In this world every transaction, agreement, every process, every task and every payment would have a digital record and signature that could be identified, validated, stored and shared.By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Blockchain has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. You don’t need to know how the blockchain works to use it. However, having a basic knowledge of this new technology shows why it’s considered revolutionary.

In this course, we will discuss about basics of blockchain, its evolution, types, applications, areas of improvement, Bitcoin in detail and forking.

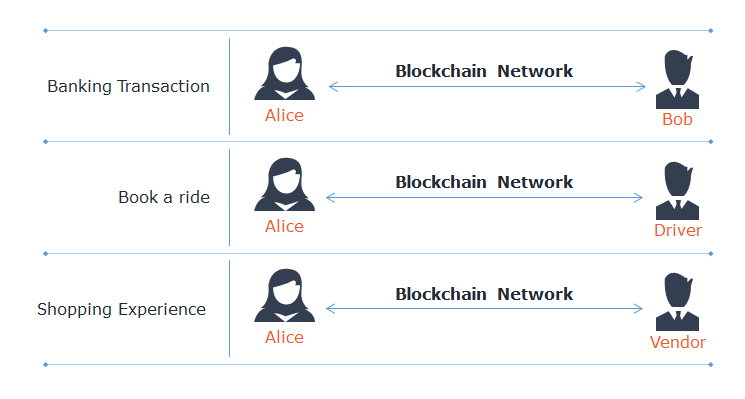
**BlockChain Start:**

Blockchain is hailed as the technology which is going to revolutionize our life with far reaching consequence than IoT. It was popularized by its first widely adopted application Bitcoin, a digital cash or Cryptocurrency which is the first step towards “Internet of Money”. Blockchain applications are evolving fast far beyond Cryptocurrency, from smart contract to dApps (the decentralized applications). It may even lay the foundation for Utopian society where we are all Global citizens governed by “code is law” **–**extending the current concept of Smart contracts**.** It enables us to do business with untrusted parties, blockchain being the trust protocol

­

* If you want to transfer money between two persons you have to go through a payment gateway or a bank
* If you want to hire a taxi you will go through a online aggregator service like Uber or Ola
* If you want to buy any goods online you have to go through an online merchant like Amazon

**Consider the same scenarios, but now using blockchain technology.**



* Without the Bank or a gateway we can transfer money to another person directly
* We can directly engage a taxi without an aggregator like Uber, but ensuring same quality of service and trust, provided both are connected to the same Blockchain network
* We can directly buy goods from a merchant without the need for an online retailer like Amazon

 In all these scenarios, we are depending on middle men as some sort of central authority who provides trust between the sender and the receiver.

* The central authorities are prone to failure

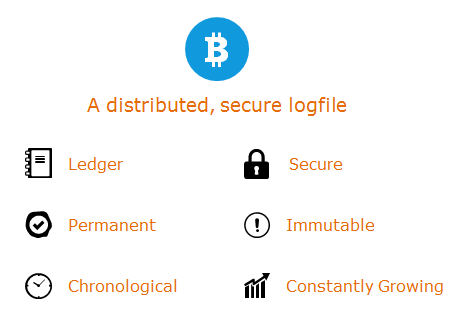
E. g. : banking Collapse of 2008

* Trusted third parties are potential security breaches

E. g. : If you have any wearable the data is uploaded to the cloud managed by the device manufacturer and there is no guarantee that your private data is monetized not misused

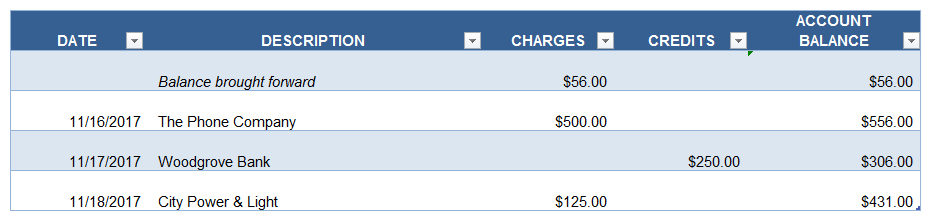
* To address this problem the idea of Blockchain was originated based on a paper published by Satoshi Nakamoto (a pseudo name) in 2008
* Blockchain is a way to do transaction between two untrusted parties directly without a central authority. Open Bazar and Mycelia are some of the examples
* Open Bazar is a free online market place where you can buy and sell anything with zero platform fees
* Mycelia is online music store running on blockchain

Blockchain is a chain of Blocks containing information. Each Block has one input from the previous block and thus it is chained. It is a distributed ledger which is secure.



Blockchain can be attributed as:

* **A ledger**
  + All transaction data can be entered

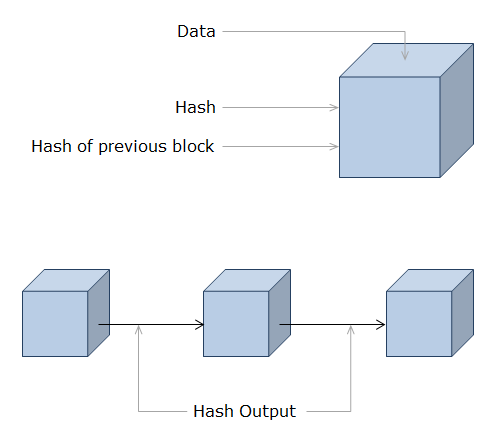


* **Constantly growing**
  + It keeps track of all transactions. As more and more transactions occur, it will be entered in the Blockchain, so it is constantly growing
* **Chronological**
  + The transaction data entered is in chronological order with which it is occurred
* **Permanent**
  + The data entered is permanent and secured, it cannot be deleted
* **Immutable**
  + No transaction data can be modified by anybody. All data entered is permanent

E. g. : If you make a mistake of transferring $100 instead of $10 you cannot cancel it or delete it. To correct the mistake, the receiver can initiate another transfer of $90/- back to you.

# Blocks and Chains

What is a Blockchain? What exactly a block and how it is chained?  Block contains data, transaction data. It also contain the hash of the previous block. Hash is a cryptographic one way function, which gives a fixed length output for any input of arbitrary length. It is like a digital fingerprint.  One of the input for any block is the hash output of the previous block, thus chaining blocks.



* Data can be any type of data stored in the Blockchain
* Hash is digital fingerprint of Block
* Hash output of the previous block will be served as one of the input to the next block

**How does the transactions work**

* Both parties need to agree on the state of the board
* Both know the starting positions of the board
* Both know the sequence of messages so far
* Now they can reconstruct the state of the board

Similarly in Blockchain if we agree on the initial state and history of transactions then we can arrive at the current state of the World.

**Ledgers** are the system of record for a business.

* Businesses will have multiple ledgers for the multiple business networks in which they participate
* Transaction: an asset transfer onto or off the ledger
  + John gives a car to Anthony (simple)
* Contract: the conditions for a transaction to occur
  + If Bob pays Alice money, then car passes from Bob to Alice (simple)
  + If car won't start, funds do not pass to Bob, as decided by third party arbitrator (more complex)

**Conventional Ledger:**

* It is kept in a central server and maintained by a central authority
* If anything happens to the central server the ledger will be inaccessible
* It is not immune to any kind of intervention by a government

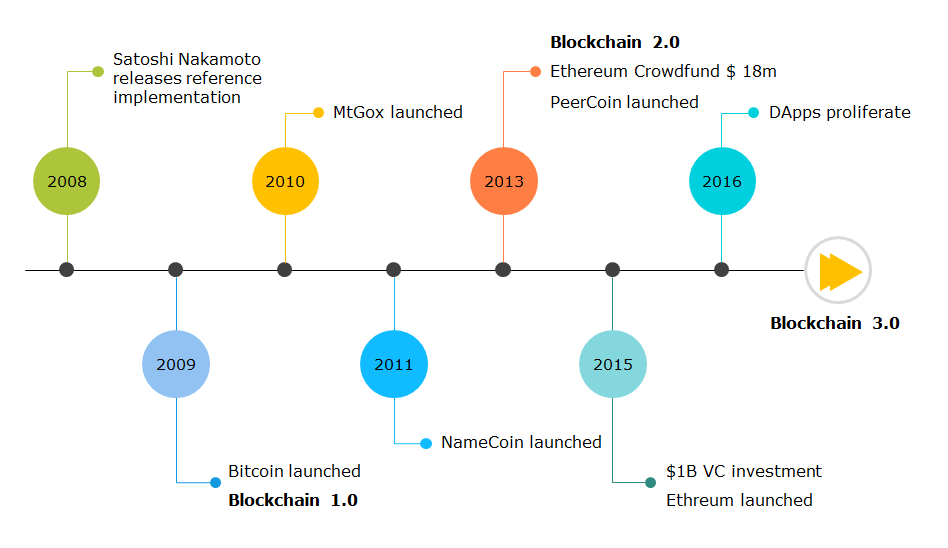
**Blockchain:**

* It is a distributed ledger, kept with all the nodes of the Blockchain peer to peer network
* All the data is distributed and kept in all the participating nodes of Blockchain in the peer to peer network
* Data is always accessible irrespective of any censorship by any country

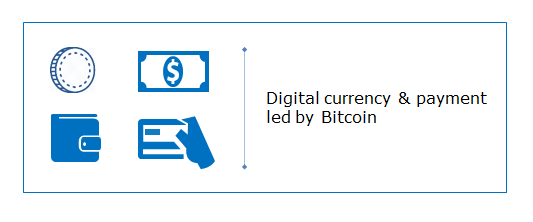
E. g. : It is similar to torrent network, you cannot shut it down

* Creates a permanent, time-stamped record of all transactions that is mathematically secured (using cryptography ) from alteration
* Allows untrusting parties with common interests to co - create a permanent, unchangeable and transparent record of exchange without relying on a central authority

Blockchain is a distributed database that maintains a continuously growing list of records called blocks secured from tampering and revision. Blockchain was first conceptualized by Satoshi Nakamoto in 2008 in his paper about Bitcoin.

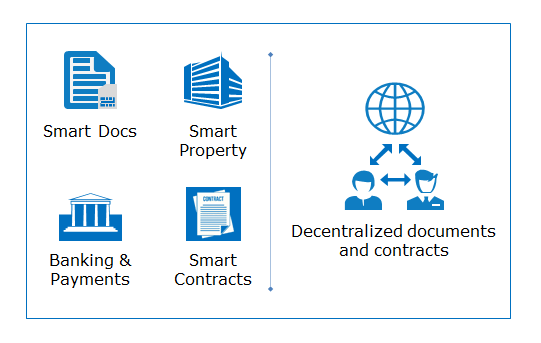


**Blockchain 1.0**



* Programmable money - Cryptocurrencies
* Satoshi in his first paper discussed only about Blockchain’s application in cryptocurrency and he created Bitcoin in Jan 3, 2009
* Blockchain 1.0 is confined to Bitcoin

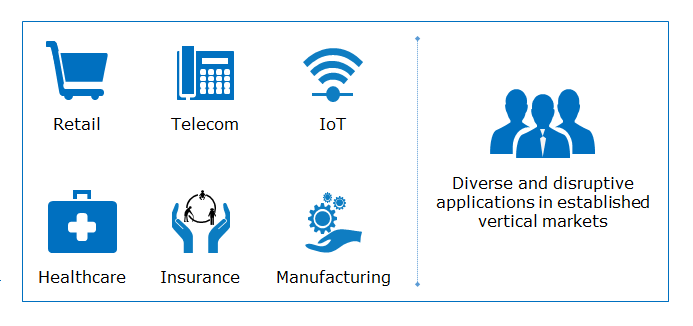
**Blockchain 2.0**

****

Blockchain 2.0 is beyond programmable money.

* Smart Contracts
* Data Protection solutions based on Blockchain
* Blockchain as a platform: transparent trusted time stamping
* Innovating in conventional market
* Legislation
* Later in 2013 Vitalik Buterin came up with an idea of applying Blockchain principles in various domains apart from financial. By 2015 Vitalik and a group of programmers launched Ethereum, which envisaged as a platform for creating Blockchain applications, smart contracts, smart property, smart docs etc. These are all decentralized documents and contracts coded using Blockchain technology running in Ethererum network

**Blockchain 3.0**

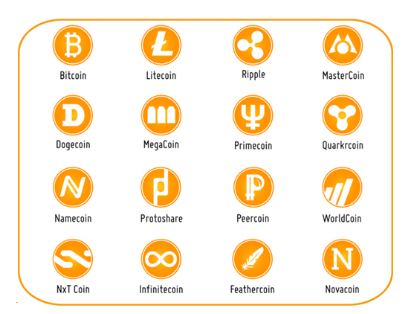
****

Blockchain finding application in every field.

