Cyber Security through Blockchain Technology

Alex. R. Mathew

Abstract**:** ***Blockchain technology has seen adoption in many industries and most predominantly in finance through the use of cryptocurrencies. However, the technology is viable in cybersecurity. This paper looked at several use cases of Blockchain in the cybersecurity industry as envisioned by 30 researchers. It found that most researchers are concentrating on the adoption of Blockchain to protect IoT (Internet of Things) devices, networks, and data. The paper examined the ways highlighted by previous researchers through which Blockchain can afford security to the three problematic areas in IT. Lastly, the paper recommended that future researchers focus on a single Blockchain on which to develop cybersecurity applications to allow for integration and uniformity among solutions.***

Keywords **:** ***Blockchain, Cybersecurity, IoT***

I. INTRODUCTION

Blockchain is a revolutionary technology set to change the future of computing and disrupt several industries with more innovative solutions. It is open, immutable and distributed thus practically applicable in many environments. The technology gained massive appeal from the rise of cryptocurrencies but it sees applications in many other sectors other than finance. Blockchain can be loosely translated as several cryptographically chained blocks[1]. A block refers to a data structure with three components; data, the hash of the previous block, and the hash of the data and previous hash[2]. Therefore, there is an order of dependency between blocks that can be used to ensure the integrity of the whole Blockchain[3]. Should the data in any of the blocks change, its hash will be changed as well. This will lead to a spiral effect where the hashes of the subsequent blocks will become invalid. This is why transactions on the Blockchain are immutable[4]. This infrastructure can be highly beneficial in offering cybersecurity solutions in problematic areas such as IoT devices, networks and data storage and transmission.

II. THEORY

The blocks in a Blockchain can never be modified since doing so will affect the integrity of all the subsequent blocks. This stringent Blockchain architecture implies that caution has to be taken when adding blocks to the chain to ensure that there will not be a need to change it later one. The following diagram illustrates a block diagram:

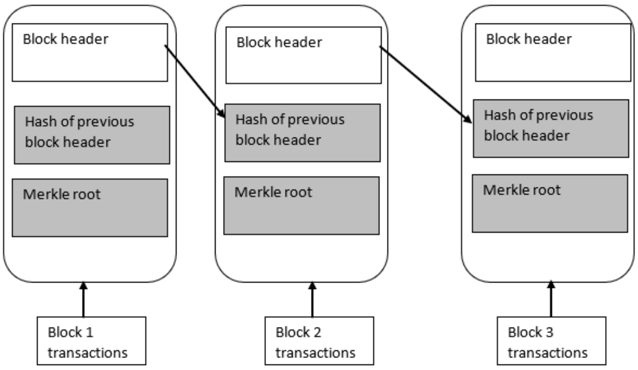

Fig 1. A block diagram

A node in the Blockchain network can add a new block by broadcasting it to the other nodes and allowing them to see the entire Blockchain at the given time. Once a block has been written and is to be added to the Blockchain, the other nodes have to come to a consensus[5]. There are two main consensus algorithms, proof of work (PoW) and proof of stake (PoS). A proof of work consensus entails the validation of a block by nodes showing that they have done some work and come to an agreement of the results[6]. The work is usually a set of complex calculations whereby nodes agree on the correct answer before appending a block to the Blockchain[7]. This is done by miners and requires a lot of computation power. In the proof of stake consensus, nodes prove that they own stake on the Blockchain thus approve of the addition of the new block to the Blockchain. This is done by owners of a stake in the Blockchain and is not necessarily resource-intensive in terms of computation power[8]. The following is an example of a PoW consensus algorithm:

```
1. The network bundles transactions from users in a memory pool
2. Miners race to verify each transaction in the pool
    a. Solve a complex puzzle to verify transaction
    b. Submit answer to the network to verify
        i. If Correct then
            •Broadcast correct answer to other miners
        ii. Else
            •Redo calculation
3. First miner with correct answer gets rewarded
4. The memory pool is verified and added as a block to the Blockchain
```

The flowchart for the algorithm is as follows:

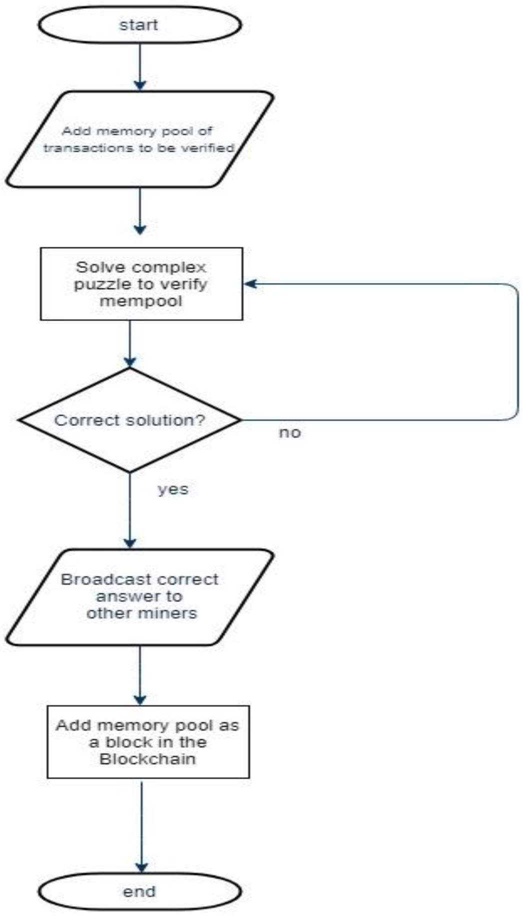
start
Add memory pool of transactions to be verified
Solve complex puzzle to verify mempool
Correct solution?
no
yes
Broadcast correct answer to other miners
Add memory pool as a block in the Blockchain
end

Fig 2: A flowchart of the PoW consensus algorithm

Another important feature in Blockchain is the distributed model of recordkeeping. Nodes in a Blockchain network can store all the data in the network if they want to. Many nodes do this as it is essential during either for consensus or reference purposes. This ensures that there is no centralized storage of data[10]. Any adversary that tries to compromise the Blockchain has to compromise a large percentage of the nodes that store the decentralized pieces of data. This is because the network checks the blocks of data stored in decentralized locations to find out the ones that differ from the rest. Normally, the majority has the correct or uncompromised data. The advanced features in Blockchain make it ideal for today's cybersecurity needs.

One of the ways Blockchain can be integrated into cybersecurity is for the development of tools that can prevent fraud and identity theft. Users are constantly facing the threat of unauthorized access to and modification of data. This is because many users have centralized data storage. It is therefore easy for a hacker to breach the data storage location and change the data with malicious intents. Blockchain prevents such cases with its distributed storage of data. Sensitive data such as election results could, therefore, be stored in millions of computers whereby each will have a copy of the data. Unless the hacker can compromise a significant number of computers with the copies of data, the breach and modification of just a few computers will not affect the rest of the data in the network. Similarly, Blockchain can be used to deter identity theft. As explained by NASDAQ, today's data theft incidents are caused by poor data management[11]. Customers are often required to disclose more than necessary information to get services from many companies. These companies promise to keep the data safe but hackers usually end up finding exploitable security gaps and infiltrating the data storage locations. Blockchain can prevent identity theft by verifying that a customer is who they claim to be through a decentralized identity system. This can be achieved through a universal system where all organizations can verify the identities of customers without necessarily having them transfer their sensitive details. This will reduce the possibility of compromise and make it expensive for hackers to steal user data.

III. METHODOLOGY

This research will use the qualitative analysis of secondary data to evaluate the applicability of Blockchain technology in today's cybersecurity industry. It will focus on a 2019 study done by Taylor et al. that reviewed 30 recent research studies on Blockchain cybersecurity use cases. The paper will focus on two aspects of all the highlighted papers. To begin with, it will look at the latest implementations of the evolving Blockchain technology in cybersecurity. Second, it will look at the methods available for deploying Blockchain cybersecurity solutions. The main takeaways from the research findings and recommendations from the analyzed papers will be used to form a discussion on how Blockchain can afford security in today's IT user environments.

