International Journal For Technological Research In Engineering
Volume 10, Issue 9, May-2023 *ISSN (Online): 2347 - 4718*

SECURITY ASPECT OF BLOCKCHAIN

[1]ANSHUL BHARDWAJ, [2]PROF. PRATIBHA GAUTAM
[1]STUDENT, [2]ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
MAHAVIR SWAMI INSTITUTE OF TECHNOLOGY, SONIPAT, INDIA

Abstract— Blockchain technology is becoming increasingly attractive to the next generation, as it is uniquely suited to the information era. Blockchain technology can also be applied to the Internet of Things (IoT). The advancement of IoT technology in various domains has led to substantial progress in distributed systems. Blockchain technology is an innovative digital ledger system that records and verifies transactions in a secure and transparent manner. It functions as a decentralized database that stores information across a network of computers, making it resistant to tampering or alteration. The technology was initially developed for Bitcoin, the first decentralized cryptocurrency, but has since evolved into a versatile tool for various industries and applications. Its unique features, such as immutability, transparency, and decentralization, make it attractive for enhancing security and trust in digital transactions. Future directions for blockchain security are focused on enhancing the privacy and scalability of the technology. One approach is to develop more advanced cryptographic techniques, such as zero-knowledge proofs, to enable private transactions without compromising security. Another direction is to improve consensus algorithms that can handle a high volume of transactions while maintaining decentralization. Additionally, there is a need for better governance models that address potential issues related to regulation and compliance.
As blockchain technology continues to evolve, ongoing research and development will be critical for ensuring its security and sustainability in the future.
Keywords: - blockchain, security, IoT

1. INTRODUCTION

Blockchain technology is a distributed ledger system that allows for secure and transparent transactions without the need for intermediaries. It is a decentralized system that operates on a network of computers, making it difficult to hack or alter data. Blockchain technology has gained significant attention in recent years due to its potential to revolutionize various domains, including finance, healthcare, and supply chain management. However, the implementation of blockchain technology also raises security concerns that must be addressed to ensure its effectiveness. This research paper aims to provide an overview of blockchain technology and its importance in various domains while highlighting the significance of security considerations in blockchain implementations.

The significance of blockchain technology extends beyond just the realm of cryptocurrencies. It has the potential to transform various domains such as finance, healthcare, supply chain management, and more. In finance, blockchain can enable faster and more secure transactions while reducing costs. In healthcare, it can help in securely storing and sharing patient data. In supply chain management, it can ensure transparency and traceability of products from source to destination. The decentralized nature of blockchain also makes it a valuable tool for governance and voting systems. The importance of blockchain in various domains lies in its ability to provide secure and transparent solutions that enhance efficiency and trust among stakeholders.

The significance of security considerations in blockchain implementations cannot be overstated. As a distributed ledger technology that allows for secure and transparent transactions, blockchain is gaining traction across various domains such as finance, healthcare, supply chain management, and more. However, without proper security measures in place, the integrity of the data stored on the blockchain can be compromised. This can lead to fraud, theft, or other malicious activities that undermine the trustworthiness of the entire system. Therefore, it is crucial to address potential security vulnerabilities and implement robust security protocols to ensure the safety and reliability of blockchain implementations.

The objectives of this research paper on blockchain security are to provide a comprehensive overview of the significance of security considerations in blockchain implementations, explore the various security challenges and threats faced by blockchain technology, examine existing solutions and techniques for securing blockchains, and propose new approaches to enhance blockchain security. The paper aims to analyze the effectiveness of current security mechanisms and identify potential vulnerabilities that may compromise the integrity, confidentiality, and availability of blockchain systems.

Furthermore, this research seeks to highlight the importance of incorporating robust security measures in all stages of blockchain design, development, deployment, and maintenance. Ultimately, this paper aims to contribute to the advancement of secure and reliable blockchain systems.
Firstly, we will provide a detailed introduction to blockchain technology and its importance in various domains. We will discuss the significance of security considerations in blockchain implementations and how they play a crucial role

in ensuring the integrity and reliability of transactions.
Secondly, we will explore the different types of attacks that can compromise the security of blockchains, such as 51% attacks and Sybil attacks.

Thirdly, we will examine various security mechanisms that can be used to mitigate these risks, such as consensus algorithms and cryptographic techniques.

