Chapter 6
Blockchain Technology: Concept, Applications, Challenges, and Security Threats

Charu Gandhi, Nitin Shukla, Gagandeep Kaur, and Kusum Yadav

6.1 Introduction to Blockchain

Blockchain technology is a combination of various digital mechanisms like cryptography, data management, and networking which supports capturing, validation, and execution of transactions between the communicating users. Blockchains are basically tamper evident and tamper resistant distributed digital ledgers implemented with a decentralized repository and has no central authority. It is a distributed and public database of all transactions executed and shared among participating parties. Basically, they enable a group of users to record transactions in a shared ledger and do not allow transactions to be changed once published [11, 15]. The blockchain contains a verifiable record of every transaction ever made which is verified by consensus of the participants in the system. Blockchain can be technically defined as (Fig. 6.1),

Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers [3].

In blockchains the cryptographically signed transactions are grouped into blocks. Each block is cryptographically linked to the previous block making the chain tamper evident. New blocks are added after validation using the consensus mechanism and replicated across the ledger of the network. Blockchain can create a shared reality across non-trusting entities where the participating nodes in the network do

C. Gandhi (✉) · N. Shukla · G. Kaur
Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India
e-mail: charu.gandhi@jiit.ac.in; nitin.shukla@jiit.ac.in; gagandeep.kaur@jiit.ac.in

K. Yadav
College of Computer Science and Engineering, University of Hail, Hail, Saudi Arabia

T. Choudhury et al. (eds.), *Blockchain Applications in IoT Ecosystem*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-65691-1_6

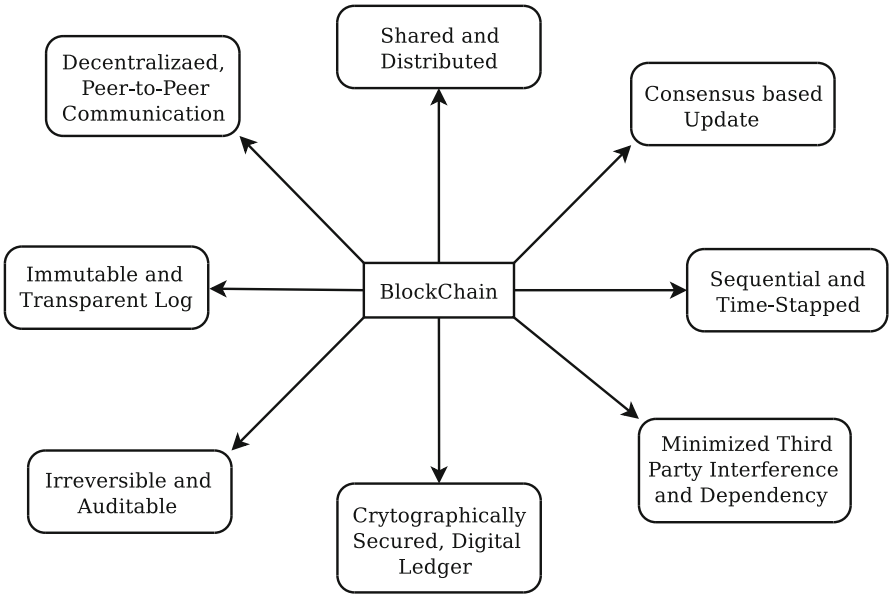

Fig. 6.1 Characteristic features of a blockchain

not need to know or trust each other. Each participant has the ability to monitor and validate chain for themselves. Prior to the use of Blockchain technology, this trust was typically delivered through intermediaries trusted by both parties. The key features of Blockchain can be summarized as:

(a) **Increased Capacity:** Due to the decentralized working principle, the blockchain technology increases the capacity of the whole network. Because of the multiple shared computing systems working together which in total offers much larger computation capacity as compared to individual systems in a centralized environment.
(b) **Better Security:** Ledger is cryptographically secure, which makes it immune to tampering and misuse. Cryptographic services ensure non-repudiation, data integrity, and data origin authentication. Blockchain in its functioning allows access to the past transactions and at the same time protects the identity of the individuals associated with the transaction. The identity theft of a user during the execution of a transaction is therefore infeasible.
(c) **Immutability:** Immutability is ability of a blockchain ledger to remain unaltered and indelible. Data in the blockchain cannot be altered. Every block contains a unique hash or digital signature for itself as well as for the previous one. Thus, the blocks are tightly coupled together and any intrusion into the systems and data modification is very difficult. Immutability along with the consensus approach makes the data auditing process more integral, efficient, cost-effective, and trust worthy.

(d) **Faster Settlement:** Network-based infrastructure of blockchain allows for the instantaneous recording and retrieval of information. It is expected to increase the efficiency of operations by improving the speed of execution and reducing resource requirement and cost. This is the major reason that the modern financial systems are currently experimenting with the use of the blockchain aiming to facilitate intermediation between banks, clearing houses, and central banks.

(e) **Distributed System:** Distributed ledger, the basis of blockchain, can be shared among a group of users connected through the internet. To ensure that all users have a latest version of the ledger, a message is relayed on creation of every new block. This feature eliminates the need of a central authority to record and validate the information. Since the ledger is stored in multiple different locations, any form of data loss due to system failure is protected. Further, other users can still access and add information on the blockchain, until there is at least one online device having the latest version.

(f) **Minting:** Crypto Minting is an integrated platform for staking cryptocurrency. Staking is the process where the Proof Of Stake (PoS) cryptocurrency wallet stakes a sum of coins when broadcasting to the network that the transaction they are processing is true and non-malicious. If the network agrees on the verdict, the verifying wallet will receive a reward in the form of coins on the associated blockchain network. With enormous growth in number of cryptocurrencies, several blockchain maintenance methods are investigated for better support.

6.2 Blockchain Origin

The blockchain generally comprises several fields like software engineering, distributed computing, cryptography, and game theory. Real-world blockchain applications are usually defined discussed under the umbrella of what is known as cryptoeconomics. Cryptoeconomics [26] is defined as, "a discipline concerned with the production, consumption and transfer of wealth using computer networks, cryptography, and game theory to enhance prosperity of groups in current and future digital market economies."

Blockchain is a basis of Bitcoin. Satoshi Nakamoto is considered as the inventor of blockchain. He published a research article to a cryptography forum outlining technique to counter the double-spend scenario. Early cryptocurrencies suffered from the problem of double spending. He described his technique by using a series of hashed timestamps, without explicitly defining blockchain. "Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones behind it" [23]. The original method was modified to adapt the needs of Bitcoin, and was defined as—*cryptographically linked chain of blocks, where each block uses hash digest of previous block for security*. Figure 6.2 depicts the simple structure of a blockchain.

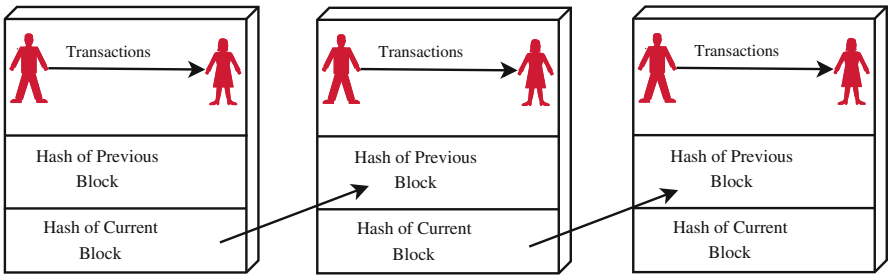

Fig. 6.2 Simple blockchain structure

To protect itself from double spending through blockchain, Bitcoin needs a methodology for its network to reach a consensus for business valuation. Therefore, a proof of work model was introduced, in which agents repeatedly hash a block with a random number until it reaches a value below the specified value. Only then will the block be added to the existing chain. Blockchain technology provided an ever-expanding collection of blocks to simplify the need for Bitcoin to record transaction order, verify the order, and secure access. Each block has a pool of transactions, and it gets linked to a high-level block after computing the cryptographic Hash Digest. The Bitcoin Network relies on a decentralized distribution and consensus model for proof of work to organize the addition of new blocks and update existing copies. Blockchain in Bitcoin acts as a database to store transactions. Bitcoin balance is not centrally managed, and no coins are printed and serialized. Users can calculate the available credit by going through the blockchain. Any attempt to change the blockchain will fail because the hash needs to be recalculated. Bitcoin was first used in January 3, 2009, by Nakamoto. He created the first block of blockchain known as genesis block. He then issued the first 50 bitcoins to himself [34].

