Loopring:
Децентрализованный протокол обмена

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

9 мая 2018 г.

Аннотация

Loopring - открытый протокол для создания децентрализованных бирж. Loopring работает как набор смарт контрактов, ответственных за торговлю и взаиморасчеты, причем объединение и передача ордеров происходит офчейн. Протокол является бесплатным, расширяемым и служит стандартным строительным блоком для децентрализованных приложений (dApps), которые включают функциональные возможности обмена. Его совместимые стандарты способствуют анонимной торговле. Важным улучшением по сравнению с существующими децентрализованными протоколами обмена является способность ордеров смешиваться и взаимодействовать с другими ордерами, устраняя ограничения торговых пар и резко увеличивая ликвидность. Loopring также использует уникальное и надежное решение для предотвращения опережающей сделки: невозможно отправить транзакции в блок быстрее, чем это сделает валидный узел. Loopring является блокчейн независимым и развертывается на любом блокчейне, поддерживающем смарт контракты. На момент написания статьи он работает на Ethereum [1] [2], а Qtum [3] и NEO [4] на стадии разработки.

1 Введение

С ростом количества активов на базе блокчейнов значительно увеличилась потребность в обмене этими активами между пользователями. По мере ввода новых токенов, включая токенизацию традиционных активов, эта потребность будет только увеличиваться. Если исключить спекулятивную составляющую торговли, возможность обмена одной криптовалюты на другую является основополагающей для более крупной экосистемы. Действительно, в криптовалютах есть скрытый потенциал [5], который полностью можно раскрыть лишь с возможностью свободно передавать и преобразовывать эти активы.

Таким образом, надежный обмен токенами является обязательным для технологии блокчейн. Однако до сих пор крипто-энтузиасты в основном торговали токенами на традиционных централизованных биржах. Протокол Loopring необходим, потому что, как отмечено еще в Биткойн [6], что в отношении электронных денег “основные преимущества теряются, если третья сторона попрежнему нуждается в предотвращении двойных расходов”, поэтому основные преимущества децентрализованных активов также исчезают, когда они должны проходить через закрытые, централизованные биржи.

Торговля токенами на централизованных биржах не имеет смысла, поскольку они не поддерживают преимущества, которыми пользуются соответствующие децентрализованные проекты. Существуют также многочисленные риски и ограничения при использовании централизованных бирж, которые описаны ниже. Децентрализованные биржи (DEXs) [7] [8] [9] попытались решить эти проблемы и, во многих случаях, преуспели в уменьшении рисков безопасности, используя блокировки. Однако, поскольку DEX становятся ключевым элементом для новой экономики, есть значительные возможности для повышения эффективности. Loopring стремится предоставить модульные инструменты для децентрализованных бирж с его открытым протоколом, не зависящем от dApp.

2 Обзор существующих бирж

2.1 Недостатки централизованных бирж

Три основных недостатка централизованных бирж; 1) Отсутствие безопасности, 2) Отсутствие прозрачности и 3) Отсутствие ликвидности.

Отсутствие безопасности возникает из-за того, что пользователи обычно делегируют контроль за своими

секретными ключами одному централизованному объекту. Таким образом, появляется возможность того, что централизованные биржи станут жертвами хакеров. Безопасность и риски хакерских атак, с которыми сталкиваются все централизованные биржи, хорошо известны [10] [11], но часто воспринимаются в качестве "вынужденных рисков" ради торговли токенами. Централизованные биржи по-прежнему являются лакомым куском для хакеров, поскольку их сервера хранят более миллиона долларов средств пользователей. Разработчики бирж также могут делать случайные ошибки в коде, от которых никто не застрахован. И самое главное, что пользователи не контролируют свои токены, когда они депонированы на централизованной бирже.

Отсутствие прозрачности подвергает пользователей риску наткнуться на мошенническую биржу. Различие здесь заключается в малейших намерениях биржевого оператора, поскольку пользователи по-настоящему не владеют своими собственными активами на централизованных биржах, а скорее имеют особый вид долговой расписки. Когда токены отправляются на кошелек биржи, она берет их на хранение и предлагает долговую расписку. Таким образом, все сделки производятся между долговыми расписками пользователей. Когда пользователи погашают свои долговые расписки перед биржей, получают токены обратно на свой внешний кошелек. Во всем этом процессе отсутствует прозрачность, и биржа может закрыть, заморозить вашу учетную запись, обанкротиться и т. д. Также возможно, что они используют активы пользователя для других целей во время хранения, например, выдавая их третьим лицам. Отсутствие прозрачности может стоить пользователям как полной потери средств, так и более высокие комиссионные сборы, задержки, регуляторные риски и неисполненные ордера.

Отсутствие ликвидности. С точки зрения биржевых операторов фрагментированная ликвидность препятствует появлению новых бирж из-за двух сценариев «победитель забирает все». Во-первых, выигрывает биржа с наибольшим количеством торговых пар, потому что пользователи считают, что желательно проводить все свои сделки на одной бирже. Во-вторых, выигрывает биржа с большей книгой заказов из-за благоприятных спрэдов между спросом и предложением для каждой торговой пары. Это препятствует конкуренции со стороны новичков, потому что им сложно создать первоначальную ликвидность. В результате многие биржи удерживают высокую долю рынка, несмотря на жалобы пользователей и даже серьезные инциденты с хакерами. Стоит отметить, что, поскольку централизованные биржи занимают большую долю на рынке, они становятся все более привлекательной целью для взлома.

С точки зрения пользователей, фрагментированная ликвидность значительно снижает удобство. В централизованной бирже пользователи могут торговать только в собственных пулах ликвидности биржи, по собственной книге заказов и между поддерживаемыми парами токенов. Для обмена токена `A` на токен `B` пользователи должны пойти на биржу, которая поддерживает оба токена или регистрироваться на разных биржах, раскрывая личную информацию. Пользователям часто приходится выполнять предварительные или промежуточные сделки, как правило, в паре с BTC или ETH, оплачивая спреды в процессе обмена. Наконец, книги заказов могут быть недостаточно глубокими, чтобы завершить торговлю без изменения цены. Даже если биржа претендует на обработку больших объемов, нет никакой гарантии, что этот объем и ликвидность не являются поддельными [12].