* Decentralized web
* Opportunities and challenges
* Expanding the application of Blockchain in all domains. Examples include: healthcare, retail, manufacturing, logistics, insurance, IoT

BlockChain 1.0

A crypto currency is a digital representation of value, that is neither issued by a central bank or public authority nor necessarily attached to flat currency, but accepted by two or three parties as a means of exchange, and can be transferred, stored or traded electronically.



                                                                  Source: TechnoMag

Crypto currencies:

* Bitcoin
* Bitcoin Cash
* Litecoin

Crypto currency is a digital or virtual currency that uses cryptography for security.

Blockchain 2.0

In the Current scenario of travel insurance 60% of the passengers insured against the delay of their flight never claimed their money.

During a hackathon in London in 2015, a team created an automated insurance system based on smart contracts.  Smart contracts are self executing code which is stored in a blockchain, so it cannot be modified.

Using Smart contract: ( A set of conditions which triggers an action automatically)

* Passengers are automatically compensated when their fight is delayed, without having to fill out any form, and thus without the company having to process the requests
* The blockchain's contribution here consists in generating the confidence and security necessary to automate the declarative phases without resorting to a third party

BlockChain 3.0

Current centralized architecture of Internet created many issues, the Big 5 (Google, Microsoft, Apple, Amazon and Facebook) handles most of the personal data.

* They can monetize your data without your permission or share with Govt. agencies
* This data is susceptible to hacking as history shows, you may loose your entire data
* If the server goes down, the data becomes inaccessible
* Centralized architecture is susceptible to DDOS attacks

Decentralized content delivery networks using Blockchain technology can guard against DDOS attacks. Using smart contracts you can specify how your personal data can be used by others in the system

# Non-permissioned Blockchain

It is a public Blockchain that is open to all and its protocols ensures trust.

* Anyone can join the network
* No centralized control
* Needs an elaborate distributed consensus mechanism to build the trust
* E. g. : Bitcoin, Ethereum and Litecoin

# Permissioned Blockchain

During the Initial stages of Blockchain development, these institutions ignored it, later realized they could not ignore it any more and found ways to adapt it to their needs, without loosing their authority. Thus Permissioned Blockchain was introduced.

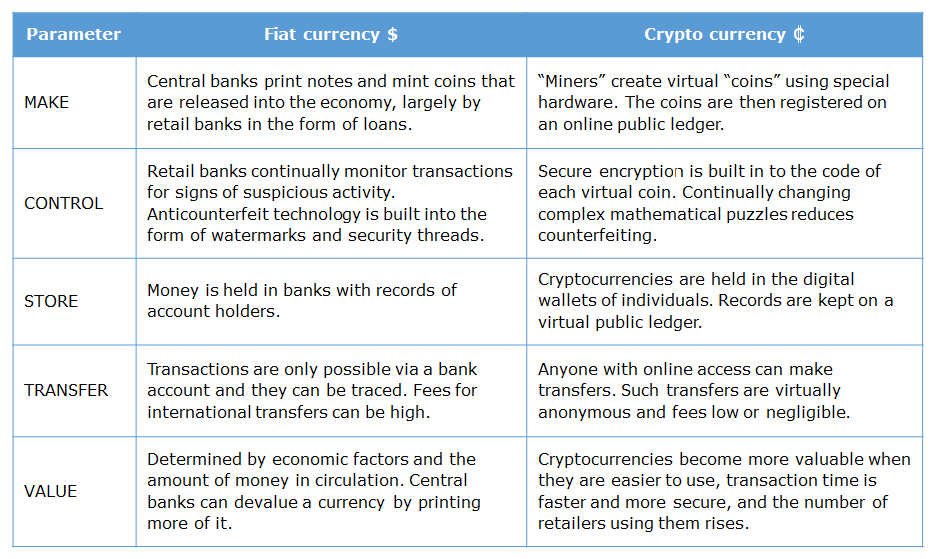
* In Permissioned Blockchain the identity of the participants are known and are trusted
* Since the participants are trusted there is no need for “mining”
* The responsibility of adding a block is assigned by the code creators rather than by lottery for non-permissioned Blockchain
* Hyperledger is a Blockchain development platform by Linux Foundation for creating enterprise class permissioned Blockchain apps

Two types of Permissioned Blockchain are:

* **Federated Blockchain** or consortium Blockchains
  + Operate under the leadership of a group
  + Admission is restricted
  + It is faster and scalable
  + E. g. : R3(Banks), EWF (energy) and B3 i( Insurance)
* **Private Blockchain**
  + Restricted to one organization
  + Members are trusted
  + E. g. : Monax, Multichain

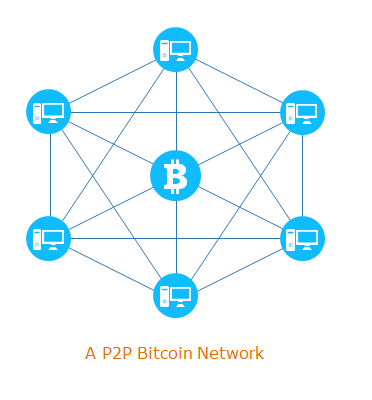
The concept of a Blockchain was first introduced by [Satoshi Nakamoto](https://www.youtube.com/watch?v=5C14TKM7yRg&ab_channel=CoinPilot) in 2008, in the midst of the financial crisis, to serve as the ledger for Bitcoin, a purely peer-to-peer version of electronic cash.

It is easier to understand Blockchain of one learn its first application, cryptocurreny, bitcoin. The following table gives a comparison of traditional currency vs cryptocurrency.

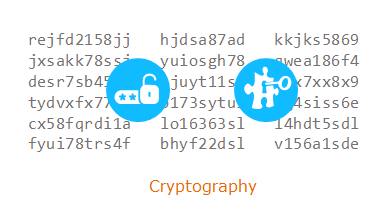


# The Bitcoin network:

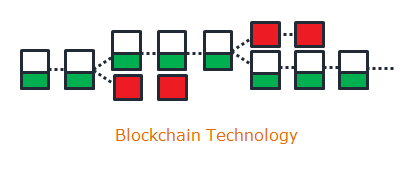
* **A P2P network like bittorrent:**
  + P2P network often called nodes, collectively validating and bundling batches of encrypted transactions together into code blocks
  + Each block is then added to the end of the chronological chain, stored not in one central location but, synchronized on each node across the network



* **Cryptography:**
  + Enables the exchange of accurate (payment) instructions between the parties of the transactions with digital signatures using public Cryptography
  + Cyptorgraphic hash functions are used to enforce discipline on writing transaction  records on public ledger



* **Blockchain Technology:**
  + It bundles together transactions in a chain of blocks and ensures transactions can be independently confirmed as unique and valid using distributed consensus mechanism without a central authority
  + Trust protocol using general distributed consensus offered by Blockchain is the main reason for the existence of Bitcoin

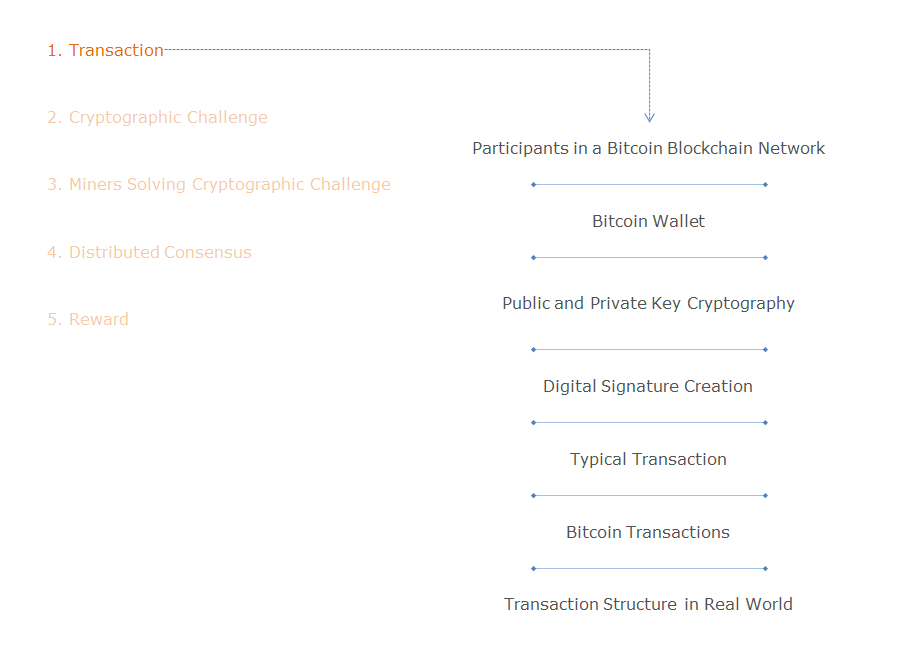


Typical flow of a Bitcoin transaction can be classified as given below.



These operations are explained in the following pages.

Let us start with transaction. How it is done in Bitcoin network. What are the steps involved in Bitcoin transaction can be seen in next few pages.



There are three participants in Bitcoin network:

* End users
  + Individuals moving value between one another, via transactions
* Full Nodes
  + Holds the entire Blockchain copy , relays and validates and broadcasted transactions and blocks
* Miners
  + Who creates the new blocks / solves cryptographic puzzle

 To start any transaction one need to create a wallet by installing the client in his / her mobile or computer.

* Once you have set up your wallet, you receive a key to the public pocket of your wallet
* It’s a string of letters and numbers 34 characters long, for example, 17fPhbmXDpye94FrNu9fnE9DztMKCxES47
* It normally begins with 1,2 or 3
* It is your account number and you can freely give it out to receive payments in Bitcoin
* The key to your wallet, the private key, where you hold or move your Bitcoin holdings, is 51 characters long and this number should be carefully guarded
* You don’t need to memorize either key. They are translated into QR codes and can be securely stored on your smartphone

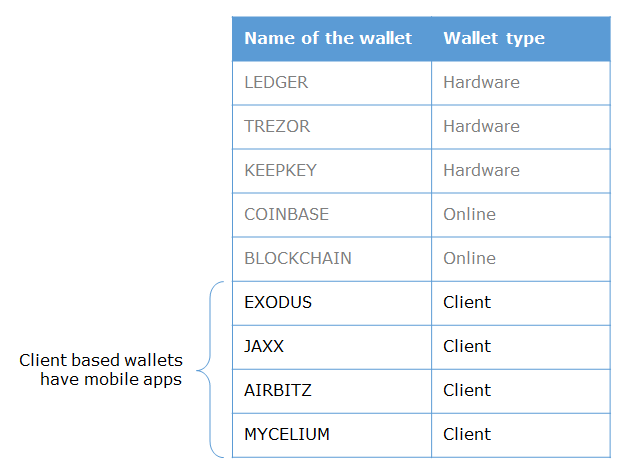


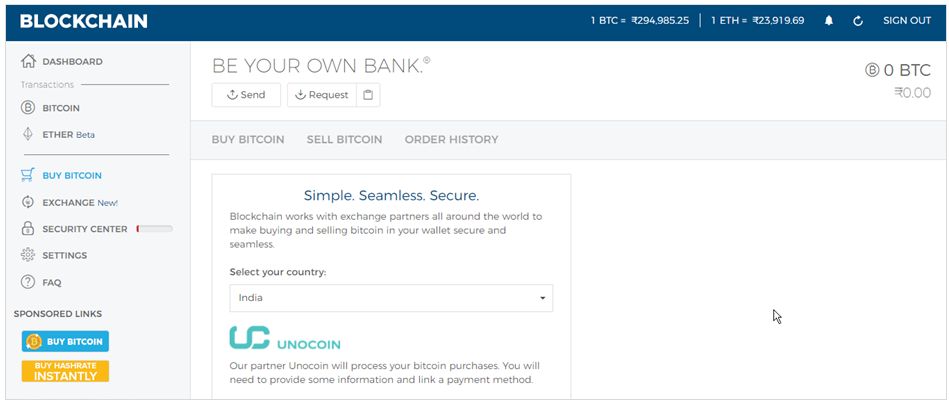
Bitcoin wallets are of two types: software based and hardware based.

