**HAN22080221**

System Security and Recovery Plan Report:

Security in blockchain

# I. Introduction

Blockchain, a distributed leger technology (DLT), has drawn interest from governments, researchers, and industries. It shows potential across various fields, particularly banking and finance. Enterprises like JPMorgan and IBM have developed their own blockchain platforms, while China has been actively testing its digital yuan for mass adoption. While blockchain inherent security benefits, it is still vulnerable against attacks and malicious actors. As the use of blockchain becomes more widespread, the critical need for security within this technology cannot be overstated.

First, the foundation aspect of blockchain technology will be provide with exploration of blockchain types and consensus algorithms. This is crucial to recognize potential threat within the blockchain and practices to safeguard it.

The second section explore tools and methods available to malicious actors for exploiting blockchain systems. Various types of attacks and manipulate techniques will be covered, from direct attacks to the blockchain peer-to-peer system to the techniques targeting the applications running blockchains. The section will provide a nuance understanding of potential vulnerabilities.

Finally, the report discusses defences against the mentioned threats, measurements for businesses to protect valuable data in the blockchain system, including robust security practices, encryption methods, and access controls. This aims to empower enterprises by fortifying their blockchain infrastructure and maintaining their data integrity.

The topic will be investigated with analysis of existing literature, case studies and practical implementation in blockchain security. With insights from diverse sources, the report aims to provide valuable knowledge about the technology and practices for securing blockchain systems.

# II. Blockchain and consensus algorithms

## 1. Blockchain fundamentals

For millennia, ledgers have been used for storing transactions and similar data in paper form. In the late 20th century, they have been digitized due to the advent of computers. However, these ledgers required a central entity to validate their authenticity. The 21st century comes with advanced algorithms, cryptography, and powerful computing, allowing distributed ledger to be a viable record form.

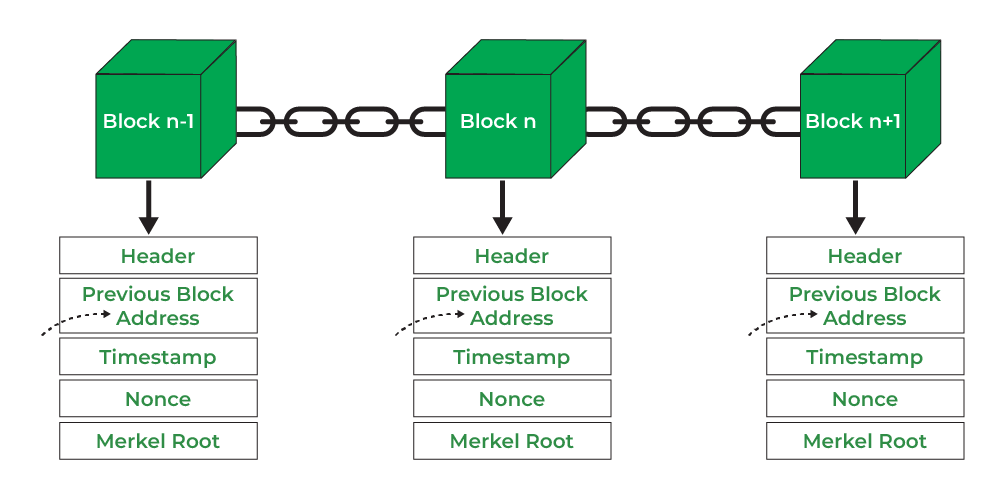
DLT uses peer-to-peer networking technology, where multiple nodes are used to store, validate, and update the leger simultaneously. This means DLT can operate when at least one node is available. These attributes of DLT eliminates the necessity for a trusted third party and has reduced risk of single point of failure.A diagram of different types of buildings

Description automatically generated

**Fig. 2.1** Comparation between distributed (Barney, 2023).

Transactions and records within DLT are handled in a decentralized and distributed fashion. Various data management and organize strategies can be implemented in DLT such as tree-like data structures or Directed Acyclic Graph. When data organized as a linear linked list of blocks, it is commonly referred as “blockchain”.

