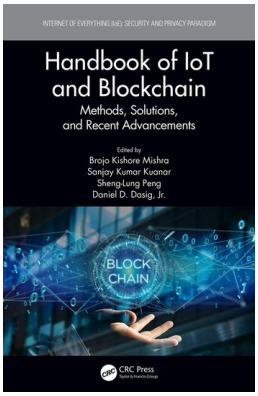

Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements

Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, Daniel D. Dasig

Security and Privacy-Enhancing Technologies for Blockchain and Cryptocurrency

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-8
Debasis Gountia, Utkalika Satapathy
Published online on: 26 Nov 2020

8 Security and Privacy-Enhancing Technologies for Blockchain and Cryptocurrency

Debasis Gountia and Utkalika Satapathy
CET (BPUT) Bhubaneshwar, India

CONTENTS

8.1 INTRODUCTION

Among recently technological advances, blockchain technology is an emerging new approach in the domain of information technologies. Blockchain is the use of advanced cryptographic proficiencies to implement a distributed system by a decentralized ledger of all existing transactions across a peer-to-peer (P2P) network, and allow fast processing of transactions in potentially trustless surroundings. It has firmly caught the imagination of cryptonerds, researchers, central bankers, and programmers, as well as politicians. By design, blockchain is a distributed decentralized tamper-proof ledger of records. Using blockchain technology, parties can control transactions without the need for a central certifying authority. Its potential applications allow fund transfers, voting, settling trades, and many other attractive uses. In blockchain, a transaction is the set of hash of the previous digitally signed transaction and the public key of the next owner. Each transaction is signed with a private key, and is verified by the public key [1], as shown in Figure 8.1.

Its working principle:

1. Anyone can request a transaction.
2. The requested transaction should broadcast to a P2P connection consisting of computers called nodes.
3. The nodes validate the transaction and the user's status using existing known algorithms.

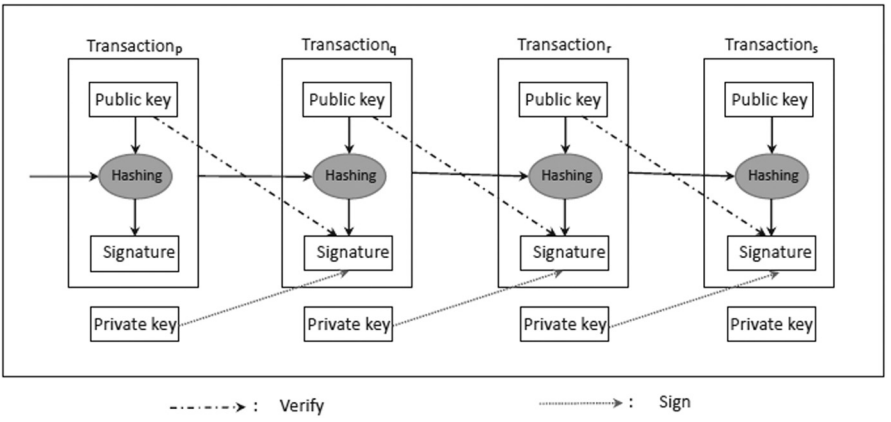

FIGURE 8.1 Network of transactions in a blockchain.

4. A validated transaction can exhibit cryptocurrency, records, contracts, and/or other important information. Cryptocurrency is a medium of exchange, generated and stored electronically in blockchain, using more secured encryption techniques to handle the generation of monetary units and to confirm the truth of the transfer of funds; bitcoin is the most suitable example.
5. Once validated, this transaction is merged with other transactions to generate a new block of information for the ledger.
6. The new data block is then combined to the existing blockchain permanently that is unalterable.
7. The transaction comes to a finish or an end.

In blockchain technology, data is stored in the form of multiple required blocks and these blocks are connected with each other through a network. A newly generated block would be connected to its former block; in this way this method creates a chain of blocks, which is called a blockchain. The process of adding new blocks to the blockchain is called mining [2]. The data stored in the block is permanent as it cannot be easily and directly changed. It is a very critical task to make any alteration or modification to the stored data. This is so because it needs agreement from all participating nodes for any update in the blockchain.

Each block of the blockchain consists of a hash of the previous block. A hash is the sequence of multiple characters and numbers. The features of transparency and verifiability prevent unauthorized access to the blocks and hence do not allow any changes. "No brainer" use cases are offered for applying blockchain technology by capital and finance markets. Bitcoin has proved itself successful in producing digital money and tracking its ownership. Today, there exist hundreds of cryptocurrencies. These blockchain technologies have become very attractive and popular due to the following facts of multi-activities in terms of privacy and confidentiality in the field of transactions:

- Support for all digital transactions
- Transparency
- Accurate tracking
- Cost reduction
- Provenance
- Permanent ledger: Creates an open permanent ledger, which makes it safe and easier to share information within the network
- Auditability
- Elimination of middleman: Avoids the need of a middleman which is able to reduce cost
- Faster time to market

Projects involving blockchain concepts should strive to prepare protocols in a manner such that their participants are incentivized to maximize the value of the system as a whole; in other words, it should be more profitable to secure and create the blockchain ecosystem more valuable than it is to cheat and make profit for oneself. This idea should be the essence for the design of the protocol underlying bitcoin's blockchain.

