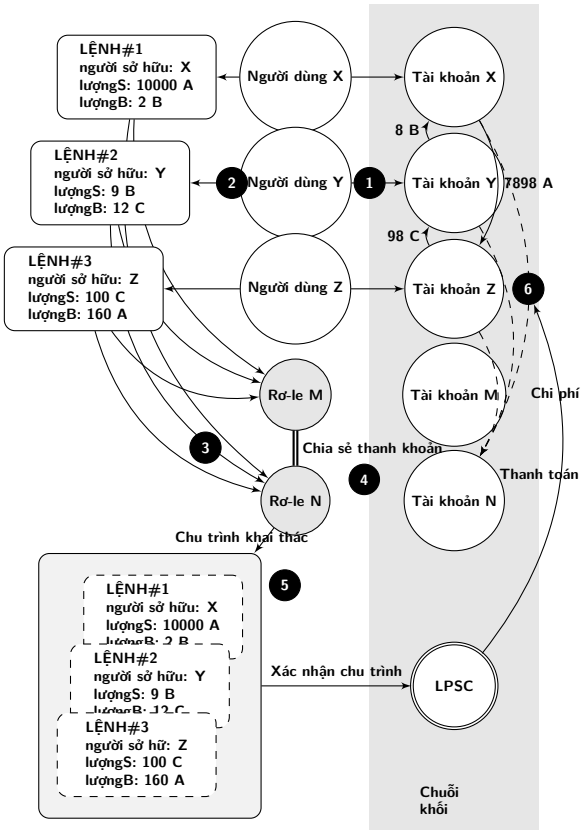

Figure 2: Quy trình trao đổi Loopring

3. **Truyền Lệnh**: Lệnh trao đổi cũng như mã xác nhận của chúng sẽ được ví điện tử gửi đến một hoặc nhiều rơ-le. Các rơ-le sẽ tiến hành cập nhật danh sách lệnh trao đổi công khai. Giao thức không yêu cầu các danh sách lệnh trao đổi phải được xây dựng theo một cách xác định, giống như ai đến trước sẽ được ưu tiên phục vụ trước. Thay vào đó, các rơ-le có quyền tự thiết kế quyết định của chúng trong việc thực hiện danh sách các lệnh mua bán.

4. **Chia Sẻ Thanh Khoản**: Các rơ-le truyền các lệnh giao dịch tới các rơ-le khác thông qua bất kỳ các phương tiện truyền thông nào. Một lần nữa cho chúng ta thấy được sự linh hoạt thông qua cách mà các nút tương tác với nhau. Để tạo điều kiện cho mức độ nhất định của kết nối mạng, chúng tôi xây dựng việc chia sẻ tính thanh khoản thông qua mạng lưới rơ-le bằng cách sử dụng một tổ hợp chuỗi khối. Như đã đề cập trong phần trước, các rơ-le vô tuyến này được sử dụng để tối ưu hóa cho tốc độ và độ phủ sóng.

5. **Chu Trình Đào (Sự Khớp Lệnh)**: Các thợ đào cố gắng hoàn thành toàn bộ hoặc một phần lệnh giao dịch đưa ra tại tỷ giá hối đoái hoặc tốt hơn bằng cách bắt cặp chúng với nhiều lệnh khác. Chu trình khai thác là nguyên nhân chính cho việc tại sao giao thức cho phép cung cấp tính thanh khoản cao trên bất kì cặp giao dịch nào. Nếu tỷ lệ thực hiện tốt hơn so với những gì người dùng `Y` đã chỉ định, thì số tiền ký quỹ được chia sẻ giữa tất cả các lệnh trao đổi trong chu trình. Như một phần thưởng, người thợ đào sẽ lựa chọn giữa việc yêu cầu một phần lợi nhuận (chia phần tiền ký quỹ, và trả lại LRx cho người dùng), hoặc đơn giản là giữ LRx làm chi phí.

6. **Xác Thực& Thanh Toán**: Chu trình xử lý lệnh mua bán được thực hiện bở LPSC. Quá trình này trải qua hàng loạt các bước kiểm tra nhằm xác thực các dữ liệu được cung cấp bởi các thợ đào và xác định rằng liệu có thể giải quyết hoàn toàn hay một phần các lệnh này (phụ thuộc vào tốc độ điền thông tin của lệnh vào trong chu trình và lượng thẻ có trong ví của người dùng). Nếu tất cả các bước kiểm tra đều được thông qua, hợp đồng thông minh sẽ tự động chuyển đổi các thẻ giữa các bên người dùng và chi trả chi phí cho thợ đào cũng như của ví trong cùng một thời điểm. Nếu số dư của người dùng `Y` được xác định bởi LPSC là không đủ, giao dịch sẽ được thu nhỏ lại: giao dịch sẽ tiếp tục được thực hiện (mở rộng đến kích thước ban đầu) khi lượng thẻ không đủ được bổ sung vào địa chỉ ban đầu, không giống như việc hủy bỏ lệnh, được thực hiện thủ công và không thể đảo ngược.

6 Sự Linh Hoạt Trong Cách Thức Hoạt Động

Có một điều quan trọng cần chú ý ở đây rằng Loopring cho phép người tham gia có sự linh hoạt đáng kể trong việc mở ra các hoạt động của chính họ. Người dùng được tự do triển khai các mô hình kinh doanh mới, mang lại lợi nhuận cho chính họ cũng như kiếm được kinh phí từ các thẻ LRx dựa trên thành quả công việc cũng như những thước đo khác trong quá trình hoạt động (nếu họ chọn). Hệ sinh thái của Loopring cũng cung cấp những khuôn mẫu và các giá trị trung bình nhằm hỗ trợ người tham gia thông qua rất nhiều các ứng dụng khác nhau.