6.2.1 Tiers of Blockchain Technology

The rapid developments in blockchain technology have led to the evolution of many applications. Based on these evolution areas and usage of blockchain, the various tiers have been categorized [34]. These functionalities and their applications are supported by majority of blockchain platforms usually with minor exceptions.

1. **Blockchain 1.0:** Introduced in 2009 along with the Bitcoin, this generation lasted till 2010. It has found its primary usage in cryptocurrencies like and has been used in applications involving payments.
2. **Blockchain 2.0:** This second generation of blockchain emerged in 2010 and finds its applications in financial sectors and smart contracts. However, its applications have expanded beyond currencies, stock markets, and finances. Different financial assets which come under Blockchain 2.0 application domain

are the derivatives, swaps, and bonds. Blockchain platforms like Ethereum and Hyperledger are considered to be the part of Blockchain 2.0.
3. **Blockchain 3.0:** Blockchain 3.0 emerged in 2012 and has found its applications in various sectors like government, healthcare, media, and justice. Since this blockchain technology tier has ability to code smart contracts, it has led to the evolution of many new blockchains apart from Ethereum and Hyperledger.
4. **Blockchain X.0:** It represents a future blockchain concept, where, public blockchain services will be available and that can be used by anybody like the Google search engine. It is expected to be a public distributed ledger with generic agents executing on the blockchain. These agents shall have the decision-making capability and can interact with intelligent and independent agents acting on user's behalf. It is also expected to be regulated by law and contracts implementable in code instead of paper.

6.3 Blockchain Categorization

Various categories of blockchain networks have been identified on the basis of their applications and access permissions. Depending on their applications, there are public, private, and hybrid variants of blockchain:

1. **Public blockchain:** Public blockchains are visible by anyone and do not have any single owner. They are fully decentralized and their consensus mechanism is open for all the users to participate in validation process. For example, Bitcoin.
2. **Private blockchain:** These blockchains use access control to manage read and write privileges for the blockchain network. A single entity has control over the ownership and block creation process. Hence, private blockchains do not usually require consensus algorithms and mining.
3. **Hybrid blockchain:** Hybrid blockchains or consortium blockchains are public only for a particular group and a few privileged servers control the consensus process. A set of agreed upon rules are used in the validation process using consensus. Additionally, only the entitled participants receive the updated copies of the blockchain. Thus, the network is only partially decentralized.

Based upon who can maintain and publish blocks in a blockchain, the two categories defined are permissionless and permissioned:

1. **Permissionless blockchains:** These networks use decentralized ledgers which allow anyone to publish the blocks, with no need of any permission from the authority. Thus, any user can read from and write transactions to the blockchain. As, these are implemented using open source software, they are highly vulnerable to the attackers, attempting to modify the transactions in the blocks. Thus, a multiparty agreement known as consensus system is utilized to prevent unauthorized access by rewarding the publishers of valid blocks with cryptocurrency.

Table 6.1 Characteristic analysis of basic blockchain

	Public blockchain	Private blockchain	Hybrid/consortium blockchain
Accessibility	Anyone	Owner organization only	Few selected and multiple organizations
Participant type	Anonymous	Known entity	Known entity
Access type	Permissionless	Permissioned	Permissioned
Security mechanism	Consensus mechanisms, Proof of Work, and Proof of Stake	Multiparty consensus and voting with pre-approved participants	Multiparty consensus and voting with pre-approved participants
Transaction speed	Slow	Light weight and fast	Light weight and fast

2. **Permissioned blockchains:** These are the networks where a centralized or decentralized authority allows the users publishing the block. Thus, it is feasible to restrict the access permissions to read and write transactions. The software used to implement these platforms can be either open or closed source. However, both permissioned and permissionless blockchain networks have the same capability to trace the digital assets passing through the blockchain. Since, they require the authentication of every user to participate as a member of the network, the consensus models used in publishing blocks do not require the expense of cryptocurrency and are faster and computationally cheaper.

Table 6.1 presents the characteristic analysis of these basic types of blockchain on various key parameters like, accessibility, type of participants and access, security levels, and transaction speed.

Based on their overall system and applications, a novel categorization of blockchains into three types has been identified [8]:

1. **Only cryptocurrency blockchain (C2C):** This type deals with only cryptocurrency chain and is totally reserved for payments or money decentralization decentralization. Bitcoin [14] introduced in 2009 is the most widely used (C2C) based cryptocurrency.
2. **Cryptocurrency to business blockchain (C2B):** This type of blockchains makes use of smart contracts, the logic tier which provides a multi-purpose programmable infrastructure. The public ledger stores financial transactions in C2B, and also facilities to deploy and execute programs on the blockchain. The tamper-proof nature of smart contracts, reduces the verification and execution costs and prevents any malicious activity. Ethereum [7] is the most widely used example of this type of blockchain.
3. **Business to business blockchains (B2B):** These blockchains do not support any currency, however, to support business logic, software execution is required. To cater to variable and distinct needs of each industry or business personalized

blockchains are required. Thus, organizations have started deploying blockchains designed to cater to their specific needs allowing them to overcome the challenges like privacy, scalability, and lack of governance, faced with other types of blockchain, These are usually implemented using Ethereum and Hyperledger.

6.4 Blockchain Working

Blockchain implements a centralized and distributed system, the distributed ledger, for storage and verification of transactions. Distributed ledger is a shared database as shown in Fig. 6.3. It is decentrally synchronized and replicated among various network users. Hence, Distributed Ledger Technology (DLT) [27], distributed across multiple computing nodes forms the backbone of blockchain. Before a transaction can be stored, it must be consented upon by majority of the users in the blockchain network. Each user in the blockchain has the most recent copy of the ledger which is updated and synchronized with any changes that occur.

A blockchain consists of several blocks with each block having many transactions. Every newly added block elongates the blockchain representing a full ledger of the transaction records. Every block in a blockchain comprises a timestamp, a random number known as nonce for verification and hash value of the previous block. These security parameters of a blockchain ensure the integrity of the overall blockchain down to the genesis block which is first block in the chain. Because of the uniqueness of the hash values, any modification made to any block in the chain will immediately get identified. Hence, any manipulation attempt in the chain is reflected and this feature makes blockchain less vulnerable to malicious attacks. All the transactions as well as the blocks are validated by most of the user nodes before adding them to the chain. This validation and consensus process is performed by special peer nodes called as miners.

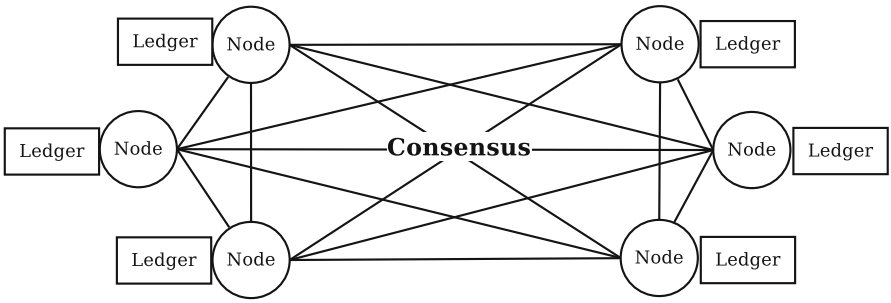

Fig. 6.3 Distributed Ledger in blockchain

6.5 Blockchain Concepts

Blockchain technology uses various digital concepts such as signatures, hashing, public-key cryptography, and transaction recording like attach-only ledgers. These key underlying functional concepts used in blockchain technology are detailed as follows.

