УДК 004.75

ГИБРИДНЫЙ АЛГОРИТМ КОНСЕНСУСА DAG–PoS–BFT ДЛЯ МАСШТАБИРУЕМЫХ БЛОКЧЕЙН-СИСТЕМ

Красников Б.Ю., Платонов А.В.
Научный руководитель – доцент Платонов А.В.
Университет ИТМО
Baga13511@yandex.ru

Работа выполнена в рамках темы НИР №3 «Анализ подтверждающих вставку алгоритмов в BlockChain».

Введение

Современные распределённые реестры сталкиваются с противоречием между пропускной способностью, безопасностью и децентрализацией, которое в научной литературе описывается как «трилемма блокчейна» [1]. Рост числа пользователей и транзакций требует масштабируемых решений, при этом система должна сохранять устойчивость к византийским сбоям и экономическим атакам. Классические алгоритмы консенсуса решают данную задачу различными способами. Proof-of-Work обеспечивает устойчивость за счёт стоимости вычислительной атаки, однако характеризуется значительным энергопотреблением и высокой задержкой подтверждения транзакций [2]. Proof-of-Stake снижает энергетические издержки и повышает скорость обработки операций, но переносит угрозы в экономическую плоскость и требует механизмов слешинга и финальности [3]. Алгоритмы класса Byzantine Fault Tolerance гарантируют детерминированную финальность и устойчивость к ограниченному числу злонамеренных узлов, однако их масштабируемость ограничена ростом коммуникационной сложности [4]. Подходы на основе Directed Acyclic Graph обеспечивают параллельную обработку транзакций и потенциально более высокую пропускную способность по сравнению с линейной цепочкой блоков, однако свойства безопасности зависят от конкретной реализации протокола [5]. Таким образом, актуальной научной задачей является разработка архитектуры консенсуса, способной объединить масштабируемость DAG-подходов, экономическую устойчивость PoS и строгую финальность BFT-механизмов без существенного увеличения энергозатрат и сетевых накладных расходов.

Основная часть

В работе предлагается гибридный алгоритм консенсуса DAG–PoS–BFT, основанный на многоуровневом разделении функций между структурным, экономическим и финализационным уровнями. На первом уровне используется DAG-архитектура для приёма и распространения транзакций. Параллельное добавление вершин графа позволяет устранить узкое место линейной цепочки блоков и повысить пропускную способность сети. Подобный подход рассматривается как перспективный в современных исследованиях масштабируемых реестров [5]. Транзакции проходят базовую криптографическую валидацию и включаются в вершины, которые подтверждают несколько предыдущих событий, формируя ациклический граф. Поскольку DAG задаёт частичный порядок событий, вводится механизм детерминированного формирования состояния. Формируется согласованный срез графа (snapshot), на основе которого вычисляется корень состояния. Единые правила упорядочивания транзакций обеспечивают одинаковый результат вычислений на всех корректных узлах. Второй уровень реализует механизм Proof-of-Stake для экономического отбора валидаторов. Участие в процедуре финализации определяется

величиной залога, что ограничивает возможность Sybil-атак и создаёт экономическую ответственность участников [3]. Ротация состава валидаторского комитета по эпохам снижает риск концентрации влияния и долгосрочных атак. На третьем уровне применяется BFT-механизм для достижения детерминированной финальности. Валидаторский комитет согласовывает корень состояния снапшота и формирует финализационный сертификат при достижении кворума подписей. Современные исследования BFT-протоколов демонстрируют возможность повышения их эффективности при ограниченном составе комитета [4]. После публикации сертификата состояние считается окончательно подтверждённым и необратимым в рамках принятой модели угроз. Предложенная архитектура позволяет разделить функции масштабирования, экономической защиты и финализации, минимизируя дублирование вычислений. Такой модульный подход рассматривается как перспективное направление развития гибридных протоколов консенсуса [1].

Выводы

Разработанный гибридный алгоритм консенсуса обеспечивает сбалансированный компромисс между пропускной способностью, задержкой подтверждения, энергоэффективностью и безопасностью. Отказ от конкурентных вычислений существенно снижает энергопотребление по сравнению с Proof-of-Work [2]. Использование BFT-финализации устраняет вероятностный характер подтверждений, характерный для ряда DAG-реализаций [5]. Экономический отбор валидаторов повышает устойчивость к Sybil-атакам и усиливает дисциплину участников [3]. Практическое применение алгоритма возможно в высоконагруженных распределённых системах, требующих строгой финальности операций: цифровые активы, корпоративные реестры, логистические платформы и финансовые сервисы. Перспективными направлениями дальнейших исследований являются формальная верификация свойств безопасности и живости протокола, а также экспериментальная оценка масштабируемости при увеличении числа валидаторов.

Литература

1. Zhang N., Lou W., Hou Y. T. A Survey of Blockchain Consensus Mechanisms: State of the Art and Future Directions // IEEE Communications Surveys & Tutorials. 2023. Vol. 25, No. 4. P. 2458–2492.
2. Stoll C., Klaaßen L., Gallersdörfer U. The Carbon Footprint of Bitcoin // Joule. 2019. Vol. 3, No. 7. P. 1647–1661. https://doi.org/10.1016/j.joule.2019.05.012
3. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Vol. 34, No. 3. P. 1156–1190. https://doi.org/10.1093/rfs/hhaa075
4. Yin M., Malkhi D., Reiter M., Gueta G., Abraham I. HotStuff: BFT Consensus with Linearity and Responsiveness // IEEE Transactions on Dependable and Secure Computing. 2023.
5. Lu X. A Survey on Consensus Algorithms of Blockchain Based on DAG // Proceedings of the 6th Blockchain and Internet of Things Conference (BIOTC 2024). 2024. DOI: 10.1145/3688225.3688232