УДК 004.4:004.056
DOI

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ПРЕДОТВРАЩЕНИЯ DDOS-АТАК

[1]Беспалова Н.В., [2]Пугачева Д.Б.

[1]ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, e-mail: NVBespalova@fa.ru;
[2]ФГБОУ ВО «МИРЭА – Российский технологический университет», Москва, e-mail: d.pugacheva@list.ru

Статья посвящена исследованию технологии блокчейн, которая позволяет не только обеспечить хранение и передачу данных в информационных системах, но и гарантирует их безопасность. Блокчейн может стать мощным инструментом для предотвращения DDoS-атак, благодаря своей децентрализованной природе и способности к криптографической защите данных. Механизм защиты от DDoS-атак с использованием технологии распределенных сетей и блокчейна представляет собой инновационный подход к обеспечению безопасности и стабильности онлайн-сервисов и веб-приложений. Рассмотрено применение технологии блокчейна для предотвращения DDoS-атак. Такие характеристики технологии блокчейна, как неизменность, децентрализация, целостность, обеспечивают жизнеспособность технологии. Данная технология находит применение в различных отраслях. Используя системы на основе блокчейна для обнаружения угроз, можно эффективно обнаруживать и реагировать на угрозы. Таким образом, эффективные методы предотвращения DDoS-атак могут быть реализованы с использованием технологий блокчейн. В работе проведен анализ готовых решений применения технологии блокчейна, предоставляющих функциональность для хранения данных в распределенных системах. В данной статье авторы представляют исследование DDoS-решений на основе блокчейна. В ходе работы были сформулированы преимущества технологии, проанализированы существующие DLT-решения и сделан вывод о необходимости разработки инновационных решений, основанных на базе технологии распределенного реестра с возможностью интеграции с SIEM-системами.

Ключевые слова: распределенные системы, технологии распределенного реестра, информационная безопасность, безопасность платежей, блокчейна, DDoS-атак

ANALYSIS OF THE CAPABILITIES OF BLOCKCHAIN TECHNOLOGY TO PREVENT DDOS ATTACKS

[1]Bespalova N.V., [2]Pugacheva D.B.

[1]Financial University under the Government of the Russian Federation, Moscow, e-mail: NVBespalova@fa.ru;
[2]MIREA – Russian Technological University Moscow, e-mail: d.pugacheva@list.ru

The article is devoted to the study of blockchain technology, which allows not only to ensure the storage and transmission of data in information systems, but also guarantees their security. Blockchain can be a powerful tool for preventing DDoS attacks due to its decentralized nature and ability to cryptographicly protect data. During the work, the advantages of the technology were formulated and algorithmic solutions were proposed for its optimal functioning. The DDoS protection mechanism using distributed network and blockchain technology is an innovative approach to ensuring the security and stability of online services and web applications. The use of blockchain technology to prevent DDoS attacks is considered. Characteristics of blockchain technology such as immutability, decentralization, and integrity ensure the viability of the technology. This technology is used in various industries. By using blockchain-based threat detection systems, threats can be effectively detected and responded to. Thus, effective methods for preventing DDoS attacks can be implemented using blockchain technologies. The work analyzes ready-made solutions for using blockchain technology that provide functionality for storing data in distributed systems. In this article, the authors present a study of blockchain-based DDoS solutions During the work, the advantages of the technology were formulated, existing DLT solutions were analyzed and a conclusion was made about the need to develop innovative solutions based on distributed registry technology with the ability to integrate with SIEM systems.

Keywords: distributed systems, distributed registry technologies, information security, payment security, blockchain, DDoS attacks

Проблема информационной безопасности становится все более актуальной в свете активного роста объема информации, циркулирующей в различных информационных системах. Необходимость комплексного подхода при решении задач информационной безопасности связана с тем, что помимо роста объема атак в мире растет их уровень сложности, что требует использования современных автоматизированных средств по мониторингу и контролю безопасности информационных систем. Одним из наиболее перспективных направлений на сегодняшний день является повышение безопасности транзакций и хранение данных в сфере банковских услуг. Рост цифровых способов оплаты повышает актуальность обеспечения безопасности платежей, на-

правленных на защиту конфиденциальности данных и транзакций клиента, для предотвращения несанкционированного использования и модификации данных.

