A Comprehensive Study of Security Aspects in Blockchain

Pranav Singh and Sushruta Mishra

Abstract Knowledge is power, and in this digital age, knowledge is represented by data, making it one of the most valuable assets. With rapidly evolving technology, there are challenges that directly or indirectly threaten the integrity of data, such as cybercrime, privacy concerns, theft, malware, and viruses. The development of Blockchain Technology has helped in the mitigation of some of these problems by safeguarding online data resources. In this chapter, we introduce the concept of blockchain, discuss its structure and features, and understand its operation. The main focus of this chapter is to observe the vulnerabilities of this technology and scrutinize several attacks exploiting them to understand their outcomes. We go over a few security improvements in an attempt to protect from attacks and alleviate the existing threats. In addition, we explore its application and implementation in various fields. We conclude by discussing the major challenges this technology is facing at present and may encounter in the future.

Keywords Blockchain technology · Vulnerabilities of blockchain · Attacks on blockchain · Applications · Future challenges

1 Introduction

Blockchain was established in 2008 by an unknown entity Satoshi Nakamoto as an underlying technology for Bitcoin, for the maintenance of records. Blockchain is defined as a distributed ledger that consists of an ordered series of blocks, generated by cryptography, and linked together sequentially. Every single block carries a hash of the preceding block, a timestamp, and transaction data (Merkle tree). It is an electronic ledger that is duplicated and synchronized across numerous nodes in the network. The underlying principle combines cryptography, peer-to-peer networking, and mathematical analysis of interactions (game theory).

P. Singh · S. Mishra (✉)
Kalinga Institute of Industrial Techonology, Bhubaneshwar, Odisha, India
e-mail: sushruta.mishrafcs@kiit.ac.in

H. K. Thakkar et al. (eds.), *Predictive Data Security using AI*, Studies in Computational Intelligence 1065, https://doi.org/10.1007/978-981-19-6290-5_1

Basically, data and information are stored, managed, and shared in this manner among parties and organizations. When one party creates and dispatches a set or block of information, it is verified by a myriad of nodes distributed across the network. After the block's verification, it is added to an immutable chain. Once any data is added, it becomes unalterable and can only be appended [1]. Modifying any single record would break the link with the adjacent block which would then require changing the entire chain composed of millions of blocks. That is somewhat impossible. Blockchain was initially used for Bitcoin and is currently the most admired representation of this technology. Blockchain has gained vast applicability in almost every industry including finance, health, supply chain management, the Internet of things, etc. With the commercialization of this technology, numerous Blockchain applications and platforms came into existence, like Bitcoin and Ethereum. Blockchain can be applied to a variety of fields far beyond bitcoin, which presently overshadows other blockchain categories. Data security and privacy, an emerging field of blockchain, is one such category that is receiving a lot of attention lately [2].

There are three types of blockchains [3]:

1. *Public blockchain*: These are permission-less and everybody can read, send, or receive transactions. Any participant can join in transactions and validate them through a consensus decision-making procedure before being added to the blockchain. They are considered to be fully decentralized blockchains. Bitcoin and Ethereum are public blockchains.
2. *Private blockchain*: These blockchains are restricted where write permissions are strictly confined to a single authority, who is responsible for granting read/write access to only a selected section of participants in the network. It's akin to a centralized system, but it's cryptographically protected as well as cheap. Everybody is not authorized to read, write, audit, or make transactions. In other words, they are permissioned blockchains. Ripple is an example of a private blockchain.
3. *Consortium blockchain*: This blockchain exists between the two extremes of private and public chains. Rather than a single governing authority, multiple designated authorities have write permissions that can administer and check the consensus procedure to approve a block. The read is not open to mass but only to a set of participants in the network, making it partially decentralized. It facilitates quicker transactions and preserves data by providing multiple points of failure [4].

2 Characteristics of Blockchain Technology

The features of blockchain, as described in Fig. 1, are discussed as follows [5]:

(1) ***Decentralization***: In contrast to conventional database systems, blockchain technology does not rely on a centralized system to authenticate transactions since every single node in the blockchain has its own replica of data. Thus, the control does not reside solely on a single server or system.

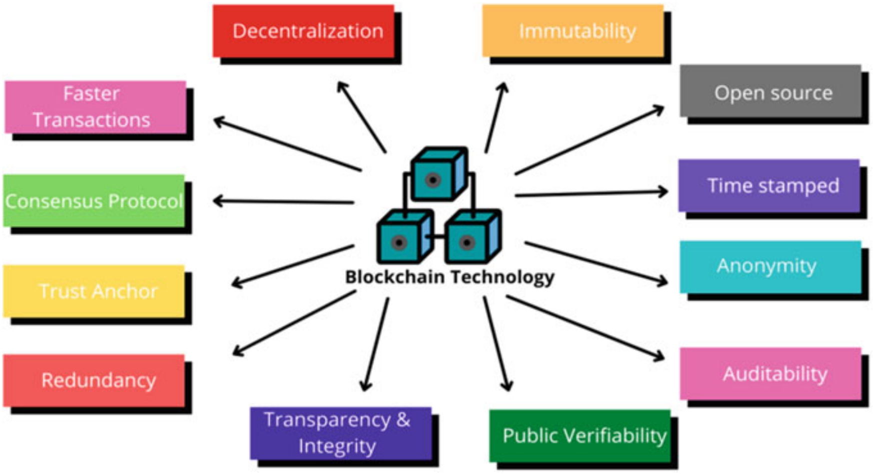


Fig. 1 Core attributes of blockchain technology

(2) ***Immutability***: Every block carries the block header, Merkle root, the hash of the preceding block, and transaction details which are altogether hashed using a famous hashing algorithm like SHA-256 (Secure Hash Algorithm 256). This unique hash value is difficult to reverse engineer, and even a small change in input completely changes the output. The cryptographic hash is difficult to generate but is easily verifiable by miners. As hashing incorporates metadata from the previous block, it sets up a connection between the current and previous nodes and the cycle continues as new blocks are chronologically added to the chain. Thus, if an attacker attempts to alter one block, its hash value will change too thereby breaking the chain. In order to restore all the subsequent blocks, each hash value will need to be recalculated which requires tremendous computational power.

(3) ***Anonymity***: Users interacting with blockchains are assigned with public and private keys. A public key is an identifier that is used to manage and verify the identity of a user and can be shared freely. On the other hand, the private key is like a password that must never be shared. A person's real identity is concealed, making transactions anonymous. In addition, a user's identity can be either anonymous or pseudonymous.

(4) ***Time-stamped***: Each block stores the date and time at which it was mined and successfully added by the blockchain network.

(5) ***Auditability***: Prior to a transaction getting incorporated into the blockchain, it should be verified by the node. The cryptocurrency should actually be owned by the spender and he/she should possess sufficient balance to carry out any given transaction. Thus, transactions rely on previous unspent transactions. This makes the verification and tracking process easy.

(6) ***Public Verifiability***: Each node in the network validates its own copy of transaction data through a general consensus protocol. Therefore, it can be verified by anyone.

(7) ***Transparency & Integrity***: Blockchain data is updated and synced across nodes for public validation. Every node has a separate copy of the data. The digital record is public and transparent to each node. This system enables public verification so anybody can certify it while maintaining its integrity.

(8) ***Redundancy***: Blockchain technology is based on a decentralized architecture which means each node holds data which is consistent across all nodes in the network. In contrast, centralized systems rely on backups and physical servers to get the stored information giving rise to redundant data.

