Blockchain Technology

- Overview of centralized system
- Distributed ledger
- Blockchain technology
- Consensus
- Smart contract
- Blockchain network
- Enterprise blockchain frameworks
- Hyperledger
- Hyperledger Sawtooth
- Hyperledger Fabric
- Development and deployment

Centralized systems

- Always owned and maintained by single authority.
- Transaction between trusted entities.
- Can easily modify or delete transactions.
- Data sharing is through API or services.
- Intermediator for participating organizations.
- Verification and Traceability very difficult.
- Not transparent for participating organizations.

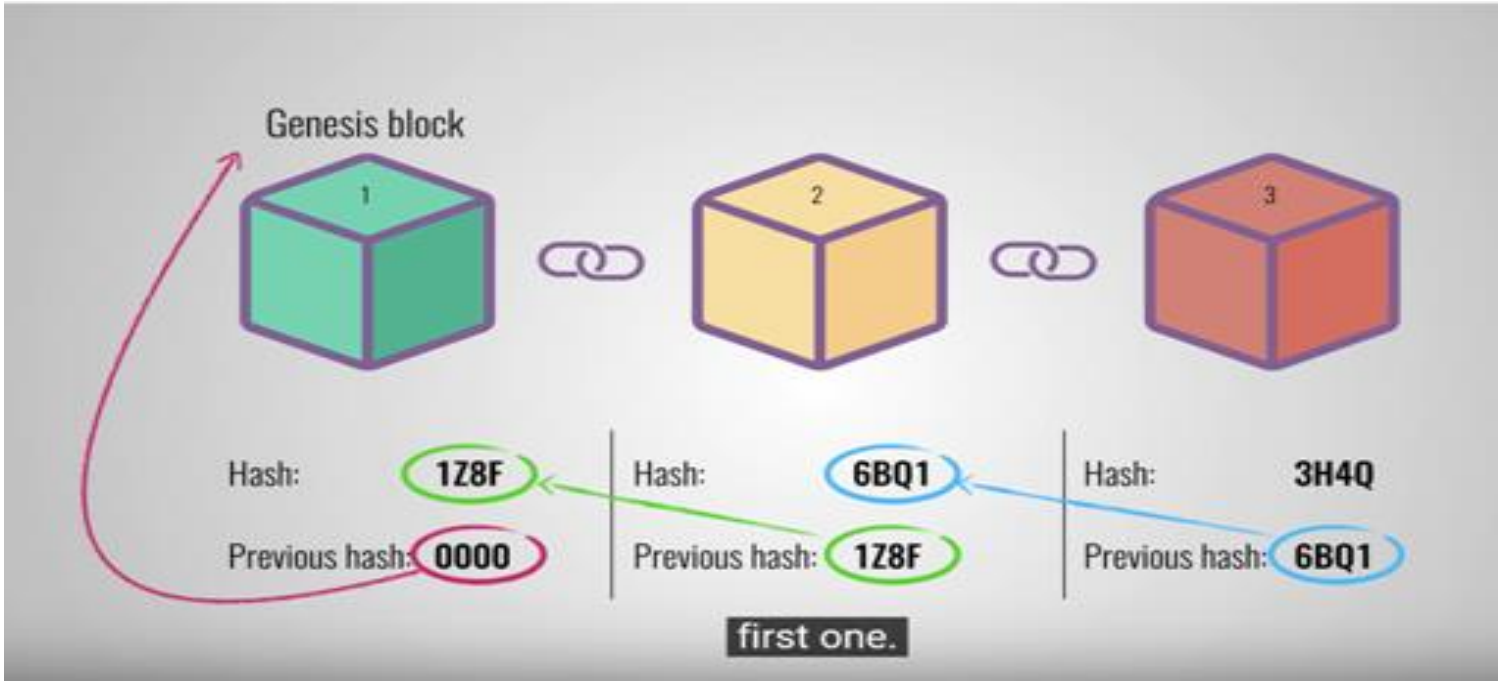
Distributed Ledger

- Digital storage system to record digital transactions/records
- Same ledger is distributed across multiple nodes
- Transaction can be submitted to any node
- Transactions are distributed and synchronized by consensus process
- Consensus is based on 3-phase commit protocol

