Volume 1 Nomor 2 May 2024
E-ISSN: 3047-2903

https://economic.silkroad-science.com/index.php/IJAIFD

SECURITY ISSUES IN BLOCKCHAIN TECHNOLOGY

Zokir Mamadiyarov
DSc, Professor, International School of Finance and Technology Institute, Uzbekistan
zokir.mamadiyarov@gmail.com

Article Info

Article history:
Received May 10, 2024
Revised May 20, 2024
Accepted May 29, 2024

Keywords:
Blockchain, security, cyber-attacks, digital currency, authentication, bitcoin

ABSTRACT

Hailed as a revolutionary innovation, blockchain technology has attracted a lot of attention from various industries due to its decentralized and immutable nature. It serves as the underlying technology for cryptocurrencies such as Bitcoin and Ethereum, providing transparency, decentralization and security. However, blockchain technology is not legally protected from security issues, and potential solutions to address security issues related to blockchain technology are being discussed . Overall, this article provides an overview of blockchain technology and its security issues.

Corresponding Author:
Zokir Mamadiyarov
DSc, Professor, International School of Finance and Technology Institute, Uzbekistan
Email: zokir.mamadiyarov@gmail.com

INTRODUCTION

Blockchain technology has emerged as a force with the potential to revolutionize many industries, from finance and supply chain management to healthcare and beyond. Its decentralized, transparent and immutable nature has attracted attention as a solution to various problems faced by traditional centralized systems. Explore the relevance of blockchain technology in today's world, its transformative impact on networks and its potential to power various aspects of the economy worldwide.

Blockchain is a technology that allows system participants to securely transfer assets to each other without an intermediary. For example, records of money statements can be stored on the blockchain. In cryptocurrencies, the blockchain is used to record information about who has transferred virtual money, to whom and how much. However, other assets can also be stored on the blockchain. In general, everything that can be written on paper can also be written on the blockchain, with only one difference - it is impossible to replace and falsify records on the blockchain.

Literature Review. Blockchain technology, a decentralized and secure digital ledger, has a wide range of applications in various fields (Mahmood, Z. (2021)) It is based on a set of distributed blocks with unique hash codes that ensure data immutability and security (Rahmani, MK (2022)). The potential of the technology is evident in its ability to support

low-cost decentralized distributed data management, making it a key breakthrough in the next generation of ICT (Kogure, J., Kamakura, K., & Shima, T. (2017)). However, there are limitations such as scalability and energy consumption (Sharma, S., Rosmin, P., & Bhagat, A. (2021)). Despite these challenges, the future of blockchain technology looks promising, with ongoing research to address these challenges.

While blockchain technology is revolutionary, it is not without security and privacy issues. Oksiiuk (Oksiiuk, O., & Dmyrieva, I. (2020)) and Huynh (Huynh, T.T, Nguyen, T.D, & Tan, H. (2019)) both emphasize the need to address these issues, the latter and suggests the use of group signature and zero-knowledge schemes as potential solutions. Alsuhaimi (Alsuhaimi, AH, & Alzahrani, S. (2021)) highlights the importance of addressing these issues in various blockchain applications such as banking, healthcare, and the Internet of Things. Gupta (Gupta, N. (2019)) also emphasizes the need to systematically investigate security threats and real-world attacks in blockchain systems and develop improvements to mitigate these risks.

Result and Discussion

A clear example of the blockchain idea is the company Ethereum. It was founded by Vitaly Buterin, a 19-year-old programmer who was born in Kolomna, Russia, and now lives in Canada. The platform is designed to create applications on the blockchain. Today, Ethereum is valued at $703 billion.

The structure of blockchain technology consists of the following seven principles (Figure 1):

Figure 1. Seven principles of organizing blockchain technology

Source: Compiled by the author.

Network integrity

Trust is created within the system, it is not transmitted from the outside. Participants are honest in their words and deeds, respect the interests of others, are ready to answer for the consequences of their actions, and their decisions are transparent. Integrity is codified at each stage of the process and shared among all participants, i.e. not owned by one person.

Distribution of loads

There is no single way to delete it. Energy costs are distributed over the entire grid. None of the participants can turn off the system. If the central authority blocks a person or group, the system will continue to work. If about half of the network wants to gain control of the network, the rest will watch what happens.

The system treats all stakeholders equally. Satoshi Nikamoto programmed the application in such a way that those who contribute to the development of the application are encouraged. An active user of the network will receive 50 bitcoins for each completed block after 4 years. After another 4 years - 25 bitcoins, then 12.5, etc

Security: Every network participant needs to use encryption. Security measures are built into the network. They ensure confidentiality and preservation of the original. The user will have two keys: one for encryption and one for decryption. This method is called "public key infrastructure" (PKI).

