International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 3, May-June 2024
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Blockchain Technology for Cybersecurity

Anamika Paswan,Vinod KT
Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
Paswananamika15@gmail.com, Vinodbhaskar1994@gmail.com

Abstract:

Blockchain technology offers novel solutions to bolster cybersecurity in an increasingly interconnected digital landscape. This paper provides a succinct overview of how blockchain's decentralized, transparent, and immutable architecture enhances security measures. Key applications including identity management, secure data sharing, supply chain integrity, and real-time threat intelligence sharing are highlighted. While acknowledging implementation challenges, this abstract advocates for integrating blockchain as a strategic component within comprehensive cybersecurity frameworks to fortify resilience against cyber threats and foster trust in digital ecosystems.

Introduction:

Cyber security is the prevention of hackers, spammers and cybercriminals from damaging equipment and services such as computers, servers, mobile devices, electronic systems, networks and data on the Internet. Businesses use these programs to protect themselves from phishing scams, ransomware attacks, theft, data breaches, and financial losses. Given how effective cybercrime has become and criminals seek new attack strategies, what is considered safe today may not be safe tomorrow. But one of the best ways to reduce future cyber risks may be blockchain. Blockchain can enable new types of business applications without intermediaries and as a basis for the content of the Internet security infrastructure. Therefore, it is important to analyze existing research on the use of blockchain for cybersecurity issues to unravel how the technology can provide solutions to mitigate emerging threats. Blockchain mainly concerned with the confidentiality, security, integrity, and accountability of information, including the use of networks such as the Internet.

What is Blockchain?

Blockchain is a decentralized system that records transactions across multiple computers securely and transparently. Decentralized management follows the principles of immutability and consensus. Simply put, blockchain is a chain of blocks where each block contains a series of transactions. These blocks are linked together using cryptographic hashes, ensuring that any changes in the block are reflected in each subsequent block, making it nearly impossible to tamper with information stored on the blockchain.

Transaction records are by far the most common use of blockchain, but other types of information can also be stored on blockchain. Digital assets are transferred, not copied or modified. Because digital assets are decentralized, multiple parties can control them and access them instantly. Blockchain ledger appears; all updates are recorded and backed by evidence. Since the ledger is public and has security features, blockchain technology is the best choice for almost any business information. The idea of blockchain is to ensure trust without the need for a trusted third party by ensuring the accuracy and security of information. This feature eliminates the easy target point. Therefore, systems or websites that are stored and connected to the network are not in one place and become difficult to hack. So, one of the best technologies that will reduce online dangers in the future is blockchain. However, like other new technologies, blockchain faces numerous commercial challenges during the difficult development process. One of the best uses would be to leverage integrity guarantees to create cybersecurity solutions for various technologies.

What are the types of blockchain?

Depending on usage and requirements, the blockchain network can be configured in a variety of ways. Methods used to create a blockchain network are explained below:

1. Public Blockchain:

- Definition: Public blockchains are fully open and decentralized networks where anyone can participate, read, write, or audit the blockchain. Transactions are transparent, and consensus is achieved through mechanisms like Proof of Work (PoW) or Proof of Stake (PoS).

- Examples: Bitcoin, Ethereum (currently transitioning to PoS), Litecoin.

2. Private Blockchain:

- Definition: Private Blockchains are permissioned networks where access and permissions are restricted to a specific group of participants. They are often used within organizations or consortiums to streamline processes and maintain privacy.

- Characteristics: Participants are known and verified, transactions are visible only to permissioned parties, and consensus mechanisms can be more efficient than those in public blockchains.

- Examples: Hyperledger Fabric, R3 Corda, Quorum.

3. Consortium Blockchain:

- Definition: Consortium blockchains are semi-decentralized networks where a predefined group of nodes controls the consensus process. Unlike public blockchains, consortium blockchains are not fully open, but they are more decentralized than private blockchains.

- Characteristics: Governance is shared among member organizations, allowing them to collectively validate transactions and maintain the blockchain.

