Fuzzy Systems and Soft Computing
ISSN : 1819-4362

THE ROLE OF BLOCK CHAIN TECHNOLOGY IN THE ENVIRONMENT OF CYBER SECURITY: A STUDY

Dr. M. Sakthivadivu Asst.Professor, Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India
Ms. E. Kanaka Asst.Professor Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India

Abstract –
Block chain challenges the traditional centralized trust framework of the Internet by introducing an innovative network architecture centered on decentralization, transparency, and audit ability. Ideally, block chain technology could enable the creation of a more decentralized, transparent, and democratic Internet. As a reliable and distributed database, block chain has potential applications across various sectors, including energy, agriculture, fishing, mining, recycling and reuse, air quality monitoring, and supply chain management. This paper examines the use of block chain technology in cyber security, analyzing three key vulnerabilities in information technology and evaluating how block chain can enhance security in these areas. Additionally, the study highlights the need for future research to focus on a specific block chain to develop cyber security applications, fostering integration and consistency among various solutions.

Keywords-
emphasizesdecentralization,transparency,auditability,Blockchain,cybersecurity.

I.INTRODUCTION

Cyber security involves safeguarding systems and networks against digital threats that seek to access, alter, eliminate digital information, often with the intent to extort money or sensitive data. As our dependence on technology and data continues to grow, it is crucial to enhance securityprotocols to ensure the protection of digital information and transaction. Cyber attacks can be carried out using various malware such as viruses, Trojans, Rootkits, etc. Some common types of cyber attacks are Phishing, Man in a middle (MITM) attack, Distributed denial of service (DDoS) attack, SQL injection, and Ransom ware attacks.

Block chain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. block chain is a technology that enables the secure sharing of information. Data, obviously, is stored in a database.

LITERATURE REVIEW

Blockchain database stores a data in blocks that are linked together in a chain. This technology which initially gained popularity with cryptocurrencies, facilities the availability ofa publicly maintained ledger of transaction.
Myriad ofother applications have emerged ever since. There has been a steady growth in the number of research studies conducted in this field; as such, there is a need to review the research in this field. This paper conducts an extensive review on 76 journal publications in the field of blockchain from 2016 to 2018 available in Science Citation Index (SCI) and Social Science Citation Index (SSCI)

database.
The aim of this paper is to present scholars and practitioners with a detailed overview of the available research in the field of blockchain. The selected papers have been grouped into 14 categories. The contentsofpapers in eachcategory are summarized and future researchdirection for each category is outlined. This overview indicates that the research in blockchain isbecoming more prominent and requires more effort in developing new methodologies and framework to integrate blockchain. It is the need of today's growing business that ventures into newtechnologies like cloud computing and Internet of Things (IoT).Block chain technology has obtained a lot of attention in recent years for its potential to magnify cyber security.

A block chain-based approach for secure data sharing in the cloud byY. Zhang,Y.Zheng, H. Zhu, and L. Zhao (2019): This paper proposes a block chain-based approach for secure data sharing in the cloud, which enhances security and privacy which was reducing the risk of data sets.SecuringIoTwithblockchain:AsystematicliteraturereviewbyA.V.S.S.K.Srinivas, S. Laxmi, and P. V. Reddy (2019): This paper presents a systematic literature review of blockchain-based solutions for securing the Internet of Things (IoT).

Blockchain-enabled secure and efficient data sharing for supplychain management byK. Liu, J. Chen, and X. Ma (2018): This paper proposes a blockchain-enabled data sharing framework for supply chain management, which enhances security, transparency, and efficiency.

A blockchain-based architecture for secure and reliable smart grid communications by L. Liang, W. Guo, H. Zhang, and J. Deng(2018): This paper proposes a blockchain-based architecture for smart grid communications, which provides secure and reliable data exchange.

A survey on block chain technology and its security, Huaqun Guo, Xingjieyub, Institute for Infocomm Research, A*STAR, Singapore. Thispaper presentsa systematic review ofthe use of blockchain technology in cybersecurity.

