I INTRODUCTION TO BLOCKCHAIN

Introduction to blockchain .

Basics of blockchain-Public Ledgers-Block Chain as Public Ledgers-Types of Block chains- Pillars of Block chain- Government Initiatives of Block Chain – Bitcoin – Smart Contracts.

1.1 Basics of Blockchain

"A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography." The concept is introduced by **Satoshi Nakamoto 2009**

Block

1.Data :"hello everyone"
2.Prev Hash:23432FRT123
3.Hash :123FFRE342

Blockchain

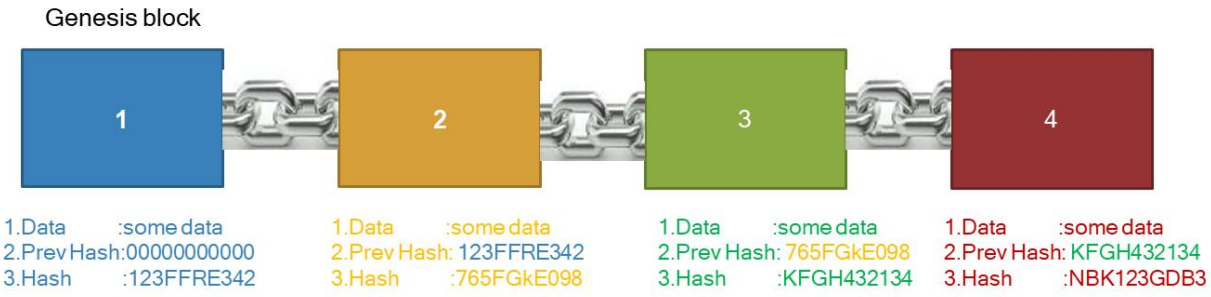


Figure 1.1.All blocks are cryptographically link together

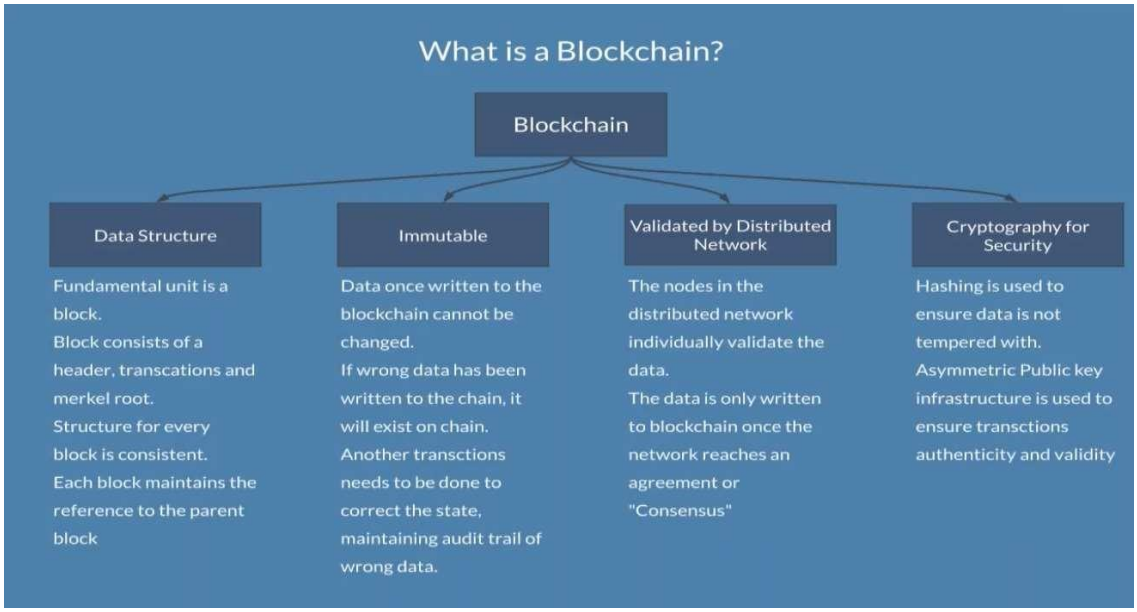


Figure 1.2 blockchain Features

Blockchain

- Blockchain is simply a data structure where each block is linked to another block in a time- stamped chronological order
- It is a distributed digital ledger of an immutable public record of digital transactions.
- Every new record is validated across the distributed network before it is stored in a block.
- All information once stored on the ledger is verifiable and auditable but not editable .
- Each block is identified by its cryptographic signature.
- The first block of the blockchain is known as Genesis block

“To access data of the first ever created block ,you have to traverse from the last created block to the first block”

How trading happens Using Current System

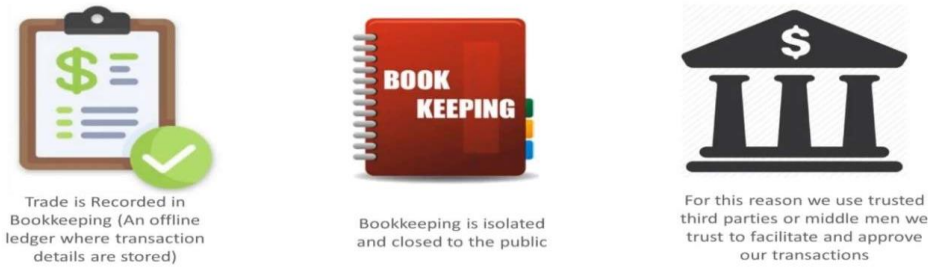


Figure 1.3 Traditional transactions

Ledger

A ledger is a record-keeping book that stores all the transactions of an organization.

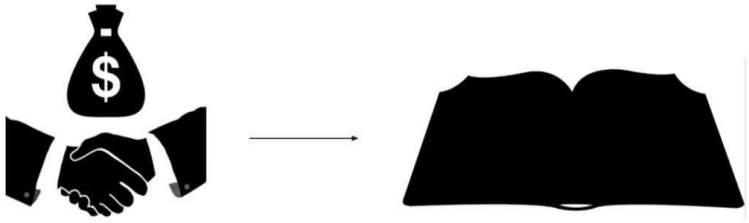


Figure 1.4 Ledger

Problems with the current system

- ❑ Banks and other third parties take fees for transferring money
- ❑ Mediating costs increases transaction costs
- ❑ Minimum practical transaction size is limited;
- ❑ Financial exchanges are slow. Checking and low cost wire services take days to complete
- ❑ System is opaque and lacks transparency and fairness
- ❑ Also, central authority in control can overuse the power and can create money as per their own will

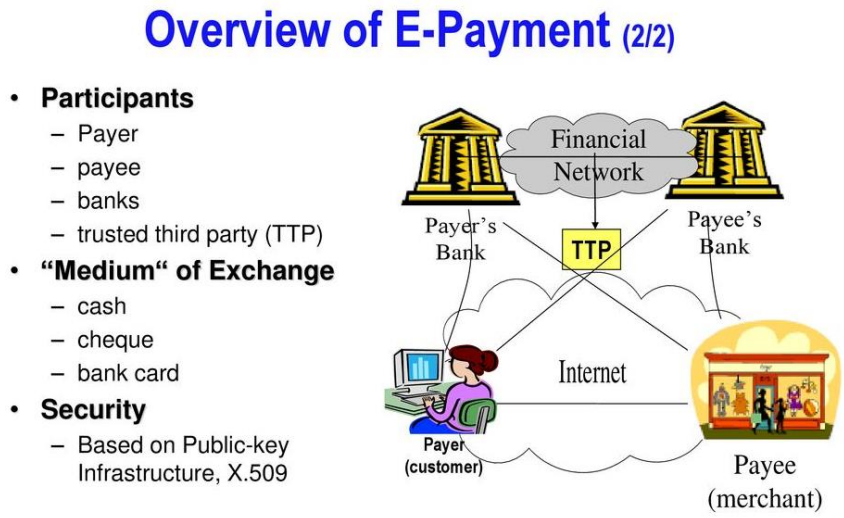


Figure 1.5 Traditional payments

We need a system which:

- Eliminates the need of middlemen or Third parties thereby making transaction costs nil or negligible.
- Enhance transaction execution speeds and can facilitate instant reconciliation.
- Is transparent and tamper resistant in order to avoid manipulation or misuse.
- Currency creation is not in control of any central authority.
- Is regulated to maintain the value of the currency.

Distributed system attempt to solve the problem

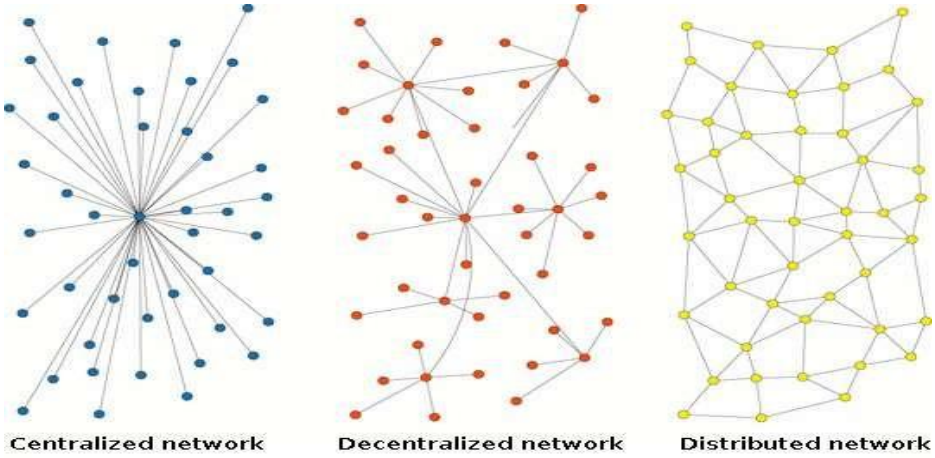


Figure 1.6 Different network of systems

Distributed system enables a network of computers to maintain a collective bookkeeping via internet this is open and is not in control of one party. it is available in one ledger which is fully distributed across the network.

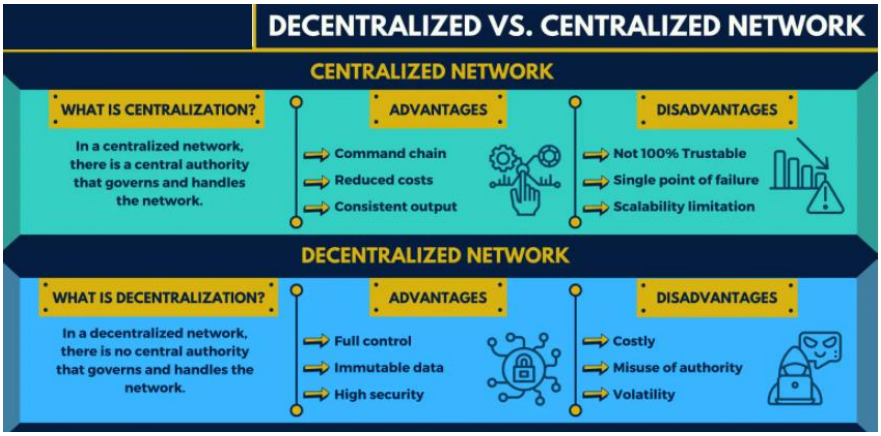


Figure 1.7 Centralized Vs Decentralized

- Most of the Internet applications we use every day are centralized, they are owned by a particular company or person that provision and maintain the source code to execute on a computer, server or maybe even a cluster.

Decentralized Applications

Figure 1.8 Decentralized network

- Decentralized means no node is instructing any other node as to what to do.
- The code runs on a peer-to-peer network of nodes and no single node has control over the dApp.
- Depending on the functionality of the dApp, different data structures can be used to store the application data.
- Bitcoin uses a blockchain decentralized ledger of transactions.

Distributed Applications

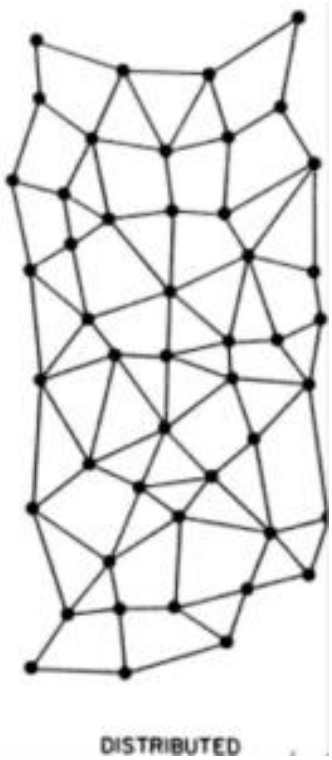


Figure 1.9 Distributed applications

- Applications in which computation is distributed across components, communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal.
- Some distributed applications examples are:
- CDN
- AWS
- Cloud Instances
- Google, Facebook, Netflix, etc

Distributed system

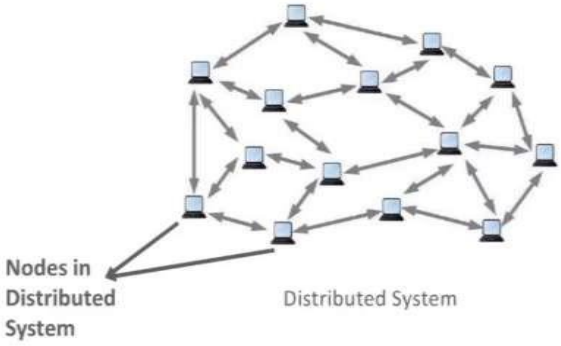


Figure 1.10 Distributed system

- A System where two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome
- It's modeled in such a way that end users see it as a single logical platform.

What is a node ?

- A node can be defined as an individual processing unit in a distributed system
- All nodes are capable of sending and receiving messages to and from each other.

Introduction – Blockchain

Blockchain technology is a **distributed ledger technology** originally proposed for the crypto-currency **Bitcoin.**

FEATURES

- Immutable and tamper-proof data store
- Sequential Chain with Cryptographic hashing
- Trust-free Consensus-based transactions
- Decentralized peer-to-peer network
- Distributed shared ledger

What is Blockchain?

A blockchain is a decentralized, distributed public ledger where all transactions are verified and recorded.

Blockchain is a system comprised of..

Transactions

Immutable ledgers

Decentralized peers

Encryption processes

Consensus mechanisms

Optional Smart Contracts

Transactions

As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken

Proof of history, provides provenance

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

Immutable

As with existing databases, Blockchain retains data via transactions.

The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.

The transaction is, immutable, or indelible

In DBA terms, Blockchains are Write and Read only

Like a ledger written in ink, an error would be resolved with another entry.

Decentralized Peers

Rather than the centralized "Hub and Spoke" type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

Figure 1.11 Legacy network Vs blockchain network

Encryption

Standard encryption practices.

Some Blockchains allow for "BYOE" (Bring Your Own Encryption)

All blocks are encrypted

Some Blockchains are public, some are private

Public Blockchains are still encrypted, but are viewable to the public, e.g. https://www.blocktrail.com/BTC

Private Blockchains employ user rights for visibility, e.g.

Customer – Writes and views all data

Auditors – View all transactions

Supplier A – Writes and views Partner A data

Supplier B – Writes and views Partner B data

Consensus

Ensures that the next block in a blockchain is the one and only version of the truth.

Keeps powerful adversaries from derailing the system and successfully forking the chain

consensus algorithm is a process in computer science used to achieve agreement on some information among the distributed systems.

The consensus algorithm was designed for the blockchain technology to achieve reliability in a blockchain network having multiple nodes.

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others....

Figure 1.12 Consensus mechanism

Smart Contracts

Computer code

Provides business logic layer prior to block submission.

Table 1.1 Example blockchain netwoks

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

How Blockchain Works?

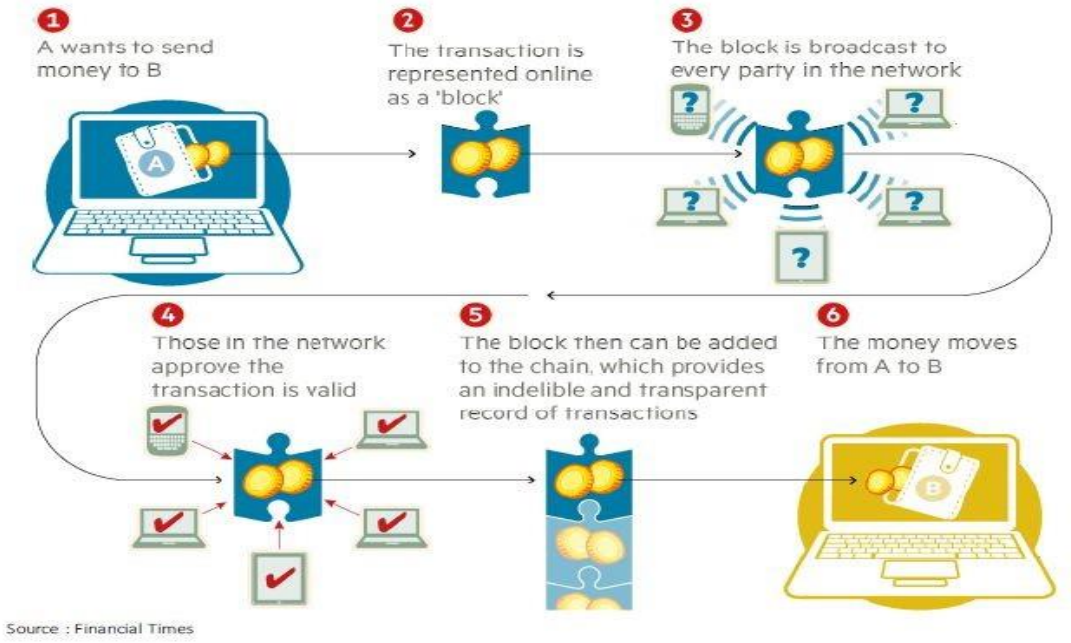


Figure 1.13 Blockchain working model

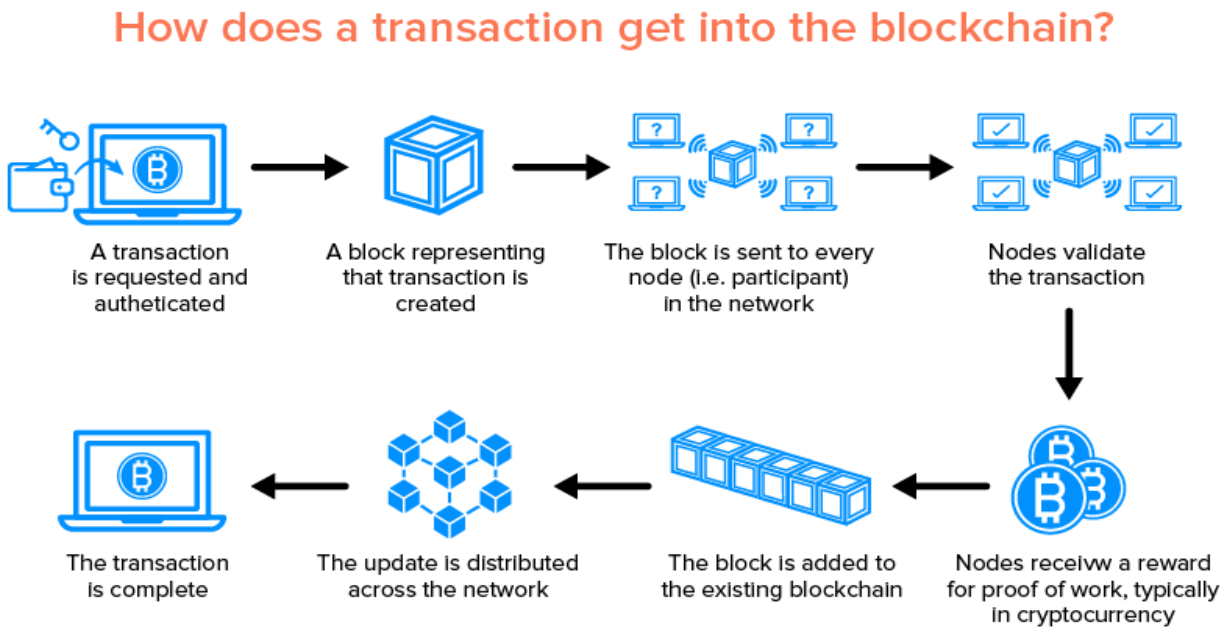


Figure 1.14 Blockchain Flow diagram

Elements of blockchain

- blockchain has five elements: Distribution, encryption, immutability, tokenization and decentralization.

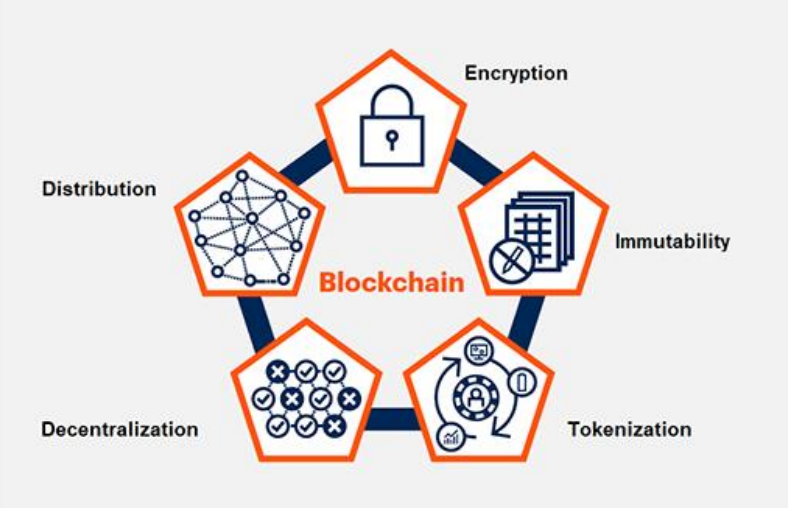


Figure 1.15 Features of blockchain

- **Distribution:** Blockchain participants are located physically apart from each other and each node copy of a ledger that updates with new transactions as they occur.
- **Encryption:** Blockchain uses technologies such as public and private keys to record the data in the blocks securely.
- **Immutability:** Completed transactions are cryptographically signed, time-stamped and sequentially added to the ledger.
- **Tokenization:** Transactions and other interactions in a blockchain involve the secure exchange of value.
- **Decentralization:**Both network information and the rules for how the network operates are maintained by nodes due to consensus mechanism.

Benefits of Blockchains

Benefits of Blockchains Over Traditional Finance

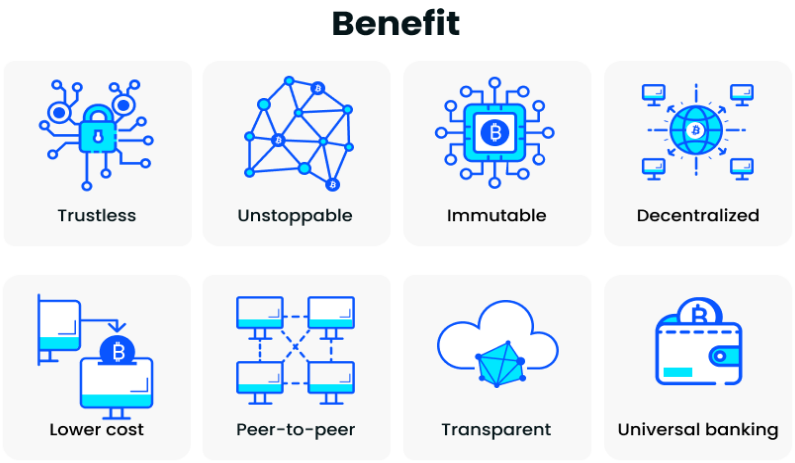


Figure 1.16 Benefits of blockchain

Trustless: The blockchain is immutable and automates trusted transactions between counterparties who do not need to know each other. Transactions are only executed when programmed conditions are met by both parties.

Unstoppable: Once the conditions programmed into a blockchain protocol are met, an initiated transaction cannot be undone, changed, or stopped. It's going to execute and nothing – no bank, government, or third party – can stop it.

Immutable: Records on a blockchain cannot be changed or tampered.

A new block of transactions is only added after a complex mathematical problem is solved and verified by a consensus mechanism. Each new block has a unique cryptographic key resulting from the previous block's information and key being added into a formula.

Decentralized: No single entity maintains the network. Unlike centralized banks, decisions on the blockchain are made via consensus. Decentralization is essential because it ensures people can easily access and build on the platform.

Lower Cost: In the traditional finance system, you pay third parties like banks to process transactions. The blockchain eliminates these intermediaries and reduces fees, with some systems returning fees to miners and stakers.

Peer-to-Peer: Cryptocurrencies like Bitcoin, let you send money directly to anyone, anywhere in the world, without an intermediary like a bank charging transaction or handling fees.

Transparent: Public blockchains are open-source software, so anyone can access them to view transactions and their source code. They can even use the code to build new applications and suggest improvements to the code. Suggestions are accepted or rejected via consensus.

Universal Banking: anyone can access the blockchain to store money, it's a great way to protect against theft that can happen due to holding cash in physical locations.

Use cases

- Dubai has been able to integrate blockchain into eight industry sectors
    - Real estate
    - Tourism
    - Security
    - Transportation
    - Finance
    - Health
    - Education.
- The end result is to become the world's first blockchain city.

Cryaptocurrency

- Cryptocurrency is a form of currency that exists solely in digital form.
- Cryptocurrency can be used to pay for purchases online without going through an intermediary, such as a bank, or it can be held as an investment.
- Example : Bitcoin, Etherium etc

How Do You Buy Crypto?

- You can buy cryptocurrencies through crypto exchanges, such as Coinbase, Kraken or Gemini. In addition, some brokerages, such as WeBull and Robinhood, also allow consumers to buy cryptocurrencies.

Example Cryptocurrencies

- Bitcoin -  1 bitcoin = $33,250
- Etherium  per-token value of $1,218.59.
- Litecoin (LTC)  per-token value of $153.88
- Cardano (ADA)  one ADA trades for $0.31.
-
  - Polkadot (DOT)  one DOT trades for $12.54.
  - Bitcoin Cash (BCH)  value per token of $513.45.
  - Stellar (XLM)  valued at $0.27 as of January 2021.
  - Chainlink  one LINK is valued at $21.53.

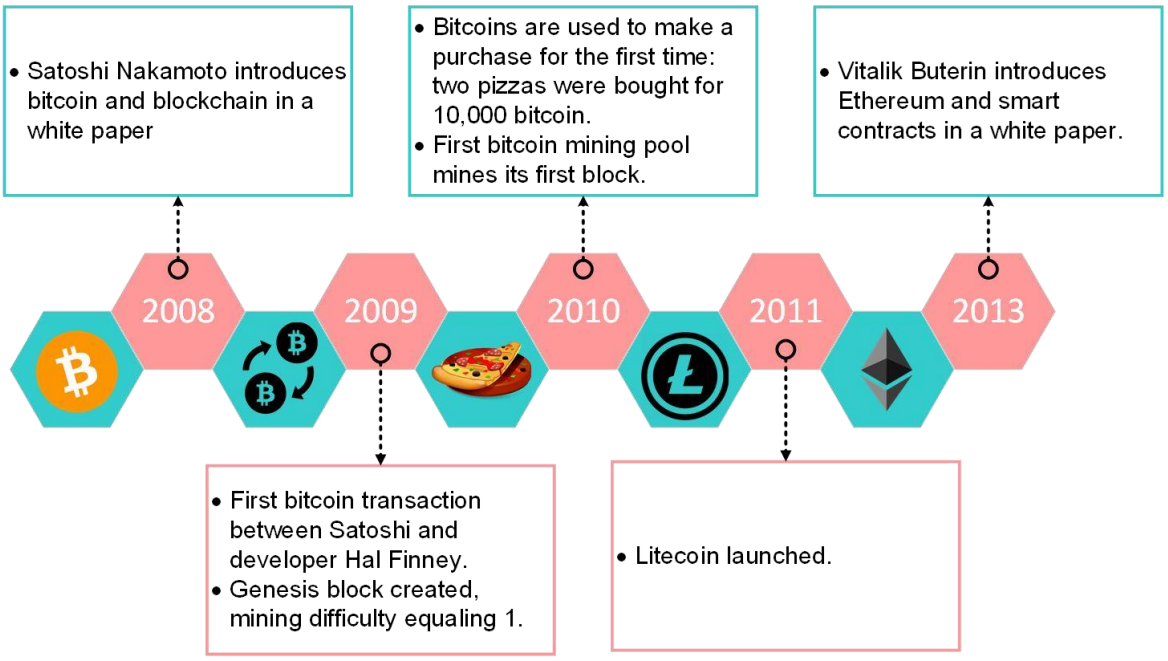
• Binance Coin (BNB)  one BNB having a value of $44.26.

• Tether (USDT)  a per-token value of $1.

• Monero (XMR)  a per-token value of $158.37.

Figure 1.17 Example Cryptocurrencies

Blockchain Evolution



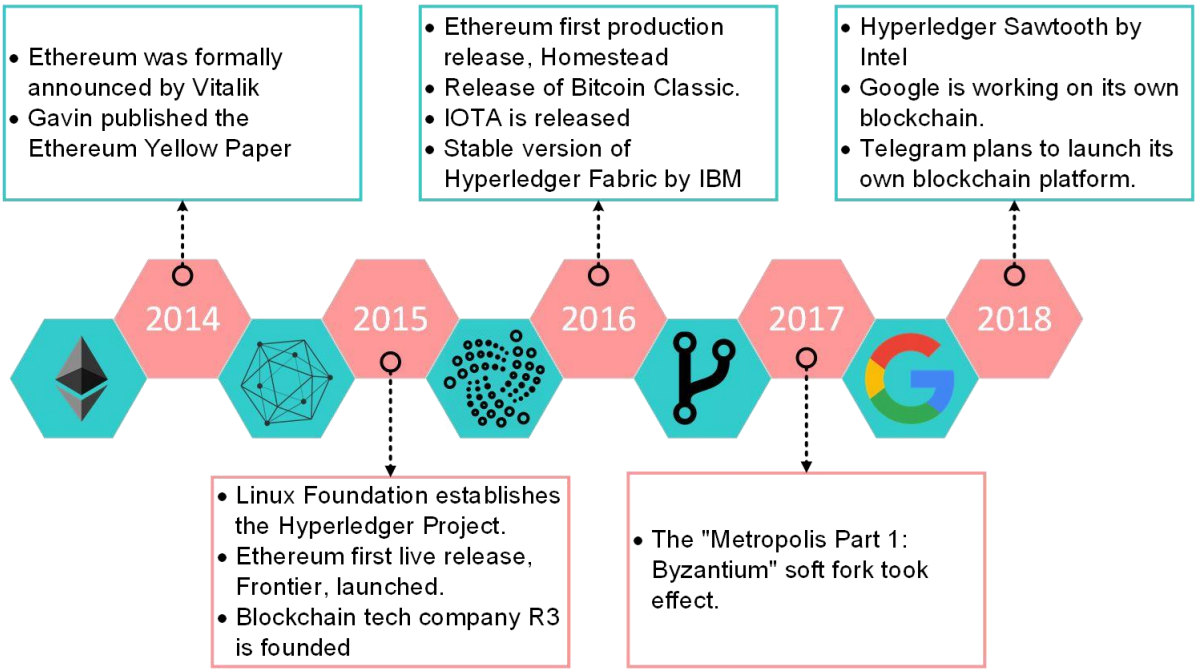


Figure 1.18 Evolution of blockchain

1.2 Public Ledger

Shared Ledger

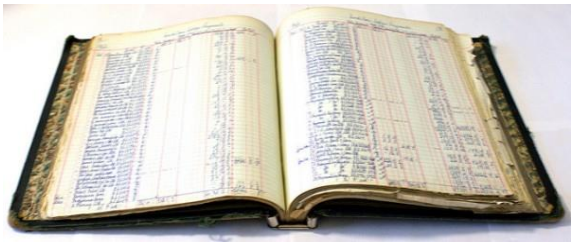


Figure 1.19 Ledger

- Records all transactions across business network
- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- It is the shared system of record.

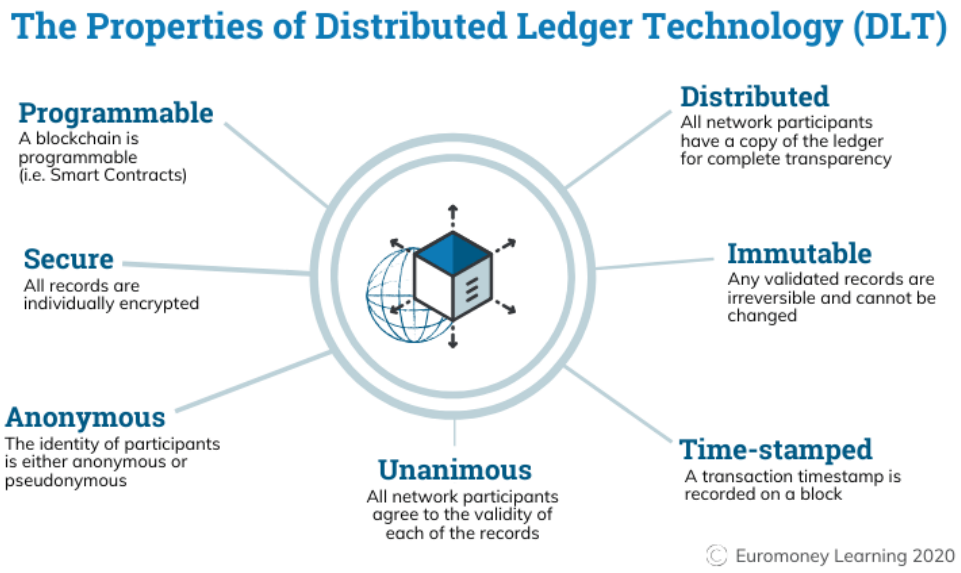


Figure 1.20 Features of Distributed Ledger

1.2 Blockchain as public ledger

How Distributed Ledgers Work

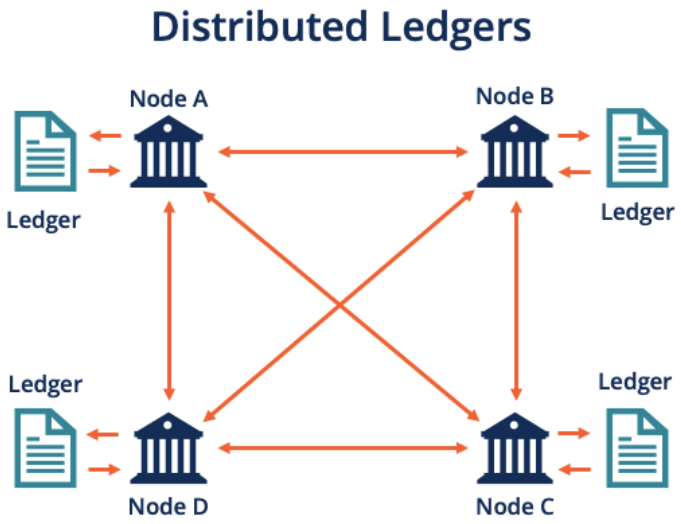


Figure 1.21 illustration of distributed ledger

- Distributed ledgers are held, reorganized, and controlled by individuals called nodes.
- The database is constructed independently by each node.
- Every transaction occurring on the network is processed, and a conclusion on the development of the database is created by each node.

- Based on the transaction, voting is carried out on the changes completed on the database. All nodes participate in the voting, and if at least 51% of them agree, the new transaction is accepted on the database.
- Afterward, the nodes update the versions of the database so that all the devices or nodes will be of the same version.
- The new transaction is written onto a block on the blockchain.
- Nodes in Proof-of-Work blockchain are also called miners.
- When a miner successfully puts a new transaction into a block, they receive a reward.
- It requires a dedicated 24×7 computer power.
- It is the responsibility of miners to compute the cryptographic hash for new blocks.
- Whoever, among the miners, successfully finds the hash first, gets the reward.
- Miners dedicating more computational power to find the hash will be more successful.
- However, as blocks keep generating, it becomes more difficult to find subsequent hash scales.
    - The goal is to keep a constant speed of generating the blocks.

Benefits of Distributed Ledgers

- Highly transparent, secure, tamper-proof, and immutable. After records are written into distributed ledgers, they cannot be altered by any other party.
- The need for a third party is eliminated
- Inherently decentralized
- Highly transparent

Advantages of Distributed Ledgers

- It is secure because there is no third-party intervention.
- It is immutable once recorded cannot be intervened.
- The data is distributed so it is tamper-proof.

Disadvantages of Distributed ledger:

- The distributed ledger is spread along with the nodes so making it vulnerable to attack.
- The transaction cost is high because of a larger network.
- The transaction speed is low because of the operation of a large number of nodes.

1.4 Types of blockchain

1. Public Blockchains
2. Private Blockchains
3. Consortiums Blockchains
4. Hybrid Blockchains

Public Blockchains

- Public blockchains are open, decentralized networks of computers accessible to anyone wanting to request or validate a transaction (check for accuracy).
- Those (miners) who validate transactions receive rewards.
- Public blockchains use proof-of-work or proof-of-stake consensus.
- permission-less distributed ledger system.
- Anyone who has access to the internet can sign in on a blockchain platform to become an authorized node and be a part of the blockchain network.
- Example : Bitcoin and Ethereum (ETH) blockchains.

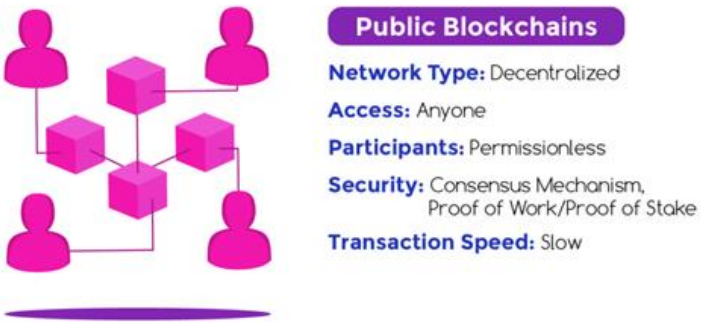


Figure 1.22 public blockchain

A public blockchain has some characteristic features:

- Write-only, immutable, transparent data storage.

- It brings trust among the whole community of users
- Decentralized, no need for intermediaries.
- Consistent state across all participants.
- Resistant against malicious participants.
- Anyone can join the public blockchain.

Disadvantages

- They suffer from a lack of transaction speed.

Private Blockchains

- A Private Blockchain is just like a relational database i.e. fully centralized and owned by a single organization.
- Private blockchains are not open, they have access restrictions.
- People who want to join require permission from the system administrator.
- They are typically governed by one entity, meaning they're centralized.
- For example, Hyperledger is a private, permissioned blockchain.

