International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Enhancing Cybersecurity through the Utilization of Blockchain Technology

Vinod Kumar Uppalapu
(Computer Science & Engg.)
Dr. Prerna Sidana (Associate Professor)
Glocal School of Technology and Computer Science

Abstract
Blockchain technology's adoption, primarily evident in the financial sector via cryptocurrencies, extends its viability to cybersecurity. This study delved into the perspectives of current studies, exploring diverse applications of Blockchain within the cybersecurity domain. Predominantly, the researchers emphasize safeguarding Internet of Things (IoT) devices, networks, and data. A comprehensive analysis revealed various mechanisms proposed by prior studies to leverage Blockchain's security benefits in addressing IT's critical challenges the spotlight remains on fortifying IoT security, stemming from the staggering count of approximately 9 billion devices with compromised configurations. A pressing concern is theirsusceptibility to hacking and subsequent enlistment into malicious botnet networks.
Keywords: *Blockchain cybersecurity; Internet of Things (IoT); Data protection; Network security*

Introduction

"Blockchain technology is a groundbreaking innovation poised to reshape the impending of computing and disrupt various industries with its innovative solutions. Its open, immutable, and distributed nature renders it highly applicable across diverse environments" **(Swan, 2015)**. While initially gaining traction from the rise of cryptocurrencies, blockchain's potential extends far beyond finance, finding applications in multiple sectors. This paper delves into the concept of blockchain, elucidating its structure and utility, with a particular focus on its potential contribution to cybersecurity, especially within challenging areas like "(IoT) devices, networks, and data storage and transmission"**(Lakhani, &Iansiti, 2017).**

Blockchain, often likened to a series of cryptographically linked blocks, embodies a decentralized and secure structure. Each block contains three crucial components: "*data, the hash of the previous block, and the hash of both the data and previous hash"***(Crosby,et al 2016).** This interconnectedness among blocks establishes a dependency order, crucial for safeguarding the reliability of the entire blockchain. Any alteration to the data within a block would alter its hash, triggering a cascade effect that invalidates subsequent blocks. This immutability ensures the permanence of transactions within the blockchain**(Zheng, et al 2016)**

The potential of blockchain in bolstering cybersecurity, particularly in IoT environments, stems from its inherent qualities. The strict architecture of blockchain mandates careful consideration when adding new blocks to maintain the integrity of the chain. Furthermore, the transparency and permanence of blockchain-based records make it an ideal candidate for a wide array of applications requiring verifiableand secure record-keeping.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