IV. RESULTS AND DISCUSSION

The assessment of the 30 studies showed that Blockchain was more viable in IoT, network and data storage security. The pie chart below summarizes the findings whereby IoT, network, data, public key infrastructure (PKI), and data privacy claim most of the recent Blockchain security implementations:

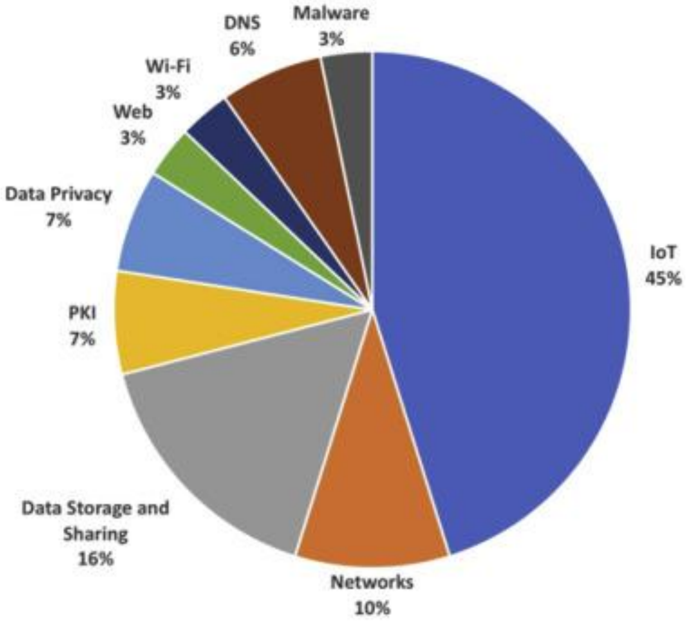

Fig 3: Most-researched Blockchain security application areas[9]

The focus of Blockchain IoT security is understandable since there are currently 9 billion such devices. These devices have weak security configurations and many are being hacked and recruited into botnet networks. One such botnet network comprised of IoT devices is the Mirai Botnet which has been used with high rates of success against big targets such as Dyn DNS, one of the Internet's largest domain name resolution companies[12]. Therefore, many security researchers are looking at ways in which these devices can be secured through Blockchain. Data storage is the second popular concentration of Blockchain cybersecurity research. This is because of the increased data theft cases where hackers have been able to exfiltrate data belonging to billions of users from companies. For instance, the cyber breach of 2014 on Yahoo led to the theft of data belonging to three billion users[13]. Therefore, security researchers are taking interest in finding Blockchain security solutions for data storage spaces including cloud platforms. It can also be seen that researchers are exploring the application of Blockchain in securing networks. Most of the research in these areas is around authentication since current network security measures such as security through WPA encryption can be compromised. Lastly, there is significant attention towards Blockchain security solution for data privacy. Most of the studies are evaluating ways of protecting personally identifiable information through a universal Blockchain authentication scheme. This will negate the need for users to send their information to organizations, instead, the organizations will authenticate users via the Blockchain.

The second focus of the research is how the Blockchain technology can be used to improve cybersecurity. Even though the existing security solutions offer commendable levels of protection to IT resources, they are still prone to failure. This is because most security tools are deployed to operate independently when securing an IT resource. As has been the case with attacks such as DDoS (Distributed Denial of Service), hackers can target a single security solution, put it out of service and then proceed to attack the now-exposed IT resource. Researchers on the ways through which Blockchain can help improve the current levels of security anchor their arguments on the increased ability of distributed security tools to be better off at offering protection than a single tool.

Going by the information provided by the pie chart above, the main focus of many researchers is how Blockchain can improve the security afforded to IoT devices, data, and networks. In IoT networks, the leading security threat is unauthorized access and control of the devices. Blockchain security solutions can help manage access control and data sharing for all IoT devices more effectively. A Blockchain security solution could be set up to ensure reliable user identification, authentication, and data transfer. It could work by keeping distributed records about the trusted historic connections and sessions to prevent unauthorized access. New connections could be set to be allowed only if a significant number of the historic connections vote or verify the new user. Therefore, an IoT device such as an IP camera in a house will only grant access to trusted devices of the household. If a hacker tries to access the camera, the Blockchain solution will prevent access until the majority of the trusted devices vote to allow the hacker to access the camera.

In data security, the researchers identified that the biggest weakness is the existence of a single point of failure or compromise. This leads to data theft, modification or loss. The security researchers discussed that Blockchain could be used to ensure data security through its stringent infrastructure. Since each block of data shared will be hashed and connected to the next block, it will be impossible for third parties to modify it. Since only the two parties in the communication will be able to read and manipulate the data, any stolen data will be unusable and third parties will also not be able to modify it. Concerning networks, the security researchers identified that the Blockchain technology can be used to offer clustered network security hence preventing unauthorized connections and communication.

