DOI 10.37539/2949-1991.2025.31.8.013
УДК 338.2

Смирнов Сергей Андреевич,
Владимирский государственный университет имени
Александра Григорьевича и Николая Григорьевича Столетовых

АЛГОРИТМЫ КОНСЕНСУСА КРИПТОВАЛЮТ: СУЩНОСТЬ, РАЗНОВИДНОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. В статье рассматриваются алгоритмы консенсуса как основа функционирования криптовалютных и блокчейн-систем. Раскрывается их экономическая и технологическая сущность, проводится сравнительный анализ основных моделей – Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) и гибридных решений. Выделяются их преимущества и недостатки, определяется область применения и перспективы развития в условиях необходимости повышения масштабируемости, энергоэффективности и устойчивости к кибератакам. Особое внимание уделяется проблеме «триилеммы блокчейна» и поиску оптимального баланса между безопасностью, децентрализацией и производительностью. Сделан вывод о важности гибридных моделей и инновационных протоколов в формировании будущей архитектуры децентрализованных финансов.

Ключевые слова: Криптовалюта, алгоритм консенсуса, блокчейн, Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Byzantine Fault Tolerance, масштабируемость, децентрализация, безопасность.

Алгоритмы консенсуса представляют собой фундаментальную основу функционирования криптовалют и распределённых реестров. В условиях отсутствия централизованного органа, который бы отвечал за достоверность транзакций и защищал участников от двойного расходования цифровых активов, именно консенсусные протоколы обеспечивают согласованность данных в сети и создают доверие между анонимными пользователями. Их экономическая и технологическая сущность заключается в том, что децентрализованное сообщество участников с помощью математических механизмов и криптографических алгоритмов приходит к единому решению о правильности записей в блокчейне, исключая возможность подделки и фальсификации информации [1].

Наиболее известным и исторически первым протоколом является алгоритм Proof-of-Work (PoW), разработанный и реализованный Сатоши Накамото в сети Bitcoin в 2008 г. Его принцип основан на необходимости решения сложных криптографических задач, которые требуют значительных вычислительных ресурсов. Участники сети, называемые майнерами, конкурируют за право добавить новый блок в цепочку, предоставляя доказательство проделанной работы в виде найденного хеша. Данный подход обеспечивает высокий уровень безопасности, так как для успешной атаки злоумышленнику потребуется сосредоточить более половины общей вычислительной мощности сети. Однако PoW характеризуется рядом недостатков: высоким энергопотреблением, низкой скоростью обработки транзакций (7 транзакций в секунду для Bitcoin) и неэффективностью в масштабировании. Экологические издержки PoW стали предметом критики как со стороны научного сообщества, так и со стороны регуляторов, что стимулировало поиск альтернативных моделей [2].

Следующим этапом развития стал алгоритм Proof-of-Stake (PoS), в основе которого лежит принцип выбора валидаторов на основании их доли владения токенами. Узлы с большей долей имеют больше шансов подтвердить транзакцию и получить вознаграждение. Это резко

сокращает энергозатраты, так как отпадает необходимость в использовании огромных вычислительных мощностей. PoS получил широкое распространение в сетях второго поколения, включая Ethereum, который в 2022 году окончательно перешёл с PoW на PoS. Вместе с тем критики отмечают проблему централизации, так как крупные держатели монет способны получать непропорционально высокий доход, усиливая своё влияние. Кроме того, в литературе выделяется так называемая проблема «nothing at stake» – возможность валидаторов подтверждать конкурирующие цепочки без дополнительных издержек, что теоретически подрывает устойчивость системы [3].

Разновидностью данного подхода является Delegated Proof-of-Stake (DPoS), предложенный Дэном Ларимером и реализованный в проектах BitShares и EOS. В данной модели пользователи не участвуют напрямую в подтверждении блоков, а делегируют свои права ограниченному числу избранных валидаторов – депутатов, которые формируют блоки. Такой механизм позволяет значительно увеличить пропускную способность сети (до нескольких тысяч транзакций в секунду) и обеспечивает более быстрый консенсус. Однако уровень децентрализации снижается, поскольку фактически контроль над сетью сосредоточен в руках небольшой группы валидаторов. В ряде случаев отмечалась высокая вероятность сговора этих узлов, что снижает устойчивость DPoS к манипуляциям [4].

Помимо PoW и PoS, важное значение имеет класс алгоритмов византийской отказоустойчивости, наиболее известным из которых является Practical Byzantine Fault Tolerance (PBFT). Данный алгоритм решает задачу византийских генералов – ситуацию, когда часть узлов может действовать злонамеренно или некорректно, но система при этом должна сохранять согласованность. PBFT позволяет достигать консенсуса даже при наличии до трети недобросовестных участников. Его ключевым преимуществом является высокая скорость подтверждения транзакций (менее 1 секунды), что делает его востребованным в корпоративных и частных блокчейнах. Недостатком является слабая масштабируемость: при росте числа участников значительно увеличиваются коммуникационные издержки, что препятствует применению PBFT в публичных криптовалютных сетях [5].

