Blockchain Security: A Systematic Review

Parshwa Shah and Madhuri Chopade

Abstract Blockchain is a technology that is decentralized. It has the ability to tackle a wide range of industrial issues. A blockchain transaction's records are secured by cryptography, and each transaction is linked to previous transactions or records. Algorithms on the nodes validate blockchain transactions. As a final point, blockchains enable transparency, allowing each participant to keep track of transactions at any point in time. Smart contracts provide for safe transactions, reducing the risk of third-party interference. Readers will have a better understanding of how blockchain technology helps protect and manage today's users. There is a thorough report on diverse blockchain studies and security proposed by the research community, and their distinct implications on blockchain, in the review. This article concludes with a detailed description of the blockchain security followed by a discussion of the many varieties of security enhancements.

Keywords Blockchain · Security · Blockchain attacks

1 Introduction

The idea of a secure chain of blocks is certainly not a fresh one. In 1991, Stuart Haber [1] proposed a method for digitally timestamping electronic documents in order to prevent manipulating. However, in recent years, it has grown in prominence as a result of its application in blockchain technology to hold transaction records for the cryptocurrency "Bitcoin". Blockchain has the ability to "revolutionize apps and reshape the digital economy," according to experts [2]. By enabling collaboration without trust, blockchain holds immense promise for re-establishing "trust" in

P. Shah (✉) · M. Chopade
Gandhinagar Institute of Technology, Moti Bhoyan, Gandhinagar, India
e-mail: parshwas09@gmail.com

M. Chopade
e-mail: madhuri.chopade@git.org.in

P. K. Singh et al. (eds.), *Futuristic Trends in Networks and Computing Technologies*,
Lecture Notes in Electrical Engineering 936,
https://doi.org/10.1007/978-981-19-5037-7_69

society. Blockchain technology offers enormous promise for a wide range of applications and provides diverse foundations with a lot of flexibility. The technology aids resource management and ensures secure and effective communication. When using blockchain to conduct financial transactions between parties, trust is increased because it reduces the chances of fraud and automatically provides a record of movement. In the traditional framework, when it comes to monetary exchanges, people must faith in a third party to complete the transaction. However, blockchain will provide optimum security in exchanges. Each exchange should be recorded in a block, which will act as a record book. When an exchange is completed, a block is added to the blockchain, which serves as a permanent information database. When a block is finished, it is either added to another block or a new block is created. Every block in a blockchain has a hash of its previous block [3]. In its most fundamental form, blockchain is called a distributed ledger. Blockchain exchanges are nearly tamper-proof thanks to hashing and appropriate calculations. People may for the most part access historical transactions provided by a blockchain, yet changing historical transactions inside the record is somewhat inconceivable. This is expected to some degree to the way that it is scattered; however, it is additionally secured with different factors.

In Sect. 2, we started with a brief explanation of different types of blockchain followed by the inherent security features of blockchain in Sect. 3. The novelty of our paper started from Sect. 4, where we discussed various possible attacks to blockchain network and research done for counter measuring those attacks. Additionally, some security enhancements to blockchain has been discussed in Sect. 5 followed by some frameworks proposed by researchers in Sect. 6. In Sect. 7, we gave some topics on which future research can be carried out followed by conclusion and references at the end.

2 Different Type of Blockchains

There are three major kinds of blockchain technology.

2.1 Public Blockchain

From the security point of view, public blockchain is more secure as it is completely decentralized and no one is able to change past transactions; however, any node from the network is able to keep an eye on transaction, hence confidentiality is not maintained. Bitcoin and Ethereum are two examples.

2.2 Private Blockchains

In private blockchain, a centralized authority is assigned that means they can change or update any transactions, as a result becomes less secure. While, transactions are kept private in this blockchain. Proof of authority consensus is often used in private blockchain.

2.3 Consortium Blockchains

In consortium blockchains, a central authority preapproves known members before they may engage in consensus on a blockchain network. When using this "semi-permissioned" strategy, a network can be dispersed or partially decentralized, while yet maintaining some level of control. In banking or supply chain management, this form of blockchain is utilized between parties as to maintain security and save it from attacks.

3 Blockchain Features for Security

See (Table 1).

4 What Are the Effects of Security Attacks to Blockchain Network and Solutions Proposed to Combat that Attack

4.1 51% Vulnerability

Effect: There is a possibility of 51% launch on blockchains with proof of work (PoW) hashing control if a miner's hashing control exceeds half the entire blockchain. The content on blockchain might be deliberately altered by an intruder by launching a 51% assault. His control over that blockchain will be total.

