# Analyzing the Attacks on Blockchain Technologies

**Vinay Kumar Vats and Rahul Katarya**

**Abstract** Blockchain technology has gained significant interest because of a wide variety of possible uses. It was first developed as a Bitcoin cryptocurrency but has since been used in many other business and non-business applications. There are various innovations available from Bitcoin to financial innovations, risk management, IoT, and public and social services. The blockchain infrastructure, instead of most current systems based on center-based architectures, combines peer-to-peer networks and distributed platforms that use blockchain registers to store transactions. But, like the Internet in 1990, the blockchain is regarded as still growing. In the future, it can alter so many aspects of technology. However, there are many setbacks, mainly due to the defense area, as a new undeveloped sector. So, it becomes important to analyze their success in multiple use cases and scenarios as more and more diverse blockchain technologies have appeared. We address the security concerns of blockchain technology in this survey. In this paper, with a focus on shared blockchains, we systematically analyze the attack surface of blockchain technologies.

**Keywords** Blockchain · Vulnerability · Smart contract · Consensus algorithms · Ethereum · Hyperledger

## 1 Introduction

Since Bitcoin's debut in 2009, its fundamental methodology, blockchain, has demonstrated exciting implementations and drawn much academic and industrial knowledge. The blockchain is Bitcoin's central system. In 2008 and 2009, blockchain was first suggested by Satoshi Nakamoto [1]. In 2015 [2] and the most powerful asset in 2016 [3], Bitcoin was ranked as the first crypto-currency and checked in May 2017 more than 300 k transactions [4] per day. The theoretical framework of blockchain's crypto-monetary technology has been investigated in previous studies

V. K. Vats (✉) · R. Katarya
Department of Computer Science & Engineering, Delhi Technological University, Shahbad Daulatpur, Delhi 110042, India

A. Tomar et al. (eds.), *Machine Learning, Advances in Computing, Renewable Energy and Communication*, Lecture Notes in Electrical Engineering 768,
https://doi.org/10.1007/978-981-16-2354-7_35

[5]. While some studies focused on blockchain's security concerns, because of rising demands for crypto-monetary and security issues, they did not concentrate on the cyber vulnerability of blockchain. The study in [6] focused on the basic sense of Bitcoin's crypto-currency, its use, and functions, and its aspects of privacy are one of these studies. Smart contracts in Ethereum [7], with general programming glitches and bugs associated with taxonomy blockchain vulnerabilities. Many blockchains are designed to increase their efficiency by improving the setup of the protocol and the creation of new consensus algorithms, for example, the performance benefits/drawbacks of the new update in comparison with the Hyperledger Fabric versions such as HLF v0.6 and HLFR v1.0 are in the same sense of calculation [8]. Besides, bottlenecks can be defined and used through performance measurement and analysis to facilitate further improvement ideas. Therefore, in the field of blockchain science, performance assessment plays an important role.

Blockchain technology is a decentralized technology for data and transaction management that offers data security, privacy, and accountability without a third-party entity. The technology can be interpreted as a shared directory of all transactions in a blockchain. This chain is constantly extended by the addition of new blocks. Blocks are arranged according to a sequence, of which the stack base is the bottom element. The previous block of the chain is connected to each block. Any block is defined by a hash created by cryptographic hash algorithms. A block contains a header forming a chain that links it to its parent blocks, consisting of a certain hatch of its parent blocks. The first block is known as a genesis block.

Blockchain technology also incorporates the technique of Hashing for security. There are some properties in cryptographic hashes that are very helpful in blockchain operations. The property's hiding property should be well built to be crash-proof and help to make puzzles easier. The hiding property can be difficult to find when a hash output is given. It is hard to find two plaintext items producing the same Hash performance because of the collision resistance function.

While there are some recent studies on blockchain performance, none of them conducts a comprehensive review of the threats to blockchain systems, the related actual attacks, and the security improvements. Some of the recent studies related to attacks and blockchain applications are also available in [9–13]. Based on these factors, our research provides a thorough analysis of security vulnerabilities in blockchain technologies by exploring attack vectors that concentrate on user security and their vulnerabilities. We also analyze the types of attacks that pose both realistic and theoretical threats to blockchain technology at different levels. The rest of the paper is organized in the following order:

I. Section 2 presents the structure and some key features of blockchain technology.
II. In Section 4 different blockchain generations and there, vulnerabilities towards the attacks are discussed.
III. In Section 5 risks related to blockchain technology are classified and discussed.

