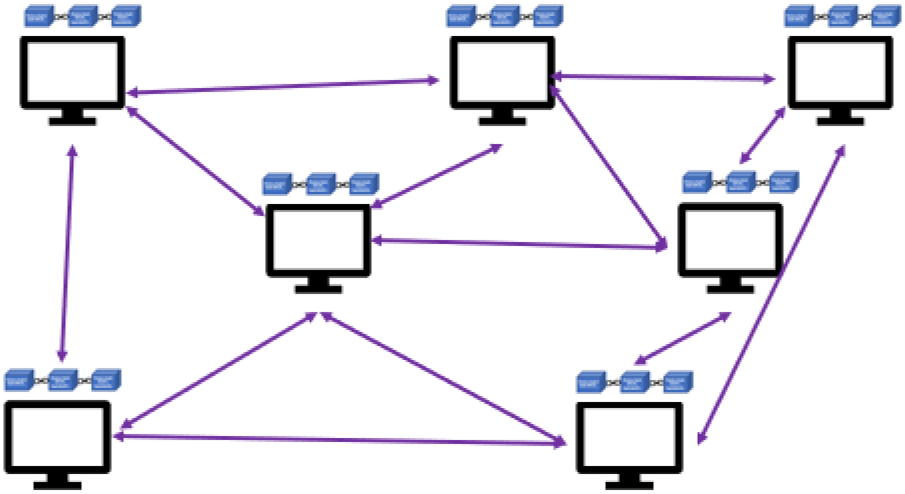
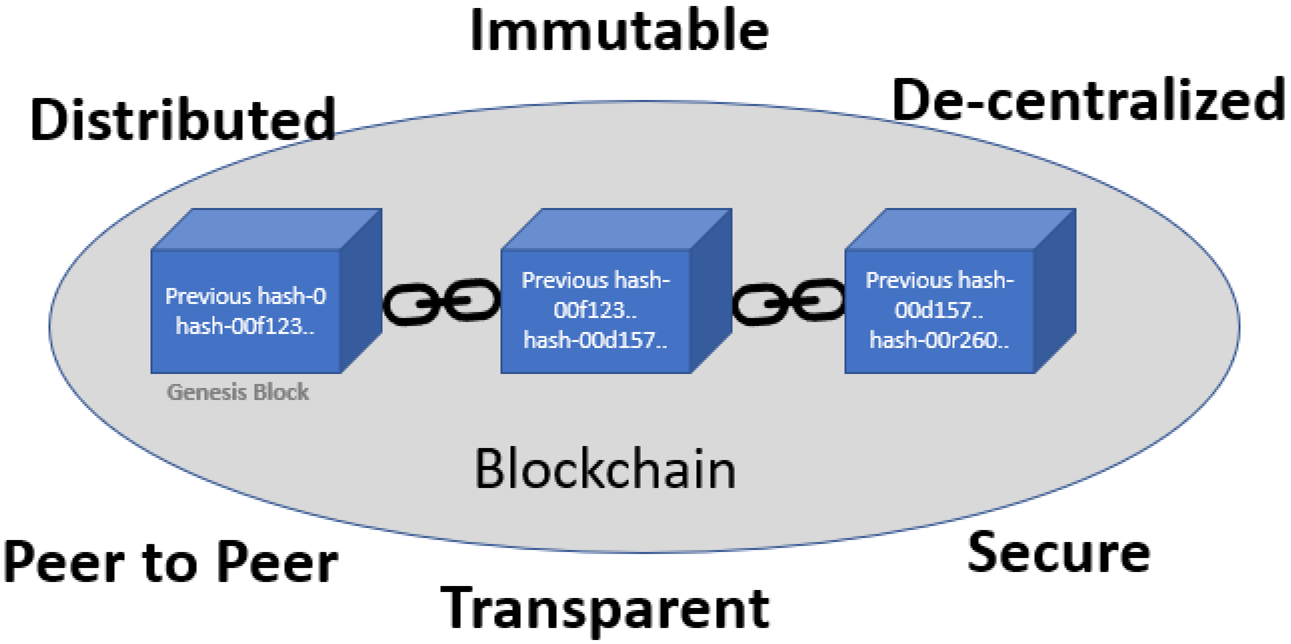
A Simple Guide to Understanding Blockchain