С развитием технологий появляются и гибридные протоколы, сочетающие преимущества разных подходов. Например, некоторые блокчейны используют комбинацию PoW и PoS, при которой создание блоков осуществляется майнерами, а их финальная валидация закрепляется за держателями токенов. Такой подход снижает энергозатраты и одновременно сохраняет высокий уровень безопасности. Другие примеры включают Proof-of-Authority (PoA), где консенсус достигается за счёт ограниченного числа доверенных валидаторов, и Proof-of-History (PoH), применяемый в блокчейне Solana для повышения пропускной способности за счёт криптографической отметки времени. Кроме того, появились инновационные протоколы, использующие иные ресурсы, например Proof-of-Space и Proof-of-Space-Time, основанные на выделении дискового пространства для хранения данных и криптографической верификации этого процесса. Ярким примером такого подхода является Filecoin [6].

Таблица 1

Для удобства анализа представим
сравнительные характеристики основных алгоритмов:

Алгоритм	**Преимущества**	**Недостатки**	**Примеры проектов**
Proof-of-Work (PoW)	Высокая безопасность, проверенная временем	Энергозатраты, низкая скорость, ограниченная масштабируемость	Bitcoin, Litecoin

Proof-of-Stake (PoS)	Энергоэффективность, высокая скорость	Риск централизации, проблема «nothing at stake»	Ethereum 2.0, Cardano
Delegated Proof-of-Stake (DPoS)	Высокая пропускная способность, демократическая модель голосования	Снижение децентрализации, риск сговора валидаторов	EOS, BitShares
PBFT	Быстрый консенсус, устойчивость к злонамеренным узлам	Плохая масштабируемость, ограниченная сфера применения	Hyperledger, Tendermint
Гибридные модели	Баланс между безопасностью и эффективностью	Сложность реализации, неопределённость регулирования	Solana (PoH), Filecoin (PoST)

Сравнительный анализ показывает, что каждая модель консенсуса имеет свои сильные и слабые стороны, что объясняет разнообразие их применения в зависимости от целей сети. PoW продолжает оставаться эталоном безопасности, но уступает новым подходам по энергоэффективности. PoS и его производные обеспечивают высокую масштабируемость, но подвержены угрозам централизации. PBFT и аналогичные решения успешно применяются в частных блокчейнах, но не подходят для публичных сетей. Гибридные алгоритмы позволяют находить компромиссные решения, объединяя преимущества нескольких моделей.

Дальнейшее развитие алгоритмов консенсуса связано с поиском баланса между тремя критериями, известными как «триилемма блокчейна» Виталия Бутерина: децентрализацией, безопасностью и масштабируемостью [7]. Одновременное достижение оптимума по всем направлениям пока невозможно, однако активно ведутся исследования в области шардинга, технологии zk-SNARKs и zk-STARKs, а также интеграции искусственного интеллекта для прогнозирования и предотвращения атак. Перспективным направлением является также разработка алгоритмов, учитывающих устойчивое развитие и минимизацию углеродного следа, что особенно актуально в условиях глобальной климатической повестки.

Таким образом, алгоритмы консенсуса представляют собой ключевой элемент архитектуры криптовалют и блокчейн-систем. Их эволюция отражает стремление индустрии найти баланс между безопасностью, эффективностью и децентрализацией. Несмотря на существующие противоречия, именно развитие гибридных и инновационных моделей открывает новые перспективы для дальнейшего распространения криптовалют, их интеграции в глобальную финансовую систему и адаптации под различные отраслевые потребности.

Список литературы:

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.
2. Antonopoulos A. Mastering Bitcoin. – O’Reilly Media, 2017.
3. Buterin V. On Stake. – Ethereum Foundation Blog, 2014.
4. Larimer D. Delegated Proof-of-Stake Consensus. – BitShares, 2014.
5. Castro M., Liskov B. Practical Byzantine Fault Tolerance. – OSDI, 1999.
6. Protocol Labs. Filecoin: A Decentralized Storage Network. – 2020.
7. Buterin V. Blockchain Trilemma. – Ethereum Research, 2018.
8. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. – 2014.

9. Gudgeon L., Perez D., Harz D. et al. The DeFi Consensus Landscape. – arXiv:2001.00572, 2020.

10. Zhang F., Cecchetti E., Croman K. Town Crier: An Authenticated Data Feed for Smart Contracts. – ACM CCS, 2016.