2. BLOCKCHAIN SECURITY AND COMPLIANCE

Successful adoption of any technology is dependent upon security compliance and risk. Doesn't matter what the technology is, security remains paramount. The blockchain paradigm is tamper-proof but not immune to hacks and security challenges. Monitoring the blockchain ecosystem is equally important as it is for other technologies. The cybersecurity measures apply to the blockchain as well. Furthermore, security becomes of utmost importance when working with big industries such as healthcare, finance, supply chain, and many more. Blockchain technology is secure, no doubt, but there are many issues that surface. There are many problems, such as regulatory compliance and data confidentiality. Notorious Hackers can find a flaw in the system and cause a loss of millions if not billions. The DAO hack was one such example. Even in the DAO hack, there was so much confusion and a lack of policies, that an ad-hoc committee was established much later. Thus, it becomes necessary for organizations to understand the security system of blockchain. In this blog, we will highlight more on blockchain security and compliance and how it can be managed.

How the Security differs in Blockchain types.
In order to build a successful blockchain application, you must determine which type of network is most appropriate for your enterprise. Blockchain networks are either public or private, which determines who can participate. Moreover, access to the networks is permissioned or permissionless, based on the way participants gain access to them.

Regarding reliability, private and permissioned networks are preferred for better security and compliance. In terms of compliance and regulation, private and permissioned networks are desirable. Decentralization and distribution can, however, be accomplished more effortlessly with public and permissionless networks.

The three pillars of blockchain security are:
Confidentiality
Data integrity
Availability of data

In the case of enterprise-grade solutions, there are a lot of legacy systems, and the input to the smart contract system is external. Ultimately, it's necessary to ensure that blockchain security and compliance frameworks are analyzed well, as technologies are changing fast.

The Four Types of Blockchain Security Attacks

Phishing Attacks
The attack is a way to get information about the individual. Wallet key owners receive emails that appear to come from an authorized source but are actually deceptive. Using fake hyperlinks, the emails request the end users for their credentials. This causes a loss for the users and of course for the blockchain network.

Routing Attacks
In routing attacks, hackers seize the data when it is being transferred to and from the internet service providers. The hackers split the blockchain network into separate parts and block the communication channel. The attacker's newly formed chains are discontinued once the attack is complete.

Sybil Attacks
A Sybil attack involves hackers creating and using many false network identities in order to overload the network and crash it. The node in a network has multiple active identities. The identities aim to gain majority power over the chain. The fake identities seem real to the outsiders making the system more vulnerable as it becomes difficult to find fault.

51% Attacks
51% of attacks are attained by renting minting hash from a third party. On a blockchain network when the mining power is exceeding 50% for a miner or group of miners. It is considered to control the network if you hold more than 50% of the power. While the likelihood of a 51% attack is relatively less, it isn't completely to be ignored.

Key Features of Security Software
Some of the key features of using security software for blockchain-compliant networks are:
Investigation and Monitoring
It is a feature that allows users to examine digital currency transactions. There is an automatic route detection to track transactions. The investigation and monitoring also involve risk assessment and further assign ratings.

Knowing Your Transactions (KYT)
With KYT, you can quickly analyze and investigate transactions. Besides providing information on blockchain addresses, KYT also includes information on their true identities. KYT does a critical analysis of the enterprise blockchain to identify fraudulent transactions.

Navigation Assistance
You gain consistent and precise knowledge of the source and destination of money with navigation assistance, which provides strong traceability and adjustable risk rules. The navigation assistance traces the blockchain path flow.

Virtual Asset Service Provider (VASP)
VASP monitors risk and ensures regulatory compliance. The VASP is essential when it comes to exchanges occurring between virtual assets. VASP helps you to become blockchain compliant as it verifies identity, tracks crypto activities, and enables law enforcement and regulations.

3. BLOCKCHAIN USE CASES

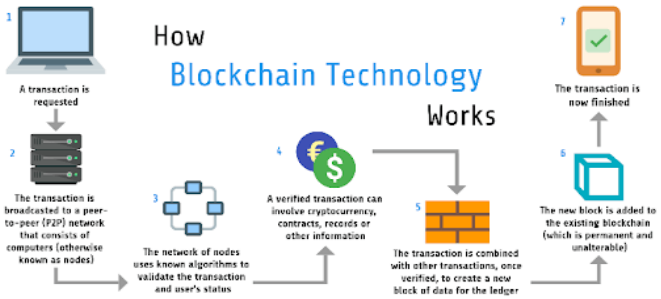
1 Cryptocurrency
Risk: Encrypted digital currencies identify the currency itself, but not its owner. Whoever holds the coin's encryption key owns the currency. This means that when a coin is stolen, it's gone—and you have no way of getting it back.
Solution: Storing your encryption keys in a FIPS-validated root of trust is critical to ensuring you own your keys and ultimately your cryptocurrency.