medium.com/swlh/a-simple-guide-to-understanding-blockchain-8dd09356b153

A simplistic explanation of what is Blockchain and how it works



Blockchain is an immutable, distributed, decentralized; peer-to-peer ledger replicated across multiple nodes connected in a network, making it possible to record data about any event or transaction as it happens. It consists of blocks in a chain used to record as digital assets using a secure algorithm.



Where can we apply Blockchain technology?

- : is working with IBM for enhanced tracking and traceability of food products, resulting in better food safety.

- : title registry system uses blockchain to make title issuance instantaneous.
- : The global money transfer is time-consuming, error-prone, costly, and subjected to money laundering. The secure, immutable, decentralized, and transparency feature of Blockchain helps solve money transfer issues without any intermediary.
- : Blockchain is very secure, immutable making any alteration to transactions very difficult.
- : Singapore-based VeChain created a permissioned blockchain-based supply chain to monitor products as they move along from manufacturer to store shelf.

Blockchain can be applied to many other applications wherever we want to record transactions securely between two parties without an intermediary.

Database and Blockchain both record transactions, but **the database is centralized and has a single point of failure. In contrast, the Blockchain is decentralized and distributed on multiple nodes across the network.**

Every node in the blockchain network collectively takes part in the consensus algorithm using Proof-of-Work.

Databases are owned by a central authority, a company, or a government institution, which **controls access** by granting different roles to different users. Whereas **Blockchain is a peer-to-peer network where each node can connect with every other node, and blocks in a chain are connected using a secure cryptographic protocol like SHA-256**.

Ledger

A ledger records transactions such as recording payments, supply chain details, medical records, real-estate contracts, etc.

SHA-256

SHA-256 is a cryptographic algorithm that accepts input of any length, scrambles the data deterministically, and returns a hash that is 256 bits or 64 characters long. SHA-256 hashing algorithm ensures the input can never be derived from the output, making it very secure.

Mining

It is the process of validating and recording new transactions on a blockchain performed by Miners for which they have a special mining software.

Node

A Node in a blockchain can be any electronic device that is part of a peer-to-peer network and maintain its own copy of the blockchain.

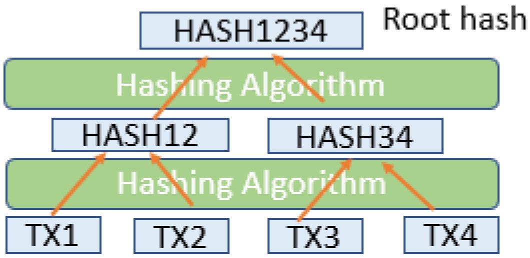
Merkle Tree

Merkle tree is also referred to as “hash binary tree,” a data structure for efficient and secure storage of transactions in a blockchain.

Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions. Merkle tree is **created by repeatedly hashing a pair of transactions from the bottom** until we have only one hash, referred to as **Root Hash or Merkle Root**.

Merkle trees are used in blockchain to store transaction as it enables users to use the root hash to verify if a transaction was part of the block.

Merkle tree requires little memory, computationally fast, and only a small amount of information needs to be transmitted over the blockchain network.



