Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
Факультет информационных технологий и программирования
Кафедра компьютерных технологий

Разработка модели криптовалюты на основе алгоритма консенсуса реализующего метод доказательства доли владения

Агапов Г.Д.
Научный руководитель: Чивилихин Д.С.

Санкт-Петербург
2018

ОГЛАВЛЕНИЕ

Стр.

ВВЕДЕНИЕ

TODO Введение

ГЛАВА 1. **ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ**

В настоящей главе проводится краткий обзор предметной области.

Вводится понятие блокчейна, рассматриваются консенсус-алгоритмы, используемые в блокчейн-системах. Вводится понятие криптовалюты, рассматриваются реализованные системы, реализующие функционал криптовалюты, спецификации к ним.

1.1. Блокчейн

Опр. 1.1. Блокчейн (в переводе с английского ”цепочка блоков”) – структура данных, представляющая собой последовательный непрерывно расширяющийся список записей, связанных между собой по принципу односвязного списка, с использованием криптографически стойкой хэш-функции для установления связей.

Запись в блокчейне вместе с её связью принято называть блоком. В реализациях структуры блокчейн, как правило, каждый связью является ссылка на предыдущий блок, где ссылкой является значение криптографически стойкой хэш-функции, примененной к предыдущему блоку.

$$
\begin{aligned}
&Blockchain_{\langle H,Data\rangle} = \{\ \langle origin, blocks\rangle \mid origin \in Data,\\
&\ blocks \in List_{\langle Data, Value_H\rangle},\\
&\ \langle index, block \equiv \langle data, value_H\rangle\rangle \in blocks\\
&\qquad \Longrightarrow \begin{cases} value_H = H(origin), & \text{if } index = 1\\ value_H = H(blocks[index-1]), & \text{otherwise} \end{cases}\\
&\}
\end{aligned}
\tag{1.1}
$$

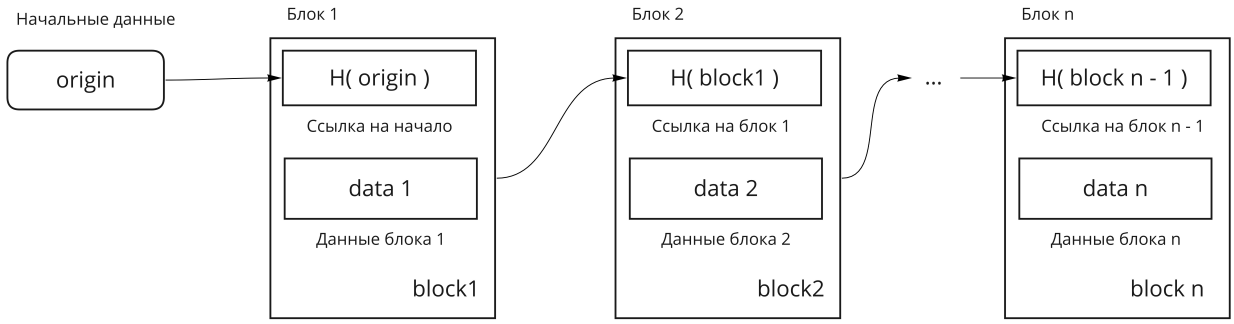

Рис. 1.1 — Диаграма структуры Блокчейн

Построенная таким образом структура данных имеет интересное свойство по сравнению с односвязным списком:

$$
\begin{aligned}
&\forall i, n, x_0, ..., x_n, x'_i \\
&\langle x_0, [\ block_1 \equiv \langle x_1, H(x_0)\rangle, ..., \\
&\qquad block_i \equiv \langle x_i, H(block_{i-1})\rangle, ..., \\
&\qquad block_n \equiv \langle x_n, H(block_{n-1})\rangle\ ]\rangle \in Blockchain_{\langle H, Data\rangle}, \\
&i \neq n, x_i \neq x'_i \implies
\end{aligned}
\tag{1.2}
$$

$$
\begin{aligned}
&\langle x_0, [\ block_1 \equiv \langle x_1, H(x_0)\rangle, ..., \\
&\qquad block'_i \equiv \langle x'_i, H(block_{i-1})\rangle, ..., \\
&\qquad block_{i+1} \equiv \langle x_{i+1}, H(block_i)\rangle, ..., \\
&\qquad block_n \equiv \langle x_n, H(block_{n-1})\rangle\ ]\rangle \notin Blockchain_{\langle H, Data\rangle},
\end{aligned}
$$

Иными словами, невозможно поменять содержание блока, не меняя при этом последующих блоков в структуре. Данное свойство опирается на предположении о стойкости криптографической функции H, в частности: для данного $h \in Value_h$ практически невозможно подобрать x такой что $H(x) = h$.

