



Chapter 1 : Introduction to Blockchain

Department of Computer Engineering, VESIT, Mumbai

Agenda

- **Prerequisite**
- **What is a Blockchain?**
- **Structure of a Block**
- **Block Header**
- **Block Height**
- **Genesis Block**
- **Linking Blocks in Blockchain**
- **Merkle Trees**



Since 1962

What is a Blockchain?



A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

- Wikipedia

What is Blockchain ?

- Blockchain is defined as a **distributed, replicated peer-to-peer network of databases** that allows multiple non-trusting parties to transact **without a trusted intermediary** and maintains an ever-growing, append-only, **tamper-resistant list** of time-sequenced records.
- Blockchain can be considered as a type of a **distributed ledger** that sits on the internet for recording transactions and maintaining a permanent and **verifiable record-set of information**.

What is Blockchain ?

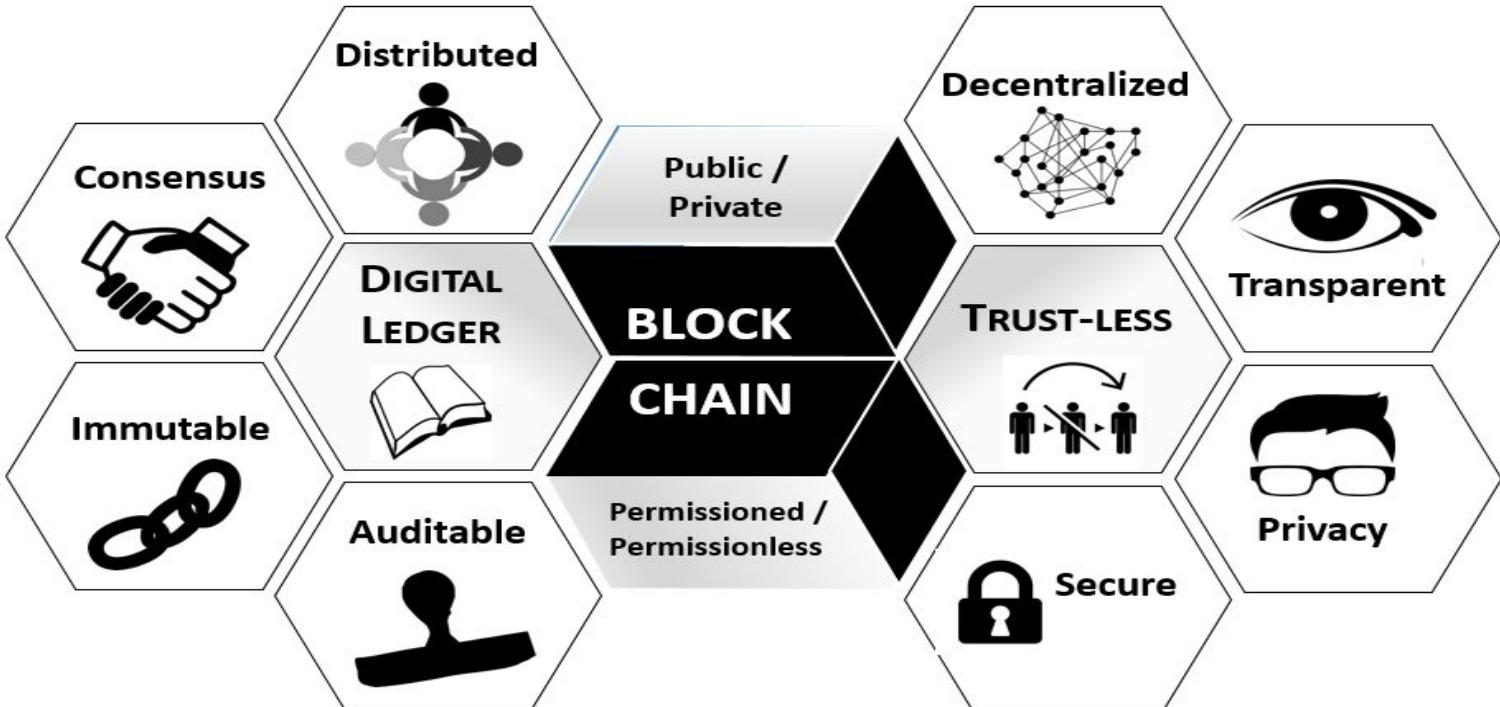
- Though the terms '**Bitcoin**' and '**Blockchain**' are often used to interchangeably, they are not the same. Blockchain is the underpinning technology that the Bitcoin was built on.
- Blockchain acts as **Bitcoin's ledger** and maintains all the transactions of bitcoin.

Blockchain : <https://blockchaindemo.io/>

Key features of Blockchain

- Write-only, immutable, transparent data storage.
- Decentralized, no need for intermediaries.
- Consistent state across all participants.
- Resistant against malicious participants.
- Open to everyone.

Characteristics of Blockchain

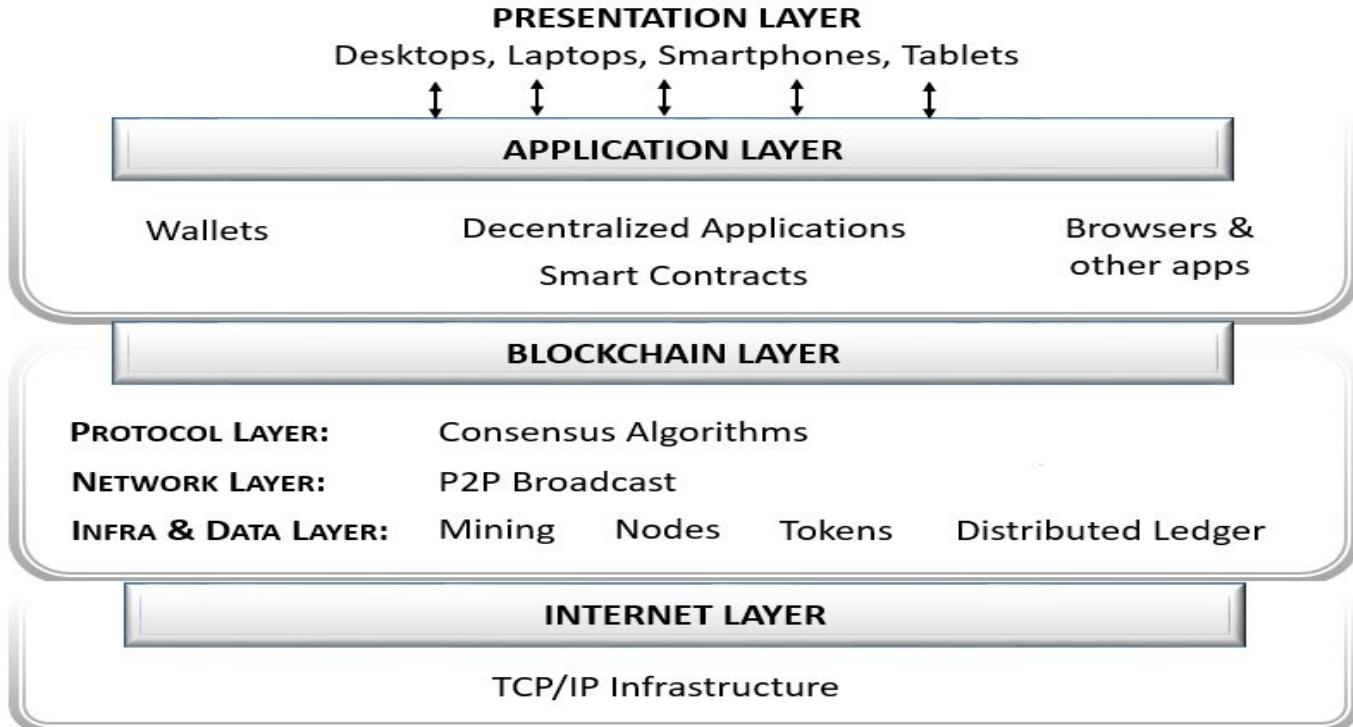




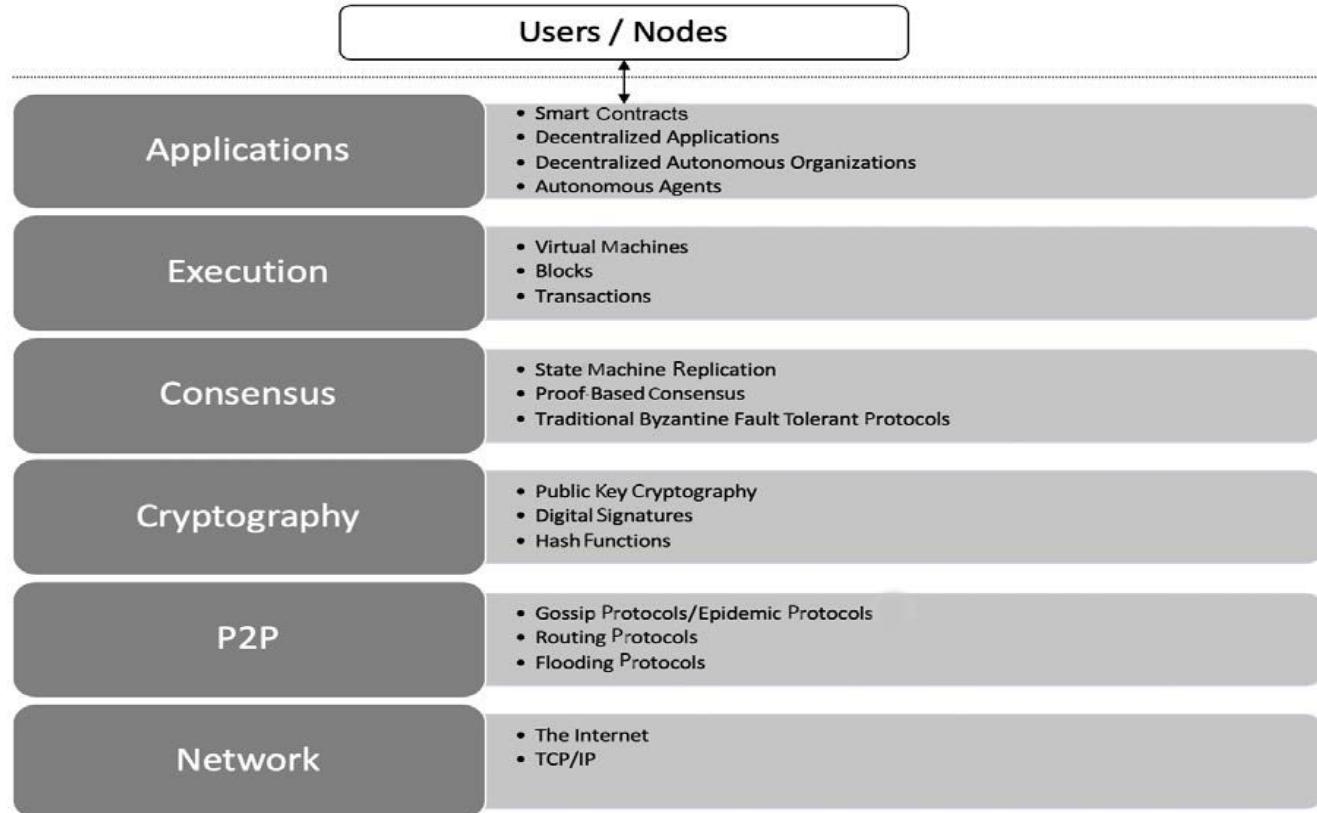
Properties of Blockchain

Tamper Resistant	Mining / Consensus	Chronological Ordering	Double Spending
<ul style="list-style-type: none">• Data is hashed• Linkage is connected through hashing of earlier block• Distributed nature	<ul style="list-style-type: none">• Public blockchain• Data available publically	<ul style="list-style-type: none">• Transactions entered in chronological order	<ul style="list-style-type: none">• Assurance through smart contracts

Blockchain Layers



The architectural view of a generic blockchain



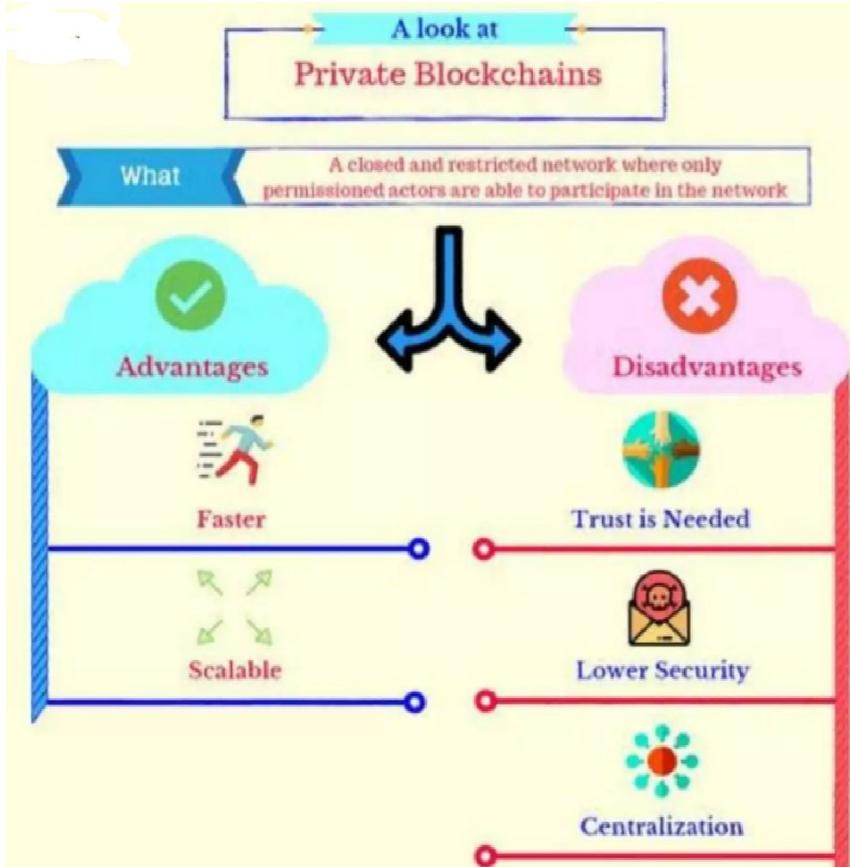
Types of BCT Applications

Public

Private

Hybrid /
Consortium

Public and Private Blockchain

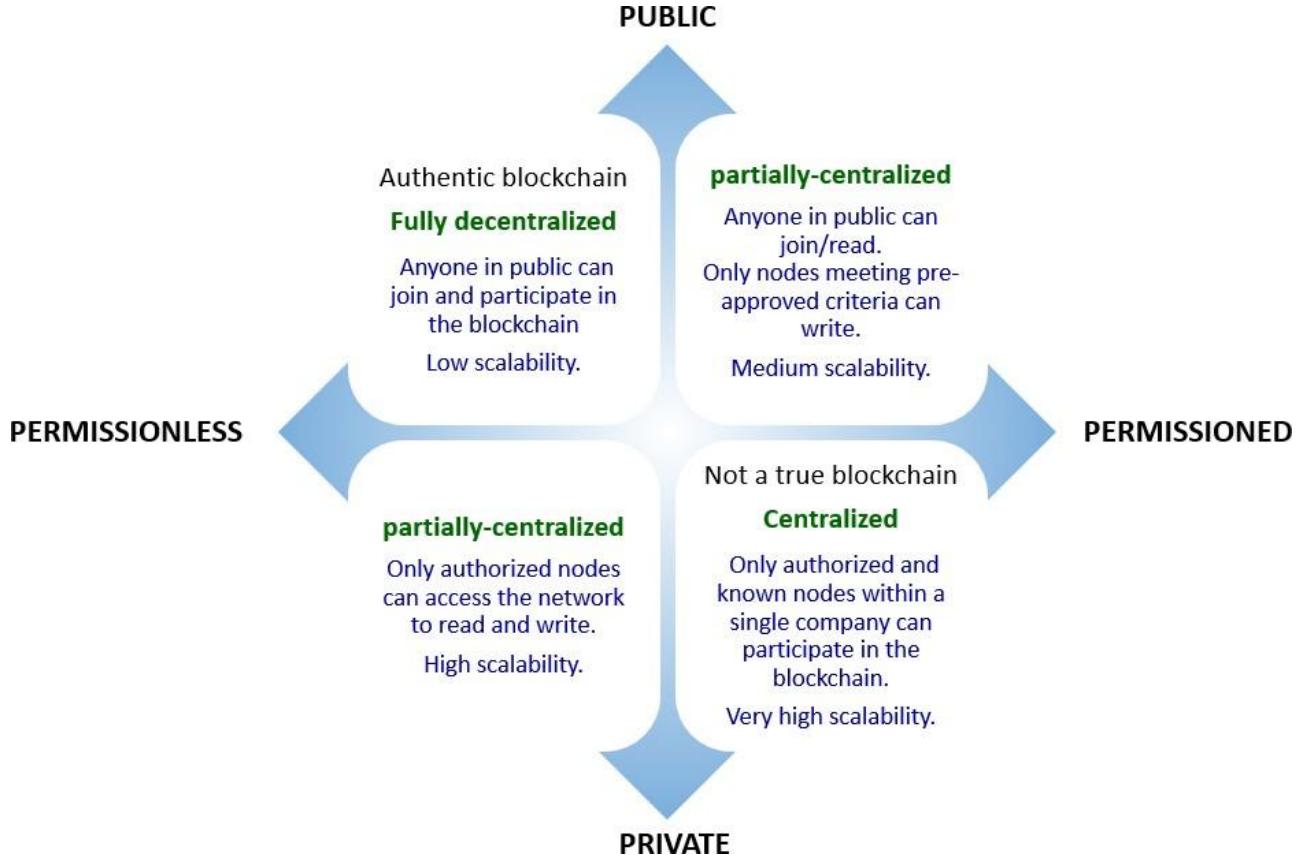


• Public Blockchain:

The public blockchains are:

- Are slower
- Has Public Ownership
- Are open and transparent
- Are Trust-Free
- And are Allegal

Types of Blockchain



Types of BCT Applications

Public BCT :

- Bitcoin
- Ethereum
- Corda R3

Private BCT :

- Polkadot
- Cosmos
- Chainlink

Hybrid BCT :

- Hyperledger Fabric
- Hyperledger Sawtooth
- Hyperledger Indi

What is a Blockchain?

