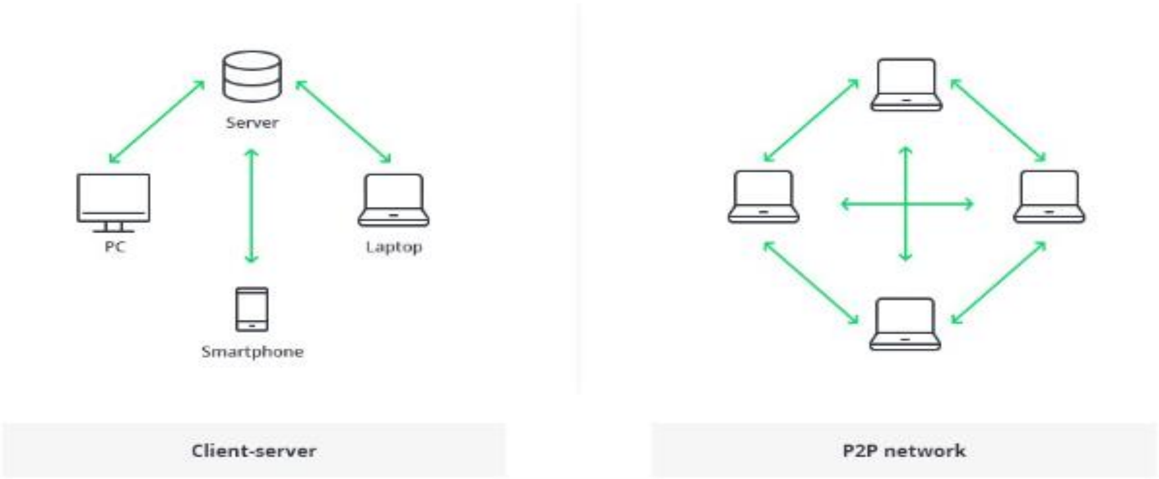
UNIT 2 COMPONENETS AND STRUCTURE OF BLOCKCHAIN

Blocks – Chain between the blocks – Digital signatures and Hashing – Block data examples: Bitcoin block, Ethereum block, Block time and Block size, Global Size – Blockchain miners and validators – Blockchain speed: Blockchain throughput and comparison with traditional network

BLOCKS:

The blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that is grouped together in a network (peer-to-peer). In other words, blockchain is a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized.To make it even simpler, the blockchain concept can be compared to working on the same Google Doc simultaneously.



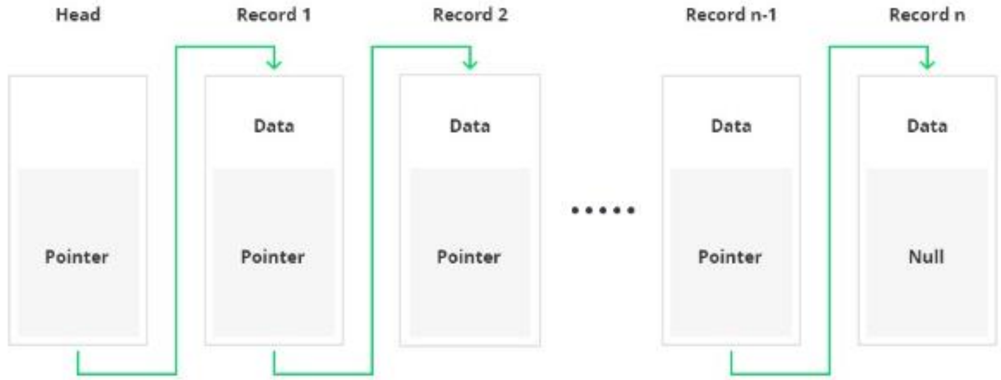
Database vs Block Chain

The traditional architecture of the World Wide Web uses a client-server network. In this case, the server keeps all the required information in one place so that it is easy to update and controlled by a number of administrators.

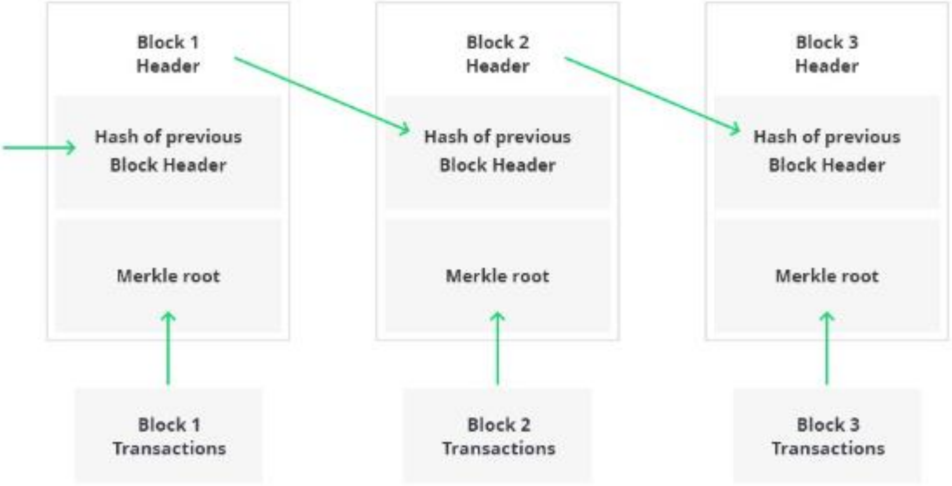
In the case of the distributed blockchain network, each participant within the network maintains, approves, and updates new entries.

The structure of blockchain technology is represented by a list of blocks with transactions in a particular order. Two vital data structures used in blockchain include:

- Pointers — variables that keep information about the location of another variable
- Linked lists — a sequence of blocks where each block has specific data and links to the following block with the help of a pointer



Basically, the following blockchain sequence diagram is a connected list of records.

