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

В последние годы такая область знаний, как обработка естественного языка (Natural Language Processing или NLP) находит все больше и больше применений в различных сферах человеческой деятельности. К этой области в частности относятся задачи информационного поиска, извлечения информации, распознавания и синтеза речи, построения систем машинного перевода, вопросно-ответных систем, а также множество других задач, приложений.

ГЛАВА 1. **ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ**

В настоящей главе проводится краткий обзор предметной области. Вводится понятие блокчейна, рассматриваются основные достижения области: консенсус-алгоритмы, разработанные системы, вариативность функционала блокчейн-систем.

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.

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

TODO new diagram

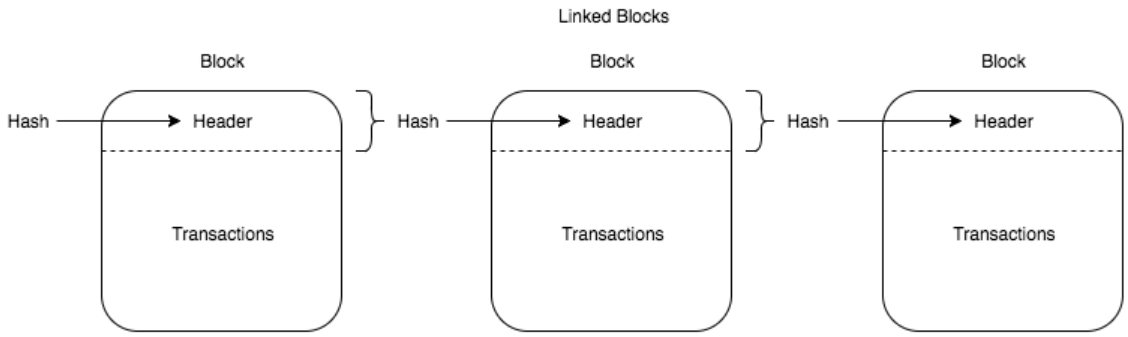

Рис. 1.1 — Диаграма структуры Блокчейн

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

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

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

Другими словами, невозможно поменять содержание блока, не меняя при этом последующих блоков в структуре.

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 авторы 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

Резюме

To be done.

ЗАКЛЮЧЕНИЕ

В настоящей работе была рассмотрена задача выравнивания синсетов тезаурусов Princeton WordNet и YARN. Был предложен метод для решения этой задачи, состоящий из двух этапов: автоматический предпроцессинг и выравнивание с применением техник краудсорсинга. Каждый из этапов был подробно рассмотрен в главах 1

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.