2 Smart Contracts
Risk: A smart contract is a computer program that describes an agreement with the ability to self-execute and enforce the terms of a contract. If the blockchain is breached, a smart contract can be altered, breaking the trust of the blockchain and removing the ability of two parties to conduct business without the need for a middleman.
Solution: Securely self-execute the terms of a contract with anonymous parties through strong authentication and storing your encryption keys in a hardware root of trust, ensuring the parties are properly identified and that no one can access your data.

3 Internet of Things (IoT)
Risk: The restrictions imposed by a traditional central-authority trust model have helped make the IoT vulnerable. Most notably Mirai-style botnets, which allowed hackers to easily take over thousands of IoT devices. Only protecting the IoT devices with default passwords allowed hackers to launch Distributed Denial of Service (DDoS) attacks.
Solution: Blockchain helps secure the IoT by providing a distributed trust model. The blockchain removes the single point of failure, in turn enabling device networks to protect themselves in other ways, for example by allowing the nodes within a given network to quarantine any nodes that start behaving unusually.

4. HOW DOES BLOCKCHAIN SECURITY WORK

In advanced times like today where everyone is equipped with technology, the security of our data has become a key concern. And especially when we are talking about an open network, point-to-point, distributed ledger system like blockchain, security becomes a topmost priority. So, in this tutorial, we are going to learn about what's under the hood when it comes to blockchain security. Here, we will understand both the theoretical and practical aspects of it.



UNDERSTANDING OF BLOCKCHAIN SECURITY
Blockchain is now a popular technology whose efficiency and potential are getting accepted and acknowledged worldwide. Up until now, we have been using blockchain mainly in cryptocurrency systems, smart contracts, and techniques related to the Internet of Things. However, with some already running and established systems like these, new domains like academics, finance, banking, and industries are showing interest in shifting their processes to a blockchain-based system in the near future.

With increasing demand and curiosity around blockchain, it becomes ever so important to have in-depth knowledge about how a blockchain system takes care of its security aspects. Security and privacy of blockchain become the most important part of its functioning because there is no point in adapting to a point-to-point network if it is not secure. Therefore, understanding the basics of security such as security concerns and properties will help us. It is of great help especially when you are part of a blockchain network or have taken up blockchain as a technology for your field.

The reason why the security and privacy of a blockchain network are so important is to keep the data in the ledger safe from theft and forgery. Blockchain claims to be the most secure, immutable, and incorruptible network, but is it really so? And if yes, how does it manage that?

The goal of a good security system for blockchain is to protect important data from falling into the wrong hands and to maintain trust within the network. Blockchain uses cryptography and hashing techniques to make sure it provides a 100% secure environment to its users. In the following sections, we will see how blockchain ensures a threat-free legitimate transaction network.

5. SECURITY ATTRIBUTES OF BLOCKCHAIN

In order to understand the concept of the security of blockchain, we need to know the key security attributes of a blockchain network. That is, what are the main focus points to make sure that a blockchain network is secure? So, let us go through these points one by one.

1. Integrity of transactions: Whenever there is a transaction taking place between two nodes in the blockchain, it's contents must be safe. No one should be able to access or change the contents of a transaction in the middle of the transition. That is, the integrity of the transaction should remain intact.

2. Tamper-resistance: Blockchain must be tamper-resistance. Meaning, no one should be able to tamper with both the objects within an active transaction or the historic data already stored in the blockchain blocks. This is made sure by the methods like SHA-256 hashing algorithm, Public-key cryptography, and Digital signature.

3. Consistency: Blockchain should achieve consistency of its ledger. By this, it means that the blockchain record should get updated at the same time on all the nodes. As we know, a blockchain network consists of a lot of nodes. Therefore, in a distributed network like a blockchain whenever a new block is added all the nodes should get instantly updated. This timely updating of blocks or records throughout the network is called consistency.

4. Access to network and data: Another important security aspect of the blockchain is for the users to be able to access data that is on the blockchain. And, also to have a properly running network system always. A user or node in the blockchain must get access to view the records saved on the ledger whenever they wish to.

5. Confidentiality of transactions: The whole point of having a robust security system in place for blockchain is to carry out point-to-point transactions without any third parties acting as intermediaries. So, the security of the content of these transactions becomes a topmost priority. Therefore, blockchain needs to maintain the confidentiality of such transactions.