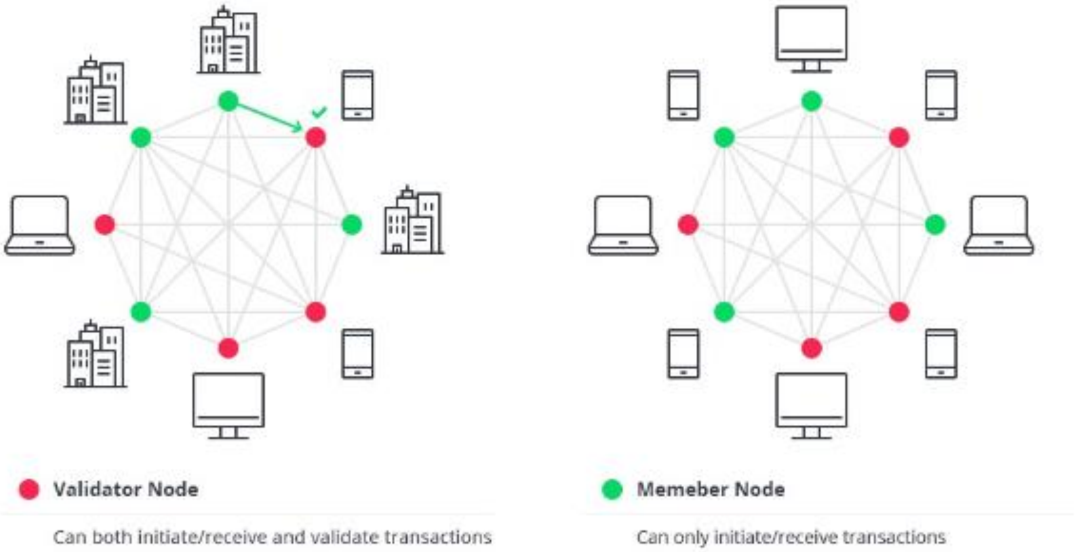


Blockchain can serve the following purposes for organizations and enterprises:

- Cost reduction

- History of data
- Data validity & security

Types of Blockchain Explained:


Validator Node
Can both initiate/receive and validate transactions
Memeber Node
Can only initiate/receive transactions

All blockchain structures fall into three categories:

- Public blockchain
- Private blockchain
- Consortium blockchain

Core Components of Blockchain: How Does It Work

These are the core blockchain architecture components:

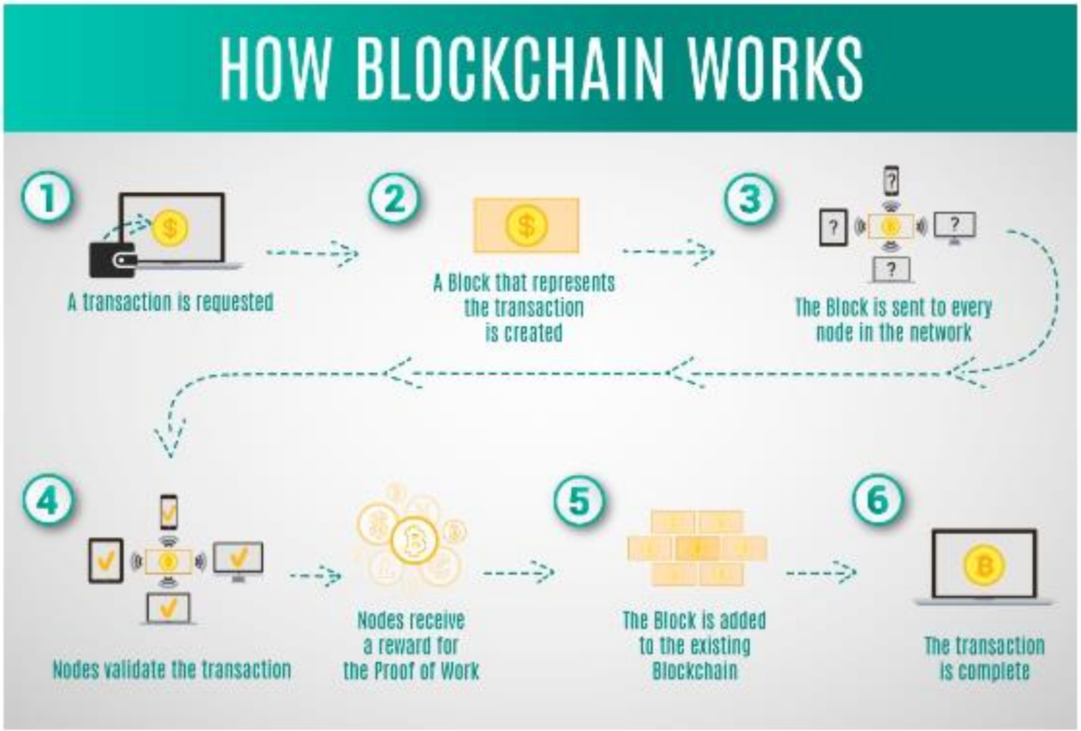
- **Node** — user or computer within the blockchain
- **Transaction** — smallest building block of a blockchain system
- **Block** — a data structure used for keeping a set of transactions which is distributed to all nodes in the network

- **Chain** — a sequence of blocks in a specific order

- **Miners** — specific nodes which perform the block verification process

- **Consensus**— a set of rules and arrangements to carry out blockchain operations

The following is a blockchain diagram that shows how this actually works in the form of a digital wallet.


