УДК 004.89

Сатымов Р. Р., студент,
Ахметгалиева Д. А., студентка,
Научный руководитель
Фот Ю. Д., к. т.н., доцент,
ФГБОУ ВО «Оренбургский государственный аграрный университет»
Оренбург, Россия

Анализ безопасности блокчейна

Аннотация: Технология блокчейн обладает значительным потенциалом, предлагая множество приложений и возможностей для различных инфраструктур. Она обеспечивает безопасность и эффективность управления ресурсами, улучшает доверие между сторонами при финансовых транзакциях, уменьшая риск мошенничества и обеспечивая автоматизированный учет деятельности. Основные характеристики блокчейна включают децентрализацию, которая повышает безопасность и гибкость, доверие, поскольку каждый блок содержит информацию о предыдущем, и прозрачность данных, которые неизменяемы. Существуют три типа блокчейна: публичный, частный и консорциумы, каждый из которых имеет свои особенности и области применения. Технология блокчейн также сталкивается с проблемами, такими как масштабируемость, утечка конфиденциальности, атак, (MITM) и распределенные атаки отказа в обслуживании (DDoS). Для решения этих проблем предлагаются различные методы, включая оптимизацию хранения и использование криптографических протоколов. Блокчейн находит применение в различных сферах, таких как здравоохранение, где он помогает защищать личные данные пациентов, и в финансовом секторе, где обеспечивает безопасные и прозрачные транзакции. Особое внимание уделяется таким аспектам, как смарт-контракты и платформы на основе блокчейна. Несмотря на существующие проблемы безопасности, технология блокчейн продолжает развиваться и находит все большее применение в различных отраслях, предлагая решения для защиты конфиденциальных данных и обеспечения надежных транзакций.

Ключевые слова: блокчейн, децентрализация, транзакции, безопасность, прозрачность, масштабируемость, DDoS-атака, MITM-атака, цифровая валюта, аутентификация, проблемы безопасности, управление ресурсами, автоматизация проверки данных, финансовые транзакции, обмен ключами

Satymov R. R., student,

Akhmetgalieva D. A., student,
Scientific supervisor:
Fot J. D., Candidate of Technical, Associate Professor,
Orenburg State Agrarian University
Orenburg, Russia

Blockchain security analysis

Annotation: Blockchain technology has significant potential, offering many applications and capabilities across various infrastructures. It ensures secure and efficient resource management, improves trust between parties in financial transactions, reduces the risk of fraud and provides automated accounting of activities. The main characteristics of blockchain include decentralization, which increases security and flexibility, trust, since each block contains information about the previous one, and data transparency, which is immutable. There are three types of blockchain: public, private and consortium, each of which has its own characteristics and applications. Blockchain technology also faces challenges such as scalability, privacy leakage, attacks (MITM) and distributed denial of service (DDoS) attacks. Various methods have been proposed to solve these problems, including storage optimization and the use of cryptographic protocols. Blockchain has applications in various fields such as healthcare, where it helps protect patients' personal data, and the financial sector, where it enables secure and transparent transactions. Particular attention is paid to such aspects as smart contracts and blockchain-based platforms. Despite existing security concerns, blockchain technology continues to evolve and is increasingly used in various industries, offering solutions to protect sensitive data and ensure secure transactions.

Keywords: blockchain, decentralization, transactions, security, transparency, scalability, DDoS attack, MITM attack, digital currency, authentication, security issues, resource management, data verification automation, financial transactions, key exchange

Актуальность: Технология блокчейн продолжает оставаться одной из самых востребованных и перспективных инноваций в современном мире. Она оказывает значительное влияние на различные аспекты управления ресурсами, финансовыми транзакциями и безопасности данных. Благодаря своей децентрализованной природе, блокчейн предоставляет уникальные возможности для повышения доверия между участниками транзакций, минимизации рисков мошенничества и автоматизации процессов проверки данных.

