УДК 004

Мочиев И.И.

студент физико-математического факультета ИнгГУ

ФГБОУ ВО «Ингушский государственный университет» г. Магас

Гасаров М.Х.

научный руководитель, кандидат педагогических наук, старший преподаватель кафедры «ИСиТ»

ФГБОУ ВО «Ингушский государственный университет» г. Магас

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ В БЛОКЧЕЙН-СЕТЯХ И МЕТОДЫ ИХ УСТРАНЕНИЯ

Аннотация: В статье рассматриваются основные уязвимости в блокчейн-сетях и методы их устранения. Анализируются ключевые типы атак, включая уязвимости консенсусных алгоритмов, смарт-контрактов, сетевой инфраструктуры и межсетевых мостов. Особое внимание уделяется практическим инцидентам, таким как The DAO hack и Ronin Network hack, продемонстрировавшим критические недостатки в реализации блокчейн-решений. Описаны современные методы обнаружения и предотвращения атак, включая аудит кода, формальную верификацию и многоуровневые механизмы защиты. Подчеркивается необходимость комплексного подхода к обеспечению безопасности в условиях развития децентрализованных технологий.

Ключевые слова: блокчейн, безопасность, уязвимости, смарт-контракты, консенсус, DeFi, аудит, атаки.

Mochiev I.I.

Student of the Physics and Mathematics Department at IngSU

Ingush State University, Magas

Gasarov M.H.

Research supervisor, Candidate of Pedagogical Sciences, Senior Lecturer at the Department «ISaT»

Ingush State University, Magas

RESEARCH ON VULNERABILITIES IN BLOCKCHAIN NETWORKS AND METHODS FOR ADDRESSING THEM

Abstract: This article examines the main vulnerabilities in blockchain networks and methods for mitigating them. Key attack types are analyzed, including vulnerabilities in consensus algorithms, smart contracts, network infrastructure, and inter-network bridges. Particular attention is given to practical incidents, such as The DAO hack and the Ronin Network hack, which demonstrated critical flaws in the implementation of blockchain solutions. Modern methods for detecting and preventing attacks are described, including code auditing, formal verification, and multi-layered defense mechanisms. The need for a comprehensive approach to ensuring security in the context of the development of decentralized technologies is emphasized.

Keywords: Blockchain, security, vulnerabilities, smart contracts, consensus, DeFi, audit, attacks.

В последние годы технологии блокчейн стали неотъемлемой частью цифровой инфраструктуры, способствуя развитию криптовалют, финансовых услуг и распределенных приложений. Их популярность обусловлена такими свойствами, как децентрализация, прозрачность и невозможность изменения данных после их записи. Однако на практике безопасность сетей блокчейн далека от абсолютной. Несмотря на криптографическую надежность базовых алгоритмов, реальные системы подвержены множеству уязвимостей на различных архитектурных уровнях.

Одна из главных причин уязвимости заключается в сложности взаимодействия компонентов блокчейн-системы. В отличие от традиционных централизованных приложений, блокчейн-системы полагаются на распределенные узлы, механизмы консенсуса, смарт-контракты и внешние сервисы. Сбой в любом из этих элементов может привести к серьезным последствиям, включая потерю средств и паралич всей сети.

Один из самых известных инцидентов — взлом DAO в экосистеме Ethereum. Точность здесь имеет решающее значение. Для того чтобы злоумышленник мог неоднократно выводить средства через это соединение, требовалось сложное подключение. Это не был ни персональный криптокошелек, ни традиционный банковский счет. Раскол сети Ethereum продемонстрировал масштаб последствий.

Уязвимости блокчейн-сетей можно разделить на несколько широких категорий. Первая касается механизмов консенсуса. Например, атака 51% позволяет злоумышленнику, обладающему большей частью вычислительной мощности или долей, контролировать процесс подтверждения транзакций, что, таким образом, позволяет осуществлять двойную трату средств и блокировку работы других пользователей. Это особенно актуально для небольших блокчейн-сетей

с низким уровнем децентрализации и ограниченной вычислительной мощностью.

Фильтрация трафика в сетевых системах позволяет частично контролировать входящие запросы и снижает нагрузку на серверную инфраструктуру. Однако даже при использовании базовых механизмов безопасности, таких как ограничение скорости запросов или фильтрация на основе правил, система остается уязвимой для более сложных атак. При перегрузке ресурсов и обходе стандартных мер безопасности могут потребоваться дополнительные меры защиты. Одним из таких подходов является использование ловушек (honeypots), которые не только обнаруживают атаки, но и анализируют поведение злоумышленников в контролируемой среде.

Вторая важная категория касается уязвимостей смарт-контрактов. Эти контракты представляют собой программы, которые автоматически выполняются в блокчейне. Ошибки реализации являются одной из наиболее частых причин атак. Помимо уязвимостей, связанных с реентерабельностью (reentrancy), к распространенным проблемам относятся переполнение целочисленных значений, плохое управление контролем доступа и логические ошибки. Поскольку контракты часто невозможно изменить после развертывания, такие ошибки могут иметь необратимые последствия.