Результатом этого являются пробои ликвидности и фрагментированная экосистема, которая напоминает классическую финансовую систему, при этом значительный объем торговли централизован на нескольких биржах. Обещания ликвидности блокчейнов не имеют смысла в рамках централизованных бирж.

2.2 Недостатки децентрализованных бирж

Децентрализованные биржи отличаются от централизованных отчасти тем, что пользователи контролируют свои секретные ключи (активы) и совершают сделки непосредственно на основном блокчейне. Они успешно уменьшают многие из вышеперечисленных рисков, связанных с безопасностью. Однако проблемы сохраняются в отношении производительности и структурных ограничений.

Ликвидность зачастую остается проблемой, поскольку пользователи должны искать контрагентов через разрозненные пулы ликвидности. Эффекты фрагментированной ликвидности присутствуют, если DEX или dApps не используют согласованные стандарты для взаимодействия, и если ордера не распространяются на большую сеть. Ликвидность списков лимитных ордеров и, в частности, их отказоустойчивость – как быстро заполненные лимитные ордера восстанавливаются – могут существенно повлиять на оптимальные торговые стратегии [13]. Отсутствие таких стандартов привело не только к уменьшению ликвидности, но и к воздействию множества потенциально небезопасных проприетарных смарт контрактов.

Кроме того, поскольку сделки производятся на блокчейне, DEXs наследуют ограничения этого блокчейна, а именно: масштабируемость, задержки в выполнении (майнинг) и дорогостоящие изменения ордеров. Таким образом, книга заказов блокчейна не очень хорошо масштабируется, так как выполнение кода на блокчейне затратно (газ), что делает несколько отмененных ордеров весьма дорогостоящей операцией.

Наконец, поскольку списки ордеров являются общедоступными, транзакция по размещению ордера видна майнерам, поскольку она ожидает, что ее добавят в следующий блок и только после этого помещают в список ордеров. Эта задержка подвергает пользователя

риску оказаться не у дел, когда его ордер никогда не исполнится.

2.3 Гибридные решения

По вышеуказанным причинам основанные на блокчейне биржи имеют ограничения, которые делают их неконкурентоспособными по сравнению с централизованными биржами. Существует компромисс между ончейн операциями, централизованными биржами и гибкостью ордеров. Протоколы, такие как Loopring и 0x [14], совмещают возможности ончейн операций с офчейн управлением ордерами. Эти решения реализованы в открытых смарт контрактах, что ограничивает возможности масштабирования, выполняя несколько функций офчейн и предоставляя узлам гибкость при выполнении критических ролей для сети. Однако и в гибридной модели остаются недостатки [15]. Протокол Loopring предлагает значимые различия в подходе к гибридному решению, описанные в этой статье.

3 Протокол Loopring

Loopring - это не DEX, а модульный протокол для построения DEX для нескольких блокчейнов. Мы разбираем на составные части традиционную биржу и предлагаем вместо нее набор открытых смарт контрактов и децентрализованных участников. Роли в сети делятся на кошельки, ретрансляторы, консорциум блокчейнов, разделяющих ликвидность, обозреватели списков ордеров, майнеров и сервисы токенизации активов. Перед определением каждого из них мы должны сначала разобраться с ордерами в Loopring.

3.1 Кольцевой ордер

Ордера в Loopring представляют собой так называемые Unidirectional Order Model (UDOM) [16]. UDOM представляет ордер как запрос на обмен токенов, `amountS`/`amountB`, (сумма для продажи/покупки) вместо цен спроса и предложения. Поскольку каждый ордер является всего лишь обменным курсом между двумя токенами, отличительной особенностью протокола является смешивание и сопоставление нескольких ордеров в кольцевой ордер. Используя до 16 ордеров вместо одной торговой пары, имеем резкое увеличение ликвидности и потенциал для выравнивания цен.

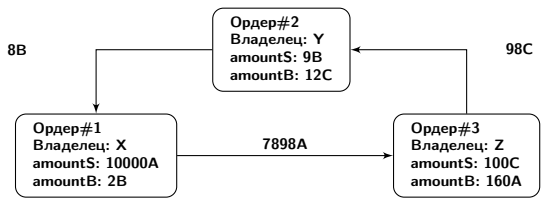

Рис. 1: Кольцевой ордер с 3 участниками

На приведенном выше рисунке показан кольцевой ордер с тремя участниками. Каждый токен ордера на продажу (`tokenS`) является другим токеном ордера на покупку (`tokenB`). Это создает цикл, который позволяет каждому заказу обменивать свои токены, не требуя обратного обмена для своей пары. Разумеется, традиционная торговля парными ордерами по-прежнему будет выполняться, она по существу является вырожденным случаем кольцевого ордера.

Definition 3.1 (кольцевой ордер) *Пусть C_0, C_1, $\cdots$, C_{n-1} n различных токенов, $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ n ордеров. Эти ордера можно объединить в кольцевой ордер для торговли:*

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

где n это длина кольцевого ордера, а $i \oplus 1 \equiv i+1 \mod n$.

Кольцевой ордер действителен, когда все составные транзакции могут быть выполнены по обменному курсу, равному или превосходящему исходную ставку, указанную пользователем. Чтобы проверить валидность кольцевого ордера, смарт контракты протокола Loopring должны получать кольцевые ордера от майнеров.

Предположим, что Алиса и Боб хотят обменять свои токены `A` и `B`. У Алисы 15 токенов `A` и она хочет за них 4 токена `B`; У Боба 10 токенов `B` и он хочет за них 30 токенов `A`.

Кто покупает и кто продает? Это зависит только от токена, который мы фиксируем, чтобы определить ценовые котировки. Если токен `A` является эталонным, тогда Алиса покупает токен `B` по цене $\frac{15}{4} = 3.75$`A`, в то время, как Боб продает 10 токенов `B` по цене $\frac{30}{10} = 3.00$`A`. В случае фиксации токена `B` как эталона, мы говорим, что Алиса продает 15 токенов `A` по цене $\frac{4}{15} = 0.26666667$`B` и Боб покупает 10 токенов `A` по цене $\frac{10}{30} = 0.33333334$`B`. Следовательно, покупатель и продавец определяются произвольным образом.