1.1.1. Применение структуры Блокчейн

Гораздо чаще термин “Блокчейн” применяется не к структуре как к таковой, а к классу систем, использующих её как одну из основных компонент. Большая часть известных систем, использующих эту структуру, представляют из себя распределенные базы данных, как правило специализированные под конкретные области применения. Примеры таких систем:

– Криптовалюты (распределенная база данных, предназначенная для хранения информации о счетах, проведения транзакций над ними).
  – Примеры: Bitcoin [1], NXT [2], Cardano [3].
– Системы для распределенных вычислений с использованием т.н. смарт-контрактов.
  – Как частный случай распределенных вычислений, используются для реализации финансовых контрактов.
  – Примеры: Ethereum [4], NEO [5].
– Распределенные базы данных.
  – Как правило, реализуются для хранения данных, относящихся к конкретной области применения
  – Примеры: Namecoin [6] (альтернатива системе DNS), Disciplina [7] (система для хранения и обмена данных об академической успеваемости)

Структура Блокчейн нашла такое широкое применение в построении распределенных баз данных в первую очередь в следствии свойства 1.2. Если участники сети достигли консенсуса (возможно, в нестрогом смысле) относительно блока b, то они автоматически находятся в солгасии со всеми блоками, предшествующим b в структуре.

1.2. Консенсус-алгоритмы в блокчейн-системах

Большинство алгоритмов консенсуса, разработанных для блокчейн-систем являются алгоритмами для достижения в системе согласованности в конечном счёте (англ. eventual consistency) или эвентуального консенсуса. В отличие от классических консенсус алгоритмов, таких как Paxos [8], Raft [9], от алгоритма консенсуса не требуется достижение полного консенсуса в системе, но полагается достаточным достижение частичного консенсуса, переходящего в полный с вероятностью увеличивающейся со временем с момента достижения согласия о некотором значении большинством узлов сети.

Первопроходцем среди распределенных систем, использующих структуру Блокчейн по праву считается криптовалюта Bitcoin [1]. В статье “Bitcoin: A Peer-to-Peer Electronic Cash System” за авторством Satoshi Nakamoto [10],

описывающей концепцию децентрализованной системы электронных денег, предлагается использование метода доказательства выполнения работы (англ. proof of work) для построения алгоритма эвентуального консенсуса. В оригинальной статье предлагается алгоритм евентуального консенсуса без подробного анализа, в последующих работах других авторов, в частности “The bitcoin backbone protocol: Analysis and applications” [11], доказано что предложенный алгоритм (с небольшими модификациями) является толерантным к атакам, если как минимум 2/3 вычислительной мощности сети находится в управлении честных участников.

Метод доказательства выполнения работы был в дальнейшем применен для построения алгоритмов эвентуального консенсуса для систем Ethereum [4], ZCash [12], IOTA [13], равно как и множества других блокчейн-систем.

Другим популярным методом для построения консенсус-алгоритмов в блокчейн-системах является метод доказательства доли владения (англ. proof of stake), нашедший своё применение в построении алгоритмов эвентуального консенсуса Ouroboros [14], Snow White [15], алгоритмов для систем NXT [2], NEO [5]. Метод может быть также применен в построении алгоритмов полного консенсуса, в частности в алгоритме Algorand [16], также возможность применения метода доказательства доли владения для разработки распределенных систем упомянута авторами алгоритма Honey Badger BFT [17].

1.2.1. Метод доказательства выполнения работы

TODO описания принципа PoW

1.2.2. Метод доказательства доли владения

TODO описания принципа PoS

1.3. Криптовалюты

Опр. 1.2. Криптовалюта – собирательный термин для систем электронных денег, использующих методы криптографии для установления собственности средств при проведении транзакций.

В определении, данном, выше, заложен следующий аспект большинства (если не всех) систем, относимых к криптовалютам: использование асинхронной криптографии. Каждая денежная единица в системе ассоциирована с некоторым адресом `Addr = CreateAddr ( PubKey )`, построенном на основе публичного ключа `PubKey`. Для проведения трансфера средств с одного адреса на другой (транзакции) требуется предоставить подпись информации о транзакции, сделанной секретным ключом `SecretKey`, соответствующим публичному ключу `PubKey`.