Privacy: People need to be in control of their personal information. They should have the right to distribute exactly what information belongs to them, when, how and in what volume.

Protection of rights: The rights of owners are transparent and reinforced. Transaction timing and PKI not only prevent double spending, but also record ownership of every bitcoin on the network. We will only be able to trade in what we own. Apart from Bitcoin, it can be anything of value, including intellectual property.

Inclusion: An economy works better when it works for everyone. This means lower barriers to entry. Anyone with a cell phone can participate in the market as a producer or consumer. Satoshi proposed a method called "simplified payment verification" (SPv).

So, to what extent are the possibilities of blockchain technologies in terms of ensuring information security? We will try to answer this question in as much detail as possible below.

Blockchain and Information Security Issues: New Blockchain technologies are contributing to a revolution in the field of information security. In addition, the introduction of blockchain technologies will help protect data in personal messages, business and consumer websites and applications.

Blockchain is a relatively new technology popularized by its first successful experiment, Bitcoin. Its unique features have led to the emergence of several startups, which specialize in blockchain technologies and have taken the field of information security to a completely new level.

Blockchain is a technology that helps encrypt the actions taken with a file or object into a file-specific code. This encryption cannot be removed, changed or circumvented, which makes the records of the files completely transparent: it is always known what transactions were made with it, when and by whom. This decentralized, autonomous approach to information security opens up new opportunities in Internet security that many industries, from business to social networks, have long anticipated.

First, and most importantly, blockchain provides an opportunity for the protection of private messages. Startups like Obsidian are designed to use blockchain technology to protect personal information in chats, messengers and social networks. Nowadays, it is known to everyone that messengers are used not only for communication, but also for making payments. Vulnerabilities in Facebook Messenger and WhatsApp are that they use sparse encryption and do not provide adequate protection of metadata, including the sender's identity, email address, and other log-in information. data too.

Protected messages:

Obsidian Messenger plans to secure user metadata using blockchain. The user will not need to use email or any other authentication information to use the messenger. Metadata will be distributed randomly throughout the book and, therefore, cannot be collected at a single point of possible corruption. They are also planning to introduce their own token to be used as a means of payment within Obsidian. This project is still under development, but other messengers may follow this scheme and protect their users' data in a similar way.

Currently, the common way to add users to any system is to use a unified approach using logins and passwords. But a company like REMME is a new development focused on using a blocker to identify devices and users and modify them.

The main strength of blockchains is to decentralize systems and random communications between files and data in general. In addition, passwords are invented, stored, and entered by humans, allowing for human error. REMME attempts to prevent errors that may be made by the user during device and user authentication.

The principles of secure authentication mechanisms that this company intends to build are based on the use of a distributed public key infrastructure. Decentralization of public keys reduces their vulnerability to attacks, which a centralized password management system cannot do. Each device is issued its own SSL certificate based on blockchain technology, which prevents the use of fake certificates by criminals.

Startups like REMME allow businesses to better protect their commercial data, while managing the data and giving access to their employees. In cases of internal violations, blockchain technology helps the company to find the employee who committed the violation. REMME is in development, just like Obsidian, but there are many more such ventures to come.

Repelling Cyber Attacks: Finally, blockchain provides many opportunities to detect and repel hacking attacks on major websites on centralized servers.

As a result of such attacks, users' access to the websites of PayPal, Twitter and Spotify was blocked. The problem is that current DNS servers lack security because they store access keys on a single server and rely too heavily on caching. Startups like Guardian and Nebulis are aiming to change that by using a distributed network of blockchain-based keys and keywords.

Ultimately, blockchain protects servers from hacker attacks and makes them an impregnable fortress.

Blockchain is undoubtedly the most promising discovery in the field of information security of the last decade. We hope that this will revolutionize the development of information security systems and provide a secure Internet for many years to come.

Security measures are implemented in the network in such a way that it has no common point of denial, not only confidentiality, but also non-repudiation and authentication. Anyone who wants to participate in the system must use encryption - it is not negotiable, and the consequences of careless actions are felt only by the person who made them.

Hacking attacks, identity theft, fraud, cyberbullying, phishing, spam, malware, and ransomware are all threats to human safety in society. Rather than making many processes transparent and making human rights violations more difficult, the early Internet era made individuals, institutions, and economic activity less secure. The average Internet user often relied on simple passwords to protect email and accounts because ISPs or employers did not require stronger passwords. It should also be said that digital currency is not stored in a simple file. It is reflected in transactions marked with a cryptographic hash . Users will have cryptocurrencies for their money and transact directly with each other. For such security, it is necessary for each of them to be responsible - to reliably protect the private keys. This is where safety standards come into play. The Bitcoin blockchain operates on the well-known and well-developed SHA-256 encryption standard issued by the US National Institute of Standards and Technology and adopted as the federal standard for information processing. The complexity of repeating the multiple mathematical calculations required to find a block solution requires the computing device to spend a lot of electricity to solve the problem and generate new bitcoins. Some other algorithms use much less energy.