По данным ЦБ рост хищения денежных средств клиентов при банковских переводах и платежах в 2023 г. составил более 11 % [1]. Перспективным решением по обеспечению безопасности хранения и передачи данных в финансовой сфере являются распределенные реестры.

Блокчейн-технология по своей сути – распределенная база данных, в которой информация о каждой транзакции фиксируется и хранится в виде блоков, связанных между собой средствами криптографии. Децентрализация и криптографические механизмы позволяют обеспечить такие аспекты информационной безопасности, как целостность данных и доступность информации [2, 3]. Распределенные атаки отказа в обслуживании (DDoS) представляют собой серьезную угрозу для онлайн-сервисов и предприятий, поскольку направлены на перегрузку информационной системы запросами, что может привести к снижению производительности или полному отказу работы системы.

Использование технологии блокчейн позволяет минимизировать возможность DDoS-атак:

– децентрализация блокчейн-сетей снижает эффективность централизованных DDoS-атак;

– прозрачность и целостность блокчейн-транзакций позволяют детектировать аномалии в сетевой активности.

Таким образом, обнаружение и предотвращение DDoS-атак становятся возможными на ранних стадиях.

Централизованные и распределенные программные системы

Программные системы, в зависимости от их внутренней архитектуры, можно разделить на два основных типа: централизованные и распределенные. Централизованные системы обычно имеют единую точку управления или хранения данных, к которой все пользователи и компоненты системы обращаются для получения информации или выполнения операций.

Распределенные системы основаны на децентрализованной архитектуре, при этом данные распределены между различными узлами, каждый из которых выполняет свою часть работы. Одними из главных преимуществ таких систем являются масштабируемость, возможность расширения сети и увеличения производительности с ростом объема обрабатываемых данных и высокая надежность, когда выход из строя одного узла не компрометирует остальные. К недостаткам можно отнести сложность и высокую стоимость разработки, настройки и поддержки распределенных систем.

Выбор между централизованной и распределенной архитектурой зависит от требований конкретного приложения, включая количество пользователей, сложность решаемых задач, требования к производительности, а также законодательные и нормативные ограничения. В некоторых случаях может быть целесообразно использовать гибридный подход, сочетающий преимущества и минимизирующий недостатки обоих типов систем [4]. Примером такой гибридной архитектуры являются централизованные пиринговые сети, в которых все участники сети имеют доступ к одним и тем же функциям, предоставляемым системой, и несут одинаковую ответственность, а узлы применяются для связей между точками доступа и координированной работы пользователей.

Использование пиринговых систем приводит к ускорению и упрощению процессов, связанных с использованием платежных систем, мониторингом целостности и конфиденциальности, поскольку данный подход сочетает в себе высокую вычислительную мощность, надежность, низкий уровень расходов и использует дополнительные вычислительные мощности для внутрисистемной координации.

Технология распределенных реестров

Технология распределенных реестров – это способ организации обмена и хранения данных, в рамках которого узлы содержат локальную копию текущего состояния реестра [5].

Основным процессом при создании транзакций в распределенном реестре является согласование – консенсус, безопасность которого базируется на вычислении хеш-функции данных и криптографических алгоритмах. Механизмы консенсуса включают обязательную проверку целостности и валидности данных и обеспечивают отказоустойчивость системы [6].

Основной задачей консенсуса является достижение общего согласия по поводу текущего состояния реестра. На практике существуют различные алгоритмы консенсуса [7, с. 52–57], наиболее популярные из них приведены в таблице.

Цель исследования – рассмотреть и проанализировать применение технологии блокчейна для предотвращения DDoS-атак. Провести анализ готовых решений применения технологии блокчейна, предоставляющие функциональность для хранения данных в распределенных системах.