В первом случае Алиса готова заплатить более высокую цену ($3,75$`A`), чем Боб, который продает свои токены за ($3,00$`A`), а во втором случае Боб готов заплатить более высокую цену (0.33333334`B`), чем Алиса, которая продает свои токены за (0.26666667`B`). Понятно, что торговля возможна, когда покупатель готов заплатить равную или более высокую цену, чем цена продавца.

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

Таким образом, для того, чтобы набор n ордеров мог быть выполнен полностью или частично, нам нужно знать, является ли произведение каждого из обменных курсов числом больше или равным 1. Если это так, все n ордеров могут быть либо частично, либо полностью выполнены [17].

Если мы представим третьего участника Чарли, причем Алиса захотела продать x_1 токенов `A` и получить y_1 токенов `B`, Боб хочет продать x_2 токенов `B` и получить y_2

токенов `C`, а Чарли хочет продать x_3 токенов `C` и получить y_3 токенов `A`. Необходимые токены присутствуют, и торговля возможна, если:

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

Смотрите главу 7.1 для более детальной информации о ордерах Loopring.

4 Участники экосистемы

Следующие участники экосистемы совместно предоставляют весь функционал, который может предложить централизованная биржа.

- **Кошельки**: Обычный кошелек, который дает пользователям доступ к их токенам и позволяет отправлять ордера в сеть Loopring. Кошельки будут стимулировать создание ордеров путем разделения комиссий с майнерами (см. главу 8). В будущем торговля будет происходить в рамках безопасных кошельков пользователей, подключение этих пулов ликвидности через наш протокол имеет первостепенное значение.

- **Обмен ликвидностью с помощью ретрансляторов**: Сеть ретрансляторов для обмена ордерами и ликвидностью. Когда узлы запускают программное обеспечение ретрансляторов Loopring, они могут присоединиться к существующей сети и обмениваться ликвидностью с другими ретрансляторами через блокчейн. Блокчейн, который мы строим в качестве первой реализации, имеет доступ к распределению ордеров в режиме реального времени (1-2-секундные блоки) и обрезает старую историю, чтобы обеспечить более быструю загрузку новыми узлами. Примечательно, что ретрансляторы не должны присоединяется к этой сети; они могут действовать в одиночку и не делиться ликвидностью, или они могут запускать и управлять своей собственной сетью обмена ликвидностью.

- **Кольцевые майнеры**: Ретрансляторы – это узлы, которые получают ордера от кошельков или сети ретрансляторов, поддерживают списки ордеров и историю торговли и, возможно, отправляют ордера на другие ретрансляторы (через любую произвольную офчейн среду) и/или узлы ретрансляционной сети. Майнинг – это функция, но не обязательная для ретрансляторов. Он вычислительно тяжелый и полностью происходит офчейн. Мы называем ретрансляторы с включенной функцией майнинга "кольцевыми майнерами", которые создают кольцевые ордера, объединяя одиночные ордера. Ретрансляторы свободны в выборе того, (1) как они предпочитают взаимодействовать друг с другом, (2) как они строят свои списки ордеров, и (3) как они обрабатывают кольцевые ордера (алгоритмы майнинга).

- **Смарт контракты протокола Loopring (LPSC)**: Набор публичных и бесплатных смарт контрактов, который проверяет кольцевые ордера, полученные от кольцевых майнеров, обрабатывает и передает токены от имени пользователей, стимулирует майнеров и кошельки посредством комиссий и выдает результаты. Ретрансляторы принимают эти результаты, чтобы хранить списки ордеров и историю торговли в актуальном состоянии. Смотри приложение **??** для более детальной информации.

- **Службы токенизации активов (ATS)**: Связь между активами, которыми нельзя напрямую торговать через Loopring. Они являются централизованными службами, управляемыми надежными компаниями или организациями. Пользователи депонируют активы (реальные, фиат или токены) и получают токены, которые могут быть погашены в будущем. Loopring не является протоколом межцепочечного обмена (пока не будет найдено подходящее решение), но ATS позволяет торговать токенам ERC20 [18] с физическими активами, а также с токенами других блокчейнов.

5 Процесс обмена

1. **Протокол авторизации**: На рисунке 2, пользователь `Y` хочет обменять токены, он разрешает LPSC обрабатывать `amountS` токенов `B`. Это не блокирует токены пользователя, которые могут свободно перемещаться во время обработки ордера.

2. **Создание ордера**: Текущий курс и список ордеров для токена `B` с токеном `C`, предоставляются ретрансляторам или другим агентами, подключенными к сети, таким как обозреватели списков ордеров. Пользователь `Y` размещает ордер (лимитный ордер) с указанием `amountS` и `amountB` и другими параметрами через любой интегрированный кошелек. Сумма LRx может быть добавлена в ордер как комиссия для майнеров; чем больше количество LRx, тем больше вероятность быть обработанным майнером раньше остальных. Хэш ордера подписан с помощью секретного ключа пользователя `Y`.

3. **Распространение ордера**: Кошелек отправляет подписанный ордер одному или нескольким ретрансляторам. Ретрансляторы обновляют свой список ордеров. Протокол не требует, чтобы списки ордеров были построены определенным образом, например, первый-пришел-первый-исполнился. Вместо этого ретрансляторы имеют право принимать собственные решения при построении своих списков ордеров.

4. **Обмен ликвидностью**: Ретрансляторы передают ордер другим ретрансляторам через произвольную среду взаимодействия. Опять же, существуют различные варианты того, как будут взаимодействовать узлы. Чтобы облегчить определенный уровень сетевого подключения, существует встроенная сеть ретрансляторов с обменом ликвидностью, использующая блокчейн. Как упоминалось в предыдущем разделе, эта сеть ретрансляторов оптимизирована по скорости и удобству подключения.