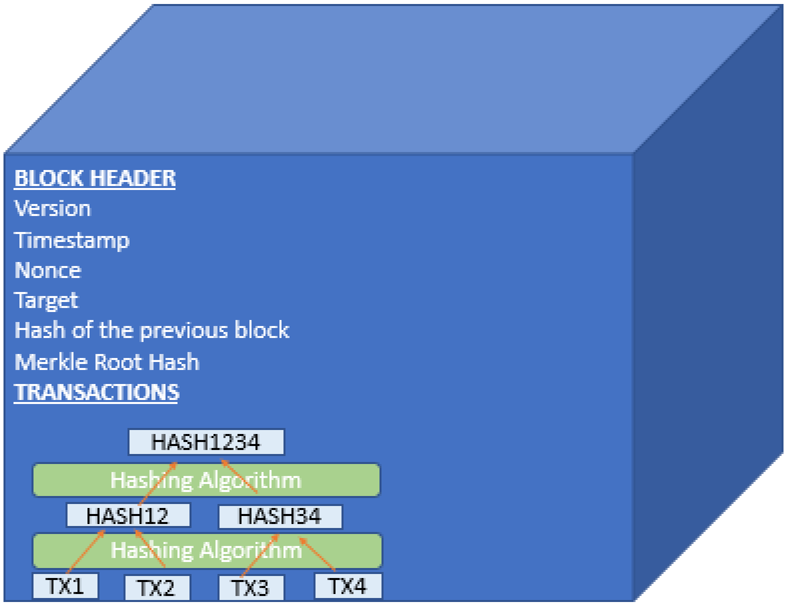
- : Blocks in blockchain are write-once append-only. Data in every block is encrypted using the SHA-256 algorithm that makes modification to data very difficult. Any change in the data renders the newly modified block invalid. This ability of blockchains prevents alteration of transactions.
- : Nodes within a distributed blockchain network have to agree on the network's true state to ensure the validity of transactions using Proof of Work or Proof of Stake.
- : Blockchain is decentralized and is distributed across multiple nodes across the entire network of computers. If one user tries to forge a transaction in the blockchain, all other nodes in the blockchain network will cross-reference each other and easily pinpoint the node with the incorrect information.

Blockchain is a shared digital ledger. **A Block in a Blockchain record transaction or transactions to organize, monitor, and control information for informed decision making.**

Every time a new transaction occurs on the blockchain, a record of that transaction is added as a new block to the chain. The new block is added to every participant’s nodes ledger only after applying a consensus algorithm like proof of work to validate the transaction. A block in the chain is immutable. It can never be updated and only be appended to the chain.

> **The Genesis block is the very first block added to the blockchain**

The Block consists of a



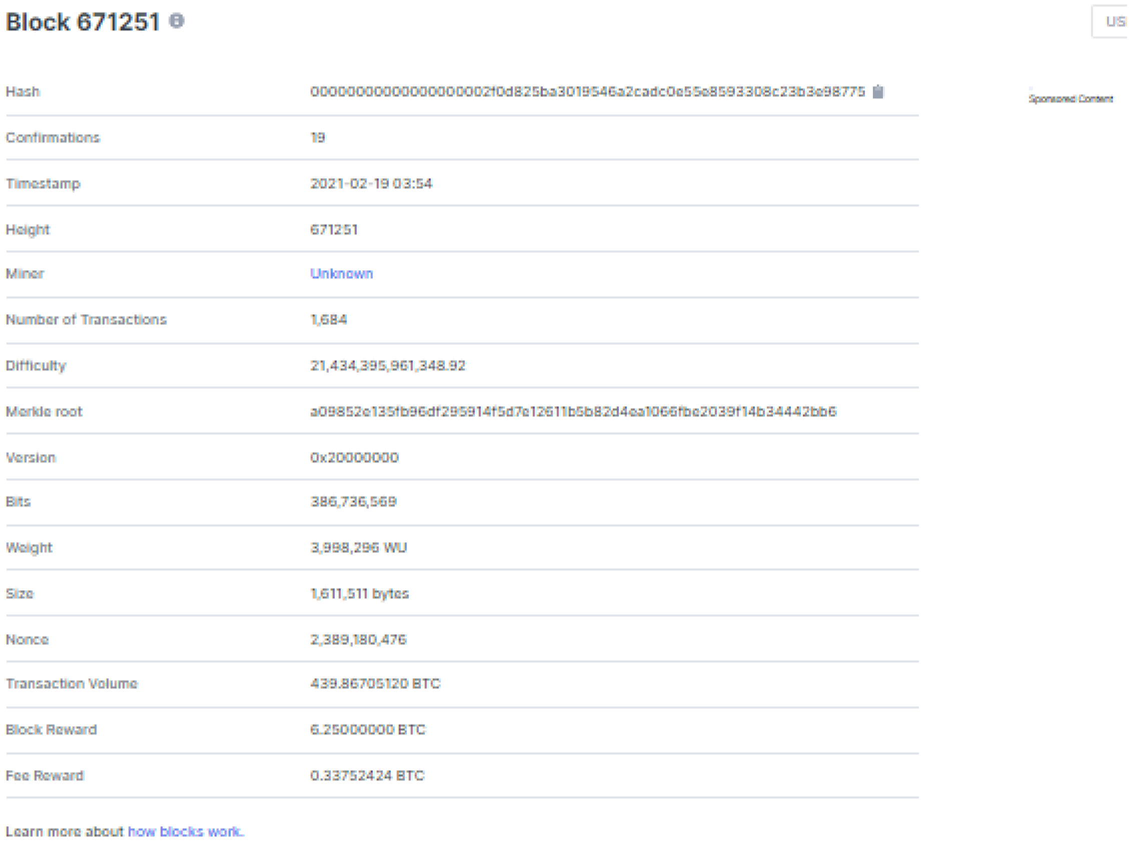
A Block header in a Blockchain contains the following attributes.

