International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Blockchain: A New Tool for Cybersecurity

Aryan Sanjeev

2nd Year B. Tech Undergrad, ASET, Amity University, Noida, India
Ph:-+918826880497, sanjeevaryan2011[at]gmail.com

Abstract: ***The evolution of blockchain (or distributed ledger technology) has been compared to the early rise of the internet, with comments and arguments about the technology's potential to disrupt multiple industries, including healthcare, government, energy, manufacturing, and, most notably, financial services, where it is predicted to be the beating heart of finance and the ultimate provider of a new industry fabric. Blockchain is a distributed, decentralized digital ledger that records transactions as blocks. Because of its immutability and restricted access to only authorized users, this ledger facilitates the transparent storage of information. Blockchain is gaining acceptance today, but skeptics who question the technology's scalability, security, and sustainability persist. The internet's and technology's reliance on today has resulted in new business models and revenue streams for enterprises, but it has also created new loopholes and opportunities for cyber attackers to exploit. Cyber-attacks have become more focused and complex as malware has become more sophisticated and professional cyber groups have become a greater menace. These hackers are aiming to steal valuable data such as intellectual property (IP), personally identifiable information (PII), health records, and financial information. They are employing very profitable strategies such as monetizing data access via advanced ransomware techniques or interrupting overall corporate operations via Distributed Denial of Service (DDoS) attacks. Blockchain could potentially aid in strengthening cyber security by safeguarding, preventing fraudulent actions through consensus processes, and detecting data tampering, based on its core qualities of immutability, transparency, auditability, data encryption, and operational resilience (including no single point of failure).***

Keywords: Blockchain, Cyber security, Cybercrime, Security, Distributed Ledger, Technology, Database

1.Introduction

A blockchain is a growing list of documents, known as blocks, which are algorithmically linked together. Each block comprises a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where leaves represent data nodes). The timestamp validates that the transaction data existed when the block was released to be hashed. Because each block contains information about the one before it, they create a chain, with each subsequent block reinforcing the ones before. As a result, blockchains are resistant to data alteration since, once recorded, the contents in any one block cannot be updated retrospectively without affecting all subsequent blocks. A peer-to-peer network commonly manages blockchains for use as a publicly distributed ledger, with nodes collectively adhering to a protocol to communicate and validate new blocks. Although blockchain records are not unalterable due to the possibility of forks, blockchains are safe by design and represent a distributed computing system with strong Byzantine fault tolerance.

Based on the work of Stuart Haber, W. Scott Stornetta, and Dave Bayer, the blockchain was published in 2008 by a person (or group of persons) going by the name Satoshi Nakamoto to serve as the public transaction log of the cryptocurrency bitcoin. Because of the blockchain implementation within bitcoin, it was the first digital currency to overcome the double-spending problem without the requirement for a trusted authority or central server. The bitcoin concept has generated variously public-readable and blockchain-based applications widely used by cryptocurrencies.

2.Blockchain in Cybersecurity

Cybersecurity is the protection of systems and networks against digital attacks intended at obtaining access to, changing, or deleting digital information to extort money or sensitive data. With greater reliance on technology and data, tightening security measures to protect digital data and transactions is vital. Malware like viruses, Trojans, and Rootkits can be used to carry out cyberattacks. Phishing, Man in the middle (MITM) attacks, Distributed denial of service (DDoS) assaults, SQL injection, and Ransomware attacks are all common types of cyberattacks.

Blockchain technology generates a data format with intrinsic security properties. It is founded on cryptography, decentralization, and consensus concepts that ensure transaction confidence. Most blockchains or distributed ledger technology (DLT) arrange data into blocks; with each block containing a transaction or set of transactions. Each new block in a cryptographic chain connects to all the blocks before it in such a way that it is nearly impossible to tamper with. A consensus process validates and agrees on all transactions within the blocks, ensuring that each transaction is truthful and correct.

2.1 Application Of Blockchain In Cybersecurity

The CIA triad model is used in cybersecurity to examine an organization's security model. The triad is made up of-

1. Confidentiality
2. Integrity
3. Availability

Blockchain helps us ensure all these policies are satisfied.

