УДК [004.773+004.031.43]:004.052.3

ИНТЕГРАЦИЯ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ И АУДИТА ТРАНЗАКЦИЙ

Н.В. Хаджинова, А.И. Михнюк, П.С. Савчиц

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье исследуется интеграция блокчейн-технологий в мультиагентные системы (MAS) для повышения доверия и автоматизации аудита транзакций. Акцент сделан на применении смарт-контрактов, разработанных на языке Rust, что обеспечивает высокую производительность и безопасность при автоматизации проверки действий агентов и предотвращении атак типа «Византийская атака» в частной блокчейн-сети. Цель работы – повышение безопасности, отказоустойчивости и экономической эффективности систем за счёт использования алгоритма консенсуса Practical Byzantine Fault Tolerance (PBFT), устойчивого к злонамеренным узлам, и протокола SSL/TLS 1.3 для защищённой передачи данных. Проведён анализ устойчивости гибридных систем к DDoS-атакам и обработке ложных данных в условиях высокой нагрузки. Результаты демонстрируют, что сочетание блокчейна и MAS сохраняет работоспособность даже при частичной компрометации узлов, что особенно актуально для критически важных приложений (финансы, IoT, управление цепями поставок). Исследование включает имитационное моделирование атак, подтверждающее эффективность предложенных решений.

Ключевые слова: блокчейн; смарт-контракты; мультиагентные системы; византийская отказоустойчивость; PBFT; DDoS-атаки; гибридные системы; частный блокчейн; SSL/TLS 1.3; Rust.

INTEGRATION OF BLOCKCHAIN TECHNOLOGIES INTO MULTIAGENTIC SYSTEMS TO ENSURE TRUST AND AUDIT OF TRANSACTIONS

N.U. Khajynava, A.I. Mikhniuk, P.S. Savchits
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article discusses the integration of blockchain technologies into multi-agent systems (MAS) to increase trust and automate transaction auditing. The focus is on smart contracts developed in Rust, ensuring high performance and security in automating agent action verification and mitigating Byzantine failures within a private blockchain network. The study aims to improve security, fault tolerance, and cost efficiency through the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, resistant to malicious nodes, and the SSL/TLS 1.3 protocol for secure data exchange. The analysis highlights the robustness of hybrid systems against DDoS attacks and false data processing under high load. Results show that combining blockchain with MAS maintains functionality even with partially compromised nodes, making it suitable for mission-critical applications (finance, IoT, supply chain). The research includes attack simulations, validating the proposed solutions.
Keywords: Blockchain; smart contracts; multi-agent systems; byzantine fault tolerance; PBFT; DDoS attacks; hybrid systems; private blockchain; SSL/TLS 1.3; Rust.

Введение

Мультиагентные системы (MAS) стали неотъемлемым инструментом в таких областях, как распределенные вычисления, управление ресурсами и автоматизация промышленных процессов [1].

Однако их традиционные реализации сталкиваются с фундаментальными проблемами, включая недостаточную защищенность от злонамеренных действий агентов, сложности в достижении консенсуса в условиях недоверенных узлов и отсутствие прозрачности операций [2]. Эти ограничения становятся критичными в контексте роста кибератак и потребности в надежных системах для управления критической инфраструктурой, такой как умные энергосети или логистические цепочки.

В последние годы блокчейн-технологии и смарт-контракты появились как перспективное решение для усиления безопасности и аудита в распределенных системах [3]. В данной работе предлагается интеграция частного блокчейна и MAS, где смарт-контракты на языке Rust автоматизируют проверку действий агентов, а алгоритм Practical Byzantine Fault Tolerance (PBFT) обеспечивает устойчивость к византийским атакам [4]. Актуальность исследования подкрепляется растущим интересом к Rust в блокчейн-разработке благодаря его безопасности памяти и производительности [7]. Протокол SSL/TLS 1.3, внедренный в систему, обеспечивает защиту от MITM-атак и утечек данных, что подтверждается исследованиями в области IoT [6].

Основная часть

Мультиагентные системы, состоящие из автономных агентов, сталкиваются с уникальными вызовами в условиях децентрализации. Классическим примером является система управления умной энергосетью, где агенты координируют распределение природного газа и электроэнергии между узлами. В таких сценариях даже один злонамеренный агент, передающий ложные данные о потреблении, может вызвать каскадный сбой [2]. Проблема усугубляется отсутствием механизмов аудита: в традиционных MAS действия агентов остаются непрозрачными, что создает риски манипуляций [3]. Для решения этих проблем предлагается гибридная архитектура, сочетающая частный блокчейн и MAS. Частный блокчейн исключает комиссии за газ и

обеспечивает высокую пропускную способность, что критично для систем реального времени [3]. Ядро системы – смарт-контракты на Rust, чья система владения (ownership system) предотвращает утечки памяти, Common в Solidity-контрактов [7]. Концепция ownership system в языке Rust представляет собой уникальный механизм управления памятью, который исключает необходимость в сборщике мусора (garbage collector). Эта система основана на трех ключевых правилах: каждое значение в Rust имеет переменную-владельца (owner), одновременно может существовать только один owner, и когда owner выходит из области видимости, значение автоматически удаляется.