Solution: Sayeed and Macro-Gisbert in their paper [9] tried focusing on cryptocurrencies that had low hashing power to demonstrate the flaws in the consensus process which bolsters this attack. They then provide 5 security techniques in their work. Another recent effort to combat this attack in named as "Permapoint" [10] minimizes the chain re-organization.

Table 1 Security features

Security feature	Definition
Ledger	It is an immutable database, in which transactions are only added. No one is able to delete or update past transactions. Data from ledger cannot be accessed by anyone [4]
Chain of block	Hash values are required for each block in blockchain. They are linked by their prior hash. If someone or an attacker changes some data then the hash of that block will change, and it will be unlinked to network which won't be possible. As a result, sensitive data or information will be better protected. It is impossible to proceed with a transaction if any of the nodes do not agree to it [5]
Smart contracts	Smart contracts are nothing but a computer program which acts as a lawyer between two transaction parties. A transaction can be carried out between two users only after they agree to smart contracts. Smart contracts, on the other hand, relate to scripts that are automatically performed on a shared database consisting of nodes that are mutually distrusting [6]
Consensus mechanism	At the point when a record update happens, an agreement cycle is used to approve exchanges and accomplish a concession to the exchange's effect. Consensus mechanisms known are: proof of work (PoW), proof of stake (PoS), proof of existence (PoE), proof of exercise (PoX), byzantine fault tolerance (BFT), proof of importance (PoI), proof of luck (PoL), and proof of elapsed time (PoET) [7]
Hash function	Corruption-resistance and one-way functioning are the hash function's fundamental criteria. In online or offline transactions, hashing is mostly used to protect the integrity of data. Using a hash function, you may verify the authenticity of a file obtained from an Internet source The usage of hashes in blockchain applications is becoming increasingly prevalent. Hash function SHA256 is the most widely used one in blockchains [8]

4.2 *Selfish Mining Attack*

Effect: By this attack, intruders can earn excessive incentives by wasting genuine miners' incentives. Forking a private chain is attempted by the attacker, who retains found blocks secretly. They would then mine on this secret chain and continue to achieve a considerably longer private branch than that of the public branch since they have more freshly found blocks on their own private chain. Fair miners are still working in public chains. So honest miners will waste computer resources and intruders will get incentives.

Solution: In order to mitigate this attack, the researchers tried using a genuine approach of mining to create truth state notation for each blocks along with allotting self-confirmation height to users' transactions.

4.3 Double Spending Attack

Effect: When some crypto assets are spent and those are then duplicated and spent again, then this process is called double spending attack. It becomes impossible to avoid double spending attacks. Example: 51% vulnerability, race, and vector76 attacks.

Solution: Nicolas and Wang introduced multistage secure pool which verify the transactions by using four well-defined steps. Begum et al. [11] present a series of countermeasures against double spending assaults.

4.4 BGP Hijacking Attack

Effect: At the point when packets are sent to their objective, border gateway protocol (BGP) is utilized as a routing protocol. Aggressors use BGP directing to capture the organization traffic of blockchain. To do BGP hijacking, network administrators should be in charge, which might be taken advantage of to postpone network traffic. A BGP attack on Bitcoin is investigated by Maria et al. [12].

Solution: A scheme named BGPCoin is proposed by Xang in [13] that creates smart contracts to conduct and manage allocation of resources on a temper-resistant Ethereum network. It is a reliable solution to this problem based on Ethereum and smart contract coding.

4.5 DAO Attack

Effect: A "decentralized and automated" smart contract allowed for duplicate withdrawals, putting people's digital assets at risk. The "DAO" hack, for example, saw $60 million US dollars stolen from a "decentralized and automated" smart contract.

Solution: To combat this attack, researchers proposed a technique on trials conducted with a tool named Contiki (A low power built tool for resource constrained environment) [14].

4.6 Liveness Attack

Effect: Liveness attack is proposed by Aggelos et al. [15] in order to delay the confirmation time of a target transaction. Both Bitcoin and Ethereum have been attacked in two different ways. There are three steps to a liveness attack, namely assault preparation, transaction denial, and blockchain retarder.

Solution: Conflux's consensus protocol effectively encapsulates two distinct block generation algorithms developed by Li et al. [16] to prevent the active liveness attack. The first is the ideal method, which allows for speedy confirmation, while the second is the cautious technique, which ensures consensus advancement. It is scalable and distributed blockchain technology with maximum bandwidth and rapid verification. It combines these two methodologies into an integrated consensus process by employing a revolutionary adaptive weight mechanism.

4.7 Sybill Attack

Effect: Attackers fabricate their identity and enter in a peer-to-peer network in order to harm the reputation of the computer security system.

