IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBERSECURITY ASPECTS OF BLOCKCHAIN

[1]Lincy N L, [2]Neenu Kuriakose

[1]Assistant Professor, [2]Research Scholar
[1]Computer Science,
[1]St Paul's College Kalamassery, Ernakulum, India

Abstract: Through the usage of cryptocurrencies, blockchain technology has been adopted in a variety of industries, the most prominent of which is banking. However, in terms of cybersecurity, the technique is practical. Since Satoshi Nakamoto's white paper on Bitcoin was published in 2008, blockchain has steadily grown in popularity as a means of safeguarding data storage and transmission through decentralized, trustless, peer-to-peer networks. In this paper we deal with how can blockchain help to improve cybersecurity and also what are its use cases in this space.

Index Terms **– Bitcoin, P2P, DDoS, Ethereum, IoT**

I. INTRODUCTION

Blockchain is a game-changing technology that is poised to transform the future of computing and disrupt a number of sectors with more inventive solutions. It is open, immutable, and distributed, making it useful in a variety of settings [1]. The amount of data we keep and process on the internet is growing, and maintaining data integrity has become one of the most difficult aspects of digital storage and communication. The blockchain is a cutting-edge technology that has the potential to solve data integrity issues. "Blockchains are tamper evident and tamper resistant digital ledgers executed in a distributed form (i.e., without a central repository) and typically without a central authority (i.e., a bank, enterprise, or government)," according to the National Institute of Standards and Technology (NIST)[2]. Stuart Haber's work is credited as being the first to propose the notion of time stamping documents and connecting the timestamps to ensure data integrity. Haber mentions in his article that he wants to discover a technique to automatically timestamp and make it impossible to update the stamp with a different date than the original. After a mysterious individual named Satoshi Nakamoto produced a whitepaper titled "Bitcoin: a peer to-peer electronic system" in 2009, the notion suggested by Stuart Haber became a reality [3]. By definition, a blockchain is a decentralized network of nodes in which each node stores data in the form of irreversible transactions. Cybersecurity professionals are continually searching for methods to strengthen security at the micro level in order to avoid data and information theft.

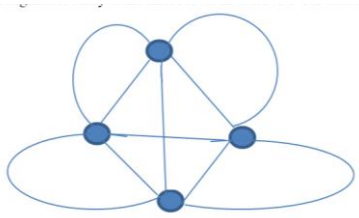

Figure 1. Blockchain Nodes

II. PRIVATE & PUBLIC BLOCKCHAIN: A COMPARISON

When bitcoin was launched in 2009, it was an open source system that anybody could use, and anybody could tweak the code to construct their own version of the blockchain. Since then, the blockchain has seen a lot of progress, and there was a need for a private blockchain. As a result, we may witness two different types of these days. There are two types of blockchain: private and public.

Public blockchains [4] are ones in which anybody may join the blockchain network and view and write data on the block. To attract additional people to join the network, the network usually contains an incentive system. Bitcoin is one of the most widely used public blockchain networks today. One of the disadvantages of a public blockchain is the vast amount of processing power required to keep a distributed ledger running at a wide scale. To obtain consensus, each node in a network must solve a sophisticated, resource-intensive cryptographic challenge known as a proof of work to guarantee that everyone is on the same page. Another

problem of public blockchain is its openness, which implies little to no transaction privacy and only supports a rudimentary idea of security [4].
Sometimes a blockchain network may only be required for select individuals, in this case, we can restrict blockchain access to the public and make this accessible for some whitelisted individuals. If the blockchain is not open to the public but only accessible to selected people, a private blockchain is termed. Most organizations employ private blockchain when the data are not made available to the public for the internal usage of organizations [1]

