УДК 004.75

АНАЛИЗ ВОЗМОЖНЫХ МОДИФИКАЦИЙ АЛГОРИТМА КОНСЕНСУСА PROOF-OF-HISTORY ДЛЯ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ БЛОКЧЕЙН-СЕТЕЙ

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

Введение. Существующие решения в сфере блокчейна в основном используют механизмы консенсуса, которые предполагают либо наличие вычислительных мощностей, либо долю владения определенным активом. В сетях с распределенными реестрами, ориентированными не на криптовалютные решения, возникает необходимость меньших ресурсных затрат и при этом не предполагается владение самой валютой, что приводит к необходимости разработки новых подходов к нахождению консенсуса. Алгоритм Proof-of-History является оптимальным с точки зрения быстродействия и обеспечения целостности данных, однако есть необходимость его доработки с целью как еще большей производительности, так и с целью минимизации риска реализации уязвимостей [1].

Основная часть. Алгоритм консенсуса Proof-of-History (PoH) имеет ряд преимуществ, основным из которых является скорость проведения транзакций, однако в криптовалютном проекте Solana, где он был представлен, также внедрен механизм Proof-of-Stake (PoS) для подтверждения последовательностей, сгенерированных основным алгоритмом, а точнее для голосования и выбора следующего генератора последовательностей [2].

В некриптовалютных сетях использование данной комбинации может быть неоправданно, в связи с чем предлагается рассмотреть возможность замены алгоритма PoS на Practical Byzantine Vault-Tolerance (PBFT), что позволит оптимизировать работу сети, например для смарт-контрактов, и исключить возможность реализации стейк-атак. Однако данное решение может увеличить вычислительные нагрузки и тем самым снизить скорость обработки транзакций.

Если использовать опыт реализации механизма Proof-of-Previous-Transactions (PoPT), который также включает в себя реализацию PBFT, то при модификации архитектуры построения цепочек можно добиться вычислений несколько потоков, что нивелирует затраты ресурсов и повысит количество единовременно обрабатываемых транзакций [3].

Выводы. Был проведен анализ алгоритма консенсуса PoH, в результате которого было выявлено, что существует возможность повышения его отказоустойчивости и быстродействия за счет внедрения PBFT и модернизации системы, используя подходы из механизма PoPT.

Список использованных источников:

1. Lashkari B., Musilek P. A comprehensive review of blockchain consensus mechanisms //IEEE Access. – 2021. – Т. 9. – С. 43620-43652.
2. Yakovenko A. Solana: A new architecture for a high performance blockchain v0. 8.13 //Whitepaper. – 2018.
3. Xiang F., Huaimin W., Peichang S. Proof of previous transactions (PoPT): An efficient approach to consensus for JCLedger //IEEE Transactions on Systems, Man, and Cybernetics: Systems. – 2019. – Т. 51. – №. 4. – С. 2415-2424.

Автор _____ Кича И.В.

Научный руководитель _____ Таранов С.В.