6.1 Sổ Lệnh

Các cảm biến có thể thiết kế sổ lệnh của họ theo rất nhiều cách để hiển thị và khớp các lệnh của người đặt lệnh. Sổ lệnh đầu tiên của chúng ta triển khai theo một như mô hình OTC, nơi mà những lệnh giới hạn được định giá dựa trên đơn giá. Timestamps (Biểu thị thời gian) của lệnh, hay nói cách khác, chẳng hề liên quan gì đến sổ lệnh. Tuy nhiên, các cảm biến tự do thiết kế sổ lệnh của họ sao cho mô phỏng công cụ của trung tâm trao đổi tập trung điển hình, nơi lệnh được xếp bằng giá, trong khi vẫn tôn trọng timestamps. Nếu cảm biến có khuynh hướng đưa ra loại sổ lệnh kiểu này, họ có thể sở hữu / tích hợp với 1 chiếc ví, và có các lệnh từ ví đó gửi đi chỉ đến 1 cảm biến đơn, họ sẽ có thể khớp các lệnh dựa trên thời gian. Bất cứ cấu hình như vậy là khả thi.

Trong khi các giao thức DEX khác đôi khi yêu cầu cảm biến phải có nguồn gốc – số dư ban đầu để đặt lệnh - Loopring Relays chỉ cần tìm các đơn lệnh khớp với phù hợp để giao dịch và có thể thực hiện giao dịch mà không cần thẻ ban đầu.

6.2 Khả Năng Chia Sẻ Tính Thanh Khoản

Các cảm biến (rơ-le) được tự do thiết kế theo cách mà người sử dụng chia sẻ tính thanh khoản (các lệnh) với nhau. Khả năng liên kết trong chuỗi khối của chúng tôi là một trong những giải pháp có thể hoàn thành việc này và hệ sinh thái được tự do liên kết và giao tiếp theo ý muốn. Bên cạnh việc gia nhập một nhóm các chuỗi khối liên kết với nhau, người dùng có thể xây dựng và quản lý chuỗi khối của riêng họ, tạo ra các quy tắc/ưu đãi khi phù hợp. Các cảm biến cũng có thể hoạt động độc lập, như trong thực hiện ví tiền nhạy cảm. Tất nhiên, có những thuận lợi rõ ràng trong việc kết nối các cảm biến khác nhau trong việc tạo ra các hiệu ứng mạng lưới, tuy nhiên, các mô hình kinh doanh khác nhau có thể có được các thiết kế chia sẻ đặc biệt và phân chia phí theo bất kỳ cách nào.

7 Miêu Tả Giao Thức

7.1 Chi Tiết Của Một Lệnh

Một lệnh (order) là một gói dữ liệu miêu tả chi tiết về mục đích giao dịch của người sử dụng. Lệnh Loopring được sử dụng mô hình lệnh Mô Hình Giao Dịch Một Chiều (UDOM), được biểu diễn như sau :

```
  message Order {
    address protocol;
    address owner;
    address tokenS;
    address tokenB;
    uint256 amountS;
    uint256 amountB;
    unit256 lrcFee
    unit256 validSince; // Tổng số giây trên thời
gian tham chiếu
    unit256 validUntil; // Tổng số giây trên thời
gian tham chiếu
    uint8   marginSplitPercentage;  // [1-100]
    bool    buyNoMoreThanAmountB;
    uint256 walletId;
    // Địa chỉ tác quyền kép
    address authAddr;
    // v, r, s là các phần của việc xác nhận
    uint8   v;
    bytes32 r;
    bytes32 s;
    // Mã cá nhân dùng cho tác quyền kép,
    // Không được dùng cho việc tính toán mã
băm của lệnh,
    // Do đó lệnh chưa được xác nhận.
    string  authKey;
    uint256 nonce;
  }
```

Để đảm bảo nguồn gốc của lệnh, nó đã được đánh dấu bằng mã bảo mật của người sử dụng để chống lại việc các tham số của nó bị băm, ngoại trừ `authAddr`. Tham số `authAddr` sẽ được sử dụng cho mục đích đánh dấu các thứ tự chu trình lệnh mà lệnh này là một phần của những chu trình lệnh đó, để ngăn cản việc chạy trước (chạy trước là một trong những cách gian lận mà người sử dụng sẽ đặt lệnh dựa trên các lệnh đang bị chờ (pending-order) từ các khách hàng khác). Để biết thêm chi tiết vui lòng tham khảo mục số 9.1. Việc đánh dấu sẽ được biểu thị bằng các `v`, `r`, và `s`, và được gửi kèm theo các lệnh tham số qua hệ thống mạng. Điều này đảm bảo trật tự lệnh sẽ không bị thay đổi trong suốt quá trình. Mặc dù trật tự lệnh không bao giờ bị thay đổi nhưng giao thức vẫn có thể tính toán để biết được tình trạng hiện tại của lệnh dựa vào số dư của địa chỉ cùng với các biến số khác.

UDOM không bao gồm giá, giá phải là một số dấu phẩy động (vì Việt Nam và hệ thống chung của thế giới sử dụng dấu chấm và dấu phẩy khác nhau nên Việt Nam có thể hiểu là dấu chấm động) nhưng thay vào đó, UDOM sử dụng tỷ lệ theo kỳ và r, được biểu diễn bằng cách : `lượngS/lượngB`. Tỷ lệ không phải là một dấu phẩy động nhưng biểu thức sẽ chỉ được đánh dấu với các số nguyên không dấu khác theo yêu cầu, để giữ cho kết quả trung gian là các số nguyên không dấu và tăng độ chính xác trong tính toán.