6.5.1 Cryptographic Hash Functions

Blockchain technology employs cryptographic hashing as its underlying operational technique. Hashing is performed by implementing a cryptographic hash function on the input, to calculate a distinct message digest. It generates the identical result for the given input for each application of the hash function. Altering a single bit in data outputs an entirely dissimilar message digest. Hence, the correctness of input can be easily proven using hashing.

Cryptographic hash functions are preimage resistant, i.e., they are one-way functions. Also, these are designed to be both second preimage resistant and collision, that is, it is mathematically unattainable for dissimilar inputs to generate same output. These perform various tasks in a blockchain operation like: address derivation and creation of unique identifiers. These also secure the block data by calculating the hash value of the block data, and inserting the digest in its header. Since, a block header's digest is passed on to the succeeding block's header, its data is inherently protected when the block's header digest is passed on to the succeeding block [13, 18, 29].

A Secure Hash Algorithm's (SHA) [35] variant, having an output of 256 bits, (SHA-256), is used for blockchain implementations. It produces a 32 bytes long output which is presented as a string of 64 hexadecimal characters. SHA-256 is widely supported by many machines in hardware, which makes it fast to compute.

6.5.2 Cryptographic Nonce

A nonce is a single use number generated randomly. It is created for a specific security purpose and often modifies the result of a cryptographic function in a secret communication. Nonces are usually numbers that change over time. This prevents some values from being reused. Nonce is commonly used to send varied input to a hash function, authentication, identification, digital signatures, etc. [36]. The basic blockchain block hashing process and the associated nonce are shown in Fig. 6.4.

In the blockchain, miners create a block, verify it, and are rewarded for using their processing power. The block that receives more than 50% of the consensus is appended to the blockchain. While verification, miners provide PoW covering all

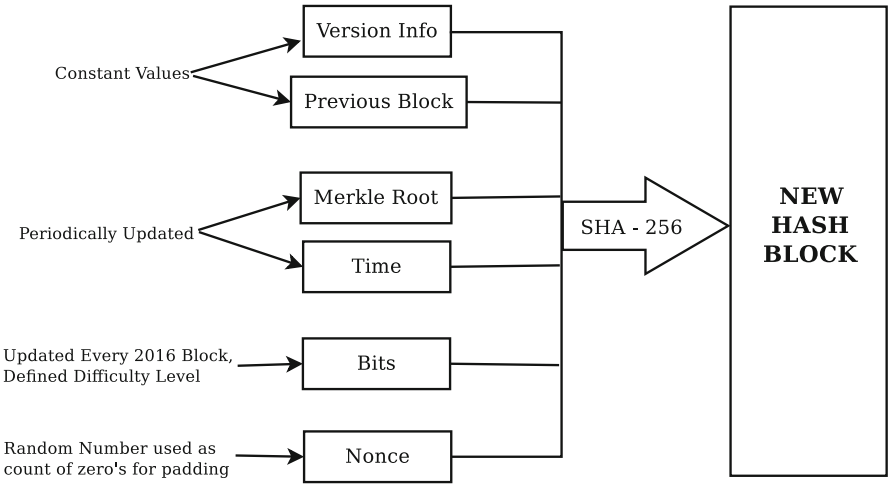

Fig. 6.4 Blockchain block hashing and the nonce

the available transactions in the block. It also checks the hash of the present block to be less than the predetermined value. To create a block that can be accepted by as many participants as possible, minors compete among themselves to provide PoW as early as possible.

The nonce is the most important for PoW. Nonce is a 4-byte random number, continuously adjusted by the miners, till it becomes valid for finding the hash value of a block. Once the perfect nonce is found, it is entered in the hashed block header. The hash value of that block is rehashed along with this number and creates a difficult algorithm. This eliminates the chances of duplicating, or exploiting the same crypto currency twice [37].

6.5.3 Transactions in Blockchain

Transactions represent the interaction between participants in a blockchain. For example, a transaction can represent the cryptocurrency transfer between the users. Every block in a blockchain has several transactions which are used by the users to send information to the blockchain network. The information sent typically includes the identifier of the sender, its public key, digital signature, and transaction inputs and outputs. A typical blockchain transaction is shown in Fig. 6.5.

The input to a transaction is the list of the digital assets to be sent. Digital assets are referenced by their sources either through the previous transaction available with the sender, or the originating event if it is a new asset. Sending the input to a transaction as a previous event reference restricts the addition or deletion of any value from the existing assets. However an asset can be bifurcated into multiple

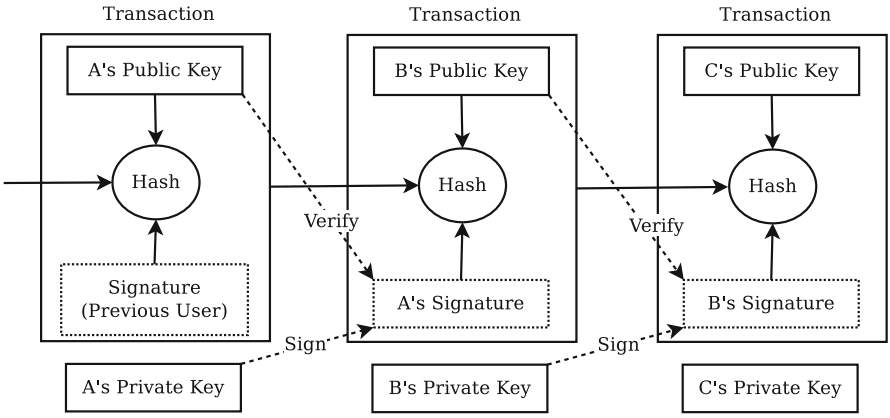

Fig. 6.5 A typical blockchain transaction

lesser value assets and, vice versa. The splitting or aggregation of assets is reflected in the transaction output correspondingly.

The outputs of a transaction are the receiving accounts' identifier, and the quantity of the asset transferred. It also specifies the various conditions to be satisfied by the new reliever/owners to be eligible to spend the received value. However, the funds received in excess of the requirement must be returned to the sender.

Furthermore, it is very crucial to validate and authenticate a transaction. Validating a transaction is a surety that the transaction adheres to the underlying protocol and data format. The authenticity of a transaction ensures that the sender is authorized to access the sent digital assets. Each sender uses its private key to sign the transactions. These digital signatures can be verified by using the public key of the sender.

6.5.4 Asymmetric Key Cryptography

Asymmetric key or public key cryptography [30], the core of the blockchain technology, uses two types of keys: public and private. The private key is available to the sender only whereas the public key is accessible to all the parties [38]. Both keys are mathematically related, however, either of them cannot be deciphered if the other one is known. User can encrypt the data with one key and needs the other one to decrypt the same.

Asymmetric key cryptography by default establishes trust between two unknown users to authenticate transactions while keeping them public. The transactions are signed using private key which can be decrypted with only the public key. As public key is accessible to all, encryption using private key confirms that the sender

is authorized to use the private key. In blockchain transactions, private keys just sign them whereas, the public keys extract the addresses and prove the signature generated by a private key.

6.5.5 Addresses

Addresses are used by the blockchain implementations to act as the sending and receiving endpoints in a transaction. An address is an alphanumeric string obtained by hashing the user's public key and other values like version number, checksum, etc. As permissionless blockchains do not require user identification for account creation, it allows a user to generate multiple addresses using multiple pairs of keys.