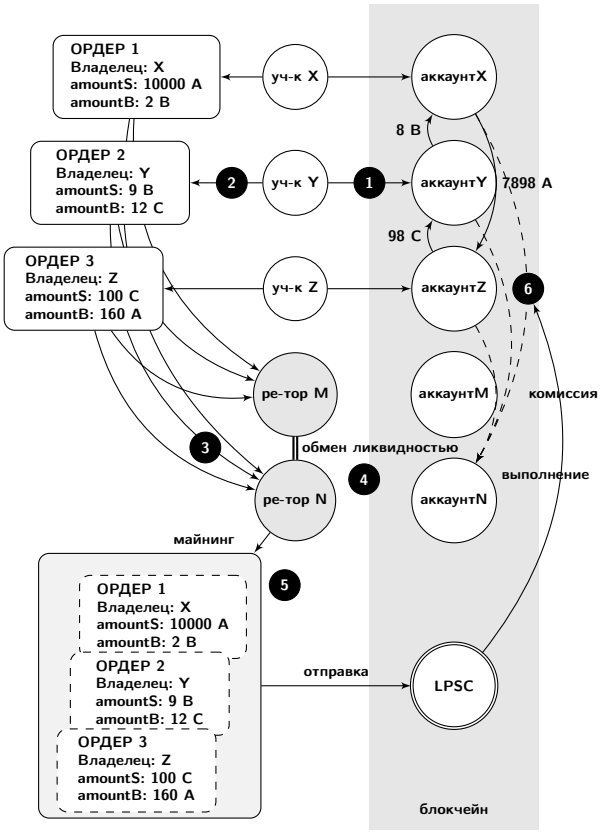

Рис. 2: Процесс обмена в Loopring

5. **Майнинг (Согласование ордеров)**: Майнеры пытаются выполнить ордер полностью или частично по данному обменному курсу, сопоставляя его с несколькими другими ордерами. Майнинг является основной причиной, по которой протокол способен обеспечить высокую ликвидность по любой паре. Если текущий курс лучше, чем заданный пользователем Y, маржа распределяется между всеми ордерами в кольцевом ордере. В качестве награды майнер выбирает между частью маржи (Margin-Split и возвратом LRx пользователю) или просто с сохранением комиссии в LRx.

6. **Верификация и выполнение**: Кольцевой ордер принимается LPSC. Он выполняет несколько проверок данных, предоставленных майнером, и определяет, может ли кольцевой ордер выполниться полностью или частично (в зависимости от курса в ордерах и токенов в кошельках пользователей). Если все проверки пройдены успешно, контракт передает токены пользователям и одновременно платит комиссию майнеру и кошельку. Если баланс пользователя `Y` недостаточен, он будет считаться уменьшенным: уменьшенный ордер будет автоматически увеличиваться до его первоначального размера, если на его адрес будут внесены достаточные средства, это отличается от аннулирования, которое является односторонней операцией, и не может быть отменена.

6 Операционная гибкость

Важно отметить, что открытый стандарт Loopring позволяет участникам иметь широкий выбор способов функционирования. Участники могут свободно внедрять новые бизнес-модели и обеспечивать удобство для пользователей, получая вознаграждения LRx или что-то другое (если они того пожелают). Экосистема является модульной и предназначена для поддержки большого количества различных приложений.

6.1 Список ордеров

Ретрансляторы могут собирать свои списки ордеров любым способом отображения и сопоставления ордеров пользователей. Первая реализация нашего собственного списка ордеров соответствует модели OTC, где лимитные ордера позиционируются только по цене. Другими словами, временные метки ордеров не имеют отношения к списку ордеров. Тем не менее, ретранслятор может свободно создавать свой список ордеров таким образом, чтобы имитировать типичный механизм согласования централизованной биржи, где заказы сортируются по цене, при этом учитывая также временные метки. Если ретранслятор склонен предлагать этот тип списка ордеров, он может владеть/интегрироваться с кошельком, и эти ордера кошелька отправляются исключительно на единственный ретранслятор, который затем сможет сопоставлять ордера в зависимости от времени. Любая такая конфигурация возможна.

В то время, как другие DEX-протоколы порой требуют, чтобы ретрансляторы имели ресурсы - исходные балансы токенов, чтобы разместить ордера на покупку - ретрансляторы Loopring должны найти только подходящие ордера для завершения сделки и могут сделать это без начального баланса токенов.

6.2 Обмен ликвидностью

Ретрансляторы могут свободно выбирать способ обмена ликвидностью (ордерами) друг с другом. Наш блокчейн является лишь одним из решений, и экосистема свободна в выборе взаимодействия. Помимо присоединения

к нашему блокчейну, они могут строить и управлять их собственным, создавая правила/поощрения по своему усмотрению. Ретрансляторы также могут работать в одиночку в виде особой реализации кошелька. Разумеется, есть явные преимущества во взаимодействии с другими ретрансляторами, учитывая сетевой эффект, однако различные бизнес-модели могут иметь своеобразные схемы обмена ликвидностью и разделять комиссии любым способом.

7 Спецификация протокола

7.1 Анатомия ордера

Ордер представляет собой пакет данных, в котором описывается намерение торговли. Ордер Loopring определяется с использованием модели Uni-Directional Order Model или UDOM следующим образом:

```
message Order {
  address protocol;
  address owner;
  address tokenS;
  address tokenB;
  uint256 amountS;
  uint256 amountB;
  unit256 lrcFee
  unit256 validSince; // Секунд с начала эпохи
  unit256 validUntil; // Секунд с начала эпохи
  uint8   marginSplitPercentage;  // [1-100]
  bool  buyNoMoreThanAmountB;
  uint256 walletId;
  // Адрес двойной авторизации
  address authAddr;
  // v, r, s - части подписи
  uint8   v;
  bytes32 r;
  bytes32 s;
  // Секретный ключ двойной авторизации,
  // не используется для вычисления хеша ордера,
  // поэтому он НЕ подписан.
  string  authKey;
  uint256 nonce;
}
```

Чтобы создать ордер, его нужно подписать закрытым ключом пользователя. Переменная `authAddr` используется для подписания кольцевых ордеров, частью которых является этот ордер, что предотвращает действия злоумышленников. Для более подробной информации обратитесь к разделу 9.1. Подпись представлена переменными `v`, `r` и `s` и передается вместе с параметрами ордера по сети. Это гарантирует, что ордер остается неизменным в течение всего его жизненного цикла. Несмотря на то, что ордер никогда не изменяется, протокол все еще может вычислять его текущее состояние на основе его адреса вместе с другими переменными.