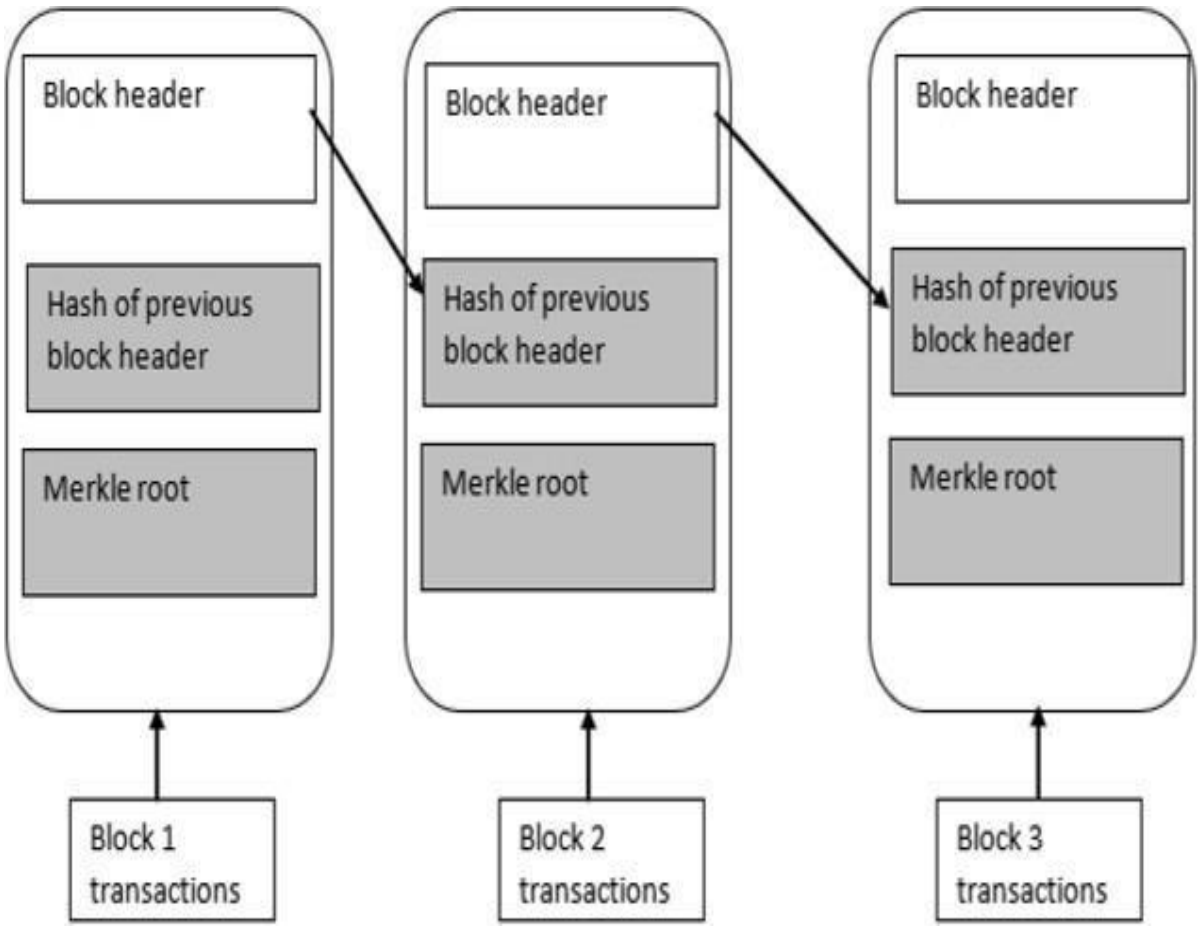

Figure 1.1 block diagram depicts Standard Sequence of Blocks **(Zheng, et al 2018)**

The operation of a blockchain network involves nodes collaborating to achieve consensus on the addition of new blocks. This consensus process ensures that the network agrees upon the validity of transactions.

Two primary consensus algorithms are prevalent:
PoW involves miners solving complex puzzles, and the first miner to solve it gets to add a block to the blockchain.
PoS, relies on participants who hold stake in the network to approve new blocks. The rigorous validation processes in both PoW and PoS contribute to the robustness of blockchain technology.

A key feature of blockchain is its decentralized paradigm of record-keeping. Nodes within the network are able to store the totality of the data, which is advantageous for consensus and orientation tenacities.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

This decentralized storage ensures that data is not stored in a vulnerable central location. Given the size of the network, any malicious attempt to alter the data would require interfering with a substantial number of decentralized nodes.

