Impact Factor: 9.2 ISSN-L: 2544-980X

DIGITAL DATA SECURITY IN BLOCKCHAIN NETWORKS

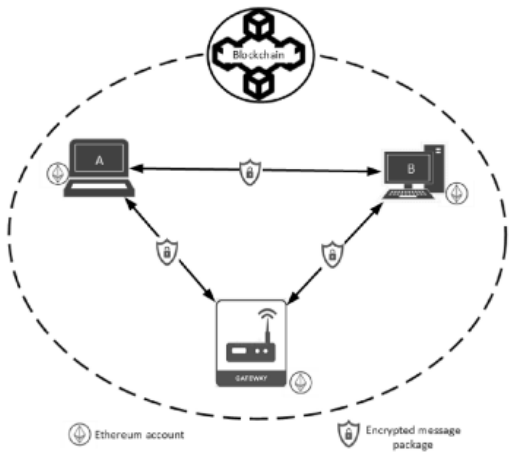
Inoyatov Ogabek Ibodullayevich
Tashkent University of Information Technologies named after Muhammad al-Khorazmi
Abduvositov Khumoyun Fakhriddin ogli
Student of Fergaana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi

Abstract: *This article explores the important problem of ensuring digital data security in blockchain networks. Blockchain, as a decentralized system for storing and transmitting information, has become an integral part of the modern digital world and has found wide application in various industries. However, despite their reliability and integrity, blockchain networks are also susceptible to data security threats.*

Key words : *Blockchain, digital security, hashing, encryption, electronic signatures, smart contracts, security threats, attacks 51.*

INTRODUCTION:

Figure 1



MAIN BODY

System model: From Fig. 1, given a message package ***x*** to be transmitted from a given node say ***A*** to another say ***B*** through a transparent private network of Ethereum blockchain, with ***A*** and ***B*** having Ethereum address of EA_A and EA_B respectively. We presumed that both ***A*** and ***B*** are registered and administered through an administrative node referred here as the gateway.

However, the gateway has no significant influence during communications between ***A*** and ***B***. Thus, interaction between ***A*** and ***B*** is absolutely peer-to-peer and distributed.

Software-based security solutions encrypt the data to protect it from theft. However, a malicious program or a hacker could corrupt the data to make it unrecoverable, making the system unusable. Hardware-based security solutions prevent read and write access to data, which provides very strong protection against tampering and unauthorized access.Digital technology has redesigned many aspects of our lives, and one of the most significant developments in this area is blockchain. Blockchain is a decentralized system that facilitates the storage and exchange of information without central control. It has found applications in a variety of areas, from financial transactions to healthcare and government registries. However, it is important to understand that digital data security in blockchain networks is a priority, and in this article we will look at key aspects of this topic.

Data security is the process through which an organization protects its digital information from unauthorized access, use, modification, corruption, exploitation, loss, and theft. It is an essential component of cybersecurity that involves implementing tools and measures to ensure the confidentiality, integrity, and availability of data.

The role of blockchain in the modern world

Blockchain security refers to the combination of cybersecurity principles, tools, and best practices in order to mitigate risk and avoid malicious attacks and unauthorized access while operating on blockchain networks.

While all blockchains run on distributed ledger technology (DLT), not all blockchains are functionally the same or equally secure. While both public and private blockchains have their own sets of advantages and disadvantages, their security models are fundamentally different due to the open versus closed nature of their networks.

Maintenance and development of public blockchains

Public blockchains often have associated organizations dedicated to advancing development and community engagement, such as the Ethereum Foundation. Even Bitcoin, created by the anonymous entity Satoshi Nakamoto, has a dedicated team of maintainers responsible for continuously updating and improving the Bitcoin Core software. Like any software, it is a “living” thing that requires regular maintenance and updates to address bugs and adapt to new circumstances. Any proposed changes to the core network must still be accepted by consensus. In Bitcoin, this is known as a Bitcoin Improvement Proposal or BIP. Anyone — not just maintainers — can propose a BIP.

The application of blockchain has expanded to many industries such as finance, logistics, healthcare, and even government data management. For example, in the medical field, blockchain can be used to store medical records and ensure that only authorized persons have access to them. However, despite all the advantages of blockchain, its

security requires special attention. Principles of data security in blockchain networks Data security in blockchain is based on four main principles: reliability, confidentiality, integrity and availability.