Blockchain users are not lone source of addresses within the network. For example in Ethereum networks, smart contracts can be accessed through a special address, the contract account address [39]. This account address facilitates the access to the smart contract after deployment. It is calculated using the smart contract owner's address and permits the execution whenever a transaction is received by it, and in turn, creates additional smart contracts.

6.5.6 Wallets

Some permissionless blockchains use a software, referred as a wallet, to secretly store their private keys. The wallet is used to securely record private and public keys, and their associated addresses. It is also used to record the number of digital assets a user is having. As recreation of private key is computationally impossible, if a user's private key is lost, all digital assets associated with it are also lost. This may result in an attacker gaining full access to all the assets that use the lost private key.

6.5.7 Digital Ledgers

A digital ledger is accumulation of transactions, oftenly stored using large databases. Owner of the ledger is a trusted third party, which manages and operates it centrally, on user's behalf. These ledgers can be centralized using single server or distributed using coordinating group of servers. However, distributed ownership of the ledger is becoming popular these days. Blockchain technology makes use of distributed ownership along with the distributed architecture for implementing the digital ledger. Distributed architecture of these networks need higher number of computers as compared to the traditional centrally managed distributed architecture.

A blockchain network is distributed by design i.e. it creates multiple copies which are all updated and synchronized to the same ledger data between the peers.

New nodes joining the blockchain network, request the latest copy of the ledger from the other users only, thereby, preventing any loss or destruction of the ledger. Blockchain network is heterogeneous, having varied types of software, hardware, and infrastructure. This heterogeneity of the nodes, guarantee for an attack on one node to have same effect on the other nodes. To provide tamper evident and resistant ledgers a blockchain network uses digital signatures and hash functions.

Distributed Ledger Technology (DLT) [16] platforms are classified mainly as permissionless and permissioned or public and private ledgers. In permissionless DLT platforms, the ledger is maintained by joint action of the nodes in the public network accessible to everyone. Here, any user can enter the network and perform block confirmation to create consensus. On the other hand, a permissioned DLT platform controls the users participating in the consensus process of the system state. Thus, the ledger is controlled by only authorized nodes and is accessible to specified users only. Permissioned DLTs allow rapid validation of transactions and provide improved privacy. Hyper Ledger Fabric [9] and R3 Cooda [5] are the popular permissioned DLTs.

6.5.8 Blocks in Blockchain

In the blockchain users put forward their transactions through various software, like desktop, web and mobile applications, e-wallets, etc. These software forward them to one or more nodes in the network. The entered transactions are further dispatched to other nodes in the network, keeping the transaction pending. A pending transaction waits in a queue before getting added to the blockchain by a publisher. A block consists of a header and data as depicted in Fig. 6.6.

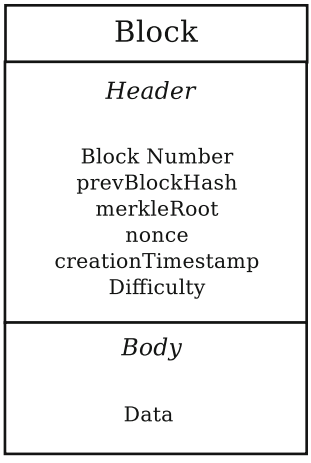

Fig. 6.6 Basic block in the blockchain

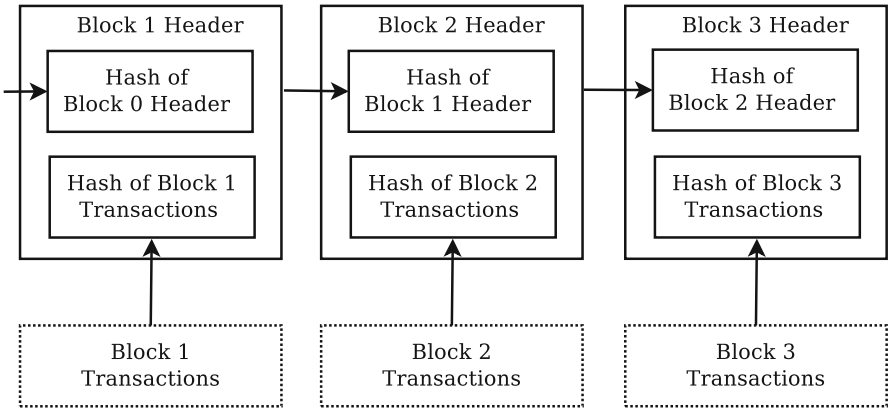

Fig. 6.7 Chaining of blocks in a blockchain

The header in the block represents the metadata for a block consists of the block number or height, hash value of preceding block header, hashed value of block data, timestamp, block size and the nonce value. Chaining of different successive blocks in the blockchain is shown in Fig. 6.7.

Block data is a list of confirmed transactions that have been published to the blockchain. The authenticity of the transaction is verified by checking the proper format and ensuring that the digital asset providers have signed the transaction. It also proves the authenticity of providers of assets to access the private key for a transaction which is used to sign them. Full nodes check the validity of all published transactions for a block and reject blocks with invalid transactions.

6.6 Consensus in Blockchain

Consensus models [32] are used in blockchains to decide upon the user who publishes the next block. In a permissionless blockchain many nodes compete simultaneously to publish the next block, in order to win the cryptocurrency. The users generally know each other only through their public addresses and have a mutual distrust among them. In such a situation, to sort out the conflicts between multiple nodes publishing a block concurrently and to allow the working of the distrusting users together, consensus models are used.

When a new user enters a blockchain, it must retrieve the system's initial state from the genesis block, which is first and the only pre-composed block. Every block is attached to the blockchain only after the genesis block is created and must agree upon the consensus model. Users can autonomously consent upon the state of the blockchain by using the initial state and verifying each block being added since then. Thus, trusted third party is not required for providing the system state. However, in

permissioned blockchain networks, there exists trust level among publishing nodes. Hence, a consensus model is not needed to decide which participant shall append the next block to the chain.

6.6.1 Poof of Work (PoW) Consensus Model

According to the PoW principle, a miner that publishes a block after solving a computationally complex problem is considered as the first miner. The result of the puzzle is considered as the proof that the user has accomplished the work. Solving this puzzle is difficult but validating the correctness of the output is straightforward. This permits all full nodes to easily authenticate any submitted block. A commonly used puzzle requires checking if the block header's hash value is lesser than a pre-specified threshold. The key aspect of PoW is that the puzzles are independent. This means that the work input to a puzzle has no impact on the probability of solving the puzzles. However, there are some major issues with the Proof of Work consensus mechanism:

- **The 51% or majority risk:** If a miner gets hold of 51% or more than 51% of the blocks, it can corrupt the blockchain by gaining the control of the majority of the network.
- **Time intensive:** Miners have to check several nonce values till they find the accurate solution to the puzzle that is required to mine the block. Since, the complexity of the puzzle is computationally very high, this process becomes very time-consuming. Also confirming a transaction is not instantaneous as it takes some time (50–60 min approx.) to mine the transaction and adding it to the blockchain.
- **Resource intensive:** Solving the puzzle to mine the block requires high computing power. Thus, miners need the machinery having high computing power. Such a machinery also consumes lot of energy.

6.6.2 Proof of Stake (PoS) Consensus Model

According to the PoS principle, the larger shares a user invests in the blockchain, the higher likelihood that it wants the system to succeed. The stake is the amount of cryptocurrency invested by a blockchain node in the system. If staked, the cryptocurrency is not available for consumption. PoS model uses this share of the user's stake as a determinant to publish the blocks. The percentage of a user's stake in the total amount staked in the network defines the probability of a user's success in publishing the block.