HOW BLOCKCHAIN WORKS
1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Let’s have a closer look at what is a block in a blockchain. Each blockchain block consists of:

- certain data

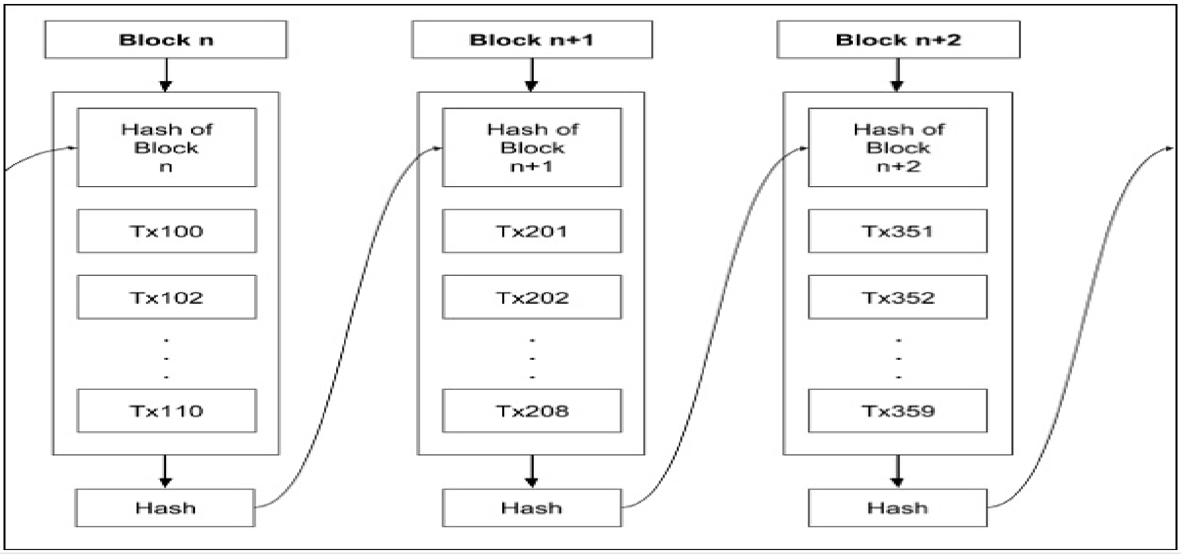
- the hash of the block

- the hash from the previous block

On the other hand, in theory, it could be possible to adjust all the blocks with the help of strong computer processors. However, there is a solution that eliminates this possibility called **proof-of-work**. This allows a user to slow down the process of creation of new blocks.

Chain between the blocks:

The blocks created by various miners are chained together to form what is known as a truly distributed public ledger.



Each block in the chain contains multiple messages (transactions) as seen earlier in Figure 8. A block in the chain may come from any miner. While creating the chain of blocks, we observe the rule that hash of the previous block is added to the current block.

Thus, a miner while creating the block, picks up the hash of the last block in the chain, combines it with its own set of messages and creates a hash for its newly created block. This newly created block now becomes the new end for the chain and thus the chain keeps on growing as more and more blocks are added to it by the miners.

Hashing and Digital Signature in the Blockchain:

Hashing and Digital Signature are the important terms that bring desired security level in blockchain with **cryptography.**

Security is one of the prominent requirements in the present times, with businesses wondering about innovative approaches for safeguarding information. One of the most innovative solutions that have emerged recently for helping businesses in secure information exchange points towards blockchain. Blockchain technology brings functionalities of distributed ledger and ensures that unauthorized parties couldn't see the information exchanged in a specific transaction.

It uses cryptography to provide the desired security while bringing attention towards hashing and digital signature in blockchain.

Both **hashing and digital signature** have a huge role to play in the blockchain landscape

The most important aspect in discussions around hashing and digital signature in blockchain primarily revolves around cryptography. **Communication** has evolved gradually over the years as we have come from pictograms to flash storage devices storing massive information. However, communications have always been following best practices of encryption to ensure that information is not visible to other individuals.

Therefore, cryptography emerged as a vital solution for ensuring safeguards for sensitive information. Cryptography involves **scrambling** the original content of the message to a **cipher** before sending it to the recipient. The recipient could use keys for unlocking the cipher, and the keys are available only with the recipient. Therefore, any other party couldn't intercept the communication in the course of its journey from sender to recipient.

Blockchain relies largely on cryptography as a major selling point. It is also interesting to note the **definition of hashing in blockchain** and the **role of digital signatures** in understanding how they fit in the blockchain equation. Let us start with hashing first.

Hashing is the process of taking an unlimited amount of input data and leveraging it for the creation of specific amounts of output data. The input data does not have any fixed size, thereby offering considerable flexibility in the selection of inputs for hashing. In addition, the importance of hashing in blockchain security is visible in the requirement of hashing for adding blocks. You should also note that there are various hashing algorithms tailored for varying requirements of users.

Interestingly, hashes have found a wide range of applications in various use cases, with the most prominent example referring to digital fingerprinting. Digital fingerprinting is just the same as an actual fingerprint, and the hashing in digital fingerprints serves as the best instrument for verifying the fingerprint.

The hash helps in offering confirmation regarding the production of output from the hashing procedure. In addition, the hash also confirms that the output of the procedure has not been subject to any unwanted tampering. The verification process generally involves calculations for confirming matches between hashes and the originally published content. Any form of mismatch could clearly showcase evidence of modification or tampering in the output hash.

- **Applications of Hashing in Blockchain**

The use of hashing in blockchain in such cases points out clarity on tamper-proofing. Every new blockchain begins with a genesis block which is responsible for capturing data regarding almost anything that has happened on the blockchain to date. As a result, the output of a hash function directly points out the most recent state of the concerning blockchain.

It is also important to note that activities are added subsequently to the chain as they happen. Most important of all, the new blocks always capture details associated with the previous block. Any form of modification could change the hash of the chain, thereby helping in easier and precise identification.

Hashing in cryptography and blockchain is primarily a one-way function that features a properly crafted algorithm without any concerns for reversal of hashing process and exposure of original input. Therefore, hashing can provide a substantial advantage over the two-way function in encryption that enables encryption and decryption through the suitable keys or key-pairs.

Another profound application of hash functions is clearly evident in data structures where you can find bloom filters or hash tables. In such cases, the objective of hashing focuses on faster data lookup rather than security. On the other hand, hash functions also find applications in the context of digital signatures where they are ideal for producing the same output for the same input with a deterministic approach.

As a result, the use of hashing and digital signature in blockchain could help recipients in recomputing the output of a hash function with the same hash function. The comparison of the message digest with the transmitted digest could help in verifying that the message didn’t go through unwanted modifications in transit.

