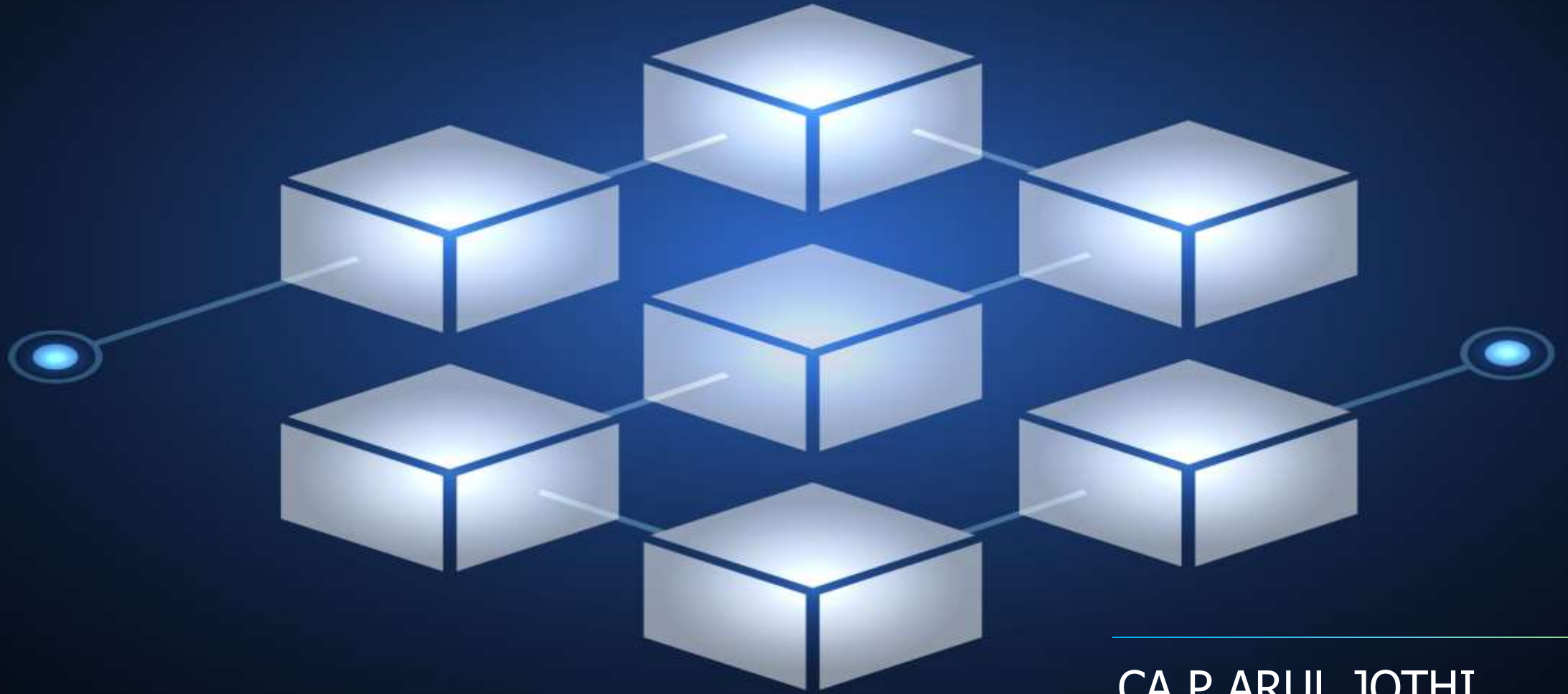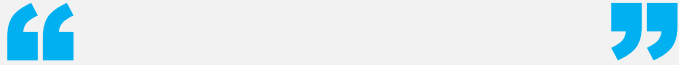# BLOCKCHAIN TECHNOLOGY

CA P ARUL JOTHI

TIRUPPUR

Best BlockChain Quotes

" "

The blockchain does one thing: It replaces third-party trust with mathematical proof that something happened

Adam Draper , American Businessman

" "

Everything will be tokenized and connected by a blockchain one day

Fred Ehrsam, American Business Executive

" "

The Internet is programmable information. The blockchain is programmable scarcity!

Balaji Srinivasan, American Entrepreneur

History

- 1982 - Cryptographer David Chaum first proposed a blockchain-like protocol

- 1991 - A cryptographically secured chain of blocks was described by Stuart Haber and W. Scott Stornetta

- 1992 - Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block.

- 2008 - Satoshi Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network

The Raise

The words *block* and *chain* were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, *blockchain,* by 2016.

Meaning

○ Blockchain is a shared, immutable ledger

○ It facilitates the process of recording transactions and tracking assets in a business network.

○ An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

○ Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

What is Blockchain?

Ex….

>> Lets Imagine a digital ledger that records transactions.

>> But it is not stored in one central location.

>> Instead, it's spread out across a network of computers.

>> This means that the information stored on the ledger is decentralized and can't be controlled by any single entity.

>> This decentralized digital ledger is known as Blockchain.

BLOCKCHAIN KEY CONCEPTS & COMPONENTS

⟶ BLOCK

⟶ NODE

⟶ LEDGER

⟶ WALLET

⟶ CONSENSUS MECHANISM

⟶ CRYPTOGRAPHY

BLOCK	NODE	LEDGER
✓ A collection of transactions that have been approved by the network are contained in each block. ✓ The data contained in a block is regarded as permanent and unchangeable once it is added to the Blockchain. ✓ The basis of a Blockchain in Blockchain technology is a block.	• The individual computers or gadgets that make up a Blockchain's network are referred to as nodes. • They are in charge of approving transactions, including new blocks, maintaining a copy of the Blockchain, and validating transactions.	• An electronic ledger is essentially an updated database that contains all transactions. • It is made up of several blocks, each of which contains at least one transaction, and these blocks are connected by a chain employing cryptography. • Types 　• Public ledger 　• Distributed ledger 　• Decentralised ledger

Ledger Types

○ **Public ledger:**

- It is accessible to everybody and transparent.