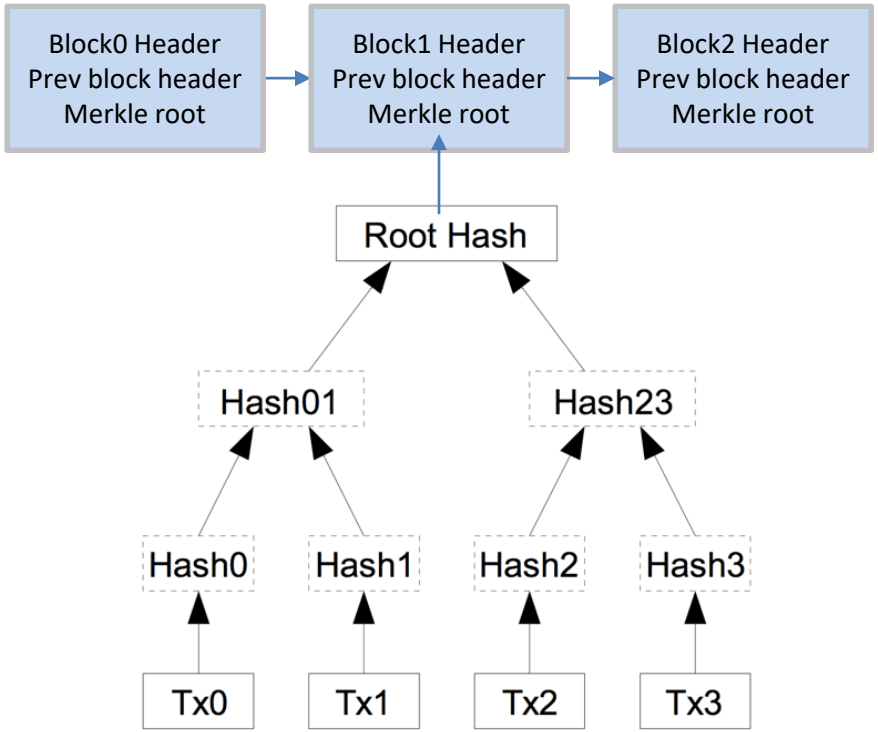
Blockchain + DLT

- Distributed system
- Immutable records
- Secured system
- Traceable transactions
- Trusted platform for data sharing

Blockchain


Genesis block
1
2
3
Hash: 1Z8F
Previous hash: 0000
Hash: 6BQ1
Previous hash: 1Z8F
Hash: 3H4Q
Previous hash: 6BQ1
first one.

How transactions are wrapped in block



Merkle Tree

- Hierarchical data structure used for organizing transactions.

- It is a binary tree where leaf node holds hash of transaction data, and middle node holds hash of its two child nodes.

- Root node hash of the tree used for determining the status of transactions in block.

Cryptography in blockchain

- Digital Certificate
- Digital Signature
- Encryption and Decryption
- Hashing
- Private Key and Public Key
- Elliptic curve cryptography is being widely used.
  (Because of its efficiency and key size, 128 bit)

Ledger store

- **Transaction store**

  - Data along with Identity in standard format
  - Transactions are verified and validated
  - A key value store for transactionid and transaction data

- **Transaction state store**

  - Holds final state of transaction after commit
  - key value store

- **Block chain store**

  - One or more cryptographically linked transactions are bundled together
  - Blocks are cryptographically linked
  - Blocks are validated before it is attached to chain
  - Genesis block is initial block of chain. It usually contains transactions related to initial settings

(Couch Db, LMDB, Level DB)

Smart contract

- Smart Contract is an agreement in digital form
- Agreement defined as **set of conditions, rules and actions**
- Actions are executed at the backend when the rules are satisfied.
- Based on state value, other actions can be triggered.
  (Payment process can be started on KYC truth from block chain)
- Access is secured (No direct access, ACL)

Consensus

- Process ensures atomic action in a distributed system
- General agreement by all participating nodes for commit or reject a transaction.
- Ensures the transactions are uniformly committed across all participating nodes.
- It ensures for consistent ledger global state.
- All or majority or certain number of node must agree.
- Must be fault-tolerant

Consensus Algorithm - PoW

Proof of Work

- Nodes compete against each other to solve a cryptographic puzzle.
- Find a Hash with specific number of zeros prefixed to it.
- Whoever solves it first, gets to add their block to the chain.
- Requires huge processing power.
- Used in public and permissioned block chain.

