ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

УДК 004.056

АНАЛИЗ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ BLOCKCHAIN В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Сабиев Олжас Нурланулы
Евразийский национальный университет им. Л.Н.Гумилева,
магистрант 2 курса ОП 7М06306 – «Системы информационной безопасности»
Есжанов Ермек Ерикович
Евразийский национальный университет им. Л.Н.Гумилева,
магистрант 2 курса ОП 7М06113 – «Менеджмент инноваций и цифровой трансформации экономики (MBA)»
Научный руководитель – Сатыбалдина Дина Жагыпаровна

Аннотация: Статья "Анализ применения технологии Blockchain в контексте обеспечения безопасности информационных систем" рассматривает роль и влияние технологии Blockchain на обеспечение безопасности информационных систем. Начиная с объяснения основных принципов работы Blockchain и его ключевых свойств, исследуются применение этой технологии в различных сферах, выявляя ее потенциал в обеспечении целостности и доступности данных. Особое внимание уделяется анализу безопасности блокчейн-решений, включая рассмотрение уязвимостей и векторов атак, а также преимуществ и ограничений использования Blockchain в контексте информационной безопасности. В результате статья предлагает взвешенный взгляд на роль Blockchain в обеспечении безопасности информационных систем и указывает на потенциальные направления его развития и улучшения.

Ключевые слова: Blockchain, безопасность информационных систем, распределенный реестр, криптография, уязвимости.

Технология Blockchain представляет собой одну из разновидностей распределенных систем хранения данных, известных как распределенные реестры. Одной из основных характеристик этого класса технологий является отсутствие централизованного управления. Каждый узел распределенной системы делает записи в своем реестре независимо от других узлов и синхронизируется с ними в рамках одноранговой сети. Особенностью Blockchain как формы распределенного реестра является формирование записей в цепочку блоков с использованием криптографических алгоритмов, отсюда и его название (Blockchain, цепочка блоков).

Итак, Blockchain – это децентрализованная база данных, в которой все записи собираются в блоки и связываются между собой с помощью криптографии. Помимо данных и идентификатора блока, в блок включаются хеш-суммы текущего и предыдущего блоков, вычисляемые криптографическими хеш-функциями. Это обеспечивает неизменность и необратимость всей цепочки блоков и транзакций.

Кроме того, важную роль в Blockchain играет алгоритм консенсуса, который генерирует и синхронизирует цепь блоков у всех участников сети. Эти особенности, включая экономические мотивации для участников сети, привели к разработке специализированных алгоритмов консенсуса.

Сочетание распределенного реестра с блочной структурой данных, основанной на криптографической связанности, позволяет Blockchain реализовывать целостность и доступность информации. Однако его традиционная модель не гарантирует конфиденциальность данных. Поэтому появилась модель приватного Blockchain, обеспечивающая конфиденциальность записей. Такие сети получают все большее распространение для корпоративных и государственных задач.

С точки зрения безопасности Blockchain стоит оценивать не как самостоятельную технологию, а как инфраструктурный слой для конкретного сценария – базу данных для корпоративной информационной системы, среду исполнения децентрализованного

приложения или смарт-контракта и т.д. Анализ многочисленных инцидентов ИБ, связанных с Blockchain-решениями, показывает, что часто самой уязвимой частью является не Blockchain-сеть, а смежные компоненты и информационные системы. В статье рассматриваются векторы атак на Blockchain -решения и особенности реализации принципов безопасности.

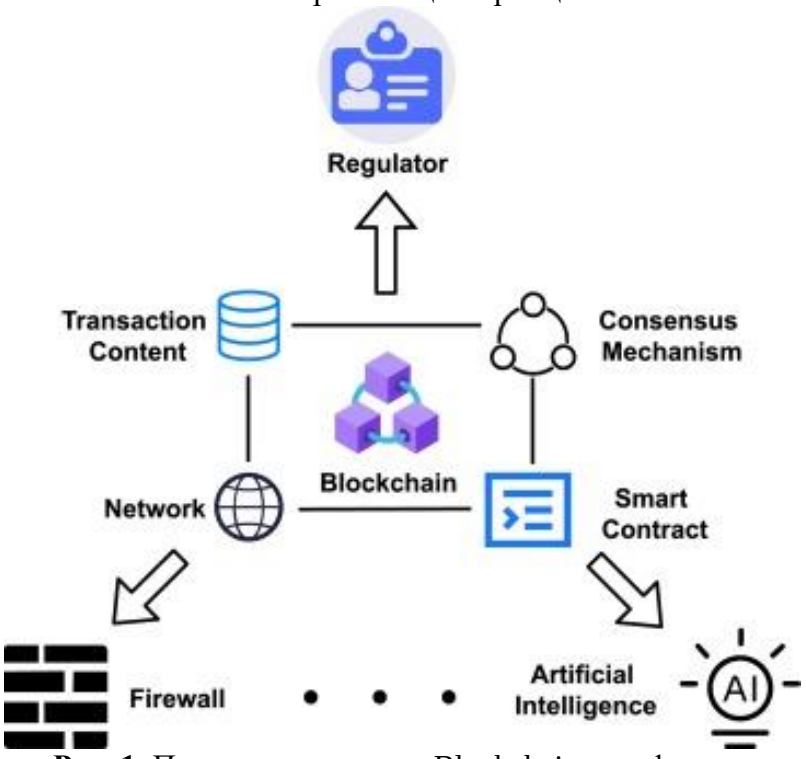

Рис. 1. Примитивная схема Blockchain платформы.