As the blockchain market has grown very quickly in the past few years, malicious people's attacks on the blockchain system are becoming a serious threat to transactions. Hence it is urgent to conduct research on the security issues of blockchain.

The remainder of this chapter is organized as follows. Section 8.2 presents related work on bitcoin scalability trade-off. Different effective attacks associated with blockchain are elaborated in Section 8.3 along with their potential defenses in Section 8.4. Comparisons and results analysis is presented in Section 8.5. Finally, conclusions are drawn in Section 8.6.

8.2 RELATED WORK ON BITCOIN SCALABILITY TRADE-OFF

Scalability is the strength of a system, process, or network to handle an increasing number of tasks with time, or its potential to be enhanced to adjust to that growth. For example, a network is considered scalable if it is capable of growing its total output when load is increased and resources such as hardware are merged with the system. Scalability is a substantial factor in computer systems, for example, databases, networking, and routers.

Bitcoin scalability trade-off refers to the discussion regarding the constraints on the number of transactions a bitcoin network can handle to process and execute successfully. It is related to the fact that records (known as blocks) in the bitcoin blockchain are limited in size and frequency. Blocks of bitcoin contain the transactions on the bitcoin network. The on chain transaction processing capacity of the bitcoin network is limited by the average block creation time of ten minutes and the block size limit. These jointly constrain the throughput of network. The transaction processing capacity maximum is estimated between 3.3 and 7 transactions per second. There are various proposed and activated solutions to address this issue efficiently.

Enhancing the transaction processing limit of a network demands various improvements to the technical principles of bitcoin, in a process known as a fork. Forks can be classified into two types: soft fork and hard fork.

8.2.1 Soft Fork

A soft fork is any change of rules that enable recognition of newly produced blocks as valid by the old software. Thus it is backward-compatible. A soft fork is also able to split the blockchain when newly generated blocks not considered valid by the non-upgraded software and the new rules.

8.2.2 Hard Fork

In contrast to a soft fork, a hard fork is a software upgrade introducing new rules to the network, thus abolishing the old software that is not able to recognize new blocks as valid [3]. In case of a hard fork, all nodes meant to work in accordance with the new rules need to update their software.

If one group of nodes continues to follow the non-upgraded old software while the other group of nodes uses the new updated software, a split will take place. For

example, platforms such as Ethereum, introduced in Vitalik Buterin's paper [4], that can allow for the production of smart contracts; digital entities with ingrained computer code that execute contractual agreements based on future events [5]. These entities represent financial instruments, currency, and land ownership, etc. Ethereum has hard-forked to make all the investors in the DAO, which had been hacked due to a vulnerability in its code [6]. In this case, the split creates Ethereum and Ethereum Classic chains by the fork.

In 2014, the NXT community considered a hard fork that could have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT against a major cryptocurrency exchange. The hard fork proposal was rejected, and a few funds were retrieved after negotiations and ransom payment [7]. Alternatively, to assure from a permanent split, maximum nodes using the new upgraded software can return to the old rules, as was the case in the bitcoin split [8]. Bitcoin Cash is a hard fork of bitcoin enhancing the maximum block size. Bitcoin XT, Bitcoin Classic and Bitcoin Unlimited all supported an enhancement to the maximum block size through a hard fork.

Lei *et al.* [5] suggested a technique for secure key management in an Intelligent Transportation System (ITS). In [9], Khan *et al*. proposed that the intrinsic features of blockchain technology can be exploited to address many privacy and security related problems of IoT systems. In [10], a decentralized system is suggested which combines Inter Planetary File System (IPFS), Ethereum blockchain, and Attribute Based Encryption (ABE) to assure fine-grained access control to the owners and the users of the stored data.

Finally, Guo *et al.* [11] approach the combined blockchain with an Attribute Based Signature (ABS) mechanism to prevent collusion attacks in multiple authority parties.

8.2.3 Efficiency Improvements

Transaction throughput is limited practically by a parameter known as block size limit. Various increases to this limit, and proposals to remove it completely, have been proposed over bitcoin history.

8.3 EFFECTIVE ATTACKS ON BLOCKCHAIN

Blockchain has successfully started up a brave new world to create, hold, and distribute digital values in the world of business. Some are too afraid of blockchain to consider it to be the next wave of technology revolution; others dismiss this concept as a passing craze for the underworld of "crypto-cyber criminals". Figure 8.2 and Figure 8.3 summarize the different types of the emerging blockchain threats, vulnerabilities, and attacks that are described in the following sections. Many of the following problems and solutions described in this article are anticipatory in nature; we pose these problems based on our best knowledge of how current transaction systems work and extrapolate from the existing security literature. However, the ideas put forth in this research article are not intended to replace existing works. Instead, these hardware-based countermeasures can be used to bolster system security or provide assurances of security that would otherwise be unachievable to the blockchain world.

