УДК 004.75

ПРИМЕНЕНИЕ ДРЕВОВИДНЫХ СТРУКТУР ДЛЯ РАСПРЕДЕЛЕННОГО ХРАНЕНИЯ ДАННЫХ

Кича И. (Университет ИТМО), **Тимкин А.К.** (Университет ИТМО)
Научный руководитель – доцент ФБИТ, кандидат технических наук, Таранов С.В.
(Университет ИТМО)

Введение. По данным различных исследования последнее десятилетие возрастает количество исследований в области систем распределенных реестров. Таким образом число разработок увеличивается и их область применения расширяется. Одним из таких направлений является возможность хранения данных. Сами системы, основанные на технологии блокчейн, в свою очередь обеспечивают конфиденциальность информации и ее целостность, что является их важным преимуществом перед традиционными подходами.

Основная часть. В результате рассмотрения возможности применения двоичных деревьев для хранения информации в блокчейне было установлено, что данная структура данных позволяет ускорить процесс проверки валидности блоков по сравнению с хеш-цепочками.
Применение деревьев Меркла позволяет получить прирост производительности системы за счет уменьшения числа необходимых действий для доказательства существования блока в структуре. Данная возможность породила появление упрощенной проверки оплаты (SPV) [1,2].
При рассмотрении модификаций дерева Меркла было обращено отдельное внимание дереву Меркла-Патриция и дереву Веркла, которые позволяют стабилизировать и оптимизировать системы хранения данных на базе распределенных реестров.
Другой более эффективной модификацией является дерево Веркла. Прежде всего данная структура позволяет быстрее доказывать принадлежность данных дереву, что является важным фактором при обеспечении целостности информации [3].

Выводы. Было установлено, что древовидные структуры являются наиболее эффективными среди рассмотренных для хранения данных. Были изучены достоинства и недостатки каждого решения, что позволило определить, какие из них оправданы для применения в области хранения данных. Таким образом, среди рассмотренных решений наиболее быстрым и удобным оказалось дерево Веркла.

Список использованных источников:

1. Antonopoulos A. M. Mastering Bitcoin: unlocking digital cryptocurrencies. 2014 //isbn: 9781449374044. – С. 272.
2. Wood G. et al. Ethereum: A secure decentralised generalised transaction ledger //Ethereum project yellow paper. – 2014. – Т. 151. – №. 2014. – С. 1-32.
3. Kate A., Zaverucha G. M., Goldberg I. Constant-size commitments to polynomials and their applications //International conference on the theory and application of cryptology and information security. – Springer, Berlin, Heidelberg, 2010. – С. 177-194.

Кича И. (автор) Подпись

Тимкин А.К. (автор) Подпись

Таранов С.В. (научный руководитель) Подпись