2.1.1 Confidentiality

Confidentiality, as defined by the National Institute of Standards and Technology (NIST), is "the property that sensitive information is not revealed to unauthorized individuals, entities, or processes.". Protecting blockchain network access is critical for data security (particularly in private blockchains). If an attacker has access to the blockchain network, they are more likely to obtain access to the data, hence authentication and permission rules, like with other technologies, must be installed. Although the technology was designed without explicit access controls (due to its open nature), certain blockchain implementations are beginning to solve data confidentiality and access control concerns by providing out-of-the-box full-block data encryption and AAA capabilities. Full encryption of blockchain data ensures that data is not accessible to unauthorized parties while in transit (especially if data is flowing through untrusted networks).

Full encryption of blockchain data ensures that unauthorized parties cannot access the data while it travels over untrusted networks. To prevent attacks from within the network, security measures such as access controls should be implemented directly at the application level. By authenticating individuals and encrypting their communication via public key infrastructure, blockchain can provide extra security features. However, backup storage of private keys in secondary storage increases the danger of private key theft. To overcome this, key management systems such as IETF or RFC should be employed, as well as cryptographic algorithms based on integer factorization problems.

2.1.1.1 Network Access

There is no need to regulate network access in public blockchains because the chain protocols allow anyone to access and participate in the network after downloading the software. Private blockchains, on the other hand, necessitate the implementation of adequate security mechanisms to safeguard network access. In an ideal world, it would be tempting to assume that, due to their private nature, local networks and systems are already well behind an organization's perimeter, protected by several internal security layers (such as firewalls, virtual private networks, VLANs, Intrusion Detection & Prevention Systems, and so on), through the implementation of a so-called defense-in-depth strategy. Relying only on the efficiency of such security procedures is insufficient. As a result, security guiding principles recommend that security controls (such as access controls) be implemented directly at the application level, as the first and most important line of defense, particularly in scenarios such as an attacker gaining access to the local network or where a malicious insider is already present.

Organizations must consider how to treat uncommunicative or intermittently active nodes when designing their blockchain network architecture, as the blockchains must continue to function without these offline nodes while also being able to bring them back up to speed if they return to their original function.

To solve these problems, organizations should develop an integrated cyber security program that includes a governance framework with roles, processes, accountability measures, well-articulated performance metrics, and, most importantly, an organizational-wide mentality shift.

2.1.1.2 Data Access & Disclosure

Today, gaining access to a blockchain network and the data does not necessarily imply that the attacker may read or recover the information. When the newest encryption standards are followed, full encryption of the data blocks can be applied to the data being transacted, effectively preserving its confidentiality. The use of end-to-end encryption, which has recently been a hot topic, in which only those with authorization to access the encrypted data, i.e. through their private key, can decode and view the data. When encryption keys are used in conjunction with PKI, companies can achieve a better level of security. Encrypting data on a blockchain can give enterprises some level of data confidentiality and access control security.

Implementing secure communication protocols on the blockchain, for example (assuming the most recent security standards and implementation guides), ensures that even if an attacker attempts a man-in-the-middle attack, the attacker will not be able to forge the interlocutor's identity or disclose any data while in transit. Even in the most severe scenario, where long-term private keys are hacked, past sessions are kept private due to the security protocols' complete forward secrecy qualities. Today's cryptographic techniques for public/private key generation are based on integer factorization issues, which are difficult to solve with today's processing power.

2.1.2 Integrity

Maintaining integrity, according to NIST, comprises "protecting against incorrect information alteration or deletion, as well as ensuring information non-repudiation and validity." Blockchain's immutability and traceability aid organizations in assuring data integrity. Consensus model methods can also help firms create procedures to prevent and regulate ledger splitting in a 51 percent cyber control attack. The previous state of the system is preserved with each succeeding iteration in Blockchain, generating a completely traceable history log. To prevent miners from mining data blocks, smart contracts can be used to verify and enforce norms between parties.