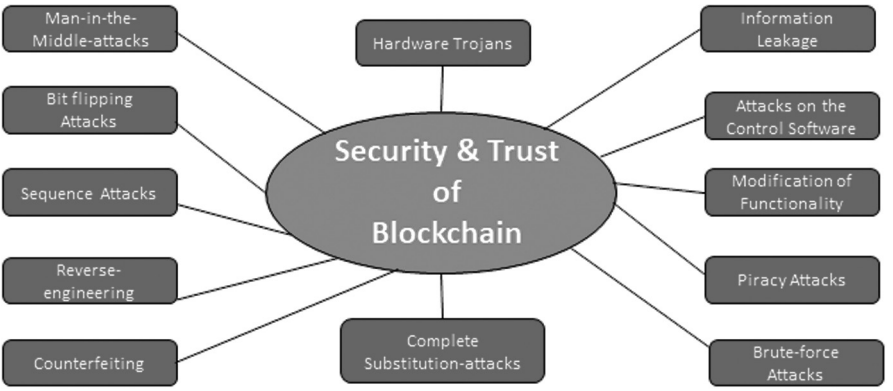

FIGURE 8.2 Blockchain security and trust consist of a diverse array of threats, vulnerabilities, and attacks.

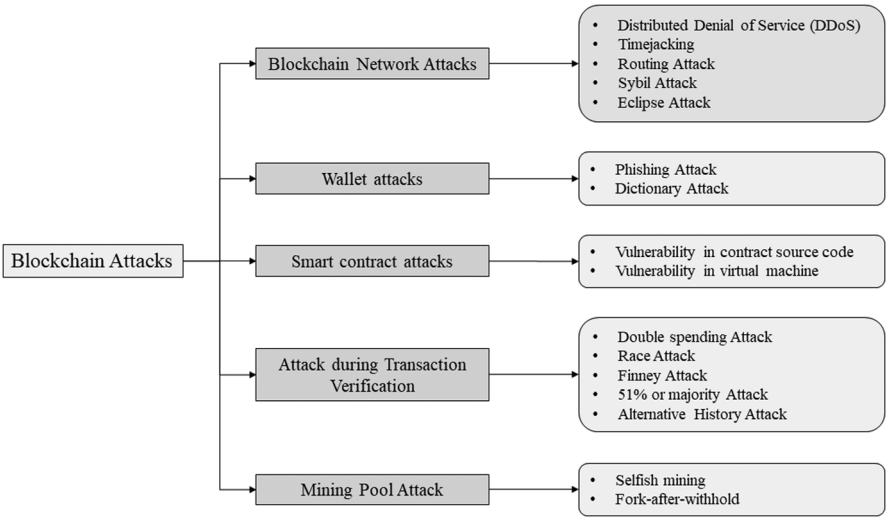

FIGURE 8.3 Different possibilities attacks on blockchain platform.

Blockchain technology is secured intrinsically. In blockchain, the data or ledger are distributed across several computers, and hence it has removed any single point failure. Furthermore, a blockchain is scarcely possible to hack due to the implementation of cryptographic proofs and consensus mechanisms such as game theory within it. With the above underlying security features; nevertheless, blockchain security issues still prevail.

8.3.1 Man-in-the-Middle Attacks

In the field of computer security, a man-in-the-middle attack is an attack where malicious people secretly relay and modify a transaction between two parties who believe

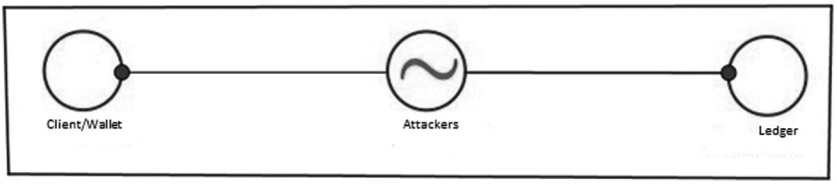

FIGURE 8.4 Man-in-the-Middle-attacks.

they are directly making a transaction with each other without any interference [12]. For example, active eavesdropping, where the attacker produces an independent connection between these victims and relays a transaction between them to produce trust that they are doing transactions directly with each other over a private network, when in fact the entire transaction is controlled by the malicious people as shown in Figure 8.4. These intruders intercept all relevant transactions passing between these victims and throw in either a new malicious one or alter the aforementioned transactions.

8.3.2 Bit-Flipping Attacks

Such types of attack are based on the substitution/replacement principle [13]. In a bit-flipping attack, a single bit of the transaction amount is modified which produces a significant error.

8.3.3 Sequence Attacks

Such attacks are also based on the substitution/replacement principle. In sequence attack, N-bits in the transaction can either be modified, inserted or deleted by an attacker. An intelligent adversary would be able to manipulate in such a way that most of the process proceeds normally.

8.3.4 Complete Substitution Attacks

Such attacks are also based on the substitution/replacement principle. A complete substitution attack is an attack in which the proposed transaction is completely replaced with an alternate one for a significant fault. This is the most extreme attack into transaction field.

8.3.5 Information Leakage

Attackers may disclose unauthorized the privileged information of different transaction involved in blockchain. Such examples of privileged information include client data, secret password, proprietary protocol, etc.

8.3.6 Attacks on Control Software

An unscrupulous coder can modify the error-recovery software in order to bypass the error-recovery mechanism. This is possible for both custom and general-purpose design flows of transactions.

8.3.7 Modification of Functionality

Attackers could maliciously force an unintended operation to execute. For instance, an attacker could subtly downgrade the performance and reliability of the functionality of blockchain, thereby depressing the end user's assurance and confidence in the blockchain system.