## 2 Structure and Overview of Blockchain Technology

The key technologies used in blockchain are presented in this section.

### 2.1 *Consensus*

At the heart of a blockchain system is a consensus protocol. The regulations are established and all nodes can be used to agree on blockchain content, for instance. Two primary modes of consensus [14] are usually focused on facts and vote. The most popular proof of work (PoW), used by many blockchain systems, is consensus-based on evidence. PoW is a very computer-based consensus. The nodes will solve an appalling puzzle to fight for the right to record. The first node (called the winner) was the only way to solve the jigsaw. In comparison to PoW, voting solutions produce a deterministic outcome and produce relatively high output in general. For each block order to achieve agreement, they depend on normal message transitions between different functions on a network. Two members of this consensus type are the Raft and Byzantine Fault Tolerance algorithms (e.g. pBFT and BFT-SMaRt). Raft tolerates the crash defects only, while the byzantine erroneous defects are fixed by pBFT and BFT-SMaRt.

### 2.2 *Block Structure*

The blockchain is a block series, including traditional public records, with an exhaustive list of transaction records. Any block points to a link called the parent block, which is mostly a previous block hash value. A block is a header and the block body. In specific Block editions, Parent Block Hash and Merkle Tree Root have block header, timestamp, and nuncio. The block body creates a counter and a transaction. The maximum number of transactions per block depends on each transaction's package size and size (Fig. 1).

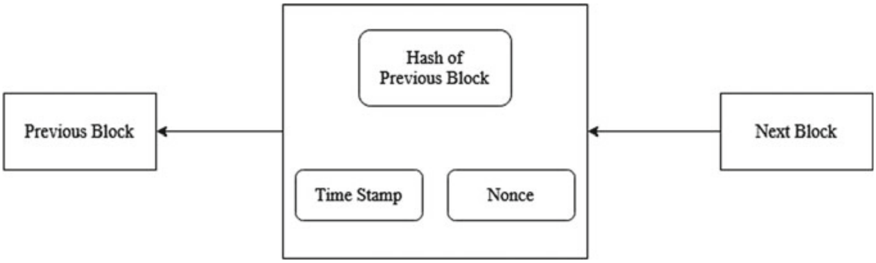

**Fig. 1** Block structure of blockchain

### 2.3 Key Cryptography

Every entity owns two basic keys, one is a private key for its encryption and the other for verification used by other users. For signing transactions, a private key is used. Digital transactions signed are distributed across the network and can only be accessed through public keys to any network user. The first step is to establish the hash value derived from the contract when a user wants to enter into a contract. Then he uses his private key to encrypt this hash value and sends the encrypted hash to another user with original information. Another user tracks the transaction obtained by matching the decrypted hash with the hash extracted from the information received (Fig. 2).

## 3 Blockchain Generations

Relating blockchain technology operations are structured and accessible as follows: (a) public blockchain in the first generation, (1.0), (b) public blockchain in the second generation, (2.0), and (c) blockchain in the third generation. In this section, we will classify the security threats faced by different blockchain generations [15] (Fig. 3).

