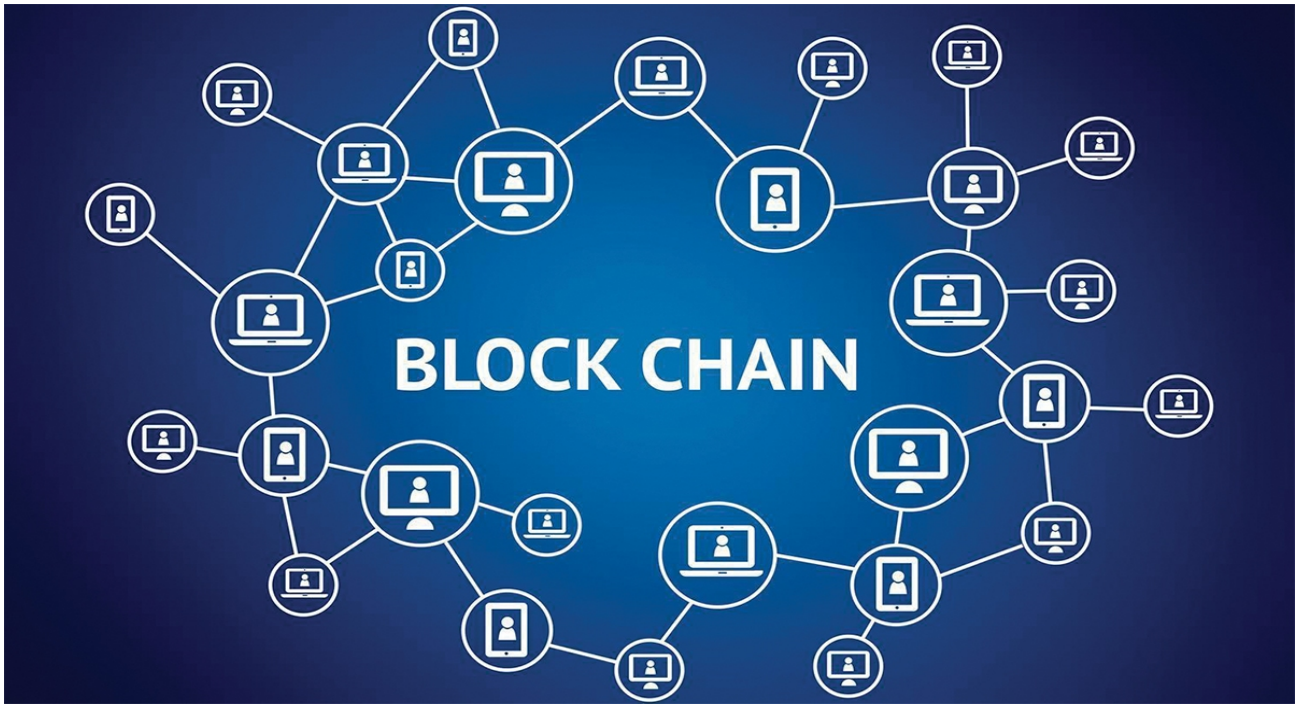
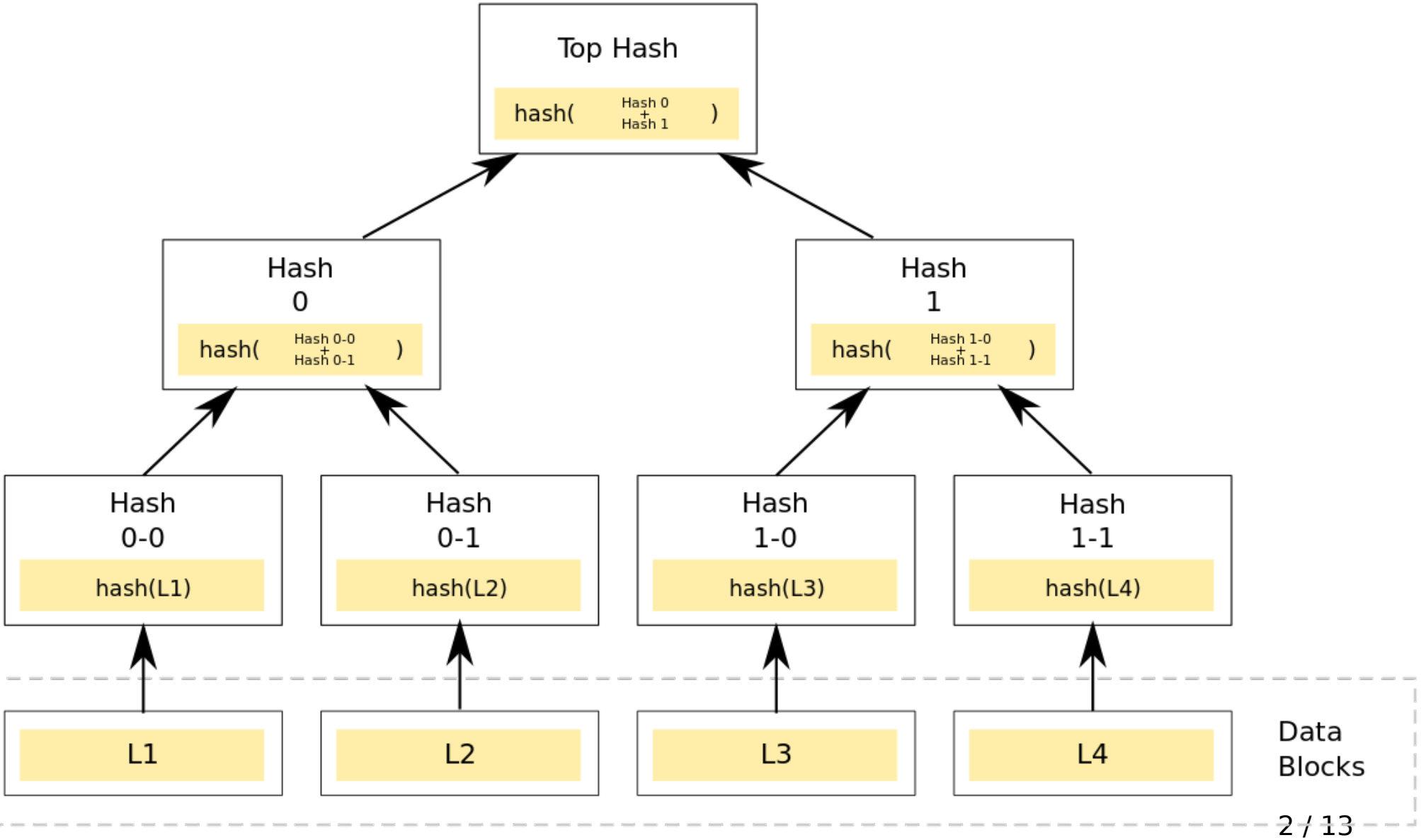


Blockchain

By – Udayveer Singh

Merkle Tree


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

Component of a Transaction

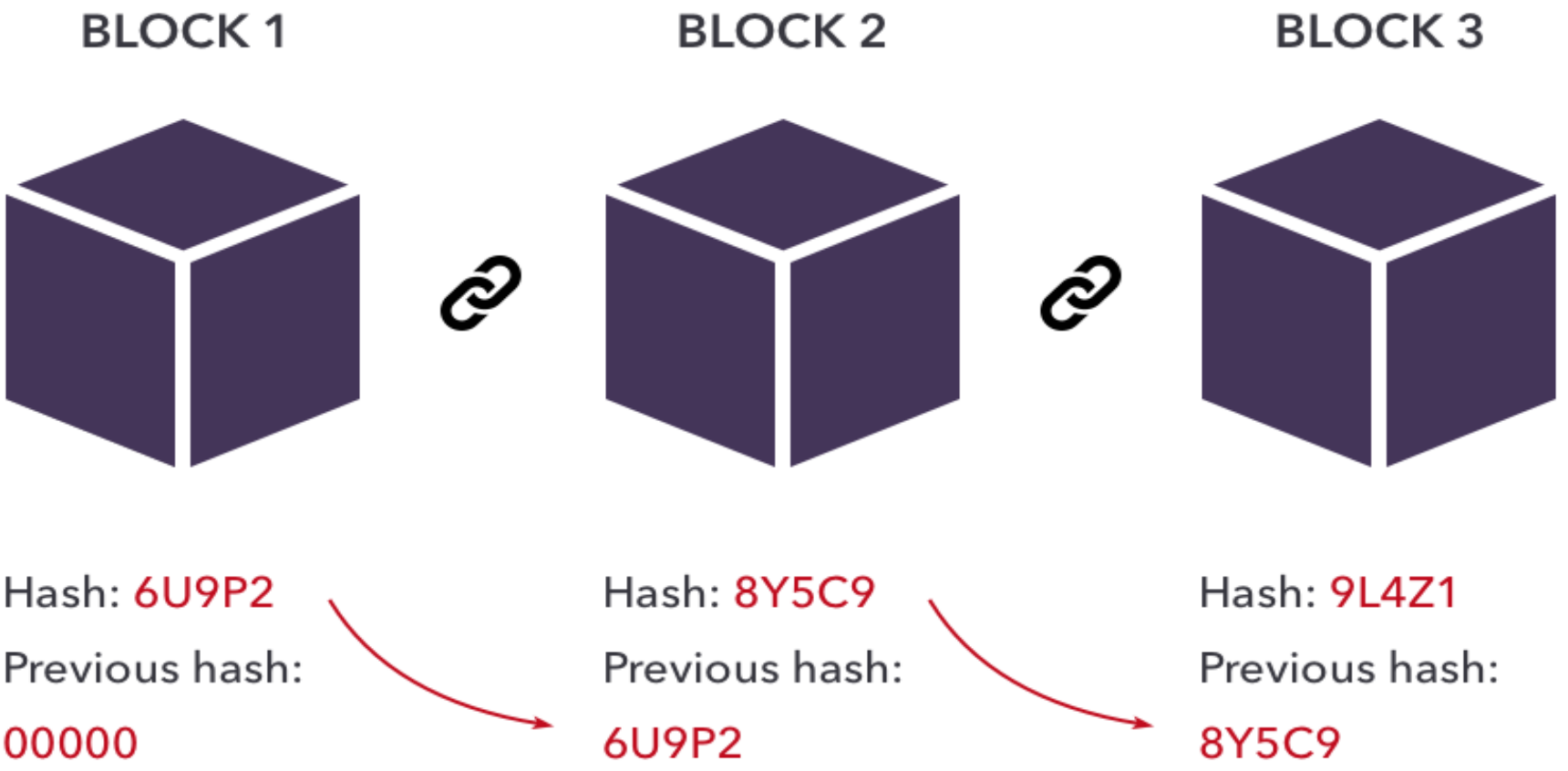
- Transaction Hash
- Timestamp
- Sender public key
- Receiver public key
- Gas fee
- Amount sent

Component of a Block

- Block Number
- Block Hash
- Timestamp
- Merkle root
- Nonce
- Previous Block hash

Formation of Chain

- The chain of block is formed when the hash of the previous block is added in the next block



Type of Blockchain

- Public Blockchain
- Private Blockchain
- Consortium Blockchain

Public Blockchain

- A public blockchain is the permission-less distributed ledger technology where anyone can join and do transactions. It is a non-restrictive version where each peer has a copy of the ledger. This also means that anyone can access public blockchain if they have an internet connection. One of the first public blockchains that were released to the public was the bitcoin public blockchain.
- Advantages
  - It brings trust among the whole community of users
  - Everyone feels incentivized to work towards the betterment of the public network
- Disadvantage
  - Lack of transaction speed
  - Scalability issues
- Use cases - Voting and Fundraising

Private Blockchain

- A private blockchain can be best defined as the blockchain that works in a restrictive environment, i.e., closed network. It is also a permissioned blockchain that is under the control of an entity. Private blockchains are amazing for using at a privately-held company or organization that wants to use it for internal use-cases.
- Example – Hyperledger, Multichain and Corda
- Advantages
  - It is fast and more scaleable
- Disadvantages
  - Private blockchains are not truly decentralized.
  - Achieving trust within private blockchain is tough.
- Use cases- Supply chain management and assest management

Consortium Blockchain

- A consortium blockchain (also known as Federated blockchains) is a creative approach to solving the needs of organizations where there is a need for both public and private blockchain features. In a consortium blockchain, some aspects of the organizations are made public, while others remain private. The consensus procedures in a consortium blockchain are controlled by the preset nodes.
- Example - Marco Polo, Energy Web Foundation, IBM Food Trust.
- Advantages
  - It offers better customizability and control over resources.
  - Consortium blockchains are more secure and have better scalability.
- Disadvantages
  - Even though it is secure, the whole network can be compromised due to the member’s integrity.
  - It is less transparent.

Advantages of Database

- **Control Database Redundancy:** It is because it stores all data in one single database file and that recorded data is placedd in the database.
- **Data sharing:** In DBMS, the authorized users of an organization can share the data among multiple users.
- **Easily Maintenance:** It is easily maintenable due to the centralized nature of the database.
- **Reduced Time:** It reduces development time and maintenance need.
- **Backup:** It provides backup recovery subsystems which create an automatic backup of data from hardware and software failures and restores the data if required.
- **Multiple user interfaces:** It provides different types of user interfaces like graphical user interfaces, application program interface.

Advantages of Blockchain

- **Time Reduction:** In the financial industry, blockchain allows the quicker settlement of the trades. It does not takes the lengthy process of verification, settlement, clearence.
- **Unchangeable Transactions:** Blockchain allows only the insertions of new transactions. That means the old transactions can never be tempered or modified.
- **Reliability:** Blockchain vertifies and verifies the identities of each interested parties. This removes double records, reducing rates and accelerating transcations.
- **Security:** Blockchain uses advanced cryptography to make sure that the information is locked inside the blockchain. It uses distributed ledger technology where each party holds the copy of the original chain, so thesystem remains operative, even the large number of other nodes fall.
- **Decentralized:** It is because there is n central authority supervising it. There are standard rules on how every node exchages the blockchain information.

Blockchain v/s Database

It is decentralized as have no admin or in-charge.	It is centralized as have admins and in-charges
It is permissionless to access	It requires permissions to access
It is slower	It is faster
It has history of records and ownership of digital records	It has no history of records or ownership of records.
It is fully confidential	It is not fully confidencial
It has only insert operation	It has create, read, write and delete operations
It is fully robust technology	It is not entirely robust technology
Disintermediations is allowed in blockchain	Disintermideations is not allowed
Anyone with right proof of work can write	Only entities entitled to read and write can do so
It is not recursive	It is recursive

Use Cases

- Charity
- Supply Chain
- Health Care
- Royalty payments
- Governance
- Payment solutions
- Internet of things(IOT)