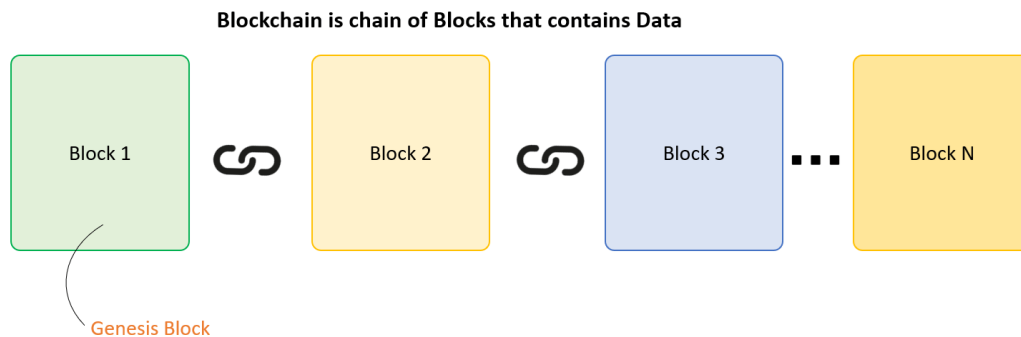


# Blockchain

## What is Blockchain?

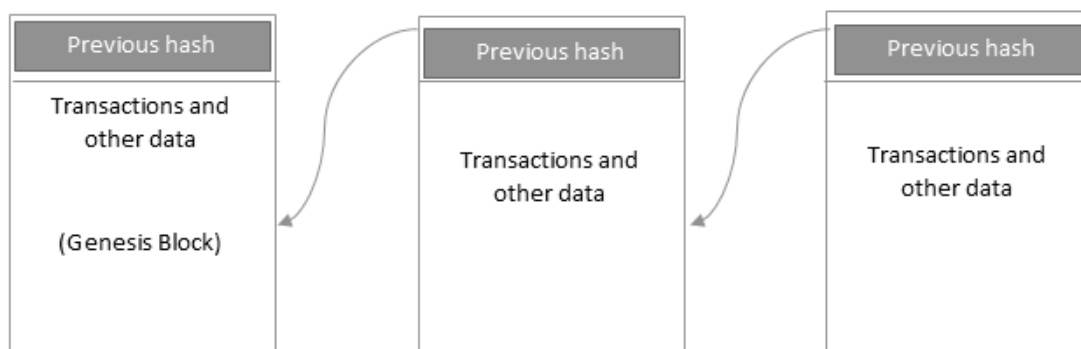
In simple words, blockchain can be defined as a chain of the block that contains information. The technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. The blockchain is used for the secure transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a blockchain, it is very difficult to change it.



## Various Technical Definitions of Blockchains:

- Blockchain is a decentralized consensus mechanism. In a blockchain, all peers eventually come to an agreement regarding the state of a transaction.
- Blockchain is a distributed shared ledger. Blockchain can be considered a shared ledger of transactions. The transaction are ordered and grouped into blocks. Currently, the real-world model is based on private databases that each organization maintains whereas the distributed ledger can serve as a single source of truth for all member organizations that are using the blockchain.
- Blockchain is a data structure; it is basically a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block.

The structure of a generic blockchain can be visualized with the help of the following diagram:



## Blockchain Architecture:

The Blockchain architecture is illustrated by describing its various components below:

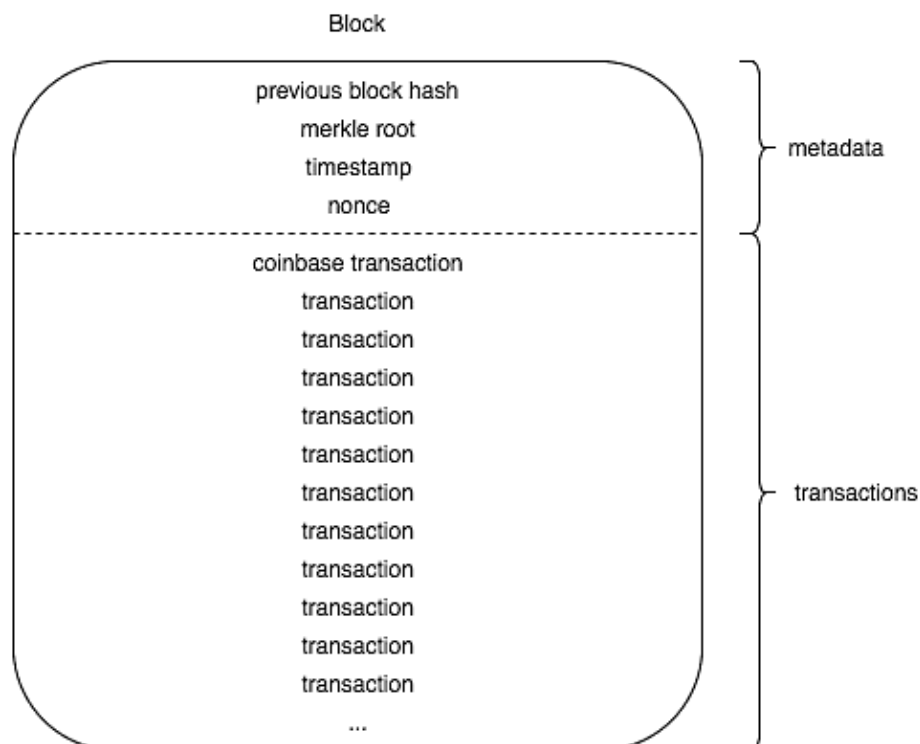
### Block / Structure of a Block:

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners (discussed in more detail below).

Blocks contain a block header, which is the metadata that helps verify the validity of a block. Typical block metadata contains:

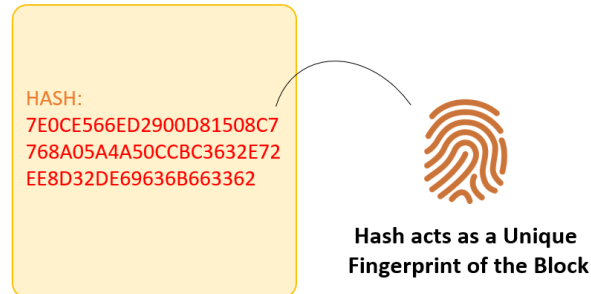
1. **Version:** The current version of the block structure.
2. **Previous Block Header Hash:** The reference of this block's parent block.
3. **Merkle Root Hash:** A cryptographic hash of all of the transactions included in this block.
4. **Time:** The time that this block was created.
5. **nBits:** The current difficulty that was used to create this block.
6. **Nonce (“number used once”):** A random value that the creator of a block is allowed to manipulate.

These 6 fields constitute the block header. The rest of a block contains transactions that the miner has chosen to include in the block that they created. Users create transactions and submit them to the network, where they sit in a pool waiting to be included in a block.



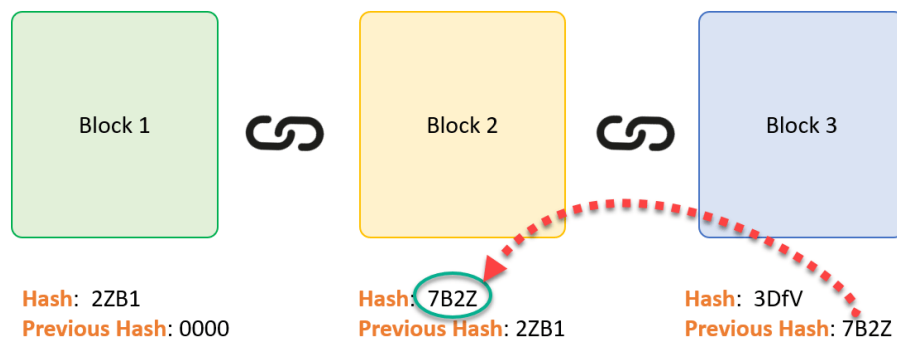
## Hashing:

A block also has a hash which can be understood as a fingerprint that is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

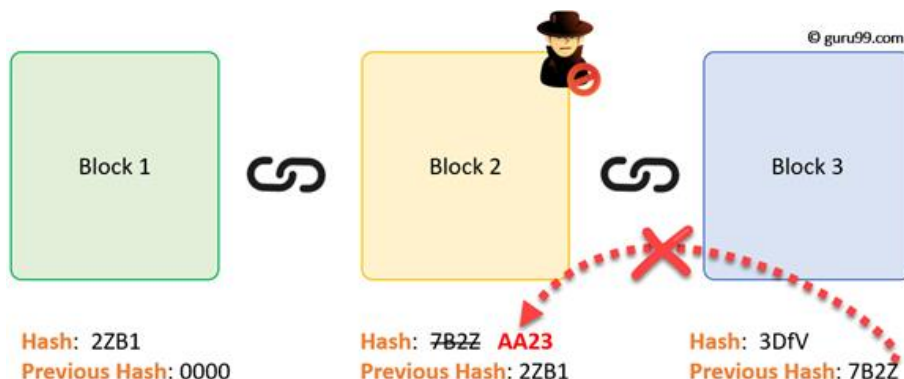


Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.



Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure.



Assume an attacker is able to tamper the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.

Therefore, changing a single block can quickly make all following blocks invalid.

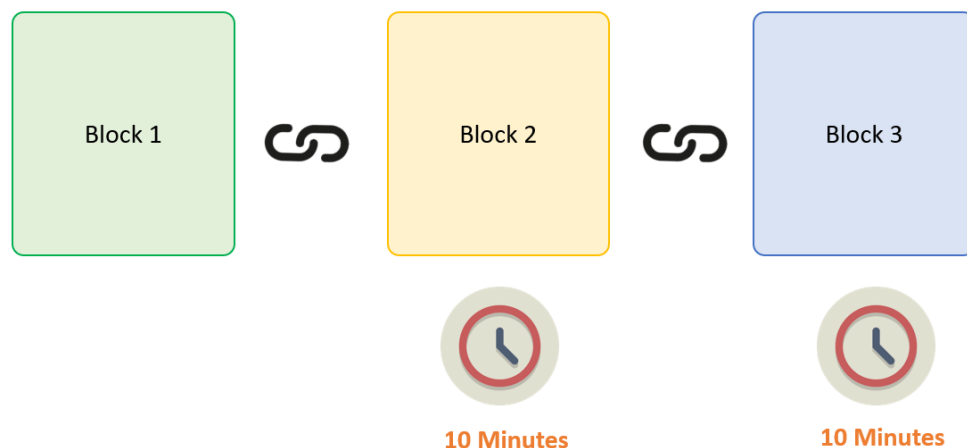
### **Proof of Work:**

Hashes are an excellent mechanism to prevent tempering but computers these days are high-speed and can calculate hundreds of thousands of hashes per second. In a matter of few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again.

To avoid the issue, blockchains use the concept of Proof-of-Work which is a mechanism that slows down the creation of the new blocks.

A proof-of-work is a computational problem that takes certain amount of effort and time to solve. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself.

In case of Bitcoin, it takes almost 10 minutes to calculate the required proof-of-work to add a new block to the chain. Considering our example, if a hacker would to change data in Block 2, he would need to perform proof of work (which would take 10 minutes) and only then make changes in Block 3 and all the succeeding blocks.

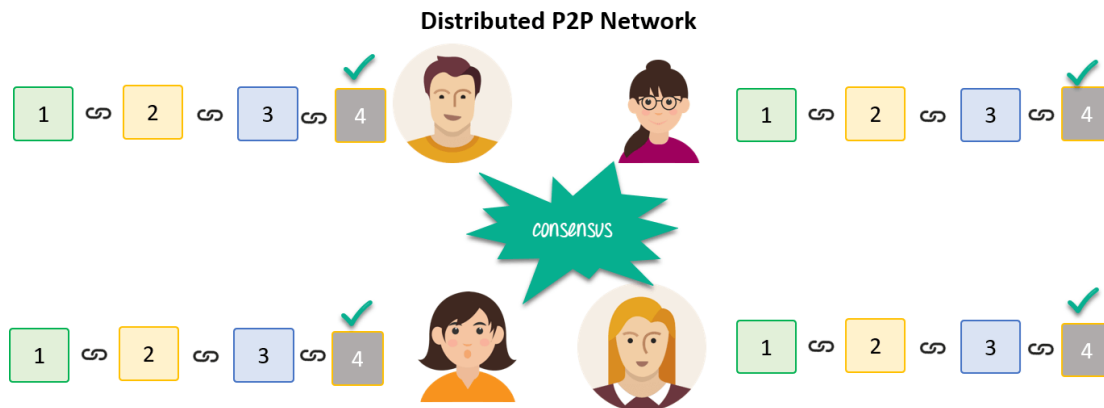


This kind of mechanism makes it quite tough to tamper the blocks so even if you tamper with even a single block, you will need to recalculate the proof-of-work for all the following blocks. Thus, hashing and proof-of-work mechanism make a blockchain secure.

## Distributed P2P Network:

However, there is one more method which is used by blockchains to secure themselves, and that's by being distributed. Instead of using a central entity to manage the chain, Blockchains use a distributed peer-peer network, and everyone is allowed to join. When someone enters this network, he will get the full copy of the blockchain. Each computer is called a node.

Let's see what happens when any user creates a new block. This new block is sent to all the users on the network. Each node needs to verify the block to make sure that it hasn't been altered. After complete checking, each node adds this block to their blockchain.



All these nodes in this network create a consensus. They agree about what blocks are valid and which are not. Nodes in the network will reject blocks that are tampered with.

So, to successfully tamper with a blockchain

1. One will need to tamper all blocks on the chain
2. Redo the proof-of-work for each block
3. Take control of greater than 50% of the peer-to-peer network.

After doing all these, the tampered block become accepted by everyone else. This is next to impossible task. Hence, Blockchains are so secure.

## How Blockchain Ensures Security?

(Write down the Hashing, Proof of Work, Distributed P2P Network described above.)

## How Blockchain Transaction Works?



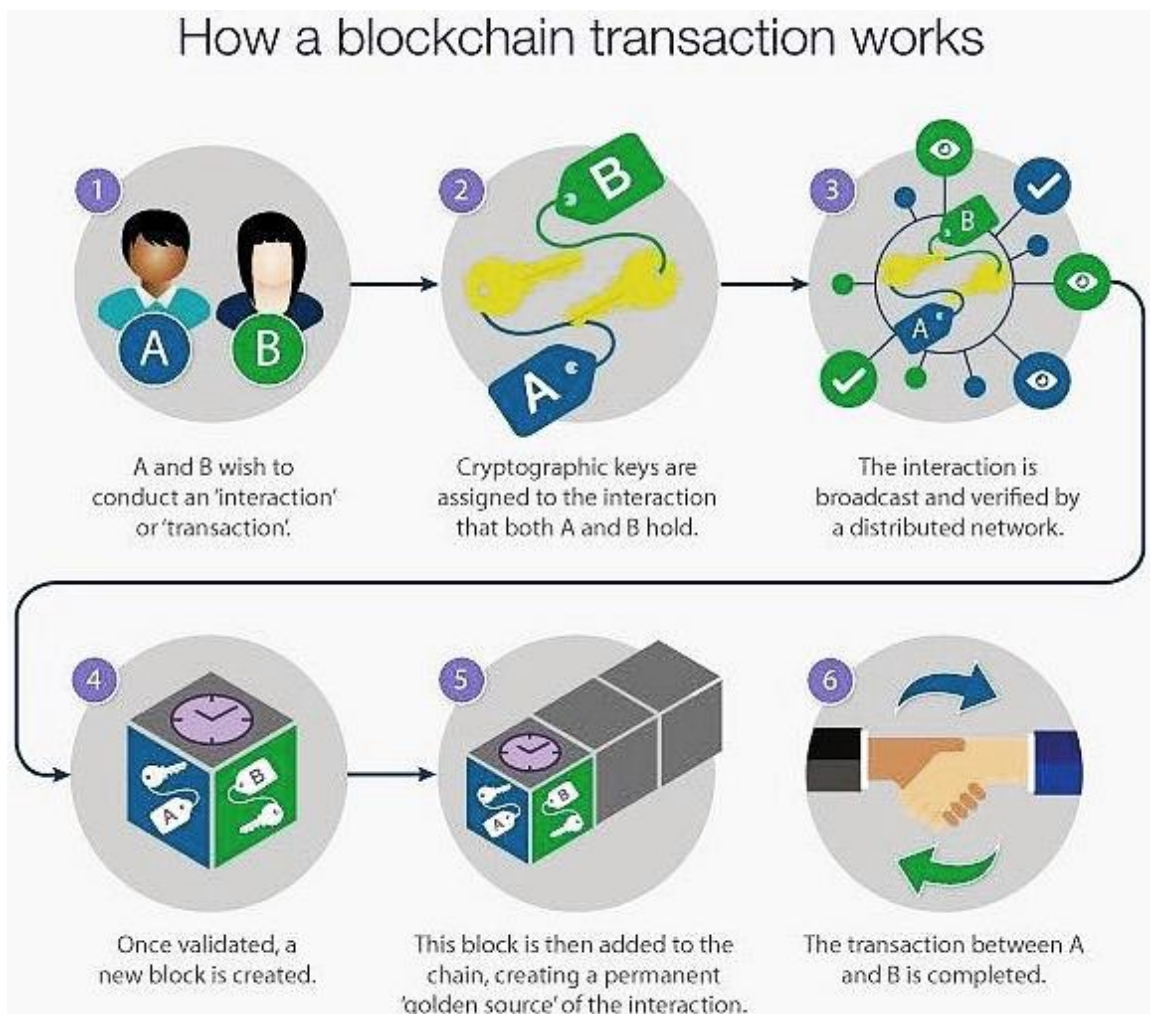
**Step 1)** Some person requests a transaction. The transaction could be involved cryptocurrency, contracts, records or other information.

**Step 2)** The requested transaction is broadcasted to a P2P network with the help of nodes.

**Step 3)** The network of nodes validates the transaction and the user's status with the help of known algorithms.

**Step 4)** Once the transaction is complete the new block is then added to the existing blockchain. In such a way that is permanent and unalterable.

A sample example is illustrated in below figure:



## What is the Genesis Block?

The first block in the blockchain is known as the genesis block. This was built in the year 2009. It is the universal parent of all the blocks in the blockchain. In other words, if people begin at any block and watch the chain counterclockwise then they will ultimately come at the genesis block.

Every node perpetually begins with a blockchain of at least one block because the genesis block cannot be modified. Every node always recognizes the genesis block's hash and structure. It also recognizes its fixed time when it was created and even its single transaction. Thus, every node has the starting point for the blockchain, a secure "root" from which to build a trusted blockchain.

## Features of Blockchain / Why Do We Need Blockchain?

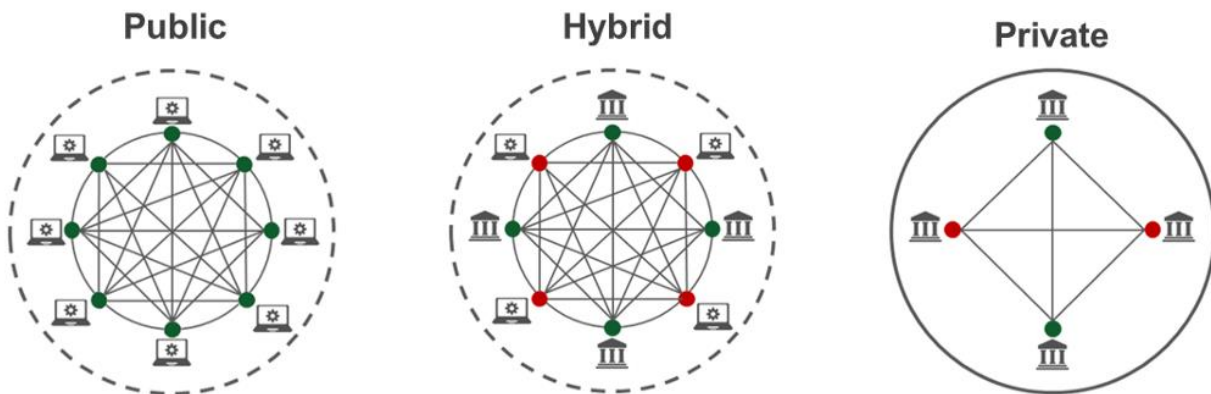
Here, are some reasons why Blockchain technology has become so popular.

- **Resilience:** Blockchains is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.
- **Time Reduction:** In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.
- **Reliability:** Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.
- **Unchangeable Transactions:** By registering transactions in chronological order, Blockchain certifies the unalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be removed or modified.
- **Fraud Prevention:** The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.
- **Security:** Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.
- **Transparency:** Changes to public blockchains are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.
- **Collaboration:** Allows parties to transact directly with each other without the need for mediating third parties.
- **Decentralized:** There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

## Different Types of Blockchains / Blockchain Variants:

There are three primary types of blockchains, which do not include traditional databases or distributed ledger technology (DLT) that are often confused with blockchains.

1. Public blockchains like Bitcoin and Ethereum
2. Private blockchains
3. Hybrid blockchains like Dragonchain



### Public Blockchains:

Public blockchains are open source. They allow anyone to participate as users, miners, developers, or community members. All transactions that take place on public blockchains are fully transparent, meaning that anyone can examine the transaction details.

- Public blockchains are designed to be fully decentralized, with no one individual or entity controlling which transactions are recorded in the blockchain or the order in which they are processed.
- Public blockchains can be highly censorship-resistant, since anyone is open to join the network, regardless of location, nationality, etc. This makes it extremely hard for authorities to shut them down.
- Lastly, public blockchains all have a token associated with them that is typically designed to incentivize and reward participants in the network.
- Public blockchains are limited in the fact that these networks are slow and transactions take a lot of time due to encryption methods
- Example: Bitcoin, Ethereum, Litecoin, etc.



## **Private Blockchains:**

Private blockchains, also known as permissioned blockchains, possess a number of notable differences from public blockchains.

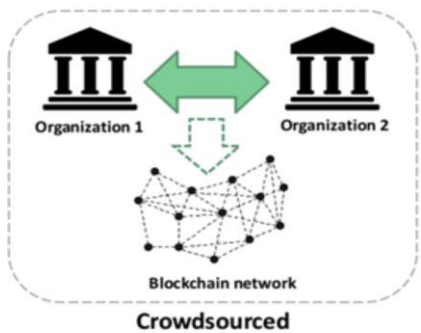

- Participants need consent to join the networks
- Transactions are private and are only available to ecosystem participants that have been given permission to join the network
- Private blockchains are more centralized than public blockchains
- Private blockchains are valuable for enterprises who want to collaborate and share data, but don't want their sensitive business data visible on a public blockchain.
- Private blockchains are much faster and cheaper as they can be controlled by a specific amount of users and the consensus can be regulated.
- Example: Hyperledger, R3 Corda, etc.

## **Hybrid Blockchains:**

Hybrid blockchain combines the privacy benefits of a permissioned and private blockchain with the security and transparency benefits of a public blockchain. That gives businesses significant flexibility to choose what data they want to make public and transparent and what data they want to keep private.

- The hybrid blockchain platform allows us to easily connect with other blockchain protocols. Allowing for a multi-chain network of blockchains
- Also, being able to post to multiple public blockchains at once increases the security of transactions, as they benefit from the combined hashpower being applied to the public chains.
- Example: Dragonchain, Bankchain, etc.

## Blockchain vs. Shared Database:

Parameters	Blockchain	Shared Database
Operations	Insert	Create / Read / Update and Delete
Replication	Full replication on every peer	Master-slave or Multi-master
Consensus	Most of the peers agree on the outcome of transactions.	Distributed transactions which held in two phases commit and Paxos.
Validation	Global rules enforced on the whole blockchain system.	Offers only local integrity constraints
Disintermediation	Allowed with blockchain.	Not allowed.
Confidentiality	Fully confidential	Not totally confidential
Robustness	Fully robust technology.	Not entirely robust.
Schematic Diagram		

## Blockchain Use Cases:

Blockchain Technology is used widely in the different sectors as given in the following table.

Sector	Usage
Markets	<ul style="list-style-type: none"><li>• Billing, monitoring and Data Transfer</li><li>• Quota management in the Supply Chain Network</li></ul>
Government Sector	<ul style="list-style-type: none"><li>• Transnational personalized governance services</li><li>• Voting, propositions P2P bond,</li><li>• Digitization of documents/ contracts and proof of ownership for transfers</li><li>• Registry &amp; Identify</li><li>• Tele-attorney service</li><li>• IP registration and exchange</li><li>• Tax receipts Notary service and document registry</li></ul>
IOT	<ul style="list-style-type: none"><li>• Agricultural &amp; drone sensor networks</li><li>• Smart home networks</li><li>• Integrated smartcity.</li><li>• Smart home sensors</li><li>• Self-driving car</li><li>• Personalized robots, robotic component</li><li>• Personalized drones</li><li>• Digital Assistants</li></ul>
Health	<ul style="list-style-type: none"><li>• Data management</li><li>• Universal EMR Health databanks</li><li>• QS Data Commons</li><li>• Big health data stream analytes</li><li>• Digital health wallet Smart property</li><li>• Health Token</li><li>• Personal development contracts</li></ul>
Finance & Accounting	<ul style="list-style-type: none"><li>• Digital Currency Payment</li><li>• Payments &amp; Remittance</li><li>• Decartelized Capital markets using a network of the computer on the Blockchain</li><li>• Inter-divisional accounting</li><li>• Clearing &amp; Trading &amp; Derivatives</li><li>• Bookkeeping</li></ul>

## Important Real-Life Use Cases of Blockchain

- **Dubai:** The Smart City In the year 2016, smart Dubai office introduced Blockchain strategy. Using this technology entrepreneurs and developers will be able to connect with investor and leading companies. The objective is to implement blockchain base system which favors the development of various kind of industries to make Dubai 'the happiest city in the world.'
- **Incent Customer Retention:** Incent is CRaaS (Consumer retention as a service) based on the Blockchain technology. It is a loyalty program which is based on generating token for business affiliated with its related network. In this system, blockchain is exchanged instantaneously, and it can be stored in digital portfolios of user's phone or accessing through the browser.
- **Blockchain for Humanitarian Aid:** In January 2017 the united nations world food program started a project called humanitarian aid. The project was developed in rural areas of the Sindh region of Pakistan. By using the Blockchain technology, beneficiaries received money, food and all type of transactions are registered on a blockchain to ensure security and transparency of this process.

## Limitations of Blockchain technology:

- **Higher Costs:** Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand.
- **Slower Transactions:** Nodes prioritize transactions with higher rewards, backlogs of transactions build up.
- **Smaller Ledger:** It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.
- **Transaction Costs, Network Speed:** The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.
- **Risk of Error:** There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.
- **Wasteful:** Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.