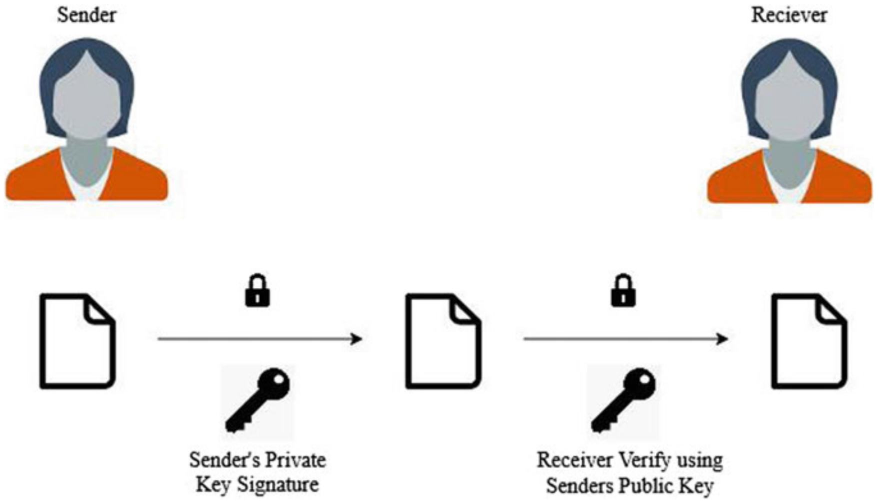

**Fig. 2** Illustration of key cryptography

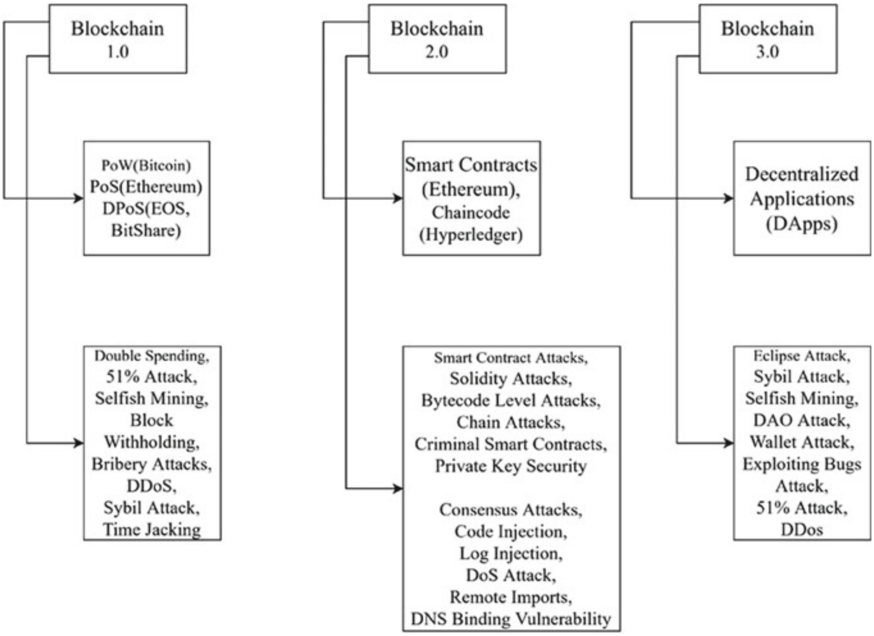
Blockchain 1.0
PoW(Bitcoin)
PoS(Ethereum)
DPoS(EOS, BitShare)
Double Spending, 51% Attack, Selfish Mining, Block Withholding, Bribery Attacks, DDoS, Sybil Attack, Time Jacking
Blockchain 2.0
Smart Contracts (Ethereum), Chaincode (Hyperledger)
Smart Contract Attacks, Solidity Attacks, Bytecode Level Attacks, Chain Attacks, Criminal Smart Contracts, Private Key Security
Consensus Attacks, Code Injection, Log Injection, DoS Attack, Remote Imports, DNS Binding Vulnerability
Blockchain 3.0
Decentralized Applications (DApps)
Eclipse Attack, Sybil Attack, Selfish Mining, DAO Attack, Wallet Attack, Exploiting Bugs Attack, 51% Attack, DDos

**Fig. 3** Generation wise attack vulnerability of blockchain system

## 3.1 First Generation of Blockchain System

Blockchain 1.0 was the first blockchain technology implementation in 2009 and is thus v1.0.0. Cryptocurrency is an exchange medium that, using encryption techniques for monitoring money generation, is manufactured and stored electronically in the blockchain and allows for verifying the transfer of money. When blockchain and cryptocurrency technology first came to the market, one of the key roles was to eliminate third-party interaction in all forms of currency movement.

## 3.2 Second Generation of Blockchain System

In effect, Blockchain 2.0 is a system that enables programmable transactions (a condition-modified transaction or collection of conditions) introduced in the year 2010, that is when Ethereum [16], a platform where the developer community can create distributed blockchain network applications, also known as “smart contracts”, was born. These are an autonomous computer program that is automatically executed and conditions specified in advance, such as facilitating, checking, or implementing the execution of a contract.

