6 – TOM 10 – SON / 2023 - YIL / 15 - OKTYABR

ЦИФРОВАЯ БЕЗОПАСНОСТЬ ДАННЫХ В БЛОКЧЕЙН-СЕТЯХ

Обухов Вадим Анатольевич
Набижонов Равшанбек Мухаммаджон ўғли
Мамаева Ойдинов Исмоилжон қизи
Абдукодиров Абдулхай Абдулазиз ўғли
rnabijonov19@gmail.com
Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий

Аннотация: *Данная статья исследует важную проблему обеспечения цифровой безопасности данных в блокчейн-сетях. Блокчейн, как децентрализованная система хранения и передачи информации, стал неотъемлемой частью современного цифрового мира и нашел широкое применение в различных отраслях. Однако, несмотря на свою надежность и неподкупность, блокчейн-сети также подвержены угрозам безопасности данных.*

Ключевые слова: *Блокчейн, цифровая безопасность, хэширование, шифрование, электронные подписи, смарт-контракты, угрозы безопасности, атаки 51.*

Цифровые технологии перепроектировали множество аспектов нашей жизни, и одним из наиболее значимых достижений в этой области стал блокчейн. Блокчейн — это децентрализованная система, способствующая сохранению и обмену информацией без центрального контроля. Он нашел применение в различных областях, от финансовых операций до здравоохранения и государственных реестров. Однако важно понимать, что цифровая безопасность данных в блокчейн-сетях является приоритетной задачей, и в данной статье мы рассмотрим ключевые аспекты этой темы.

Роль блокчейна в современном мире

Применение блокчейна расширилось на множество отраслей, таких как финансы, логистика, здравоохранение и даже управление государственными данными. Например, в медицинской сфере блокчейн может использоваться для хранения медицинских записей и обеспечения доступа к ним только уполномоченным лицам. Однако, несмотря на все преимущества блокчейна, его безопасность требует особого внимания.

Принципы безопасности данных в блокчейн-сетях

Безопасность данных в блокчейне строится на четырех основных принципах: надежности, конфиденциальности, целостности и доступности.

1. Надежность: Этот принцип означает, что данные в блокчейне должны быть защищены от фальсификации и вмешательства. Это достигается за счет

использования криптографических методов и консенсусных алгоритмов, которые требуют согласия большинства участников сети для внесения изменений в блокчейн.

2. Конфиденциальность: Важно обеспечивать конфиденциальность данных, особенно когда речь идет о личной или чувствительной информации. Блокчейн-сети могут использовать методы шифрования для защиты данных на уровне хранения и передачи.

3. Целостность: Этот принцип гарантирует, что данные остаются неизменными и достоверными. Хэш-функции широко используются для обеспечения целостности блоков данных в блокчейне.

4. Доступность: Блокчейн должен быть всегда доступен пользователям, когда это необходимо. Для этого требуется эффективное управление сетью, а также защита от атак, направленных на выключение узлов блокчейна.

Криптографические методы обеспечения безопасности данных в блокчейн-сетях

Криптография играет важную роль в обеспечении безопасности данных в блокчейн-сетях. Вот несколько криптографических методов, используемых для защиты данных в блокчейне:

1. Хэширование: Хэш-функции преобразуют данные в фиксированный набор символов (хэш), который уникален для каждого набора данных. Это позволяет обнаруживать даже малейшие изменения данных, так как любое изменение приведет к изменению хэша.

2. Шифрование: Симметричное и асимметричное шифрование используются для защиты данных на уровне передачи и хранения. Асимметричное шифрование, например, используется для подписи транзакций в блокчейне, обеспечивая аутентификацию участников.

3. Электронная подпись: Электронные подписи используются для подтверждения авторства транзакций и обеспечивают аутентификацию и целостность данных в блокчейне.

4. Смарт-контракты: Смарт-контракты включают логику и правила, которые должны выполняться в сети блокчейн. Они также используют криптографию для обеспечения безопасности и автоматизации выполнения соглашений между участниками сети. Каждое действие, выполняемое в рамках смарт-контракта, должно быть подписано и верифицировано криптографически, чтобы обеспечить надежность и безопасность.

Угрозы безопасности данных в блокчейн-сетях

Несмотря на высокий уровень безопасности, который обеспечивает блокчейн, существуют угрозы, которые могут подвергнуть риску данные и участников сети. Некоторые из них включают:

1. 51% атака: Это атака, при которой злоумышленники получают контроль над более чем половиной вычислительной мощности сети. Это может позволить им проводить манипуляции с данными.

2. Атаки на уровне приложений: Вредоносные смарт-контракты или приложения могут создавать риски для участников сети, приводя к потере средств или утечке данных.

3. Социальная инженерия: Злоумышленники могут попытаться манипулировать участниками сети, чтобы получить доступ к их частным ключам или другой чувствительной информации.

4. Деление ключей: Потеря доступа к частным ключам может привести к полной потере доступа к средствам или данным в блокчейне. Такие ситуации требуют тщательного управления ключами и их резервирования.

