Марква Т.Д. Безопасность и приватность в блокчейн сетях. методы и технологии защиты данных // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 10(48) с. 90–95

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

БЕЗОПАСНОСТЬ И ПРИВАТНОСТЬ В БЛОКЧЕЙН СЕТЯХ. МЕТОДЫ И ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ

Марква Т.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: norm_staffchik@mail.ru

В данной статье рассматриваются ключевые аспекты обеспечения безопасности блокчейн-сетей. Обсуждаются криптографические основы, консенсусные механизмы и многоуровневый подход к защите, охватывающий уровни узлов, сети, приложений и пользователей. Особое внимание уделяется перспективным направлениям исследований, таким как гомоморфное шифрование, блокчейн с нулевым разглашением информации, применение искусственного интеллекта и противодействие угрозам квантовых вычислений. Подчеркивается важность государственного регулирования, отраслевых стандартов и международного сотрудничества для создания безопасной и надежной блокчейн-экосистемы. В заключении отмечается, что обеспечение безопасности является фундаментальным требованием для массового внедрения блокчейна и реализации его революционного потенциала.

Ключевые слова: Блокчейн, безопасность, криптография, консенсус, смарт-контракты, кибербезопасность, гомоморфное шифрование, нулевое разглашение информации, искусственный интеллект, квантовые вычисления, регулирование, стандарты, международное сотрудничество.

SECURITY AND PRIVACY IN BLOCKCHAIN NETWORKS. DATA PROTECTION METHODS AND TECHNOLOGIES

Markva T.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: norm_staffchik@mail.ru

This article discusses the key aspects of ensuring the security of blockchain networks. Cryptographic foundations, consensus mechanisms, and a multi-layered approach to protection covering node, network, application, and user levels are discussed. Special attention is paid to promising areas of research, such as homomorphic encryption, zero-disclosure blockchain, the use of artificial intelligence and countering the threats of quantum computing. The importance of government regulation, industry standards and international cooperation to create a secure and reliable blockchain ecosystem is emphasized. In conclusion, it is noted that ensuring security is a fundamental requirement for the mass adoption of blockchain and the realization of its revolutionary potential.

Keywords: Blockchain, security, cryptography, consensus, smart contracts, cybersecurity, homomorphic encryption, zero disclosure of information, artificial intelligence, quantum computing, regulation, standards, international cooperation.

Введение

Технология блокчейна, лежащая в основе криптовалют, получила широкое распространение и признание в качестве революционной инновации, способной трансформировать различные отрасли за пределами финансовой сферы. Одним из ключевых преимуществ блокчейна является его децентрализованная природа, обеспечивающая высокую

степень прозрачности, неизменности и отказоустойчивости данных. Однако вместе с этими преимуществами возникают серьезные вопросы безопасности и защиты конфиденциальности информации, циркулирующей в блокчейн-сетях. Поскольку все транзакции и данные распределены и доступны для просмотра всеми участниками, существует риск раскрытия конфиденциальной информации, подверженности атакам и злонамеренному использованию данных. Обеспечение надлежащего уровня безопасности и конфиденциальности является критически важным для широкого принятия и доверия к технологии блокчейна, особенно в таких чувствительных областях, как финансы, здравоохранение, управление цепочками поставок и защита интеллектуальной собственности.

Криптографические основы блокчейна

Безопасность и неизменность данных в блокчейн-сетях обеспечивается с помощью криптографических алгоритмов и протоколов. В основе технологии блокчейна лежат асимметричное шифрование на базе криптосистем с открытым ключом и цифровые подписи. Каждый участник блокчейна имеет пару ключей: открытый (публичный) ключ, который используется для получения криптовалюты и проверки подписей, и закрытый (приватный) ключ для подписания транзакций и доступа к средствам. Транзакции подписываются отправителем с помощью приватного ключа, гарантируя их подлинность и неизменность. Открытые ключи участников распределяются по сети для проверки подписей. [1, с.262]

Другой важной криптографической техникой в блокчейне является хеширование – применение криптографических хеш-функций для получения цифрового отпечатка или дайджеста данных. Каждый блок в цепочке содержит хеш предыдущего блока, образуя связанную структуру. Изменение любых данных в предыдущих блоках приведет к нарушению последовательности хешей, что легко обнаружить. Помимо хеширования, используются другие криптографические примитивы, такие как деревья Меркла для эффективной проверки транзакций.