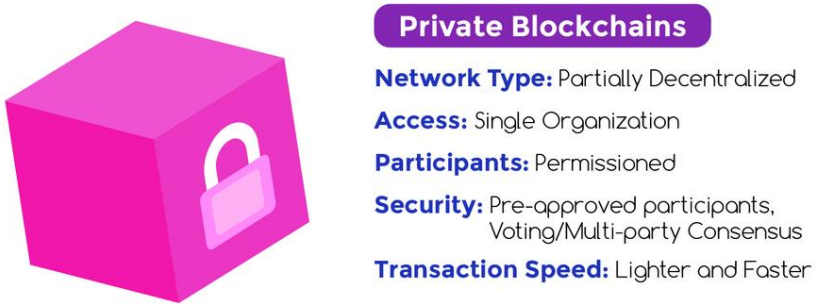


Figure 1.23 private blockchain

Consortiums blockchain

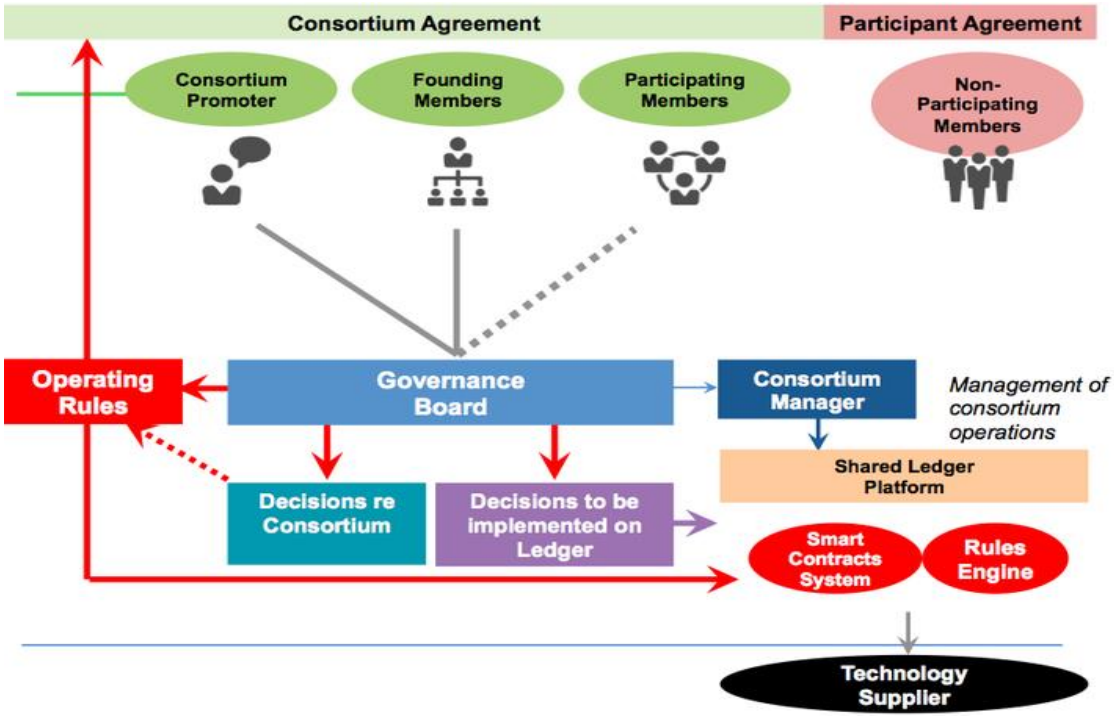


Figure 1.24 Consortium blockchain

- Validation is conducted by known and identified members of the limited network of nodes
- greater privacy since the information from verified blocks is not exposed to the public.
- There are no transaction fees
- consensus is reached by a relatively small number of nodes in accordance to the governance scheme.
- Increased scalability - Bitcoin's block transmits only up to 1 Mb* (from 1500 to 2700 transactions) per 10 minutes, when a consortium blockchain can optimize it to 1000 and more transactions per second.
- A consortium platform is more flexible.
- voting-based system, it ensures low latency and superb speed.

Hybrid Blockchain

- like a consortium blockchain, but it is not.
- Hybrid blockchain is best defined as a combination of a private and public

blockchain.

- It has use-cases in an organization that neither wants to deploy a private blockchain nor public blockchain and simply wants to deploy both worlds' best.
- **Example of Hybrid Blockchain:** Dragonchain, XinFin's Hybrid blockchain

Advantages

- Works in a closed ecosystem without the need to make everything public.
- Rules can be changed according to the needs.
- Hybrid networks are also immune to 51% attacks.
- It offers privacy while still connected with a public network.
- It offers good scalability compared to the public network.

Disadvantages

- Not completely transparent.
- Upgrading to the hybrid blockchain can be a challenge.
- There is no incentive for participating and contributing to the network.

Table 1.2 Types of blockchain

	Public	**Private**	**Hybrid**
Definition	The public blockchain is **open to everyone** where anyone can participate.	Private blockchain is controlled by owners and **access is limited** to certain users.	The hybrid blockchain is a combination of the public and private blockchain. This means that some process is kept private and others public.
Transparency	The public blockchain is **completely transparent.**	The private blockchain is only **transparent to the users who are granted access.**	Hybrid blockchain transparency depends on how the owners set the **rules**.
Incentive	Public blockchain **incentivizes** participants for growing the network.	The private blockchain is limited and hence have **no** similar incentive as that of a public blockchain.	Hybrid blockchain can opt to incentivize users if they want to.

Use-case	Can be used in almost every industry. **Good for public projects**. It is also good for creating cryptocurrency for commercial use.	Private blockchain is great for organization blockchain implementation as they **require complete contro**l over their workflow.	Hybrid is best suited for projects that can neither go **private or public** and have a lack of trust. The supply chain is a great example. It is also effective in banking, finance, IoT, and others.
Example	Bitcoin, Litecoin, Ethereum	Ripple, Corda	Hyperledger
KYC needed	No	Yes	Yes
Transactional Cost	Costly	Not so costly	Not so costly
Carries basic property of blockchain	Yes	Yes	Yes

1.5 Pillars of Blockchain

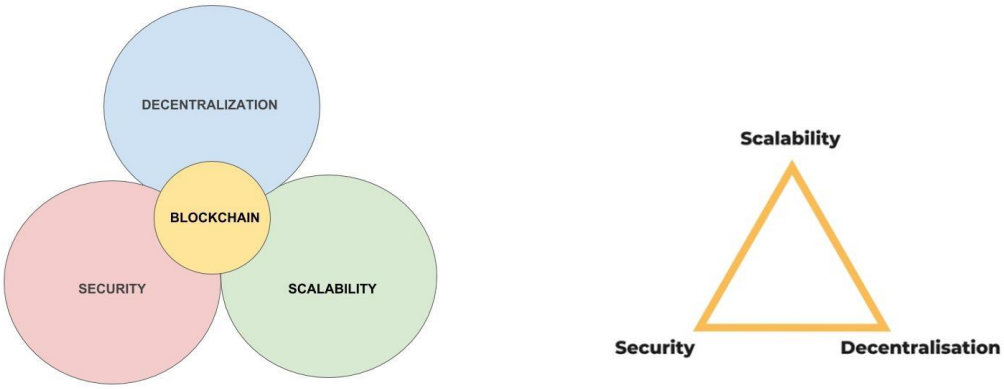


Figure 1.25 Pillars of blockchain

- Every Blockchain can be rated on the basis of 3 components: Decentralization, Scalability, and Security.
- It is a challenge to keep all of these three components in balance. Usually, one of them is partly sacrificed to get the other two.
- **Scalability**
- **Decentralization** (censorship resistance)
- **Security**

- **security, scalability, and decentralization**. These are among the most prominent driving factors in ongoing development (privacy/anonymity is another contender).

Security:

- The network is secure from both internal and external flaws.
- **Security** is the most crucial concept, and without it, the technology would be unusable.
- Security is the most important of them all, as no one would use banks or Bitcoin without it. For example, we could say the lack of security in has stopped us in adopting that scalability solution.

Scalability:

- The technology must be able to grow to and handle a commercially viable scale.
- **Scalability** is required for the technology to gain broad adoption

Decentralization:

- The network must not, in practice, be vulnerable to control by a few entities.
- **Decentralization** is necessary to cut costs (middlemen) and to build trust.

1.6 Government Initiatives of Block Chain

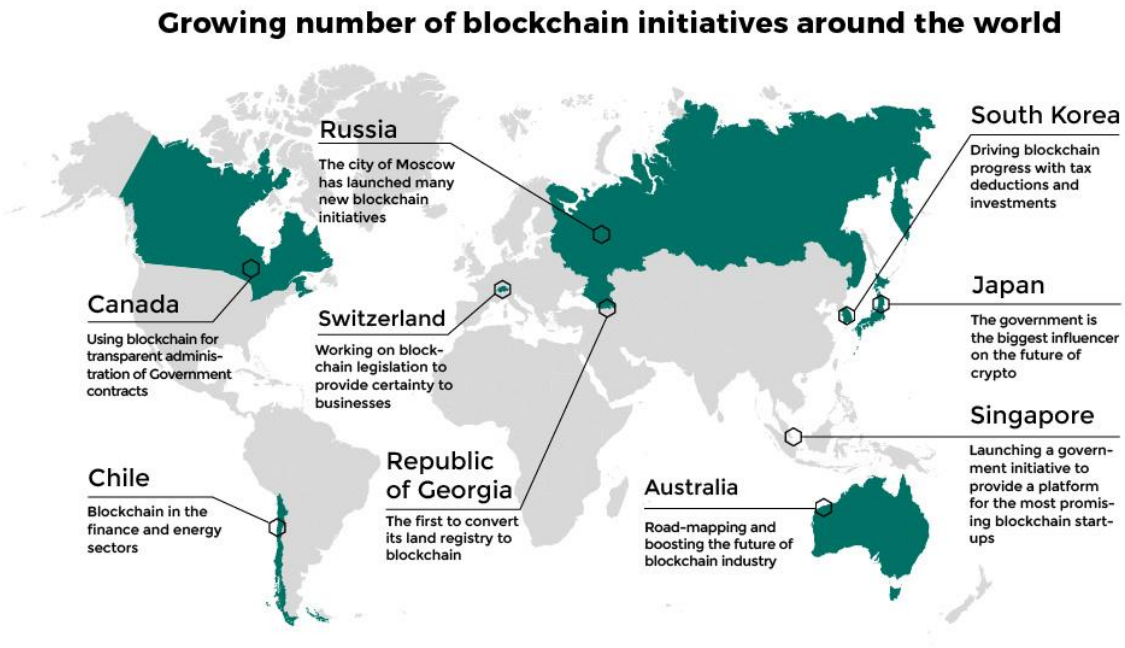
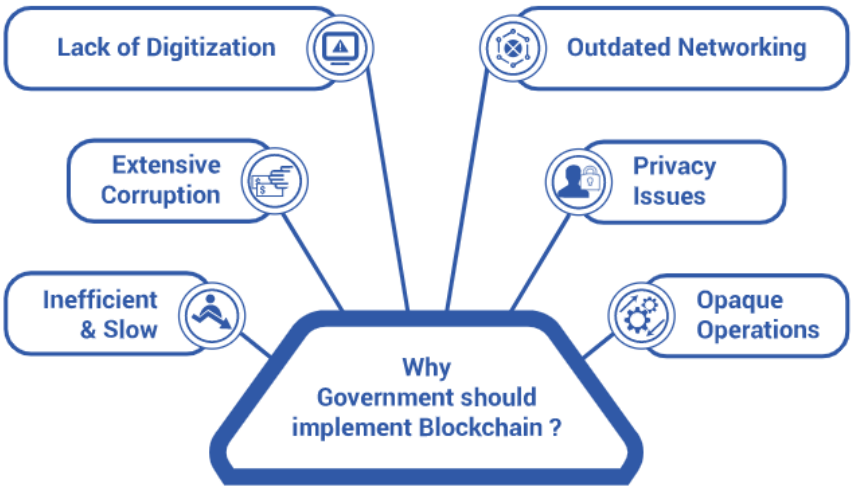


Figure 1.26 Government Initiatives of Block Chain

Why Use Blockchain in Government Processes?



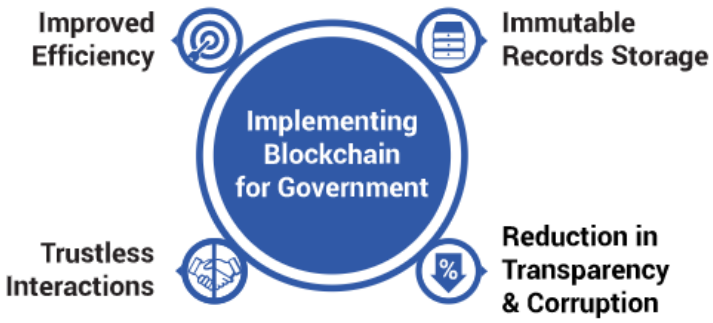


Figure 1.27 Benefits of Blockchain Government Initiatives

Blockchain Government Use Cases

e-Estonia

digital ID, e-tax, i-voting

Georgia – Land Registry

The project supplements the traditional land registry protocol with Blockchain.

Malta – Academic Record

Using the Blockcerts app, the citizen enlists their academic institution as an issuer of certificates.

Switzerland – Decentralized Identity

limited to residential proof in its first phase

Blockchain for Government – The Obstacles

Scalability

Risk of private-key theft and the consequent data breach

Lack of Blockchain awareness

The ideal case blockchain implementation - India

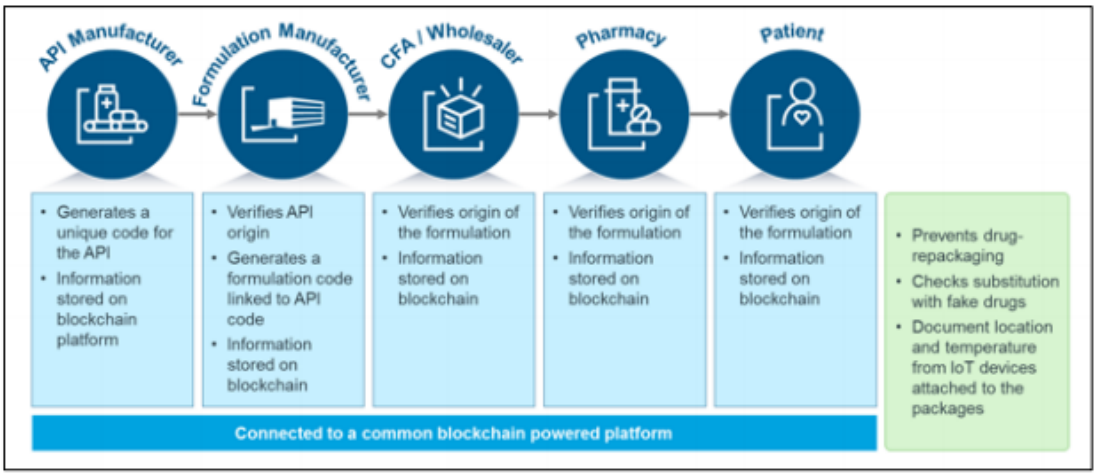


Figure 1.28 blockchain initiatives

1.7 Bitcoin

- Released in 2008 by Satoshi Nakamoto.
- Focus on crypto-currencies and micro-payments
- Proof of Work Consensus

Bitcoin vs. bitcoins

Bitcoin is the system

bitcoins are the units

What is Bitcoin?

- A **peer-to-peer** internet currency that allows **decentralized** transfers of value between **individuals and businesses**.

Before Bitcoin

- DigiCash (1989): The 1st Electronic Cash System

- David Chaum's company, featuring *ecash* (1983)
- Ecash notes backed by fiat from bank
- Relied on blind signatures

- The idea was published in 2009 by an pseudonymous person/group of people, named **Satoshi Nakamoto.**

Goal with Bitcoin was:

- To create a **trustless** system, using cryptography
- Solve double-spending problem of previous digital currencies
- Create digital assets that can be owned, with proof of ownership

Creating a currency from scratch

- Motivation
    - Distrust of financial institutions
    - Transaction costs
- Primary concerns
    - Transaction security
    - Double spends

Distrust of financial institutions

- Any noncash transaction requires a trusted third-party administrator—commonly a bank or financial service provider.
- The system forces participants to trust financial institutions that are not always trustworthy.

Transaction security

- Two levels of verification
    - Source is legitimate
    - Coins are legitimate
- Public/private key verification ensures the legitimacy

Double spends

- If the money is just digital codes, why not copy and paste to make more money?
    - Timestamps
    - Hashes
    - Block chain
- Timestamp
    - Each transaction is packaged and publically recorded in the order it was carried out.
- Hash
    - The time-stamped group of transactions are given a unique algorithmically derived number

Bitcoin

- **Bitcoin** is the official first cryptocurrency that had been released in 2009. It is basically a digital currency and only exists electronically.
- Bitcoin is the first successful electronic cash system and coincidentally, the first instance of a successful Blockchain.
- Secure, trustless, borderless
- No bank needed to authorize/process transactions
- Transactions are stored on a **distributed ledger**

Bitcoin introduced the concept of **cryptocurrency**; decentralized digital money secured by cryptography, and used to create valuable digital assets that cannot be counterfeited.

Bitcoin transactions are authorized in a peer-to-peer network.

- Each node stores the history of the chain of blocks, containing validated transactions
- Counterfeiting is impossible because if one node's history is corrupted the others stay the same, and no central authority (i.e. bank) needs to confirm; this is called **decentralization**
- Unlike previous P2P network models, members of the Bitcoin network are

incentivized to participate through **cryptocurrency**.

- Specifically, the incentive is for the people who mint (create) Bitcoin, called **miners**.

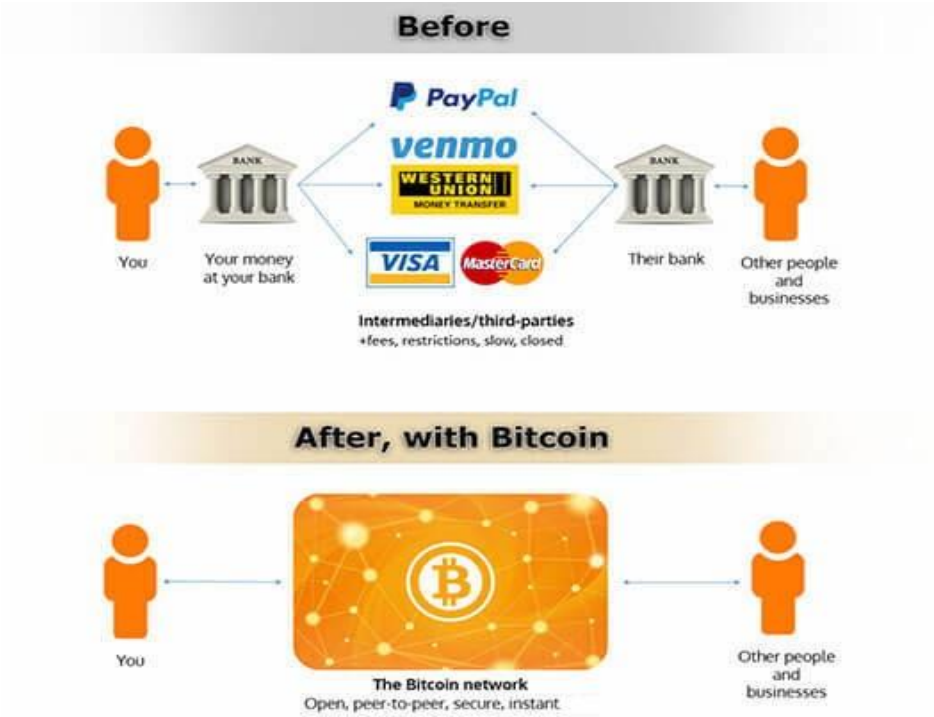


Figure 1.28 before and after bitcoin

Bitcoin Properties

- Bitcoins can be possessed.
- Bitcoins can be transferred.
- Bitcoins are impossible to copy.

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.
- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount paid per hash goes down by half about every 4 years.

Owning bitcoins

- Users create accounts called wallets.
- Wallets are secured using passwords and contain the private keys used for transferring bitcoins.

Spending bitcoins

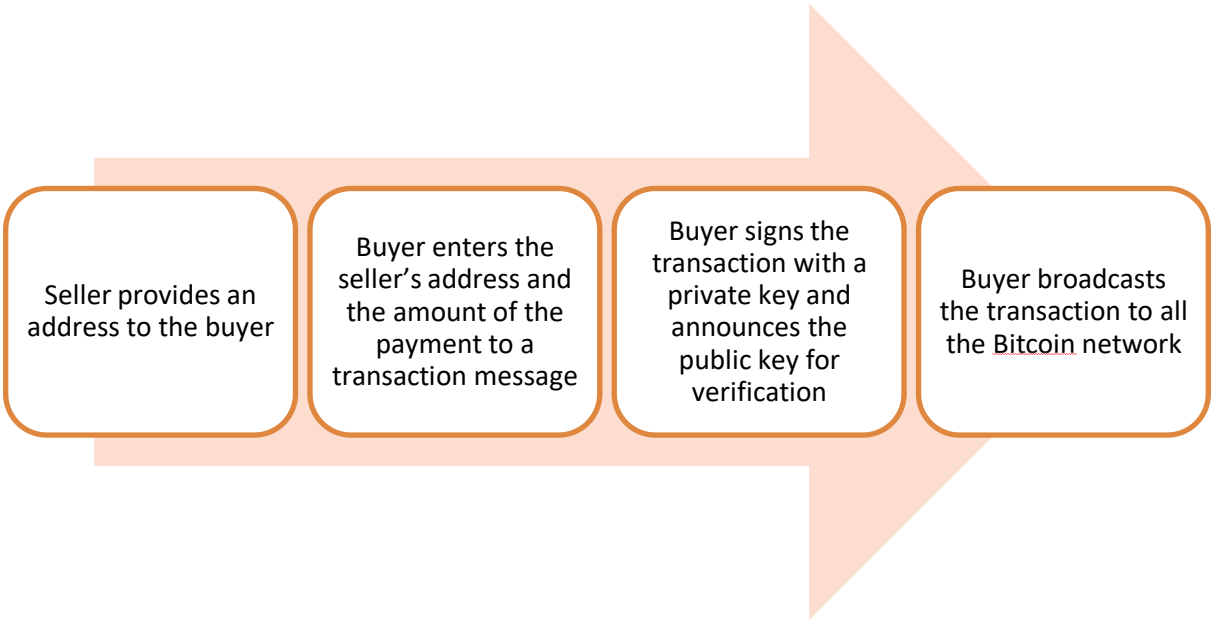


Figure 1.29 bitcoin transaction

Wallets

- A wallet is a combination of public address and private key.

Figure 1.30 botcoin wallets

Hardware wallets

- Most popular hardware wallets are Ledger Nano S and Trezor.

Figure 1.31 Hardware Walet

- Hardware wallets are hardware devices that individually handle public addresses and keys.
- It looks like a USB with OLED screen and side buttons.
- when you open a wallet (in the hardware wallet or software wallet) you are provided with 2 pair of keys (sometimes more).
- **Public key** and **the private key**.
- **public key** is used to generate the public **cryptocurrency address** you can use to

receive the cryptocurrency,

- the **private key** is used to sign the transactions confirming your ownership over it.
- This is a reason why private key must be **kept secret**

Paper Wallets

- It is a physically printed QR coded form wallet.
- Some wallets allow downloading the code to generate new addresses offline.

Figure 1.32 Paper Wallet

Desktop Wallet

- Desktop wallets are programs that store and manage the private key for your Bitcoins on your computer's hard drive.

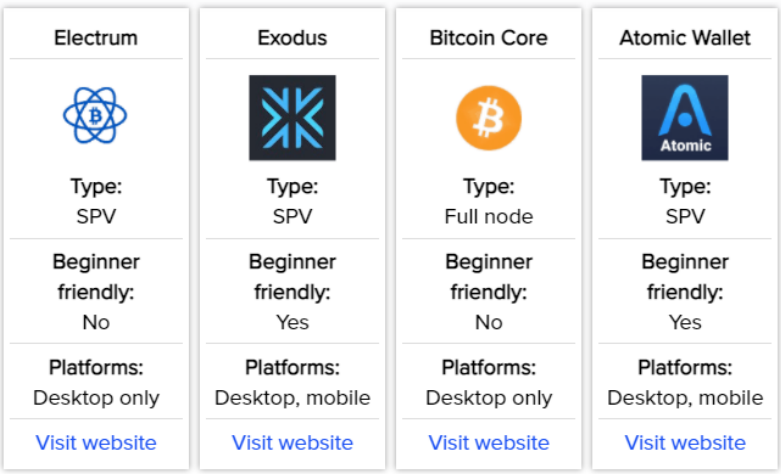


Figure 1.33Desktop Wallet

Mobile wallets

- A mobile wallet is a virtual wallet that stores payment card information on a mobile device.
- They are quite convenient as it uses QR codes for transactions
- Some mobile wallets are Coinomi and Mycelium

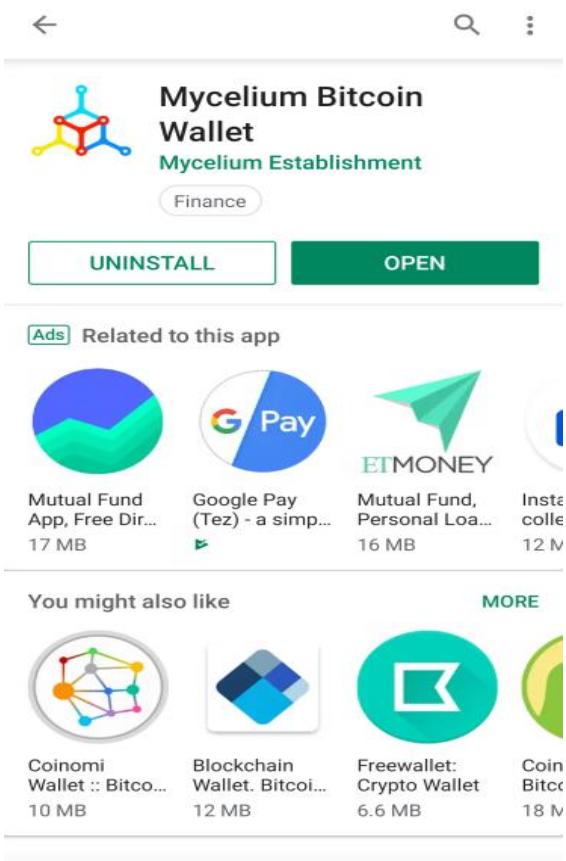


Figure 1.34 Mobile Wallet

Web Wallets

- These wallets are accessed by internet browsers.
- They are the least secure wallets.
- They are not the same as hot wallets.
- They are ideal for small investments and allow quick transactions.
- Some of these are MetaMask and Coinbase.

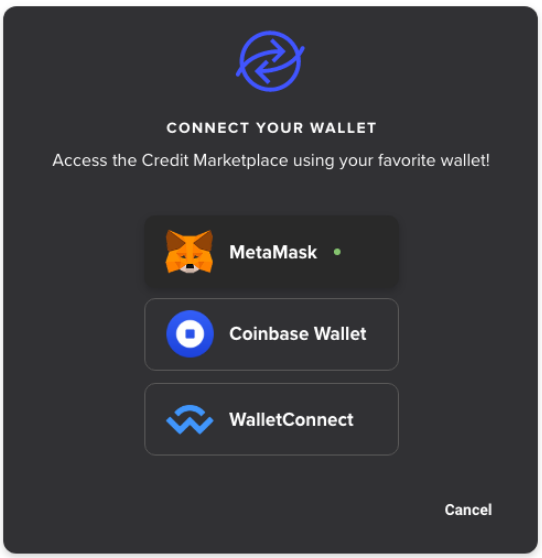


Figure 1.35 Web Wallet

Bitcoin Transactions

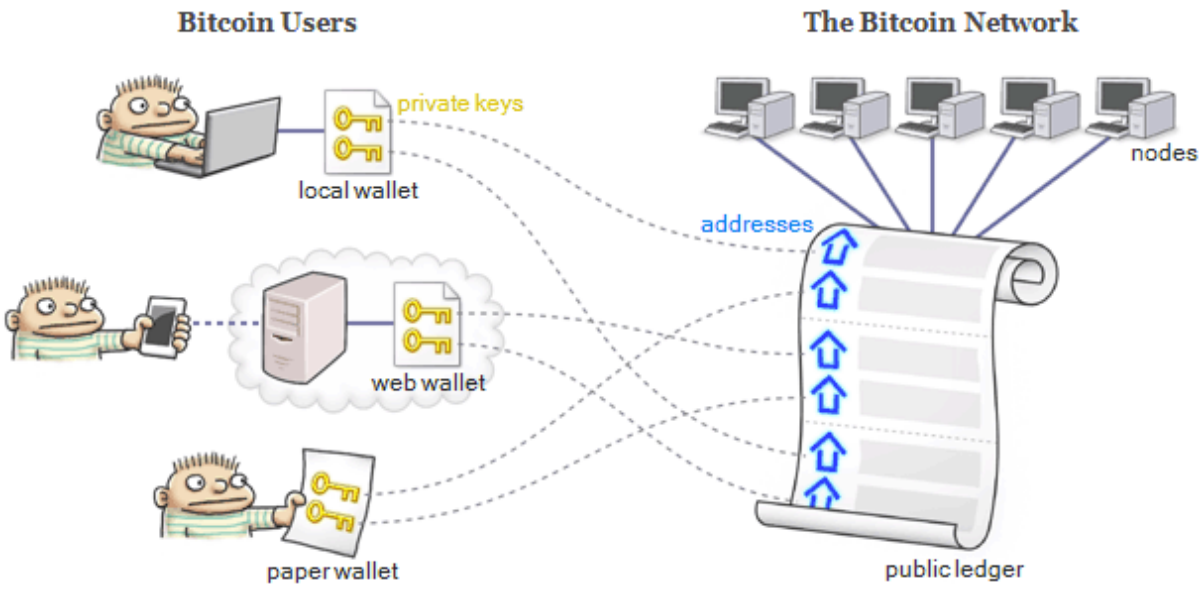


Figure 1.36 Bitcoin Transactions

- A full node is basically an electronic bookkeeper, and anybody in the world can set up and run one.
- Each node has a complete copy of the **public ledger** – that's a record of every Bitcoin transaction

Sample Transaction

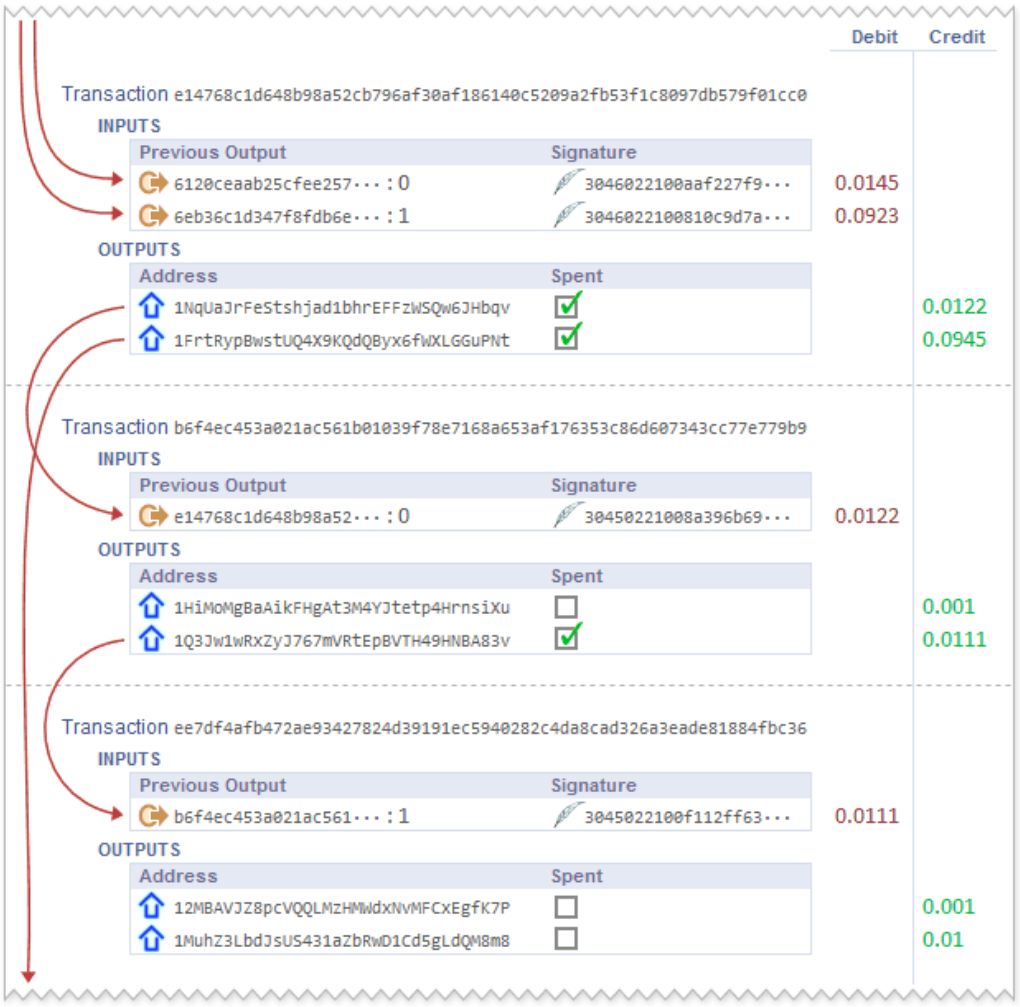


Figure 1.37 Transactions with Hash values

- Every transaction has a set of inputs and a set of outputs.
- The **inputs** identify which bitcoins are being spent, and the **outputs** assign those bitcoins to their new owners.
- Each input is just a digitally signed reference to some output from a previous transaction.
- Once an output is spent by a subsequent input, no other transaction can spend that output again.
- Each unspent output represents some amount of bitcoin that is currently in someone's possession.
- Note that nobody's real name appears anywhere within a transaction. That's why Bitcoin

is often said to be **pseudonymous**.

- Instead of real names, bitcoins are assigned to **addresses** such as 1PreshX6QrHmsWbSs8pHpz6kLRcj9kdPy6.

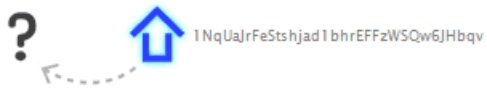
Where Do Addresses Come From?

- Obviously, if you want to receive bitcoins, you need to have a Bitcoin address. Your wallet can generate addresses for you.
- In order to generate an address, your wallet first generates a **private key**. A private key is nothing but a large number roughly between 1 and 2^{256}.
- To make such numbers shorter to write, it's customary to encode them as sequence of numbers and letters.

Bitcoin Address

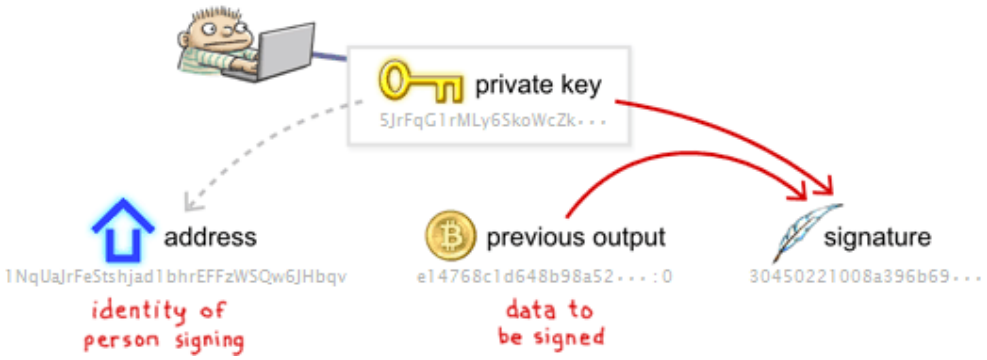
- Next, your wallet converts that private key to a Bitcoin address using a well-known function. This function is very straightforward for a computer to perform.
- it uses elliptic curve cryptography to generate Bitcoin addresses
- If anyone knows your private key, they could easily convert it to a Bitcoin address, too.

- If someone knows *only* your Bitcoin address, it's virtually impossible to figure out what the private key was.



How Are Transactions Authorized

- In Bitcoin, a valid digital signature serves as proof that the transaction was authorized by the address's owner.
- Just as a private key was required to generate that address, the same private key is required, once again, to generate a valid digital signature.



- A digital signature is only valid if a specific equation is satisfied by the address, the previous output and the signature.

The Bitcoin lifecycle

- Sender wants to send 1 Bitcoin to Receiver. This is what is going to happen:

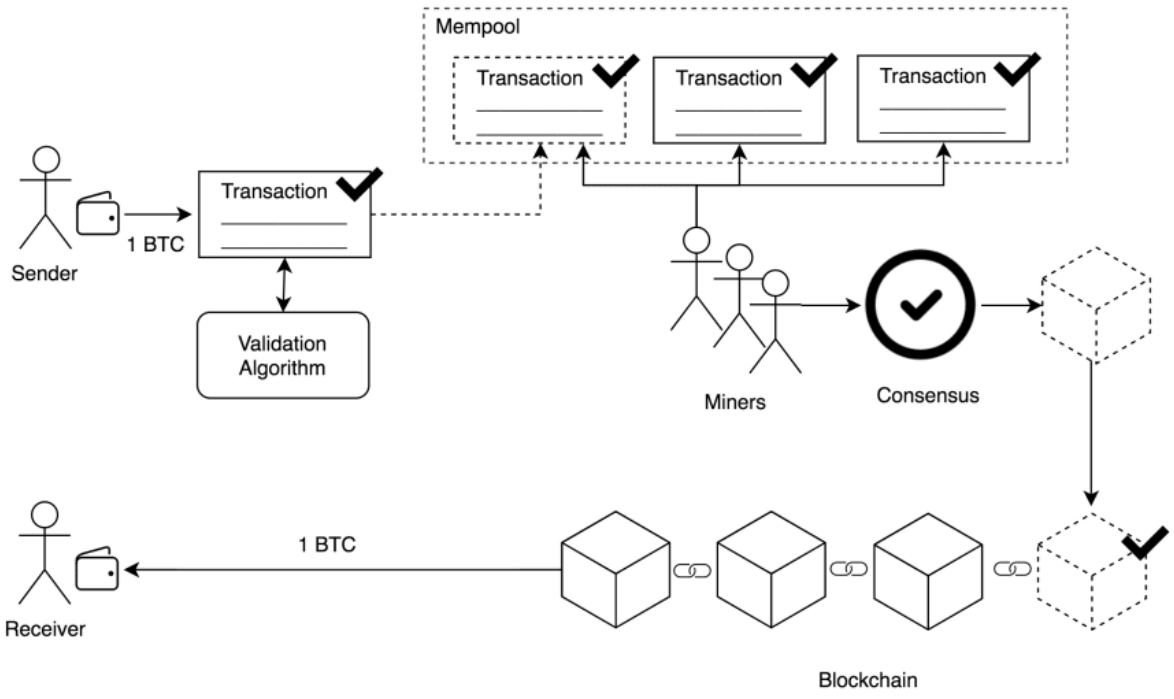


Figure 1.38 Bitcoin Life cycle

1. Sender creates a transaction.

2. Sender's bitcoin wallet validates the transaction.
3. The transaction is sent to Mempool.
4. Miners get the transaction from Mempool and start mining the block using a consensus algorithm.
5. After the block is fully mined, it is added to the network.
6. The chain validates the new block and every peer in the network will get the blockchain with the new block added.
7. Finally, the Receiver get your BTCs

Mempool

- The Mempool (Shortcut for Memory Pool) is where the transactions stay until the miner is ready to get them.
- In the bitcoin's blockchain, the miner prioritize the biggest transactions over the smallest ones.
- This happens because here is where the miner makes money.
- Miner "mine" the block through the consensus algorithm.

