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.

TODO remove [1]

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

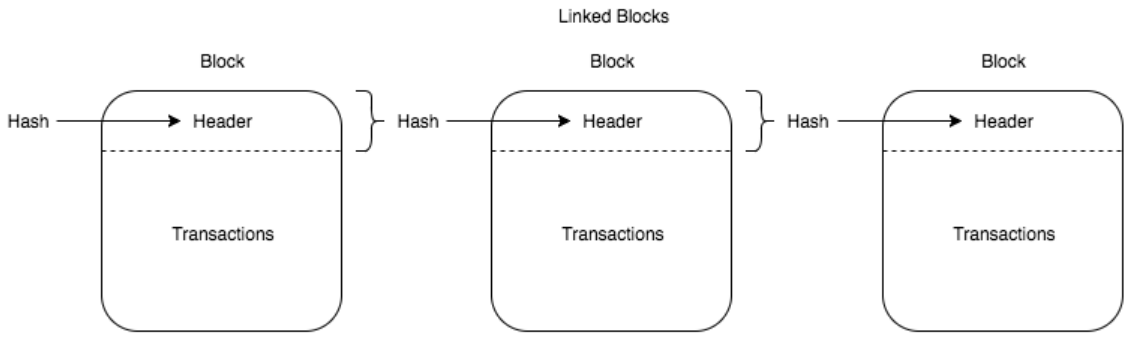

Рис. 1.1 — Диаграма структуры Блокчейн

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, 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 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.

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. Word2Vec. [Электронный ресурс]. URL: https://code.google.com/archive/p/word2vec/.