Consensus Algorithm - PoET

Proof of Elapsed Time

- Developed by Intel Corporation that enables permissioned blockchain networks to determine block winners
- PoET follows a lottery system that spreads the chances of winning equally across network participants
- It generates a random wait time for each node in the blockchain network; each node must go to sleep for that duration.
- The node with the shortest wait time will wake up first and being allowed to commit a new block to the blockchain.

Consensus Algorithm - RAFT

- Leader based consensus
- At a given point of time one node would be a leader and rest are fallowers.
- Leader node is selected based on election among the participating nodes.
- RAFT is CFT but not Byzantine fault tolerant (BFT) complaint
- CFT is crash fault tolerant. Consensus is arrived even during certain number of node failure.
- BFT prevents bad leader node.

Transaction process

- Client submits transaction to blockchain network node with identity details.
- Submitted transaction is distributed to all participating nodes.
- Node verifies the identity of transaction.
- Transactions are wrapped in to Blocks.
- Consensus process selects leader / coordinator node.
- Coordinator ships its blocks to all the node for commit after validation.
- Block added to chain, transaction final state is created or updated.

Components of Blockchain network

- Node
- Peer/Orderer/Validator
- Client, API
- Consensus engine
- Ledger
- Smart contract/Transaction processor/Chain code
- Certifying Authorities

Types of Blockchain network

Public	Consortium	Private
-Permission less - Anybody can participate	-Permissioned - Group of organizations	-Permissioned - Single organization
-PoW Consensus -Slower -Requires huge processing power	-PoET, RAFT, PBFT -Faster -Requires Less processing power	-PoET, RAFT, PBFT -Faster -Requires Less processing power
-Transaction takes more time (10 min or more	-Short 100 X msec	-Short -100 X msec

Database Vs Blockchain

Database

- Centralized
- Only selected group have authoritative control
- Data assets can be changed
- Transactions are hidden from each other
- Faster, suitable for OLTP
- For orgs those who trust each other

Blockchain

- Distributed
- No one has central authority
- modification of asset or record is not possible
- Transaction details are transparent
- Slower, and not for OLTP
- For orgs those who not trust each other

Enterprise Blockchain frameworks

Ethereum

Hyperledger

Corda (r3 consortium)

Multichain

Ripple

Hyperledger

- A project from Linux Foundation supported by Intel, IBM, SAP …

- Blockchain tools and products from Hyperledger are
  - Sawtooth
  - Fabric
  - Indy (Digital Identity management)
  - Grid (supply chain)
  - Cello (Tool for block chain provisioning)
  - Explorer (Dashboard for Fabric)
  - Composer (ui for designing fabric network)