(9) ***Trust Anchor***: Providing read and write access to a system is the responsibility of the trust anchor. They control, access, and grant permissions.

(10) ***Consensus Protocol***: Blockchain eliminates the need for intermediaries. As there is no central authority to validate the transactions, it is important to reach a consensus among the untrustworthy nodes. Nodes cannot trust each other in order to identify illegal and invalid transactions. Hence to maintain the consistency through all the nodes, they settle on an agreed consensus protocol thus ensuring accountability. Consensus mechanisms resolve this problem of trust between corrupt nodes. New blocks are appended to the chain when the majority of the nodes verify the transactions unanimously.

(11) ***Faster transactions***: With blockchain technology, transactions are completed within a matter of few minutes thus conserving time. Traditional payment methods involve various paperwork which takes ample time for approval.

(12) ***Open Source***: Most blockchain systems are open source which means everyone can use blockchain technologies to build their own applications.

3 Working of Blockchain

To fully comprehend the vulnerabilities of blockchain, it is essential to get acquainted with its working [5]. Before we dive deeper into this subject, we examine a few fundamental key components of a blockchain.

Node: It is simply a computer system that preserves replicated copies of the database as well as stores details associated with payment and ownership. There are several nodes depending on the level of participation and type of blockchain network. Full nodes work separately and inspect all the rules of the system. Lightweight nodes only download the headers of blocks and confirm the transactions through SPV (Simple Payment Verification).

Block: Similar to a record in a public ledger, a block stores the information of all the transactions happening over a time period. These blocks are connected to each other via a hash pointer, which points to its predecessor's data. The very first block in the starting of each chain has no parent block and is called the genesis block. A

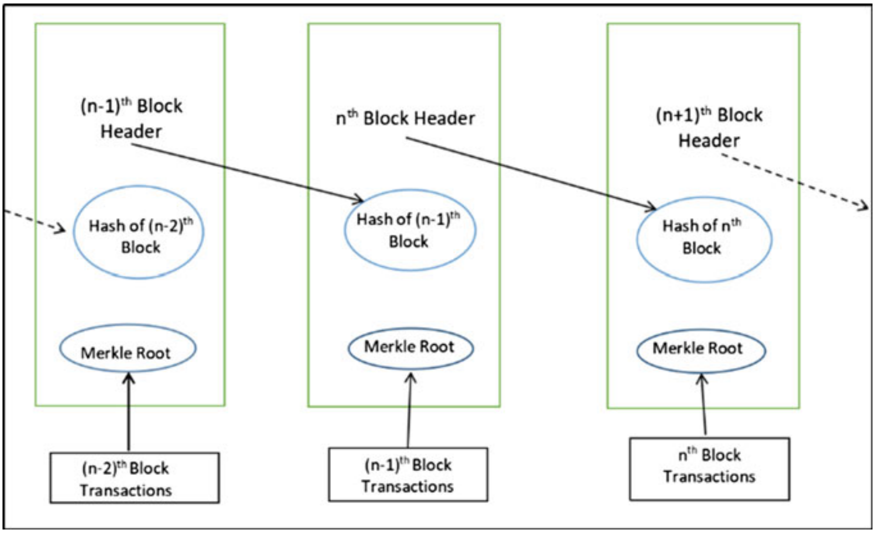


Fig. 2 Structure of a block

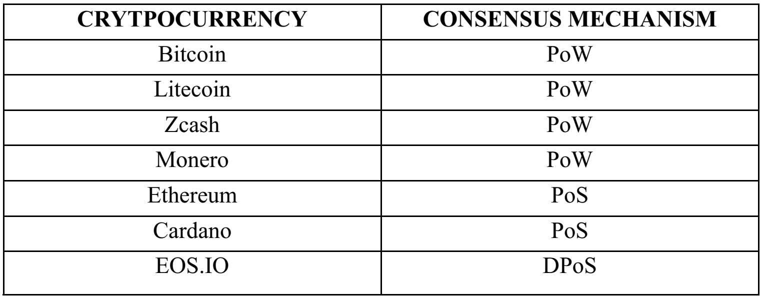
block is divided into two components: block header and the block body. The block header contains metadata such as block version, Merkle tree root hash, nBits, parent block hash, timestamp, and nonce. Transactions make up the block body along with a transaction counter. The typical structure of a block is shown in Fig. 2.

Transaction: Transactions are data structures that represent the exchange of digital currency between a sender and receiver over a blockchain network. Every transaction is kept in an invalidated transaction pool and distributed in the network by applying a flooding protocol called the Gossip protocol. Miners typically prefer transactions with a higher transaction fee [6].

Miner: Mining is the most important feature of blockchain through which new cryptocurrency is added to circulation. In blockchain, mining is the process of adding new blocks of transactions, which are then authenticated. The peer who uses its computing power to mine a block is called a miner [7].

Hash and Hash function: Hash function is a mathematical algorithm that takes an input and converts it into an output of a specific length. It is collision resistant which means that it is quite challenging to create the input data again from the hash value alone. It is associated with the immutability feature of blockchain, discussed earlier.

Consensus mechanism: To maintain data consistency, it is necessary to reach consensus among the untrustworthy nodes through a set of predefined rules known as consensus algorithms. Figure 3 shows some of the most common consensus procedures like PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of



CRYTPOCURRENCY	CONSENSUS MECHANISM
Bitcoin	PoW
Litecoin	PoW
Zcash	PoW
Monero	PoW
Ethereum	PoS
Cardano	PoS
EOS.IO	DPoS

Fig. 3 Consensus mechanisms used by well-known cryptocurrencies

Stake), PBFT (Practical Byzantine Fault Tolerance), etc. used by popular cryptocurrencies to solve the Byzantine Generals Problem. Each consensus mechanism has its own merits and demerits.

Digital signature: By using a cryptographic algorithm, a digital signature certifies if data is legitimate or not. Each participant has two types of keys. One is public, which represents transactions and is openly visible to everyone, so anyone in the network can decrypt the transaction. As for the private key, it is used to digitally sign the transactions and prove ownership. The signature is composed of 256 bits which means any attacker needs to apply 2256 permutations to fake it, which is simply a waste of resources [8].

How Does a Transaction Work in Blockchain?

Figure 4 summarizes the entire transaction process in blockchain. A sender issues a transaction and this transaction is added to the unconfirmed transaction pool. The node clubs all the transactions in a given period of time into a block. Before a miner adds the block, he checks its validity by verifying the digital signature and blockchain's history to see if the user has sufficient currency to trigger the said transaction [9]. The miners compete to solve an extremely complicated mathematical puzzle to generate a hash value, whose value should be less than the current target value. Its difficulty is determined by the network and is dynamically set by the system after every 10 min. When a winner emerges, he gets to add the block to the distributed ledger. The successful miner is rewarded with some cryptocurrency for using his resources to create this block. Any transaction fees acquired by the miner are also sent in this transaction. The verified block is then relayed to its peers, who may or may not choose to mine the transaction. All the peers in the network verify the new block using a consensus mechanism. If two blocks have the same parent block, a fork is created. Blockchain protocol deems the longest chain of two branches to be valid. Each miner will have this same blockchain making it consistent across the network [10].

