https://dx.doi.org/10.22161/ijaers.ncitsa.2025.21 ISSN: 2349-6495(P) | 2456-1908(O)

# A Review study on Blockchain Security in digital transactions

Ms. Preeti Sharma[1] , Shankar Kumar[2],Satish Kumar[3]

[1]Assistant Professor Department of Information Technology,Jaipur Engineering College & Research Centre, Jaipur
[2]Student Department of Information Technology, Jaipur Engineering College and Research Centre, Jaipur
Email: shankarkumar.it25@gmail.com
[2] Student Department of Information Technology, Jaipur Engineering College and Research Centre, Jaipur
Email : satishkumar.it25@gmail.com

Abstract—In today's digital world, online transactions are an everyday occurrence. From shopping and sending money to sharing information, these digital exchanges provide convenience but also come with significant risks. Ensuring the safety of these transactions is crucial, as a single security breach can lead to substantial financial losses and erode trust in the system. Blockchain technology presents a promising solutionby decentralizing control, making it much harder for hackers to manipulate the data. This paper explores how blockchain protects digital transactions, the challenges it faces, and its potential to transform various industries, such as finance and healthcare. Understanding blockchain security helps us appreciate its role in fostering trust and transparency in our online activities, ultimately making digital interactions safer for everyone involved.

Keywords—Data,Technology,Analysis ,blockchain

## I. INTRODUCTION

The rise of digital transactions has fundamentally changed how we conduct business and communicate. We rely on these transactions daily for activities like purchasing groceries, managing bank accounts, and conducting business deals. However, with the increasing reliance on digital transactions comes a growing concern for their security. Many traditional systems rely on a single authority, such as banks or payment processors, to manage these transactions. While this centralization simplifies processes, it also creates vulnerabilities. If hackers target a central authority, they can access sensitive information, steal funds, or disrupt services, leading to serious consequences for users.

Blockchain technology offers a solution to these security challenges. By decentralizing data,blockchain distributes control across a network of computers, meaning that no single person or organization can fully control the system. This decentralization significantly reduces the chances of interference from malicious actors. Furthermore, each transaction is recorded on a publicledgervisibletoallnetworkparticipants,which enhances transparency and allows users to verify the integrity of the data. In this synopsis, we will delve into how blockchain ensures the safety of digital transactions. We will highlight its benefits, such as improved security, reduced fraud, and increased trust among users. Additionally, we will discuss the challenges that must be addressed, including scalability,energyconsumption,andtheneedforclear regulationstoensureeffectiveintegrationintoexisting systems. Problem Addressed

## PROPOSED WORK

Blockchain security involves a combination of cryptography, consensus algorithms, and decentralized architecture to safeguard data and ensure trust in digital transactions. Key features include encryption of data, immutability, and decentralized validation processes.

ThreatstoBlockchainSystems:

1. PrivateKeyTheft:

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.21 ISSN: 2349-6495(P) | 2456-1908(O)

Blockchainreliesonprivatekeystoauthorizetransactions. If someone steals the key, they get full control over the assets or data, with no way to recover it. This usually happens through phishing, weak storage practices, or malware.

2. 51%Attack:

A blockchain network is secure as long as no single entity controls the majority of its computing power. But if a groupgainsmorethan50%ofthenetwork'sminingpower (hashrate), they can manipulate the ledger — such as double-spending coins or stopping transaction confirmations. This especially affects smaller blockchains.

3. SmartContractVulnerabilities:

Smart contracts are self-executing codes on theblockchain. If they have bugs or security loopholes, attackers can exploit them to drain funds or disrupt operations. Once deployed, these contracts are hard to modify, making preventive auditing crucial.

4. SybilAttack:

In this attack, a single entity creates many fake identities (nodes) in the network to gain influence or disrupt consensus. It can affect voting mechanisms and misleadthe network into false decisions.

5. PhishingAttacks:

Users may receive fake emails, websites, or wallet interfaces that mimic legitimate platforms. Once they unknowingly enter their credentials or private key, attackers gain access to their assets.

6. RoutingAttacks:

Since blockchain data is transmitted through the internet, attackers can intercept or delay data flow between nodes. This can lead to delayed transactions or network splits, especially in large-scale blockchain systems.

7. EndpointVulnerabilities:

Evenifftheblockchainitselfissecure,theappsandwallets usedtoaccessit(calledendpoints)maybeweak.

Attackers target mobile apps, browser extensions, or desktop wallets to exploit user-side vulnerabilities.

8. DoubleSpending:

In this scenario, an attacker tries to spend the same cryptocurrency twice. While blockchains use consensus to prevent this, it's still a risk on poorly designed or lightly secured networks.

9. RugPullsandScamProjects:

Especially in DeFi (Decentralized Finance), some developers launch tokens, raise investor funds, and then disappear with the money. These scams affect trust and result in heavy financial losses.

10. InadequateGovernance:

Decentralized systems often lack strong governance. Disputes, poor decision-making, or slow updates can weaken the network and open doors for exploitation.

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.21 ISSN: 2349-6495(P) | 2456-1908(O)

## CONCLUSION

As we continue to embrace digital transactions in our everyday lives, the need for strong security measures becomes increasingly clear. Blockchain technology has

emerged as a powerful tool for safeguarding these transactions in a decentralized environment. By enhancing transparency and reducing the risk of fraud, blockchaincanfostertrustamongusers,leadingtosignificantchanges in various industries like finance and healthcare. For instance, in finance, blockchain can streamline cross- border payments, making them faster and more affordable. In healthcare, it can secure patient records, ensuring that sensitive information is accessible only to authorized individuals.

However, challenges such as scalability, energy consumption, and the need for clear government regulations must be addressed for blockchain to reach its full potential. By focusing on improving blockchain security and tackling these challenges, we can work towards a safer and more trustworthy digital world. This focus is crucial for ensuring that everyone feels confident using digital transactions in their daily lives, paving the way for a more secure and efficient digital economy.

## REFERENCES

[1] Nakamoto,S.(2008).Bitcoin:APeer-to-Peer Electronic Cash System.
[2] Retrievedfromhttps://bitcoin.org/bitcoin.pdf

[3] Mougayar, W. (2016). The Business Blockchain: Promise,Practice,andtheApplicationofthe NextInternetInternetTechnology.Retrieved from https://www.forbes.com/sites/gilpress/2016/05/30 /the-business-blockchain-promise-practice-and- the- application-of-the-next-internet-technology/

**[4]** BlockchainRevolution:HowtheTechnology BehindBitcoinisChangingMoney,Business, and the World. Retrieved from https://hbr.org/2016/03/a-very-simple- introduction-to- blockchain