8.3.8 Piracy Attacks

There are protocols for different transaction applications. These are known as Intellectual Property (IP) of blockchains. Attackers can violate these IPs, for example, make a duplicate of the previous transactions and repeat the same again and again. Piracy of a transaction is an important unique factor of proprietary blockchains which security aspects require much efforts for which billions of dollars will be acquired. However, their piracy is not guaranteed to be well protected. Hence, traditional blockchains are vulnerable under IP thief threat as the attacker can easily pirate test protocols of transactions.

8.3.9 Brute-Force Attacks on the Blockchain

Attackers could try to their best to crack the confidential password of a transaction by applying all combinations of digits, letters, and special characters. This is known as a brute-force attack. Greater security guarantee is achieved by hardening resistance to brute-force attacks with high confusion and diffusion.

8.3.10 Reverse Engineering

Reverse engineering (RE) is the technique of analyzing a system to identify its components and their internal structures, interconnections, etc., and produce the representation of the system in another form or a higher level of abstraction [14]. RE is rigorously applied to disassemble a device in different ways such as cloning, duplicating, and reproduction. In this subsection, the RE of blockchain systems is acquired by extracting their internal physical structures and information using destructive techniques for secret information detection by foreign attackers.

8.3.11 Counterfeiting

A counterfeiting transaction is one which is a repeat of an already done transaction. Therefore counterfeit is a threat to blockchain like other attacks.

8.3.12 Hardware Trojans

A hardware Trojan (HT) is able to modify the circuit system of transaction or insert a malicious circuitry into the design to disable/destroy the whole system for a specific input/time. This HT is able to modify the designed circuit during either fabrication or design and cause unwanted behavior. These are also designed to disclose

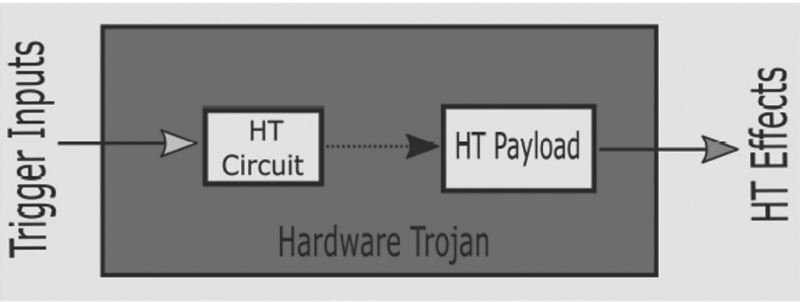

FIGURE 8.5 A typical structure of hardware Trojan.

the transaction secret information, Denial of Service, and alter system functionality. Attackers can insert HTs at any level from high-level system design specification to the transistor level of IC design flow [15].

A typical structure of HTs that could be inserted into a blockchain is shown in Figure 8.5. Some key terms related to HTs are with their meanings:

- Trigger: an event which initiates the HT. When this particular event starts, the HT circuit is automatic activated for deadly functionality.
- Payload: an event that activates the Trojan, responsible for implementing HT attacks, which could result in serious effects such as information leakage, denial of service (DoS), and blockchain reliability degradation.

Hardware Trojans can be inserted into blockchain as per the following categories:

- **Insertion phase**: Blockchain HTs can be inserted in any of the following phases:
- Specification: Blockchain HTs can maliciously alter the specification, for example, US Dollar (USD) to Euro (EUR) during runtime to make the transaction incorrect.
- Design: The blockchain designer can alter the transaction to alter the outcome.
- Fabrication: A hardware Trojan can be maliciously inserted during chip fabrication by tampering in the chip factory.
- Assembly: During the assembly of blocks, a malevolent integration engineer enacts the collection of blocks wrongly to produce erroneous output.
- Calibration and testing: A malicious tester can also insert an HT maliciously during the testing and calibration phase to overcome the blockchain concept.
- In-field: In the blockchain field, attackers falsify the transaction protocol by altering their agreement.
- **Abstraction level:** Hardware Trojans are able to insert at the following phases of abstraction level:
- System level: At system level, elements of individual domain and their interconnections are mentioned by the system engineer. Blockchain can be modified to result in erroneous output.

- Physical level: Each physical components of the blockchain, i.e., hardware components and wiring, chip platform and their locations and dimensions are defined at physical level. Hardware Trojans can be inserted by altering any of the aforementioned physical components and/or their dimensions.
- **Activation mechanism:** This describes the internal and external triggering mechanism of hardware Trojans.
  - Internal trigger: This trigger is executed for a particular instance of time slot.
  - External trigger: This type of trigger is executed externally due to output of a specific transaction.
- **Effect:** The effect of HTs is to alter ledger functionality, disclose secret transaction information, degrade performance, cause DoS attacks, and so on.

8.3.13 Double Spending

One of the major issue of a cryptocurrency developer is the problem of double spending. As per the name, this refers to when a person spends a coin multiple times, which creates an inconsistency between the spending ledger and the amount of available cryptocurrency. This happens when a blockchain network is tampered with and cryptocurrencies are stolen. The malicious node would send a copy of the transaction to make it looks legitimate, or might delete the transaction entirely as shown in Figure 8.6.

