The Effectiveness of Blockchain Technology in Detecting, Mitigating and Securing Cyber Threats

Vinitha Kandukuri
Gannon University, Square, Wrie, PA 16541, USA

OPEN ACCESS

Key Words
Cyber threats, blockchain technology, security, several factors, cyber security, secure data sharing

Corresponding Author
Vinitha Kandukuri,
Gannon University, Square, Wrie, PA 16541, USA

Received: 30 December 2023
Accepted: 15 May 2024
Published: 25 May 2024

Citation: Vinitha Kandukuri, 2024. The Effectiveness of Blockchain Technology in Detecting, Mitigating and Securing Cyber Threats. Asian J. Inf. Technol., 22: 1-7, doi: 10.36478/makajit.2024.1.1.7

Abstract

The rise of cyber threats has created a pressing need for effective cyber security solutions. However, traditional security measures may not be enough to address the expanding and evolving threat landscape. Block chain technology has emerged as a promising solution for improving cyber security by providing a secure and decentralized platform for data sharing and storage. This study explores the effectiveness of block chain-based security measures in detecting and mitigating cyber risks, including applications such as smart contracts and decentralized identity management. The study analyzes the advantages and limitations of block chain technology and the factors that affect its effectiveness, such as network size, consensus method, interoperability and scalability. The study also highlights the challenges and opportunities associated with the implementation of block chain-based security measures, including legal and regulatory considerations. The results of the study show that block chain technology has the potential to automate security procedures and give users more control over their personal data, thus improving cyber security. However, the effectiveness of these measures depends on several factors, including the complexity of the network, the type of consensus method used and the interoperability of different block chain systems. Further research and development are needed to fully leverage the potential of block chain technology for enhancing cyber security.

INTRODUCTION

As the number of cyber threats and attacks continues to rise, traditional cyber security measures may not be sufficient to address the evolving threat landscape. In recent years, block chain technology has emerged as a promising solution for improving cyber security. Block chain is a decentralized and distributed ledger technology that enables secure and transparent transactions without the need for intermediaries or trusted third parties. By offering a safe and open framework for data sharing and storage, block chain technology can enhance cyber security by providing better protection against cyber risks.

Block chain-based security measures can help detect and mitigate cyber threats by automating security procedures and giving users more control over their personal data. For example, smart contracts can be used to automatically execute security protocols based on predefined conditions, while decentralized identity management systems can provide users with more control over their personal information. Block chain technology can also provide better resilience against cyber-attacks by ensuring data integrity and reducing the risk of data tampering or manipulation[1].

Its decentralized nature has the potential to completely transform how companies conduct business in a variety of sectors, from healthcare to supply chain management. By fully utilizing this technology, businesses can radically restructure their operations. Additionally, Blockchain can strengthen internet security, reducing its susceptibility to hacker attacks. It can also give people more power by giving them more control over their data.

However, the effectiveness of block chain-based security measures depends on numerous factors, such as the network size, consensus method and interoperability of different blockchain systems. For instance, the consensus method used in a blockchain system can affect its security and scalability, while the interoperability of different blockchain systems can impact their ability to share data and resources. Therefore, it is important to examine the advantages and limitations of block chain technology and the factors that affect its effectiveness in detecting and mitigating cyber risks.

Block chain offers a special route to stronger security that is less vulnerable to cyber attacks. This strategy decreases vulnerabilities, employs strong encryption and more effectively verifies the ownership and integrity of data. It may even make it unnecessary to need passwords, which are frequently seen as cyber security's weakest link.

This study explores the effectiveness of block chain-based security measures in enhancing cyber security, with a focus on the factors that affect their effectiveness. The study aims to provide insights into the potential of block chain technology for improving cyber security and to identify the challenges and opportunities associated with the implementation of block chain-based security measures. By analyzing the advantages and limitations of block chain technology, the study seeks to provide a better understanding of its potential for enhancing cyber security in the face of expanding cyber threats.

Public, Private and Hybrid Block Chains

Public Block Chain: Anyone may join and contribute to a public block chain, which has completely open read access. To encourage participation, public block chains frequently use Proof of Work consensus algorithms.

Private Blockchain: Often the opposite of a public block chain, a private block chain allows only authorized users to write, read and join the network. This frequently requires an invitation to join, after which the network creator or a set of rules established determines if a person is eligible to join[2].

Hybrid: A consortium block chain, commonly referred to as a hybrid block chain, combines features from both private and public chains. It alludes to a closed environment where numerous parties collaborate to share data and conduct transactions. Additionally, members can choose which activities should be confined to a smaller set of members and which ones can remain public.