As mentioned above, a blockchain is made of “blocks”, the first block is called genesis block. The transactions are encrypted in a block using cryptographic function to not be tampered. Blocks usually contain timestamp, Merkle root, a nonce, transactions, and previous block hash(Kibet, et al., 2019; Yang, et al., 2019). Then blocks will be validated by node using the blockchain consensus method. Once verified, these blocks are linked together, simply in a linear order, forming a blockchain.

**Fig. 2.2** Typical blocks linked in the blockchain network (m0hitkirange, 2022).

The following points will address the features of blockchain:

* **Decentralization**

Blockchain has no central entity to control and validate transactions, the control capabilities are shared among the users.

* **Transparency**

Blockchain (particularly public blockchain) are highly transparent. Anyone can track transactions and transactions history, making them transparent. However, this high level of transparency may affect anonymity and (Preethi, Khare and Tripathy, 2020).

* **Availability**

Blockchain can operate when having at least one node running, making the system availability higher than centralized systems (with single point failures).

* **Immutability**

Transactions added to the blockchain and validated by the participating nodes. The transaction cannot be changed or tampered.

* **Pseudonymity**

Blockchain allows pseudonymity, users can perform transactions on the network using pseudo-anonymous addresses (Nakamoto, 2008). However, Research showed that users on the network can be de-anonymized (Nasser & Zhang, 2019; Wang, et al., 2018; Ndung'u, 2022).

* **Security**

The blockchain is secured using strong public/private keys, hashing-algorithms, digitals signature, and encryption techniques.

* **Data tampering**

Blockchain current block store the hash of the previous block, this serves as a reliable method to detect data tampering within the network.

Despite blockchain powerful advantages, the technology also has its own limitations, challenges, and threats. These will be explained in the below:

* **Storage capacity**

Blockchain is read and append only, meaning the blockchain is always on- going growth in size. Furthermore, within traditional blockchains, each participating node has a copy of the entire blockchain. As the chain continues to grow, so does storage demand on individual nodes. Hence, raise the requirement of physical hardware for storage (Alizadeh, et al., 2020) and computing performance. Methods such as pruning, sharding and off-chain storage are presented to solve the issue, however, with trade-offs (Halim, 2022).

* **Blockchain trilemma**

The concept was popularized by Vitalik Buterin stating that a blockchain problem of achieving decentralization, scalability, and security simultaneously. Popular blockchains such as Bitcoin (Nakamoto, 2008), Ethereum (Buterin, 2014)and Near Protocol’s Nightshade (Skidanov & Polosukhin, 2019) all affect from the blockchain trilemma. See the following example analysis:

* + Bitcoin:

Bitcoin low throughput is well-known, the blockchain can only handle 27 transaction per second (TPS) maximum (Georgiadis, 2019). Research shows that the size of blockchain has great impact on its performance (Reyna, et al., 2018; Wang, et al., 2018; Preethi, et al., 2020; Alshahrani, et al., 2023). Currently, bitcoin is handling an average of 5 to 6 TPS (Blockchain.com, 2023) To summarize, bitcoin sacrificed scalability for decentralization and security.

* + Ethereum:

Ethereum tackled bitcoin scaling and resource issues by switching its consensus protocol to Proof-of-Stake (Kapengut & Mizrach, 2022). This does solve the scalability and computing problem but the blockchain becomes more centralized (Tang, et al., 2023; Werth, et al., 2023).

* + Near Protocol:

Near implemented Nightshade, a sharding protocol, aiming for scalability. However, Nightshade sharding is complicated process and upheld potential vulnerabilities (Skidanov & Polosukhin, 2019).

* **Privacy**

Despite blockchain is known for its anonymity, users in the network can be de-anonymized. Behaviour analysing, or IP address mapping can be used to link the pseudo address with the owner (Nasser & Zhang, 2019; Wang, et al., 2018; Ndung'u, 2022).

* **Future computation**

In the future, computer may be able to decrypt blockchain’s encryption or the recent quantum computer. Although post-quantum computation solutions (Tiago & Paula, 2020) are presented, it is not guaranteed that blockchains are immune to these attacks.

## 2. Types of blockchain

Due to the blockchain technology wide applications in many fields, blockchain comes in variety to suit the needs within organizations. The types of blockchain can be classified from 2 different perspectives: node management and structure based.