* Bitcoin hardware wallets are the most secure type of Bitcoin wallet
* What differentiates hardware wallets from software wallets is that when they are plugged out it is in “cold storage”
* Your hardware wallet is disconnected from the Internet and impossible to touch
* Hackers, Trojans, and other malware can’t get to anything to it when it is in cold storage

# Wallet Example:

Some of the most popular soft as well as hardware based wallets are listed here.

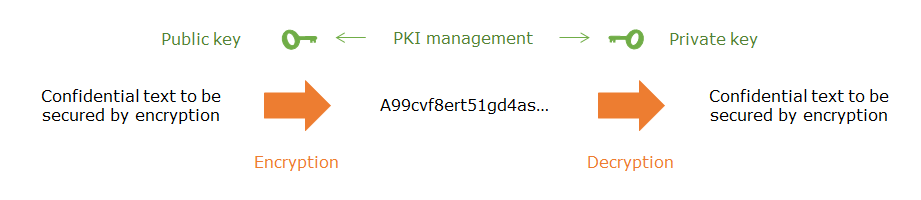




                                                                                                                                       Source: [Blockchain info](https://blockchain.info/wallet/)

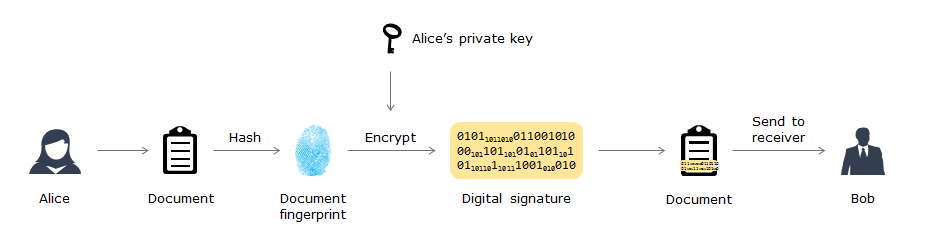
Public and private keys are two large prime numbers that have a mathematical relation with each other.

* A string encrypted with one key can only be decrypted with the other
* One key needs to be kept private, the other one can be made publicly known
  + This can be used by other parties to exchange data with you in a secure manner
* Private keys need to be stored that it is accessible only for owner
  + This can be done on personal devices (PC, smart card, USB stick, phone, ...) or remotely with a service provider (cold and hot wallets)



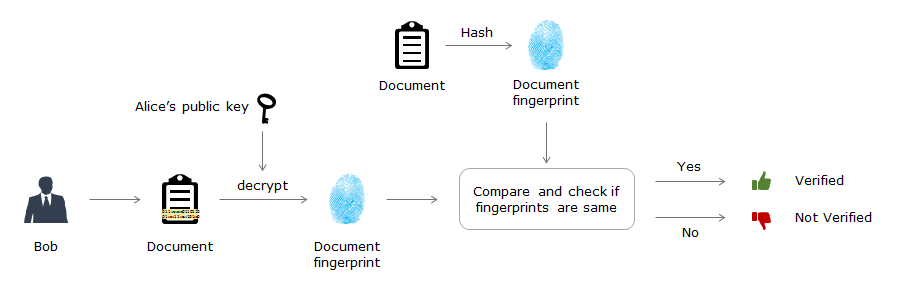
Digital signatures ensures authentication, non- repudiation and integrity of the message.

# ****Digital signature creation****



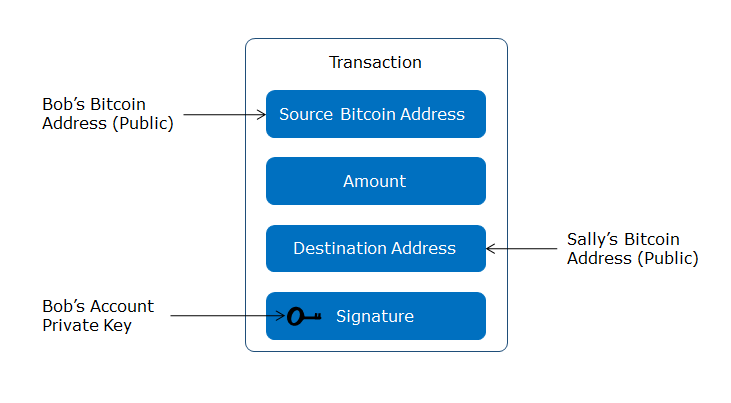
# 

# ****Digital signature verification****

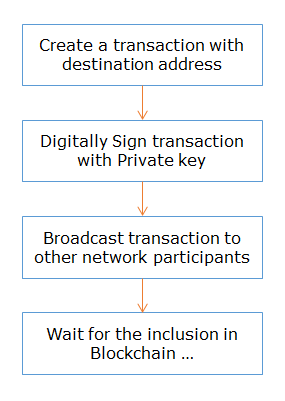


Alice wants to send a document to Bob. She wants it to be tamper proof, so she append the document with her digital signature and sent it to Bob. Bob should be able to verify the Alice's signature ensuring that the document is sent by Alice only and it is not tampered. The following steps are done to ensure this:

* Digital signature uses the PK encryption algorithm, public and private key pair. Alice takes the digital fingerprint of the document she wants to send using Hash algorithms like SHA -64 (Secure Hash Algorithm, 64 bit)
* It is then encrypted with her private key to get the digital signature. This is appended with the document and sent it to Bob
* Bob upon receiving the document calculates its digital finger print using the same Hash function
* Bob decrypts Alice's Digital signature using her public key to get the digital finger print sent by Alice
* Now both finger prints are compared, one calculated by Bob and the other decrypted by Bob
* If both are equal the document is sent by Alice and it is not tampered. If they are not the same, then the document is tampered



* A transaction is a transfer of value between Bitcoin Wallets that gets included in the Blockchain
* Bitcoin address is a single use token
* The flow diagram for a digital transaction is given below:



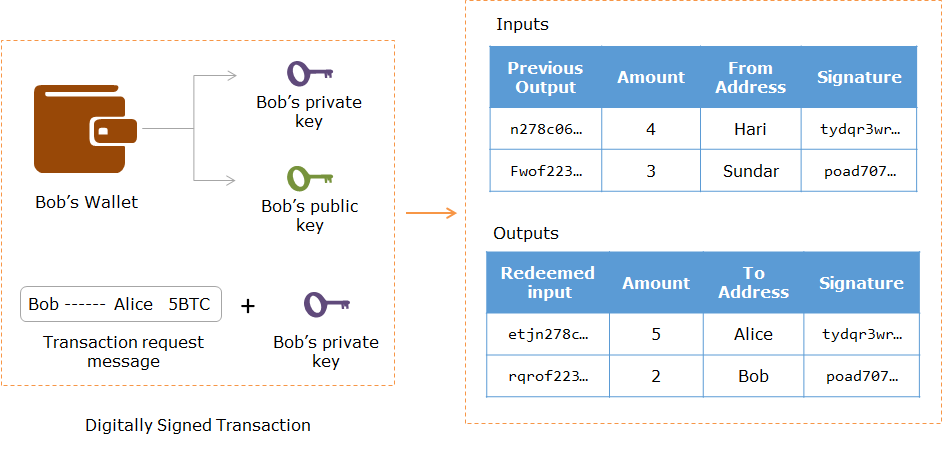
A Bitcoin transaction has 3 parts:

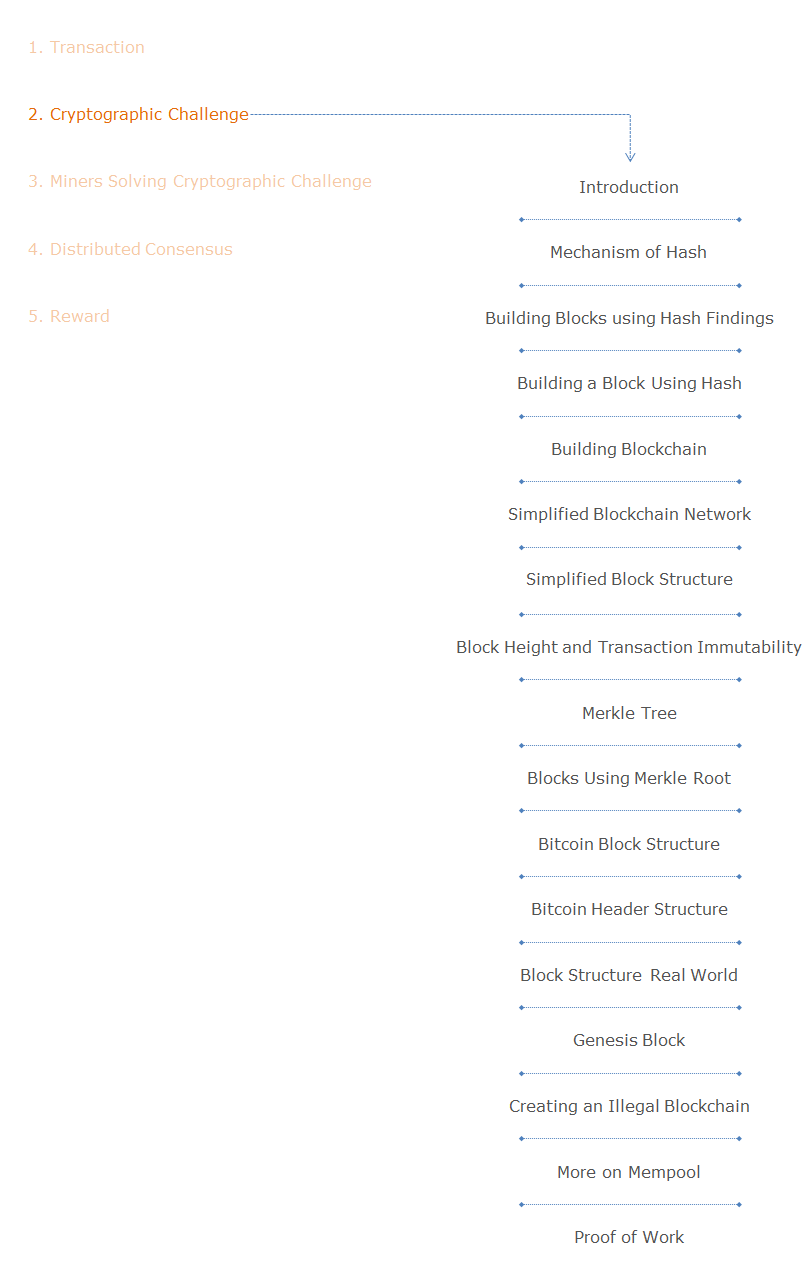
1. Input
   * Input is reference to an output from a previous transaction. Multiple inputs are often listed in the transactions to make up the value you want to transfer
2. Output
   * Output contains instructions for sending bitcoins. Value is the number of Satoshi (1BTC = 100,000,000 Satoshi) this output is worth when claimed
3. Verification
   * To verify that inputs are authorized to collect the values of referenced outputs

* Transaction example:
  + Alice wants to transfer 5 BTC to Bob. Alice checked her previous transactions and found that she had one transaction output with 4 and another with 3 BTC
  + She needs combine these two transactions to make it 5 for Bob and another transaction output back to her 2 BTC
  + In practice there will be one more output which is the transaction fee to be paid to the successful miner for including your transaction in the newly created block

A Bitcoin transaction has 3 parts:

1. Input
   * Input is reference to an output from a previous transaction. Multiple inputs are often listed in the transactions to make up the value you want to transfer
2. Output
   * Output contains instructions for sending bitcoins. Value is the number of Satoshi (1BTC = 100,000,000 Satoshi) this output is worth when claimed
3. Verification
   * To verify that inputs are authorized to collect the values of referenced outputs

* Transaction example:
  + Alice wants to transfer 5 BTC to Bob. Alice checked her previous transactions and found that she had one transaction output with 4 and another with 3 BTC
  + She needs combine these two transactions to make it 5 for Bob and another transaction output back to her 2 BTC
  + In practice there will be one more output which is the transaction fee to be paid to the successful miner for including your transaction in the newly created block
* Consider a scenario where Bob wants to transfer 5 BTC to Alice. The following figure depicts the processes involved:
* 
* Any output can be only once as input and can be tracked using transaction ID.