1. Reliability: This principle means that data on the blockchain must be protected from tampering and tampering. This is achieved through the use of cryptographic methods and consensus algorithms, which require the consent of the majority of network participants to make changes to the blockchain.

2. Confidentiality: It is important to maintain data confidentiality, especially when personal or sensitive information is involved. Blockchain networks can use encryption techniques to protect data at the storage and transmission level.

3. Integrity: This principle ensures that data remains unchanged and reliable. Hash functions are widely used to ensure the integrity of data blocks in the blockchain.

4. Availability: Blockchain should always be available to users when needed. This requires effective network management, as well as protection against attacks aimed at shutting down blockchain nodes.

Types of blockchain security breaches

Blockchain vulnerabilities and security breaches can be broadly broken down in three distinct categories: ecosystem vulnerabilities, attacks on smart contracts and protocols that operate on top of the blockchain, and attacks on popular infrastructure (like wallets) and users. It’s important to note that this is not an exhaustive list of all the possible types of vulnerabilities.

Cryptographic methods for ensuring data security in blockchain networks Cryptography plays an important role in ensuring data security in blockchain networks. Here are a few cryptographic methods used to protect data on the blockchain:

1. Hashing: Hash functions convert data into a fixed set of characters (hash) that is unique for each data set. This allows even the slightest changes in data to be detected, since any change will result in a change in the hash.

2. Encryption: Symmetric and asymmetric encryption are used to protect data at the transmission and storage levels. Asymmetric encryption, for example, is used to sign transactions on the blockchain, ensuring the authentication of participants.

3. Electronic Signature: Electronic signatures are used to confirm the authorship of transactions and provide authentication and integrity of data on the blockchain.

4. Smart Contracts: Smart contracts include the logic and rules that must be executed on the blockchain network. They also use cryptography to provide security and automate the execution of agreements between network participants. Every action performed within a smart contract must be signed and verified cryptographically to ensure reliability and security.

Threats to Data Security in Blockchain Networks Despite the high level of security that blockchain provides, there are threats that can put data and network participants at risk. Some of them include:

1. 51% attack: This is an attack in which attackers gain control of more than half of the network's computing power. This may allow them to manipulate the data.

2. Application level attacks: Malicious smart contracts or applications can create risks for network participants, leading to loss of funds or data leakage.

3. Social Engineering: Attackers may try to manipulate network participants to gain access to their private keys or other sensitive information.

4. Key Sharing: Losing access to private keys can result in complete loss of access to funds or data on the blockchain. Such situations require careful key management and backup.

CONCLUSION

Blockchain provides many benefits in the area of digital data security, but this does not mean that the system is completely secure. It is important to consider specific threats and implement appropriate security measures such as encryption, electronic signatures, access control and network monitoring. Only with the right combination of technical methods and attention to social and organizational aspects can complete data security be ensured in blockchain networks.

REFERENCES

1. Saminjonova Z. I. Q., Abduvositov X. F. O. G. L. YOLG ‘IZLIK HODISASINING NAZARIY TAHLILI //Oriental renaissance: Innovative, educational, natural and social sciences. – 2022. – Т. 2. – №. 10-2. – С. 368-375.

2. Юлдашев Ф. А., Юлдашева М. Б. Гносеологические аспекты концепции познания аль-Фараби в формировании ответственности личности //Социальная, профессиональная и персональная ответственность личности в современном обществе. – 2020. – С. 63-67.

3. Юлдашев Ф. А. Концепция познания аль-Фараби в истории философии //ФИЛОСОФИЯ ИННОВАЦИЙ И СОЦИОЛОГИЯ БУДУЩЕГО В ПРОСТРАНСТВЕ КУЛЬТУРЫ: НАУЧНЫЙ ДИАЛОГ. – 2020. – С. 389-393.

4. Юлдашев Ф. А., Юлдашева М. Б. Экзистенциональные проблемы изучения одиночества //Материалы международной конференции “Проблемы психологического благополучия”. УРГПУ Екатеринбург. Стр. – 2021. – С. 281-284.

9. Юлдашев Ф. А., Юлдашева М. Б. Гносеологические аспекты концепции познания аль-Фараби в формировании ответственности личности

//Социальная, профессиональная и персональная ответственность личности в современном обществе. – 2020. – С. 63-67.

10. Temirxon E. et al. Yuzni Aniqlash Algoritmlarini Qiyosiy Tahlil Qilish //Intellectual Education