Цель: Цель данной статьи заключается в том, чтобы предоставить всесторонний обзор технологии блокчейн, её ключевых свойств, проблем и потенциальных приложений. Статья описывает, как блокчейн работает, его децентрализованную природу, механизмы доверия и прозрачности, а также различия между публичными и частными блокчейнами. Он также рассматривает проблемы, с которыми сталкивается блокчейн, такие как масштабируемость, утечка конфиденциальности и различные виды атак, и предлагает возможные решения этих проблем. В заключении статьи

подчеркивает значимость блокчейна, его безопасность и перспективы использования в различных областях, включая финансовые транзакции, здравоохранение и защиту персональных данных.

Технология блокчейн обладает огромным потенциалом и множеством применений, предоставляя широкие возможности для различных инфраструктур. Она способствует эффективному управлению ресурсами и обеспечивает безопасное и надежное взаимодействие. Использование блокчейна в финансовых транзакциях повышает доверие между сторонами, так как снижает вероятность мошенничества и автоматически ведет учет деятельности. Благодаря своим децентрализованным свойствам блокчейн позволяет автоматизировать проверку данных любого участника системы, обеспечивая надежность и снижая риски при заключении деловых соглашений с незнакомыми сторонами. Сегодня все активно используют передовые технологии для общения через Интернет. Голосовые вызовы, видеозвонки, сообщения и изображения передаются напрямую от отправителя к получателю. Однако для таких транзакций требуется надежная третья сторона, которая будет посредником между отправителем и получателем. В традиционных денежных транзакциях также необходимо доверие к третьей стороне для выполнения операции. Но в случае с блокчейном безопасность транзакций обеспечивается идеально. Каждый блок записывает транзакцию и действует как книга записей. После завершения транзакция добавляется в блокчейн как постоянная база данных. Если блок завершен, к нему добавляется новый блок, содержащий хеш предыдущего блока [1].

Децентрализация полностью отличается от централизации. Она обеспечивает большую безопасность и гибкость по сравнению с централизованными приложениями. Существует необходимость в быстром принятии решений, и поэтому многие организации предпочитают децентрализацию. В централизованной среде все операции выполняются в одном месте, в то время как в децентрализованной среде работа происходит в различных местах. Децентрализация способна обеспечить как эффективность, так и инновации. Эффективность связана с экономией затрат и времени, при этом гарантируется достижение лучших результатов. Инновации приносят новые идеи и должны стать новым преимуществом [2].

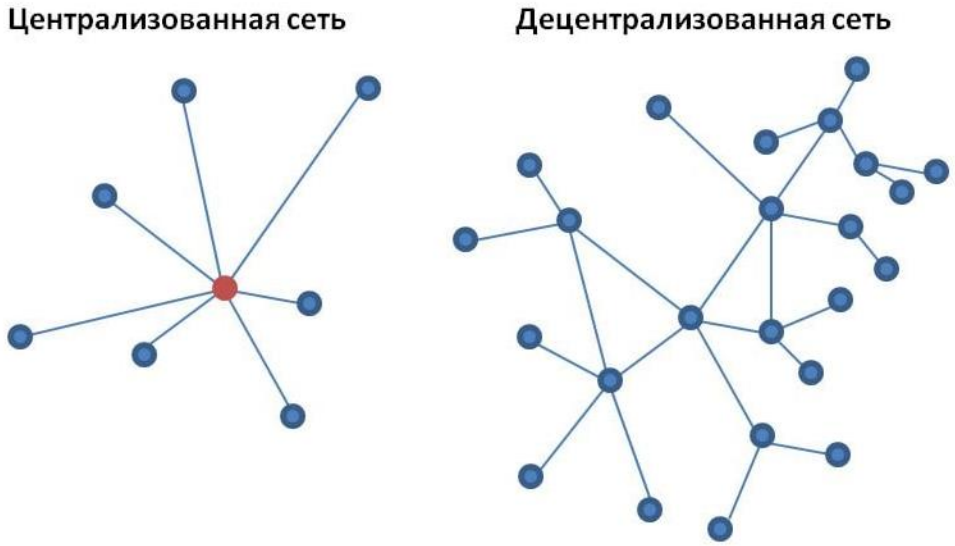

Рисунок 1. Централизованная и децентрализованная сеть

В технологии блокчейн каждый блок содержит информацию о предыдущем блоке, что обеспечивает механизм аутентификации во время транзакции. Здесь нет необходимости в связи с третьими лицами; вместо этого используется общедоступный реестр, в который автоматически записываются все транзакции [3].

