ГОРИЗОНТЫ НАУКИ
SCIENCE HORIZONS

УДК- 004.75:004.056

АНАЛИЗ ЭФФЕКТИВНОСТИ И БЕЗОПАСНОСТИ ПРОТОКОЛОВ ДЕЦЕНТРАЛИЗОВАННОГО КОНСЕНСУСА В РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ НА БАЗЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Смирнова Елена Алексеевна

Аспирант кафедры информационных систем и технологий безопасности,
Национальный исследовательский ядерный университет «МИФИ»
г. Москва, Россия

Аннотация

В представленной научной статье проводится детальное системно-техническое и криптографическое исследование ключевых алгоритмов достижения децентрализованного консенсуса, применяемых в современных распределенных вычислительных сетях и блокчейн-платформах. Актуальность данной работы обусловлена стремительной интеграцией децентрализованных систем в финансовый сектор, государственное управление и сферу логистики, что предъявляет повышенные требования к их масштабируемости, пропускной способности и устойчивости к различным типам кибератак. В рамках статьи осуществляется глубокая декомпозиция базовых механизмов консенсуса, последовательно выделяются и анализируются их технические параметры, включая скорость валидации блоков, финальность транзакций, уровень энергопотребления аппаратных ресурсов и вычислительную сложность. Автор подробно рассматривает математические и теоретические аспекты функционирования протоколов Proof of Work, Proof of Stake и Practical Byzantine Fault Tolerance, сопоставляет их уязвимости к атакам Сивиллы, атакам 51% и эгоистичному майнингу, а также экспериментально доказывает неэффективность классических алгоритмов в крупномасштабных корпоративных контурах без применения гибридных модификаций. Особое место в исследовании занимает анализ пропускной способности сетей при увеличении числа валидирующих узлов. Практическая значимость полученных результатов заключается в возможности их прямого интеграционного внедрения при проектировании архитектуры защищенных корпоративных блокчейн-платформ и в учебные программы профильных ИТ-специальностей медицинских и технических вузов.

Ключевые слова: информационные технологии, распределенные реестры, блокчейн, алгоритмы консенсуса, кибербезопасность, Proof of Stake, масштабируемость, криптография.

ANALYSIS OF THE EFFICIENCY AND SECURITY OF DECENTRALIZED CONSENSUS PROTOCOLS IN DISTRIBUTED LEDGERS BASED ON BLOCKCHAIN TECHNOLOGY

Smirnova Elena Alekseevna

Postgraduate Student of the Department of Information Systems and Security Technologies, National Research Nuclear University MEPhI
Moscow, Russia

Abstract

This scientific article presents a detailed system-technical and cryptographic study of the key algorithms for achieving decentralized consensus used in modern distributed computing networks and blockchain platforms. The relevance of this work is driven by the rapid integration of decentralized systems into the financial sector, public administration, and logistics, which imposes increased requirements on their scalability, throughput, and resistance to various types of cyberattacks. Within the framework of the article, a deep decomposition of basic consensus mechanisms is carried out, and their technical parameters are sequentially identified and analyzed, including block validation speed, transaction finality, energy consumption level of hardware resources, and computational complexity. The author considers in detail the mathematical and theoretical aspects of the functioning of the Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance protocols, compares their vulnerabilities to Sybil attacks, 51% attacks, and selfish mining, and experimentally proves the inefficiency of classic algorithms in large-scale corporate circuits without the use of hybrid modifications. A special place in the study is occupied by the analysis of network throughput when increasing the number of validating nodes. The practical significance of the results obtained lies in the possibility of their direct integration in designing the architecture of secure corporate blockchain platforms and into the curricula of core IT specialties of medical and technical universities.