In PoS, since all the nodes are not competing against each other to attach a new block to the blockchain, and no computation is to be done, this save a lot on

resources and energy. Also, PoS is completely decentralized. That is, in Proof of Stake, rewards are proportional to the amount of stake. Hence, it provides absolutely no extra rewards to join a mining pool. It also ensures a secure network as a person attempting to attack a network must own 51% of the stakes which is highly expensive.

6.6.3 Round Robin Consensus Model

This model is implemented by a Permissioned Blockchain network in which nodes alternately create blocks. These systems set a timer that allows the current node to publish the block so that unavailable nodes do not delay the block's publishing. Also, it ensures that a single node does not create the bulk of the block. The Round Rodin model has the advantage of a simple, low power approach. However, they do not use crypto puzzles, and Round Robin does not work efficiently on the blockchain without permission.

6.6.4 Proof of Authority/Identity Consensus Model

The proof of authority or proof of identity consensus model is implemented in permissioned blockchains as they require very high levels of trust. In this model the publishing nodes establish trust through their real-world identities like identification documents that are usually verified and publically notarized. Publishing nodes must have their identities provable in the blockchain network. Thus, the publishing node has placed its reputation on publishing new blocks. Blockchain users can directly affect a publishing node's reputation, where it can lose or regain its reputation by acting in a mode to which other users agree or disagree. The lower the reputation of a publishing node, the less likely it is to publish a block.

6.6.5 Proof of Elapsed Time (PoET) Consensus Model

PoET is the fairest and widely used consensus model in a permissioned blockchain. In this model, every validating node on the network adds proof of their wait in the block. Based on this random waiting time only, a node gets the fair chance to create their own block. Newly created blocks are then sent to other nodes for consideration. Validator having the lowest timer value in the proof wins the consensus and its block is appended to the blockchain. A dishonest publishing node can stay back for minimum time and thus, control the system. This model uses a random wait time for the publishing node and also that it must wait for actual time and did not start early.

6.6.6 *Proof of Burn (PoB) Consensus Model*

In Proof of Burn (PoB) [19], valuators burn coins by transferring them to an address where they cannot be claimed again. Thus, they obtain the autonomy to mine on the basis of a random selection process. "Burning coins" provides authenticators a long term dedication instead of short term loss. The more coins the miner burns, the more likely he is to be selected for the mining of subsequent blocks. However, the protocol involves an unnecessary waste of resources since the mining power is directly supplied to those who burn more money.

6.7 Smart Contracts

A smart contract consists of code and data implemented by digitally signed transactions and executed by blockchain network nodes. All nodes executing a smart contract should receive the same results, which are then written to the blockchain, as shown in Fig. 6.8. Smart contracts provide publicly available functions that are performed with data provided by the user to perform a service. Since the code runs from the blockchain, it is transparent and tamper-proof and is used in various applications as a trusted third party.

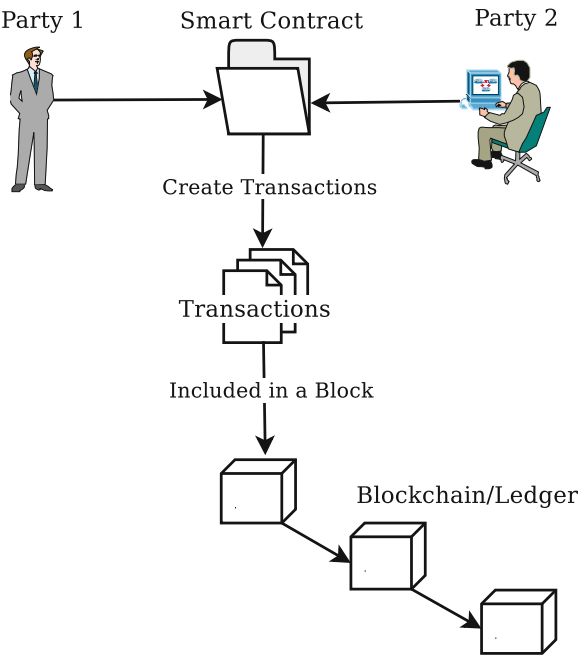

Fig. 6.8 The blockchain smart contract

A smart contract can perform many business enterprise functions including calculations, storing information, exposing properties, and spontaneous fund transfers. It also represents business process transactions involving many parties. The output of smart contracts must be predetermined for a given input. In addition to this, new state after the execution of smart contract must be accepted by all the nodes. A smart contract that operates on the data outside its system context uses an 'Oracle' [6].

In many blockchain implementations, publishing nodes execute the smart contracts concurrently while publishing the new blocks. In other implementations, the results of contract execution by other nodes are validated by only publishing nodes. In permissionless blockchain networks, the user sending the transaction to a smart contract pays the code execution cost. Further, depending upon the complexity of the code, the execution time duration dissipated by a call smart contract is restricted. The execution halts as soon as this limit is exceeded and the transaction is then discarded. This method not only remunerates the publishers for executing the smart contract, it also prevents malicious users from installing and then accessing smart contracts. Since, a malicious user can attack the publishing node and consume all the resources by deploying a denial of service.

However, in permissioned blockchain networks implementing smart contracts, trusted network avoids the users to pay towards code execution for smart contracts. The trusted participants and other mechanisms like revocation of access rights to prevent malicious behavior.

6.8 Challenges in Blockchain

In spite of having huge potential, blockchain faces multiple challenges which restrict its usage widely. Some of the major challenges faced by the blockchain network are as follows.

1. **Scalability:** As the volume of transactions is increasing, each node on a blockchain has to store and validate all the transactions to the blockchain. Further, because of the limited block size and the time interval in generating a new block, a limited set of transactions can be processed at an instance. For example, a typical Bitcoin blockchain processes approximately 7 transactions per second. Thus, it does not fit for the real time applications which require processing billions of transactions. Also, since the capacity of blocks is very less and the miners favor the transactions having higher transaction fee, several small transactions are therefore delayed.
2. **Privacy Leakage:** Blockchains can protect their privacy through asymmetric key cryptography. Users transact using private and public keys without revealing their real identity. However, blockchain does not undertake transactional privacy [33], because for each public key, the values of the transactions and balances are openly visible. Also a user's alias can be associated with its IP address even when it is behind Network Address Translation (NAT) and the firewall. In certain

cases, a client can simply be identified by a group of nodes it is connected to and which can be learned and be utilized to track the origin of a transaction.

3. **Selfish Mining:** A selfish mining or block withholding attack [21] is a malevolent attempt to disrupt the integrity of the blockchain network. In selfish mining, miner in a mining pool withholds a validated block to be broadcasted to the rest of the pool. It then continues with mining the next block, resulting in the selfish miner to present more proof of work as compared to others in the mining pool. Thus, the selfish miner affirms to the block and all financial rewards while the rest of the network take on their block solutions. A selfish miner maintains its own chain, and releases it publicly speculatively, in order to get higher rewards that would otherwise be granted based on their real contributions to the mining pool.
4. **Security:** Security aims to maintain the integrity, availability, and confidentiality of a system. Confidentiality and integrity are major concerns in distributed networks like blockchain. In such systems, availability is not an issue as replication due to replication. Since, all the transactions happening on the Blockchain have to be validated by the major chunk of miners present in the network, it makes it highly vulnerable to 51% or the majority attack as, in this situation, one miner can get the control of the chain completely.
5. **Energy consumption:** Blockchain networks, use Proof of Work mechanisms that validate transactions and add them to the network. These require highly complex mathematical calculations and hence, PoW requires large amount of energy to provide power to computers doing this task. To better understand this issue, blockchain proponents have developed many efficient consensus algorithms, like Proof of Stake (PoS), that are less taxing on energy.
6. **Integration with legacy systems:** The major challenge for corporate these days is to merge the blockchain with already existing systems. In most cases, the use of blockchain requires either complete restructuring of the existing system, or designing the ways to successfully integrate the two technologies. To replace existing system with blockchain based system will involve high cost and time. Furthermore, the blockchain technology suffers the insufficiency of specifically trained and qualified people for developing and managing peer-to-peer networks. As a result, organizations are unable to approach the desired group of blockchain professionals to take part in transition process.
7. **Regulation and standardization problems:** A major challenge faced in the implementing blockchain is the regulatory of various countries because, the decentralized structure is expected to loosen the control of centralized banks in terms of economic policies and transaction amounts. With so many different types of networks being implemented in various industrial domains, the blockchain space suffers a major issue of disarray due to absence of common standards to allow the communication between networks. This disparity across blockchain protocols also restricts technology in basic processes like security and mass adoption. Thus, creation of industry standards for different blockchain protocols can help businesses to collaborate on various fronts like application development, validating proof of concept, and sharing blockchain solutions and its integration with existing systems.

