Роль технологии блокчейн в реализации кибербезопасности

Х.Х. Пахаев[1], Т.Г. Айгумов[2], Ф.М. Абдулмукминова[2]

[1] ФГБОУ ВО «Чеченский государственный университет им. А.А.Кадырова»

[2] ФГБОУ ВО «Дагестанский государственный технический университет»

Аннотация: Технология блокчейн принята в различных областях, в первую очередь в финансах, за счет использования криптовалют. Однако эта технология также полезна в кибербезопасности. В этой статье рассмотрены различные методики блокчейн для сектора кибербезопасности, предложенные различными исследователями. Данное исследование показало, что большинство исследователей сосредоточены на использовании блокчейна для защиты устройств, сетей и данных Интернета вещей. В данной работе рассматривались стратегии, используемые более ранними исследователями для защиты трех проблемных ИТ-областей с использованием блокчейна. Основной вывод исследования заключался в том, чтобы обеспечить интеграцию и единообразие решений, чтобы будущие исследователи сосредоточились на едином блокчейне для создания приложений кибербезопасности.

Ключевые слова: Блокчейн, Интернет вещей, IoT, кибербезопасность, компьютерная безопасность.

Публикация официального доклада Сатоши Накамото «Биткоин: одноранговая электронная кассовая система» в 2008 году стала первым случаем, когда общественность услышала о технологии блокчейн. В документе описан полностью одноранговый метод обработки интернет-платежей, исключающий традиционные финансовые учреждения. Автор поясняет, что эта система будет опираться на блокчейн, новаторскую технологию, которая появилась за последние десять лет и может оказать влияние на другие секторы, помимо банковского дела, такие, как производство, образование и кибербезопасность [1]. В качестве примера для объяснения того, что такое блокчейн, можно использовать реестр.

Блокчейн по своей сути представляет собой набор записей транзакций, каждая из которых включает пару сторон. Однако ключевым атрибутом в этом случае является то, что данные распределяются, а не копируются по

сети компьютеров. Нет централизованного сервера или органа, который выбирает правильную версию событий для остальной части сети.

Клиент-серверный подход используется в традиционной архитектуре всемирной веб-сети с центральным сервером, содержащим всю необходимую информацию. Это сделано для того, чтобы упростить его обновление и передачу изменений на все подключенные машины. Блокчейн, с другой стороны, децентрализован, и каждый компьютер в сети отвечает за правильность и порядок сбора записей. Чтобы изменить данные, вся сеть должна согласиться с тем, что изменение действительно. При этом, это изменение отражено в характеристиках последовательных блоков. Данные, хранящиеся в блокчейне, заслуживают доверия и в значительно меньшей степени подвержены манипуляциям из-за использования консенсусного протокола (общий набор правил для проверки новых дополнений) и финансового поощрения (вознаграждение для пользователей, которые точно проверяют дополнения) [2]. В блокчейне есть множество важных компонентов, которые следует учитывать, когда мы говорим о блокчейн-транзакциях. Они определены ниже, чтобы обеспечить контекст для потенциальных приложений в области кибербезопасности:

- Узел: один компьютер в одноранговой сети. Каждый узел имеет полную копию реестра блокчейна.
- Транзакция: мельчайший компонент любой цепочки блоков. Он ведет запись информации.
- Блок: структура данных, содержащая несколько транзакций. Блоки распределяются по всем узлам сети.
- Цепочка: определенная последовательность блоков.
- Майнеры: подгруппа узлов, которые проверяют блоки перед добавлением их в более крупную структуру блокчейна (проверка может быть

вознаграждена в финансовом отношении). Когда узел майнера установлен, он будет транслировать измененный блокчейн в остальную часть сети.

- Консенсус (протокол консенсуса): набор правил, которым необходимо следовать для выполнения операций с блокчейном.