### 2.1. Node Management

This refers to the characteristics of the blockchain as permissioned, permissionless, or both.

* **Permissionless**

The blockchain is open for anyone, allowing anyone to join, participate and validate transactions and become a node without requiring permission. Viable for operations that the requirements transparency and immutability is critical.

* **Permissioned**

The right to participate and validate in the network is restricted only to a specific group of participants. Participants can only join and become nodes if permitted. Suitable for businesses and enterprises operations that requires a higher degree of privacy and centralized governance.

### 2.2. Blockchain Structure

Based on the blockchain structure, the blockchain can be classified as public, private, consortium or hybrid.

* **Public blockchains**

Also known as permissionless blockchain, it’s a decentralized blockchain network that allows anyone to participate, validate, and make transactions without any permission. Can be used for crypto currency, voting systems, etc.

* **Private blockchains**

In private blockchain, only a permitted group of users is allowed to access and participate in the network. Can be used for healthcare, governmental services, etc.

* **Consortium blockchains**

Consortium blockchain is semi-decentralized network where multiple organizations collaborate and share control over the blockchain. Can be used in supply chain, connect multi sector industries, etc.

* **Hybrid blockchains**

Hybrid blockchain offers flexibility by combining elements from both public and private blockchains to achieve specific goals. The blockchain usually has a public layer for transparency and a private layer to store restricted information. Capable of all the use cases of consortium, private and public blockchain.

**Table 2.1** Comparison of the 4 blockchain structures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Public | Private | Consortium | Hybrid |
| Type | Permissionless | Permissioned | Permissioned | Both |
| Decentralization | Truly decentralized | Partly decentralized | Semi-decentralized | Semi-  decentralized |
| Transparency | Transparent | Controlled transparency | Controlled transparency | Partial transparent |
| Speed | Slow | Fast | Fast | Fast |
| Scalability | Low | High | High | High |
| Consensus algorithm | Proof-of-Work, Proof-of-Stake | PBFT, Proof of Elapsed Time | PBFT, RAFT | Any |
| Immutability | Complete immutability | Partial immutability | Partial immutability | Partial immutability |
| Example | Bitcoin (Nakamoto, 2008), Ethereum (Buterin, 2014) | Hyperledger Fabric (Hyperledger Foundation, 2018), Quorum (Consensys, 2018) | IBM food trust (IBM, 2019), Interbank Information Network | DragonChain (DragonChain, 2017) |

## 3. Consensus Algorithm

This report will primarily focus on the three most well-known algorithms.

### 3.1 Proof of Work (PoW)

The concept of PoW is requiring computing effort as a mean of verification (Back, 2002). In Bitcoin, miner compete to find the nonce value that, when hashed with the block data, produces a hash with the required 0 bits (Nakamoto, 2008). In a PoW network, miners compete to reveal the next block, as the first wins the block reward.

However, the consensus suffers greatly from high energy consumption and low throughput and scalability. Bitcoin annal energy consumption is 139.16 TWh, higher than Ukraine (digiconomist.net, 2023).

### 3.2 Proof of Stake (PoS)

PoS, an energy-effecient alternative design for PoW, is proposed (King & Nadal, 2012) as a consensus that uses the blockchain currency holdings for verification.

Validators send their holdings into the network; this action is called “staking”. The network then selects a few validators to perform minting of the block, the chance of being selected is affected by the staking amount and some randomness. Once the new block is minted, the validators are award with the block’s transaction fees.

PoS is more scalable and energy-efficient compared to PoW; Ethereum after shifting to PoS consensus witnessed 98% drop of power (Kapengut & Mizrach, 2022). However, PoS is more centralized as the highest bidders are to be chosen all the time.

### 3.3 Practical Byzantine Fault Tolerance (PBFT)

PBFT addresses the Byzantine Generals Problem, enabling consensus even in the presence of malicious nodes (Castro & Liskov, 1999). PBFT should contain at least 3f+1 total of nodes, where f is the number of malicious/faulty node the network can handle. Nodes within network takes turn as primary, backup and client in the three-phases commit protocol:

1. **Pre-Prepare**

* Primary broadcast a “pre-prepare” message with proposed block in the network to initiate the consensus process.

