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

Blockchain for CyberSecurity

Aayush Manish Chitnis

Gems Cambridge International School, Abu Dhabi, United Arab Emirates
Email: *aayushmanish09[at]gmail.com*

Abstract: ***In an increasingly interconnected digital world, the rise in sophisticated cyberattacks pose significant threats to individuals, businesses and governments. This research paper explores the role of blockchain technology in enhancing cybersecurity, focusing on how its decentralised and immutable nature can mitigate various cyber threats. While traditionally associated with cryptocurrencies, blockchains potential extend to applications such as supply chain management, digital identity, and network security. This paper discusses these applications and evaluates the advantages and challenges of using blockchain for cybersecurity.***

Keywords: Blockchain, Cybersecurity, Cyberattacks, Decentralized technology, Digital Security

1. Purpose

The purpose of this research paper is to explore the potential of blockchain technology in enhancing cybersecurity measures by addressing various cyber threats.

2. Significance

This article contributes to the ingoing research in cybersecurity by highlighting the unique capabilities of blockchain technology in preventing and mitigating cyberattacks, thus offering a potential paradigm shift in digital security practices.

3. Introduction

A cyber - attack is a deliberate and malicious attempt to breach the information system of an individual, organisation or government for the purpose of stealing or damaging sensitive information, disrupting operations or gaining unauthorised access. [1] Cybersecurity refers to the practice of protecting computers, networks and systems from cyber - attacks and to ensure the confidentiality, integrity and smooth functioning of systems. [2] Though it is almost impossible to build a perfectly secure system, organizations around the world spend huge amount of money to secure their systems and prevent such attacks. A blockchain is essentially a type of digital register, that store and maintains transaction records. The information is stored in regular batches known as "blocks" that link together to form a continuous chain. [3] In this research paper, we would discuss different types of cyberattacks and explore on how blockchain can be used for cyber security.

4. Types of Cyber Attacks

1) Malware

Malware is a common cyber - attack; that disrupts the normal functions of computers or servers. Malware can be classified into several types:

a) *Ransomware*: Ransomware is type of malware that blocks a victim's access to their data or applications remotely. Attackers encrypt the victim's data and demand payment for the decryption key. Without the decryption key, the data becomes inaccessible to the victim. In May 2021, Colonial Pipeline, which transports fuel from Texas to the Southeastern USA, suffered a ransomware attack on its computer system. The company paid a $4.4 million ransom within hours, but the disruption lasted for days as the company worked to restore its operations. [4]

b) *Spyware*: Spyware is a malicious software that infects a computer or other devices. It gathers sensitive information from the device and sends it to third parties without the user's consent. Spyware is used by both cyber - criminals and governments for surveillance. Finspy is a malware, employed by governments for surveillance activities, affecting 32 countries [5]. Darkhotel is another known spyware that targets high - profile guests in luxury hotels via hotel wi - fi networks and collects their sensitive information. [6]

c) *Trojan*: Named after the Trojan Horse from Greek mythology, a Trojan is a program that appears to be a harmless, legitimate program which is downloaded either by the user themselves or by trusted programs like updaters. It is different from ransomware and spyware because Trojan can be installed on a computer without user interaction. Trojans can be hidden as an attachment in an email or as a free downloadable file. Once the trojan is downloaded, it gains access to systems, and can spy on user's activity or steal sensitive data. Zeus Trojan, one of the first trojan, discovered in 2007 stole financial information [7]

d) *Scareware*: Typically, scareware can pop - up as a warning on the screen, that the user's device is infected. The pop - up persuades people to install fake antivirus software. Once the fake antivirus is downloaded, malware infects the system.

2) DoS & DDoS attacks

Denial - of - service (DoS) and Distributed denial - of - service (DDoS) attacks target websites or portals to make them inaccessible. A DoS attack overwhelms a server with more traffic than it can handle, causing it to crash and making the website unavailable to legitimate users. DDoS attacks are similar, but involve malicious traffic from multiple IP addresses, often originating from a botnet. These botnets consist of computers infected with malware, forming a network used specifically for DDoS attacks. [8]

When a server is overwhelmed with more requests than it can handle, the site may crash, data could become corrupted, and the system may be paralysed. DoS & DDoS attacks typically do not result in loss of data; however, they cause financial

losses, waste time, and can drive away clients due to poor performance or downtime. The strength of these attacks is measured in bits per second; with extreme attacks measured in gigabits per second. According to Cloudflare, a web hosting service provider, DDoS attacks in 2023 reached 201 million requests per second [9]

3) Phishing

Similar to a Trojan, phishing attacks deceive users into clicking a link or opening an attachment, granting cybercriminals access to sensitive data. These attacks use emails, SMS, and social media to lure victim into revealing sensitive information like account numbers and passwords. [10] This can result in financial loss or unauthorised sharing of content. In January 2016, the Austrian aerospace manufacturer FACC fell victim to a phishing email, resulting in a loss of € 42 million. [11]

4) Spoofing

Similar to phishing, spoofing is a technique where cyber - criminals impersonate as a legitimate source to compromise victim's device. They may impersonate an email address, display name, phone number, or website URL to deceive the user [12]. Once they have compromised the device, criminals can steal information, extort money or install malicious software.