In a bitcoin network, there is a probability that a buyer can make a copy of the digital currency and send it to multiple retailers while keeping the original one. The most typical technique of double spending is when a blockchain hacker sends multiple transactions to the network and reverses the transactions, appearing as if those transactions never occurred. (www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp).

This double-spending problem could be avoided in the bitcoin network or other blockchain-based cryptocurrencies by implementing a Proof-of-Work (PoW)

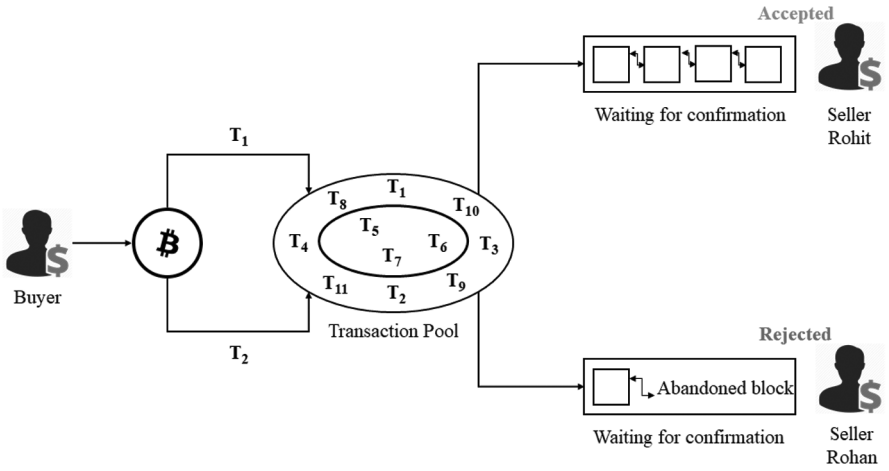

FIGURE 8.6 Double Spending.

consensus algorithm. This PoW is executed by miners who not only ensure the fidelity of past transactions on the blockchain's ledger but also detect and avoid double spending.

8.3.14 51% Attack

In a blockchain network, a 51% attack is a probable attack that can happen when an organization governs the mining power or so-called hash rate with a majority ratio. A bitcoin network is made secure by making all miners give consent on a shared ledger, i.e. blockchain. Every node in bitcoin ensures that these are working on a valid transaction at any point of time by looking at each other. Miners would have the potential to determine which transaction to give consent to given that the majority of miners are handled by a single entity. Hence this will give power to the miner to block other transactions and allow their own coins to be spent multiple times. This is also known as double spending as shown in Figure 8.7 [16, 17] (ref: https:// learncryptography.com/ cryptocurrency/ 51- attack).

With this attack an attacker can perform the activities mentioned below:

- They can reverse his transactions that have already happened.
- They can block transactions from gaining any confirmations.
- They can block other miners to mine any other valid blocks.

However, an attacker cannot perform the activities below:

- They cannot reverse the transactions of others.
- Block transactions to be sent at all.
- Modify the number of coins generated per block.
- Generate coins out of nowhere.
- Send coins that were never owned by them.
- These attacks are valid till the attacker is in control (i.e., owns 51%). The transactions which had been turned down can be added just after the attacker loses their majority [18].

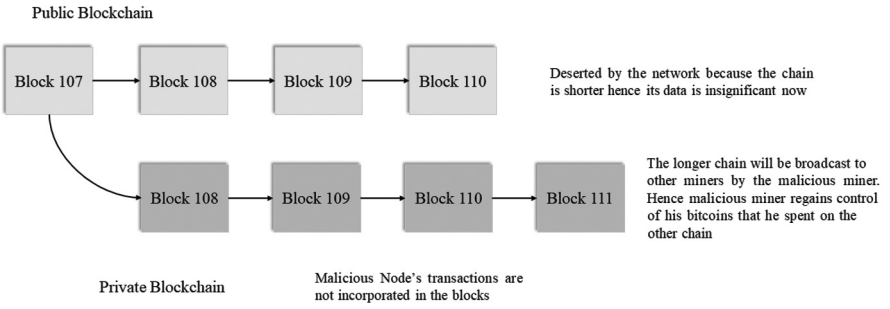

FIGURE 8.7 51% Attack Simplified.

If a blockchain network implements a Proof-of-Work (PoW) consensus mechanism, then it should have the proper security measures to avoid a 51% attack to be carried out. A few viable options are to be vigilant of mining pools, implementation of merged mining on a blockchain network with a higher hash rate, or utilizing a different consensus mechanism.

8.3.15 Race Attack

When a hacker sends two conflicting transactions in succession rapidly into the bitcoin network, this is known as race attack. This attack is comparatively easy to accomplish in blockchains which have utilized PoW as consensus algorithm. The dealer who receives payment instantly with "0/unconfirmed" status is vulnerable to reversal of transaction. An attacker performs a transaction by sending coins to the dealer directly, however, he will not wait for confirmation from the dealer and instantly sends a conflicting transaction (with the same coin used before for the dealer) to himself to the rest of the blockchain network. It is more likely that the conflicting transaction which happened later will be mined into a block and accepted by bitcoin nodes as valid node.

8.3.16 Finney Attack

An attacker first finds a dealer who accepts unconfirmed transactions. Then he performs a transaction to himself with the same amount to be sent to the dealer and find the block; however, he does not broadcast the block. Once the above step is completed the attacker will send the same amount to the dealer and wait till the item gets delivered. Finally, he broadcasts his previous block with the original transaction in it. This block will include the transaction that sent the coins to himself, hence the unconfirmed payment to the dealer will be invalidated. Moreover, the attacker will regain his coins and also the item for free.