1. **Prepare**

* Upon receiving the “pre-prepare” message, each backup node broadcasts a “prepare” message which expresses its agreement.
* To advance, a node needs “prepare” messages from at least 2f+1 nodes.

1. **Commit**

* Having received enough messages, a node broadcasts a “commit” message.
* The block is considered as committed when received “commit” message from at least 2f+1 nodes.

In case the primary node went faulty or inactive, PBFT uses a view change protocol to find a replacement.

PBFT may suffer in larger networks due to the communication overheads in the network. Consequently, PBFT is most suitable for permissioned blockchains with limited number of nodes.

# III. Attacks on Blockchain

## 1. The 51% Attack

The 51% attack or the majority attack is a well-known vulnerability of the blockchain technology that happen when an individual or a group managed to attain over haft of the network hash rate. Having most of the hash rate, the attacker can perform the following:

* Attacker can prevent blocks and transactions from being verified, invaliding them.
* Attacker can reverse transactions during their control, allowing them to perform double-spending transactions.
* Attacker can create a hard fork of the blockchain and split the network.
* Miners are prevented from finding block for a period.

Notably, the purpose of this attack is still achievable even without sufficient hash rate, malicious mining pool or lending hash power can be combined with selfish mining behaviour to perform fraudulent transactions (Saad, et al., 2019; Dey, 2018).

The bigger the blockchain, the less feasible this attack will be. It costs an estimate of $1,573,409 USD to perform an hour of 51% attack on the bitcoin network (Crypto51, 2023). Other blockchain such as Ethereum, the majority attack requires occupying have the blockchain’s token, making it even more economically impractical. However, PBFT, commonly used in private blockchain, is more vulnerable to this attack. PBFT systems can only handle 33% of the network fault, comparing to 50% from PoW and PoS.

For example, in 2014, GHash.io’s Bitcoin mining pool hash rate reached over the threshold of 51% of the network. Even though no harm was done, the event showed the vulnerability and problem in Bitcoin-based systems. Later in 2018, Bitcoin Gold was exploited by this vulnerability, resulting in $18 million USD worth of cryptocurrency stolen.

## 2. Distributed Denial of Service Attacks

Distributed Denial of Service (DDoS) is a well-known attack on online services, Blockchains are not exception for this attack. DDoS attacks can be manifested in various ways based on the network architecture, application nature and peer behaviour.

For instance, 51% attacks can cause denial-of-service. A group or individual with majority hashing rate can invalidate transactions and blocks from other miners, causing failures in the network. In PBFT based network, the attacker can calculate the required “f” number of sybil nodes in such way the total node less than 3f+1, then the attacker can launch a DoS on the network (Saad, et al., 2019)

Malicious actor floods the network with low value transactions using Sybil identities; The attacker that processes multiple wallets. By creating a burst of transactions, the network can experience congestion as blocks are filled with those transactions. This may also lead to mempool flooding, causing an increase in gas price. When the pool contains many unconfirmed transactions, the urgency for mining raises. Honest users are tempted to pay more for their transactions to be mined, while attacker’s is not and will be rejected. Hence, a DoS attack was launched on the network.

November 2017, Attacker flooded Bitcoin mempool with dust transactions, causing transactions stalled reach $700 million USD in total (Memoria, 2021). Another case in 2022, a play-to-earn game Sunflower Farmer consumed over 50% of Polygon network, result in 60% gas fee spike (Thurman, 2022).