- In the Blockchain network, everything can be read or written by anyone.

○ **Distributed ledger:**

- All nodes in a distributed ledger have a local copy of the database.

- Here, a number of nodes work together to complete the task,

- i.e., confirm transactions and add blocks to the Blockchain.

○ **Decentralized Ledger:**

- No single node or group of nodes has central control in a decentralized ledger.

- Every node takes part in the job's execution.

| WALLET	MERKLE TREE	CRYPTOGRAPHY
• A software program called a crypto wallet, often called a digital wallet or a cryptocurrency wallet, enables users to transmit, receive, and store **DIGITAL CURRENCY.** • The Blockchain network's nodes each have a wallet. • Using public and private key pairs, a Blockchain network may maintain the privacy of a wallet.	• Every leaf node is labelled with the cryptographic hash of a data block • Every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. • Hash trees allow efficient and secure verification of the contents of large data structures..	• It is an essential part of Blockchain technology because it protects the confidentiality and integrity of transactions on the Blockchain. • Cryptography has developed **UNBREAKABLE ENCRYPTION** techniques by using **HASH** functions drawing on a foundation of mathematics, particularly probability theory, and knowledge of game theory.

How Blockchain Works.....
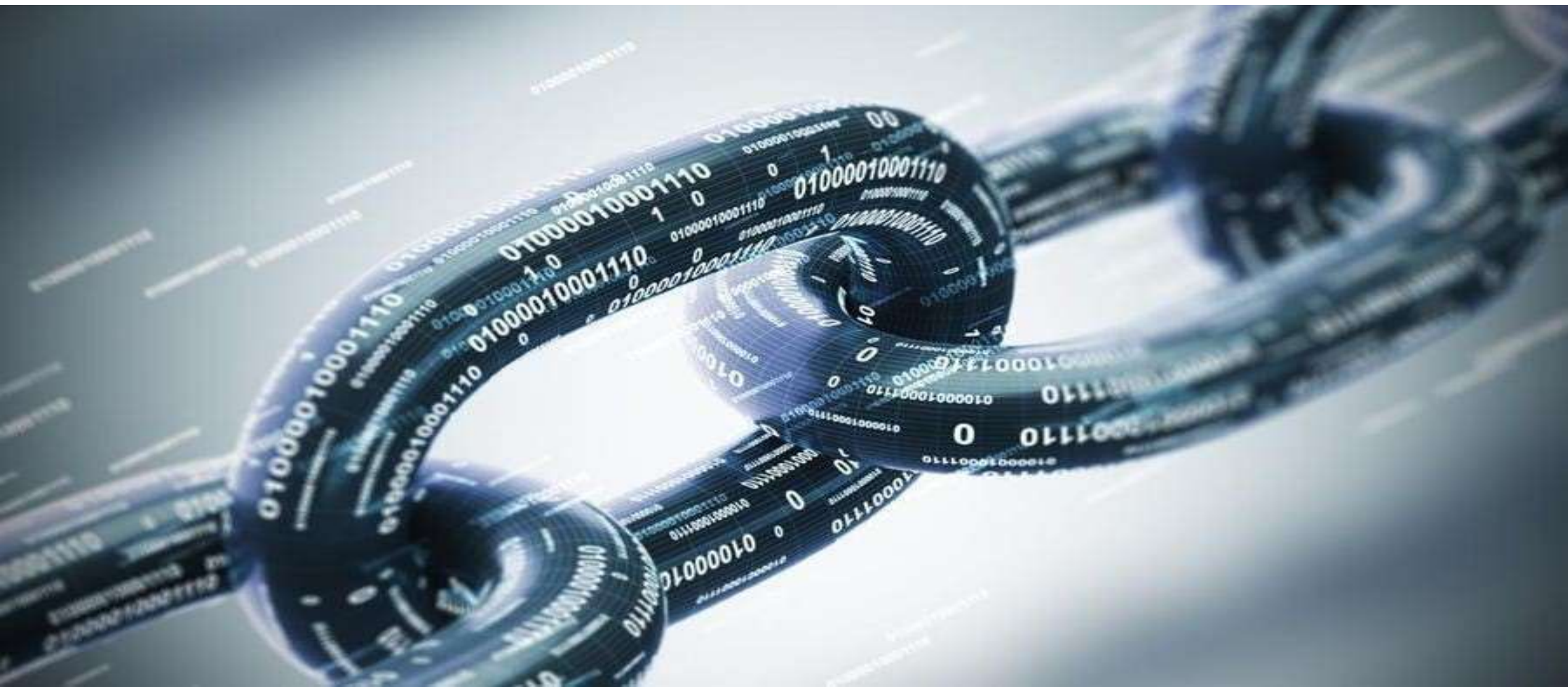
# As each transaction occurs, it is recorded as a "block" of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.
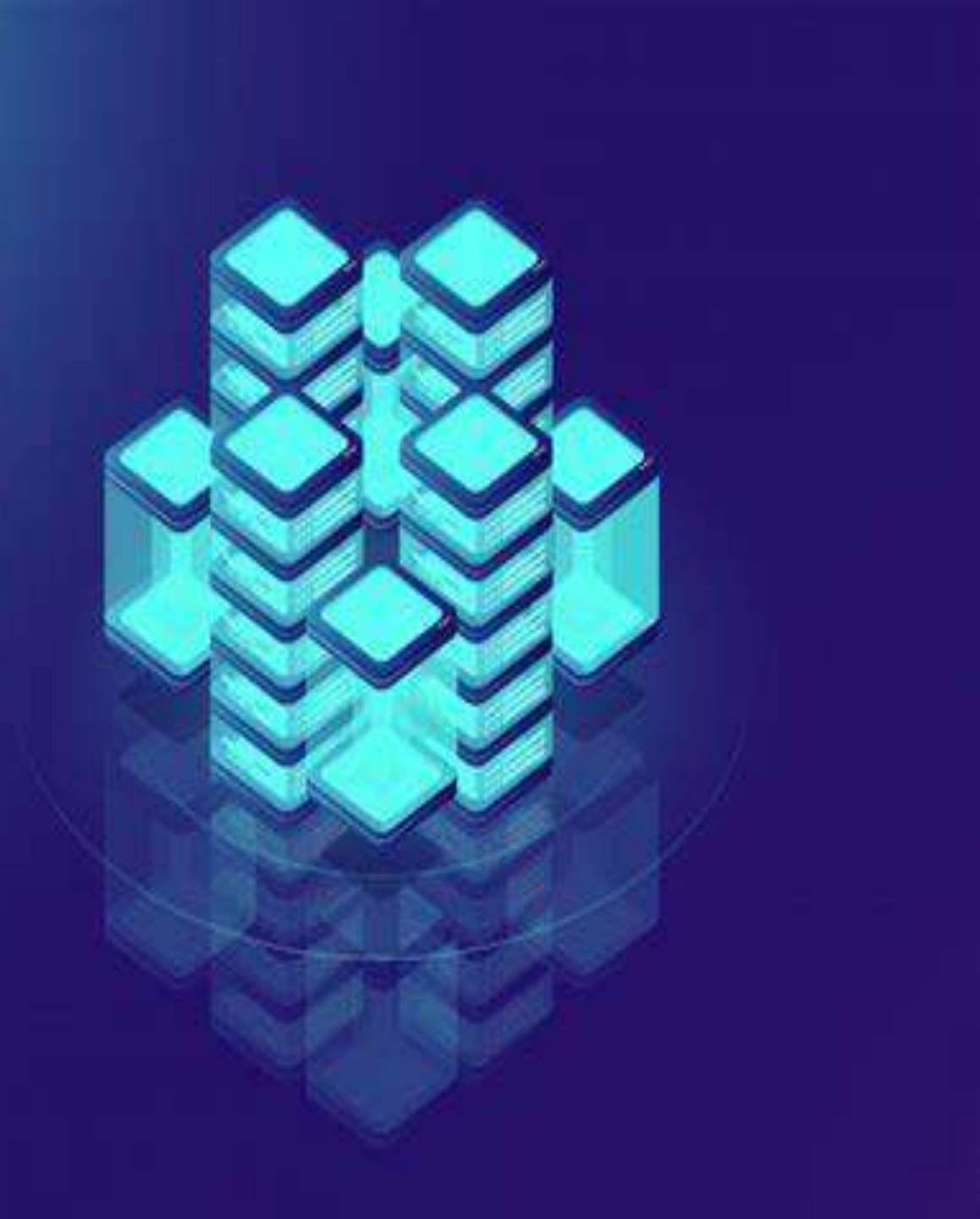
How Blocks are Created?

○ A majority of nodes must verify and confirm the legitimacy of the new data before a new block can be added to the ledger.

○ **Ex**… For a cryptocurrency, they might involve ensuring that new transactions in a block were not fraudulent, or that coins had not been spent more than once.

○ This is different from a standalone database or spreadsheet, where one person can make changes without oversight.

○ How these new blocks are created is key to why blockchain is considered highly secure.

# Each block is connected to the ones before and after it
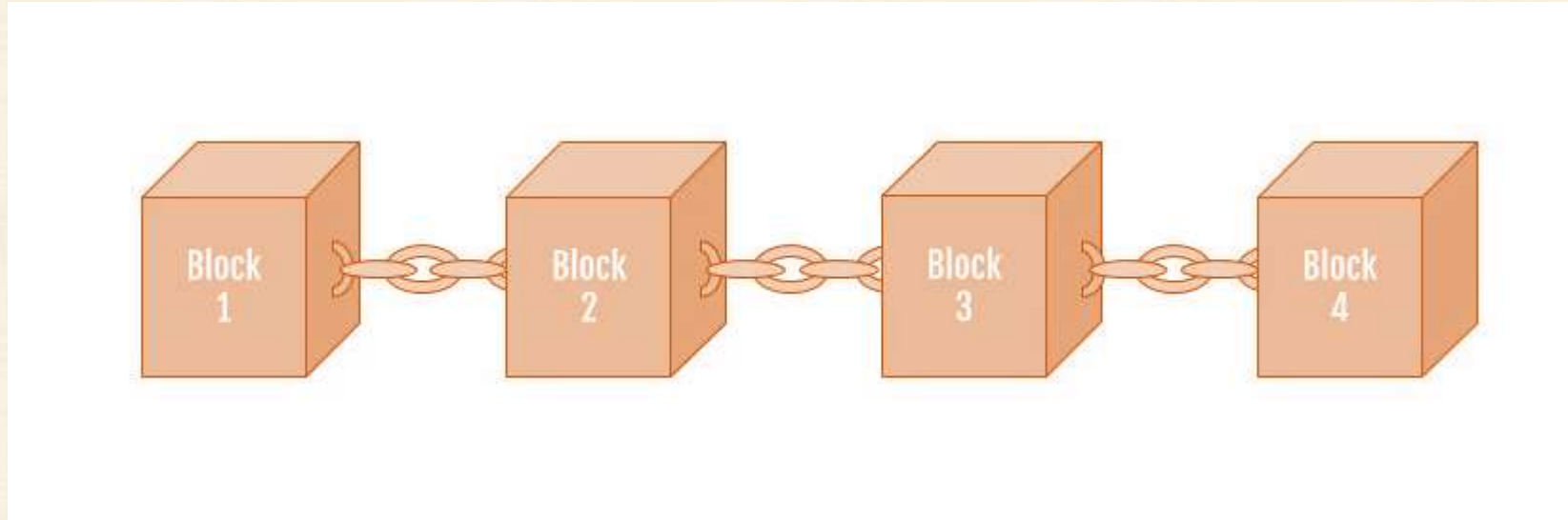
These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

Transactions are blocked together in an irreversible chain:
A Blockchain

- Each additional block strengthens the verification of the previous block and hence the entire blockchain.