Bitcoin Flow of Transaction

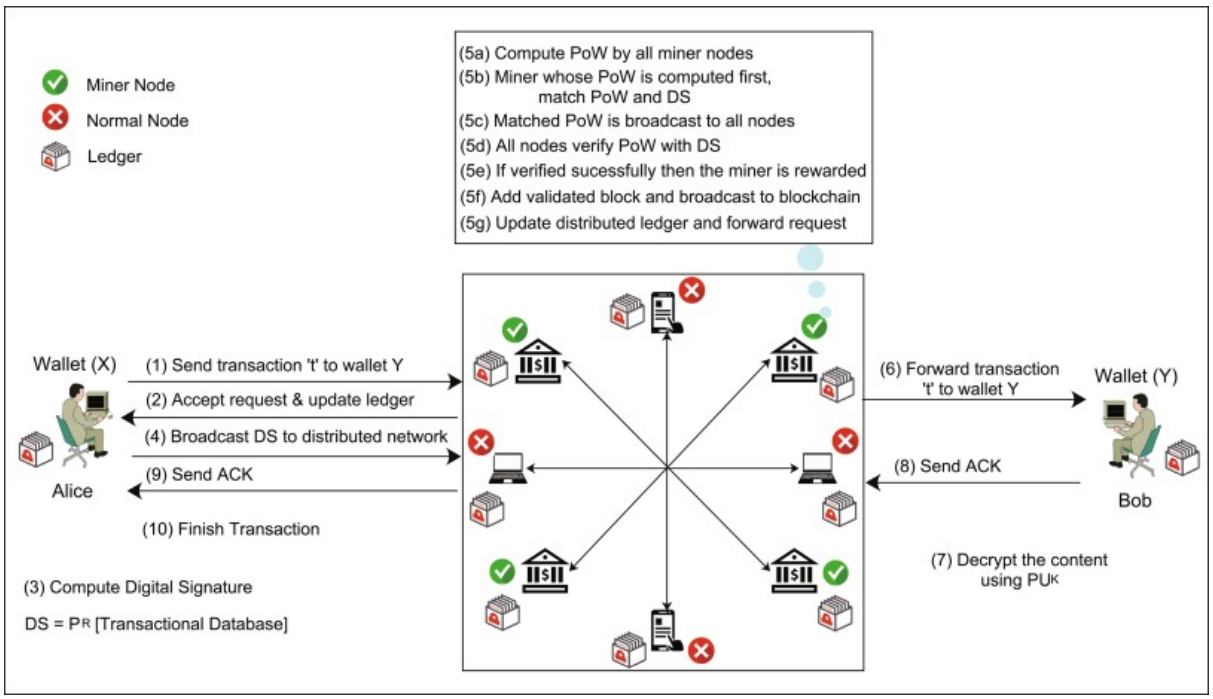


Figure 1.38 Bitcoin Flow diagram

- Let us say that there are two parties *Alice and Bob* who want to communicate with each other for funds transfer over an insecure channel, Internet. Then following sequence of activities are performed between two parties.

- If *Alice* wants to send some coins from her wallet*X* to *Bob's* wallet *Y*, then a request of transactional data "*t*" is sent to *Bob*. This request is broadcasted in the entire network.
- The distributed nodes accept the request and update their ledgers with the transactional information of *Alice–Bob*.
- After updating ledgers, Alice computes digital signature (*DS*) and broadcasts it in the network.
- A miner node is selected to verify and validate the transaction. It computes proof-of-work (PoW) to match the *DS* received. If PoW is successfully matched with *DS*, then the result is broadcast to all the nodes for verification and validation.
- The other miner nodes also verify the PoW with *DS*. If the verification is successful, then the miner node is (financially) rewarded for computing the PoW.
- The validated block is added in the validated chain and the transaction is broadcasted to the entire blockchain.
- Using the validated transaction "*t*," the bitcoins are added to wallet*Y* of *Bob*.
- *Bob* decrypts the content using the paired public key (*PUK*) of Alice and sends the acknowledgment (*ACK*) to *Alice*.
- The transaction is finished once Alice receives the transaction acknowledgment.

Consensus Algorithm

- The consensus algorithm is probably the most important part of any implementation of blockchain.
- The Bitcoin uses one consensus algorithm called Proof Of Work.
- Try to get the right nonce number by checking the hash created for the block until the result hash have the same number of zero's in it's prefix.
- This execution to try to get the right nonce number takes a lot of energy cost and

computational work, and that's why the miners get the fees from the transaction.

Proof of Work consensus algorithm

- Proof of Work" because it requires some type of work - usually computer processing.
- consensus algorithm is a set of rules that governs a blockchain network.
- It is an agreement on the rules of a specific blockchain and how users can participate in the network
- Miners who carry out the validation of transactions in the blockchain.
- Miners have downloaded the full Bitcoin blockchain and chosen to run it on powerful computers.
- These users (nodes) in the Bitcoin network are called "miners" because they check and prove the accuracy of a transaction in a process called mining - similar to the computation of a complex mathematical problem.
- Once a request to record and complete a transaction is disseminated into the blockchain, usually the transactions with the highest fee offered are selected to go into the next block on the blockchain.
- In order to reach consensus on a valid block in the blockchain, the Bitcoin algorithm provides a difficulty as a parameter that needs to be met for a block to be valid.
- This "difficulty" is regularly modified by the Bitcoin network depending on the computational power of the miners.
- Difficulty may be decreased or increased to maintain a constant speed at which new blocks are added.
- An arbitrary number called a nonce (the abbreviation for "number only used once") is added to the block for purposes of cryptography.
- Miners alter the nonce until a value is found that gives the block's hash the required difficulty level
- Once this requirement is met the block cannot be changed without redoing the work.
- During hashing, an algorithm called a hash function is used to convert one value (the selected set of data) into a fixed-size as the output - the hash value, thus masking the

original value.

- A hash function cannot be reverse-engineered, meaning that the hash value cannot be used to find out the original data.
- Thus, the hash value is a “fingerprint” providing thorough authentication and ensuring that no tampering took place with the transmitted content.
- Each hash value contains information on all previous network transactions.
- The newly generated hash is checked against the current difficulty.
- A hash value always has to contain a specific number of zero-bits. If the hash meets the criteria of difficulty, it is broadcast to the other miners in the network.
- If it does not, another nonce is selected and hashed. Miners generate many hashes with different nonces until they find one that meets the needed criteria.
- This repetitive process is known as “mining” and now you know why it requires so much energy.
- Therefore, the first miner who finds a valid hash validates the block into a new block and gets a block reward in Bitcoin.

Disadvantages of Proof of Work

- Bitcoin transactions per second has been seven transactions,
- VISA network’s estimated 1,700
- vast amounts of energy are required for the mining process in the Bitcoin blockchain.
- larger mining pools have more computational power at their access and thus greater chances of mining valid blocks, putting individual miners at disadvantage.
- Source : https://www.bitpanda.com/academy/en/lessons/consensus-algorithms-proof-of-work/

Proof of Work Vs Proof of Stake

Proof of Work	Proof of Stake
Participating nodes are called miners	Participating nodes are called validators or forgers

Mining capacity depends on computational power	Validating capacity depends on the stake in the network
Mining produces new coins	No new coins are formed
Miners receive block rewards	Validators receive transaction fees
Massive energy consumption	Low to moderate energy consumption
Significantly prone to 51% attacks	51% attacks are virtually impossible

Proof of work and mining

- To create new digital currencies by rewarding miners for performing the previous task.
- **When you want to set a transaction this is what happens behind the scenes:**
- Transactions are bundled together into what we call a block;
- Miners verify that transactions within each block are legitimate;
- To do so, miners should solve a mathematical puzzle known as proof-of-work problem;
- A reward is given to the first miner who solves each blocks problem;
- Verified transactions are stored in the public blockchain.

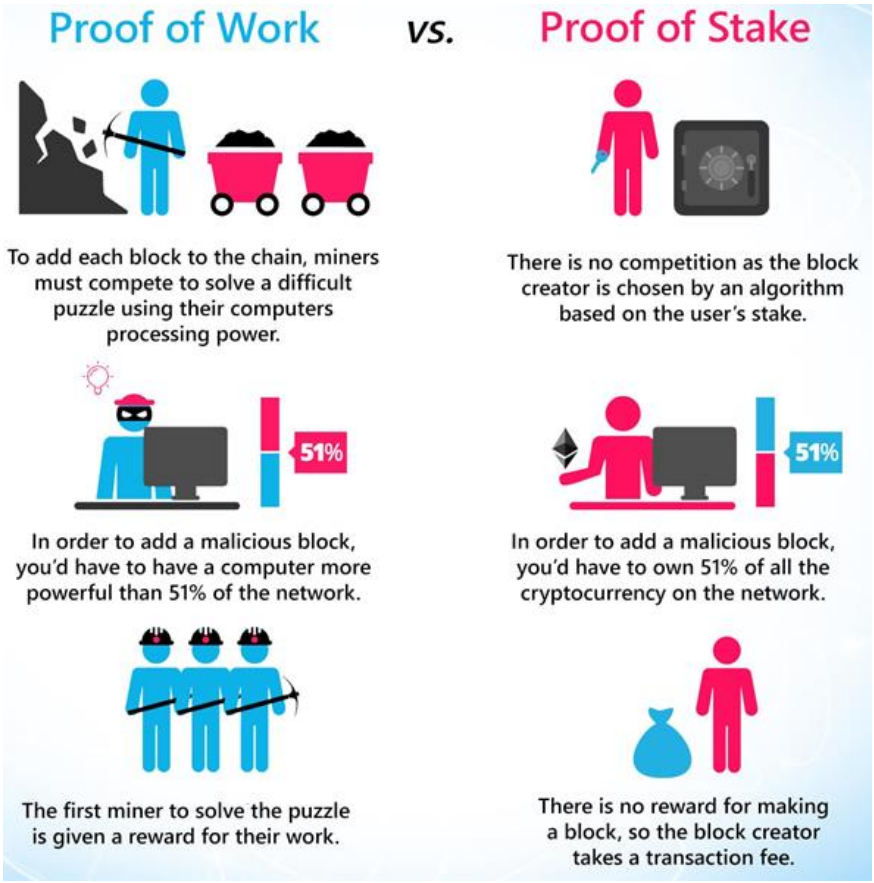


Figure 1.39 Proof of Work Vs Proof of stake

Mining Process

- From a technical point of view, the mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold.
- This threshold, called difficulty, is what determines the competitive nature of mining: more computing power is added to the network, the higher this parameter increases, increasing also the average number of calculations needed to create a new block.

Bitcoin Address Example

- Bitcoin addresses are 26-35 characters long, consist of alphabetic and numeric characters, and either begin with "1", "3", or "bc1".
- Currently, there are three Bitcoin address formats in use:

1. **P2PKH (address starts with the number "1")**

- The P2PKH concept stands for "Pay to Public Key Hash".

- P2PKH means “pay to this Bitcoin address”. It serves as an instruction on the blockchain for users wanting to transfer Bitcoin to one another.
- Behind every transaction, there are underlying codes working behind the scene. This scripting language is known as the Bitcoin Scripting Language.
- Example:

  1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

P2PKH

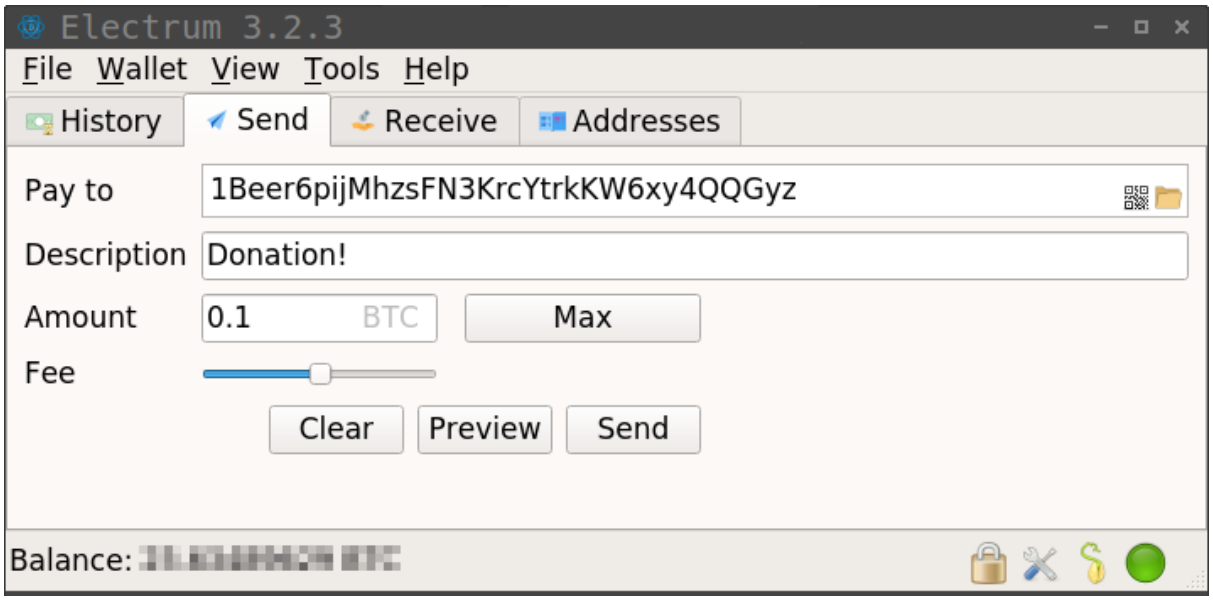


Figure 1.40 GUI of Pay to Public Key Hash

2. P2SH (address starts with the number “3”)

- Pay to script hash (**P2SH**) is an advanced type of transaction used in Bitcoin and other similar cryptocurrencies.
- P2SH or *Pay-to-Script-Hash* was a patch to Bitcoin added in 2012 which altered the way it validated transactions. It is most commonly identifiable as the addresses in Bitcoin that start with a “3” instead of a “1”.
- Unlike P2PKH, it allows sender to commit funds to a hash of an arbitrary valid script.

Example:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

3. Bech32 (address starts with "bc1")

Example:

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

How to Get a Bitcoin Address

- To get a Bitcoin address, you first need to download a Bitcoin wallet, which is software that allows you to securely send, receive, and store Bitcoin funds in the Bitcoin network.
- Bitcoin wallets also store your private key, which is essentially your Bitcoin password.
- The software will generate a brand new Bitcoin address for you every time you create an invoice or receive a payment request for Bitcoins too.
- There are four types of Bitcoin wallets that you can use: **mobile, web, desktop, and hardware**.
- Source: https://blog.hubspot.com/marketing/bitcoin-address

1.8 Smart Contract

- A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code.
- The code and the agreements contained therein exist across a distributed, decentralized blockchain network.
- The code controls the execution, and transactions are trackable and irreversible.

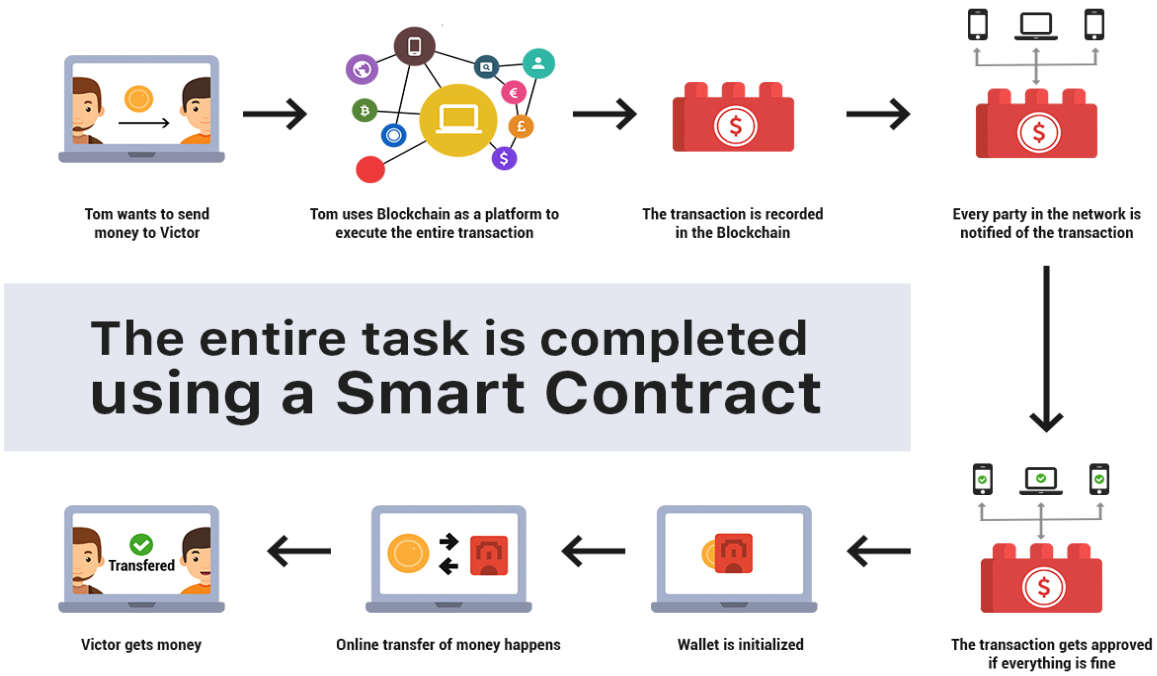


Figure 1.41 illustration of Smart contract

- Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain.
- A network of computers executes the actions when predetermined conditions have been met and verified.
- These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket.
- The blockchain is then updated when the transaction is completed.
- That means the transaction cannot be changed, and only parties who have been granted permission can see the results.
- Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily.
- Participants must determine how transactions and their data are represented on the blockchain.
- Participants agree on the "if/when...then…" rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

- The smart contract can be programmed by a developer.

organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

Benefits of smart contracts

Speed, efficiency and accuracy

Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process. No time spent reconciling errors that often result from manually filling in documents.

Trust and transparency

Because there's no third party involved, and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.

Security

Blockchain transaction records are encrypted, which makes them very hard to hack.

Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

Savings

Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

Applications of smart contracts

Smart contracts can be used across industries to streamline and automate doing business around the world**.**

Government - voting system

Management

single ledger as a source of trust, accuracy, transparency, and automated system

Supply chain

automates tasks and payment

Automobile

with the help of smart contract insurance company can be connected for claim

Real Estate

No need of Brokers, real estate agents

Healthcare

Architecture and Conceptualization of Block Chain, Crypto Currencies

Block in a Block chain-find Transactions-Distributed Consensus-Proof of work, Stake, Space-Attacks on POW-Ethereum-Pos/POW Hybrids-Crypto currency to block chain 2.0, Model of Blockchain- Algorand.

2.1 BLOCK IN A BLOCK CHAIN

Definition of Blockchain

A block chain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way without the need for a central authority.

Key Characteristics to be remembered:

Open: Anyone can access blockchain.

Distributed or Decentralised: Not under the control of any single authority.

Efficient: Fast and Scalable.

Verifiable: Everyone can check the validity of information because each node maintains a copy of the transactions.

Permanent: Once a transaction is done, it is persistent and can't be altered.

Contents of a Block

Blockchain starts with a block called genesis block. Each block stores the following information in it:

Index: Position of the block in blockchain. Index of genesis block is 0.

Time stamp: The time when that particular block was created.

Hash: Numeric value that uniquely identifies data just like our fingerprints.

Previous hash: Hash value of the previous block. For genesis block, this value is 0.

Data: Data stored on the node. For example, transactions.

Nonce: It is a number used to find a valid hash. To generate this number, the processing power is used.

Genesis Block	
Previous Hash	0
Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
Data	Welcome to Blockchain CLI!
Hash	000001803 5a828da0…
Nonce	56551

Fig.2.1 Genesis block

Mechanism of Blockchain

Fig 2.2 Blocks connected in backward direction

- Blockchain works like a public ledger.
- Any small change in the data value can affect the hash value. Hence, affecting the whole block chain.
- Every peer in a Blockchain network maintains a local copy of the Blockchain.
- All the replicas need to be updated with the last mined block.
- All the replicas need to be consistent — the copies of the Blockchain at different peers need to be exactly similar.

Structure of a Block (Reference: Bitcoin)

The blockchain is a chain of data blocks. Each block can be thought of as a page in a ledger. The individual blocks are composed of several components.

Roughly these can be differentiated into

- the head of the block (block header) and
- the body (block body).

Block header

The head of the block is divided into six components:

1. the version number of the software
2. the hash of the previous block
3. the root hash of the Merkle tree
4. the time in seconds since 1970–01–01 T00: 00 UTC
5. the goal of the current difficulty
6. the nonce

- **The version number of the software:** The software version number does not matter in most cases. However, a miner with a particular version number can signal which protocol decisions he supports.
- **The hash of the previous block :**The hash of the previous block is, so to speak, the chain of blockchains. Because the hash of the previous block is contained in the hash of the new block, the blocks of the blockchain all build on each other. Without this component, there would be no connection and chronology between each block.
- **The root hash of the Merkle tree :**All transactions contained in a block can be aggregated in a hash. This is the root hash of the Merkle tree.
- **The time in seconds since 1970–01–01 T00: 00 UTC:** A timestamp in the block itself. The time is given in seconds since 1.1.1970.
- **The goal of the current difficulty :**The goal indicates how small the new hash must be to claim validity. In other words, every hash has a size in bits. The lower the goal in bits is, the harder it is to find a matching hash. A hash with many zeros at the beginning is smaller than a hash without zeros. Find out more about the difficulty of the proof of work.
- **The Nonce:**The nonce is the variable incremented by the proof of work. In this way, the miner guesses a valid hash, a hash that is smaller than the target.

The six components form the block header. The block header plays a fundamental role in Bitcoin because it connects all blocks together. You can imagine it like the cockpit of a truck. Here are the important papers with which the truck comes through the controls of the network.

Block Body

The block body is conceivable as the loading space of a truck. It contains all transactions that are confirmed with the block.

When a miner constructs a block, it validates the transactions. That is, he checks that the sender actually has enough money to spend. He can easily read this information from the blockchain. The miner looks in the past blocks to see if the sender has even gotten ten Bitcoins if he wants to send ten Bitcoins. The transactions in a block are not just in a list, but in a so-called Merkle Tree.

Merkle Tree

The Merkle Tree takes its name from the mathematician Ralph Merkle. The discovery was that much information can be represented in a single hash. For this, the data itself is first hashed. Then the hashes are hashed again and merged. Finally, the Merkle Tree is merged into a single hash. This last hash is also called the root hash, the root of the tree. It represents all the information of its “leaves” (individual transactions) and “branches” (hashes of the leaves) in a relatively short string.

Creating the root hash is quick and easy, as long as all branches and leaves are known. We remember the function of a hash function: it works clearly and quickly in one direction and is impossible to break down in the other direction. If the root hash is known, but the transactions are unknown, it is impossible to guess the transactions.

A root hash alone is therefore not enough, and the rest of the block must be saved. Thus, the miner can validate the root hash at any time by hashing the information contained in the block again. As long as the hash function is the same, the miners always get the same hash for a given input of data. This is very handy because they can only check if they are on the same level as the hash.

Mining: The search for a special hash

In this context, it is easier to understand the mining of the proof of work. When mining, the block header of the block is incrementally changed to get a special hash. The header consists of five constants and one variable. The constants are the version number of the software, the hash of the previous block, the root hash of the Merkle tree, the timestamp, and the target size of the searched hash in bytes.

The variable is the nonce. A nonce is a number raised by one. Then the miner hashes the data and checks if the data results in a hash that is below the searched target value. If the hash value is greater than the target, the miner repeats the process; So it increases the nonce by one, hashes and checks again. It repeats this until it finds a hash below the target, or it gets another block from another networker whose hash is below the target. Then takes this new block and uses it as the basis for the next block (using the new hash as the "hash of the previous block").

Mining is a hyper-repetitive process whose goal is to find a special hash. Once the hash is found, the game starts again. The probability of finding a special hash depends on the difficulty. On average Bitcoin finds a new block every ten minutes. The difficulty keeps adapting, so this average stays the same.

The special feature of this process is that the special hash can only be found by guessing. This rate costs computing power and therefore energy. A look at the special hash is enough to see that it is special because it begins with zeros.

Here is an example of such a hash from the Bitcoin blockchain:

000000000000000000094bfa4edb1245c347e42452e4418e9fe5a1d24e335b16

Hashes: The matryoshka of the blockchain

A block can be simplified as a matryoshka image. The smallest doll is the unhashed transaction. The next envelope is the hashed form of this transaction. Thereafter, two hashed transactions are hashed together. So the hashes are merged more and more. In the end, there is only one hash remaining, the root hash, or the biggest matryoshka.

2.2 DISTRIBUTED CONSENSUS

Consensus is the process by which peers agree to the addition of next block in the block chain. Distributed Consensus ensures that different nodes in the network see the same data at nearly the same point of time. Hence in case of any failure, the system can still provide a service as the data is decentralised. To maintain anonymity in this large network, the permission less protocol is used where you don't need to record your identity while participating in the consensus.

Consensus Algorithms

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

Now, we will discuss various consensus algorithms and how they work.

2.2.1 Proof of Work (PoW):

The idea for Proof of Work(PoW) was first published in 1993 by Cynthia Dwork and Moni Naor and was later applied by Satoshi Nakamoto in the Bitcoin paper in 2008. Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The term "proof of work" was first used by Markus Jakobsson and Ari Juels in a publication in 1999.

Principle: A solution that is difficult to find but is easy to verify.

The purpose of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don't trust each other.

All the transactions in the new block are then validated and the new block is then added to the blockchain. Note that, the block will get added to the chain which has the longest block height(see blockchain forks to understand how multiple chains can exist at a point of time). Miners(special computers on the network) perform computation work in solving a complex mathematical problem to add the block to the network, hence named, Proof-of-Work. With time, the mathematical problem becomes more complex.

Working of POW(Proof of Work)

"The Proof of Work consensus algorithm involves solving a computational challenging puzzle in order to create new blocks in the Bitcoin blockchain. Colloquially, the process is known as 'mining', and the nodes in the network that engage in mining are known as 'miners'. The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 12.5 bitcoins(at the time of writing this article; this reward will get reduced by half its current value with time) and a small transaction fee."

The process of verifying the transactions in the block to be added, organizing these transactions in a chronological order in the block and announcing the newly mined block to the entire network does not take much energy and time. The energy consuming part is solving the 'hard mathematical problem' to link the new block to the last block in the valid blockchain. When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the PoW protocol. At the time of writing this article, mining a block in the bitcoin network gives the winning miner 12.5 bitcoins. The amount of bitcoins won halves every four years or so(thats how the bitcoin network is designed). So, the next deduction in the amount of bitcoin is due at around 2020-21(with the current rate and growth).

With more miners comes the inevitability of the time it takes to mine the new block getting shorter. This means that the new blocks are found faster. In order to consistently find 1 block every 10 minutes (That is the amount of time that the bitcoin developers think

is necessary for a steady and diminishing flow of new coins until the maximum number of 21 million is reached (expected some time with the current rate in around 2140)), the Bitcoin network regularly changes the difficulty level of mining a new block.

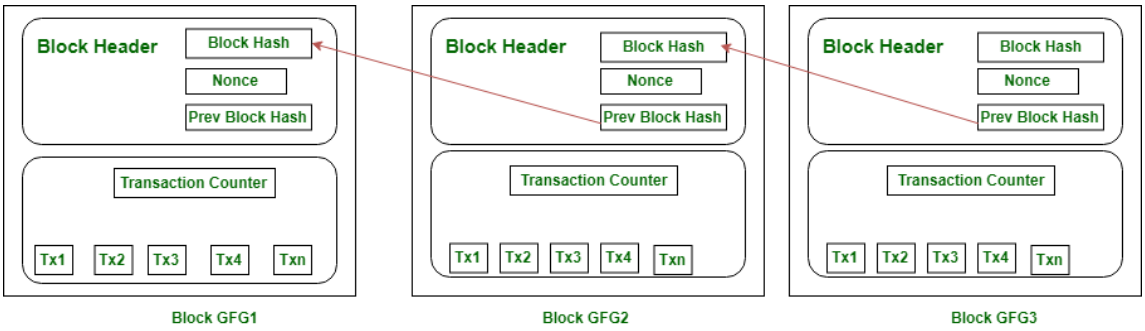


Fig 2.3 Proof of Work

The fact that Block GFG1 is connected to Block GFG2 through its hash number is important. The significance lies in the fact that this 'hash number' connects new block to the last block in the valid blockchain. If, on the other hand, the Block GFG1 Hash number on Block GFG2 had a different hash number than Block GFG1 they would not match up, and Block GFG2 would not be verified.
First block in the blockchain is called the Genesis Block and has no Prev Block Hash value.

Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain (amounting to calculating the entire chain of 'hard mathematical problems') which is practically impossible. This protects the blockchain from tampering.

Bitcoin's Proof-of-Work system:

Bitcoin uses the Hashcash Proof of Work system as the mining basis. The 'hard mathematical problem' can be written in an abstract way like below :

Given data A, find a number x such as that the hash of x appended to A results is a number less than B.

The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be solved. This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid. The answer to the

problem needs to be a lower number than the hash of the block for it to be accepted, known as the 'target hash'.A target hash is a number that the header of a hashed block must be equal to or less than for a new block, along with the reward, to be awarded to a miner. The lower a target is, the more difficult it is to generate a block.

A miner continues testing different unique values (known as nonce(s)) until a suitable one is produced. The miner who manages to solve the problem gets the bitcoin reward and adds the block into the blockchain by broadcasting that the block has been mined. The target hash adjusts once every 2016 blocks or approximately once every 2 weeks. All the miners immediately stop work on the said block and start mining the next block.

Common cryptographic protocols used in Proof of Work systems: The most widely used proof-of-work consensus is based on SHA-256 and was introduced as a part of Bitcoin. Others include Scrypt, SHA-3, scrypt-jane, scrypt-n, etc.

Features of Proof of Work system:

There are mainly two features that have contributed to the wide popularity of this consensus protocol and they are:

- It is hard to find a solution for the mathematical problem
- It is easy to verify the correctness of that solution

Main issues with the Proof-of-Work consensus:

\The Proof-of-Work consensus mechanism has some issues which are as follows:

- The 51% risk: If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.
- Time consuming: Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time consuming process.
- Resource consumption: Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that the 0.3% of the world's electricity will be spent to verify transactions by the end of 2018.

- Transaction confirmation takes about 10–60 minutes. So, it is not an instantaneous transaction; because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.

Cryptocurrencies using PoW:

- Litecoin
- Ethereum
- Monero coin
- Dogecoin

2.2.2 Proof of Stake (PoS):

Proof of Stake (PoS) is a type of algorithm which aims to achieve distributed consensus in a Blockchain. This way to achieve consensus was first suggested by Quantum Mechanic here and later Sunny King and his peer wrote a paper on it. This led to Proof-of-Stake (PoS) based Peercoin. A stake is value/money we bet on a certain outcome. The process is called staking. A more particular meaning of stake will be defined later on.

Need of Proof-of-Stake:

Before proof of stake, the most popular way to achieve distributed consensus was through Proof-of-Work (implemented in Bitcoin). But Proof-of-Work is quite energy(electrical energy in mining a bitcoin) intensive. So, a proof-of-work based consensus mechanism increases an entity's chances of mining a new block if it has more computation resources. Apart from the upper two points, there are other weaknesses of a PoW based consensus mechanism which we will discuss later on. In such a scenario, a Proof-of-Stake based mechanism holds merit.

Proof-of-Stake:

As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

- **Coin-age based selection:** The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.

- **Random Block selection:** The validator is chosen with a combination of 'lowest hash value' and 'highest stake'. The node having the best weighted-combination of these becomes the new validator.

A typical PoS based mechanism workflow:

1. Nodes make transactions. The PoS algorithm puts all these transactions in a pool.
2. All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like 'coin-age' or 'randomized block selection' to select the validator.
3. The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can 'OK' the new block.
4. If the block is 'OK'-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block's has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
5. If the block is not verified by other nodes on the network, the validator loses its stake and is marked as 'bad' by the algorithm. The process again starts from step 1 to forge the new block.

Features:

Fixed coins in existence:

There is only a finite number of coins that always circulate in the network. There is no existence of bringing new coins into existence(as in by mining in case of bitcoin and other PoW based systems). Note that the network starts with a finite number of coins or 'initially starts with PoW, then shifts to PoS' in some cases. This initiation with PoW is meant to bring coins/cryptocurrency in the network.

Transaction fee as reward to minters/forgers:

Every transaction is charged some amount of fee. This is accumulated and given to the entity who forges the new block. Note that if the forged block is found fraudulent, the transaction fee is not rewarded. Moreover, the stake of the validator is also lost(which is also known as slashing).

Impracticality of the 51% attack:

To conduct a 51% attack, the attacker will have to own 51% of the total cryptocurrency in the network which is quite expensive. This deems doing the attack too tedious, expensive and not so profitable. There will occur problems when amassing such a share of total cryptocurrency as there might not be so much currency to buy, also that buying more and more coins/value will become more expensive. Also validating wrong transactions will cause the validator to lose its stake, thereby being reward-negative.

Advantages of PoS:

- **Energy-efficient:** As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved(as in case of Proof-of-Work system) thus saving the energy.
- **Decentralization:** In blockchains like Bitcoin(Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system(like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.
- **Security:** A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

Weakness of a PoS mechanism:

- **Large stake validators:** If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.

- **New technology:** PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.

- **The 'Nothing at Stake' problem:** This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

Blockchains using Proof-of-Stake:

- Ethereum(Casper update)
- Peercoin
- Nxt

Variants of Proof-of-Stake:

- Regular Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-of-Stake
- Masternode Proof-of-Stake

2.2.3 Proof of Space/ proof of capacity

Proof of space is a type of consensus algorithm achieved by demonstrating one's legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.

Proofs of space are very similar to proofs of work (PoW), except that instead of computation, storage is used to earn cryptocurrency. Proof-of-space is different from memory-hard functions in that the bottleneck is not in the number of memory access events, but in the amount of memory required. the release of Bitcoin, alternatives to its PoW mining mechanism were researched and PoS was studied in the context of cryptocurrencies. Proofs of space are seen as a fairer and greener alternative by blockchain enthusiasts due to the general-purpose nature of storage and the lower energy cost required by storage, but have been criticized for increasing demand for storage. Several theoretical and practical implementations of PoS have been released and discussed, such as SpaceMint, Burstcoin, and Chia.

Concept Description

A proof-of-space is a piece of data that a prover sends to a verifier to prove that the prover has reserved a certain amount of space. For practicality, the verification process needs to be efficient, namely, consume a small amount of space and time. For security, it should be hard for the prover to pass the verification if it does not actually reserve the claimed amount of space. One way of implementing PoS is by using hard-to-pebble graphs.The verifier asks the prover to build a labeling of a hard-to-pebble graph. The prover commits to the labeling. The verifier then asks the prover to open several random locations in the commitment.

2.3 Types of Attacks on PoW (Proof of Work) based systems

As we know, the idea of Proof of Work was by Cynthia Dwork and Moni Naor. This permissionless consensus uses double SHA 256 which makes it secure from hackers. With proof of work, miners compete with each other to complete the transaction and get the bounty. Even it has many advantages like solving the double-spending problem and very difficult to tamper it, but it is not impossible to tamper if the hacker has high computational power.

There are two major attacks by which PoW based systems can crash.They are :

1. Sybil Attacks
2. Denial of Service(DOS) Attacks

These are explained as following below with their solutions.

Sybil Attacks :

In Sybil attacks, the attacker attempts to fill the network with the clients under its control. When this thing happens the attacker can actually control or get a monopoly over the network and these clients can do different kinds of actions based on the instruction from the attacker. They can refuse to relay the valid blocks or they can only relay the blocks which are generated by the attackers and those blocks can lead to double-spending.

In Simple language, The attacker can include multiple nodes in the network who can collectively compromise the Proof of Work mechanism.

Solution –

To prevent Sybil attacks we have to diversify the connections i.e allowing outbound connection to one IP per / 16 IP address. So by diversifying the network it is expected that if

the attacker generates multiple false miners the attacker will generate them within the same clustered network or subnet.

Denial of Service (DOS) Attacks :

In this attack, the attacker sends a lot of data to a particular node so that node will not able to process normal Bitcoin transactions. As a result, the metabolism of the mining procedure will get delayed which wastes the power for computation and in that meantime, the attacker can also send new nodes to the network resulting in a monopoly which is nothing but a Sybil attack.

Solution –

To prevent DOS attacks there are several rules bitcoin have which are:

- No forwarding of orphaned blocks.
- No forwarding of double-spend transactions.
- No forwarding of same block or transactions
- Disconnect a peer that sends too many messages
- Restrict the block size to 1 MB (1mb according to Satoshi Nakamoto)
- Limit the size of the bitcoin script up to 10000 bytes.

1.4 Ethereum

Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum, and its own programming language, called Solidity.

As a blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions. The network's users can create, publish, monetize, and use applications on the platform, and use its Ether cryptocurrency as payment. Insiders call the decentralized applications on the network "dapps."

. The Enterprise Ethereum Alliance (EEA) has some big-name founding members too, including Microsoft, Intel, and JPMorgan Chase, according to The Motley Fool. “The adoption of Ethereum by the corporate world,” says CNBC, “means it could eventually be bigger than its early stage rival.” That means it’s time to get to know the Ethereum platform, including its features and applications, and what makes Ethereum different from Bitcoin.

Our “Ethereum Explained” Ethereum tutorial video lays it all out for you, and here we’ll cover what’s discussed in the video.

Ethereum

Ethereum is a blockchain-based computing platform that enables developers to build and deploy decentralized applications—meaning not run by a centralized authority. You can create a decentralized application for which the participants of that particular application are the decision-making authority.

Ethereum Features

- Ether: This is Ethereum's cryptocurrency.
- Smart contracts: Ethereum allows the development and deployment of these.
- Ethereum Virtual Machine: Ethereum provides the underlying technology—the architecture and the software—that understands smart contracts and allows you to interact with it.
- Decentralized applications (Dapps): Ethereum allows you to create consolidated applications, called decentralized applications. A decentralized application is called a Dapp (also spelled DAPP, App, or DApp) for short.
- Decentralized autonomous organizations (DAOs): Ethereum allows you to create these for democratic decision-making.