After verification, the block containing the transaction is added to the existing blockchain and is now considered legitimate. The current block links itself with the another newly created block by using a cryptographic hash pointer. In other words,

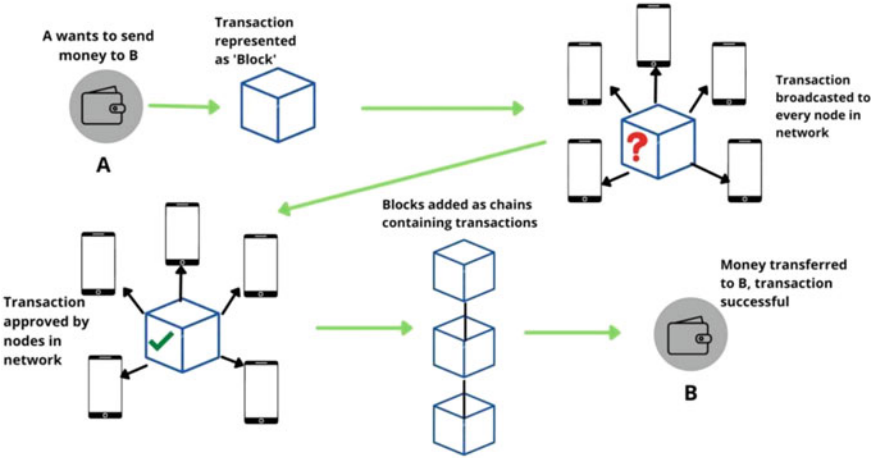

A wants to send money to B
A
Transaction represented as 'Block'
Transaction broadcasted to every node in network
Transaction approved by nodes in network
Blocks added as chains containing transactions
Money transferred to B, transaction successful
B

Fig. 4 Roadmap of a transaction in blockchain

this hash pointer points to the data in the parent block. Now the block receives its first confirmation while the transaction obtains the second confirmation. Additionally, with each new block added to the chain, the transaction is reconfirmed.

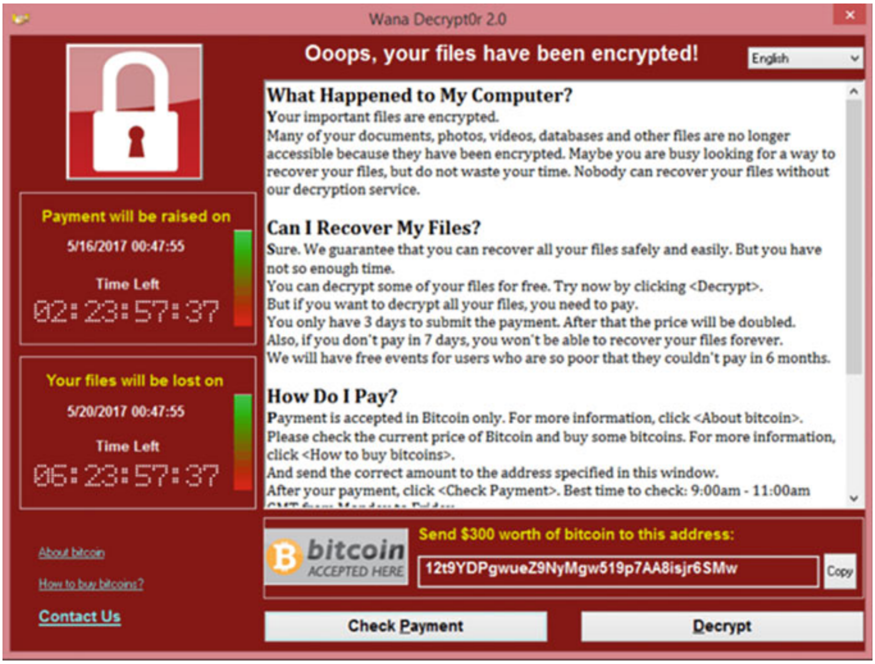
4 Analysis of Security in Blockchain

Given the risks involved with blockchain, there arises the urgent need to safeguard data and preserve online data resources. Over time security assaults have become more effective and powerful, resulting in old techniques becoming weak or redundant. The protection of important data in the present times can be ascertained with the help of blockchain technology.

The global outbreak of the virus WannaCry in 2017, which demanded ransom payments from the targeted users, made blockchain a hot topic in the world [11]. It caused damage worth millions and billions of dollars by infecting computers worldwide. A snapshot of the ransom message is displayed in Fig. 5.

4.1 Risks to Blockchain

Blockchain security is affected by many factors like the types of attacks, network state, scientific advancement, etc. A malicious actor can abuse this technology's vulnerabilities and gain unauthorized access for nefarious purposes [12]. Below we discuss some common risks to Blockchain technology:



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Fig. 5 Snapshot of WannaCry ransomware attack (*Source: wikipedia*)

(1) ***51% Attack***: Blockchains are distributed ledgers that use consensus protocols to authenticate transactions and maintain data consistency. In PoW (Proof of Work)-based blockchains, if an individual or a group of miners' computational hashing power is >50% of the total hashing power of the complete blockchain network, then this attack can be launched. Giving them an edge over honest miners, they can solve the puzzle faster, allowing them to earn undue rewards for completing new blocks. Higher the hashing power faster the attack.

It is possible for an attacker to exploit this vulnerability by posing the following threats:-

a. The attacker might be able to avoid new transactions from receiving confirmations, stopping them between merchants and clients.
b. They can manipulate transactions and reverse them allowing them to spend the same coins many times. (Double Spending)
c. Adversely affect the mining power of honest miners.
d. Exclude or alter the correct sequence of transactions.

(2) ***Double Spending***: Double spending is the situation in which the consumer utilizes the same cryptocurrency numerous times for carrying out transactions [13]. Before blockchain, it was difficult to ascertain the order in which the transactions arrived in the pool. Transaction A might happen prior to Transaction

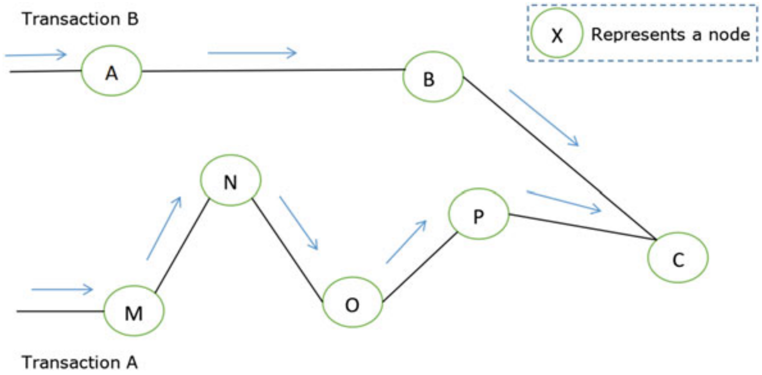


Fig. 6 (Double spending) Transaction B gets recorded due to fewer nodes than Transaction A

B, but the number of nodes Transaction A has to go through could be greater than that of Transaction B. As a consequence, Transaction B gets recorded in a node first. Figure 6 demonstrates this problem in a comprehensible manner. This lead to the problem of double spending and was resolved to some extent with the introduction of blockchain technology. Double spending can be carried out in yet another way.

PoW-based blockchain is more vulnerable to double spending problem since the attacker can utilize the transitional time between a transaction's initiation and verification. We illustrate this problem using the diagram shown in Fig. 7. We assume that an attacker performs two transactions. First transaction X is sent to the merchant's address and second transaction Y to a colluding address, which is owned by the attacker himself.