The Role of Blockchain in Detecting and Preventing Cyberattacks: With blockchain technology, you can protect your company from data breaches, cyberattacks and identity theft to guarantee the privacy and security of your critical information and your organization. The blockchain revolution in Cyberattacks detection and prevention are only getting started., things will only get better and better. Here are several ways blockchain can aid in the detection and advertence of cyberattacks[3].

Eliminating Human Factor from Authentication: Businesses may authenticate individuals and gadgets without the need for a password by utilizing blockchain technology in their operations. By removing human interaction from the authentication process, this stops human interference from being an attack vendor. By enabling an organization's security system to utilize a distributed public key infrastructure, blockchain authenticates people and devices. This installs a unique SSL certificate on each device in place of a password. Since the certificate data is handled on the blockchain, it is extremely difficult for attackers to use fictitious certificates.

Distributed Storage : There is no central organization or repository in the chain due to the way that blockchain is designed. Instead, each member of the network contributes to the storage of some or all the blockchain. Verifying the data that is shared and/or maintained is the responsibility of every user on the network. This removes the possibility of adding bogus data to the blockchain network or removing current data from it.

Traceability: Each transaction made on the blockchain network, whether it is added to a private or public blockchain, is electronically signed and time stamped. This enables enterprises to locate the matching participant on the blockchain using their public address and go back in time for each transaction.

The audit feature of the blockchain guarantees an elevated level of safety and transparency for each network transaction. Businesses are reassured that their data is real and not tampered with by this in terms of cyber security.

DdoS: The present Domain Name System is a barrier to thwarting assaults that result in distributed denial-of-service. (DDoS). Businesses may totally decentralize the Domain Name System (DNS) by integrating blockchain technology, allowing material to be distributed to numerous different nodes and making it hard for hackers to compromise a system.

Data Manipulation and Fraud: Immutability is one of the key characteristics of blockchain technology. Together with the network's decentralized structure, the use of cryptography and sequential hashing in blockchain makes it almost impossible for any person to unilaterally change the ledger's data. Organizations can use this capability to maintain data integrity and detect and prevent any tinkering with data.

Enhanced Risk Management: Fraudulent incidents can be dealt with very effectively by deploying a fraud prevention system that is based on a distributed ledger approach, like in the case of the blockchain network. A distributed ledger system, the blockchain network will keep a record of previous transactions for reference and verification. With blockchain technology, organizations can mitigate, or in some cases, eliminate risks posed by current systems.

Proponents of the blockchain technology claim that it improves risk management by ensuring data records that are hard to change, which helps preserve records and proof. By increasing transparency for all parties, blockchain also improves risk management.

Secure IoT: To create IoT solutions, an unprecedented level of connectivity, coordination and cooperation amongst all the devices in the IoT ecosystem is needed. Additionally, all gadgets need to communicate with one another and integrate with one another. But they must interact and communicate with connected systems in a secure way. It can be time-consuming, challenging and expensive to secure IoT devices without a new strategy.

The IoT ecosystem may find some benefit from blockchain. Blockchain technology makes it feasible to keep track of billions of connected devices and makes it simpler to perform transactions and coordinate across devices, which can save IoT device manufacturers a significant amount of money. But more significantly, it will do away with single points of failure to guarantee a more robust IoT ecosystem from which devices may operate.

Literature Reviews:

- This literature review explores the potential of blockchain technology for enhancing cyber security, including its applications for identity management, secure data sharing and distributed ledger technology. The authors examine the advantages and limitations of blockchain-based security measures, including the need for standardization, scalability and interoperability[4].
- This literature review provides an overview of the role of blockchain technology in cyber security, including its potential applications for threat detection, secure data storage and secure communication. The authors explore several types of blockchain-based security measures, such as smart contracts and consensus mechanisms and their effectiveness in mitigating cyber threats[5].
- This literature review discusses the challenges and opportunities of using blockchain technology for enhancing cyber security, including the need for regulatory frameworks, interoperability and scalability. The authors examine the potential applications of blockchain technology for cyber security, such as secure identity management and secure data sharing and the challenges associated with implementing these measures[6].
- This literature review explores the potential of blockchain technology for enhancing cyber security, including its applications for secure data sharing, secure communication and identity

management. The authors examine the advantages and limitations of blockchain-based security measures, such as smart contracts and consensus mechanisms and the challenges associated with implementing these measures[7].