6.9 Applications of Blockchain

Blockchains have recently been adopted worldwide in different applications as decentralized mechanisms to fraud defiant computing and without a requirement of a trusted central entity. Various sectors where blockchain is contributing in a larger degree are described below [1, 4, 10, 22, 24, 31]:

1. **Financial Services:** Traditional financial systems tend to be extremely slow, cumbersome, and prone to errors. They require an Intermediary in the process mediation and conflict resolution. This results in high levels of stress and expenditure, both in terms of time and money. In contrast, users and businesses these days find the use of block chain technology as cheaper, more transparent, and cost-effective. The prominent applications of blockchain in financial sectors can be detailed as:
   (a) **Assets Management:** The asset management, where parties trade and manage resources, needs remarkable processing of confidential and expensive transactions involving more than two parties, usually in a cross boundary scenario. The parties maintain copy of their transactions. Leading to the unwanted usage of space and processing resources. Additionally, it makes the system prone to human errors, inconsistencies in the records. The distributed ledger system in the blockchain reduces such risks of errors by encrypting the records. The use of ledger further reduces the procedural complexity by omitting the need for intermediaries.
   (b) **Insurance:** Claims processing is often a difficult task for the insurance officials because of falsified cases, mounted incidents, tough clients, and many more. These significantly increase the chances of errors and misclassifications. In such scenarios, blockchain provides a perfect framework for safer processing of the cases. Use of cryptographic tools enables guarantors to make sure that processing is safe and reliable.
2. **Health Care:** Several characteristics like transparency, auditability, collaborations, no intermediation, and designing of customized models make the blockchain suitable for healthcare organizations. The scattered medical records of a patient due to visits to different medical institutions is a major issue that hinders the effective IT based healthcare. The blockchain comes to the rescue in such situations by providing platform for distributed and reliable health records maintenance and monitoring. It enables the scattered healthcare records to be integrated for tracking personal health records. Also, medical applications require stringent integrity tracing potential, privacy assurance. And the inherent intricacy of medical records makes historical diagnosis dearer. Blockchain-based solutions can provide continuous tracing of the sequence of treatment and hence, expenditures can be worked out at reduced levels.
3. **Manufacturing, Supply Chain, and retail services:** Various manufacturing, retail, and logistics industries have taken on blockchain to perform different tasks in a supply chain network. Blockchains have found their usage in transparent

movement of a product from producer to the customer in supply chains. These are also being used for product tracking and tracing during transportation and intermediary payments are implemented using various crypto currencies such as Bitcoin, etc. During the manufacturing process, blockchain-based techniques can be used to make sure that standards are adhered to and the environmental affect of the product is within limits. A decentralized blockchain-based market platforms are underway to facilitate the trading process without any mediator. In e-retail systems, blockchain-based payment gateways, loyalty programs, and gift coupons are also being designed.

4. **Intellectual Property Rights (IPR) and copyright protection:** The Internet based technologies have led to copyright issues in last two decades. From file sharing applications to photographs on the Web, copyright rules have not always been followed. As a file is replicated across the network, regular updation and reconciling of all the copies need to be done to maintain the consistency of all records. In blockchain network, with the absence of a central storage location and central authority, manipulating or corrupting the files becomes a tedious task. Since, the modifications made in the ledger can be traced down to the starting record, any illegal use of a copyrighted file can be easily detected.
5. **Governance and Identity management:** Governments at national, state, and local levels are responsible for maintaining citizen records like birth and death certificates, Universal ID's, property transfers, etc. The use of blockchain shall aid in reducing paper based record management. The efforts and time of citizens expended to visit government offices for any renewal, updation, and issuance of any such document can be saved. Further, since, the records can be traced back, applying for any new document will require least amount of information. This can further aid in filing of taxes and other financial transactions very convenient and free of unauthorized access. Blockchain can play a very crucial role in voting systems too, as the government can now ensure a tamperproof casting and counting of the votes.
6. **Smart city development:** Smart cities are the upcoming frameworks to undertake the modern day challenges of urbanization by integrating new technology planning, energy conservation, and transportation management. However, due to lack of standardization and varied requirements the technology infrastructure design can cause some challenges. Blockchain systems can be used to connect these technologies together to achieve the automation of smart cities. The key potential smart city development applications of blockchain are the smart transportation management (ride sharing and vehicle leasing), energy management(trading of energy, billing, promoting renewable energy, tracking emission footprints, etc.), waste management (financial rewards in form of cryptocurrencies for depositing non-recyclable products), governance (voting, tracking find transfers, tax management, etc.), and identity management (preventing illegal migration, identity record keeping, etc.).
7. **Blockchain for Internet of Things:** Blockchain technology has provided solutions to some of the key challenges of IoT like scalability, data management, privacy, and reliability. It has provided an efficient means to track and monitor

millions of connected devices, thereby enabling the sharing and processing of transactions between them. Being a decentralized system, it eliminates the single point of failure, generating a more flexible ecosystem for devices. With help of an efficient P2P application, large volume of transactions between interconnected devices can be processed reducing the installation and maintenance costs of large centralized data centers.

6.10 Blockchain Security Threats and Attacks

Blockchain technology is inherently secure since distributing data using a ledger across several computers, blockchains prevent any single point of failure. Moreover, use of cryptographic constructs like hashing, private keys, etc. and game theory based consensus mechanisms make a blockchain difficult to access and tamper. However, these basic safety features do not ensure the non-vulnerability of blockchain to security threats. Blockchains have exposure to their own specific set of security issues as defined below [20, 25].

6.10.1 Blockchain Structure Attacks

The potential vulnerabilities of the blockchain structures can be exploited to generate structural attacks and these can compromise the entire blockchain-based application.

1. **Blockchain Forks:** Forking is a condition arising in the network where nodes have different viewpoint about a particular state of the network which usually persists. Protocol malfunctioning and client software upgradation related incompatibilities result in creation of forks unintentionally. These can also be created by malicious actions like inserting nodes, which keep to the varying validation rules, known as Sybil nodes or by performing selfish mining. Fork is a representation of an inconsistent state which is used by the attackers to create ambiguous system state, illicit transactions, and mistrust in the network.
2. **Stale and Orphaned Blocks:** Consensus process can result in two major types of inconsistencies leaving valid blocks out of blockchain, stale blocks and orphaned blocks. A stale block was well mined; however, it was not adopted in the blockchain. These occur often in the public blockchains because of the race condition where, miners compete to look for the next valid block with two or more miners being able to find a valid solution. In such situation, the network goes for one of the winner blocks and scraps the remaining. Hence, remaining blocks that are valid but unaccepted and added to the current blockchain become stale blocks. On the other hand, a block where hash of the parent block pointing to an invalid block and is rejected from the blockchain, becomes an orphan block. Orphaned blocks can either be inserted by an attacker or is the resultant of the race conditions among the miners.