7.1.1 Lượng Mua Vào

Khi một chu trình thợ đào khớp với các lệnh, có thể tỷ lệ tốt hơn sẽ được hiện được, cho phép người dùng nhận được nhiều `thẻB` hơn là `lượngB` đã được chỉ định. Tuy nhiên, nếu `buyNoMoreThanAmountB` được đặt là `True`, Giao thức sẽ đảm bảo người sử dụng không nhận nhiều hơn `lượngB` của `thẻB`. Như vậy, tham số UDOM của `buyNoMoreThantokenB` sẽ được xác nhận khi một lệnh được lắp hoàn toàn đầy. `buyNoMoreThantokenB` áp dụng giới hạn cho một trong hai là `lượngS` hoặc `lượngB` và cho phép người sử dụng thể hiện

ý định giao dịch chi tiết hơn so với lệnh mua/bán truyền thống.

Ví dụ : với `lượngS` = 10 và `lượngB` = 2, tỷ lệ r là = 10/2 = 5. Như vậy người sử dụng sẽ sẵn sàng bán 5 `thẻS` cho mỗi `thẻB`. Chu trình thợ đào tìm và khớp ở tỷ lệ 4, cho phép người sử dụng nhận được 2.5 `thẻB` thay vì chỉ 2. Tuy nhiên, nếu người dùng chỉ muốn 2 tokenB và lập trình `buyNoMoreThanAmountB` thành `True`, LPSC thực hiện giao dịch theo tỷ lệ 4 và người sử dụng bán 4 `thẻS` cho mỗi `thẻB`, điều này sẽ tiết kiệm 2 `thẻS`. Lưu ý nhớ rằng, việc này sẽ không tính phí khai thác (Xem phần 8.1).

Thật vậy, nếu chúng ta sử dụng

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

tĐể biểu diễn cho một lệnh dưới dạng đơn giản, tỷ lệ ETH/USD của thị trường trên sàn giao dịch truyền thống, mô hình mua-bán truyền thống có thể thể hiện lệnh thứ nhất và lệnh thứ ba nhưng không theo 2 cái đó:

1. Bán 10 ETH tại giá 300 USD/ETH. Lệnh này sẽ được biểu diễn như sau: `Order(10, ETH, 3000, USD, False)`.
2. Bán ETH tại giá 300 USD/ETH để nhận 3000 USD. Lệnh này sẽ được biểu diễn như sau: `Order(10, ETH, 3000, USD, True)`.
3. Bán 10 ETH tại giá 300USD/ETH. Lệnh này sẽ được biểu diễn như sau: `Order(3000, USD, 10, ETH, True)`.
4. Chi trả 3000 USD để mua được lượng ETH tối đa với mức giá chấp nhận được là 300 USD/ETH. Lệnh này sẽ được biểu diễn như sau: `Order(3000, USD, 10, ETH, False)`.

7.2 Chu Trình Xác Minh

Những hợp đồng thông minh Loopring thì không thực hiện các phép tính toán chuyển đổi tỷ giá hoặc số lượng. nhưng nó phải nhận và xác minh việc cung cấp các giá trị này từ nhóm bộ phận chu trình thợ đào. Những tính toán này được thực hiện bởi vòng thợ đào vì 2 lí do chính : (1) ngôn ngữ lập trình cho hợp đồng thông minh chẳng hạn như solidity [19] trên Ethereum thì không có hỗ trợ cho toán dấu phẩy động, đặc biệt là pow(x,1/n) (tính toán gốc thứ n-th của dấu phẩy động), và (2) Đó chính là mong muốn việc tính toán làm bởi ngoài chuỗi để giảm blockchain tính toán và chi phí.

7.2.1 Kiểm Tra Chu Trình Phụ

Bước này ngăn chặn những nhà đầu cơ hưởng chênh lệnh (arbitrageurs) xử lý tất cả các khoản ký quỹ trong một chu trình lệnh bằng cách triển khai những lệnh mới bên trong nó. Về cơ bản, một khi chu trình lệnh hợp lệ được tìm thấy bởi 1 chu trình thợ đào, nó có thể là tạm thời thêm vào những lệnh khác vào chu trình lệnh đó để tận dụng mọi lợi nhuận của người sử dụng margin (tỷ lệ chiết khấu). Minh họa bằng hình 3 bên dưới, tính toán cẩn trọng x1, y1, x2 và y2 sẽ làm cho sản phẩm của tất cả các tỷ lệ của lệnh là chính xác.

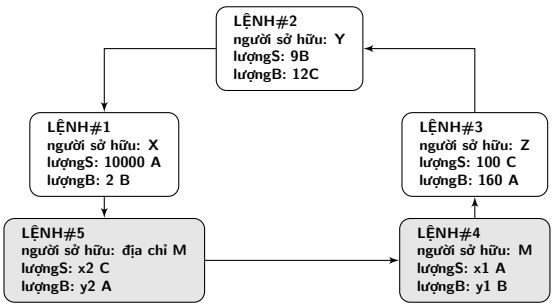

Figure 3: Một chu trình trao đổi với chu trình phụ

Đây được coi không có rủi ro, không có bất kỳ giá trị nào thêm vào hệ thống mạng và được coi là hành vi không công bằng với chu trình thợ đào. Để ngăn chặn điều này, Loopring yêu cầu một loop có hiệu lực không được chứa bất kỳ chu trình phụ nào. Để kiểm tra, LPSC đảm bảo mã không thể nằm ở vị trí mua và bán hai lần. Trong biểu đồ trên, chúng ta có thể thấy thẻ `A` là một mã thông báo bán hai lần và một mã thông báo mua hai lần, điều này sẽ không được phép thực hiện.