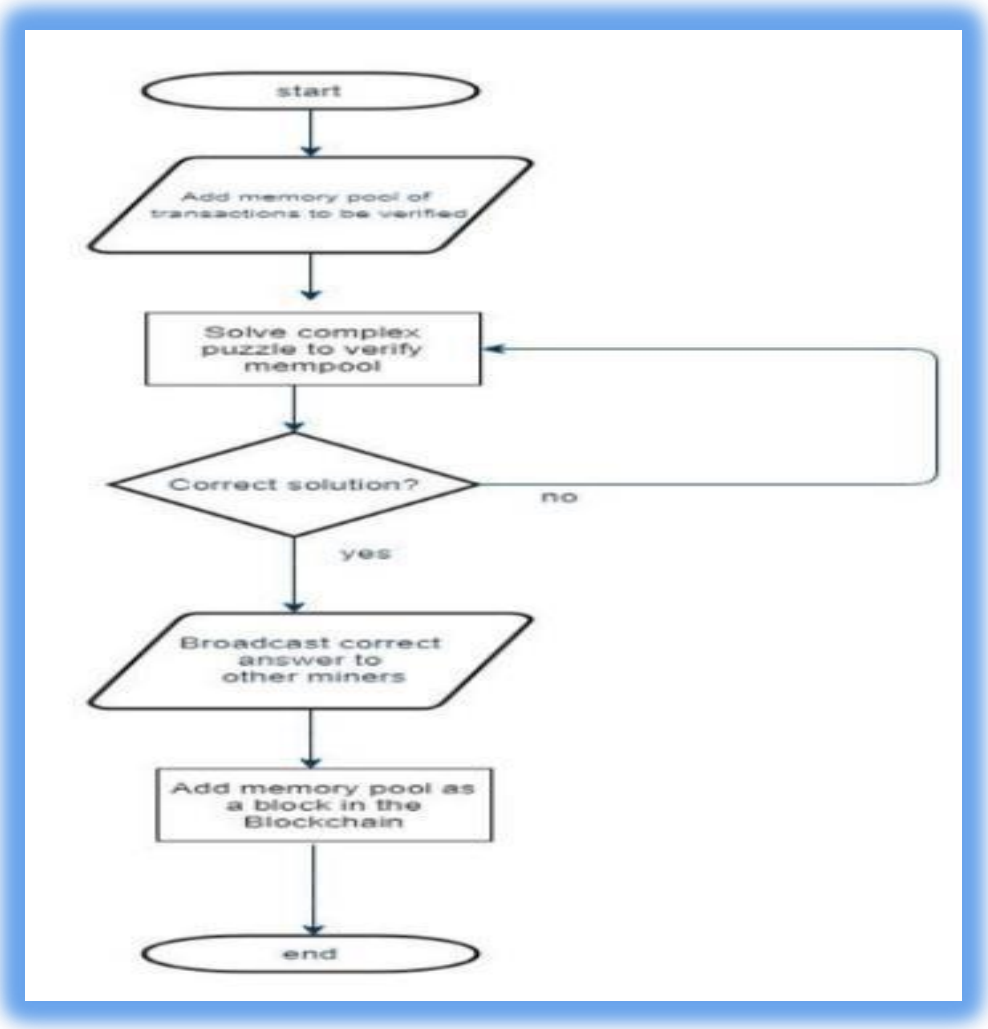

Figure 1.2: The PoW consensus algorithm depicted as a flowchart **(Zheng, et al 2018)**

Blockchain's advanced attributes lend themselves seamlessly to addressing contemporary cybersecurity challenges. The technology presents promising solutions for fraud prevention and identity theft. By embracing distributed data storage, blockchain safeguards against unauthorized access and modification of data. Data breaches that exploit centralized storage locations become significantly more difficult as blockchain's distributed nature disperses data across millions of computers. This ensures that breaches in a few computers do not compromise the rest of the network's data.**(Srivastava, et al 2019)**

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Moreover, blockchain offers potential solutions for identity theft. In the current landscape, data breaches arise from inadequate data management, with users divulging excessive information to access services. Blockchain's decentralized identity system could enable universal verification without requiring users to reveal sensitive details. This approach not only enhances security but also makes data theft a costly endeavor for hackers.

The advent of blockchain technology brings forth an array of transformative possibilities, extending beyond its association with cryptocurrencies. Its immutable and decentralized nature has the potential to revolutionize cybersecurity practices, addressing the challenges posed by IoT environments and data breaches. By providing robust mechanisms for data verification, secure record-keeping, and identity protection, blockchain emerges as a formidable solution for the contemporary cybersecurity landscape.

Methodology

The research proposed herein aims to assess the viability of incorporating Blockchain technology into the contemporary cybersecurity landscape in a comprehensive evaluation of a study conducted by **(Taylor et al. 2020),** which reviewed recent research endeavors focusing on Blockchain's applicability in enhancing cybersecurity. The research will delve into two key dimensions highlighted by the selected papers.

Results and Discussion

Recent research evaluations concluded that Blockchain offered superior viability in protecting IoT, network, and data storage. The following diagram illustrates the distribution of current Blockchain security implementations, with the Internet of Things (IoT), networks, data, PKI, and data privacy accounting for the vast majority.