## 3. Network Attacks

### 3.1 DNS Attack

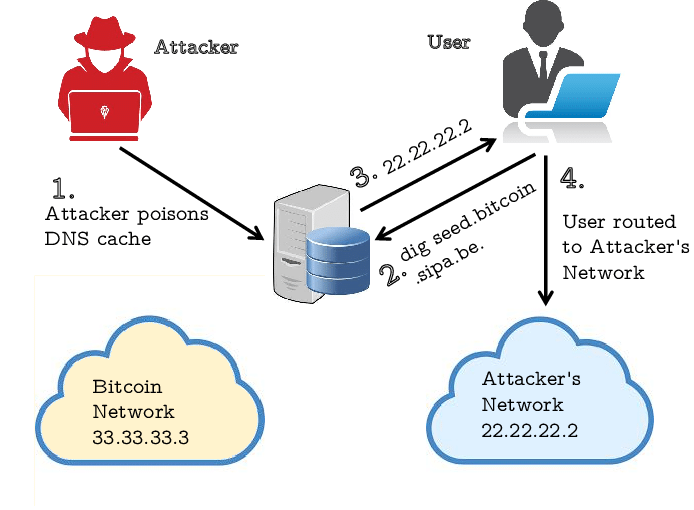
When the first time a node connects to the network, the node uses bootstrap mechanisms such as DNS to discover active peers in the network. The initials DNS query returns DNS A record along with IPs of active peers from DNS seed servers. Such techniques can be vulnerable to man-in-the-middle attacks, cache poisoning and stale records. Saad et al (2019) showed potential DNS resolution attack where the attacker injected a fake seeders list to redirect the user.

Fig 3.1 DNS poisoning attack (Saad, et al., 2019)

### 3.2 Eclipse Attack

A node maintains an honest view on the blockchain by communicating with its neighboring peers. The attacker may compromise the node by isolating it using IP addresses, therefore controlling its traffic, and feeding it false information. An honest node maintains its blockchain view when it is connected to one or more honest nodes.

Fig 3.2 Eclipse attack. A remained honest with an honest neighbour. Once they disconnect (isolated), A and the peer got compromised.

## 4. Smart Contract Exploitation

With the advent of Blockchain 2.0, Ethereum introduced smart contracts using Solidity. As decentralized applications (DApps) gain popularity, deficiency in smart contracts programming poses significant threats to the application.

Most DApps are fully open-sourced, project developers usually have a public GitHub repository. Some other do not but their smart contract are visible in blockchain explorers. Hackers can take advantage of this to view the project source code.

A screenshot of a computer

Description automatically generated**Fig 3.3 & 3.4** Uniswap V3 smart contract on [GitHub](https://github.com/Uniswap/v3-core) and [Etherscan](https://etherscan.io/address/0xe592427a0aece92de3edee1f18e0157c05861564#code).

Then, hacker attempt to read the code for vulnerabilities with assistance of various tools:

* Visualization: Solidity Visual Developer, Sūrya, Solgraph, EVM lab
* Static and Dynamic Analysis: MythX, Mythril, Slither, MadMax
* Classification: EEA EthTrust Security Levels

### 4.1 Reentrancy Attack

A computer screen shot of a program code

Description automatically generatedReentrancy is vulnerability where an attacker exploits an unsynchronized state during external contract call, allowing an unintended loop of recursive callbacks to main function.

**Fig 3.5** The DAO inspired reentrancy vulnerability example.

### 4.2 Overflow and Underflow

A computer screen shot of code

Description automatically generatedThis type of attack occurs when an attacker sends wrong transaction information to the smart contract, causing the calculation to go upper bound () or lower bound (-1), the calculation value is set to 0 or respectively.

**Fig 3.6** Overflow and underflow vulnerability example.

### 4.3 Short Address Attack

A computer screen with text

Description automatically generatedThis attack exploits a bug in the Ethereum’s virtual machine. By using address that is less than 20 bytes long, EVM will pad the data with the right 0 bytes to meet expected length. This can cause vulnerable contracts to interpret the zeros as valid data, leading to unexpected behaviour.

**Fig 3.7** Example short address vulnerability contract.

### 4.4 Denial-of-Service (DoS) Attack

A computer screen shot of a program code

Description automatically generatedHappens when the attacker send execute a poorly optimized function or intended loop to exhaust the smart contract gas. Once smart contracts exhaust their limit gas, transactions and functions are prevented from executing, causing a DoS attack.