UDOM не включает цену (которая должна быть числом с плавающей запятой(float)), но вместо этого использует переменную `rate` или r, которая вычисляется как `amountS`/`amountB`. `rate` не является числом с плавающей запятой, а значением, которое будет сравниваться только с другими целыми числами без знака, чтобы сохранить все промежуточные результаты в виде целых чисел без знака и увеличить точность вычислений.

7.1.1 Процесс покупки

Когда майнер проверяет ордера, возможно, будет исполнена более высокая ставка, что позволит пользователям получить больше `tokenB`, чем `amountB` они указали. Однако, если `buyNoMoreThanAmountB` установлен в `True`, протокол гарантирует, что пользователи получат не более `amountB` из `tokenB`. Таким образом, UDOM параметр `buyNoMoreThantokenB` определяет, когда заказ считается полностью выполненным. `buyNoMoreThantokenB` указывает максимум `amountS` или `amountB`, и разрешает пользователям выражать более грамотные торговые намерения, чем традиционные ордера на покупку/продажу.

Например: `amountS` = 10 и `amountB` = 2, курс $r = 10/2 = 5$. Таким образом, пользователь готов продать 5 `tokenS` за каждый `tokenB`. Майнер проверяет и находит пользователя с курсом 4, позволяя пользователю получить 2.5 `tokenB` вместо 2. Однако, если пользователю требуется только 2 `tokenB` и установлен флаг `buyNoMoreThanAmountB` в `True`, LPSC выполняет транзакцию с курсом 4 и пользователь продает 4 `tokenS` за каждый `tokenB`, сохраняя тем самым 2 `tokenS`. Имейте ввиду, что это не учитывает комиссии за майнинг (см. Раздел 8.1).

Действительно, если мы используем

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

для представления ордера в упрощенной форме, то для пары ETH/USD на традиционной бирже возможны ордера 1-й и 3-й, но не другие два:

1. Продать 10 ETH по цене 300 USD/ETH. Этот ордер может быть выражен как: `Order(10, ETH, 3000, USD, False)`.
2. Продать ETH по цене 300 USD/ETH, чтобы получить 3000 USD. Этот ордер может быть выражен как: `Order(10, ETH, 3000, USD, True)`.
3. Купить 10 ETH по цене 300 USD/ETH, Этот ордер может быть выражен как: `Order(3000, USD, 10, ETH, True)`.
4. Потратить 3000 USD на покупку максимального количества ETH по цене 300 USD/ETH, Этот ордер может быть выражен как: `Order(3000, USD, 10, ETH, False)`.

7.2 Проверка кольца

Смарт контракты Loopring не выполняют расчеты по обменному курсу или сумме, но должны получать и проверять, какие майнеры это сделали. Эти вычисления выполняются майнерами по двум основным причинам: (1) язык программирования смарт контрактов, такой как solidity [19] на Ethereum, не поддерживает вычисления с плавающей запятой, особенно $pow(x, 1/n)$ (вычисление n-го корня из числа с плавающей запятой), и (2) желательно, чтобы вычисление было сделано офчейн, чтобы уменьшить стоимость и облегчить блокчейн.

7.2.1 Проверка подкольца

Этот шаг не позволяет арбитражникам нечестно реализовать всю маржу в кольцевом ордере, внедряя в нее новые ордера. По сути, как только валидный кольцевой ордер находит майнер, может возникнуть соблазн добавить в него другие ордера, чтобы полностью присвоить маржу пользователей (скидки). Как видно из рисунка 3 ниже, тщательно рассчитанные значения $x1$, $y1$, $x2$ и $y2$ сделают произведение всех ордеров равным 1, поэтому скидки не будет.

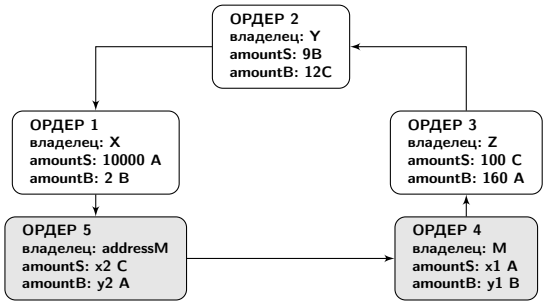

Рис. 3: Кольцевой ордер с подкольцом

Это нулевой риск, добавление нулевой ценности в сеть и считается нечестным поведением со стороны майнера. Чтобы предотвратить это, Loopring требует, чтобы валидный цикл не мог содержать никаких подколец. Чтобы проверить это, LPSC гарантирует, что токен не может быть в позиции покупки или продажи дважды. На приведенной выше диаграмме мы видим, что токен `A` был дважды продан и дважды куплен, такое будет запрещено.

7.2.2 Проверка курса

Расчеты обменного курса в кольцевом ордере производятся майнерами по указанным выше причинам. Именно LPSC должен убедиться, что они верны. Во-первых, он проверяет, что курс покупки, который может выполнить майнер для каждого ордера, равен или меньше первоначального курса покупки, установленного пользователем. Это гарантирует, что пользователь получит обменный курс, который он запросил или даже лучше. Как только обменные курсы подтвердятся, LPSC гарантирует, что каждый ордер в кольцевом ордер имеет одинаковую скидку. Например, если разность курсов равна γ, тогда цена за каждый заказ будет равна:

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

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

следовательно:

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

Если транзакция содержит n ордеров, `скидка` будет:

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

где r^i – курс i-го ордера. Очевидно, что только если разность курсов $\gamma \geq 0$, ордера могут быть выполнены; и фактический обменный курс i-го ордера (O^i) $\hat{r^i} = r^i\cdot(1-\gamma)$, $\hat{r^i} \leq r^i$.

