JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain in CyberSecurity

[1]Tejas Rasane, [2] Sairaj Sarde, [3] Omkar Lakade

[1] Btech Student, [2] Btech Student, [3] Btech Student
[1] IT department,
[1] VIIT, Pune, India.

Abstract : This abstract aims to explore the potential of blockchain technology in cybersecurity. The paper will first provide an overview of blockchain technology and its key features. It will then discuss the various use cases of blockchain in cybersecurity, including secure data storage and sharing, identity management, and secure communication. The paper will also examine the limitations of blockchain technology and its potential impact on cybersecurity. The conclusion will summarize the potential benefits of blockchain technology in cybersecurity and discuss future research directions. Overall, the paper will show that blockchain technology has the potential to significantly enhance cybersecurity and protect against the growing threat of cyber attacks.

Blockchain is a disruptive technology intended to implement secure decentralised distributed systems, in which transactional data can be shared, stored, and verified by participants of the system without needing a central authentication/verification authority. Blockchain-based systems have several architectural components and variants, which architects can leverage to build secure software systems. However, there is a lack of studies to assist architects in making architecture design and configuration decisions for blockchain-based systems. This knowledge gap may increase the chance of making unsuitable design decisions and producing configurations prone to potential security risks. To address this limitation, we report our comprehensive systematic literature review to derive a taxonomy of commonly used architecture design decisions in blockchain-based systems. We map each of these decisions to potential security attacks and their posed threats. MITRE's attack tactic categories and Microsoft STRIDE threat modeling are used to systematically classify threats and their associated attacks to identify potential attacks and threats in blockchain-based systems.

I. INTRODUCTION

Cybersecurity is the practice of protecting systems and networks from digital attacks which aim to access, change or destroy digital information either to extort money or sensitive data. With the increasing reliance on technology and data, it becomes very important to reinforce security measures to protect digital data and transactions.

Cyberattacks can be carried out using various malware such as viruses, Trojans, Rootkits, etc. Some common types of cyberattacks are Phishing, Man in a middle (MITM) attack, Distributed denial of service (DDoS) attack, SQL injection, and Ransomware attacks.

The blockchain technology is redefining the way business function. There are several vulnerabilities associated with blockchain technology. This text mining literature analysis demonstrates and discusses prominent blockchain vulnerabilities. The findings show ever-evolving security threats related to the blockchain technology. Highlights future research dimensions for designing secure blockchain applications and platforms.

II. LITERATURE REVIEW

Blockchain consists of an ordered list with nodes and links where the nodes store information and are connected through links called chains. This technology supports the availability of a publicly maintained ledger of transactions, first gaining mainstream attraction with cryptocurrencies. A myriad of other 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 contents of papers in each category are summarized and future research direction for each category is outlined. This overview indicates that the research in blockchain is becoming 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 new technologies like cloud computing and Internet of Things (IoT) . Certainly! Blockchain technology has gained a lot of attention in recent years for its potential to enhance cybersecurity.

Here are some research papers that explore the intersection of blockchain and cybersecurity:

"Blockchain technology for improving cybersecurity in the internet of things" by A. Dorri, M. Steger, S. Kanhere, and R. Jurdak (2017): This paper explores how blockchain technology can enhance the security of the Internet of Things (IoT) by creating a decentralized, secure, and tamper-resistant network.

"Blockchain-based secure firmware update for embedded devices in an Internet of Things environment" by T. Kim, J. Kim, and H. Chung (2019): This paper proposes a blockchain-based secure firmware update mechanism for IoT devices.

"Blockchain technology in healthcare: A systematic review" by S. Xu, S. Ou, Y. Li, and X. Zhou (2018): This paper reviews the use of blockchain technology in healthcare.

"A survey on the security of blockchain systems" by Y. Zhang, X. Wen, and G. Zhao (2018): This paper provides a comprehensive survey of the security of blockchain systems, including threats, vulnerabilities, and countermeasures.