MATERIALS AND METHODS

Based on the Ethereum blockchain platform, the suggested design is adaptable to other blockchain platforms. Scalable open source blockchain platform Ethereum blockchain can manage numerous concurrent transactions. The Ethereum blockchain network is additionally adaptable and compatible with common operating systems. It uses distributed computing with smart contracts that is built on the blockchain. An agreement between consortium members stored on the chain and managed by all participants is called a smart contract. Despite being a public blockchain, the Ethereum platform is set up and operated in this work as a secure blockchain network that can accept public nodes without authorization[8]. As a result, both private and public blockchain networks' characteristics are present in the architecture. To safely store and distribute Cyberattacks features and signatures, it mixes both public and private blockchain qualities. It is referred to as a public blockchain because open nodes are free to join or depart the network, whereas it is considered a private blockchain since only approved nodes can prepare, verify and validate transactions.

Authorized Nodes: A second name for the permitted nodes is miners. The conditions that are included in the smart contract are established by the nodes. They hold the privilege to prepare, submit and verify transactions because they are the trusted nodes. They may act as independent nodes or as entry points to other networks. Additionally, they execute the consensus algorithm, validating transaction blocks. The database is updated by all approved nodes.

Unauthorized Nodes: Also go by the name "public nodes." They connect to the network to access information about previous attacks. Aside from serving as standalone nodes, they can also act as network gateways. Because they are not trusted, public nodes do not add transactions to the blockchain[9].As a result, they lack the authority to create, check, approve, or run the consensus algorithm.

Data Base: The addresses of the mined blocks are kept in the database, which is available to all nodes. Authorized nodes change the block information, but all public nodes only have read-only access to it. The genesis block of the blockchain network is also kept in the database. Each node that desires to become part of the blockchain network needs the genesis block.

Cyber Security use Cases for BlockChain Technology

Secure Private Messaging: Social networking sites allow for the collection of a considerable number of metadata and most users use flimsy and unreliable passwords to secure their accounts and data. To enable end-to-end encryption and secure user data, many messaging firms are converting to Blockchain. A common safety system is built using blockchain. To provide cross-messenger interaction features, it creates a uniform API structure[9]. Social networking sites like Face book and Twitter have been the target of countless hacks that resulted in data breaches and gave user information to the wrong people. Such cyberattacks are prevented by blockchain technology.

IoT Security: The usage of routers and thermostats by attackers to enter the system is on the rise. Smart switches, a vulnerable edge component, give hackers simple access to the entire house automation system.

By decentralizing the management of such susceptible systems and devices, blockchain effectively safeguards them. Devices are now capable of making security choices on their own thanks to blockchain, AI, and IoT technology. The lack of centralized authority increases the security of IoT devices and enables them to recognize and respond to questionable commands coming from unidentified networks.

Secure DNS and DDoS : The Domain Name System (DNS) is a centralized system that provides an easy target for attackers to exploit the connection between IP addresses and website names. This leaves website vulnerable to DNS attacks that can result in cashable, inaccessible and redirected sites. Additionally, Distributed Denial of Service (DDoS) attacks can overload resources such as servers and website, causing them to slow down or shut down completely.

However, the emergence of Blockchain technology presents a potential solution to these issues by decentralizing DNS entries[10]. By removing the single-point entry that attackers typically exploit, decentralized systems make it more difficult to carry out DNS and DDoS attacks. In this way, Blockchain technology offers a promising remedy to the vulnerabilities associated with centralized DNS systems.

Provenance of Software: The MD5 cryptographic algorithm is commonly used to ensure the security and integrity of firmware updates, patches and installers, as well as to prevent malware from entering systems. This algorithm functions by comparing the identity of new software to hashes stored on the vendor's website. However, MD5 has been shown to be vulnerable to attacks, as the hashes on the vendor's website may have already been compromised.

Fortunately, Blockchain technology provides a solution to these vulnerabilities. By permanently recording hashes and preventing any changes to the data, Blockchain technology offers a more secure and efficient method of verifying software identity. In this way, Blockchain provides a more reliable method for comparing hashes to those stored on the ledger, offering greater protection against potential attacks.

Verification of Cyber-Physical Infrastructures: Cyber-physical systems are vulnerable to system misconfiguration, data tampering and component failure, leading to the compromise of data integrity. However, Blockchain technology can be utilized to prevent such threats by ensuring data integrity and performing verification to validate the status of cyber-physical infrastructure. By leveraging Blockchain, data generated from physical infrastructure components is more reliable and trustworthy, providing a more secure chain of custody[11]. Blockchain's tamper-proof and decentralized nature ensures that data cannot be modified or manipulated, thereby providing a robust solution for maintaining the integrity of data generated by cyber-physical systems.