Вспомним наш предыдущий пример, где у Алисы 15 токенов `A`, и она хочет за них 4 токена `B`, у Боба 10 токенов `B`, и он хочет за них 30 токенов `A`. Если токен `A` является эталоном, тогда Алиса покупает токен `B` за $\frac{15}{4} = 3.75$ `A`, а Боб продает токен `B` за $\frac{30}{10} = 3.00$ `A`. Подсчитаем разность курсов: $\frac{150}{120} = 1.25$, таким образом, $\frac{1}{1.25} = 0.8 = (1-\gamma)^2$. Обменный курс, который делает торговлю справедливой для обеих сторон, составляет $\sqrt{0.8}\cdot 3.75 \approx 3.3541$ token `A` на токен `B`.

Боб отдает 4 токена `B` и получает 13.4164 токенов `A`, больше, чем 12, которые он ожидал. Алиса получает 4 токена `B` как и предполагалось, но отдает только 13.4164 токенов `A` взамен, меньше, чем она была готова отдать (15). Обратите внимание: часть этой маржи будет направлена на оплату комиссии, чтобы стимулировать майнеров (и кошельки). (См. Раздел 8.1).

7.2.3 Отслеживание выполнения и отмены

Пользователь может частично или полностью отменить ордер, отправив специальную транзакцию в LPSC, содержащую сведения об ордере и суммах для отмены. LPSC учитывает это, сохраняет суммы для отмены и посылает событие `OrderCancelled` в сеть. LPSC отслеживает выполненные и отмененные суммы, сохраняя их значения, используя хеш ордера в качестве идентификатора. Эти данные являются общедоступными и события `OrderCancelled` / `OrderFilled` посылаются в сеть по мере необходимости. Отслеживание этих значений имеет решающее значение для LPSC во время этапа расчета кольцевого ордера.

LPSC также поддерживает отмену всех ордеров для любой торговой пары с помощью события `OrdersCancelled` и отмена всех ордеров для адреса с помощью события `AllOrdersCancelled`.

7.2.4 Масштабирование ордера

Ордера масштабируются в соответствии с историей выполненных и отмененных сумм и текущего баланса счетов отправителей. Процесс находит ордер с наименьшей суммой, которая должна быть выполнена в соответствии с вышеуказанными характеристиками, и использует ее как эталон для масштабирования всех транзакций в кольцевом ордере.

Поиск ордера с наименьшим значением может помочь определить объем выполнения для каждого ордера. Например, если i-ый ордер является ордером с наименьшим значением, то количество токенов, проданных из каждого ордера $\hat{s}$, и количество токенов, купленных из каждого ордера $\hat{b}$, могут быть рассчитаны как:

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

где $\overline{s}_i$ баланс, который остается после того, как ордера частично выполнены.

Во время реализации мы можем смело предположить, что любой ордер в кольцевом ордере имеет самое наименьшее значение, затем пройти по кольцевому ордеру не более двух раз, чтобы рассчитать объем выполнения каждого ордера.

Пример: если наименьшая сумма, которую нужно выполнить по сравнению с первоначальным ордером, равна 5%, все транзакции в кольцевом ордере уменьшаются до 5%. Как только транзакции будут завершены, ордер, который имеет наименьшее значение, должен быть полностью выполнен.

7.3 Кольцевой ордер

Если кольцевой ордер выполняет все предыдущие проверки, он может быть закрыт, и транзакции могут быть выполнены. Это означает, что все n ордеров из кольцевого ордера связаны, как показано на рисунке 4:

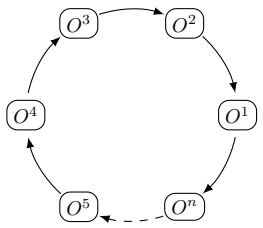

Рис. 4: Кольцевой ордер

Для совершения транзакций LPSC использует смарт контракт `TokenTransferDelegate`. Внедрение такого делегата улучшит протокол, сделав смарт контракт проще, так как все ордера требуют авторизации этого делегата вместо различных версий протокола.

Для каждого ордера в кольцевом ордере, оплата `tokenS` делается в следующем или предыдущем ордере в зависимости от реализации. Затем комиссия майнера оплачивается в зависимости от модели вознаграждения, выбранной майнером. Наконец, как только все транзакции сделаны, событие `RingMined` посылается в сеть.

7.3.1 Посылаемые события

Протокол посылает события, которые позволяют ретрансляторам, обозревателям ордеров и другим участникам получать обновления списка ордеров как можно более эффективно. Посылаемые события:

- **OrderCancelled**: Отмена конкретного ордера.
- **OrdersCancelled**: Отмена всех ордеров торговой пары, связанных с адресом.
- **AllOrdersCancelled**: Отмена всех ордеров всех торговых пар, связанных с адресом.
- **RingMined**: Кольцевой ордер успешно выполнен. Это событие содержит данные, относящиеся к каждой передаче токена внутри кольца.

8 Токен LRx

LRx - это обобщенное обозначение токена. LRC - это токен Loopring на Ethereum, LRQ на Qtum, LRN на NEO и т. д. Другие типы LRx будут введены в будущем, поскольку Loopring будет развернут на других публичных блокчейнах.

8.1 Комиссии

Когда пользователь создает ордер, он указывает количество LRx, которое должно быть выплачено майнеру, выполневшему ордер, в качестве платы, также указывает процент от маржи (`marginSplitPercentage`). Это называется разделение маржи. Решение о том, что из них выбрать (комиссия или маржа), предоставляется майнеру.

