Chapter 1 : Introduction to Blockchain

Priya R L, Lifna C S

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
- Applications of Hashing in Blockchain

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 ?

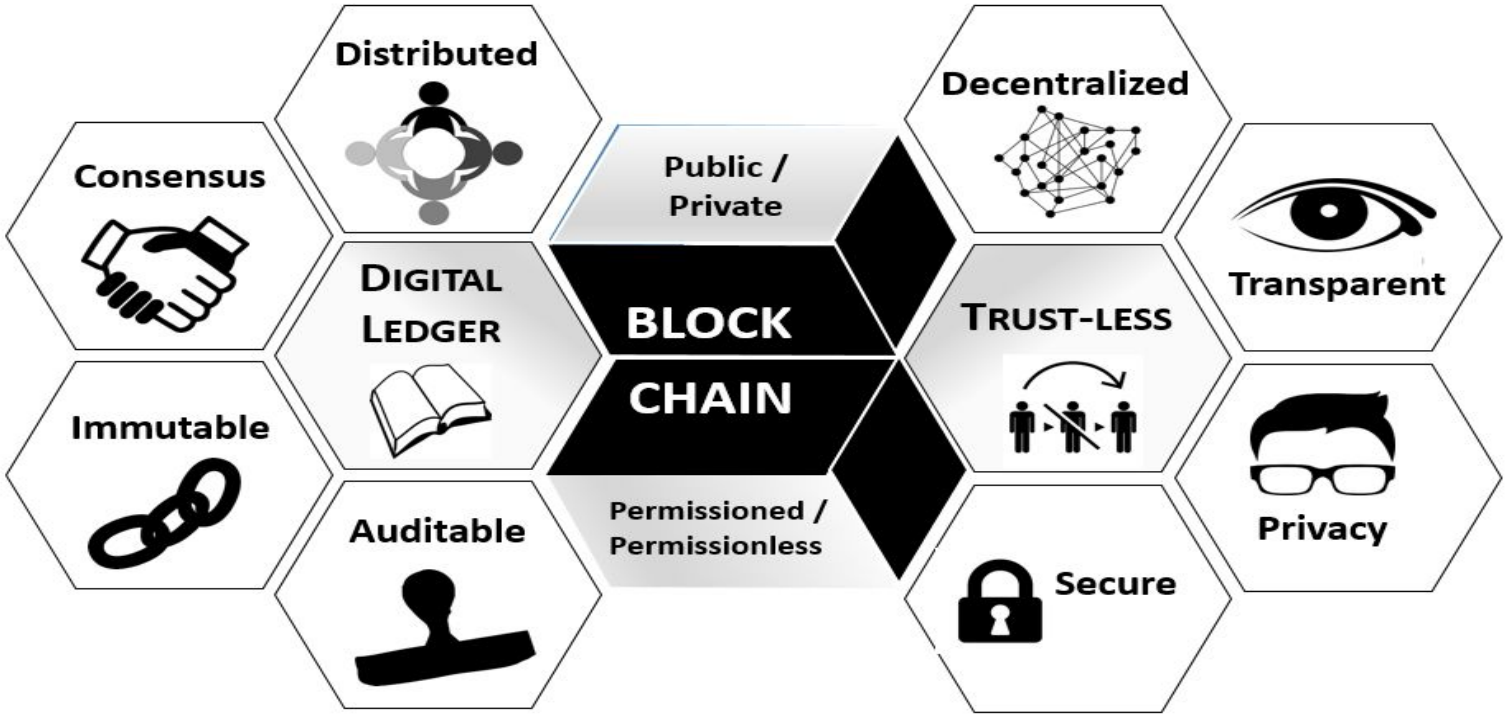
- Though the terms **‘Bitcoin’ and ‘Blockchain’** are often used to interchangeably, they are not the same. Blockchain is the underpinning technology that the Bitcoin was built on.

- Blockchain acts as Bitcoin’s ledger and maintains all the transactions of bitcoin.

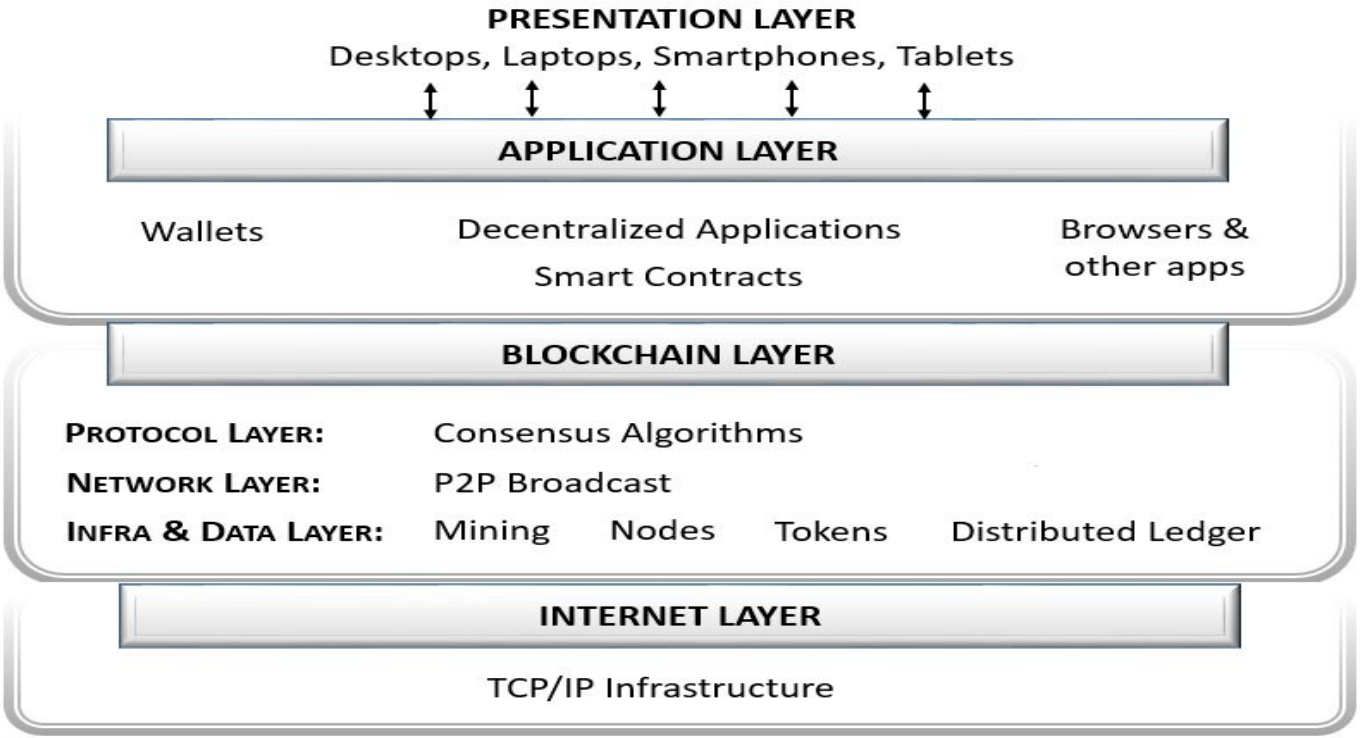
Key features of Blockchain

- 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



Blockchain Layers

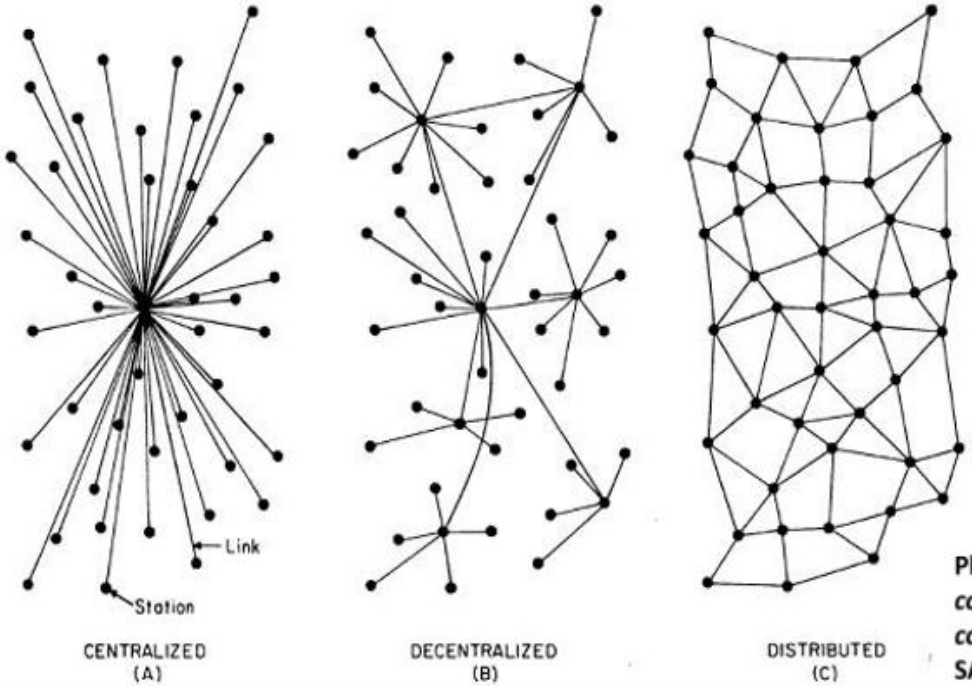


Blockchain Components

Blockchain is a system comprised of:

- Transactions
- Decentralized peers
- Encryption processes
- Consensus mechanisms
- Optional Smart Contracts

Decentralized Peers

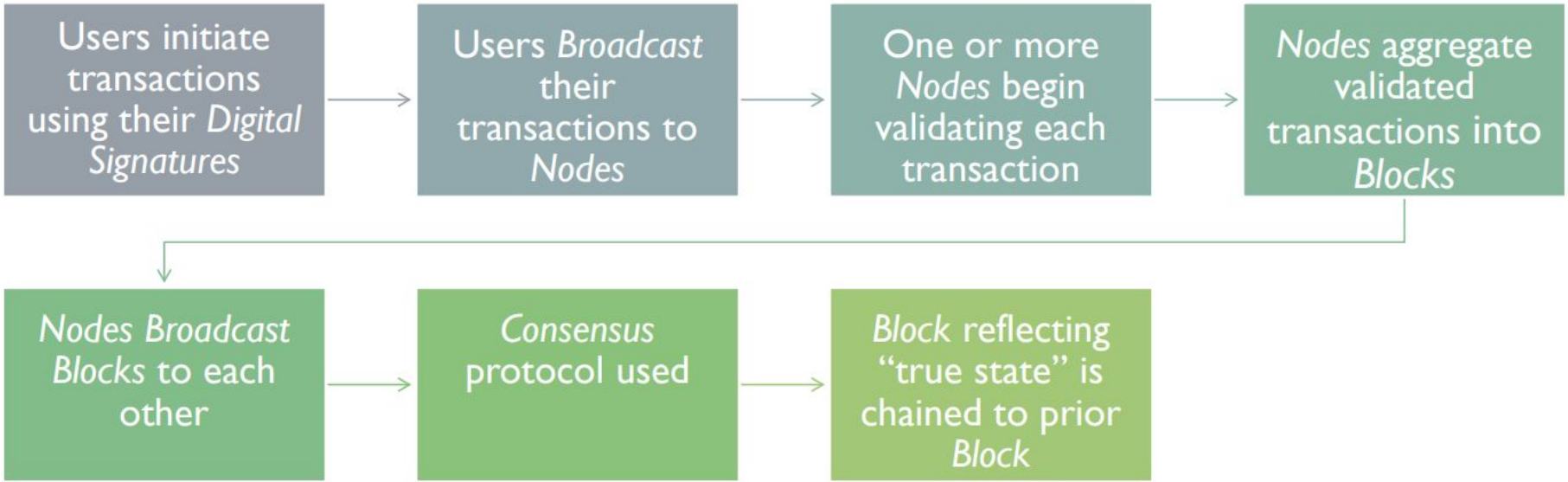


Complete reliance on single point (centralized) is not safe

- 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.

