DOI 10.37882/2223-2966.2025.06-2.43

РОЛЬ БЛОКЧЕЙНА В СОЗДАНИИ УСТОЙЧИВЫХ СИСТЕМ ЗАЩИТЫ ДАННЫХ

THE ROLE OF BLOCKCHAIN IN CREATING SUSTAINABLE DATA PROTECTION SYSTEMS

K. Khananov

Summary. Blockchain technology has radically changed approaches to storing, managing, and protecting information. Its key features — decentralization, openness of the system and resistance of records to changes — create fundamentally new opportunities for ensuring digital security. This article analyzes the possibilities of integrating blockchain solutions into the field of data protection: the basic principles of the technology, operating algorithms, practical examples of implementation, as well as the associated advantages and limitations are examined. Based on industry cases, the article demonstrates the transformative impact of blockchain on countering cyber risks, emphasizing its role as a tool for creating reliable security systems in the face of growing digital threats.

Keywords: data, blockchain, data security, cybersecurity, cryptography, decentralization.

Хананов Кирилл Русланович
Аспирант, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
mr.hananov@gmail.com

Аннотация. Блокчейн-технология кардинально изменила подходы к хранению, управлению и защите информации. Ее ключевые особенности — децентрализация, открытость системы и устойчивость записей к изменениям — создают принципиально новые возможности для обеспечения цифровой безопасности. В данной статье анализируются возможности интеграции блокчейн-решений в сферу защиты данных: исследованы базовые принципы технологии, алгоритмы функционирования, практические примеры внедрения, а также связанные с этим преимущества и ограничения. На основе отраслевых кейсов статья демонстрирует трансформационное влияние блокчейна на противодействие киберрискам, подчеркивая его роль как инструмента для создания надежных систем безопасности в условиях растущих цифровых угроз.

Ключевые слова: данные, блокчейн, безопасность данных, кибербезопасность, криптография, децентрализация.

Введение

Технология блокчейн быстро трансформирует ландшафт безопасности данных. Отходя от централизованных систем, блокчейн предлагает надежный и защищенный от несанкционированного доступа подход к защите данных. Быстрая оцифровка информации и экспоненциальный рост генерации данных потребовали надежных механизмов безопасности. Традиционные централизованные системы становятся все более уязвимыми для утечек данных, несанкционированного доступа и кибератак. Технология блокчейн, впервые концептуализированная в 2008 году с появлением биткоина, предлагает децентрализованный подход к управлению данными и безопасности, потенциально устраняя многие ограничения традиционных методов.

Анализ литературы

Основной целью статьи является исследование применения технологии блокчейн в области безопасности данных. Это включает в себя понимание ее основных принципов, изучение различных функций безопасности и анализ ее применения в различных секторах для защиты целостности и конфиденциальности данных. Технология блокчейн широко используется для повышения безопасности данных во многих различных областях. Она используется для защиты данных беспроводных датчиков в сетях IoT, обеспечивая конфиденциальность и предотвращая кражу [1]. Кроме того, системы на основе блокчейна обеспечивают безопасный обмен данными для приложений IoT, уделяя особое внимание конфиденциальности данных, анонимности и подотчетности без необходимости в доверенных сторонах [2]. В секторе здравоохранения предлагается децентрализованная безопасность на основе блокчейна (BCDS) с Crypto-Proof of Stake (CPoS) для защиты персональных медицинских записей от несанкционированного доступа и утечки ключей, тем самым обеспечивая целостность и аутентификацию данных [3]. Кроме того, механизмы, вдохновленные блокчейном, интегрируются в защищенные системы обработки данных датчиков для обеспечения контроля доступа, неизменности и защиты от несанкционированных изменений, тем самым повышая общую безопасность и целостность данных [4]. Кроме того, фреймворк Access Control Enabled Blockchain (ACE-BC) использует механизмы шифрования атрибутов и контроля доступа для повышения безопасности и конфиденциальности данных в сетях обмена информацией о безопасности, тем самым повышая конфиденциальность и эффективность данных [5]. Технология блокчейн важна для улучшения мер безопасности данных с помощью различных

инновационных методов. Например, фреймворк Access Control Enabled Blockchain (ACE-BC) использует методы шифрования атрибутов и механизмы контроля доступа для повышения безопасности данных в обмене информацией о кибербезопасности (CIS) [6]. Аналогичным образом, модель децентрализованной безопасности на основе блокчейна (BCDS) использует доказательство доли владения (CPoS) и политику агрегации ключей главного узла (MNKAP) для надежной аутентификации и защиты конфиденциальных данных в пуле. Персональная медицинская карта (PHR) [7]. Кроме того, использование блокчейна для защиты журналов доступа обеспечит целостность и надежность аутсорсинговых данных за счет использования его функций безопасности и неизменности [8]. Стираемая модель иерархического контроля доступа на основе блокчейна повышает безопасность данных, позволяя владельцам данных определять политики доступа и контролировать изменения с помощью шифрования на основе атрибутов и техники хеширования хамелеон, обеспечивая эффективный и безопасный обмен данными [9]. Эти подходы демонстрируют, как технология блокчейна значительно улучшает меры безопасности данных в различных приложениях [10].