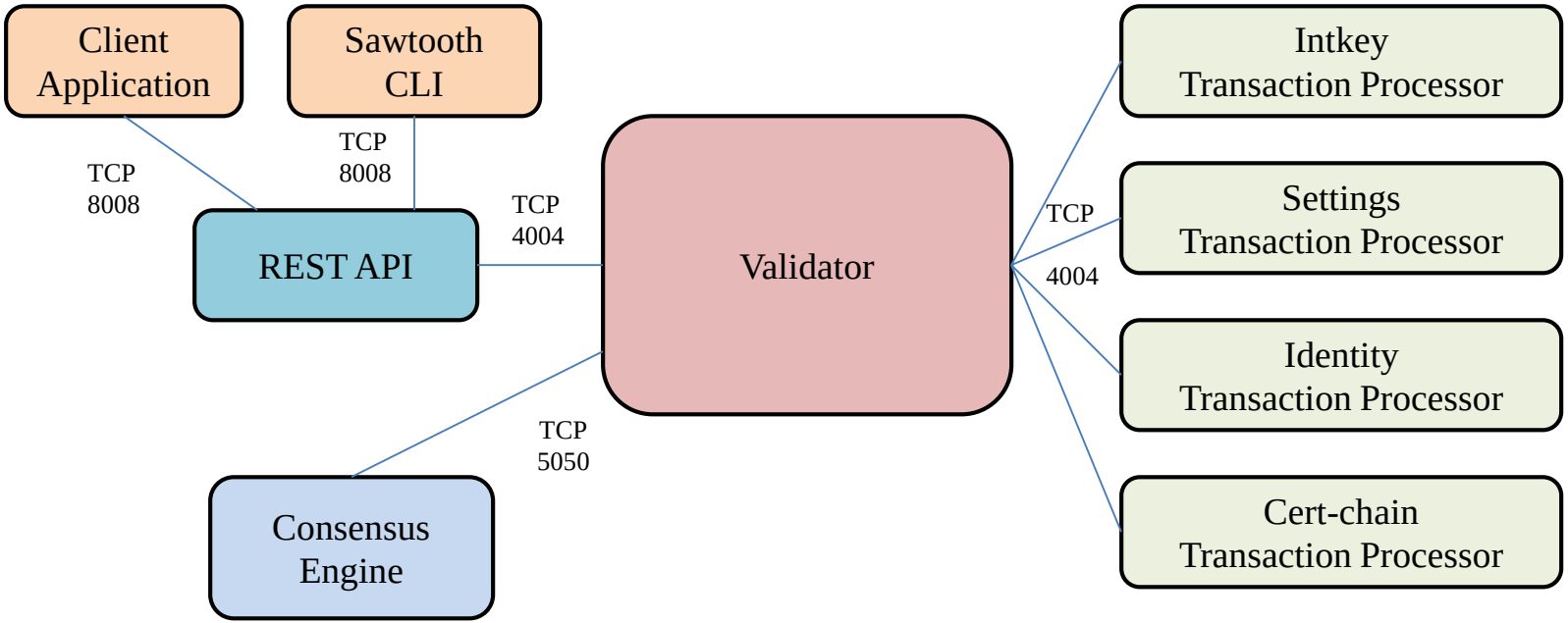
Hyperledger Sawtooth

- An enterprise blockchain framework
- Open source and community-based development
- Supported by Intel