Maintaining data consistency and integrity throughout its life cycle is critical in information systems. Data encryption, hash comparison (data digestion), and the use of digital signing are some examples of how system administrators can ensure the integrity of data regardless of its stage (in transit, at rest, and in use storage). Blockchain's inherent qualities of immutability and traceability already provide enterprises with a mechanism to secure data integrity.

2.1.2.1 Immutability

Blockchain technology is considered a secure technology because it allows users to believe that the transactions logged on the tamper-proof ledger are authentic. In comparison to a traditional database, the combination of sequential hashing and cryptography, as well as its decentralized structure, makes it extremely difficult for any party to tamper with it. This gives enterprises that use the technology certainty regarding the data's integrity and honesty. The consensus model protocols linked with the technology also provide enterprises with an additional level of assurance over data security, as 51% of users in public and private blockchains must agree a transaction is genuine before it is added to the platform. In the event of a 51% cyber control attack, organizations can build additional procedures to avoid and regulate ledger splitting, such as monitoring if one of the nodes boosts processing capacity and executes a significantly higher number of transactions.

2.1.2.2 Smart Contracts

Smart contracts, which are computer programs that run on the ledger, have now become a key element of blockchains. This type of application can be used to help parties facilitate, verify, or enforce rules, allowing for straight-through processing and interactions with other smart contracts. Because such software has a broad attack surface area, an assault on one smart contract could have a domino effect on other components of the platform, such as the language itself or contract implementation. Because blockchain introduces a new paradigm to software development, safe development standards and procedures (such as establishing secure code and security testing) must be established (and modified) to account for the life cycle of smart contracts (creation, testing, deployment, and management).

2.1.3 Availability

According to the National Institute of Standards and Technology, availability is defined as "ensuring timely and dependable access to and use of information." Cyberattacks aimed at disrupting the availability of technology services have increased in recent years, with DDoS attacks being the most common type. In blockchain-based systems, however, DDoS attacks are costly since the attacker attempts to overwhelm the network with a huge number of small transactions. Because blockchains have no single point of failure, IP-based DDoS attacks are less likely to impair daily operations. Data is always available through a large number of nodes, allowing full copies of the ledger to be obtained at all times. Platforms and systems are more resilient because of the combination of several nodes and distributed activity.

2.1.3.1 No Single Point of Failure

Because blockchains have no single point of failure, the odds of an IP-based DDoS assault affecting normal operations are greatly reduced. If a node fails, data is still available through other nodes in the network since they all keep a complete copy of the ledger at all times. The technology's distributed nature eliminates the Byzantine General's problem of false consensus. Even though a blockchain network is thought to have no single point of failure, enterprises may still face risks from external events outside their control. A global internet outage, for example, would affect even a widely distributed public blockchain network like Bitcoin or Ethereum, causing interruptions that would damage an organization's operations in the same way that any other technology would.

2.1.3.2 Operational Resilience

The platform is operationally resilient due to the peer-to-peer architecture of the network and the number of nodes working in a distributed and 24/7 way. Given that both public and private blockchains are made up of numerous nodes, organizations can make a node under assault redundant while continuing to operate normally proves a result, even if a significant portion of the blockchain network is attacked, it will continue to function due to the distributed structure of the technology. This does not imply that the network is "bullet-proof." Since the introduction of blockchain in 2008, platforms have faced risks in which attackers attempted to compromise their stability through various attack vectors.

Transaction malleability is a problem discovered when transactions are in the pending validation phase, resulting in a Bitcoin network attack in 2014, negatively impacting user experience. In 2016, an attacker leveraged smart contracts in Ethereum and the manner they can be used to cause a network overflow, causing block generation and transaction validation to be severely hampered, causing the network to crash. A hard fork has been created to fix this issue (permanent divergence from the previous blockchain version).

2.2 Possible Blockchain Use Cases for Cybersecurity

- **IoT (Internet of Things) Security:**

With the increased use of AI and IoT, data and system security from hackers have always been a big worry. A potential use case to maintain cybersecurity in the IoT system is the usage of Blockchain for increased security by leveraging device-to-device encryption to secure communication, key management techniques, and authentication.

- **The reliability of software downloads:**

To prevent malicious software from infecting devices, blockchain can be used to verify updates and installers. Hashes are logged in the blockchain here, and new software identities can be compared to the hashes to validate the downloads' integrity.