6. Anonymity of the user: In a blockchain network it is not necessary for the users to know each other personally or reveal their real identity in order to participate in the network. A node or user can easily carry out transactions using the public address assigned to them. Blockchain users can keep their identity anonymous and still be a part of the network safely. Also, it is important to note that a user can have multiple pseudonymous addresses to ensure unlikability and prevent attacks.

7. Resistance to attacks: A blockchain network is susceptible to different kinds of attacks such as DDoS (Distributed Denial of Service) attacks, Double Spending attacks, and Majority (51%) Consensus attacks. A security system must be so designed that it can protect the ledger contents and transactions from such malicious attacks and forgery.

6. MAJOR SECURITY CONCERNS OF BLOCKCHAIN

While opting for or even designing a security solution for blockchain, there are four main security concerns that are kept in mind. If a security solution addresses all of these four corners, then it is said to be perfect for blockchain. Let us discuss the four key security concerns for blockchain in detail.

1. Confidentiality

The basic idea behind using a blockchain network is to be able to share information or important content between trusted users. In this scenario, the confidentiality of the content that we are exchanging becomes very important. Suppose Raj is a node on the blockchain network and so is Shalini. Raj wants to share his bank details with Shalini. Raj will expect the blockchain network is so secure that no one from the network should be able to access and tamper with this information in the middle of exchanging.

If the security system of the blockchain is not good enough, any third node from the network, says Rahul will access the information. Rahul will then know Raj's bank details and may even change the details and send them further to Shalini. Prevention from such scenarios to maintain the confidentiality of the data is a crucial security concern.

2. Integrity

Associated with confidentiality is another crucial security concern i.e., integrity of the data. By maintaining the integrity of data, we mean that it should not change in any way. The data sent by one user should reach the exact same state as the receiver. If a third party interferes in the middle and changes some parts of the information then its integrity is lost. To make sure that the integrity of the content being exchanged is retained, the proper security protocol is needed.

3. non-repudiation

By non-repudiation, we mean the inability to deny or take accountability for a transaction. This becomes an important security concern when someone denies sending a piece of information to another node. Or someone denies receiving any. This is a problem of unaccountability which we will not like to happen in a peer-to-peer network like blockchain.

The security procedures should also address the issue of non-repudiation. It is done by providing a proofing method for the transaction where both the sender and receiver have proof of the transaction.

4. Authentication

Another important security concern in the blockchain is the authentication of the users. Blockchain is a widespread network with a lot of users as participants. What can happen in such a case is that users can forge their identities to do fraud. To prevent this from happening, proper authentication of a user is necessary.

Cryptographic techniques like digital signatures make sure that no user can fake their identity to others. Only the authentic and authorized nodes can take part in transacting within a blockchain network.

7. CONCLUSION

Blockchain is just one of several evolving technologies that will support what others have called the Fourth Industrial Revolution. But unlike AI, the Internet of Things, and other more visible digital technologies, it is largely an invisible enabler. It is vital to safeguard enterprises and organizations from various fraudulent activities. The blockchain needs to be scrutinized more in the coming years as the technology is going to be adopted to a greater extent. For long-term viability, blockchain security monitoring and compliance services will be helpful for an organization. With appropriate security management, the infiltration in the ecosystem reduces too much extent. The existing challenges can be removed using correct mitigation strategies and partnering with a blockchain platform with accurate information about the blockchain system and its challenges. There should be more training for professionals, frequent code reviews, patching, and data integrity checks.

REFERENCE

[1] Z. Cai, Z. He, X. Guan, Y. Li Collective data-sanitization for preventing sensitive information inference attacks in social networks IEEE Trans. Dependable Secur. Comput., 15 (4) (2018), pp. 577-590, 10.1109/TDSC.2016.2613521 View article View in ScopusGoogle Scholar

[2] Z. Cai, X. Zheng A private and efficient mechanism for data uploading in smart cyber-physical systems IEEE Trans. Netw. Sci. Eng., 7 (2) (2020), pp. 766-775, 10.1109/TNSE.2018.2830307 View article View in ScopusGoogle Scholar

[3] C. Cai, J. Weng, X. Yuan, C. Wang Enabling reliable keyword search in encrypted decentralized storage with fairness IEEE Trans. Dependable Secur. Comput., 18 (1) (2021), pp. 131-144, 10.1109/TDSC.2018.2877332 View article View in ScopusGoogle Scholar

[4] X. Zhang, C. Xu, H. Wang, Y. Zhang, S. Wang FS-PEKS: lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial internet of things IEEE Trans. Dependable Secur. Comput., 18 (3) (2021), pp. 1019-1032, 10.1109/TDSC.2019.2914117 View article Google Scholar

IJTRE
Since 2013

