

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, существующие наработки по их моделированию.

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.

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

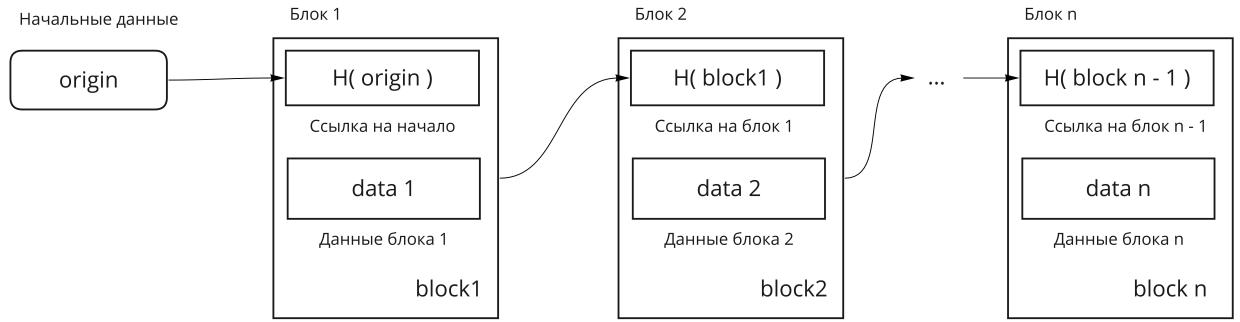


Рис. 1.1 — Диаграмма структуры Блокчейн

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

$$\begin{aligned}
 & \forall i, n, x_0, \dots, x_n, x'_i \\
 & \langle x_0, [\text{block}_1 \equiv \langle x_1, H(x_0) \rangle, \dots, \\
 & \quad \text{block}_i \equiv \langle x_i, H(\text{block}_{i-1}) \rangle, \dots, \\
 & \quad \text{block}_n \equiv \langle x_n, H(\text{block}_{n-1}) \rangle] \rangle \in \text{Blockchain}_{\langle H, \text{Data} \rangle}, \\
 & i \neq n, x_i \neq x'_i \implies
 \end{aligned} \tag{1.2}$$

$$\begin{aligned}
 & \langle x_0, [\text{block}_1 \equiv \langle x_1, H(x_0) \rangle, \dots, \\
 & \quad \text{block}'_i \equiv \langle x'_i, H(\text{block}_{i-1}) \rangle, \dots, \\
 & \quad \text{block}_{i+1} \equiv \langle x_{i+1}, H(\text{block}_i) \rangle, \dots, \\
 & \quad \text{block}_n \equiv \langle x_n, H(\text{block}_{n-1}) \rangle] \rangle \notin \text{Blockchain}_{\langle H, \text{Data} \rangle},
 \end{aligned}$$

Другими словами, невозможно поменять содержание блока, не меняя при этом последующих блоков в структуре. Заметим, что данное свойство опирается на предположении о стойкости криптографической функции H , в частности: для данного $h \in \text{Value}_h$ 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, представля-

ют 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 [?], NXT [?], Cardano [?].
- Системы для распределенных вычислений с использованием т.н. смарт-контрактов.
 - Как частный случай распределенных вычислений, используются для реализации финансовых контрактов.
 - Примеры: Ethereum [?], NEO [?].
- Распределенные базы данных.
 - Как правило, реализуются для хранения данных, относящихся к конкретной области применения
 - Примеры: Namecoin [?] (альтернатива системе DNS), Disciplina [?] (система для хранения и обмена данными об академической успеваемости)

Структура Блокчейн нашла такое широкое применение в построении распределенных баз данных в первую очередь в следствии свойства ??. Если участники сети достигли консенсуса (возможно, в нестрогом смысле) относительно блока b , то они автоматически находятся в согласии 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 [?], Raft [?], 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 [?]. В статье “Bitcoin: A Peer-to-Peer Electronic Cash System” за авторством Satoshi Nakamoto [?], 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 эвентуального консенсуса без подробного анализа, в последующих работах других авторов, в частности “The bitcoin backbone protocol: Analysis and applications” [?], 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 [?], ZCash [?], IOTA [?], 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 [?], Snow White [?], алгоритмов для систем NXT [?], NEO [?]. Метод может быть также применен в построении алгоритмов полного консенсуса, в частности в алгоритме Algorand [?], также возможность применения метода доказательства доли владения для разработки распределенных систем упомянута авторами алгоритма Honey Badger BFT [?].