Теоретические основы

Блокчейн — это технология распределенного реестра, которая обеспечивает безопасное, прозрачное и защищенное от несанкционированного доступа ведение записей. Каждый блок содержит список транзакций и криптографически связан с предыдущим блоком, образуя цепочку. Децентрализованная природа блокчейна означает, что ни одна организация не контролирует всю сеть, что повышает безопасность и доверие.

Основные компоненты.

1. Децентрализация: в отличие от централизованных баз данных, блокчейн работает по одноранговой схеме, где каждый участник (хаб) включает дубликат полного блокчейна.
2. Неизменяемость: информация не может быть изменена или стерта после того, как она внесена в блокчейн. Эта постоянство достигается с помощью криптографического хеширования и инструментов соглашения.
3. Прозрачность: все коммуникации в блокчейне видны всем участникам, что подтверждает прозрачность и ответственность.
4. Механизмы консенсуса: многочисленные процессы (например, Proof of Work, Proof of Stake) достигают компромисса между узлами, аутентифицируя и блокируя коммуникации.

Типы блокчейнов.

1. Публичный блокчейн: открыт для всех; участники могут читать, писать и проверять блокчейн.
2. Частный блокчейн: ограниченный доступ; только авторизованные участники могут взаимодействовать с блокчейном.
3. Консорциумный блокчейн: контролируется группой организаций; доступ разделен между консорциумом организаций.

Функции безопасности блокчейна

Криптографическое хеширование

Каждый блок в блокчейне содержит три ключевых элемента: криптографический хеш предыдущего блока, временную метку и данные транзакции. Хеш-функция гарантирует целостность информации, генерируя уникальный идентификатор (хеш) для любого набора входных данных. Даже минимальное изменение в данных приводит к полному изменению хеша, что мгновенно сигнализирует о попытке несанкционированного вмешательства.

Для подтверждения транзакций и поддержания согласованности реестра блокчейн использует алгоритмы соглашений. Основные из них:

1. Proof-of-Work (PoW, «Доказательство работы») — майнеры решают сложные математические задачи для валидации транзакций и создания новых блоков. Процесс требует значительных вычислительных ресурсов, что делает атаки на сеть экономически невыгодными.
2. Proof-of-Stake (PoS, «Доказательство доли») — валидаторы выбираются на основе количества криптовалюты, которую они «замораживают» в качестве залога. Этот метод потребляет меньше энергии по сравнению с PoW.
3. Delegated Proof-of-Stake (DPoS) — участники сети голосуют за делегатов, которые проверяют транзакции от их имени, объединяя преимущества PoW и PoS.

Отсутствие централизованного управления исключает риски, связанные с единой точкой отказа. Данные дублируются на множестве узлов сети, что обеспечивает их сохранность даже при компрометации части системы.

Также в блокчейне используют смарт-контракты — это программные алгоритмы, автоматически исполняющие условия соглашений при наступлении заданных событий. Они минимизируют человеческое вмешательство, снижая риски ошибок и мошенничества.

Применение блокчейна в защите данных

Блокчейн позволяет хранить данные в распределенной сети, где информация не сосредоточена в одном хранилище. Такой подход сокращает риск утечек и не-

санкционированного доступа, так как злоумышленнику потребуется взломать большинство узлов одновременно.

Благодаря неизменности и прозрачности блокчейна технология становится оптимальным решением для гарантии достоверности информации. Все изменения фиксируются в публичном реестре, что позволяет участникам сети оперативно выявлять попытки манипуляций. Это свойство делает блокчейн эффективным инструментом для подтверждения аутентичности данных, исключая возможность их несанкционированного изменения после записи в систему.

Блокчейн-решения трансформируют подходы к управлению цифровыми идентификаторами, предлагая распределенное и защищенное хранение персональных данных. Пользователи получают возможность самостоятельно контролировать свою идентификационную информацию, что снижает риски краж и мошенничества. Среди ключевых возможностей таких систем:

1. Децентрализованные идентификаторы (DID) — уникальные цифровые ID, создаваемые и управляемые самими пользователями без участия посредников.
2. Самоуправляемая идентификация — полный контроль над предоставлением и отзывом доступа к личным данным, минуя централизованные органы.