We believe that any economy works best when it works for everyone. This means lowering the barriers to participation. This means not redistributing capital, but creating a platform for redistributed capitalism . The early internet era created many wonders for many people. However, as mentioned above, a large part of the world's population remains disconnected from the system, with no access to technology, finance, or economic opportunities. Moreover, the hope that the new means of communication would bring prosperity to all was not fulfilled. Yes, the Internet has allowed companies in developed countries to provide jobs to millions of people in developing economies. It lowered the barriers to entering the market for many entrepreneurs and provided new opportunities and access to basic information to the low-income segments of the population (Zakir Toshtemirovich Mamadiyarov. 2022.).

We believe that blockchain technology is a technology capable of protecting everyone's rights and humanity. The global financial services industry is currently plagued with many challenges. It is quite outdated because it is lagging behind the highly dynamic digital world and is therefore based on slow and unreliable technologies left over from the last century. It is a monopoly, denying billions of people access to basic financial instruments. It is centralized and therefore susceptible to information leakage and other attacks and denials. It is monopolized and thus tends to support the status quo and discourages innovation. Blockchain allows innovators and entrepreneurs to solve these and many other problems while finding new ways to create value on this powerful platform. Global finance professionals should consider the following ideas related to blockchain:

Check . For the first time in history, different entities can transact and conduct business without knowing or trusting each other. Verification of identity and establishment of trust has ceased to be the right and privilege of the financial intermediary. Moreover, from a financial services perspective, a deed of trust takes on a new meaning. Blockchain can establish a trusting relationship by verifying each party's exact identity and solvency based on transaction history (on the blockchain), reputation value (based on aggregated opinions), and other macroeconomic indicators when needed.

Value . A blockchain clears and regulates peer-to-peer transfers of value on the network, doing so continuously, so its ledger is always up-to-date. If the banks had taken advantage of this opportunity from the beginning without changing their business model , they would have saved about 20 billion dollars in operating costs per year - these calculations belong to the Spanish bank Santander, but the real numbers are much higher. Due to devaluation, banks would be able to provide greater access to financial services, markets and capital to private and corporate clients in underserved communities. It was considered beneficial not only for market leaders, but also for start-ups around the world. Anyone can join the world's financial flows from anywhere with just a smartphone and an internet connection.

Speed . Currently, it takes seven days to settle the cash flow, two to three days to settle a stock transaction, and 23 days for a bank loan. The SWIFT network transfers fifteen million payments a day between tens of thousands of financial institutions around the world, but takes days to settle and clear them. The same thing happens with the ACH (Automated Clearing House) system, which transfers trillions of dollars a day in the US. It takes an average of 10 minutes to settle and clear all transactions made on the Bitcoin network at this time. Other blockchains are even faster, and modern innovative solutions such as the Bitcoin Lightning Network aim to increase the size of the Bitcoin blockchain by reducing settlement and clearing times to fractions of a second. "In the banking system, where the money sender is in one network and the receiver is in another network, money can pass through many registers, intermediaries, transit areas and literally get lost on the way. In fact, the shift to a more instantaneous and cost-free form of value transfer frees up capital that has long remained in an intermediate state; This, of course, does not please the middlemen who profit from the funds "on the road".

Risk management. Blockchain technology promises to eliminate several different types of financial risk. First, regulatory risk is the risk that the payment will not go through as a result of any error in the process of regulating the transaction. Second, counterparty risk is the risk that the other party will declare default before settlement of the transaction. Finally, the most serious systemic risk is the sum of all major counterparty risks in the system.

Value innovation . The Bitcoin blockchain was created to transfer bitcoins, not to work with other financial assets. However, it is an open-source technology that encourages experimentation. Some innovators create separate blockchains, i.e. altcoins, that are not intended for bitcoin payments, but for other purposes. Sidechains are blockchains that differ from the Bitcoin blockchain in terms of capabilities and functionality, but use Bitcoin's computer infrastructure and advanced network without compromising its security. Sidechains communicate with the blockchain using a two-

channel pin, a cryptographic means of transferring assets to and from the blockchain without the involvement of a third party. There are also innovators who seek to exclude the use of bitcoin and other tokens altogether by creating trading platforms on private blockchains. Financial institutions are using blockchain technology to record, exchange and sell assets and liabilities, which may eventually replace traditional exchanges and centralized markets, changing the way we think about value and how we trade it.