1. to track the software or protocol that will allow other computers to read the block correctly.
2. when the transaction was recorded, or the block was created and is expressed as seconds since 1970–01–01T00:00 UTC.
3. header that links one block with another block in a Blockchain. This ensures the integrity of the previous block all the way back to the first block referred to as a Genesis block.
4. stands for
5. It regulates the speed at which new blocks are added to the blockchain and are adjusted roughly every 2016 block. Higher difficulty in generating the nonce represents a lower target value.
6. for all the transactions in a block.

Transaction or Transactions are stored in the Block using the Merkle tree hash.

> **The block hash is a separate hash derived from data in the block header using SHA-256.**

Block hash uses nonce, and hence hash is tied to the nonce forever. **The nonce is used to come up with a secure hash that meets the criteria as per the target.** Hash must start with a huge number of zeroes based on the target.



Block 671251

US

Sponsored Content

Hash	00000000000000000002f0d825ba3019546a2cadc0e55e8593308c23b3e98775
Confirmations	19
Timestamp	2021-02-19 03:54
Height	671251
Miner	Unknown
Number of Transactions	1,684
Difficulty	21,434,395,961,348.92
Merkle root	a09852e135fb96df295914f5d7e12611b5b82d4ea1066fbe2039f14b34442bb6
Version	0x20000000
Bits	386,736,569
Weight	3,998,296 WU
Size	1,611,511 bytes
Nonce	2,389,180,476
Transaction Volume	439.86705120 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.33752424 BTC

Learn more about how blocks work.

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, it becomes what is called a 'node.'

Blockchain can be used to record any transaction like real estate contracts when person A sells a property to Person B at x amount or when food is produced at the farm, travel through the entire supply chain, and finally consumed by the consumer.

Step 1: Sender or Originator of Transaction digitally signs the transaction

Digital signatures are a fundamental building block in blockchains; they are primarily used to verify the authenticity of transactions. The sender of the transaction uses the data and the private key to encrypt the message.

If Peter wants to transact with Patty, he must digitally sign the transaction using his private key and the transaction data and send it to nodes on the network.

Step 2: Transaction is broadcasted to the network

After a transaction is transmitted to the network, it gets verified by all of the available Blockchain nodes.

Step 3: Nodes authenticates the transaction

Knowledge of Peter's public key will enable confirm the authenticity of the transaction. Peter's public key, transaction, and Peter's digitally signed transaction will authenticate the transaction.

