Cyber Security – Blockchain Security

[**1. Introduction**](#_1nbp2elh2b8t) **1**

[**2. What is blockchain?**](#_axqxubvybl1q) **1**

[**3. Tools to exploit blockchain**](#_e0y9b7trvaeh) **2**

[**4. Different types of blockchain**](#_ksor4mhf9dya) **3**

[a, Public blockchain](#_sm8mz2cr4ua6) 3

[b, Private blockchain](#_vwypj3mm4x67) 3

[c, Hybrid blockchain](#_qgf74srg7620) 4

[d, Consortium blockchain](#_lmg0iag6d5fe) 4

[**5. Protect different types of blockchain from fraudsters**](#_s4g94dekdvtt) **5**

[**6. Different ways for enterprise to protect their data in blockchain**](#_kzejqh1uks2h) **5**

[**7. Conclusion**](#_t7sz1l6pdjsw) **6**

[**8. References**](#_ttihu8979fzd) **7**

## 1. Introduction

Blockchain technology brings plenty of advantages in property transaction management, such as improving security and advance in efficiency. Due to its importance, blockchain technology has become an ideal target for hackers to attack. Therefore, this discussion will explore different ways and tools that frauders can use to exploit this technology, as well as clarify different types of blockchain, methods to protect each type from frauders, and give solutions for enterprises to protect their own data.

## 2. What is blockchain?

Blockchain is a high-digital-technology, decentralized, distributed ledger, which will record transactions between users in a network. Data will be stored in blocks and linked together in a chain. All data recorded in the network is unaltered and stays constant over time due to its link algorithm, cryptographic hashes. In a blockchain network, there will be two main components:

● A participant or a machine that keeps a copy of the blockchain network's complete transaction history and takes part in transaction validation and verification is referred to as a "node". The distributed ledger of the blockchain is an ever-expanding list of blocks, and each node has a copy of it.

● Other main part of a blockchain is a "block". A batch of validated and confirmed transactions are contained in this data structure. The structure of the blocks is usually chained together, with each block including a reference to the one before it. The blockchain's integrity and immutability are guaranteed by this connectivity between blocks.

## 

## 3. Tools to exploit blockchain

Although blockchain's features such as decentralization, immutability or integrity make it seem safe and very secure, its network infrastructure can still have vulnerabilities for hackers or fraudsters to exploit. Here are various tools and techniques fraudsters can use to attack blockchain:

1. Phishing: This is a common technique fraudsters use to steal personal data from victims. Blockchain participants will be sent an email impersonating a blockchain or e-wallet that appears trustworthy and legitimate, and it will require the user to enter personal information such as password, or private key. This will lead to losses of data and assets of the victims and the whole network.

2. Malware: Malware, when accessing a person's device in the blockchain, will cause great danger to the blockchain. There are various ways malware is used, such as:

● Keyloggers: Keyloggers are tools that will record and steal every keystroke of the victim, causing personal information to be exposed. Some popular software include Windows Keyloggers, IwantSoft Keyloggers,...

● Wallet and Account Hijacking: Malware may directly attack blockchain accounts or wallets. It might replace or alter trustworthy wallet software, causing users to inadvertently install dangerous versions of the wallet. Once installed, the virus might cause the user to lose money by hijacking transactions, changing addresses, or rerouting cash to the attacker's address.

● Smart contract exploit: Once malware penetrates the blockchain, it will utilize vulnerabilities scanner and analyzer tool to find possible weakness in the code of smart contract, such as reentrancy attacks or integer overflow/underflow, or Decompilers and Debuggers, which aid in analyzing and decompiling smart contract bytecode to identify potential vulnerabilities or hidden functions. When it has altered or corrupted the smart contract's code. This may lead to unexpected activities being carried out or unlawful access to the money stored in the smart contract, which might cause losses of money or upset the blockchain ecosystem.

3. 51% Attack Tools: A group of miners manipulating more than 50% of the network's mining hash rate can launch a 51% attack on a cryptocurrency blockchain. The parties in charge might potentially change the blockchain if they had 51% of the network's nodes. The attackers would be able to stop transactions between some or all users by blocking fresh transactions from gaining confirmations. In addition, transactions that were finished while they were in charge might be undone. One of the problems that consensus algorithms like PoW were designed to prevent is that reversing transactions might allow them to double-spend coins, meaning attackers spend some cryptocurrencies to purchase a product, they can reverse the transaction and get their money back, while still owning the product. Fraudsters can use thí these tools to make a 51% attack:

● Mining Power: An attacker may accumulate a significant amount of computing power or control a large portion of the network's mining nodes to gain majority control and manipulate transactions.