- **Data transmission protection:**

The data in transit will be safeguarded from illegal access by utilizing encryption.

- **Decentralized storage of critical data:**

With the exponentially expanding amount of data generated every day, blockchain-based storage solutions aid in decentralized storage, hence securing digital data.

- **Mitigating DDoS Attacks:**

One of the most popular cyberattacks today is DDoS attacks where hackers aim to generate a flood of Internet traffic and thus disrupt the flow of services. The properties of immutability and cryptography help Blockchain prove to be an effective solution for these attacks.

- **DNS Security:**

The Domain Name System (DNS) is a public directory that connects domain names to IP addresses. Over time, hackers have attempted to get access to the DNS and abuse these links, causing websites to crash. Because of the immutability and decentralized nature of Blockchain, the DNS may be securely stored.

2.3 Advantages of Using Blockchain in Cybersecurity

- **User confidentiality:**

In a Blockchain network, public-key cryptography helps to ensure user confidentiality.

- **Data transparency and traceability:**

All of these transactions are recorded in a history that may be accessed at any time. Members of the Blockchain network digitally sign transaction data, ensuring openness.

- **Secure data storage and processing:**

Blockchain's main attribute of immutability and records of any modifications to the data aid in the safe and secure storage of data.

- **Safe data transfers:**

The Public Key Infrastructure (PKI) in Blockchain ensures data transmission authentication. Smart contracts aid in the automatic execution of agreements between two parties throughout the course of a transfer.

- **No single point failures:**

Because blockchain systems are decentralized, a single node failure does not disrupt the entire network. As a result of the multiple copies of ledgers maintained, the system is not compromised even during DDoS attacks. Private blockchains do not have this advantage.

2.4 Disadvantages of Using Blockchain in Cybersecurity

- **Reliance on private keys:**

Blockchains rely largely on Private Keys to encrypt data, however, if lost, these private keys cannot be retrieved. This could result in permanent loss of access to encrypted data.

- **Adaptability and scalability challenges:**

Because blockchain networks have fixed block volumes and transaction rates, it is critical to evaluate the network's scalability. Integrating Blockchain technology necessitates a complete replacement of present systems, which may pose challenges for businesses.

- **High operating costs:**

Blockchain takes a lot of computational power and storage space. When compared to non-Blockchain applications, this results in greater costs.

- **Lack of governance:**

Blockchain principles are not yet universally regulated. To sustain governance in Blockchain applications, regulations and frameworks must be implemented.

- **Blockchain literacy:**

Learning Blockchain technology necessitates a thorough understanding of numerous development, programming languages, and other tools. Thus, despite the multiple applications of Blockchain Technology, there are not enough Blockchain developers available in the current context.

3.Real-Life Application Examples

- **Indian Government (New Delhi, India):**

A National Blockchain Framework (NBF) has been proposed which can be built with three sorts of participants: a) technology experts (application developers), b) technology providers or operators (infrastructure and services, BaaS), and c) entire technology stack builders (IP creator). Security audit and evaluation techniques and guidelines may be developed with smart contracts and other Blockchain-specific features in mind. A smart Contract security study may be launched in order to understand the danger scenario better and develop audit rules and methods. Identity, authentication, and role-based access control should be enforced at appropriate layers of the technology stack in a permissioned Blockchain system. Access to Blockchain data may be granted to LEAs (Law Enforcement Agencies) in accordance with applicable legal provisions.

- **Barclays (London, England), Traditional Banking:**

Barclays has applied for a patent to use blockchain to improve the security of fund transactions. It intends to use Distributed Ledger Technology to stabilize cryptocurrency transfers (DLT). As a result, blockchain assists the bank in storing customer information on a secure blockchain.

- **CISCO (San Jose, California), IoT:**

Cisco intends to leverage blockchain technology to secure IoT devices since ledger technology eliminates single points of failure and encryption aids in data security.

- **Coinbase (San Francisco, California), Cryptocurrencies:**

Coinbase stores wallets and passwords in a secure database using encryption. It also conducts background checks on staff to protect the security of their crypto.