**Fig 3.8** DoS vulnerable contract example.

# IV. Countering Measure and Practices

## 1. Countering Peer-to-Peer Attacks

Research has been conducted to address the 51% attack. Bastiaan (2015) proposed a defense against 51% attack by a stochastic analyst of two-phase Proof-of-Work (2P-PoW), presented Ittay and Emin (2018), in the bitcoin network. 2P-PoW is a continuous-time Markov chain that contains two cryptographic challenges instead of one for the mine to solve. 2P-PoW removes incentives for miners in large pools and prevents large pools from reaching the threshold by either outsourcing their hash rate or exposing their private keys. Tuyet, Lei and Hong-Sheng (2017) proposed 2-hop blockchain, a combination of PoW and PoS, allowing honest users to maintain control of the network even if the adversary has the majority hash rate. For PBFT-based systems, solutions have been proposed to improve the algorithm scalability and fault tolerance rate (YANG, et al., 2022; Gao, et al., 2019).

Johnson et al. (2014) introduced a game-theoretic approach to protect mining pool from DDoS attacks. Saad, Thai and Mohaisen (2018) proposed fee-based and age-base design for mempools. Other countermeasures include creating a minimum value in transactions or increasing the blockchain throughput by having big block size or lower block creation time. Each of them has their own caveats.

Regarding network-based attacks, research has been made to enhance the blockchain with safeguard against DNS attack. Apostolaki et al. (2017) proposed a list of countermeasures for short and long term. They proposed peer monitoring systems, methods to increase node connection diversity and long-term solutions such as adopting Message Authentication Code and other networking security measures.

## 2. Countering Smart contract Attacks

To counter smart contract attacks, developers should implement a multi-faceted security strategy. This includes code audits, employing secure coding practices to identify and mitigate risks. Additionally, staying informed about emerging threats and regularly updating their smart contracts is essential. Implementing access controls, utilizing established security tools like Slither and MythX for automated analysis, and setting appropriate gas limits are crucial steps. Lastly, the blockchain network should be monitored for unusual activities and potential vulnerabilities to defense proactively.

## 3. Blockchain Data Protection for Enterprises

### 3.1 Blockchain Type

Permissioned Blockchain are prefer for its restriction to the network only for authorized participants.

### 3.2 Data Encryptions and Key Management

Data stored on the blockchain should be encrypted, encryption methods such as asymmetric and homomorphic are reliable. Sensitive data can be stored off-chain and the blockchain is used solely for references or hashes. This keeps the data immutable without exposing direct access to sensitive information.

As cryptographic keys are used for end-to-end encryption and decryption, management is crucial. It is recommended to use cryptographic key management standard from Enterprise Security Office (2018) and NIST framework such as Cryptographic Key Management Systems (Barker, et al., 2013).

### 3.3 Access Control

Enforce strict access controls to permit who can read or modify data on the blockchain. The NIST standards are recommended including Non-Discretionary Access Control, Discretionary Access Control, Mandatory Access Control and Role-based Access Control, and policies such as Chinese Wall policy (Hu, et al., 2006).

### 3.4 System Security

Protocols, blockchain nodes, smart contracts, and software should be kept up to date with the latest security patches. Employees should be educated and trained about the security implications of blockchain technology, secure practices, such as safeguarding private keys and security protocols.

Regular security audits should be conducted to identify and mitigate vulnerabilities and immutability audits to maintain data integrity. Implement continuous monitoring solutions to detect any suspicious activities or unauthorized access in real-time.

# V. Conclusion

This report discussed the current types of blockchain, investigate various tools and methods used by fraudsters to exploit the technology, and how to protect the blockchain and its data.