Алгоритмы консенсуса

Наименование консенсуса	Механизм консенсуса	Преимущества	Недостатки
Доказательство выполненной работы (PoW)	Узлы получают сложную вычислительную задачу, лидером признается первый нашедший правильное решение узел	Высокий уровень безопасности	Высокий уровень энергозатрат
Доказательство доли владения (PoS)	Лидерство определяется суммой владения	Энергоэффективность, экономическая безопасность	Сложность реализации справедливого распределения
Доказательство доли владения (PoA)	Лидер выбирается из ограниченного круга авторитетных узлов, произвольный узел не может стать лидером	Высокая пропускная способность, надежность	Централизация, ограниченный доступ
Практический Византийский отказоустойчивый консенсус (RBFT)	Консенсус без выбора лидера, использующий репликированные службы	Отказоустойчивость, использование консенсуса на основе голосования	Отсутствие масштабируемости, требуется наличие не более трети вредоносных делегатов для поддержки отказоустойчивости
Делегированный Византийский отказоустойчивый консенсус (dBFT)	Аналогичен RBFT с тем отличием, что не все узлы равноправны, в процессе консенсуса участвует только подмножество узлов – делегатов	Отказоустойчивость, использование консенсуса на основе голосования, улучшенная масштабируемость в сравнении с RBFT	Требуется наличие не более трети вредоносных делегатов для поддержки отказоустойчивости

Материалы и методы исследования

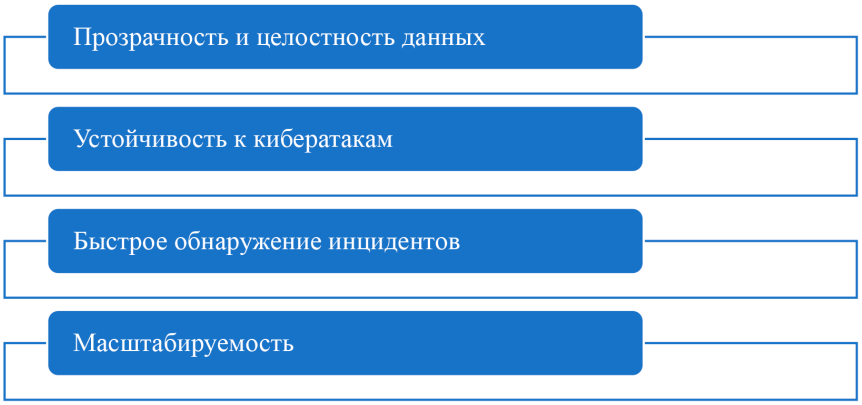
Блокчейн представляет собой мощный инструмент для предотвращения DDoS-атак. Это связано со структурой блокчейна, представляющей собой распределенную базу данных с возможностью криптографической защиты данных. Благодаря этому данная технология обеспечивает эффективное и надежное решение для защиты от DDoS-атак.

DDoS-атаки можно классифицировать по следующим параметрам, таким как объем вредоносного трафика (сотни Гбит/с), по атакуемому уровню абстракции, к ним относятся софт, железо, сеть, а также по таким параметрам, как атакуемый ресурс [8].

Наиболее распространенные типы DDoS-атак: перебор, спуфинг, ICMP-флуд и UDP флуд. Перебор – атака, при которой злоумышленник посылает большое количество запросов на целевой сервер или сеть, чтобы перегрузить их и вызвать отказ в обслуживании. Спуфинг – атака, направленная на подмену IP-адресов или других идентификаторов, чтобы скрыть источник атаки. Флуд-атаки направлены на переполнение канала связи жертвы большим количеством трафика, что может привести к его блокировке. Все эти атаки могут быть очень эффективными, если они правильно спланированы и реализованы.

Информационная безопасность систем основывается на характерных особенностях технологий распределенных реестров. К одной из особенностей относится децентрализованность, что означает, что данные не хранятся в одном месте, и снижает вероятность их потери или повреждения. Децентрализация позволяет бороться с DDoS-атаками за счет распределения ресурсов на различных узлах и для успешного проведения атаки необходимо вывести из строя абсолютно все составляющие. Применение хэш-функции к данным гарантирует чувствительность к фальсификации, кроме того, особенностью системы является возможность проследить историю изменения данных на узлах. Совокупность описанных особенностей позволяет с высоким уровнем точности отследить попытки совершения атак на систему [9, 10].

Механизм защиты от DDoS-атак, основанный на технологии распределенных сетей и блокчейна, представляет собой инновационный подход к обеспечению безопасности и стабильности онлайн-сервисов и веб-приложений. Одним из ключевых преимуществ использования блокчейна для защиты от DDoS является его способность сохранять данные в виде распределенной сети, что делает их более защищенными от кибератак и взломов. Кроме того, блокчейн обеспечивает прозрачность и неизменность данных. В основе механизма защиты лежит использование распределенных сетей для обработки запросов от пользователей. Это позволяет снизить нагрузку на сервер и предотвратить перегрузку системы.