● Selfish Mining Software: Selfish mining is a strategy where an attacker with a smaller share of the network's computing power can still manipulate the blockchain by strategically withholding or selectively releasing blocks to gain an advantage.

4. Distributed Denial of Service: Blockchain’s characteristic, decentralization, has protected itself from being attacked by DDos as one or several nodes is down or offline, the rest can still work normally. However, fraudsters can still find ways to apply DDoS on blockchain: transaction flooding. Transactions that have not been added to the current block due to the block reaching capacity will be recorded in the Mempool, a virtual waiting room for unprocessed transactions, and will be added to the next block. The attacker will then flood the current block with spams and errors continuously, making the pending transaction unable to proceed and the blockchain will lose its functionality.

## 4. Different types of blockchain

### a, Public blockchain

The first type of blockchain, public blockchain, is a non-restricted and permissionless blockchain network, in which all participants of the blockchain can read, change as well as authenticate transactions without authority. It uses distributed-ledger-technology that data is distributed across a network of nodes, which means public blockchain is decentralized and its consensus mechanisms, Proof-of-Work (PoW) and Proof-of-Stake (PoS), allow members to agree on the current condition of transactions . Therefore, the independence of the public blockchain is extremely high, as no individual or organization can unilaterally control the blockchain, all nodes in the blockchain must coordinate with each other to maintain and validate the ledger. Besides, immutablity is also a notable feature of this blockchain as any node added to the blockchain, it is very difficult to change any data inside that block because of the combination of its cryptographic hashing and consensus mechanism. However, due to its decentralization, the blockchain may expand to an enormous scale and organizations or governments cannot take control or restrict access to the network. Moreover, because every node must work together, it consumes a huge amount of time and energy to maintain the blockchain, which reduces the scalability of this blockchain as the more nodes added, the more time and energy the network takes.

Bitcoin is the most outstanding use case of public blockchain. Bitcoin, the first blockchain-implemented cryptocurrency, utilizes peer-to-peer transfers to send and receive digital currency between participants and its mechanism is PoW that miners verify transactions and add them to the blockchain by dealing with difficult mathematical problems.

### b, Private blockchain

The second type of blockchain is private blockchain. Despite using peer-to-peer manner and decentralization like public blockchain, private blockchain is only used in a small scope within a company or organization, and is managed by an entity, any activity in the blockchain requires permission from the network administrators. Therefore, accessing control is the biggest advantage of private blockchain. Admin can grant or revoke rights to any node, such as allow a node to view data but cannot change anything. Besides, it is so private that no third party can access it because only authorized or trustworthy entities are available to see transactions and data. However, due to the privacy of private blockchain, all authority is concentrated in one individual or group of people, making network behavior less objective and transparent. Besides, the more nodes in the blockchain, the more work the administrator has to control, making it difficult for the blockchain to expand.

A typical use case of private blockchain is the medical industry, where personal patient data is stored and accessed only by authorized parties. Thanks to that, doctors can easily look up the patient's condition on the system, making medical examinations more convenient.

### c, Hybrid blockchain

Hybrid blockchain is the combination of two above blockchain, including components of private and public blockchain. Businesses can allow which data is visible to all participants and which particular individual can access specific data stored in the blockchain by combining a private, permission-based system with a public, permissionless system. Hybrid blockchain’s feature is that transactions and data are not in public, but can be checked when needed, and they are unalterable even with the blockchain administrators. Therefore, privacy is one of its advantages, compared to public blockchain because not all data is accesible, each participant must be authorized or meet some requirements to reach that data. Besides, attackers cannot use 51% technique to take control over the network. Transactions are also affordable, quick and scalable rather than public blockchain. However, the operation of hybird blockchain is much more complicated than public and private, as it requires smooth coordination of the public side and private side, and there may be vulnarables in operation. Since information may be hidden, this kind of blockchain isn't totally transparent. Users have little motivation to engage with the network or contribute, and upgrading might be difficult.

Hybrid blockchain is widely used in many fields, and is largely used in the supply chain. Businesses may gain from greater traceability, higher security, simpler processes, and more transparency by implementing a hybrid blockchain for supply chain management. It facilitates communication between supply chain players while safeguarding confidential data, which eventually results in an ecosystem of the supply chain that is more reliable and efficient.

### d, Consortium blockchain

A consortium blockchain is a semi-decentralized blockchain, formed by a group of businesses or organizations sharing a common goal, in which only pre-licensed members can access the network, and each member is a node and has equal power and responsibility. While every node may read and publish transactions, only a supermajority of nodes is allowed to add to a block. This rule must be fulfilled in order for the block to be added. The limited number of members with access helps prevent external data disclosure, providing greater data privacy and security within a federation. Organizational members are often highly responsible and trustworthy, so every member of the organization is empowered to make decisions within the network. In addition, the number of participating nodes is small so it can be easily scaled and not be clogged. However, if there is a conflict between nodes, the operation of the blockchain will be interrupted as it requires nodes to agree and cooperate closely with each other.