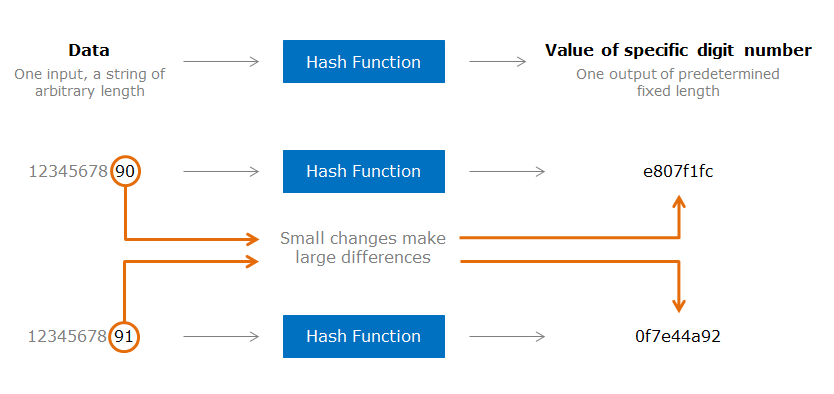
During a transaction between two entities:

* Initially, when a Bitcoin transaction is transmitted to the network it first gets verified by all of the Bitcoin nodes available
* After it successfully passes verification it goes and sits inside the “Mempool” (short for Memory Pool) and patiently awaits until a miner picks it up to include it in the next block. So the Mempool is basically the holding area for all the pending transactions
* The next step is to create a block. A block contains multiple transactions done within a certain period.   Creating the new block is structured as a  cryptographic puzzle which needs to be solved by miners
* Any node can become a miner but the success rate depends on the CPU power
* To understand cryptographic challenge we need to understand hash algorithms and the concept of Merkle tree
* Hash is digital fingerprint of Block
* Hash output of the previous block will be served as one of the input to the next block

A cryptographic hash function takes a string of arbitrary length as input and returns a string with predetermined length.

For a hash function:

* The length of output always remain the same
* It is like a digital fingerprint
* It is a one-way function

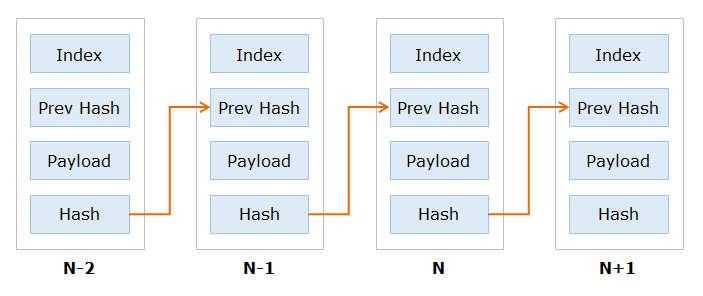


For Bitcoin, hash functions provide one of its very important characteristics, immutability.

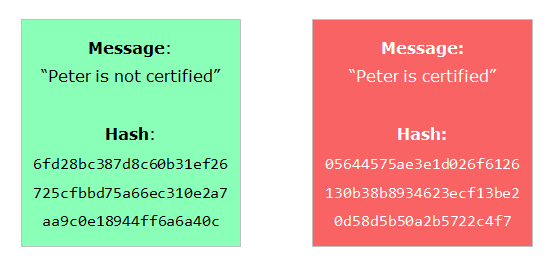
Let us look at how hash function provides immutability.

* For a change in single character (even 0 or 1), it will give a different output
* For the same input it always gives the same output

This characteristics of hash function is very useful in detecting any changes in input and its use in Blockchain gives it the property of immutability.



* A hash chain is a sequence of records in which each record contains the hash of the previous record in the chain, and the hash of all the current record’s contents
* Blockchain uses a cryptographic hash function like SHA256
* Nobody can find two inputs with the same hash value
* Hash chains have the property that every record contains a commitment to all previous records
* Record N+1 contains a commitment to record N which contains a commitment to record N-1, which contains a commitment to record N-3, and so on
* If you change record N, this changes the final hashes of records N+1, N+2, ...
* Result: Once we all accept record N, we have locked in the contents of record 1, 2, 3, ..., N-1 as well



**Scenario 1**

The green card shows a message “Peter is not certified” and its hash. In the red card the message is altered to “Peter is certified”, the system calculates the hash and it turns out to be totally different. But looking at the hash alone one cannot assume that it is tampered. The hash value is random which we cannot predict.

**Scenario 2**

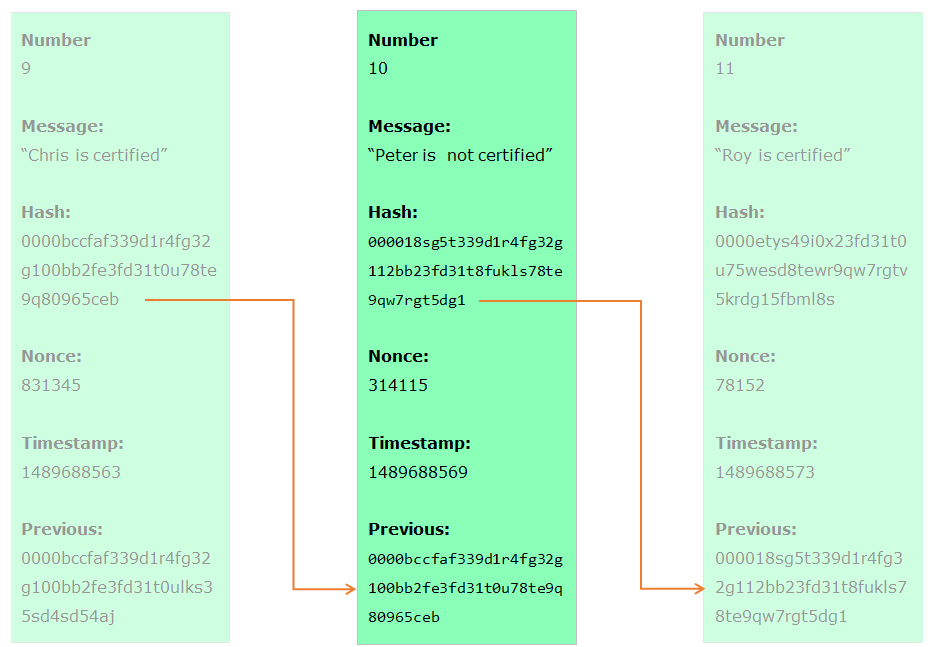
To make it easy to find whether it is tampered we have appended the input with a random number so that the resultant hash output should start with a fixed number of zeros.This random number is called nonce or number used once.



In this scenario, the green card shows a message “Peter is not certified” and its hash which starts with 3 zeros. These 3 zeros make it clear that the hash is less than predetermined value as per the rules of the Blockchain network. If the resultant hash is not starting with 3 zeros, immediately one knows the message is tampered. This random number can be found out only using iteration, ie. using brute force.

**In Bitcoin network:**

* It is necessary to make it more difficult for somebody to tamper with the message and make the hash output less than the predetermined value
* Thus one more variable is introduced, nonce (number used once) and the miner is supposed to try various nonce so that the hash of the message and nonce together should produce a hash value which is less than a predetermined value
* For a nonce calculated already by a miner along with the message gives hash value less than the pre determined number or it starts with certain number of zeros
* If somebody tamper with the message to change “Peter is certified”, the hash value changes and won’t start with so many zeros for the same nonce
  + In-order to get the desired result, one has to find a new nonce which can be done only iteratively and is tough task when it needs to start with many zeros. This is the extra work that must be done by the fraudster to make the message look identical
  + It requires lots of CPU power



Now let us look at what happens when the blocks are chained.

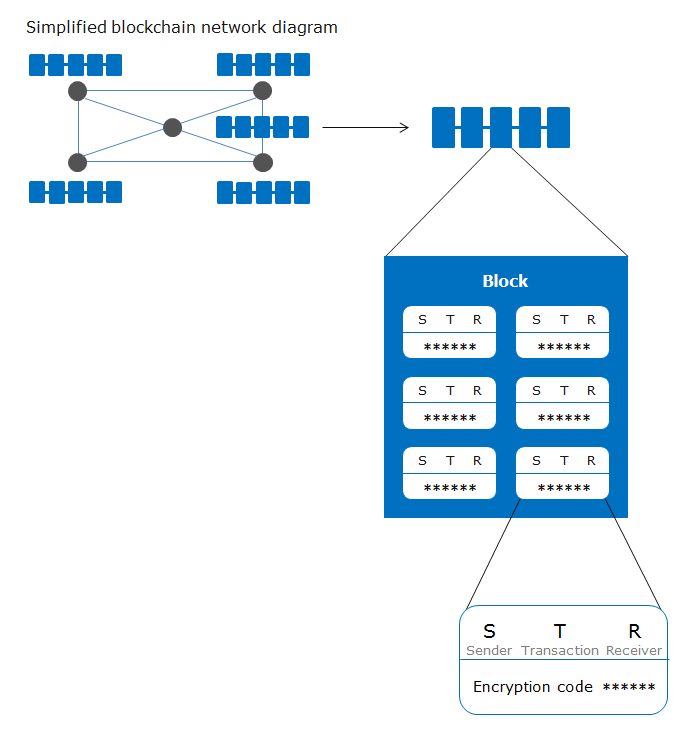
In  Bitcoin Blockchain each block has :

* the message
* Nonce
* hash value from the previous block
* hash value of the present block
* its timestamp

For every block the hash value of the previous block is one of the input. If you tamper with the message in one block its hash value will change and will break the block as well as the all subsequent blocks. This cascading effect, which necessitates to recalculate the nonce for every subsequent block which needs enormous computing power.

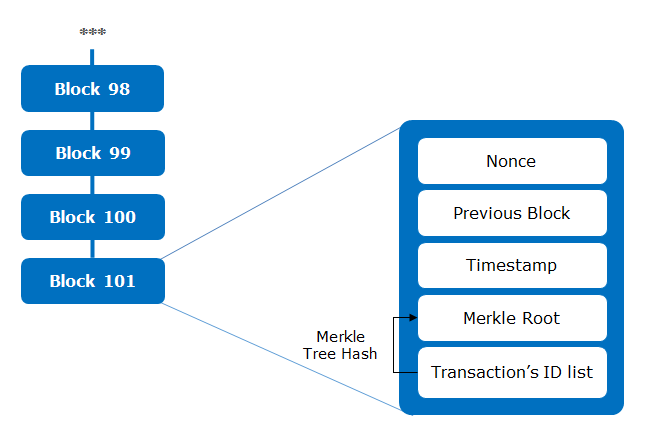
For example just imagine there are 10 blocks at present. If you tamper with the 6th block all the subsequent  blocks will also be broken. Now to re-calculate the nonce it requires lot of CPU power and for bitcoin network typically it takes 10 minutes for creating each block. So to recreate all the subsequent blocks 7, 8, 9 and 10 it takes approximately 50 minutes assuming all nodes have more or less same CPU power.

Bitcoin rule is that the longest Blockchain is the authentic one, with the same difficulty level (same set of preceeding zeros). So other honest miners who builds on the 10th Block onward always will be ahead and win the game.