Блокчейн – это прорывная технология, которая может положительно повлиять на будущее компьютерных технологий и эволюционировать различные отрасли, благодаря прозрачным и инновационным решениям. Блокчейн представляет из себя открытую, неизменяемую и распределенную систему цепочек, поэтому практически применим во многих сферах. Рост криптовалют увеличил популярность этой технологии, хотя она используется во многих областях, помимо финансов. Блокчейн определяется, как серия криптографически связанных блоков. Блок – это структура данных, состоящая из трех частей: данные хэша предыдущего блока, хэша текущих данных и предыдущего хэша. В результате между блоками существует порядок зависимости, который можно использовать для проверки целостности всей цепочки блоков. Если данные в любом из блоков изменятся, изменится и хэш. Это вызовет цепную реакцию, в которой хэши следующих блоков станут недействительными. Вот почему транзакции в блокчейне неизменяемы. Эта инфраструктура может быть чрезвычайно полезной для предоставления решений кибербезопасности в проблемных областях, таких, как устройства Интернета вещей, сети, а также хранение и передача данных [3].

Методология исследования технологии Блокчейн

Блокчейн – это распределенная модель ведения записей. Узлы в сети блокчейн могут хранить все данные сети. Многие узлы делают это, потому что необходимо либо для консенсуса, либо для справки. Это устраняет необходимость в централизованном хранении данных. Любой злоумышленник, пытающийся скомпрометировать блокчейн, должен

скомпрометировать большую часть узлов, в которых хранятся децентрализованные данные. Это связано с тем, что сеть проверяет блоки данных, хранящиеся в децентрализованных местах, чтобы идентифицировать те, которые отличаются от других. Чаще всего большинство блоков имеют правильные или неизменные данные. Расширенные функции блокчейна делают его пригодным для современных стандартов безопасности.

В этом исследовании используется качественный вторичный анализ данных для оценки применения технологии блокчейн в современной индустрии кибербезопасности. Он основан на многочисленных исследовательских работах о роли блокчейна в кибербезопасности. В данной работе основное внимание уделено двум аспектам исследуемого материала. Для начала будут рассмотрены самые последние применения новой технологии блокчейн в кибербезопасности. Во-вторых, анализ оценит подходы к внедрению решений кибербезопасности блокчейн. Ключевые выводы и рекомендации из рассмотренных исследований будут использованы для обсуждения того, как блокчейн может обеспечить безопасность в современных средах ИТ-пользователей [4].

Результаты исследования

Многочисленные исследования пришли к выводу, что блокчейн более эффективен в IoT, сети и безопасности хранения данных. Результаты обобщены в таблице ниже, где IoT, сеть, данные, инфраструктура открытых ключей (PKI) и конфиденциальность данных охватывают большинство последних реализаций безопасности блокчейн.

Поскольку в настоящее время существует 9 миллиардов таких устройств, акцент на безопасности блокчейна на устройствах Интернета Вещей понятен. Эти устройства имеют недостаточную конфигурацию безопасности, и многие из них взламываются и включаются в сети ботнетов. Так, например, Mirai Botnet, сеть, состоящая из IoT-устройств, была успешно

развернута против крупных целей, таких как Dyn DNS, одна из крупнейших фирм по разрешению доменных имен в Интернете [5]. Вследствие этого, многочисленные исследователи безопасности изучают способы защиты устройств IoT с помощью блокчейна.

Таблица №1

Рекомендации для эффективной реализации безопасности на устройствах, реализующих технологию блокчейн

Проблемы	Решения/Рекомендации
Конфиденциальность	Компромисс между децентрализацией и авторизацией
	Методы смешивания (частные и общедоступные платформы)
	Метод MimbleWimble
Целостность	Иерархический дизайн блокчейн
	Идентификация и аутентификация сообщений
Доступность	Периодическая проверка контрмер
	Улучшенные методы хранения данных
Аутентификация	Сочетание смарт-контрактов с облегченными методами шифрования
	Методы SSI и DID
	Идентификация и аутентификация сообщений
Уязвимости	Шифрование на основе эллиптических кривых, подписи на основе атрибутов, цифровые сертификаты, временные метки для обеспечения уникальности, размеры криптографических ключей
	Безопасные каналы, разделение транзакций, низкий приоритет для новичков
	Управление доступом с несколькими чейнкодами в иерархической цепочке блоков
Доверие	Глобально согласованная модель оценки репутации
	Цифровизация блокчейна

Второй наиболее распространенной темой исследований кибербезопасности блокчейн является хранение данных. Это связано с увеличением случаев кражи данных, когда хакерам удавалось украсть данные у фирм, принадлежащих миллиардам людей. Например, взлом Yahoo в 2014

году привел к краже данных, принадлежащих трем миллиардам клиентов или в октябре 2021 года взлом Instagram привел к утечке данных 1,5 миллиарда пользователей. Как следствие из этого, исследователи безопасности заинтересованы в разработке решений безопасности блокчейн для мест хранения данных, таких, как облачные платформы [6].