Even if the message features minor differences in punctuation, content, or spacing, the message digest in the output would have radical differences. In addition, it is difficult to find out the level of difference between two different messages through comparison of the digest. As you must have understood, the smallest difference in inputs could result in a completely unique digest value.

So, it is quite clear that hashing has a formidable significance for cryptography in the blockchain. However, the applications of hashing in blockchain have to follow certain important requirements such as,

1. Input could feature variable length
2. Output must have a fixed length
3. The hash function for any specific input presents relative ease of computing
4. Hash function features the collision-free trait, which ensures that you could not have two different messages that produce a similar hash value.
5. Hash function is always one-way and clearly implies the extreme difficulty associated with determining the input by referring to the output.

Hashing Algorithms:

The secure hashing algorithm or SHA is the most common hash function recommended by the National Institute of Standards and Technology (NIST). The notable successors of SHA such as SHA-1, SHA-2, and SHA-3 have gained profound recognition for their capabilities.

SHA-1 could take input of practically any length and then generate a 160-bit message alongside processing messages in blocks of 512-bit size. If message length is not a multiple of 512-bit, then the SHA algorithm could pad up the message with data so that it could reach the next closest multiple of 512-bit.

SHA-2 is presently one of the favorite algorithms in the cryptography community, although with certain setbacks like in the SHA-1 algorithm. After its introduction in 2001, SHA-2 has been through substantial changes over the years with the arrival of four variants. The four different variants include SHA-256, SHA-224, SHA-512, and SHA-384, with SHA-256 being a widely adopted cryptographic algorithm.

SHA-256 can create a 256-bit message digest through the use of 512-bit block size, while SHA-224 utilizes a truncated version of SHA-256 for creating a 224-bit message digest using the 512-bit block size. SHA-512 could create a 512-bit message digest by using the 1024-bit block size, and SHA-384 utilizes a truncated version of SHA-512. SHA-384 can generate a 384-bit message digest by leveraging a 1024-bit block size.

The SHA-3 algorithms are the latest additions in secure hashing algorithms showing the importance of hashing in blockchain. SHA-3 came into existence in 2015 and fall on the same lines as MD5 algorithm standards. It has the capability to serve as a replacement for SHA-2 while also offering similar variants and hash lengths. The only difference of SHA-3 is that it presents possibilities of better security.

MD2- Message Digest

The MD2 Message Digest algorithm came forward in 1989 as an alternative for offering secure hash functions for 8-bit processors. MD2 helps in padding up the message to the length of multiples of 16-bit and the creation of a 16-byte checksum.

MD4 is an enhanced alternative to MD2 and provides padding for a message to a length that is 64-bit smaller than 512-bit multiples. Subsequently, it could process 512-bit blocks of the message in different rounds for producing a 128-bit message digest.

MD5 is the latest version of message digest algorithm and could offer the same padding requirements as MD4. In addition, it brings some additional security features which end up reducing the speed of producing message digest.

Digital Signature in Blockchain:

Definition:

- A digital signature is a mathematical scheme that is used to authenticate the sender of an electronic document .
- A digital signature is nothing but an attachment to any piece of electronic information, which represents the content of the document and the identity of the owner of that document uniquely

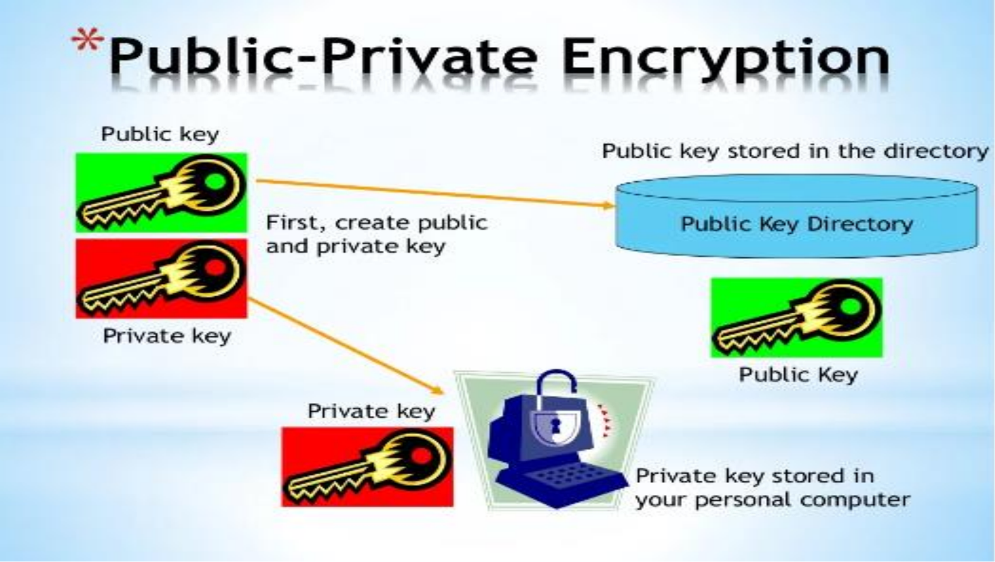
Objective:

- To provide Authenticity, Integrity and Non-repudiation to electronic documents.
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance

Requirements

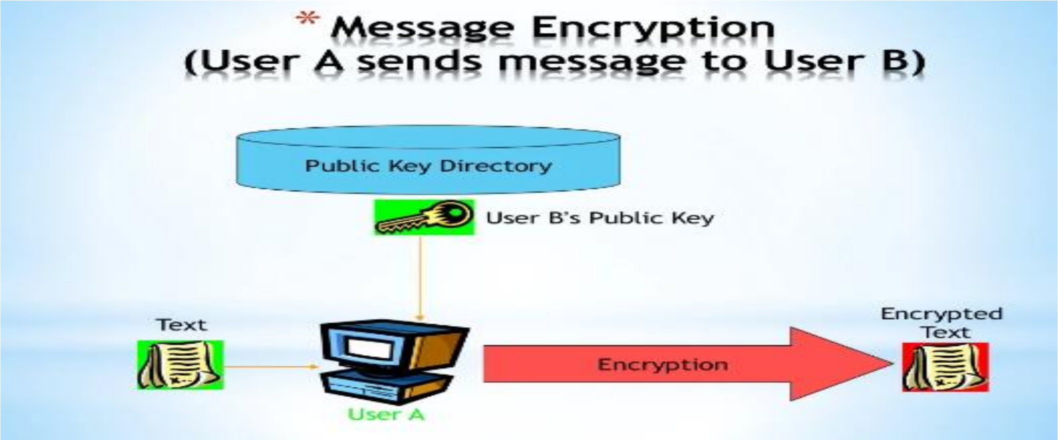
- Private Key is one which is accessible only to the signer.
- It is used to generate the digital signature which is then attached to the message.

- public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message

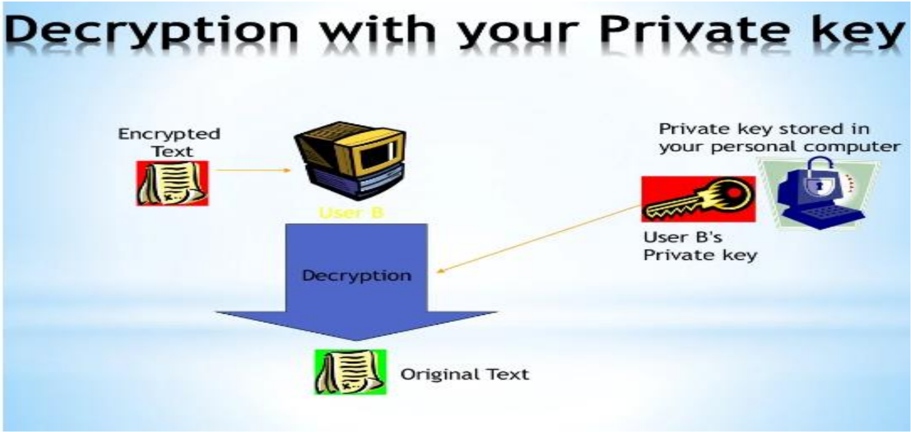


*Public-Private Encryption

Public key
Public key stored in the directory
Public Key Directory
First, create public and private key
Private key
Public Key
Private key
Private key stored in your personal computer

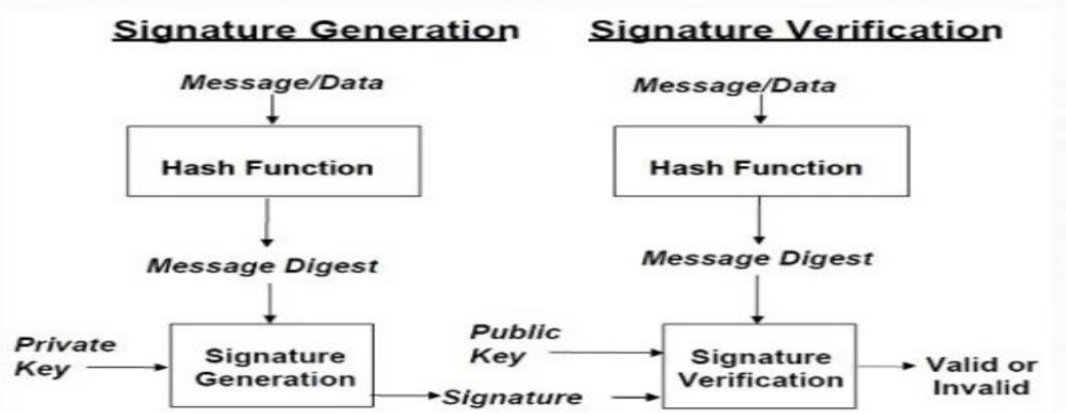


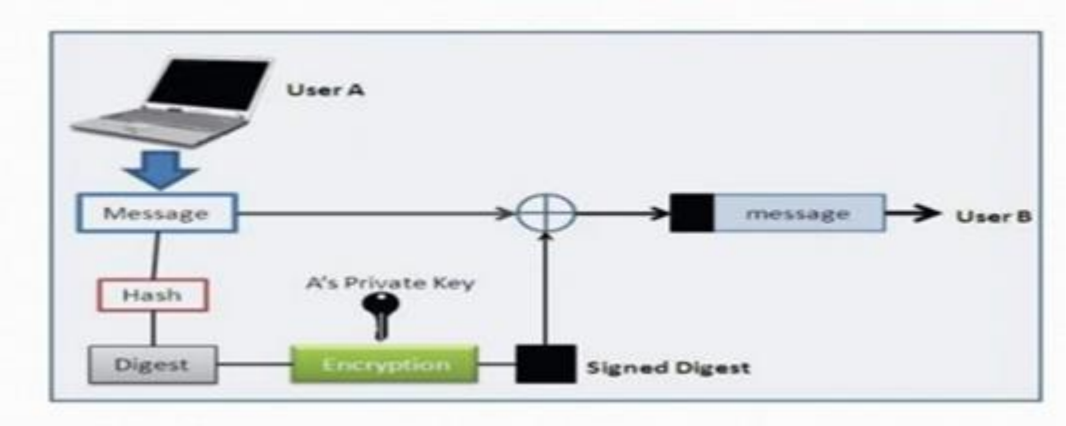
* Message Encryption (User A sends message to User B)


Decryption with your Private key
Encrypted Text
User B
Private key stored in your personal computer
User B's Private key
Decryption
Original Text

Digital certificate

- A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber.
- But in case of any dispute between the two sides, there must be some entity with the receiver which will allow the receiver of the message to prove that the message was sent by the subscriber of the key pair.
- This can be done with the Digital Signature Certificate





Application:

- Electronic Mail
- Data storage
- Electronic funds transfer
- Software Distribution
- Smart Cards
- ISDN
- Time Stamped Signature

- **Authentication:**

Identification of the person that signs.