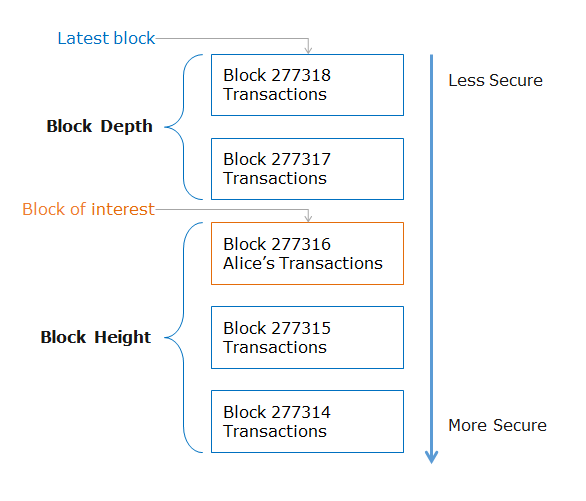


Blockchain network is a peer to peer network where all its members are connected

* All transactions are broadcasted to the network
* Miners who are a subset of members connected to the network is responsible for :
* Directing the transactions requests from users
* Aggregating them
* Validating them
* Adding them to a Blockchain as new blocks
* Each new block is “chained” to the previous block, in linear, chronological order, using a cryptographic hash
* Records cannot be revised and any attempted changes are visible to all participants

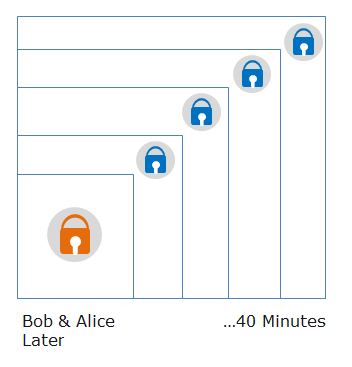


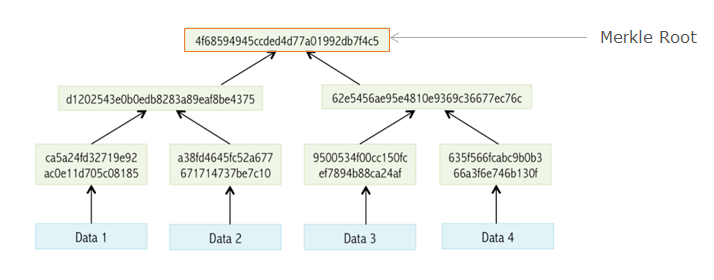
* Every block contains aggregated transactions in a Bitcoin network. It is of 1MB size. Each block is chained to the previous block using hash function and is added in chronological order
* If anybody tamper with any block, its hash value becomes invalid and in turn make all the subsequent blocks also invalid
* To make the Blockchain look valid, the miner has to compute the nonce and hash value for all the subsequent blocks which requires enormous CPU power. As per the Blockchain rule the longest chain is the valid chain
* The rest of the miners will be adding new blocks to the genuine Blockchain while the miner who wants to commit fraud will be wasting time in reconstructing the rest of the blocks
* He can win the race only if he is faster than the rest of the miners combined which is an impossible task unless he has 51% of the computing power of the Blockchain network
* 1 MB Block size limit was introduced by Satoshi foreseeing DOS attacks using dummy transactions
* 1 MB block size can have only 4.4 transactions per second, 65% of it is signature data



* Blocks are normally referenced from their block height number, ie how many blocks from the first block created in 2009
* Block depth is the depth of the block of interest (which contains Alice’s transaction) from the latest block
* The deeper a particular block is from the latest block, the more difficult it is to alter the transactions in that block
* This does not mean that the later blocks are easier altered. This illustration just explains that it is relatively more difficult to alter (double spend etc) the transactions as we go deeper in the earlier chain of blocks
* This makes the records ‘immutable’ or cannot be altered after creation

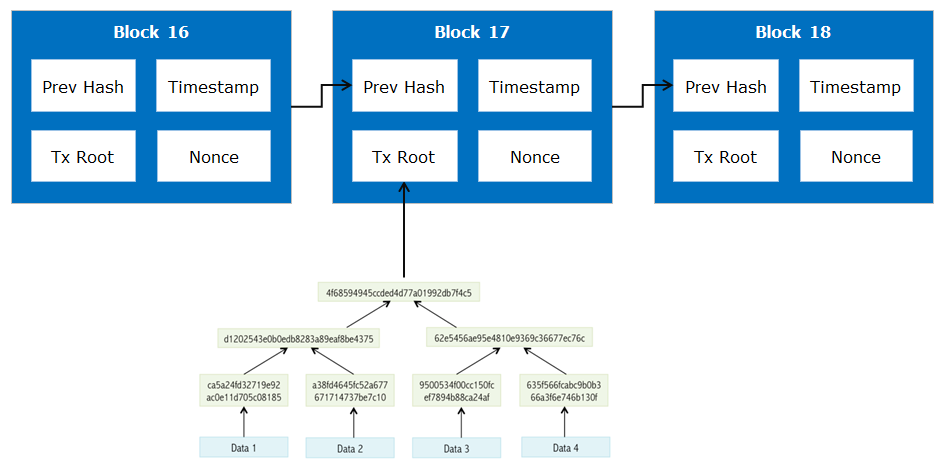
It can be observed from the figure that security increases as more blocks are added.

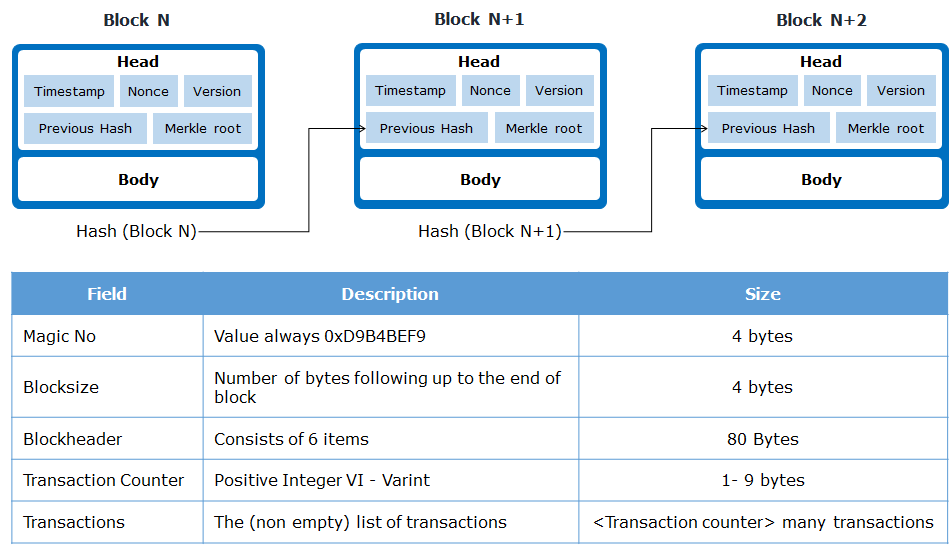




Merkle Tree is the hash of hashes.

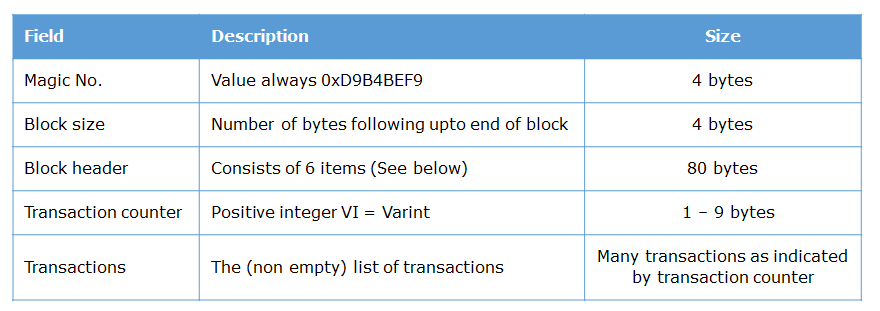
* A tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root
* A block of one or more new transactions is collected into the transaction data part of a  block
* Copies of each transaction are hashed and the hashes are then paired, hashed, paired again and hashed again until a single hash remains called merkle root



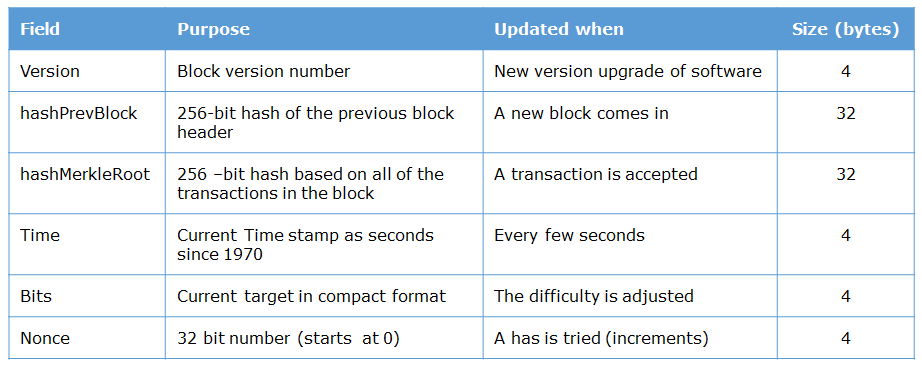
* The blocks are tied together and ensures that a transaction cannot be modified without modifying the block that records it and all other following blocks
* New blocks are added to the blockchain using the concensus protocol
* In a Blockchain, each block is numbered starting from the first block. Each subsequent block is addressed with its block height, which represents the number of blocks between it and the genesis block
* The first-ever block is known as the genesis block
* Block structure is shown here. 4 bytes are allocated for Block size and 80 bytes are allocated for Blockheader.
* 

Block header contains the following information:

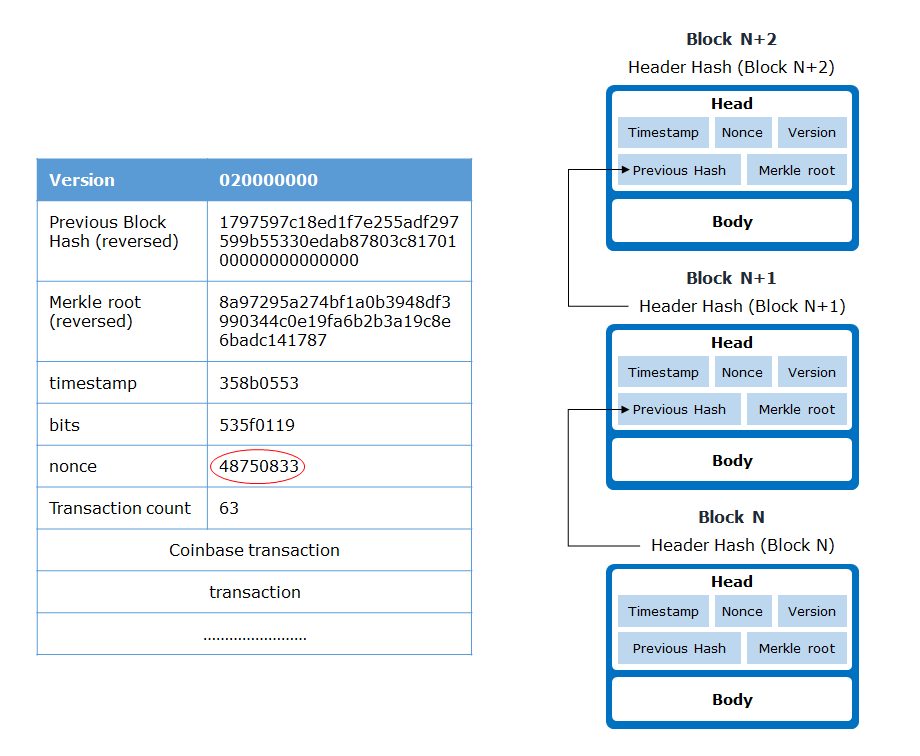
* Version
* Hash of the previous block
* Merkle root hash of all the transactions
* Time stamp
* Nonce
* Difficulty level (bits) which will be explained in later slides



**Block header**



Structure of a block is given below:



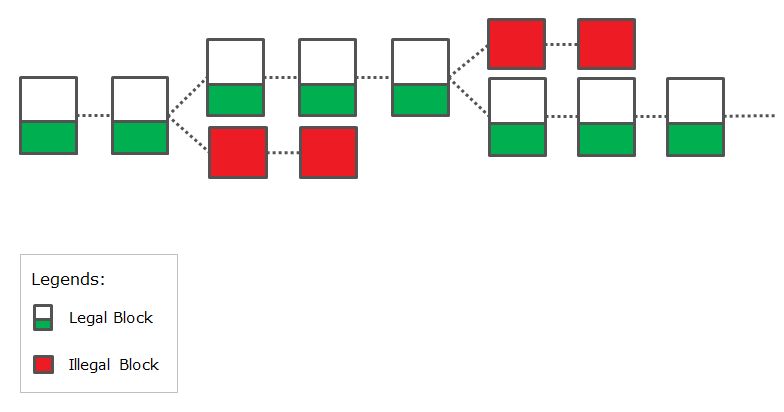
* Bits define the difficulty level
* Block structure has the following information
  + Version number, previous block hash
* Nonce is calculated using brute force with all possible values of nonce in order to find a hash smaller than the target hash. It is the most tedious process in block creation.

The Coinbase transaction, or Generation transaction, is a special transaction in the Bitcoin protocol that differs from a standard transaction as it creates coins from nothing. It is the reward that miner gets for successfully mining the block. So it is the mining reward plus the sum of all transactions fees included in the block

Genesis block was created on 3rd Jan 2009 by Satoshi Nakamoto, it is hard coded.