"A blockchain-based architecture for secure and decentralized sharing of medical imaging data" by A. E. A. Al-Hamami, Y. Al-Dhuraibi, and A. Al-Hamami (2021): This paper proposes a blockchain-based architecture for secure and decentralized sharing of medical imaging data.

"A blockchain-based approach for secure data sharing in the cloud" by Y. Zhang, Y. Zheng, H. Zhu, and L. Zhao (2019): This paper proposes a blockchain-based approach for secure data sharing in the cloud, which enhances security and privacy while reducing the risk of data breaches.

"Securing IoT with blockchain: A systematic literature review" by A. 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 supply chain management" by K. 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.

"Blockchain technology in cybersecurity: A systematic review" by A. V. S. S. K. Srinivas, S. Laxmi, and P. V. Reddy (2018): This paper presents a systematic review of the use of blockchain technology in cybersecurity.

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 2023 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.

Blockchain technology has the potential to revolutionize the field of cybersecurity. Its decentralized nature and strong cryptographic security make it an attractive option for securing sensitive data and transactions. In conclusion, the methodology of blockchain in cybersecurity involves the use of decentralized systems, cryptographic security, immutable ledgers, smart contracts, private and public key encryption, and consensus mechanisms. These techniques work together to create a secure and tamper-proof system that can protect sensitive data and transactions from malicious attacks.

IV. TERMINOLOGIES IN BLOCK CHAIN TECHNOLOGIES:

- Node: Any computer running block chain software is called nodes.
- Mining nodes: Subset of nodes and set of computers running block chain software
- Full nodes: The job of a full node is to store the 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 of the 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 either competitive, voting or luck-based methods dependant on the consensus protocol chosen.
- Cryptographic Nonce: An arbitrary number (usually randomly selected) that is used once.

V. AIM AND OBJECTIVE

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

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed.

Blockchain offers a different path toward greater security, one that is less traveled and not nearly as hospitable to cybercriminals. This approach reduces vulnerabilities, provides strong encryption, and more effectively verifies data ownership and integrity.

VI. USE-CASES OF BLOCKCHAIN FOR CYBER SECURITY

One of the most secure ways to conduct transactions in the digital world has made it an alluring proposition for many sectors, including financial services. Organizations can develop cybersecurity solutions for many other applications and technologies by leveraging integrity assurance -

DNS and DDoS Attack Mitigation

A distributed denial of service (DDoS) is when a cybercriminal floods a network with malicious traffic that prevents it from functioning correctly. These attacks slow down or completely shut down a website or resource system. In the case of Domain Name System (DNS) attacks, attackers either compromise a network's DNS or exploit underlying attributes to launch a broader attack. It enables the establishment of peer-to-peer (P2P) and zero-trust networks, removing the need for devices to trust each other and eliminating single centralized points of failure. Organizations can decommission the attacked node and continue working as usual. Even if large parts of its network are attacked, the system will continue to function due to its decentralized structure.

Resilience and availability

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

Distributing information and communications technology networks helps reduce data exposure and redirect users when a centralized database goes offline or is attacked.

Decentralizing DNSes is helpful for redundancy in the event of a DDoS attack.

In an IoT context, distributing operations and administrative controls away from a central hub enables security decisions to be made closer to the periphery of the network.

KYC Verification

Fraudulent e-KYC renewal is one of the latest methods scammers use to trick naive people. The scammer poses as her service provider and asks for confidential information such as their Aadhaar number and bank account details. This scenario can be avoided by using their KYC verification method.

As a distributed ledger, it allows data from various governments and private data portals to be collected and stored in a single, immutable, secure database. Cryptographic keys (a means of encrypting data in machine-readable form) protect each user's private information on the ledger. Hackers and cybercriminals will have difficulty cracking the keys and gaining access to the necessary credentials.