- **Integrity of data:**

Every change will be detected.

- **Non repudiation:**

Because the author cannot be denied of his work (he created and sent).

- **Imposter prevention:**

Elimination of possibility of committing fraud by an imposter Advantages

Disadvantages:

- **Expiry:** In this era of fast technological advancements, many of these tech products have a short shelf life.
- **Certificates:** In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates.
- Digital signatures are difficult to understand.
- Digital signatures will be championed by many players that the public distrusts, including national security agencies, law enforcement agencies, and consumer marketing companies

Relationship between Hashing and Digital Signatures

Now that you know ‘what is hashing and digital signature in the blockchain?’ it is important to find out the link between them. In the case of blockchain, a digital signature system focuses on three basic phases such as hashing, signature, and verification. Let us take a look at the working of a blockchain-based digital signature.

- **Step 1:** First of all, the blockchain hashes the message or digital data through the submission of data via a hashing algorithm. The algorithm helps in generating a hash value or the message digest with messages differing profoundly in size only to give the same length of hash values upon hashing. As we already know, this is the most fundamental trait in a hash function and exhibits a clear influence on digital signatures. Hashing is mandatory in most blockchain applications for the flexibility in using fixed-length message digests for the complete process.
- **Step 2:** The next step in the working of digital signature in blockchain refers to signing. The sender of the message must sign it after hashing of information in the message. At this point of the process, public key cryptography plays a critical role. Many digital signature algorithms offer unique mechanisms, albeit with the single approach of asymmetric cryptography. Since digital signatures are related directly to the content in each message, digitally signed messages are likely to have different digital signatures.
- **Step 3:** The final step in the use of blockchain-based digital signature refers to verification. Recipients could easily check the validity of digital signatures through the use of a public key. The signature could work as a unique digital fingerprint of the concerned message. However, it is also important to pay attention to the secure storage and management of keys for avoiding unwanted circumstances.
- The applications of digital signature in blockchain could help in achieving the important results of non-repudiation, authentication, and data integrity. As a result, hashing and digital signatures have prominent contributions in improving the security of blockchain applications.

Block Time:

Block time is the measure of the time it takes the miners or validators within a network to verify transactions within one block and produce a new block in that blockchain.

Blockchains were first popularized by Bitcoin when it was introduced in 2009. The technology has grown as more cryptocurrencies are created, each of which can use different or the same blockchain, validation methods, and techniques for creating new blocks.

Understanding Block Time

A blockchain is a distributed database that records all transactions within a cryptocurrency network. You can think of a block within the database as a cell in a spreadsheet where transaction information is stored. Miners verify the transactions, which takes time because finding the solution to the block requires the computers to make a vast amount of trial and error calculations.

This is called hashing—using an algorithm to verify all the transactions within a block, which validates the authenticity of the transactions and stored information. When the block solution is found, a new block is created. The amount of time to find the solution and create a new block is the block time.

Features:

- A block is a file that records a number of the most recent cryptocurrency transactions.
- Each block contains a reference to the block that preceded it (that's why it is theoretically impossible to alter cryptocurrency).
- Cryptocurrency "miners" race against each other to solve the hash, which is the hexadecimal number generated that verifies the transactions. The winner receives a crypto coin.

Bitcoin Block:

- A block is **a place in a blockchain where information is stored and encrypted**.
- Blocks are identified by long numbers that include encrypted transaction information from previous blocks and new transaction information.
- Blocks and the information within them must be verified by a network before new blocks can be created.

Bitcoin per Block:

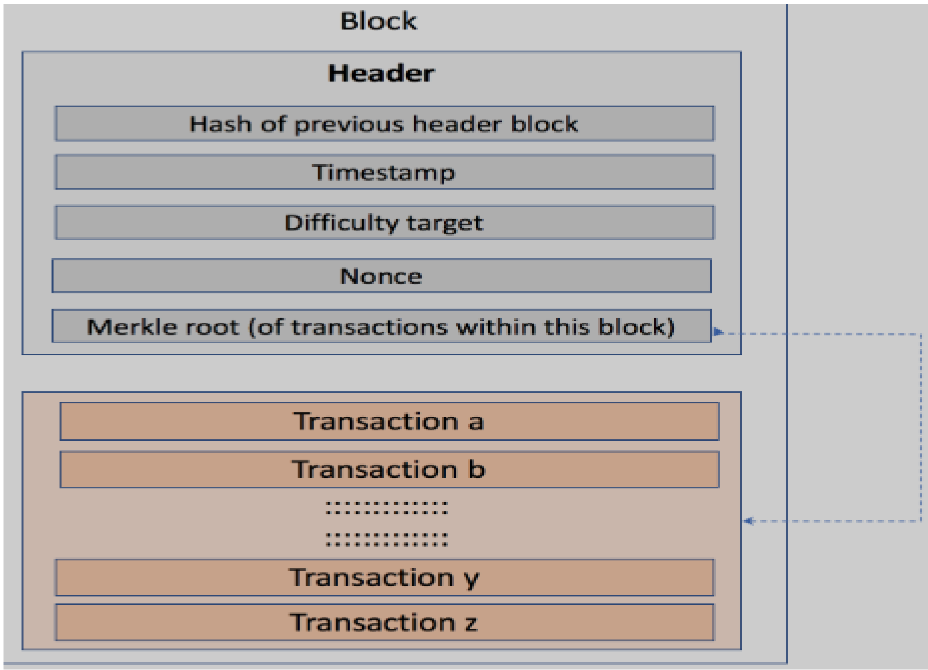
- 144 blocks per day are mined on average, and there are 6.25 bitcoins per block.

Bitcoin Block Creation:

- To create a new block, miners must go through a process to solve a math problem.
- When finding a valid solution for the network, a new block can be taken for granted that will be added to the blockchain by consensus.
- And for which, the miner who found the solution, will receive a reward for the new block.