Reduced Human Safety Adversity Caused by Cyberattacks: Blockchain technology can provide a solution for preventing cyber-attacks on automated military vehicles and equipment. These systems operate on a closed network, making it challenging for hackers to gain access to sensitive data. However, if a single point of the network is compromised, the entire system can be at risk. By implementing data verification through Blockchain technology, any potential data tampering can be detected and prevented, ensuring the security and safety of military operations.

Existing System: Rotational cyber security solutions, including firewalls, intrusion detection systems and antivirus software, have been developed to detect and mitigate known cyber threats by analyzing network traffic and data. However, as cyber threats multiply and become more complex, these solutions may not be sufficient to protect against all potential attacks. This has resulted in the development of more advanced cybersecurity solutions that incorporate machine learning, artificial intelligence and blockchain technology.

Blockchain-based security solutions have been developed for a range of applications, including identity management, data encryption and supply chain management. These solutions leverage blockchain's decentralized architecture to create secure and transparent systems that give users control over their data[11]. For example, some solutions use blockchain to create decentralized identity management systems, while others use it to establish secure data sharing and storage mechanisms.

As cyber threats continue to evolve, existing systems for detecting and mitigating these threats must also evolve. Incorporating blockchain technology into these systems provides an opportunity to enhance cyber security by creating a safe and open framework for data sharing and storage, automating security procedures and empowering users to take control of their personal data.

Proposed System: The proposed system in a research paper on the effectiveness of blockchain technology in detecting and mitigating cyber threats would be a blockchain-based security solution incorporating smart contracts and decentralized identity management. It aims to enhance cyber security by automating security procedures and giving users control over their data. Smart contracts could be used to enforce security protocols and[12] automate the detection of cyber

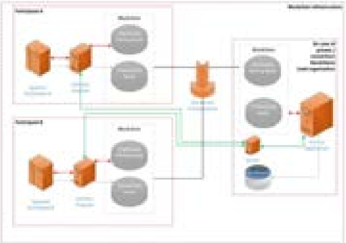
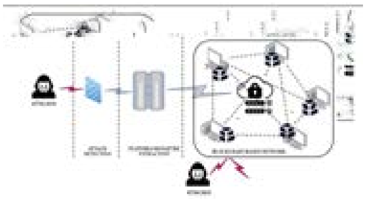


Fig 1: Example of Block chain showing private and public



Picture 2: Block chain based network

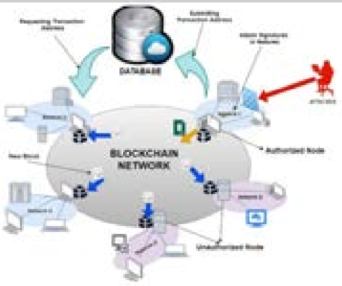


Fig 3: A visual illustration of the suggested architecture.

Table 1: Summarizes the distinctions between public and private blockchain types and their traits with Examples.

	Public	Private
Examples	Bitcion and Ethereum	Hyper ledger-Fabric and R3 Corda
Consensus algorithm	Commonly used are Proof of Stoke and Proof of Work	Agreed upon with pre-defined rules Proof of Authority mostly used in the Netherlands
Scalability of the network (Txs/second)	Low	High
Participation in network	Mostly Permissions users are free to join	Mostly Permissioned. A defined groups of participants
Development	Determined by the community	Controlled by a central party
Privacy when using personal data	Not recommended	Not recommended. Links to data thought back chains is safe up to A certain degree.
Identity of the modes in the network	Anonymous or Pseudonymous	known identities

threats, while decentralized identity management could prevent unauthorized access.

The proposed system could be tested in a real-world setting to evaluate its effectiveness in detecting and mitigating cyber threats, considering factors such as network size, consensus method and interoperability. By testing the proposed system, this research could contribute to the development of more robust and effective cyber security measures against an expanding threat landscape.

Application of Blockchain in CyberSecurity: The CIA triad model is used as a standard in cybersecurity to evaluate a company's safety architecture.
Blockchain enables us to guarantee that these rules are followed[13].

Confidentiality: Ensuring that only authorized parties can access relevant data is crucial and full encryption of blockchain data can help achieve this by making it inaccessible to unauthorized parties on untrusted networks. Additionally, access controls should be implemented at the application level to prevent attacks from within the network. Public key infrastructure can be used by blockchain to provide advanced security controls that authenticate parties and encrypt communication, but storing private keys in secondary storage is risky and could lead to theft. To prevent this, key management procedures like IETF or RFC and cryptographic algorithms based on integer factorization problems should be used.