5) IoT - based attacks

Internet - of - Things (IoT) includes all devices embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems via the internet. They include devices used in smart homes, such as security cameras and door locks, devices employed in smart health systems to monitor and support human health. [13] Cybercriminals may exploit vulnerabilities in IoT devices to gain unauthorised access and steal sensitive information. For example, outdated firmware on IoT devices may contain security vulnerabilities that attackers might exploit or smaller companies developing IoT devices may lack resources to implement rigorous security protocols. [13]

5. What is Block Chain Technology

A blockchain refers to blocks of data linked together into immutable digital chains. It is a type of digital ledger, which stores information that is shared among all parties that can access it. When data is transferred from one user to another within the blockchain network (e. g. cryptocurrency transfers), that is referred to as a "transaction". Each transaction is recorded in a "block", and these blocks are stored in a distributed ledger, called the "chain. " Every time a new transaction is approved and done, a record of it (block) is added to all the participants' ledger. Hence the blocks are continuously added, forming the blockchain. [14] Multiple participants manage the blockchain, meaning that all information and transactions are shared among all authorised participants, regardless of their location. This decentralised system is known as Distributed Ledger Technology (DLT).

1) Structure of a Blockchain:

A block in a blockchain is the main component that contains critical data about the transactions. It is made up of three main components:

a) *Header*: It is the core part of the Block, which identifies the block in a blockchain. It contains the following:
- Timestamp records when the block was created.
- the previous block's hash, which "chains" the blocks together.
- Merkle Tree is summary of all the transactions in a single block.
- Target defines the difficulty level of mathematical problem that miners must solve.
- Nonce is a random number used in the computation of the hash. [15]

b) *Data Section*: It contains the critical information about the transaction of that block. For cryptocurrency that would be the value of that transaction. For other kinds of blockchains the data contained would be different. [15]

c) *Hash*: It is a cryptographic value that acts as a digital fingerprint for the block. [10] When a transaction occurs, its converted into a fixed - sized string of numbers and letters using a hash function. This unique hash function is nearly impossible to reverse engineer. When a new block is created, it contains the previous block's hash, creating a blockchain. Any alteration in a block changes its hash, breaking the chain and alerting the system to potential tampering. [16]

2) Types of a Blockchain:

a) *Public Blockchain* - It is open to the public and anyone with a computer and internet access can participate in the network. These blockchains are large in size, the records are more distributed and hence public blockchains are more secure. It is decentralised and every user has a copy of the ledger. However, due to its large size, the processing rate is very slow. It has no central governing authority, so governments have not accepted this technology till date. E. g. Bitcoin and Ethereum. [17]

b) *Private Blockchain* - It is open to few authorised users only and it operates in a closed network, like a company or organisation. The processing speed is high, due to its small size and has increased level of security. However, as the number of nodes is limited, these blockchains can be more easily manipulated than a public blockchain. E. g. Hyperledger, Corda. [17]

c) *Hybrid Blockchain* – It is a mix of private and public blockchain, where some part is controlled, and other part is visible as a public blockchain. It can be customised and still can maintain transparency and security. E. g. Ripple Network and XRP token. [17]

d) *Consortium Blockchain* - It is like hybrid blockchain, but more than one organisation manages the blockchain. E. g. Tendermint and Multichain. [17]

3) How does a Blockchain Work:

A node starts a transaction and signs it with its private key. A block representing the transaction is then created and broadcast to the peers in the blockchain network. Network nodes (users) will first validate the transaction, and once verified, it is added to the ledger, and it linked to the previous block. A new block cryptographically links back itself to the previous block, and the distributed ledger is then updated across all network nodes. [18]

Consensus mechanisms such as Proof - of - Work (PoW) or Proof - of - Stake (PoS), are used to verify transactions and

create blocks. PoW requires users to solve complex computational puzzles to earn rewards and add new blocks to the blockchain. PoS allows users to validate transactions based on the number of coins they hold and stake for the network's security. [19]

4) Advantages and Disadvantages of Blockchain:

The biggest advantage of a blockchain is immutability, meaning it is impossible to erase or replace the recorded data, hence it prevents tampering withing the blockchain.