Bitcoin Block Structure

- The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size.
- The block header is 80 bytes, whereas the average transaction is at least 250 bytes and the average block contains more than 500 transactions.



Ethereum block:

Blocks are batches of transactions with a hash of the previous block in the chain. This links blocks together (in a chain) because hashes are cryptographically derived from the block data.

Ethereum Block use:

The Ethereum blockchain is powered by its native cryptocurrency — ether (ETH) — and enables developers to create new types of ETH-based tokens that power dApps through the use of smart contracts. The most common ETH-based cryptocurrencies are built on the ERC-20 token standard.

Ethereum block size

The current size of an Ethereum block is usually about 80 KB, and about 4 MB in 10 minutes. However, when it comes to synchronizing Ethereum nodes, the size of the block is never the point. Comparing the size of the blockchain of Ethereum and Bitcoin, the blockchain of Bitcoin is actually larger than Ethereum.

Working:

Both in bitcoin blockchain and ethereum blockchain, there is an expected block time, and an average block time. In bitcoin, the expected block time is 10 minutes, while in ethereum it is between 10 to 19 seconds.

A new Ethereum block is created every 14 seconds. 18 Million Ether are mined every year.

Ethereum is more future-proofed than any other protocol. Secondly, future-proofing can refer to the actual function of a blockchain. A blockchain stores data immutably and is a more secure record than a centralized, third party-owned database.

Features:

- understanding what block is and its role
- Structure(fields) of block
- Uncle block

Block and its role:

A block is a core concept that can be thought of as a page in a ledger. Blocks contain transactions and some important data such as previous hash that ensures immutability and security in the blockchain network. Each block stores a previous hash sequentially so it is almost infeasible to reverse and tamper data.

Ethereum uses Proof-of-Work as its consensus algorithm and is gradually shifting to Proof-of-Stake. As Proof-of-Work is not eco-friendly due to its too much electricity consuming. Proof-of-Stake can mine blocks based on the amount of money miner has, and faster than PoW.

Ethereum block stores several important data such as previous block hash, Merkle trie based root hash, timestamp, difficulty, and more.

Block Size:

Block size is pretty straightforward — it is the amount of data a single block can hold. For example, as of May 2021, one block on the Bitcoin blockchain can hold data equivalent to 1 MB. This limitation was enforced in 2010, in an effort to limit the opportunity for overwhelming the blockchain and stop possible DoS attacks.

Initially, the Bitcoin blockchain was designed to work with blocks of up to 36 MB in size; however, security concerns enforced the need for significantly smaller block sizes.

Block time:

Block time is the measure of the time it takes the miners or validators within a network to verify transactions within one block and produce a new block in that blockchain.

Blockchains were first popularized by Bitcoin when it was introduced in 2009. The technology has grown as more cryptocurrencies are created, each of which can use different or the same blockchain, validation methods, and techniques for creating new blocks.

Understanding Block Time

A blockchain is a distributed database that records all transactions within a cryptocurrency network. You can think of a block within the database as a cell in a spreadsheet where transaction information is stored. Miners verify the transactions, which takes time because finding the solution to the block requires the computers to make a vast amount of trial and error calculations.

This is called hashing—using an algorithm to verify all the transactions within a block, which validates the authenticity of the transactions and stored information. When the block solution is found, a new block is created. The amount of time to find the solution and create a new block is the block time.

Global Block Size:

The global blockchain market is rapidly growing and is expected to continue to do so in the future years, due to the expanding number of innovations and consumer awareness of the benefits of employing blockchain technology is expected to propel the industry forward in the near future. The key aspects driving the growth of the global blockchain market include the adoption of blockchain technology across BFSI, healthcare, media and entertainment, and many others.

Wide acceptance of blockchain solutions for payment, digital identities, and smart contracts are also among some of the prospects that drive the industry growth during the forecast period. The increased venture capital investing in blockchain technology startups can also be attributed to the market's growth.

Blockchain miners and validators:

Blockchain "mining" is a metaphor for the computational work that nodes in the network undertake in hopes of earning new tokens. In reality, miners are essentially getting paid for their work as auditors. They are doing the work of verifying the legitimacy of Bitcoin transactions.

A peer-to-peer computer process, Blockchain mining is used to secure and verify bitcoin transactions. Mining involves Blockchain miners who add bitcoin transaction data to Bitcoin’s global public ledger of past transactions. In the ledgers, blocks are secured by Blockchain miners and are connected to each other forming a chain.

When we talk in-depth, as opposed to traditional financial services systems, Bitcoins have no central clearinghouse. Bitcoin transactions are generally verified in decentralized clearing systems wherein people contribute computing resources to verify the same. This process of verifying transactions is called mining.

It is probably referred to as mining as it is analogous to mining of commodities like gold—mining gold requires a lot of effort and resources, but then there is a limited supply of gold; hence, the amount of gold that is mined every year remains roughly the same.

In the same manner, a lot of computing power is consumed in the process of mining bitcoins. The number of bitcoins that are generated from mining dwindles over time. In the words of Satoshi Nakamoto, there is only a limited supply of bitcoins. Only 21 million bitcoins will ever be created.

At its core, the term ‘Blockchain mining’ is used to describe the process of adding transaction records to the bitcoin blockchain. This process of adding blocks to the blockchain is how transactions are processed and how money moves around securely on Bitcoins. This process of Blockchain mining is performed by a community of people around the world called ‘Blockchain miners.’

Process:

- Blockchain miners install and run a special Blockchain mining software that enables their computers to communicate securely with one another.
- Once a computer installs the software, joins the network, and begins mining bitcoins, it becomes what is called a ‘node.’
- Together, all these nodes communicate with one another and process transactions to add new blocks to the blockchain which is commonly known as the bitcoin network.
- This bitcoin network runs throughout the day. It processes equivalent to millions of dollars in bitcoin transactions and has never been hacked or experienced downtime since its launch in 2009.

Types of Mining:

The process of mining can get really complex and a regular desktop or PC cannot cut it. Hence, it requires a unique set of hardware and software that works well for the user. It helps to have a custom set specific to mining certain blocks.