Представление разделения маржи:

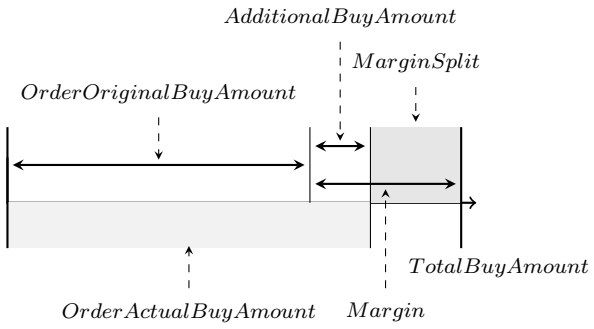

Рис. 5: 60% разделение маржи

Если маржа в кольцевом ордере слишком мала, майнер будет выбирать комиссию в LRx. Если, наоборот, маржа достаточно существенна, и полученное разделение маржи будет стоить гораздо больше, чем плата LRx, майнер будет выбирать часть маржи. Однако существует еще одна оговорка: когда майнер выбирает разделение маржи, он должен заплатить пользователю (создателю ордера) комиссию, которая предназначалась майнеру. Это повышает порог того, где майнер будет выбирать разделение маржи ради двухкратного увеличения комиссии ордера, увеличивая склонность к выбору платы в LRx. Это позволяет майнерам получать постоянный доход на кольцевых ордерах с низкими маржами в противовес получения меньшего дохода от более высокой маржи в кольцевых ордерах. Наша модель вознаграждения основана на ожидании того, что по мере роста и созревания рынка будет появляться меньшее количество ордеров с высокой маржой, что потребует фиксированных сборов LRx в качестве награды. В итоге получим следующий график:

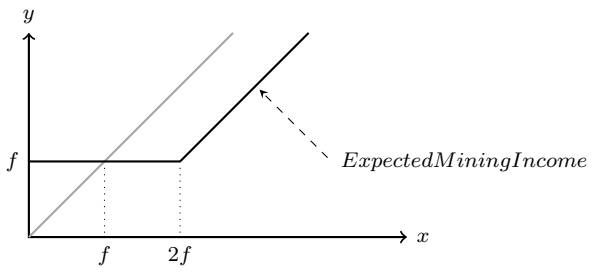

Рис. 6: Модель комиссий в Loopring

где f – комиссия LRx, x – разделение маржи, y – доход от майнинга. $y = max(f, x - f)$ как указано сплошной линией; если комиссия LRx ордера равна 0, равенство примет вид $y = max(0, x - 0)$, что упрощается до $y = x$, как указано серой линией. Последствия:

1. Если разделение маржи равно 0, майнеры выбирают комиссию LRx и все еще стимулируются.

2. Если комиссия LRx равна 0, получаем серую линию и линейный рост доходов.

3. Когда доход от разделение маржи больше, чем удвоенная комиссия LRx, майнеры выбирают разделение маржи и платят LRx пользователю.

Следует отметить, что если комиссия LRx отлична от нуля, независимо от того, какой вариант выбирает майнер, всегда будет передача LRx между майнером и создателем ордера. Либо майнер получает комиссию LRx, либо платит комиссию LRx обратно создателю ордера, чтобы забрать часть маржи. Майнеры будут делиться определенным процентом сборов с кошельками. Когда пользователь отправляет ордер через кошелек и он выполняется, кошелек вознаграждается комиссией или частью маржи. Несмотря на то, что возможны и другие уникальные реализации или бизнес-модели, наша склонность состоит в том, чтобы кошельки получали приблизительно 20% – 25% от заработанных наград. Кошельки представляют собой основную цель для интеграции протокола Loopring, поскольку у них есть пользовательская база, но малый или вообще нет источника дохода.

8.2 Децентрализованное управление

Протокол Loopring является социальным протоколом в том смысле, что он полагается на координацию между участниками для эффективной работы по достижению цели. Это не отличается от крипто протоколов в целом, и действительно, его полезность в значительной степени обусловлена теми же механизмами согласования задач [20], постоянным достижением консенсуса и ограниченной функциональностью. С этой целью токены LRx используются не только для оплаты комиссии, но и для выравнивания финансовых стимулов различных участников сети. Такое согласование необходимо для широкого принятия любого протокола, но особенно остро стоит для биржевых протоколов, учитывая, что успех в основном связан с повышением ликвидности в надежной децентрализованной экосистеме.

Токены LRx будут использоваться для обновления протокола через децентрализованное управление. Смарт-контракт обновления будет регулироваться держателями токенов для обеспечения целостности и безопасности, а также для ослабления рисков частичной ликвидности за счет несовместимости. Учитывая, что смарт контракты не могут быть изменены после их развертывания, существует риск того, что dApps или конечные пользователи будут продолжать взаимодействовать с устаревшими версиями, а не с обновленными контрактами. Возможность обновления имеет решающее значение для успеха протокола, поскольку он должен адаптироваться к требованиям рынка и базовым целям. Децентрализованное управление держателями LRx позволит обновлять смарт-контракты без нарушения работы dApps или конечных пользователей. Сначала это будет осуществляться с помощью простого смарт контракта с мультиподписью с целью продвижения к функционированию на оспове DAO.

9 Мошенничество и защита от атак

9.1 Предотвращение опережающей сделки

В децентрализованных биржах опережающая сделка - это, когда кто-то пытается скопировать торговое решение другого узла и выполнить его до первоначальной транзакции, которая находится в пуле ожидания транзакций (mempool). Это может быть достигнуто путем

указания более высокой комиссии за транзакцию (цена на газ). Основная схема опережающей сделки в Loopring (и любом протоколе для согласования ордеров) - это кража: когда злоумышленник крадет один или несколько ордеров из ожидающей выполнения транзакции; и, в частности, для Loopring: когда злоумышленник крадет весь кольцевой ордер из ожидающей транзакции.

Когда транзакция submitRing не подтверждена и все еще находится в пуле ожидания, любой может легко обнаружить такую транзакцию и заменить `minerAddress` их собственным адресом (`filcherAddress`), тогда он может повторно подписать полезную нагрузку с `filcherAddress`, чтобы заменить подпись кольцевого ордера. Злоумышленник может установить более высокую цену на газ и предложить новую транзакцию в надежде, что майнеры выберут ее в следующий блок вместо первоначальной транзакции submitRing.

Предыдущие решения этой проблемы имели важные недостатки: требовалось больше транзакций и, таким образом, стоило майнерам больше газа; и, по крайней мере, вдвое больше блоков для выполнения кольцевого ордера. Наше новое решение Двойная авторизация (Dual Authoring) [21] включает механизм настройки двух уровней авторизации для ордеров - один для создания и один для майнинга.