- Examples: IBM Blockchain Platform, B3i (insurance industry blockchain consortium), Komgo (commodity trading consortium).

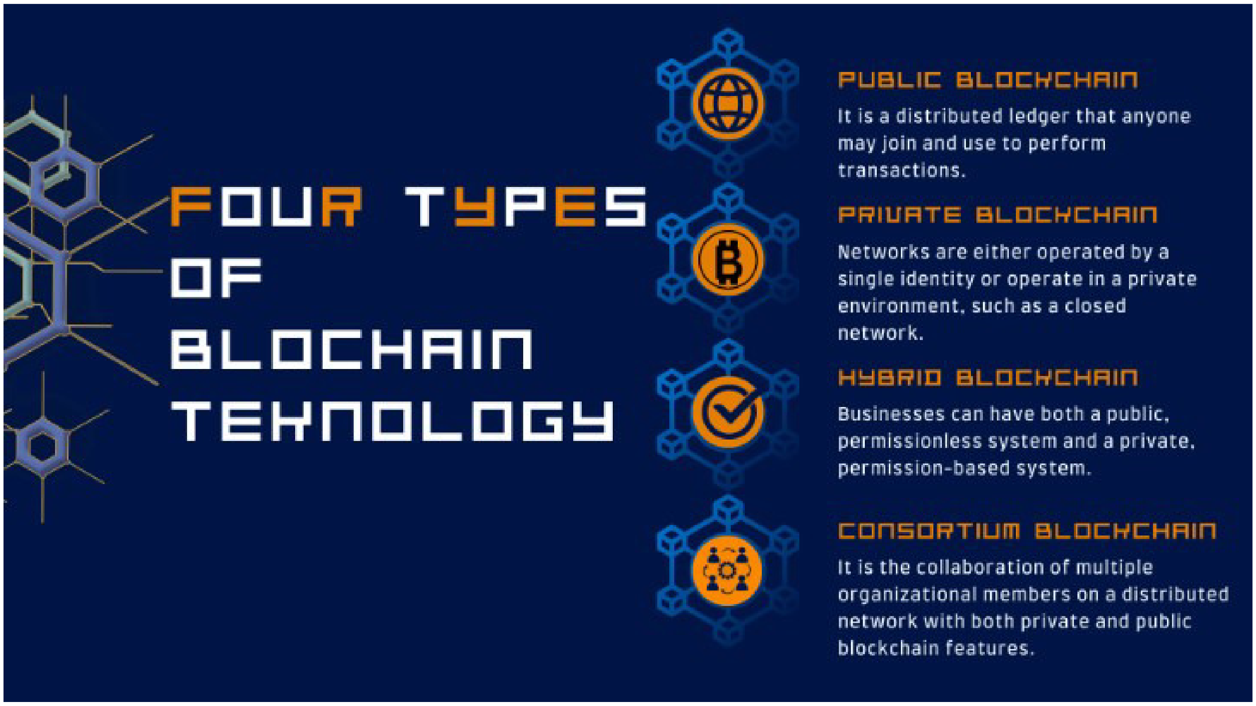
4. Hybrid Blockchain:

- Definition: Hybrid blockchains combine elements of both public and private blockchains, offering a flexible solution that caters to various use cases. They typically allow for private transactions within a public network, ensuring data privacy while benefiting from the security and transparency of a public blockchain.

- Characteristics: Portions of the blockchain are public, while other portions are private or permissioned, offering the advantages of both models.

- Examples: Dragonchain, VeChain.

These different types of blockchains offer varying degrees of decentralization, privacy, scalability, and control, allowing organizations and developers to choose the most suitable blockchain architecture for their specific use cases and requirements.



PUBLIC BLOCKCHAIN
It is a distributed ledger that anyone may join and use to perform transactions.

PRIVATE BLOCKCHAIN
Networks are either operated by a single identity or operate in a private environment, such as a closed network.

HYBRID BLOCKCHAIN
Businesses can have both a public, permissionless system and a private, permission-based system.