Cryptocurrency can be doubly spent provided that the following requirements are fulfilled:

(a) X is added to the merchant's account.
(b) Y is mined valid by the blockchain network.
(c) Before any anomaly can be detected, the merchant transacts the output to the attacker.

Transaction X is recognized as an invalid transaction eventually, and the attack becomes successful. The attacker has received the merchant's output while still owning the cryptocurrency resulting in double spending. The attacker revels in the service despite not spending any currency.

(3) ***Private key security***: Unique private and public keys are assigned to each client of the blockchain. The public key acts as the address which allows transactions to be received or sent. The private key is like a password used to access the transaction output (cryptocurrency). It also acts like a proof of ownership. As opposed to public keys, a person can only have one private key. This key is

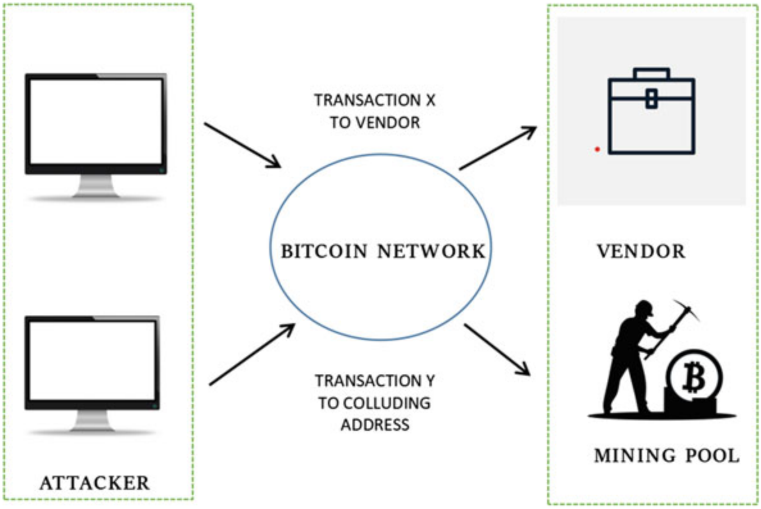


Fig. 7 Double spending

used to encrypt and sign transactions ensuring their security. If this private key is lost, it is quite challenging to retrieve. The user's blockchain account will be compromised if this key falls into the wrong hands. Since there is no central governing authority in blockchain, it is tough to track the malicious activities of a criminal and undo any tampered data. Hence, private keys must not be shared.

(4) ***Criminal Activity***: Criminals rely on funds and cannot operate usual bank accounts for storing them as they are highly regulated institutions [14]. Alternatively, Bitcoin can be conveniently used in illegal activities since it offers anonymity. Users can engage in illegal trade and buy or sell anything without being tracked. Bitcoin acts as the financial enabler of money laundering, fraud, human trafficking, cybercrime, terror funding, and other unlawful acts. According to a blog from Chainalysis, cryptocurrency crime reached an all time high in the year 2021. Some frequent activities involve the following:

a. Ransomware: Criminals use Bitcoin as the trading currency when it comes to deploying ransomware for ulterior motives as it offers anonymity. These programs encrypt the user's files and demand money in exchange for the decryption key which is essential to restore the affected files. In July 2014, a ransomware CTB-Locker (Curve-Tor-Bitcoin Locker) was transmitted around the globe by concealing itself as downloadable mail attachments. When a user clicks on this attachment, the virus infiltrates the system and begins encrypting files using elliptic curve cryptography. Unless the victim pays the attacker within 96 h through Bitcoin, the files remain scrambled leading to permanent loss of data.

b. Underground market: Bitcoin is frequently used as the currency in the underground market. Silk Road is an incognito and international online black market which runs on Tor hidden service. It allows the trade of illegal goods and services like drugs, illicit content, proprietary information, military-grade arms, etc. with Bitcoin, leaving no trail behind. This ultimately poses a threat to the social security of the countries.

c. Money laundering: Bitcoin's features of anonymity and virtual payment allow consumers to hide their assets and launder money across seas. Dark Wallet uses advanced cryptography and zero-knowledge proofs to enable users to hold their own money and control their finances. It provides advanced security features that improve upon the existing Bitcoin protocol. It facilitates money laundering by mixing the user's authentic cryptocurrency with chaff coins.

(5) ***Transaction privacy leakage***: Blockchain systems take actions to safeguard the transaction privacy of users. In Bitcoin and Zcash, one-time accounts are used for stocking the received cryptocurrency and a private key is allocated to each transaction. This is done so that the attacker cannot deduce if the transactions are collected by the same user. In Monero, users may comprise some chaff coins (known as mixins) when a transaction is initiated. As a result, the attacker is oblivious of the actual coins expended by the transaction. Unfortunately, blockchain does not provide adequate privacy protections. Blockchain transactions are public and the addresses of the sender and receiver are easily traceable. Using statistical analysis, an attacker can make out the total amount of cryptocurrency being transferred. In other words, the transactions from a targeted user can be linked making the user's behavior traceable. Analysis shows that 66.08% of all Monero transactions don't include any mixins and 62.32% of transaction inputs having mixins are deducible.

(6) ***Criminal Smart Contracts***: Criminals can use smart contracts for a variety of malicious activities, which may pose a threat to our daily life. CSCs (Criminal Smart Contracts) can promote the exposure of confidential information, theft of cryptographic keys, and multiple real-world delinquencies like terrorism, murder, arson, etc.

(7) ***Vulnerabilities in smart contracts***: Smart contracts may have security vulnerabilities caused by program defects that can be taken advantage of in the following ways:

a. Transaction-ordering dependence: TOD (Transaction-Ordering Dependent) contracts rely on the miners heavily for smooth execution. Blocks may contain multiple transactions making the order in which they are mined and added to the blockchain crucial for TOD contracts.

b. Timestamp dependence: Each block in the blockchain consists of a timestamp. Some smart contracts' trigger conditions rely on this timestamp that the miner sets according to its local standard time. This endangers the contract since an attacker may try to alter it.

c. Mishandled exceptions: Sometimes contracts are linked to each other and depend on the other's completion. When contract X calls contract Y, if Y runs unusually, Y will halt and give back false. Suppose contract X calls contract Y, which unusually halts running and conveys back a false value. This makes it necessary for contract X to specifically check if the call has been executed successfully. Not checking the exception information may make contract X vulnerable.

d. Reentrancy vulnerability: When a smart contract is invoked, the actual state of the contract account is altered after the call is finished. The intermediate state can be used by the malicious actor to invoke a call that sets a chain of calls that repeatedly call to the smart contract.

(8) ***Under-priced operations in Smart Contract***: Gas is simply a transaction fee in Ethereum based on the computational resources and parameters like bandwidth, execution time, memory occupancy, etc. It is payable by the sender and used to reward miners. Gas is the product of gas price (set by the sender) and gas cost. Every transaction has a gas limit which acts as a protective measure to prevent the abuse of resources by throwing an out-of-gas exception, if the execution is more gas costly. For example, if some demanding input–output operations' gas values are fixed at a very low level, these operations can be repeatedly implemented in quantity in a single transaction. If the gas cost set for EVM operations is not just then an attacker can commence DoS (Denial of Service) attack, whose purpose is to waste valuable computational resources at a low cost. This slows down the network leading to low transaction processing speeds which consequently pulls down the market value of Ethereum.
EXTCODESIZE and SUICIDE are two DoS (Denial of Service) attacks that abuse this vulnerability of under-priced executions in smart contracts. Ethereum has applied new settings to mitigate such attacks but it still does not solve the problem completely [15].

