IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

A Study on Cyber Security Using Blockchain Technology

Mohan Vishal Gupta, Assistant Professor
College Of Computing Sciences And Information Technolog, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email id- mvgsrm@indiatimes.com

ABSTRACT: ***Blockchain is posing a threat to the established Internet's centralized trust infrastructure by advocating for a new approach to network architecture based on decentralization, transparency, and audibility. In a perfect world, blockchain would create an Internet that is decentralized, transparent, and more democratic. Blockchain, which is a trustworthy and decentralized database, has applications in a diverse range of industries, including the energy industry, agriculture, fishing, mining, recycling and reuse, air quality tracking, management of supply chains, and also the activities related to these. Several cybersecurity-related applications of Blockchain were examined in this paper. The author analyzed the three vulnerable areas of IT and the methods by which Blockchain has been shown to provide security. Furthermore, this study discussed that in the future, scholars should concentrate on a single Blockchain from which to construct cybersecurity apps to facilitate integration and consistency across solutions.***

KEYWORDS: ***Blockchain, Cyber Security, Cryptography, Distributed Denial of Service (DDoS).***

1. INTRODUCTION

The data format that blockchain generates has intrinsic safety features. Cryptography, decentralization, and consensus are the underlying ideas that make this system trustworthy and allow for honest exchanges to take place. Common to most forms of distributed ledger technology (DLT), blockchain organize their data into blocks, with each block containing a transaction or group of transactions. A cryptographic chain is formed as each subsequent block is linked to the ones that came before it. A consensus process verifies and approves every transaction inside each block, guaranteeing the validity and accuracy of every single one [1]. Distributed ledger technology (blockchain) facilitates decentralization via the involvement of users over a broad network. No one user or system component may compromise the integrity of the transaction log. But there are important ways in which blockchain systems diverge from one another in terms of safety.

Blockchain is an amazing new technology that will shake up multiple sectors by introducing better ways of doing things. It may be used in various settings since it is public, unchangeable, and decentralized. Cryptocurrencies helped propel the technology to the forefront of the public consciousness, but the technology has wide-ranging potential uses outside the financial industry. Blockchain technology is a group of cryptographically linked blocks [2]. Bitcoin's foundation is Blockchain, a distributed ledger software technology. It may be used to create a decentralized public ledger that is managed by a computer network, offering an alternative to the centralization that is typical of most currencies. Its foundational ideas are:

- Database Distribution System
- Peer-to-Peer Transmission

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

- Using a Pseudonym While Maintaining Transparency
- Immutability of Records
- Computational Logic

There is some flexibility in who can join a blockchain network and who has access to the information on that network. Common classifications for networks include "public," "private," "permission," and "permission less," each of which outlines the rules for accessing the network.

Cybersecurity refers to the process of safeguarding computer systems and networks against malicious cyberattacks that seek to steal money or private information by gaining unauthorized access to, altering, or destroying digital data. As more and more of our lives grow dependent on digital data and transactions, people must take extra precautions to ensure their safety. Malware such as viruses, Trojans, rootkits, etc., are already used in cyberattacks. Phishing, Man in the Middle (MITM), Distributed Denial of Service (DDoS), SQL Injection, and Ransomware are all prevalent forms of cyberattacks.

Simply said, a blockchain is a "distributed ledger or database" that records all transactions involving all parties involved. Each block in the chain of blocks that make up the blockchain may be thought of as a page in a ledger. As miners unearth more blocks, they are added to the growing chain. Cryptographic communication is used to broadcast each transaction across the network, and miners compete to amass the most transactions before verifying them using "proof-of-work" and adding them to a new block. Mining pools would compete to produce these blocks. A decentralized public ledger is created when a successful block is added to the Blockchain and a fresh copy of the transaction is broadcasted to the existing system. Although miners are rewarded for their efforts in verifying transactions and adding new transactions to the Chain, this is not their only motivation [3].

2. DISCUSSION

Blockchain makes it simple to safely access, distribute, and save digital information. In addition, all financial dealings are encrypted using cryptography. It's a great way for banks to increase their already stellar levels of safety and openness [4]. Blockchain technology may help improve online safety in these ways:

- Many individuals have many social media accounts, and most of them use passwords that are easy to guess. The vast amounts of metadata generated by social media conversations are a target for hackers.
- Since blockchain technology is more secure than end-to-end encryption, it may be utilized to create a universal security protocol. In addition to securing private conversations, it may facilitate communication across different messaging apps by establishing a single API architecture.
- There have been instances of hackers breaking into mainframes through peripherals. Despite the popularity of home automation systems, there is still a risk that insecure

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

Internet of Things (IoT) equipment, such as smart switches, would let hackers into the house.

