International Journal of Research in Engineering, Science and Management
Volume 6, Issue 2, February 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Cyber Security in Blockchain Technology

K. P. Shana Sherin[1*], T. Ambikadevi Amma[2], K. Sivakumar[3], S. Divya[4]
[1]PG Student, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India
[2,3]Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India
[4]Assistant Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India

***Abstract*: Numerous qualities of blockchain technology are available, such as decentralisation, dependability, trackability, and immutability. But by itself, this technology is unable to ensure cybersecurity. This study seeks to present a thorough analysis of the methods and components proposed to achieve cybersecurity in blockchain-based systems. Our research investigates the many potential forms of assaults before making recommendations for how to defend against them. Our findings demonstrate that fresh blockchain applications can benefit from the Internet of Things (IoT), networks and machine visualisation, public key cryptography, online apps, certification systems, and safe keeping of personally identifiable information (PII). Blockchain has steadily grown in popularity as one of the best ways to protect data storage and transmission using decentralised, trustless, and transparent mechanisms. However, recent research on the security and privacy of blockchain technology has revealed that effective attacks have been launched against a number of apps.**

***Keywords*: Blockchain technology, Cyber security.**

1. Introduction

Cybersecurity has become more important in the business world due to the rise in cloud computing and internet applications. One of the most significant and cutting-edge technologies in the current computer paradigm, blockchain technology (BCT) increases the security of information system applications. Although BCT has many advantages, it also has several disadvantages, including a high risk of external cybersecurity threats, expensive capital costs, and excessive energy usage. New forms of data and compute outsourcing are now conceivable thanks to the Internet of Things (IoT), and network technologies are advancing swiftly. Decentralized storage offered by blockchain technology allows for the safe storing of data without the requirement for a single trustworthy entity. This essay examines the many cybersecurity measures that have been suggested when blockchain technology is involved.

In order to investigate how cybersecurity is addressed when blockchains are deployed, this study looks at 128 business endeavours and 272 scholarly works. It offers a taxonomy of the elements utilised in the suggested study, such as cybersecurity traits, methods for each property, geographical areas, technical developments, and the appropriate application of blockchains. With a primary focus on user privacy and transaction anonymity, it examines the security concerns and challenges that already-existing cryptocurrencies confront, including the potential for attacks. The majority of system users have certified the authenticity of Bitcoin, a decentralised peer-to-peer digital currency that maintains shared transactions between users and keeps track of all digital happenings in a public ledger. Blockchain is a promising technology that might make single point hacks less likely, but a coded infiltration or system weakness might still make things worse.

This paper provides a comprehensive investigation of BT security flaws. Blockchain technology enables reliable transactions between untrusted network users by way of a distributed ledger with a cryptographic underpinning. It has been used commercially, impacted the world's currency exchanges, supported the expansion of illicit dark web marketplaces, and significantly contributed to the rise of cyberattacks with a financial motivation. This article focuses on the research that has already been done on the use of blockchain as a supporting technology for cyber security applications, covering the business domains of data privacy, security, integrity, and accountability as well as its application in protecting networked devices like the Internet of Things (IoT). The main objective is to establish a community-driven project for a more in-depth examination of blockchain and cyber security with a particular emphasis on the connections between the two hotly debated topics.

2. Methodology

In this study, blockchain technology-based cybersecurity initiatives are investigated. It addresses five issues: how cybersecurity was achieved in blockchain-based systems, which application fields benefited from blockchains, which blockchain technologies were combined with cybersecurity, whether there is evidence of poor cybersecurity use of this technology in academic works, as well as how the industry is approaching the use of blockchains for cybersecurity. The purpose of this work is to provide a current assessment of the literature on current research, to contribute to the growth of a body of accepted knowledge, to identify research gaps based on discoveries from earlier literature, and to suggest new avenue of academic inquiry. The collection of papers being considered consists of published articles as well as papers from conferences and workshops. All articles are obtained from the DBLP database, and conferences are chosen from class A conferences in accordance with the GII-GRIN-SCIE categorization.

*Corresponding author: shanasherinkp999@gmail.com

The use of Google Scholar to exclude works having 100 or more citations. Case study papers, state-of-the-art technical blockchain implementations, and commentary on how incorporating blockchain technology has increased current security procedures are some examples of studies that may be included. Studies must present empirical data.

Several primary studies are published every year, the total number of times a particular phrase appeared across all primary studies, and the third most frequent term in the dataset are the most crucial information in this article. An examination of the 51 research articles chosen for the coding sheet for this phase was done to compile pertinent data. To ensure that the publication addressed one of the study subjects, the team members subjected six out of 205 papers to inclusion and exclusion criteria. The data were organised into themes and significant categories according to Salvato and Corbetta's technique, and each team member categorise each document separately. The selected bids are carefully examined and categorised using a number of criteria. The terms "blockchain" and "security" are the most commonly used in publications, followed by "IoT," "network," and "transaction," which indicates a growing trend in the application of blockchain in cyber security.