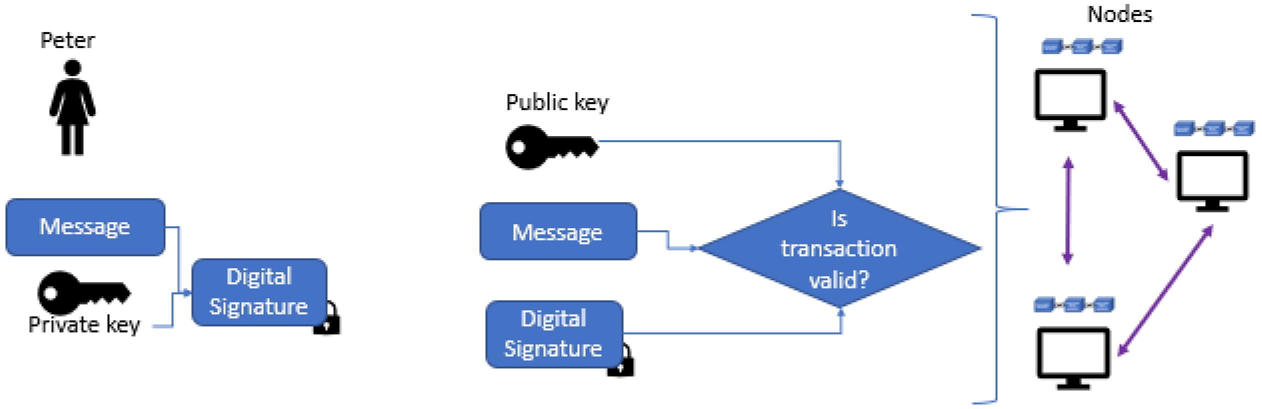


image by author

Step 4: valid transactions are stored in mempool

The mempool stores all valid transactions waiting to be confirmed by the network. Miners pull transactions from the mempool for them to be bundled together into a block.

Step 5: Miners validate using consensus to add the block

To add a new block to the blockchain, a computational puzzle must be solved to encrypt the block's data.

Miners pull authenticated transactions from the mempool and try to solve the complex mathematical problem. **Miners find the nonce such that the hash of the block is less than or equal to the current target of the Blockchain network, also called POW(Proof of Work)**

> Proof of Work requires miners to solve complex mathematical problem to validate and confirm transactions over the network using consensus mechanisms to produce a new block to the chain.

Proof of work makes blockchain secure as any alteration on the blocks requires remaining all subsequent blocks to be altered, and this is extremely difficult.

The first Miner that has solves the cryptographic challenge then broadcasts the newly generated block using the Gossip protocol. Once a block of transactions has been verified, then it is added to the blockchain network.

A reward is given to the first miner who solves each cryptographic problem.

POS(Proof of Stake)

In a distributed consensus-based on the **Proof of Work(POW), miners need a lot of energy to come up with the hash for the block that is less than or equal to the target for the blockchain network. In contrast, the Proof of Stake creator of the next block is chosen deterministically based on the stake in the blockchain.**

> POS is a low-energy consuming alternative to POW algorithm. POS has validators who own the stakes and the responsibility of maintaining the public ledger instead of Miners in POW.

Weakness of Blockchain

- High Energy consumption to solve the cryptographic challenge in order to add a block to the blockchain
- Susceptible to 51%attack

> **51% attack is an attack on the blockchain orchestrated when** a group of miners on the blockchain network control more than 50% of the network's hash rate or computing power to prevent new transactions from gaining confirmations, or ability to invalidate transactions that introduce double spend.

Types of Blockchain

Public blockchain:

- Public blockchains are
- and the transactions that are recorded in the blockchain.
- .

Examples of a public blockchain: Bitcoin, Ethereum, or Litecoin.

Private blockchain

- A private blockchain is
- Controlled by Enterprises for.
- Transactions are private and are

Examples of a private blockchain: hyper ledger

Hybrid blockchain

- Hybrid blockchain is a.
- .
- decides which users can view the data on the blockchain or add data to the blockchain.

Conclusion:

Blockchain is a secure, immutable, peer-to-peer distributed ledger that is decentralized. It contains a secure block that is linked in a chain and replicated across multiple nodes connected in a blockchain network. The public, private and hybrid blockchain can be used based on features of blockchain helpful