8.3.17 Vector76 Attack

Vector76 attack otherwise known as one-confirmation attack. This attack is an amalgamation of the race attack and the Finney attack such that a transaction that even has one confirmation is still reversible. It is one of the variations of the double-spending attack. The attacker performs double spending by using the privately mined block during exchange. The wallet service such as exchange of cryptocurrency is vulnerable to this attack because of the acceptance of direct connections. If the Vector76 attack is successful then the attacker has to sacrifice one block because by not broadcasting it and only by broadcasting the attacked node.

8.3.18 Alternative History Attack

This attack occurs when an attacker initiates a transaction by sending coins to the dealer. Concurrently, the attacker will mine an alternative block privately which includes a conflicting double-spending transaction. The dealer will deliver the item to

the attacker after waiting for *m* confirmations. Right away, if the attacker finds more than *m* blocks untie his chain and gets his coins back again; If not, he keeps trying to continue extending his chain of blocks with the hope of being able to catch up with the network. When the attacker is not ever able to extend his private blockchain compared to the public blockchain, then the attack fails.

8.3.19 Selfish Mining Attack

A selfish mining attack happens when an attacker (selfish miner in this case), does not broadcast a valid solution to the rest of the network. Rather than act like a regular miner and publish blocks to the network instantly after finding them, the attacker selectively releases blocks, or publishes many blocks all at once thus forcing the rest of the network to discard their blocks and lose revenue. The primary motives of selfish mining are to obtain an unfair reward which is bigger than their share of computer power spent, and confuse other honest miners and lead them to waste their resources in the wrong direction as shown in the Figure 8.8.

8.3.20 System Hacking

It is relatively hard to hack and tamper the records stored in a blockchain; however, the programming codes and systems that implement its technology can be vulnerable. The largest Tokyo-based bitcoin exchange, i.e., MtGox, was hacked in March 2014, and bitcoins worth $700 million were stolen. The reason behind this attack was ill-maintained and outdated codes which allowed hackers to perform double-spend. More recently, a DAO (Decentralized Autonomous Organization) that holds large quantities of Ethereum was exploited through a software vulnerability and the hacker stole $50 million worth of Ethereum [19].

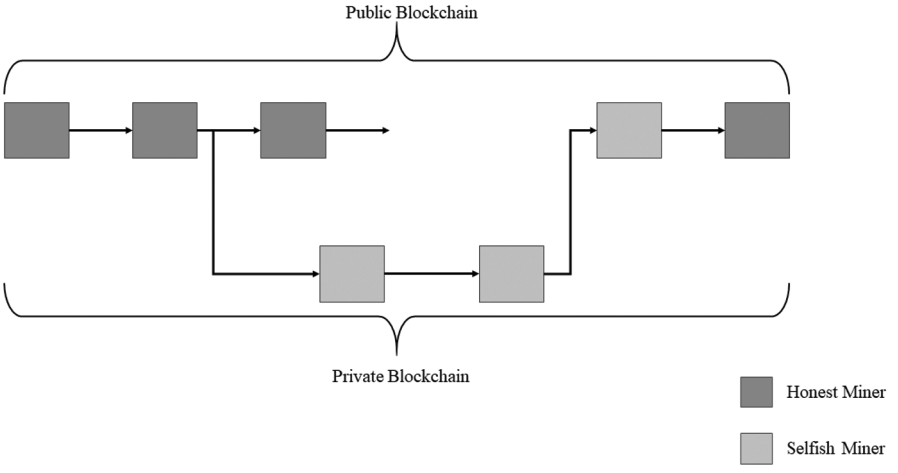

FIGURE 8.8 Selfish Mining Attack Simplified.

8.3.21 Illegal Activities

An illicit group of people can utilize the blockchain network or platform to perform various illegal activities. For instance, the Silk Road website was an online marketplace for illegal drug where sellers and buyers whose identities are anonymous did business using bitcoin (Hong 2015). Cryptocurrency that uses blockchain technology may also facilitate money laundering. Although bitcoin is not yet treated as a fiat currency, it makes it possible to create an "underground" channel for illegal movement of funds within its network.

8.3.22 Identity Theft

Although Blockchains preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is acquired or stolen, no third party can recover it. Consequently, all the assets this person owns in the blockchain will vanish, and it will be nearly impossible to identify the thief. The consequences may be more devastating than identity theft in the offline world, where third-party institutions (e.g., credit card companies) or central authorities safeguard transactions, control risks, detect suspicious activities, or help find culprits. Also, current cryptography standards are not completely uncrackable (Swan 2015). With the advent of quantum computing, it is not impossible for cryptographic keys to be cracked quickly, demolishing the foundation of blockchain technology (Crosby *et al.* 2016).

