# Cyber Security Through Blockchain Technology

**[1]Dr. C. Sunitha, [2]R. Sanjana, [3]M. Krishna priya**

[1]Head of the Department, [2]Student, [3]Student
Department of Computer Science,
Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.

**Abstract**: **Blockchain technology has been used by various industries, mostly in the field of finance, through the usage of cryptocurrencies. Technology is very useful in cybersecurity. This paper is proposed by examining various Blockchain use cases by 30 researchers. It shows that the majority of researchers are focusing on using Blockchain to secure IoT (Internet of Things) devices, networks, and data. The study stated the strategies used by earlier academics to secure the three complex IT areas using blockchain. To enable integration and uniformity among solutions, the paper states the future of academics which concentrates on a single Blockchain on which to create cybersecurity applications.**

**Index Terms: Blockchain, Cybersecurity, IoT.**

## I. INTRODUCTION

Blockchain is a revolutionary technology that is expected to transform computing in the future and provide more creative solutions in a number of industries. Since it is distributed, immutable, and open, it can be used usefully in a variety of settings. Even though the technology has many uses in outside finance, the rise of cryptocurrencies gave it huge popularity. The definition of the term "blockchain" is multiple cryptographically chained blocks. A block, a kind of data structure, is made up of three components: data, the hash of the previous block, and the hash of the data and the previous hash. In order to ensure the integrity of the entire Blockchain, it is therefore, possible to take use of the order of dependence between blocks. Whenever the contents in a block change, the block's hash will also change. The hashes of the next blocks will become invalid as a result of the spiral effect that will result from this. Because of this, blockchain transactions are unchangeable. This architecture can be very helpful in providing cybersecurity solutions for challenging areas including IoT devices, networks, and data transmission and storage.

## II. THEORY

The block of a Blockchain cannot be changed because it would compromise the integrity of all upcoming blocks. Due to the strict Blockchain architecture, we must be very careful while adding blocks to the chain to make sure that it won't need to be changed in the future. A block diagram is shown in the diagram below:

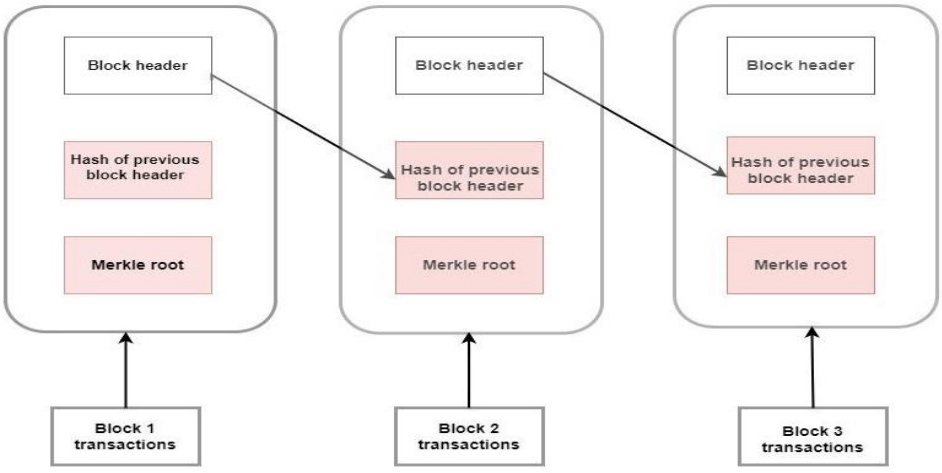


Fig. 1 Block diagram

By broadcasting the new block to all other nodes in the Blockchain network at the specified time, a node can add a new block and provide them access to the full Blockchain. The other nodes must reach an agreement once a block has been written and is ready to be added to the Blockchain. The two primary algorithms for reaching consensus are proof of work (PoW) and proof of stake (PoS). A proof of work algorithm requires nodes to validate a block by demonstrating that they have completed some work and reached an understanding of the outcomes. Before adding a block to the Blockchain, nodes must often agree on the outcome of a series of complicated calculations. This is carried out by miners and calls for a lot of processing power. In the proof of stake algorithm, nodes demonstrate that they have a stake in the blockchain and, as a result, agree to the insertion of the new block. This is carried out by those who own a stake in the Blockchain and doesn't necessarily require a lot of computational resources.