These are the essential features of Ethereum and before going deep into the Ethereum tutorial, let's discuss each of these features in more detail.

Ether

Ether (ETH) is Ethereum's cryptocurrency. It is the fuel that runs the network. It is used to pay for the computational resources and the transaction fees for any transaction executed on the Ethereum network. Like Bitcoins, ether is a peer-to-peer currency. Apart from being used to pay for transactions, ether is also used to buy gas, which is used to pay for the computation of any transaction made on the Ethereum network.

Also, if you want to deploy a contract on Ethereum, you will need gas, and you would have to pay for that gas in ether. So gas is the execution fee paid by a user for running a

transaction in Ethereum. Ether can be utilized for building decentralized applications, building smart contracts, and making regular peer-to-peer payments.

Smart Contracts

Smart_contracts are revolutionizing the way how traditional contracts worked, which is why you need to know about them in this Ethereum tutorial. A smart contract is a simple computer program that facilitates the exchange of any valuable asset between two parties. It could be money, shares, property, or any other digital asset that you want to exchange. Anyone on the Ethereum network can create these contracts. The contract consists primarily of the terms and conditions mutually agreed on between the parties (peers).

The primary feature of a smart contract is that once it is executed, it cannot be altered, and any transaction done on top of a smart contract is registered permanently—it is immutable. So even if you modify the smart contract in the future, the transactions correlated with the original contract will not get altered; you cannot edit them.

The verification process for the smart contracts is carried out by anonymous parties of the network without the need for a centralized authority, and that's what makes any smart contract execution on Ethereum a decentralized execution.

The transfer of any asset or currency is done in a transparent and trustworthy manner, and the identities of the two entities are secure on the Ethereum network. Once the transaction is successfully done, the accounts of the sender and receiver are updated accordingly, and in this way, it generates trust between the parties.

a) **Smart Contracts Vs. Traditional Contract Systems**

In conventional contract systems, you sign an agreement, then you trust and hire a third party for its execution. The problem is that in this type of process, data tampering is possible. With smart contracts, the agreement is coded in a program. A centralized authority does not verify the result; it is confirmed by the participants on the Ethereum blockchain-based network. Once a contract is executed, the transaction is registered and cannot be altered or tampered, so it removes the risk of any data manipulation or alteration.

Let's take an example in which someone named Zack has given a contract of $500 to someone named Elsa for developing his company's website. The developers code the agreement of the smart contract using Ethereum's programming language. The smart contract

has all the conditions (requirements) for building the website. Once the code is written, it is uploaded and deployed on the Ethereum Virtual Machine (EVM).

EVM is a runtime compiler to execute a smart contract. Once the code is deployed on the EVM, every participant on the network has a copy of the contract. When Elsa submits the work on Ethereum for evaluation, each node on the Ethereum network will evaluate and confirm whether the result given by Elsa has been done as per the coding requirements, and once the result is approved and verified, the contract worth $500 will be self-executed, and the payment will be paid to Elsa in ether. Zack's account will be automatically debited, and Elsa will be credited with $500 in ether.

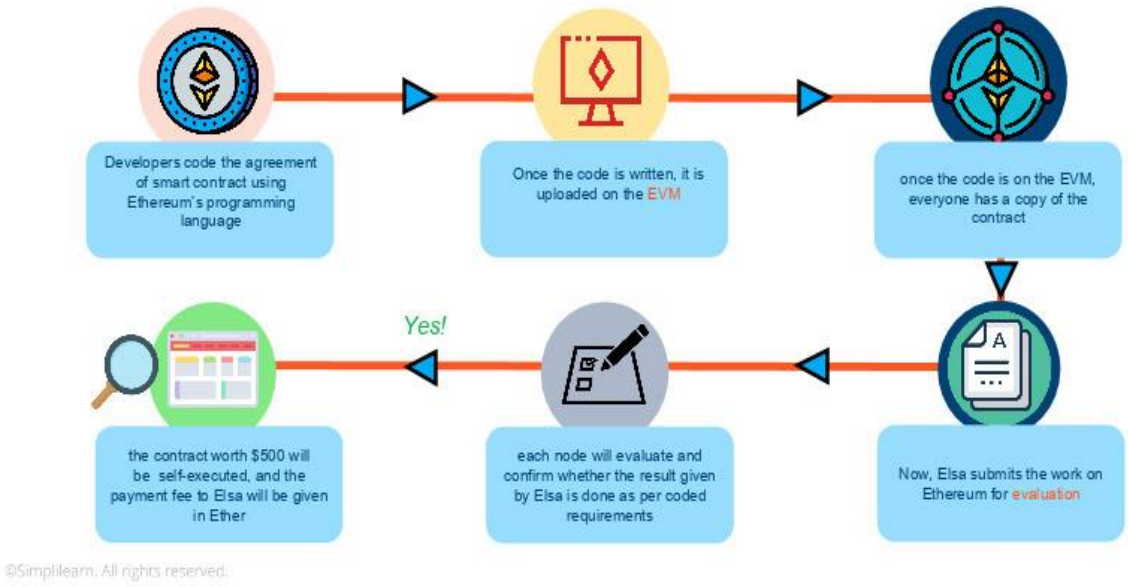


Fig 2.4 Smart contract

Ethereum Virtual Machine

EVM, as mentioned above in this Ethereum tutorial, is designed to operate as a runtime environment for compiling and deploying Ethereum-based smart contracts. EVM is the engine that understands the language of smart contracts, which are written in the Solidity language for Ethereum. EVM is operated in a sandbox environment—basically, you can deploy your stand-alone environment, which can act as a testing and development environment, and you can test your smart contract (use it) "n" number of times, verify it, and then once you are satisfied with the performance and the functionality of the smart contract, you can deploy it on the Ethereum main network.

Any programming language in the smart contract is compiled into the bytecode, which the EVM understands. This bytecode can be read and executed using the EVM. One of the most popular languages for writing a smart contract in Solidity. Once you write your smart contract in Solidity, that contract gets converted into the bytecode and gets deployed on the EVM. And thereby EVM guarantees security from cyberattacks.

a)Working *of EVM*

Suppose person A wants to pay person B 10 ethers. The transaction will be sent to the EVM using a smart contract for a fund transfer from A to B. To validate the transaction; the Ethereum network will perform the proof-of-work consensus algorithm.

The miner nodes on Ethereum will validate this transaction—whether the identity of A exists or not, and if A has the requested amount to transfer. Once the transaction is confirmed, the ether will be debited from A's wallet and will be credited to B's wallet, and during this process, the miners will charge a fee to validate this transaction and will earn a reward.All the nodes on the Ethereum network execute smart contracts using their respective EVMs.

b) Proof of Work

Every node in the Ethereum network has:

- The entire history of all the transactions—the entire chain
- The history of the smart contract, which is the address at which the smart contract is deployed, along with the transactions associated with the smart contract
- The handle to the current state of the smart contract

The goal of the miners on the Ethereum network is to validate the blocks. For each block of a transaction, miners use their computational power and resources to get the appropriate hash value by varying the nonce. The miners will vary the nonce and pass it through a hashing algorithm—in Ethereum, it is the Ethash algorithm.

This produces a hash value that should be less than the predefined target as per the proof-of-work consensus. If the hash value generated is less than the target value, then the block is considered to be verified, and the miner gets rewarded.

When the proof of work is solved, the result is broadcast and shared with all the other nodes to update their ledger. If other nodes accept the hashed block as valid, then the block gets added to the Ethereum main blockchain, and as a result, the miner receives a reward, which as of today stands at three ethers. Plus the miner gets the transaction fees that have been generated for verifying the block. All the transactions that are aggregated in the block—the cumulative transaction fees associated with all the transactions are also given as a reward to the miner.

c) Proof of Stake

In Ethereum, a process called proof of stake is also under development. It is an alternative to proof of work and is meant to be a solution to minimize the use of expensive resources spent on mining using proof of work. In proof of stake, the miner—who is the validator—can validate the transactions based on the number of crypto coins he or she holds before actually starting the mining. So based on the accumulation of crypto coins the miner has beforehand, he or she has a higher probability of mining the block. However, proof of stake is not widely used as of now compared to proof of work.

d) Gas

Just like we need fuel to run a car, we need gas to run applications on the Ethereum network. To perform any transaction within the Ethereum network, a user has to make a payment—shell out ethers—to get a transaction done, and the intermediary monetary value is called gas. On the Ethereum network, gas is a unit that measures the computational power required to run a smart contract or a transaction. So if you have to do a transaction that updates the blockchain, you would have to shell outgas, and that gas costs ethers.

In Ethereum, the transaction fees are calculated using a formula (see screenshot below). For every transaction, there is gas and its correlated gas price. The amount of gas required to execute a transaction multiplied by the gas price equals the transaction fees. “Gas

limit" refers to the amount of gas used for the computation and the amount of ether a user is required to pay for the gas.

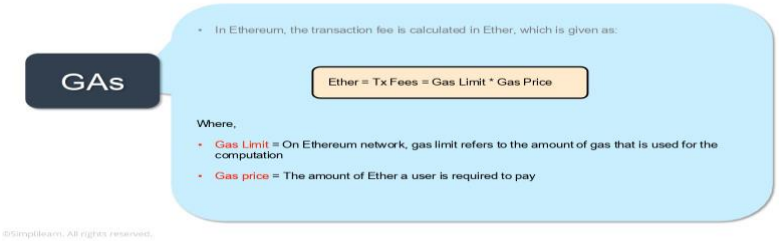


Fig 2.5 Gas value

Below is a screenshot from the Ethereum network showing the transaction cost. You can see for this particular transaction, the gas limit was 21,000, the gas used by the transaction was 21,000, and the gas price was 21 Gwei, which is the lowest denomination of ether. So 21 Gwei * 21,000 gave the actual transaction fees: 0.000441 ethers, or about 21 cents as of today. As mentioned, the transaction fee goes to the miner, who has validated the transaction.

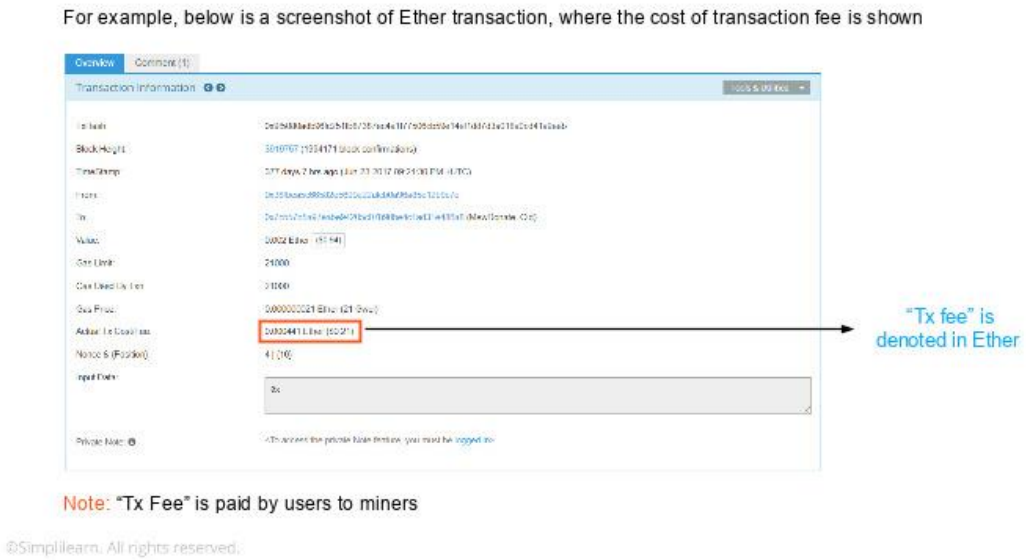


Fig 2.6 Transaction fees in ethereum

To understand the gas limit and the gas price, let's consider an example using a car. Suppose your vehicle has a mileage of 10 kilometers per liter and the amount of petrol is $1 per liter. Then driving a car for 50 kilometers would cost you five liters of petrol, which is

worth $5. Similarly, to perform an operation or to run code on Ethereum, you need to obtain a certain amount of gas, like petrol, and the gas has a per-unit price, called gas price.

If the user provides less than the amount of gas to run a particular operation, then the process will fail, and the user will be given the message "out of gas." And Gwei, as noted above, is the lowest denomination of ether used for measuring a unit of a gas price.

***e*) Ethereum Mining Vs. Bitcoin Mining**

The hashing algorithm is the primary difference between Ethereum mining and Bitcoin mining.

Bitcoin uses SHA-256, and Ethereum uses Ethash. The average time taken on Bitcoin for mining a block is 10 minutes, whereas on Ethereum it is 12 to 15 seconds. As of today, the mining reward for Bitcoin is 12.5 bitcoins; for Ethereum it's three ethers plus the transaction fee—the cumulative transaction fees of all the transactions of a block. As of April 10, 2019, the value of 1 bitcoin is $5249.03, whereas one ether is $180.89.

f) Ethereum Mining VS Bitcoin Mining

Table 1 comparison of Bitcoin and Ethereum

	Bitcoin	Ethereum
Hashing Algorithm	SHA-256	Ethash
Time is taken to mine a block	An average of 10 minutes	An average of 12-15 seconds
Reward	12.5 BTC	3 ETH
USD - 04/10/2019	1 Bitcoin = 5249.03	1 Ether = 180.89

Below is a screenshot of an Ethereum reward that has been given to the miner of the block. As you can see, the reward is three ethers plus the total accumulated transaction fees of all the underlying transactions in this block, which are 0.0666 ethers.

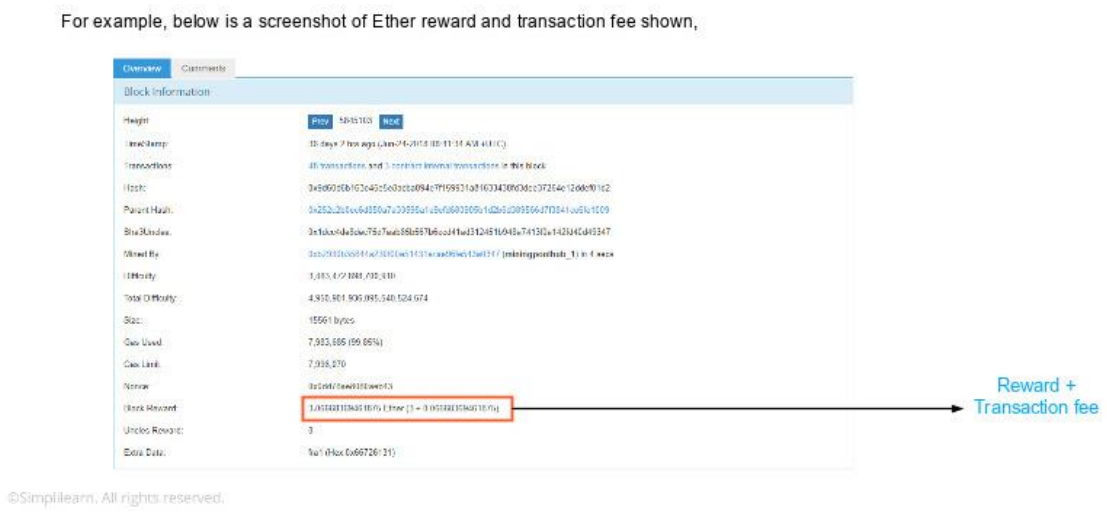


Fig 2.7 Reward calculation in ethereum

Decentralized Applications (Dapps)

Let's compare decentralized applications with traditional applications. When you log in to Twitter, for example, a web application gets displayed that is rendered using HTML. The page will call an API to access your data (your information), which is centrally hosted. It's a simple process: your front end executes the backend API, and the API goes and fetches your data from a centralized database.

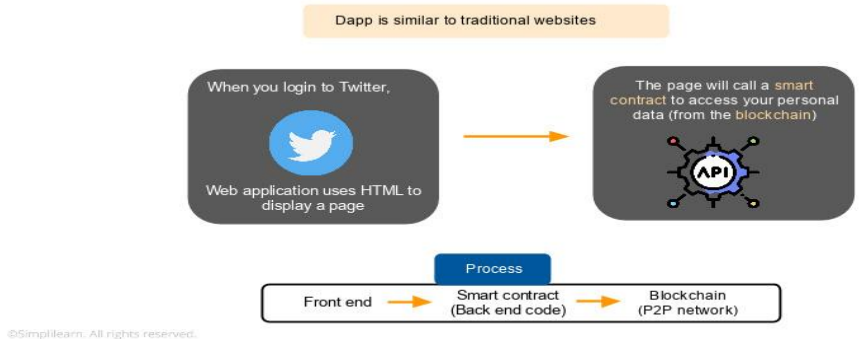


Fig 2.8 Dapps

If we transform this application into a decentralized application when you log in, the same web application gets rendered, but it calls a smart contract-based API to fetch the information from the blockchain network. So the API is replaced by a smart contract

interface, and the smart contract will bring the data from the blockchain network, which is its backend.

That blockchain network is not a centralized database; it's a decentralized network in which the participants of the network (the miners) validate (verify) all the transactions that are happening using the smart contract on the blockchain network. So any transaction or action happening on a Twitter-type application that has now been transformed will be a decentralized transaction.

A Dapp consists of a backing code that runs on a distributed peer-to-peer network. It is a software designed to work in the Ethereum network without being controlled by a centralized system, as mentioned, and that is the primary difference: it provides direct interaction between the end-users and the decentralized application providers.

An application qualifies as a Dapp when it is open-source (its code is on Github), and it uses a public blockchain-based token to run its applications. A token acts as fuel for the decentralized application to run. Dapp allows the backend code and data to be decentralized, and that is the primary architecture of any Dapp.

Decentralized Autonomous Organizations (DAOs)

A DAO is a digital organization that operates without hierarchical management; it works in a decentralized and democratic fashion. So basically a DAO is an organization in which the decision-making is not in the hands of a centralized authority but preferably in the hands of certain designated authorities or a group or designated people as a part of an authority. It exists on a blockchain network, where it is governed by the protocols embedded in a smart contract, and thereby, DAOs rely on smart contracts for decision-making—or, we can say, decentralized voting systems—within the organization. So before any organizational decision can be made, it has to go through the voting system, which runs on a decentralized application.

Here's how it works. People add funds through the DAO because the DAO requires funding in order to execute and make decisions. Based on that, each member is given a token that represents that person's percentage of shares in the DAO. Those tokens are used to vote in the DAO, and the proposal status is decided based on the maximum votes. Every decision within the organization has to go through this voting process.

Real-World Applications of Ethereum

Voting Systems

As we've seen with DAO, voting systems are adopting Ethereum. The results of polls are publicly available, ensuring a transparent and fair democratic process by eliminating voting malpractices.

Banking Systems

Ethereum is getting adopted widely in banking systems because with Ethereum's decentralized system; it is challenging for hackers to gain unauthorized access. It also allows payments on an Ethereum-based network, so banks are also using Ethereum as a channel to make remittances and payments.

Shipping

Deploying Ethereum in shipping helps with the tracking of cargo and prevents goods from being misplaced or counterfeited. Ethereum provides the provenance and tracking framework for any asset required in a typical supply chain.

Agreements

With Ethereum smart contracts, agreements can be maintained and executed without any alteration. So in an industry that has fragmented participants, is subject to disputes, and requires digital contracts to be present, Ethereum can be used as a technology for developing smart contracts and for digitally recording the agreements and the transactions based on them.

2.3 POS/POW HYBRID

Understanding POW

In the blockchain network**,** there are various ways to validate transactions in a decentralized manner, one is Proof of Work (PoW), and the other is Proof of Stake(PoS). Now, as we have understood the concept of consensus mechanism, let's start discussing with Proof-of-Work (PoW) consensus.

The central principle behind this consensus is to solve complex mathematical problems and make the largest number of guesses as quickly as possible. Such requires a lot of computational power, and by using a more efficient mining machine to run calculations, a miner is able to maximize profitability in terms of crypto rewards. In this type of consensus mechanism, miners compete to be the first one to find a hash regarding a particular block, which can only be solved using sheer computing power to make the largest number of

guesses. When a miner finds the right solution, they advertise it to the whole network, receiving a reward in cryptocurrency, provided by the protocol. Bitcoin is a classic example that achieves consensus using Proof-of-Work.

The Concept of PoS

Proof-of-Stake is a consensus algorithm that deals with the main drawbacks of PoW. In this mechanism, every block gets validated before the network adds another block to the blockchain ledger. Unlike PoW, where miners have to solve complex puzzles, in PoS, miners can join the mining process using their coins to stake. It allows users to mine for rewards using very minimal hardware and software resources. Here, the mining capacity of a particular miner depends on how many coins they already have; thus, the more coins one has, the better chances are, which indicates only the richest can have control of the consensus. Moreover, a person with enough money to invest can purchase an insane amount of coins, thereby reducing the decentralization of the system.

The Hybrid of PoW and PoS

Hybrid PoW/PoS consensus mechanisms utilize elements of both PoW and PoS models when determining transaction validation rights, and for doing so, hybrid aims to mitigate the weaknesses of each consensus mechanism.

Decred is the most notable project to utilize both the consensus mechanisms (PoW & PoS) in recognizable forms and merge them together to produce a hybrid consensus mechanism. It is a governance-focused cryptocurrency that utilizes neither solely the 1 CPU = 1 vote of PoW nor the '1 token = 1 vote' of a PoS consensus. Instead, it opts for a hybrid approach where transactions on the Decred network are validated through a hybrid of both the consensus mechanisms.

A hybrid consensus starts with having PoW miners to create new blocks containing transactions to be added to the blockchain. Once these blocks are created, PoS miners decide whether to confirm them or not. PoS miners purchase votes by staking a portion of their tokens. However, instead of examining the total vote count, the hybrid PoW/PoS mechanism randomly chooses 5 'votes' to determine the efficacy of the newly created block; if 3 of the 5 chosen votes are affirmative, the block is added to the blockchain. In exchange for these services, PoW miners receive 60% of the block reward, PoS miners receive 30%, and the remaining 10% is dedicated to developmental efforts.

It is clear that consensus algorithms make the nature of the blockchain networks versatile. But it is not a single consensus algorithm that can claim it to be perfect. There are various other consensus mechanisms such as Proof of Activity, Proof-of-Burn, Proof-of-Weight, amongst others.

Similar to Decred, as already discussed, Hcash is a decentralized, open-source, cross-platform cryptocurrency that works under the hybrid Pow + PoS consensus mechanism. It ensures that all PoW-generated blocks must be verified by PoS miners in order to join the blockchain. Having both miners and stakeholders participating in block production, hybrid eliminates the possibility of hash power monopoly to a great extent and ensures the security of the network.

2.5 Cryptocurrency to blockchain 2.0

Blockchain technology has to be one of the biggest innovations of the 21st century given the ripple effect it is having on various sectors, from financial to manufacturing as well as education. Unknown to many, is that the history of Blockchain dates back to the early 1990s.

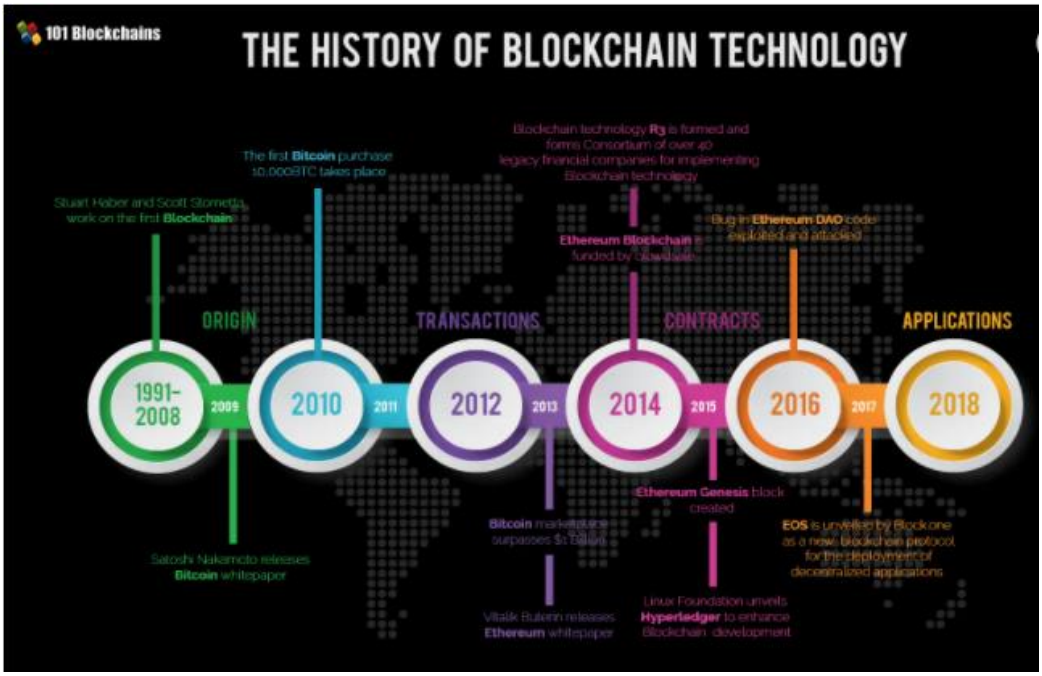


Fig 2.9 Evolution of block chain

History of Blockchain Technology

It is important to know about the history of Blockchain for Blockchain enthusiasts and Blockchain aspirants. So, to help our reader know the Blockchain history and understand the

Blockchain evolution, here we bring a detailed guide to the history of blockchain technology with its detailed evolution.

1991-2008: Early Years of Blockchain Technology

How did blockchain emerge? Stuart Haber and W. Scott Stornetta envisioned what many people have come to know as blockchain, in 1991. Their first work involved working on a cryptographically secured chain of blocks whereby no one could tamper with timestamps of documents.

In 1992, they upgraded their system to incorporate Merkle trees that enhanced efficiency thereby enabling the collection of more documents on a single block. However, it is in 2008 that Blockchain History starts to gain relevance, thanks to the work one person or group by the name Satoshi Nakamoto.

Satoshi Nakamoto is accredited as the brains behind blockchain technology. Very little is known about Nakamoto as people believe he could be a person or a group of people that worked on Bitcoin, the first application of the digital ledger technology. Nakamoto conceptualized the first blockchain in 2008 from where the technology has evolved and found its way into many applications beyond cryptocurrencies. Satoshi Nakamoto released the first whitepaper about the technology in 2009. In the whitepaper, he provided details of how the technology was well equipped to enhance digital trust given the decentralization aspect that meant nobody would ever be in control of anything.

Ever since Satoshi Nakamoto exited the scene and handed over Bitcoin development to other core developers, the digital ledger technology has evolved resulting in new applications that make up the blockchain History.

Blockchain Structure

In simple terms, Blockchain is a peer-to-peer distributed ledger that is secure and used to record transactions across many computers. The ledger's contents can only be updated by adding another block linked to the previous block. It can also be envisioned as a peer-to-peer network running on top of the internet.

In layman or businesses term, blockchain is a platform where people are allowed to carry out transactions of all sorts without the need for a central or trusted arbitrator.

The created database is shared among network participants in a transparent manner, whereby everyone can access its contents. Management of the database is done autonomously using peer-to-peer networks and a time stamping server. Each block in a blockchain is arranged in such a way that it references the content of the previous block.

The blocks that form a blockchain hold batches of transactions approved by participants in a network. Each block comes with a cryptographic hash of a previous block in the chain.

Evolution of Blockchain: Phase 1- Transactions

2008-2013: Blockchain 1.0: Bitcoin Emergence

Most people believe that Bitcoin and Blockchain are one and the same thing. However, that is not the case, as one is the underlying technology that powers most applications of which one of them is cryptocurrencies.

Bitcoin came into being in 2008 as the first application of Blockchain technology. Satoshi Nakamoto in his whitepaper detailed it as an electronic peer-to-peer system. Nakamoto formed the genesis block, from which other blocks were mined, interconnected resulting in one of the largest chains of blocks carrying different pieces of information and transactions.

Ever since Bitcoin, an application of blockchain, hit the airwaves, a number of applications have cropped all of which seek to leverage the principles and capabilities of the digital ledger technology. Consequently, blockchain history contains a long list of applications that have come into being with the evolution of the technology.

Evolution of Blockchain: Phase 2- Contracts

2013-2015: Blockchain 2.0: Ethereum Development

In a world where innovation is the order of the day, Vitalik Buterin is among a growing list of developers who felt Bitcoin had not yet reached there, when it came to leveraging the full capabilities of blockchain technology, as one of the first contributors to the Bitcoin codebase.

Concerned by Bitcoin’s limitations, Buterin started working on what he felt would be a malleable blockchain that can perform various functions in addition to being a peer-to-peer

network. Ethereum was born out as a new public blockchain in 2013 with added functionalities compared to Bitcoin, a development that has turned out to be a pivotal moment in Blockchain history.

Buterin differentiated Ethereum from Bitcoin Blockchain by enabling a function that allows people to record other assets such as slogans as well as contracts. The new feature expanded Ethereum functionalities from being a cryptocurrency to being a platform for developing decentralized applications as well.

Officially launched in 2015, Ethereum blockchain has evolved to become one of the biggest applications of blockchain technology given its ability to support smart contracts used to perform various functions. Ethereum blockchain platform has also succeeded in gathering an active developer community that has seen it establish a true ecosystem.

Ethereum blockchain processes the most number of daily transactions thanks to its ability to support smart contracts and decentralized applications. Its market cap has also increased significantly in the cryptocurrency space.

Evolution of Blockchain: Phase 3- Applications

2018: Blockchain 3.0: the Future

Blockchain History and evolution does not stop with Ethereum and Bitcoin. In recent years, a number of projects have cropped up all leveraging blockchain technology capabilities. New projects have sought to address some of the deficiencies of Bitcoin and Ethereum in addition to coming up with new features leveraging blockchain capabilities.

Some of the new blockchain applications include NEO, billed as the first open-source, decentralized, and blockchain platform launched in China. Even though the country has banned cryptocurrencies, it remains active when it comes to blockchain innovations. NEO casts itself as the Chinese Ethereum having already received the backing of Alibaba CEO Jack Ma as it plots to have the same impact as Baidu in the country.

In the race to accelerate the development of the Internet of Things, some developers, so it fit, to leverage blockchain technology and in the process came up with IOTA. The cryptocurrency platform is optimized for the Internet of things ecosystem as it strives to provide zero transaction fees as well as unique verification processes. It also addresses some of the scalability issues associated with Blockchain 1.0 Bitcoin.

In addition to IOTA and NEO, other second-generation blockchain platforms are also having a ripple effect in the sector. Monero Zcash and Dash blockchains came into being as a way of addressing some of the security and scalability issues associated with the early blockchain applications. Dubbed as privacy Altcoins, the three blockchain platform seek to provide high levels of privacy and security when it comes to transactions.

The blockchain history discussed above involves public blockchain networks, whereby anyone can access the contents of a network. However, with the evolution of technology, a number of companies have started adopting the technology internally as a way of enhancing operational efficiency.

Large enterprises are investing big in hiring professionals as they seek to gain a head start on the use of technology. Companies like Microsoft and Microsoft appear to have taken the lead when it comes to exploring blockchain technology applications resulting in what has come to be known as private, hybrid, and federated blockchains.

2015: Hyperledger

In 2015, the Linux Foundation unveiled an Umbrella project of open-source blockchain. They went on to call it Hyperledger, which until to date acts as collaborative development of distributed ledgers. Under the leadership of Brian Behlendorf, Hyperledger seeks to advance cross-industry collaboration for the development of blockchain and distributed ledgers. Hyperledger focuses on encouraging the use of blockchain technology to improve the performance and reliability of current systems to support global business transactions.

2017: EOS.IO

EOS brainchild of private company block.one came into being in 2017, on the publishing of a white paper detailing a new blockchain protocol powered by an EOS as the native cryptocurrency. Unlike other blockchain protocols, EOS tries to emulate attributes of real computers including CPU and GPU.

For that reason, EOS.IO doubles up as a smart contract platform as well as a decentralized operating system. Its main purpose is to encourage the deployment of decentralized applications through an autonomous decentralized corporation.

Table 2 Blockchain Evolution Timeline

Timeline	Blockchain	Bitcoin	Ethereum
1991-2008	Stuart Haber and Scott Stornetta Work on The First Blockchain		
2009		Satoshi Nakamoto Releases Bitcoin White Paper	
2010		The First Bitcoin Purchase 10,000BTC take place	
2013		Bitcoin Marketplace Surpasses $1 Billion	Vitalik Buterin Releases Ethereum White Paper
2014			Ethereum Blockchain Is Funded By Crowdsale
2014	Blockchain Technology R3 is Formed and forms a Consortium of Over 40 Legacy financial for implementing Blockchain Technology		
2014			
2015			Ethereum Second Blockchain Is Unveiled
2015	Linux Foundation Unveils Hyperledger To Enhance Blockchain development		
2017	EOS.IO is Unveiled by block.one as a new blockchain protocol for the deployment of decentralized applications		
2015-2018	Blockchain Technology Continues To Evolve		

Timeline	Blockchain	Bitcoin	Ethereum
	Depicted by increased number of cryptocurrencies as well as Companies leveraging the Technology To enhance Efficiency		

2020: Blockchain History & The Future

The future of Blockchain technology looks bright, in part, because of the way governments and enterprises are investing big as they seek to spur innovations and applications. It is becoming increasingly clear that one day there will be a public blockchain that anyone can use.

Advocates expect the technology to help in the automation of most tasks handled by professionals in all sectors. The technology is already finding great use in supply management as well as in the cloud computing business. The technology should also find its way into basic items such as search engines on the internet in the future.

As the technology evolves, Gartner Trend Insights expects at least one business built on blockchain to come into being valued at more than $10 billion by 2022. Due to the Blockchain Digital Transformation, the research firm expects the business value to grow to over $176 billion by 2025 and exceed the $3.1 trillion by 2030. The evolution of Blockchain Technology in recent years has increased the demand for Blockchain professionals. the companies are also implementing Blockchain to get benefits of the Blockchain applications.

2.6 Model of Blockchain- Algorand

Algorand is a block chain-based cryptocurrency platform that aims to be secure, scalable, and decentralized The Algorand platform supports smart contract functionality, and its consensus algorithm is based on proof-of-stake principles and a Byzantine Agreement protocol.Algorand's native cryptocurrency is called Algo.

In the Algorand network, the consensus algorithm is permissionless, and all users who hold an Algo balance can participate. The consensus algorithm works in rounds, with each round made up of two phases. The first phase is the block proposal phase, during which

blocks are proposed as the new block; the second phase is the block finalization phase, during which a vote on the proposed blocks is taken.

The first phase (the block proposal phase) uses proof of stake principles. During this phase, a committee of users in the system is selected randomly, though in a manner that is weighted, to propose the new block. The selection of the committee is done via a process called "cryptographic sortition." In cryptographic sortition, there is not a central authority that designates who the members of the committee are and then communicates that information across the network; rather, each user determines whether they are on the committee or not by locally executing a Verifiable Random Function (VRF). If the VRF indicates that the user is chosen, the VRF returns a cryptographic proof that can be used to verify that the user is on the committee.

Only a given user knows whether they are on the committee, unless/until they send a message to other users indicating that they are. The likelihood that a given user will be on the committee is influenced by the "stake" (i.e., the number of Algo tokens) held by that user, in proportion to the size of the user's stake. After determining that they are on the block selection committee, a user builds a proposed block and disseminates it to the network for review/analysis during the second phase. The user includes the cryptographic proof from the VRF in their proposed block, which demonstrates that the user was in fact an eligible committee member.

In the second phase (the block finalization phase), a Byzantine Agreement protocol (called "BA⋆") is used to vote on the proposed blocks. In this second phase, cryptographic sortition as described above is again used to determine a committee; this second-phase voting committee will be different from the committee from the first phase, though it is possible that there could be overlap in membership between the two committees. When users have determined that they are in this second-phase voting committee, they analyze the proposed blocks they have received (this will include verifying that they were in fact proposed by users from the first-phase committee) and vote on whether any of the blocks should be adopted or not. If the voting committee achieves consensus on a new block, then the new block is disseminated across the network as the new block.

The Algorand consensus algorithm possess the characteristic of "player replaceability"; i.e., as noted above, membership in the different committees (in both the block proposal and block finalization phase) changes every time the phase is run. This

protects users against targeted attacks, as an attacker will not know in advance which users are going to be in a committee.

Algorand is resilient against arbitrary partitions, also known as asynchronous safety. Two different blocks cannot reach consensus in the same round, i.e. it is mathematically guaranteed that Algorand will not fork.The asynchronous safety has also been formally verified by Runtime Verification Inc. and compared to their previous verification models, the model also accounts for timing issues and adversary actions, e.g., when the adversary has control over message delivery.

Smart contracts

Algorand supports two types of smart contracts: stateless smart contracts and stateful smart contracts. Stateless smart contracts are intended for the purpose of authorizing transactions; stateful smart contracts store data persistently and can be used for broader purposes.

Algorand smart contracts can be written in a programming language called Transaction Execution Approval Language (TEAL). TEAL is a bytecode-based stack language, with a programming interface for Python that is called PyTeal. While some smart contract programming models are Turing-complete (for example, Solidity is Turing-complete), the Algorand smart contracts model is *not* Turing-complete. The Algorand smart contracts model does support transaction atomicity. In some other blockchain systems, smart contracts are used to define user-defined assets; for example, in Ethereum, smart contracts implement the ERC20 and ERC721 interfaces to define new assets. In Algorand, in contrast, user-defined assets are supported natively, and Algorand smart contracts are able to manipulate user-defined assets (for example, by transferring ownership of given amounts of them) using built-in transaction types.

Crypto Primitives, Securing and Interconnecting Public and Private Block Chains

Syllabus

Hash Function and Merle Tree-Security Properties-Security Considerations for block chain-Digital Signature-Public Key Cryptography-Bitcoin blockchain incentive structures- Nash Equilibriums- evolutionary stable strategies,-and Pareto efficiency (game theory) Weaknesses and news Points of Failure, Mitigation Methods, Redundancies and fall-back methods.

3.1 Hash Function and Merle Tree

Block

With blockchain technology, each page in a ledger of transactions forms a block. This block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks or a blockchain.