Integrity: The inherent features of immutability and traceability in blockchain technology enable organizations to maintain data integrity. Additionally, consensus protocols can aid in preventing and managing ledger splitting during a cyber-attack. Blockchain records every state of the system in every iteration, creating a complete and transparent history log[14]. Furthermore, smart contracts can ensure compliance with rules and prevent miners from manipulating data blocks.

Availability: Lately, there has been an increase in cyberattacks aimed at disrupting technology services, particularly through DDoS attacks. Nevertheless, such attacks are expensive in blockchain-based systems since the attacker needs a considerable number of small transactions to overpower the network. Unlike other systems, blockchains do not have a central point of failure, which reduces the possibility of IP-based DDoS attacks from interrupting normal operations. Data is accessible through various nodes, allowing complete copies of the ledger to be accessed at any time. The use of multiple nodes and distributed operation makes these platforms and systems more resistant to attacks.

RESULTS AND DISCUSSIONS

The research paper highlights the effectiveness of blockchain technology in detecting, mitigating, and securing against cyber threats. The advanced security features of blockchain, such as immutability, decentralization and data encryption, make it a promising technology for mitigating cyber risks. The paper recommends a multi-layered approach to cybersecurity that includes blockchain technology as one of the key components. Overall, the research paper suggests that blockchain technology can be one of the most efficient strategies for mitigating cyber threats in the coming days. that blockchain technology has the potential to be one of the most efficient mitigation strategies for cyber threats in the coming days. However, further research is needed to explore its full potential and address implementation challenges.

CONCLUSION

Blockchain technology may emerge as one of the most effective strategies for mitigating cyber threats due to its advanced security features such as immutability, decentralization, and data encryption. However, it is important to note that blockchain technology alone cannot provide comprehensive protection against cyber threats and should be used in combination with other security measures. As the risk of cyber-attacks continues to increase, organizations should consider implementing a multi-layered approach to cybersecurity that includes blockchain technology as one of the key components. BlockchainBlockchain technology can be highly effective in detecting, mitigating and securing against cyber threats. By providing an immutable ledger, decentralization, smart contracts, digital identity verification, and data encryption, blockchain can offer a secure and transparent system that is resistant to tampering and cyber-attacks. However, it is important to recognize that blockchain technology is not a panacea for cybersecurity and has its limitations and challenges, such as scalability and interoperability. Therefore, organizations must employ a multi-layered approach to cybersecurity that includes other security measures alongside blockchain technology. Despite these challenges, blockchain technology is a promising technology that can help organizations combat cyber threats and protect digital assets and transactions. As the technology continues to evolve, further research is needed to explore new applications and use cases for blockchain in cybersecurity.

REFERENCES

1. utcher, J.R., Steptoe, L.L.P. Johnson, C.M. Blakey and L.L.P.P. Hastings, 2017. Cybersecurity tech basics: Blockchain technology cyber risks and Issues: Overview. Thomson Reuter., https://www.steptoe.com/a/web/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf.
2. Taylor, P.J., T. Dargahi, A. Dehghantanha, R.M. Parizi and K.K.R. Choo, 2020. A systematic literature review of blockchain cyber security. Digital Commun. Networks, 6: 147-156.
3. Nandinidey, 2021. Role of blockchain in cybersecurity.,https://www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/.
4. Lu, H., K. Huang, M. Azimi and L. Guo, 2019. Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. IEEE Access, 7: 41426-41444.
5. Abdelwahed, I.M., N. Ramadan and H.A. Hefny, 2020. Cybersecurity risks of blockchain technology. Int. J. Comput. Appl., Vol. 177, No. 42.
6. Lima, C., 2018. Developing open and interoperable DLT\/blockchain standards [standards]. Computer, 51: 106-111.
7. Developer eXperience Hub, 2023. Blockchain and cybersecurity: Enhancing data protection and privacy.,ttps://wwwh.linkedin.com/pulse/blockchain-cybersecurity-enhancing-data-protection-privacy/.
8. Seker, E., 2020. Using blockchain technologies in cyber security. Data Driven investor, https://medium.datadriveninvestor.com/using-blockchain-technologies-in-cyber-security-6f3dd2ad9678.
9. Scannella, M., 2017. The future of digital authentication.,https://wayfinder.digital/blog/blockchain-cybersecurity.html.