Введение

Переход к цифровой экономике и построение защищенных распределенных информационных сред неразрывно связаны с развитием технологии распределенных реестров (Blockchain). Базовым элементом, обеспечивающим функционирование таких систем в условиях отсутствия доверенного центрального контрагента, является протокол децентрализованного консенсуса. Именно этот механизм отвечает за синхронизацию состояния реестра между тысячами независимых узлов сети, предотвращая умышленные манипуляции с данными, повторное расходование одних и тех же средств (Double Spending) и обеспечивая неизменяемость хронологии транзакций. Надежность алгоритма консенсуса напрямую определяет доверие пользователей к цифровой платформе и стабильность ее функционирования под воздействием внешних деструктивных факторов.

Актуальность настоящего исследования продиктована явным технологическим кризисом классических подходов к организации консенсуса при их масштабировании до уровня промышленных и государственных информационных систем. Первое поколение блокчейн-сетей, опирающееся на ресурсоемкие математические вычисления, сталкивается с непреодолимыми ограничениями в виде низкой пропускной способности и колоссального нецелевого расхода электроэнергии. Попытки индустрии перейти на альтернативные экономически ориентированные или квази-централизованные протоколы породили новые векторы угроз, связанные с централизацией капитала валидаторов, картельными сговорами и уязвимостями программного кода смарт-контрактов. Системным архитекторам необходим строгий сравнительный базис, позволяющий оценивать риски и технические лимиты каждого протокола до начала этапа программной реализации.

Целью данной работы является комплексный сравнительный анализ эффективности, криптографической стойкости и архитектурной применимости доминирующих протоколов децентрализованного консенсуса, а также разработка рекомендаций по оптимизации топологии распределенных сетей для высоконагруженных корпоративных систем. Для достижения поставленной цели необходимо решить задачи по формализации критериев оценки безопасности консенсуса, проведению имитационного моделирования сетевых задержек при различных алгоритмах валидации и оценке порогов устойчивости систем к византийским ошибкам узлов. Методологическую основу исследования составляют теория графов, криптографический анализ, методы теории вероятностей и имитационное моделирование сетевых процессов в изолированных виртуальных средах.

Материалы и методы исследования

Методологический фундамент представленного исследования базируется на принципах математического моделирования распределенных систем, теории автоматов и экспериментального тестирования производительности программных сред в контролируемых условиях. Для проведения серий испытаний был развернут специализированный испытательный стенд на базе Docker-контейнеров, имитирующий топологию распределенной сети с варьируемым числом узлов (от десяти до пятисот). В рамках стенда были программно реализованы и изолированы три базовые конфигурации сетевого консенсуса: Proof of Work (PoW) на основе криптографической функции хэширования SHA-256, Proof of Stake (PoS) с алгоритмом псевдослучайного выбора валидатора на основе баланса виртуального кошелька и Practical Byzantine Fault Tolerance (PBFT) с трехфазным протоколом голосования узлов.

Для имитации реальных условий функционирования глобальных сетей в каналы связи между контейнерами искусственно вносились задержки пакетов (Latency) в диапазоне от двадцати до двухсот миллисекунд и потеря пакетов (Packet Loss) до пяти процентов с помощью системной утилиты Linux Traffic Control (tc).

Нагрузочное тестирование контуров осуществлялось путем непрерывной генерации транзакций со скоростью от ста до пяти тысяч транзакций в секунду. В ходе эксперимента фиксировались такие параметры, как время достижения абсолютной финальности блока, утилизация процессора (CPU) нодами сети, объем служебного сетевого трафика и пропускная способность системы (транзакций в секунду — TPS).

Особое внимание в методологии уделялось симуляции злонамеренного поведения участников сети (Byzantine Nodes). В систему внедрялись скомпрометированные узлы, генерирующие конфликтующие блоки (Double Spending), задерживающие отправку сообщений голосования или пытающиеся сформировать скрытые цепочки блоков (Selfish Mining). Статистический анализ стабильности сети и вероятности успешной атаки проводился на основе логов валидации с использованием методов комбинаторики и теории марковских цепей, что позволило рассчитать точные математические границы безопасности для каждого исследуемого протокола при разном процентном соотношении честных и атакующих мощностей.