Open source code. The financial services industry is a vast technological complex of outdated systems that can fail at any time. It is difficult to improve technologically because every innovation requires the ability to be reversible. And blockchain, being an open-source system, can constantly change, evolve, and improve based on network compromises.

These advantages - certification, very low cost, instantaneous speed, reduced risk, high innovation, adaptability - will not only affect payments in the future, but also securities transactions, investment banking, accounting and auditing, venture capital. , can change insurance, business risk management, private banking and other fundamentals of the network.

People should be in control of their own information. Everyone has the right to decide what, when, where and in how much detail about their personality to share. Respecting the privacy of personal data and protecting the security of personal data are not the same thing. We need both. By eliminating the need to trust each other, Satoshi Nakomoto thus eliminated the need to know the other party's identity well in order to interact with him. Privacy is a basic human right and the foundation of a free society. Over the past two decades since the advent of the Internet, central databases, both public and private, have collected a wide variety of confidential information about private individuals and organizations, including without their knowledge. People everywhere fear that corporations will create some kind of cyberclones , scouring the digital world in search of information . And in the blockchain, participants can maintain a certain level of anonymity at will - they are not obliged to report any additional information or store this information in a central database. The importance of this situation cannot be underestimated. There is no personal data storage in the blockchain . Blockchain protocols allow you to choose the desired level of anonymity for each specific transaction or situation. In this way, we better manage our electronic copies and their interactions with the world.

CONCLUSION

In conclusion, blockchain technology is highly relevant in today's world and offers transformative solutions to various problems faced by traditional centralized systems. Its decentralized nature, enhanced security, efficiency and potential for financial inclusion make it a powerful vehicle for empowerment and innovation across industries. Blockchain will continue to evolve and become mainstream, growing in importance and shaping the future of decentralized and transparent ecosystems around the world.

We offer potential solutions to solve existing problems in the study of security issues related to blockchain technology:

- The development and adoption of new consensus algorithms that reduce PoW and PoS vulnerabilities can increase blockchain security. Consensus mechanisms such as Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) offer alternative approaches that address scalability and security issues;
- Conducting thorough code reviews and applying formal verification techniques during smart contract development can identify and mitigate vulnerabilities. Additionally, establishing standardized security protocols and best practices for smart contract development can minimize the risk of exploitation.
- Developing a regulatory compliance framework specific to blockchain technology can facilitate compliance with existing regulations, taking into account the unique characteristics of decentralized systems. Collaboration between regulators, industry stakeholders and technologists is essential to create clear guidelines and ensure regulatory clarity;
- Integrating dynamic data management solutions that provide selective deletion or encryption of data while maintaining blockchain immutability can solve data retention and privacy compliance issues such as GDP

REFERENCES

[1]. Mahmood, Z. (2021). Blockchain Technology. Advances in Data Mining and Database Management
[2]. Rahmani, MK (2022). Blockchain Technology. Blockchain Technology and Computational Excellence for Society 5.0
[3]. Kogure, J., Kamakura, K., & Shima, T. (2017). Blockchain Technology for Next Generation ICT.
[4]. Sharma, S., Rosmin, P., & Bhagat, A. (2021). Blockchain Technology Blockchain Applications in IoT Security
[5]. Oksiiuk, O., & Dmyrieva, I. (2020). Security and privacy issues of blockchain technology. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 1-5.
[6]. Huynh, TT, Nguyen, TD, & Tan, H. (2019). A Survey on Security and Privacy Issues of Blockchain Technology. 2019 International Conference on System Science and Engineering (ICSSE), 362-367.
[7]. Alsuhaimi, AH, & Alzahrani, S. (2021). Security and Privacy Issues of Block-Chain Technology.
[8]. Gupta, N. (2019). Security and Privacy Issues of Blockchain Technology. Studies in Big Data.
[9]. Zakir Toshtemirovich Mamadiyarov. 2022. Risk Management in the Remote Provision of Banking Services in the Conditions of Digital Transformation of Banks. In The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021). Association for Computing Machinery, New York, NY, USA, 311–317. https://doi.org/10.1145/3508072.3508119
[10]. Toshtemirovich, MZ INNOVATIVE APPROACHES OF REMOTE BANKING TYPES OF SERVICES IN THE PROCESS OF TRANSFORMATION OF BANKS TO E-COMMERCE. International Journal of Innovations in Engineering Research and Technology, 1-9.
[11]. Mamadiyorov, Z., Sultanova, N., Makhmudov, S., Khamdamov, SJ, Mirpulatova, L., & Jumayev, A. (2023, December). The Impact of Digitalization on Microfinance

Services in Uzbekistan. In Proceedings of the 7th International Conference on Future Networks and Distributed Systems (pp. 453-463).

[12]. Mamadiyarov, Z. (2019). Remote Banking Services and Development Prospects in Uzbekistan. International Finance and Accounting