- By decentralizing their management, these types of systems and individual devices may be made more secure with the use of blockchain technology.
- Blockchain technology may assist stop Distributed Denial of Service (DDoS) assaults by decentralizing the system for domain names.
- As more and more information is created every day, putting it in a concentrated location might make it open to hacking attempts that target a single weak spot. It will be very difficult for criminals to get access to data storage systems if the information is stored in a decentralized manner utilizing blockchain [5].
- Patching, installing software, and updating firmware are all examples of operations that may be validated using blockchain technology. Data in transit may be encrypted using blockchain technology to prevent unwanted access [6].

Since its inception, blockchain technology has been developed to provide the greatest levels of data integrity and transparency. Since blockchain technology automates digital data, human error is mitigated or eliminated [7]. Blockchain technology has the potential to significantly contribute to the battle against cybercrime, which is the biggest danger to businesses today. Blockchain technology's intrinsic decentralization has several potential uses, one of which is improving cyber security. Blockchain prevents data manipulation by automatically referencing and locating the nodes on the network that has the incorrect record [8].

2.1.Cybersecurity Applications of Blockchain Technology:

- *IoT Security*:

As AI and IoT find more and more uses, protecting sensitive information and infrastructure from malicious actors has been an ongoing need. One possible use of Blockchain for preserving IoT cybersecurity is the application of device-to-device encryption to safeguard information exchange, key management approaches, and verification [9].

- *The reliability of software downloads:*

To stop malicious programs from attacking the computers, blockchain may be used to validate updates and installations. The blockchain stores hashes, which may then be compared to new software identifiers to ensure download authenticity [10].

- *Security during Data Transmission:*

By encrypting the data in transit, it will also be safe from public scrutiny.

- *Critical data storage that is not centralized:*

Blockchain-based storage solutions assist establish decentralized storage, which helps preserve electronic information in light of the continuous growth in the amount of data created every day.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

- *Mitigating Distributed Denial of Service (DDoS) Attacks:*

DDoS assaults, which try to interrupt the flow of services by generating an overwhelming volume of Internet traffic, are now one of the most common forms of malicious cyber activity. Blockchain, because of its immutability and cryptographic capabilities, has the potential to be an efficient defense mechanism against these threats.

- *Domain Name System (DNS) security:*

The Domain Name System, often known as DNS, functions in a manner very similar to that of a public directory in that it connects domains to their respective IP addresses. Hackers have, with time, attempted to access the DNS and exploit these linkages to bring down websites. The Domain Name System (DNS) can be kept with increased security because of the irreversibility and decentralized that are aspects of Blockchain [11].

2.2.Use of Blockchain Technology for Cybersecurity:

When evaluating a company's security posture in the realm of cybersecurity, the CIA triad model is often used as a benchmark. Three things make up the triad:

2.2.1. Confidentiality

It entails making sure that only the right people may see sensitive information. Data stored in a blockchain may be fully encrypted to protect it from prying eyes as it travels through insecure networks. The best way to stop assaults from within the network is to put security measures, including access restrictions, into place directly in the applications themselves. By using public-key encryption for user authentication and data encryption, blockchain technology could provide superior safety measures. However, storing private keys in a separate location increases the danger of private key theft. Integer factorization-based cryptographic techniques and other key management processes are needed to avert this [12].

2.2.2. Integrity:

The immutability and suitability of blockchains are two features that assist businesses to guarantee the accuracy of their records. When a 51 percent cyber control assault occurs, consensus model protocols may aid companies in implementing procedures to avoid and manage ledger splitting. In Blockchain, the past state of the system is kept with each subsequent iteration, allowing for a completely auditable record of events. To stop miners from stealing data, smart contracts may be used to monitor and enforce regulations between parties [13].

2.2.3. Availability:

Cyberattacks targeting the availability of technical services, especially distributed denial of service attacks (DDoS), have been on the rise in recent years. With blockchain-based systems, however, DDoS assaults are prohibitively expensive since the attacker must first conduct a large number of cheap transactions to overwhelm the system. Since blockchains don't use a central server, the likelihood of an IP-based DDoS attack causing downtime is reduced. All of the information in the ledger is always accessible since it is distributed among several nodes. By using a distributed architecture with several nodes, the platforms and systems may better withstand failures [14].

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

2.3.Block chain's Benefits for Cybersecurity:

- *Confidentiality for the Users:*

The usage of cryptography with public keys inside a Blockchain network contributes to the users' ability to keep their anonymity.

- *Transparency and Traceability of the Data :*

All of these dealings are recorded and will always be accessible for review. Members of the Blockchain network verify the information on transactions, ensuring its authenticity.