An illustration of a PoW consensus algorithm is the following:

1. The network groups user transactions into a memory pool.

2. Miners compete to solve a challenging challenge to validate each transaction in the pool or submit an answer to the network to verify.
If the answer is right, tell the other miners. If not, redo the calculation.
3. The first miner to provide the right response is rewarded.
4. The memory pool is authenticated and added to the Blockchain as a block.

The flowchart of the PoW consensus algorithm is as follows:

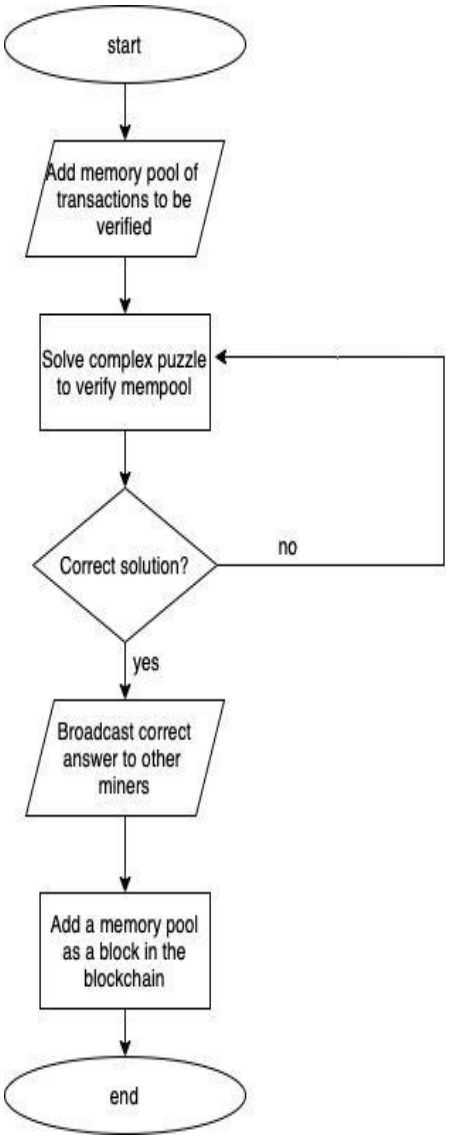


Fig. 2 Flowchart of the PoW consensus algorithm

The distributed approach of record keeping is another crucial component of blockchain technology. A Blockchain network's nodes have the option to store all of the network's data if they so want. Numerous nodes carry out this action since it is crucial for reference or consensus purposes. This guarantees that there is no centralized data storage. Almost all of the nodes that store the decentralized pieces of data must be compromised for any adversary trying to undermine the Blockchain. This is so that the network can identify the blocks of data that are different from the others among those stored in decentralized places. Typically, the majority has accurate or unaltered data. Blockchain is the perfect solution for modern cybersecurity needs thanks to its unique characteristics.

The development of technologies that help stop fraud and identity theft is one way that blockchain can be incorporated into cybersecurity. Users are continuously at risk of having their data accessed and changed without their permission. This occurs as a result of the widespread use of centralized data storage. As a result, it is simple for a hacker to access the site where the data is stored and change it for nefarious purposes. Blockchain's distributed data storage prevents such situations. Because each computer will have a copy of the data, millions of computers might be used to store sensitive data like election results. The breach and modification of just a few machines won't affect the rest of the data in the network unless the hacker is able to penetrate a sizable number of systems with copies of the data. Blockchain can be used to stop identity theft as well. According to NASDAQ, occurrences of data theft today are brought on by inadequate data management.

## III. METHODOLOGY

For the purpose of this study, the application of blockchain technology in the current cybersecurity sector will be assessed through the qualitative analysis of secondary data. The study will concentrate on a Taylor et al. paper from 2019 that examined 30 recent research studies on Blockchain cybersecurity application cases. Two characteristics of each of the highlighted papers will be the topic of the essay. It will start by examining the most recent applications of the developing Blockchain technology in cybersecurity. It will then examine the approaches for implementing Blockchain cybersecurity solutions. A debate on how Blockchain might provide security in today's IT user environments will be based on the key conclusions from the study findings and suggestions from the analyzed papers.