4.2 Attacks on Blockchain

Various types of attacks have emerged since the advent of blockchain technology which take advantage of different weaknesses of the system. The BCSEC reports that around 2 billion dollars of economic losses were incurred because of blockchain security incidents in 2018. This rising trend in losses from attacks is clearly shown in Fig. 8. As the blockchain's value grows, the likelihood of attacks will also rise [16].

Securing data is always the focus of people's attention, and it is also the main reason why blockchain has not been widely used all over the world. Below we discuss some attacks that threaten the basic nature of this technology.

(1) ***Selfish mining attack***: The main strategy behind this attack is keeping a new set of blocks secret and releasing them at an advantageous time earning them undue rewards while invalidating the work of honest miners. The attacker or selfish miner keeps undiscovered blocks private and tries to fork a private chain to create another branch/chain of blocks. A miner strategically publishes blocks

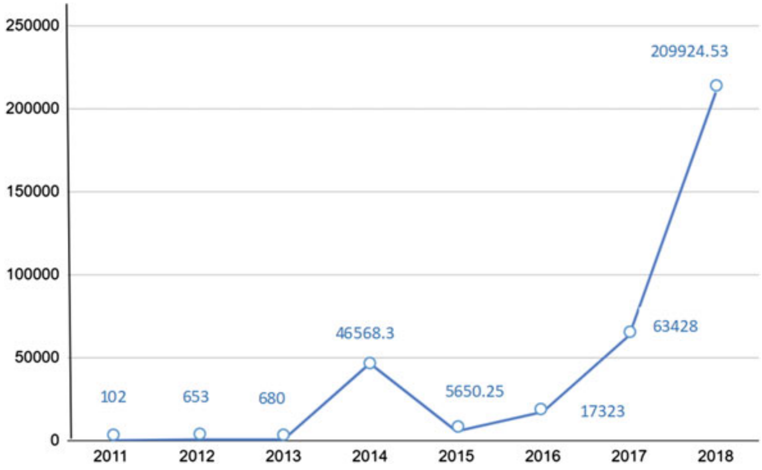


Fig. 8 Losses due to blockchain security incidents in tens of thousands of dollars (Year 2018)

once the public chain reaches the length of the private chain and consequently the blocks in the private chain become stale or orphaned [17]. The private chain now becomes the longest chain in the network so the honest miners are motivated to switch and start mining this chain. Hence, the honest miners end up wasting their time and resources in solving a computationally expensive puzzle fruitlessly. This attack is designed to waste the computational power of others. Selfish-Mine is a proposed attack plan, in which initially the length of the public as well as private chains are the same.

The following three situations can arise afterward:

a. Both the selfish miners and honest miners discover the first new block simultaneously which gives rise to two concurrent forks initially of the same length. Honest miners may mine any branch of the two whereas the selfish miners carry on mining the private chain. If selfish miners discover the second new block too, they publish it to the chain and are rewarded for mining the pair of blocks. The private chain will now become the valid branch due to the fact that it is the longest chain. On the condition that honest miners initially discover the second new block and then add it to the private chain, selfish miners collect the first new block's rewards, whereas honest miners will acquire rewards associated with the second new block. On the other hand, if the said block is written to the public chain, honest miners gain rewards for two new blocks while selfish miners receive none.
b. Considering the hashing power of selfish miners is relatively less and assuming the public chain is longer than the private one, they may update the private chain based on the public chain. This scenario does not reward them.

c. Selfish miners discover both the first and second blocks. In this scenario, they keep on mining blocks on the private chain while secretly withholding the two blocks. On the discovery of the first block by the sincere honest miners, selfish miners will broadcast their own first new block and the same process follows for the second new block. The selfish miners will carry on responding in this manner until the public chain exceeds the private chain by one block. Selfish miners will publish their last new block ahead of its discovery by honest miners, whereupon, the private chain will be deemed valid. As a result, selfish miners will be credited unwarranted rewards for all new blocks.

(2) ***BGP hijacking attack***: BGP (Border Gateway Protocol) is an external routing protocol governing how IP packets are forwarded to their destination. The main purpose is to intercept and divert the traffic by an ISP. In order to intercept the blockchain's network traffic, attackers either use BGP routing or manipulate it. Generally, hijacking BGP involves gaining control over the network operator, which can be exploited. An attacker can intercept the blockchain network by manipulating the BGP, and then data can be routed and the traffic can be modified to the attacker's favor. Taking a look at the node-level as well as network-level attacks, on Bitcoin, the number of the successfully to-be-hijacked Internet prefixes has a direct correlation with the distribution of mining power. Because of the high centralization of some Bitcoin mining pools, if they are encroached by BGP hijacking, it will have a striking effect. The hacker can slow down the pace of block propagation and divide the blockchain network.

(3) ***Liveness attack***: This type of attack can hinder the time it takes for a targeted transaction's confirmation or acknowledgment and cause unnecessary delay. Liveness attack consists of three phases which are (I) attack preparation phase, (II) transaction denial phase, and (III) blockchain delay phase.

a. Attack preparation phase: Similar to the selfish mining attack, an attacker tries to attain a profit over the honest miners and builds his private chain, before a specific transaction is broadcasted to the public chain. In this scenario, the private chain is of a greater length than the public chain.

b. Transaction denial phase: The attacker tries to delay the block comprising the targeted transaction by withholding it from the public chain. When he can no longer hold the block, he moves on to the next phase.

c. Blockchain delay phase: As the public chain grows, it is no longer possible to hold the targeted block and the block is broadcasted. In some blockchain systems when the depth of a block is greater than a constant, it will be declared valid and so the attacker keeps on mining the private chain for the sake of building an advantage over the public one. He will then publish privately held blocks in the public chain and try to slow down the growth rate of the chain. When the targeted transaction's validity is confirmed by miners in the public chain, the liveness attack ends.

(4) ***Balance attack***: In balance attack, the attacker can compensate for his low mining power by momentarily disrupting the connections between subgroups that have equivalent mining power. By abstracting the blockchain, the attacker creates a DAG (directed acyclic graph) tree. He then inserts a delay between valid subgroups and performs a transaction in one subgroup termed as transaction subgroup and mines the other sub-tree (block subgroup). This is done so that the block sub-tree dominates the transaction sub-tree and the attacker can disregard that transaction and the attacker can alter the block containing the concerned transaction with high probability despite the transaction being committed.

The attacker recognizes the subgroup with the targeted merchant and issues transactions to purchase goods from them. Afterward, the attacker gives out transactions to this subgroup and mines the blocks in the group. The attacker delays the communication until the merchant ships the goods. The attacker could re-create another transaction using exactly the same cryptocurrency given that with a high probability, the DAG tree seen by the merchant is outweighed by another tree. The attacker makes the nodes disregard the valid transaction allowing him to double spend successfully. The balance attack clearly proves that block obliviousness is a limitation of PoW-based blockchain systems. This means that a malicious actor can issue a transaction to a merchant and later remove it from the main valid branch.

(5) ***DDoS attack***: A denial-of-service (DoS) attack is a type of cyber attack that disrupts the normal operations of the host's services by overwhelming the network resource or machine making it unavailable to its users. It overloads the target system or network by flooding it with unwanted Internet traffic so as to cripple the normal services of the host.