7.2.2 Kiểm Tra Tốc Độ Thực Hiện

Các tính toán chuyển đổi tỷ lệ trong chu trình lệnh được thực hiện bằng chu trình thợ đào bởi các lý do đã nêu ở bên trên. LPSC phải xác minh rằng các tính toán của chu trình thợ đào đưa ra là đúng hay không. Đầu tiên, nó xác minh rằng tỷ giá mua của chu trình thợ đào có thể đặt ra cho mỗi lệnh có bằng hoặc thấp hơn tỷ giá mua ban đầu do người sử dụng đặt hay không. Điều này đảm bảo người dùng nhận được tỷ lệ họ yêu cầu hoặc nhiều hơn. Một khi tỷ lệ chuyển đổi được xác nhận, LPSC đảm bảo mỗi đơn lệnh trong chu trình lệnh sẽ có cùng mức tỷ lệ chiết khấu. Ví dụ, nếu tỷ lệ chiết khấu là γ thì giá cho mỗi đơn lệnh sẽ là::

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

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

Vì vậy:

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

Nếu giao dịch vượt lệnh thứ n, thì chiết khấu lệnh sẽ là:

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

Trong đó r^i là tỷ lệ doanh thu của lệnh thứ i-th. Rõ ràng, chỉ khi tỷ lệ chiết khấu là $\gamma \geq 0$, các lệnh lắp mới này có thể thực hiện; và tỷ lệ hối đoái thứ i-th (O^i) là $\hat{r^i} = r^i\cdot(1-\gamma)$, $\hat{r^i} \leq r^i$.

Trở lại vị trí, khi mà Alice có 15 thẻ `A và muốn có 4 thẻ \verbB|`. Bob có 10 thẻ `B` và muốn có 30 thẻ `A`. Nếu lấy thẻ `A` làm tham chiếu, và Alice mua thẻ `B` với tỷ giá $\frac{15}{4} = 3.75$`A`, lúc đó Bob bán thẻ `B` với tỷ giá $\frac{30}{10} = 3.00$`A`. Tính chiết khấu : $\frac{150}{120} = 1.25$ do vậy $\frac{1}{1.25} = 0.8 = (1 - - \gamma)^2$. Do đó tỷ giá trao đổi được trả lại cho công bằng của giao dịch 2 bên là $\sqrt{0.8} \cdot 3.75 \approx 3.3541$ thẻ `A` với mỗi thẻ `B`.

Bob đưa 4 thẻ `B` và nhận 13.4164 thẻ `A`, nhiều hơn số mà Bob mong đợi là 12 cho 4 thẻ của Bob. Alice nhận 4 thẻ B như dự định nhưng chỉ mất 13.4146 thẻ A, ít hơn con số mà Alice sẽ đưa là 15 thẻ A đổi lại 4 thẻ B của cô. Lưu ý, một phần lợi nhuận sẽ được dùng để thanh toán các phí để khuyến khích thợ đào (và ví) . (Xem mục 8.1).

7.2.3 Theo Dõi&Hủy Nạp

Người dùng có thể hủy một phần hoặc toàn bộ lệnh của mình bằng cách gửi một giao dịch đặc biệt tới LPSC, chứa các thông tin chi tiết về lệnh của mình và số lượng hủy. LPSC nhận tài khoản này, lưu trữ số lượng muốn hủy và phát ra lệnh `OrderCancelled` tới hệ thống mạng. LPSC giữ theo dõi số lượng đã nạp và hủy số lượng đó bằng cách sử dụng mã băm của đơn đặt hàng có số nhận dạng. Dữ liệu này có thể truy cập công khai và `OrderCancelled` / `OrderFilled` đã phát ra khi nó thay đổi. Việc theo dõi các giá trị này rất quan trọng đối với LPSC trong quá trình giải quyết chu trình lệnh.

LPSC cũng hỗ trợ hủy bỏ tất cả các lệnh cho bất kỳ cặp giao dịch nào với lệnh `AllOrdersCancelled` và hủy tất cả lệnh cho một địa chỉ có lệnh `AllOrdersCancelled`.

7.2.4 Mở Rộng Giao Dịch

Các lệnh được mở chia theo lịch sử đã nạp và hủy số lượng, đồng thời cả số dư của tài khoản người gửi. Quá trình tìm lệnh với số lượng nhỏ nhất để nạp dựa theo các đặc điểm trên và sử dụng nó làm tham chiếu để mở rộng quy mô các giao dịch trong những chu trình lệnh.

Việc tìm chu trình lệnh có giá trị thấp nhất có thể giúp tìm ra khối lượng nạp của mỗi lệnh. Ví dụ, nếu lệnh thứ i-th là lệnh thấp nhất, khi số mã được bán từ mỗi lệnh $\hat{s}$ và số lượng mã đã mua $\hat{b}$ từ mỗi lệnh có thể được tính như sau:

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

Trong đó $\overline{s}_i$ là số dư còn lại sau khi các lệnh được điền một phần.

Trong quá trình thực hiện, chúng ta có thể đảm bảo an toàn bất kỳ lệnh nào trong chu trình lệnh để có giá trị nhỏ nhất, sau đó lặp lại thông qua chu trình lệnh nhiều nhất hai lần để tính khối lượng nạp của mỗi đơn lệnh.

Ví dụ: Nếu số lượng nhỏ nhất được nạp so với lệnh ban đầu là 5%, tất cả giao dịch trong vòng lệnh được thu nhỏ xuống 5%. Một khi giao dịch đã hoàn thành, lệnh mà có số lượng nhỏ nhất sẽ được nạp đầy hoàn toàn.