GENESIS BLOCK



What is a Genesis Block?

GENESIS BLOCK



Data: ...

Prev.Hash: 000000000

Hash: 034DFA357

What is a Blockchain?

GENESIS BLOCK



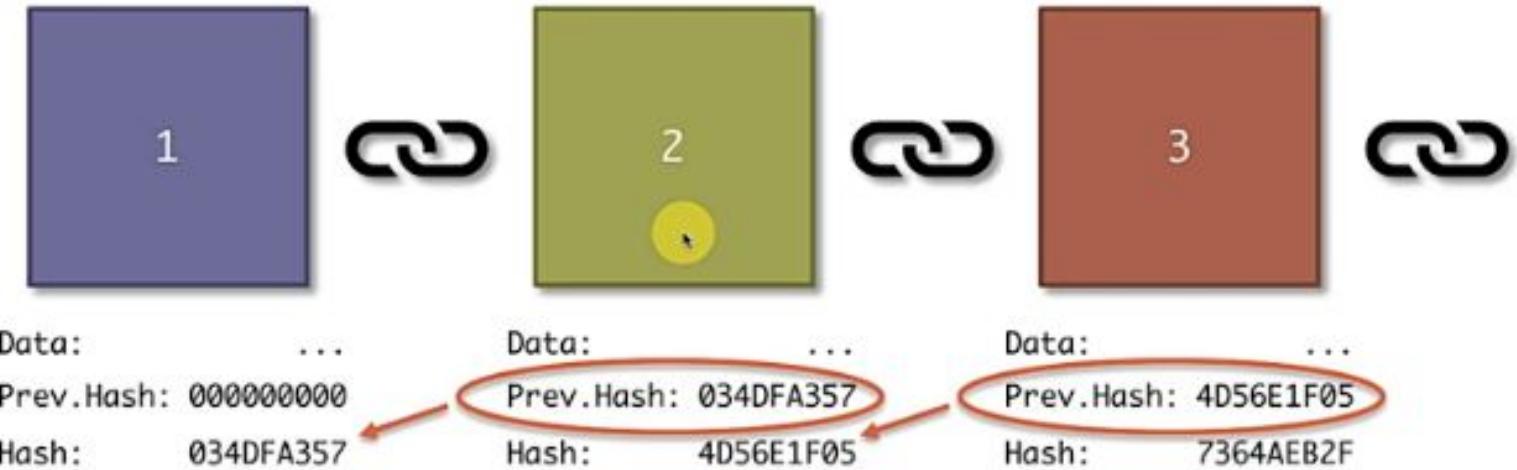
Data: ...
Prev.Hash: 000000000
Hash: 034DFA357

Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05

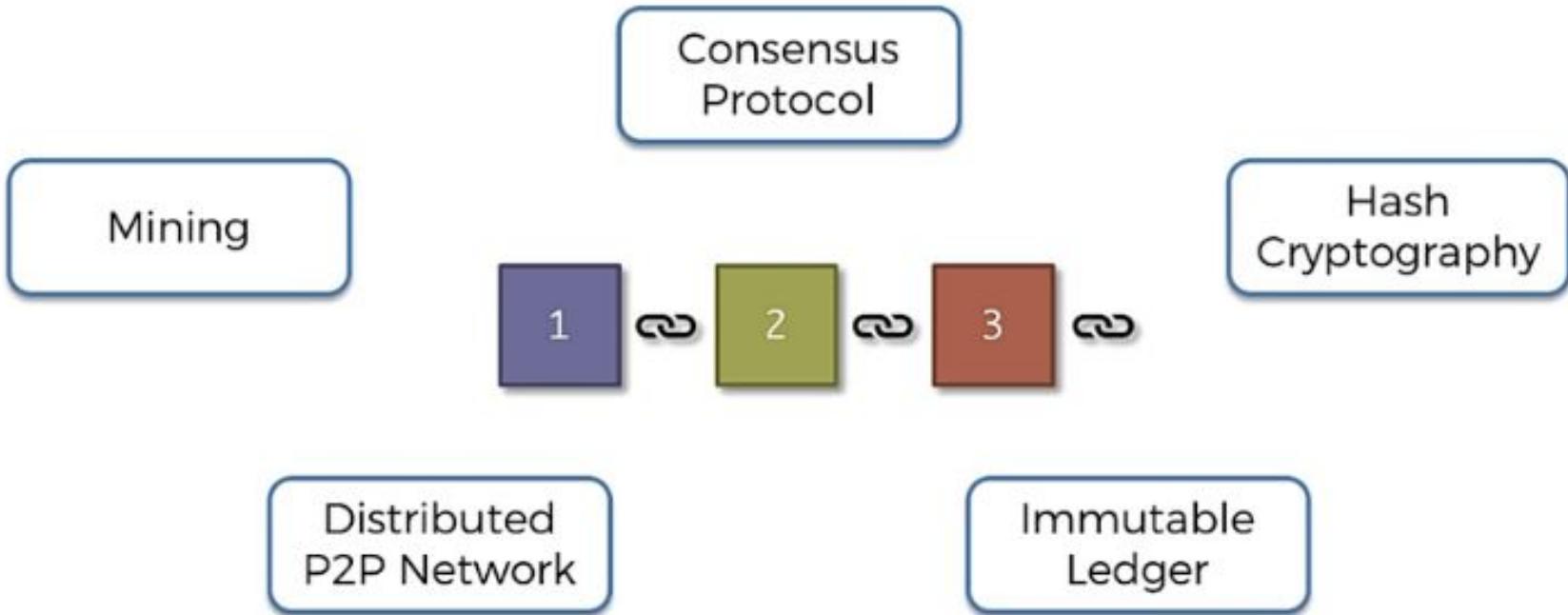


Linking Blocks in a Blockchain

GENESIS BLOCK



What is a Blockchain?

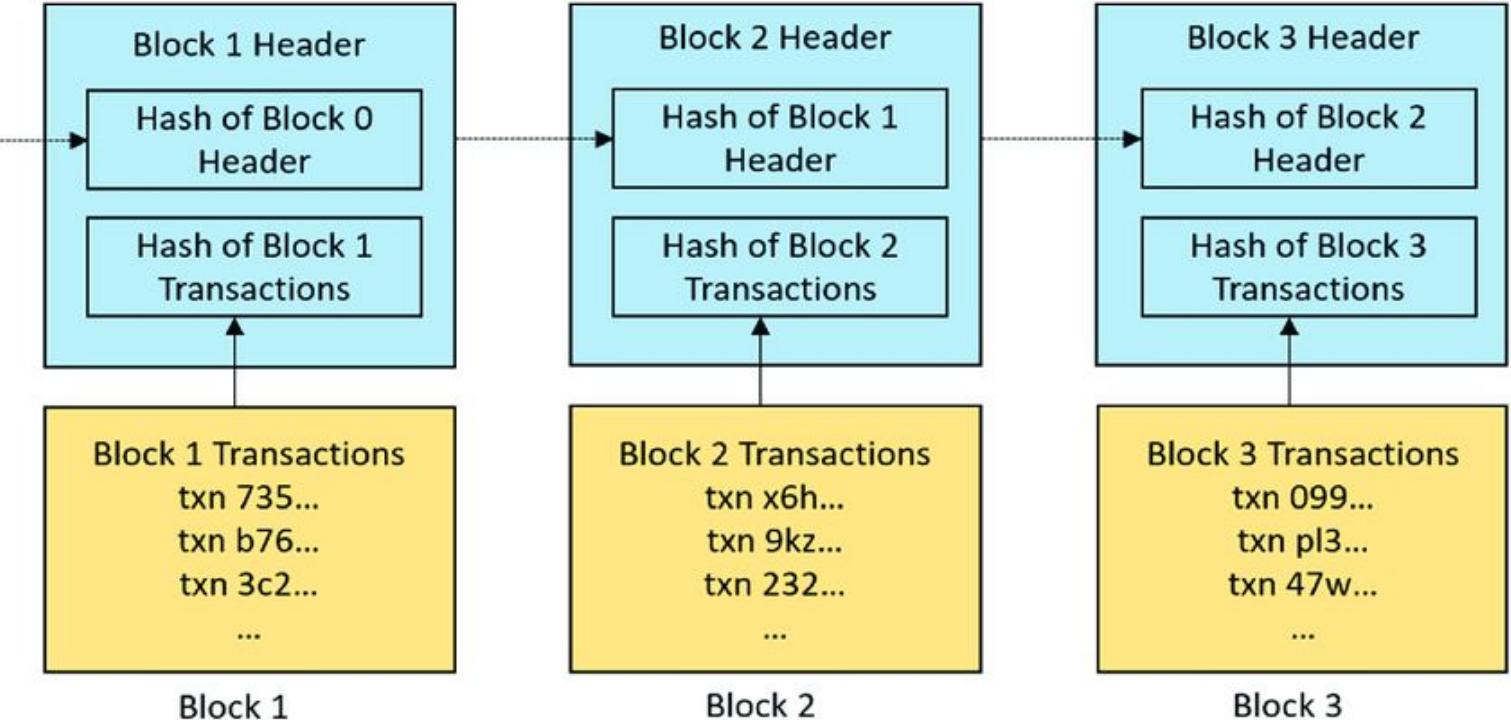


What is a Block?

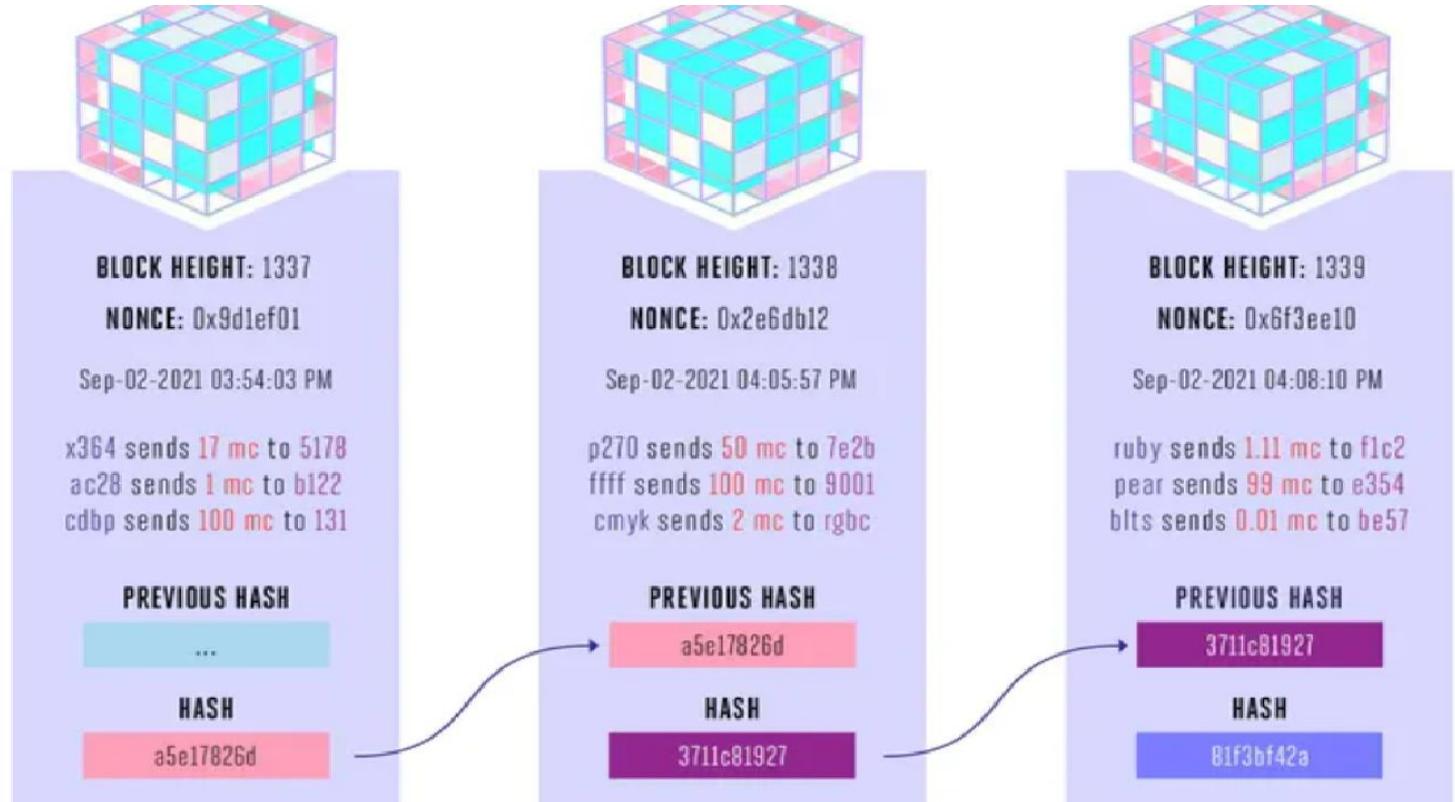
The block is a **record that contains the transaction data details**. It comprises of :

- Hash of the block – Alphanumeric number to identify the block
- Hash of the previous block.
- Timestamp
- Nonce – the random number used to vary the value of the hash
- Merkle Root – hash of all the hashes of all the transactions in the block
- Transaction data. (Note: This contains details of several transactions)

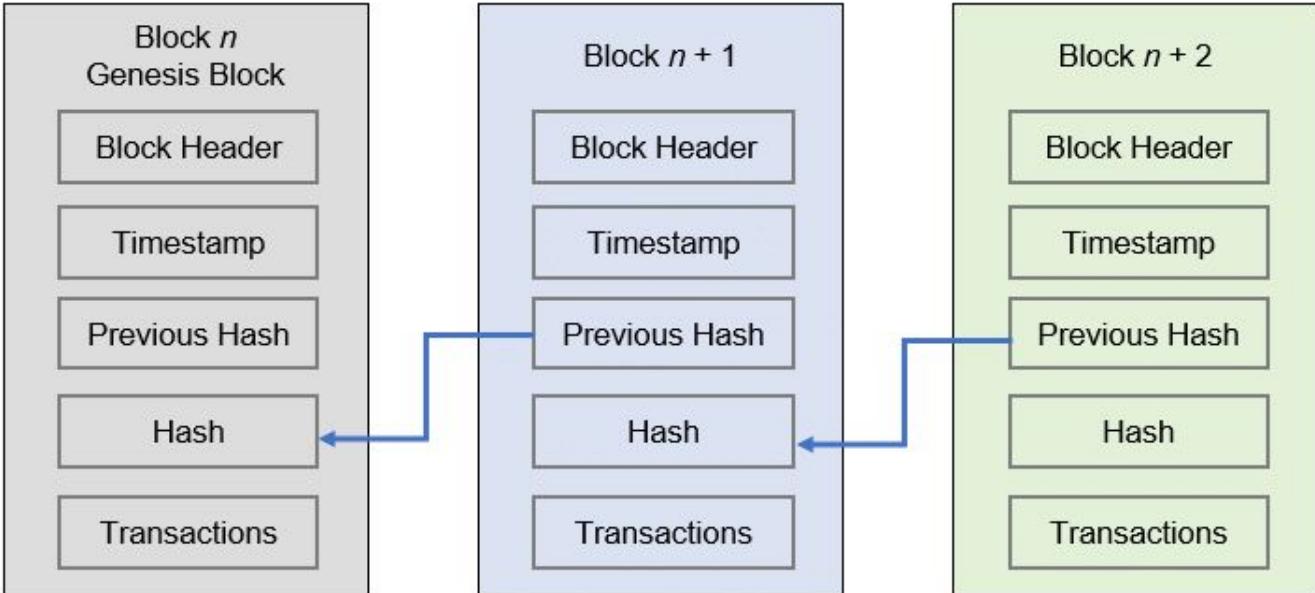
What is a Block?