Преимущества модуля хранения SIEM на основе DLT

Кроме того, использование блокчейна обеспечивает надежное хранение и защиту данных, предотвращая их потерю или изменение. Суть данного механизма заключается в том, что при попытке DDoS-атаки распределенная сеть обрабатывает запросы от пользователей и отправляет их на сервер через блокчейн.

В качестве практического решения проблемы обмена и хранения информации на основе технологии распределенного реестра можно предложить совокупность следующих криптографических решений: использование в качестве протокола установки защищенного канала протокола TLS (Transport Layer Security) версии 1.3 с поддержкой российских криптонаборов. Защита согласно протоколу TLS осуществляется в три этапа, каждый из которых сопровождается применением уникальных криптографических алгоритмов, определенных в стандартизирующих документах и включающих алгоритм выработки симметричного ключа, алгоритм шифрования и алгоритм выработки хэш-функции. Первый этап – проверка установки соединения (Handshake), второй этап – процедура возобновления сессии (False Start) и третий этап – проверки каждого компонента аппаратного и программного обеспечения от конечного объекта до корневого сертификата (Chain of trust).

Одним из удачных решений по управлению информационной безопасности являются системы управления событиями и инцидентами информационной безопасности (SIEM), которые обеспечивают высокий уровень безопасности информационных систем от различных угроз, таких как хакерские атаки, несанкционированный доступ, утечка данных и пр. [11]. SIEM-системы позволяют не только идентифицировать уязвимости в системах, но и контролировать соблюдение корпоративных политик безопасности. SIEM собирают и аккумулируют данные, сгенерированные различными источниками, такими как системы управления базами данных, системы мониторинга и контроля доступа.

Модуль хранения системы управления событиями и инцидентами информационной безопасности (SIEM) на базе технологии распределенного реестра (DLT) представляет собой инновационное решение для обеспечения безопасности и мониторинга информационных систем.

Основные преимущества модуля хранения SIEM на основе DLT представлены на рисунке.

Результаты исследования и их обсуждение

На сегодняшний день существует ряд готовых DLT-решений, используемых для хранения данных в распределенных системах.

– Fluree – децентрализованная платформа управления данными. Fluree обладает высоким уровнем защиты модуля хранения системы управления событиями и инцидентами информационной безопасности, гибкостью, масштабируемостью, слабой стороной Fluree является низкая производительность и сложность в эксплуатации [12].

– Enigma – децентрализованная вычислительная платформа с гарантированной конфиденциальностью. К преимуществам Enigma можно отнести высокий уровень конфиденциальности, поскольку данные остаются в зашифрованном виде даже в процессе вычислений, повышенную масштабируемость, отказоустойчивость. Недостатками данной системы являются ограниченная совместимость и излишняя трата ресурсов на обеспечение конфиденциальности, что существенно сказывается на производительности в целом [13].

– Ethereum – открытая блокчейн-платформа с возможностью создания смарт-контрактов, предоставляет гибкую среду разработки DApps и управления данными

в децентрализованных сетях. Данная платформа обладает необходимым уровнем безопасности, однако интеграция Ethereum с SIEM-системами затруднена, также к недостаткам можно отнести проблемы масштабируемости, уязвимость смарт-контрактов, сложность разработки, использование значительных вычислительных ресурсов.

− Corda – открытая блокчейн-платформа, ориентированная на потребности финансового сектора, поддерживает интеграцию с SIEM-системами при определенной модификации со стороны разработчиков. Corda обеспечивает высокий уровень безопасности за счет шифрования и контроля аутентификации, что, однако, не исключает компрометации информации в случае утечки или взлома системы. К основным недостаткам можно отнести ограниченную гибкость и сложность миграции проектов на другие платформы.

− Новый подход к безопасности использует Guardtime MIDA, сопоставляя данные с криптографическим контейнером, который обеспечивает целостность с высокой точностью. Криптографические контейнеры для своей работы используют распределенный реестр, тем самым существенно повышая целостность хранимых данных. Данное решение эффективно в плане взаимодействия с удаленными инфраструктурами, таких как облако и Интернет вещей. К преимуществам системы можно отнести выявление нарушений в режиме реального времени, низкий уровень операционных расходов, к недостаткам – достаточно ограниченный спектр решаемых задач [14, с. 25–29].