II. STRATEGY

Blockchain technology could revolutionize the cybersecurity space. The distributednature and strong cryptographic security make it an attractive option for securing sensitive data andtransactions. In summary, block chain methods in cyber security include the use of distributed systems, cryptographic security, immutable ledgers, intelligent contracts, private and public key encryption and consensus mechanisms. These techniques work together to create a secure, operational system that can protect sensitive data and transaction from malicious attacks.

III. PHARSE LOGIES IN BLOCKCHAIN TECHNOLOGIES:

- ✓ Node:Acomputerrunningblockchainsoftwareis called nodes.
- ✓ Miningnodes:Subsetofnodesandsetofcomputersrunningblockchainsoftware
- ✓ Full nodes: The job ofa full node is to storethe blockchain data, pass along the data to other nodes, and ensure newly added blocks are valid.
- ✓ Lightweight nodes: Lightweight nodes do not need to store full copies ofthe blockchain and often pass their data on to full nodes to be processed. Lightweight nodes are generally found on smartphones and Internet of Things (IoT) devices i.e. devices with limited computational and/or storage capability.
- ✓ Miner: A miner is a participant in a Blockchain that participates in securing the network and validating new transactions. The mining and validation process happens via competitive, voting or luck-based methods dependant on the consensus protocol chosen.
- ✓ CryptographicNonce: Anarbitrarynumber(usuallyrandomlyselected)that isusedonce.

IV. AIM AND OBJECTIVE

Blockchain is decentralized ledger systemthat's duplicate and distributed across a whole network of computer systems. It allows information access to all designed nodes or members who can record, share and view encrypted transactional data on their blockchain.

Block chain offers a different path toward greater security, one thatis less traveled and not nearlyashospitable to cybercriminals. This approach reduces vulnerabilities, provides strong encryption, and more effectively verifies data ownership and integrity.

V. USE-CASES OF BLOCKCHAIN FOR CYBER SECURITY

Technologies involved in building blockchain based platforms and applications have the potential for improved security, but technologies are never the starting point. Security leaders must work with product and platform builders to first identify the problems, interactions and tradeoffs for new security capabilities and then they can actively design, test, implement and manage them.

1. Resilience and availability

Decentralized infrastructure helps support resilience against attacks, corruption and downtime. This process mitigates the following vulnerabilities:

2. Data integrity

Data on blockchains can't be altered because network nodes cross-reference and build upon each other and require consensus to verify transactions. Data off-chain, however, can be corrupted. This iswhereon-chain signaturescanenable new blockchainuse caseswheresecurity is paramount. Decentralized voting, health and scientific data collaboration across institutions, and decentralized metadata.

3. Traceability and provenance

Transparency and traceability are core to blockchain designs, but their security benefits manifest differently in different applications. In a supply chain context, a digital distributed ledger stores tamper-proofrecords oftransactions and freight data across parties and the product lifecycle. This reduces the risks ofcounterfeiting and tampering by any single party. In financial usecases, transparencyand immutabilityofpayment historyreducetheneed for acentralbroker. Blockchains can also improve the security and privacy of transactions, such as remittances and cross-border payments.

4. Authentication of software and device interactions

Transactions on a blockchain are not always finance-based; they can be used for any verifiable interaction, such as helping prevent IoT device compromise. Blockchain hashing can help organizations verifyupdates, downloads and patcheswith the product'sdeveloper. This also helps prevent supply chain attacks, particularly as software and edge IoT devices are prime targets for network entry.

5. Authentication of individuals

Several components of blockchain can be applied numerous security benefits, including the following:

Sensitive Data Protection: Block chain technology can modify how information is stored on-chain, such as using a hash instead of directly storing personally identifiable information.

Data Minimization: IT teams can utilize cryptographic techniques like zero-knowledge proofs or selective disclosure to reveal only the necessary information for an application's functionality.

Identity Theft Prevention: Block chain employs cryptographic keys to authenticate identity attributes and credentials, reducing the risk of identity theft.

Multi signature Access Controls and Decentralized Administration: Blockchain helps prevent errors, takeovers, or fraud by ensuring that no single entity has complete control.