- *Safekeeping of information and processing of data:*

The Block chain's primary benefit is its capacity to record and track any modifications made to data, which ensures that information is stored in a reliable and auditable manner.

- *Transmission of Information in a Secure Manner*:

The Block chain's use of a Public Key Infrastructure (PKI) ensures that all data transfers remain legitimate. Smart contracts provide the automated carrying out of transfer programs between parties.

*2.4.*Challenges with Blockchain Technology for Cybersecurity:

- *Reliance on private keys*:

Data encryption in blockchains is dependent on Private Keys, however, lost private keys cannot be retrieved. Data encryption might be compromised in this way.

- *Adaptability and scalability challenges:*

It is crucial to verify the scalability of a blockchain network due to its fixed block capacity and constraints on transactions per second. Companies may encounter challenges while attempting to integrate Blockchain technology due to the extensive system overhaul that is required.

- *High operating costs:*

The expense of maintaining a blockchain network is considerable since it needs plenty of space and processing power. Because of this, the expenses associated with using Blockchain-based apps are greater.

- *Blockchain literacy:*

To master Blockchain technology, one must have a comprehensive understanding of a wide range of development, programming languages, and other resources. This means that there are not yet enough Blockchain developers to fully realize the potential of the technology, despite the many uses for which it has been proposed.

3. CONCLUSION

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

More and more applications are being found for blockchain technology as it develops and becomes more widespread in the contemporary world. Cybersecurity is one of the areas where it has been explored and implemented. IoT devices, networks, and data in storage and transmission all have unique security difficulties, but Blockchain technology makes it possible to effectively solve these issues. Through more robust authentication and data transmission procedures, Blockchain technology may be utilized to safeguard IoT devices. These may protect these devices, which often arrive with insecure settings, from being compromised by hackers. Encrypted blocks in a blockchain keep data safe during transmission and storage; these blocks may only be accessed by the intended recipients of the data and cannot be tampered with. While the aforementioned three use cases have received the most attention, more use cases are being investigated. Since most existing solutions utilize various Blockchains, hindering integration, it is advised that future academics investigate the viability of a single Blockchain that could be used to construct cybersecurity.

REFERENCES:

[1] A. Schumacher, "Blockchain and Healthcare - 2017 Strategy Guide," *Epigenetics Axel Open*, 2017.

[2] M. Swan, *Blockchain: Blueprint for a new economy*. 2015.

[3] D. Peter, "Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?," *Open Univ. Repos. Res. Publ. other Res. outputs*, 2015.

[4] M. Buitenhek, "Understanding and applying Blockchain technology in banking: Evolution or revolution?," *J. Digit. Bank.*, 2016.

[5] C. Rogers, "Why marketers need to get to grips with Blockchain," *Mark. Week*, 2017.

[6] M. Morini, "How the Business Model Must Change to Make Blockchain Work in Financial Markets: A Detailed Example on Derivatives, Two Years Later.," *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3075540.

[7] D. X. Yang, Z. Hu, H. Zhao, H. F. Hu, Y. Z. Sun, and B. J. Hou, "Through-metal-wall power delivery and data transmission for enclosed sensors: A review," *Sensors (Switzerland)*. 2015. doi: 10.3390/s151229870.

[8] P. Rosati, B. Nair, and T. G. Lynn, "# Bitcoin Vs # Blockchain : The Role of Trust in Disrupting Financial Services # Bitcoin Vs # Blockchain : The Role of Trust in Disrupting Financial Services," *7th Eur. Bus. Res. Conf. 15 - 16 December 2016, Univ. Roma Tre, Rome, Italy ISBN 978-1-925488-203-4*, 2016.

[9] Y. V. Gulyaev *et al.*, "Dynamic-chaos information technologies for data transmission, storage, and protection," *Radioelektronika, Nanosistemy, Inf. Tehnol.*, 2018, doi: 10.17725/rensit.2018.10.279.

[10] X. Wang *et al.*, "Data Transmission and Access Protection of Community Medical Internet of Things," *J. Sensors*, 2017, doi: 10.1155/2017/7862842.

[11] European Commission, "EU Cybersecurity Initiatives," *Eur. Comm.*, 2017.

[12] S. A. Rutenberg and R. W. Wenner, "Blockchain Technology: A Syndicated Loan Revolution?," *Financ. Technol. Regul.*, 2017.

[13] M. Bal, "Securing property rights in India through distributed ledger technology," *Obs. Res. Found. Occas. Pap.*, 2017.

[14] D. B. Rawat and C. Bajracharya, *Vehicular cyber physical systems: Adaptive connectivity and security*. 2016. doi: 10.1007/978-3-319-44494-9.