Solution: Swathi in her paper [17] presented strategy to combat this attack by observing other nodes' behavior and scanning the nodes that are only transmitting the blocks to a single user.

5 Solutions/Research Proposed for Better Security

Security is the primary emphasis when it comes to blockchain technology, which is continuously being discovered and enhanced in order to achieve the goal of giving customers with better sufficient protection.

5.1 Mixing

Mixing services were created to keep users' addresses separate. As a consequence, the observer's ownership of coins is obscured through mixing, which is essentially a random exchange of user's coins with other users' coins. These mixing services, however, do not offer security against currency theft.

Mixcoin

CoinJoin was the first mixing technique [18]. Bonneau et al. suggested Mixcoin in 2014 as a way to make anonymous payments in Bitcoin and Bitcoin-like coins. The first stage was the introduction of Mixcoin, a cryptocurrency that aims to minimize the risk of robbery by holding the mixing service "responsible" if it takes a customer's money. Mixcoin expands the anonymity set to enable all users to mix coins at the same time to protect against passive attackers.

TumbleBit

To solve Mixcoin's accountability and anonymity issues, TumbleBit [19] proposes a solution that is completely compatible with Bitcoin. TumbleBit enables parties to send money to each other via an untrustworthy Tumbler. During a TumbleBit era, no one, not even the Tumbler, can identify which payment paid which payee.

CoinShuffle

CoinShuffle [20] is a protocol that enables users to use Bitcoin anonymously. CoinShuffle is based on the dissent accountable anonymous group communication system and has many benefits over the Bitcoin mixing methods that came before it. It does not need the involvement of a third party (whether trusted, responsible, or untrustworthy), and it is fully compatible with the existing Bitcoin system.

5.2 Non-Interactive Zero-Knowledge Proof (NIZK)

Zcash, zk-SNARK

Zerocoins, on employ fixed-value coins, therefore the e-cash outcome could not support full-fledged nameless payments. Also, before payment, unnamed coins must be converted into nameless coins by someone else. Transactions, on the other hand, do not allow for the concealment of information or transaction amounts. It was thus recommended that we use a currency called Zerocash in order to solve these difficulties. Anonymity and data transaction privacy are particularly important features of Zerocash, which uses anonymous currencies. As a result of this, transactions using a coin are much smaller, and the verification duration is much shorter particularly less than six minutes.

Zero-Knowledge (Range) Proof

Making them unlikable is a common way to safeguard the secrecy and anonymity of a transaction. To complete the transaction, the electronic cash system must verify that the online payer has access to classified information, such as the address from where the cash is coming. Notably, the zero-knowledge proof was designed specifically for situations such as those described in the previous sentence.

5.3 Digital Signature

Hellman and Diffie created the notion of digital signature in 1976 when they invented public key cryptography [8]. In public key cryptography, digital signatures are used for source authentication, integrity, and non-repudiation [8]. Forgery is impossible with the digital signature algorithm (DSA). Some of the signature schemes are discussed below.

Group signature

This method [21] enables members of a group to characterize cluster signed communications anonymously. The following eight criteria must be met by the security components created by group signatures: dependability and integrity, no framing, unforgeability, traceability, anonymity, unlink ability, unforgeable tracing verification, and coalition resistance.

Aggregate signature

A typical digital signature method with an aggregation function based on co-GDH, and bilinear mapping is an aggregate signature [22]. When there are some different signatures on different messages from several users then all these signatures is summarized into one single signature. The burden of signature storage and verification is significantly reduced by the aggregate signatures.

Monero Ring Signature

It was initially based from CryptoNote to protect the source of certain transaction or user handling that transaction. Monero is a hybrid cryptographic model which protect users' anonymity as it utilizes ring signature technology. It is also worth noting that a collection of prospective signatories is put together to generate an individual signature that may be used for transaction authorization. Its security is so powerful that even in case of any dispute or theft, the original identity of user cannot be revealed.

Blind signature

The issue of big number factor decomposition, discrete logarithm problem, and elliptic curve is used to create a blind signature [23]. Its unique property is because it distinguishes message before it is signed. The main aim is to secure transmitter's privacy. Encrypted voting systems and digital currency schemes utilizes blind signatures.

Another digital signature technique is proxy signature [24].

6 Other Security Enhancements

There are some frameworks proposed by researchers in order to make blockchain network more secure and private. The following table provides details about the same. These concepts can be explained in detail but due to space constraint, they are summarized below (Table 2).