7.3 Chu Trình Thanh Toán

Nếu mỗi chu trình lệnh mua bán thỏa mãn tất cả các lần kiểm tra trước đó, thì chu trình lệnh có thể đóng lại và các giao dịch có thể thực hiện. Điều này có nghĩa là tất cả các lệnh n tạo thành một chu trình khép kín, được kết nối như trong hình 4 :

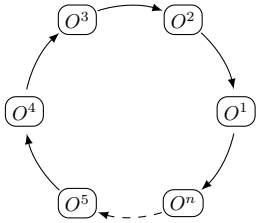

Figure 4: Chu trình thanh toán

Để thực hiện giao dịch, LPSC sử dụng hợp đồng thông minh `TokenTransferDelegate`. Việc giới thiệu một đại biểu như vậy làm cho việc nâng cấp giao thức hợp đồng thông minh dễ dàng hơn vì tất cả các lệnh chỉ cần ủy quyền cho đại biểu này thay vì cần các phiên bản khác nhau của giao thức.

Đối với mỗi lệnh trong vòng lệnh, một khoản thanh toán của thẻ `S` được thực hiện theo thứ tự tiếp theo hoặc lệnh bị hoãn trước, tùy thuộc vào triển khai, Sau đó, phí của vòng thợ đào được trả tùy thuộc vào mô hình phí được chọn bởi thợ đào. Cuối cùng, khi tất cả các giao dịch được thực hiện, `RingMined` sẽ được phát ra báo cáo

7.3.1 Phát Thông Báo Hoạt Động

Giao thức sẽ phát ra các báo cáo đã được cho phép chuyển tiếp, trình duyệt lệnh, và các lệnh khác để nhận bản cập nhập lệnh hiệu quả nhất. Lệnh phát ra báo cáo là:

- **OrderCancelled**: Một lệnh đặc biệt cụ thể đã bị hủy.
- **OrdersCancelled**: Tất cả các lệnh của một cặp giao dịch từ một địa chỉ đã bị hủy.
- **AllOrdersCancelled**: Tất cả các lệnh của tất cả các lệnh từ tất cả các cặp giao dịch từ một địa chỉ đã bị hủy.
- **RingMined**: Một chu trình lệnh đã được giải quyết thành công. Chu trình lệnh thành công này sẽ chứa dữ liệu liên quan đến việc chuyển từng chu trình thẻ bên trong.

8 Thẻ LRx

LRx là ký hiệu mã chung cho hệ sinh thái. LRC là ký hiệu cho các thẻ của Loopring trên nền Ethereum, LRQ trên nền Qtum và LRN trên nền NEO,vv.... Các loại mã LRx khác sẽ được giới thiệu trong tương lai trên các nền các nền tảng mở khác.

8.1 Mô Hình Tính Phí

Khi một người sử dụng dịch vụ tạo một lệnh, họ chỉ định số lượng LRx phải trả cho thợ mỏ theo mức phí và theo tỷ lệ phần trăm lợi nhuận (`marginSplitPercentage`), tỉ lệ phần trăm lợi nhuận do thợ mỏ yêu cầu. Đây gọi là lợi nhuận phân chia. Thợ mỏ sẽ quyết định chọn 1 trong 2 : phí hoặc lợi nhuận phân chia.

Một ví dụ cho việc phân chia lợi nhuận:

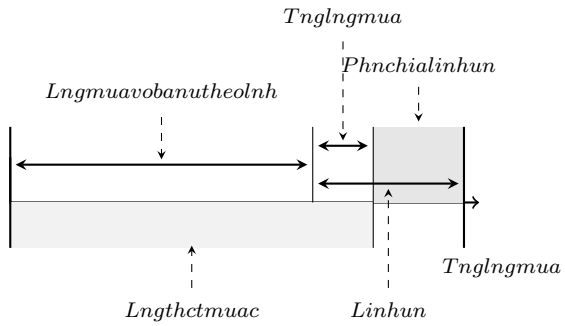

Figure 5: Một lợi nhuận phân chia 60%

Nếu lợi nhuận trong chu trình lệnh quá nhỏ, 1 thợ mỏ sẽ chọn phí LRx. Nếu ngược lại, nếu lợi nhuận phân chia lớn hơn phí LRx thì thợ mỏ sẽ chọn lợi nhuận phân chia. Tuy nhiên, có điều kiện đối với thợ mỏ khi chọn lợi nhuận phân chia, họ (người tạo lệnh) phải trả cho người đặt lệnh một khoản phí, khoản phí này bằng với khoản phí mà người đặt lệnh sẽ trả cho thợ mỏ. Điều này làm tăng khả năng người thợ mỏ sẽ chọn phí LRx. Ngoài ra, điều kiện này còn làm cho thợ mỏ thu được lợi nhuận liên tục trên các lệnh có tỷ lệ phân chia lợi nhuận thấp so với các lệnh đặt hàng giá trị cao hơn. Mô hình tính phí này giúp cho chúng ta có kỳ vọng khi thị trường tăng trưởng và ổn định sẽ có ít lợi nhuận bị đặt quá cao, và tỉ lệ phí LRx phải được giữ ở mức ổn định. Chúng ta tổng kết lại mô hình bằng biểu đồ sau:

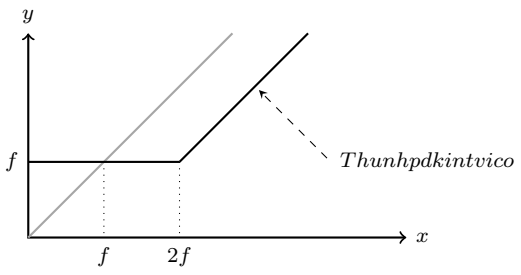

Figure 6: Mô hình tính phí của Loopring

Trong đó f là phí LRx, x là phân chia lợi nhuận, y là thu nhập từ hoạt động khai thác mỏ. $y = max(f, x - f)$ là đường thẳng cố định, nếu chi phí dùng LRx cho việc giao dịch là 0 thì phương trình $y = max(0, x - 0)$ được đơn giản hóa thành phương trình $y = x$ là đường thẳng được chỉ định bởi đường màu xám. Vậy thì kết quả là:

1. Nếu phân chia lợi nhuận bằng 0, thợ mỏ sẽ chọn phí LRx, mức này giữ mức ổn định.
2. Nếu phí LRx bằng 0, kết quả là dòng màu xám và thu nhập của thợ mỏ sẽ chạy trên mô hình tuyến tính chung.
3. Nếu lợi nhuận phân chia lớn hơn 2 lần phí LRx, thợ mỏ sẽ chọn lợi nhuận phân chia và trả LRx về cho người đặt lệnh.

Cần phải lưu ý rằng nếu phí LRx khác 0, cho dù thợ mỏ có chọn phí LRx, thì sẽ luôn luôn có sự chuyển đổi LRx giữa thợ mỏ và người đặt lệnh. Hoặc là thợ mỏ nhận phí LRx, hoặc là thợ mỏ trả lại phí LRx cho người đặt lệnh và nhận phân lợi nhuận phân chia. Thợ mỏ sẽ chia sẻ khoản phí nhất định đối với ví. Khi một người đặt lệnh đặt một đơn lệnh bằng ví và lệnh đó đầy ví thì Ví sẽ trả thưởng lại một phần phí LRx hoặc một phần lợi nhuận phân chia. Mặc dù đây mới chỉ là ước tính, nhưng chúng tôi dự tính sẽ trả thưởng khoảng 20% - 25% của phí thu được. Ví tích hợp giao thức Loopring chính là một trong những mục tiêu chính cho những người sử dụng có ít hoặc ko có thu nhập.

8.2 Quản lý Tính Phân Quyền

Bản chất của vấn đề là giao thức Loopring là giao thức cộng đồng vì nó dựa vào sự phối hợp, đồng tâm giữa các thành viên trong giao thức để cùng hoạt động hiệu quả theo mục tiêu đã hướng tới. Điều này không giống với các giao thức mã hóa kinh tế lớn khác, nó có tính hữu ích trong việc bảo vệ các vấn đề có tính cơ chế [20], grim trigger cân bằng và biên hợp lý. Để giải quyết vấn đề này, thẻ LRx không chỉ đóng vai trò là phí sử dụng mà còn đóng vai trò như là ưu đãi tài chính cho các thành viên trong hệ sinh thái. Sự liên kết này là cần thiết để có thể áp dụng rộng rãi cho bất kỳ giao thức nào, đặc biệt là các giao thức trao đổi, vì giao thức trao đổi có thành công hay không dựa vào khả năng thanh khoản trong hệ sinh thái phân quyền mạnh mẽ Các mã LRx sẽ được sử dụng trong các bản cập nhập giao thức trong hệ quản lý phân quyền. Bản cập nhập hợp đồng thông minh cũng sẽ quản lý bởi những người giữ mã trong tay nhằm mục đích đảm bảo cho sự an toàn và xuyên suốt, đồng thời đảm bảo giảm thiểu rủi ro thông qua sự không tương thích. Vì lí do hợp đồng thông minh không thể thay đổi khi đã triển khai, nên giảm thiểu các nguy cơ do dApps hoặc người sử dụng cuối sử dụng các phiên bãn cũ hoặc không cho tự cập nhập hợp đồng. Khả năng nâng cấp rất quan trọng đối với giao thức vì nó phải thích ứng với thị trường và các blockchain nền. Quản lý phân quyền bởi những người nắm LRx chính sẽ cho phép giao thức được cập nhật mà không

làm gián đoạn đến dApps, người sử dụng, hoặc không dựa quá nhiều vào sự quá tải của hợp đồng thông minh. Thẻ LRx có nguồn cung cố định, và trong trường hợp của LRC, tỷ lệ phần trăm nhất định lượng thẻ được khóa từ tổ chức Loopring và được phân bố cho các quỹ có mục đích cộng đồng [21]. Tuy nhiên, những người nắm chính LRx không phải là những người duy nhất có khả năng đề xuất hướng cập nhập cho giao thức mà còn có : các thợ đào/rơ –le, ví, các nhà phát triển và những người khác nằm trong hệ sinh thái đều có tiếng nói và tiếng nói của họ đều sẽ được lắng nghe. Trong thực tế, những thành phần không nắm bất kỳ thẻ LRx nào để thực hiện các vai trò tương ứng của họ (người tạo lệnh/ người khớp lệnh truyền thống, những nhà tạo lập thị trường không bắt buộc trữ thẻ) chúng tôi phải cho họ phương pháp thay thế để đảm bảo tôn trọng lợi ích của họ. Hơn nữa, việc bỏ phiếu bằng tokenbased "đơn giản", bao gồm cả trên chuỗi và ngoài chuỗi, thì không hoàn hảo chọ việc không đồng ý, như việc cử tri bỏ phiếu thấp và sỡ hữu thẻ tập trung sẽ gây ra rủi ro. Do đó, mục tiêu là triển khai một mô hình quản trị được xây dựng trong những lớp nền, và dựa trên sự chia sẻ kiến thức để đưa ra một số quy trình là tiêu chuẩn. Điều này có thể được tạo điều kiện bởi các tổ chức phối hợp cung cấp tín hiệu từ một nhóm người tham gia đa dạng, và, có lẽ, từ các đầu mối giao thức đã được thiết lập trước. Như thế cho ra kết quả, quỹ Loopring sẽ chắc chắn được phát triển từ các nhà phát triển giao thức thành những nhà quản lý giao thức.