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-proof records of transactions and freight data across parties and the product lifecycle. This reduces risks of counterfeit and tampering by any single party. In financial use cases, transparency and immutability of payment history reduce the need for a central broker. Blockchains can also improve security and privacy of transactions such as remittances.

End User Security

Hackers are increasingly using edge devices such as thermostats and routers to penetrate systems. Cybercriminals can easily infiltrate through centralized control and edge devices with the rapid proliferation of smart devices and home automation.

It helps secure IoT systems and end-user devices by decentralizing management. The device can make security decisions without relying on central administrators or permissions. These advantages are one of the primary reasons for the popularity of this technology in financial institutions such as banks. For example, end-user security in banking is a complicated problem. Simple logins centralized IT infrastructure, and weak passwords often allow cyber attackers to penetrate network infrastructure. It enables passwordless authentication of users and devices with multi-party verification via SSL certificates. The decentralized and decentralized nature of the network that checks the integrity of transactions and account balances makes attacks virtually impossible.

Limitations

This complete analysis considers the different phases of the blockchains since the early evolution in 2013 to study their cyber security aspects. We have also analyzed over 60 vulnerabilities in different blockchain networks and applications. The work concludes that we have successfully figured out the trade-off between cyber attacks on BC technologies due to new vulnerabilities and growth in the cybersecurity-related research works done in blockchain over the last decade.

The outcome of our study gives insights to plan for detecting and mitigating specific vulnerabilities for secure development practices in blockchains. However, our study is carried out on an uneven number of research works done for different domains of application for cyber security in blockchains. Although the insights tell that it might be needed to specify a different approach for different blockchain networks or solutions based on their application domain, architecture, and complexity.

VII. BLOCKCHAIN SECURITY ISSUES AND CHALLENGES

Blockchain has got very complex and rugged structure. In spite of this, in this technology there exists following problems and challenges w.r.t to security.

Traditional Challenges:

The use of a distributed ledger implies that data is shared between all counterparties on the network. On one side this could potentially have a negative impact on the confidentiality; while on the other, it has a positive impact on availability with many nodes participating in the Blockchain, making it more robust and resilient. Some of traditional security challenges are:

a. **Key Management** : Private keys are the direct means of authorizing activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys. Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a 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. If a user loses a private key, then any asset associated with that key is lost. If a private key is stolen, the attacker will have full access to all assets controlled by that private key and once a criminal steals the key and transfer funds to another account, it cannot be undone.

b. **Cryptography** : Blockchain implementations always operate on the cryptographically generated public and private keys. In case of cryptography, stringent policies and procedures always be followed when managing keys, including people, processes and technology. The software which is used to generate cryptographic keys should generate strong keys which could not be decrypted easily.

c. **Privacy :** Privacy is an additional issue that emerges from the use of Blockchain technology. In a permissionless ledger, all counterparties are able to download the ledger, which implies that they might be able to explore the entire history of transactions, including those to which they are not members. In a permissioned ledger, exploitation of authorised agent' or smart contract capabilities could lead severe exposure of privacy, according to the access right of the agent or smart contract authors.

VIII. CONCLUSION AND FUTURE WORK

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

This research has identified available recent research on how blockchain solutions can contribute to cyber security problems. The initial keyword searches for this research and current media reports highlight blockchain as a standalone technology that brings with it an exorbitant array of possible solutions for finance, logistics, healthcare and cyber security. This research has focused solely on cyber security. Undoubtedly, there are worthy applications for blockchain, however, a decentralized, trustless system cannot by itself solve all problems one may uncover in the field of cyber security.

Blockchain applications for cyber security have evolved and bolstered the existing efforts to enhance security and to deter malicious actors. This research highlights opportunities available for future research to be conducted in areas of cyber security outside the realm of IoT. As the World WideWebmovestowards a massadoption of https encryption and the end users are increasingly using some forms of encryption for everyday communication, there is an ever increasing need to securely manage the surrounding cryptography and certification schemes.

IX. 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.