Также можно отметить, что исследователи изучают использование блокчейна в сетевой безопасности. Большая часть этого исследования сосредоточена на аутентификации, поскольку современные методы сетевой безопасности, такие, как шифрование WPA, могут быть скомпрометированы и использованы для получения доступа злоумышленником [7].

Еще одним применением блокчейна в кибербезопасности является разработка решений для предотвращения мошенничества и кражи личных данных. Пользователи постоянно подвергаются опасности из-за несанкционированного доступа к данным и их изменения. Это связано с тем, что многие пользователи имеют централизованное хранилище данных. В результате удаленной атаки на уязвимые компоненты, злоумышленник может взломать сайт хранения данных, а далее, получить или изменить данные. Блокчейн с распределенным хранилищем данных предотвращает такие случаи. Конфиденциальные данные, такие, как результаты выборов, могут, таким образом, храниться на тысячах компьютеров, причем каждый компьютер имеет копию данных. Если хакер не сможет проникнуть на достаточное количество машин с копиями данных, взлом и модификация всего нескольких систем не повлияют на остальные данные в сети [8].

Наконец, существует большой интерес к решениям безопасности блокчейн для обеспечения конфиденциальности данных. В большинстве исследований изучаются способы защиты информации, позволяющей установить личность, с помощью универсальной схемы аутентификации блокчейн. Это избавляет пользователей от необходимости передавать свою

информацию организациям; вместо этого блокчейн будет использоваться для аутентификации людей.

Теперь возникает вопрос о том, как технология блокчейн может быть использована для повышения кибербезопасности. Несмотря на то, что современные решения безопасности обеспечивают превосходный уровень защиты ИТ-ресурсов, они не лишены недостатков. Это связано с тем, что большинство продуктов безопасности предназначены для автономной работы при защите ИТ-ресурса. Как и в случае DDoS-атак (распределенный отказ в обслуживании), хакеры могут нацелиться на один компонент безопасности, отключить его, а затем перейти к атаке на открытый ИТ-ресурс [9]. Исследователи, изучающие, как блокчейн может помочь повысить нынешний уровень безопасности, основывают свои аргументы на способности распределенных инструментов безопасности обеспечивать лучшую защиту, чем один инструмент. Согласно полученным данным в таблице 1, многих исследователей интересует, как блокчейн может повысить безопасность устройств, данных и сетей Интернета вещей. Несанкционированный доступ и управление устройствами – самая серьезная уязвимость безопасности в сетях IoT [10].

Решения по безопасности блокчейна могут помочь более успешно управлять контролем доступа и обменом данными для всех устройств IoT. Чтобы обеспечить точную идентификацию пользователя, аутентификацию и передачу данных, можно настроить решение безопасности блокчейн. Чтобы предотвратить несанкционированный доступ, блокчейн может работать путем ведения распределенных записей об истории доверенных соединений и сеансах. Новые подключения могут быть ограничены авторизацией только в том случае, если достаточное большинство предыдущих подключений проголосовало или подтвердило нового пользователя. В результате устройство IoT, такое, как домашняя IP-камера, будет предоставлять доступ

только к доверенным бытовым устройствам. Если хакер попытается получить доступ к камере, решение блокчейн запретит доступ до тех пор, пока большинство доверенных устройств не проголосует за разрешение доступа хакера. Исследователи обнаружили, что наличие единой точки отказа или компрометации является самой большой слабостью в безопасности данных. Это приводит к краже, изменению или потере данных [11].

Выводы

Технология блокчейн развивается и находит все больше применений в современном мире. Кибербезопасность является одной из жизнеспособных областей, где эта технология была изучена и реализована. Инфраструктура блокчейна позволяет решать существующие проблемы безопасности в таких областях, как устройства Интернета вещей, сети, хранение и передача данных. В данной работе проводится анализ применения технологии блокчейн в исследованиях современных ученых. Было отмечено, что большинство исследователей безопасности блокчейн в значительной степени сосредоточены на развертывании безопасности блокчейн для устройств IoT. Сети и данные также являются важными аспектами безопасности блокчейна. Несмотря на то, что исследовались и другие области применения блокчейн - технологий, безопасность является наиболее важной в современном мире цифровых технологий. Данная работа демонстрирует, что блокчейн способен закрывать серьезные недостатки безопасности, которые выходят за рамки традиционных технологий безопасности.

