Оценка предельной скорости распространения блоков в Blockchain

Литвинцева Дарья Сергеевна

Студентка

ФИВТ МФТИ, Москва, Россия

E-mail: litv.daria@gmail.com

Научный руководитель *— Драль Алексей Александрович*

На данный момент существуют сотни различных протоколов Blockchain. Несмотря на то, что в 2018 году вышло более 400 статей, посвященных исследованию этой технологии, в сообществе до сих пор не выработан единый язык, и каждый автор использует собственную терминологию. Это приводит к тому, что под одним и тем же термином подразумеваются разные понятия, что затрудняет исследование проблемы. В 2017 году была опубликована статья «Ouroboros: A provably secure proof–of–stake Blockchain protocol» [1], авторы которой одними из первых стали рассматривать проблему формализации протоколов Blockchain. В настоящей работе мы используем предложенную терминологию и, развивая идею, предлагаем фреймворк для сравнения различных Blockchain–протоколов.

В связи с наличием разных протоколов, возникает необходимость в их сравнении по определенным метрикам (например, скорости распространения блока по сети; времени, которое требуется для того, чтобы транзакция почти наверное сохранилась в истории и др). Эти метрики можно посчитать эмпирически, но также хотелось бы иметь и теоретические оценки пределов этих метрик, в зависимости от конфигурации сети (число узлов, скорость соединения, топология) для разных реализаций Blockchain-протоколов. С помощью модели random rumour spreading [2], в представленной работе выводится оценка скорости распространения блока в сети в зависимости от ее параметров.

Литература

1. A. Kiayias, A. Russell, B. David, R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference, Springer, pp. 357–388, 2017.
2. A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry. Epidemic Algorithms for Replicated Database Maintenance. In Proceedings of the 6th ACM Symposium on Principles of Distributed Computing, pp. 1–12, 1987.