Internal Structure of a Block

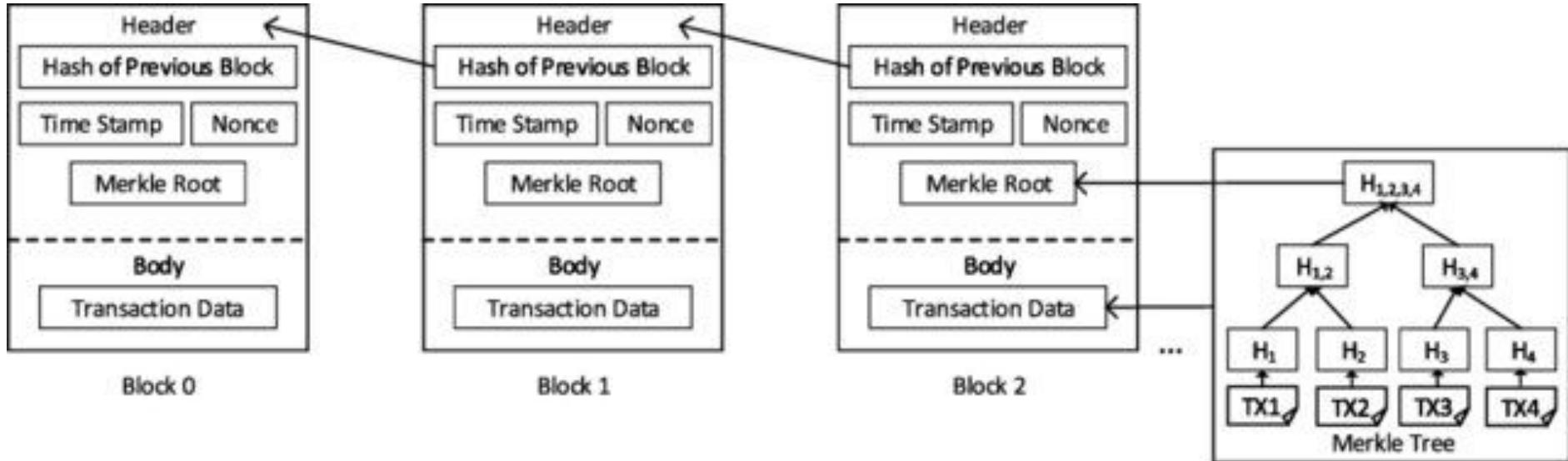


What is inside a Block?



- A block is a **bunch of transactions** that have been added to the blockchain.

What is inside a Block?

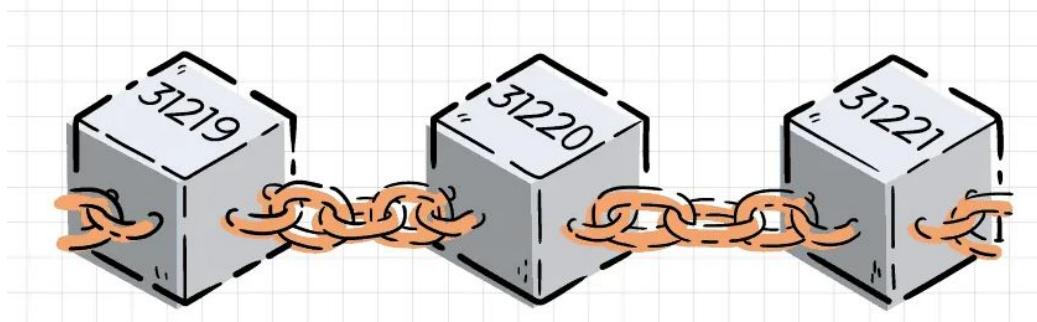


Courtesy : https://www.researchgate.net/publication/337306138_Blockchain_for_Dynamic_Spectrum_Management/figures?lo=1

What is a Block Height?

- The block height of a particular block is defined as the **number of blocks preceding it in the blockchain**
 - As of April 2021, the block height for the **Bitcoin blockchain exceeds 677,350 blocks**, with approximately 144 new blocks added daily

Courtesy : <https://explorer.bit2me.com/btc/block/000000000000000000007b1766512f8ef190bb9896e8bcb8977b043a8945978ef00>



What is a Block Height?

- Decentralized consensus algorithms typically function by **agreeing to mine the chain with the longest block height.**
- The very first block on a blockchain is called the **genesis block**. It has a block height of zero, as no blocks precede it in the blockchain.
- The total height of the blockchain is taken to be the **height of the most recent block, or the highest block, in the chain.**
- Another important point is the block height **helps the cryptocurrency protocol** make the necessary adjustments to the mining difficulty. This allows to improve the security of the cryptocurrency and **maintain a controlled inflation rate.**

What is a Block Height?

BITCOIN BLOCK #350



00000000e286ad94972e44b0532f2823bcda3977661a5136ff4d9d7db10
7d944



Number of transactions	1	Relayed by	Unknown
Height	350	Difficulty	1
Date	1231865478	Bits	1d00ffff
Creation date	1/13/09, 10:21 PM	Block size (bytes)	216
		Version	1
		Nonce	2183056385
		Block reward	BTC50.00

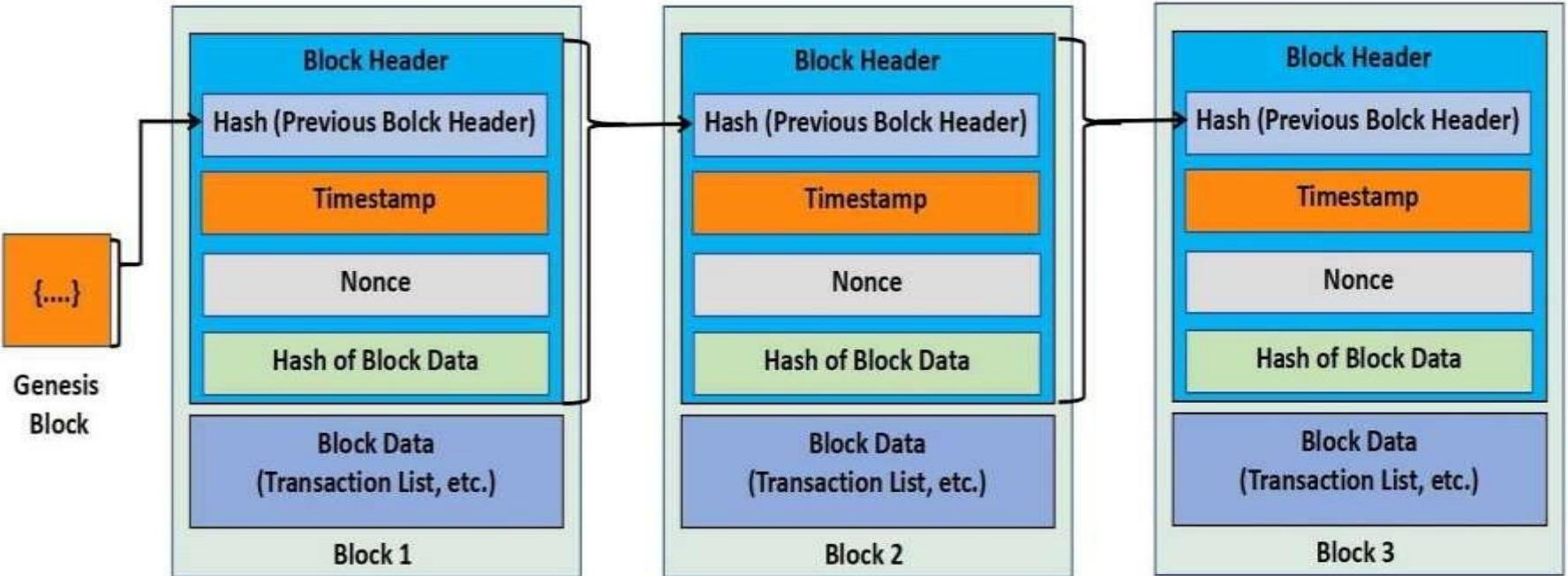
Transactions

272da16bce9a03c3aea2b294616e8e72e45dd29557938c10ed0848e62ad76018
748755 Confirmations 1/13/09, 10:21 PM

BTC50.00

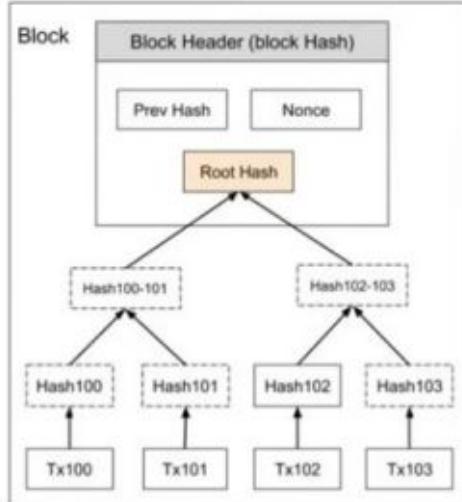


Blockchain

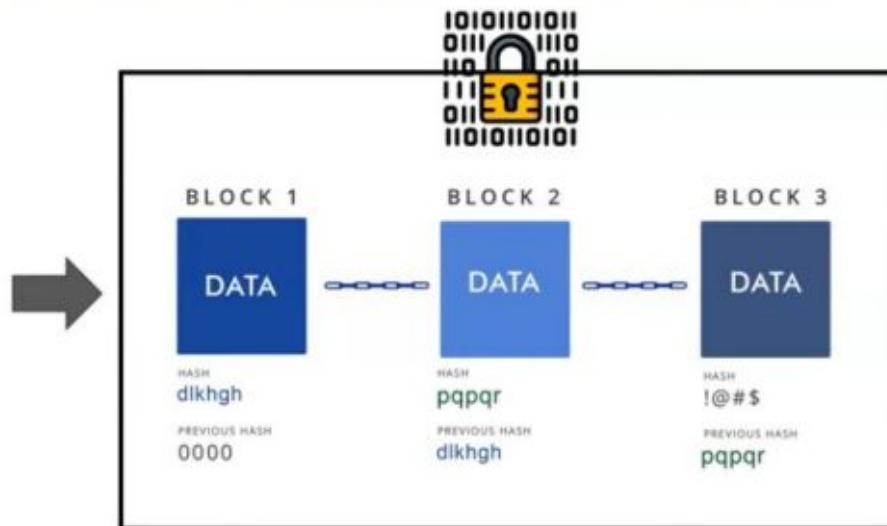


What is a Merkle Tree ?

Merkle trees are a type of data structure commonly used in computer science. They are used to encrypt blockchain data more effectively and securely in bitcoin and other cryptocurrencies.



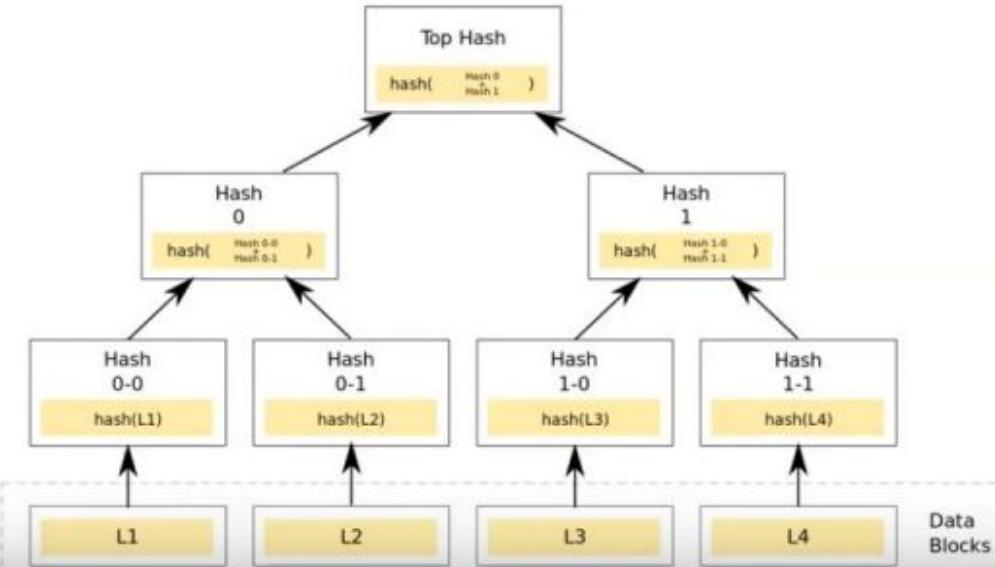
Merkle Tree



Blockchain Data encrypted Securely

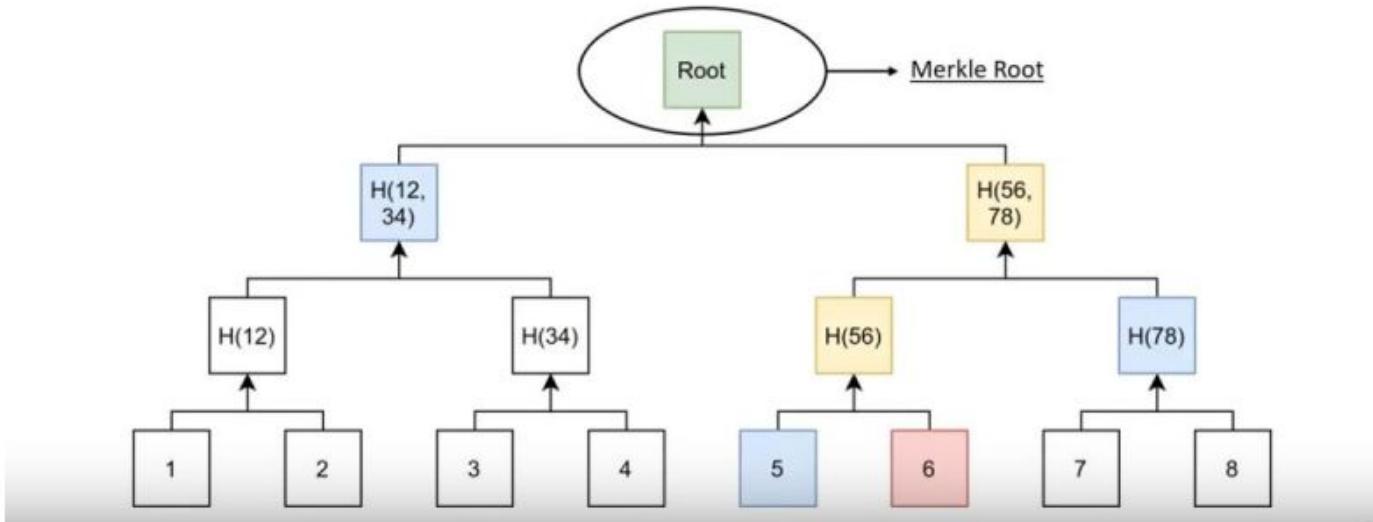
What is a Merkle Tree ?

