УДК 004.056

РАЗРАБОТКА БЕЗОПАСНОГО ПРОТОКОЛА ОБРАБОТКИ МЕЖДУ-ШАРДОВЫХ ТРАНЗАКЦИЙ В БЛОКЧЕЙНЕ

Лэ Ван Хиеу (ИТМО)
Научный руководитель – кандидат физико – математических наук, доцент Комаров И.И. (ИТМО)

Введение. Шардинг — это техника, которая позволяет разделить данные на несколько логических частей, называемых шардами. Это может быть полезно для повышения производительности и масштабируемости системы. Шардинговые блокчейны сочетают в себе технологию шардинга в области баз данных и блокчейн для реализации связи, вычислений и хранения данных [1]. Таким образом, шардинговые блокчейны могут обеспечить масштабируемость возможностей обработки транзакций. Когда количество узлов в сети увеличивается, возможности обработки транзакций можно улучшить за счет увеличения количества шардов [2].

Основная часть. Полный шардинговый блокчейн состоит из нескольких компонентов, таких как выбор участников шарда, генерация случайности, алгоритм консенсуса внутри шарда, межшардовая коммуникация, реконфигурация шарда и т. д [2]. Среди них алгоритм внутришардового консенсуса и межшардовая коммуникация являются двумя наиболее важными компонентами [3]. В этой работе предлагается безопасный протокол обработки между-шардовых транзакций для защиты от злонамеренного лидера, запускающего атаку цензуры между шардами транзакций. Протокол включает в себя несколько ключевых этапов и, как доказано, удовлетворяет свойствам стойкости и живучести. Автор сначала представляет общую схему коммуникации в шардинг-блокчейн системе. Затем описывает алгоритмы внутришардового консенсуса, на этом основе построит безопасный протокол обработки между-шардовых транзакций. В конце работы доказывает безопасности разработанного протокола.

Выводы. Предложенный безопасный протокол обработки транзакций между шардами может быть применен к большинству шардинговых блокчейнов, которые используют алгоритм в стиле BFT (Byzantine Fault Tolerance) в качестве консенсуса внутри шарда.

Список используемых источников

1. Zamani, M., Movahedi, M., Raykova, M. Rapid chain: scaling blockchain via full sharding // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018. – pp. 931–948.

2. Liu Y., Liu J., Zhang Z., Li T., et al. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems // Computer Science Review. – Vol 46. – 2022. https://doi.org/10.1016/j.cosrev.2022.100513.

3. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P. A secure sharding protocol for open blockchains // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria. – 2016. – pp. 17–30.

Автор: Лэ В.Х. _____

Научный руководитель: Комаров И.И. _____