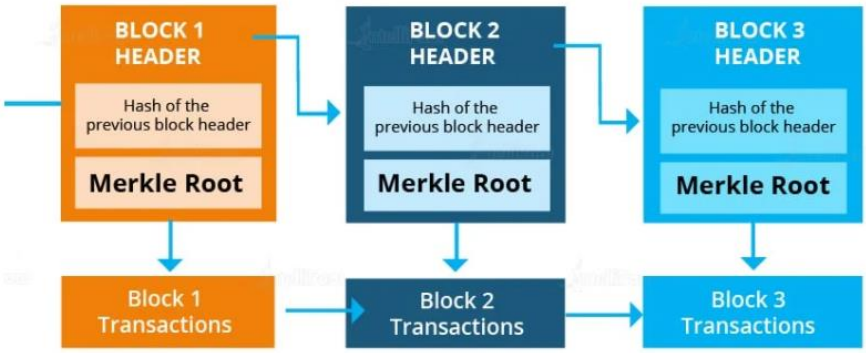


Figure 3.1 Blockchain Diagram on how blocks are connected

Blockchain working model

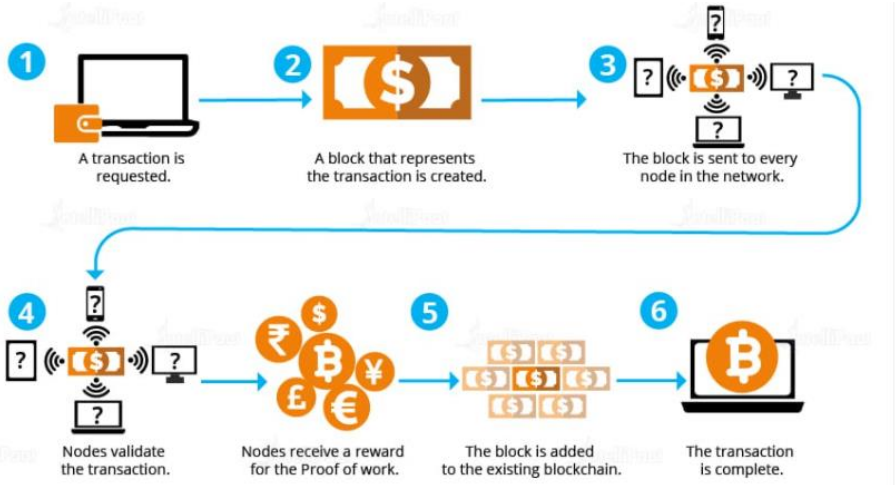


Figure 3.2 Blockchain working model

Blockchain Diagram: Only when the transaction is verified and validated, values can be transferred to another place.

Whenever a blockchain is introduced to a new blockchain transaction or any new block is to be added to the blockchain, in general, numerous nodes within the same blockchain implementation are required to execute algorithms to evaluate, verify and process the history of the blockchain block. If most of the nodes authenticate the history and signature of the block, the new block of blockchain transaction is accepted into the ledger and the new block containing data is added to the blockchain. If a consensus is not achieved, the block is denied being added to the blockchain. This distributed consensus model allows blockchains to function as a distributed ledger without requiring any central or unifying authority to validate the blockchain transactions. Thus, the blockchain transaction is extremely secure.

Blockchain Architecture

When we investigate the DNA of blockchain architecture for a better understanding, we need to analyze several aspects that contribute to this disruptive technological marvel. How does blockchain work? These aspects include the blockchain platform, nodes, transactions that makeup blocks, security implementations, and the process of adding new blocks to the chain. The blockchain architecture is undoubtedly complex, but once you get a hold of it you will get acquainted with the same.

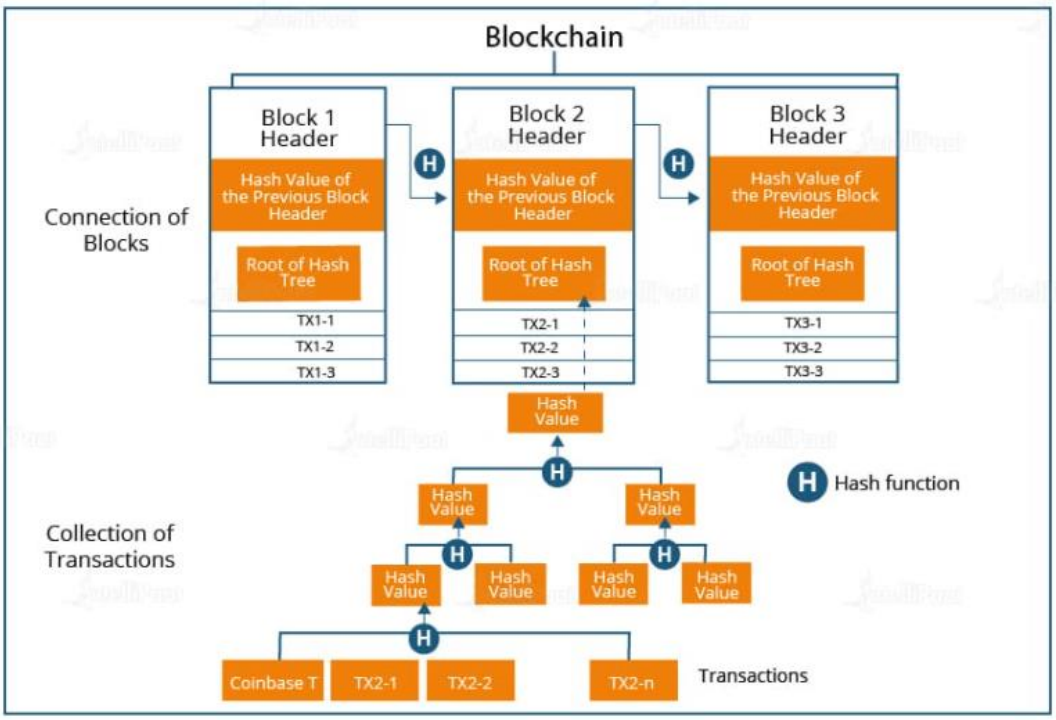


Figure 3.3 Basic architectural representation of a blockchain.

With blocks being connected with each other through their respective hash codes, the whole blockchain ecosystem becomes a Fort Knox technically. Whenever a blockchain transaction flag is raised, a blockchain consensus needs to be achieved to update the same in the blockchain. Instead of relying on a third party to mediate transactions, member nodes in the blockchain network stick to a blockchain consensus protocol to agree on the ledger content and cryptographic hashes and digital signatures to ensure the integrity of transactions. Once authenticated, these blockchain transactions are considered successful and irreversible. Transactions rely a lot on hash values and hash functions. These hash functions are mathematical processes that take input data of any size, perform required operations on it, and return the output data of a fixed size. These functions can be used to take a string of any length as input and return a sequence of letters of a fixed length. This functionality of hash functions makes them apt for transaction processing. Regardless of the size of transactions, the final output will always be fixed and untampered.

After coming across the term 'hashing' these many times, it has become a matter of innate necessity for us to understand what hashing depicts. Also, let's shed some light on the 'identity' of blocks. Under the hood of blockchains, hashing is necessarily a process that helps differentiate between blocks. The process of hashing gives blocks in a blockchain a unique identity. Technically, blocks in a blockchain are identified by their hash, which serves the purposes of both identification and integrity verification. An identification string that also provides its own integrity is called a self-certifying identifier. The hashing functions generate public keys. Here's an example pertaining to hashing for a bitcoin blockchain. Bitcoin uses SHA-256 hash function that produces a hash code of size 256 bits or 32 bytes.

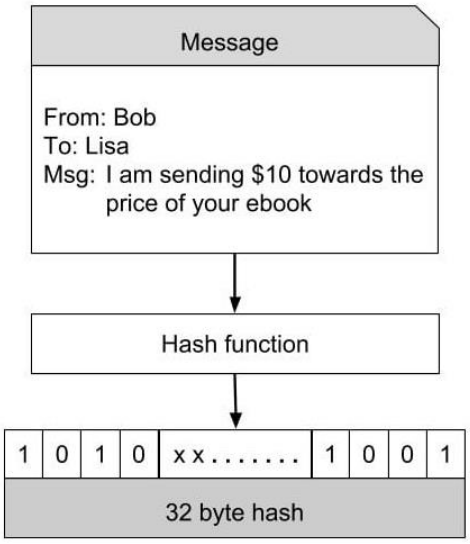


Figure 3.4 Hash message

Blockchain Diagram: Bob, while placing an order with Lisa, creates a message which is like the one shown above. This message is hashed through a hash function that produces a 32 bytes hash code. The beauty of the hash is that for all practical purposes it can be considered unique for the contents of the message. If the message is modified, the hash value will change. This makes it impossible to reconstruct the original message. Hacking, therefore, is a distant dream with hash functions.

Cryptographic Keys and Digital Signatures

As the information on the blockchain is transferred over peer-to-peer (P2P) networks across the globe, cryptographic keys are incorporated to send data throughout the network without compromising the safety and integrity. These keys not only allow blockchains to respect the privacy of users but also uphold the ownership of assets and secure the information of blocks in the network. Cryptography is applied throughout the entire blockchain onto all the information that is stored and transacted. This provides users with cryptographic proof that serves as the basis for trusting the legitimacy of a user's claim to an asset on the blockchain. Cryptographic hashes also help a great deal as they ensure that even the smallest change to a transaction will result in a different hash value being computed, which will eventually indicate a clear change in the transactional history. While cryptographic keys are necessary for safety and integrity, digital signatures provide verification and authentication of ownership on the blockchain. Using cryptographic digital signatures, a user can sign a transaction proving the ownership of that asset and anyone on the blockchain can digitally verify the identity to be true.

Blockchain Nodes

In simple terms, every participant in a blockchain network is a node. Being a decentralized network where a central authority is absent, there is great value for blockchain nodes. There exist several types of blockchain nodes, and each of them requires specific hardware configurations to get hosted or connected. Basically, there are two types of nodes: full nodes and lightweight nodes. These types comprise a constellation of a variety of nodes that are grouped under them.

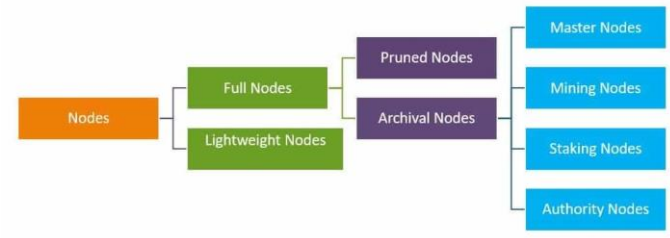


Figure 3.4 Blockchain nodes

Full nodes act as a server in a decentralized network. Their main tasks include maintaining the consensus between other nodes and verifying the transactions. They also store a copy of the blockchain, thus being able to securely enable custom functions such as instant send and private transactions. When making decisions for the future of a network, full nodes are the ones that vote on proposals.

Pruned Full Nodes: The specific characteristic here is that these nodes begin to download blocks from the beginning, and once they reach the set limit, the oldest ones are deleted, retaining only their headers and chain placement.

Archival Full Nodes: These are what most people refer to when they talk about full nodes. These nodes envision a server that hosts the full Blockchain in its database.

Compared to full nodes, Master nodes themselves cannot add blocks to the blockchain. Their only purpose is to keep a record of transactions and validate them. Whether Mining or Staking nodes, they're the ones who write blocks on the blockchain.

Lightweight or Simple Payment Verification (SPV) nodes, on the other hand, are used in day-to-day cryptocurrency operations. These nodes communicate with the blockchain while relying on full nodes to provide them with necessary sets of information. They do not store a copy of the blockchain but only query the current status for the last block. Also, they broadcast transactions to other nodes in the network for processing.

Blockchain Consensus

The set of rules by which a blockchain network operates and validates the information of blocks is known as 'consensus'.

Figure 3.5 Blockchain consensus

Since cryptocurrencies operate on a decentralized P2P network, it won't be wrong to assume that complications are bound to arise when a decision needs to be taken. This is where consensus comes in handy. While consensus must be achieved by a certain type of

nodes, in P2P networks any user can become a full node and thus gain supremacy over others. When at least 51% nodes agree on to something, the decision is validated on behalf of the whole of the blockchain. This 51% rule may result in threats even. The most common threat to a blockchain is the 51% attack, where more than half of nodes are concentrated in one entity. This paves the way for the entity to change consensus rules as it sees fit, which could lead to a monopoly.

Blockchain Proof of Work

A popular consensus mechanism for blockchains, Proof of Work is a requirement through which expensive computations, also called mining, can be performed in order to facilitate transactions on the blockchain. Although it might be hard for nodes to generate a valid block, it is quite easy for the network to validate the block's authenticity. This is achieved through hash functions. Since hashes are quite sensitive to changes and even minute modifications will result in a completely different hash output, they can be used to validate and secure blocks.

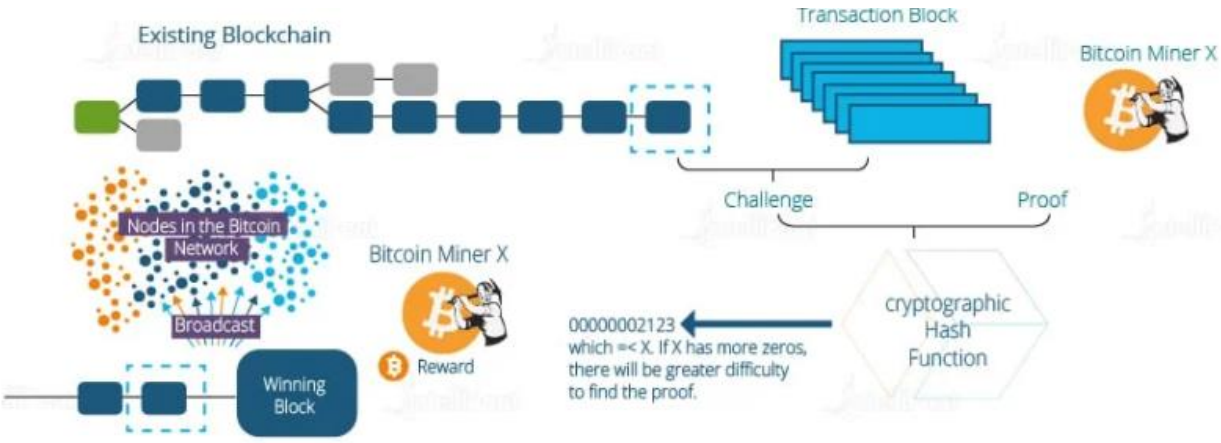


Figure 3.6 Bitcoin mining

For a block to be confirmed as valid, miners are required to generate two hashes: a hash of all the transactions in the block and one proving that they have expended the energy required to generate the block by solving a special cryptographic puzzle with a pre-set level of difficulty. The difficulty of solving the puzzle can be automatically adjusted in **Proof of Work** systems to create a consistent time period for blocks that are to be added to the blockchain. In summary, a miner creates a block of valid transactions. Further, the miner runs a Proof of Work algorithm on it to find a valid hash. When a valid block is generated, the block is added to the blockchain, and the miner receives network fees and the newly created cryptocurrency.

Blockchain Protocols

As blockchains are being rolled out at an exponential rate for everything from cross-border financial transactions to supply chain management, the lack of scalability has remained a constant issue since the genesis of blockchains. As more computers join the P2P network, the efficiency of the whole blockchain ecosystem typically deteriorates. Through the process of sharding, a way of partitioning, blockchain miners can maintain a consistent throughput throughout the network. Blockchain protocols, however, demand constant attention for their efficient functioning.

Table 3.1 Blockchain Protocol Characteristics

Blockchain Protocol Characteristics	Each party maintains its own copy of the information, and all nodes must validate updates collectively.
	The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form.
	Entries are permanent, transparent and searchable, which make it possible for community members to view transaction histories in their entirety.
	Each update is a new block added to the end of a chain. A protocol manages how new edits or entries are initiated, validated, recorded, and distributed.
	Cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole.

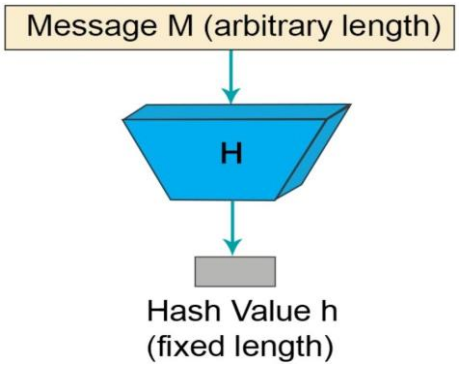
Major blockchain protocols are listed below:

- **Bitcoin:** The first application of blockchains, Bitcoin enables users to perform non-reversible transactions trustlessly. This protocol includes technologies such as hash, digital signature, public-key cryptography, P2P networking, Proof of Work and Proof of Work mining.
- **Ethereum:** Known for smart contracts, Ethereum features a native cryptocurrency, namely Ether, and an Ethereum wallet. This protocol allows users to create decentralized applications and democratic autonomous organizations.
- **Ripple:** Ripple supports tokens that are used to represent fiat, other cryptocurrencies, commodities, or other value units such as mobile minutes and frequent flyer miles.
- **Hyperledger:** Developed by the Linux Foundation in 2015, Hyperledger supports Python, endorsement policies for transactions and confidential channels for private information sharing.

- **Openchain:** A scalable and secure blockchain protocol, Openchain is suitable for organizations that wish to issue and manage their digital assets.
- **IOTA:** Known for its blockless distribution ledger 'Tangle', IOTA enables infinitesimally small payments without charging extra fees.
- **Lisk:** A relatively new blockchain protocol, Lisk allows the development of decentralized applications in pure JavaScript.
- **BigchainDB:** This open-source system starts with a big data distributed database and then adds blockchain characteristics to the network including decentralized control and digital asset transfers.

Blockchain Hashing

Hashing, or a hashing algorithm, is a one-way process that converts your input data of any size into fixed-length enciphered data.



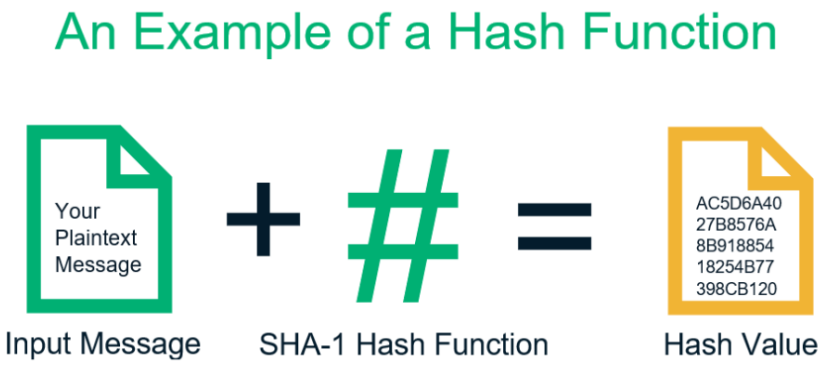


Figure 3.7 Hash message

A hash function is a one-way mapping.

That means that it can take an input (the input is usually a large sequence of bits;

It can be a movie, a song, an e-book, a picture, or any digital data) and produce a fixed-size value as output, often much smaller than the input size.

However, if I change only one bit in this input, the output will be completely different.

hash functions are unidirectional.

output hash is a fixed-length random bit sequence.

hexadecimal format and looks alphanumeric.

Hash Properties

- Fixed length
- Unique
- One-way function
- Eg:- SHA256

Hash – Example -1

SHA 256

Input

from: person1

to: person2

amount: 5000

Hash

A1BA93299F5836B8A58543CAD52B8818F0C95F12991635609B0F7CAAF6388A58

Hash – Example -1

SHA 256

Input

from: person1

to: person2

amount: **5001**

Hash

C677256A3CD1F73CD4476204BCA19050E0A11AB11FAEBF14CD7B37FB696F73C5

Characteristics of Hash Function

- Ensure data integrity.
- Serve as a check-sum
- Hash digest changes completely when any of the email content gets modified after being digitally signed
- Secure against unauthorized modifications.

- The smallest of changes to a message will result in the creation of an entirely new hash value.
- Protect stored passwords
- Websites typically do is hash passwords to generate hash values.
- Operate at different speeds to suit different purposes.
- Different hash functions serve different purposes depending on their design and hash speeds

Popular Hash Functions

Message Digest (MD) – MD5

128-bit hash function.

provide assurance about integrity of transferred file.

Secure Hash Function (SHA)

160-bit hash function

Each block has the following key components: ***data, hash, previous hash and metadata (timestamp, block number).***

- *Data* in a block could be a simple string such as "Blockchain Data Structure" or a list of transactions
- *Hash* is a unique identifier for a block and is analogous to a fingerprint for a human
- *Previous Hash* is the hash value of the previous block in the blockchain
- *Metadata is information about the data; e.g., block number, timestamp, etc.*

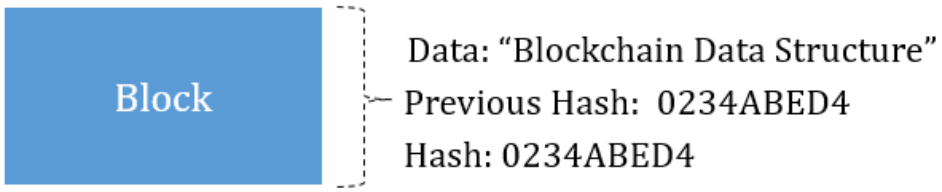


Figure 3.8 Blockchain Data Structure

Hash is calculated by cryptographic algorithms employed in the blockchain. They take a block's data and its previous hash value as input and determine its hash.

Hash = function(data, previous hash, metadata)

A different unique hash value is generated for different combinations of previous hash value and data. The demo available ***here*** [2] allows you to generate hash for different data sets. You will notice that the hash gets completely changed even if there's a little change in inputs; i.e., data and previous hash.

As illustrated below, blocks are cryptographically linked through *hash*; i.e., *hash* of a block is same as the *previous hash* of the block succeeding it in the blockchain. The first block in a blockchain is called "Genesis Block" and its *previous hash* is zero as there is no block preceding it. Matching of a block's *hash* with the *previous hash* value of the next block is mandatory for the blockchain to be considered valid.

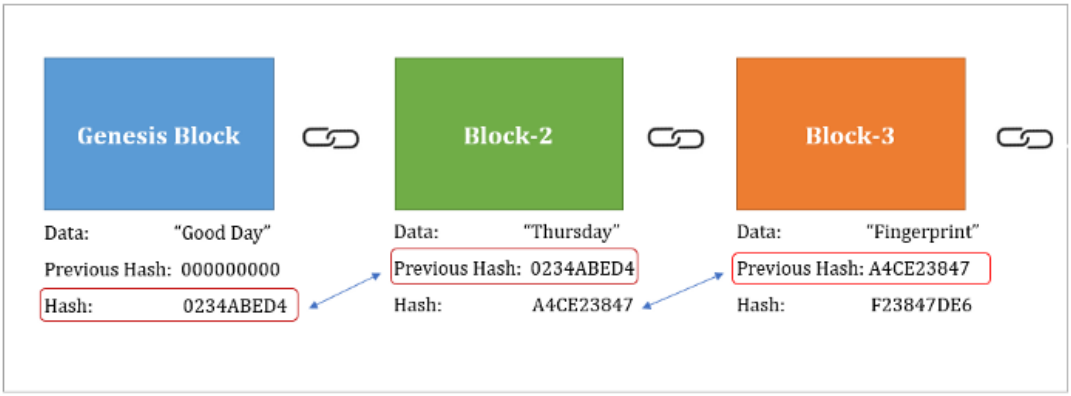


Figure 3.9 Blocks in a blockchain linked cryptographically through hash

Key properties of Secure Hash Algorithms (SHA)

SHA-256 used in Bitcoin is one of the examples of a cryptographic hashing algorithm. SHA-256 always generates a 256-character hash value irrespective of the input data size. Secure hash algorithms used in blockchain should have the following properties:

- Same hash value should always be generated for the same input
- Hash should be calculated from the data, but it shouldn't be possible to derive data from the hash
- Even a slight change in the data should change the hash value completely
- Algorithm should be able to compute the hash quickly

The same input data produces same hash but a single change completely changes the hash. The result returned is the verifiable fingerprint. Bitcoin uses the SHA256 hash function that returns a fixed 256-bit fingerprint.

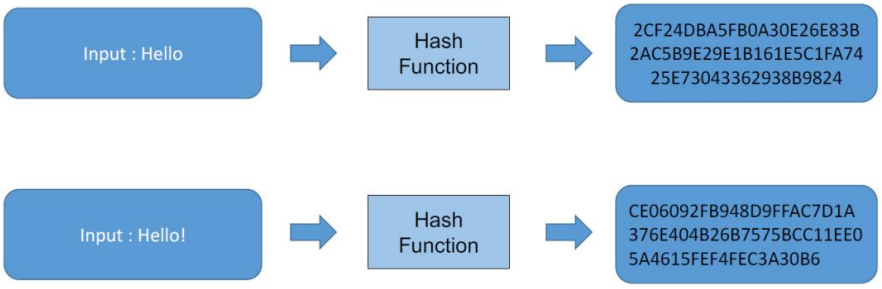


Figure 3.10 Hash messages

Blockchain is called an **immutable ledger** because it stores a record of transactions in blocks which cannot be changed, once created. New blocks can be added to the block chain but data in the existing blocks cannot be changed. If a malicious actor alters the data in a block, the hash of that block gets changed and it does not match with the previous hash value of the next block. The blockchain system realizes this and makes the change in the data invalid.

Data integrity

blockchain is distributed to all the peers in the blockchain network in real-time. Blockchain solution looks for updates constantly and replicates the blockchain that is in majority of the actor's systems in the network.

The immutable nature of blockchain combined with its decentralized framework ensures data integrity because it is extremely difficult to tamper with the data in the entire block chain in majority of the systems in a blockchain within seconds especially when there are numerous entities in the blockchain. The only possibility of a malicious actor being successful in tampering block chain is when that actors has more computational power than the rest of the blockchain network combined. This is called 51% attack.

Use of Cryptographic Hashes

Proof-of-work

- Block contains transactions to be validated and previous hash value.
- Pick a nouce such that H(prev hash, nounce, Tx) < E. E is a variable that the system specifies. Basically, this amounts to finding a hash value who's leading bits are zero. The work required is exponential in the number of zero bits required.
- Verification is easy. But proof-of-work is hard.

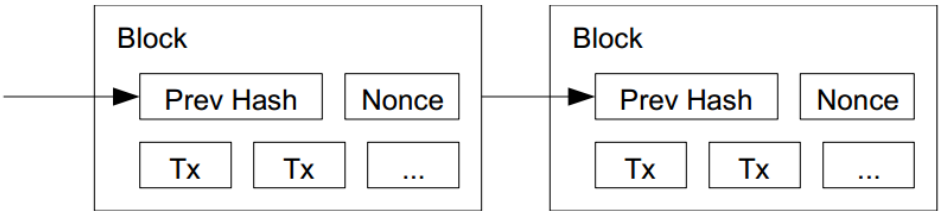


Figure 3.11 Block

Merkle Tree

The concept was patented by Professor Ralph Merkle back in 1979. Now it helps to solve problems in large decentralized networks.

- A Merkle tree is a data structure that is used for secure verification of data in a large

content pool.

- It is also efficient and consistent when it comes to verifying the data.
- Ethereum and Bitcoin both utilize Merkle Trees.

Problem in blockchain :

- Each data is copied among the nodes. So, it is a challenge to efficiently access data.
- The challenge is also to make a copy of the data and share it among nodes. On top of that, the shared data needs to be verified for each of the receiving nodes.

Solution :

- Merkle Trees enable decentralized blockchains to share data, verify them, and make them trustworthy.
- Merkle trees are data structure trees where the non-leaf node is defined as a hash value of its respective child nodes.

The Merkle tree is inverted down where the leaf nodes are the lowest node.

At the core of Merkle trees, we need to learn three important terms. They are as below:

- Merkle Root
- Leaf Nodes
- Non-Leaf Nodes

- It is an upside-down tree
- The tree is capable of summarizing a whole set of transactions by itself. This means that the user can verify if a transaction is part of the block or not.

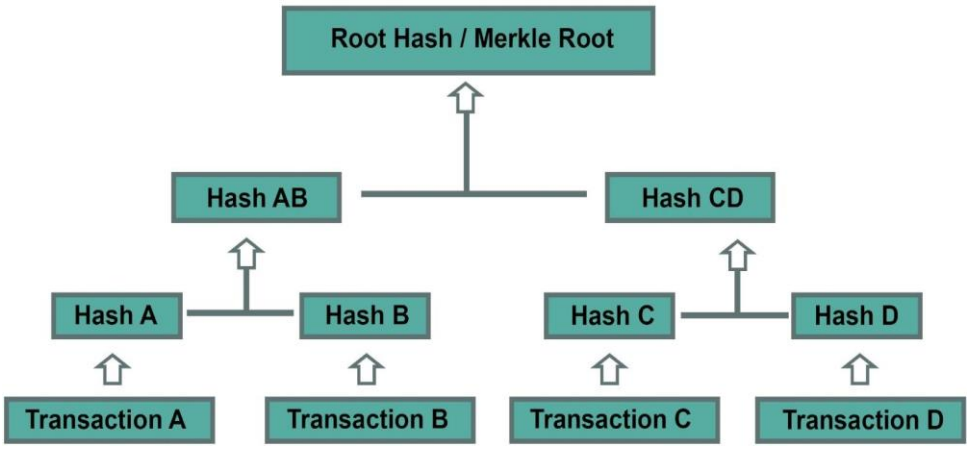


Figure 3.12 Merkle Tree

Merkle tree is a complete data structure in the form of a tree, in the leaf vertices of which there are hashes from data blocks, with the inner vertices containing hashes from

adding values in child vertices. This connects all the elements with information among themselves. In the end, it looks like this.

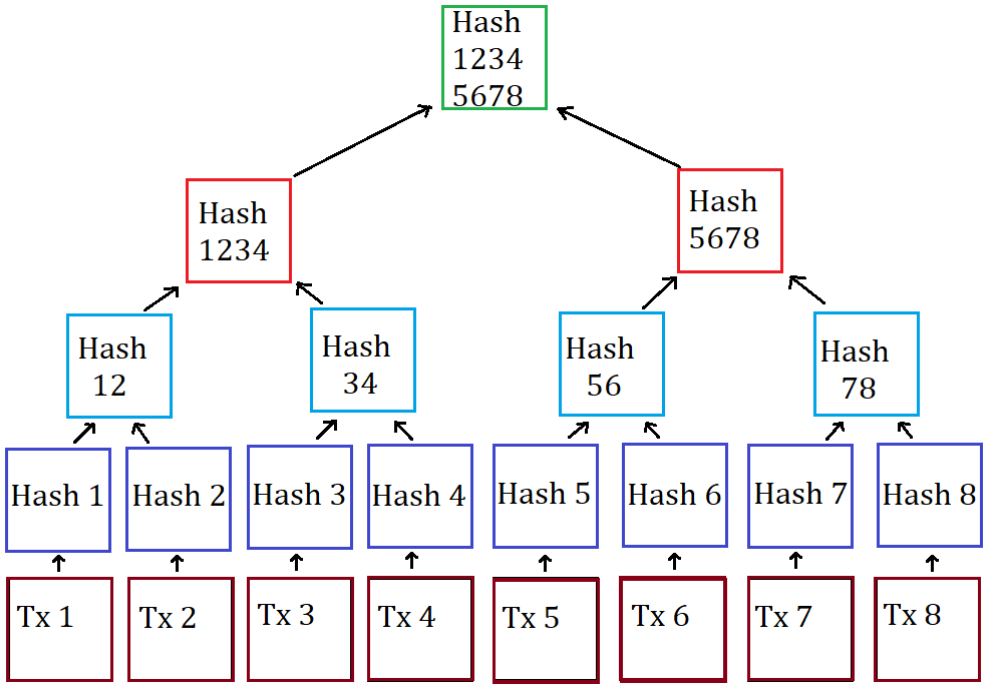


Figure 3.13 Merkle Tree example

A hash is a result of converting a hash function. It is a function that converts an array of input data of arbitrary length into an output string of a specified length in accordance with a specific algorithm.

- To make Merkle trees work, hasing is used. It simply does the hashing pairs of nodes repeatedly until only one hash value is left.
- The left hash value is known as Merkle Root or the Root Hash.
- The tree is created from the bottom up using the individual transactions hashes.
- The individual transaction hashes are also known as Transaction IDs.
- The leaf nodes are the nodes that contain transactional data hashes.
- In the case of the non-leaf nodes, they store the hash of the two previous hashes.
- Another important property of Merkle trees is that it is binary in nature.
- This means that it requires leaf nodes to be even for it works.
- In case, if there is an odd number of leaf nodes, it will simply duplicate the last hash and make it even.

Merkle Tree of odd number of transections

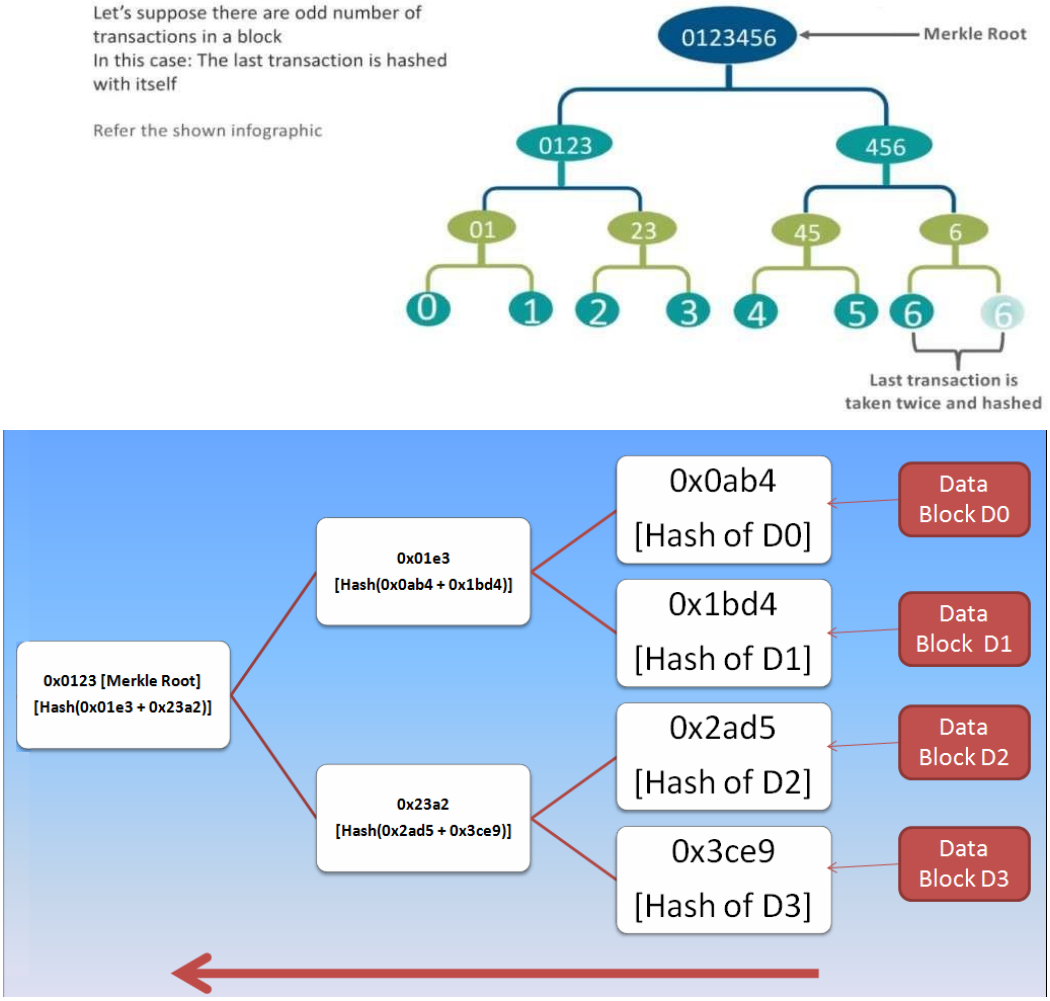


Figure 3.14 : Merkle tree using four data blocks D0, D1, D2, and D3

- It is a data structure tree in which every leaf node labelled with the hash of a data block.
- A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions.
- It allows the user to verify whether a transaction can be included in a block or not.
- Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left.
- This hash is called the Merkle Root, or the Root Hash.
- The Merkle Trees are constructed in a bottom-up approach.
- Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes.
- Merkle trees are in a binary tree, so it requires an even number of leaf nodes.

- If there is an odd number of transactions, the last hash will be duplicated once to create an even number of leaf nodes.

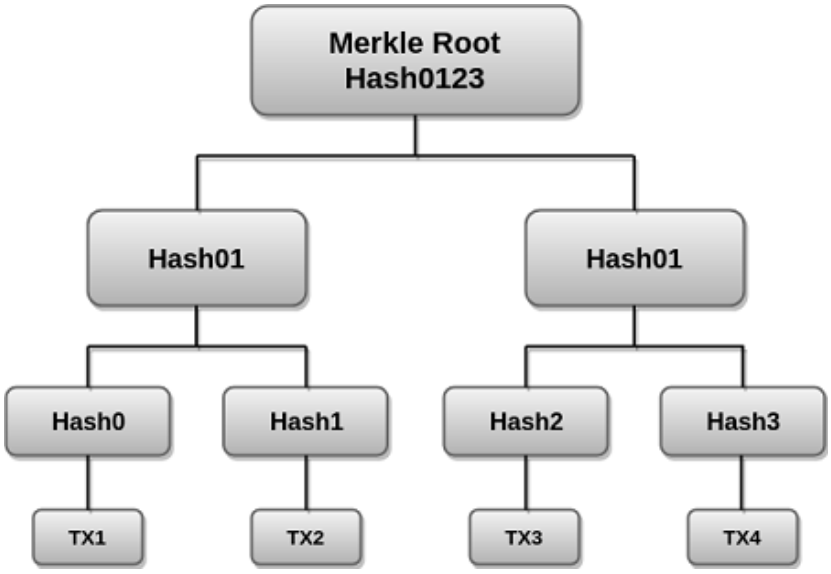


Figure 3.15 : Merkle tree

- Merkle Root is stored in the block header. The block header is the part of the bitcoin block which gets hash in the process of mining.
- It contains the hash of the last block, a Nonce, and the Root Hash of all the transactions in the current block in a Merkle Tree.
- So having the Merkle root in block header makes the transaction tamper-proof.
- As this Root Hash includes the hashes of all the transactions within the block, these transactions may result in saving the disk space.

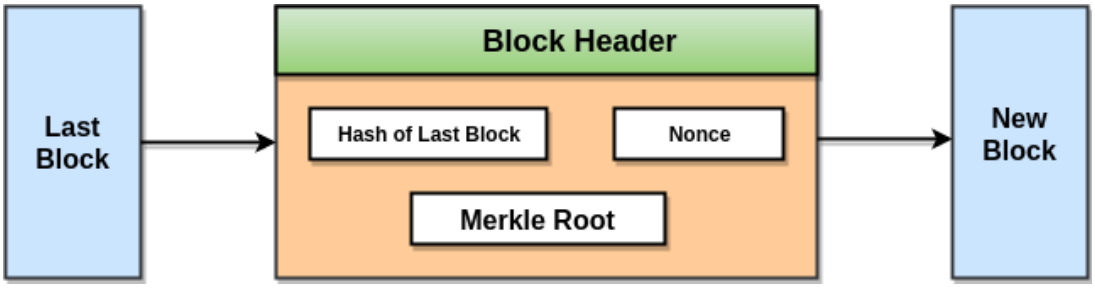


Figure 3.16 : Merkle tree with block

- The Merkle Tree maintains the integrity of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction.