1.3.1. Функциональность криптовалюты

Базовой функциональностью криптовалюты, является отправление транзакций между различными участниками сети: участник S имеет возможность послать средства на сумму c участнику T при условии что ему известен адрес участника T и на его адресах содержится средств на сумму, не меньшую c. Однако, уже в первой криптовалюте, нашедшей широкое распространение, Bitcoin [1], создателями было реализовано множество дополнительных функциональностей, в частности:

- Поддержка комиссий за проведение транзакций
- Поддержка скриптовых транзакций
- Поддержка транзакций типа M из N
- Поддержка децентрализованной пириноговой сети

Комиссии за проведения транзакций является важным механизмом для противодействия атакам отказа в доступе, равно как и механизмом поощрения участников, поддерживающих сеть (выпускающих блоки).

Поддержка скриптовых транзакций представляет собой возможность создания адреса, правила валидации права владения которым задаются при помощи предоставляемой пользователем программы (скрипта), запускаемой участниками сети, поддерживающими сеть, при проверки транзакции, использующей средства с данного адреса. Скриптовые транзакции являются очень мощным механизмом, позволяющие реализовать семантику многих составных финансовых операций. Однако, возможности использования скриптовых транзакций для построения финансовых контрактов с помощью скриптового языка в Bitcoin [1] весьма ограничены, т.к. семантика использования скриптовых транзакций не ползволяет описать конечный автомат (только ко-

нечный автомат, выполняющий ровно один переход из начального состояния в конечное). Это ограничение было устранено в системе Ethereum [4].

Поддержка транзакций типа M из N является частным случаем финансового контракта. Задача состоит в предоставлении N участникам сети возможности создания адреса A для списания средств с которого требуется взаимодействие как минимум M участников из N, участвоваших в создании адреса. В простейшем случае, адрес A будет представлять из себя конкатенацию публичных ключей N участников и предоставление подписей транзакции M участниками требуется для валидации транзакции. Именно так транзакции типа M из N реализованы в Bitcoin [1], при использовании скриптового языка. Однако возможны и приницпиально отличные реализации этого типа транзакций, например с использованием пороговых криптосистем [18].

Большинство криптовалют разрабатываются как открытые децентрализованные пиринговые (Peer-to-peer или P2P) сети, т.е. позволяют любому пользователю сети Интернет стать участником сети. Однако это не является необходимым требованием для создания криптовалюты. Существуют проекты криптовалют с закрытой топологией сети (например, проект Hyperledger [19]), равно как и централизованные (RSCoin [20]). Создателями Bitcoin протоколы для поддержки пиринговой сети были реализованы с нуля. Создатели сети Ethereum взяли за основу своей сети протокол Kademlia [21], внеся в него ряд модификаций.

Помимо упомянтых выше функциональностей существуют и другие, поддерживаемые во многих блокчейн-системах:

- Делегация
  - Реализовано во многих криптовалютах, реализующих метод доказательства доли владения, в частности в NEM [22].
- Поддержка обновления протоколов
  - Поддержка “ручного” обновления протоколов (достижения согласия между участниками сети) реализована в большинстве блокчейн-систем посредством, как правило, версионирования форматов блока, протоколов сети и установления процедур коммуникации между командами людей, поддерживающих узлы сети.

    - Поддержка полностью автоматизированных обновлений протокола анонсирована для криптовалюты Tezos [23], не поддерживается подавляющим большинством блокчейн-систем.
- Поддержка обновления программного обеспечения участников сети.
- Расширения понятия блокчейна до понятия ациклического графа блоков
    - Реализовано в криптовалюте IOTA [13].
- Поддержка криптографических протоколов доказательства с нулевым разглашением [24]
    - Реализовано в криптовалюте ZCash [12]

1.3.2. Спецификации существующих систем

Стандартом блокчейн-индустрии является написание технической спецификации, часто форматируемой по типу научной публикации, задача которой состоит в описании основных технических решений системы.

В таблице 1.1 рассмотрены технические спецификации некоторых известных криптовалют с точки зрения детализации, содержания.

Следует заметить что большинство существующих блокчейн-систем не предоставляют должного качества спецификаций, что сужает возможность их анализа с целью рассмотрении их модели. Многие системы являются клонами или несущественными (с точки зрения проблем, рассматриваемых в настоящей работе) модификациями систем, рассмотренных в таблице 1.1. Документы, упомянутые в таблице 1.1 являются одними из лучших, имеющихся в доступе.

Таблица 1.1 — Сравнение документации некоторых криптовалют

Документ	Детализация	Комментарий
Ethereum yellow paper [25]	Высокая	Спецификация консенсус протокола вынесена в отдельную статью. В подробной форме специфицирована логика валидации транзакций, блоков.