Распределенный консенсус между узлами сети является ключевым компонентом блокчейна, обеспечивающим согласованное состояние реестра. Популярными алгоритмами консенсуса являются Proof-of-Work (PoW) и Proof-of-Stake (PoS), основанные на криптографических вычислениях. Распределенная архитектура и согласование данных между множеством узлов делает блокчейн устойчивым к отказам и атакам, поскольку для успешной атаки требуется скомпрометировать значительную часть сети.

Методы защиты конфиденциальности данных

Одной из главных проблем безопасности в блокчейн-сетях является защита конфиденциальности персональных данных и деталей транзакций. Поскольку все операции в блокчейне распределены и потенциально видны всем участникам, существует риск раскрытия конфиденциальной информации, такой как суммы переводов, состояния счетов и связи между адресами. [5, с.267]

Для решения этой проблемы были разработаны различные криптографические методы и технологии, направленные на сохранение приватности пользователей и анонимности транзакций в блокчейне. Одним из базовых подходов является использование псевдонимов и анонимных адресов вместо реальных идентификаторов пользователей. Однако этот метод не

обеспечивает полной конфиденциальности, так как транзакции все равно видны, а адреса могут быть связаны с реальными личностями путем анализа блокчейна.

Для более надежной защиты конфиденциальности применяются технологии обфускации и микширования (mixers), которые объединяют множество транзакций от разных источников, затрудняя отслеживание связей между адресами отправителей и получателей. Также используются кольцевые подписи, позволяющие скрыть отправителя транзакции в группе из нескольких возможных подписантов.

Одной из наиболее перспективных технологий являются криптографические доказательства с нулевым разглашением информации (zk-SNARKs), которые позволяют проверить корректность транзакций, не раскрывая их содержимого. Эта технология лежит в основе таких проектов, как Zcash и конфиденциальный вариант Ethereum, обеспечивая полную конфиденциальность и невозможность отслеживания транзакций. [3, с.77]

Кроме того, существуют специализированные конфиденциальные блокчейны, например, Monero, которые изначально ориентированы на повышенную приватность за счет использования кольцевых подписей, технологии взаимного сокрытия (stealth addressing) и других методов.

Важно отметить, что обеспечение приватности в блокчейне часто имеет компромиссы, такие как снижение производительности или увеличение размера данных. Поэтому выбор и внедрение соответствующих методов защиты конфиденциальности должны учитывать требования конкретных случаев использования и находить баланс между безопасностью, производительностью и масштабируемостью.

Многоуровневая безопасность блокчейн-сетей

Обеспечение всесторонней безопасности в блокчейн-экосистеме требует принятия многоуровневого подхода, охватывающего различные компоненты и слои системы. Меры защиты должны распространяться на уровни отдельных узлов, сети в целом, уровень приложений и смарт-контрактов, а также учитывать безопасность конечных пользователей.

На уровне отдельных узлов необходимо применять традиционные методы защиты, такие как антивирусное программное обеспечение, брандмауэры, регулярное обновление программного обеспечения и операционных систем. В блокчейнах, использующих алгоритм консенсуса Proof-of-Work, важно обеспечить достаточную вычислительную мощность для защиты от потенциальных атак 51%. Также необходимо тщательно защищать закрытые ключи узлов с помощью надежных средств хранения и резервного копирования.

На уровне сети безопасность обеспечивается распределенной архитектурой блокчейна и консенсусными механизмами. Тем не менее, существуют угрозы, такие как DDoS-атаки, направленные на перегрузку и дестабилизацию сети. Для противодействия этим атакам применяются специальные протоколы и методы обнаружения аномального трафика, а также повышение производительности и пропускной способности сети. [2, с.92]

На уровне приложений и смарт-контрактов крайне важен тщательный аудит исходного кода на предмет уязвимостей и ошибок, которые могут привести к потере средств или раскрытию данных. Технологии, такие как формальная верификация и изоляция смарт-контрактов, помогают снизить риски. Кроме того, необходимо постоянно отслеживать появление новых угроз и своевременно выпускать обновления безопасности.

Наконец, безопасность конечных пользователей является важным фактором. Необходимо обеспечить надежную защиту кошельков и приватных ключей, а также повышать осведомленность пользователей о потенциальных угрозах, таких как фишинг и мошеннические схемы. Кроме того, следует предоставлять простые в использовании инструменты для резервного копирования и восстановления средств в случае потери доступа.

Новые технологии и исследования в области безопасности блокчейна

Область безопасности и приватности в блокчейн-сетях является активно развивающейся и привлекает значительные усилия исследователей и разработчиков. Помимо совершенствования существующих методов, ведутся работы по созданию принципиально новых технологий для повышения уровня защиты данных в этой экосистеме.