8.4 POTENTIAL DEFENSES AGAINST SECURITY THREATS ON BLOCKCHAIN

Potential defenses which assure security against man-in-the-middle-attacks, hardware Trojans, etc., include the following schemes:

- **Watermarking:** Someone requests a transaction directly known as client or via something called a wallet. The transaction directly request from the client will deliver either a commit or by a process at the server where the transaction initiated known as the master. In watermarking, the original client's digital signature is provided with the request. Watermarks are able to assure ownership as these are much more difficult to identify and modify. Unfortunately, the watermarking technique is not able to guarantee security against hardware Trojans.
- **Metering:** In this technique, both the public signature of wallet/master and the client's digital signature are added to the transaction request as processing constraints. This metering scheme is not also able to assure protection against hardware Trojans as the attacker is able to create and hide a malicious Trojan in the circuit due to availability of the design functionality.
- **Side-channel fingerprinting:** This scheme is able to detect hardware Trojans easily as the manufactured parametric characteristics, such as power, area, delay, and block characteristics of the transaction are compared with those of

statistical model. Any significant variation/deviation would be considered to be a Trojan. Side-channel fingerprinting is not able to assure authenticity or piracy, counterfeiting, or reverse-engineering attacks.

- **Reverse Engineering (RE):** This technique can also be constructively utilized to detect hardware Trojans. For RE, the state-of-the-art of blockchain should be made aware by the researcher to become successful in the detection of HTs inserted by foreign attackers. A typical RE flow should pass through de-packaging, delayering, and image processing of a blockchain.

  Mainly, its design and blocks are uncovered by RE scheme following the aforementioned steps is studied with a golden one (this means with no attack).

  This RE approach is both time-consuming and also destructive in nature. Hence, the RE technique is less applicable for HTs detection [20]. RE is generally used to assure about the Trojan-free blockchain used in the golden blockchain model development required for test time and runtime golden blockchain models.
- **Code analysis:** The code of blockchain functionality is analyzed to detect for any hardware Trojans inserted into the system. Also, any secured encryption algorithm and hash functions can be used for the confidentiality of transaction and hence protect from Trojan attacks on blocks. Code analysis is not able to protect the blockchain against piracy, reverse engineering, and counterfeiting attacks.
- **Obfuscation:** A code-obfuscation technique can be used by the blockchain designer for the mystification of transactions. This obfuscation is able to prevent hardware Trojan attacks indirectly as attackers would not be able to insert meaningful and stealthy hardware Trojans in such an obfuscated transaction sequences. Obfuscation is able to prevent hardware Trojans and reverse engineering, but not piracy or counterfeiting.
- **Locking:** A blockchain designer is able to add locks (i.e., digital multiplexers) which manage and control the flow of transactions among blocks or other blockchain components. These transactions will proceed further in a correct manner if and only if the correct secret key is applied, otherwise wrong

TABLE 8.1
Summary of potential defenses

Name of Defense	Name of Attack			
	Trojans	Piracy	Reverse Engineering	Counterfeiting
Watermarking	No	No*	Yes	No*
Metering	No	No*	Yes	No*
Side-channel Fingerprinting	No*	No	No	No
Reverse Engineering	Yes	No	---	No
Code Analysis	No*	No	No	No
Obfuscation	Yes	No	Yes	No
Locking	Yes*	Yes	Yes	Yes

transactions will proceed which results in an erroneous output. This key should be preserved in a tamper-proof memory in order to protect from vulnerabilities as the key is erased during reverse-engineering duration. Hardware Trojans are not able to be inserted since the blockchain functionality is hidden by the key. Locking prevents all aforementioned attacks: piracy, reverse engineering, and counterfeiting attacks, Trojans after fabrication, except for Trojans inserted during chip fabrication of the blockchain in industry.

8.5 COMPARISONS AND RESULTS ANALYSIS

In this section, all the potential defenses are summarized in Table 8.1 along with the statistics of comparisons among them. From the aforementioned Table, it is confirmed that the locking defense provides the best assurance for security issues in blockchain, followed by the obfuscation defense.

Depending on their business strategy and budget, companies and industry firms can choose any one or multiple aforementioned techniques to protect the blockchain against different known and existing attacks.

Symbols used in Table 8.1 meanings:

- Yes means both detection and prevention possible.
- Yes* means detect and prevent those Trojans inserted only after fabrication, but not those before fabrication.
- No means cannot detect, also not prevent.
- No* means only detection, but not prevention.

8.5.1 Discussion about Critical Infrastructures for Securing Blockchain

Because all the aforementioned techniques have their own pros and cons, one proposed direction is to use each for the highest HT coverage. For example, an RE-based scheme can guarantee a golden blockchain required for test time and run-time golden blockchain models. Side-channel and functional testing approaches are able to detect large and small HTs respectively that were inserted during chip fabrication. Runtime approaches can finally conclude to work as a last scheme of defense.

8.6 CONCLUSIONS

Though blockchain technology was designed to act as a backbone for crypto currency bitcoin from the beginning, blockchain is applied in other fields such as clinical diagnostic healthcare, government organizations, Intelligent Transportation System, etc., due to its open and decentralized framework, secure environment and tamper-proof characteristics. Though blockchain is a complex technology, it has had proved the potential to handle all record keeping processes, audit and assurance in the means transactions are initiated, processed, authenticated, recorded and reported at the time of demand with providing secured, trust and integrity. While blockchain technology

cannot achieve its goal of other demanding features such as scalability, privacy and confidentiality. Hence it needs the attention of researchers as active areas of research and development due to the fact that these features are less matured. In the last few years, a number of cryptocurrencies, consensus protocols, and hashing functions have been developed in the networks. A few examples of the cryptocurrencies are NXT, Ripple, NEO, Cardano, Stellar, EOS, Litecoin, IOTA, Dash, Lisk, Zcash, Dogecoin, and many more. Finally, we hope that blockchain has the power to shape the 21st century.