A DDoS attack refers to a distributed DoS attack in which unexpected traffic emerges from different distributed sources spanning all over the Internet network. DDoS attacks utilize the compromised systems to send large amounts of data to the host ultimately clogging the communications. Counteracting this by isolating each individual source and jamming them one by one is barely effective in this case. By knocking out a network partially or completely, this attack can render the blockchain inaccessible. On one side is the recovering rate of the compromised nodes and on the other is the success rate of the attack on the network.

(6) ***Sybil attack***: In Sybil attack, a malicious node forges multiple identities and operates them simultaneously in real time, which obliterates the reputation of the blockchain network. To an outside viewer, these identities appear as separate real entities and give unfair majority influence over the network to a particular node. Sybil attacks are capable of being executed directly or indirectly through a middle node.

Private blockchains automatically prevent this attack as they authenticate a node's identity before it joins that network. Consensus algorithms like PoW, PoS, and DPoS make Sybil attacks impractical [18]. These algorithms make the mining process so resource intensive that it discourages a miner from attempting a Sybil attack and it is in the attacker's favor to continue mining honestly.

5 Security Enhancements

(1) ***Hawk***: As we have already discussed that the privacy protection measures in blockchain are not very robust. Research suggests that deanonymization is attainable with careful analysis of transactions. In blockchain, not only the transactions but also the smart contracts are publicly visible. Hawk is a framework that separates smart contracts into portions that are public and private, thereby granting some degree of privacy to smart contracts. Private data like personal information of the user and financial transactions can be confined to the private part and the rest of the data can be written to the public portion. It allows the users to write easy encryption-free code as Hawk provides its own cryptographic protocol to conceal confidential information. Hawk ensures transactional privacy through contractual security and on-chain privacy [19].

(2) ***SegWit***: SegWit or Segregated witness is an additional protocol upgrade that runs alongside blockchain. It separates the signature information or witness information and stores it outside in a side chain, allowing more transactions to be included in each block. This increases the throughput of the blockchain system, reduces transaction fees, and also improves scalability. In addition, the segregation of data makes the network more secure. Note that it does not increase the block size. It was originally deployed to combat transaction malleability problems.

(3) ***Oyente***: Oyente is an open-source tool used for finding bugs in smart contracts deployed on Ethereum. It uses the technique of symbolic execution with constraint solver Z3 to analyze the bytecode of the smart contracts without having to execute them. Ethereum blockchain stores this EVM (Ethereum virtual machine) bytecode. As illustrated in Fig. 9, it is made of four key components: CFG Builder, Explorer, Core Analysis, and Validator. The CFG builder accepts the byte code and global state as input to construct a CFG (control flow graph) in which nodes represent the execution blocks and edges represent the jump between them. Explorer runs the contract virtually and executes the states until there are none remaining or the time runs out. Z3 eliminates the proven impractical traces. The core analysis identifies the four major security flaws: TOD, timestamp dependence detection, mishandled exceptions, and reentrancy detection. The last part, the validator eliminates false positives. Oyente flags the contracts which are potentially vulnerable. This feature can be used by users for writing problem-free and better contracts.

(4) ***Lightning network***: Bitcoin users have to wait for a fixed period of time before transactions are confirmed and assured that they won't be reversed. In bitcoin, users have to wait for six block confirmations or about an hour to make the transactions full and final. With payments involving small amounts, the transaction fee is minimal which makes the transaction uneconomical. The lightning framework, a two-layer transaction mechanism, was introduced to resolve these problems. These transactions do not rely on block confirmations but on double

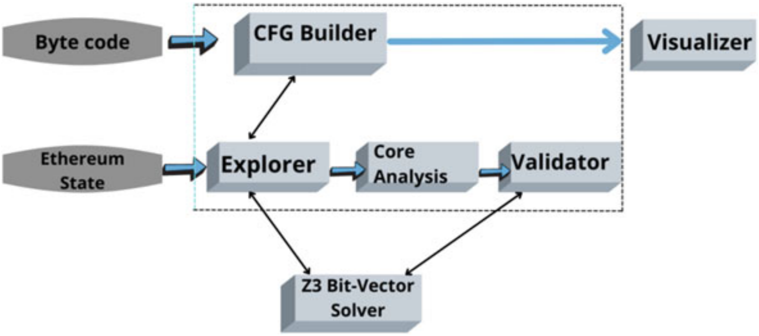


Fig. 9 Architecture of Oyente

signing from both the involved parties of the channel. The channel is bidirectional and can be opened by committing a simple fund. It allows users to conduct transactions between themselves and off the blockchain without making them public. Each user can have multiple channels across the network allowing for mass transfer of funds. These are free from the interference of a third-party miner. They can be closed unilaterally when one party decides to end the channel or when the transactions are completed. Only when the channel is closed, the final settlement is added to the blockchain [20].

6 Applications of Blockchain

Blockchain technology has a wide range of applications. A vast variety of fields like healthcare, voting, real estate, energy, governance, education, and many more can benefit from the advancement of blockchain technology. Blockchain is also expected to have an impact on the digital environment just like the Internet [21]. Initially, when the Internet was introduced, nobody had any idea about the great changes that it would bring to the world. Now in the present world, nearly every small and big activity is dependent on it. The time will come when Blockchain will have a similar impact too as it is gradually progressing every day. Outlined in Fig. 10, we highlight a few of the applications of blockchain that researchers across the globe have suggested.

Healthcare

- Introduction of blockchain in healthcare systems eliminates the need for intermediate entities making the traditional system more efficient and cheaper. It allows patients to timely receive required aid without any unwanted delay.
- Every patient has a distinct physical profile and the treatment strategy may differ from doctor to doctor. Blockchain technology improves the interoperability of health reports by integrating the medical records, allowing doctors/specialists from different institutions to work in cohesion and deliver better healthcare to the

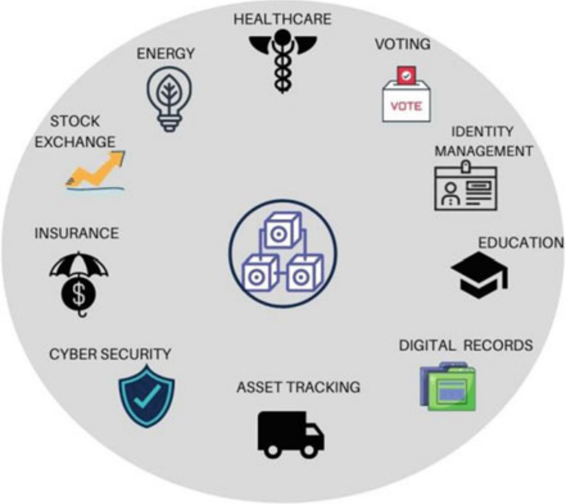


Fig. 10 Applications of blockchain technology

patients. It makes every patient's absolute medical history easily accessible by granting a secure sharing platform.

- The BCT will provide transparency in the healthcare system when all the medical practitioners have access to accurate and unaltered data and information which prevents malpractices.
- Blockchain can be a solution to the fabrication of drugs in the pharmaceutical industry as all the transactions added to the distributed ledger are unalterable and digitally timestamped, which makes it easier to track any product and discourage such malignant practices. These drugs endanger a patient's life rather than curing the diseases; they may have negative side effects that can be fatal.
- The current medical record-keeping system lacks privacy. Blockchain offers significantly more security to keep each patient's sensitive information private. This decentralized information is also difficult to hack or alter as multiple copies are maintained in the network.
- Smart contracts can be utilized to implement health insurance that can release funds when the patient gets discharged. It streamlines the claim verification process and can be done automatically when some conditions are met, preventing false claims.