It's a mathematical data structure or a method of organizing data, made up of hash number of various data blocks of transactions performed of the Blockchain Network. It acts as a summary of all the transactions.



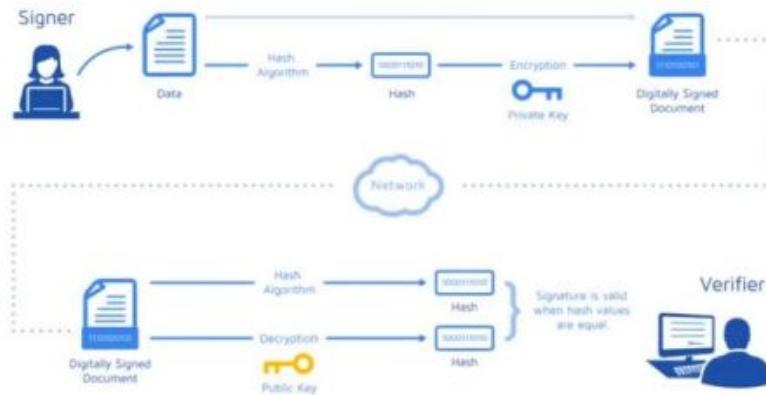
What is a Merkle Root ?

Merkle root is a simple mathematical method for confirming the facts on a Merkle tree. They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are secure.



How does a Merkle Tree work ?

A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether a transaction is included in the block.



How does a Merkle Tree work ?

They're built from the bottom, using Transaction IDs, which are hashes of individual transactions. Consider the following scenario: A, B, C, and D are four transactions, all executed on the same block.

Transaction ID A

Transaction ID B

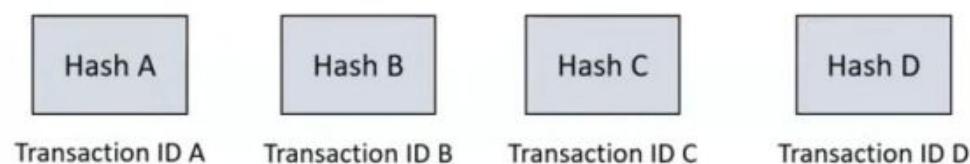
Transaction ID C

Transaction ID D

How does a Merkle Tree work ?

Each transaction is then hashed, leaving us with:

Hash A
Hash B
Hash C
Hash D



How does a Merkle Tree work ?

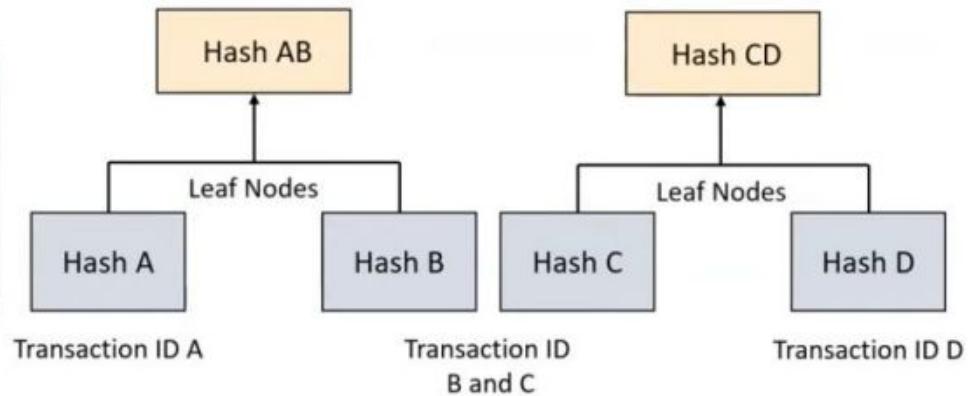
The hashes are paired together resulting in:

Hash AB

and

Hash CD

Our Merkle Root is formed by combining these two hashes: Hash ABCD.



How does a Merkle Tree work ?

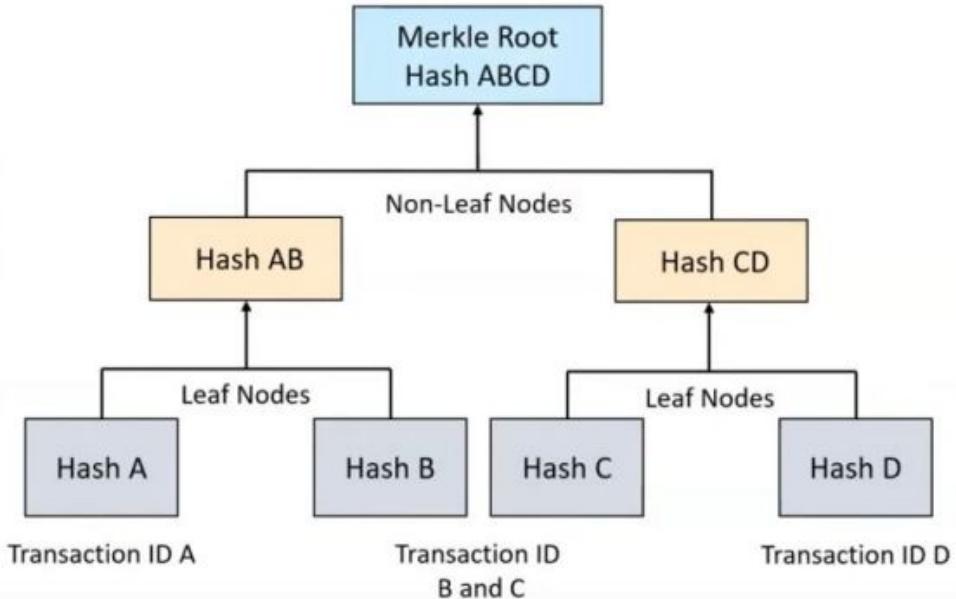
The hashes are paired together resulting in:

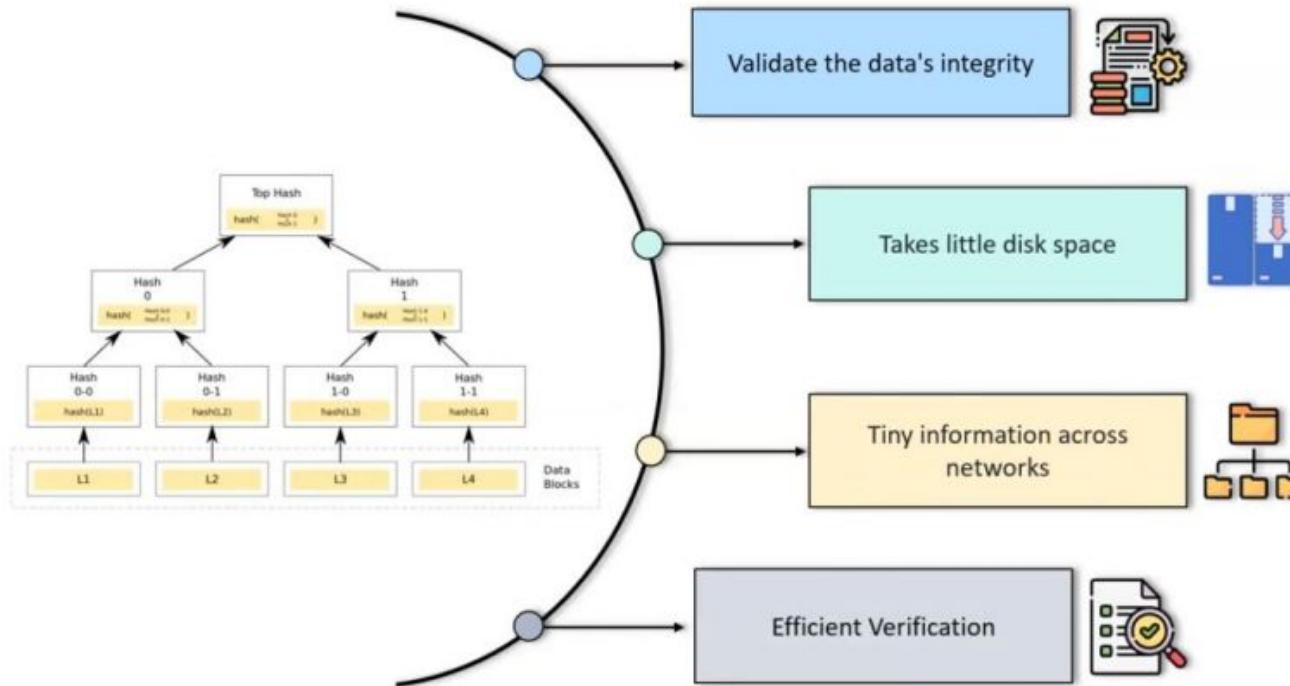
Hash AB

and

Hash CD

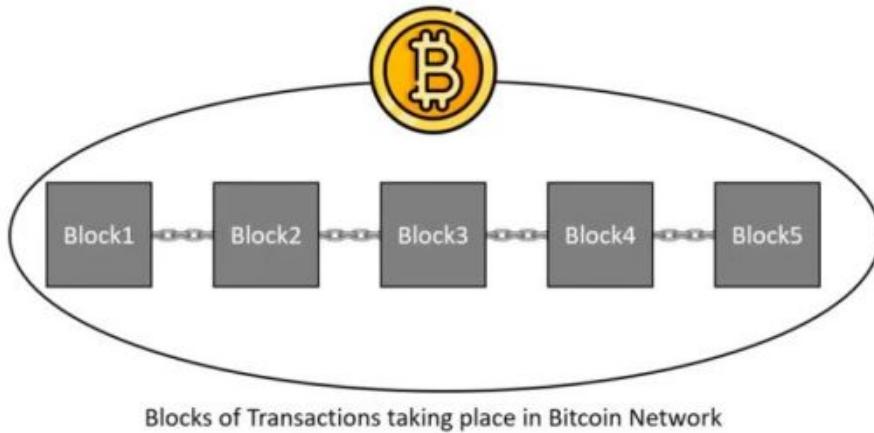
Our Merkle Root is formed by combining these two hashes: Hash ABCD.





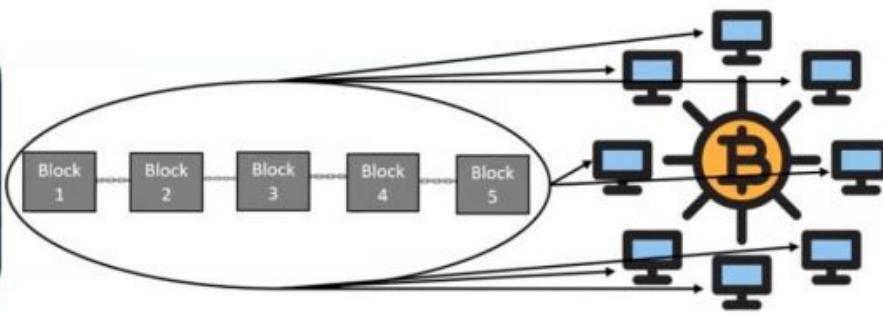
Why is it essential for Blockchain ?

Let's imagine a blockchain without Merkle Trees to get a sense of how vital they are for blockchain technology.



Why is it essential for Blockchain ?

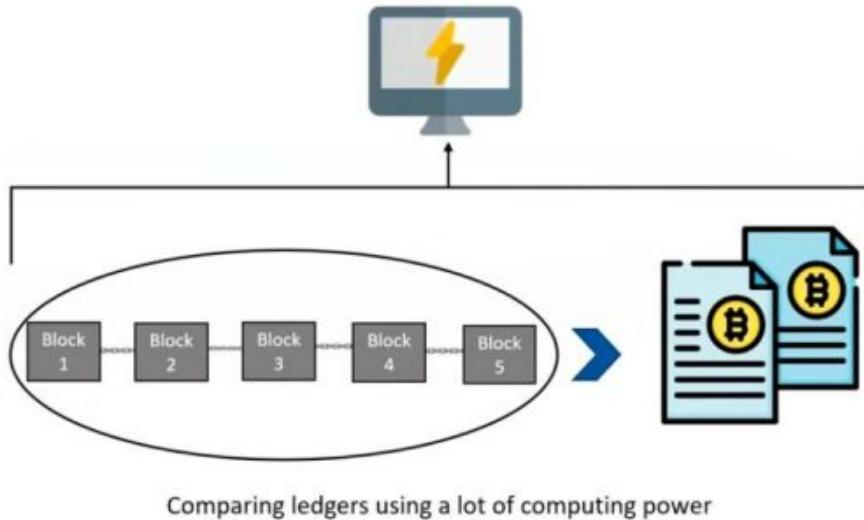
If Bitcoin didn't include Merkle Trees, for example, every node on the network would have to retain a complete copy of every single Bitcoin transaction ever made.



Too much information for every node to validate on their own

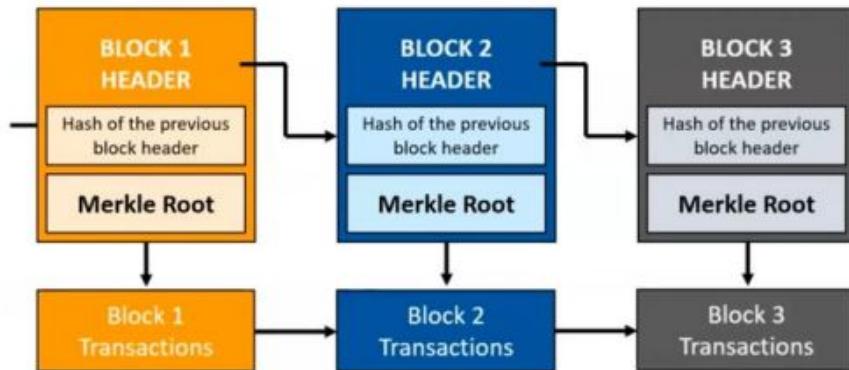
Why is it essential for Blockchain ?

To confirm that there were no modifications, a computer used for validation would need a lot of computing power to compare ledgers.



Why is it essential for Blockchain ?

Merkle Trees hash records in accounting, thereby separating the proof of data. Proving that given information across the network is all that is required for a transaction to be valid.



Merkle Tree breaking the data into tiny parts of information

Use cases of Merkle Tree



It is used in Git to handle projects by programmers from all around the world.

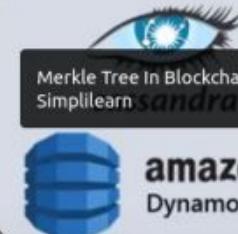


It's also open-source and implements Merkle Tree to allow computers to join and use a centralized file system.



It's part of the technique that generates verifiable certificate transparency logs.

RE VIDEOS



During the data

Merkle Tree In Blockchain | What Is The Merkle Tree In Blockchain | Merkle Tree In Blockchain | Simplilearn sandra

are used by these No-SQL distributed databases to control discrepancies.



Chapter 3

Introduction to Bitcoin

Priya R L

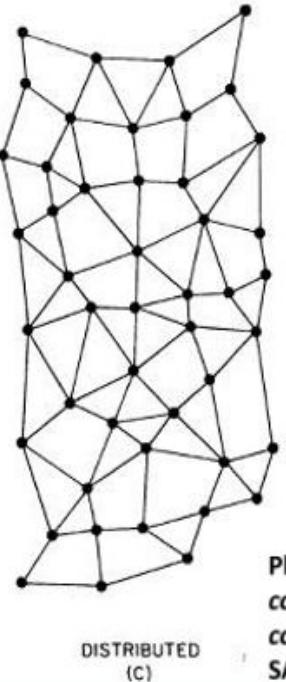
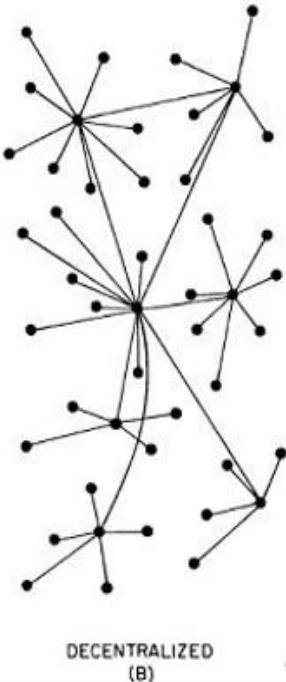
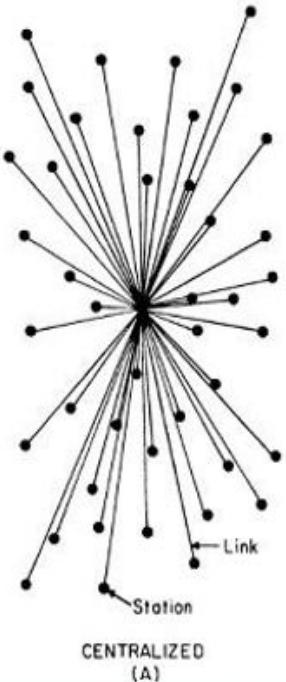
Department of Computer Engineering, VESIT, Mumbai

Blockchain Components

Blockchain is a system comprised of:

- Decentralized peers & Distributed Ledger
- Encryption processes
- Transactions
- Consensus mechanisms
- Optional Smart Contracts

Decentralized Peers



Complete reliance on single point (**centralized**) is not safe

- **Decentralized:** Multiple points of coordination
- **Distributed:** Everyone collectively execute the job

Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks*. No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.