Table 2 Different types of countermeasures

Framework	Definition	Impact
Quantitative framework	It consists of a blockchain simulator and security model plan. The input parameters for consensus are network and protocol [25]	It generates a high-level fundamental process for detecting attacks
Oyente	It is mainly built to flaws in Ethereum contracts with the help of evaluating bytecode of contracts that are stored on Ethereum technology [26]	It is easy and simple to install on a system. All the bugs in Ethereum contracts are reported efficiently
Town crier	Town crier works as a mediator between clients and HTTP Web, as it gathers information from Web and then directs it to clients through blockchain network [27]	Information is secured will traveling as blockchain is used and also improves the reliability of transaction
Hawk	To improve security, developers use codeless smart contracts. This method increases privacy of smart contracts	The transactions on blockchain which are private are stored in a private part, while information which is not so important can be seen publicly [28]. It automatically generates cryptographic model in private smart contract
Lighting network	It uses double signing concept. A successful transaction is carried out only after both the parties involved signs the transaction receipts [27]	Third-party miner is not needed, which maintains confidentiality. Security is ensured due to double signing [29]
SegWit	It runs side by side, parallely to a blockchain network and signature data generated at the blockchain level is transferred to SegWit channel [30]	More blockchain space is liberated which results in faster transactions [31]. The signature data is stored in a Merkle tree. Network security has improved due to data diversity

7 Future Recommendations and Conclusion

There are various issues which are yet to be solved. Some of them are mentioned here:

- Firstly, many frameworks are there to mitigate attacks but a framework that can combat multiple attacks at the same time is a future research prospect in this field.
- Secondly, decentralized applications are increasing day by day and with that increases issues of data leakage. This problem should be solved using application hardening, code obfuscation, etc.

- Furthermore, at present, Bitcoin is used worldwide, and the use of cryptocurrencies at global level is increasing exponentially. This results in more criminal activities, with the help of cryptocurrencies, like money laundering, ransomware, and purchase of illegal goods like weed, cocaine, etc. For this, a friendly crypto architecture should be proposed which aids governments to find out those users who are performing suspicious illegal transactions to punish them accordingly.
- In future with the increasing use of quantum computing, traditional algorithms of digital signature can be easily decoded. For this, some researchers have suggested to use quantum cryptography. So, quantum-base key distribution requires more research.
- Consensus algorithms play a vital role in blockchain networks and prior research focused significantly on probabilistic reasoning. The difficulty of finding an efficient collection of parameters, modeling options, protocol variations, and compromises in the implementation of these algorithms is still unresolved.
- As private keys are an important feature, a framework for end-to-end communication of keys should be introduced.

This paper extensively discusses blockchain security and despite the fact that blockchain security is constantly improving, vulnerabilities continue to be discovered, and security research is ongoing. Furthermore, this study explored the many security difficulties, obstacles, and assaults that restrict the growing use of blockchain technology from a range of perspectives. For each assault, we discussed its effect and possible consequence. Eventually, we review recent advancements in blockchain security by different researchers and offered some recommendations for further research.

References

1. Anderson JR Security engineering: a guide to building dependable distributed sys
2. Singh S, Singh N (2016) Blockchain: future of financial and cyber security, in tems, 2nd ed. Indianapolis, IN, USA; Wiley, 2008. In: 2016 2nd international conference on contemporary computing and informatics IC3I, pp 463–467. https://doi.org/10.1109/IC3I.2016.7918009
3. Stephen R, Alex A (2018) In: IOP conference series: materials science and engineering 396: 012030
4. https://www.coindesk.com/information/who-created-ethereum
5. https://www.business2community.com/tech-gadgets/issues-blockchain-security-02003488
6. Bartoletti M, Pompianu L (2017) An empirical analysis of smart contracts: platforms, applications, and design patterns. In: Financial cryptography and data security: Springer, Cham
7. Abeyratne SA, Monfared RP (2016) Blockchain ready manufacturing supply chain using distributed ledger. Int J Res Eng Technol 5(9):1–10
8. Salman T, Zolanvari M, Erbad A, Jain R, Samaka M (2019) Security services using blockchains: a state of the art survey. IEEE Commun Surveys Tuts 21(1):858–880, 1st Quart
9. Sayeed S, Marco-Gisbert H (2019) Assessing blockchain consensus and security mechanisms against the 51% attack. Appl Sci 9(9):1788