Из рассмотренных DLT-решений только Fluree и Corda используют возможность интеграции с SIEM-системами, при этом большинство решений обладает избыточным функционалом, что значительно снижает производительность систем. Еще одним недостатком готовых решений является отсутствие универсальности спектра решаемых задач. Сделанные выводы говорят о необходимости разработки инновационных решений для хранения информации об инцидентах информационной безопасности с возможностью интеграции с SIEM-системами, основывающихся на технологии распределенного реестра, обладающих гибкостью, высокой производительностью и надежностью.

Заключение

Применение технологии распределенного реестра является перспективным направлением, поскольку сочетает целостность и доступность информации, экономичность системы, а также высокий уровень безопасности хранения и передачи данных. Преимущества технологии распределенного реестра способствуют росту эффективности операций на финансовом рынке. В работе проведен анализ существующих DLT-решений, используемых для хранения данных в распределенных системах, определены их основные преимущества и недостатки и выявлена необходимость разработки решения с возможностью интеграции с SIEM-системами, основывающегося на технологии распределенного реестра и обладающего универсальностью, гибкостью, высокой производительностью, наряду с обеспечением высокого уровня безопасности данных.

Список литературы

1. Усков В.С. К вопросу о цифровизации российской экономики // Проблемы развития территории. 2020. № 6 (110). С. 157–175.

2. Andriyanov N., Khasanshin I., Utkin D., Gataullin T., Ignar S., Shumaev V., Soloviev V. Intelligent system for estimation of the spatial position of apples based on YOLOv3 and real sense depth camera D415 // Symmetry. 2022. Т. 14, № 1. С. 148.

3. Gataullin T.M., Gataullin S.T. Endpoint Functions: Mathematical Apparatus and Economic Applications // Mathematical Notes. 2022. Т. 112, № 5–6. С. 656–663.

4. Дюдикова Е.И., Куницына Н.Н. Распределенные реестры в цифровой экономике: база данных, технология или протокол? // Инновации. 2019. № 9 (251). С. 98–106.

5. Горбунова М.В., Ометов А.Я., Комаров М.М., Беззатеев С.В. Обзор проблем внедрения технологии распределенного реестра // Информационно-управляющие системы. 2020. № 2 (105). С. 10–19.

6. Ivanyuk V. Forecasting of digital financial crimes in Russia based on machine learning methods // Journal of Computer Virology and Hacking Techniques. 2023. С. 1–14.

7. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. Litres, 2022. 538 с.

8. Zhang J. et al. A Secure and Lightweight Multi-Party Private Intersection-Sum Scheme over a Symmetric Cryptosystem // Symmetry. 2023. Т. 15, № 2. С. 319.

9. Timofeev I., Pleshakova E., Dogadina E., Osipov A., Kochkarov A., Ignar S., Suvorov S., Gataullin S., Korchagin S. Mathematical Models and Methods for Research and Optimization of Protein Extraction Processes from Chickpea and Curd Whey Solutions by Electroflotation Coagulation Method // Mathematics. 2022. Т. 10, № 8. С. 1284.

10. Yerznkyan B.H., Gataullin T.M., Gataullin S.T. Mathematical Aspects of Synergy // Montenegrin Journal of Economics. 2022. Т. 18, № 3. С. 197–207.

11. Petrosov D.A., Pleshakova E.S., Osipov A.V., Ivanov M.N., Zelenina A.N., Lvovich I.Ya., Preobrazhenskiy Yu.P., Petrosova N.V., Lopatnuk L.A., Kupriyanov D.Y., Roga S.N. Modeling of resource allocation in industrial organizations // Procedia Computer Science. 2022. Т. 213. С. 355–359.

12. Petrosov D.A., Pleshakova E.S., Osipov A.V., Ivanov M.N., Lopatnuk L.A., Radygin V.Y., Roga S.N. Mathematical apparatus of artificial neural networks for genetic algorithm controlling under structural parametric synthesis of large discrete systems // Procedia Computer Science. 2022. Т. 213. С. 346–354.

13. Беларев И.А., Обаева А.С. О распределенном реестре и возможности его применения // Финансы: теория и практика. 2017. Т. 21, № 2. С. 94–99.

14. Walport M. Distributed ledger technology: Beyond block chain. Government Office for Science, 2016. 88 p.