CONSORTIUM BLOCKCHAIN
It is the collaboration of multiple organizational members on a distributed network with both private and public blockchain features.

How does blockchain work?

Blockchain technology works through a combination of cryptographic methods, distributed computing, and consensus mechanisms. Here's a simplified explanation of how blockchain technology works:

1. Decentralized Network:

Blockchain works on a decentralized network of computers, called as nodes. Each node stores a copy of the entire blockchain.

2. Transactions:

Transactions are begin by participants in the network. These transactions could involve anything like sending cryptocurrency, recording data, executing smart contracts, or any other action depending on the blockchain's purpose.

3. Transaction Verification:

When a transaction is starts, it is broadcasted to the network.Each node verifies the transaction using predefined rules specific to the blockchain's protocol. This verification involves checking the digital signature, ensuring the sender has sufficient funds (in the case of cryptocurrency), and validating the transaction against the blockchain's consensus mechanism.

4. Block Creation:

Validated transactions are grouped together into a "block." Each block contains:

- A list of transactions.

- A reference to the previous block's hash (creating a chain of blocks).

- A timestamp.

- A unique identifier called a "nonce" (used in Proof of Work consensus mechanisms).

5. Consensus Mechanisms:

Consensus mechanisms are used to agree on the validity of transactions and the order of blocks in the blockchain. The most common mechanisms are:

- Proof of Work (PoW): Nodes compete to solve complex mathematical puzzles. The first node to solve the puzzle broadcasts its solution to the network. Other nodes verify the solution, and if valid, they add the block to the blockchain.

- Proof of Stake (PoS): Nodes are chosen to validate transactions and create new blocks based on the amount of cryptocurrency they hold or "stake." This method reduces energy consumption compared to PoW.

6. Consensus and Block Addition:

Once consensus is reached, the validated block is added to the blockchain.Each node independently adds the block to its copy of the blockchain.

7. Blockchain Security:

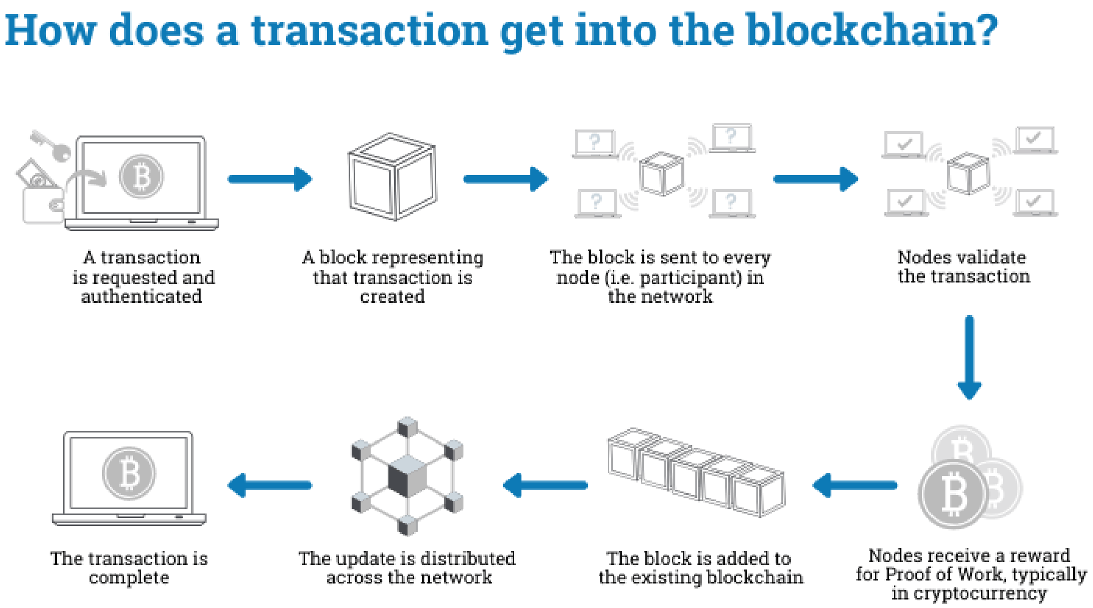
Blockchain's security is based on decentralization and immutability:

- Decentralization: No single entity controls the network, reducing the risk of tampering or fraud.