6.10.2 Blockchain's Peer-to-Peer System Attacks

Blockchain network can ensure security and accessibility due to its peer-to-peer architecture. On the contrary, this architecture makes a blockchain network vulnerable to different attacks like selfish mining, 51% attack, Distributed Denial of Service (DDoS), and DNS attacks, eclipse attacks, and consensus delay.

1. **Selfish Mining:** Here malicious miners try to increase rewards by privately holding their blocks. In this attack, the dishonest miners hide the data by keeping back a mined block and harm truthful miners by a twofold process: (a) Acquiring an unfair higher compensation than deserved, and (b) confusing others by eventually forcing them to deplete their resources. Selfish mining affects all applications since the miners are the only ones to add the blocks into the blockchain. Thus, addition of genuine blocks becomes difficult if miners are involved in withholding valid blocks and adding invalid blocks.
2. **The Majority or 51% Attack:** It is the most common security threat to the blockchain system. This is realized when a set of Sybil nodes, a mining pool or a single attacker, achieves most of the network's hash rate to control the blockchain. By gaining the maximum hash rate, these nodes can harm the network by:

   (a) Making blocks invalid by preventing transactions being verified,
   (b) Allowing double spending by reversing the transactions while they are under their control,
   (c) Splitting the network by forking the main blockchain, and
   (d) Preventing rest of the miners from finding any blocks for a brief time.

3. **DNS Attacks:** A new node joining the blockchain network discovers its peers identified by the IP addresses using the Domain Name System (DNS). The reply to a DNS query returns type A-records containing the addresses of available peers ready to connect to the blockchain. As the upcoming node connects with the peers, it sends its IP address and port number to establish connections with other peers. The DNS resolution process is prone to man in the middle attacks, cache poisoning, and stale records at the resolver side.
4. **BGP hijacks and spatial partitioning:** Most blockchain applications have two types of nodes: full nodes and lightweight nodes. Full nodes perform the relaying of blocks and transactions and maintenance of an updated copy of the blockchain. Whereas, the services of the full nodes are utilized by the lightweight nodes, in accessing the network and creating their picture of the blockchain. Therefore, exploiting a full node compromises all its associate lightweight nodes. Spatially concentrated nodes within an Autonomous system (AS) or an Internet Service Provider (ISP) are highly vulnerable to the routing attacks, like BGP hijacking. Here, an adversary AS hijacks the traffic to a destination AS hosting the blockchain application nodes. Thus, the information being sent to other nodes in the target AS is disrupted. If targeted nodes are among the miners, the

malicious node can reduce the rate of the blockchain hashing, hence, hitting the smooth network functioning.

5. **Eclipse Attacks:** In eclipse attack [28], a set of attacker nodes isolate its neighbor nodes by using their IP addresses and compromising the traffic. When, such malicious nodes surround the honest nodes, they become susceptible to the eclipse attack. Malicious nodes feed these nodes with fraudulent transactions and blocks resulting in them developing the wrong picture of blockchain state and becomes the part of the cluster having malicious nodes. When a trusted node connects to this cluster, it also propagates fake transactions and blocks, without knowledge.
6. **Distributed Denial of Service Attacks (DDoS):** In blockchain system, DDoS attacks [28] are realized in many ways as per the structure of the network, applications and participating peers. Out of total attacks, 51% attacks are denial of service attacks. Some miners gain access to immense hashing power and restrict other sets of miners from publishing new blocks. Also, the intentional forks can convert into hard forks, causing denial of service. Another possible attack, known as stress testing, limits the number of transactions per block processed by a blockchain application in a given time. Mempool flooding is also a DDoS attack that is performed at the cryptocurrency memory with an intention to shoot up the mining fee.
7. **Block Withholding Attacks:** In this attacker, a malicious node creates a contradictory view of the blockchain. With this, the attacker can forge, mask, or hold back the data that is required to be communicated. This type of attacks are also known as Finney Attacks. The Finney attack is a form of the double-spending attack where, a miner induces additional delays to double his share of cryptocurrency benefit for a transaction [40]. Fork after withholding (FAW) [19] is more rewarding than block withholding attacks, since, a malicious miner attaches itself to two mining pools and computes a valid Proof of Work in one mining pool. However, he holds back its solution and publishes this block after the second mining pool adds the block. One of the available block gets selected by the network and the dishonest miner is rewarded in any case.
8. **Consensus Delay:** Here, an attacker places the incorrect blocks in the blockchain and introduces the latency intercepting the peers from reaching consensus. The delays introduced in blockchain include authentication time delay, transmission delay and propagation delay in messages and block transmission. While the former category is dependent on the size of block, the latter one depends upon link bandwidth between the nodes. Thus, attackers can introduce intentional delays in the network by sending stale blocks and double spent transactions.
9. **Timejacking:** An attacker can alter a node's network timer by encompassing majority of peers and broadcasting the incorrect timestamps in the network. This speeds up the peers and cuts off the target out of the network without intervention of the legitimate nodes.

6.10.3 Application Based Attacks

In this section, we discuss the possible attacks on blockchain applications. Depending upon the type of application, blockchain networks suffer from various threats and a significant number of attacks exist which can be detailed as:

1. **Blockchain Ingestion and Anonymity:** Public blockchains are usually less anonymous, and provide easier data access for the public. Thus, analyzing the public blockchain can let out sensitive information to an opponent, which is commonly called as blockchain ingestion. Ingestion of blockchain is usually not useful to underlying application and the users. Anonymity in cryptocurrencies also gives worthwhile chances to attackers to carry out fraudulent activities. The tamper-proof, append only and decentralized nature of blockchain where a committed transaction is reversible, results in several irreparable scam activities online. Here, the users are misled to send money through wallets and the lack of central authority further makes it difficult to notify the fraud and look forward to payment reversal.
2. **Double Spending:** In this attack, the same digital currency is spent more than once. That is, it is an instance in which two transactions use the same input and one of them has already been broadcast on the network. A malicious user can realize double spending by sending two contradicting transactions in prompt succession. Hence, same bitcoins are spent redundantly in multiple transactions. These two transactions are carried out in a very close time interval. For example, an unfair customer can transact at time t1 using some bitcoins with a recipient address of a producer. The client publishes this transaction information at time t2 considering that t1 and t2 are close enough. It makes another redundant transaction at t2 with same set of coins and recipient address as his own address or the address of the wallet under his control. Hence, if the unfair customer is able to dupe the merchant with this transaction, the purchased products are delivered to him, with merchant never receiving the payment.
3. **Cryptojacking:** In cryptojacking or covert mining, cloud and web-based services are exploited to illegitimately perform the Proof of Work (PoW) consent [41]. The in-browser cryptojacking, websites are turned into the mining pools which further enhance their hashing capacity by collaborating with other miners and buying high-performing hardware with ample resources. Consequently the mining process becomes more expensive and competitive, preventing small scale miners from mining the blocks singly.

   In cloud-based cryptojacking, malicious miners attack the system by restricting the working of trusted nodes and virtual machines for mining and thus, exhausting cloud resources. Web-based cryptojacking is performed by attackers by injecting harmful JavaScript code in websites. In browser-based cryptojacking, browser on the client machine executes a JavaScript code which creates a Web Socket with a remote system. The server then asks client to compute hashes for the PoW and transmitting them back. This computation task requires a lot of resource, resulting in excessive usage of CPU and battery exhaustion.

4. **Wallet Theft:** Digital wallets store credentials of the nodes present in the blockchain network. In many blockchains, the wallet is stored non-encoded, thereby, permitting an opponent to access the credentials linked with it and also type of transactions issued. Although a wallet is secured, instigating an attack on the host allows the opponent to perform wallet theft. Moreover, there are various third party services that enable storage of wallets, compromising them can leak the wallets to an adversary.
5. **Replay attacks:** It involves implementing same transaction on two separate blockchains [41]. For example, when forking occurs in a blockchain, it separates into two different chains and the users hold equal resources on both the ledgers. It can make a transaction on either of the available chains. Here, the attacker gains access to the transaction information available in one ledger and repeats the same transactions on other, thereby making a user lose its assets on both the chains.