                                                                                                                                 Source: [blockchain info](https://blockchain.info/block-height/0)



In order to conclude an illegal transaction as a consensus in the Bitcoin blockchain, it is necessary to continue creating blocks faster than the authentic fork or re-create all past blocks.

* This requires a 50% or larger percentage of the total computing power necessary
* It is much more economically rational to obtain rewards through proper mining, which discourages people from conducting illegal transactions
* Trying to submit an altered block would change hash function of that block and all following blocks—nodes would detect and reject block

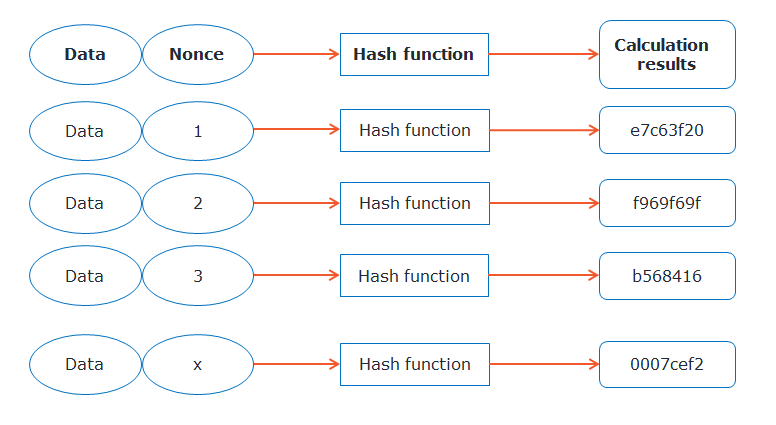
Mempool:

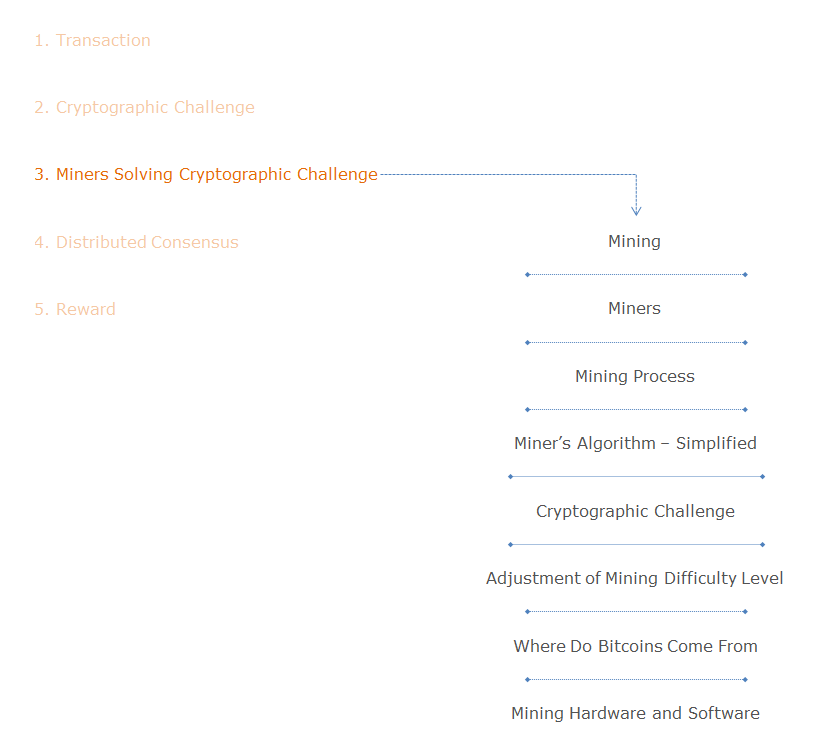
When a Bitcoin transaction is transmitted to the network it first gets verified by all of the Bitcoin nodes available. After it successfully passes verification it goes and sits inside the “Mempool” (short for Memory Pool) and patiently awaits until a miner picks it up to include it in the next block. So the Mempool is basically the node’s holding area for all the pending transactions.

* The bitcoin mempool is a collection of all transactions waiting to receive a network confirmation, waiting to be picked up by a miner
* Each node has it’s own mempool and can set the preferred size
* When a new block is broadcasted to the network, each node removes the transactions that are in the mempool that have been confirmed
* If the Mempool size gets too close to the RAM capacity, the node sets up a minimal fee threshold
* Transactions with fees per kB lower than this threshold are immediately removed from the Mempool
* Only new transactions with a fee per kB large enough are allowed access to the Mempool
* Mempool is a bottleneck in Bitcoin network waiting to be addressed as part of BIP (Bitcoin Improvement Protocol)

In Bitcoin, the security of the network relies on a proof of Work (POW) algorithm called mining.POW is based on HashCash invented by Adam in 1990

* Each node that wants to participate in the mining is required to solve a computationally difficult problem to ensure the validity of newly mined block.
* A miner with a p fraction of the total computing power can win the reward and create a new block with a probability p
* An attacker is required to solve the same task as the rest of the bitcoin network; so an attack on bitcoin needs exceptionally large computing power (more than 50% of the total computing power of the network)





Mining



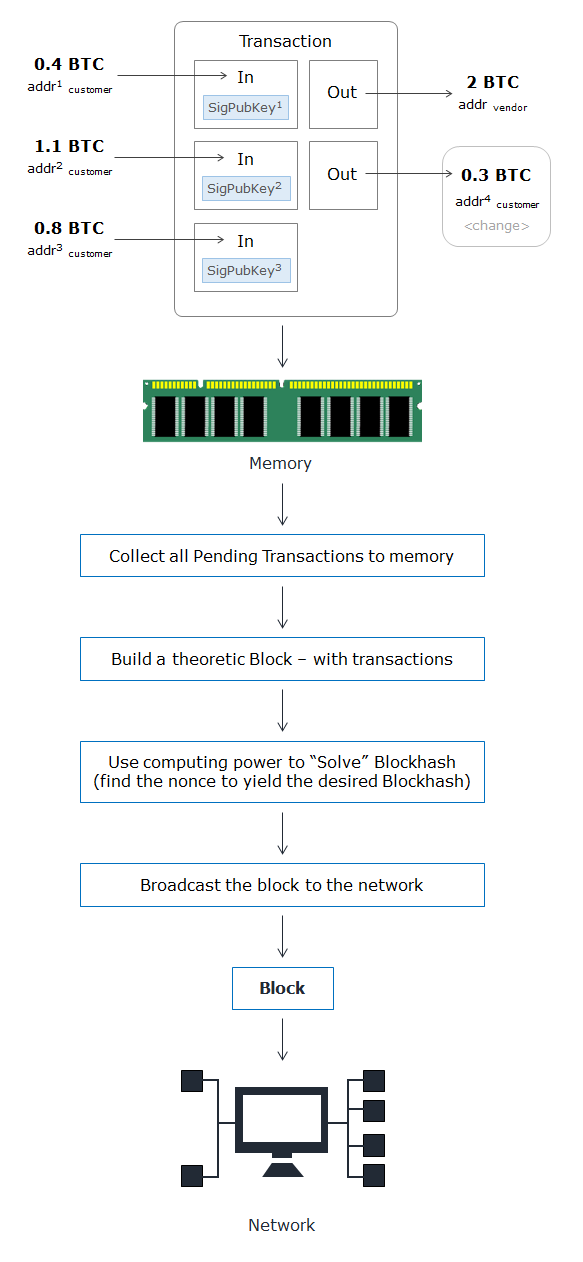
Miners are responsible for creating new block which involves lots of computational work. So they are rewarded with new bitcoins, so the name miners. Creating hashes is computationally trivial, but the Bitcoin System requires that the new hash value have a particular form, specifically it starts with a certain number of zeros.

* Miners have no way to predict which nonce will produce a hash value with the required number of leading zeroes
* Miners need to try with as many random nonce needed to arrive at the hash value desired
* Miners are are responsible for:
  + Detecting transaction requests from users
  + Verifying a transaction
  + Aggregating transactions into a block
  + Mining new block
  + Validating the new block

Miners are of three types, individuals, group / pool and professional. Mining requires lots of computational power and electricity. In early days people mined using a single Laptop. Now with the number of transactions increasing, the CPU power requirement has gone up a lot. We need specialized hardware to mine; which is often extremely difficult. Hence, many miners join together as a group and mine so that they are more successful. Ordos City in New Mongolia Province in China is known for its large concentration of Bitcoin Miners. You can see the details in the link given here. https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/

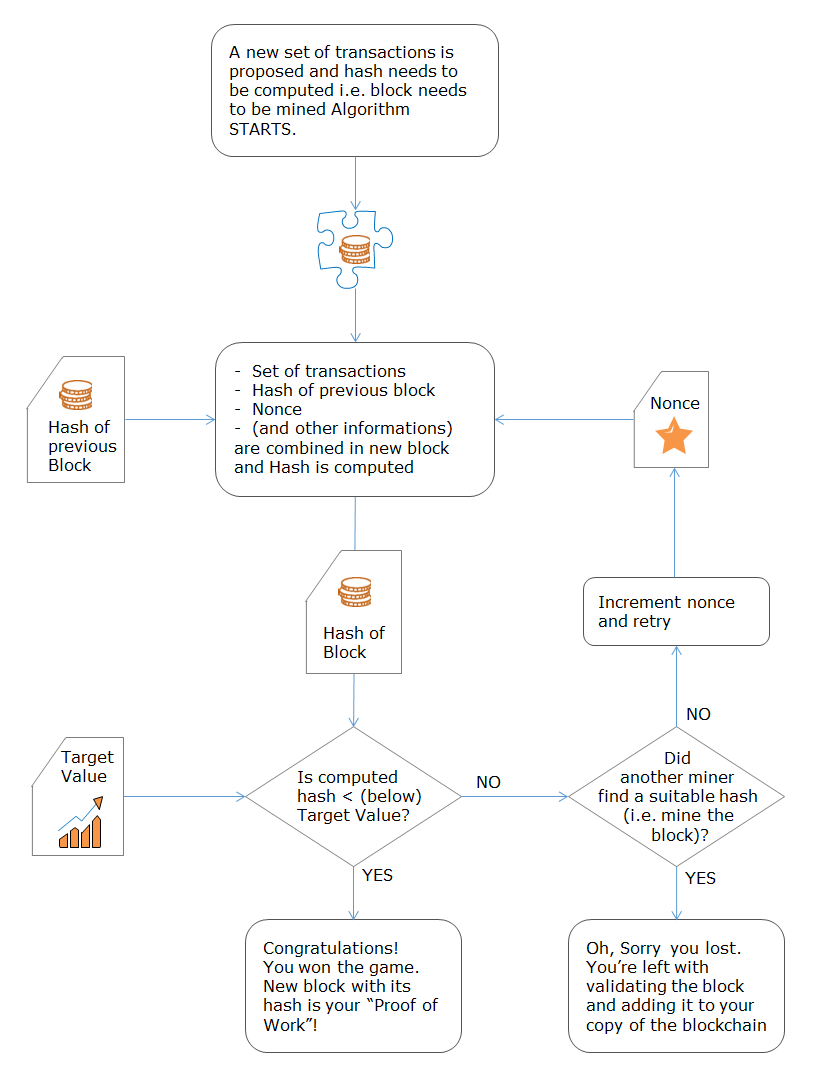
* **Individuals**
  + Setup with a single computer to mine bitcoins
  + The investment in equipment and energy now needed to be successful are high, hence individual miners are now rare
* **Group or Pool**
  + Several people or organizations pool their computing power to maximize their probability of success in validating a block
  + Each miner receives payment based on the total volume of bitcoins received by the group, in proportion to the power that was made available to the community
* **Professional**
  + Highly organized professional mining companies have developed techniques for mastering the mining chain from end to end and maximizing use of their hardware and computing power

Mining Process :



Mining process as depicted above deals with the following operations:

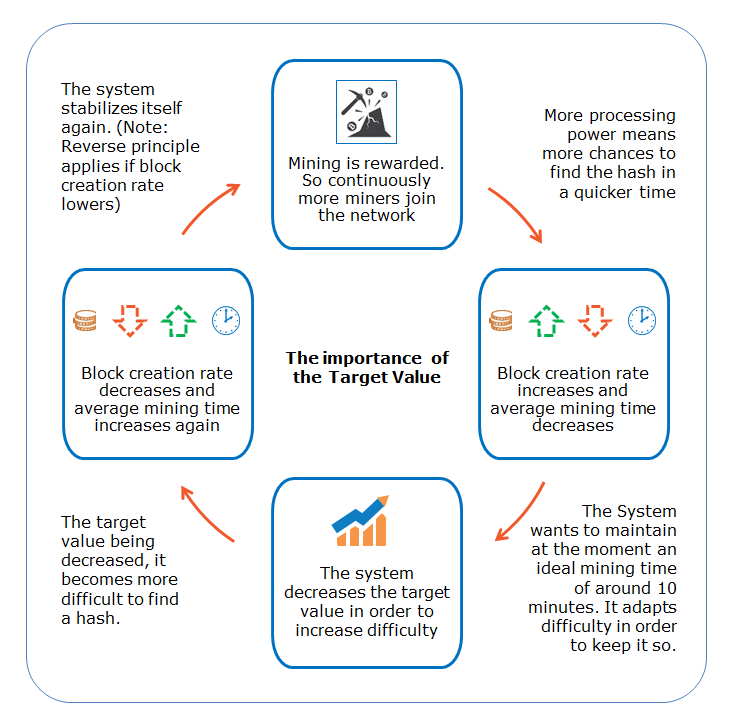
* All transactions are broadcasted to every node for verification
* Once verified it is stored in a temporary memory called mempool to be picked by the miners
* Miners pickup transactions from mempool queue and work on solving the cryptographic puzzle (to find the nonce) so as to give a hash starting with predetermined number of zeros
* Whoever first solves this puzzle creates the new block and broadcast it to the network for all other miners to verify
* Once it is validated by the majority miners, the new block is appended to the existing Blockchain and miner will get a reward of 12.5 BTC as of now
* Solving the puzzle involves huge CPU power and it is called Proof of Work
* POW is designed in such a way that it is tough to produce but easy to verify



* The block chain serves to confirm transactions to the rest of the network as having taken place
* Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere
* Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady
* Individual blocks must contain a proof of work to be considered valid
* This proof of work is verified by other Bitcoin nodes each time they receive a block

Adjustment of mining difficulty

Ideal Mining Time is 10 minutes, any variation in this has to be dealt with.



* Time decreases as more and more miners join or improving the computing power
* Time increases when the target value (hash) decreases

So difficulty level is increased / decreased to maintain the same average mining time. For bitcoin, every 2016 blocks the difficulty level is adjusted (2 weeks).

Where do bitcoins come from:



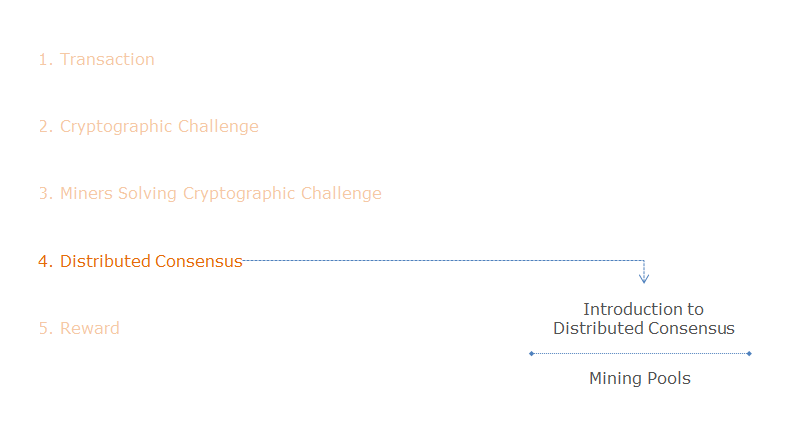
                                                                                    Source: [KryptoMoney](http://kryptomoney.com/)

* Bitcoin miner creates a new block at every 10 minutes and gets 12.5 BTC as reward
* In every 21000 transactions, difficulty level of solving the cryptographic puzzle is adjusted to maintain the time (10’)
* The reward will be halved every 210000 blocks
* There are currently 16million BTC in circulation and there is a cap of 21M BTC as per the rules and the cap will be reached by 2140 AD

Mining hardware and software

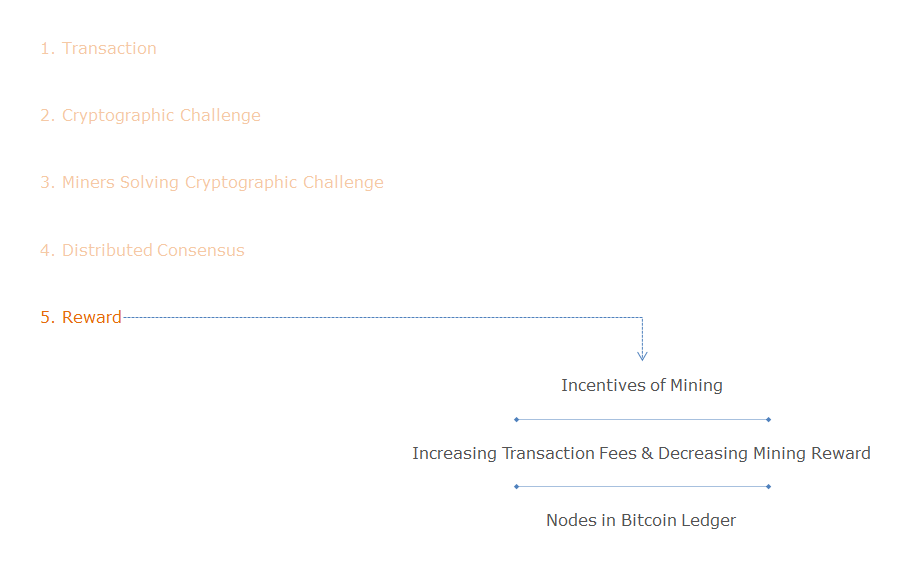
Mining needs specialized hardware to be successful. These equipped with ASICS specialized for solving this puzzle. Mining hardware is available from many vendors Avalon, Bitfury etc..

* Get [mining hardware](http://profit.hashflare.eu/en/?ref_id=539A7635)
* Download free [Bitcoin mining software](http://https/www.bitcoinmining.com/bitcoin-mining-software/)
* Join a [Bitcoin mining pool](http://p2pool.in/)
* Setup [Bitcoin wallet](https://www.youtube.com/watch?v=N4rCBTTInyg&ab_channel=SmartITSolution)
* Stay upto date with [Bitcoin news](https://news.bitcoin.com/)



The following steps take place once a cryptographic challenge is solved.

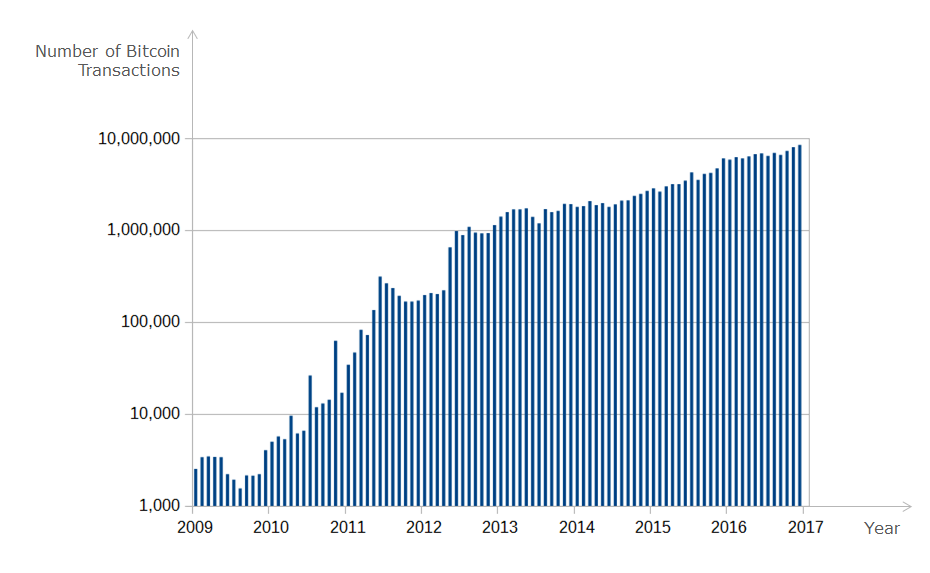
* Once the miner is successful in finding the desired nonce he has all the inputs to create the new block
* He creates the new block and broadcast to the network for approval by others
* The miners pick it up, verify it and add it to their current Blockchain
* Once the majority approves, the newly added block is confirmed and is added to the end of the blockchain
* This process is called consensus



Incentives of mining is mainly the reward earned by miners for solving each puzzle and the transaction fees. As the time goes by the mining rewards decreases but the amount earned through transaction fees increases. So in the future it will become almost steady.

* Miner gets a reward of newly mined 12.5 BTC and transaction fees
* Block reward is halved in every 2100000 blocks, which becomes 0 by 2140, 33rd phase
* In the coming years as the transactions increase, transaction fees are meant to replace block rewards

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 BTC.



                                                                                                                                         Source: [wikiwand](https://www.wikiwand.com/en/History_of_bitcoin)

Above graph depicts the number of bitcoin transactions per month (logarithmic scale).

* For every transaction miner expects a fee and it is not constant
* In the initial days of bitcoin the transaction fees were in fraction of a penny, now it is in the range of few dollars, and it does not depend on  the transaction amount but depends on the space it needs in the block
* Bitcoin block space is a scarce commodity, getting a transaction mined can be seen as purchasing a portion of it
* The price of block space is set by supply and demand
* In the real world the supply of space for transactions is extremely noisy, because more becomes available (and has to be immediately consumed or it’s lost forever) every time a block is mined
* As the mining reward comes down over time the number of transactions increases and transaction fees compensates for the loss of revenue for miners

Forking

A Fork takes place when a Blockchain splits into two different path forward.

* Bitcoin is an open source software. Changes and modifications in the working of software has to be approved by consensus
* If a group of nodes modify their software without consensus, those nodes then invalidate a rule held by the rest of the network and create their own fork of the blockchain

Forking is generally clasiified into two:

1. **Hard Fork**
   * Broadening or removing the rules
   * Introduces a change that forces every one to upgrade
2. **Soft fork**
   * Tightening the rules
   * Introduces a change that is backward compatible
   * Upgrading is not required

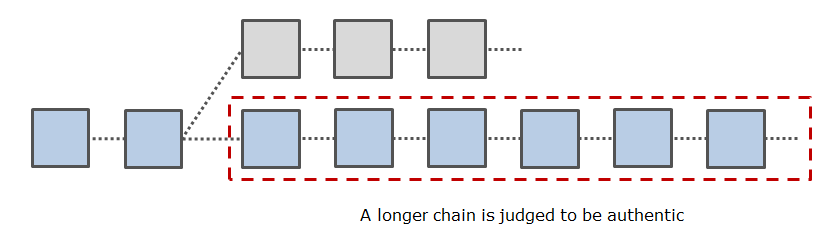
In order to conclude an illegal transaction as a consensus in the Bitcoin blockchain, it is necessary to continue creating blocks faster than the authentic fork or re-create all past blocks.

* This requires a 50% or larger percentage of the total computing power necessary
* It is much more economically rational to obtain rewards through proper mining, which discourages people from conducting illegal transactions

Blockchain Forking

A fork can also be generated temporarily in the Bitcoin blockchain. In such cases, multiple nodes in a P2P network almost simultaneously succeed in PoW.

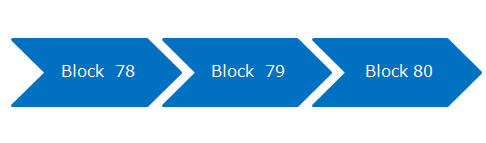
* In such a case, a chain that becomes longer thereafter is judged as the authentic one
* To finalize a transaction, it is necessary to confirm that the relevant blockchain does not fork after the transaction data is incorporated in the block and multiple blocks are created thereafter
* When approximately six blocks are additionally created, the relevant blockchain is considered to be the authentic one
* There may be temporary disagreement if two proposals occur at the same time; eventually, with very high probability, one proposal will be established by picking the longest blockchain



Resolve Conflicts

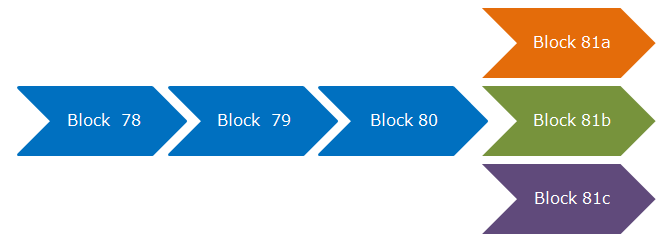
A common conflict is when multiple miners create blocks at roughly the same time. Because blocks take time to be shared across the network. Which one should be counted as the legit block?