9 Phòng Chống Gian Lận và Tấn Công

9.1 Ngăn Ngừa Hành Động Chạy trước

Trong các giao dịch phân quyền, "chạy trước" là việc khi ai đó cố gắng sao chép giải pháp thương mại của một nút khác và khai thác nó trước khi giao dịch ban đầu nằm trong vùng giao dịch đang được chờ xử lý (mempool). Điều này có thể xảy ra khi người thực hiện việc chạy trước với mức phí giao dịch cao hơn (giá gas). Quy trình chính để có thể thực hiện việc "chạy trước" trong Loopring (và bất kỳ giao thức nào đối với khớp lệnh) là dựa theo nguyên tắc lệnh-hoán đổi: khi một người thực hiện việc chạy trước đánh cắp một hoặc nhiều lệnh từ một giao dịch đang trong quá trình chờ xử lý; và, cụ thể cho Loopring: khi một người chạy phía trước đánh cắp toàn bộ vòng đặt hàng từ một giao dịch đang chờ xử lý. Khi một giao dịch submitRing chưa được xác nhận và vẫn ở trong vùng nhớ và đang chờ xử lý, bất kỳ ai cũng có thể dễ dàng phát hiện ra một lệnh như vậy và thay thế địa chỉ khai thác `minerAddress` bằng địa chỉ riêng của họ (`filcherAddress`), sau đó họ có thể xác nhận lại lệnh mới với `filcherAddress` để thay thế lệnh cũ của chu trình. Người tấn công có thể đặt giá gas cao hơn và gửi một giao dịch mới với hy vọng rằng người khai thác mỏ sẽ chọn giao dịch mới của mình vào khối tiếp theo thay vì giao dịch submitRing gốc. Các giải pháp trước đây nhằm giải quyết vấn đề này vẫn còn nhiều nhược điểm quan trọng như: yêu cầu nhiều lệnh hơn và vì vậy gây tốn nhiều chi phí cho việc đào; và sử dụng ít nhất hai lần khối để giải quyết một lệnh. Giải pháp mới của chúng tôi, Tác quyền kép (Dual Authoring) [22], bao gồm cơ chế thiết lập hai mức ủy quyền cho các lệnh - một áp dụng cho việc xử lí, và một áp dụng cho khai thác chu trình. Quá trình Tác quyền kép bao gồm:

1. Đối với mỗi lệnh được đưa ra, phần mềm ví điện tử sẽ tạo ra cặp khóa công khai /khoá cá nhân ngẫu nhiên và đặt cặp khóa vào đoạn mã JSON của lệnh. (Một thay thế là sử dụng địa chỉ có nguồn gốc từ khóa công khai thay vì sử dụng chính khóa công khai để giảm kích thước dung lượng (byte). Chúng ta sử dụng `authAddr` để biểu diễn một địa chỉ như vậy, và `authKey` đại diện cho khóa cá nhân kết hợp `authAddr`).

2. Tính toán băm của lệnh với tất cả các trường theo thứ tự ngoại trừ`r`, `v`, `s`, và `authKey`), và ký vào bảng băm bằng khóa cá nhân của chủ sở hữu (chứ không phải `authKey`).

3. Ví sẽ gửi đơn lệnh cùng với `authKey` để chuyển tiếp cho chu trình khai thác. Thợ đào sẽ xác minh rằng`authKey` và `authAddr` đã được ghép nối chính xác và lệnh của chữ ký có giá trị đối với địa chỉ chủ sở hữu.

4. Khi một chu trình lệnh được xác định, thợ đào sẽ sử dụng `authKey` của mỗi lệnh để ký vào các mã băm, `minerAddress` của chu trình và tất cả các tham số khai thác. Nếu một order-ring có chứa n đơn đặt hàng, sẽ có n chữ ký của n `authKey`. Chúng tôi gọi những chữ ký này là những `authSignature`. Người khai thác chu trình cũng có thể cần phải ký kết băm của vòng cùng với tất cả các tham số khai thác bằng khoá cá nhân của `minerAddress`.

5. Người khai thác chu trình gọi hàm submitRing với tất cả các thông số, cũng như tất cả các `authSignature` phụ. Lưu ý rằng các `authKey` KHÔNG phải là một phần của giao dịch trên chuỗi và do đó vẫn chưa được biết đối với các bên không phải là người khai thác chu trình.

6. Giao thức Loopring sẽ xác minh mỗi `authSignature` với `authAddr` tương ứng của mỗi đơn đặt hàng, và từ chối chu trình lệnh nếu bất kỳ `authSignature` nào bị thiếu hoặc không hợp lệ.

Kết quả cho thấy:

- Xác nhận của lệnh (bằng khoá cá nhân của địa chỉ chủ sở hữu) đảm bảo thứ tự không thể sửa đổi, bao gồm `authAddr`.
- Xác nhận của thợ đào (bằng mã khóa cá nhân của `minerAddress`) nếu được cung cấp, đảm bảo rằng không ai có thể sử dụng danh tính của mình để khai thác một lệnh giao dịch.

- Các `authSignature` đảm bảo toàn bộ chu trình giao dịch không thể sửa đổi, bao gồm minerAddress, và không có giao dịch nào có thể bị đánh cắp.

