

УДК 004.75

ВОЗМОЖНОЕ ПРИМЕНЕНИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В ЗАЩИТЕ ИНФОРМАЦИИ

Какорин И.А.¹

магистр,

Волгоградский государственный университет,

Волгоград, Россия¹

Аннотация

В статье рассматривается возможность применения технологии блокчейн, а именно способность защищать от различных угроз, присущих традиционным централизованным системам. Блокчейн значительно повышает безопасность, обеспечивая децентрализованное управление, что предотвращает подделку данных и мошенничество, устраняет единые точки отказа. Технология также способствует прозрачности цепочек поставок и защищает от кибератак, таких как DDoS. Блокчейн представляет собой инновационное решение, способное изменять подходы к киберзащите и повысить доверие в цифровых системах.

Ключевые слова: блокчейн, угрозы, атака, идентификация, механизм консенсуса, хеш.

POSSIBLE APPLICATION OF BLOCKCHAIN TECHNOLOGIES IN INFORMATION SECURITY

Kakorin I.A.

master,

Volograd State University,

Volgograd, Russia

¹ Научный руководитель – к.ф.-м.н., доцент О.А. Какорина, Волгоградский государственный университет.

Scientific supervisor – Ph.D., Associate Professor O.A. Kakorina, Volgograd State University.

Annotation

The article discusses the possibility of using blockchain technology, namely the ability to protect against various threats inherent in traditional centralized systems. Blockchain significantly increases security by providing decentralized management, which prevents data forgery and fraud, and eliminates single points of failure. The technology also promotes transparency in supply chains and protects against cyber attacks such as DDoS. Blockchain is an innovative solution capable of changing approaches to cyber defense and increasing trust in digital systems.

Keywords: blockchain, threats, attack, identification, consensus mechanism, hash.

В настоящее время для защиты информации необходимо разрабатывать и использовать новые технологии. Одной из таких технологий является блокчейн [6]. Блокчейн - это децентрализованный реестр, состоящий из блоков с уникальными криптографическими хэшами. Блоки образуют неизменяемую цепочку, которую может проверить каждый пользователь. Технология блокчейн – это безопасный подход к управлению данными и обработке транзакций, устраняет ряд угроз, существующих в традиционных централизованных системах [5]. Рассмотрим преимущества блокчейна для повышения безопасности в различных областях.

Удвоение расходов при цифровых транзакциях.

В цифровых транзакциях риск двойных трат возникает, когда пользователь тратит один и тот же цифровой актив несколько раз, используя время, необходимое традиционным платежным системам для обработки и подтверждения транзакций [1]. Технология блокчейн решает эту проблему с помощью механизмов консенсуса, таких как Proof of Work или Proof of Stake, которые проверяют и подтверждают транзакции децентрализованным образом. Таким образом, транзакция проверяется и добавляется в блокчейн, предотвращая двойные расходы и обеспечивая целостность цифровых

Дневник науки | www.dnevniknauki.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

транзакций [2]. Эта особенно важно при обмене криптовалютами и цифровыми активами.

Предотвращение кражи личных данных.

Способность блокчейна устанавливать защищенные цифровые идентификационные данные может значительно снизить уровень кражи личных данных и мошенничества. Используя криптографические методы и пары открытых и закрытых ключей, люди могут безопасно управлять своими идентификаторами и контролировать доступ к своей личной информации. Системы идентификации на основе блокчейна обеспечивают самостоятельную идентификацию, снижая зависимость от централизованных органов проверки личности и сводя к минимуму риск кражи личных данных. Прозрачная и защищенная от несанкционированного доступа структура блокчейна гарантирует, что идентификаторы остаются безопасными и заслуживают доверия.

Прозрачность цепочки поставок и предотвращение контрафакта.

Технология блокчейн обеспечивает прозрачность в цепочках поставок, позволяя заинтересованным сторонам отслеживать и проверять происхождение, перемещение и подлинность продуктов. Благодаря записи каждой транзакции и перемещения товаров в блокчейне становится практически невозможным внедрение контрафактной продукции в цепочку поставок. Такая прозрачность укрепляет доверие потребителей, облегчает соблюдение нормативных требований и помогает бороться с такими проблемами, как отзыв продукции и контрафактные товары. Неизменяемая природа блокчейна гарантирует, что данные, записанные в блокчейне, точно отражают историю и происхождение продуктов, обеспечивая надежное решение для устранения уязвимостей цепочки поставок.

Распределенные атаки типа "Отказ в обслуживании" (DDoS).

Децентрализованная архитектура блокчейна может обеспечить устойчивость к распределенным атакам типа "Отказ в обслуживании" (DDoS).