The use cases discussed demonstrated the increasing viability of the Blockchain technology in cybersecurity[14]. Even though there were other areas explored, the three highlighted areas are most vital in the modern IT environment. They show that Blockchain could potentially seal challenging security loopholes that are beyond the scope of conventional security tools.

V. CONCLUSION

Blockchain technology continues to evolve and find more use cases in the modern world. One of the viable areas where it has been studied and applied is cybersecurity. The Blockchain infrastructure makes it highly practical in addressing the existing security challenges in areas such as IoT devices, networks, and data in transmission and storage. The paper has evaluated the applicability of the Blockchain technology from the perspective of 30 researchers reviewed by Taylor et al. It has been observed that most Blockchain security researchers are concentrating a lot on the adoption of Blockchain security for IoT devices. Alongside this, other major areas of Blockchain security are networks and data. As observed in the discussion, the Blockchain technology can be used to secure IoT devices through more reliable authentication and data transfer mechanisms. These can prevent hackers from breaching into these devices which often ship with poor security configurations. The technology can also be used to secure networks by using the stringent infrastructure to prevent unauthorized connections and communication[15]. Lastly, Blockchain can secure data in transmission and storage through encrypted blocks which can only be opened by the communicating parties and are not prone to manipulation. More use cases are being studied but these three have taken center stage. It is recommended that future researchers look into the practicality of a single Blockchain that can be used to develop security solutions since most of the current solutions use different Blockchains hence hampering integration.

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. Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017, 8(1), 297-315.
7. 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.
8. Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network. 2017;44:13-6.
9. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019, 12(5), pp. 1-14.
10. Sharma PK, Moon SY, Park JH. Block-VN: A distributed blockchain based vehicular network architecture in smart City. JIPS. 2017, 13(1), pp. 184-95.
11. "How Blockchain Can Fight Fraud Based on Know-Your-Customer Data", Nasdaq.com, 2019. [Online]. Available: https://www.nasdaq.com/articles/how-blockchain-can-fight-fraud-based-know-your-customer-data-2019-02-11. [Accessed: 19- Sep- 2019].
12. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017,50(7), pp. 80-4.
13. 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. Kshetri N. Can blockchain strengthen the internet of things?. IT professional, 2017, 19(4), pp. 68-72.
15. Yeoh P. Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance. 2017, 25(2), pp. 196-208.

AUTHORS PROFILE

Ph.D. in Computer Science and Engineering (Cyber Security)
Certified Information Systems Security Professional- CISSP - (ISC)2
Microsoft Certified Solutions Expert – MCSE - (Microsoft)
Certified Ethical Hacker – CEH- (EC-Council)
Computer Hacking Forensic Investigator - CHFI- (EC-Council)
Cisco Certified Network Associate (CCNA) – (Cisco)
Cisco Certified Network Associate (CCNA R &S) – (Cisco)
IBM Certified Ecommerce Specialist
ZAP Certified Web Designer
Security+ (CompTIA)
ECSA -EC-Council Certified System Analyst (EC Council)
CREST Practitioner Security Analyst- CPSA

Memberships:
IEEE, Cisco, EC Council, CompTIA, IBM, Microsoft, CSTA.

Alex's, areas of expertise include Cyber Security, Ethical Hacking, Cyber Crimes and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives in India, Asia, Cyprus and Middle East. With over 20 years’ experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences. He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cyber Security, Technology, Innovation and education. Alex's profile describes a confident and outgoing individual who enjoys the company of other people. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily. His levels of self-confidence mean that he rarely doubts his abilities in a social situation, although he may find it a little harder to deal with practical or impersonal situations. Alex's communicative and open style means that he tends to be trusting of others, or at least confide information more readily than many other personality types. Because of his social orientation, however, he finds it rather difficult to deal with rejection by other people, thriving as he does on their positive attention. His current research activities are directed towards Cyber Security, Internet of Things (IoT), Security in Next Generation Networks, Smart Technologies, Cybercrimes Investigations.

Retrieval Number: A9836109119/2019©BEIESP
DOI: 10.35940/ijeat.A9836.109119

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication