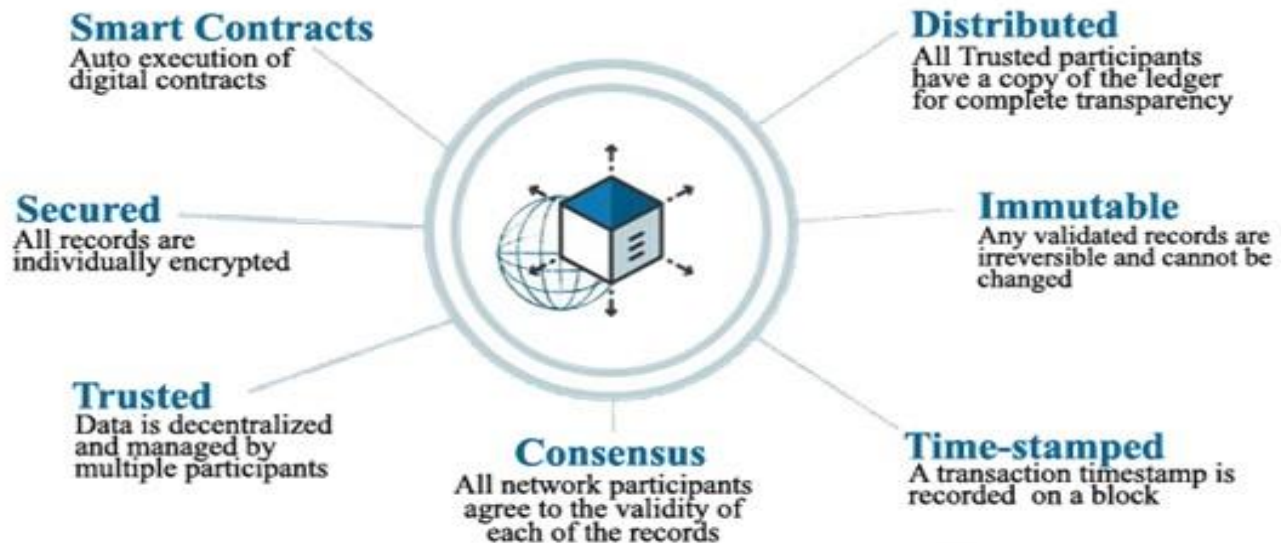# blockchain

Smita Kulkarni-Pai

What is blockchain?

- Blockchain is a shared, immutable ledger that 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.

Properties of Block Chain

Smart Contracts
Auto execution of digital contracts

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

Secured
All records are individually encrypted

Immutable
Any validated records are irreversible and cannot be changed

Trusted
Data is decentralized and managed by multiple participants

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

Time-stamped
A transaction timestamp is recorded on a block

Why is Blockchain important?

- Business runs on information. The faster information is received and the more accurate it is, the better.

- Blockchain is ideal for delivering that information because it provides immediate, shared, and observable information that is stored on an immutable ledger that only permissioned network members can access.

- A blockchain network can track orders, payments, accounts, production and much more.

- And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, and new efficiencies and opportunities.

Key elements of a blockchain

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

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.

Key elements of a blockchain

Smart contracts

To speed transactions, a set of rules that are called a smart contract is stored on the blockchain and run automatically. A smart contract defines conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

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. It can even record the condition, such as the temperature of a food shipment.

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.

How blockchain works

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. Rendering the blockchain tamper-evident, delivering the key strength of immutability. Removing the possibility of tampering by a malicious actor, and builds a ledger of transactions you and other network members can trust.

Benefits of blockchain

Greater trust

With blockchain, as a member of a embers-only network, you can rest assured that you are receiving accurate and timely data. And that your confidential blockchain records are shared only with network members to whom you granted access.

Greater security

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

More efficiencies

With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules that are called a smart contract can be stored on the blockchain and run automatically.

Types of blockchain networks

- **Public blockchain networks**

- A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include the substantial computational power that is required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

- **Private blockchain networks**

- A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, run a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.
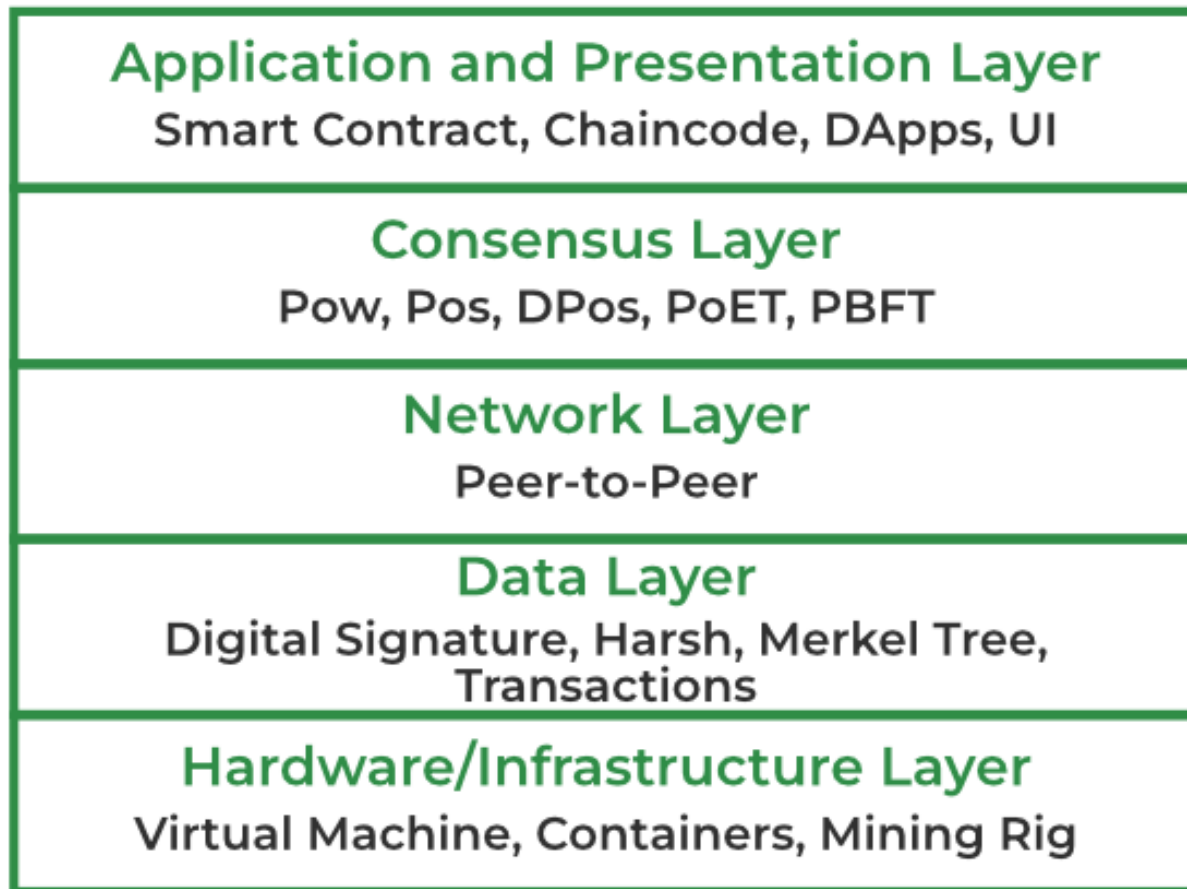
Types of blockchain networks

- **Permissioned blockchain networks**
- Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

- **Consortium blockchains**
- Multiple organizations can share the responsibilities of maintaining a blockchain. These preselected organizations determine who submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.
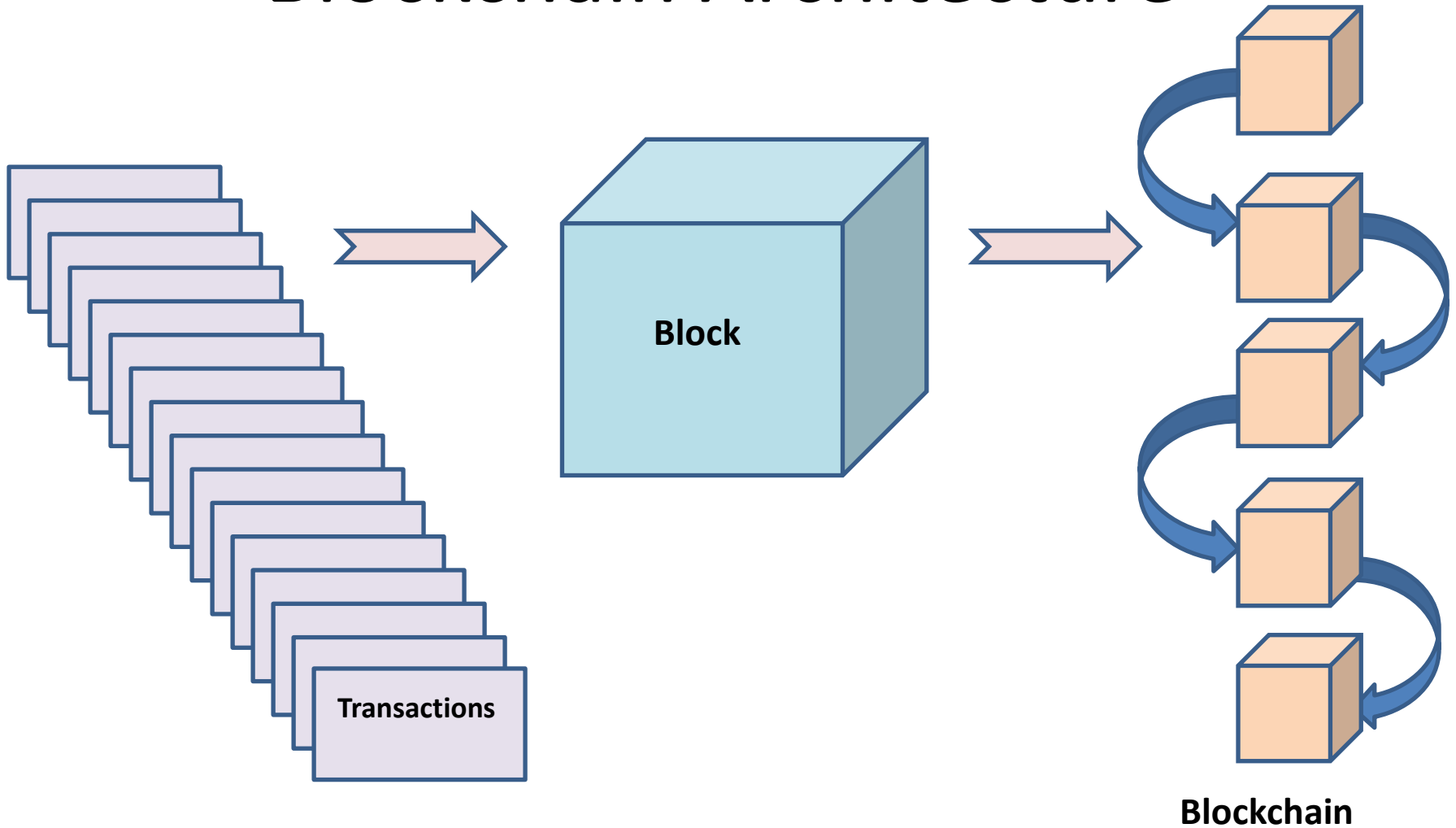
Comparision between Public, Private and Consortium Blockchain