Публичный, частный и консорциумный блокчейн. Блокчейн в основном делится на три типа: публичный, частный и консорциумный. В данной статье уделяется сравнению публичного и частного блокчейна на основе некоторых недавних свойств. Публичный и частный блокчейн имеют много сходств, но также существуют различия в их функциональности [4].

Таблица 1. Сравнительная таблица

Свойство	Публичный	Частный блокчейн
Разрешение на чтение	Общественный	Может быть общедоступным или ограниченным
Неизменность	Без вмешательства	Может быть подделано
Эффективность	Низкая	Высокая
Централизованный	Да	Нет

Проблемы, возникающие в области блокчейна. Блокчейн столкнулся с некоторыми проблемами в индустрии, особенно в контексте транзакций биткойнов. Эти проблемы, связанные с функционированием блокчейна Bitcoin, перечислены ниже. Ниже приведены некоторые типичные проблемы

Количество транзакций растет с каждым днем, и многие компании предлагают использовать блокчейн для обработки этих транзакций. Необходимость сохранения и проверки всех транзакций приводит к

небольшой емкости блока. Некоторые транзакции могут быть отложены из-за высокой комиссии, которую требуют майнеры. Это может привести к замедлению скорости обработки транзакций из-за большого размера блока. Поэтому проблема масштабируемости является серьезной. Существует несколько способов решения проблемы масштабируемости в блокчейне: оптимизация хранения данных блокчейна, переработка архитектуры блокчейна [5].

Пользователи считали, что блокчейн обеспечивает высокий уровень конфиденциальности при обработке чувствительных данных. В блокчейне пользователи могли генерировать адреса вместо раскрытия своей личности. Однако исследования Мейкледжона в 2013 году и Косба в 2016 году показали, что блокчейн не гарантирует абсолютной конфиденциальности данных на трансграничном уровне. Недавние исследования также указывают на то, что транзакции биткойнов могут быть прослежены по адресам пользователей, что в итоге раскрывает их личность. Проблема заключается в утечке личной информации пользователей. Для решения этой проблемы можно использовать эллиптическую кривую Диффи-Хеллмана-Меркла (ECDHM), работающую с открытыми и закрытыми ключами. Это позволит обмениваться общими секретами между участниками, обеспечивая безопасную передачу сообщений через Интернет. Кроме того, были разработаны защищенные платформы, такие как смарт-контракты и Ethereum, для обеспечения безопасных транзакций [6].

MITM-атака (Man-in-the-Middle) представляет собой форму взаимодействия с третьей стороной, где злоумышленник встраивается в коммуникационный поток между двумя сторонами. В такой атаке злоумышленник может представляться в середине обмена, имея возможность использовать поддельные открытые ключи для расшифровки конфиденциальной информации. В блокчейне открытые ключи распределяются среди участвующих узлов, и каждый блок связан ссылкой с предыдущим и последующими блоками. Это обеспечивает неизменяемость открытых ключей, что делает их устойчивыми к атакам с использованием поддельных ключей [7].

DDoS-атака (Distributed Denial of Service) представляет собой форму атаки, направленной на перегрузку определенной системы, такой как компьютер, веб-сайт, сервер или другие сетевые ресурсы. В результате входящие сообщения или соединения с целевой системой могут замедляться или даже полностью прекращаться. DDoS-атаки представляют значительный риск для бизнеса, особенно в контексте блокчейна, их практически невозможно предотвратить. Одним из распространенных решений для борьбы с DDoS-атаками является использование устройства анализа потока. Это устройство способно наблюдать и реагировать на действия злоумышленников, предоставляя информацию о дальнейших шагах. Такое устройство помогает снизить нагрузку на сеть, перенаправляя нежелательный трафик [8].