Word count: 3247 words Total:4219

# References

1. Alizadeh, M., Andersson, K. & Schelen, O., 2020. *Efficient Decentralized Data Storage Based on Public Blockchain and IPFS.* [Online]   
   Available at: https://www.diva-portal.org/smash/get/diva2:1510141/FULLTEXT01.pdf
2. Alshahrani, H. et al., 2023. *Sustainability in Blockchain: A Systematic Literature Review on Scalability and Power.* [Online]   
   Available at: https://www.researchgate.net/publication/368273999\_Sustainability\_in\_Blockchain\_A\_Systematic\_Literature\_Review\_on\_Scalability\_and\_Power\_Consumption\_Issues
3. Anon., n.d. s.l.:s.n.
4. Apostolaki, M., Zohar, A. & Vanbever, L., 2017. *Hijacking Bitcoin: Routing Attacks on Cryptocurrencies.* [Online]   
   Available at: https://ieeexplore.ieee.org/document/7958588
5. Back, A., 2002. *Hashcash - A Denial of Service Counter-Measure.* [Online]   
   Available at: http://www.hashcash.org/papers/hashcash.pdf
6. Barney, N., 2023. *Diagram of distributed ledger technology.* [Online]   
   Available at: https://cdn.ttgtmedia.com/rms/onlineimages/cio-distributed\_\_vs\_central\_ledger-f.png
7. Bastiaan, M., 2015. *Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin.* [Online]   
   Available at: https://fmt.ewi.utwente.nl/media/175.pdf
8. Blockchain.com, 2023. *blockchain.com.* [Online]   
   Available at: https://www.blockchain.com/explorer  
   [Accessed 2023].
9. Buterin, V., 2014. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform..* [Online]   
   Available at: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum\_Whitepaper\_-\_Buterin\_2014.pdf
10. Castro, M. & Liskov, B., 1999. *Practical Byzantine Fault Tolerance.* [Online]   
    Available at: https://pmg.csail.mit.edu/papers/osdi99.pdf
11. Consensys, 2018. *Quorum Whitepaper.* [Online]   
    Available at: https://github.com/Consensys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf
12. Crypto51, 2023. *Crypto51.* [Online]   
    Available at: https://www.crypto51.app/  
    [Accessed 19 November 2023].
13. Dey, S., 2018. *Securing Majority-Attack In Blockchain Using Machine Learning And Algorithmic Game Theory: A Proof of Work.* [Online]   
    Available at: https://arxiv.org/pdf/1806.05477.pdf
14. digiconomist.net, 2023. *digiconomist.net.* [Online]   
    Available at: https://digiconomist.net/bitcoin-energy-consumption   
    [Accessed 19 November 2023].
15. DragonChain, 2017. *DragonChain.* [Online]   
    Available at: https://whitepaper.io/document/58/dragonchain-whitepaper
16. Duong, T., Fan, L. & Zhou, H.-S., 2017. *2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely.* [Online]   
    Available at: https://eprint.iacr.org/2016/716.pdf
17. Eyal, I. & Sirer, E. G., 2014. *How to Disincentivize Large Bitcoin Mining Pools.* [Online]   
    Available at: https://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/
18. Gao, S., Yu, T., Zhu1, J. & Cai, W., 2019. *T-PBFT: An EigenTrust-Based Practical Byzantine Fault Tolerance Consensus Algorithm.* [Online]   
    Available at: https://mypage.cuhk.edu.cn/academics/caiwei/paper/papers/GaoYZC2019.pdf
19. Georgiadis, E., 2019. *How many transactions per second can bitcoin really handle ?.* [Online]   
    Available at: https://eprint.iacr.org/2019/416.pdf
20. Halim, R. P., 2022. *Decentralization, Scalability, and Security Trade-off in Blockchain System: Comparison on Different Approaches.* [Online]   
    Available at: https://essay.utwente.nl/91994/1/Halim\_BA\_EEMCS.pdf
21. Hyperledger Foundation, 2018. *An Introduction to Hyperledger.* [Online]   
    Available at: https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/HL\_Whitepaper\_IntroductiontoHyperledger.pdf
22. IBM, 2019. *About IBM Food Trust.* [Online]   
    Available at: https://www.ibm.com/downloads/cas/8QABQBDR
23. Johnson, B. et al., 2014. *Game-Theoretic Analysis of DDoS Attacks Against Big and Small Mining Pools.* [Online]   
    Available at: https://www.researchgate.net/publication/263605255\_Game-Theoretic\_Analysis\_of\_DDoS\_Attacks\_Against\_Big\_and\_Small\_Mining\_Pools