- This renders the blockchain tamper-evident, delivering the key strength of immutability.

- This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.
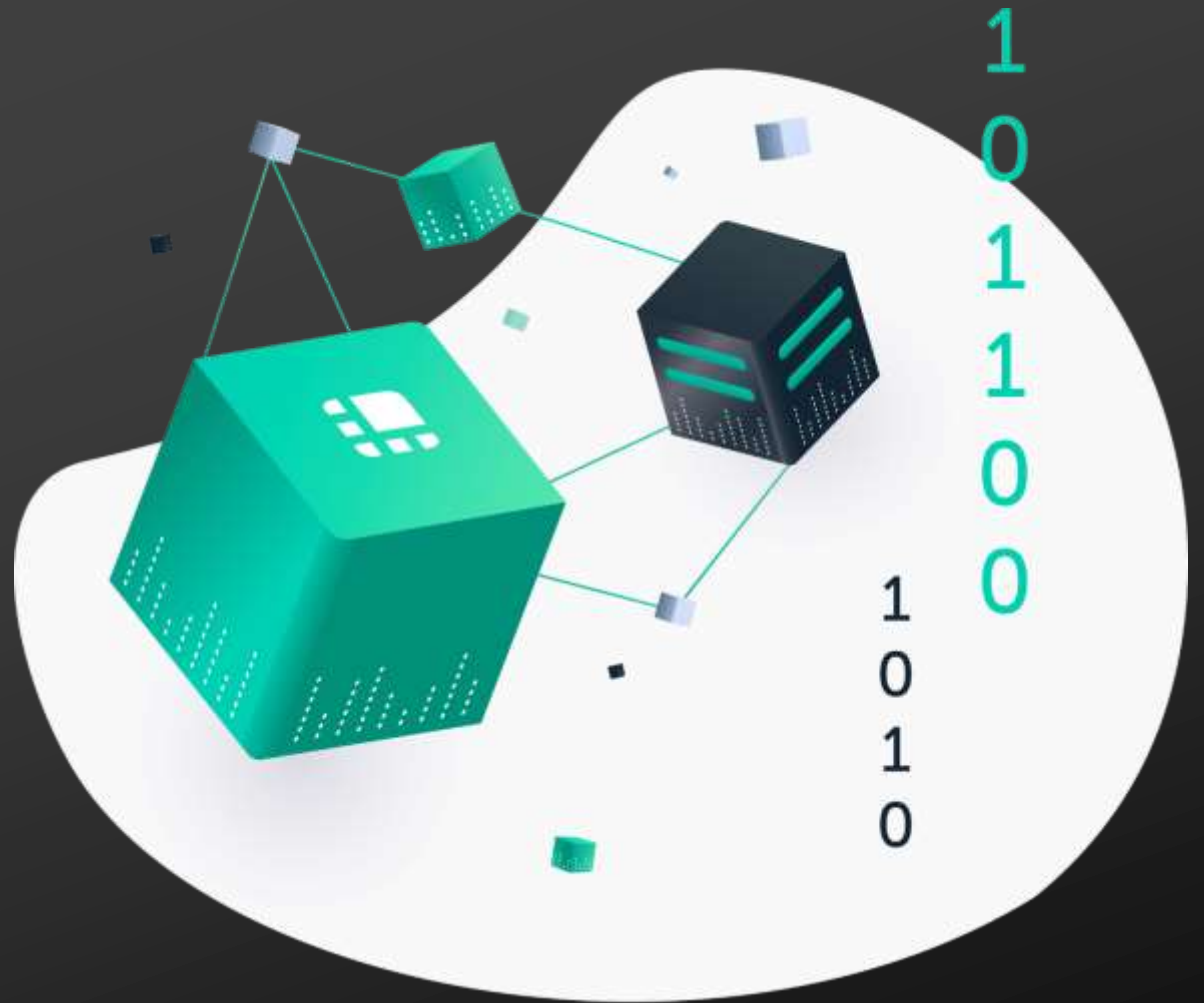
Distributed network

- Blockchain is a decentralized ledger tracking of one or more digital assets on a peer-to-peer network

- When we say a peer-to-peer network, it means a decentralized peer-to-peer network where all the computers are connected in some way, and where each maintains a complete copy of the ledger and compares it to other devices to ensure the data is accurate.

- This is unlike a bank, where transactions are stored privately and are managed only by the bank.

Key Elements

Immutable Records

○ No participant can change or tamper with a transaction after it's been recorded to the shared ledger.

○ If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart Contracts

○ To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically.