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

The Block in a Blockchain - Securing Data Cryptographically

- Digitally signed and encrypted transactions **verified by the peers**
- **Cryptographic security** – Ensures that participants can only view information on the ledger that they are authorized to see

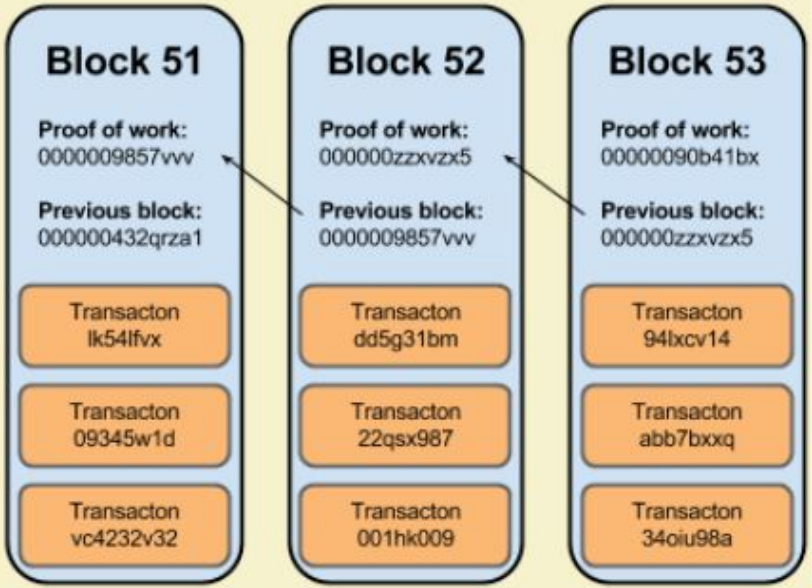


Image source: http://dataconomy.com/

Structure of a Block

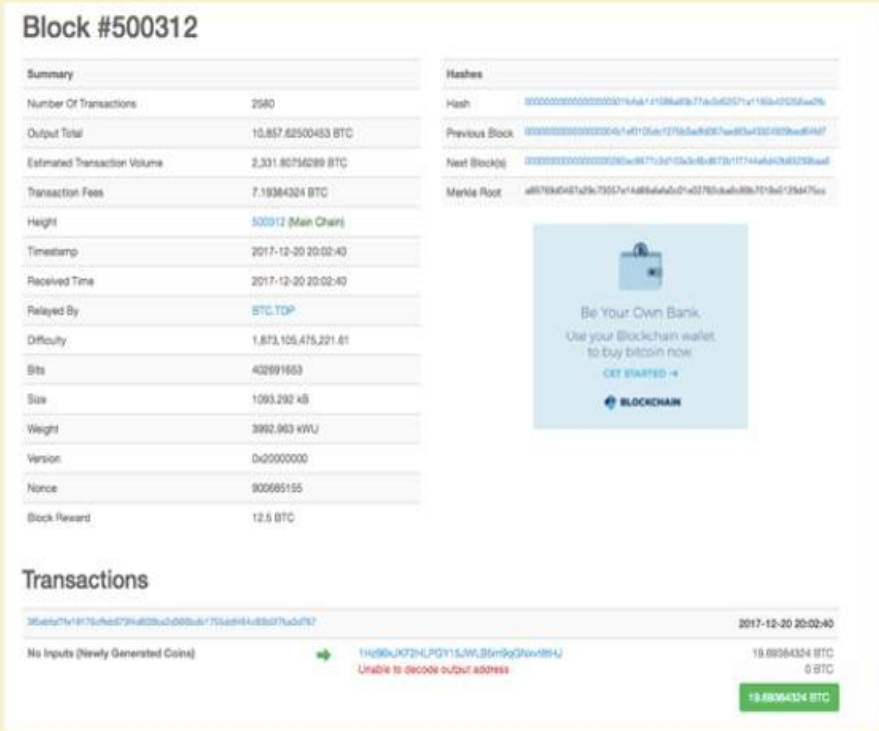
- A block is a **container data structure** that contains a series of transactions

- **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.

Structure of a Block (Reference : Bitcoin)

- Two components:
  - Block Header
  - List of Transactions

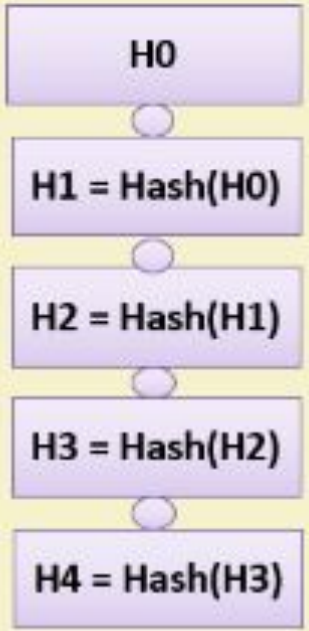
k Source:



Block Header (Reference : Bitcoin)

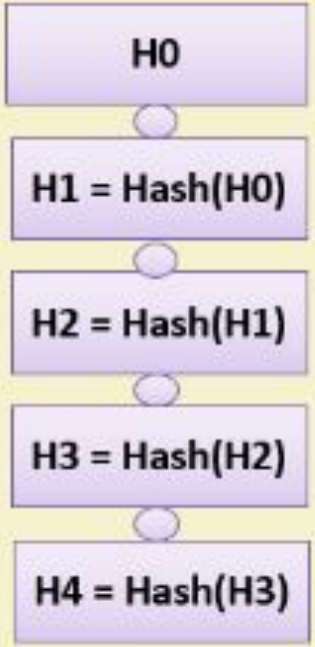
- Metadata about a block – (1) Previous block hash, (2) Mining statistics used to construct the block, (3) Merkle tree root

- **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**.



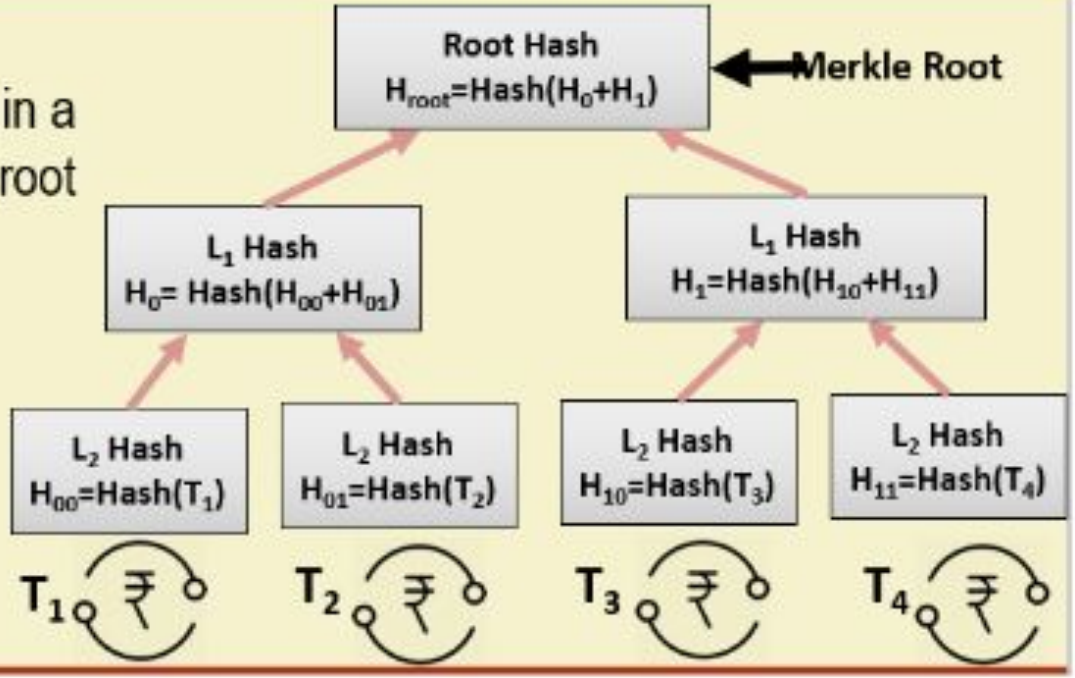
Block Header (Reference : Bitcoin)

- **Mining** – the mechanism to generate the hash
  - –The mechanism needs to be complicated enough, to make the blockchain **tamper proof**
  - –**Bitcoin Mining:** $H_k = Hash(H_{k-1} \| T \| Nonce)$
  - –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.



Block Header (Reference : Bitcoin)

Summary	
Number Of Transactions	2580
Output Total	10,857.62500453 BTC
Estimated Transaction Volume	2,331.80756289 BTC
Transaction Fees	7.19384324 BTC
Height	500312 (Main Chain)
Timestamp	2017-12-20 20:02:40
Received Time	2017-12-20 20:02:40
Relayed By	BTC.TOP

Difficulty	1,873,105,475,221.61
Bits	402691653
Size	1093.292 kB
Weight	3992.963 kWU
Version	0x20000000
Nonce	900685155
Block Reward	12.5 BTC

Block Source: https://blockchain.info/

The Hashes in a Block Header (Reference : Bitcoin)

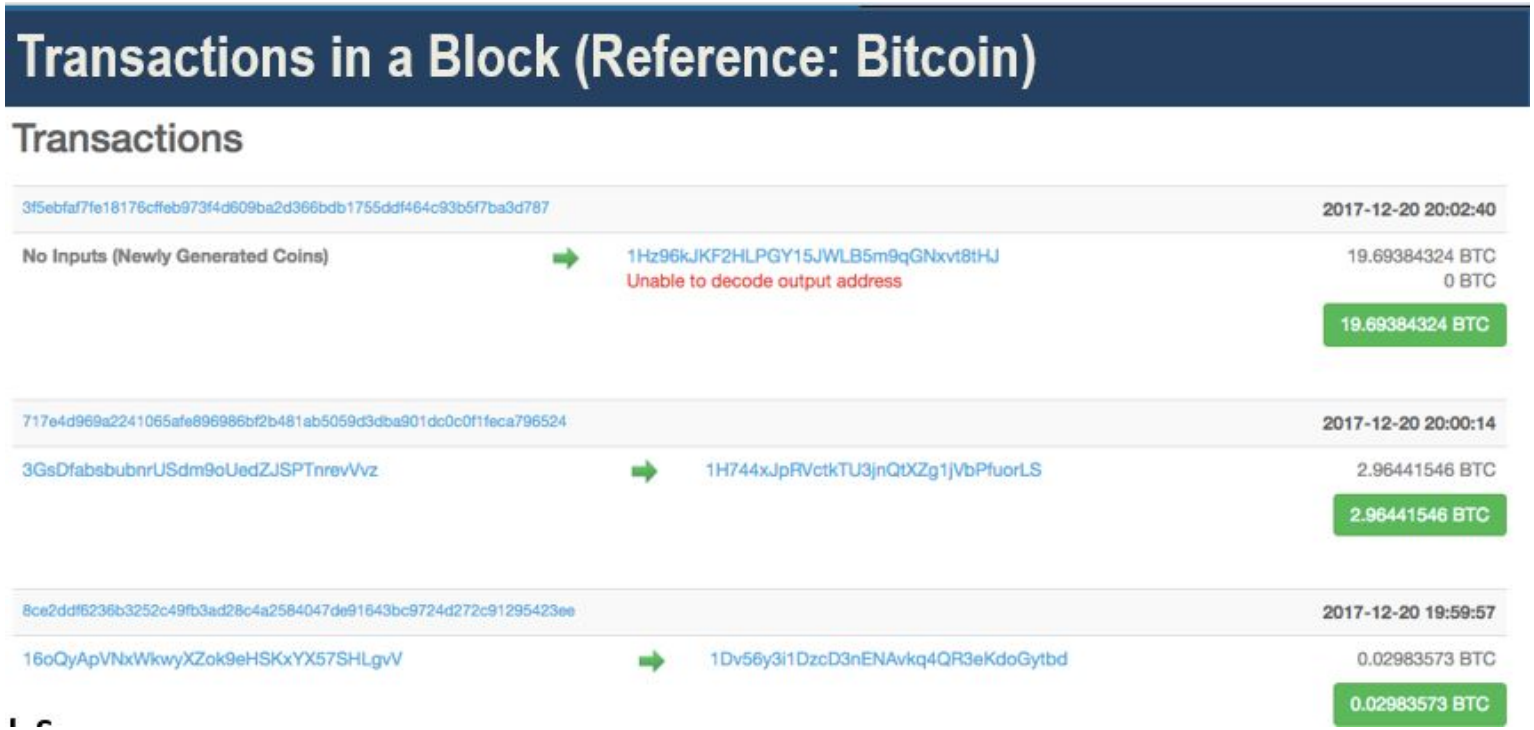
Hashes	
Hash	00000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb
Previous Block	00000000000000000004b1ef0105dc1275b3adfd067aed63a43324929bed64fd7
Next Block(s)	00000000000000000282ac9977c3d103a3c6bd873b1f7744e8d42b83239baa6
Merkle Root	a89769d0487a29c73057e14d89afafa0c01e02782cba6c89b7018e5129d475cc

- Block identifier – the hash of the current block header (Hash algorithm: Double SHA256)
- Previous block hash is used to compute the current block hash

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

Transactions in a Block



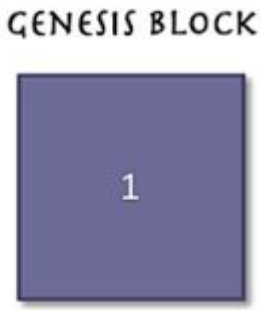
Block in a Blockchain : Summary

- 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**

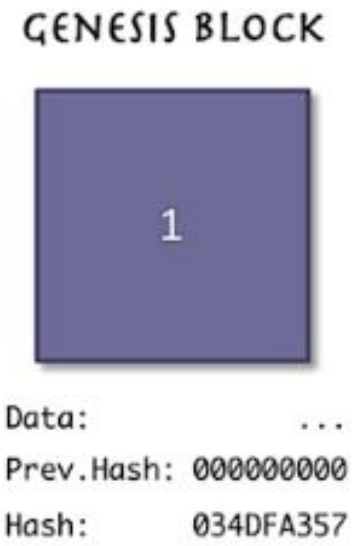
Blockchain Replicas

- 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**

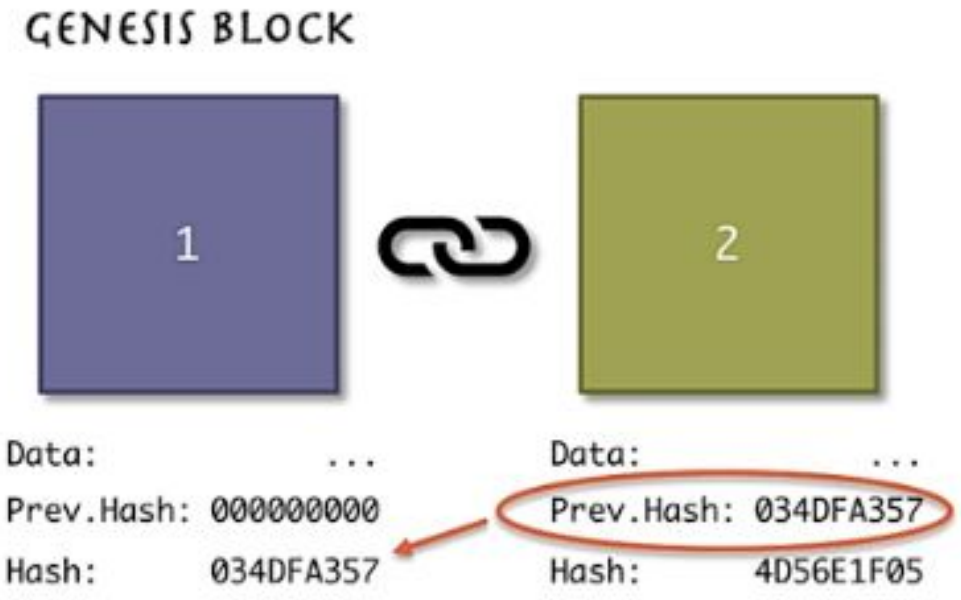
What is a Genesis Block?



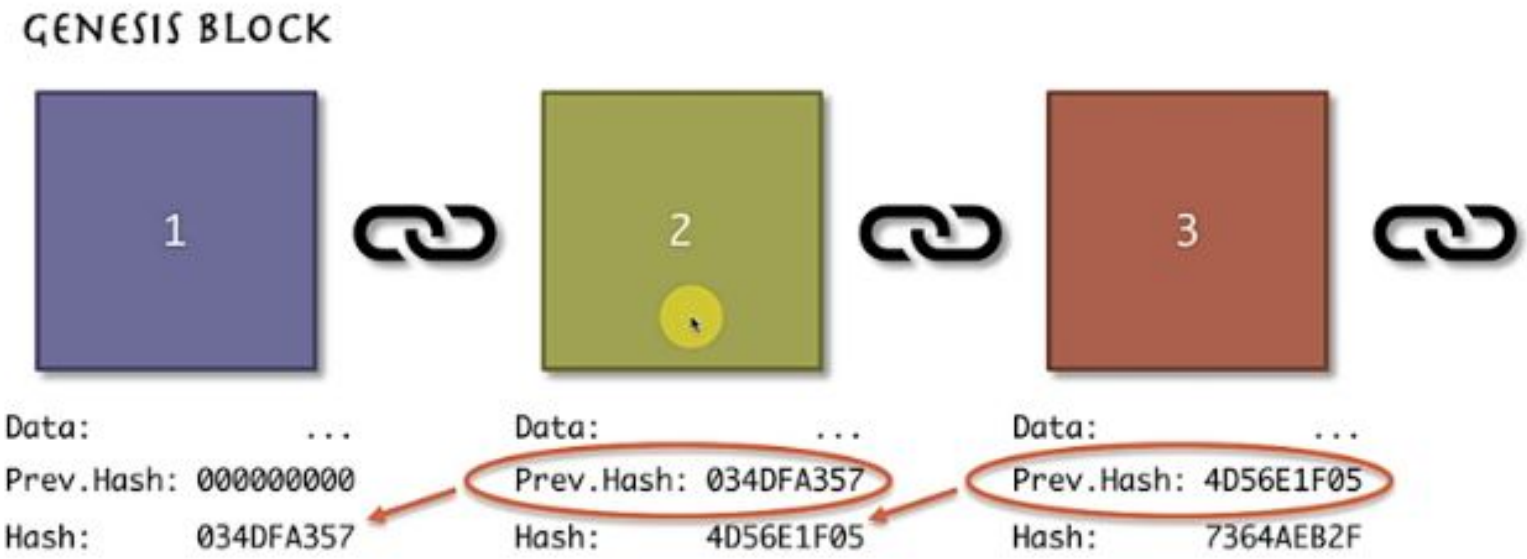
What is a Blockchain?



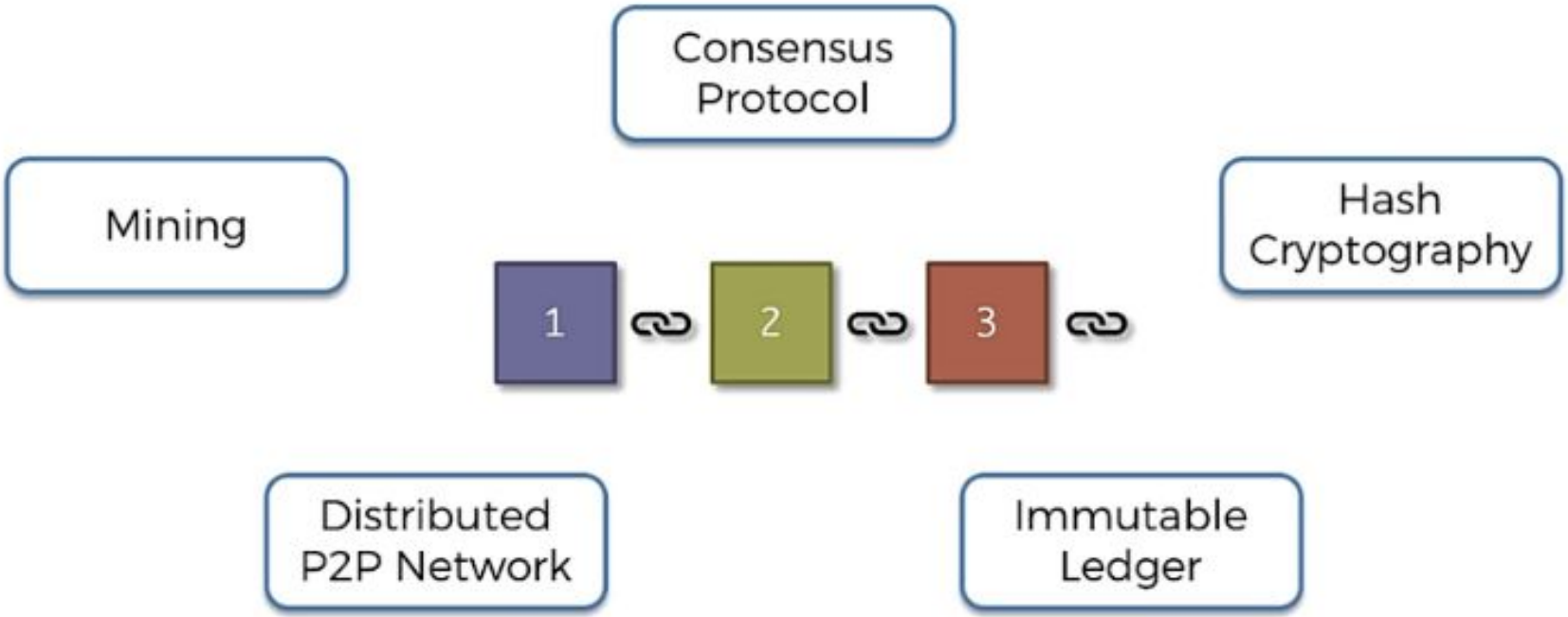
Linking Blocks in a Blockchain



Linking Blocks in a Blockchain



Blockchain

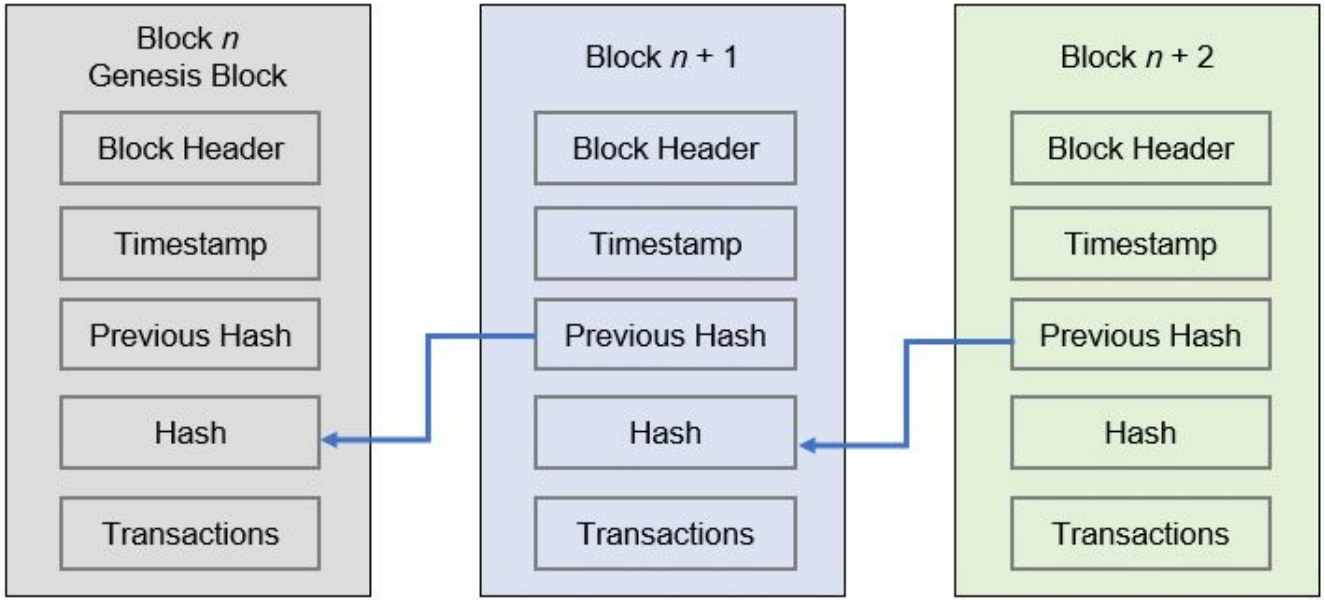

Consensus Protocol
Mining
Hash Cryptography
1
2
3
Distributed P2P Network
Immutable Ledger

What is a Block?

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

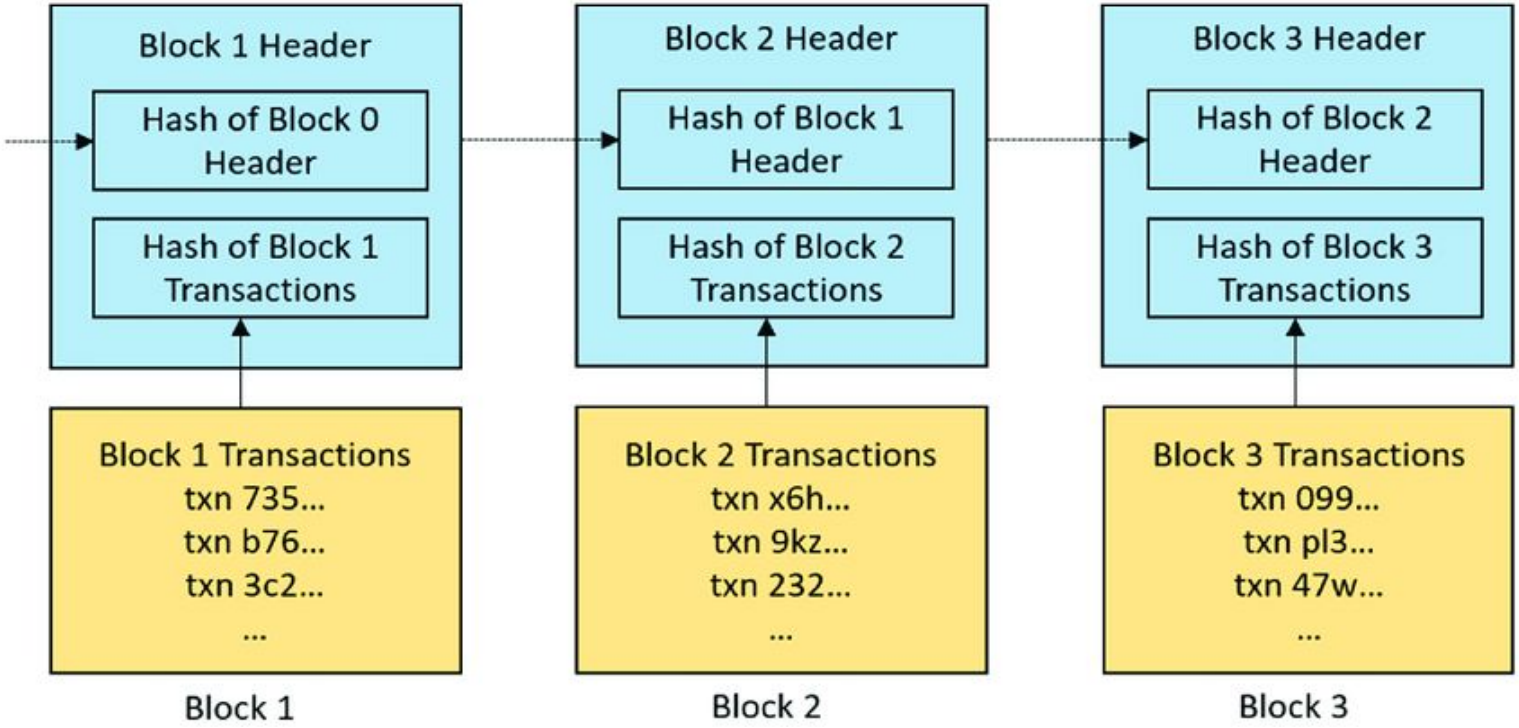
- Hash of the block – Alphanumeric number to identify the block
- Hash of the previous block.
- Timestamp
- Nonce – the random number used to vary the value of the hash
- Merkle Root – hash of all the hashes of all the transactions in the block
- Transaction data. (Note: This contains details of several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

What is inside a Block?

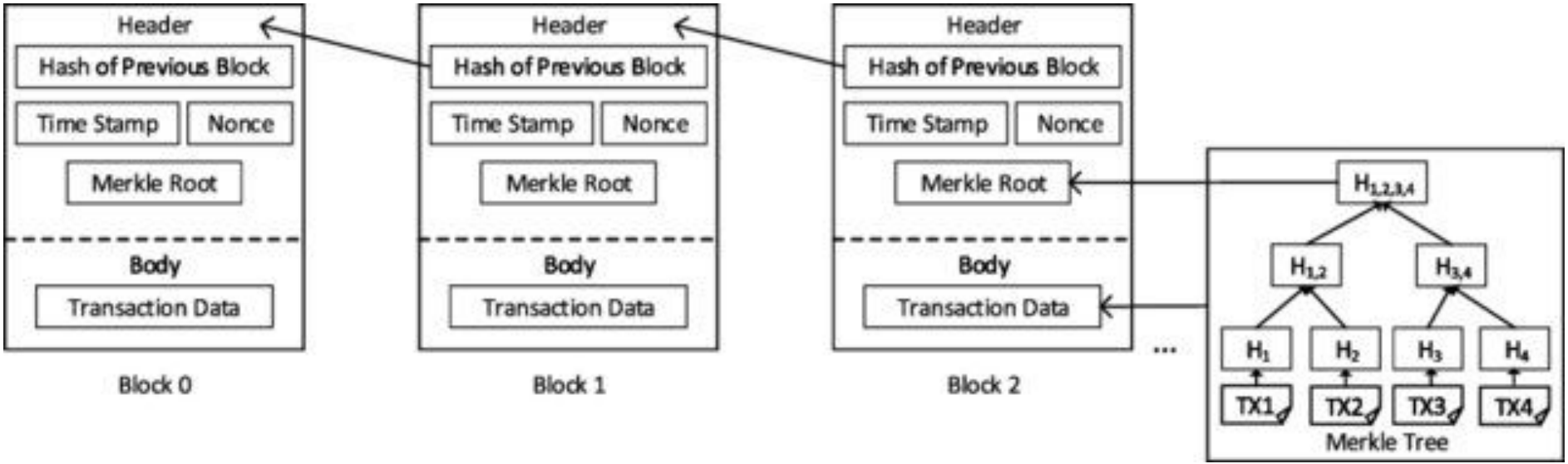


- A block is a bunch of transactions that have been added to the blockchain.

What is a Block?



What is a Block?

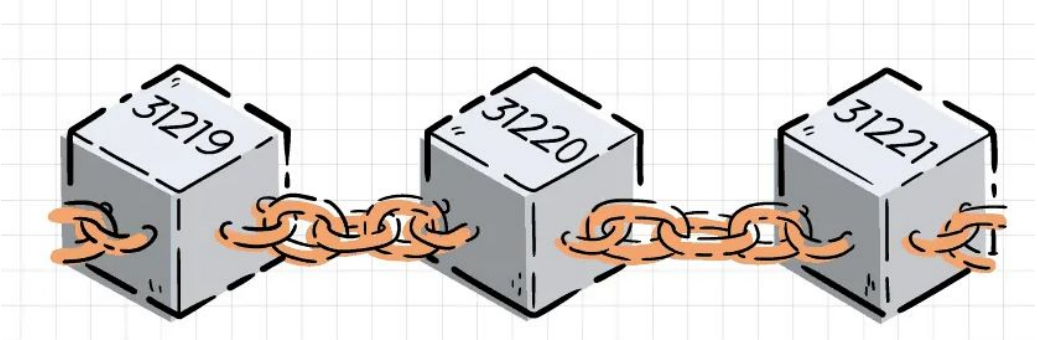


Courtesy : https://www.researchgate.net/publication/337306138_Blockchain_for_Dynamic_Spectrum_Management/figures?lo=1

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

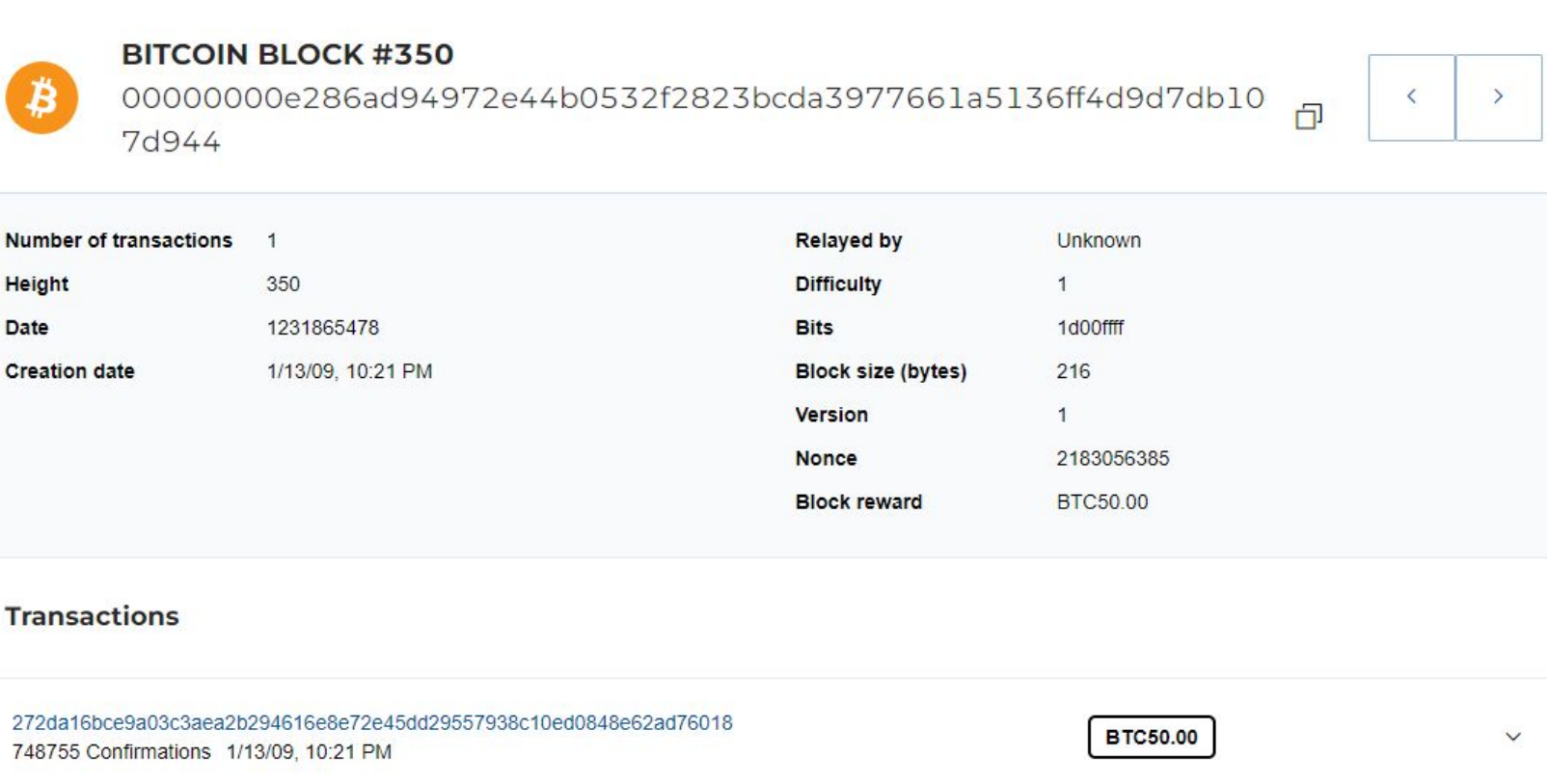
Courtesy : https://explorer.bit2me.com/btc/block/00000000000000007b1766512f8ef190bb9896e8bcb8977b043a8945978ef00



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

00000000e286ad94972e44b0532f2823bcda3977661a5136ff4d9d7db107d944

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

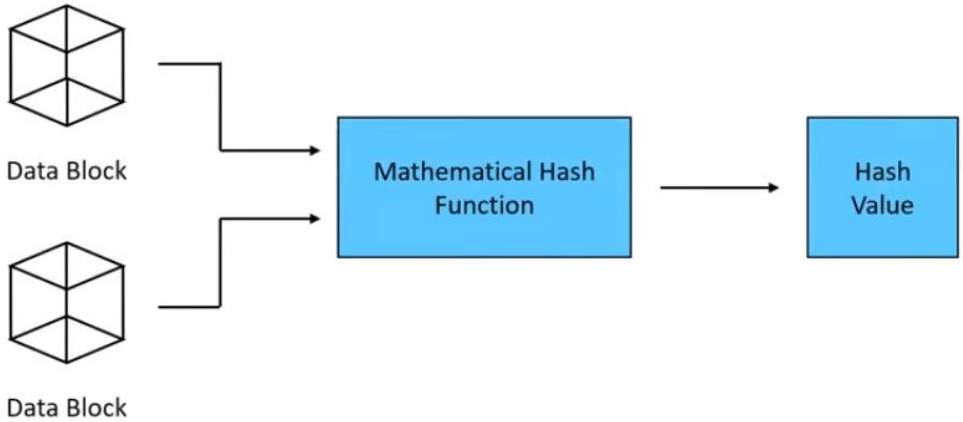
272da16bce9a03c3aea2b294616e8e72e45dd29557938c10ed0848e62ad76018
748755 Confirmations 1/13/09, 10:21 PM

BTC50.00

Cryptographic Hash Functions

A hash function maps any type of arbitrary data of any length to a fixed-size output. They are efficient and are well-known for one property: they can't be reversed.

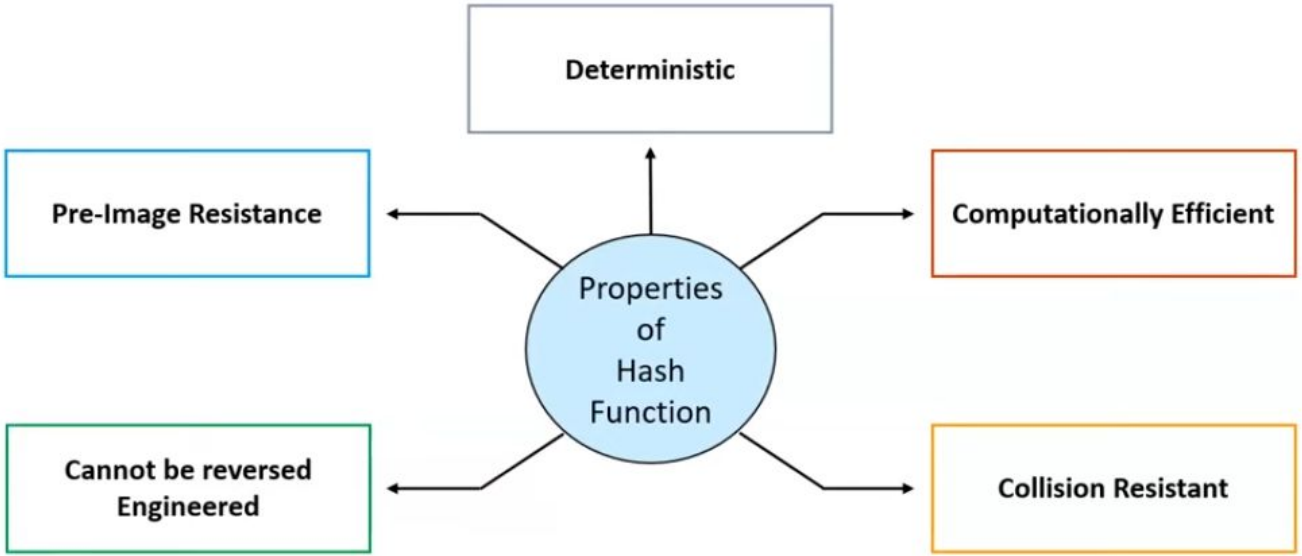
Hash Function for Blockchain



Courtesy : https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain

Cryptographic Hash Functions

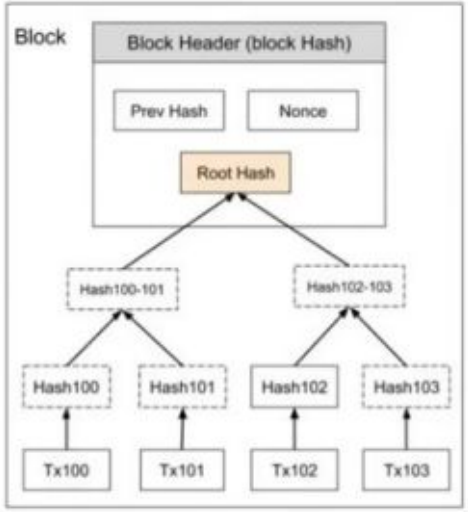
Let's take an example - If you use the SHA256 hash algorithm and pass 101Blockchains as input, you will get the following output:
fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9



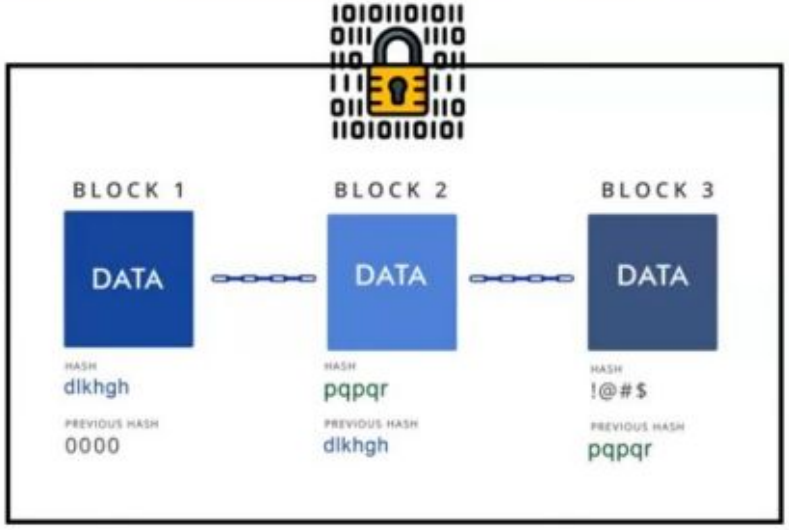
Courtesy : https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain

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.



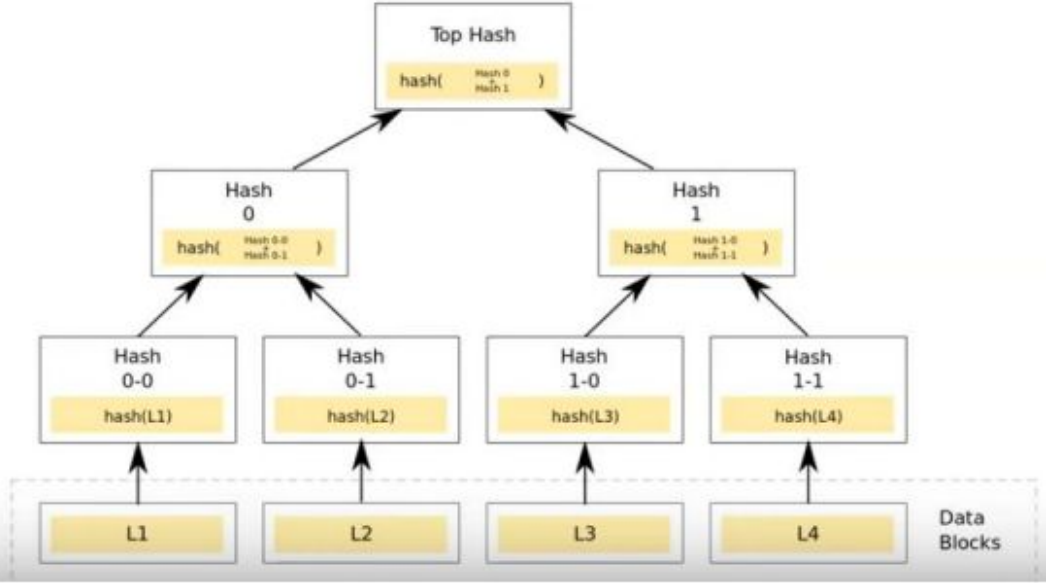
Merkle Tree



Blockchain Data encrypted Securely

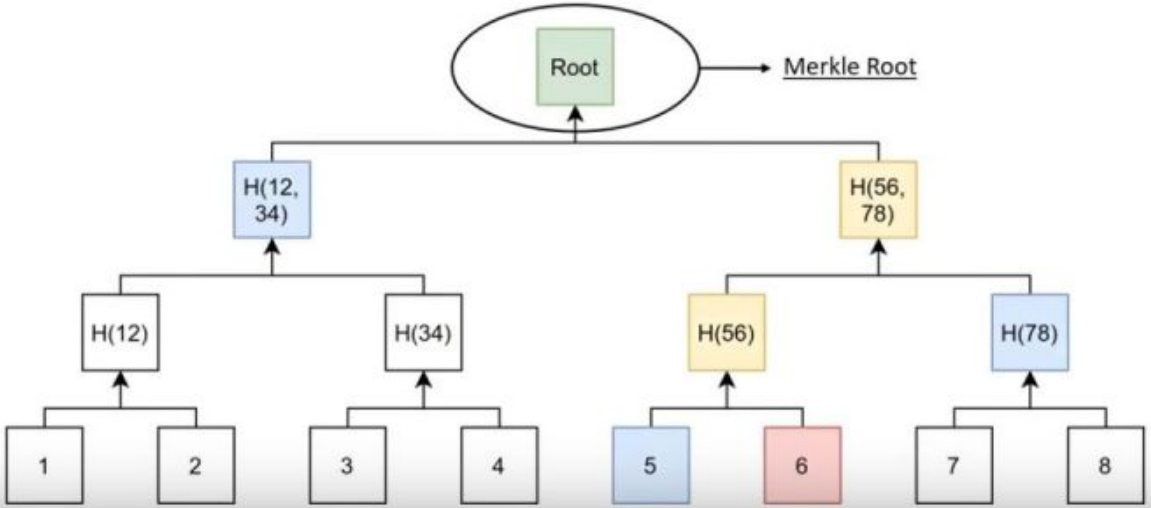
What is a Merkle Tree ?

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.



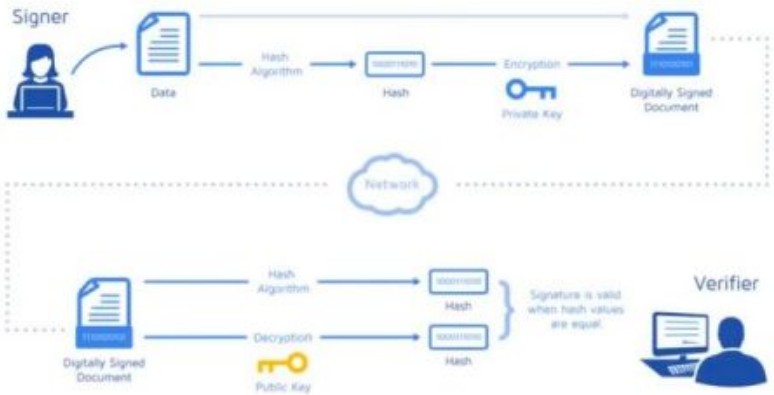
What is a Merkle Root ?

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.



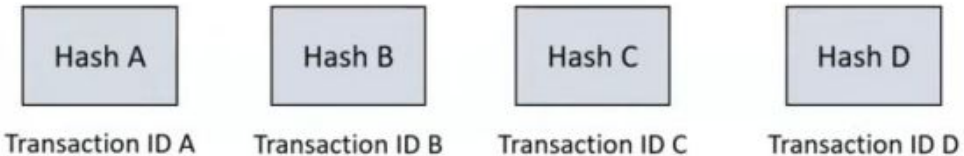
How does a Merkle Tree work ?

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

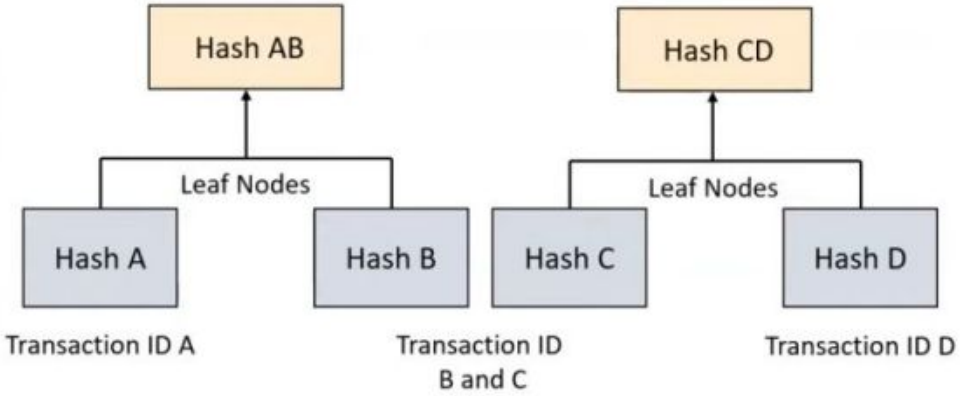
How does a Merkle Tree work ?

Each transaction is then hashed, leaving us with:
Hash A
Hash B
Hash C
Hash D



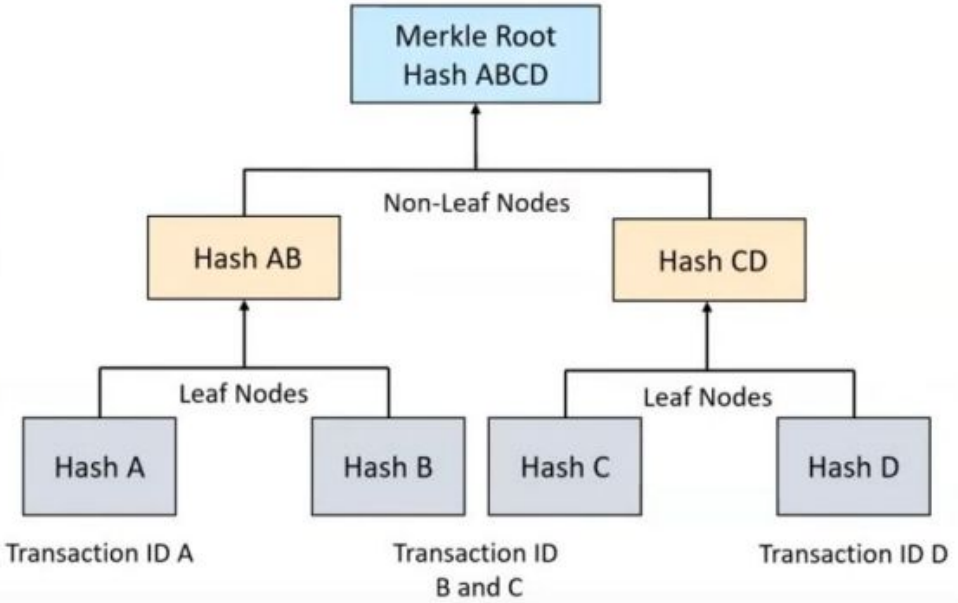
How does a Merkle Tree work ?

The hashes are paired together resulting in:
Hash AB
and
Hash CD
Our Merkle Root is formed by combining these two hashes: Hash ABCD.

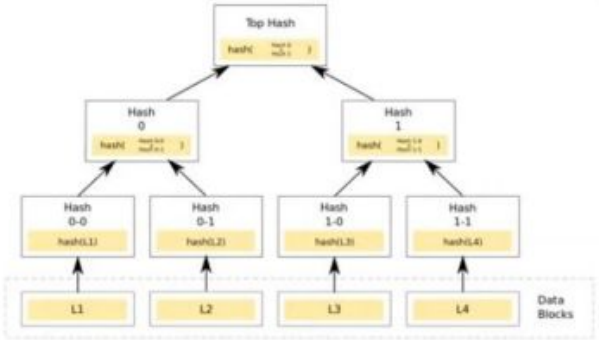


How does a Merkle Tree work ?

The hashes are paired together resulting in:
Hash AB
and
Hash CD
Our Merkle Root is formed by combining these two hashes: Hash ABCD.



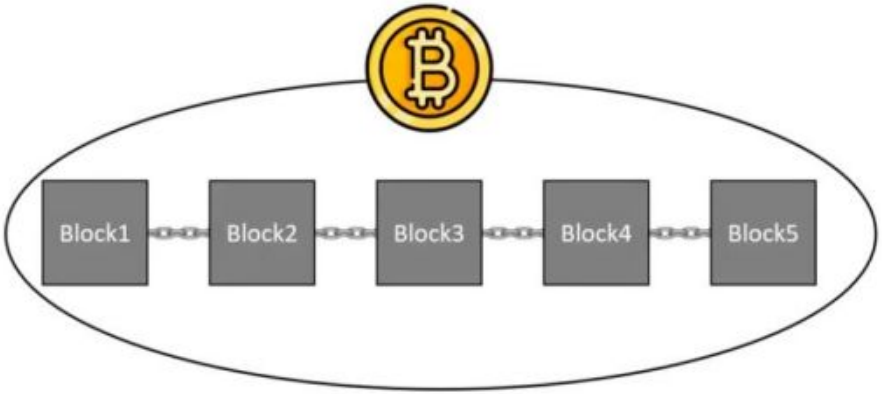
Benefits of Merkle Tree



- Validate the data's integrity
- Takes little disk space
- Tiny information across networks
- Efficient Verification

Why is it essential for Blockchain ?

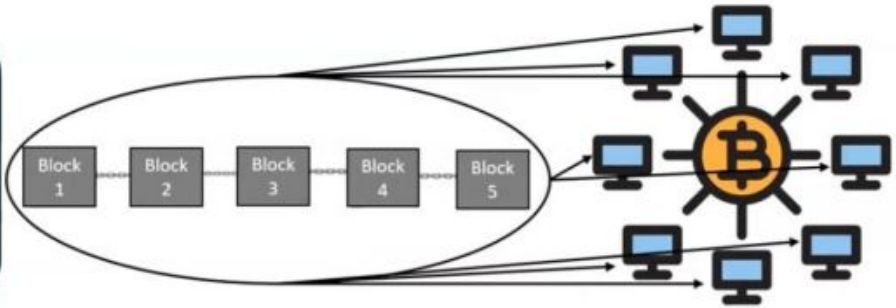
Let's imagine a blockchain without Merkle Trees to get a sense of how vital they are for blockchain technology.



Blocks of Transactions taking place in Bitcoin Network

Why is it essential for Blockchain ?

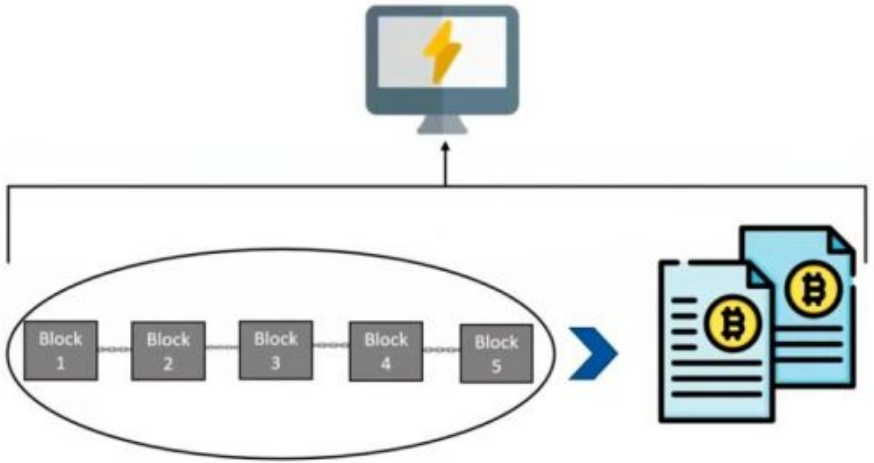
If Bitcoin didn't include Merkle Trees, for example, every node on the network would have to retain a complete copy of every single Bitcoin transaction ever made.



Too much information for every node to validate on their own

Why is it essential for Blockchain ?

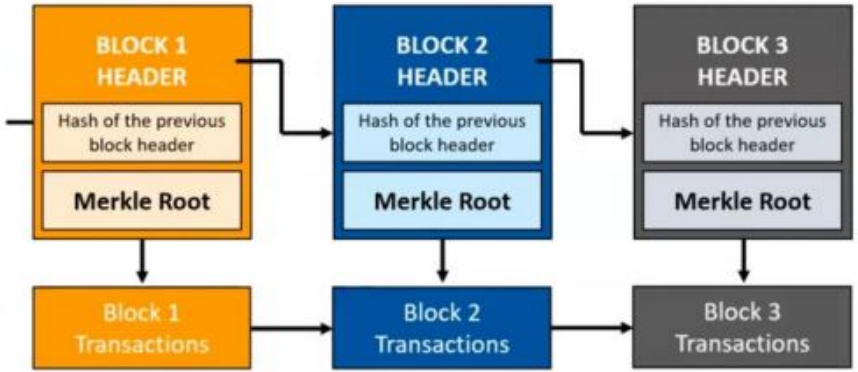
To confirm that there were no modifications, a computer used for validation would need a lot of computing power to compare ledgers.



Comparing ledgers using a lot of computing power

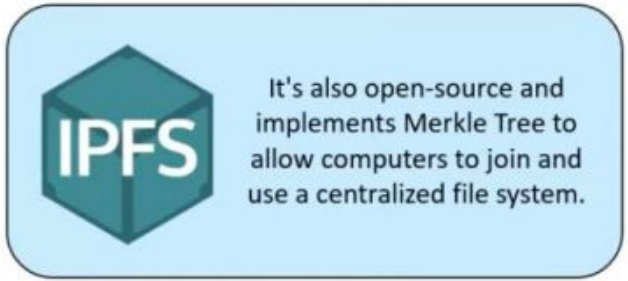
Why is it essential for Blockchain ?

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



Encryption Process : Cryptocurrency

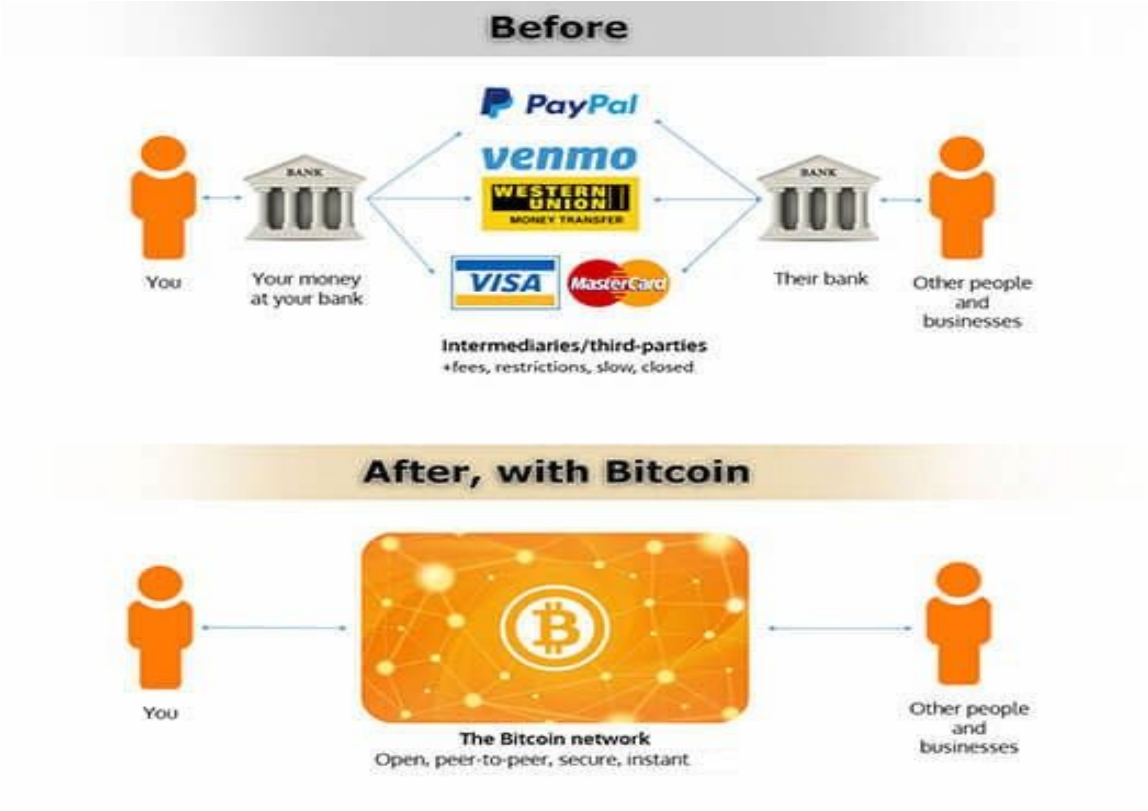
Cryptocurrency is an **internet-based medium of exchange** which uses **cryptographic functions** to conduct financial transactions.

- **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)

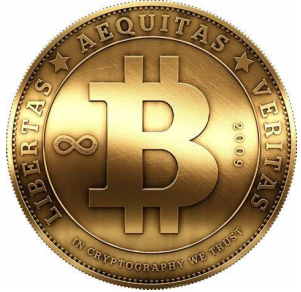
Bitcoin : Introduction

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

Bitcoin : Introduction

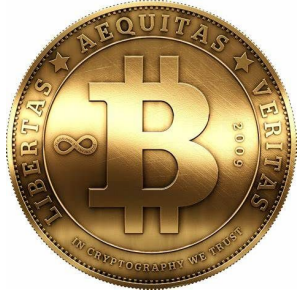
- **cryptocurrency.**
- It is a **decentralized digital currency without a central bank** that can be **sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.**
- **Transactions are verified by network nodes** through **cryptography** and **recorded in a public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

Why Bitcoin is Popular?



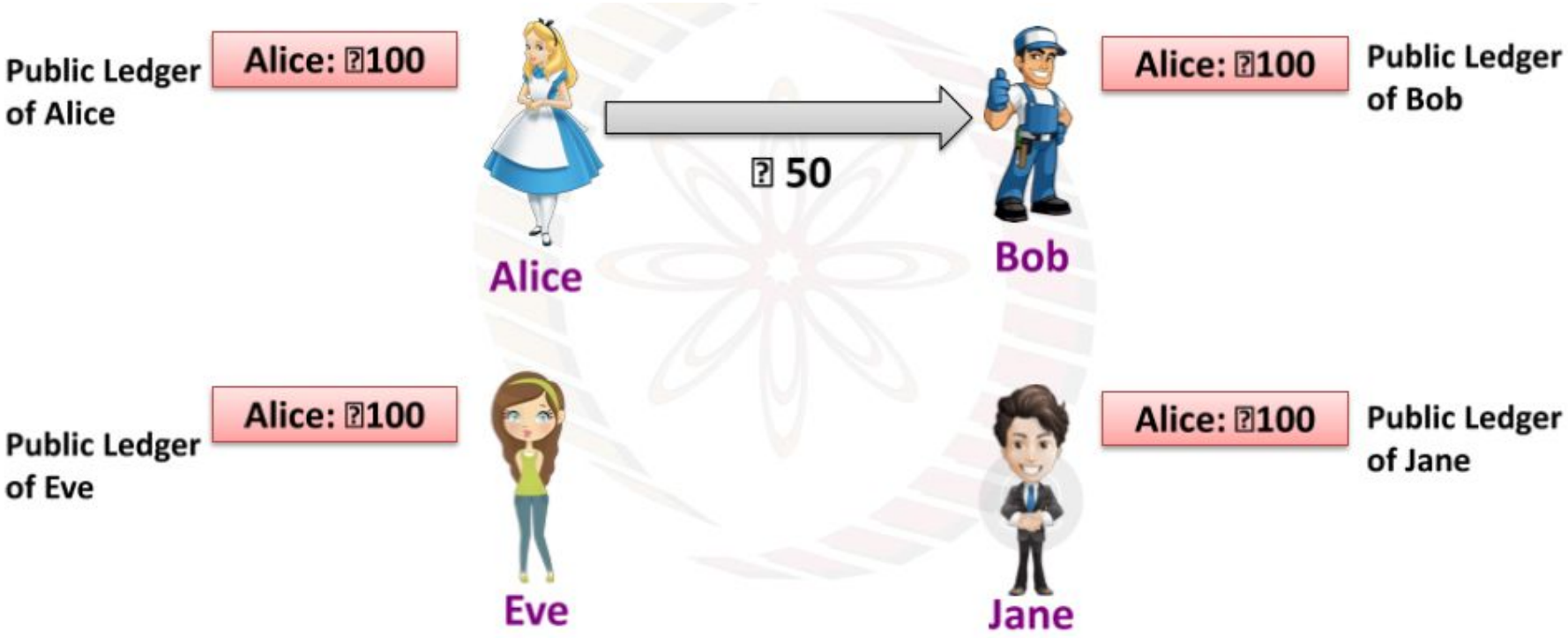
- It was the only cryptocurrency
- It is **decentralised currency** (Regulate by users, not any bank)
- It **allow user to do transaction anonymously**
- It is **tax free** (No matter how many bitcoins you have)
- **Transfer fund easily at very low cost**; Worldwide

Transactions using Bitcoin

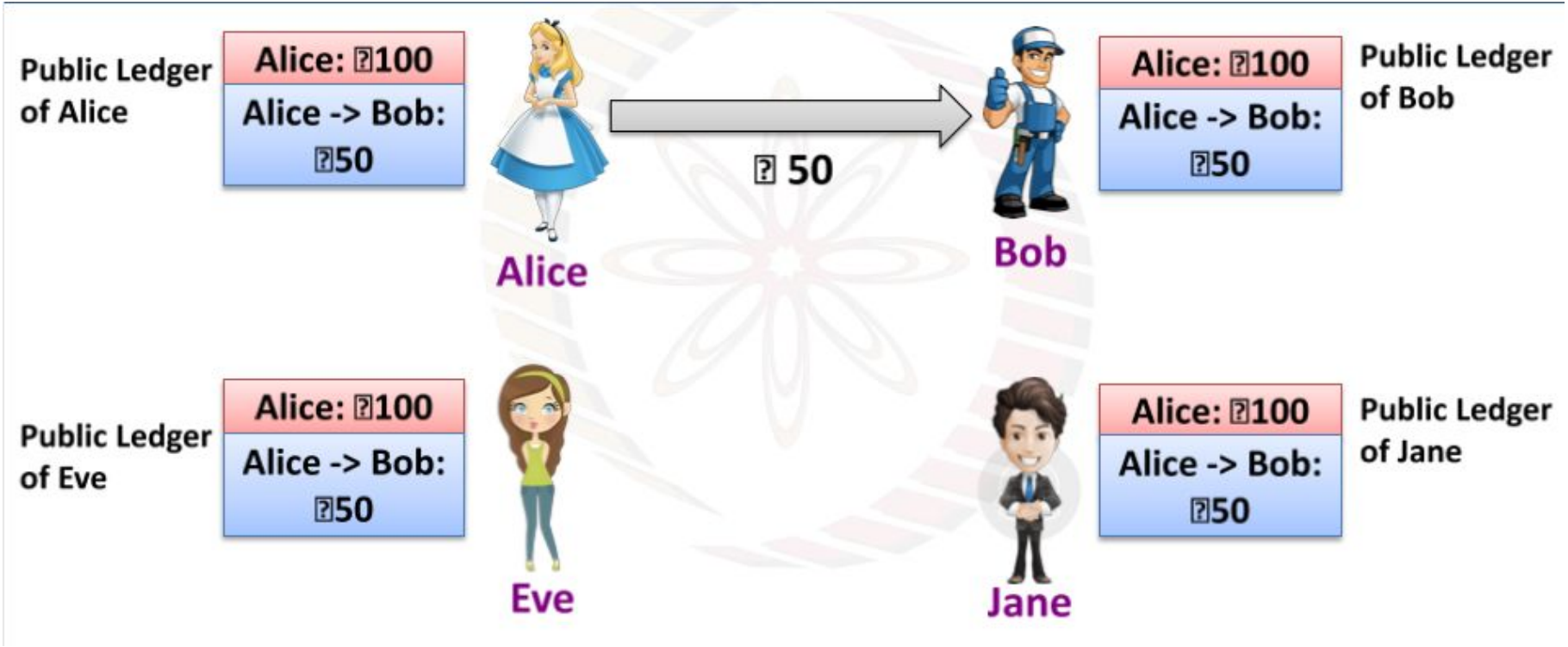


- **Every transaction** of bitcoin is **stored in a ledger called Blockchain**
- **Every bitcoin user** has **a copy of this ledger**
- **Every transaction** on Blockchain is **publicly visible** but **parties remain private**
- When a **transaction happens** it is **updated in the blockchain of all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

Transactions using Bitcoin



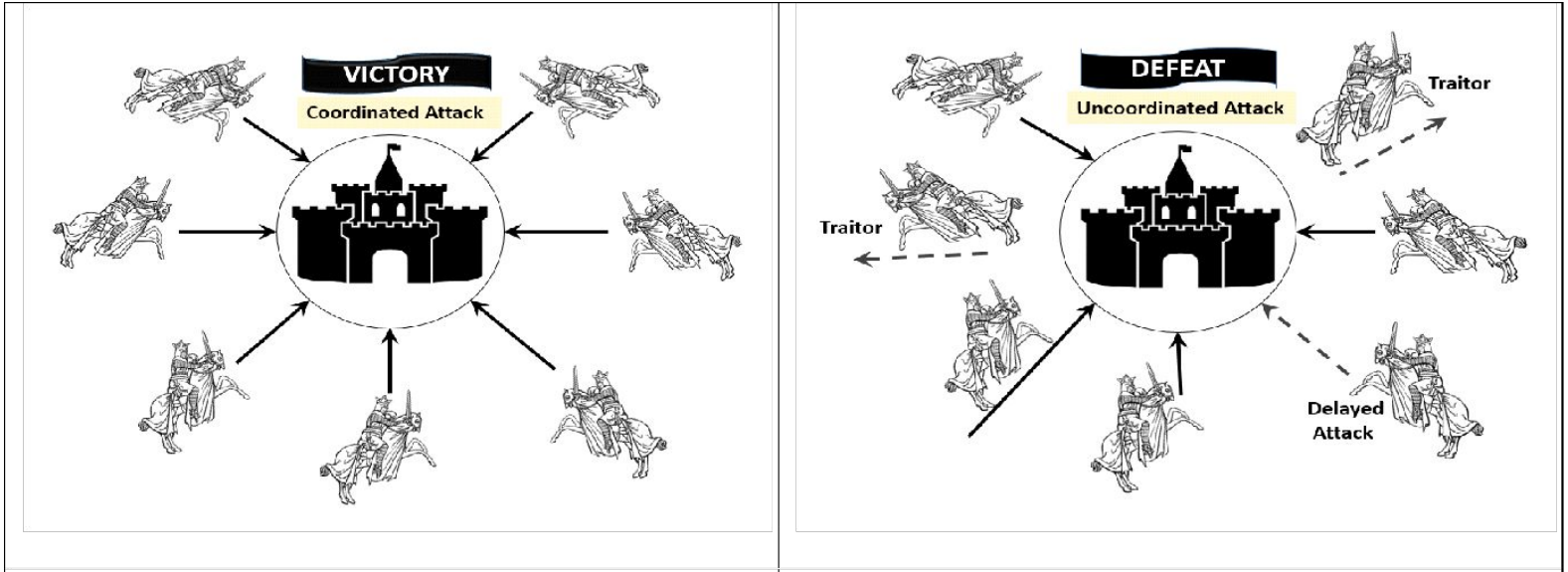
Transactions using Bitcoin



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



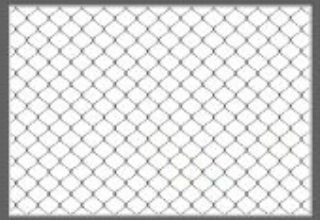
Coordinated attack leading to victory

Uncoordinated attack leading to defeat

Figure 2.12: Byzantine Generals 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

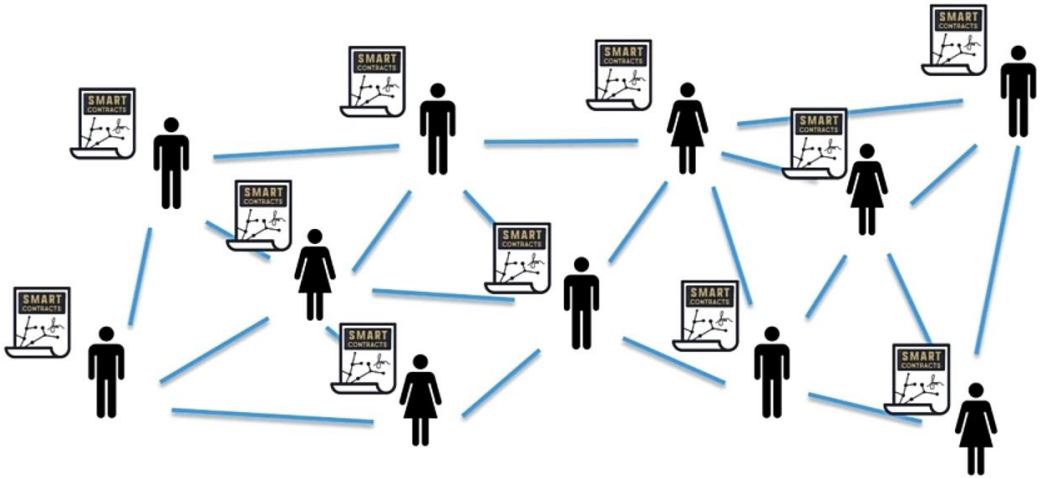
Other Consensus Algorithms

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



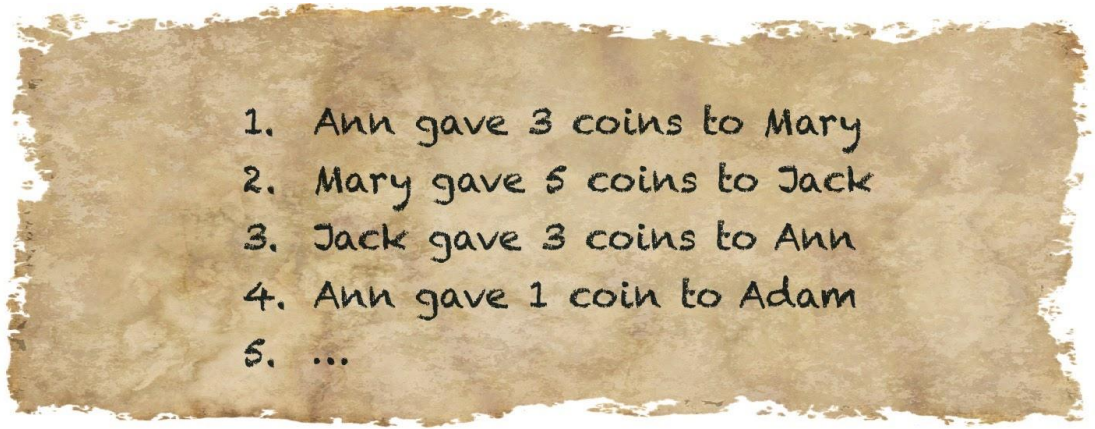
© SuperDataScience

Some Application of Hashing..

- Password storage
- To generate Digital signature
- Integrity check

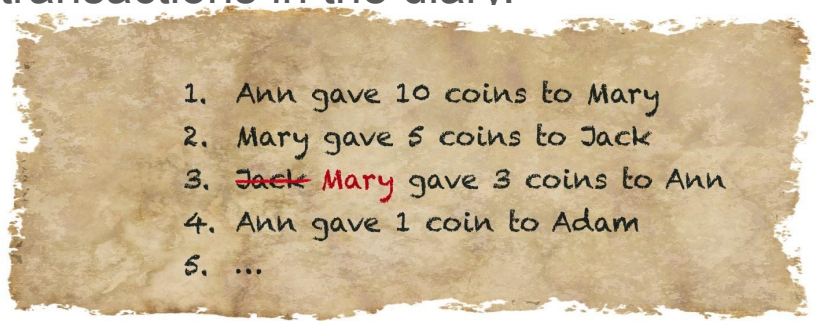
Application of hashing in Blockchain

- Consider following transactions recorded in a diary of Bob:



Application of hashing in Blockchain

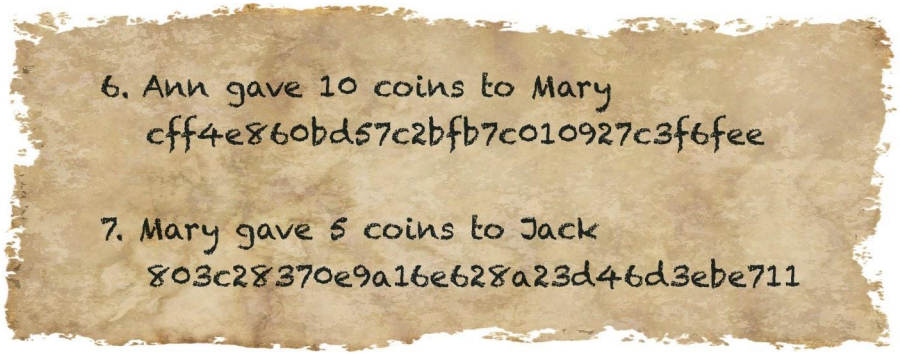
- Let's say Jack wants to steal money. With this intention, he makes some changes in the transactions in the diary.
-



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

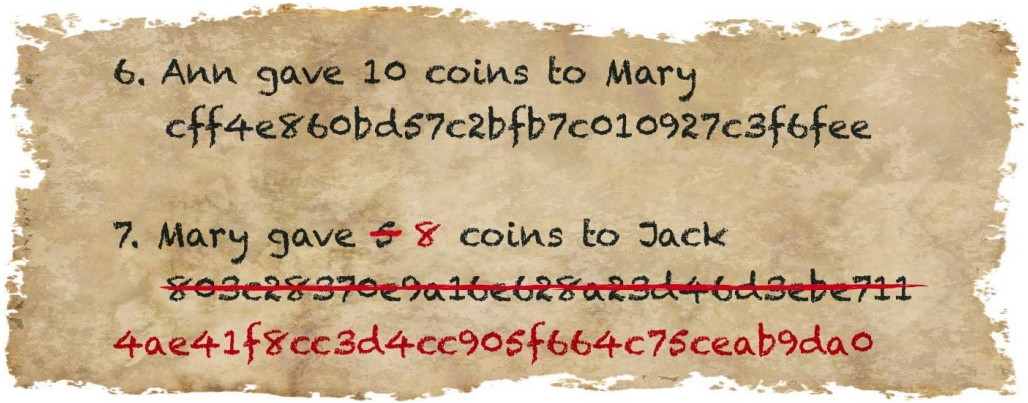
Application of hashing in Blockchain

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



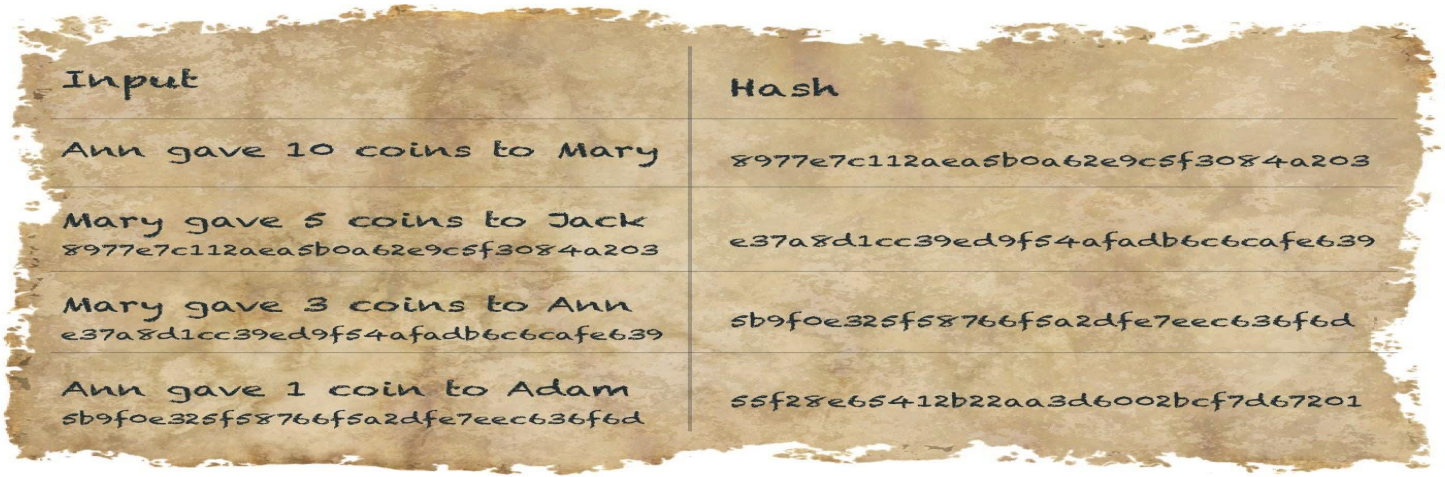
Application of hashing in Blockchain

- Jack is smart !!



Application of hashing in Blockchain

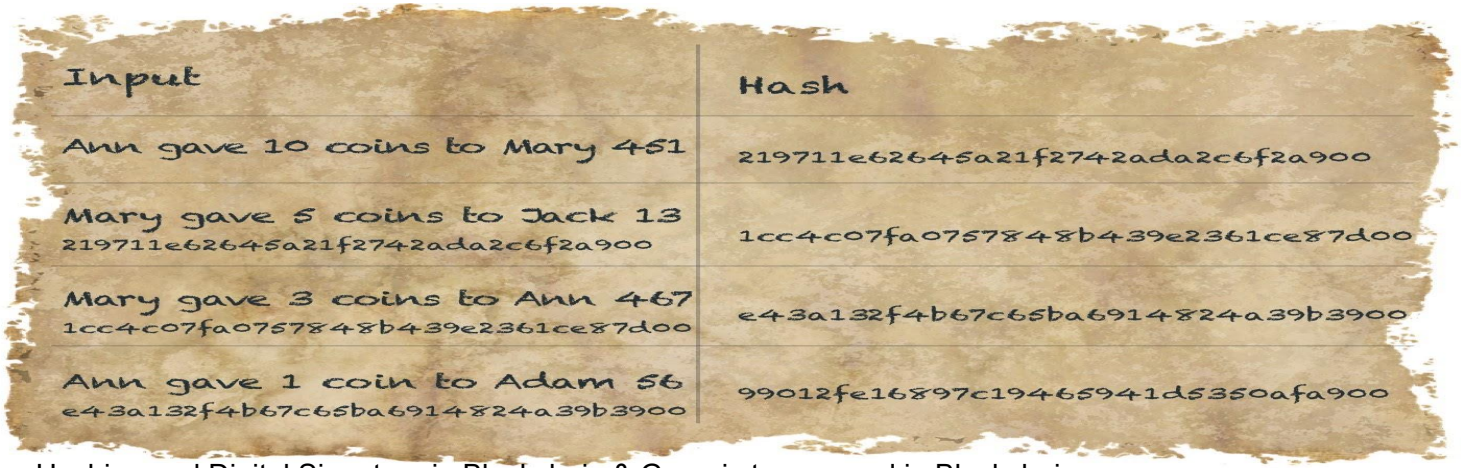
- Bob wants to make life of attacker complex!!
- New hash = (Record + previous hash)



Input	Hash
Ann gave 10 coins to Mary	8977e7c112aea5b0a62e9c5f3084a203
Mary gave 5 coins to Jack 8977e7c112aea5b0a62e9c5f3084a203	e37a8d1cc39ed9f54afadb6c6cafe639
Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639	5b9f0e325f58766f5a2dfe7eec636f6d
Ann gave 1 coin to Adam 5b9f0e325f58766f5a2dfe7eec636f6d	55f28e65412b22aa3d6002bcf7d67201

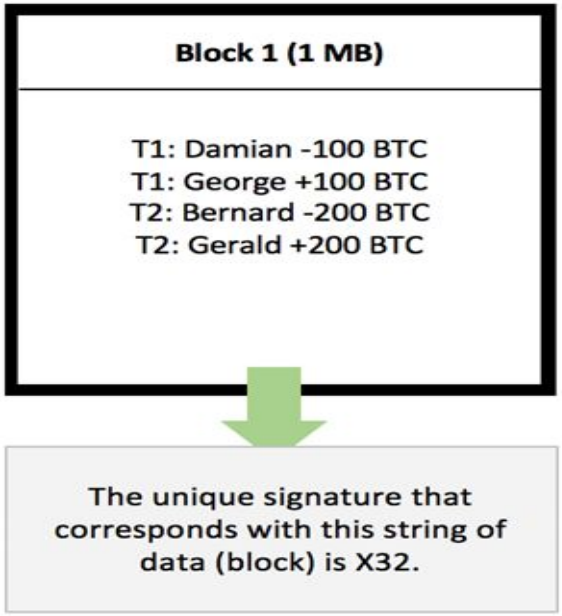
Hashing + Nonce

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

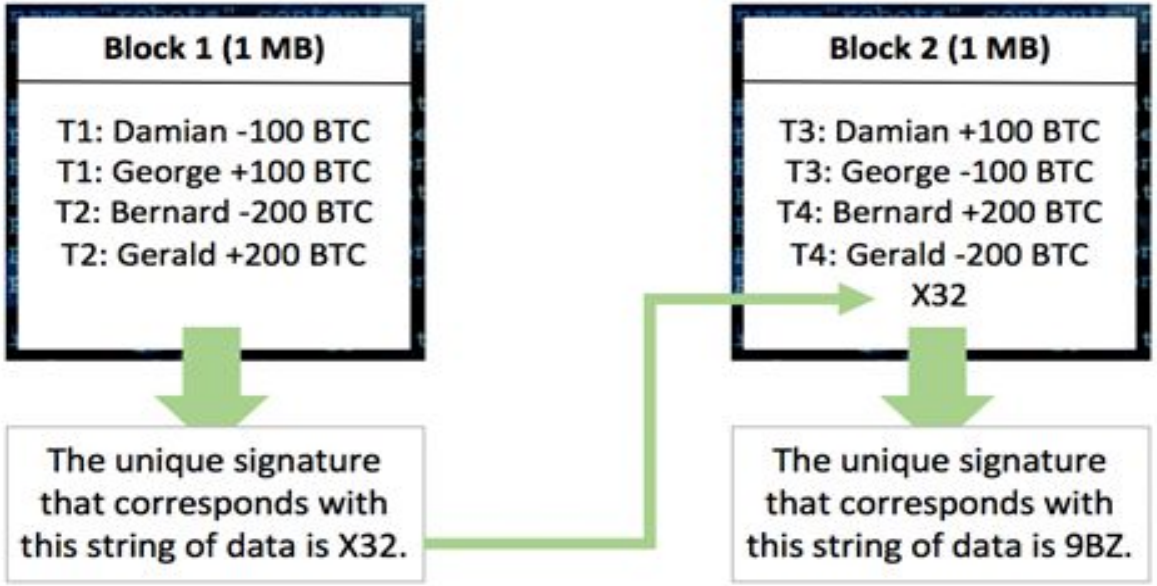


Input	Hash
Ann gave 10 coins to Mary 451	219711e62645a21f2742ada2c6f2a900
Mary gave 5 coins to Jack 13 219711e62645a21f2742ada2c6f2a900	1cc4c07fa0757848b439e2361ce87d00
Mary gave 3 coins to Ann 467 1cc4c07fa0757848b439e2361ce87d00	e43a132f4b67c65ba6914824a39b3900
Ann gave 1 coin to Adam 56 e43a132f4b67c65ba6914824a39b3900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

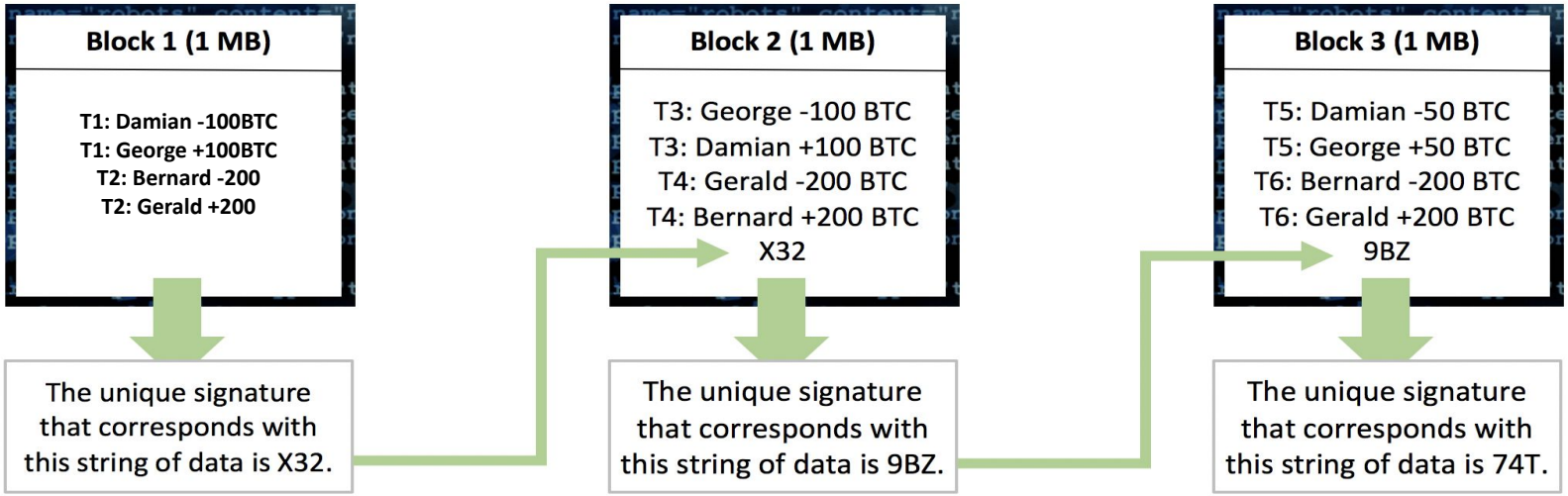
Hashing in Blockchain- 1st Block



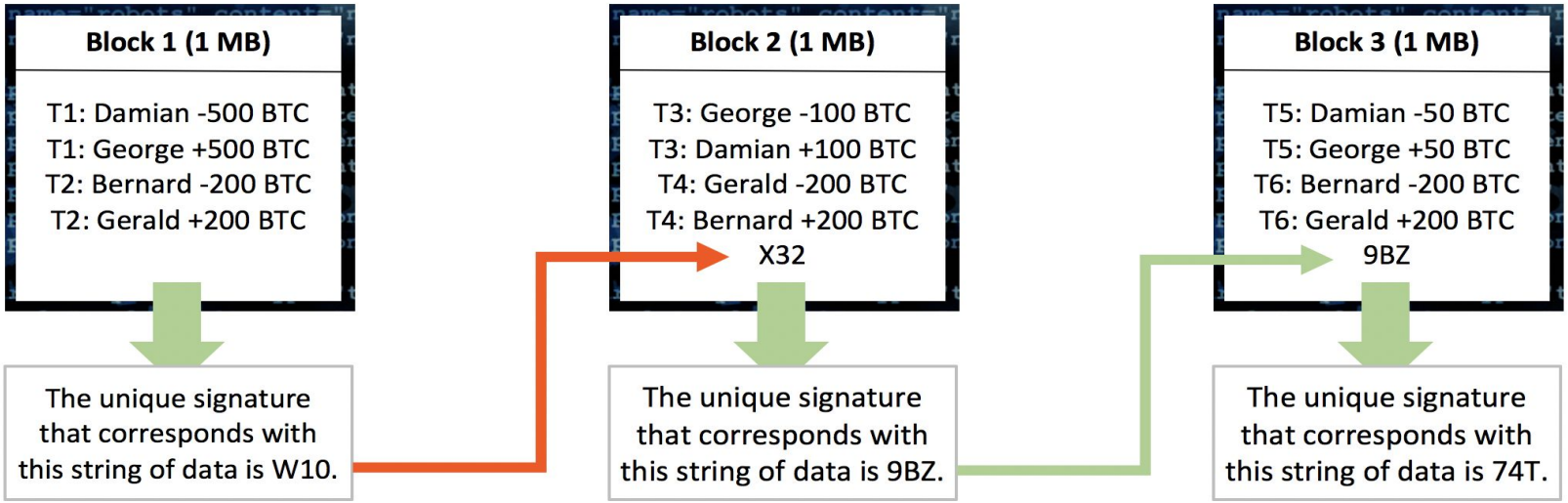
2nd Block of transaction added



3rd Block of transaction added



What if block 1 is altered..



Error propagates in Block 2

Error propagates to Block 3 and so on..