Insurance

- Smart contracts can be used to automate the insurance policies. This reduces the cost by eliminating the administration, processing, and other overhead costs. The terms are structured using digital protocols that precisely follow the predefined terms which prevent frauds by misinterpretation and disagreement of conditions.
- It reduces the level of paperwork, making underwriting easier and storage of data related.

Identity Management

- In real life, verifying identity using physical documents and ids is easy but it is hardly effective in online systems. Blockchain may permit people to make an encrypted identity, which requires neither username nor password making it more secure and giving the user more control of his private data.
- Blockchain technology might allow the consumer to access and verify online payments by the mere use of an app for authentication rather than the usual username, password, and biometric security system enhancing transparency.
- Cryptography segregates data from the individuals' identities for better security. With the help of separate data, management companies can acquire only that data which is of their use thereby preventing the misuse of personal information like frauds in banking, trading, etc. It only protects from the leakage of confidential data by companies.
- By using blockchain-based identity management systems, we can eliminate the involvement of third parties for digital or manual identity management, identity theft, and identity sprawl.

Supply Chain

- Blockchain can drastically improve the transparency of products. It can verify the genuineness of products making the supply chains more efficient and competent.
- Blockchain improves the management and storage of inventory and reduces the related paperwork.
- It enhances traceability in a supply chain by offering real-time tracking of goods. It helps in locating the goods and hastening the operations. Tracking allows for locating the goods in cases of human error and fraud and makes operations swift and secure.
- Smart contracts in blockchain can connect the logistics related to delivery and its payments using digital contracts, improving the efficacy of the supply chain.
- Blockchain can transform the automobile industry. The whole vehicle history can be stored on a distributed ledger with an immutable feature which allows the buying of used vehicles trust-less and reserves the resale price of the currently used new vehicle. Information on the public ledger will help the future buyers know the exact value of the vehicles and also help the owners to receive the correct value for their vehicles. This technology will also help to eliminate the counterfeiting in the automotive industry.
- Blockchain can transform the automobile industry. A vehicle's complete history can be stored on the distributed ledger which makes buying and selling second-hand automobiles trustworthy and easy. The exact market value of a vehicle can be evaluated during resale, eliminating frauds and counterfeiting in the industry.
- In food-based supply chains, blockchain can be helpful in tracing the food products in case of an outbreak of a food-borne disease and identifying the contaminated sources.

Financial Services

- With blockchain technology, the transactions become faster which are predominantly slow in the existing banking systems [22]. Sometimes the transfer of funds across borders takes days to be successful. Blockchain provides for seamless transactions which are processed and verified within a matter of seconds across time zones.
- Blockchain facilitates inter-banking borrowing and lending of funds that are speedy, robust, and transparent.
- Auditing can be done in significantly less time as data stored in blocks is immutable and verifiable. Audits generally take from weeks to months to finish. The distributed ledgers can make verifying the integrity of transactional data using digital fingerprints possible.
- Investors can invest in decentralized hedge funds which eliminate the use of a hedge fund manager and minimize security risks.
- Credits score reports can be stored in blockchains. Due to its immutable nature, this information cannot be tampered with or sold or leaked. It enables small businesses to easily get approval for credits.

Music Industry

- Blockchain fixes the existing problems in the music industry of ownership in-clarity, royalty distribution, and monetization of music. Smart contracts in blockchains can deliver the required reliability and transparency, with music owners getting their rightful share of royalty.
- Blockchain can provide a vast decentralized platform for the music industry where artists and musicians can collaborate and directly share their content, eliminating the need for any intermediaries. Blockchain can also be used to form separate music streaming platforms.
- Copyright claims and issues are a big problem in the music industry and blockchain technology can provide the means to authenticate copyrighted music and prevent the sharing of pirated versions. It gives the music artists their well-deserved rights to the music.

Other Applications

- Blockchain can provide an E-voting system where people can simply vote from their mobile phones or PCs at a cheaper rate. It will guarantee a secure, anonymous, transparent, truly democratic, and completely safe system with data encryption and no breach of security.
- Blockchain in real estate assures direct means of connection between the buyers and sellers thus reducing the costs of intermediaries' fees and commissions. It also allows the estate to be tokenized and traded like cryptocurrencies thereby offering a chance for fractional ownership too.
- The distribution and encryption of data in blockchain provide transparency and records of the transactions. It also ensures reduced costs and increased speed of transactions hence making the entire IoT(Internet-of-Things) ecosystem proactive.

7 Trade-Offs and Challenges of Blockchain Technology

Blockchain is a fascinating and revolutionary technology and is being adopted by various industries belonging to diverse sectors. As per May 2019, 44% of the total global institutions have implemented blockchain [23]. However, like every other emerging technology, it has its disadvantages and restrictions. In this section, we talk about some fundamental difficulties encountered by blockchain technology.

(1) ***Performance & Scalability***: Latency and throughput are two variables in performance. Throughput refers to the number of transactions completed in a unit time, whereas latency refers to the time taken to add a block to the chain. Protocols like Proof of Work deliver low throughput and high latency because a lot of computational power and resources are required to work out the puzzles before a block of transactions can be added to a chain. For example, Bitcoin provides a low throughput of 6–7 transactions per second.

With a huge number of transactions taking place each minute, miners prefer those which have a high transaction fee since the size of each block is limited. The size of blocks in Bitcoin is 1 MB. This delays the small transactions making the system slow. A decentralized blockchain cannot have all the characteristics of decentralization, consistency, and scalability as stated in the DCS triangle given below in Fig. 11. Blockchain can fulfill only two conditions of DCS at a time. One provides high latency and low throughput while the other provides reduced transaction speed and low volume. Using alternative consensus algorithms can be a remedy to this problem.

(2) ***Energy consumption***: The blockchain network deals with a tremendous amount of message exchange and processing which includes computing complex mathematical problems to satisfy the consensus protocols. Hence, the consensus algorithms like Proof of Work are energy inefficient making them unsustainable. Whenever a miner successfully adds a block to a chain, he is rewarded Bitcoins for this painstaking work and this serves as an incentive to attract more miners

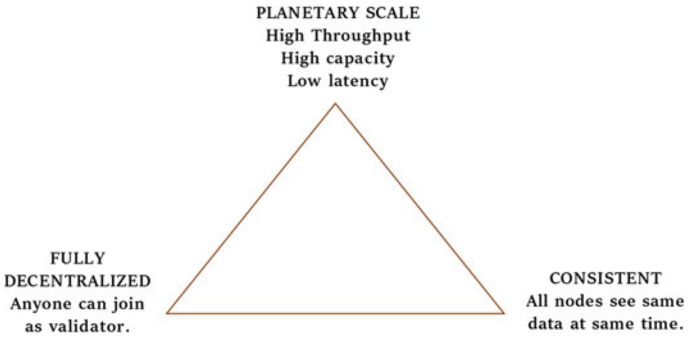


Fig. 11 DCS triangle

to run high-energy demanding devices. This process in turn adds more cryptocurrency to circulation. Subsequently, the total energy consumption of Bitcoin reached a new high. According to International Energy Agency, the total energy consumption of Bitcoin is higher than in a few countries. It is also predicted that the mining of Bitcoin could add to significant global warming and temperature may rise as much as 2 °C within a span of three decades [24]. According to estimates, each transaction alone has a carbon footprint of 274.29 kg of CO_2 per transaction. Although the application of blockchain technology in several cases cuts down intermediary costs, it comes at a greater price to pay.