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. Спецификации криптовалют

Стандартом блокчейн-индустрии является написание технической спецификации, часто форматируемой по типу научной публикации, задача которой состоит в описании основных технических решений системы. В таблице ?? рассмотрены технические спецификации некоторых известных криптовалют. Во всех из них 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 (как в случае с спецификацией системы Ethereum [?]), слабо подходят для дальнейшего анализа в силу своей монолитности, большого объёма.

Авторы статьи, предлагающей дизайн криптовалюты Tezos ([? , 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 [?] 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.

Таблица 1.1 — Сравнение документации некоторых криптовалют

Документ	Детализация	Комментарий
Ethereum yellow paper [?]	Высокая	Спецификация консенсус протокола вынесена в отдельную статью. В подробной форме специфицирована логика валидации транзакций, блоков.
Bitcoin developer guide [?]	Средняя	Многokrатно подчеркнuto, что документация не является спецификацией и для спецификации следует обращаться к реализации клиента bitcoind.
EOS.IO Technical White Paper [?]	Низкая	Документ покрывает только основные идеи механизмов, используемые в системе EOS. Для описанных механизмов не даётся подробной спецификации, только высокоуровневый обзор.
Peercoin [?]	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).

Документ	Детализация	Комментарий
NEM technical reference [?]	Средняя	Документ является подробной спецификацией технических компонент системы NEM. Спецификация не предлагает модели, описывая компоненты отдельно. Кроме того, логика валидации опускается (т.е. предполагается что её можно извлечь из описаной семантики, что является затруднительным).

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

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

1.3.2. Фреймворк Scorex

Авторы фреймворка Scorex [?] поставили своей целью создание модульного фреймворка для прототипирования различных систем. Фреймворк разработан на языке Scala и сопровождается достаточно подробной документацией [?], 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.

1.3.3. Модели криптовалют с PoS

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

В фреймворке Scorex [?] приведена лишь абстрактная модель, без специализации относительно метода PoS. Кроме того, отсутствие явной 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 [?], NEM [?], Peercoin [?] не удовлетворяют требованиям детализации. Спецификация криптовалюты NEM выделяется среди остальных сравнительно полной детализацией, но авторами не приводится формальная модель. Кроме того, в последующих главах будет указано на несколько несогласованностей в дизайне этой криптовалюты.

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.

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. Wood Gavin. Ethereum: A secure decentralised generalised transaction ledger. 2014. URL: <https://ethereum.github.io/yellowpaper/paper.pdf>.
19. Goodman LM. Tezos: A self-amending crypto-ledger position paper. [Электронный ресурс]. 2014. URL: https://www.tezos.com/static/papers/white_paper.pdf.
20. Bitcoin developer documentation. [Электронный ресурс]. URL: <https://bitcoin.org/en/developer-documentation>.
21. EOS Technical whitepaper. [Электронный ресурс]. URL: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>.
22. Peercoin whitepaper. [Электронный ресурс]. URL: <https://peercoin.net/assets/paper/peercoin-paper.pdf>.
23. NEM Technical reference. [Электронный ресурс]. URL: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf.
24. Chepurnoy Alex. Scorex 2.0 framework. [Электронный ресурс]. 2016. URL: <https://github.com/ScorexFoundation/Scorex>.
25. Chepurnoy Alex. Scorex 2.0 framework tutorial. [Электронный ресурс]. 2016. URL: <https://github.com/ScorexFoundation/ScorexTutorial/blob/master/scorex.pdf>.