24. Kapengut, E. & Mizrach, B., 2022. *An Event Study of the Ethereum Transition to Proof-of-Stake.* [Online]   
    Available at: https://arxiv.org/abs/2210.13655
25. Kapengut, E. & Mizrach, B., 2023. *An Event Study of the Ethereum Transition to Proof-of-Stake,* s.l.: s.n.
26. Kibet, A., Bayyou, D. G. & Esquivel, R., 2019. *BLOCKCHAIN: IT'S STRUCTURE, PRINCIPLES, APPLICATIONS AND FORESEEN ISSUES.* [Online]   
    Available at: https://www.researchgate.net/publication/332858253\_BLOCKCHAIN\_IT'S\_STRUCTURE\_PRINCIPLES\_APPLICATIONS\_AND\_FORESEEN\_ISSUES
27. King, S. & Nadal, S., 2012. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.* [Online]   
    Available at: https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf
28. m0hitkirange, 2022. *Structure of Blockchain.* [Online]   
    Available at: https://media.geeksforgeeks.org/wp-content/uploads/20221111160733/Structureofblocksinblockchain.png
29. Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]   
    Available at: https://bitcoin.org/bitcoin.pdf
30. Nasser & Zhang, B., 2019. *SoK: A Systematic Study of Anonymity in Cryptocurrencies.* [Online]   
    Available at: https://www.researchgate.net/publication/338370170\_SoK\_A\_Systematic\_Study\_of\_Anonymity\_in\_Cryptocurrencies
31. Ndung'u, R. N., 2022. *Blockchain as a Solution of Information Security and Data Privacy Issues: Review.* [Online]   
    Available at: https://www.researchgate.net/publication/362577744\_Blockchain\_as\_a\_Solution\_of\_Information\_Security\_and\_Data\_Privacy\_Issues\_Review
32. Preethi, D., Khare, N. & Tripathy, B., 2020. *Security and Privacy Issues in Blockchain Technology.* [Online]   
    Available at: https://www.researchgate.net/publication/347192637\_Security\_and\_Privacy\_Issues\_in\_Blockchain\_Technology
33. Reyna, A. et al., 2018. *On blockchain and its integration with IoT. Challenges and opportunities.* [Online]   
    Available at: https://www.sciencedirect.com/science/article/pii/S0167739X17329205#sec2
34. Saad, M. et al., 2019. *Exploring the Attack Surface of Blockchain: A Systematic Overview.* [Online]   
    Available at: https://arxiv.org/pdf/1904.03487.pdf
35. Saad, M., Thai, M. T. & Mohaisen, D., 2018. *POSTER: Deterring DDoS Attacks on Blockchain-based Cryptocurrencies through Mempool Optimization.* [Online]   
    Available at: POSTER: Deterring DDoS Attacks on Blockchain-based Cryptocurrencies through Mempool Optimization
36. Skidanov, A. & Polosukhin, I., 2019. *Nightshade: Near Protocol Sharding Design.* [Online]   
    Available at: https://pages.near.org/downloads/Nightshade.pdf
37. Tang, D., He, P., Fan, Z. & Wang, Y., 2023. *Pool competition and centralization in PoS blockchain network.* [Online]   
    Available at: https://www.tandfonline.com/doi/abs/10.1080/00036846.2023.2274311
38. Thurman, A., 2022. *CoinDesk.* [Online]   
    Available at: https://www.coindesk.com/tech/2022/01/06/polygon-under-accidental-attack-from-swarm-of-sunflower-farmers/
39. Tiago, M. F.-C. & Paula, F.-L., 2020. *Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks.* [Online]   
    Available at: https://www.researchgate.net/publication/338779877\_Towards\_Post-Quantum\_Blockchain\_A\_Review\_on\_Blockchain\_Cryptography\_Resistant\_to\_Quantum\_Computing\_Attacks
40. Wang, H. et al., 2018. *Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services.* [Online]   
    Available at: https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf
41. Werth, J. et al., 2023. *A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma.* [Online]   
    Available at: https://www.researchgate.net/publication/369452419\_A\_Review\_of\_Blockchain\_Platforms\_based\_on\_the\_Scalability\_Security\_and\_Decentralization\_Trilemma
42. YANG, J. et al., 2022. *Improved Fault-Tolerant Consensus Based on the PBFT Algorithm.* [Online]   
    Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9718319
43. Yang, X., Liu, J. & Li, X., 2019. *Research and Analysis of Blockchain Data. Journal of Physics: Conference Series.* [Online]   
    Available at: https://www.researchgate.net/publication/334424125\_Research\_and\_Analysis\_of\_Blockchain\_Data/