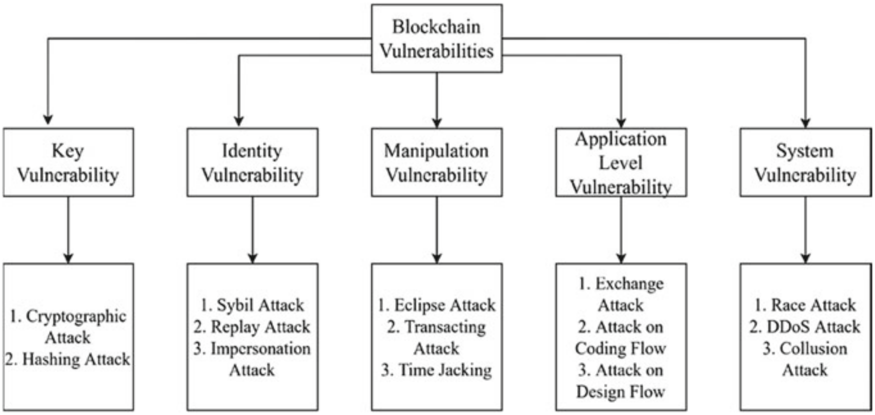

**Fig. 4** Classification of blockchain attacks

### 3.3 *Third Generation of Blockchain System*

Blockchain 3.0 is a summary of attempts in blockchain industries to solve current problems, particularly scalability, interoperability, and privacy problems. Here is a new concept for Decentralized Apps (DApp). Decentralized storage and decentralized network are used because most DApps operate a blockchain, decentralized peer-to-peer network with their backend code. However, a DApp can host its portfolio in decentralized storages like Ethereum, Swarm [17], and Hyperledger [18] (Fig. .4).

## 4 Risks and Vulnerability

### 4.1 *Key Vulnerability*

In most blockchain processes, cryptographic hashes are used to protect chain integrity and transactional property [19]. The most common algorithms for blockchain implementations are digital signature (DSA) algorithms based on asymmetric key encryption and cryptographic hacking.

### 4.1.1 Cryptographic Attacks

A cryptographic attack is a method of discovering a loophole in a document, cipher, cryptographic protocol, or key management system to bypass the security of a cryptographic system. The attacker's objective in cryptography is to crack the confidentiality of encryption and to learn the hidden message and the secret key.

### 4.1.2 Hashing Attacks

There occurs a condition when the attacker attacks the hashing algorithms used by the blockchain system. A pass-the-hash attack (PtH) was a technique used by an attacker to collect the hash key, which it transmits to other networked systems for authentication and possibly lateral access, as opposed to key functionality. To obtain a plain password, the threat actor needs to decode the hash.

## *4.2 Identity Vulnerability*

When stored over a blockchain, information is cryptographically encrypted and cannot be changed or erased, rendering large breaches of information extremely difficult, if not technically impossible. With the digital identities of users cryptographically stored directly on a blockchain inside an internet browser, technically, users will no longer need to provide any third party with sensitive data. Some of the attacks are listed below.

### 4.2.1 Sybil Attack

These types of attacks are common and are used by a single rogue group to recognize and monitor multiple false identities. To isolate the target node from the rest of an honest network in the blockchain network, this method of attack is used.

### 4.2.2 Replay Attack

This kind of attack spooks the attacker and gives the two legitimate parties access to correspondence. Stealing and reuse the hash key make the attacker a legitimate user to block the ecosystems.

#### 4.2.3 Assault Impersonation

The impersonation of a legit consumer is commonly used to get entry. An ECDSA algorithm can also be extended to some other approaches suggested for using a distributed incentive-based approach. In comparison, BSeiN [20] used the users to validate an attribute-based signature.

### *4.3 Manipulation Vulnerability*

If the rest of the network can partition one or more nodes in the blockchain system, different routing attacks may occur for malicious purposes. The use of such attacks, DoS attacks, and large portions of network mining resources can be postponed for a significant period, and other attacks can be carried out. The three major forms of attacks are eclipse, time jack, and transaction malleability-based assault.