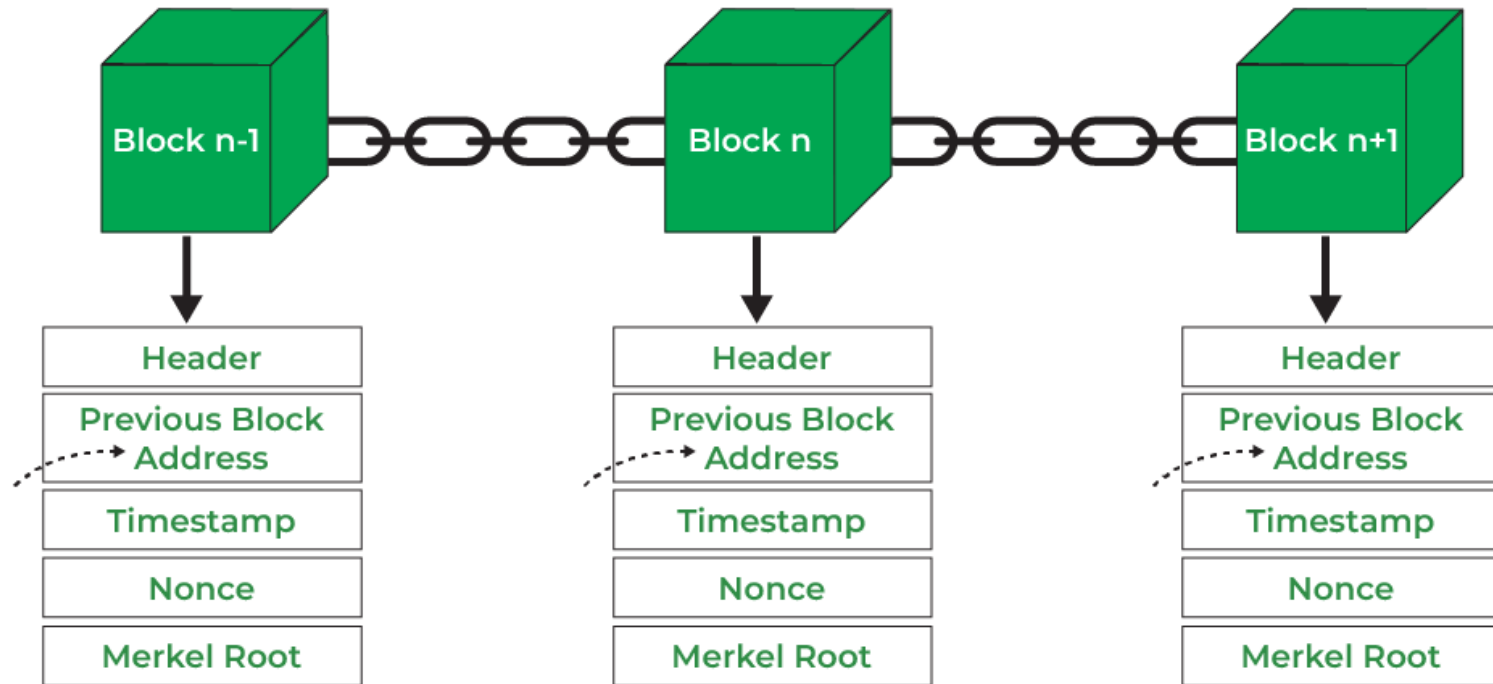| Common Features	Public Blockchain	Private Blockchain	Consortium Blockchain
Network	Fully Decentralized	Centralized	Partially Decentralized
Accessibility	Open to Anyone	Central Incharge or Single individual	more than one central incharge
Failure	No single point of failure	single pont of failure	multiple point of failure
Transaction Speed	Slower	High	Very High
Prticipants	everyone is anonymous	known and trusted participants	known and trusted participants
Energy Consumption	Very High	Low	Low
Scalability	Limited	Better	Better
Computation Power Required	High	Low	Low
Trust	Trust-free	Trusted	Trusted
Efficiency	Low	High	High
Consensus determination	All miners	Single Organization	Selected set of members
Immutability	Tampering is nearly impossible	Tampering can be possible	Tampering can be possible
Consensus Process	Permissionless	Permissioned	Permissioned
Time for Block creation	More then 10 minuts	In seconds	In seconds
Read Permission	Public	Public or Restricted	Public or Restricted
Security	Based on consensus protocols and hash functions	depends on blockchain architecture	depends on blockchain architecture
Consensus Mechanisms	PoW,PoS, etc	voting or different PoW/PoS consensus Algorithms	voting or different PoW/PoS consensus Algorithms

Blockchain Layered Architecture

Application and Presentation Layer Smart Contract, Chaincode, DApps, UI
Consensus Layer Pow, Pos, DPos, PoET, PBFT
Network Layer Peer-to-Peer
Data Layer Digital Signature, Harsh, Merkel Tree, Transactions
Hardware/Infrastructure Layer Virtual Machine, Containers, Mining Rig

Blockchain Architecture

Transactions

Block

Blockchain

Block structure in blockchain

Genesis block

- The Genesis Block, as the veritably first block in a blockchain, has several unique features. **No Previous Block:** The Genesis Block is the first block in a blockchain, which means that it has no former block to reference. As a result, it generally contains a hardcoded set of data that initializes the network and sets the foundation for posterior blocks.

- The Genesis Block has a **unique block hash and** is generally hardcoded into the blockchain software to ensure that it identifies the Genesis Block.