Power of a distributed ledgers

The degree of trust between users determines the technological configuration of a distributed ledger.

It can be used without a central authority by individuals or entities with no basis to trust each other

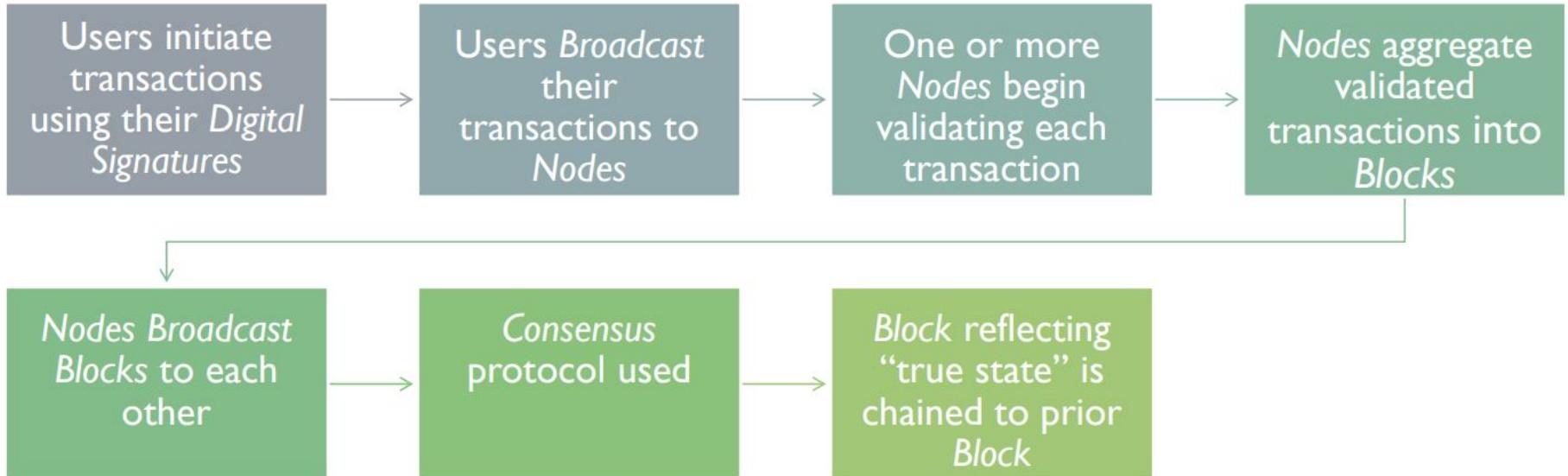
It can be used to create value or issue assets

It can be used to transfer value or the ownership of assets
A human being or a Smart Contract can initiate the transfer

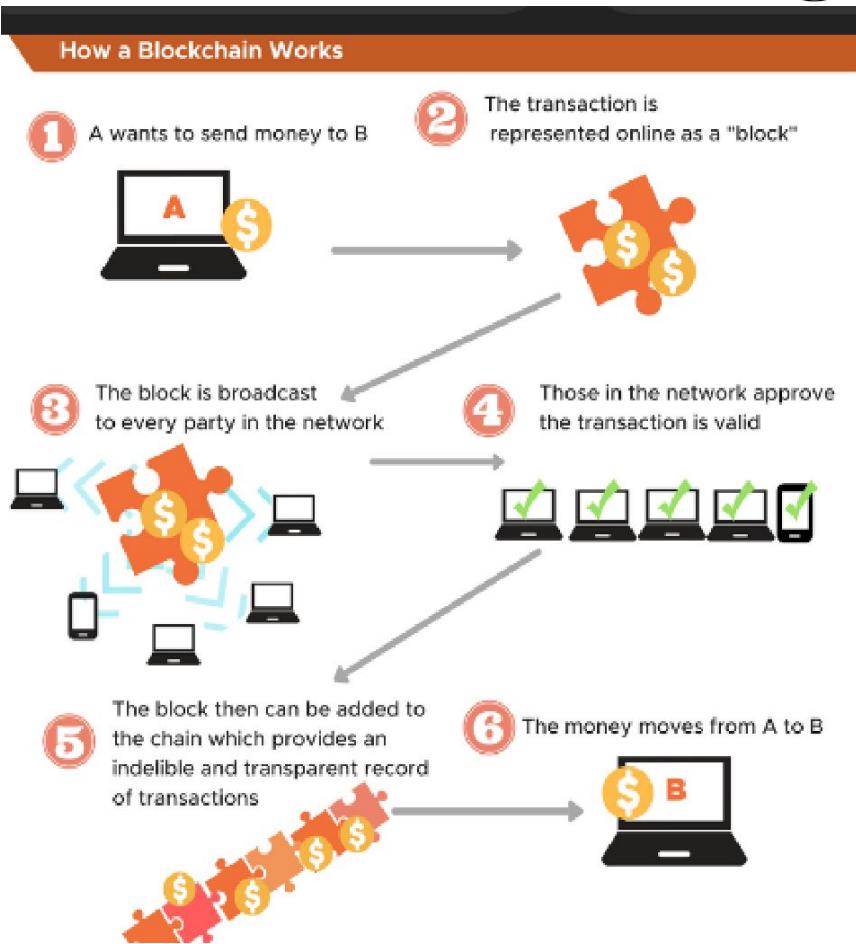
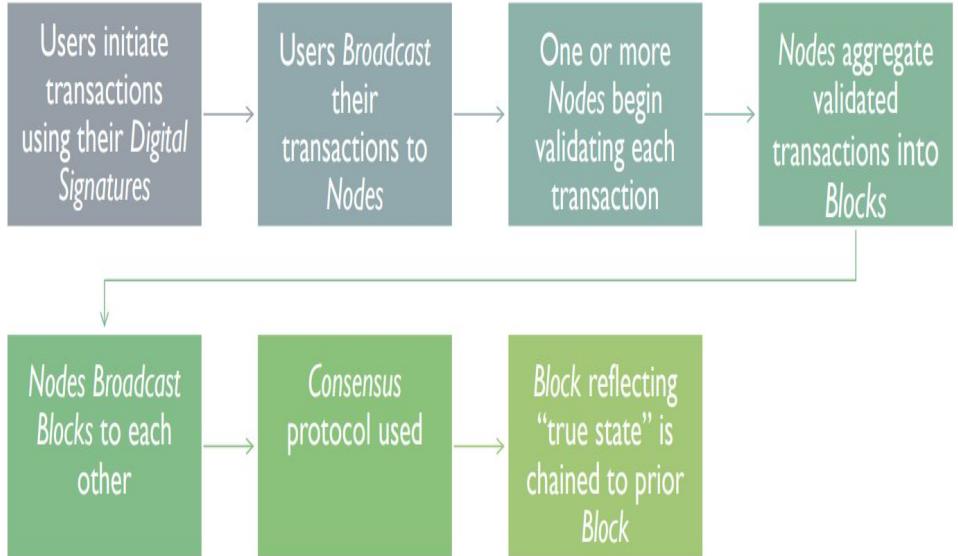
It can be used to record those transfers of value or ownership of assets
These records may be very difficult to alter, such that they are sometimes called effectively immutable

It can be used to allow owners of assets to exercise certain rights associated with ownership, and to record the exercise of those rights.
• Proxy Voting

How might a distributed ledger work?



How might a distributed ledger work?



Where might Blockchain use Cryptography?

*Initiation and Broadcasting
of Transaction*

- Digital Signatures
- Private/Public Keys

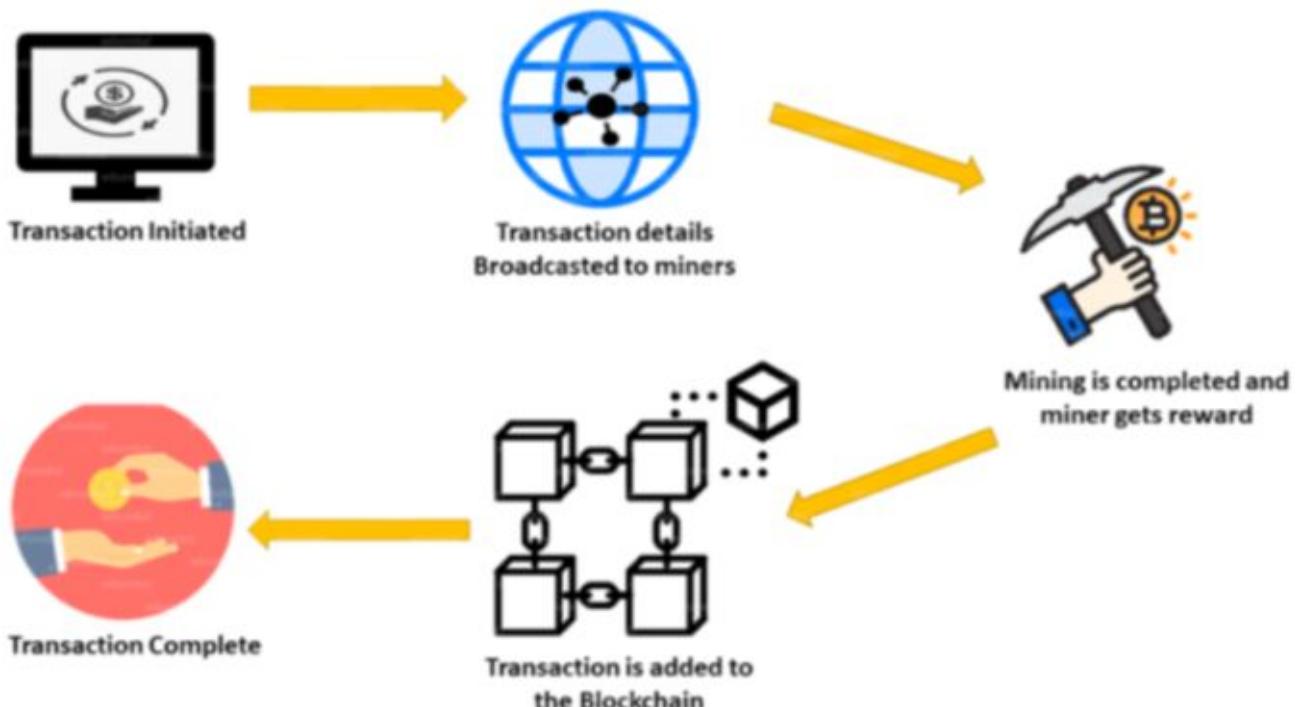
Validation of Transaction

- Proof of Work and certain alternatives

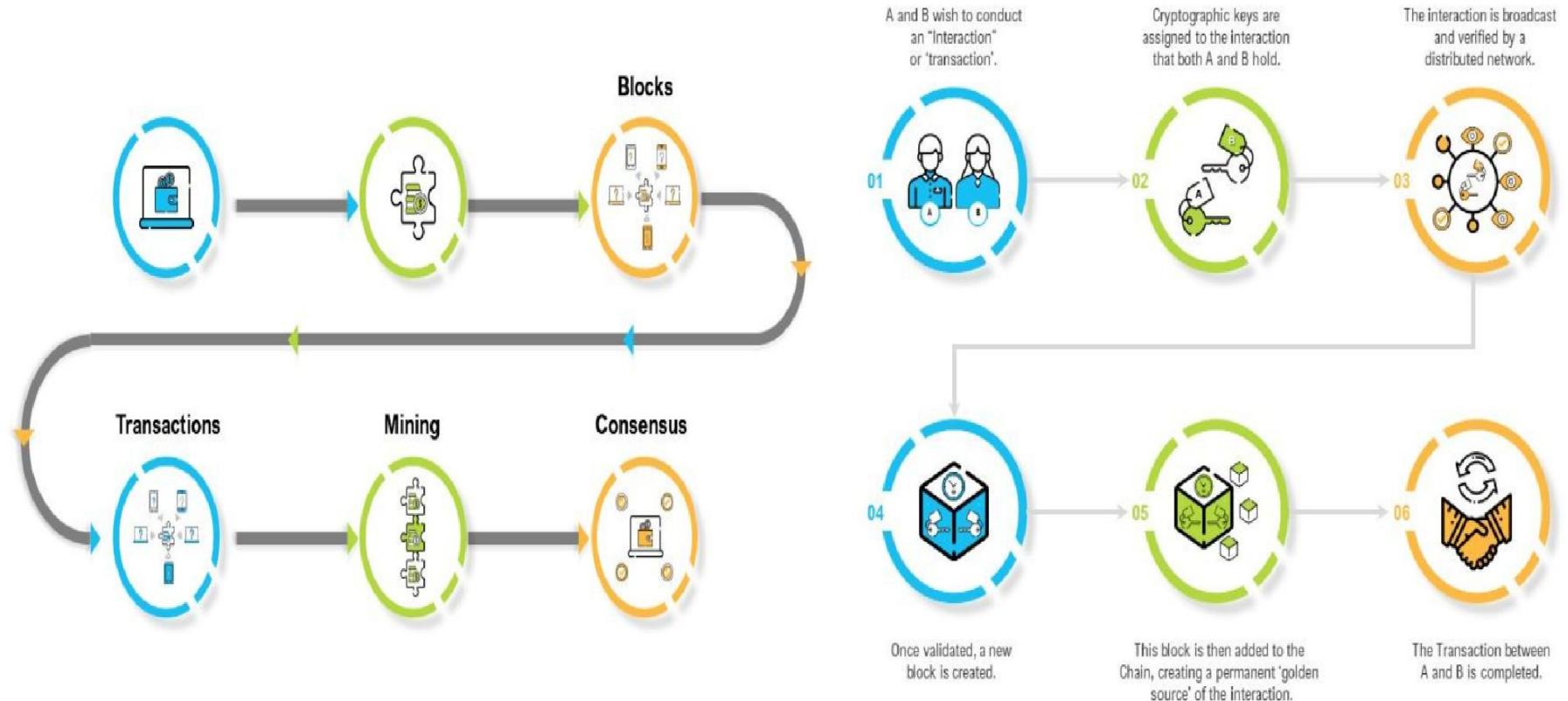
Chaining Blocks

- Hash Function

Miner and Mining



Transaction



Transaction Requirements

- one can directly transact with another person without involving a third party, like a bank, to verify and validate the transaction and thus avoiding the cost of mediation.
- Transaction is not backed and controlled by a central authority and can assure the value of the money is maintained
- There is transparency in transactions, while still maintaining the users' privacy

Solution: Cryptocurrency

Encryption Process : Cryptocurrency

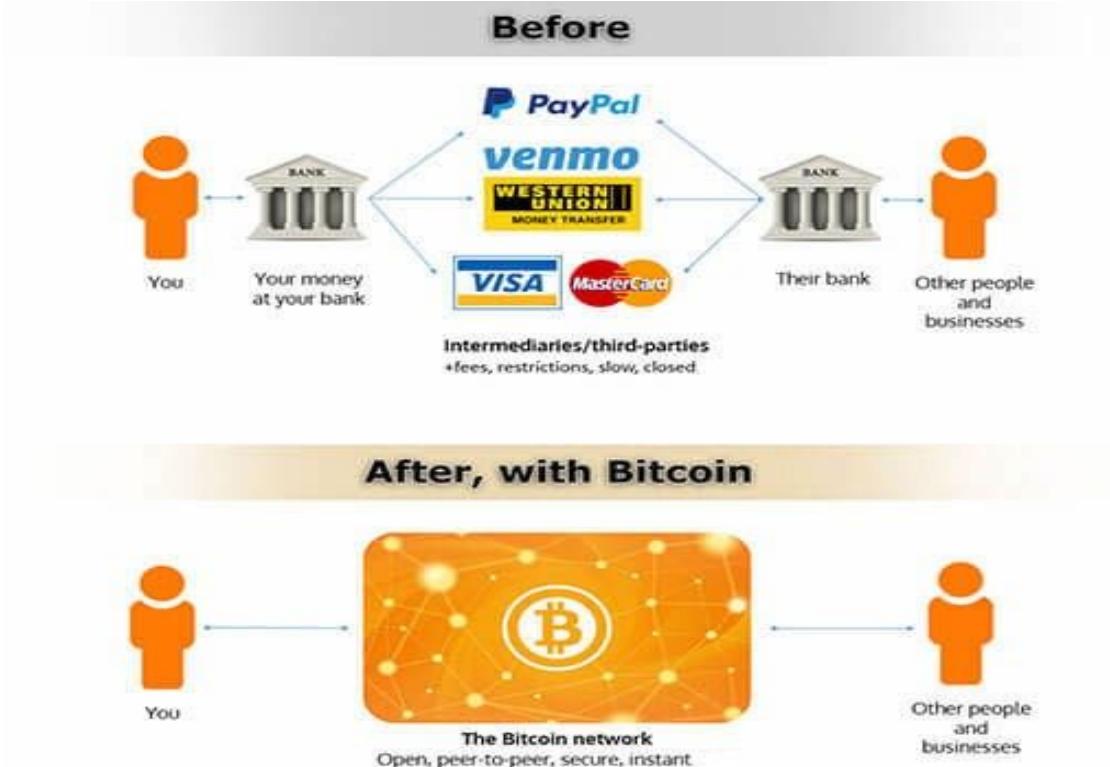
Cryptocurrency is an **internet-based medium of exchange** which uses **cryptographic functions** to conduct financial transactions.