## IV. RESULTS AND DISCUSSION

According to the analysis of the 30 studies, blockchain technology offers greater potential for IoT, network, and data storage security. IoT, networks, data, public key infrastructure (PKI), and data privacy claim the majority of recent Blockchain security implementations, according to the findings shown in the pie chart below:

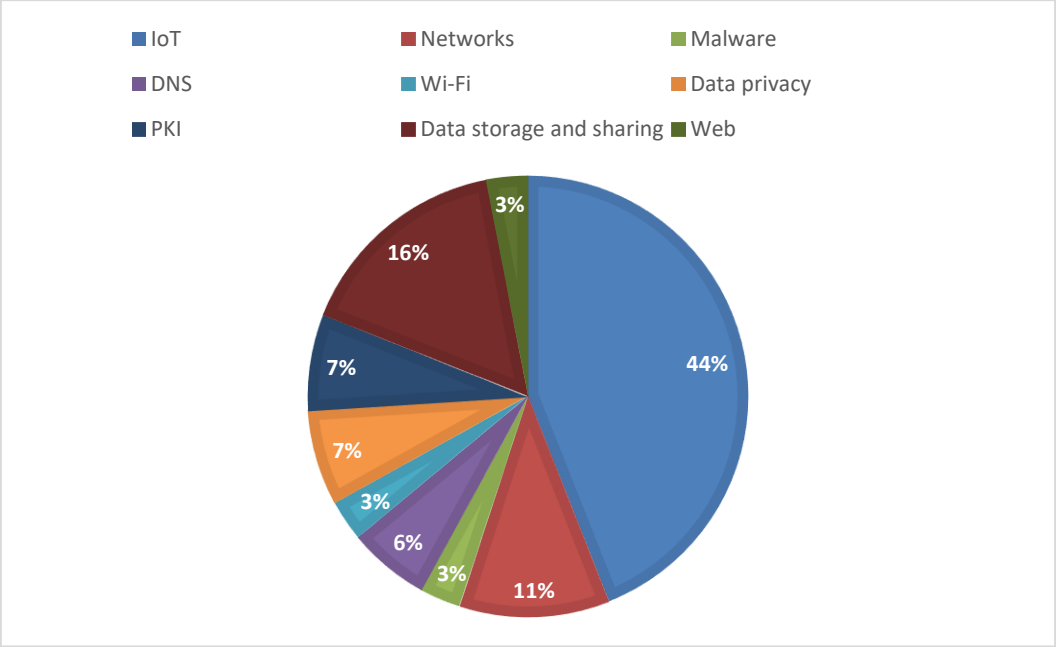


Fig. 3 Most-researched Blockchain security application areas

| Application areas | Percentage used |
|---|---|
| IoT | 44% |
| Networks | 11% |
| Malware | 3% |
| DNS | 6% |
| Wi-Fi | 3% |
| Data privacy | 7% |
| PKI | 7% |
| Data storage and sharing | 16% |
| Web | 3% |

Tabular representation of Most-researched Blockchain security application areas

Given that there are currently 9 billion such devices, the focus on Blockchain IoT security is understandable. These devices have bad security setups, and lots of them are becoming hacked and joining botnet networks. The Mirai Botnet is one such IoT-based botnet network that has been successfully utilized against significant targets like Dyn DNS, one of the biggest domain name resolution firms on the Internet. As a result, numerous security researchers are investigating how to use Blockchain to safeguard these devices. The second often-studied area in blockchain cybersecurity research is data storage. This is a result of an upsurge in data theft cases where hackers have been successful in stealing information from businesses belonging to billions of people. For instance, the 2014 Yahoo cyberattack resulted in the theft of three billion users' personal data. As a result, security researchers are interested in developing Blockchain security solutions for cloud platforms and other data storage facilities. Additionally, it is clear that experts are looking into how Blockchain technology might be used to secure networks. Since current network security mechanisms like security through WPA encryption can be broken, the majority of the research in these areas focuses on

authentication. Last but not least, Blockchain security solutions for data privacy are receiving a lot of attention. The majority of the research examines various strategies for securing personally identifiable data using a global Blockchain authentication system. Users won't need to submit organizations their personal information as a result; instead, organizations will authenticate users using the Blockchain.