Одним из перспективных направлений является применение гомоморфного шифрования, позволяющего выполнять вычисления над зашифрованными данными без их расшифровки. Это открывает возможность для создания приватных смарт-контрактов и конфиденциальных вычислений в блокчейне без раскрытия входных данных. Компании, такие как Microsoft, IBM и другие ведущие технологические гиганты, активно исследуют применение гомоморфного шифрования в блокчейн-средах.

Другим многообещающим подходом являются так называемые "блокчейны с нулевым разглашением информации" (zk-Rollups), которые используют современные криптографические доказательства с нулевым разглашением для масштабирования и повышения конфиденциальности транзакций. Этот метод позволяет проверять корректность транзакций, не раскрывая их содержимого, и агрегировать большое количество операций в одну, снижая нагрузку на основную блокчейн-сеть. Проекты вроде Starkware и ZCash работают над внедрением этой технологии.

В сфере кибербезопасности активно изучается применение методов искусственного интеллекта, таких как машинное обучение, для выявления аномалий, мошеннических схем и потенциальных атак на блокчейн-системы. Возможность анализировать огромные объемы данных о транзакциях и поведении узлов позволит своевременно обнаруживать подозрительную активность и принимать соответствующие меры защиты.

Важным направлением исследований является разработка методов защиты блокчейнов от угроз, связанных с квантовыми вычислениями. Поскольку квантовые компьютеры могут нарушить многие современные криптографические алгоритмы, необходимо заранее подготовить постквантовые криптосистемы, устойчивые к атакам с использованием квантовых вычислений.

Кроме технологических инноваций, важную роль играет стандартизация и создание передовых практик в области безопасности блокчейна. Различные отраслевые организации и консорциумы, такие как Всемирный экономический форум и Институт стандартов IEEE, работают над разработкой стандартов и рекомендаций по обеспечению кибербезопасности в блокчейн-экосистеме.

Регулирование, стандартизация и сотрудничество

Обеспечение надлежащего уровня безопасности и конфиденциальности в блокчейн-экосистеме невозможно без соответствующих регуляторных мер, отраслевых стандартов и тесного сотрудничества между различными заинтересованными сторонами.

Регулирующие органы играют важную роль в создании нормативно-правовой базы для безопасного и ответственного внедрения блокчейн-технологий. Необходимо разработать четкие требования и руководящие принципы в области кибербезопасности, защиты данных, соблюдения конфиденциальности и противодействия финансовым преступлениям, связанным с блокчейном. Своевременное регулирование поможет устранить правовую неопределенность и создаст благоприятные условия для развития инноваций в этой сфере.

Наряду с государственным регулированием, крайне важна разработка отраслевых стандартов и передовых практик безопасности блокчейнов. Такие организации, как Институт инженеров по электротехнике и электронике (IEEE), Международная организация по стандартизации (ISO) и Консорциум распределенных реестров (Decentralized Identity Foundation), работают над созданием всеобъемлющих стандартов, охватывающих различные аспекты блокчейн-безопасности, включая криптографию, управление идентификационными данными, смарт-контракты и многое другое.

Кроме того, необходимо тесное сотрудничество и координация усилий между различными участниками блокчейн-экосистемы, включая разработчиков, владельцев узлов, поставщиков услуг, регуляторов и исследовательские организации. Обмен информацией об актуальных угрозах, уязвимостях и передовых методах защиты имеет решающее значение для повышения общего уровня безопасности.

На международном уровне важную роль играют такие инициативы, как Глобальная платформа по управлению киберпространством Всемирного экономического форума, которая объединяет правительства, компании и экспертов для координации усилий по обеспечению безопасности новых технологий, включая блокчейн. [4, с.149]

Заключение

В заключение следует отметить, что безопасность является фундаментальным требованием для массового внедрения блокчейна в различных областях человеческой деятельности. Только путем объединения усилий разработчиков, исследователей, регуляторов и всех заинтересованных сторон мы сможем создать надежную и защищенную блокчейн-экосистему, способную реализовать весь революционный потенциал этой технологии.

Безопасность блокчейна – это непрерывный процесс, требующий постоянного внимания и совершенствования. Будущее этой технологии во многом зависит от нашей способности эффективно противостоять новым угрозам и вызовам, которые неизбежно возникнут. Только тогда мы сможем в полной мере воспользоваться преимуществами открытой, прозрачной и децентрализованной среды, создаваемой блокчейнами.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019.
2. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8.

3. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018.
5. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019.

References

1. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019.
2. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – №. 8.
3. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. – 2020. – Vol. 12. – No. 4.
4. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics" RI-2018". – 2018.
5. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019.