Документ	Детализация	Комментарий
Bitcoin developer guide [26]	Средняя	Многократно подчеркнуто, что документация не является спецификацией и для спецификации следует обращаться к реализации клиента `bitcoind`.
EOS.IO Technical White Paper [27]	Низкая	Документ покрывает только основные идеи механизмов, используемые в системе EOS. Для описанных механизмов не даётся подробной спецификации, только высокоуровневый обзор.
Peercoin [28]	Низкая	В документе описывается в неформальной форме консенсус-алгоритм, не приводится никакой математической модели алгоритма, равно как и анализа. В документе не описывается иные компоненты криптовалюты (помимо консенсус-алгоритма).
NEM technical reference [22]	Средняя	Документ является подробной спецификацией технических компонент системы NEM. Спецификация не предлагает модели, описывая компоненты раздельно. Кроме того, логика валидации опускается (т.е. предполагается что её можно извлечь из описаной семантики, что является затруднительным).

Резюме

В данной главе был проведен обзор предметной области блокчейн-систем, криптовалют в частности. Рассмотрены основные подходы к построению консенсус-алгоритмов в них Приведены результаты анализа спецификаций существующих блокчейн-систем, существующих попыток построения модели блокчейн-систем.

ГЛАВА 2. **ПОСТАНОВКА ЗАДАЧИ**

В настоящей главе формулируется задача построения модели криптовалюты на основе консенсус-алгоритма, использующего метод доказательства доли владения.

Формируются критерии оценки решения задачи, рассматриваются предыдущие попытки её решения. Формулируются цели настоящей работы.

2.1. Задача построения модели криптовалюты

2.2. Существующие попытки построения модели криптовалюты

Во всех документах, расмотренных в таблице 1.1 приводится техническое описание (разной степени детализации) системы в целом, но ни в одной из них не была предпринята попытка модульного (поэтапного) построения формальной модели. Приведенные же модели, даже в случае достижения высокой степени детализации, слабо подходят для дальнейшего анализа в силу своей монолитности, большого объёма.

Авторы статьи, предлагающей дизайн криптовалюты Tezos ([23, 2.1 Mathematical representation]) предлагают некоторую математическую нотацию для формирования модульной модели криптовалюты, однако используют её только для описания понятия глобального состояния и блока как изменения этого состояния (самых базовых понятий), в дальнейшем описании дизайна системы нотация не используется. Авторы технической спецификации Ethereum [25] достаточно подробно вводят формулировки состояния, однако все структуры, равно как и логика валидации, описаны как части одной цельной (и довольно громоздкой) модели, без модульной структуры.

В статьях, посвященных описанию и анализу консенсус алгоритмов (не криптовалют целиком), таких как Ouroboros [14], Algorand [16], авторами предлагается только математическая модель консенсус-алгоритма, к остальным компонентам системы предъявляется набор требований (но описание этих компонент выходит за рамки тем данных работ).

2.2.1. Фреймворк Scorex

Авторы фреймворка Scorex [29] поставили своей целью создание модульного фреймворка для прототипирования различных блокчейн-систем. Фреймворк разработан на языке Scala и сопровожден достаточно подробной документацией [30], объясняющей основные концепции, стоящие за фреймворком. Авторы фреймворка отдельно выделяют транзакционный уровень, уровень консенсуса. Это единственная известная автору попытка построения модели криптовалюты в общем смысле.

Как негативный фактор, в документации описываются только некоторые отдельные компоненты модели. Сведение отдельных компонент в единую модель в документации отсутствует. Код фреймворка на Scala, впрочем может рассматриваться как модель криптовалюты (в достаточно общем смысле). Однако, следует заметить, реализация многих компонент Scorex не является абстрактным обобщением конструкций, но является упрощенной реализацией таковых, позволяющей использовать их в прототипировании других компонент.

2.2.2. Модели криптовалют с PoS

Автору неизвестны детальные модели криптовалют, построенные для консенсус-алгоритмов, реализующих метод доказательства доли владения (PoS).

В фреймворке Scorex [29] приведена лишь абстрактная модель, без специализации относительно метода PoS. Кроме того, отсутствие последовательной формулировки модели в документации является минусом (код на Scala часто слишком специализирован, чтобы использовать его для построения абстрактной модели, не следующей определениям аналогичным принятым в коде).

Спецификация Ethereum достаточно детальна, но не предлагает модульной модели и кроме того относится к системе, использующей консенсус-алгоритм, реализующий метод доказательства выполнения работы.

Спецификации систем, реализующих метод доказательства доли владения EOS [27], NEM [22], Peercoin [28] не удовлятворяют требованиям детали-

зации. Спецификация криптовалюты NEM выделяется сравнительно полной детализацией, однако авторами не приводится формальная модель. Кроме того, в последующих главах будет указано на несколько несогласованностей в дизайне этой криптовалюты.