Consortium blockchains find applications in the energy sector for managing and trading renewable energy credits, optimizing energy distribution, and enabling peer-to-peer energy trading. Multiple energy producers, consumers, and grid operators can collaborate on a shared blockchain to improve transparency, automate transactions, and optimize energy usage.

## 5. Protect different types of blockchain from fraudsters

Besides considering what type of blockchain to use, making sure the blockchain is safe from fraudsters is also crucial to maintain the integrity, trust between users and the cyber security in overall. Therefore, some techniques can be applied:

● Consensus mechanism: By compelling participants to invest time and money in the process and providing incentives for acting in good faith as well as wasting bad actors time and money, consensus procedures serve as a defense against these kinds of attacks. Among them are the following:

- Proof-of-Work (PoW): This mechanism requires participants to spend time and effort by presenting complicated mathematical puzzles and requiring participants to solve them in order to verify newly created transaction blocks. When validating transaction finishes, a new block is added to blockchain and user will receive rewards.

- Proof-of-Stake (PoS): In PoS, participants must compete with each other to become validators of the blockchain. The more coins they own, the higher the rate of becoming a validator. The job of the selected people is to verify transactions and send the results into blocks. If correct, they will receive a transaction fee as a reward, otherwise, they have to pay a penalty for validating bad data.

By utilizing both consensus mechanisms, hackers cannot use 51% method to take control of the blockchain because though hackers can gain 51% of computer power or stake as the public side of the network still uses PoS or PoW consensus mechanism, the private side is independent and safe.

● Strong authentication method: The authentication method is the most direct and basic solution to prevent fraudsters from accessing the blockchain by adding one more layer of protection. There are some methods to be used:|

- Biometric authentication: The user's physical characteristics or behavior such as fingerprint, face, voice are used to ensure that only authorized users can participate in the network.

- Multi-factor authentication: Users are required to answer several questions that they set up before such as PIN or password, what is your favourite pet, what is the name of your middleschool, etc… to prove their identity.

- Public and private key authentication: two unique keys, public and private keys, will be given to each participant of the network. Private key is used to sign and decode the transactions while public key function is to verify and encrypt them.

● Code reviews and audits: Always check and asset the source code of smart contracts and transactions to identify vulnerabilities, bugs that fraudsters can exploit to attack the blockchain.

## 6. Different ways for enterprise to protect their data in blockchain

Data breaches to organizations and businesses happen regularly, while businesses today store their data on electronic platforms such as blockchain. Therefore, blockchain is an ideal target for hackers to attack and steal data. In order to prevent attacks and safeguard data, some strategies and techniques can be deployed by enterprises:

● Indentity and Access Management (IAM): to ensure that there is no unauthorized external access to the blockchain nor any unauthorized access to sensitive information within its network. Authority holders need to grant permissions to the right subjects and use multi-layer verification for targets wanting to participate in the blockchain.

● Data encryption: Encrypt private, confidential, and integrity-preserving data that is kept on the blockchain. Protecting data while it's in transit or at rest may be accomplished with encryption techniques like symmetric or asymmetric encryption combined with powerful cryptographic algorithms.

● Smart contract security: If the smart contract has vulnerabilities, hackers can invade and change the contract's behavior or steal information. Since every behavior in the blockchain is immutable, that will cause serious consequences. In order to find and address vulnerabilities, firms must thoroughly audit and test smart contracts. To guarantee the integrity and security of smart contracts, apply code reviews, secure coding techniques, and take into account independent security evaluations.

● Key management: private keys are generated and used to sign transactions and secure ownership of assets, helping to ensure the authenticity and integrity of transactions.

● Secure network infrastructure: Building structure in blockchain is very important. To ensure the safety of the blockchain, isolate threat actors from sensitive information, a firewall and threat detection system need to be installed. Besides, properly arranging nodes and blocks also helps the network operate smoother.

● Employee training: Technology is always changing and evolving, making ongoing employee training a must. They need to be educated about practices, or potential dangers that can occur with blockchain as well as how to prevent threats.

● Collaborate with security experts: cybersecurity experts can help businesses identify vulnerabilities, patch them, and enforce blockchain security.

## 7. Conclusion

In conclusion, despite various blockchain technology benefits such as decentralization, transparency, immutability, it can still be a target for fraudsters and hackers to exploit vulnerabilities. They can use different tools and techniques to impact the network. Therefore, understanding about these tools as well as safety measures may help organizations and enterprises protect themselve from being victims.