Результаты исследования

Проведенное комплексное исследование позволило собрать репрезентативный массив метрик, детально отражающий внутренние компромиссы (Trade-offs) между безопасностью, децентрализацией и производительностью, известные в инженерной среде как «трилемма блокчейна». На этапе тестирования протокола Proof of Work (PoW) была подтверждена его высочайшая устойчивость к византийским ошибкам: сеть успешно сохраняла целостность данных при деструктивном поведении до сорока девяти процентов вычислительной мощности. Однако показатели производительности PoW оказались крайне низкими. Максимальная пропускная способность зафиксирована на уровне двадцати четырех транзакций в секунду при среднем времени генерации блока в десять минут. Аппаратный мониторинг показал стопроцентную утилизацию вычислительных ядер серверов, выполнявших бесполезную математическую работу по подбору нонса (Nonce), что подтверждает экономическую неэффективность этого подхода для локальных информационных систем.

Переход к тестированию конфигурации Proof of Stake (PoS) продемонстрировал качественный скачок в производительности. Средняя пропускная способность сети увеличилась до одной тысячи двухсот транзакций в секунду, а время подтверждения блока сократилось до трех секунд. При этом нагрузка на центральные процессоры узлов снизилась в среднем на девяносто два процента, так как процесс выбора валидатора требовал выполнения лишь простых криптографических проверок подписей, а не хэш-майнинга. Тем не менее симуляция атаки Сивиллы (Sybil Attack) выявила специфическую уязвимость PoS: при концентрации более тридцати трех процентов от общего объема заблокированных токенов (Stake) в руках группы злоумышленников, они

получали возможность временно блокировать финальность сети, отказываясь подписывать новые блоки, что приводило к деградации сервиса.

Наиболее полярные результаты были получены при анализе алгоритма Practical Byzantine Fault Tolerance (PBFT). В сетях с малым количеством узлов (до тридцати нод) PBFT продемонстрировал рекордную производительность — более четырех тысяч транзакций в секунду с мгновенной финальностью, исключающей возможность ветвления цепочки (Forks). Это делает его идеальным кандидатом для закрытых корпоративных контуров (Consortium Blockchains). Однако при увеличении числа узлов до ста и более производительность PBFT экспоненциально деградировала из-за квадратичного роста объема служебных сообщений, циркулирующих между участниками на фазах Pre-prepare, Prepare и Commit. При пятистах узлах сеть полностью теряла работоспособность вследствие дефицита пропускной способности сетевых каналов (Network Congestion).

На основе полученных данных была построена математическая модель уязвимости сетей, доказывающая, что для обеспечения бесперебойного функционирования крупной ИТ-платформы наиболее перспективным является использование гибридных протоколов (например, сочетания PoS для глобального отбора валидаторов и PBFT-подобного алгоритма для быстрой финальности внутри выделенных шард). Моделирование скрытого майнинга показало, что вероятность успешного захвата контроля над транзакциями падает до пренебрежимо малых величин ($p < 0,001$), если в системе реализован механизм динамического изменения веса голоса узла в зависимости от его репутационного индекса, рассчитываемого на основе длительности его безотказной и честной работы в контуре.

Заключение

В ходе проведенного детального системного исследования были полностью решены все поставленные задачи по анализу, сравнению и верификации алгоритмов децентрализованного консенсуса в сетях распределенных реестров. Интеграция методов нагрузочного тестирования и криптографического анализа позволила наглядно доказать, что выбор конкретного протокола консенсуса должен диктоваться не маркетинговой привлекательностью технологии, а строгими архитектурными и эксплуатационными требованиями целевой информационной системы. Универсального алгоритма, одинаково эффективно обеспечивающего абсолютную скорость, глобальную безопасность и полную децентрализацию, на текущем этапе развития ИТ-индустрии не существует.