6.11 Blockchain Prospects for Internet of Things (IoT)

The Internet of Things (IoT) interconnects people, products, and places and provides freedom for value creation. Several micro level sensing elements, chips, and actuators are inserted into physical items, each sending data to the IoT network, which is analyzed to convert insights into action. However, there are several technical and security issues in IoT systems that need to be addressed. Security concerns in IoT systems have shadowed its mass deployment. IoT devices usually suffer from security threats which makes them an easy victim of Distributed Denial of Service (DDoS) attacks. Scalability is yet another key issue with IoT networks. With the exponentially growing number of devices communicating via an IoT network, centralized systems used currently to connect, authenticate, and authorize different nodes will turn into a processing bottleneck.

Blockchain with its underlying Distributed Ledger Technology (DLT) is capable to address these challenges in the following ways [12]:

- Tamper-proof nature of the distributed ledger in a blockchain system alleviates the need to establish trust among the users. Moreover, no standalone entity shall control the enormous volume of data created by IoT devices.
- Storing IoT data over blockchain shall add an extra layer of security for the adversaries to bypass before accessing it. Since, blockchain provides a robust level of encryption deleting or modifying existing data records is nearly impossible.
- Blockchain is transparent as it allows only authorized users to gain access to the network and enable them to trace the transactions that occurred in the past. It also aids in identification of the source of any data leakages.
- Blockchain can facilitate the speedy processing of transactions and synchronizing billions of connected devices. With the increase in number of such devices, the DLT technology provides a feasible solution for processing large number of transactions efficiently.

- Enabling the trust among users, blockchain can help IoT based enterprises to reduce their costs by reducing the processing and communication overheads associated with IoT gateways.

Thus, the future blockchain enterprise areas where IoT can be combined with blockchain can be outlined as in [2, 17, 42], supply chain management and logistics and transportation, automated industry, smart homes, cities and agriculture, sharing economy and pharmacy industry.

6.12 Conclusion

With the progressing computer technologies, several things that seemed impossible have been realize, the prominent ones being the contactless operations, cashless payments, e-commerce, and cryptocurrencies. Secured online payments with no added fee have influenced all the economic industries and have been made possible due to blockchain solutions. Blockchain is expected to prove its worth in modifying traditional industry owing to its main characteristics like decentralization, persistence, anonymousness, and verifiability. Thus, the blockchain technology needs to be introduced with an objective to bring operational efficiencies and the proper implementation of the blockchain technology is expected to have wider and more progressive implications.

References

1. A.B. Ayed, M.A. Belhajji, The blockchain technology: applications and threats, in *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications* (IGI Global, New York, 2020), pp. 1770–1781
2. A. Banerjee, Blockchain with IoT: applications and use cases for a new paradigm of supply chain driving efficiency and cost, in *Advances in Computers*, vol. 115 (Elsevier, Amsterdam, 2019), pp. 259–292
3. I. Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained* (Packt Publishing Ltd, Birmingham, 2018)
4. U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for industry 4.0: a comprehensive review. IEEE Access **8**, 79764–79800 (2020)
5. R.G. Brown, The Corda platform: an introduction. Retrieved **27**, 2018 (2018)
6. J. Buck, Blockchain oracles, explained. Cointelegraph, October, vol. 18 (2017)
7. V. Buterin et al. *A Next-Generation Smart Contract and Decentralized Application Platform*. White Paper **3**(37) (2014)
8. V. Buterin, A. Todd, G. Nguyen, A. Rosic, P. Westerhof, J. Beranger, A. Guerra, C. Mulder, M. Urling, S. Andonov et al. *What are Smart Contracts? A Beginner's Guide to Smart Contracts* (2016)
9. C. Cachin et al. Architecture of the hyperledger blockchain fabric, in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, vol. 310 (2016)

10. W. Chen, Z. Xu, S. Shi, Y. Zhao, J. Zhao, A survey of blockchain applications in different domains, in *Proceedings of the 2018 International Conference on Blockchain Technology and Application* (2018), pp. 17–21
11. A.S. Chhabra, T. Choudhury, A.V. Srivastava, A. Aggarwal, Prediction for big data and IoT in 2017, in *Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)* (IEEE, New York, 2017), pp. 181–187
12. H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: a survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019)
13. V. Fore, A. Khanna, R. Tomar, A. Mishra, Intelligent supply chain management system, in *Proceedings of the 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE)* (IEEE, New York, 2016), pp. 296–302
14. W. Gao, W.G. Hatcher, W. Yu, A survey of blockchain: techniques, applications, and challenges, in *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)* (IEEE, New York, 2018), pp. 1–11
15. G. Garg, S. Sharma, T. Choudhury, P. Kumar, Crop productivity based on IoT, in *Proceedings of the 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (IEEE, New York, 2017), pp. 223–226
16. S. Kadam, Review of distributed ledgers: the technological advances behind cryptocurrency, in *Proceedings of the International Conference Advances in Computer Technology and Management (ICACTM)* (2018)
17. M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)
18. A. Khanna, A. Sah, T. Choudhury, Intelligent mobile edge computing: a deep learning based approach, in *Proceedings of the International Conference on Advances in Computing and Data Sciences* (Springer, Berlin, 2020), pp. 107–116
19. Y. Kwon, D. Kim, Y. Son, E. Vasserman, Y. Kim, Be selfish and avoid dilemmas: fork after withholding (FAW) attacks on bitcoin, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017), pp. 195–209
20. X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
21. M.H. Miraz, M. Ali, Applications of blockchain technology beyond cryptocurrency (2018). arXiv preprint arXiv:1801.03528
22. A.A. Monrat, O. Schelen, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
23. S. Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System. Technical report, Manubot (2019)
24. M. Pilkington, Blockchain technology: principles and applications, in *Research Handbook on Digital Transformations* (Edward Elgar Publishing, Cheltenham, 2016)
25. M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, A. Mohaisen, Exploring the attack surface of blockchain: a systematic overview (2019). arXiv preprint arXiv:1904.03487
26. K. Sultan, U. Ruhi, R. Lakhani, Conceptualizing blockchains: characteristics and applications (2018). arXiv preprint arXiv:1806.03693
27. F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials **18**(3), 2084–2123 (2016)
28. M. Vasek, M. Thornton, T. Moore, Empirical analysis of denial-of-service attacks in the bitcoin ecosystem, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, 2014), pp. 57–71
29. A. Verma, A. Khanna, A. Agrawal, A. Darwish, A.E. Hassanien, Security and privacy in smart city applications and services: opportunities and challenges, in *Cybersecurity and Secure Information Systems* (Springer, Berlin, 2019), pp. 1–15
30. L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains. J. Network Comput. Appl. **127**, 43–58 (2019)

31. J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Commun. Surv. Tutorials **21**(3), 2794–2830 (2019)
32. D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain technology overview (2019). arXiv preprint arXiv:1906.11078
33. Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
34. A. Zohar, Bitcoin: under the hood. Commun. ACM **58**(9), 104–113 (2015)
35. https://en.bitcoinwiki.org/wiki/SHA-256
36. https://paybis.com/blog/what-is-a-blockchain-nonce/
37. https://www.tutorialspoint.com/what-is-a-nonce-in-block-chain
38. https://www.tutorialspoint.com/difference-between-private-key-and-public-key
39. https://ethereum.stackexchange.com/questions/760/how-is-the-address-of-an-ethereum-contract-computed
40. https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack
41. https://hackerbits.com/programming/what-is-cryptojacking/
42. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/IoT-powered-by-Blockchain-Deloitte.pdf