УДК 004.056.5

АНАЛИЗ ПРОТОКОЛОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, ПРИМЕНЯЕМЫХ В БЛОКЧЕЙН-СИСТЕМАХ

Еритенко Н.А. (Университет ИТМО), **Беляев В.В.** (Университет ИТМО)
Научный руководитель – Давыдов В.В. (Университет ИТМО)

Аннотация. В данной работе представлен анализ современных протоколов с нулевым разглашением, применяемых в различных блокчейн-системах, и их сравнительная характеристика.

Введение. Доказательство с нулевым разглашением – криптографический протокол, позволяющий проверяющей стороне установить факт достоверности некоторого утверждения без раскрытия дополнительной информации со стороны доказывающего. Одной из областей применения подобных протоколов являются блокчейн-системы: например, в криптовалютах они используются для сокрытия информации о транзакции, например, о ее размере. В настоящее время блокчейн-системы активно внедряются в различные бизнес-процессы. При этом необходимо учитывать ресурсоемкость и производительность как блокчейн-системы в целом, так и ее составных частей, в частности, протоколов с нулевым разглашением. Для этого будет проведен анализ протоколов с нулевым разглашением, применяемых в современных блокчейн-системах.

Основная часть. В ходе работы проведен анализ протоколов с нулевым разглашением, применяемых в современных блокчейн-системах, в частности, в различных криптовалютах. Проведено моделирование данных протоколов, по результатам которого произведено сравнение данных протоколов по следующим параметрам: объем памяти, необходимой для работы протокола, и время, затрачиваемое на работу протокола.

Выводы. Результаты проведенного анализа протоколов с нулевым разглашением в рамках систем с распределенным реестром могут быть использованы как для определения дальнейшего вектора направления работ по оптимизации существующих протоколов, так и при разработке собственного протокола. Кроме того, представленные результаты анализа возможно использовать для выбора протокола с нулевым разглашением при проектировании блокчейн-системы.

Беляев В.В. (автор) Подпись

Давыдов В.В. (научный руководитель) Подпись