- Immutability: Once a block is added to the blockchain, it cannot be altered or deleted without altering subsequent blocks, which would require consensus from the majority of the network.

8. Transaction Finalization:

Once a transaction is included in a block and added to the blockchain, it is considered confirmed.The number of confirmations a transaction receives depends on the blockchain's consensus mechanism and protocol. More confirmations increase the security of the transaction.This process repeats for every new transaction, creating a transparent, secure, and immutable ledger of transactions known as the blockchain.


How does a transaction get into the blockchain?
A transaction is requested and authenticated
A block representing that transaction is created
The block is sent to every node (i.e. participant) in the network
Nodes validate the transaction
Nodes receive a reward for Proof of Work, typically in cryptocurrency
The block is added to the existing blockchain
The update is distributed across the network
The transaction is complete

What are the Benefits of Blockchain in Cybersecurity?

Blockchain has many advantages in the field of cybersecurity, leveraging its decentralized, immutable and transparent structure to solve various security problems.This change ensures the integrity and reliability of data, making blockchain an ideal tool to create tamper-proof data and significantly protect the integrity of data. Here are some key benefits of blockchain in cybersecurity:

1. Decentralization: Blockchain operates on a decentralized network of nodes, eliminating points of failure and reducing the risk of attack. Decentralized management makes it difficult for attackers to manipulate or destroy information stored on the blockchain.
2. Improve Data Integrity: The cryptographic hashing and confirmation process used in the blockchain to ensure the integrity of data stored on the blockchain. Any attempt to transfer data would require

the attacker to control most of the network, making it nearly impossible to intercept data without being detected.

3. Transparent and Auditable: Blockchain transactions are transparent and visible to all participants in the network. This transparency enables instant analysis and monitoring of transactions, making it easier to investigate and investigate suspicious activity or security breaches.
4. Security Management: Blockchain-based identity management solutions reduce the risk of identity theft and fraud by providing authentication and security. Users have better control over their personal information, and personal information is stored securely on the blockchain, reducing dependence on central service providers.
5. Smart Contracts for Automated Security: Smart contracts are implemented contracts where recommendations are written directly into the program code. It enables efficient and secure transactions on the blockchain, reducing the need for intermediaries and reducing the risk of fraud or manipulation.
6. Secure Supply Chain : Blockchain can be used to create a transparent and traceable supply chain where every step of the supply chain is recorded on the blockchain. This increases supply chain security by reducing the risk of fraud, improving traceability and ensuring the integrity of delivery information.
7. Decentralized Threat Intelligence: Blockchain can facilitate the creation of threat intelligence systems where security-related information, where tokens of agreement (IOCs) and malware are embedded names, can be shared and verified by multiple parties. This ensures threats are fast and responsive.
8. Data Privacy and Privacy: Blockchain provides privacy and confidentiality through technologies such as zero-knowledge authentication and encryption. This process protects the privacy of users and organizations by allowing secure transactions and information sharing without exposing sensitive information.
9. Resistant to DDoS attacks: Due to its decentralized nature, blockchain networks are resistant to decentralized denial of service (DDoS) attacks. Even if some nodes are affected or offline, the network can continue to operate, ensuring continuous operation and data availability. Integrity, transparency, self-regulation, automated security through smart contracts, and improved privacy and protection against attacks. These benefits make blockchain an important tool in combating cyber threats.