В традиционных централизованных системах DDoS-атаки поражают единственную точку входа, делая систему недоступной. Однако в блокчейн-сети нет единой точки отказа, и вычислительная мощность распределяется между участниками сети. Такое распределение ресурсов значительно усложняет злоумышленникам задачу по нарушению работы системы с помощью DDoS-атаки.

Подделка данных и мошенничество.

Технология блокчейн обеспечивает целостность и неизменяемость данных за счет использования криптографических хэшей и механизмов консенсуса. Как только транзакция или фрагмент данных записываются в блокчейн, их становится практически невозможно изменить или подделать. Такая защита необходима в управлении цепочками поставок, финансовых транзакциях и проверках цифровой личности.

Централизованные точки отказа.

Традиционные системы часто полагаются на централизованные серверы или центры управления, которые действуют как единые точки отказа. Любая атака на эти центральные объекты приводят к серьезным последствиям - утечке данных, сбоям в обслуживании или несанкционированному доступу. Блокчейн работает в децентрализованной сети узлов, где каждый участник владеет своей копией, эта возможность устраняет отдельные точки отказа, что делает систему устойчивой к кибератакам и системным сбоям. Даже если некоторые узлы в сети скомпрометированы, остальные узлы продолжают поддерживать целостность и безопасность блокчейна.

Хранение данных.

Традиционные централизованные системы хранения файлов уязвимы к утечкам данных. Децентрализованные системы хранения файлов на основе блокчейна распределяют данные по сети, снижая риск единой точки отказа. Это не только повышает безопасность конфиденциальных файлов, но и обеспечивает конфиденциальность, сводя к минимуму подверженность данных. Дневник науки | www.dnevniknauki.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

потенциальным утечкам. В децентрализованной модели хранения файлы фрагментируются и шифруются перед распределением по нескольким узлам. Это означает, что даже если один узел будет скомпрометирован, данные останутся в безопасности и недоступны для неавторизованных пользователей [3]. Такой подход не только повышает безопасность, но и повышает доступность и устойчивость данных, гарантируя, что критически важная информация останется доступной даже перед лицом киберугроз.

Технология блокчейн доказывает свою применимость в защите и обеспечении безопасности в цифровом пространстве, с которыми сталкиваются организации сегодня [4]. Поскольку цифровизация общества продолжает развиваться, внедрение стратегий блокчейна может оказаться необходимым для создания устойчивых и безопасных систем, способных противостоять постоянно растущему числу киберугроз. Блокчейн часто называют «невзламываемой» технологией. Но атаки 51% позволяют злоумышленникам получить контроль над более чем половиной вычислительной мощности блокчейна и нарушить целостность общего реестра, т.е. если одна сторона владеет 51% пула для майнинга, можно подделать запись в блокчейн, что позволит осуществить двойную трату и даже создать новую цепочку в интересах пула для майнинга. Хотя эта конкретная атака является дорогостоящей и сложной, но специалисты в области информационной безопасности должны рассматривать блокчейн как полезную технологию, а не как волшебное решение всех проблем.

Библиографический список

1. Анвар, К. С. Блокчейн технологии как инструмент укрепления экономики развивающихся стран / К. С. Анвар // Известия Исык-Кульского форума бухгалтеров и аудиторов стран Центральной Азии. – 2022. – № 3-1(38). – С. 425-429.

2. Анвар, К. С. Особенности работы технологии блокчейн / К. С. Анвар // Известия Иссык-Кульского форума бухгалтеров и аудиторов стран Центральной Азии. – 2022. – № 3-1(38). – С. 429-433.
3. Исроилов, С. Г. Разработка защищенной системы электронного документооборота на основе блокчейн-технологии / С. Г. Исроилов, С. Н. Верзунов // Проблемы автоматизации и управления. – 2021. – № 2(41). – С. 61-76.
4. Липницкий, Д. В. Возможности и вызовы для блокчейн в новой индустриализации / Д. В. Липницкий // Экономика промышленности. – 2019. – № 1(85). – С. 82-100. – DOI 10.15407/econindustry2019.01.082.
5. Принципы работы технологии блокчейн / А. Е. Тойлыбаев, М. Ж. Айтимов, Ж. Бимураткызы, У. Ж. Айтимова // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева. – 2017. – № 4(103). – С. 249-257.
6. Чумбуридзе, Я. А. Изучение технологий, повышающих конфиденциальность / Я. А. Чумбуридзе, О. А. Какорина // НБИ технологии. – 2023. – Т. 17, № 3. – С. 38-43. – DOI 10.15688/NBIT.jvolsu.2023.3.5..

Оригинальность 79%