There are several tools that fraudsters may employ to exploit blockchain technology. These include 51% attacks, where an attacker gains control of the majority of the network's computing power, allowing them to manipulate transactions and double-spend coins. Additionally, smart contract vulnerabilities, such as code bugs or logic flaws, can be exploited to execute unauthorized actions or drain funds. Phishing and Malware can also be used to steal users’ personal data for bad purposes.

In order to prevent those attacks, organizations and companies should consider which type of blockchain they should implement. Public blockchain brings free and openless nature, therefore increases the danger and threat toward the blockchain. Private blockchain, in contrast, offers more control over participants and can implement stricter security measures. Hybrid and consortium blockchain combine two above types and have typical characteristics.

Protecting assets and data from fraudsters requires many approaches. Some security measures may include implementing authentication methods, using consensus mechanisms, or encrypting the data. Moreover, private keys, smart contracts, network infrastructure are things that can be actively secure to avoid threats.

In summary, protecting data in the field of blockchain requires a comprehensive and proactive security strategy.

**Word count: 2765 words exclude References and Headings**

## 8. References

Campbell, C. (2023) What are the 4 different types of blockchain technology?: TechTarget, CIO. Available at: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology (Accessed: 11 December 2023).

Crypto fraud in 2023: How can security teams fight (2023) Security Intelligence. Available at: https://securityintelligence.com/articles/crypto-fraud-in-2023-how-can-security-teams-fight/ (Accessed: 11 December 2023).

Das, T. (2023a) What is Blockchain Security? 2023 comprehensive guide, SelectHub raquo. Available at: https://www.selecthub.com/endpoint-security/blockchain-security/ (Accessed: 11 December 2023).

Das, T. (2023b) What is Blockchain Security? 2023 comprehensive guide, SelectHub raquo. Available at: https://www.selecthub.com/endpoint-security/blockchain-security/ (Accessed: 11 December 2023).

Gondek, C. (no date) What is a consortium blockchain?, OriginStamp. Available at: https://originstamp.com/blog/what-is-a-consortium-blockchain/#what-is-consortium-blockchain (Accessed: 11 December 2023).

Groopman, J. (2023) How to secure blockchain: 10 best practices: TechTarget, Security. Available at: https://www.techtarget.com/searchsecurity/tip/8-best-practices-for-blockchain-security (Accessed: 11 December 2023).

Reiff, N. (no date) Bitcoin vs. Ethereum: What’s the difference?, Investopedia. Available at: https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp (Accessed: 11 December 2023).

Spydra (2023) Benefits of private blockchain & its use cases, LinkedIn. Available at: https://www.linkedin.com/pulse/benefits-private-blockchain-its-use-cases-spydra#:~:text=Private%20blockchains%20are%20often%20used,the%20data%20on%20the%20network (Accessed: 11 December 2023).

Team, C. (2023) The importance of Blockchain Security , Chainalysis. Available at: https://www.chainalysis.com/blog/blockchain-security/ (Accessed: 11 December 2023).

What is ... (1978) Amazon. Available at: https://aws.amazon.com/what-is/blockchain/ (Accessed: 11 December 2023).

What is Blockchain Security? (no date) IBM. Available at: https://www.ibm.com/topics/blockchain-security (Accessed: 11 December 2023).

Cybersecurity (2023) What are the best ways to secure blockchain-based systems using Authentication Research and Innovation?, How to Secure Blockchain Systems with Authentication Innovation. Available at: https://www.linkedin.com/advice/0/what-best-ways-secure-blockchain-based-systems-using-kfq9e (Accessed: 11 December 2023).

DDoS in Blockchain (2022) GeeksforGeeks. Available at: https://www.geeksforgeeks.org/ddos-in-blockchain/ (Accessed: 11 December 2023).

Development, S. (2023) How do you conduct code reviews and audits to identify and fix security vulnerabilities?, Code Reviews and Audits: Secure Coding Best Practices. Available at: https://www.linkedin.com/advice/0/how-do-you-conduct-code-reviews-audits-identify (Accessed: 11 December 2023).

Frankenfield, J. (no date) 51% attack: Definition, who is at risk, example, and cost, Investopedia. Available at: https://www.investopedia.com/terms/1/51-attack.asp (Accessed: 11 December 2023).

Kickidler (no date) Top 10 best free keyloggers softwares for Windows, mac, and linux, Kickidler. Available at: https://www.kickidler.com/info/top-10-keylogging-tools-for-employee-monitoring.html (Accessed: 11 December 2023).