Tác quyền kép giúp ngăn chặn việc tráo đổi chu trình và tráo đổi lệnh trong khi vẫn đảm bảo việc giải quyết các lệnh trao đổi trong chu trình và có thể được thực hiện trong một giao dịch duy nhất. Ngoài ra, tác quyền kép mở cửa cho rơ-le để chia sẻ đơn đặt hàng 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 đơn đặt hàng giá giới hạn, có nghĩa là các dấu thời gian của đơn đặt hàng bị bỏ qua. Điều này ngụ ý rằng hoạt động thương mại ở phía trước không ảnh hưởng đến giá thực tế của thương mại đó, nhưng có ảnh hưởng đến việc nó được thực hiện hay không.

10 Những Nguy Cơ Tấn Công Khác

10.1 Tấn Công Mạo Danh (Sybil) hoặc Tấn Công Từ Chối Dịch Vụ (DOS)

Một số người dùng có ý định xấu có thể thực hiện trực tiếp hoặc giả dạng để 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 dựa trên các tiêu chí của riêng chúng – bằng cách ẩn hoặc hiện - hầu hết các lệnh này sẽ bị từ chối do không mang lại giá trị khi khớp lệnh. Bằng cách sử dụng các cảm biến để kiểm soát các lệnh được đưa ra, chúng ta nhận thấy rằng việc tấn công bằng cách gửi hàng loạt các lệnh nhỏ không còn là mối đe dọa đến mạng lưới nút của Loopring.

10.2 Tấn Công Bằng Cách Sử Dụng Các Địa Chỉ Không Đủ Số Dư

Một số người có thể xác nhận và gửi các lệnh có giá trị đặt hàng lớn hơn không nhưng địa chỉ thực sự có số dư bằng không. Các nút có thể theo dõi và nhận thấy rằng một số lệnh thực tế xuất phát từ các địa chỉ có số dư bằng không, cập nhật các trạng thái lệnh cho phù hợp và sau đó loại bỏ chúng. Mặc dù cần phải tốn thời gian để các nút có thể cập nhật trạng thái của một lệnh, nhưng cũng có thể thông qua cách lựa chọn để giảm thiểu điều này, ví dụ, các nút có thể bỏ qua các lệnh từ các địa chỉ có trong danh sách đen và cũng như các lệnh có liên quan.

11 Kết Luận

Giao Thức Loopring thiết kế thành một lớp nền cơ sở cho trao đổi phi tập trung. Trong khi làm như vậy, giao thức này đã đào sâu vào cái cách mà con người chúng ta trao đổi tài sản và giá trị. Tiền, như một vật trung gian, giúp cho thuận tiện hoặc thay thế các hình thức trao đổi hàng hóa và giải quyết vấn đề trùng hợp về nhu cầu [23], theo đó hai bên trao đổi phải có nhu cầu mỗi lợi ích và dịch vụ khác với bên còn lại. Tương tự như vậy, giao thức Loopring hướng đến nhiệm vụ phân phối các sự trùng hợp về nhu cầu trong các cặp giao dịch, bằng cách sử dụng khớp vòng để hoàn thành trao đổi dễ dàng hơn. Điều này có ý nghĩa đối với xã hội và thị trường trao đổi mã điện tử, tài sản truyền thống và nhiều thứ nữa. Thật vậy, cũng như tiền mã hóa phi tập trung là mối đe dọa đối với tiền của riêng một quốc gia kiểm soát tiền đó, thì ở quy mô khác, giao thức tổ hợp này có thể phù hợp với những người trao đổi (người tiêu dùng/ nhà sản xuất) , là mối đe dọa về mặt lý thuyết đối với khái niệm về tiền bạc. Các lợi ích của giao thức, bao gồ:

- Quản lý lệnh ngoài chuỗi và thanh toán trên chuỗi mang ý nghĩa giảm thiểu chi phí cho việc bảo mật.
- Tính thanh khoản lớn hơn nhờ chu trình thợ đào và tính chia sẻ lệnh.
- Tác quyền kép giải quyết vấn đề lỗi "chạy-trước" đối với tất cả các sàn giao dịch phi tập trung và người dùng của họ hiện nay phải đối mặt.
- Miễn phí và công khai các hợp đồng thông minh để cho phép bất kỳ dApp nào cso thể xây dựng và tương tác với giao thức.
- Tiêu chuẩn hóa những người tham gia cho phép tạo mạng lưới và cải thiện trải nghiệm người dùng cuối.
- Mạng lưới được duy trì linh hoạt thông qua sổ lệnh và giao tiếp.
- Giảm rào cản các đường vào có nghĩa là làm giảm chi phí các nút tham gia mạng và người dùng cuối.
- Ẩn danh trực tiếp giao dịch từ ví của người dùng.

12 Lời Cảm Ơn

Chúng tôi muốn bày tỏ lòng biết ơn của chúng tôi với các cố vấn của chúng tôi, những người đã đưa ra lời khuyên cũng như tất cả người trong cộng đồng đã chào đón và hào phóng chia sẻ kiến thức của các bạn. Đặc biệt, chúng tôi xin cảm ơn Shuo Bai (từ ChinaLedger); xin cảm ơn các giáo sư Haibin Kan; Alex Cheng, Hongfei Da; Yin Cao; Xiaochuan Wu; Zhen Wang, Wei Yu, Nian Duẩn, Jun Xiao, Jiang Qian, Jiangxu Xiang, Yipeng Guo, Dahai Li, Kelvin Long, Huaxia Xia, Jun Ma và Encephalo Path đã xem xét và cung cấp phản hồi về dự án này của chúng tôi.

References

[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.