Блокчейн обеспечивает безопасность как финансовых, так и нефинансовых операций, создавая прозрачную и не редактируемую историю всех действий. Это позволяет участникам проверять легитимность транзакций, исключая ошибки и подлоги. Примеры применения:

1. Криптовалюты (Bitcoin, Ethereum) — использование блокчейна для шифрования и валидации операций с цифровыми активами.
2. Цепочки поставок — отслеживание происхождения товаров и подтверждение их подлинности на каждом этапе логистики.

Неизменность данных в блокчейне упрощает соблюдение законодательных требований и проведение аудиторских проверок. Организации могут использовать технологию для:

- Ведения точных журналов операций, соответствующих нормативным стандартам.
- Автоматизации аудита: проверяющие получают доступ к достоверной истории транзакций, что минимизирует риски ошибок и фальсификаций.

В сфере здравоохранения блокчейн позволяет безопасно хранить и передавать электронные медицинские карты пациентов, ограничивая доступ к ним только авторизованным лицам (врачам, лабораториям, страховым компаниям). Технология повышает конфиденциальность, предотвращает утечки и улучшает взаимодействие между учреждениями, обеспечивая актуальность данных для всех участников процесса лечения.

Блокчейн создает прозрачную и неизменяемую систему регистрации прав на интеллектуальную собственность. Авторы могут фиксировать временные метки создания контента, патентов или дизайнов в блокчейне, что служит юридическим доказательством их авторства. Это упрощает разрешение споров и предотвращает незаконное использование объектов ИС.

Реальные кейсы внедрения

Разработанная MIT система MedRev использует блокчейн для управления электронными медкартами. Децентрализованное хранение данных позволяет пациентам гибко предоставлять доступ к своей истории болезней клиникам или исследователям, сохраняя контроль над информацией. Решение устраняет дублирование записей, снижает риск ошибок и повышает доверие к медицинским данным.

Платформа IBM Food Trust применяет блокчейн для отслеживания цепочек поставок продуктов питания. Каждый этап — от фермы до магазина — фиксируется в реестре, что исключает подмену данных о качестве, сроке годности или происхождении товаров. Это сокращает случаи фальсификаций и позволяет мгновенно выявлять источники заражения продукции.

Протокол Ripple оптимизирует международные платежи за счет блокчейна, обеспечивая переводы за секунды с минимальными комиссиями. Децентрализованная сеть валидаторов гарантирует безопасность операций, а встроенные алгоритмы предотвращают двойное расходование средств. Банки и платежные системы используют Ripple для снижения издержек и повышения надежности транзакций.

Проблемы и ограничения

Основным вызовом для блокчейн-систем остается ограниченная пропускная способность. Рост числа транзакций приводит к увеличению нагрузки на сеть, замедлению обработки операций и росту комиссий. Для решения этой проблемы разрабатываются технологии:

- **Шардинг** — горизонтальное разделение сети на части для параллельной обработки данных.
- **Офчейн-транзакции** — выполнение операций вне основного блокчейна с последующей фиксацией итогов.
- **Решения второго уровня** (например, Lightning Network) — надстройки, ускоряющие и удешевляющие микроплатежи.

Правовая неопределённость замедляет интеграцию блокчейна. Разрозненные требования разных стран к конфиденциальности данных, AML-политикам (противодействие отмыванию) и налогообложению крипто активов создают сложности для бизнеса. Например, в ЕС действует регламент MiCA, а в США — правила SEC, что усложняет кросс-граничные операции [11].

Другой проблемой развития технологии блокчейн остается энергопотребление. Алгоритмы Proof of Work (PoW), используемые в Bitcoin и ранее в Ethereum, требуют огромных вычислительных мощностей, что критикуется за негативное влияние на экологию [11]. Альтернативы:

- Proof of Stake (PoS) — Ethereum 2.0 сократил энергозатраты на 99.95 % после перехода на PoS.
- Другие алгоритмы — Delegated Proof of Stake (DPoS), Proof of Authority (PoA).

Взаимодействие между различными сетями блокчейнов и существующими системами является серьезной проблемой. Обеспечение бесперебойной связи и обмена данными между различными платформами имеет важное значение для широкого внедрения технологии блокчейна.

Несмотря на криптографическую защиту, риски сохраняются [12]:

1. Уязвимости смарт-контрактов — Ошибки в коде (как в случае взлома DAO в 2016 году) позволяют злоумышленникам похищать средства.
2. Атака 51 % — Захват контроля над большинством вычислительных мощностей сети для изменения транзакций.
3. Риски управления ключами — Утрата приватного ключа означает безвозвратную потерю доступа к активам. Решение: аппаратные кошельки (Ledger, Trezor) и мультиподпись.