Литература

1. Базанов С. Биткоин: Одноранговая электронная денежная система // Medium.com, 2019, URL: medium.com/bitcoin-review/биткоин-одноранговая-электронная-денежная-система-c66b254385d2

2. Алтынов Д.С., Пиневич Е.В., Годунов А.Е., Шенявский Н.И. Blockchain в системе обеспечения транспортной безопасности // Инженерный вестник Дона, 2022, №1. URL: ivdon.ru/ru/magazine/archive/n1y2022/7422

3. Сидорова Д.Н., Подготовка данных для кластеризации событий в журналах информационной безопасности // Инженерный вестник Дона, 2022, №6. URL: ivdon.ru/ru/magazine/archive/n6y2022/7736

4. Пескова О.Ю., Половко И.Ю., Захарченко А.Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Инженерный вестник Дона, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5801

5. Ibrahim R.F., Abu Al-Haija Q., Ahmad A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. Sensors 2022. 22(6806). pp. 1-21.

6. Менциев А.У., Пахаев Х.Х., Айгумов Т.Г. Угрозы безопасности узкополосного Интернета Вещей и меры противодействия // Инженерный вестник Дона, 2021, №10. URL: ivdon.ru/ru/magazine/archive/n10y2021/7249

7. Radivilova T., Hassan H.A. Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-Enterprise. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). 2017. pp. 1-4.

8. Леонов Д.В. Моделирование, с внедрением блока адаптивного мониторинга, системы комплексной защиты конфиденциальной информации, от кибернетических атак // Инженерный вестник Дона, 2019, №6. URL: ivdon.ru/ru/magazine/archive/N6y2019/6035

9. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

10. Mentsiev A.U., Dzhangarov A.I. VoIP security threats // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

11. Тихонова К.В., Гаранова М.В., Бурдова Д.В., Тихонов Д.А. Оптимизация системы управления объектами недвижимости на основе внедрения технологии блокчейн в учетно-регистрационную процедуру // Инженерный вестник Дона, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N7y2019/6078

References

1. Bazanov S. Translation "Bitcoin: Peer-to-Peer Electronic Cash System" // Medium.com, 2019, URL: medium.com/bitcoin-review/биткоин-одноранговая-электронная-денежная-система-c66b254385d2

2. Altynov D.S., Pinevich E.V., Godunov A.Y., Shenyavsky N.I. Inzhenernyj vestnik Dona, 2022, №1. URL: ivdon.ru/ru/magazine/archive/n1y2022/7422

3. Sidorova D.N. Inzhenernyj vestnik Dona, 2022, №6. URL: ivdon.ru/ru/magazine/archive/n6y2022/7736

4. Peskova O.Yu., Polovko I.Yu., Zakharchenko A.D. Inzhenernyj vestnik Dona, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5801

5. Ibrahim R.F., Abu Al-Haija Q., Ahmad A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. Sensors 2022. 22(6806). pp. 1-21.

6. Mentsiev A.U., Pakhaev Kh.Kh., Aygumov T.G. Inzhenernyj vestnik Dona, 2021, №10. URL: ivdon.ru/ru/magazine/archive/n10y2021/7249

7. Radivilova T., Hassan H.A. Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-Enterprise. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). 2017. pp. 1-4.

8. Leonov D.V. Inzhenernyj vestnik Dona, 2019, №6. URL: ivdon.ru/ru/magazine/archive/N6y2019/6035

9. Mentsiev A.U., Chebieva Kh.S. Inzhenernyj vestnik Dona, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

10. Mentsiev A.U., Dzhangarov A.I. Inzhenernyj vestnik Dona, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

11. Tikhonova K.V., Garanova M.V., Burdova D.V., Tikhonov D.A. Inzhenernyj vestnik Dona, 2019, №3 URL: ivdon.ru/ru/magazine/archive/N7y2019/6078