○ A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.
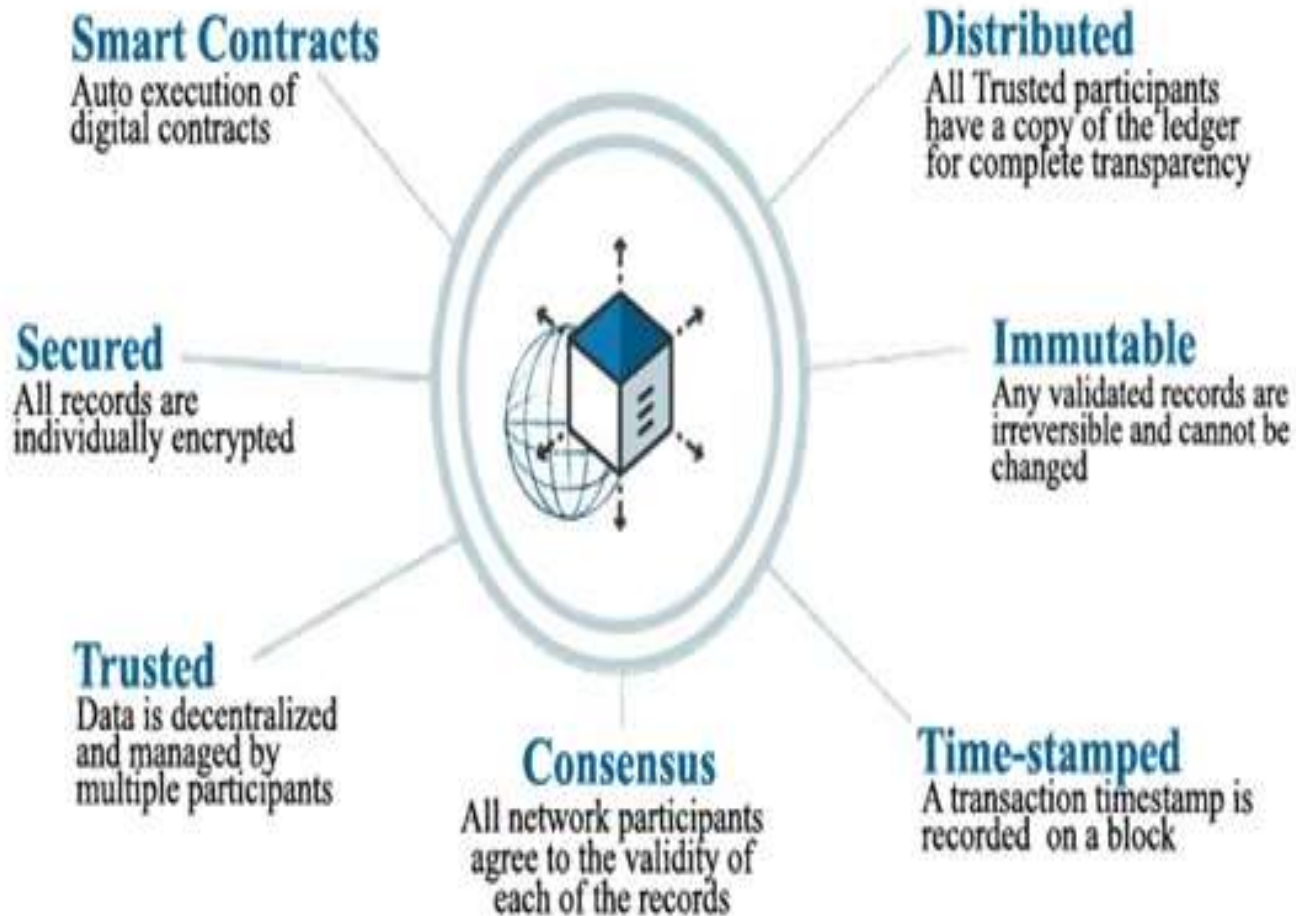
Cryptocurrency & Blockchain

➢ Cryptocurrency is a digital money.

➢ Cryptocurrency units are referred to as coins or tokens.

➢ Blockchain is the technology that enables cryptocurrency

➢ A Blockchain is a distributed peer-to-peer database with strict data-addition rules

Metaverse & Blockchain

○ In the Metaverse, people can interact with one another, create and monetize their own content, and interact with virtual objects.

○ Blockchain is used to create a more transparent and secure way to handle digital assets in the Metaverse, such as virtual property and non-fungible tokens (NFTs).

○ In other words, Blockchain is a technology used to create a secure and transparent way to handle digital assets in the Metaverse, but the Metaverse is a broader concept that includes the virtual reality shared by millions of users, in which people can interact with each other and with virtual objects.

Properties of Block Chain

Smart Contracts
Auto execution of digital contracts

Secured
All records are individually encrypted

Trusted
Data is decentralized and managed by multiple participants

Consensus
All network participants agree to the validity of each of the records

Distributed
All Trusted participants have a copy of the ledger for complete transparency

Immutable
Any validated records are irreversible and cannot be changed

Time-stamped
A transaction timestamp is recorded on a block

CONSENSUS

❖ Every blockchain succeeds because of the consensus algorithms.

❖ In simple, the consensus is a decision-making process for the group of nodes active on the network.

❖ Here, the nodes can come to an agreement quickly and relatively faster.

❖ When millions of nodes are validating a transaction, a consensus is absolutely necessary for a system to run smoothly.

❖ Nodes might not trust each other, but they can trust the algorithms that run at the core of it.

Block Chain Types

Public

Private

Consortium

Hybrid

❏ A distributed ledger system **without restrictions, and permissions** .

❏ It makes the system transparent and trustless by allowing anybody to join the network and validate transactions.

❏ Such Blockchains are primarily used for cryptocurrency exchange and mining.

❏ The Bitcoin Blockchain, the most well-known example of a public Blockchain, uses a proof-of-work consensus process to confirm transactions and add them to the Blockchain.
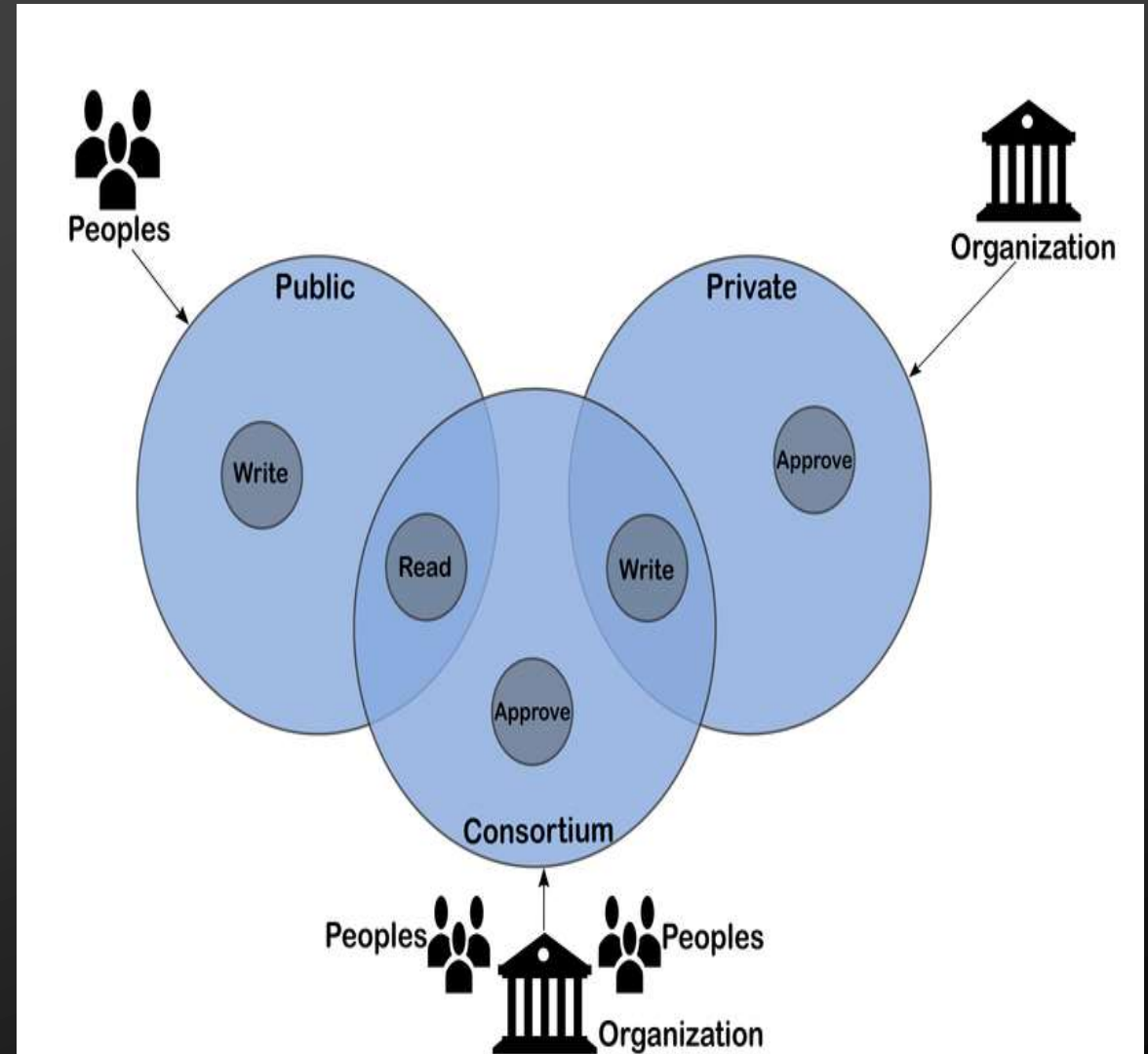
PUBLIC BLOCKCHAIN

PRIVATE BLOCKCHAIN
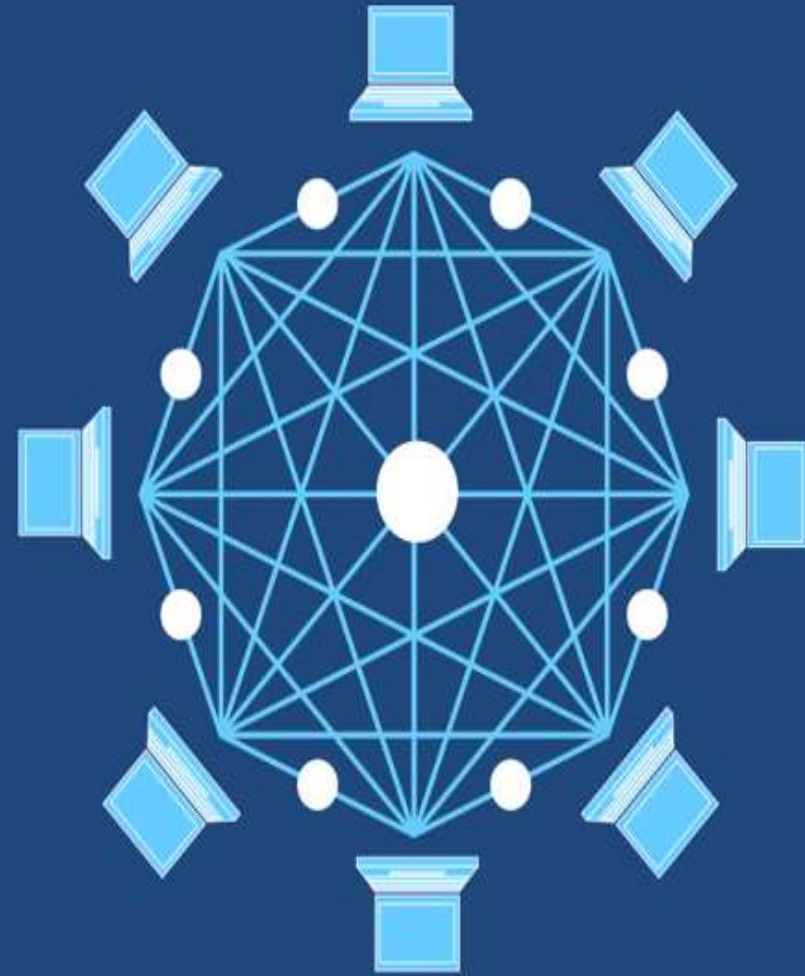
- Referred to as a **permissioned Blockchain**,

- It is a digital ledger that only allows a certain number of users to access it.

- Only through an invitation where their identification or other necessary information is valid and verified may join a private Blockchain network.

- Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network.

- Controlled Organisation controls the Network and its permissions

- Thus, private blockchains are similar in use as a public blockchain but have a small and restrictive network.

❑ A private Blockchain that is owned and run by a number of different companies is referred to as a consortium Blockchain

❑ Here more than one organization is involved in providing access to pre-selected nodes for reading, writing, and auditing the Blockchain, **or** we might say that more than one central authority is in control.

❑ A particular kind of semi-decentralized network is a consortium Blockchain.

❑ An example of a consortium Blockchain is IBM Food Trust.

CONSORTIUM BLOCKCHAIN

❑ The term "hybrid Blockchain" is frequently used to describe a system that combines both public and private Blockchains.

❑ It combines key elements from both private and public Blockchains.