Blockchain is decentralized, meaning any network member can verify the recorded data. Due to this transparent nature, blockchain is trustworthy. [20]

The blockchain has no central authority, meaning no single organisation controls it. Therefore, no authority including governments can interrupt the operation of the network. [20]

Blockchain creates an irreversible audit trail and allows easy tracing of any changes on the network. [20]

Blockchain technology has a limit for transactions per second, hence scalability is an issue. Every transaction requires verification and consensus from every node, and as the network grows, and many nodes are added, the consensus mechanism becomes even more time and energy consuming. [20]

Blockchain technology does not allow easy data modification once the data is recorded. It requires rewriting the codes in all the blocks, which is time consuming and expensive. Hence it is hard to correct any mistakes or make adjustments. [20]

Scalability of blockchain means it should be capable to add thousands of globally distributed nodes, while still processing thousands of transactions per second. Currently none of the prevailing blockchains are scalable. [21]

Blockchain depends extensively on private keys for data encryption, but these private keys if lost, stolen, or compromised in any way, all encrypted communications using that key become vulnerable to unauthorised access. [22]

The costs of operating a blockchain application are high due to the requirements of high computing power and storage capabilities. [20]

6. Using Block Chain for Cyber Security

Blockchain Technology can find applications in many fields of Cybersecurity due to its inherent structure and design.

- It is exceedingly difficult for hackers to breach the blockchain system, as it would require simultaneously compromising multiple nodes in a decentralised network. So, the decentralised security is a powerful feature to safeguard data and systems.
- The data stored on the blockchain cannot be modified or deleted once it is recorded. Any changes made to the already recorded data are processed as new transactions and data integrity is ensured. This feature can be used to create tamper - proof audit trails and transaction logs. The feature of immutable records can be useful for detecting and preventing frauds.
- Self - executing contracts, where the terms of agreement between buyer and seller (two parties) are directly written into a line of code. This feature is useful to automate the process and eliminate the need of intermediaries.
- Blockchain Technology uses cryptographic hashes and digital signatures, and this prevents data tampering and ensures that the information recorded/stored on blockchain is legitimate and valid. Data is also encrypted using advanced algorithms and cryptography.
- There are many nodes in a Blockchain, and each node has a copy of the distributed ledger and so the correct Blockchain is always accessible to other peers even when a few nodes are not available or compromised.

All these features make Blockchain technology a valuable tool to prevent cyberattacks, data breach or identity theft.

a) **Preventing Data Manipulation:** Blockchain uses combination of public and private keys for secure transactions. [23] A public key is a user's address on the blockchain, while a private key is a secret information that allows them to initiate trades. Only individuals with correct private key can access and share their data for identity verification. Which ensures integrity and security of data. [24]

b) **Protecting Identities:** The transaction details like sender addresses, recipient addresses, amounts etc. can be obscured. Anonymity plays important role for individual privacy and freedom. With pseudonymous addresses and cryptographic techniques reduces the risk of personal information being exploited for malicious purposes. [24]

c) **Preventing DDoS attacks:** DDoS attacks are easy because the parts of Domain Name System (DNS) aka phonebook of internet are stored centrally and susceptible to attacks and thefts. The use of decentralised Blockchain can minimise DNS theft and DDoS attacks. Additionally, cyberattacks are promptly identified and prevented from entering the system because every block modification in the Blockchain must be confirmed with the other blocks. [24]

7. Conclusion

Blockchain technology offers significant potential in enhancing cybersecurity through its decentralized and immutable nature, which can prevent data breaches and cyberattacks. Its potential to revolutionise data protection and trust in current digital era is immense. However, its widespread adoption faces challenges such as scalability, regulatory acceptance, and the need for high computational power. Overcoming these challenges could position blockchain as a transformative tool in digital security, paving the way for more secure and resilient systems. Blockchain has the potential to usher in a new era of safeguarding our digital infrastructure.

References

[1] Gillis, A. S., & Pratt, M. K. (2024, July 5). *What is a cyber - attack? | Definition from TechTarget.* Security; TechTarget. https: //www.techtarget. com/searcgsecurity/definition/cyber - attack