Архитектура, криптографические функции и алгоритмы консенсуса децентрализованной Blockchain-сети также могут быть потенциально проэксплуатированы, тем самым подвергая угрозе базовый принцип Blockchain – неизменность данных. Ниже перечислены основные виды атак на инфраструктуру публичных Blockchain-сетей. Многие из них существуют пока в теории и обсуждаются как концептуальные.

Атака 51%. Это концепция, при которой контроль над более 50% ресурсами Blockchain-сети, позволяет создать свой форк, который заменит текущий реестр Blockchain (блоки других участников тогда перестанут подтверждаться) и станет актуальным. При этом можно будет откатить предыдущие транзакции или смарт-контракты или провести «двойную трату» – провести в Blockchain несколько транзакций с использованием одних и тех же цифровых активов. Отдельным подвидом является атака дальнего действия смысл которой в том, чтобы начать собирать ложный форк задолго до актуального блока. В некоторых видах консенсуса это будет стоить меньше ресурсов. В зависимости от алгоритма консенсуса, реализация атаки будет отличаться. На текущий момент выделяется две основные группы алгоритмов: на основе доказательства работы (Proof-of-Work) и на основе подтверждения доли (Proof-of-Stake). В случае первого алгоритма (напр., Bitcoin и Ethereum) атакующему требуется завладеть 51% вычислительных ресурсов сети. В случае с Proof-of-Stake (напр., Tezos и Waves), для реализации атаки 51% атакующему требуется завладеть 51% основного актива сети.

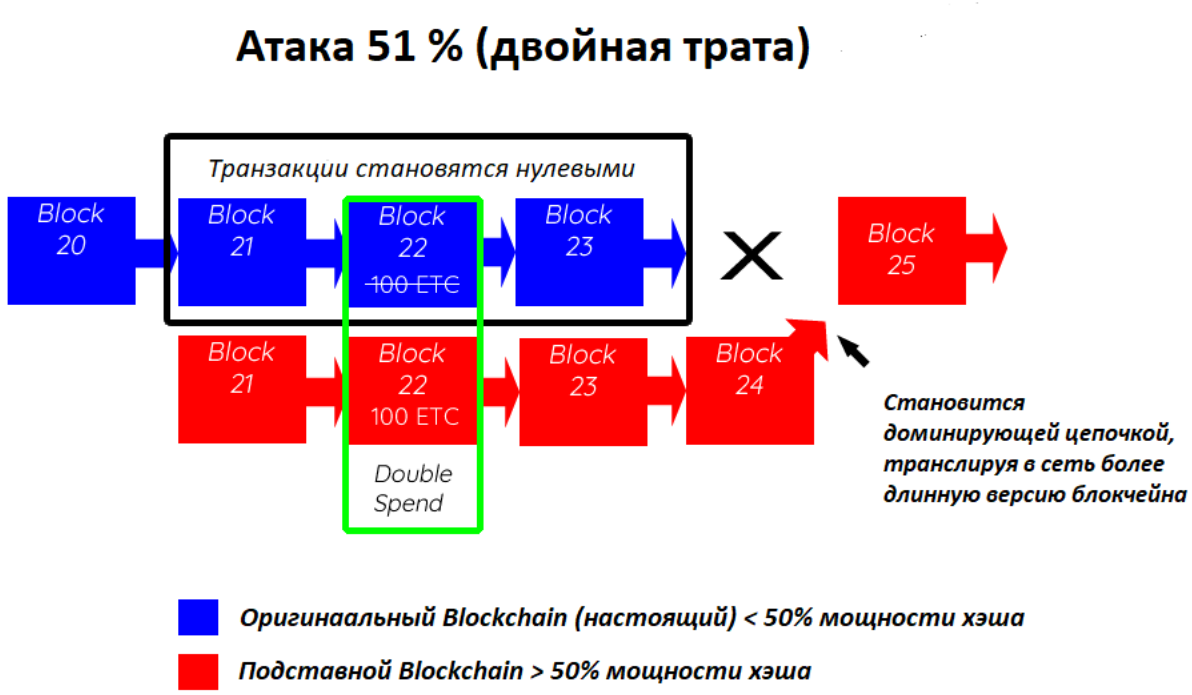

Рис. 2. Иллюстрация атаки 51% на Blockchain систему.