❑ Members of the hybrid Blockchain can determine which transactions are made public and who is allowed to use the Blockchain.

❑ In such Blockchains, transactions can be made public for verification purposes but are often not made accessible to everyone.

HYBRID BLOCKCHAIN
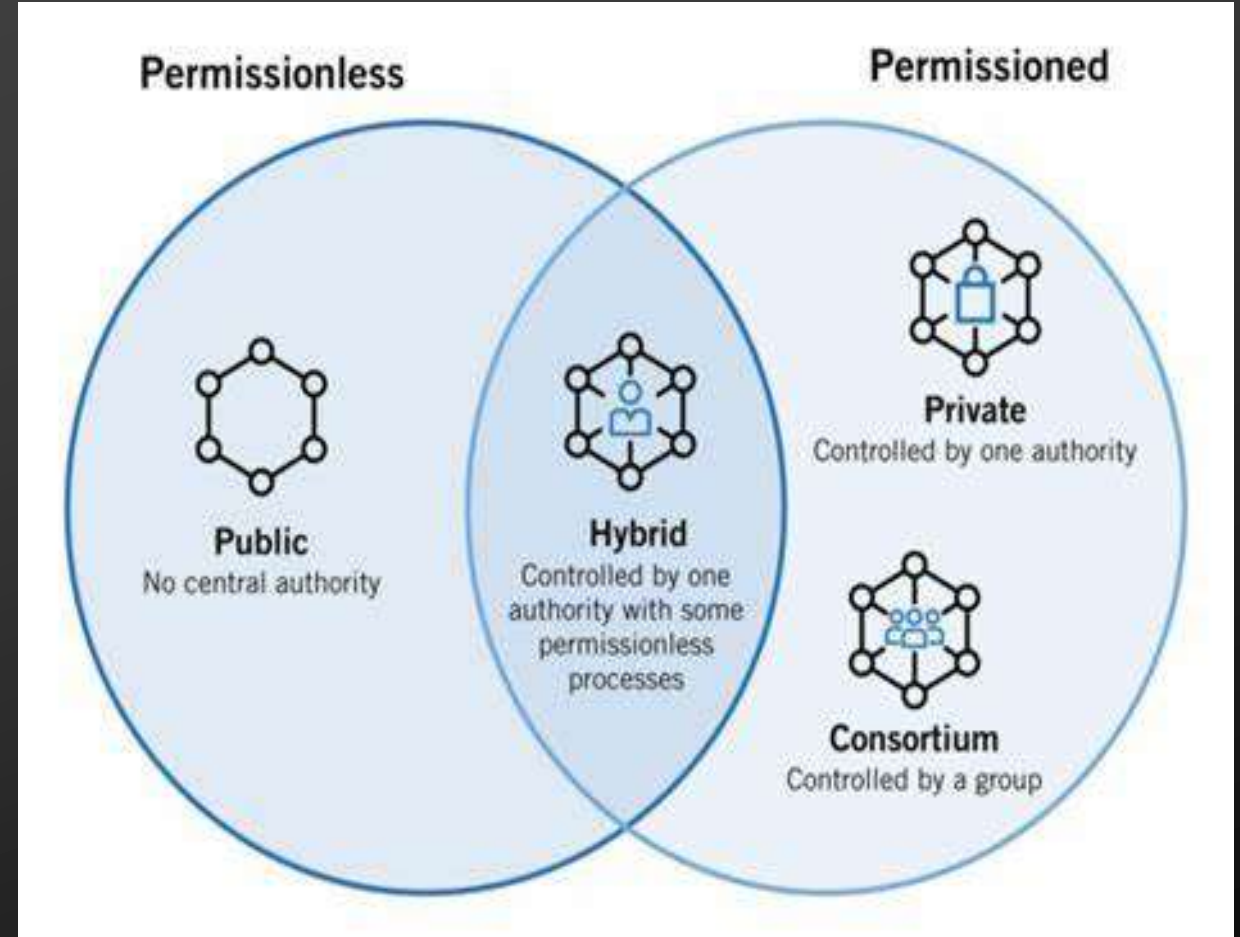
Use cases of Blockchain