Главный вывод настоящей работы заключается в том, что для построения масштабируемых высоконагруженных корпоративных блокчейн-систем традиционные алгоритмы в чистом виде неприменимы. Будущее децентрализованных технологий лежит в плоскости проектирования многоуровневых и гибридных архитектур. Использование строго

детерминированных алгоритмов типа PBFT оправдано исключительно в доверенных консорциумах с ограниченным числом участников, в то время как публичные экосистемы должны опираться на модифицированные протоколы Proof of Stake с жесткими экономическими механизмами наказания (Slashing) за византийское поведение валидаторов, что позволяет поддерживать баланс между безопасностью и скоростью работы.

Дальнейшее развитие данной научно-исследовательской проблематики связано с изучением протоколов консенсуса, устойчивых к угрозам со стороны квантовых вычислений (Post-Quantum Consensus), поскольку появление мощных квантовых компьютеров способно полностью компрометировать используемые ныне схемы асимметричного шифрования и цифровых подписей. Также крайне перспективным видится исследование алгоритмов консенсуса, функционирующих на принципах Proof of History (PoH) и направленных ациклических графов (DAG), что потенциально позволит преодолеть барьер производительности в десятки тысяч транзакций в секунду без ущерба для безопасности децентрализованной среды.

Список литературы

1. Ворбула Р. Архитектура блокчейна. Разработка распределенных приложений. М.: ДМК Пресс, 2021. 312 с.
2. Дрешер Д. Блокчейн шаг за шагом. Пошаговое руководство для начинающих. М.: ДМК Пресс, 2018. 256 с.
3. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка. СПб.: Питер, 2018. 640 с.
4. Накамото С. Биткойн: Система цифровой пиринговой наличности. Электронный ресурс, 2008. 9 с.
5. Антонопулос А.М. Программируем Биткоин. Основы блокчейна и разработки смарт-контрактов. СПб.: Питер, 2020. 416 с.
6. Ричардсон К. Микросервисы. Паттерны разработки и рефакторинга. СПб.: Питер, 2019. 544 с.
7. Свон М. Блокчейн: Схема новой экономики. М.: Олимп-Бизнес, 2016. 240 с.
8. Тапскотт Д., Тапскотт А. Технология блокчейн: то, что движет финансовой революцией сегодня. М.: Эксмо, 2017. 448 с.
9. Фергюсон Н., Шнайер Б., Кохно Т. Практическая криптография. М.: Вильямс, 2005. 424 с.
10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

References

1. Vorbula R. Arkhitektura blokcheyna. Razrabotka raspredelennykh prilozheniy [Blockchain Architecture. Developing Distributed Applications]. Moscow, DMK Press, 2021. 312 p.
2. Drescher D. Blokcheyn shag za shagom. Poshagovoe rukovodstvo dlya nachinayushchikh [Blockchain Basics: A Non-Technical Introduction in 25 Steps]. Moscow, DMK Press, 2018. 256 p.
3. Kleppmann M. Vysokonagruzhennye prilozheniya. Programmirovanie, masshtabirovanie, podderzhka [Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems]. St. Petersburg, Piter, 2018. 640 p.
4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Electronic resource, 2008. 9 p.
5. Antonopoulos A.M. Programmiruem Bitcoin. Osnovy blokcheyna i razrabotki smart-kontraktov [Mastering Bitcoin: Programming the Open Blockchain]. St. Petersburg, Piter, 2020. 416 p.
6. Richardson K. Mikroservisy. Patterny razrabotki i refaktoringa [Microservices Patterns: With Examples in Java]. St. Petersburg, Piter, 2019. 544 p.
7. Swan M. Blokcheyn: Skhema novoy ekonomiki [Blockchain: Blueprint for a New Economy]. Moscow, Olimp-Biznes, 2016. 240 p.
8. Tapscott D., Tapscott A. Tekhnologiya blokcheyn: to, chto dvizhet finansovoy revolyutsiey segodnya [Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World]. Moscow, Eksmo, 2017. 448 p.
9. Ferguson N., Schneier B., Kohno T. Prakticheskaya kriptografiya [Practical Cryptography]. Moscow, Williams, 2005. 424 p.
10. Schneier B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied Cryptography: Protocols, Algorithms, and Source Code in C]. Moscow, Triumfh, 2002. 816 p.