- **Australian Government (Canberra, Australia):**

The Australian government intends to build a DLT-based cybersecurity network. The government has also collaborated with IBM to create a blockchain ecosystem to protect the storage of official records.

- **Philips Healthcare (Andover, Massachusetts), Healthcare:**

Philips Healthcare has collaborated with hospitals all around the world to develop a healthcare ecosystem based on blockchain and artificial intelligence. This ecosystem will aid in discovering and analyzing various operational, administrative, and medical data.

- **Chinese Military (Beijing, China), Defense and Military:**

Using blockchain cybersecurity, China's government and military are striving to safeguard important government and military information, as well as intelligence information.

- **Founders Bank (Valletta, Malta), Cryptocurrencies:**

They intend to be the world's first decentralized bank, with buyers owning the bank rather than any central authority. To store and safeguard users' bitcoins, concepts like encryption and distributed ledgers will be used.

- **The State of Colorado (Denver, Colorado), Government:**

According to a Senate bill, the government would examine utilizing Blockchain to safeguard record storage, attempting to reduce the growth in attempted attacks.

- **J. P. Morgan (New York, NY), Traditional Banking:**

They created the Quorum platform, which uses Blockchain to handle private transactions. To ensure transaction security, it employs the ideas of smart contracts and cryptography.

- **Health Linkages (Mountain View, California):**

They aim to use Blockchain to keep patient records secure allowing only certain personnel to access the records. It will also be used to maintain a chronological record of major healthcare events which will help doctors make better decisions.

4.Conclusion

Blockchain provides a different road to higher security, one that is less traveled and less inviting to cyber criminals. This method lowers vulnerabilities, provides robust encryption, and checks data ownership and integrity more effectively. It can even do away with some passwords, which are commonly referred to as the weakest link in cybersecurity. Despite its benefits, businesses should continue to adhere to security best practices such as rate limits, encrypting important configuration files, and weeding out vulnerabilities during the development process. A related 2019 World Economic Forum article warned against blockchain hype and "exaggerated security expectations."

According to the report, "many regarded its cryptographic base to be the ultimate answer to security." "As a result, they have failed to implement the security safeguards essential for the emergence of trust in a blockchain." According to the authors, the technology is seen as either intrinsically unsecure or unhackable, with the "reality lying somewhere in the between."

Although adoption is currently restricted, the integration of blockchain and cybersecurity is not occurring exclusively on the outskirts. It is already regarded as a powerful instrument in areas where security is of the utmost importance.

The use of blockchain to improve cybersecurity is gaining popularity around the world. The recent economic and logistical disruptions produced by the COVID-19 pandemic, on the other hand, give firms new incentives to find inventive solutions.
Even as the economy enters a recession, businesses are seeking better visibility and security from their networks and supply chains. In a more tough and unpredictable world, digitization and resilience are essential. Companies aspire to balance security, visibility, and privacy with appropriate governance. Blockchain will hold the answers for many businesses.

References

[1] Role of Blockchain in Cybersecurity. Retrieved July 13, 2022, from GeeksforGeeks website,

https://www.geeksforgeeks.org/role-of-blockchain-in-cybersecurity/
[2] Blockchain Security. Retrieved July 12, 2022, from IBM, Blockchain website, https://www.ibm.com/in-en/topics/blockchain-security
[3] Piscini (Deloitte US), Eric, Dalton (Deloitte Ireland), David, & Kehoe (Deloitte Ireland), Lory. Blockchain & Cyber Security. Let's Discuss. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf
[4] Napoli, Robert. (2022). How Blockchain Could Revolutionize Cybersecurity. Forbes, Innovation. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/?sh=33b8848b3a41
[5] Shelke, Yogesh. Rethinking Cybersecurity through Blockchain. Infosys Newsletter, Insights. Retrieved from https://www.infosys.com/insights/cyber-security/cybersecurity-blockchain.html
[6] Government of India, Ministry Of Electronics & Information Technology. (2021). National Strategy on Blockchain. Retrieved from https://www.meity.gov.in/content/national-strategy-on-blockchain