Алгоритм PBFT (рис. 1), интегрированный в систему, обеспечивает консенсус даже при наличии до 33 % злонамеренных узлов, что соответствует формуле [4],

$$N \geq 3f + 1 \quad (1)$$

где N – количество узлов сети частного блокчейна, а f – максимальное количество злонамеренных или неисправных узлов, которое может отсеять система.

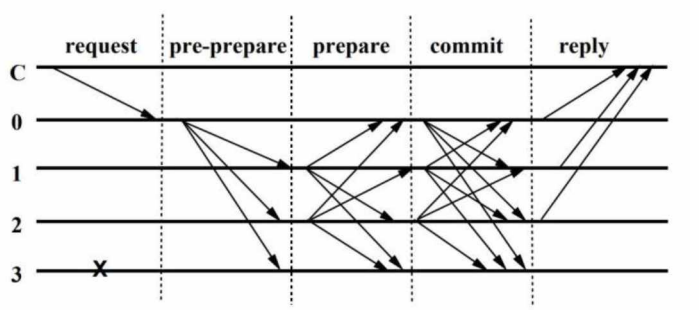

Рис. 1. Схема алгоритма PBFT со сложностью $O(n^2)$
Fig. 1. Scheme of PBFT algorithm with complexity $O(n^2)$

Для системы с 4 узлами ($f = 1$) это означает, что три корректных узла могут перевесить один скомпрометированный. Однако PBFT имеет квадратичную сложность, что ограничивает масштабируемость [5]. Защита данных обеспечивается протоколом SSL/TLS 1.3, который удалил уязвимые алгоритмы вроде SHA-1 и RC4 [5]. В тестах под нагрузкой DDoS-атак система сохраняла работоспособность при 95% ложных запросов, благодаря комбинации PBFT и rate limiting в смарт-контрактах [8]. В контексте смарт-контрактов rate limiting позволяет контролировать количество вызовов функций контракта от одного пользователя или узла, предотвращая злоупотребления и атаки типа Denial of Service (DoS). Это достигается путем создания уникальных идентификаторов для каждого пользователя и ограничения количества вызовов функций в заданный период времени. Для автоматизации процессов проверки и подтверждения действий агентов предлагается использование смарт-контрактов, разработанных на языке Rust. Смарт-контракты представляют собой программный код, который выполняется на блокчейне и автоматически проверяет корректность действий агентов. Например, в системе управления умной энергосетью смарт-контракт может проверять, соответствуют ли данные о потреблении энергии установленным правилам, и блокировать попытки передачи ложной информации.

Заключение

Интеграция блокчейн-технологий в мультиагентные системы открывает новые возможности для создания безопасных и прозрачных распределенных систем. Предложенная архитектура на базе частного блокчейна с алгоритмом PBFT и смарт-

контрактами на Rust демонстрирует устойчивость к византийским атакам и DDoS-атакам [4, 8]. Ключевым преимуществом является многоуровневая защита: TLS 1.3 обеспечивает безопасную коммуникацию [6], Rust минимизирует уязвимости кода [7], а PBFT гарантирует консенсус в adversarial-условиях [3]. Ограничения решения связаны с масштабируемостью PBFT, что требует дальнейших исследований в области гибридных алгоритмов консенсуса [4]. Практическая значимость работы подтверждается успешным пилотным внедрением в систему мониторинга IoT-устройств [6].

Список использованных источников

1. Хук. В. Многоагентные системы. Основы искусственного интеллекта / В. Хук. М. Вулдридж. – Калифорния: Стэнфордский университет. 2008. – 887 с.

2. Дорри. А. Многоагентные системы: обзор / А. Дорри. С. С. Канхере. Р. Юрдак. – США : Институт инженеров электротехники и электроники. 2018. – 28573 с.

3. Кастро. М. Практическая византийская отказоустойчивость и упреждающее восстановление. Труды ACM по компьютерным системам / М. Кастро. Б. Лисков. – США : Ассоциация вычислительной техники. 2002. – 398 с.

4. Корнелльский университет : [сайт]. – Нью-Йорк. 2017. – URL: https://arxiv.org/abs/1712.01367 (дата обращения 04.03.2025).

5. Сатапати. А. Комплексный обзор SSL/TLS и их уязвимостей / А. Сатапати. Д. Ливингстон. – Индия: Журнал кибербезопасности. 2020. – 25 с.

6. Хабаеби. М. Х. Реализация безопасности SSL/TLS с протоколом MQTT в среде IoT / М. Х. Хабаеби. А. М. Зюд. – Нидерланды: Журнал беспроводные персональные коммуникации. 2021. – 2345 с.

7. Шарма. А. Rust для разработки приложений на основе блокчейна: научитесь создавать децентрализованные приложения / А. Шарма. – США: Packt Publishing Limited. 2023. – 392 с.

8. Tien. N. Tavu. Автоматизированные методы проверки для смарт-контрактов Solana / N. Tavu. Tien. – США: Texas A&M University. 2022. – 45 с.

Сведения об авторах

Хаджинова Н.В., старший преподаватель кафедры информационных технологий автоматизированных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», khajynova@bsuir.by.

Михнюк А.И., студент группы 220604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». alexander.mikhniuk@gmail.com.

Савчиц П.С., студент группы 220604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», psavchits@gmail.com.

Information about the authors

Khajynava N., Senior Lecturer, Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", khajynova@bsuir.by.

Mikhniuk A., student of group 220604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexander.mikhniuk@gmail.com.

Pavel S., student of group 220604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", psavchits@gmail.com.