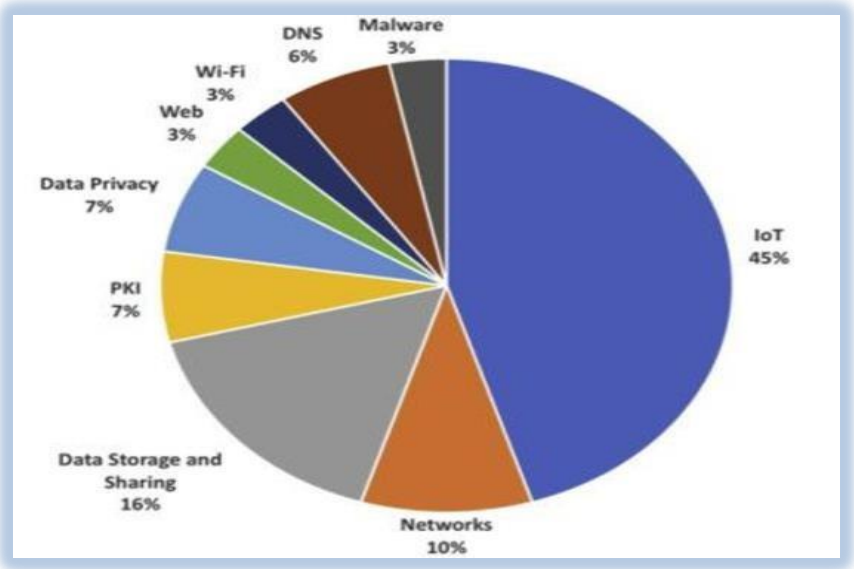

Fig 1.2: Most-researched Blockchain security application areas

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

With 9 billion IoT devices now in use, it only makes reasonable that Blockchain's first focus would be on safety. Because of their poor security measures, many of these devices are being hacked and added to hacker networks. The Mirai Botnet is an Internet of Things (IoT) device-based botnet network. The Internet's largest domain name resolving service, Dyn DNS, is one of the targets it has been deployed against effectively **(Matthew, 2019).** This is why many researchers are investigating the potential of Blockchain in protecting these devices. The second area where Blockchain hacking research is commonly concentrated is data storage. This is due to the fact that hackers have been making increasingly large thefts of sensitive company data. They have collected data on billions of people. In 2014, for instance, hackers were able to access the personal data of three billion Yahoo users at once **(Trautman & Ormerod, 2016).** Security professionals are thus keen to explore Blockchain-based protection mechanisms for data storage environments like cloud services. It's also obvious that researchers are investigating Blockchain's potential for enhancing network security. Since current network security techniques may be overcome, including WPA encryption **(Kolias et al., 2017)**. Most of the research concentrates on how PHI can be shielded by using a generic Blockchain authentication approach. Users will no longer be required to provide data to other parties. Companies will instead rely on Blockchain technology for user verification **(Kshetri, 2017).**

Most security tools are set up to work on their own when an IT resource needs to be protected **(Yeoh, 2017).** As has happened with attacks like DDoS, hackers can go after a single security solution, take it offline, and then attack the IT resource that is now vulnerable. Researchers who are trying to figure out how Blockchain can help make security better base their cases on the fact that spread security tools are better at protecting than a single tool.

According to the above diagram, there is a lot of focus on how Blockchain might strengthen protections for IoT infrastructure, data, and devices. The most significant threat to the safety of IoT networks is the possibility of unauthorized access to and manipulation of connected devices. Blockchain security solutions can aid all IoT devices in more effectively restricting access and sharing data **(Sharma et al., 2017).**

To ensure that users are properly recognized and validated and that data transfers without hiccups, a Blockchain security system might be implemented. To prevent intrusion, it may function by storing historical connections and sessions in many locations. One option is to need widespread approval from existing connections before allowing a new one. Therefore, a home IP camera or other IoT device will only allow connections from other devices already established in the home. Until the majority of devices in circulation agree to let a hacker in, the Blockchain approach will prevent them from accessing the camera. According to research **(Gao and Nobuhara, 2017),** having a single point of failure or exposure is the greatest vulnerability in data security. Theft, alteration, or loss of information is facilitated by this. Researchers in the field of cybersecurity discussed the advantages of using Blockchain's stringent architecture to safeguard sensitive information. Third parties will be unable to alter the provided data since each block will be hashed and connected to the next block. Data that has been stolen is rendered useless since no one other than the two persons involved in the conversation can read or alter it. When it comes to networks, Blockchain technology has been deemed to be useful by security experts for providing clustered network security, which prevents unlawful linkages. The discussed application circumstancesrevealed the growing use of Blockchain technology in security

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

(Gao, &Nobuhara, 2017). Although research was conducted in other areas, the three highlighted here are the most crucial in the field of information technology today. They demonstrate that Blockchain has the potential to remedy intractable security flaws that cannot be addressed by more conventional means.

Conclusion

The blockchain evolves and finds new uses as time goes on. Cybersecurity is one field where it has been investigated and used. Check out the results of recent research to see what experts think about Blockchain technology and its potential uses for securing Internet of Things (IoT) devices, networks, and data storage and transfer. Protecting Internet of Things devices using Blockchain technology is an issue that has been carefully considered by most Blockchain security experts. The Blockchain's emphasis on data and network security is also essential. As we've seen, Blockchain technology has the potential to increase the safety of IoT devices by making identification and data sharing more reliable. These devices are hack-proof despite having default settings that aren't very secure. The method may also be used to keep networks secure by blocking access to them from unwelcome parties. Finally, Blockchain can safeguard data from being viewed or altered by intruders by using encoded blocks that can only be read by the designated parties. Although this list is not exhaustive, the three scenarios above receive the most attention. Experts of the future should examine how useful a single Blockchain that can be used to construct security solutions would be, given that most present solutions use distinct Blockchains and make it hard to join them.

References

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Lakhani, K. R., &Iansiti, M. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 119-127.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

Srivastava, G., Parizi, R. M., Dehghantanha, A., & Choo, K. K. R. (2019, November). Data sharing and privacy for patient iot devices using blockchain. In *International Conference on Smart City and Informatization* (pp. 334-348). Singapore: Springer Singapore.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.

Mathew, A. R. (2019). Cyber security through blockchain technology. *Int. J. Eng. Adv. Technol*, *9*(1), 3821-3824.

Kolias, C., Kambourakis, G., Stavrou, A., &Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84.

Trautman, L. J., & Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *Am. UL Rev.*, *66*, 1231.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May- 2023
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Kshetri, N. (2017). Can blockchain strengthen the internet of things?. *IT professional*, *19*(4), 68-72.
Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of information processing systems*, *13*(1).
Gao, Y., &Nobuhara, H. (2017). A proof of stake sharding protocol for scalable blockchains. *Proceedings of the Asia-Pacific Advanced Network*, *44*(1), 13-16.