Over the next decade, researchers will try a number of blockchain concepts and ideas, out of which some will succeed. But in the process some real-world problems will be solved and new businesses along with business models will emerge for the use of blockchain in better real-life state-of-the-art applications.

REFERENCES

1. D. Vujicic, D. Jagodic, and S. Randic, (2018) Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview, March 2018, in 17th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1–6.
2. F. Tschorsch and B. Scheuermann, (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123.
3. S. Nakamoto, (2008) Bitcoin: a peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.
4. A. Castor, A short guide to Bitcoin forks, March 2017. Available at: www.coindesk.com/short-guide-bitcoin-forks-explained/.
5. T. Lee, (2013) Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%, Arstechnica.
6. V. Buterin, (2013) Ethereum white paper: a next generation smart contract & decentralized application platform, Available at: www.theblockchain.com/docs/Ethereum_white_paper_a_next_generation_smart_contract_and_decentralized application platform-vitalik-buterin.pdf
7. F. Coppola, (2016) A Painful Lesson For The Ethereum Community, Forbes.
8. C. M. Gillespie, (2016) Official NXT Decision: No Blockchain Rollback, Cryptocoin News.
9. A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, (2017) Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832–1843.
10. M. A. Khan and K. Salah, (2018) IoT security: Review, Blockchain solutions, and open challenges, Future Generation Computer Systems, vol. 82, pp. 395–411.
11. S. Wang, Y. Zhang, and Y. Zhang, (2018) A Blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access, vol. 6, pp. 38437–38450.
12. M. Conti, N. Dragoni, V. Lesyk, (2016) A survey of man in the middle attacks, IEEE Communications Surveys Tutorials 18 (3), 2027–2051.
13. J. Tang, M. Ibrahim, K. Chakrabarty, R. Karri, (2018) Secure Randomized Checkpointing for Digital Microfluidic Biochips, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 6, pp. 1119–1132.
14. N. Jacob, D. Merli, J. Heyszl, and G. Sigl. (2014) Hardware Trojans: current challenges and approaches. IET Computers Digital Techniques, vol. 8, no. 6, pp. 264–273.

15. G. Maxwell, (2013) Coinjoin: Bitcoin privacy for the real world. Available at: https://bitcointalk.org/index.php?topic=279249.0.2013.
16. Baliga, Arati (2017) "Understanding blockchain consensus models." Persistent.
17. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In 2016 IEEE international conference on consumer electronics (ICCE) (pp. 467–468). IEEE.
18. Bastiaan, M. (2015, January). Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. Available at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin. pdf.
19. Xu, Jennifer J. (2016) "Are blockchains immune to all malicious attacks?" Financial Innovation 2.1 (2016): 25.
20. S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, (2016) A survey on chip to system reverse engineering, J. Emerg. Technol. Comput. Syst., vol. 13, pp. 6:1–6:34.
21. Bruice Schneier, Applied Cryptography, Wiley Press, Second Edition.
22. Douglas R. Stinson, Cryptography Theory and Practice, CRC Press, Second Edition.
23. Cryptocurrency Market Capitalizations, Available at: https://coinmarketcap.com/
24. A. Ali, M. M. Afzal, (2018) Confidentiality in Blockchain, International Journal of Engineering
25. Science Invention (IJESI), vol. 7, no. 1, pp. 50–52.
26. D. Shrier, W. Wu, A. Pentland, (2016) Blockchain & Infrastructure (Identity, Data Security), Available at: www.getsmarter.com/career-advice/wp-content/ uploads/2017/07/mit blockchain and infrastructure report.pdf.
27. C. Bao, D. Forte, and A. Srivastava, (2014) On application of one-class SVM to reverse engineering-based hardware trojan detection, in ISQED, IEEE, pp. 47–54.
28. R. Guo, H. Shi, Q. Zhao, and D. Zheng, (2018) Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems, IEEE Access, vol. 776, no. 99, pp. 1–12.
29. Blockchain has the power to shape 21st century. Available at: https://economictimes.indiatimes.com/markets/stocks/news/blockchainhas-the-power-to-shape-21st-century/articleshow/ 65680293.cms
30. Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, (2019) Blockchain Technologies for the Internet of Things: Research Issues and Challenges, IEEE Internet of Things Journal, in Press.
31. Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz, (2018) Cyber Security of Critical Infrastructures, ICT Express (Elsevier), volume no. 4, issue no. 1, pp. 42–45.
32. Leandros Maglaras, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, Stylianos Rallis, (2018) Threats, Protection and Attribution of Cyber Attacks on National Critical Infrastructures, EAI Transactions on Security and Safety, volume no. 5, issue no. 16, pp. 1–9.
33. D. Gountia (2019) Towards Scalability Trade-off and Security Issues in State-of-the-art Blockchain, EAI Endorsed Transactions on Emerging Topics in Security and Safety, vol. 5, issue no.18, pp. 1–9.