УДК 004.75

АНАЛИЗ АЛГОРИТМОВ ДОКАЗАТЕЛЬСТВА ПРИНАДЛЕЖНОСТИ УЗЛА ДЛЯ ДЕРЕВЬЕВ ВЕРКЛА В БЛОКЧЕЙНЕ

Тошматов Х.Х. (ИТМО), **Кича И.В.** (ИТМО)
Научный руководитель – кандидат технических наук, доцент Таранов С.В.
(ИТМО)

Введение. Использование деревьев Веркла дает возможность значительно ускорить процесс доказательства принадлежности узла за счет иной структуры данных в блоке. Если ранее в деревья Меркла-Патриция была необходимость в том, чтобы предоставлять сестринские узлы, то в рассматриваемой структуре вместо этого нужно просто указать путь с небольшим дополнительным доказательством. Именно поэтому необходимо подробно рассмотреть, каким может быть это доказательство [1].

Основная часть. В самом просто виде речь идет о векторных обязательствах, которые на самом деле представляют собой разновидность хэш-функции, которой на вход подается список. Но векторные обязательства обладают особым свойством: для обязательства и значения можно сделать короткое доказательство, которое представляет собой обязательство для некоторого списка, где значение находится на i-й позиции.

На практике же применяет полиномиальное доказательство, которое хэширует уже не список, а полином, что в перспективе дает больше возможностей. Две схемы полиномиальных обязательств, которые будут рассмотрены, это обязательства KZG и bulletproof.

Предполагается взять ширину дерева 256 и 48-байтовые обязательства для алгоритма KZG. Использование алгоритма позволило уменьшить размер доказательства примерно в 6–8 раз по сравнению с идеальными деревьями Меркла и более чем в 20–30 раз по сравнению с деревьями Патриции [2]. Если вместо KZG используются обязательства bulletproof, можно безопасно уменьшить размер обязательства до 32 байт, что позволяет уменьшить общий размер доказательства еще на 1/3.

Выводы. Был проведен анализ алгоритмов принадлежности узла деревьям Веркла, в результате чего было обнаружено, что использование полиномиального обязательства KZG позволяет уменьшить размер доказательства в 6-8 раз, а использование bulletproof еще на 1/3.

Список использованных источников:

1. Vitalik Buterin's blog: Verkle trees [Электронный ресурс]. Режим доступа: https://vitalik.eth.limo/general/2021/06/18/verkle.html (дата обращения: 31.01.2024).
2. 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.

Автор _____ Тошматов Х.Х.

Научный руководитель _____ Таранов С.В.