- This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block.
- So everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Merkle trees – benefits

- Validate the integrity of data: It can be effectively used to validate the integrity of the data.
- Takes little disk space: Merkle tree takes little disk space compared to other data structures.
- Tiny information across networks: Merkle trees can be divided into tiny information for verification.
- Efficient verification: The data structure is efficient and takes only a while to verify the integrity of the data.

3.2 Security Considerations for block chain

The followings are the key security features of blockchain

- Identity and access management.
- Key management.
- Data privacy.
- Secure communication.
- Smart contract security.
- Transaction endorsement.

In the Bitcoin network, for instance, the proof of work is used for block validation. Any node in the network can attempt to validate the block through a process called mining. Miners are awarded in cryptocurrency for every successful validation of a new block.

Is blockchain secure?

Blockchains have a heterogeneous architecture made up of cryptographic algorithms and mathematical models. The structure of the blocks plays a crucial role in enabling distributed consensus and ensuring the security of the system.

- Data which may include transaction records, contracts, or even IoT device telemetry.
- Hash value of the current block is generated to serve as a cryptographic image of the block that can be verified by anyone.

- Hash value of the previous block is an encrypted string used to link to the previous block in order to form the chain.
- Timestamp. A record of the time when the block was created.
- Additional information including digital signatures, nonce value, etc.

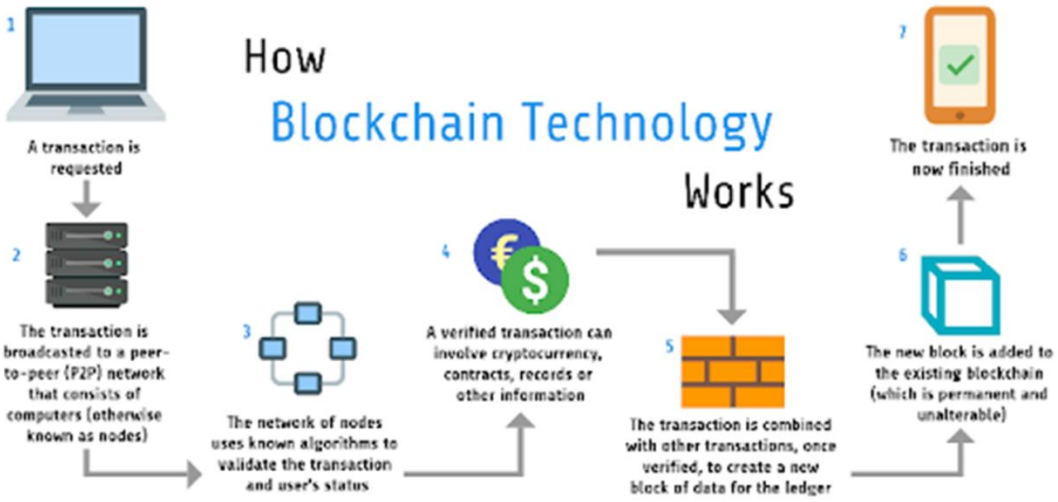


Figure 3.17 : blockchain sample transaction

Survey shows that financial and manufacturing use cases are facing more targeted cyber-attacks. According to an article in Fortune magazine, more than 4 million bitcoins are missing. This number accounts for 17% to 23% of the total cryptocurrency, which worth more than $8,500 each.

Blockchain has some other inherent properties that can provide additional security. Some of the properties of Blockchain technology are:

1. Increased Capacity

   The structure of the linked system of blockchain is more than capable of increasing the capacity of an entire network.

2. Immutability

   It means that once a transaction is done, it is impossible to erase it from the database.

3. Faster Settlements

   banking transactions take time, but blockchain transaction save lot of time.

4. Encryption

   Asymmetric-key algorithm and Hash function encryption.

5. Decentralization: collaborative manner.

‘51% Attacks’

Phishing

- Phishing is one of the most common hacking techniques.
- It can mimic the emails from trusted and reputed sources.
- These emails are sent to the owners of digital wallets, asking them to fill their personal information on the fake links.
- As per a report of Chainalysis, more than $225 million were lost to phishing scams in the first of 2017.

Sybil Attacks

- Sybil attacks involve the use of multiple fake identities.
- In other words, a single party can run a number of nodes at the same time, using fake identities to disrupt the activities of the network by crashing it.

Routing Attack

- The information of blockchains can be intercepted by hackers by compromising ISPs.
- The compromised Internet Service Providers can also be the cause of this type of attack.

Direct Denial of Service

- DDoS attacks are also a major security issue for blockchain applications.
- In this attack, hackers flood the network with false requests consequently increasing the traffic of the network and disrupting legitimate requests or they target applications with the low and slow attacks to make these applications unavailable for its users.

Some of the most common issues

- 51% vulnerability
- Private key security
- Exchange hacks
- Social engineering
- Double spending
- Transaction privacy leakage.

51% vulnerability

- Blockchain’s consensus mechanism has a 51% security vulnerability that can be exposed by malicious attackers in an attempt to control the network.

- PoW - a 51% attack occurs when a single miner or a pool of miners own more than 50% of total hashing power.
- PoS - a 51% attack can be performed by a single miner who owns more than 50% of all the funds.
- a 51% attack would be extremely expensive to undertake.
- Smaller blockchains that have less hashing power are more vulnerable to such attacks.

Private key security (wallet security)

- blockchains today, public and private keys are generated using the elliptical curve digital signature algorithm (ECDSA).
- The public key can be derived from the private key, but not vice-versa.
- While the public key can be shared and used as the address for sending transactions, the private key should always be kept safe, known only to the owner.
- In spite of the blockchains being inherently secure structures, their security is directly related to the private key.
- private key will give an attacker access to one's blockchain wallet.
- Once lost, private keys cannot be recovered.
- If the private key is by any chance stolen by attackers, it will give them full access to the associated blockchain account and the opportunity to initiate transactions
- Since the blockchain is not controlled by any centralized authority, it is difficult to track and recover the lost funds or information.

Exchange hacks

- Exchange is considered as quick investment return.
- For the exchange to work, the users are register their wallets in third party databases.
- It is prone to attacks
- The safest methods of storing cryptocurrency are either using hardware or paper wallets.
- These wallets are so-called cold storage wallets that have minimal exposure to malicious online attacks.
- Solution: perform trading on decentralized exchanges (DEX) as they communicate directly with the cryptocurrency wallet.

Social engineering attack

- Manipulate individuals into uncovering and sharing their private keys, passwords, and other sensitive information that can be used for fraudulent purposes.

- Identity theft - result in significant financial losses.
- Phishing - the attacker impersonates a trustful resource and sends out messages, notifications, and emails requiring the victims to click on malicious links, fill out forms, and give out their sensitive information.
- Scenario involves the attacker using the domain name similar to the legit one.

Social engineering attacks - Solutions

- To avoid falling prey to a phishing scam, make sure to:
- Never share login credentials or private keys.
- Educate yourself and the people around you about common cases of social engineering.
- Never click on the email attachments, links, ads, or websites of unknown origin.
- Use anti-malware software and keep the software applications and operating systems updated.
- Use multi-factor authentication solutions whenever possible.

Double spending attacks

- Double-spending is a situation in which the same digital funds are spent multiple times.
- In the blockchain-based decentralized network, a reliable consensus mechanism has to be put in place to prevent double-spending.
- Bitcoin network, double spending attacks are prevented by evaluating and verifying the authenticity of each transaction using the transaction logs stored in Bitcoin's blockchain protocol.

Transaction privacy leakage

- In public blockchain networks, transactions are open and transparent.
- Their architecture makes every transaction traceable as well.
- Transactions could contain sensitive information about their issuers.
- In some blockchain applications, such as the internet of things or mobile crowdsourcing, transaction privacy leakage is a critical issue.
- Solution : mixing service (cryptocurrency tumbler).

The architecture of Blockchain.

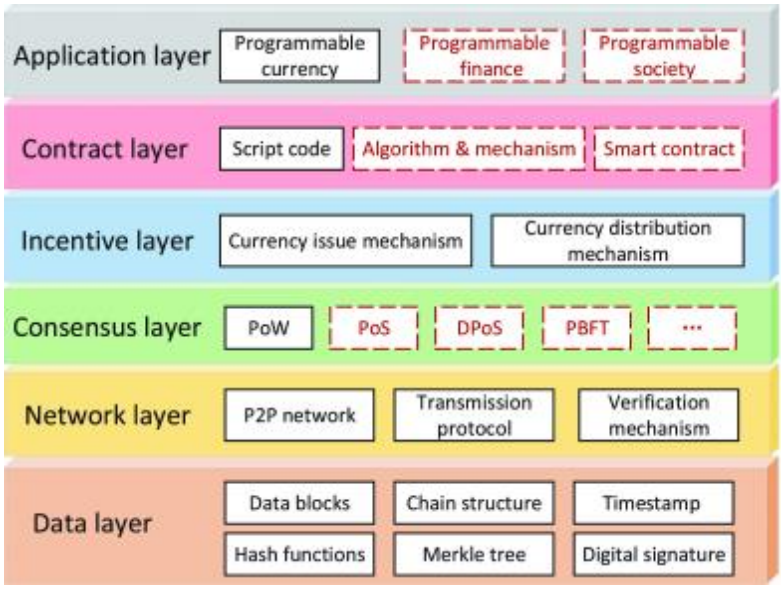


Figure 3.18 The architecture of Blockchain.

Table 3.2 Security and Privacy Requirements, Properties

S&P requirements Supported in bitcoin	S&P properties	Corresponding S&P techniques	Corresponding S&P techniques
	Consistency	Consistency	Consensus algorithms
	Integrity	Tamper-resistance	Hash chained storage
	Availability	Resistance to DDoS attacks	Consensus algorithms with Byzantine fault
	Prevention of double-spending	Resistance to double-spending attacks	Signature and verification
	Anonymity	Pseudonymity	Public key as pseudonyms

Mitigation Methods

- Performing Static Analysis testing (SAST) - analyze the source code to identify security loopholes.
- Performing Dynamic Analysis testing (DAST) eliminate vulnerabilities during software development

- to test for security vulnerabilities in applications in the production environment.
- Performing Interactive Application analysis/testing (IAST) to thoroughly test for hidden inputs, hidden files, and configuration information, etc. in an application running in real-time, in the development process, QA, or in production.
- Performing Software Composition Analysis (SCA) to check for any vulnerable outdated libraries, open-source components, and containers used in the development. You can use thisOWASP dependency-check tool to do this.
- Performing a detailed penetration testing for your Blockchain-based application to test and discover security loopholes and vulnerability exploits using the hacker approach. You can do this by using a variety of open-source tools that are available on the Internet.

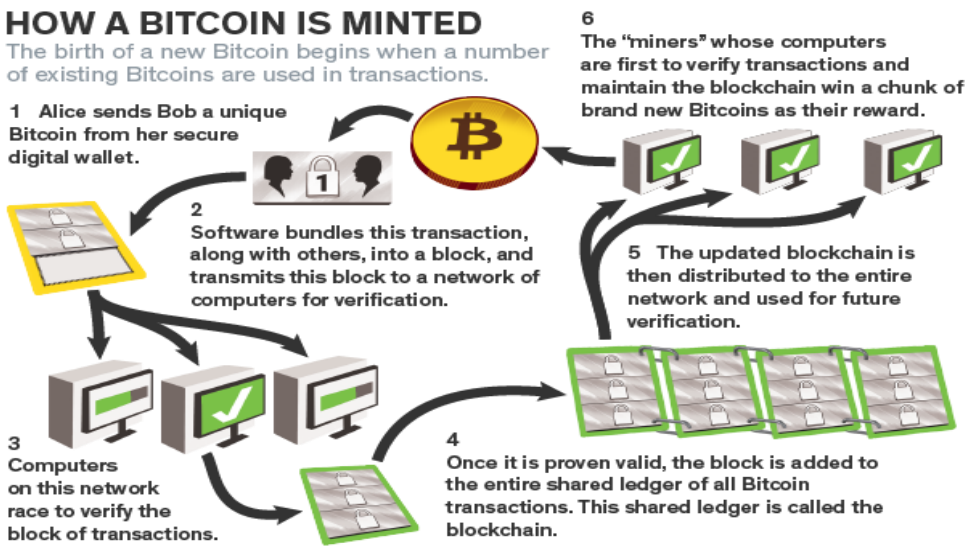


Figure 3.19 bitcoin mining process

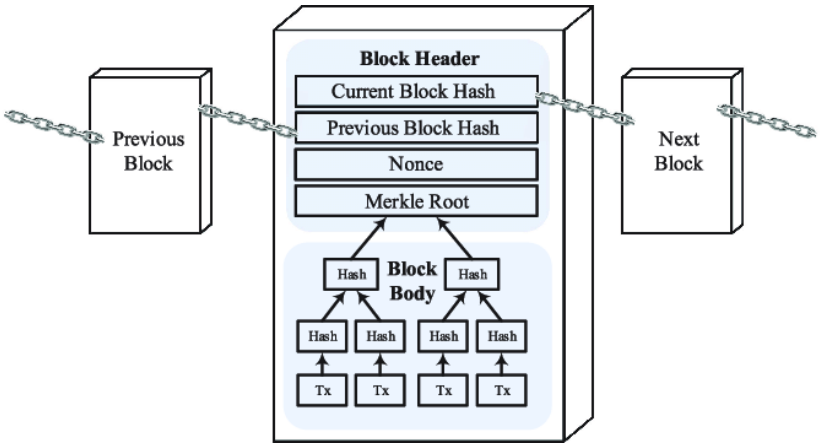


Figure 3.20 Block

3.3 Public Key Cryptography

Public key cryptography uses a pair of a public key and a private key to perform different tasks. Public keys are widely distributed, while private keys are kept secret. Using a person's public key, it is possible to encrypt a message so that only the person with the private key can decrypt and read it. Using a private key, a digital signature can be created so that anyone with the corresponding public key can verify that the message was created by the owner of the private key and was not modified since.

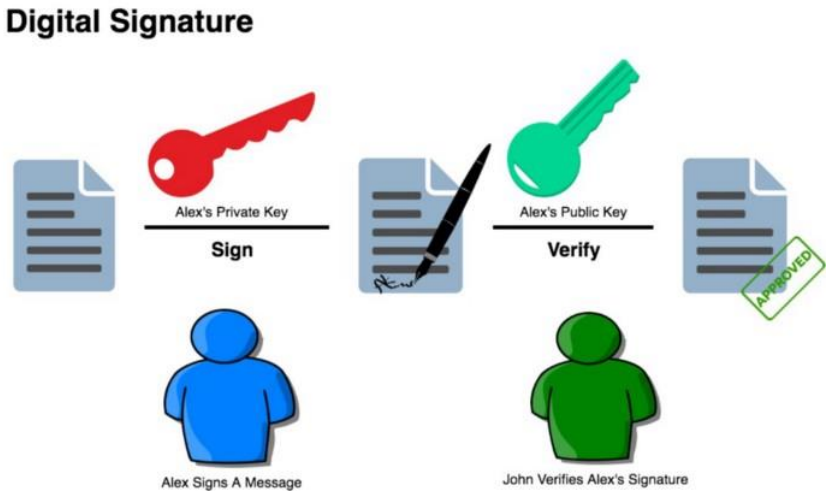


Figure 3.21 Digital signature flow diagram

Public-key algorithms are *asymmetric* algorithms and, therefore, are based on the use of two different keys, instead of just one. In public-key cryptography, the two keys are called the *private key* and the *public key*

Private key: This key must be know *only* by its owner.

Public key: This key is known to everyone (it is *public*)

Relation between both keys: What one key encrypts, the other one decrypts, and vice versa. That means that if you encrypt something with my public key (which you would know, because it's public :-), I would need my private key to decrypt the message.

A secure conversation using public-key cryptography

- In a basic secure conversation using public-key cryptography, the sender encrypts the message using the receiver's *public* key.
- Remember that this key is known to everyone. The encrypted message is sent to the receiving end, who will decrypt the message with his *private* key.

- Only the receiver can decrypt the message because no one else has the private key. Also, notice how the encryption algorithm is the same at both ends: what is encrypted with one key is decrypted with the other key using the same algorithm.

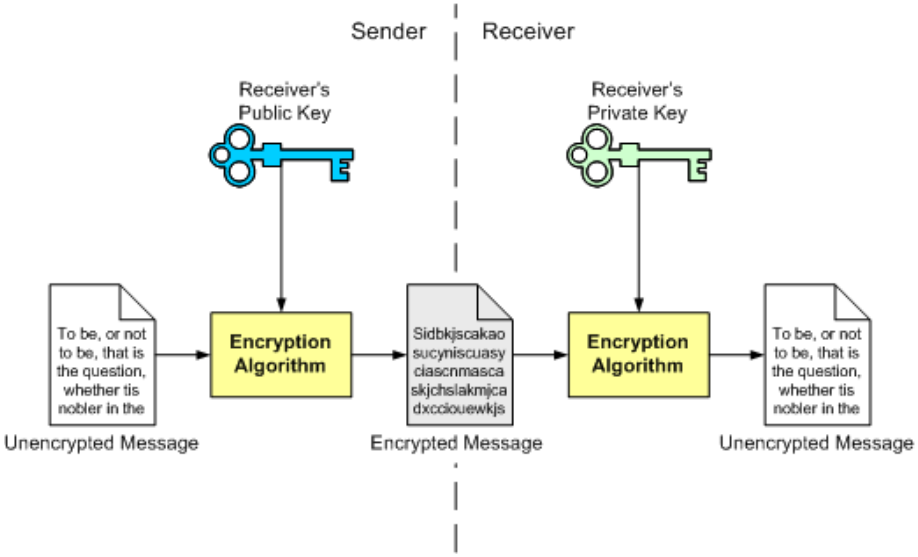


Figure 3.21 secure conversation using public-key cryptography

Pros and Cons of public-key systems

- Public-key systems have a clear advantage over symmetric algorithms: there is no need to agree on a common key for both the sender and the receiver.
- As seen in the previous example, if someone wants to receive an encrypted message, the sender only needs to know the receiver's public key (which the receiver will provide; publishing the *public* key in no way compromises the secure transmission).
- As long as the receiver keeps the private key secret, no one but the receiver will be able to decrypt the messages encrypted with the corresponding public key.
- This is due to the fact that, in public-key systems, it is relatively easy to compute the public key from the private key, but *very hard* to compute the private key from the public key (which is the one everyone knows).
- In fact, some algorithms need several *months* (and even years) of constant computation to obtain the private key from the public key.

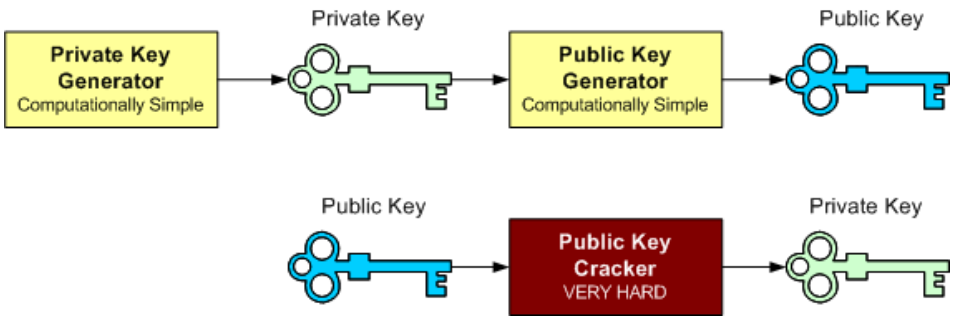


Figure 3.22 public-key cryptography

Another important advantage is that, unlike symmetric algorithms, public-key systems can guarantee integrity and authentication, not only privacy. The basic communication seen above only guarantees privacy. We will shortly see how integrity and authentication fit into public-key systems. The main disadvantage of using public-key systems is that they are not as fast as symmetric algorithms.

Digital signatures: Integrity in public-key systems

Integrity is guaranteed in public-key systems by using *digital signatures*.

A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation (e.g. through the intervention of a malicious user)

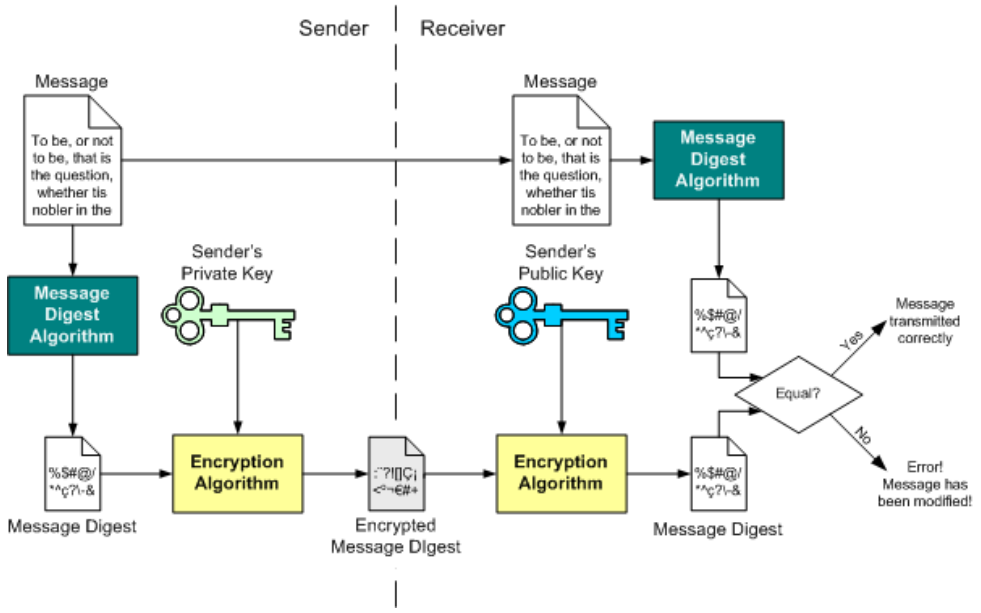


Figure 3.23 Digital signature for a message

The digital signature for a message is generated in two steps:

A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: (1) It is always smaller than the message itself

and (2) Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.

The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*. The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:

Using the sender's public key, decrypts the digital signature to obtain the message digest generated by the sender. Uses the same message digest algorithm used by the sender to generate a message digest of the received message. Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver). If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

Using public-key cryptography in this manner ensures integrity, because we have a way of knowing if the message we received is exactly what was sent by the sender. However, notice how the above example guarantees *only* integrity. The message itself is sent unencrypted. This is not necessarily a bad thing: in some cases we might not be interested in keeping the data private, we simply want to make sure it isn't tampered with. To add privacy to this conversation, we would simply need to encrypt the message as explained in the first diagram.

Authentication in public-key systems

The above example does guarantee, to a certain extent, the authenticity of the sender. Since *only* the sender's public key can decrypt the digital signature (encrypted with the sender's *private* key). However, the only thing this guarantees is that whoever sent the message has the private key corresponding to the public key we used to decrypt the digital signature. Although this public key might have been advertised as belonging to the sender, how can we be absolutely certain? Maybe the sender isn't really who he claims to be, but just someone impersonating the sender. Some security scenarios might consider that the 'weak authentication' shown in the previous example is sufficient. However, other scenarios might require that there is absolutely no doubt about a user's identity. This is achieved with *digital certificates*, which are explained in the next page.

3.4 Nash Equilibriums evolutionary stable strategies,and Pareto efficiency (game theory)

Evolutionary game theory (EGT) is the application of game theory to evolving populations in biology. It defines a framework of contests, strategies, and analytics into which Darwinian competition can be modelled. The mathematical criteria that can be used to predict the results of competing strategies.

What are market structures?

Figure 3.24 Market structure

- The organization and fundamental characteristics of any market are called market structure.
- The market structures are differentiated based on many factors like a number of producers, control over prices and barriers to entry. Based on these factors, there are four different kinds of market structures:

Based on these factors, there are four different kinds of market structures:

- Perfect Competition.
- Monopoly.
- Monopolistic Competition.
- Oligopoly.

Perfect Competition

- Perfect competition is a market place where it is easy for anyone to get into the market and individual sellers don't have any power over the price of the product.
- Think of mangoes. It is easy for anyone to get into the market, all that anyone has to do is to grow mangoes.
- Plus, they can't willingly change the price of the mangoes. If one person sells a mango for $10 then the buyer can simply buy it from someone who is selling mangoes for $5.

Monopoly

- A monopoly is the polar opposite of a perfect competition.
- This is a market place which is dominated by one corporation and the barriers to entry are so high that nobody else can enter it.
- De beers diamonds are a great example of a monopolistic market.

Monopolistic Competition

- This is a marketplace which has a lot of sellers and very low barriers. Their products are similar but not really identical.
- Think of the pizza delivery service. Now, dominoes and pizza hut have the same product with subtle differences.
- Obviously one can slightly price their product a little higher based on factors like customer preferences. However, if dominoes price their pizzas way too high, then people will simply go over to pizza hut.
- Consequently, if dominoes and pizza hut both start overcharging, since the barriers to entry is so low, another player can come in and take all the customers.

Oligopoly

- Oligopolies are market places which are dominated by a few markets and the barriers to entry are high.
- One of the best examples of an oligopoly is the smartphone market. The market is dominated by few number of companies like Samsung, Apple, and Huawei. Much like monopolistic competitions, the products are similar but not identical.
- If tomorrow, Apple decides to price their iPhones at $4000, apart from the Apple fanatics, most will simply opt for an Android phone.
- Obviously, they can always get together and decide as a group to mutually increase the prices, but this is called “collusion” and is illegal in many countries, including the United States.
- So, when they can’t compete by changing prices, how can they get that edge over their competitors? They do so by “non-price competition”, which means competing without changing the price.
- How do they do that? They do so by changing the look and style of their products and giving a unique experience. However, the most recognizable form of non-price competition is advertising.
- Advertising is one of the most effective ways of showing unique qualities of your products and to introduce new products.

- But then again, there is a problem. How many of the advertisements do you watch actually stick? Chances are that you have been bombarded by tons of ads today itself, how many of them do you actually remember? If you are a player in an oligopoly and you keep blindly advertising, you are going to be spending a lot of money.
- As a result of that, in order to make up all that money, you are going to invariably have to increase the price of your products.
- If that happens, your buyers are simply going to go to your competitors. So how do you go about this? How do you advertise your products without losing out on your customers?
- You will have to basically take decisions based on the actions that your competitors will take. In order to do that, you will have to use **Game Theory.**

What is the Game theory?

Game theory is the study of strategic decision making. This is how many corporations make decisions while keeping in mind the actions that their competitors will take. Game theory was devised by John Van Nuemann and Osker Morgenstern in 1944 and was considered a breakthrough in the study of oligopoly markets. Since then the game theory has found a life of its own and has seen widespread implementations in various other technologies and fields.

A game theory model has at least 3 components:

Players: The decision makers. Eg. The managers in the firms.

Strategies: The decisions they want to take to further their companies.

Payoff: Outcome of the strategies.

In game theory, there are two types of games.

Zero sum game: It is a game in which the gain of one player comes at the expense of another player.

Non zero sum game: A game where the gain of one player doesn't come at the expense of another player. So, how does one apply game theory? Let's go back to what we were discussing again, should or shouldn't a company advertise a particular aspect of their product. Suppose there are two firms A and B.

Table 3.3 Pay-off matrix

		Firm B	
		Advertise	Don't Advertise
Firm A	Advertise	(4, 3)	(5, 1)
	Don't Advertise	(2, 5)	(3, 2)

The table that you see above is called a "payoff matrix". The table basically reads like this:

If Firm A and B both decide to advertise then the payoff for both of them is 4 and three respectively.

If Firm A doesn't advertise and B decides to advertise, then the payoff is 2 and 5.

If Firm A advertises and B doesn't advertise then the payoff is 5 and 1.

If both Firms A and B don't advertise then the payoff is 3 and 2.

Firstly, let's look at Firm B.

Case 1: If Firm A advertises

Then Firm B has a payoff of 3 if they advertise and one they don't advertise. So, obviously, their best payoff lies in advertising.

Case 2: If Firm A doesn't advertise

Then Firm B has a payoff of 5 if they advertise and 2 if they don't advertise. In this case their best payoff lies in advertising.

Conclusion: Regardless of what Firm A does, Firm B should advertise.

Now, let's look at Firm A.

Case 1: If Firm B advertises

The Firm A has a payoff of 4 if they advertise and 2 if they don't advertise. So, once again, their best payoff lies in advertising.

Case 2: If Firm B doesn't advertise

In this case, Firm A has a payoff of 5 if they advertise and a payoff of 3 if they don't advertise. Once again, their best payoff lies in advertising.

Conclusion: Regardless of what Firm B does, Firm A's best strategy lies in advertising.

So, in this example, for both Firm A and Firm B, their most stable state will be if they both advertise, which is: For both Firm A and Firm B, this is their dominant strategy. A dominant strategy is the best course of action for a player regardless of what the opponent does. In this example, (4,3) is also the Nash Equilibrium.

Nash Equilibrium

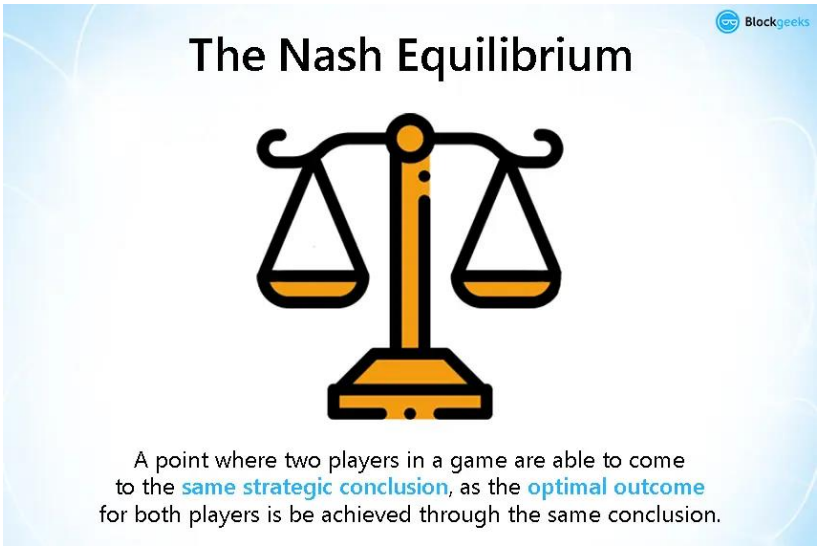


Figure 3.25 Nash Equilibrium

- The Nash equilibrium is a solution to a game where each player chooses their optimal strategy given the strategy was chosen by the other and they have nothing to gain by shifting their strategy.
- This was formulated by John F Nash who was portrayed by Russell Crowe in the movie, “A Beautiful Mind”.
- This has humongous implications in a distributed computer system like the blockchain. In fact, the blockchain is “cheat-free” because the entire protocol is in a Nash Equilibrium.

Blockchain and Cryptocurrency Game Theory

A block is a series of blocks which contains individual transactions in it. Each block also contains the hash of the previous block and this, in turn, links each subsequent block to the previous block making a chain. Hence the term, “blockchain.” This is a rough visual representation of a blockchain.

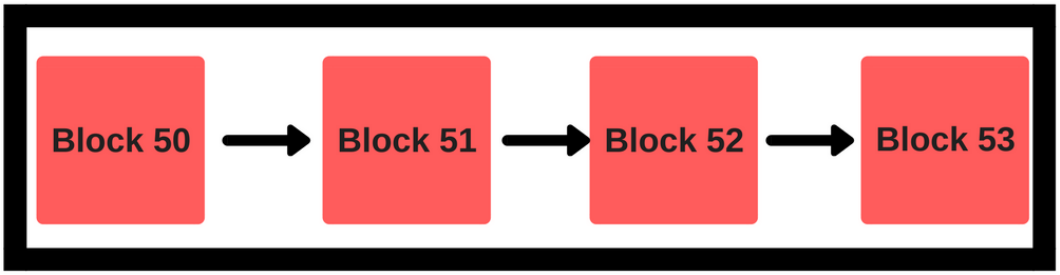


Figure 3.25 Chain of blocks

Some terms:

- Genesis block: The first block of the blockchain is called a “genesis” block.
- Proof of work: The amount of computational work required to create the block.
- Parent block: The block that immediately precedes a block is the parent block of that block. So in the diagram above, Block 50 is the parent block of Block 51.
- Every block in the blockchain has a scoring function.
- Score(genesis) = 0.
- Score(Block) = Score (parent block) + Proof of work
- The current state of the chain is the block with the highest score.
- In a system based on blockchain bitcoin there are two players:
- Users.
- Miners.

Users, in bitcoin, have only two functions available to them:

- Send coins.
- Receive coins.
- In order to do that they need two keys, the public, and the private key.
- What miners do is that they authenticate the transactions AND they do the process of mining.
- Mining is how new blocks are discovered and added to the blockchain.

Block Mining

- Through a series of computations, miners find a block and add it to the blockchain.In Ethereum, adding the block gives the miner(s) a reward of 5 ether and In bitcoin, the mining reward is 25 BTC (both as of writing).

- Miners have a lot of power in the blockchain system and if they do choose to cheat for their own personal gain, they can cause havoc in the system.
- To mitigate that, the blockchain uses game theory mechanics to keep the system bulletproof.
- In order to understand how game theory keeps the miners honest, let's take a look at another peer-to-peer system which has allowed its users to, time and again, get away with cheating.
- Torrenting is one most popular peer to peer systems in the world.
- While using torrents, users have two roles: downloading and seeding.
- After downloading a file, they are supposed to share it the network via a method called seeding.
- However, they get no compensation for seeding the said file and hence more often than not they refuse to do so.
- Most torrent users are "cheats" because they do not seed their files.
- They can get away with cheating because the system doesn't have a "punishment model" the way blockchain does.

How can miners cheat? – Cryptocurrency Game Theory

- They can include an invalid transaction and give themselves extra coins.
- Add blocks randomly without worrying about Proof of work.
- Mine on top of invalid blocks to get more BTC.
- Mine on top of a sub-optimally scoring block.
- Let's take an example. Consider the block below:

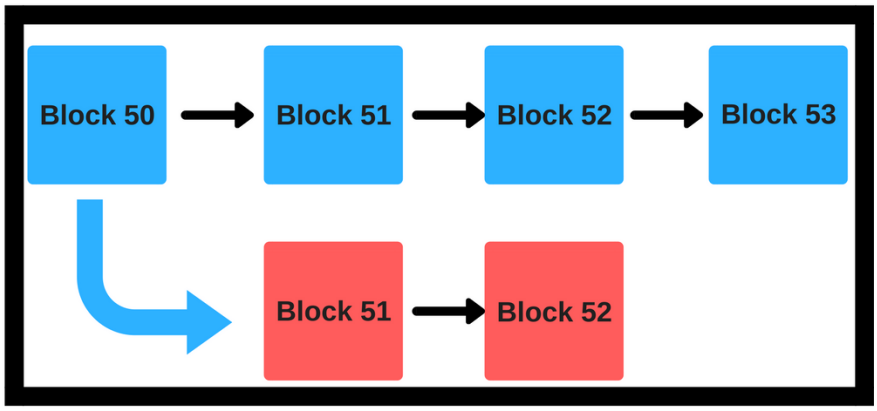


Figure 3.26 Forking of chain

- The blocks in blue are the main chain. Now suppose there is a miner who, in blue block 51, spends 20 bitcoins to get 500 litecoins (hypothetically).
- And now he wants to create a parallel chain with a new block 51 (red), where in he never did this transaction. So, to simplify what he just did, let's do a quick recap:
- In blue block 51 spends 20 bitcoins to get 500 litecoins.
- Creates a new chain (fork) from block 50 and in the alternate block 51, he doesn't do the litecoin transaction.
- In the end, he comes out with his original 20 BTC and 500 new litecoins.
- What just happened here is called "double spending." Obviously now miners can, theoretically, mine on top of the new red chain and keep double spending and mining extra bitcoins.
- As you can imagine, this can destroy the bitcoin system.
- The blockchain was designed in a way that it is a self-enforcing Nash Equilibrium. The reason why that happens is that mining has a recursive punishment system.

The Nash Equilibrium in mining and the punishment system.

- If a miner creates an invalid block then others won't mine on top of it because of a rule that has been defined in blockchain mechanics.
- Any block that is mined on top of an invalid block becomes an invalid block.
- Using this rule, miners will simply ignore the invalid block and keep on mining on top of the main chain aka the blue chain in the diagram.
- This similar logic stands for sub-optimally scoring block. Look at the diagram again.
- No miner will want to mine on Red Block 52 because the Blue Block 53 will have a higher score than the red block.
- Both of these scenarios get mitigated because miners., as a group will choose the most stable state aka the state with a Nash Equilibrium.
- Obviously, you can make all the miners mine on the red block and make it the new blockchain.
- As the co-ordination game states, if a majority of the people in the group are not changing their state, the minority will not have any incentive to stay in the new state.
- Seeing this, why will a miner spend all their computation power and risk ostracization in a futile cause?

Why will users use the main chain instead of the other chain?

So, now that we have seen the reason WHY miners will prefer the blue chain…What about the users? In the blockchain game, there are two players, miners, and users. Why will users prefer the blue chain over the red chain? Once again, game theory mechanics come into play. The first thing that you need to keep in mind is that cryptocurrency has value is because the people give it value. So, why will a normal user assign a value to coins coming out of the blue chain and not to the coins coming out of the red chain? The reason is simple. The main chain is a Schelling point from the users perspective. They give it value because the main chain seems natural and special to them.

Bounded Rationality: Another reason why users will value the main chain more is that they are simply used to it. Like bounded rationality states, people will simply opt for the simplest solution every time. Moving through a newer chain needlessly complicates things.

- Vitalik Buterin gave a great example of the Takeover problem and we are going to expand on it. Suppose, someone makes a hypothetical smart contract for an activity. The terms of the contract go like this:
- Any miner can join the activity by sending a very large deposit into the contract.
- The miners must send shares of the partially completed blocks that they have mined into the contract and the contract verifies it and also verifies that you are a miner and that you have sufficient hash power.
- Before 60% of the miners in the system join you can leave anytime you want.
- After 60% of the miners join, you will be bound to the contract until the 20 blocks have been added to the hard fork chain aka the red chain.
- Yes, it is indeed very diabolical and you can see the problem that this attack can have.
- Not only will the new chain grow bigger and longer, since 60% of the entire miners are bound contractually to this new chain this will quickly make the original older chain aka the blue chain irrelevant. This will make double spends all over the place and the value of the currency will fall fast.

Now, you might be asking why miners will join in a takeover?

- **Well, let's see their incentive for joining:**
- The possible reward at the end.

- No risk of joining on their part.
- **What is their incentive to follow through with the contract?**
- The huge amount they have deposited in the beginning.
- Once again, the possibility of a great reward.
- Theoretically, a takeover like this can end any currency, but this is not that likely to happen because of…You guessed it…. game theory mechanics.