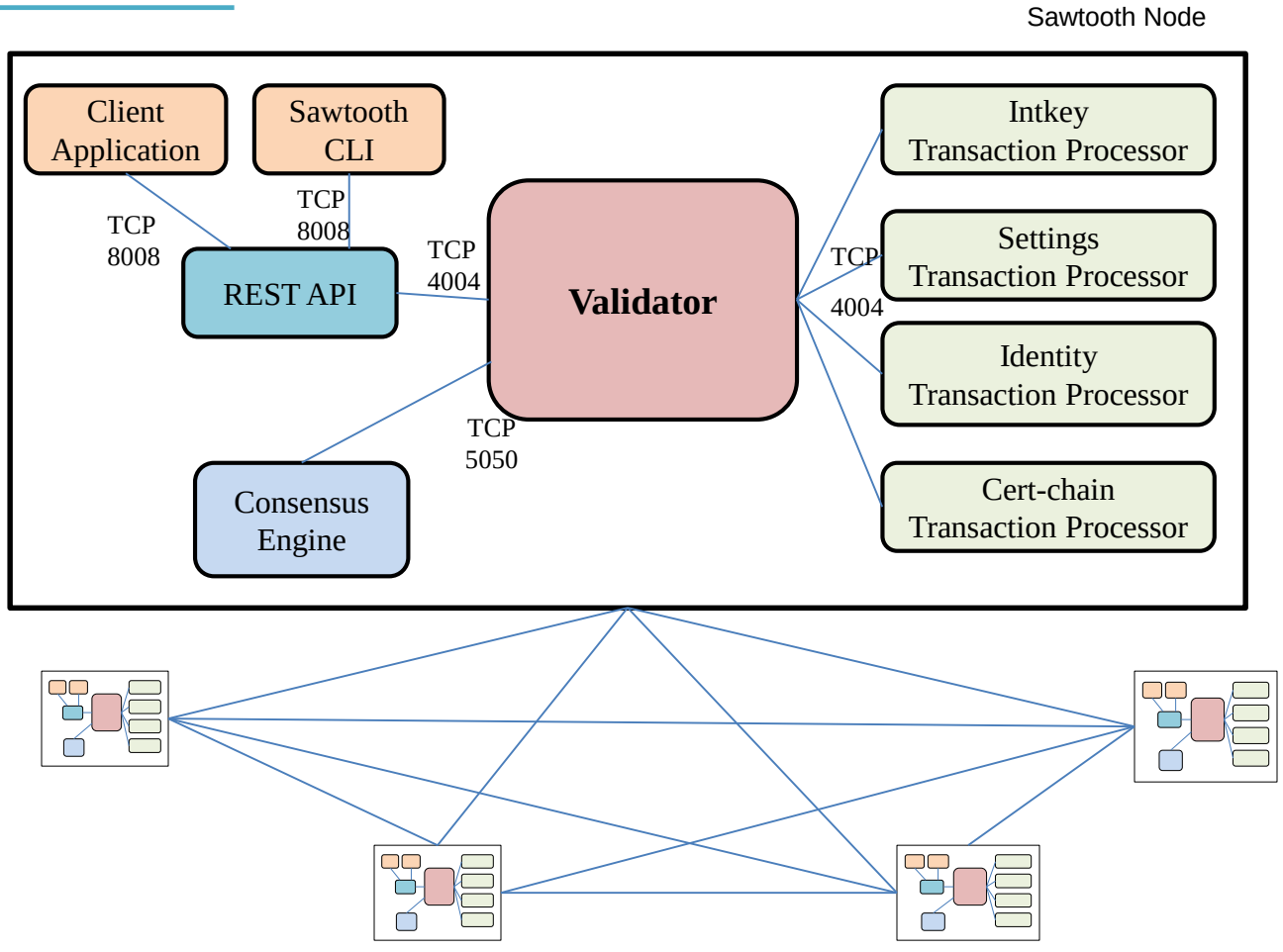
Key features

- Separation in Application Level and the Core System
- Parallel transaction execution
- Event system
- Pluggable consensus algorithms
- Supports multiple programming languages
- Is a generic framework

Sawtooth node



Sawtooth Network



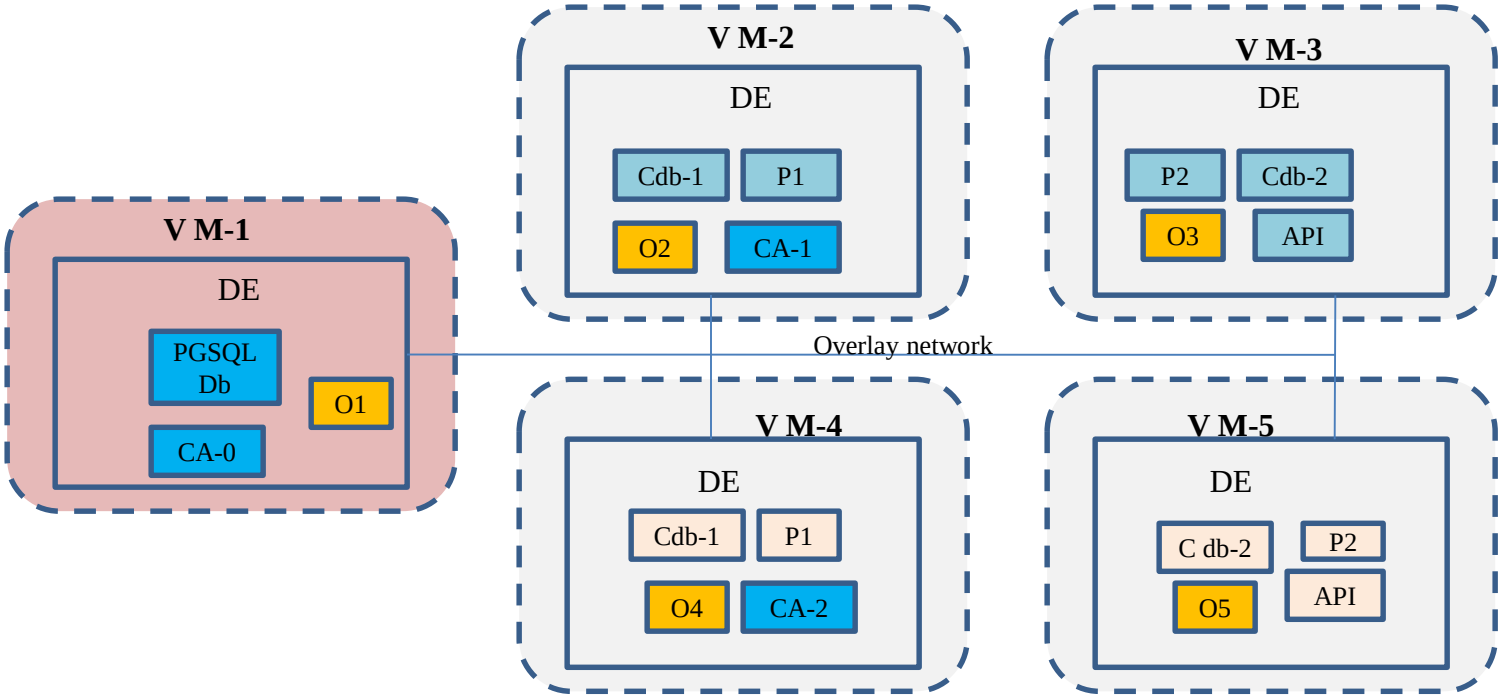
Fabric

- A project under Hyperledger from Linux Foundation
- An **enterprise-grade framework** and accommodates the diversity of enterprise use cases.
- It is a **permissioned blockchain network** where all access to the network is based on digital certificate.
- Simple leader based consensus process is used in this framework.
- It receives contributions from active community and IBM.