Заключение

Блокчейн предоставляет множество преимуществ в области цифровой безопасности данных, но это не означает, что система абсолютно надежна. Важно учитывать конкретные угрозы и применять соответствующие меры безопасности, такие как шифрование, электронные подписи, контроль доступа и мониторинг сети. Только при правильном сочетании технических методов и внимания к социальным и организационным аспектам можно обеспечить полную безопасность данных в блокчейн-сетях.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Набижонов , Р., & Обухов , В. (2023). Дальнейший вклад блокчейн-сетей в развитие дистанционного образования. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/772

2. Обухов, В., Ходжиматов Ж., & Набижонов , Р. (2023). Развитие блокчейн технологий в узбекистане: современные вызовы и перспективы. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/768

3. Обухов , В., Хамидов Э., & Набижонов , Р. (2023). Поэтапное внедрение блокчейн технологий в Республике Узбекистан. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/770

4. Xonto'rayev, S. (2023). Oliy ta'lim muassasalarida Web resurslarda mavjud dasturiy, texnik va uslubiy muammolarni bartaraf etish. Scientific-technical journal (STJ FerPI, ФарПИ ИТЖ, НТЖ ФерПИ, 2023, Т. 27. спец. выпуск№ 2).

5. Nabijonov , R., & Rasulov , A. (2023). Zamonaviy media portal imkoniyatlaridan unumli foydalanish. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/767

6. Sobirov Muzaffarjon Mirzaolimovich, Nabijonov Ravshanbek Mukhammadjon Ugli, & Khaitboev Elbekjon Iminjon Ugli (2023). Development of automated management system in technical processes. Science and innovation, 2 (A4), 195-198. doi: 10.5281/zenodo.7868406

7. Умаров, Ш. А., & Умарова, М. И. (2021). Понятие о древовидных структуры данных. Интернаука, (5-1), 9-12.

8. Umarov, S. A., & Akbarov, D. E. (2016). Working out the new algorithm enciphered the data with a symmetric key. Journal of Siberian Federal University. Engineering & Technologies, 9(2), 214.

9. Porubay O. V. Decision-making under conditions of definition and risk based on strict methods //Chemical Technology, Control and Management. – 2020. – Т. 2020. – №. 5. – С. 77-82.

10. Порубай О. В., Амиров А. Р. Проблемы принятия решений в условиях определенности и риска на основе строгих методов //Universum: технические науки. – 2021. – №. 6-1. – С. 32-33.

11. Азимов, Р. К., Шипулин, Ш. Ю., Холматов, У. С., Абдуллаев, Т. А., & Исмоилов, Х. А. (2016). Морфологический метод структурного проектирования оптоэлектронных преобразователей на основе полых и волоконных световодов (ОЭГТВС). In Современные материалы, техника и технологии в машиностроении». III Международная научно-практическая конференция (pp. 15-19).

12. Шипулин, Ю. Г., Рустамов, Э., Абдуллаев, Т. М., & Мейлиев, С. Н. (2019). Интеллектуальный оптоэлектронный датчик температуры с волоконно-оптическими элементами. In Проблемы получения, обработки и передачи измерительной информации (pp. 248-253).

13. Шипулин, Ю. Г., & Абдуллаев, Т. М. (2020). Состояние и развитие интеллектуальных оптоэлектронных преобразователей перемещений на основе волоконных и полых световодов. Universum: технические науки, (5-1 (74)), 5-9.

14. Абдуллаев, Т. М. (2021). Оптоэлектронное устройство сортировки сельскохозяйственной продукции.

15. Шипулин, Ю.Г. , & Мейлиев, С.Н. (2022). Состояние и развитие оптоэлектронных дискретных преобразователей перемещений на основе волоконных и полых световодов. Oriental renaissance: Innovative, educational, natural and social sciences, 2 (Special Issue 4-2), 1201-1208.

16. Tolipov, N., Xudoynazarov, Q., & Munavarjonov, S. (2023). Об одной некорректной задаче для бигармонического уравнения в полушаре. Research and implementation.

17. Tolipov, N., Isaxonov, X., & Zunnunov, M. (2023). Shar tashqarisidagi soha uchun garmonik davom ettirish masalasi. Research and implementation.

18. Isaqovich, T. N. (2023). Chorak doira tashqarisida bigarmonik tenglama uchun nokorrekt qo ‘yilgan masala. Talqin va tadqiqotlar ilmiy-uslubiy jurnali, 1(18), 73-83.

19. Siddikov, I. X., & Umurzakova, D. M. (2021, November). Configuring Smith Predictor Parameters for a Variable Line Feature. In 2021 Dynamics of Systems, Mechanisms and Machines (Dynamics) (pp. 1-8). IEEE.

20. Siddikov, I. X., & Umurzakova, D. M. (2020, November). Synthesis algorithm for fuzzy-logic controllers. In 2020 Dynamics of Systems, Mechanisms and Machines (Dynamics) (pp. 1-5). IEEE.

21. Umurzakova, D., Siddikov, I., & Bakhrieva, H. (2020). ADAPTIVE SYSTEM OF FUZZY-LOGICAL REGULATION BY THE TEMPERATURE MODE OF THE DRUM BOILER. IIUM Engineering Journal, 21(1), 182-192.

22. Umurzakova, D. (2021). System of automatic control of the level of steam power generators on the basis of the regulation circuit with smoothing of the signal. IIUM Engineering Journal, 22(1), 287-297.

23. Umurzakova, D. M. (2020). DEVELOPMENT OF MODELS AND ALGORITHMS FOR STUDYING THE DYNAMICS OF MULTIDIMENSIONAL SYSTEMS WITH PULSE-WIDTH MODULATION. In САПР и моделирование в современной электронике (pp. 59-62).