Будущее блокчейн-технологий

Совершенствование механизмов согласования данных — ключевой вектор развития. Гибридные модели, такие как Delegated Proof of Stake (DPoS) и Practical Byzantine Fault Tolerance (PBFT), повышают скорость обработки транзакций и устойчивость сетей к сбоям. Например, переход Ethereum на PoS уже сократил энергопотребление на 99 %, сделав блокчейн экологичнее [12]. Синергия блокчейна с ИИ, IoT и квантовыми вычислениями открывает новые горизонты [10]:

- ИИ + блокчейн — аудит алгоритмов машинного обучения для прозрачности решений.
- IoT + блокчейн — защищённые децентрализованные сети для умных устройств (например, отслеживание поставок в реальном времени).
- Квантовые решения — разработка криптографии, устойчивой к квантовым атакам.

Усилия по разработке стандартизированных протоколов и структур для технологии блокчейнов могут улучшить совместимость между различными сетями блокчейнов и существующими системами. Это может способствовать более широкому принятию и интеграции решений блокчейнов в различных отраслях.

Технологии ZKP (Zero-Knowledge Proofs), и гомоморфное шифрование позволяют проверять данные без раскрытия содержимого. Это решает дилемму между прозрачностью блокчейна и конфиденциальностью пользователей [11].

По мере развития технологии блокчейна нормативные рамки, скорее всего, будут адаптироваться для решения ее уникальных проблем и возможностей. Четкие и последовательные правила могут обеспечить благоприятную среду для роста и принятия решений на основе блокчейна.

Заключение

Блокчейн-технология демонстрирует революционный потенциал в сфере защиты данных, предлагая инновационные решения для различных отраслей. Базируясь на принципах децентрализации, неизменности записей и прозрачности операций, она формирует устойчивую основу для противодействия кибератакам, фальсификациям и несанкционированному вмешательству.

Несмотря на текущие вызовы — ограничения в скорости обработки транзакций, правовую неопределённость и высокие энергозатраты — активные исследования и инновационные подходы (переход на PoS, шардинг) постепенно нивелируют эти барьеры.

Перспективы технологии очевидны: интеграция с ИИ и IoT, внедрение стандартов интероперабельности и развитие «зелёных» алгоритмов консенсуса открывают новую эру в управлении цифровыми активами. Блокчейн не просто улучшает существующие системы безопасности — он переопределяет стандарты хранения, обработки и защиты информации, становясь краеугольным камнем цифровой трансформации XXI века.

ЛИТЕРАТУРА

1. Hsiao S.J., Sung W.T. Повышение кибербезопасности с использованием технологии блокчейна на основе слияния данных IoT. IEEE Internet Things J.2023;10(1):486–98.
2. Wu T., Wang W., Zhang C., Zhang W., Zhu L., Gai K. и др. Анонимный обмен данными на основе блокчейна с ответственностью за Интернет вещей. IEEE Internet Things J. 2023;10(6):5461–75.
3. Deepika K.M., Murthy M. Децентрализованная безопасность на основе блокчейна с использованием крипто-доказательства доли для защиты конфиденциальных персональных медицинских записей. Adv Eng Software. 2022; 173:103235.
4. Zhao W., Aldama I.M., Gangwani P., Joshi S., Upadhyay H., Lagos L. Система безопасной обработки и регистрации данных зондирования с использованием блокчейна. IEEE Access. 2023;11.
5. Alharbi A. Применение структуры блокчейна с поддержкой контроля доступа (ACE-BC) для управления безопасностью данных в системе CIS. Sens.2023;2023(6):3020
6. Manogaran G., Alazar M., Hsu C.H. Модель безопасного обмена данными с использованием блокчейна для интеллектуальных отраслей на основе Интернета вещей. IEEE Trans Reliability. 2022;71(1):348–58.
7. Benkhaddra I., Kumar A., Bensalem Z.E., Hang L. Безопасная передача секретных данных с использованием методов встраивания на основе оптимизации в блокчейн. Expert Syst Appl. 2023; 211:118469.
8. Sifah E.B., Xia Q., Agyekum K.O., Xia H., Smahi A., Gao J. Подход на основе блокчейна к обеспечению происхождения аутсорсинговых облачных данных в экосистеме совместного использования. IEEE Syst J. 2022;16(1):1673–84.
9. Ram B., Yadav S., Singh K.K. Применение облачных вычислений в библиотечных службах. В: 5-й Международный симпозиум по новым тенденциям и технологиям в библиотеках и информационных службах; 2018. стр. 75–8.
10. Hosen A.S., Yoon B. Атаки на безопасность блокчейна, проблемы и решения для будущей распределенной сети Интернета вещей. IEEE Access.2017.
11. Estevam G.; Palma, L.M.; Silva, L.R.; Martina, J.E.; Виджил, М. Точная и децентрализованная временная метка с использованием смарт-контрактов на блокчейне Ethereum. Inf. Process. Manag. 2021,58, 102471
12. Чжан С.; Ли Дж. Х. Анализ основных консенсусных протоколов блокчейна. ICT Express 2020,6, 93–97.

Журнал «Современная наука: актуальные проблемы теории и практики»