- **Digital:**
 - Cryptocurrency **only exists on computers.**
 - There are no coins and no notes.
- **Decentralized:**
 - Cryptocurrencies **don't have a central computer or server.**
 - They are **distributed across a network** of (typically) thousands of computers.
 - Networks without a central server are called decentralized networks.
- **Peer-to-Peer:**
 - Cryptocurrencies are **passed from person to person online.**
 - **Users don't deal with each other** through banks, PayPal or Facebook. They deal with each other directly.

Encryption Process : Cryptocurrency

- **Pseudonymous:**
 - This means that **you don't have to give any personal information to own and use cryptocurrency.**
 - There are **no rules about who can own or use cryptocurrencies.**
- **Trustless:**
 - **No trusted third parties** means that **users don't have to trust the system for it to work.**
 - **Users are in complete control of their money and information at all times.**
- **Encrypted:**
 - user has **special codes that stop their information from being accessed by other users.**
- **Global:**
 - Cryptocurrencies **can be sent all over the world easily.**
 - Cryptocurrencies are **currencies without borders!**

Why Cryptocurrencies?



Cryptocurrencies other than Bitcoin

- Ethereum (ETH)
- Ripple (XRP)
- Litecoin (LTC)
- Tether (USDT)
- Bitcoin Cash (BCH)
- Libra (LIBRA)
- Binance Coin (BNB)

Bitcoin : Introduction

- Bitcoin is one of the **famous cryptocurrencies**.
- Bitcoin was found by **Satoshi Nakamoto**.
- Bitcoin is a **Peer-to-Peer Electronic cash system (2008)**
- Bitcoin is **not something physical**
- It is **easy to transport anywhere with low cost**
- **No third party (intermediary)**



Bitcoin : Introduction



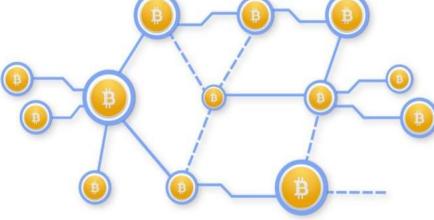
- It is a **decentralized digital currency without a central bank** that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.
- Transactions are **verified by network nodes** through **cryptography** and recorded in a public distributed ledger called a **blockchain**.
- Launched in **2009**, Bitcoin is the **world's largest cryptocurrency** by market cap.

Why Bitcoin is Popular?



- It was the only cryptocurrency
- It is **decentralised currency** (Regulate by users, not any bank)
- It **allow user to do transaction anonymously**
- It is **tax free** (No matter how many bitcoins you have)
- **Transfer fund easily at very low cost**; Worldwide

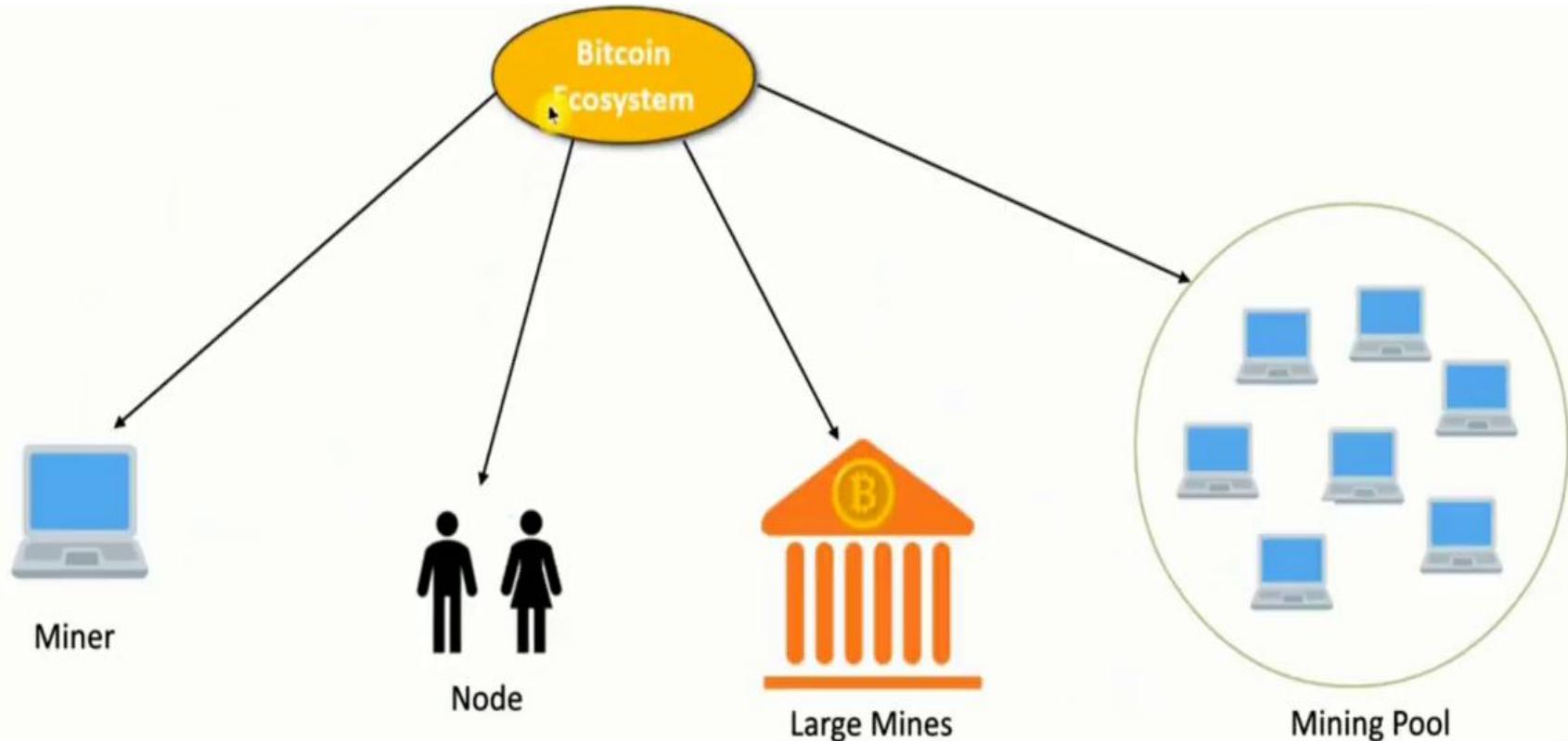
Why Bitcoin is Popular?



www.newsbtc.com

- Bitcoin network is public - Source code is open source
- Owner uses **private key** to spend bitcoins
- **Public ledger:** All bitcoin exchanges are visible to everyone on the network
- Transfer/Spending of coins require very little fee
- Transactions are validated by miners who get rewarded

Bitcoin Ecosystem



Elements of Bitcoin - A User's Perspective

- Digital keys and Addresses
- Transactions
- Blockchain
- Miners
- The Bitcoin network
- Wallets (client software)

Bitcoin - A User's Perspective

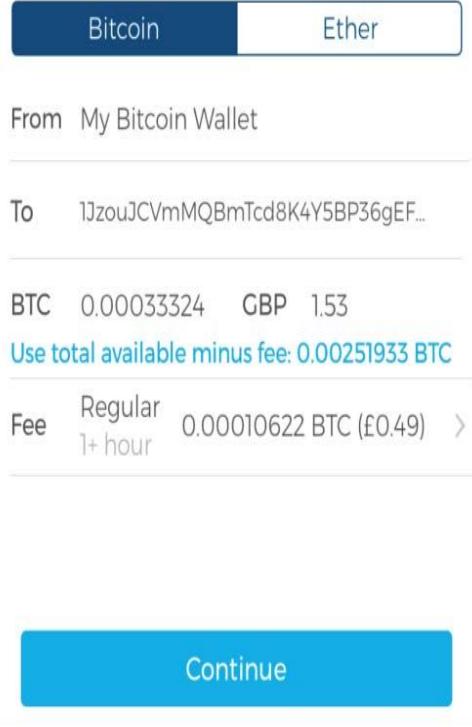


Please send 0.00033324 BTC to the Bitcoin address
1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3.

[bitcoin://
1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3?amount=0.00033324](bitcoin://1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3?amount=0.00033324)



The screenshot shows a mobile application interface for sending a Bitcoin payment. At the top, there are tabs for "BITCOIN" and "ETHER". Below the tabs, a message says "Tap to copy this address. Share it with the sender via email or text." In the center is a large QR code. Below the QR code, the recipient address is displayed: 1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3. Underneath the address, the amount is listed as "BTC 0.00033324". To the right of the amount is "USD 2". At the bottom of the screen is a large blue button labeled "REQUEST". Below the "REQUEST" button are icons for a smiley face, a house, a list, and a download arrow, followed by the word "Request".



The screenshot shows a transaction confirmation page. At the top, there are tabs for "Bitcoin" and "Ether", with "Bitcoin" selected. Below the tabs, the transaction details are shown: "From My Bitcoin Wallet" and "To 1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3...". The transaction amount is listed as "BTC 0.00033324 GBP 1.53". A note below the amount says "Use total available minus fee: 0.00251933 BTC". The transaction status is "Regular" and it is estimated to take "1+ hour". At the bottom of the screen is a large blue button labeled "Continue".

Bitcoin - denominations

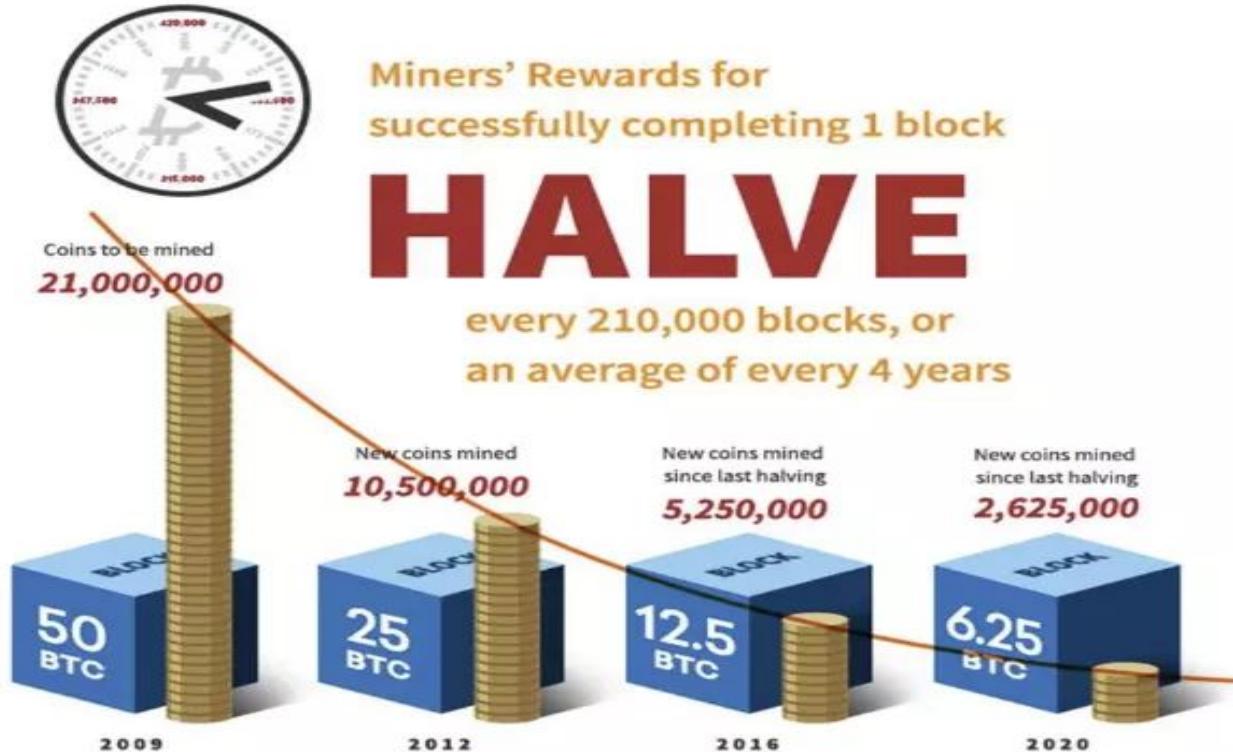
DENOMINATION	◆ ABBREVIATION	◆ FAMILIAR NAME	◆ VALUE IN BTC
Satoshi	SAT	Satoshi	0.00000001 BTC
Microbit	µBTC (uBTC)	Microbitcoin or Bit	0.000001 BTC
Millibit	mBTC	Millibitcoin	0.001 BTC
Centibit	cBTC	Centibitcoin	0.01 BTC
Decibit	dBTC	Decibitcoin	0.1 BTC
Bitcoin	BTC	Bitcoin	1 BTC
DecaBit	daBTC	Decabitcoin	10 BTC
Hectobit	hBTC	Hectobitcoin	100 BTC
Kilobit	kBTC	Kilobitcoin	1000 BTC
Megabit	MBTC	Megabitcoin	1000000 BTC



Bitcoin - Monetary Policy

- Digital Currency Regulation
- Demand-supply
- The Halving every 4-year or after 2,10,000 blocks.
- The Block Frequency

Bitcoin - The Halving



Bitcoin - Block Frequency

This states that **on an average** it will take 10 minute to create a new block.



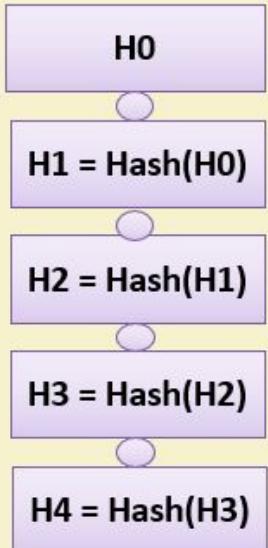
Structure of a Block

- A block is a **container data structure** that contains a series of transactions
- In Bitcoin: A block may contain more than 500 transactions on average, the average size of a block is around 1 MB (an upper bound proposed by Satoshi Nakamoto in 2010)
 - May grow up to 8 MB or sometime higher (as of March 2018)
 - Larger blocks can help in processing large number of transactions in one go.