The research's second main focus is on how Blockchain technology might be applied to enhance cybersecurity. The current security solutions provide IT resources with admirable levels of protection, but they are nevertheless prone to malfunction. This is due to the fact that the majority of security products are set up to function independently while protecting an IT resource. Hackers can target a single security solution, disable it, and then proceed to attack the now-exposed IT resource, as has been the case with attacks like DDoS (Distributed Denial of Service). Researchers who study how Blockchain can help boost security levels base their claims on the greater capacity of distributed security tools to provide protection better than a single tool.

According to the data in the pie chart above, a lot of researchers are primarily interested in how Blockchain might enhance the security offered to IoT devices, data, and networks. The biggest security risk to IoT networks is unauthorized access to and control of the devices. Access control and data sharing for all IoT devices can be managed more effectively with the aid of blockchain security solutions. In order to guarantee accurate user identity, authentication, and data transfer, a Blockchain security solution could be put up. To prevent unwanted access, it might work by maintaining distributed records of trustworthy historical connections and sessions. New connections might only be permitted if a sizable portion of the existing connections approve them or verify the new user. As a result, an IoT device like an IP camera in a home will only allow access to trusted household devices. The Blockchain approach will block access to the camera if a hacker tries to do so until the majority of the trusted devices approve the hacker's request.

The researchers determined that a single point of failure or compromise is the biggest weakness in data security. This results in data loss, modification, or theft. The security experts highlighted how Blockchain's rigid infrastructure may be leveraged to guarantee data protection. It will be impossible for other parties to alter the shared data because each block will be hashed and connected to the next block. Any data that is stolen will be useless and unable to be altered by outside parties because only the two parties to the communication will be able to access and manipulate the material. Blockchain technology can be used to provide clustered network security for networks, limiting unwanted connections and communication. This was discovered by security researchers studying networks.

The application cases mentioned illustrated how Blockchain technology is becoming more and more useful in cybersecurity. Although other topics were investigated, the three that were highlighted are the most crucial in the current IT world. They demonstrate how Blockchain may be able to close difficult security gaps that are unreachable by traditional security measures.

## V. Conclusion

In the contemporary world, blockchain technology is still developing and finding more applications. Cybersecurity is one of the useful fields where it has been researched and used. It is quite practical to handle the security issues that now exist in sectors like IoT devices, networks, and data in transmission and storage thanks to the Blockchain infrastructure. The report assessed the blockchain technology's applicability from the viewpoint of 30 researchers who were subjected to the Taylor et al review. The adoption of Blockchain security for Internet of Things (IoT) devices has been shown to be a major focus for the majority of Blockchain security researchers. In addition to this, networks and data are two other crucial components of blockchain security. As was noted throughout the conversation, the implementation of more dependable techniques for data transfer and authentication can help protect IoT devices. These can stop hackers from breaking into the devices, which frequently have weak security configurations out of the box. By employing a rigid architecture to block unwanted connections and communication, the technology can also be utilized to secure networks. As a last measure, Blockchain can protect data during transmission and storage by using encrypted blocks that can only be opened by the parties involved in communication and are impervious to tampering. Although other use cases are being investigated, these three are in the spotlight right now. Future researchers are advised to investigate the viability of a single Blockchain that may be used to create security solutions, as the majority of existing solutions utilize many Blockchains, which makes integration difficult.

## References

1. Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015
2. Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): pp. 118-127.
3. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): pp. 71.
4. Cachin C. Architecture of the hyperledger blockchain fabric. InWorkshop on distributed cryptocurrencies and consensus ledgers 2016, 310(1), pp. 4.
5. . Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services, 2018, 14.4, pp.352-375.
6. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. Asystematic literature review of blockchain cyber security. DigitalCommunications and Networks. 2019, 12(5), pp. 1-14.10.
7. Yeoh P. Regulatory issues in blockchain technology. Journal ofFinancial Regulation and Compliance. 2017, 25(2), pp. 196-208.
8. Trautman LJ, Ormerod PC. Corporate Directors' and Officers'Cybersecurity Standard of Care: The Yahoo Data Breach. Am. UL Rev..2016, 66(1), pp. 1231.14.
9. Kshetri N. Can blockchain strengthen the internet of things?. IT professional, 2017, 19(4), pp. 68-72.15.
10. Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." Computer Science-Research and Development, 2018, 33.1, pp. 207-214.