Атака Сивиллы. Вид атаки в одноранговых сетях, при которой злоумышленник наполняет сеть подконтрольными ему узлами, к которым подключаются узлы других участников. Атакующий окружает узел жертвы так, чтобы иметь контроль над всеми исходящими и входящими транзакциями. В крупных децентрализованных сетях такую атаку реализовать крайне сложно, так как узел участника для подтверждения транзакции выбирает другой узел сети практически случайно. Хотя процесс соединения практически рандомизирован, можно взломать журнал доверенных адресов жертвы – он будет содержать адреса узлов злоумышленника. Атака Сивиллы позволяет отключать других пользователей от сети, наблюдать за их транзакциями или реализовывать «двойную трату».

Взлом подписей и хеш-функций. В Blockchain-сетях используются различные криптографические механизмы, многие из них (например, алгоритмы SHA-256 и ECDSA) считаются крайне стойкими ко взлому текущим поколением вычислительных мощностей. Но появление квантовых компьютеров позволит преодолевать нынешнюю стойкость, и в результате взламывать механизмы, лежащие в основе Blockchain.

Конечно, не все возможные атаки на инфраструктуру Blockchain-сетей описаны здесь. Мы также можем упомянуть атаку P+Epsilon, DDoS и замедление времени, эксплуатацию уязвимостей в программном обеспечении узлов сети и другие угрозы. Однако большинство из них пока не было осуществлено.

Заключение: Хотя Blockchain-сети представляют собой уникальный метод защиты данных и их обмена, они также могут стать целью как специализированных, так и стандартных атак. При разработке безопасных Blockchain-решений необходимо ответить на ряд вопросов в области информационной безопасности:

- Насколько криптостойкими являются используемые криптографические алгоритмы?
- Как обеспечивается безопасность ключей, и каким образом они будут восстановлены или заменены в случае компрометации?
- Исследованы ли возможные атаки на алгоритмы консенсуса?
- Существуют ли рекомендации по безопасной настройке платформы Blockchain?
- Каков процесс разработки и тестирования Blockchain-решения?

- Планируется ли проверка безопасности узлов сети?
- Будет ли внедрен мониторинг безопасности сети и решений?
- Каков план реагирования на инциденты, и кто за него отвечает?

Кроме того, Blockchain, так же как и другие формы распределенных реестров, может быть использован в качестве средства обеспечения информационной безопасности. В настоящее время наблюдается увеличение проектов в области кибербезопасности, основанных на этой технологии, таких как проверка целостности прошивок IoT-устройств, защита от DDoS-атак, децентрализованная идентификация и аутентификация, новое поколение инфраструктуры открытых ключей и др.

Список использованных источников

1. Frankfurt School Blockchain Center: Security in Blockchain Applications, 2018. https://fsblockchain.medium.com/security-in-blockchain-applications-43e73193512d

2. Md Rafiqul Islam, Md Mahmud, Ataur Rahman: A Review on Blockchain Security Issues and Challenges, 2021. https://www.researchgate.net/publication/354039550_A_Review_on_Blockchain_Security_Issues_and_Challenges

3. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen: A Survey on the Security of Blockchain Systems, 2020. https://csxqli.github.io/files/FGCS'20.pdf

4. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom workshop on security privacy and trust in the internet of thing, 2017

5. Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: International Journal of Web and Grid Services, 2016

6. Zamani E., He Y., Phillips M.: On the security risks of the blockchain. 2018. https://eprints.whiterose.ac.uk/143412/1/JCIS%20new%20manuscript%20FINAL%20NEW%20without%20codes.pdf

УДК 004.056.5

ӘЛЕМДІК КОМПАНИЯЛАРДЫҢ ҚАУІПСІЗДІК САЯСАТЫН ӘЗІРЛЕУ ТӘСІЛДЕРІ

Сарсембаев Нурбол Жалгасович
nur_bol_@mail.ru
магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.
Сагиндыков Каким Молдабекович
жетекші,т.ғ.к, доцент, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

Аңдатпа. IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS және т.б. жетекші технологиялық компаниялардың тәжірибесіне негізделген ақпараттық қауіпсіздік саясатын құрудағы ең жақсы тәжірибелерге шолу жасайды. Өнеркәсіпте кеңінен танылған саясаттарды, процедураларды, стандарттарды және қауіпсіздік нұсқаулықтарын әзірлеу әдістері қарастырылуда. Ірі көшбасшы компаниялардың қауіпсіздік стандарттарын қалыптастыруға қатысуының маңыздылығы және олардың ақпаратты қорғаудың инновациялық тәсілдерін әзірлеудегі рөлі атап өтіледі. Бұл шолу ақпараттық қауіпсіздік тәжірибесін жақсартуға ұмтылатын ұйымдар үшін пайдалы нұсқаулық бола алады.

Кілт сөздер: қауіпсіздік саясаттары, процедуралар, қауіпсіздік стандарттары, технологиялық көшбасшы.

IBM компаниясының қауіпсіздік саясатын әзірлеуге көзқарасы: практикалық ұсыныстар

Ақпараттық қауіпсіздік саласындағы әлемдегі жетекші сарапшылардың бірі болып саналатын IBM көп жылдық тәжірибе мен озық стандарттарға негізделген қауіпсіздік