Longest Chain Rule

- A blockchain is a list of blocks linked by hash values with each block containing a batch of ordered transactions.
- To make all participants agree on the same chain of blocks, NC leverages two components: the Proof-of-Work (PoW) mechanism and the longest chain rule (LCR).
- Each participant collects valid and unconfirmed transactions from the network, orders and packs these transactions into a block.

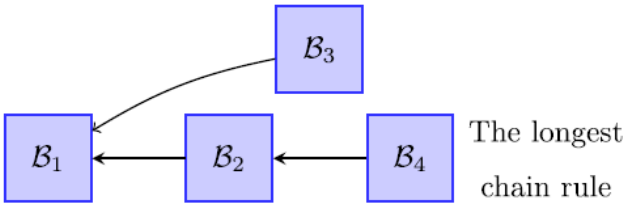
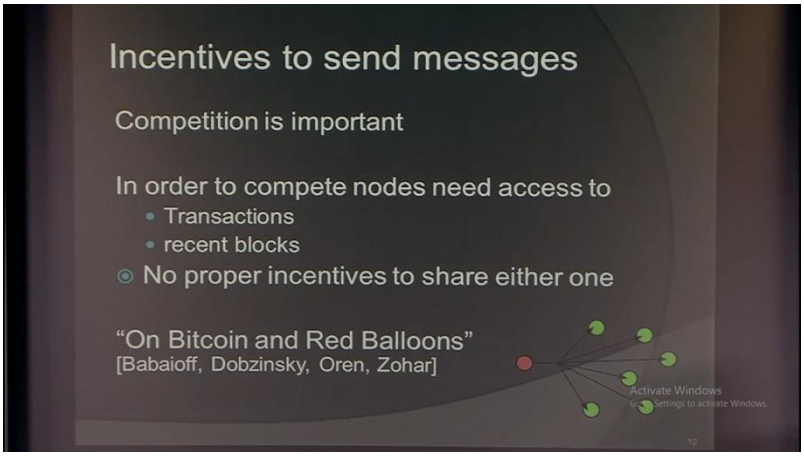


Figure 3.26 Longest chain rule

- In addition, a valid block needs to contain a proof of work, i.e., its owner needs to find a value of the nonce (i.e., a changeable data field) such that the hash value of this block has required leading zeros.
- The length of leading zeros is also known as the mining difficulty, which can be tuned by the system so that new blocks are mined every ten minutes on average.
- In reality, two new blocks might be mined around the same time, leading to a fork in which two ‘‘child’’ blocks share a common ‘‘parent’’ block.
- To resolve such a fork, an honest miner always accepts the longest chain as the valid one. See Fig. 1 for an illustration. Block B3 is a forking block, which will be abandoned by the honest miners according to the longest chain rule.

- In Bitcoin, a block miner will receive a block reward (if its block is eventually included in the longest chain) as well as transaction fees as another type of reward.
- In Bitcoin, the mining of blocks has two functionalities: (1) electing leaders (i.e., the owners of valid blocks) by miners, and (2) ordering and verifying transactions.
- Transaction fee is used to incentivize miners to include transactions in their blocks.
- Therefore, the higher the transaction fee is, the more miners try to include the transaction into the latest block.
- The results show that about 77.8% transactions have a quite small fee (less than 0.0001 BTC).

3.5 Incentive Structure



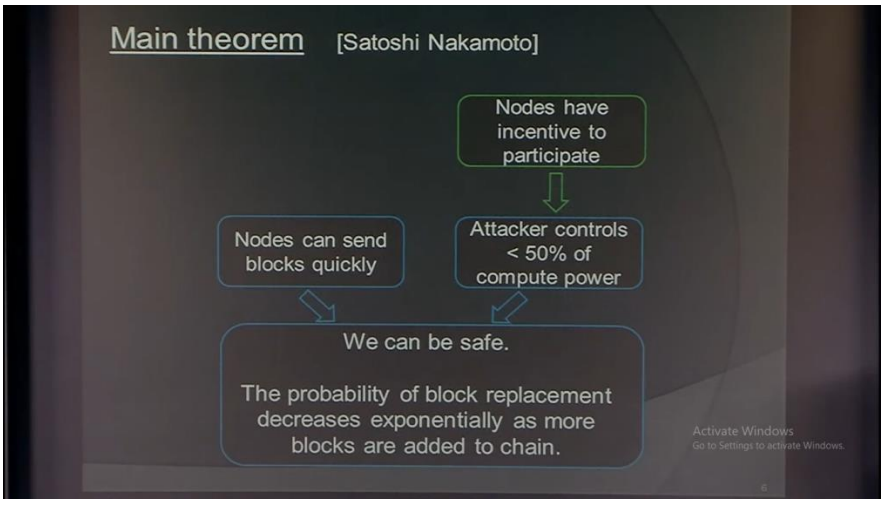
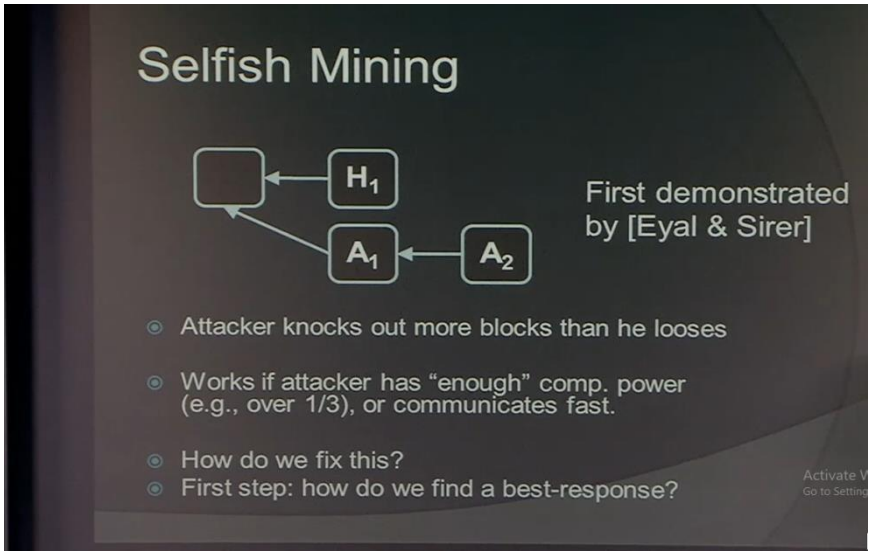


Figure 3.27 Blockchain incentive structure

Selfish Mining

- NC is designed to fairly reward miners according to their contributions to the system (i.e., miners' revenue is proportional to their devoted computation power).
- the studies show that a selfish miner can gain more revenue than its fair share by deviating from the protocol.
- This mining attack is called selfish mining. In this attack, a selfish miner can keep its newly generated blocks secret, mine on top of these blocks, and create forks on purpose when necessary.
- In particular, when some honest miner generates a new block, a selfish miner will publish one secret block to match this honest block as a competition or publish two blocks to override this honest block because honest miners follow LCR.



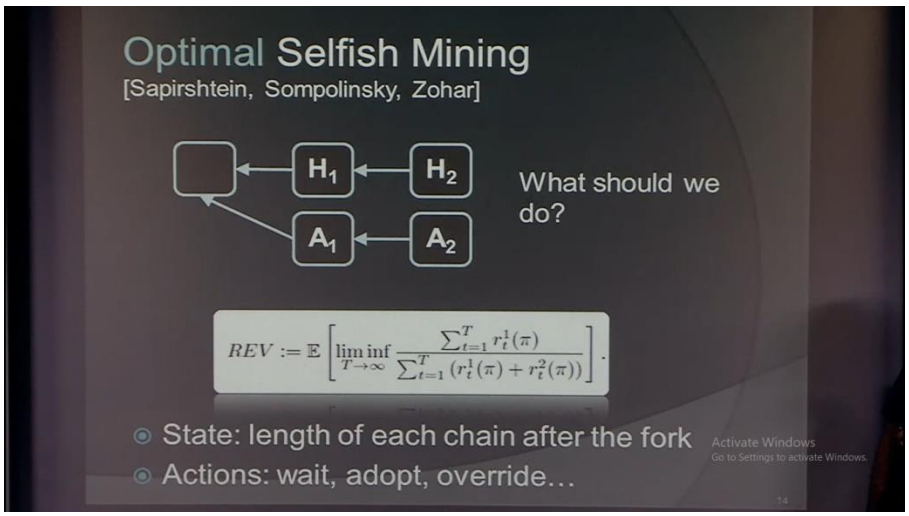


Figure 3.28 Selfish Mining

Forks

- The Nakamoto consensus does not guarantee that the blockchains of all miners are the same at all points in time.
- Thus, some conflicting chains may form, known as forks.
- When a fork occurs, these blocks are usually created by different creators, and these creators are in competition; thus, only the creator in the longest chain can win the reward.
- In the Nakamoto consensus, miners only admit the blocks in the longest chain, and the transactions in other forks are invalid.
- In addition, when the longest chains are not unique, miners usually follow the highest block they received first.

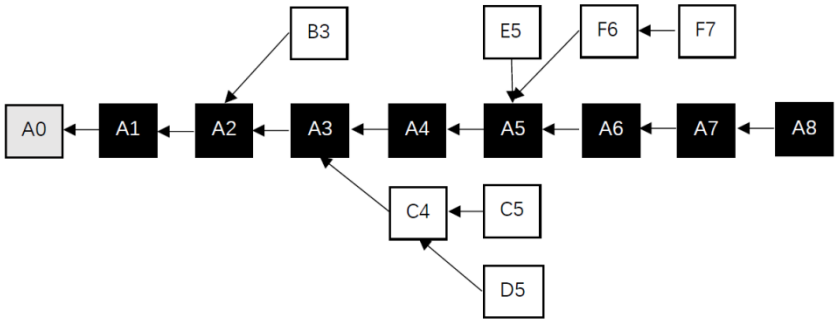


Figure 3.29 Block is added into the chain of network

The above figure shows an example of a blockchain with the Nakamoto consensus. In this example, the longest chain is from the genesis block (A0) to the black leaf block (A8), and other blocks in shorter forks are colored white. In this example, the miners follow block (A8).

Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Tie breaking

- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

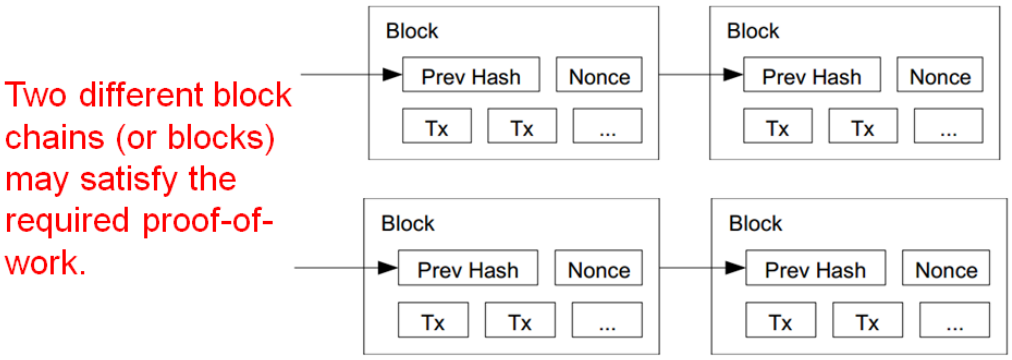


Figure 3.30 blocks

3.6 Blockchain Security Mitigation Methods

Blockchain technology enforces distributed consensus and cryptographic transactions. It is very difficult to compromise the integrity of its records without being noticed by an entire network. Because of blockchain's ability to facilitate decentralized, trustless, encrypted transactions, and events to be recorded and stored publicly. Therefore, it can prevent online frauds such as double spending and hacking.

Maliciousness on the Internet encompasses identity theft, fraud, and network or system intrusions.

Figure 3.31 blockchain security threats

Maliciousness on the Internet encompasses identity theft, fraud, and network or system intrusions. Blockchain can help in preventing frauds involving assets other than currency and credit. Smart contracts used to ensure transacting parties comply with contracts, reducing defaults by buyers or poor service by providers. blockchain technology can prevent several types of malicious attacks and reduce many associated risks, it cannot eliminate all attacks.

Blockchain technology: unavoidable attacks

The 51% Attack

- Occur when a single minor node that is having more computational resources than the rest of the network nodes.
- In such a situation, this node dominates the verification and approval of transactions and controls the content of a blockchain.
- As it possesses more than half (51%) of the network's processing power, the dominant node can outpace all other nodes.
- Thus, it can manipulate the blockchain, insert fraudulent transactions, double-spend funds, or even steal an asset from others.

Identity Theft

- Although blockchain can preserve anonymity and privacy, the security of assets depends on safety of the private key, a form of digital identity.
- If one's private key is acquired or stolen, no third party can recover it.

Illegal Activities

- Blockchain technology can become a venue for illegality.

- Crypto-currency that uses blockchain technology may also facilitate money laundering.

Using Detection Technologies

- blockchain technology prevents fraudulent behavior, it is not able to detect fraud by itself.
- Implementing innovative techniques and methods that are needed to detect attacks.
- Use of machine learning and data-mining algorithms for creating new applications for detecting fraud and intrusions in blockchain-based transactions.
- Implementation of techniques such as profiling, monitoring, and detecting behavioral patterns based on people's transaction histories.
- Development of supervised machine learning approaches that can help in detecting outlier behaviors.

Establishing Identity In Blockchain Technology

- Loss of a key is equal to the loss of identity on the network.
- Solution : building an identity and reputation system using a blockchain that can record "fingerprint" events.
- This can also track life events such as the opening of bank accounts, car purchases, etc.
- It is difficult to steal because it is unforgetable, publicly monitored, and time-stamped.

Mitigating Denial-of-Service (DDoS) Attacks

- A distributed denial-of-service attack occurs when a network is intentionally flooded with unsustainable amounts of traffic or specific information that triggers a crash.
- These attacks are typically not aimed at acquiring personal information or holding a system for ransom
- Attackers generally unleash such attacks simply to claim credit for the mayhem.
- The IoT is a primary reason why DDoS attacks were up 91% last year.
- BlockArmor – Leveraging blockchain technology to increase network size and make DDoS attacks more difficult.

The CIA security triad model, composed of three areas;

(1) Confidentiality,

(2) Integrity

(3) Availability

- Authentication, Authorization and Audit (AAA), and Non Repudiation, fundamental security aspects for protecting information and designing / managing new systems and networks

Confidentiality

The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

- Network Access
- Data Access & Disclosure

Integrity

Integrity is defined as the "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

Immutability

- The combination of sequential hashing and cryptography along with its decentralized structure makes it very challenging for any party to tamper with it in contrast to a standard database
- Right to be Forgotten
- Traceability
- Smart Contracts
- Data Quality

Availability

- Ensuring timely and reliable access to and use of information.
- No Single Point of Failure
- Operational Resilience

Redundancies in blockchain Network

In a blockchain network, for every node to be processed, it has to traverse and process every intermediate node independently to reach the target node. Thus, the redundancy involved in blockchain technology affects its performance.

Table 3.4 Preview of Blockchain Weaknesses - (Cloud Security Alliance - CSA)

Name of weakness	Description
API Exposure	If an API is improperly exposed an attacker can attack it
Block Mining Race Attack	A variation on the Finney attack
Block Mining Timejack	By isolating a node the time signal can be manipulated

Attack	getting the victim out of synchronization
Block Reordering Attack	Certain cryptographic operations such as using CBC (Cipher Blocker Chaining) or ECB (Electronic Codebook) incorrectly allow blocks to be re-ordered and the results will still decrypt properly
Blockchain Peer flooding Attack	By creating a large number of fake peers in a network (peer to peer or otherwise) an attacker can cause real nodes to slow down or become non responsive as they attempt to connect to the newly announced peers.

Advantages of Blockchain

Blockchain Pros

- Near-instant updating
- Chronological and timestamped
- Cryptographically sealed
- Irreversible and auditable
- Operates without trust
- Fewer third parties

Weakness of Blockchain

- Blockchain is not a Distributed Computing System
- Scalability Is An Issue
- transactions are completed depending on the network congestion.
- Some Blockchain Solutions Consume Too Much Energy
- high energy consumption is what makes these complex mathematical problems.
- Blockchain Cannot Go Back — Data is Immutable
- He will be unable to remove its trace from the system when he doesn't want it there.
- Blockchains are Sometimes Inefficient
- storage problems - ledger can easily cross 100's of GBs
- Not Completely Secure
- 51% attack, Double-spending, DDoS's attack:

Users Are Their Own Bank: Private Keys

Make sure that they do not share it with anyone else. If they fail to do so, their wallet is in danger. Also, if they lose the private key, they will lose access to the wallet forever.

- Cost And Implementation Struggle
- Expertise Knowledge
- Maturity

    - It is only a decade old and it requires time to mature.
- Interoperability
- Legacy Systems
- if they want to adopt blockchain technology, they need to completely get rid of their systems and change to blockchain technology

MINING AND CRYPTO CURRENCIES - HOW TO USE AND INTERACT

Mining-Pools-Impact of CPU and GPU-Transaction in Bit coin Network- Block Mining-Block propagation and block relay.

4.1 MINING

- Blockchain mining is a process to validate every step in the transactions while operating bitcoin or other cryptocurrencies.
- The people involved here are known as blockchain miners, and these miners' function in a labyrinth of computational hardware and software — their primary aim to authenticate the transfer of currency from a computer in the network to another.
- Blockchain are so-called because of their 'blocks' and 'chain' structure.
- The blocks are composed of numerous bitcoins which are individual units that store all the data code individually.
- The chain refers to the links from one neighbourhood block to another. Each blockchain represents a specific code authentication explicitly encrypted on the network software.
- The process is rewarding, as well. A single user does not handle the mining process, but a number of them compete on a unified authentication to get the rewards. Each mining success comes with a bonus of several bitcoins.

4.1.1 The Mining Process

The encrypted data needs decryption to prove validity. Decrypting the data encoded in blocks is not an easy task and demands computational hardware and software alongside human efforts. One single code decryption will take an enormous amount of time and energy both for the computer and the human.

A combination of the computational speed and human intelligence will result in the decrypted data, which, when linked with the adjacent blocks, verifies the transaction. The bitcoin blocks link together by codes named hash-codes. These hash codes meet specific requirements in the encrypted data's solution.

The miners need to solve the complex problem to find the perfect solution hash that matches and fits. The solution to the hidden code encryption is known as the 'Proof-of-work.' As the name suggests, it is a proof of the abundance of resources, time, and energy that is spent by the miner. This proof-of-work is challenging to produce and may sometimes prove to be of lower profitability.

4.1.2 Types of Mining

The process of mining can get really complex and a regular desktop or PC can't cut it. Instead, 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

In Individual Mining, the user has to register itself as a miner. As soon as a transaction occurs, all the single users in the blockchain network will receive a mathematical problem. The first one to solve the complex mathematical problem gets rewarded. The solution comes after rigorously using the hardware and software properties of the computer, which is being used by the miner.

With the solution onboard, all the other network miners will validate the decrypted value and then add the same to the blockchain. Thus, verifying the transaction that just occurred.

2. Pool Mining

Another type of mining is Pool Mining, where several users operate together to approve the transaction. Numerous transactions occur every second. Sometimes, due to the complexity of the data encrypted in the blocks, a single user can't decrypt the data encoded. Then the entire team of miners in the network operate together to solve the complex numerical and computational problem. After the result is validated, the reward is then also split between all users.

3. Cloud Mining

Eliminating the use of multiple computer hardware and software, another way in which you can mine blockchain is through cloud mining. Without juggling with the hardware and software parameters, electricity, or power usage and the connectivity or bandwidth issues, you can extract the blocks hassle-free with this method.

Cloud mining allows the users to operate in peace, not having to worry about the heating of the equipment or ventilation issues in managing the hardware. The constant worry to deal with handling all the machinery and worrying about its order timings or selling profits is eliminated altogether.

It seems profitable, according to the mining hardware parameters, but has its own set of disadvantages. These include limiting operational functionality with the limitations on bitcoin hashing. Lowering the reward profits results in the operational expenses to increase with cloud mining. The software up-gradation gets restricted with this type of mining, and so does the verification process involved.

4.1.3 Use of Blockchain Mining

1. Validating Transactions

Bitcoins are decentralized digital currencies, which are managed on a peer-to-peer computer network and transferred from one user to another. Bitcoin transactions occur in huge figures daily. But there is a certain lag in the entire framework.

Since these cryptocurrencies operate without a central administrator, there is a substantial amount of insecurity with the transactions that transpire. While dealing with printed currency, the validation lies in the printed numerical codes in each of them. Accordingly, what is the authentication with such cryptocurrencies?

With each transaction, blocks are added to the blockchain. The validation lies in the mining results from the blockchain miners.

2. Confirming Transactions

Bitcoins get embedded in the blockchain network, encoded explicitly in the blocks. A transaction takes place in the bitcoin networks that are present in the blocks. Miners work the blockchain mining process to confirm whether the transaction is authentic or not. Transactions get confirmed on completing the inclusion in the block.

3. Securing Network

Bitcoin Miners work together to secure the transaction network. Network security increases with the increase in the operators mining the blockchain. The decentralized network makes it difficult to account for responsibility to anyone in case of an attack or duplicity or cheating activity. Network security ensures no fraudulent activity is undertaken with the cryptocurrencies.

A process in verifying transactions using blocks and chains, with the combinational commitment of computational activity and human intellect, the blockchain mining has fastened areas toward validating specific methods and securing network transactions.

There is always a possibility of threats in losing the funds while managing cryptocurrencies. With the availability of different mining processes, these miners (working either individually or in a group), now have increased options. Operating with the primary aim to authenticate deliveries in bitcoin transactions, the miners accomplish every detail of the encrypted code.

4.1.4 Bitcoin mining

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 continues 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.

Mining Bitcoins on your own:

- Purchase a custom mining hardware: You need to purchase an Application-specific Integrated Circuit (ASIC) miner to mine bitcoins. While purchasing an ASIC Blockchain miner, you should consider its efficacy in hashing power and take a note of its pricing policies.
- Purchase a power supply: Blockchain miners consume a lot of power. So, get a dependable power supply which is compatible with the ASIC miner that you purchase.
- 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.

- 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.
- Connect the power supply to the ASIC Blockchain miner.
- Connect the ASIC Blockchain miner to your router.
- Boot up your ASIC miner.
- Enter your router's IP address in a web browser.
- Find 'connected devices' in the router miner page.
- Find your ASIC miner and click on it to display the device information.
- Copy and paste the IP address of your ASIC miner into your web browser.
- Log in to the ASIC miner with the default username and password that are 'Root' and 'Root.'
- Select 'Miner Configuration' to set up the miner according to your preferences.
- Enter the URL, username, and password for your mining pool on the Miner Configuration page of the ASIC Miner.
- Click 'Save and Apply' to save your credentials for future use.
- Start mining and in periodic intervals check your profitability.
- 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.

4.2 POOLS

Mining Pool

- Cryptocurrency mining pools are groups of miners who share their computational resources.
- Mining pools utilize these combined resources to strengthen the probability of finding a block or otherwise successfully mining for cryptocurrency.
- If the mining pool is successful and receives a reward, that reward is divided among participants in the pool.

4.2.1 Working of Mining Pool

Individually, participants in a mining pool contribute their processing power toward the effort of finding a block. If the pool is successful in these efforts, they receive a reward, typically in the form of the associated cryptocurrency.

Rewards are usually divided between the individuals who contributed, according to the proportion of each individual's processing power or work relative to the whole group. In some cases, individual miners must show proof of work in order to receive their rewards.

Anyone who wants to make a profit through cryptocurrency mining has the choice to either go solo with their own dedicated devices or to join a mining pool where multiple miners and their devices combine to enhance their hashing output. For example, attaching six mining devices that each offers 335 megahashes per second (MH/s) can generate a cumulative 2 gigahashes of mining power, thereby leading to faster processing of the hash function.

4.2.2 Mining Pool Methods

Not all cryptocurrency mining pools function in the same way. There are, however, a number of common protocols that govern many of the most popular mining pools.

Proportional mining pools are among the most common. In this type of pool, miners contributing to the pool's processing power receive shares up until the point at which the pool succeeds in finding a block. After that, miners receive rewards proportional to the number of shares they hold.

Pay-per-share pools operate somewhat similarly in that each miner receives shares for their contribution. However, these pools provide instant payouts regardless of when the block is found. A miner contributing to this type of pool can exchange shares for a proportional payout at any time.

Peer-to-peer mining pools, meanwhile, aim to prevent the pool structure from becoming centralized. As such, they integrate a separate blockchain related to the pool itself and designed to prevent the operators of the pool from cheating as well as the pool itself from failing due to a single central issue.

4.2.3 Benefits of a Mining Pool

While success in individual mining grants complete ownership of the reward, the odds of achieving success is very low because of high power and resource requirements. Mining is often not a profitable venture for individuals. Many cryptocurrencies have become increasingly difficult to mine in recent years as the popularity of these digital currencies has grown and the costs associated with expensive hardware necessary to be a competitive miner as well as electricity oftentimes outweigh the potential rewards.

Mining pools require less of each individual participant in terms of hardware and electricity costs and increase the chances of profitability. Whereas an individual miner might stand little chance of successfully finding a block and receiving a mining reward, teaming up with others dramatically improves the success rate.

4.2.4 Disadvantages of a Mining Pool

By taking part in a mining pool, individuals give up some of their autonomy in the mining process. They are typically bound by terms set by the pool itself, which may dictate how the mining process is approached. They are also required to divide up any potential rewards, meaning that the share of profit is lower for an individual participating in a pool.

A small number of mining pools, such as AntPool, Poolin, and F2Pool, dominate the bitcoin mining process, according to blockchain.com.1 Although many pools do make an effort to be decentralized, these groups consolidate much of the authority to govern the bitcoin protocol. For some cryptocurrency proponents, the presence of a small number of powerful mining pools goes against the decentralized structure inherent in bitcoin and other cryptocurrencies. Some of the best mining pools are Slush Pool, ViaBTC,Antpool,BTC.com,kanopool,f2pool etc.,

4.3 Impact of CPU and GPU

Despite the Central Processing Unit’s (CPU) knack for problem solving, it’s not the first component that comes to mind for the crypto convert. Nowadays, mining outfits rely on racks of super-charged ASICs and GPUs to churn out Bitcoin and Ethereum—or even the almighty Dogecoin.

4.3.1 Impacts on CPU MINING

The basics of CPU mining are similar to GPU mining, but the devil's in the details. There are a few key differences worth mentioning before you get started.

(#1) Protocol Optimization

Many coins are optimized to take advantage of both CPU and GPU power. Salad uses your CPU to mine for Monero (XMR) via XMRig. It’s one of the best known and most reliably profitable coins for CPU mining—though results aren't always guaranteed.

(#2) Variable Earning Rates

CPU earning rates are affected by many of the same factors as GPU mining, such as:

- hashrate
- cooling and hardware maintenance
- mining difficulty and luck

(#3) Lower Hash Power

Graphics cards generally perform specialized processes like rendering game graphics and particle effects, whereas the CPU is a jack-of-all-trades. It's like your computer's brain, tasked with overseeing everything from your Excel spreadsheets to those 50 browser tabs you've got open for someday.

The more background processes you have running, the less spare power your CPU will have to contribute to hashing. This makes CPU mining essentially ineffectual unless you’re truly AFK. The CPU's wide range of responsibilities benefit from its equally wide skill set. But when it comes to the highly parallelized computations required for mining, the GPU shines. A CPU can't output the same raw hash power that a GPU produces, and you may earn more slowly as a result.

Hardware Specialization

Outside of Bitcoin mining (which is dominated by ASICs), the majority of blockchain hash power is derived from GPUs. That's because CPU miners run up against notable hardware limitations, including:

- relying on RAM instead of VRAM for hashrates
- elevated sensitivity to background processes and apps
- fewer arithmetic logic units (ALUs)—they do less math.

In plain English: unlike most consumer graphics cards, your CPU doesn't have dedicated RAM. It relies entirely on the sticks in your motherboard for support. You may have a badass CPU with 12 cores, hyperthreading, and the works—but you can't go the distance with 2GB of RAM.

4.3.1.1 Will CPU Mining Harm Your Computer?

While GPU mining is considered safe for long-term use, the jury's still out on CPU mining. Your primary concern with any important piece of PC hardware should be **overheating**. Unsafe temperatures in vital components (like your GPU and CPU) can result in immediate failure, and possibly inflict permanent damage on your rig.

For those of you breaking out in a nervous sweat, take comfort! The worst you'll typically encounter is a blue screen or shutdown. Drivers are smart, and they'll use whatever means necessary to protect your PC from total meltdown.

But many CPUs don't have extraneous drivers, and won't get upgraded as often as your GPU—so it's your job to protect your PCs brains from getting scrambled. Here are some pro tips to mining safely with your CPU:

Keep CPU Temperature Low

Most CPUs allow you to check running temperature directly in BIOS, but third-party software like HWMonitor can be handy for keeping an eye on it. We generally recommend keeping your CPU temperature below 80°C. There's wiggle room on either side of that number (depending on your specific model, overclocking, and other factors) but it's a good benchmark.

Limit Other Processes

The more that you ask your CPU to do, the harder it will work. The harder it works, the hotter it will get. To avoid crashing your PC—from heat or simple overload—keep background and simultaneous processes to a minimum while mining.

Trying to watch YouTube videos, play games, or even browse the internet may put unnecessary strain on your CPU and cause performance issues. Not to mention, it will seriously reduce your earning rates. CPU mining is a strictly AFK activity.

Clean Your Computer Often

There should be as little dust and detritus as possible on the inside of your PC, down to the fans and boards alike. Get a can of compressed air and go to town on the inside of your PC—it all needs a good spring cleaning once in a while.

Pay special attention to the fans on the GPU and CPU, as these directly cool your hottest components and tend to get clogged quickly. Take care to give your PC breathing room, too.

Install Cooling Systems or Components

Extra cooling is never a bad thing, so long as you pay attention to maintaining proper airflows. There's a range of components that you can add to help keep your PC nice and chilly, such as:

- PC case fans
- dust filters
- aftermarket CPU coolers
- ice baths and liquid nitrogen

Any of these extras may help to keep your vital components in safe temperature ranges.

Mine With Caution on Laptops

Laptops have become increasingly powerful over the years, and many of them are on par with high-performance gaming rigs. Yet there's one disadvantage a laptop can never overcome: cramped insides.

Laptop designers need to preserve economy of space, and that often means shoving important components right next to each other, with no elbow room for extra fans and cooling components. As a result, laptops tend to run hot. If you're not watching the internal temperature, using a laptop for CPU mining can be risky (unless you live in the Arctic). Miners using laptops should take extreme caution to ensure proper cooling as best you can.

4.3.2 Impacts on GPU MINING

- A GPU, or graphics processing unit, is responsible for the digital rendering in a computer system.
- Due to a GPU's power potential vs. a CPU, or central processing unit, they have become more useful in blockchain mining due to their speed and efficiency.
- The blistering pace of technological advancement will determine if GPUs will remain the standard for high-level cryptocurrency mining.

4.3.2.1 GPUs Help in Cryptocurrency Mining

Cryptocurrency mining was originally performed using CPUs, or Central Processing Units. However, its limited processing speed and high power consumption led to limited output, rendering the CPU-based mining process inefficient.

Enter GPU-based mining, which offered multiple benefits over the use of CPUs. A standard GPU, like a Radeon HD 5970, clocked processing speeds of executing 3,200 32-bit instructions per clock, which was 800 times more than the speed of a CPU that executed only 4 32-bit instructions per clock.

It is this property of the GPU that makes them suitable and better for cryptocurrency mining, as the mining process requires higher efficiency in performing similar kinds of repetitive computations. The mining device continuously tries to decode the different hashes repeatedly with only one digit changing in each attempt.

GPUs are also equipped with a large number of Arithmetic Logic Units (ALU), which are responsible for performing mathematical computations. Courtesy of these ALUs, the GPU is capable of performing more calculations, leading to improved output for the crypto mining process.

4.3.3 GPU vs. CPU

Each standard computer is equipped with a Central Processing Unit (CPU), which is a processing device that acts as a master of the whole computer system. It performs the controlling functions for the whole computer based on the logic of the operating system and the software installed on the computer. Typical functions—like save this file as MS Word, print this spreadsheet, or run that video in VLC Media Player—are controlled by the CPU.

A GPU is another processing device, but one that works solely for handling display functions. It is the part of a computer that is responsible for its video rendering system.

The typical function of a GPU is to perform and control the rendering of visual effects and 3D-graphics so the CPU doesn't have to get involved in minute details of video-rendering services. It takes care of graphics-intensive tasks such as video editing, gaming display, and decoding and rendering of 3D videos and animations.

To draw an analogy, the master (CPU) managing the whole organization (the computer system) has a dedicated employee (GPU) to take care of a specialized department (video-rendering functions).

This setup allows the CPU to perform the high-level diversified tasks for managing the whole computer, while the GPU is in charge of the video functions of which it is a specialist. A CPU will perform the function to open a video file in Windows Media Player, but once the file opens, the GPU takes over the task of displaying it properly.

GPUs have been around for years, but face competition from improved, new-age devices. They include the Field Programmable Gate Arrays (FPGAs) and the Application Specific Integrated Circuits (ASICs), which score better than both CPUs and GPUs at performing hash calculations, an essential function to blockchain management in cryptocurrency.

4.4 Transaction In Bitcoin

- Bitcoin is a digital currency, a decentralized system that records transactions in a distributed ledger called a blockchain.

- Bitcoin miners run complex computer rigs to solve complicated puzzles in an effort to confirm groups of transactions called blocks; upon success, these blocks are added to the blockchain record and the miners are rewarded with a small number of bitcoins.
- Other participants in the Bitcoin market can buy or sell tokens through cryptocurrency exchanges or peer-to-peer.
- The Bitcoin ledger is protected against fraud via a trustless system; Bitcoin exchanges also work to defend themselves against potential theft, though high-profile thefts have occurred.
- Bitcoin transaction is a section of data confirmed by a signature of Bitcoin. It is sent to the Bitcoin network and forms blocks. It typically contains references to preceding transactions and associates a certain number of bitcoins with one or several public keys (Bitcoin addresses). It is not encrypted because there is nothing to encrypt in the Bitcoin system. A Blockchain browser is where all transactions are combined in the form of a blockchain. They can be found and verified. This is necessary to determine technical transaction parameters as well as verify the details of payments.

Table 1 The general format of all bitcoin transactions

Field	**Description**	**Size**
Version number	Currently 1	4 bytes
In-Counter	Positive integer VI = Varlnt	1-9 bytes
List of inputs	The first input of the first transaction is also called a coinbase	<In-counter> many inputs
Out-counter	Positive integer VI = Varlnt	1-9 bytes
List of outputs	The first output of the first transaction use Bitcoins found for the block	<out-counter> many outputs
Lock time	If not equal to 0 and sequence numbers are inferior to OxFFFFFFFF: block height or timestamp (for final transactions)	4 bytes

Data

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501
Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

Fig 4.1 bitcoin with input and output

Interpretation

Input in this transaction imports 50BTC from output # 0 in transactions f5d8…, then the output sends 50 BTC to a Bitcoin address (expressed here in the form of a hexadecimal system – 4043…). When the recipient wants to spend their money, he will reference this transaction's output # 0 for his own transaction's input.

Input

The mining ecosystem

Input is a reference to the output of another transaction. A transaction often possesses several inputs. The values of these references are resumed and the total value of bitcoins can be used for the current transaction output. Previous tx is the hash of a preceding transaction. Index is a certain output from this transaction. ScriptSig is the first half of the script (see below for more details about this).

The script is composed of two elements: the signature and the public key. The public key belongs to the user who applies the transaction outputs and confirms that the creator of the transaction has the right to have at his disposal the sum of money obtained from the outputs. Another element is EDCSA (hash signature of a simplified version of the transaction). In combination with the public key, this signature confirms that the transaction has been created by the real owner of this Bitcoin address.

Output

The output contains instructions about sending the bitcoins. The value is an amount in satoshi (1 BTC = 100000000 satoshi), which can be used by the transaction for which the current transaction is the input. ScriptPubKey is the second half of the script (this will be elaborated upon afterwards). There can be more than one output and these will share the amount sent from the inputs. Each transaction output may only be used as the input for the subsequent transaction once, with the effect that the sum of all current transaction inputs must be used in the output. Otherwise the remaining sum from the transaction inputs will be lost. For example, if the input is equal to 50BTC and the user must only send 25BTC, Bitcoin creates two outputs of 25BTC each: one will go to the destination, the other will go to the owner of the funds again (the so-called 'change' – a transaction in which the user in fact sends money to himself). Any amount remaining from the input of bitcoins not used in the transaction will become the fee for the transaction. The person generating the block will receive this fee.

Transaction verification

In order to verify if the inputs are permitted to collect the requisite sums from the outputs of the preceding transactions, Bitcoin uses the standard system of the script (see below) of scriptSig input and scriptPubKey output which this transaction references. They are evaluated with the help of scriptPubKey using the remaining values in the scriptSig stack.

The input is confirmed if the scriptPubKey script returns a "true" value. Using the script system, the sender can create very complex conditions to fulfill by those who wish to obtain the output value. For example, it is possible to create an input which any user will obtain without authorization. It is equally possible to request that the input be signed by 10 different keys or verified by password.

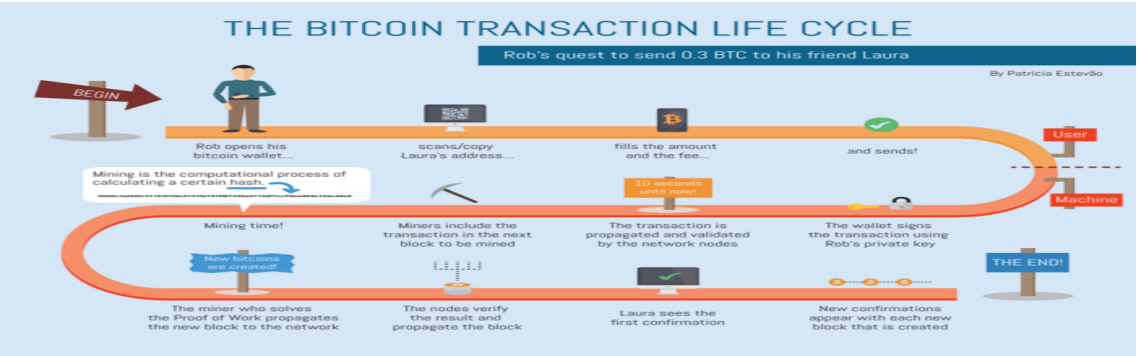


Fig 4.2 Bitcoin transaction lifecycle

Table 4.2 General format of each transaction input – Txin

Field	Description	Size
Hash of preceding transaction	Hashed double SHA256 of preceding transaction	32 bytes
Previous Txout-index	Arithmetical integer. It indexes outputs of the preceding transaction	4 bytes
List of inputs	The first input of the first transaction is also called a coinbase	<In-counter> many inputs
Length of Txin script	Arithmetical integer VI = Varlnt	1-9 bytes
Txin-script / scriptSig	Script	<length within the script> many bytes
Sequence number	Normally 0[FFFFFFFF; functions in the case that the lock time of the transaction > 0	4 bytes

The input adequately describes where and how the number of bitcoins can be obtained which can be redeemed by their new owner. If it is the only input of the first transaction in the block, it is called the generated transaction input. Its contents are completely ignored.