[2] *What is cybersecurity? – Cisco*. Cisco. Retrieved August 2, 2024, from https: //www.cisco. com/site/us/en/learn/topics/security/what - is - cybersecurity. html
[3] Houston, R., & Campbell, T. (2024, July 20). Blockchain 101: Definition, Explanation, Pros & Cons. Business Insider; Insider. https: //www.businessinsider. com/personal - finance/investing/what - is - blockchain
[4] Kerner, S. M. (2022a, April 26). *Colonial Pipeline hack explained*: *Everything you need to know*. WhatIs; TechTarget. https: //www.techtarget. com/whatis/feature/Colonial - Pipeline - hack - explained - Everything - you - need - to - know
[5] Moes T, (2024). *Spyware Examples (2024): The 5 Worst Attacks of all Time.* Software Labs. https: //softwarelab. org/blog/spyware - examples/
[6] Zetter K. (2014 November 10). *DarkHotel: A sophisticated New Hacking Attack Targets High - Profile* Guests. WIRED. https: //www.wired. com/2014/11/darkhotel - malware/
[7] Reed J. (2023, May 8). *How the ZeuS Trojan info stealer changed cybersecurity.* Security Intelligence. https: //securityintelligence. com/articles/how - the - zeus - trojan - info - stealer - changed - cybersecurity/
[8] Keary, T. (2018, November 21). *DoS vs DDoS: Key Differences and Prevention in 2024.* Comparitech. https: //www.comparitech. com/net - admin/dos - vs - ddos - attacks - differences - prevention/
[9] Yoachimik, O., & Pacheo J. (2024, January 9). *DDoS threat Report for 2023 Q4.* The Cloudfare Blog; https: //blog. cloudfare. com/ddos - threat - report - 2023 - q4
[10] Kosinski, M. (2024, May 17). *What is Phishing?* | IBM. https: //www.ibm. com/topics/phishing
[11] Irwin L. (2022, October 20). *The 5 Biggest Phishing Scams of All Time – IT Governance Blog.* En. IT Governance Blog En. https: //www.itgovernance. eu/blog/en/the - 5 - biggest - phishing - scams - of - all - time
[12] Folger, J. (2006, May 15). *What is Spoofing? How Scam Works and How To Protect Yourself.* Investopedia. https: //www.investopedia. com/terms/s/spoofing. asp
[13] Baker, K. (2024, April 25). *What is an IoT Attacks and How Can you Prevent it?* | Enterprise Technology News - IT Community EM 360 Tech. https: //em360tech/tech - artcile/what - is - iot - attack
[14] Ravikiran, A. (2020, May 11). *What is Blockchain Technology? How does Blockchain Work?* Simplilearn. https: //www.simplilearn. com/tutorials/blockchain - tutorial/blockchain - technology
[15] Nathan, C. (2024 March 20). *What are blocks in a blockchain?* TheBlock. https: //theblock. co/learn/245697/what - are - blocks - in - a - blockchain
[16] MacDonald R. (2024, April 17). *Blockchain Identity Management: A Complete Guide - 1Kosmos.*1Kosmos. https: //www.1kosmos. com/blockchain/blockchain - identity - management - a - acomplete - guide/
[17] *Types of Blockchains - Geeksforgeek. (*2022, April 27). GeeksforGeeks. https: //www.geeksforgeeks. org/types - of - blockchain/
[18] Smith, A. (2024, July 8). *What is Blockchain Technology, and How Does It Work?* Blockchain, AI & Web3 Certifications | Online Training & Courses | Blockchain Council; https: //www.blockchain - council. org/blockchain/what - is - blockchain - and - how - does - it - work/
[19] McFadden, C. (2023, March 14). *Proof of Work vs. Proof of Stake: understanding the key differences.* Interesting Engineering. https: //interestingengineering. com/innovation/difference - between - pos - and - pow/
[20] Budhi V. (2022, October 20). *Advantages and disadvantages of Blockchain Technology*. Forbes. https: //www.forbes. com/sites/forbesbesttechcouncil/2022/10/20/advantages - and - disadvantages - of - blochain - technology/
[21] Lim, S. Y., Fotsing, P. T., Almasri, A., & Musa, O. (2018). *Blockchain Technology the Identity Management and Authentication Service Disruptor: A survey.* ResearchGate; International Journal on Advanced Science, Engineering and Information Technology. https: // www.researchgate. net/publication/ 328919940 _ Blockchain _Technology_the_Identity_Management_and_Authentication_Service_Disruptor_A_Survey
[22] Edward R. (2023, June 21). *Unveiling the Achilles Heel: The Major Disadvantage of Using a Private Key for Data Encryption.* https: /newsoftware. net/blog/major - disadvantge - of - using - a - private - key - for - data - encryption/
[23] Newbie's Guide: *Private key vs Public Key – How They Work? (2021, June 6).*101 Blockchains. https: //101blockchains. com/private - key - vs - public - key/
[24] R. (2023, March 31). *Blockchain: The secret weapon for Cybersecurity*|

Web Links

[25] https: //www.infosys. com/insights/cyber - security/cybersecurity - blockchain. html
[26] https: //www.encora. com/insights/blockchain - the - weapon - for - cybersecurity