#### 4.3.1 Eclipse Attack

The eclipse attacks [15] constitute a kind of attack and the assailant tries to isolate a target by monopolizing all incoming and incoming links. This lets the attacker damage the blockchain's goal vision, waste his computing energy, or weaken the target's computer power for malicious purposes.

#### 4.3.2 Transactional Attacks

The malleability of transactions faults the design of Bitcoin, which may change transactions before being added to a block after generation. It is not possible to change the source/government addresses or transaction numbers, but another component of the transaction can be modified.

#### 4.3.3 Time Jacking

The Time Jack is an attempt by communicating with several people to skew the time signature for the target node and reporting the time to the target. To validate fresh blocks, the node network time is used. When a network time view from a node is skewed, a timestamp greater than a given time frame is rejected for new blocks. It makes it easy to isolate a target node from the rest of the network. Betrayed transactions can be created and transferred to the target by isolating a target node.

## *4.4 Application-Level Vulnerability*

Utilities that operate on or connect with the blockchain are by far the poorest link to blockchain protection. While the underlying blockchain protocol is robust, monetary loss and the people affected, of course, have all been the target of a variety of attacks that have fallen prey to trade, wallet, and decentralized apps (DApps).

### 4.4.1 Design Flow Attacks

The Ethereum blockchain is a strong framework for intelligent contracts and DApps to be built and run. A decentralized independent organization (DAO) is a clever contract-based system in which citizens can fund voting by proposals.

### 4.4.2 Code Flow Attack

Some wallet applications were also targeted because of code errors. By accident in November 2017, the 513,753 ether "kill" bug in Parity's wallet program, which at the time of this writing was worth some 355 million. This is possible because Parity has concluded every multi-signature agreement in a library.

### 4.4.3 Exchange Attack

The term exchange refers to the place where the transaction and exchange of currencies take place for keeping the wealth moving. So, sometimes the attackers directly try to attack the exchange where payments and transactions, and parties take place. This happens because most exchanges are relatively small enterprises with less money to invest in cybersecurity and are (or were) start-up companies.

## *4.5 System Vulnerability*

Blockchain technology systems are based on a data structure that is only connected to network storage and transaction. The system-based attacks attack the network architecture and physical hardware, servers, and access terminals of the working network. The attacker tries to overload the whole connected terminals with service requests and this overflow of requests degrades the system performance and ultimately the attacker tries to crash or manipulate the network.

### 4.5.1 Race Attack

The race attack enables the attacker to produce two transactions, one real and one false. The purpose is to allow any node accepting 0 unconfirmed status transactions that show that the transaction is not yet visible in a block. As a network peer, the attacker links the target directly.

### 4.5.2 DDoS Attack

The term DDoS refers to Distributed Denial of Service. A hijacked computer in this type of attack is normally used by an attacker to overload a network with disproportionate requests to impede the network's ability to support the supply of high traffic [9].

### 4.5.3 Double Spending Attack

The attacker here tries to spend the same currency multiple times. After waiting for some trust, the assailant created and put him into a new fraudulent block and a fraudulent dispute settlement. The attacker then eliminates or leases a large part of the network's mining power.

### 4.5.4 Collusion Attack

The 51% attack is perhaps the most established attack due to its ability to fully subvert the blockchain. The mining force of more than 50% of the network is dominated by one entity or group in this form of attack (Tables 1 and 2).

**Table 1** Vulnerabilities and their precautionary measures

| Vulnerability | Flaws | Precautionary measures |
|---|---|---|
| Key | Vulnerable cryptographic algorithm | A strong and powerful cryptographic algorithm, password-protected secret sharing, hardware wallets |
| Identity | A weak network system | Stronger authentication |
| Manipulation | Network process | Network encryption |
| Application | Weak development process | Better design and development |
| System | Service speed vs. Time tradeoff | Trained user base |

**Table 2** Classification of attacks based on blockchain surface

| Blockchain surface | Attacks |
|---|---|
| Blockchain structure attack | Forks, orphans |
| Peer to peer system attacks | Eclipse attacks, selfish mining, DDoS attacks, DNS hijacks, BGP hijacks, time jacking, block withholding |
| Attacks over blockchain applications | Double spending, wallet theft, crypto-jacking, blockchain ingestion, overflow attacks, replay attacks |