Block Header (Reference: Bitcoin)

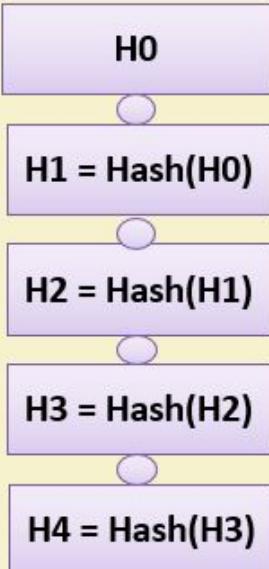
- Metadata about a block – (1) Previous block hash, (2) Mining statistics used to construct the block, (3) Merkle tree root

- **Previous block hash:** Every block inherits from the previous block – we use previous block's hash to create the new block's hash – make the blockchain **tamper proof**.



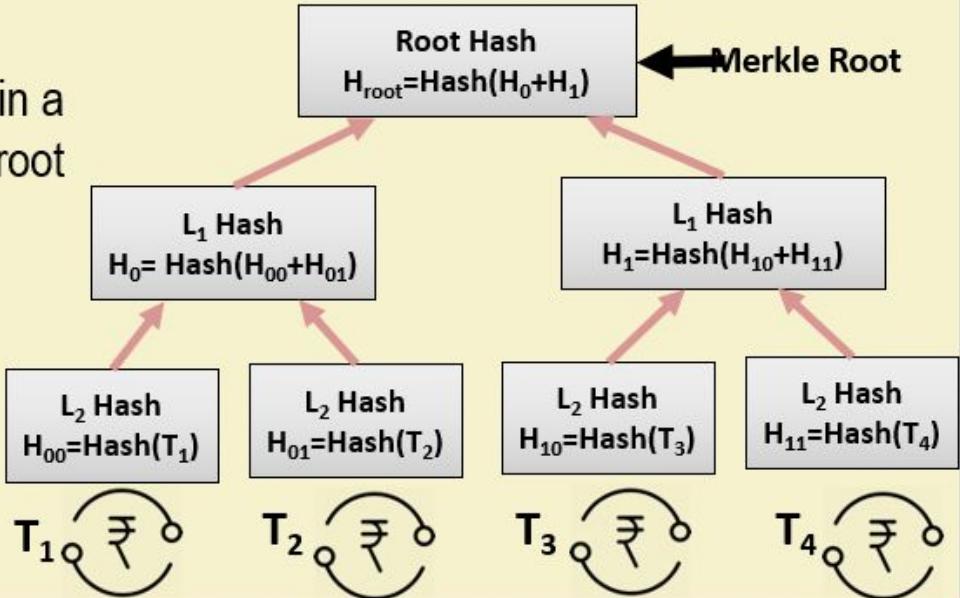
Block Header (Reference: Bitcoin)

- **Mining** – the mechanism to generate the hash
 - The mechanism needs to be complicated enough, to make the blockchain **tamper proof**
 - **Bitcoin Mining:** $H_k = \text{Hash}(H_{k-1} \parallel T \parallel \text{Nonce})$
 - Find the nonce such that H_k has certain predefined **complexity** (number of zeros at the prefix)
- The header contains mining statistics – timestamp, nonce and difficulty



Block Header (Reference: Bitcoin)

- **Merkle Tree Root:** The transactions are organized in a Merkle Tree structure. The root of the Merkle tree is a verification of all the transactions.



Transactions in a Block (Reference: Bitcoin)

- Transactions are organized as a Merkle Tree. The Merkle Root is used to construct the block hash
- If you change a transaction, you need to change all the subsequent block hash
- The **difficulty** of the mining algorithm determines the **toughness** of tampering with a block in a blockchain

Bitcoin Anonymity

- Bitcoin is permission-less, you do not need to setup any “account”, or required any e-mail address, user name or password to login to the wallet
- The public and the private keys do not need to be registered, the wallet can generate them for the users
- The **bitcoin address** is used for transaction, not the user name or identity

Bitcoin Anonymity

- A **bitcoin address** mathematically corresponds to a public key based on ECDSA – the digital signature algorithm used in bitcoin
- A sample bitcoin address: 1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz
- Each person can have many such addresses, each with its own balance
 - Difficult to know which person owns what amount

Transactions in a Block (Reference: Bitcoin)

Transactions

3f5ebfaf7fe18176cffeb973f4d609ba2d366bdb1755ddf464c93b5f7ba3d787		2017-12-20 20:02:40
No Inputs (Newly Generated Coins)	→	1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ Unable to decode output address
		19.69384324 BTC 0 BTC 19.69384324 BTC
717e4d969a2241065afe896986bf2b481ab5059d3dba901dc0c0f1fec796524		2017-12-20 20:00:14
3GsDfabsubnbrUSdm9oUedZJSPTnrevVvz	→	1H744xJpRVctkTU3jnQtXZg1JvbPfuorLS 2.96441546 BTC 2.96441546 BTC
8ce2ddfb236b3252c49fb3ad28c4a2584047de91643bc9724d272c91295423ee		2017-12-20 19:59:57
16oQyApVNxWkwyXZok9eHSKxYX57SHLgvV	→	1Dv56y3i1DzcD3nENAvkq4QR3eKdoGytbd 0.02983573 BTC 0.02983573 BTC

The Block in a Blockchain - Summary

- The Block contains two parts – **the header** and **the data (the transactions)**
- The header of a block connects the transactions – any change in any transaction will result in a change at the block header
- The headers of subsequent blocks are connected in a **chain** – **the entire blockchain needs to be updated if you want to make any change anywhere**

The Blockchain Replicas

- Every peer in a Blockchain network maintains a local copy of the Blockchain.

- Requirements

- 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**

Transactions using Bitcoin

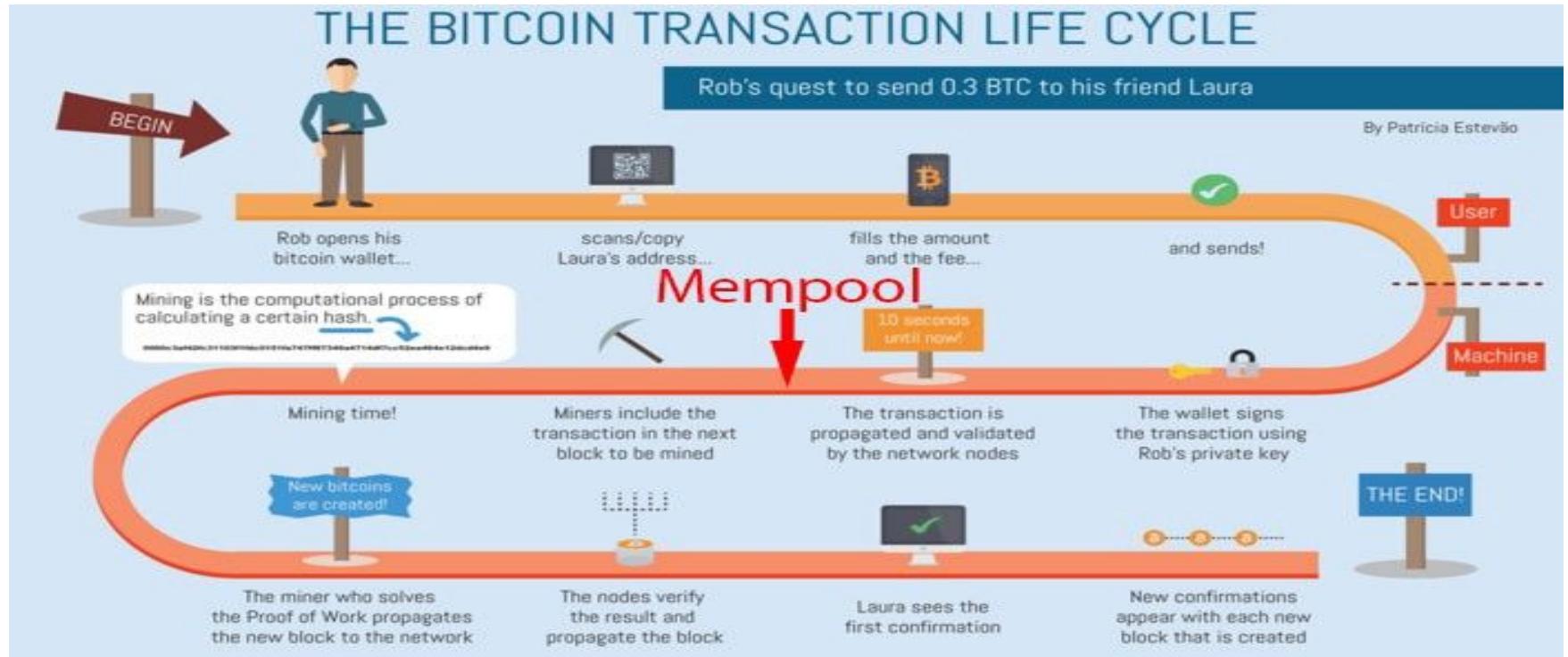


- Every transaction of bitcoin is **stored in a ledger called Blockchain**
- Every bitcoin user has a **copy of this ledger**
- Every transaction on Blockchain is **publicly visible** but **parties remain private**
- When a **transaction happens** it is **updated in the blockchain of all bitcoin users.**

CUTTING THE MIDDLEMAN



Bitcoin Transaction Lifecycle





Mempool



blockchain.com/btc/unconfirmed-transactions

Gmail YouTube Maps CSDF How to Setup... Ethical Hackin... Cloud Comput... Experts review... Other bookmark...

Blockchain.com Wallet Explorer Buy Bitcoin Trade

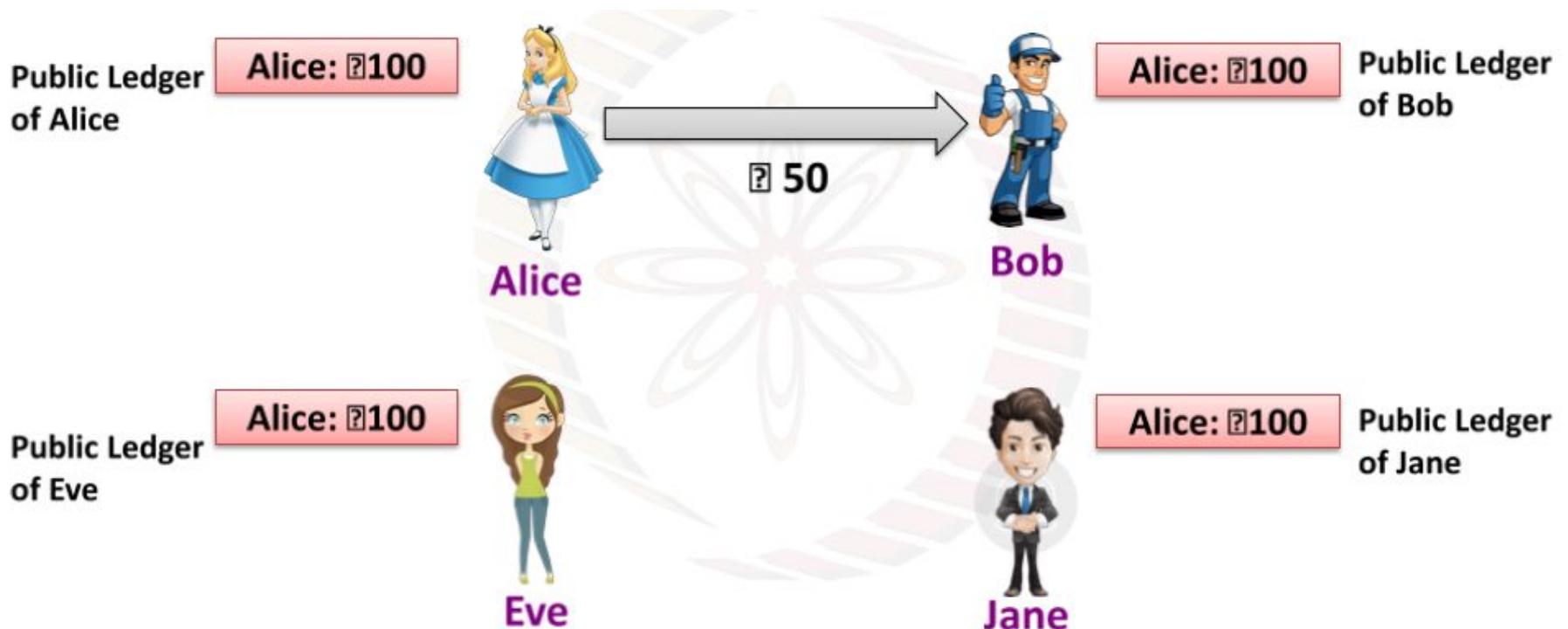
Home Prices Charts DeFi NFTs Academy Developers Assets

Explorer > Bitcoin Explorer > Unconfirmed Tx USD Search your transaction, an add ON OFF

Unconfirmed Transactions ⓘ

Hash	Time	Amount (BTC)	Amount (USD)
be20bef53006d458b987764a82645d3df34aab6d0759343b6eea2e1c7...	22:00	0.01565894 BTC	\$603.96
5a922399c16ffe760d638e2e17008b3e43eb636f0cc354ac7b8a27ebe2...	22:00	0.46999656 BTC	\$18,127.61
162c6919599aec9f6a9f6d922f1405ce266c9a50390a07d2f573224e36d...	22:00	0.00486940 BTC	\$187.81
d4aa7655f6382382d23f7717d27f0825ef8ef469384a8dead3e6c2b32ab...	22:00	0.36864630 BTC	\$14,218.56
b2ec966145a97cb619e10a72a5df47b0988239df8a6cd9c28951ae47a00...	22:00	0.00297423 BTC	\$114.72

Transactions using Bitcoin



Transactions using Bitcoin

Public Ledger
of Alice

Alice:	₹100
Alice -> Bob:	₹50



Alice



Bob

Public Ledger
of Bob

Alice:	₹100
Alice -> Bob:	₹50

Public Ledger
of Eve

Alice:	₹100
Alice -> Bob:	₹50



Eve



Jane

Public Ledger
of Jane

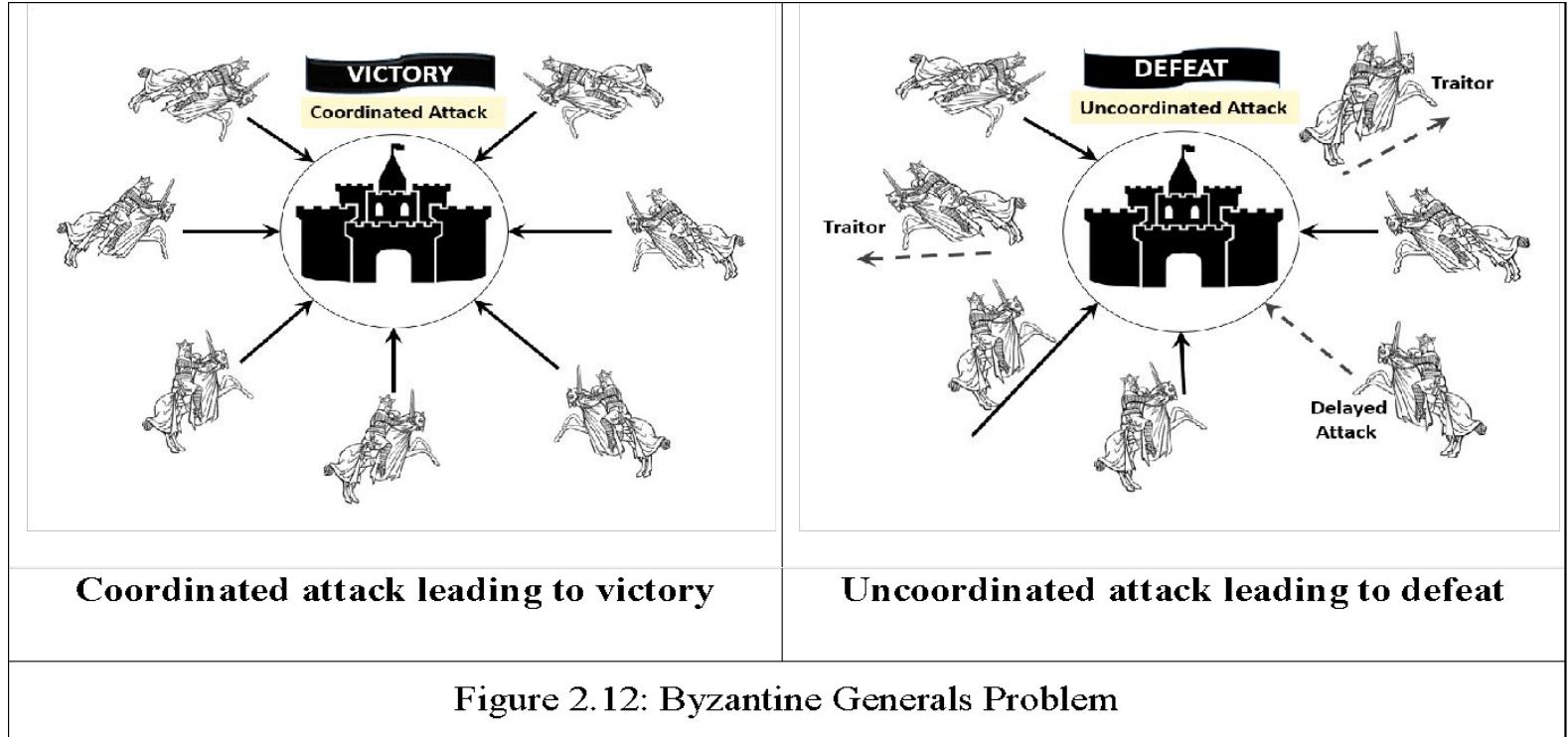
Cryptocurrency Wallets

- Cryptocurrency transaction can be done only using a **digital wallet**
- A digital wallet or **cryptocurrency wallet** is a software program that stores the user's private and public keys enabling the user to transact crypto assets.
- It is a **management system** that interacts with various users to send and receive digital currency and monitor their balance.
- Cryptocurrencies are stored **immutably on the blockchain using your public key**, i.e., your public key is used by other wallets to send funds to your wallet's address. However, the private key is required if you want to spend cryptocurrency from your address.