Особенности безопасности блокчейна:

Использование бухгалтерской книги: Каждая транзакция в блокчейне должна быть записана в реестре, который является неизменным. Данные, уже существующие в реестре, невозможно изменить или удалить. Благодаря децентрализованной природе этого реестра никто не может получить доступ к транзакциям или другим конфиденциальным данным. Пользователи могут только просматривать информацию в реестре.

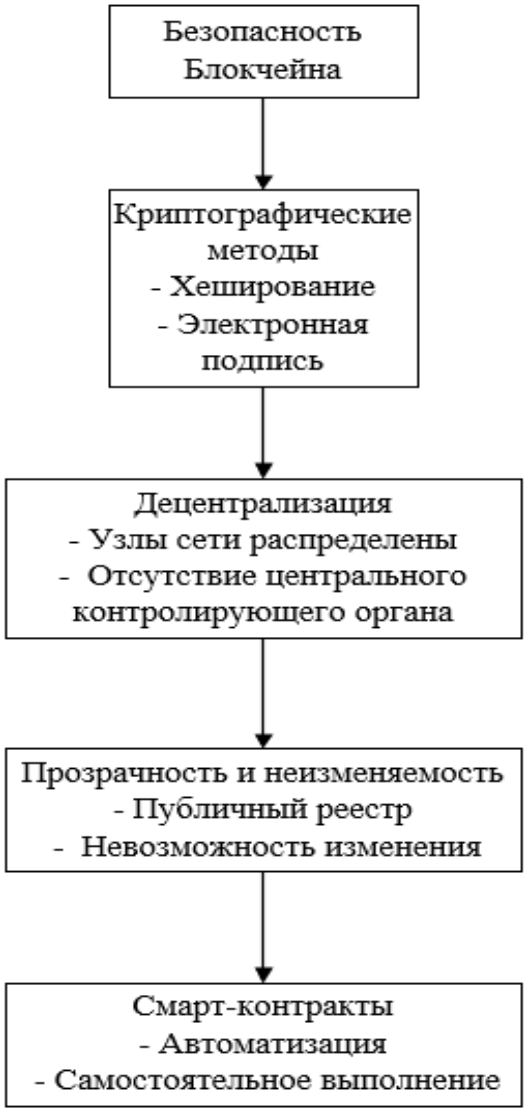

Рисунок 2. Особенности безопасности блокчейна

Криптографические методы:

Хеширование: Использование криптографических хеш-функций для создания уникальных идентификаторов блоков и транзакций.

Электронная подпись: Гарантия подлинности транзакций с помощью криптографических ключей.

Децентрализация:

Узлы сети распределены по всему миру, что снижает риск

централизованных атак и отказов.

Отсутствие центрального контролирующего органа повышает устойчивость к цензуре и манипуляциям.

Прозрачность и неизменяемость:

Все транзакции публичны и доступны для просмотра всеми участниками сети.

После добавления в блокчейн данные не могут быть изменены или удалены, что предотвращает мошенничество.

Смарт-контракты:

Автоматизация выполнения контрактов при наступлении определенных условий.

Обеспечение выполнения условий контракта без необходимости доверия к третьим сторонам [9].

Цепочка блоков: В блокчейне каждый блок содержит хэш-значение, и эти блоки связаны своим предыдущим хешем. Если злоумышленник попытается изменить данные, хэш изменится, что повлияет на всю цепочку. Это обеспечивает защиту конфиденциальности данных и информации [10].

Децентрализованность: Блокчейн представляет собой децентрализованное приложение, которое поддерживает одноранговую сеть. В сети узлами являются компьютеры, каждый из которых должен иметь копию распределенного реестра. Это обеспечивает аутентификацию транзакций: если узел не согласен с транзакцией, она не может быть продолжена и будет отменена. Это защищает от мошенничества [11].