Процесс двойной авторизации:

1. Для каждого ордера программное обеспечение кошелька генерирует случайную пару публичный/приватный ключ и помещает ее в JSON сниппет (Альтернативой является использование адреса, полученного из открытого ключа, а не самого открытого ключа для уменьшения размера. Мы используем `authAddr` для представления такого адреса и `authKey` для представления соответствующего приватного ключа `authAddr`).

2. Вычислить хэш ордера со всеми полями, кроме `r`, `v`, `s` и `authKey`), и подписать хэш с помощью приватного ключа `owner` (не `authKey`).

3. Кошелек отправит заказ вместе с `authKey` ретранслятору для майнинга. Майнер проверит, что `authKey` и `authAddr` составляют валидную пару, а подписи ордеров соответствуют `owner` адресам.

4. Когда кольцевой ордер идентифицирован, майнер будет использовать все `authKey` для подписи хеша кольцевого ордера, `minerAddress` и всех параметров для майнинга. Если в кольцевом ордере содержится n ордеров, то будет n подписей n `authKey`. Мы называем эти подписи `authSignature`. Майнер может также подписать хеш кольца вместе со всеми параметрами для майнинга, используя приватный ключ `minerAddress`.

5. Майнер вызывает функцию submitRing со всеми параметрами, а также все дополнительные `authSignature`. Обратите внимание, что ключи `authKey` НЕ являются частью транзакции в блокчейне и, таким образом, остаются неизвестными для всех, кроме майнера.

6. Протокол Loopring проверяет соответствие пары `authSignature` и `authAddr` в каждом ордере и отклоняет кольцевой ордер, если какая-нибудь `authSignature` отсутствует или недействительна.

В результате имеем:

- Подпись ордера (приватным ключом адреса `owner`) гарантирует, что ордер не может быть изменен, в том числе `authAddr`.

- Подпись майнера (с помощью приватного ключа `minerAddress`), если она сделана, гарантирует, что никто другой не сможет добавить в блокчейн этот кольцевой ордер.

- `authSignature` гарантируют, что весь кольцевой ордер не может быть изменен, в том числе `minerAddress`, и никакие ордера не могут быть украдены.

Двойная авторизация предотвращает кражу ордера и кольцевого ордера, все еще гарантируя, что кольцевые ордера могут быть выполнены в одной транзакции. Кроме того, двойная авторизация позволяет ретрансляторам обмениваться ордерами двумя способами: совместимым и несовместимым. По умолчанию Loopring функционирует как OTC-модель и поддерживает только лимитные ордера, что означает, что временные метки заказов игнорируются. Это означает, что опережающая сделка не влияет на фактическую цену этой сделки, но влияет на ее выполнение.

10 Другие атаки

10.1 Атака Сибиллы или DOS

Злоумышленники, действуя сами или маскируясь, могут отправить большое количество небольших ордеров для атаки узлов Loopring. Однако, поскольку мы разрешаем узлам отклонять заказы на основе их собственных критериев, которые они могут скрывать или раскрывать, большинство этих ордеров будут отклонены. Уполномочивая ретрансляторы самостоятельно оценивать ордера, мы не рассматриваем DOS атаку как угрозу.

10.2 Недостаточный баланс

Злоумышленники могут подписывать и распространять ордера, чей адрес на самом деле имеет нулевой баланс. Узлы могут отслеживать и замечать, что фактический баланс некоторых ордеров равен нулю, обновляя статус этих ордеров, а затем отбрасывать их. Узлы должны

тратить время, чтобы обновить статус ордера, поэтому рекомендуется также вести черные списки для минимизации усилий.

11 Выводы

Протокол Loopring представляет собой базовый уровень для децентрализованной биржи. При этом он имеет глубокие последствия в том, как люди обмениваются активами и ценностями. Деньги, как промежуточный товар, облегчают или заменяют бартерный обмен и решают проблему двойного совпадения потребностей [22], в соответствии с которой два участника должны предложить друг другу определенный товар или услугу. Аналогичным образом, протокол Loopring направлен на то, чтобы отказаться от нашего желания для совпадения потребностей в торговых парах, используя кольцевое соответствие для быстрейшего совершения сделки. Это имеет смысл, когда группа людей обменивается токенами, традиционными активами с кем-то другим. Действительно, так же, как децентрализованные криптовалюты создают угрозу национальному контролю над деньгами, комбинаторный протокол, который может удовлетворять любому количеству торговцев (потребителей/производителей), представляет собой теоретическую угрозу для самой концепции денег.

Преимущества протокола включают:

- Офчейн управление ордером и ончейн выполнение означает, что нет уменьшения производительности ради обеспечения безопасности.
- Большая ликвидность благодаря кольцевым ордерам и распределению ордеров.
- Двойная авторизация решает проблему опережающей сделки, с которой сталкиваются все DEX и их пользователи.
- Свободные, публичные смарт контракты позволяют любому dApp взаимодействовать с протоколом.
- Стандартизация между участниками позволяет создавать сетевые эффекты и улучшать работу конечного пользователя.
- Сеть поддерживает различные виды списков ордеров и взаимодействия.
- Снижение барьеров для входа означает снижение затрат на узлы, соединяющие сеть и конечных пользователей.
- Анонимная торговля непосредственно из кошельков пользователей.

12 Благодарности

Мы хотели бы выразить благодарность нашим наставникам, советникам и многим людям в сообществе, которые были настолько приветливы и охотно делились своими знаниями. В частности, мы хотели бы поблагодарить Shuo Bai (из ChinaLedger); профессора Haibin Kan; Alex Cheng, Hongfei Da; Yin Cao; Xiaochuan Wu; Zhen Wang, Wei Yu, Nian Duan, Jun Xiao, Jiang Qian, Jiangxu Xiang, Yipeng Guo, Dahai Li, Kelvin Long, Huaxia Xia, Jun Ma, and Encephalo Path за обзор и предоставление отзывов по этому проекту.

Список литературы

[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] 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.

[22] 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.