(3) ***Privacy leakage***: Although blockchain provides security and privacy, it does not assure transactional privacy. A peer is anonymous in the blockchain network but research shows that IP addresses can be traced back to the peers' pseudonyms exposing the user's identity, even while hiding behind a firewall or NAT (network address translation). Peers may also be identified through its set of connected nodes. The main reason behind this is that all the transactions and the associated public keys are openly visible.

(4) ***Initial cost***: The initial cost of building the infrastructure of blockchain is quite high. It includes the cost of software development and a team of experts to launch the application.

(5) ***Public trust & perception***: People lack a technical understanding of blockchain technology usually. Blockchain involves several complicated terms and jargons, which makes it important for people to be fully aware of it before entering this ecosystem. Common man finds blockchain technology synonymous with Bitcoin. Furthermore, people also don't have much faith and trust in this new form of money (cryptocurrency) hence it requires meticulous marketing strategies to gain people's confidence and make it a worthy investment.

(6) ***Regulatory problems***: Cryptocurrency weakens the control of central banks on the economy of a state. There are no international laws to regulate cryptocurrency or bitcoin and its legal status varies from country to country. Canada has a bitcoin-friendly status and treats it like a commodity while Australia considers it a currency. There are no uniform regulations in the European Union. In contrast, Bitcoin is banned in countries like Iran, Ecuador, Pakistan, Morocco, etc.

(7) ***Immutability***: The immutable nature of blockchains may not be a fit model for scientific research where new findings and literature are published every day. This requires the scientific literature to be updated, changed, or may altogether contradict the previous findings.

(8) ***Cybercrime***: We have already discussed the role of blockchain-based cryptocurrency and how it is being exploited by criminals and terrorists to further aid their ill motives. This puts in question the legitimacy of blockchain as means of storing and managing data in information centers and libraries [25].

8 Conclusion

We have discussed the core concepts of blockchain technology and some of the most important characteristics. Blockchain technology is widely recognized and highly reputed due to its decentralized and immutable nature. In this chapter, we theoretically discussed various vulnerabilities as well as attacks on blockchain that obstruct the increased adoption of this technology. While we enjoy the perks of this disruptive technology, it is important to stay cautious of the existing security risks. With the expansion of its applications, new security threats are emerging as well. The way to strengthen the security is to divert the emphasis from applications to the analysis of blockchain security and advance research in this area.

Blockchain technology has shown great advancements in various fields since its establishment in 2009 extending from the traditional cryptocurrency to the present smart contract. Although it is still in the infant stage, we should not underestimate the optimistic socio-economic advantages of this remarkable technology. Some of its issues have been solved but it has still got a long way to go. The governments of various nations have to make regulatory laws for this technology before it can be embraced by even more companies and organizations. To conclude this chapter, in the final section, we have covered the uses, benefits, and future applications.

References

1. Mishra, S., Dash, A., Ranjan, P., Jena, A.K.: Enhancing heart disorders prediction with attribute optimization. In: Advances in Electronics, Communication and Computing, pp. 139–145. Springer, Singapore
2. Ekblaw, A., Halamka, J.D., Lippman, A.: A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data (2016)
3. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: International Conference on Open and Big Data, OBD, pp. 25–30
4. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 218 (2016)
5. Mishra, S., Mishra, B.K., Tripathy, H.K.: A neuro-genetic model to predict hepatitis disease risk. In: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1–3. IEEE (2015)
6. Mishra, S., Panda, A., Tripathy, K.H.: Implementation of re-sampling technique to handle skewed data in tumor prediction. J. Adv. Res. Dyn. Control Syst. **10**, 526–530 (2018)
7. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: The 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16
8. Mishra, S., Thakkar, H.K., Mallick, P.K., Tiwari, P., Alamri, A.: A sustainable IoHT based computationally intelligent healthcare monitoring system for lung cancer risk detection. Sustain. Cities Soc. **72**, 103079 (2021)
9. Christin, N.: Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: The 22nd International Conference on World Wide Web, pp. 213–224 (2013)
10. Juels, A., Kosba, E.S.: The ring of gyges: investigating the future of criminal smart contracts. In: The ACM SIGSAC Conference on Computer and Communications Security, pp. 283–295

11. Zhang, F., Cecchetti, E., Croman, K., Juels, A., Shi, E.: Town crier: an authenticated data feed for smart contracts. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 270–282
12. Chen, T., Li, X., Luo, X., Zhang, X.: Under-optimized smart contracts devour your money. In: IEEE 24th International Conference on Software Analysis, Evolution and Reengineerin, SANER, pp. 442–446
13. Mondal, S., Tripathy, H.K., Mishra, S., Mallick, P.K.: Perspective analysis of anti-aging products using voting-based ensemble technique. In: Advances in Systems, Control and Automations, pp. 237–246. Springer, Singapore (2021)
14. Tripathy, H.K., Mishra, S., Thakkar, H.K., Rai, D.: Care: a collision-aware mobile robot navigation in grid environment using improved breadth first search. Comput. Electr. Eng. **94**, 107327 (2021)
15. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. In: Financial Cryptography and Data Security—18th International Conference. Lecture Notes in Computer Science, vol. 8437, pp. 436–454 (2014)
16. Apostolaki, M., Zohar, A., Vanbever, L.: Hijacking bitcoin: routing attacks on cryptocurrencies. In: IEEE Symposium on Security and Privacy, pp. 375–392 (2017)
17. Yan, H., Oliveira, R., Burnett, K., Matthews, D., Zhang, L., Massey, D.: BGPmon: a real-time, scalable, extensible monitoring system. In: Cybersecurity Applications Technology Conference for Homeland Security, pp. 212–223 (2009)
18. Singh, A., Ngan, T., Druschel, P., Wallach, D.S.: Eclipse attacks on overlay networks: threats and defenses. In: 25th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies (2006)
19. Tripathy, H.K., Mallick, P.K., Mishra, S.: Application and evaluation of classification model to detect autistic spectrum disorders in children. Int. J. Comput. Appl. Technol. **65**(4), 368–377 (2021)
20. Greveler, U., Justus, B., et al.: A privacy preserving system for cloud computing. In: 11th IEEE International Conference on Computer and Information Technology, pp. 648–653 (2011)
21. Mishra, S., Tripathy, H.K., Thakkar, H.K., Garg, D., Kotecha, K., Pandya, S.: An explainable intelligence driven query prioritization using balanced decision tree approach for multi-level psychological disorders assessment. Front. Pub. Health **9** (2021)
22. Wang, Q., Wang, C., et al.: Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE (2010)
23. Mohapatra, S.K., Mishra, S., Tripathy, H.K., Bhoi, A.K., Barsocchi, P.: A pragmatic investigation of energy consumption and utilization models in the urban sector using predictive intelligence approaches. Energies **14**(13), 3900 (2021)
24. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: The ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16 (2016)
25. Stolfo, S.J., Salem, M.B., Keromytis, A.D.: Fog computing: mitigating insider data theft attacks in cloud. In: IEEE CS Security and Privacy Workshop (2012)