Применение технологии блокчейн в индустрии здравоохранения: В современном мире пациенты предпочитают сохранять конфиденциальность своих медицинских данных. Благодаря технологии блокчейн они могут защитить свою информацию от посторонних. Эту технологию можно использовать как веб-сайт или мобильное приложение. У каждого пользователя в блокчейне есть два ключа: открытый и закрытый. Только тот, кто обладает правильным закрытым ключом, может осуществлять транзакции. Например, если Алиса хочет отправить защищенные данные Бобу, она подписывает цифровую подпись с помощью своего закрытого ключа. Затем данные хешируются с использованием открытого ключа и генерируется адрес. После этого Боб подтверждает цифровую подпись, и если она действительна, происходит транзакция. Таким образом, с использованием таких методов безопасности информация о здоровье может быть защищена от посторонних [12].

Электронные медицинские карты: Пациенты могут управлять своими электронными медицинскими записями с помощью технологии блокчейн. В большинстве медицинских учреждений пациентам не предоставляется доступ к своим медицинским данным, что вызывает разочарование в отношении конфиденциальности. Блокчейн может помочь избежать этой проблемы. При использовании блокчейна для электронных медицинских записей необходимо реализовать механизмы управления аутентификацией,

конфиденциальностью и ответственностью. Электронные записи в блокчейне функционируют как децентрализованное приложение, что отличается от централизованной среды, где все приложения выполняются в одном месте. Реализация электронных медицинских записей в блокчейне должна решить проблемы и ограничения, включая вопросы индивидуального контроля. Некоторые записи, контролируемые лично, могут быть загружены в институциональную запись для сохранения существующих данных. Использование блокчейна может помочь избежать этих проблем, так как транзакции в блокчейне осуществляются на основе обмена ключами между двумя сторонами, сохраняя при этом их анонимность. Каждый пользователь в блокчейне должен иметь один открытый и один закрытый ключ [13].

Блокчейн для защиты личных данных. В последнее время увеличилось количество случаев нарушения безопасности личных данных пользователей, вызывая беспокойство. Третьи стороны часто собирают личную информацию, что вызывает опасения. Блокчейн предлагает решение этой проблемы, устраняя необходимость третьих сторон и позволяя данным передаваться напрямую между участниками. Объем личных данных постоянно растет в современном мире. К примеру, Facebook, крупнейшая онлайн-социальная сеть, уже накопила 300 петабайт персональных данных. Однако, персональные и конфиденциальные данные должны быть защищены от несанкционированного доступа и злоупотреблений третьими лицами. Блокчейн позволяет пользователям управлять своими данными, лишь доверяя самим себе, а не третьим сторонам. В блокчейне каждый пользователь является владельцем своих данных. Для обеспечения безопасности и соблюдения правил блокчейн использует смарт-контракты. Перед проведением транзакции хранитель шлюза создает правила, которые записываются в виде контракта. Это гарантирует соблюдение условий и обеспечивает безопасное взаимодействие между участниками. Блокчейн доказал свою эффективность в финансовой сфере, в частности, с помощью биткойна. Он стал символом доверия и показал, что вычисления могут быть осуществлены в децентрализованной сети. Хотя блокчейн изначально разработан для обработки биткойнов, его применение не ограничивается только цифровыми валютами [14].

Смарт-контракт. Также известный как криптоконтракт, был предложен Ником Сабо в 1994 году. Это компьютерная программа, которая управляет передачей цифровой валюты напрямую. Смарт-контракты хранятся на технологии блокчейн и являются децентрализованной системой. Они работают в двух партиях, и нет необходимости платить посреднику, что экономит время и помогает избежать конфликтов. В смарт-контракте используется бухгалтерская книга, что делает его децентрализованным приложением.