10. Odera L (2020). Ethereum Classic and IOHK team up to find solutions to prevent 51% attacks on the blockchain. Accessed on 20 Dec 2020. [Online]. Available: https://bitcoinexchangeguide.com/ethereumclassic-iohk-team-up-to-find-solutions-to-prevent-51-attacks-on-the-blockchain/
11. Begum A, Tareq AH, Sultana M, Sohel MK, Rahman T, Sarwar AH (2020) Blockchain attacks, analysis and a model to solve double spending attack. Int J Mach Learn Comput 10(2):1–6
12. Apostolaki M, Zohar A, Vanbever L (2017) Hijacking bitcoin: routing attacks on cryptocurrencies. In: IEEE symposium on security and privacy, pp 375–392
13. Xing Q, Wang B, Wang X (2017) POSTER: BGPCoin: a trustworthy blockchain-based resource management solution for BGP security. In: 2017 proceedings ACM SIGSAC conference on computer and communications security, pp 2591–2593
14. Ghaleb B, Al-Dubai A, Ekonomou E, Qasem M, Romdhani I, Mackenzie L (2019) Addressing the DAO insider attack in RPL's Internet of Things networks. IEEE Commun Lett 23(1):68–71
15. Kiayias A, Panagiotakos G (2016) On trees, chains and fast transactions in the blockchain. URL https://eprint.iacr.org/2016/545.pdf
16. Chenxin L, Peilun L, Dong Z, Zhe Y, Ming W, Guang Y, Wei X, Fan L, Andrew CY (2020) A decentralized blockchain with high throughput and fast confirmation. In: Proceedings USENIX annual technical conference (USENIX ATC), pp 515–528
17. Swathi P, Modi C, Patel D (2019) Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In: Proceedings 10th international conference on computing, communication and networking technologies (ICCCNT), pp 1–6
18. Meiklejohn M et al (2016) A fistful of bitcoins: characterizing payments among men with no names. Commun ACM 59(4):86–93. https://doi.org/10.1145/2896384
19. Heilman E, Alshenibr L, Baldimtsi F, Scafuro A, Goldberg S (2017) TumbleBit: an untrusted bitcoincompatible anonymous payment hub. In: Proceedings of NDSS https://doi.org/10.14722/ndss .2017.23086
20. Ruffing T, Moreno-Sanchez P, Kate A (2017) P2P mixing and unlinkable bitcoin transactions. In: Proceedings of NDSS. https://doi.org/10.14722/ndss .2017.23415
21. Chaum D, Heyst EV (1991) In: Proceedings of advances in cryptology—EUROCRYPT '91. Group Signatures (Springer, Berlin, Heidelberg, 1991), pp 257–265
22. Dan B, Gentry C, Lynn B, Shacham H (2003) In: Proceedings of international conference on the theory and applications of cryptographic techniques. Aggregate and verifiably encrypted signatures from bilinear maps (Springer, Berlin, Heidelberg, 2003), pp 416–432
23. Chaum D (1984) Blind signature system. In: Proceedings of advances in cryptology—CRYPTO '83, Santa Barbara, California, USA, August 21–24, pp 153
24. Mambo M, Usuda K, Okamoto E (1996) Proxy signatures for delegating signing operation. In: Proceedings of the 3rd ACM conference on computer and communications security. New Delhi, India, March 14–16, pp 48–57
25. Er-Rajy L, El Kiram My A, El Ghazouani M, Achbarou O (2017) Blockchain: bitcoin wallet cryptography security, challenges and countermeasures. J Internet Banking Commerce 22(3):1–29
26. Karame G, Androulaki E (2016) Bitcoin and blockchain security. Norwood, MA, USA: Artech House
27. Idelberger F, Governatori G, Riveret R, Sartor G, Evaluation of logic-based smart contracts for blockchain systems. In: Proceedings international symposium on rules and rule markup languages for the semantic web, Cham, Switzerland: Springer, pp 167–183
28. Aitzhan NZ, Svetinovic D (2018) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Depend Sec Comput 15(5):840–852
29. Zaghloul E, Li T, Mutka MW, Ren J (2020) Bitcoin and blockchain: security and privacy. IEEE Internet Things J 7(10):10288–10313. https://doi.org/10.1109/JIOT.2020.3004273
30. Kiayias A, Panagiotakos G (2015) Speed-security tradeoffs in blockchain protocols. IACR Cryptol ePrint Arch 2015:1–27

31. Cachin C (2017) Blockchains and consensus protocols: snake oil warning. In: Proceedings 13th European dependable computing conference (EDCC), pp 1–2
32. https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/securityand-privacy-in-blockchain-environments
33. Natoli C, Gramoli V (2016) The balance attack against proof-of-work blockchains: the r3 testbed as an example. ArXiv preprint: arXiv:org/1612.09426
34. Rivest RL, Shamir A, Tauman Y [n. d.] How to leak a secret, pp 552–565