УДК 004.75

АСИНХРОННЫЕ ОТКРЫТЫЕ КРИПТОВАЛЮТЫ НА ОСНОВЕ ДОКАЗАТЕЛЬСТВА ДОЛИ ВЛАДЕНИЯ

Пономарев П.Н. Университет ИТМО, г. Санкт-Петербург
Научный руководитель – Кузнецов П.В., PhD, научный сотрудник ФИТиП, Университет ИТМО, г. Санкт-Петербург

В рамках данной работы были изучены существующие подходы в реализации асинхронных криптовалют. Был предложен алгоритм для открытой криптовалюты с использованием механизма доказательства доли владения (proof-of-stake), а также доказана корректность алгоритма.

Введение. Основной задачей криптовалюты является *задача передачи активов* – осуществление перевода средств между участниками распределенной системы. В открытой *(permissionless)* системе данная задача достаточно сложна: стоит выбор между согласованностью и эффективностью решения. В частности, протоколы, применяемые в открытых системах, должны выдерживать атаку Сивиллы [2], при которой противник может создать огромное количество «поддельных» участников в сети.

Предполагая, что сеть синхронна и что противник может обладать только менее чем половиной общей вычислительной мощности, сети Bitcoin и Ethereum гарантируют, что честные участники соглашаются о порядке совершенных транзакций. Для этого данные системы используют консенсус, а также механизм доказательства работы (proof-of-work*)* с целью искусственного замедления участников. Однако такие алгоритмы заведомо медленны и тратят огромное количество энергии.

Существуют и другие протоколы, которые устраняют потребность в огромных энергозатратах, используя механизмы доказательства доли владения (proof-of-stake), доказательства пространства (proof-of-space) или доказательства пространства-времени (proof of space-time). Однако данные алгоритмы по-прежнему предполагают использование синхронных систем, рандомизации и нетривиальной криптографии.

Относительно недавно было показано [3], что для решения задачи криптовалюты, как правило, от пользователей не требуется согласование общего порядка транзакций, в котором они должны обрабатываться. Вместо использования консенсуса, который необходим для реализации полного порядка, можно построить систему передачи активов поверх надежной широковещательной абстракции (reliable broadcast), предполагая, что система статическая. В отличие от консенсуса, reliable broadcast позволяет использовать простые асинхронные решения, обеспечивая эффективное решение задачи передачи активов, которые превосходят аналоги, основанные на консенсусе [1]. Reliable broadcast базируется на использовании системе кворумов. Традиционная система кворумов предполагает, что в системе с количеством участников n, и в которой как максимум f $(f < n/3)$ могут быть нечестными, кворумы состоят из себя множества участников размера $n - f$. В динамической системе, уязвимой для атаки Сивиллы, использовать традиционные системы кворумов не представляется возможным.

Основная часть. Мы предлагаем динамическую систему передачи активов, использующую взвешенные кворумы, что оказывается естественным для систем подразумевающих понятие (ценных) активов. Вместо традиционных кворумов мы используем сертификаты, подписанные участниками, владеющими достаточным количеством активов, так называемой *долей (stake)*. Однако понятие «доля участника» в любой данный момент времени нечетко определено в децентрализованной системе без консенсуса, в которой активы динамически обмениваются, и участники не согласовывают общий порядок обменов. Мы решаем эту проблему, используя понятие *конфигурации*. Конфигурации помогают представить частично упорядоченный набор транзакций, однозначно определяющих распределение доли в системе.

В свою очередь, множество конфигураций можно представить таким образом, что они будут образовывать решетку. Чтобы гарантировать, что все честные участники должным образом согласовывают свои представления о текущей конфигурации, мы реализуем вариацию протокола соглашения в решетке (lattice agreement).
Основываясь на таких абстракциях как reliable broadcast и lattice agreement, мы представляем протокол *Pastro* для решения задачи передачи активов в условии присутствия *динамического противника*, который может выбрать, каких участников системы захватить во время исполнения, учитывая доли, которыми они владеют. В работе предполагается, что участники, не следующие предписанному алгоритму, владеют менее чем одной третью всех средств в *активной* конфигурации. Мы также доказываем, что наш протокол удовлетворяет всем необходимым свойствам криптовалюты при наложенных условиях.

Выводы. Был разработан протокол *Pastro*, решающий задачу передачи активов в открытой распределенной системе с использованием механизма доказательства доли владения, также была доказана его корректность. Мы считаем, что *Pastro* является правильной альтернативой тяжеловесным алгоритмам, основанных на консенсусе. Наше решение использует механизм proof-of-stake вместо proof-of-work, полностью асинхронно, а также не полагается на сложные криптографические примитивы, что делает его эффективным и надежным. Что более важно, в отличие от всех предложенных решений на данный момент, *Pastro* устойчив к динамическому противнику, который может захватывать участников по мере времени в зависимости от исполнения.

Литература.

1. Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Yvonne Anne Pignolet, Dragos-Adrian Seredinschi, Andrei Tonkikh, and Athanasios Xygkis. 2020. Online Payments by Merely Broadcasting Messages. In 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2020, Valencia, Spain, June 29 - July 2, 2020. IEEE, 26–38.
2. John R. Douceur. 2002. The Sybil Attack. In Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers. Springer, Heidelberg, 251–260.
3. Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, and Dragos-Adrian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In PODC. https://arxiv.org/abs/1906.05574.

Пономарев П.Н. (автор) Подпись

Кузнецов П.В. (научный руководитель) Подпись