3. Results

A scoping review was done between 2017 and 2022 to help identify patterns in the most recent literature. For the purpose of assessing the validity and accuracy of the review, a thematic analysis was performed. The results show that the oil and gas, accounting and finance, agricultural, governmental, supply chain, and energy sectors all need study on cybersecurity-related issues. The research studies in our collection revealed that the most frequent cybersecurity issue in BCT was malleability attacks, which were followed by wallet security assaults, which were listed at 51%. Other noteworthy cyberattacks listed in BCT included system flaw attacks, double-spending attacks, and smart contract loophole attacks, which were all at 30%.

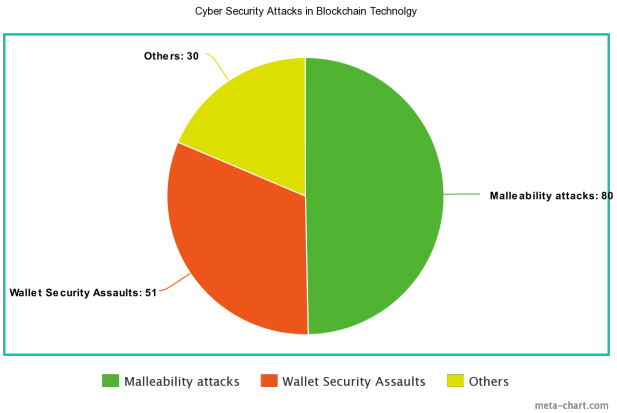

Fig. 1. Cyber security attacks in blockchain technology

When it comes to cybersecurity, there has been a noticeable increase in academic interest in blockchain since 2016, however there are relatively few energy applications developed in industrial projects and very little in academics. For many research papers, research studies evaluating solutions to these numerous cybersecurity challenges are necessary. The most important aspects in this essay are the usage of smart contracts in industrial approaches, the lack of clarity in industrial ideas, the need for deeper understanding of cybersecurity skills, and the ubiquity of Ethereum-based technologies in academia and industry. The preferred option is Ethereum, which is followed by Bitcoin-based alternatives, Hyperledger project technologies, and so forth. Many business concepts lack details, which begs the question of whether using blockchains is actually beneficial. With IoT devices being the most prevalent theme, primary studies should include a topic or subjects connected to how a certain problem was being solved through blockchain. Wi-Fi, the web, and malware are the least well-liked subjects.

4. Conclusion

This scoping review looked at the breadth, depth, and gaps in the existing literature on cybersecurity challenges in BCT. The majority of the study sample, it was discovered, revealed cybersecurity challenges generally without mentioning any particular industry sector. The bulk of the sample study emphasises that the most frequent assaults when implementing BCT are those involving wallet security, 51% attacks, and malleability attacks. Future researchers should concentrate on how to better comprehend the existing literature on this subject and what kinds of questions to ask. In recent years, blockchain-based methods for supplying cybersecurity guarantees have exploded, and business and academia are strikingly comparable in this regard.

Industrial proposals, however, frequently overlook crucial information in their strategies. It is advised that researchers and business professionals collaborate to better understand and identify solutions for the cybersecurity issues discovered during the introduction of BCT. This study has concentrated on how blockchain-based solutions might assist with concerns related to cyber security. It has uncovered unresolved problems like the dangers presented by third-party technologies when using the blockchain, which could be useful for creating fresh assaults. A stand-alone technology called blockchain offers an enormous range of potential solutions for the fields of banking, logistics, healthcare, and cyber security.

A decentralised, trustless system, however, cannot by itself address every issue that may arise in the area of cyber security. This study emphasises the possibilities for future investigations into cyber security topics unrelated to the Internet of Things. Additionally, https encryption is rapidly being used by end users and the world wide web as a whole for regular communication.

The main subjects of research on IoT security using blockchain applications have been network latency and power consumption necessary to maintain the distributed network. Future research could standardise the information offered in the original studies by assessing Blockchain-based IoT networks' latency, power usage, and data packet flows. Additionally, cutting-edge cyber security solutions have been created using

Ethereum and other Blockchain technologies with or without authorization. However, there has been an increase in interest in creating a cryptocurrency architecture that is forensically friendly to enable legal (forensic) investigation of questionable cryptocurrency transactions. The most widely used decentralised cryptocurrency with the longest, most trustworthy blockchain is still Bitcoin. Although it is commonly known that permissionless blockchain frameworks, such as those used by Bitcoin and Ethereum, frequently take between minutes to reach consensus, such latency may not be acceptable for time- and delay-sensitive applications, including the rollout of the Internet of Things (IoT). Designing blockchain-based solutions with lower latency, for instance in tandem with hardware-based techniques, is thus potentially on the research agenda.

References

[1] Samreen Mahmood, Mehmood Chadhar, and Selena Firmin, "Cybersecurity Challenges in Blockchain Technology: A Scoping Review," April 2022.

[2] Mar Gimenez-Aguilar, Jose Maria de Fuentes, Lorena Gonzalez-Manzano, David Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," May 2021.

[3] Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, "A Systematic Literature Review of Blockchain Cyber Security," 2018

[4] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, vol. 6, no. 2, pp. 147–156, 2020.

[5] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C. Soong, J.C. Zhang, "What will 5g be?," IEEE J. Sel. Areas Commun. 32(6), (2014) 1065–1082.

[6] T. Aste, P. Tasca and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," in Computer, vol. 50, no. 9, pp. 18-28, 2017.