2.3. Цели настоящей работы

Резюме

В данной главе была сформулирована задача построения модели криптовалюты на основе консенсус-алгоритма, использующего метод доказательства доли владения, рассматрены предыдущие попытки её решения. Задача была разбита на состовляющие, были сформулированы критерии для оценки состовляющих. На основе проведенного анализа критериев и составляющих, были сформулированы цели настоящей работы.

ЗАКЛЮЧЕНИЕ

TODO Заключение

СПИСОК ИСТОЧНИКОВ

1. Bitcoin blockchain. [Электронный ресурс]. URL: https://bitcoin.org.
2. NXT blockchain. [Электронный ресурс]. URL: https://nxtplatform.org.
3. Cardano blockchain. [Электронный ресурс]. URL: https://www.cardano.org/en/home.
4. Ethereum blockchain. [Электронный ресурс]. URL: https://ethereum.org.
5. NEO blockchain. [Электронный ресурс]. URL: https://neo.org.
6. Namecoin blockchain. [Электронный ресурс]. URL: https://namecoin.org.
7. Disciplina blockchain. [Электронный ресурс]. URL: https://disciplina.io.
8. Lamport Leslie [и др.]. Paxos made simple // ACM Sigact News. 2001. Т. 32, № 4. С. 18–25.
9. Ongaro Diego, Ousterhout John K. In search of an understandable consensus algorithm. // USENIX Annual Technical Conference. 2014. С. 305–319.
10. Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.
11. Garay Juan, Kiayias Aggelos, Leonardos Nikos. The bitcoin backbone protocol: Analysis and applications // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. 2015. С. 281–310.
12. ZCash blockchain. [Электронный ресурс]. URL: https://z.cash.
13. IOTA blockchain. [Электронный ресурс]. URL: https://iota.org.
14. Ouroboros: A provably secure proof-of-stake blockchain protocol / Aggelos Kiayias, Alexander Russell, Bernardo David [и др.] // Annual International Cryptology Conference / Springer. 2017. С. 357–388.
15. Bentov Iddo, Pass Rafael, Shi Elaine. Snow White: Provably Secure Proofs of Stake. // IACR Cryptology ePrint Archive. 2016. Т. 2016. с. 919.
16. Micali Silvio. Algorand: The efficient and democratic ledger // arXiv preprint arXiv:1607.01341. 2016.

17. Miller Andrew, Xia Yu, Croman Kyle [и др.]. The Honey Badger of BFT Protocols. Cryptology ePrint Archive, Report 2016/199. 2016. https://eprint.iacr.org/2016/199.
18. Pedersen Torben Pryds. A Threshold Cryptosystem without a Trusted Party // Advances in Cryptology — EUROCRYPT '91 / под ред. Donald W. Davies. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991. С. 522–526.
19. Hyperledger: permissioned blockchain framework. [Электронный ресурс]. URL: https://www.hyperledger.org.
20. Danezis George, Meiklejohn Sarah. Centrally Banked Cryptocurrencies // CoRR. 2015. Т. abs/1505.06895. URL: http://arxiv.org/abs/1505.06895.
21. Maymounkov Petar, Mazieres David. Kademlia: A peer-to-peer information system based on the xor metric // International Workshop on Peer-to-Peer Systems / Springer. 2002. С. 53–65.
22. NEM Technical reference. [Электронный ресурс]. URL: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf.
23. Goodman LM. Tezos: A self-amending crypto-ledger position paper. [Электронный ресурс]. 2014. URL: https://www.tezos.com/static/papers/white_paper.pdf.
24. Goldwasser Shafi, Micali Silvio, Rackoff Charles. The knowledge complexity of interactive proof systems // SIAM Journal on computing. 1989. Т. 18, № 1. С. 186–208.
25. Wood Gavin. Ethereum: A secure decentralised generalised transaction ledger. 2014. URL: https://ethereum.github.io/yellowpaper/paper.pdf.
26. Bitcoin developer documentation. [Электронный ресурс]. URL: https://bitcoin.org/en/developer-documentation.
27. EOS Technical whitepaper. [Электронный ресурс]. URL: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.
28. Peercoin whitepaper. [Электронный ресурс]. URL: https://peercoin.net/assets/paper/peercoin-paper.pdf.
29. Chepurnoy Alex. Scorex 2.0 framework. [Электронный ресурс]. 2016. URL: https://github.com/ScorexFoundation/Scorex.

30. Chepurnoy Alex. Scorex 2.0 framework tutorial. [Электронный ресурс]. 2016. URL: https://github.com/ScorexFoundation/ScorexTutorial/blob/master/scorex.pdf.