Private Message Protection: Companies can leverage blockchain’s encryption and hashing capabilities to safeguard data shared in messaging, chat, and social media applications.

Ownership validation

Proving ownership of online assets was difficult before the existence of digital ledgers. Even in the physical world, deeds can be destroyed, certifications don't always hold up across borders and hundreds ofmillions ofpeople lack access to stable government identityor financial services.Just asnon-fungibletokens(NFTs)enableartiststodigitallywatermarktheir media,the ability to create an immutable record of authenticity and ownership with cryptographic keys has numerous security benefits across many blockchain use cases, including the following:

VI. BLOCKCHAIN SECURITY ISSUES AND CHALLENGES

Blockchain hasgot verycomplex and rugged structure. Inspite ofthis, in this technology there exist following problems and challenges:

Traditional Challenges:

When a distributed ledger is used, data is shared among all counterparties on thenetwork.Thissharing ofdata may have a potential negative impact onconfidentiality, but it also hasapositive impact onavailability.

Key Management: Private keys serve as the direct means of authorizing activities from an account. If these keys are accessed by an adversary, it can compromise any wallets or assets secured by them. It is worth noting that potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to dataset would be able to read the underlying data. A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. Ifa user loses a private key, then any asset associated with that key is lost. If a private key is stolen, the attacker will gain full access to all assets controlled by that private key. Once a criminal steals the key and transfers funds to another account, the action cannot be undone.

a. Cryptography: Blockchain implementations always rely on cryptographically generated public and private keys. When it comes to cryptography, it is crucial to adhere to stringent policiesandproceduresformanagingkeys,encompassingpeople,processes,andtechnology. The software responsible for generating cryptographic keys should produce strong keys that are not easily decrypted.

b. Privacy:Privacyisanadditionalissuethat emerges fromtheuseofBlockchaintechnology. In permission less ledger, all counterparties have the abilityto download the ledger, allowing them toexploretheentire historyoftransactions, eventhose inwhichtheyarenot directlyinvolved.In a permissioned ledger, the utilization of authorized agent or smart contract capabilities could result in a serious exposure of privacy, depending on the access rights granted to the agent or smart contract authors.

VII. CONCLUSION AND FUTUREWORK

Blockchain technology is continuously developing and discovering new applications in the modern world. One such area of interest is cybersecurity, where it has been extensively studied and implemented. The Blockchain infrastructure offers practical solutions to address security challengesinvarious domains,includingIoT devices, networks, and data transmission and storage. A study, conducted by Taylor et al., assessed the feasibility of applying Blockchain technology and involved the input of 30 researchers. The study revealed a notable focus among Blockchain security researchers on implementing Blockchain security for IoT devices. In addition to IoT devices, other significant areas of interest for Blockchain security include networks and data. The discussions highlighted the potential of Blockchain technology in enhancing the security of IoT devices through more robust authentication and data transfer mechanisms.

Blockchain applications have advanced and strengthened existing efforts in cybersecurity to enhance security and deter malicious actors. This research emphasizes the potential for future studies in cyber security areas beyond the realm of IoT. As the World Wide Web moves towards widespread adoption of HTTPS encryption, and as end users increasingly utilize various forms of encryption for everyday communication, there is a growing need to securely manage the surrounding cryptography and certification schemes.

VIII. REFERENCES

1. Swan,Melanie.Blockchain:Blueprintforaneweconomy,O'ReillyMedia,Inc.,2015.
2. Iansiti,Marco,andKarimR.Lakhani."Thetruthaboutblockchain."HarvardBusinessReview 95.1 (2017.
3. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016).
4. CachinC.Architectureofthehyperledgerblockchainfabric.InWorkshopondistributed crypto currencies and consensus ledgers2016, 310(1).
5. Zheng,Zibin,et al."Block chain challenges and opportunities: A survey."International Journal of

Web and Grid Services, 2018,14.4.
6. Li, Wenting, et al. "Securingproof-of-stakeblockchainprotocols."DataPrivacyManagement, Crypto currencies and Block chain Technology. Springer, Cham, 2017.
7. Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." Computer Science-Research and Development, 2018.
8. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019.