Третья группа включает в себя сетевые уязвимости. В распределенных системах надежная передача данных между узлами имеет решающее значение. Атаки Сибиллы позволяют злоумышленнику создавать множество псевдонимных узлов и влиять на работу сети. Также возможны атаки на уровне маршрутизации, такие как перехват трафика, которые могут привести к задержкам или изменениям в передаваемых данных.

С развитием кроссчейн-технологий появились новые угрозы, связанные с сетевыми шлюзами. Эти механизмы позволяют передавать активы между различными сетями, но часто представляют собой уязвимость в системе безопасности. Взлом сети Ronin, позволивший злоумышленникам получить контроль над валидаторами и совершить крупномасштабную кражу активов, является ярким примером. Этот инцидент продемонстрировал, что даже при высокой степени защиты некоторых блокчейнов уязвимости в базовой инфраструктуре могут иметь критические последствия.

Для выявления уязвимостей можно использовать различные методы анализа. Наиболее распространенным является аудит смарт-контрактов, который может

проводиться вручную специалистами или с помощью автоматизированных инструментов. Формальная верификация математически доказывает корректность выполнения программного кода, что особенно важно для критически важных финансовых приложений. Также широко используются программы вознаграждения за обнаружение ошибок (bug bounty programs), которые стимулируют независимых исследователей к тестированию систем.

Методы устранения уязвимостей и повышения уровня безопасности основаны на принципе многоуровневой защиты. На уровне смарт-контрактов используются проверенные подходы к разработке для предотвращения распространенных атак. Использование стандартных библиотек и ограниченных прав доступа значительно снижает риск эксплуатации.

На уровне консенсуса крайне важно обеспечить достаточную децентрализацию сети. Чем больше независимых участников, подтверждающих транзакции, тем сложнее злоумышленнику получить контроль над сетью. Экономические механизмы стимулирования, используемые в алгоритмах Proof-of-Stake, также способствуют повышению устойчивости системы к атакам.

Инфраструктурный уровень включает защиту закрытых ключей, внедрение мультиподписей и использование изолированных сред хранения. Потеря или компрометация ключей остаются одной из наиболее частых причин кражи активов; поэтому обеспечение их безопасности имеет критически важное значение.

Для обеспечения безопасности сетевых соединений разрабатываются более надежные механизмы проверки транзакций, включая использование криптографических доказательств и независимых валидаторов. Это снижает уровень доверия, требуемый к каждому компоненту системы, и повышает ее общую отказоустойчивость.

Таким образом, анализ уязвимостей блокчейн-сетей показывает, что основная проблема заключается не в самой технологии, а в ее реализации и использовании. Несмотря на высокий теоретический уровень безопасности, такие системы требуют постоянного мониторинга, аудита и совершенствования.

В заключение важно подчеркнуть, что обеспечение безопасности блокчейн-сетей возможно только при комплексном подходе, интегрирующем технические, организационные и экономические меры. Постоянное развитие

технологий и появление новых типов атак требуют регулярного обновления методов обеспечения безопасности. Только сочетание различных подходов может гарантировать надежную и устойчивую работу современных децентрализованных систем.

Список литературы

1. **Kumar K., Kumar D., Baghel S., Arora K.** Blockchain Security: Threats, Vulnerabilities and Countermeasures - A Review
(Дата обращения: 06.04.2025).В работе рассматриваются основные угрозы блокчейна, включая атаки 51%, уязвимости смарт-контрактов и методы их устранения.

2. **Zhang et al.** Blockchain security threats: A comprehensive classification and impact assessment
(Дата обращения: 15.03.2025).Представлена классификация угроз по уровням архитектуры блокчейна и анализ их влияния на систему.

3. **World Journal of Advanced Research and Reviews**Blockchain Security: Vulnerabilities and Protective Measures
(Дата обращения: 22.07.2025.)Описываются ключевые уязвимости, включая Sybil-атаки и проблемы смарт-контрактов, а также методы защиты.

4. **Mishra D. U. et al. Blockchain Security in Focus: Smart Contracts and Cross-Chain** https://www.researchgate.net/publication/390360112
(Дата обращения: 01.03.2025**)**
Анализ уязвимостей мостов, DeFi и смарт-контрактов.

5. **Dwivedi K. et al. A Novel Classification of Attacks on Blockchain Layers**
https://arxiv.org/abs/2404.18090
(Дата обращения: 24.04.2024)
Подробная классификация атак по уровням блокчейн-архитектуры.

6. **Azimi S. et al. Smart Contract Security Design Patterns: A Systematic Review**
https://link.springer.com/article/10.1007/s10664-025-10646-w
(Дата обращения: 10.10.2025)
Методы безопасной разработки смарт-контрактов и шаблоны защиты.

7. **Zafar M. Z. et al. Blockchain Security: Vulnerabilities and Protective Measures** https://www.researchgate.net/publication/390089329
(Дата обращения: 31.5.2025)

Обзор атак и предложений по построению комплексной защиты блокчейна.