Let’s say all the nodes on the network have synchronized their blockchains and they are all on block number 80.

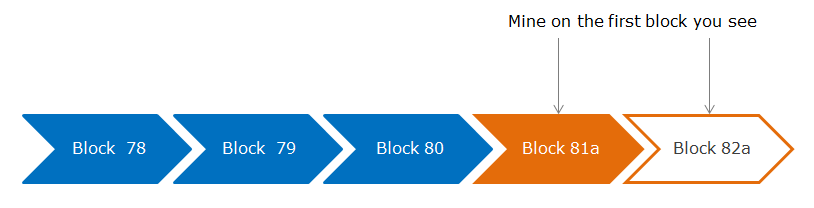


If three miners across the world create ‘Block 81’ at roughly the same time. Which ‘Block 81’ should be considered valid?

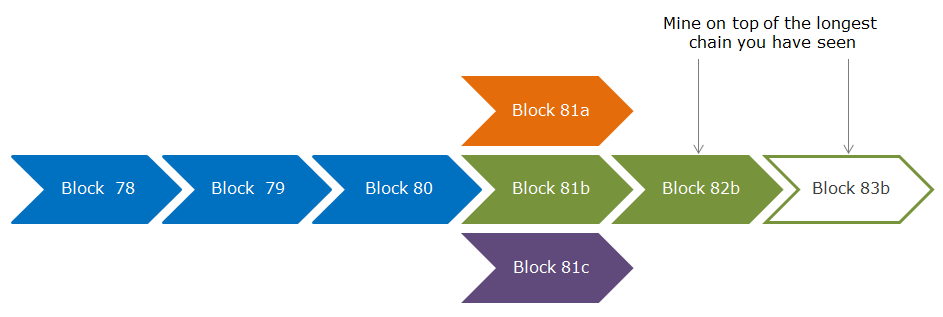
* Remember that each ‘Block 81’ will look slightly different, they will certainly contain a different payment address for the 25 BTC block reward; and they may contain a different set transactions. Let’s call them 81a, 81b and 81c.



* Treat the first block you see as legitimate



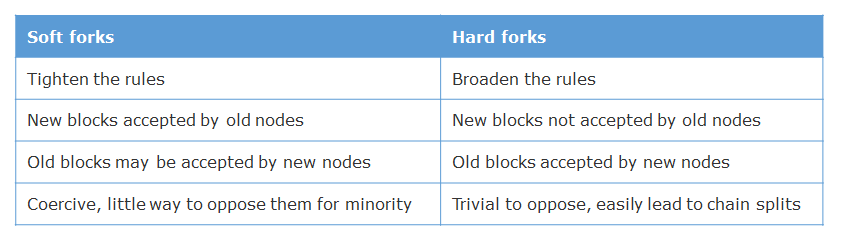
* Longest Chain rule: If you see multiple blocks, treat the longest chain (with most difficulty) as legitimate



Software forks proposing consensus rule forks: Bitcoin Unlimited, Bitcoin Classic and Bitcoin XT.

* Soft consensus forks render previously valid blocks invalid and create security risks for non-upgrading nodes
* Hard consensus forks render previously invalid blocks valid and make non-upgrading nodes incompatible
* Unplanned forks pose the greatest risk and are generally caused by poorly understood software complexity or rushed changes
* Both soft and hard consensus forks can be used to make complex changes to bitcoin; soft forks merely require a lower amount of consensus

The main differences between the two types of forking, Soft fork and hard fork are tabularised below.

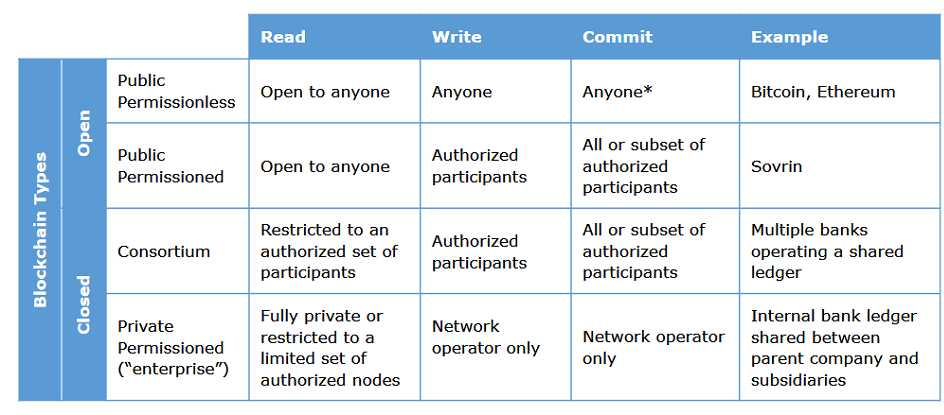


The following links are examples of how blockchain operations happen in the real world.

* [Block explorer](http://blockexplorer.com/)
  + Block size is less than 1MB
  + Less than 2000 transactions in a block
  + One block is added every 10 minutes
* [Blockchain info](http://blockchain.info/)
* Blockchain.info - [Blockchain Charts](https://blockchain.info/charts)

 Types of block chain

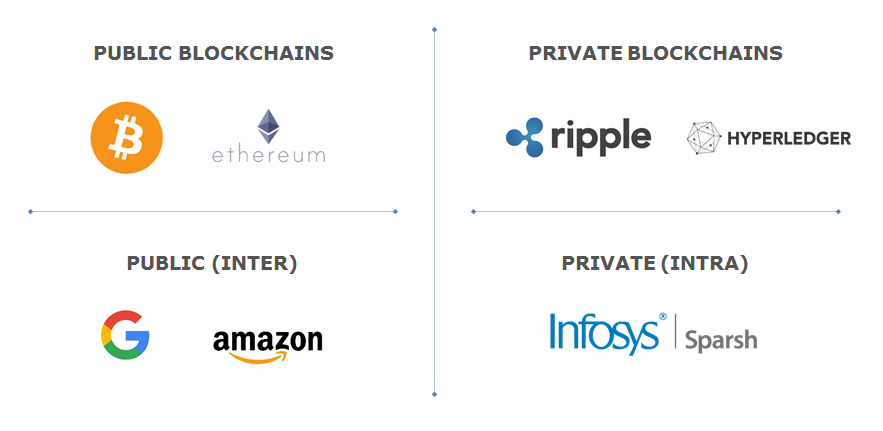
Let us look at the types of Blockchain; basically there are three types of blockchain: Public or Permissionless, Private or Perminssioned and hybrid Blockchain. Bitcoin Blockchain network is a permissionless blockchain where no permissions are required to become members, so the members of this Blockchain network are un-trusted. Hence, it needs extensive CPU power to work on the creation and approval of new blocks. In contrast the permissioned Blockchain members require permission to join and are considered to be trust worthy. Therefore mining using POW can be omitted. This saves lot of energy as well as latency issues. Thus it is widely used in enterprises and transaction between banks. Then there are systems which uses a mix of permissioned and permissionless blockchains. These are called Hybrid blockchains.



* Public and permissionless blockchains resemble bitcoin, the original Blockchain uses complex consensus protocols
* Private and permissioned blockchains use simple consensus protocols
* Hybrid blockchains, another emerging concept of sidechain, allows for different blockchains (public or private) to communicate with each other, enabling transactions between participants across blockchain networks

In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored and shared.

* As we move from permissionless public shared system to permissioned private shared systems, we are moving from distributed ledgers to centralized ledgers. The members who have access need to be more and more trusted and it require less and less computing power to validate
* The chain could also be modified so that stricter access control applies. The strictest access control is that, only the owner of the chain could have full access of the chain whereas others have no access at all. This may be similar to the way a central database stores confidential data



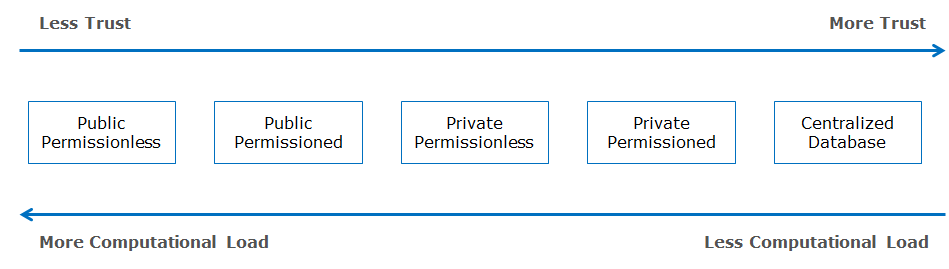
Public blockchain is based on complex consensus protocol whereas private blockchain runs on simple consensus protocols. So permissioned blockchain is ideally suited for enterprise application where the members of the blockchain network will be their own employees who can be trusted. So there is lot of interest in permissioned blockchain.

Turst Model:

Look at how the trust model changed over the years.

* Oldest Trust Model (Hunter Gatherer)
  + Show me your armies
* Old Trust Model
  + Show me your reputation and relationships
* Current Trust Model
  + Show me your license
* New Trust Model (Civilized society)
  + Show me your code

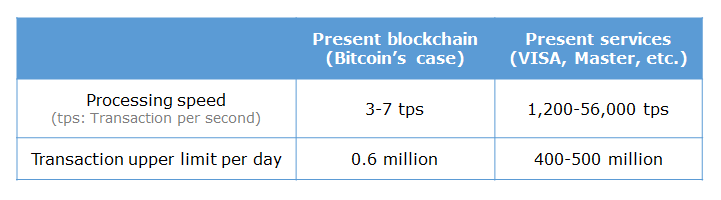
Below given is the blockchain spectrum of trust:



Following are the disadvantages of bitcoin technology :

* **Difficult to use**
  + Bitcoin software is not customer friendly
  + Most of the bitcoin software used to control, custody, operate and transact are complex
* **Difficult to access**
  + Purchase of bitcoins is regulated in many countries
* **Difficult to secure**
  + Blockchain and cryptographic protocols used in bitcoin are secure but the users must safeguard their private key. The whole security depends on the storage and handling of one’s private key
  + Lack of protections against mistakes
  + Transactions done cannot be reversed. Any mistake cannot be corrected
  + Loosing private key results in the loss of the entire bitcoin fund, administrators cannot help to regain access
* **Limited institutional adoption**

The adoption of bitcoin is limited compared to the existing financial payment systems

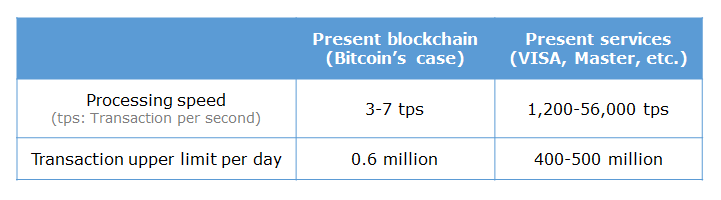


Disadvantages of bitcoin:

Following are the disadvantages of bitcoin technology :

* **Difficult to use**
  + Bitcoin software is not customer friendly
  + Most of the bitcoin software used to control, custody, operate and transact are complex
* **Difficult to access**
  + Purchase of bitcoins is regulated in many countries
* **Difficult to secure**
  + Blockchain and cryptographic protocols used in bitcoin are secure but the users must safeguard their private key. The whole security depends on the storage and handling of one’s private key
  + Lack of protections against mistakes
  + Transactions done cannot be reversed. Any mistake cannot be corrected
  + Loosing private key results in the loss of the entire bitcoin fund, administrators cannot help to regain access
* **Limited institutional adoption**

The adoption of bitcoin is limited compared to the existing financial payment systems



Pursuit of Alternate blockchain:

Every technology needs improvement. Blockchain is at its younger years, so a better one that solves all the demerits of the current technology is being sought after. The main attributes of this alternative blockchain are:

* Faster settlement
* Larger transaction sizes
* Additional consensus methods
* Varying degrees of anonymity
* Advanced functionality
* Adjustable permissions

Links:

<https://blockchaininformer.com/>

<https://www.facebook.com/BlockchainInstituteofTechnology/>

https://twitter.com/Blockchaininfos