Fabric components

- Certifying Authority
- Orderer
- Peer (anchor, endorser, commit)
- Channels
- Ledger database (LevelDb, CouchDb)
- Chain code
- API - Client application
- Fabric SDK (Fabric-network, Fabric-contract, Fabric-ca)

Fabric deployment architecture



Sawtooth Vs Fabric

	Sawtooth	Fabric
Mode of operation	Permissioned and Permissionless	Permissioned
Access restriction	by permissioning Transactor keys, Validator keys and transaction family	by means of MSP and Certifying Authority. Very tight governance framework
Consensus	PoET, pBFT, RAFT	RAFT and KAFKA
Language support	Python,NodeJs Go, JAVA, C++	NodeJs, Go, JAVA
Enterprise ready	Yes	Yes
Ledger	Key value store (lmdb)	Key value store (Level Db and CouchDb
Components	Validator, RestAPI, Consensus Engine, TP and CLI	Orderer, CA, Peers, CouchDb,Chaincode, Consensus and CLI

Ledger database

- Ledger database consists of 3 key value data stores (for chain, transaction receipt and final transaction state)
- **Chain db** stores cryptographically linked blocks
- **Transaction receipt db** is to stores the transaction along with commit status
- **State db** is to store final state of asset after transaction

Deployment

- **As OS service**
  - develop service file
  - one set of node services per VM

- **As Container service**
  - develop container manifest files
  - can co-host more than one set of node services

As Kubernetes pods
- develop pod, service manifest files
- can co-host more than one node services

Requirements for development

- OS: Ubuntu 18.0.4 (LTS)
- Blockchain Platform: Hyperledger,Corda,Multichain
- IDE: VS Code
- Programming Language: Python, NodeJs, Golang, Java, C++
- Off chain storage: Postgres/MinIO/IPFS
- Docker engine, Docker swarm, Kubernetes

Use Cases

Verification, Traceability

Certificate Chain (SSLC/PUC, CBSE)