Use cases of blockchain technology in cybersecurity

1. Decentralized Storage Solution

Information has become more valuable than the same. Your business collects a lot of sensitive information about your customers. Unfortunately, this information also attracts the attention of hackers. One of the easiest things for cybercriminals is to store all their information in one place. It's a bit like keeping all your money and jewelry in a shoebox at home and then being surprised when a thief steals it all. However, this situation seems to be slowly changing. Blockchain-based solutions are becoming popular. For example, Apollo Data Cloud allows users to store data on the blockchain and authorize it to third parties.

2.IoT security

Encrypted keys can be reversed at any time, reducing the risk of leakage. Due to the nature of blockchain technology, hackers do not have a single point of entry and once inside, they cannot access all of the stored information. supplied. These include routers and switches. Now other devices such as smart thermostats, alarm systems, and even security cameras are also vulnerable. In short, there is often no stringency when it comes to making sure these IoT devices are secure. Blockchain technology can be used to protect systems and devices from attacks. For example, the device can improve a team's understanding of normal situations in a network and target nodes that are behaving suspiciously. It can be used to complete secure data transfers at close range and enable timely communication between devices thousands of miles away. Additionally, blockchain security means that there is no central organization that controls the network and verifies the information passing through it. It will be harder to attack (if possible).

3. More DNS Security

DNS is very important. Therefore, hackers can enter and damage the connection between the website name and IP address. They can take money from the site, direct people to a fraudulent site, or make the site unusable. They can also combine DNS attacks with DDoS attacks, making the website unusable for long periods of time. Currently, the best solution for such problems is to monitor log files and instantly alert to suspicious activity. Since it is decentralized, it will be more difficult for hackers to find and exploit the same vulnerability point. Your registration information can be stored immutably on a decentralized ledger, and connections can be enforced via immutable smart contracts.

4. Ensuring Security in Private Messaging

As social networks become more popular, more metadata is collected from users during social interactions. End-to-end encryption is used, but other systems are also starting to use blockchain to secure data. Currently, most messaging applications lack a security protocol and integrated API framework to enable communication. The secure blockchain communication ecosystem solves this problem and works to create a new communication system. Blockchain is a great solution because it secures all information exchanged and enables the connection of different communications. The important thing is decentralization. When access control, network connections, and even the data itself are no longer in one place, it becomes difficult for cybercriminals to take advantage. This means more security and fewer vulnerabilities.

5. KYC Verification

Scam electronic KYC renewal is a new method used by fraudsters to deceive the unscrupulous. Fraudsters trick the service provider and ask for confidential information like Aadhar number and bank details. This can be avoided by using KYC verification. As a document of record, it allows data from various government and private data portals to be collected and stored in a single, immutable, secure repository.

Encryption keys protect each user's private information on the list. Hackers and cybercriminals will have a hard time cracking the keys and obtaining the necessary credentials.

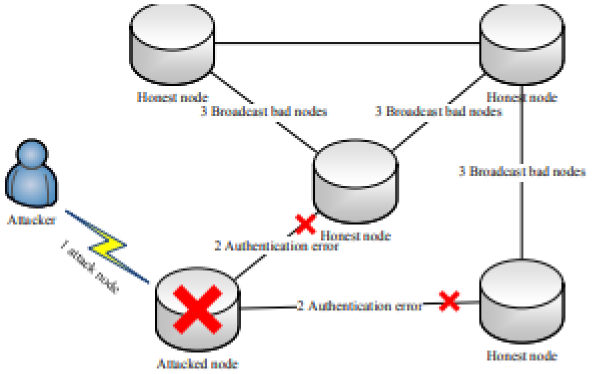
6. Improved PKI

PKI or Public Key Infrastructure keeps messaging applications, emails, websites and other forms of communication secure. But they all rely on third-party certificate authorities to issue, revoke or store key pairs. These certificate authorities can become an easy target for hackers with spoof identities trying to penetrate encrypted communications. On the other hand, when keys are published on a blockchain, it leaves no scope for a false key generation or identity theft as the applications verify the identity of the person you're communicating with. CYBRI is a good place to go if you want to keep your messaging apps and communication secure. It is found that CYBRI penetration testing has given users positive outcomes.