III. COMPUTER SECURITY IN BLOCKCHAIN

Blockchain is basically a network that logs and preserves multi-device, Peer-to-Peer network transactions and interactions (most commonly cryptocurrency transactions and records, for example). The decentralized nature of blockchain makes it safer to fight hackers and other cyber threats through the establishment of a network of devices. Because no one server is available for crooks and viruses. Blockchain has evolved so strongly in recent years initially responsible for securing financial transactions online. Something may be said about the incredible (and fearsome) strength of the increase in technological improvement in recent years, yet protection mechanisms are at least being created and increased simultaneously [5]. The CIA triad is an industry standard and all people who operate in the field of cyber security must know these three words and conditions. In the cyber-security industry Blockchain has the ability to leverage these three qualities. Blockchain features and it's implication to the CIA triad is explained below:

3.1.Confidentiality

Confidentiality on CIA triad refers to the privacy of information stored and processed digitally. It states that the information should be only available to the person who it belongs to. Although the blockchain transaction on a public blockchain is open to everyone and it is available publicly, it can provide confidentiality to the information of the user. Blockchain can fix this privacy concern since we may conduct a blockchain transaction and save our information without giving the third party our information. Because of the decentralization of the blockchain to peer database, there is no central authority to check our information. The data can only be viewed by an authorized user using the private secret key[1]

3.2.Integrity

The blockchain is a series of connected blocks that saves the hash value of previous linked blocks. If the information stored in the block changes, the hash value of the block changes as well. If a block's hash value is modified, then the hash value recorded in the following block will not be equal to. This makes the whole blockchain and blocks are not considered as a legitimate block in the blockchain. So it is difficult to change the data.

3.3 Availability

All the blockchain nodes will have a complete blockchain database so that if a node is unavailable, it won't affect the blockchains performance.[1] On blockchain there isn't a single fault point, because it is decentralized and all participating nodes have data saved. Traditional IT system has one fault and is susceptible to typical assaults such as DDoS.In the blockchain, assaults like DDoS are almost impossible since central servers that save and process information are not available.
When we study the current pattern of cyber assaults, we can understand the risk of possible cyber assaults for individuals, businesses and governments. Equifax's 2017 violation of data reveals that 143 million Americans, nearly 50% of the United States population, share sensitive personal data [6]. The personal information of half the US population was exposed in a single data breach. This case shows the risk of data infringements and the necessity for a strong information security system. The cyber danger is not simply the risk of digitally stored information, but goes well beyond that constraint. An assault by cyber can destroy the facilities and take a person's life. Stuxnet was a computer malware designed to attack Iran's nuclear power station launched to gain physical access to the machine [7].
Initially established as a coin, blockchain technology may be employed to tackle our current digital security dilemma. Giving a user a tracking experience during the production process, blockchain may be utilized in digital networks because it is a tamperproof technology. NIST engineer Thomas Hedberg noted, "We can develop confidence in the digital manufacturing networks since Blockchain provides us both skills" [8]. The information held inside the blockchain blocks cannot be modified to prevent misplay during the transmission.

IV. BLOCKCHAIN TO STRENGTHEN CYBERSECURITY

Blockchain is a P2P (peer to peer) decentralized network. Computers are termed "nodes" on this network. There is equal authority in all nodes of a public blockchain network such as Bitcoin, and no central admin. You cannot abuse the privileges of administrators and influence the network. Blockchain is a P2P (peer to peer) decentralized network.[9] Computers are termed "nodes" on this network. There is equal authority in all nodes of a public blockchain network such as Bitcoin, and no central admin. We cannot abuse the privileges of administrators and influence the network. With digital signatures, users of blockchain networks authenticate. These signatures cannot be hacked by cybersecurists as long as users safeguard their secret key[10]. Each blockchain node such as Bitcoin holds the whole data. By compromising one node, Hackers cannot stop this network, as each node has its own "distributed ledger" [11][12]. Data is encrypted on blockchain networks. With the computer capability now available cyber thieves cannot penetrate powerful encryption algorithms such as AES-256[13]. Consensus methods and cryptographic hash functions are used in blockchain networks. On a public blockchain network like Bitcoin or Ethereum, this prohibits hackers from altering or deleting entries[14]..