Supply Chain

Drug Logistics

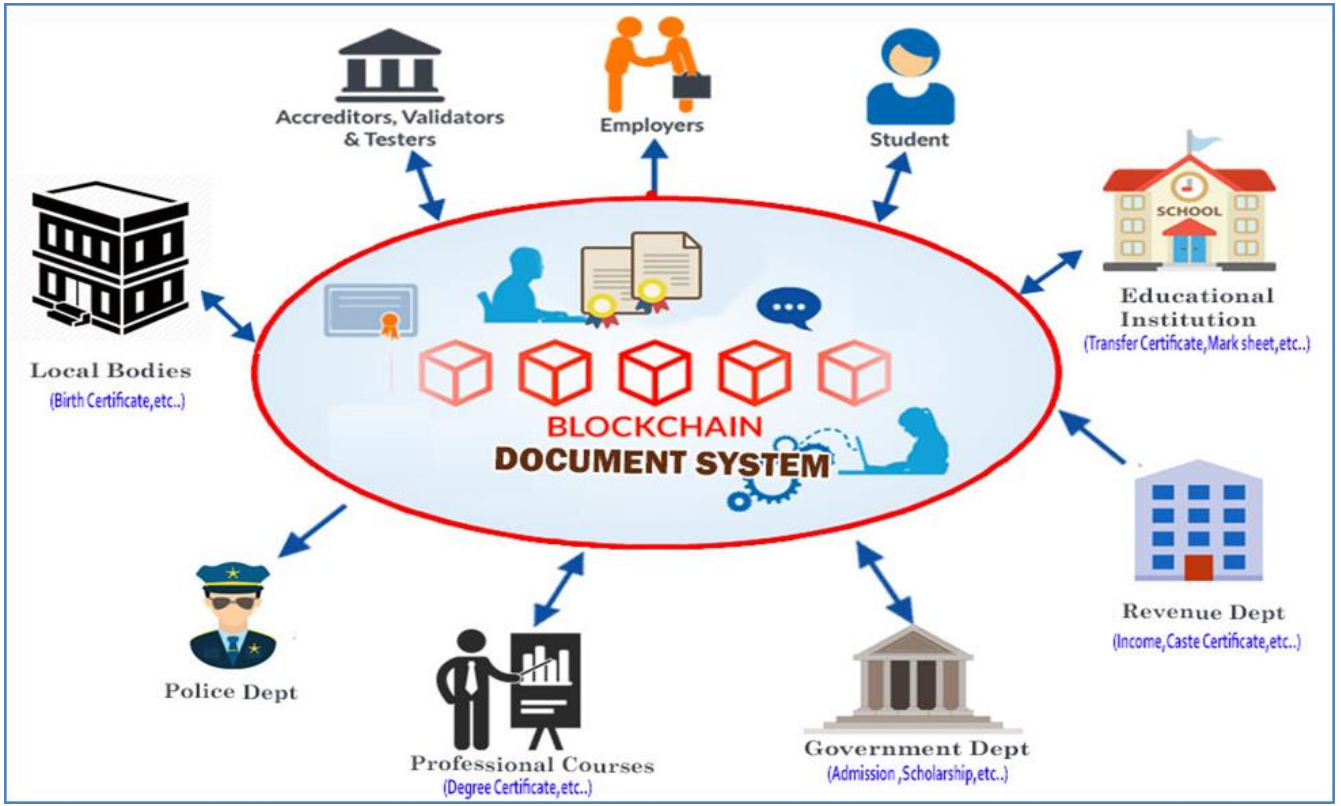
Blood Bank supply chain

e-Abgari

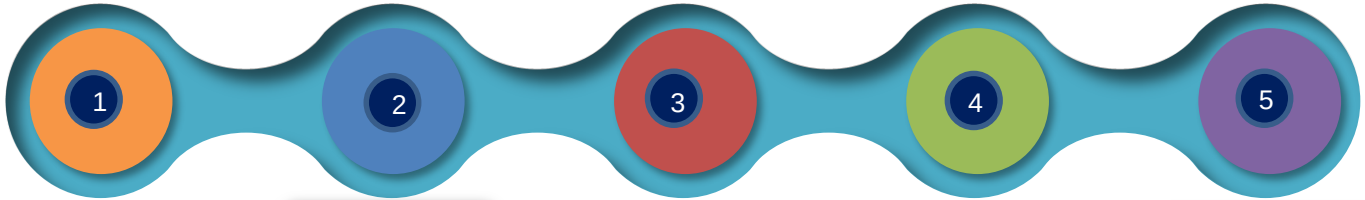
Sectors : Finance, Health, Agriculture

…

Certificate Chain



Drug Logistics



Procurement

- NOA Number
- PO Number
- Supplier
- Drug Name
- PO Date
- Rate
- Warehouses
- Quantity

Warehouse Inward

- PO Number
- Supplier
- Drug Name
- Warehouse
- Receipt Date
- Invoice No
- Invoice Date
- Rate
- Batch No.
- Mfg. Date
- Exp. Date
- Batch Qty

Quality Check

- Drug Name
- Batch No
- Warehouse
- Qty Lifted
- QC Code
- Test Result

Warehouse Outward

- Institute Indent #
- Warehouse
- Institute
- Batch No
- Mfg Date
- Exp Date
- Qty
- Supplier
- Rate
- Drug
- Outward No
- Outward Date.

Hosp Inward

- Inward No
- Inward Date
- WH Outward No
- Warehouse
- Indent No
- Drug
- Batch No
- Mfg Date
- Exp Date
- Qty

Drug Logistics

End-to-end traceability of health products
streamlined visibility of movement of drugs or medicines in the supply chain to all Stake holders
The improved traceability facilitates the optimization of flows of goods and an efficient stock management system.

Reduced losses related to counterfeiting
It would become possible to examine vulnerable points in the supply chain and reduce the chances of frauds and the costs associated with it.

Transparency to enhance accountability
The receiving and shipping of health products throughout the supply chain can be traced.
Results in greater accountability of logistics

Drug Logistics

Efficient recall management
Identification of exact locations of medicines is possible. The recalls can be made quickly enabling increased safety to patient's health.

Governance to surveillance
Facilitates the governance model to move from regulation to surveillance

Non repudiation
Unauthorized individuals cannot carry out transactions in the drug supply chain ecosystem without a valid private key.