7.Data Storage Protocol Based on Blockchain

The data source is stored in the blockchain, and the blockchain is the distributed data accounts book that each node shares. The transaction information and authentication information in the block are transparent. The data information is stored after encrypted by private key and can be accessed and authorized by the data owner.

Architectural security-The current Internet platform is built on the structure of the central server. Traditional relational database leads to the over-centralization of data storage, causing the security of the data greatly depends on the central server security. The majority of data leaks result from hacker attacks on the server, such as DDOS attacks, SQL injection attacks, CC attacks .



As shown in Fig, the big data de-centered storage mode allows the block information to be maintained by nodes in the network. Hackers can control only few nodes in the network, but the data in the blockchain encrypted through the private key, which ensures the confidentiality of the data. If hackers tamper with the block data, the network's consensus model will ensure that other nodes reject the bad node. This model has resisted all attacks against traditional data storage patterns.

Future research directions of blockchain cyber security

1.Blockchain for IoT security-Security of IoT networks is seen as an urgent need in the industry and has become a priority for development and implementation; however, current research shows that almost all research on blockchain network security is included in the data. Security powered by blockchain technology The security of IoT systems can be renewable. However, the circumstances surrounding the decision and possibility of using this technology and how and where it can be used to solve the immediate problem of IoT security/threats clearly allow for imagination and then allow for little or no discussion. Therefore, future research should develop some guidelines and tools to help fill this gap in the literature. Additionally, proposing a blockchain-based solution for resource-augmenting IoT devices (running at the edge of the network) could be another area for further research.

2.Artificial Intelligence Blockchain for information security- In today's business ecosystem, information is captured from various sources and sent to a network of devices (like the Internet of Things). Artificial intelligence (AI) and its derivatives are being used as powerful tools to analyze and process data that will be useful in solving security problems. Although artificial intelligence is powerful and can play a role in calculating issues, measurement fraud can occur if malicious third parties intentionally or unintentionally interact with products that are not fair or foul for the purpose of counterattack. As a popular ledger technology, Blockchain can be used in many areas of cyberspace. Blockchain attempts to reduce the risks of transaction and financial fraud through distribution, authentication, non-interference, and other features to equitably ensure the authenticity, trust, and integrity of the record. Intelligence can produce better and more reliable results when the reliability and trustworthiness of data is guaranteed. Future research directions will be to investigate the security of blockchain for information intelligence in B2B and M2M environments.

3.Sidechain security: Sidechain technology has recently emerged as an independent chain linked to the main chain along with the business in order to reduce the risk to the main blockchain (usually a function). In the future, we envision a decentralized, multi-blockchain ecosystem where different mainchains and sidechains cooperate with each other in various scenarios. However, practical applications of side chains are still not understood and many important scientific questions are still debated. For example,

1. How do these sidechains establish security defaults to prevent attacks?

2. How could blockchain customers be assured of the integrity and confidentiality of their data through sidechains?

Answering these questions is vital for the future investigations to have a more sustained blockchain cyber security research .

4.Publish open source software and data and engage the community-Blockchain cybersecurity research is split between academia and the developer community. To close this gap, academic researchers must work and begin working to make applications, tools, and data more open to business participation. In fact, there are many communities interested in blockchain analysis (as evidenced by the popularity of open tools such as Bitcoin-abe or BlockBench), so researchers should involve the community involved in research work, development, verification and maintenance research results.

Conclusions:

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.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 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 . As the World Wide Web moves towards a mass adoption 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.

Reference:

1. https://www.sciencedirect.com/science/article/pii/S2352864818301536#bib58
2. https://huangjunqin.com/papers/LiBIGCOM2017Big.pdf
3. https://ieeexplore.ieee.org/abstract/document/8113055/
4. https://www.zenarmor.com/docs/network-security-tutorials/what-is-blockchain#how-does-blockchain-transform-cybersecurity
5. https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/?sh=57b3fb793ac3
6. https://www.investopedia.com/terms/b/blockchain.asp