V. EMERGING BLOCKCHAIN USE CASE : SECURING IOT NETWORKS

The Internet of Things (IoT) is important in smart appliances, smart grids, smart cities, and other areas[15] .Sensors in IoT-enabled devices collect data and send it to IoT application servers, which then control the necessary actions. Hackers can eavesdrop on IoT networks since data is sent through the Internet. They have the ability to intercept data, modify it, and wreak significant harm. Consider the ramifications of hackers gaining control of smart power systems [15].End-to-end encryption is used in blockchain. Hackers won't be able to eavesdrop on IoT communications if this is done. The immutability of blockchain is provided by the combination of consensus methods and cryptographic hash functions. Blockchain databases include qualities such as decentralized trust model, high security, high public access, low to high privacy, and transferable identities, whereas centralized databases have qualities such as centralized trust model, poor security, low public access, high privacy, and non-transferable identities[16]. The blockchain is more sophisticated than centralized storage based on the qualities listed above. The following platforms are used to create blockchain-based IoT applications.

A. IOTA: IOTA is a new blockchain and IoT platform known as Next Generation Blockchains. This platform allows for great data integrity, transaction speed, and block validity while consuming fewer resources. It overcomes the drawbacks of blockchains [17].
B. IOTIFY: It offers a web-based internet of things solution in the form of bespoke apps to help overcome the limitations of blockchain technology [28].
C. iExec is a blockchain-based open source utility. It allows your programmes to benefit from the decentralized cloud benefits [21].
D. Xage: It's a secure blockchain platform for IoT that aims to boost automation and protect data [22].

VI. CONCLUSION

The blockchain is more than just cryptocurrencies. It is possible to build a large number of cases of use using the blockchain as a reliable infrastructure because of its security features. In this paper, we have outlined a number of these uses. With our ability to tap into blockchain technology, we gain an understanding of its potential, which includes a wide range of applications and covers various application cases in different fields. Using Blockchain can improve the basic features of a computation efficiency. Businesses using Blockchain can save on infrastructure and gain greater flexibility in the services they provide. In addition, features related to durability, safety, reliability and performance can be improved.

REFERENCES

[1] Bhattarai, Amar, Blockchain in Cybersecurity, Pros, and Cons (May 9, 2019). Available at SSRN: https://ssrn.com/abstract=3527922 or http://dx.doi.org/10.2139/ssrn.3527922
[2] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. (2018, October), Blockchain Technology Overview, Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Retrieved from: https://bitcoin.org/bitcoin.pdf
[4] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[5] https://blogs.unsw.edu.au/thedigitalage/blog/2019/02/blockchain-instrumental-in-digital-security-and- privacy/
[6] The Equifax Data Breach Retrieved from: https://www.ftc.gov/equifax-data-breach
[7] Stuxnet Malware Retrieved from: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet
[8] National Institute of Standards and Technology. (2019 February). Blockchain Provides Security, Traceability for Smart Manufacturing,Retrieved from: https://www.nist.gov/news-events/news/2019/02/nist- blockchainprovides-security-traceability-smart-manufacturing
[9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016,308 p.
[10] Alphand, Olivier, et al. "IoTChain: A blockchain security architecture for the Internet of Things." Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018.
[11] T. Swanson, Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems. R3 CEV, 2015.
[12] V. Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework," in IEEE Future Technologies Conference, June 2017.
[13] Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, A systematic literature review of blockchain cyber security,Digital Communications and Networks,Volume 6, Issue 2,2020,Pages 147-156,ISSN 2352-8648,
[14] Alex. R. Mathew, "Cyber Security through Blockchain Technology" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019
[15] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) 395411.
[16] Dorri, Ali & Kanhere, Salil & Jurdak, Raja & Gauravaram, Praveen. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 10.1109/PERCOMW.2017.7917634.
[17]. https://www.iota.org
[18] https://iotify.org
[19] https://iex.ec/overview
[20] https://xage.com
[21] Gokhan Sagirlar, Barbara Carminati, Elena Ferrari, John D. Sheehan, Emanuele Ragnoli "Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things – PoW Sub-blockchains", 2018 IEEE Blockchain International Conference