○ Blockchain use cases in Financial Sector

○ Blockchain use cases in Business Sector

○ Blockchain use cases in Government & Public Sector

○ Blockchain in Retail Fashion & Luxury

○ Blockchain in sports and E-sports

○ Blockchain in Legal Industry

○ Decentralised Finance – DeFi etc…

Blockchain in INDIA

LIVE CHAINS

Certificate Chain

CBSE

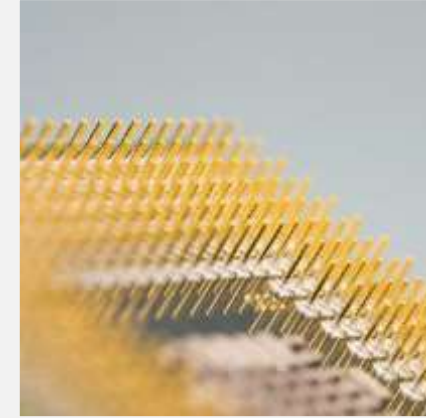&

Karnataka

SSLC & PUC

Property Chain

Karnataka

Bhoomi

e-asthi &

e-swathu

Document Chain

Karnataka

Birth Certificates

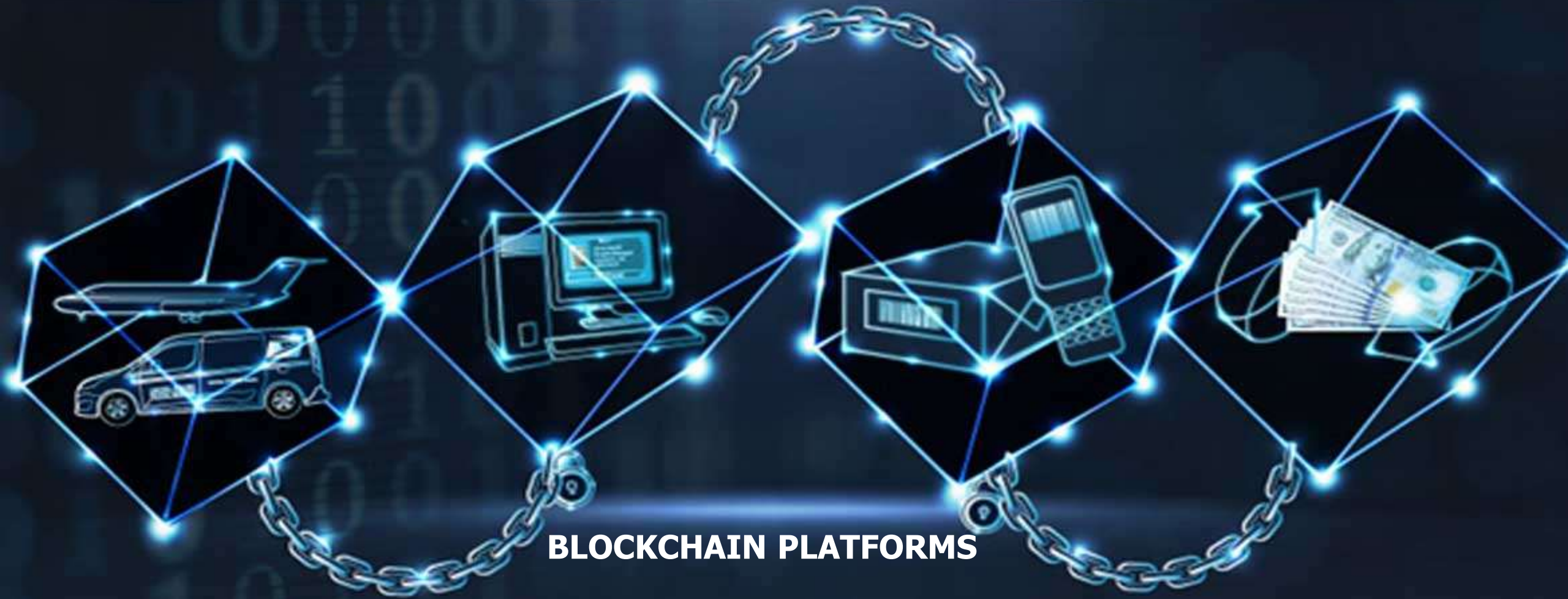Death Certificates

Caste Certificates

Income Certificates

Logistics Chain

The Karnataka State Drugs Logistic and Warehousing Society is using this chain

for more refer

https://dlc.kar.nic.in/

BLOCKCHAIN PLATFORMS

by
Indian Ministry of Electronics & Information Technology

Ministry of Electronics & Information Technology
NATIONAL INFORMATICS CENTRE

CENTRE OF EXCELLENCE IN BLOCKCHAIN TECHNOLOGY

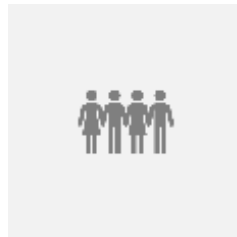| Hyperledger Fabric	Hyperledger Sawtooth	Ethereum
• It has a membership service and consensus. • Members of the fabric network can use network work together in this platform. • Hyperledger Fabric provides the user a secure and scalable platform to support their confidential contracts and private transactions..	• It has consensus mechanism known as Proof of Elapsed Time. • A Sawtooth Library is being developed, which will allow programmers of customized distributed ledgers to select and choose whatever parts of Sawtooth to employ in their applications.	• The main aim of this platform is to nullify the third parties' access who save data for further financial instrument tracking. • Ethereum has the largest community of core protocol developers, crypto-economic researchers, cypherpunks, and mining organizations.

CASE STUDIES / PILOT START
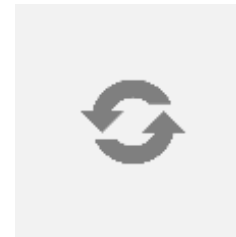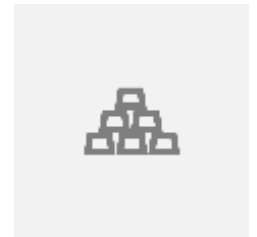
There is an opportunity for success
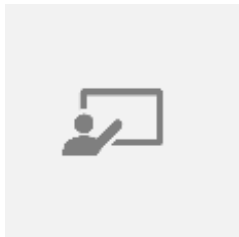
GST Chain   Land Registeration   Blood Bank   PDS   Remote Voting Chain

Pros

- Higher Accuracy of Transactions

- No Need for Intermediaries

- Extra Security

- More Efficient Transfers

- Automated Process

- No Alteration of Transactions

Cons

- Limit on Transactions per Second

- High Energy Costs

- Risk of Asset Loss

- Potential for Illegal Activity

How To Build a Blockchain?

Python

Lorem ipsum dolor sit amet

Javascript

Lorem ipsum dolor sit amet

Node.js

Lorem ipsum dolor sit amet

Real-time Applications

Supply Chain Management:

○ Walmart Canada, for instance, used Blockchain to develop an automated system for controlling payments to and invoices from its 70 third-party freight providers.

○ The company currently uses a Blockchain-based system to track the origin of over 25 products from 5 different suppliers.

○ This aids the business in ensuring food safety and enhancing client confidence.

Banking and Finance:

○ J.P. Morgan, a multinational financial services company, employs Blockchain technology to facilitate payments between international banks.

○ This includes transfers made to beneficiary banks in other markets by Taiwanese banks.

○ JPMorgan Chase & Co. declared the adoption of Blockchain technology for collateral settlements last year.

Real Estate:

○ ATLANT has created a Blockchain-based. It enables real estate and rental property transactions using Blockchain technology.

○ Real estate can be tokenized, and after that, it can be exchanged online, like equities on a stock exchange.

Thank You

CA P ARUL JOTHI

+91 97906 13451

caaruljothi@live.com