Ledger: Леджер. Леджер — это децентрализованное приложение, связанное с каждым пользователем в блокчейне. После завершения транзакции она автоматически записывается в реестр. Например, есть два

человека, А и Б. Человек А должен передать 100 рупий человеку Б. В этом блокчейне есть еще какой-то человек. У них также есть отдельный реестр. Эти данные автоматически обновляются в общей книге. Человек А утверждает, что Б должен ему вернуть только 10 рупий. В этом случае применяется механизм голосования, который может опровергнуть заявление человека А, если оно не подтверждено. Этот публичный реестр идеально подходит для всех транзакций с криптовалютой, поскольку в нем нет центрального администратора или централизованного хранилища данных.

Блокчейн - увлекательная тема в последнее время, она будет поддерживать разнообразные приложения. Блокчейн гарантирует высокий уровень безопасности во время транзакций любого размера. Эта технология в основном используется для обработки транзакций в сети биткойн. Смарт-контракт, Ethereum и распределенный реестр - некоторые из приложений блокчейна. Они также обеспечивают повышенную безопасность. Самое подходящее и широко используемое применение блокчейна - биткойн. Блокчейн обеспечивает более быстрые и экономичные транзакции по сравнению с другими приложениями. Это также гарантирует высокий уровень безопасности, особенно для конфиденциальных данных. Приложения блокчейна часто обладают дополнительными преимуществами в прозрачности и неизменности [15].

Список источников

1. Алексашкин А. В. (2018). Блокчейн: технологии и практика применения. Москва: Альпина Паблишер. С.46-57.
2. Варламов А. А. (2019). Безопасность блокчейн-систем: угрозы и методы защиты. Санкт-Петербург: Питер. С. 107-115.
3. Дорофеев М. В. (2019). Криптографические методы защиты информации в блокчейн-системах. Москва: Физматлит. С. 14-20.
4. Зайковский Б.Б., Корниенко М.В. Современные банковские технологии и перспективы развития электронного обслуживания клиентов // Социальные науки. 2017. № 4. С. 10-17.
5. Исмаил С. 2013. Факторы, влияющие на внедрение B2B. технологии электронной коммерции. Электрон. Коммерческий. Рез. 13: 199–236.
6. Исмаил С. 2013. Факторы, влияющие на внедрение B2B. технологии электронной коммерции. Электрон. Коммерческий. Рез. 13: 199–236.
7. Киреев И. В. (2020). Блокчейн и криптовалюты: технологии, экономика, безопасность. Москва: Издательский дом МЭИ. С. 98-104.
8. Мырзагалы Н.С., Когай Г.Д. Анализ существующих подходов к автоматизации банковской деятельности // Молодой ученый. 2016. № 9. С. 220-237.
9. Никитин, А. С. (2017). Блокчейн: введение в технологию распределенных реестров. Москва: Бином. Лаборатория знаний. С. 211-216.

10. Хоул, К.Дж., В. Моен и Т. Тьостхайм, 2006 г. Случай. исследование: Безопасность онлайн-банкинга. IEEE Безопасность. Прив. 4.2: 14-20.

12. Харрис Л. и Дж. С. Лаура, 2002. Этика электронной почты. банковское дело. Дж. Электрон. Коммерческий. Рез. 3(2): 59–66.

13. Хилтген А., Т. Крамп и Т. Вейгольд, 2006 г. Безопасно. аутентификация в интернет-банке. IEEE Безопасность. Прив. 4.2: 21-29.

14. Шамин Е.А., Генералос И.Г., Завиваев Н.С., Черемухин А.Д. Сущность информатизации, ее цели, субъекты и объекты // Вестник НГИЭИ. 2015. № 11. С. 99-107.

15. Филатов, В. В., & Чистов, Д. А. (2021). Кибербезопасность блокчейн-систем. Москва: Юрайт. С. 134-140.

16. Морозова О. Ю., Пономарева Н.В. Влияние искусственного интеллекта на рынок электронной коммерции//Актуальные вопросы современной экономики. 2022.- №10. С.643-647