## 5 Conclusion

The blockchain's decentralized platform and peer-to-peer design are highly regarded and endorsed. Through storing data across the network, blockchain has removed the threats that come with data centralization. The use of encryption technology in blockchain security systems improves defense. In this paper, we present a thorough investigation into the blockchain. First, we give an overview of blockchain architecture and main blockchain functionality. Then we discuss the different generations of blockchain development over the years of work and risks related to them. Also, many risks can complicate the implementation of a blockchain that is classified and compared in the survey.

For future work, we are planning toward an in-depth investigation and analysis of blockchain 2.0 and 3.0 generation-based applications including Smart contracts, Hyperledger, and some blockchain-based Decentralized Applications (DApps).

## References

1. Nakamoto S (2008) A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 12 August 2020
2. Desjardins J (2016) It's official: bitcoin was the top-performing currency of 2015. http://money.visualcapitalist.com/its-official-bitcoin-wasthe-top-performing-currency-of-2015/. Accessed 06 Aug 2020
3. Adinolfi J (2016) 2016's best-performing commodity is ... bitcoin? http://www.marketwatch.com/story/and-2016s-best-performing-commodity-isbitcoin-2016-12-22. Accessed 16 Aug 2020
4. Blockchain.info (2017) Confirmed transactions per day. https://blockchain.info/charts/n-transactions?timespan=all/
5. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun Surv Tutor 18:2084–2123
6. Conti M, Sandeep Kumar E, Lal C, Ruj S (2018) A survey on security and privacy issues of bitcoin. IEEE Commun Surv Tutor 20(4):3416–3452
7. Atzei N, Bartoletti M, and Cimoli T (2017) A survey of attacks on ethereum smart contracts (SoK). Lect Notes Comput Sci 164–186
8. Saad, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, Mohaisen D (2020) Exploring the attack surface of blockchain: a comprehensive survey. IEEE Commun Surv Tutor 22(3):1977–2008

9. Aggarwal S et al (2020) Meta heuristic and evolutionary computation: algorithms and applications. Springer Nature, Berlin, p 949. https://doi.org/10.1007/978-981-15-7571-6. ISBN 978-981-15-7571-6
10. Yadav AK et al (2020) Soft computing in condition monitoring and diagnostics of electrical and mechanical systems. Springer Nature, Berlin, p 496. https://doi.org/10.1007/978-981-15-1532-3. ISBN 978-981-15-1532-3
11. Gopal et al (2021) Digital transformation through advances in artificial intelligence and machine learning. J Intell Fuzzy Syst 1–8. https://doi.org/10.3233/JIFS-189787
12. Smriti S et al (2018) Special issue on intelligent tools and techniques for signals, machines and automation. J Intell Fuzzy Syst 35(5):4895–4899. https://doi.org/10.3233/JIFS-169773
13. Sood YR et al (2019) Applications of artificial intelligence techniques in engineering, vol 1. Springer Nature, London, p 643. https://doi.org/10.1007/978-981-13-1819-1. ISBN 978–981-13-1819-1
14. Zheng Z, Xie S, Dai H, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 14(4):352
15. Heilman E, Zohar A, Goldberg S (2015) Eclipse attacks on bitcoin's peer-to peer network. In: Proceedings of the USENIX conference on security symposium, pp 129–144
16. Gavin W (2014) Ethereum: a secure decentralised generalised transaction ledger. In: Proceedings of the ethereum project yellow paper. https://ethereum.github.io/yellowpaper/paper.pdf
17. Trón V, Fischer A, Nagy (2016) State channels on swap networks: claims and obligations on and off the blockchain (tentative title). Ethersphere orange papers, ethersphere, Tech. Rep.
18. Hyperledger Fabric. Available https://hyperledger-fabric.readthedocs.io. Accessed 06 July 2018
19. Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, Alazab M (2020) Blockchain for Industry 4.0: a comprehensive review. IEEE Access 8:79764–79800
20. Lin C, He D, Huang X, Choo KR, Vasilakos A (2018) BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J Netw Comput Appl 116:42–52