The mining process undertaking can be divided into three categories:

1. Individual Mining

When mining is done by an individual, user registration as a miner is necessary. As soon as a transaction takes place, a mathematical problem is given to all the single users in the blockchain network to solve. The first one to solve it gets rewarded.

Once the solution is found, all the other miners in the blockchain network will validate the decrypted value and then add it to the blockchain. Thus, verifying the transaction.

2. Pool Mining

In pool mining, a group of users works together to approve the transaction. Sometimes, the complexity of the data encrypted in the blocks makes it difficult for a user to decrypt the encoded data alone. So, a group of miners works as a team to solve it. After the validation of the result, the reward is then split between all users.

3. Cloud Mining

Cloud mining eliminates the need for computer hardware and software. It’s a hassle-free method to extract blocks. With cloud mining, handling all the machinery, order timings, or selling profits is no longer a constant worry.

While it is hassle-free, it has its own set of disadvantages. The operational functionality is limited with the limitations on bitcoin hashing. The operational expenses increase as the reward profits are low. Software upgrades are restricted and so is the verification process.

Bitcoins Mining Procedure:

- You can buy and trade for bitcoins, or you can mine them.
- For mining bitcoins, users are rewarded in bitcoins. This mechanism forms the pivot around which the bitcoin economy revolves.
- While the cost and difficulty of mining bitcoins individually continue to increase, several cloud-based mining services have gradually emerged.
- These services allow individual users to lease the processing power of mining equipment and mine bitcoins remotely. However, you can mine bitcoins in person too.

Mining Bitcoins on Cloud

- ***Obtain a bitcoin wallet*****:** Bitcoins are stored in digital wallets in an encrypted manner. This will keep your bitcoins safe.
- ***Secure the wallet*****:** Since there is no ownership on bitcoins, anyone who gains access to your wallet can use it without any restriction. So, enable two-factor authentication and store the wallet on a computer that does not have access to the Internet or store it in an external device.
- ***Choose a cloud mining service provider*****:** Cloud mining service providers allow users to rent processing or hashing power to mine bitcoins remotely. Popular cloud mining service providers are Genesis Mining and HashFlare.
- ***Choose a cloud mining package*****:** To choose a package, you will need to decide on how much you are willing to pay and keep your eyes open to the hashing power the package will offer. Cloud mining companies will mostly envisage the Return on Investment (ROI) based on the current market value of Bitcoins.
- ***Pick a mining pool*****:** This is the best shot you can get to earn bitcoins easily. There are many mining pools which charge a mere 2 percent of your total earnings. Over here, you will have to create workers which are basically subaccounts that can be used to track your contributions to the pool.
- ***Put your earnings in your own secure wallet*****:** Whenever you witness an ROI, simply withdraw your earnings and put them in your own secure wallet.

Uses of Blockchain Mining

1. Validating Transactions

Bitcoin transactions take place in huge figures every day. Cryptocurrencies function without a central administrator and the insecurity can be substantial with the transactions that transpire. So, what is the authentication method with such cryptocurrencies? With each transaction, new blocks are added to the blockchain in the network and the validation lies in the mining results from the blockchain miners.

2. Confirming Transactions

Miners work the blockchain mining process to confirm whether the transaction is authentic or not. All confirmed transactions are then included in the blockchain.

3. Securing Network

To secure the transaction network, bitcoin miners work together. With more users mining the blockchain, the blockchain network security increases. Network security ensures that there are no fraudulent activities happening with cryptocurrencies.

Blockchain speed:

- The current Bitcoin block generation time is 10 minutes; i.e., every ten minutes, a new block is mined. In ten minutes (600 seconds), Bitcoin can average around 2,759.12 transactions based on previous assumptions. In other words, the Bitcoin blockchain can currently guarantee only 4.6 transactions per second.

To Increase speed:

- If you have sent a transaction that is taking a long time to confirm, you can speed it up by using our increase fee feature. This resends your unconfirmed transaction with a higher fee. Bitcoin miners prioritize transactions with higher fees when selecting transactions to include in a block.

Blockchain throughput:

Throughput is a measure of how many actions are completed within a given time frame. In the blockchain space, transaction throughput refers to a rate of how fast a blockchain processes transactions, which is commonly expressed in transactions per second (TPS), but may also be expressed in minutes (TPM) or hours (TPH).

comparison with traditional network:

Blockchain	**Database**
Decentralized Control- In Blockchain, we have no centralized system of control. It allows different parties who don’t know each other or trust each other to share information without the need for a central system or administrator. With the decentralized system, it eliminates the risk of accessing the data and corrupting it and thus,	Centralized Control- It is centrally controlled by the administrator. Any change in the data can change the information everywhere. In the centralized database, anyone who has access to the system can corrupt or destroy the data. It has led to the cases of hacking and forgery. It is not the case with the Blockchain.

makes the information safe and secure.	
History of records – The information which is relevant for now and the information that existed before exist together. It creates a database which has histories of themselves. Tio sum, you can say, that it has all the information in real-time and also the information that was there before. Thus, you get a complete picture of everything. This feature of blockchain makes it useful for tracing the records and knowing the authenticity of a product.	No history of records- In a case of centralized database or traditional database we have the information which is up-to-date at a particular moment. You can say that it is a snapshot of the current status.
Confidentiality of information- Well, hiding information on blockchain requires a lot of cryptography. There is no confidentiality of information. It is visible to everyone in the system.	Confidentiality of database- When it comes to the traditional database then the information is only visible to the members.
Read and write Operations- In blockchain, the user can add more data in the form of additional blocks. It doesn't mean that the old data will be deleted, both the data remains in the system, and you can check it. There are two operations of blockchain : 1. Read- Query and retrieve data from the blockchain 2. Write- it adds more data to the blockchain	CRUD- in a traditional database, the client does four functions: 1. Create, 2. Read, 2. Update and 4. Delete which is together known as CRUD