Table 4.3 General format of each transaction output – Txout

Field	Description	Size
Value	Arithmetical integer giving a satoshi amount (BTE/10^8) necessary for transactions	8 bytes
Length of Txout-script	Arithmetical stack	1-9 bytes
Txout-script / scriptPubKey	Script	<length of output script> many bytes

The output determines the conditions of use of the Bitcoin data in the following transactions, the sum of the output values of the first transaction in the block is a value of bitcoins taken for the block. Here a fee amount is added from the other transactions added to this block.

Transaction Confirmation

A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin transactions are not immediate. When a user wishes to send bitcoins, information is broadcast from her wallet to the (users in the) network, who verify that she has enough coins, and that they have never been spent before. Once validated, miners will include this transaction – along with others – in a new block in the blockchain. This is called a transaction confirmation. The transaction is now said to be "0/unconfirmed"

Each time a new block is added to the chain (every ten minutes), the transaction is said to be confirmed again. As a consensus, many users wait for a transaction to be confirmed six times (after roughly sixty minutes) before accepting it as payment, to avoid double-spending. Users will usually show a transaction as "n/unconfirmed" until it is six blocks deep.

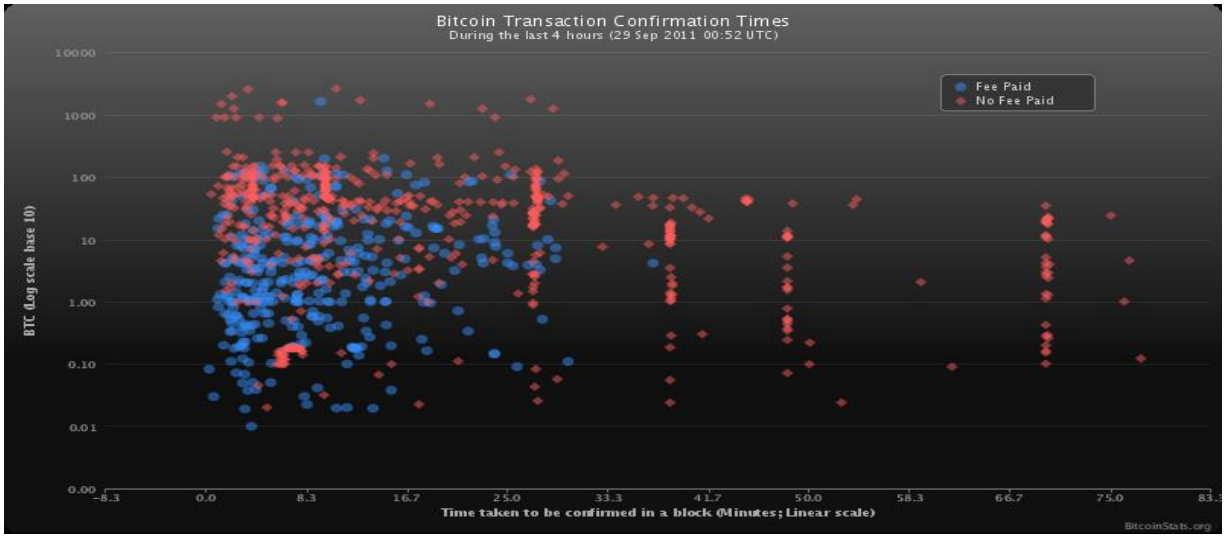


Fig 4.3 Bitcoin transaction confirmation times

Current bit coin transaction fee

Currently a large amount of transactions is processed in a way that commission isn't necessary. At the same time in case if transaction has a lot of entry points (e.g. it carries large amounts of data) a small commission is not uncommon.

Any miner can be the one who processes the transaction and earns the commission fee. When the network finds a new block it includes all information about transactions including their commission. Thus any user of group of users who find that block will gain both the reward for the block and the commission fees for every transaction included in it.

Including commission in a transaction is a voluntary decision but a user who finds a block can attach any transactions he wants to the said block. That way transactions with 0

commission have the lowest priority when transactions with even the minimal possible commission (~0.0001 BTC at the current moment) have standard priority and will more probably be included in the block.

Cost of Bit coin Transaction

Transaction fees (cost of Bitcoin transaction) are included with your bitcoin transaction in order to have your transaction processed by a miner and confirmed by the Bitcoin network. The space available for transactions in a block is currently artificially limited to 1 MB in the Bitcoin network. This means that to get your transaction processed quickly you will have to outbid other users. Bitcoin transaction price shown at the historic charts and tables are in US dollars per transaction and in satoshis per byte

4.5 BLOCK MINING

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 clearing house. Bitcoin transactions are generally verified in decentralized clearing systems wherein people contribute computing resources to verify the same. This process of verifying transactions in 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 which 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 words of Satoshi Nakamato, there's 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.'

Anyone can apply to become a Blockchain miner. These 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 a downtime since its launch in 2009

4.6 BLOCK PROPOGATION

The lack of scalability is known to be the foremost obstacle standing in the way of mass adoption of blockchain technology. All existing blockchain projects look for solutions that could improve the performance of their network.Many emerging projects claim that they have a magic bullet that could solve the problem. However, such assertions are not always valid. Unfortunately, many observers and investors do not realize the core and root of this problem.

Without deep investigation and considerable technical background, it's difficult to determine hidden bottlenecks and trade-offs. In this post, we are going to discuss one well-known bottleneck that prevents Bitcoin from scaling.

Shortly after the invention of decentralized peer-to-peer network Bitcoin, researchers got interested in what determines the limits of Bitcoin's scaling. Soon the core issue was determined and described in terms of block propagation time or block propagation delay. It's an average time that is needed for the new block to reach the majority of nodes in the network. In a large decentralized network like Bitcoin, whenever the new block is generated, it is broadcasted according to the Gossip protocol. If some node has got the new valid block, it informs nodes connected to it about its new possession. Then the node transfers this block to those nodes which asked it to do that. Before the block reaches each full-node in the network, it passes through 7 intermediary nodes. It's important that every honest node verifies the block before relaying it to other peers.

Obviously, the whole thing takes a while. Every new block shakes the network and makes nodes and ethernet connections between them work at full power. One might argue that since the launch of the network, there have been many improvements to the Gossip protocol. For example, the Bitcoin improvement proposal BIP 0152 introduced the option to transfer only short transaction IDs, instead of the whole list of transactions, in the block body.

However, if the node doesn't have that transaction in its mempool, it has to ask its peers to transfer it in a separate message. If there is a large number of such transactions in the block, then improvement from BIP 0152 disappears. Since data transmission is the most time-consuming part of the block relay, researchers got interested in determining how much time is required for a data packet of a certain size to reach 50%, 90%, or 95% of nodes in the network.

It was found that for blocks of a size larger than 20kB, the block propagation delay is nearly proportional to the block size. According to research published in 2013, every extra kB of data in the block caused an extra 80ms of block propagation delay. Since then, a couple of academic papers and surveys on this topic have been published every year. They update the aforementioned data and discuss various improvement proposals. Moreover, the site monitors the current state of the Bitcoin network and the block propagation time. Also, it provides charts with historical data on this subject.

The majority of well-established blockchain networks have the same design as Bitcoin. As a result, the block propagation time in these networks obeys the same rules. Unfortunately, the block propagation time has a massive effect on the blockchain security. The longer the propagation time in the network, the more often miners mine on top of old blocks.

As a result, the forking of the main chain occurs more often, and the percentage of orphan blocks rises. The long propagation delay leads to the so-called Verifiers Dilemma. Some nodes may find that skipping the block verification step could be a profitable strategy. In this case, they face the risk of mining on top of the wrong block. However, if block verification time is significant, this strategy could be profitable. Researchers found that long propagation delay reduces the node's resistance against 51% attacks and selfish mining.

In order to address the aforementioned problem, blockchain developers often try to keep the block propagation time to be less than 1% of the average block time. This is true for Bitcoin, Ethereum, and other major blockchain networks that are based on PoW consensus. For this reason, block propagation time to 50% of the nodes in the Bitcoin network is often below 6 seconds. Although fast block relay, like the one described in BIP 0152, reduces the average block propagation time, in the worst-case scenario it could take more time than the basic protocol. It's important that even in the worst-case scenario, the propagation delay should be

reasonable so that miners will keep their nodes synchronized most of the time, and will always verify proposed blocks.

Whenever people talk about the scalability of the blockchain, they mention the transaction throughput of the system. However, people forgot that improvements in transaction throughput shouldn't compromise the network's security, or raise data storage requirements for nodes desiring to participate in the network. These modifications could decrease the number of independent transaction validators in the network, thereby reducing decentralization.

Transaction throughput in Bitcoin could be easily calculated using the formula:

$$\text{Throughput} = \frac{B_{size}}{T_{size} \cdot B_{time}},$$

where

Bsize is the block size in bytes,
Tsize is the average size of transaction record in the block,
Btime is the average time between consecutive blocks in the blockchain.

Obviously, transaction throughput could be increased by increasing the block size, by reducing the transaction record size, or by reducing the interval between blocks. It's rather hard to reduce the size of the transaction records.

One might instead try the other two options. However, these actions will increase the percentage of time that is spent on block propagation. Thus, the security and decentralization of the network could get compromised.
One might notice that in the described Bitcoin protocol, network resources are used inefficiently. Every node processes and transmits the vital data about a new block only a small fraction of time. Its network bandwidth is really important, but it is used in full for only a few seconds at a time. The rest of the time, this node transmits only pending transactions and auxiliary data. This observation has inspired researchers to look for more efficient

protocol designs that could dramatically improve transaction throughput without compromising the security and decentralization of the network.

4.7 Block relay

The blockchain networks consist of tens of thousands of nodes. Let's imagine every node was relaying every transaction to every other node. The more nodes there are in the network, the more relaying you'd have to do. At a certain point, you would spend so much time relaying transactions that you will not have any time to produce blocks.

Fig 4.4 Block relay

Instead the relaying follows a bit more relaxed rules. Here are a couple of interesting examples of such rules:

– Instead of sending to every other node in the blockchain network, the nodes pick a subset of nodes to send to. For example, a node might relay transactions to ever 7th node they know of. Due to different nodes picking different subsets, very quickly everyone receives the information.

– Every node relays one and the same transaction only once. If they receive the same transaction again, they no longer relay it (as they've already sent it to their chosen subset)

The act of relaying transactions and other important information between nodes has the playful name of “gossiping”.

USE CASES-APPLICATIONS IN DIFFERENT AREAS

Syllabus

Industry applications of Blockchain - Blockchain in Government-Government use cases-Preventing Cybercrime through block chain-Block Chain in defense, tax payments.

5.1 Industry applications of Blockchain

Industry applications rely on blockchain records for innovative mobility services, supply chain traceability and trustworthy financial transactions. location of defective or counterfeit parts, the amount of data that automotive industry players must keep track of is exploding. The Blockchain can help build efficiency, transparency, and trust with a shared, permissioned record of ownership, location and movement of parts and goods. The versatility of blockchain records makes them perfect for keeping up with innovative new business models.

Today's cars are not just standalone transportation devices — they're complex, networked software platforms on wheels. Vehicles increasingly need to incorporate secure, seamless mobility services, handling micropayment and other interactions with ride-sharing services, smart transportation infrastructure and electric vehicle charging. blockchainbacked car eWallet service delivered through IBM Cloud™, enabling cashless micropayments for tolls, congestion fees, electric charging, parking and even making payments between vehicles. The system can also allow a vehicle to be used as a secure drop point for packages, with permissioned access to its trunk.

Supply chain

Challenges Auto manufacturing is truly global. Parts are sourced worldwide — and completed vehicles might be driven anywhere on earth. To contend with counterfeit parts and defect-driven product recalls, traceability is crucial in understanding a vehicle's post-sale movements. To maintain safety and reliability, makers must be able to track vehicle movements for regulators and purchasers. Analogous to the auto industry, Boeing is implementing a solution based on IBM Blockchain to make information from across the supply chain accessible to component vendors, aircraft owners and maintainers, and regulators. And in the case of a component safety issue, the same kind of IBM technology being applied to enable timely, efficient food recalls can help automobile makers and parts suppliers quickly understand where parts are.

Finance

Challenges From parts orders and fleet-purchase financing to managing letters of credit and arranging insurance coverage, every step of the automotive supply chain is underpinned by payments. Blockchain's traceability and transparency makes it perfect for keeping track of transactions that drive purchases, shipping arrangements, dealer transactions and millions of micropayments in mobility services. Blockchain-backed smart contracts go far beyond tracking and visibility to include funds released only on satisfactory delivery. Manufacturing powerhouse Mahindra implemented supply chain in finance one such example. Now, they're working with IBM to create a common blockchain platform for supplier-to-manufacturer transactions, allowing near-real-time transaction visibility and simplified communications to drive trust and transparency across its business ecosystem.

Blockchain Use Cases in Banking & Finance

International Payments

Blockchain provides a way to securely and efficiently create a tamper-proof log of sensitive activity. This makes it excellent for international payments and money transfers. For example, in April 2018, Banco Santander launched the world's first blockchain-based money transfer service. Known as "Santander One Pay FX," the service uses Ripple's xCurrent to enable customers to make same-day or next-day international money transfers.

Capital Markets

Blockchain-based systems also have the potential to improve capital markets. A McKinsey report identifies benefits that blockchain solutions offer capital markets, some of which include:

- Faster clearing and settlement
- Consolidated audit trail
- Operational improvements

Startup Axoni was founded in 2013 and builds blockchain-based solutions specifically for capital market improvement. Most recently, Axoni announced the launch of a distributed ledger network to manage equity swap transactions - enabling both sides of an equity swap to be synchronized throughout their lifecycle, communicating changes to each other in real time.

Trade Finance

Historic methods of trade financing have been a major pain point for businesses because the slow processes often interrupt business and make liquidity hard to manage. Cross-border trade involves a large number of variables when communicating information - such as country of origin and product details - and transactions generate high volumes of documentation. Blockchain has the ability to streamline trade finance deals and simplify the process across borders. It enables enterprises to more easily transact with each other beyond regional or geographic boundaries.

The extremely secure nature of blockchain makes it rather useful for accounting and auditing because it significantly decreases the possibility of human error and ensures the integrity of the records. On top of this, no one can alter the account records once they are locked in using blockchain tech, not even the record owners. The trade off here is that blockchain tech could ultimately eliminate the need for auditors and erase jobs.

Money Laundering Protection

Once again, the encryption that is so integral to blockchain makes it exceedingly helpful in combating money laundering. The underlying technology empowers record keeping, which supports "Know Your Customer (KYC)," the process through which a business identifies and verifies the identities of its clients.

Insurance

The blockchain application for insurance is through smart contracts. These contracts allow customers and insurers to manage claims in a transparent and secure manner. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims, since the blockchain would reject multiple claims on the same accident. For example, openIDL, a network built on the IBM Blockchain Platform with the American Association of Insurance Services, is automating insurance regulatory reporting and streamlining compliance requirements.

Peer-to-Peer Transactions

P2P payment services such as Venmo are convenient, but they have limits. Some services restrict transactions based on geography. Others charge a fee for their use. Many are vulnerable to hackers, which is not appealing for customers who are putting their personal

financial information out there. Blockchain technology, with all its aforementioned benefits, could fix these roadblocks.

Blockchain Applications in Business

Supply Chain Management

Blockchain's immutable ledger makes it well suited to tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using a blockchain opens up several options for companies transporting these goods. Entries on a blockchain can be used to queue up events with a supply chain - allocating goods newly arrived at a port to different shipping containers, for example. Blockchain provides a new and dynamic means of organizing tracking data and putting it to use.

Healthcare

Health data that's suitable for blockchain includes general information like age, gender, and potentially basic medical history data like immunization history or vital signs. These information not able to specifically identify any particular patient, which is what allows it to be stored on a shared blockchain that could be accessed by numerous individuals without undue privacy concerns. Blockchain can connect the medical devices with the patient record. Devices will be able to store the data generated on a healthcare blockchain and append it to personal medical records.

Real Estate

The average homeowner sells his or her home every five to seven years, and the average person will move nearly 12 times during their lifetime. With such frequent movement, blockchain could certainly be of use in the real estate market. It would expedite home sales by quickly verifying finances, reduce fraud thanks to its encryption, and offer transparency throughout the entire selling and purchasing process.

Media

Media companies have already started to adopt blockchain technology to eliminate fraud, reduce costs, and even protect Intellectual Property (IP) rights of content - like music records. According to MarketWatch, the global market for blockchain in media and entertainment is estimated to reach $1.54 billion by 2024. Eluvio, Inc. Formally launched in 2019, Eluvio Content Fabric uses blockchain technology to enable content producers to

manage and distribute premium video to consumers and business partners without content delivery networks.

Energy

Blockchain technology could be used to execute energy supply transactions, but also to further provide the basis for metering, billing, and clearing processes, according to PWC. Other potential applications include documenting ownership, asset management, origin guarantees, emission allowances, and renewable energy certificates.

Table 5.1 Blockchain in Energy

Areas	Blockchain Usage	Benefits
Energy trading	Transaction management	Real-time and peer-to-peer exchange
Smart energy	IoT management, resource management	Secure asset management
System protection (SCADA)	Data and service protection	Intrusion tolerance

5.2 Blockchain Applications in Government –Government Use cases

Record Management

National, state, and local governments are responsible for maintaining individuals' records such as birth and death dates, marital status, or property transfers. Traditionally some of these records only exist in paper form. And sometimes, citizens have to physically go to their local government offices to make changes, which is time-consuming, unnecessary, and frustrating. Blockchain technology could simplify this recordkeeping and make the data far more secure.

Identity Management

Proponents of blockchain tech for identity management claim that with enough information on the blockchain, people would only need to provide the bare minimum (date of birth, for example) to prove their identities.

Voting

Blockchain technology has the ability to make the voting process more easily accessible while improving security. Hackers would be no match to blockchain technology, because even if someone were to access the terminal, they wouldn't be able to affect other nodes. Each vote would be attributed to one ID, and with the ability to create a fake ID being impossible, government officials could tally votes more efficiently and effectively.

Taxes

Blockchain tech could make the cumbersome process of filing taxes, which is prone to human error, much more efficient with enough information stored on the blockchain.

Non-Profit Agencies

Blockchain could solve the anti-trust problems charities are increasingly facing through greater transparency. The technology has the ability to show donors that NPOs are in fact using their money as intended. Blockchain tech could help those NPOs tribute those funds more efficiently, manage their resources better, and enhance their tracking capabilities.

Compliance/Regulatory Oversight

The majority of regulatory oversight stems from recordkeeping, but the consequences of not maintaining records is inarguably much worse. Thus, compliance is non-negotiable for companies. Blockchain can make record updates available to regulators and businesses in real time, in turn reducing time lags and allowing red flags and inconsistencies to be spotted sooner.

Blockchain Applications in Other Industries

Financial Management and Accounting

If the blockchain is truly as secure as it has shown itself to be in the last several years, then such impenetrable security would be tantalizing for customers concerned with financial fraud.

Record Management

As stated earlier, the encryption that is central to blockchain makes it quite useful for record management because it prevents duplicates, fraudulent entries, and the like.

Cybersecurity

The biggest advantage for blockchain in cybersecurity is that it removes the risk of a single point of failure. Blockchain tech also provides end-to-end encryption and privacy.

Big Data

The immutable nature of blockchain, and the fact that every computer on the network is continually verifying the information stored on it, makes blockchain an excellent tool for storing big data.

Data Storage

The same principles for big data apply to data storage, as well.

IoT

Blockchain is poised to transform practices in a number of IoT sectors, including:

The supply chain: Tracking the location of goods as they are shipped, and ensuring that they stay within specified conditions. Asset tracking: Monitoring assets and machinery to record activity and output as an alternative to cloud solutions. Despite these key areas where blockchain can be leveraged, the technology in the IoT is still dependent on startups. In fact - only 17% of respondents to Business Insider Intelligence's survey of IoT providers think that blockchain will become a universal standard in the IoT.

Travel & mobility

Automotive manufacturing

Recording physical assets — like auto parts — on a blockchain is a prime example of where the technology might come in handy to track ownership with a tamper-proof, neutral, and resilient system. Paper records are prone to forgery and/or physical degradation, Centralized databases may be subject to hacking, human error, and/or tampering, Solution : blockchains are immutable and have no single entity controlling the ledger.

Car leasing & sales

The experience of leasing, buying, or selling a vehicle is a notoriously fragmented process for stakeholders on all sides of a transaction, but blockchain could change that.

Ride-hailing

Ride-hailing apps like Uber and Lyft represent the opposite of decentralization. since they essentially operate as dispatching hubs and use algorithms to control their fleets of drivers (and dictate what they charge). Blockchain could inject new options into that dynamic: with a distributed ledger, drivers and riders could create a more user-driven, value-oriented marketplace.

Trucking

The assets that can be tracked and recorded using blockchain aren't just digital transactions — they also include physical items, like shipping trucks. Blockchain can improve transactions, shipment tracking, and fleet management, as well as protect assets and increase fleet efficiency. It can help track contamination in food, for example, by tracking a truck that carries ingredients and noting if safe storage conditions were maintained during any delays.

Aerospace & defense

According to Accenture, 61% of aerospace and defense companies are working with blockchain or distributed ledger solutions. Blockchain technology has the potential to streamline parts inventory and authentication, personnel certification tracking, and more.

Air travel

Think of the data that goes into booking a flight: names, birthdays, credit card numbers, immigration details, destinations, and sometimes even hotel or rental car information, depending on how flights are booked. Transforming a material ticket into a digital token provides a new layer of security. Using a smart contract as part of the ticket token can help airlines control the sale and use of tickets to provide verified experiences for customers. It can also be used to create more accurate logs of aircraft maintenance, prevent overbooking, and more.

Hospitality

Large hotel chains lose 10% to 15% of their total revenue in the form of commissions paid to third-party booking services. Small chains and independent hotels fork over even more — between 18% and 22% of their revenue — to third-party services. Blockchain technology can help cut out the middlemen, encouraging direct provider-to-consumer interaction and reducing costs. blockchain-based platform Winding Tree has been working

with hotels, airlines, and tourism offices to provide a “decentralized open-source B2B travel marketplace.”

Infrastructure

Industrial IoT

A number of companies are leveraging blockchain tech to allow any device to securely connect, interact, and transact independently of a central authority.

3D printing

3D printing and “additive manufacturing” (aka building 3D objects by adding layer-upon-layer of material) are highly technology-driven processes, whereby the digital files involved can be easily transmitted with the click of a mouse. Consequently, parts and products are easier to share and track — leading to smarter digital supply networks and supply chains.

Construction, architecture, & building

A blockchain-based ecosystem could help solve this challenge by making it simpler for general contractors to verify identities and track progress across multiple teams.

Real estate

Real estate blockchain applications can help record, track, and transfer land titles, property deeds, liens, and more, and can help ensure that all documents are accurate and verifiable.

Healthcare

Health information exchanges

EHRs that must be addressed by any blockchain solution: governance, interoperability, privacy, scalability, and security. Healthcare institutions suffer from an inability to securely share data across platforms. Better data collaboration between providers could ultimately mean more accurate diagnoses, more effective treatments, and more cost-effective care. Use of blockchain technology could allow hospitals, payers, and other parties in the healthcare value chain to share access to their networks without compromising data security and integrity.Example : HealthVerity

The blockchain characteristics to meet those needs include immutability, cryptography, distribution, decentralization, transparency, auditability, and nonrepudiation

Pharma

Blockchain can also enforce safer drug production. If errors are made, they can be caught and traced to the source. This helps prevent recalls, or at least allows manufacturers to quickly contact retailers to lessen the impact of unsafe drugs on patients' health and businesses' finances.

Agriculture & mining

Crops & agriculture

A decentralized blockchain system could improve transactions, market expansions, and product-specific logistics throughout the agriculture supply chain.

Animal husbandry

blockchain tech is helping to improve food safety, traceability, and sustainability in animal husbandry — the breeding and raising of livestock.

Fishing

Between 20-30% of the fish sold in the US are caught illegally. Fishing is also one of the largest industries in the world using forced labor, according to the Wall Street Journal. Blockchain-based systems could help make the industry more sustainable, eco-friendly, and legally compliant.

Logging & timber

track wood and wood fiber from the forest to the consumer." The initiative aims to promote trust in the international trade of lumber and give transparency into the origins of imported lumber.

Table 5.2. Blockchain Use Cases Adopted by Governments and the Focus of Blockchain Applications

Use Cases	Representative Countries	Focus
Medical and healthcare	China, United States, Switzerland, Phillippines, Japan, Brazil, etc.	Supply chain, Internet-of-Things, etc.
Financial applications	(Almost) All	Cryptocurrencies, asset management, etc.

Critical infrastructures	South Korea	Asset management, optimization, etc.
Blockchain city	Malaysia	Cryptocurrency, data management
Asset management	Georgia, Sweden, Switzerland	Land registry, property transactions, etc.
Education	Japan, Malta	Certificate management
Data management	Phillipines, Australia	Cloud data management

U.S. Government

Health and Human Services (HHS) department has developed an application called ***Accelerate*** for management of contract billing that utilizes blockchain, AI, ML, and process automation. Disease Control and Prevention (CDC) to use blockchain to help track public health outbreaks such as hepatitis A using blockchain to track COVID-19 is a consideration.

Asian Governments

In 2019, the Filipino government approved the adoption of an Ethereum-based solution for approximately 80 rural banks to get access to financial services. Motivating the effort is the fact that only 42% of Filipinos aged 15 or older have a bank account due to a combination of factors. The concept of *blockchain city* has been used and made live at Malaysia's Melaka Straits city, a tourist city funded by the Chinese government. The project aims to use blockchain to track tourist visas, passengers, luggage, and booking services. The city will also manage its own token, the DMI coin, for tourists to exchange their money into digital currencies for payment in the city via their mobile phones. South Korea's government announced a 4B Korean won (about $3.5 million) award to set up a blockchain-enabled virtual power plant in the city of Busan, the country's second-most populous city.

European Governments

European Horizon program supports blockchain projects across the European Union. Luxembourg initiative in 2017, with a focus of building a blockchain governance framework. e-Estonia program supports multiple features such as e-identity, e-healthcare, and e-

governance. 98% of Estonians filing tax declarations completed online, and 99% of their health data is digitized and stored on blockchain. Georgia has implemented blockchain for land title registry and related property transactions. Sweden has also created a blockchain-based application for land registration and real estate transactions. The Maltese government recently completed the first national pilot of a blockchain to manage academic credentials such as diplomas, school certificates, and transcripts

Other Governments

Several major Australian government departments use cloud-based blockchain solutions, or Blockchain-as-a-Service. The Canadian government launched a pilot recently to use blockchain for digital credentials management, allowing employees to maintain a permanent, self-owned, and secure record of their digital credentials.

5.3 Preventing fraud and data theft

Blockchain technology provides one of the best tools we currently have to protect data from hackers, preventing potential fraud and decreasing the chance of data being stolen or compromised. In order to destroy or corrupt a blockchain, a hacker would have to destroy the data stored on every user's computer in the global network. This could be millions of computers, with each one storing a copy of some or all the data. Unless the hacker could simultaneously bring down an entire network (which is near impossible), undamaged computers, also known as "nodes", would continue running to verify and keep record of all the data on the network. The impossibility of a task like taking down a whole chain increases along with the amount of users on a network. Bigger blockchain networks with more users have an infinitely lower risk of getting attacked by hackers because of the complexity required to penetrate such a network.

Bitcoin too operates on blockchain technology. The entire blockchain is retained on a huge network of computers. So no person has control over history. Say, a user learns Cryptocurrency-related data from Crypto Head, buys bitcoins, and pays another using bitcoins. What happens next? Computers on the Bitcoin blockchain rush to check the accuracy of the transaction. This step certifies everything that has happened in the chain.

Thus, no one can go back and change things. So the blockchain can't be easily tampered with. This complex structure provides blockchain technology with the ability to be the most secure form of storing and sharing information online that we've discovered so far. That's why innovators have begun applying the technology in different sectors to prevent fraud and

increase protection of data. To make Blockchain transactions even more secure, users can benefit from VPN technology to mask their original IP address and spoof their online locations. The best VPN for anonymity lets users protect their data so third-parties can't track their online activities at all.

How Guardtime uses blockchain technology to safeguard data

Guardtime has already become successful in using blockchain technology to keep important data safe. The company takes away the need to use keys for verification. Instead, they distribute every piece of data to nodes throughout the system. If someone tries to alter the data, the system analyses the whole mass of chains, compares them to the metadata packet and then excludes any that don't match up. This means that the only way to wipe the entire blockchain out is to destroy every single separate node. If just one node remains running with the correct data, the whole system can be restored, even if all of the other nodes are compromised. Guardtime's system works in such a way that it's always able to detect when a change has been made to the data and is constantly verifying the changes. This ensures that there is no discrete way to tamper with blocks in the chain and the data remains uncompromised.

Preventing Distributed Denial of Service (DDoS) attacks

The principle behind DDoS attacks is simple but devastating. Hackers can use several techniques to instigate an attack, essentially sending myriads of junk requests to a website, increasing traffic until the site can no longer keep up with the requests. The attack goes on until the site gets overwhelmed with requests and crashes. DDoS attacks have been happening at an increased frequency recently, affecting bigger companies like Twitter, Spotify, SoundCloud, and more. The current difficulty in preventing DDoS attacks comes from the existing Domain Name System (DNS). DNS is a partially decentralized one-to-one mapping of IP addresses to domain names and works much like a phone book for the Internet. This system is responsible for resolving human-readable domain names (like steelkiwi.com) into machine-readable IP addresses (made up of numbers). The fact that it is only partially decentralized means that it is still vulnerable to hackers because they are able to target the centralized part of DNS (the one which stores the main bulk of data) and continue crashing one website after another.

5.4 Block Chain in defense

Blockchain would be particularly useful in defence. This technology has several advantages that stem from its decentralised nature. the distributed structure of the blockchain ensures its availability. It also makes this technology less expensive. its resilience, security and immutability are particularly useful to store the data and are a strong asset for many military applications. Also, defence departments all over the world are increasingly attracted by the power of the blockchain. the defence research community is expected to search for new applications for the military based on blockchain technology with predominant candidate areas such as cyber defence, secure messaging, resilient communications, logistics support and the networking of the defence Internet of Things." Blockchain technology has many utilities in the defence sector, as it can be used both in operational and support roles.

Technically, in the field of defence, it seems that the private blockchain would be the most useful. With a public blockchain, access to the chain would not be controlled, which could be dangerous to protect sensitive information. Since private blockchains are characterised by barriers to entry, with one administration in charge of accepting the participants and defining the rules of the chains (read and write permissions), they are the most suited to defence uses. Access and system rules could be controlled by one entity: the Army Chief. In a context of inter-services governance, a hybrid blockchain would also be possible. Cyber defence and data integrity The many benefits of blockchain make it a powerful prevention tool against cyber-attacks and explain why this technology is helpful in several fields linked with cyber defence.

In 2017, 235 GB of classified information belonging to South Korean and American intelligence services were stolen by North Korea. The same year, the European Commission stated that "there were more than 4,000 ransomware attacks per day and 80% of European companies experienced at least one cybersecurity incident. The economic impact of cyber-crime has risen fivefold over the past four years alone" (European Commission, State of the Union, 2017). The US federal government has been the target of more than 60,000 cyberattacks, notably in the energy sector, which is made vulnerable by its connectedness and dependence on computing technology (Mire, 2018). Storing large amounts of highly sensitive information in the same place is particularly risky.

It can lead to the “terabyte of death”, an expression used to describe the theft of massive classified information by foreign actors. In this context, the resilience offered by the blockchain, with its distributed nature and its ability to detect and block any penetrative attempt, can be significantly helpful. On the battlefield, soldiers need to be sure that the orders and information they receive are valid and accurate. A centralised entity in charge of digital communication is more vulnerable to attacks that can result in the communication being intercepted or altered. Additionally, if a part of a network is affected, the integrity of the system is not promised, and the whole network can collapse. Once again, blockchain appears as a solution to this challenge.

By sharing data horizontally, it democratises the battlespace and establishes a secure environment within which the failure of one node will not imply the failure of the others. As regards critical weapon systems, traditional weaponry is increasingly combined with the digitalisation of the military. For instance, the US Navy is working on improving the ageing Aegis Combat System by using blockchain to secure more effectively the centralised command-and-control system that links the sensors with weapons within the system. This would enable the weapon to detect targets and fire in under a millisecond (Babones, 2018). Many actors in the defence industry are eager to rely on blockchain, which gives a single, shared and immutable source of truth. As another report 9 Blockchain in defence: a breakthrough? by Accenture points out (Schmidt, Gelle, and Wheless, 2018), “inaccurate, manipulated, or biased data can have far-reaching, adverse consequences, such as corrupted business insights and skewed decisions”. That explains why, according to the report, 86% of aerospace and defence firms in Europe and the US plan to integrate the blockchain technology by 2021.

5.5 Blockchain in tax payments

In the majority of developed countries, matters related to payroll are mostly digitalized. However, the systems for payroll taxes have a significant flaw. Many government institutions involved and each one holds their own register. The Problem is duplicating data.

By embedding smart contracts that fully automate the process, which could be done in the following steps:

1. The employer inserts the gross amount of salary into the system,

2. Within the Blockchain system (limited only to the tax administration, banks and the other necessary parties), tax data is matched with the payment by smart contract technology and calculates the correct tax and social security amounts,

3. The net salary is automatically transferred to the employee's account and the calculated tax to the government,

4. As a result, the payroll tax process is faster and less costly and cash-flow is more efficient.

Problems in VAT

VAT is the key driving factor of tax administrations and the largest contribution to governmental budgets. tax authorities search for ways of more effective VAT collection in order to gain more revenue and shorten the budget gap. correctly calculate the amount of VAT due and submit it to the tax authorities, which is a burden especially to SMEs. In an international context, controlling VAT data is troublesome as each country maintains their own ledgers, making it difficult to obtain wholesome data on VAT movements.

How can Blockchain benefit everyday VAT transactions?

Benefits:

a) The administrative burden of companies is significantly reduced, saving time and the cost of accounting services,

b) All of the transactions are conducted in real-time,

c) All the transactions executed by smart contracts are tamper proof and transparent,

d)Reduced risk of fraud and mistakes,

e) Immediate insight into a company's finances,

f) High speed of money transfers between businesses and the government,

g) Taxpayers get the burden of VAT amount calculations on invoice level and VAT amount due on tax return level taken away,

h) Room for VAT frauds is drastically reduced because the same system allowing for processing VAT from transactional point of view, allows at the very same time for multi-dimension checks and verifications of the transaction, parties of the transactions and legal and business context of the transaction.

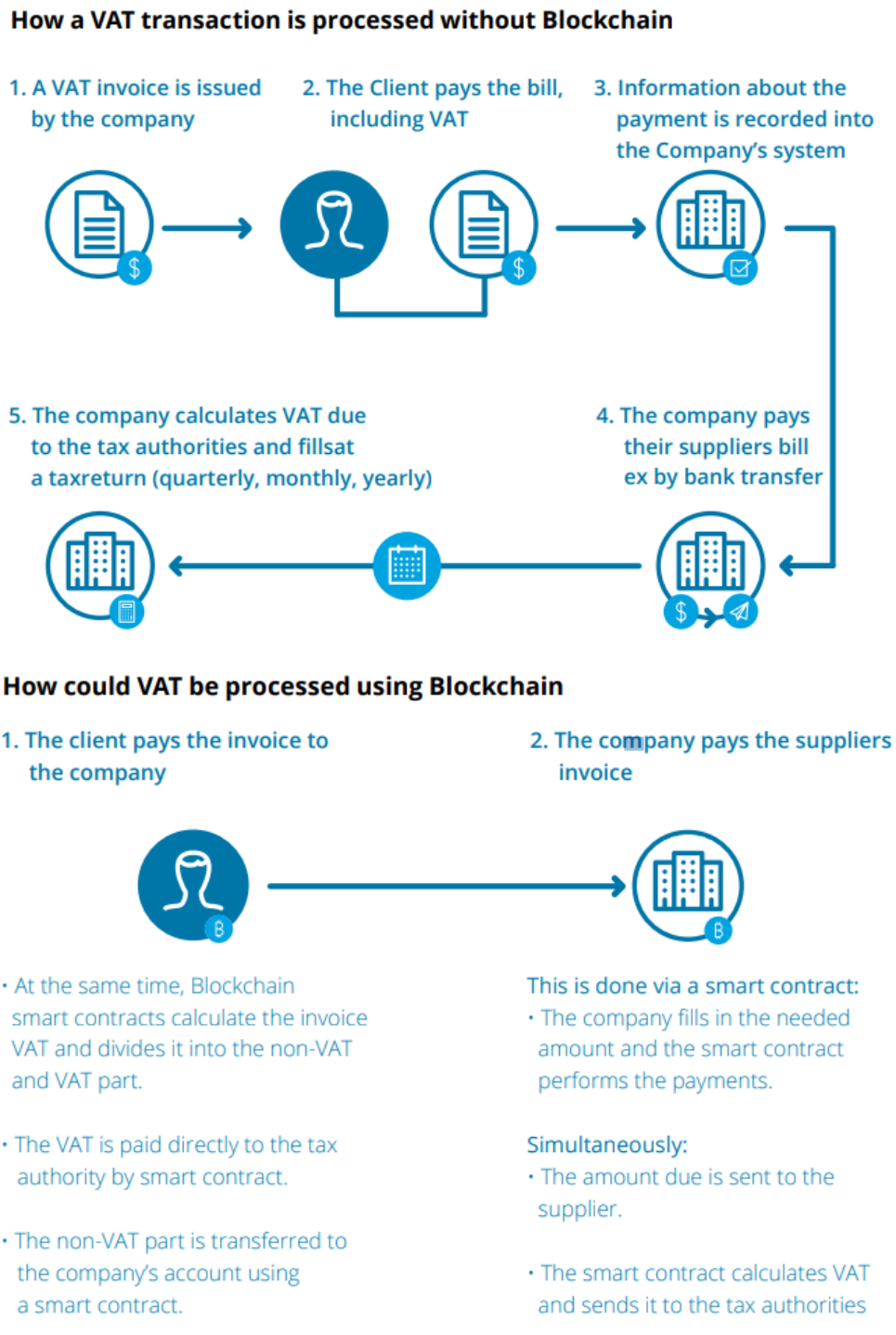


Figure 5.1 Blockchain in Tax payment