What is Consensus?

- As per Webster dictionary, a consensus is a **general agreement or opinion shared by all the people in a group.**
- A protocol is a **system of standard rules that are acceptable by all parties** to control the exchange of information in a network. Thus, a **consensus protocol** in Blockchain can be defined as **a set of rules and procedures for attaining a unified agreement (consensus) between the participating nodes** on the status of the network.
- The consensus protocol aims to overcome the classic problem of a **distributed computing system known as the Byzantine Generals Problem**

Byzantine General Problem



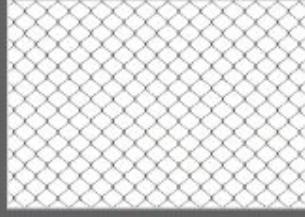
Objectives of Consensus Protocol

1



Unified
Agreement

2



Fault Tolerant

3



Collaborative
and Participatory

4



Egalitarian

5



Incentivisation

6



Prevent Double-Spend

BUILDING CONSENSUS



After a finite time, all participants agree on a single state.

E.g. on who owns how many Bitcoin.

CREATING WITNESSES



If something is published on a public blockchain, all participants become witnesses.

This is used, for example, by OriginStamp to create a secure timestamp for documents.

Different Consensus Algorithms

1. Proof of Work (PoW)
2. Proof of Elapsed Time(PoET)
3. Proof of Stake (PoS)
4. Delegated Proof of Stake (DPoS)
5. Proof of Authority (PoA)
6. Practical Byzantine Fault Tolerance
7. RAFT

Other Consensus Algorithms

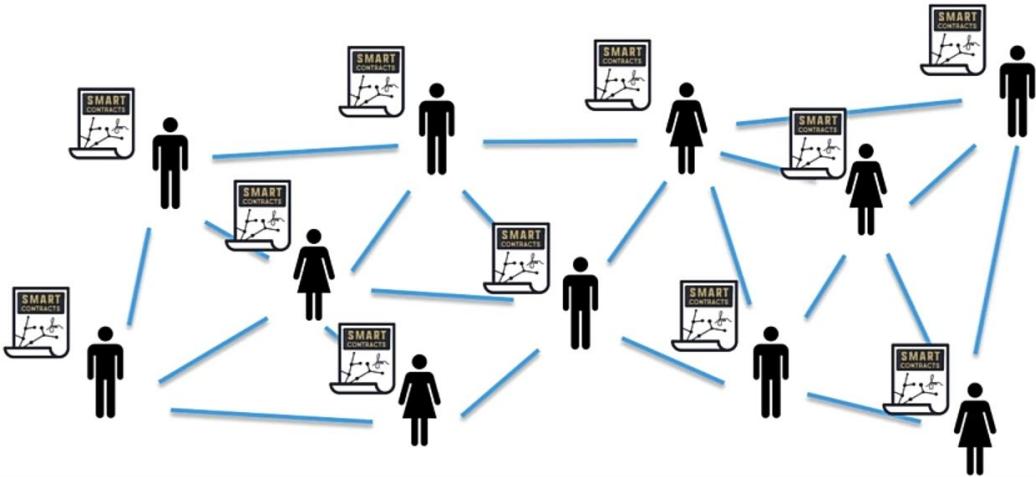
1. Proof of Stake Anonymous (PoSA):
2. Leased Proof of Stake (LPoS):
3. Proof of Importance (PoI):
4. Proof of Storage
5. Proof of Burn
6. Proof of Activity
7. Proof of Capacity
8. Directed Acyclic Graph (DAG)

What is a Smart Contract?



Each Node has:

1. History of all smart contracts
2. History of all transactions
3. Current state of all smart contracts



Some Application of Hashing..

- Password storage
- To generate Digital signature
- Integrity check

Application of hashing in Blockchain

- Consider following transactions recorded in a diary of Bob:

- Ann gave 3 coins to Mary
- Mary gave 5 coins to Jack
- Jack gave 3 coins to Ann
- Ann gave 1 coin to Adam
- ...

Application of hashing in Blockchain

- Let's say Jack wants to steal money. With this intention, he makes some changes in the transactions in the diary

-

1. Ann gave 10 coins to Mary
2. Mary gave 5 coins to Jack
3. ~~Jack~~ Mary gave 3 coins to Ann
4. Ann gave 1 coin to Adam
5. ...

- However, Bob notices this change. To prevent this from happening, he decides to use hashing.

Application of hashing in Blockchain

- So after each record of transaction he now enters the hash value.

6. Ann gave 10 coins to Mary
cff4e860bd57c2fb7c010927c3f6fee

7. Mary gave 5 coins to Jack
803c28370e9a16e628a23d46d3ebe711

Application of hashing in Blockchain

- Jack is smart !!

6. Ann gave 10 coins to Mary
cff4e860bd57c2bfb7c010927c3f6fee

7. Mary gave ~~5~~ 8 coins to Jack
~~803c28370e9a16e628a23d46d3eb711~~
4ae41f8cc3d4cc905f664c75ceab9da0

Application of hashing in Blockchain

- Bob wants to make life of attacker complex!!
- New hash = (Record + previous hash)

Input	Hash
Ann gave 10 coins to Mary	8977e7c112aeasboa62e9csf3084a203
Mary gave 5 coins to Jack 8977e7c112aeasboa62e9csf3084a203	e37a8d1cc39ed9f54afadb6c6cafe639
Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639	5b9foe325fs8766fsa2dfe7eec636f6d
Ann gave 1 coin to Adam 5b9foe325fs8766fsa2dfe7eec636f6d	55f28e65412b22aa3d6002bcf7d67201

- Jack is hardworking too!!

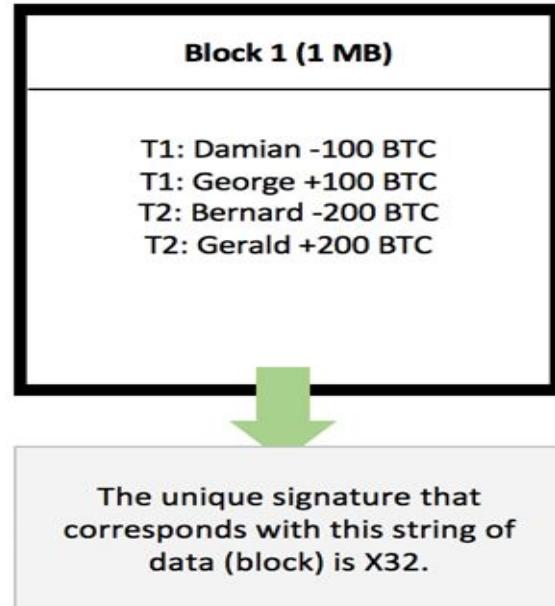
Hashing + Nonce

- Bob uses Nonce!!
- Nonce (random Number – Number used only once)

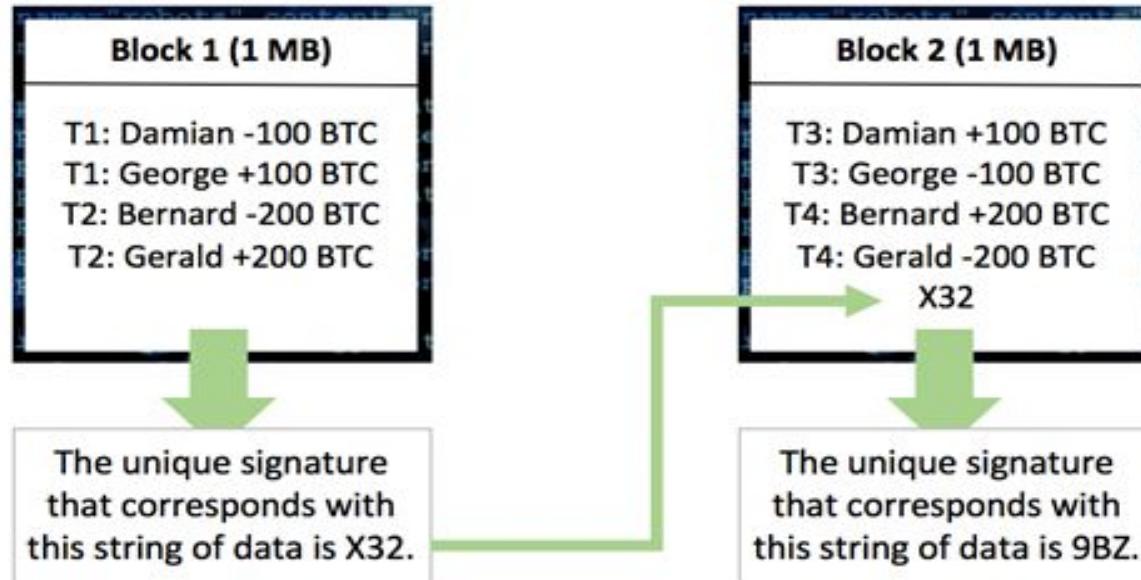
Input	Hash
Ann gave 10 coins to Mary 451 219711e62645a21f2742ada2c6f2a900	219711e62645a21f2742ada2c6f2a900
Mary gave 5 coins to Jack 13 1cc4c07fa0757848b439e2361ce87d00	1cc4c07fa0757848b439e2361ce87d00
Mary gave 3 coins to Ann 467 1cc4c07fa0757848b439e2361ce87d00	e43a132f4b67c65ba6914824a39b3900
Ann gave 1 coin to Adam 56 e43a132f4b67c65ba6914824a39b3900	99012fe16897c19465941d5350afa900

Hashing and Digital Signature in Blockchain & Generic terms used in Blockchain

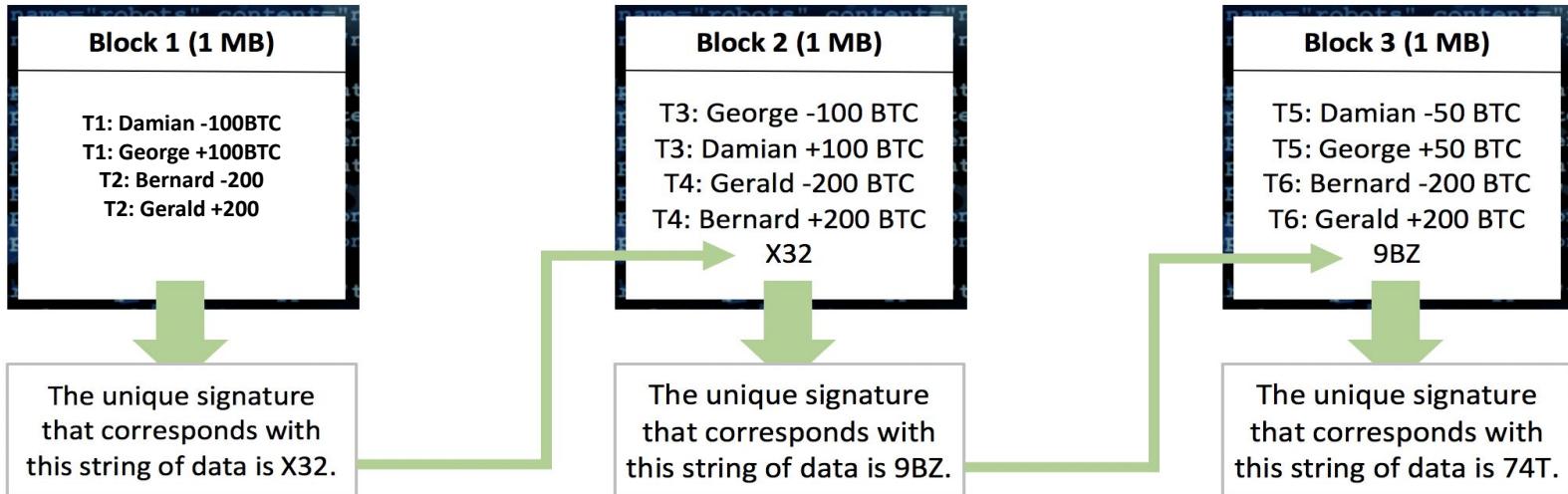
Hashing in Blockchain- 1st Block



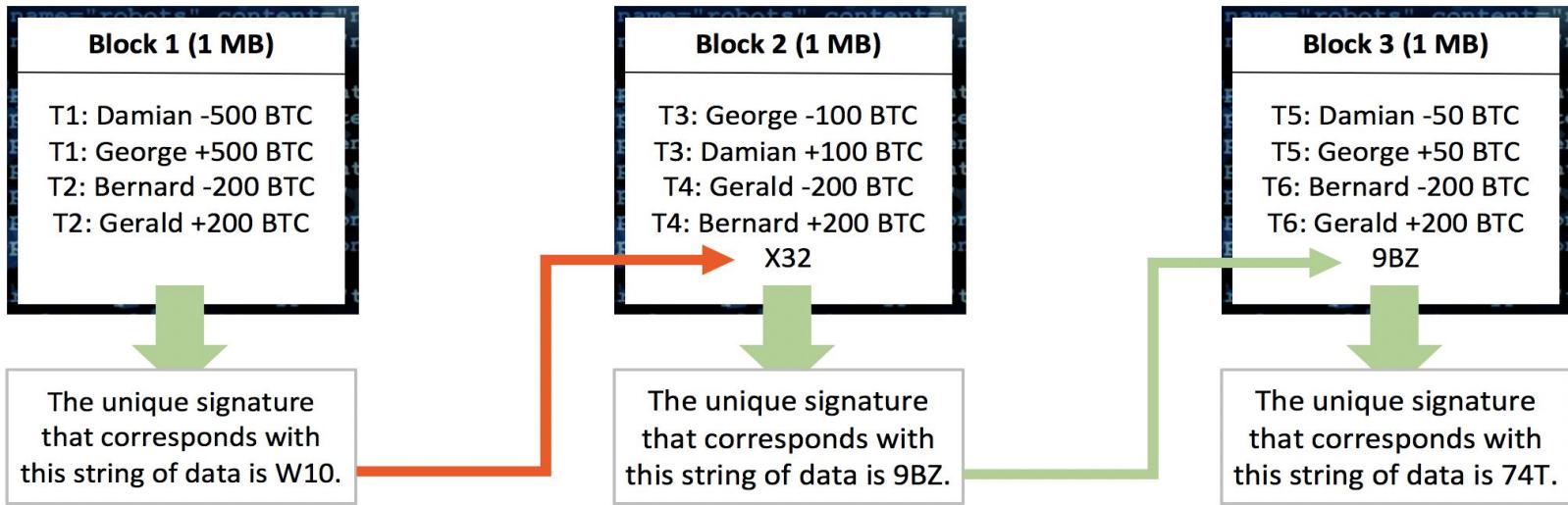
2nd Block of transaction added



3rd Block of transaction added



What if block 1 is altered..



Error propagates in Block 2

Error propagates to Block 3 and so on..

