Models of Blockchain Network

Models of Blockchain Network

- Two models of Blockchain network – Permission-less (an open environment) and Permissioned (a close environment)

Similarities

- Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions.

- Both maintain the replicas in sync through a protocol referred to as consensus.

- Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious

Distinction

- The distinction between two models of blockchain is related to
  - who is allowed to participate in the network,
  - execute the *consensus* protocol and
  - maintain the shared ledger.

The Permission-less Model

- Works in an open environment and over a large network of participants
  - Any one can participate / join the network

- To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work (incentivizing mechanism) to ensure all are in sync.

The Permission-less Model

- The users do not need to know the identity of the peers, and hence the users do not need to reveal their identity to others

- Good for financial applications like banking using cryptocurrency

Privacy and Security

- The system is tamper-proof – it is "**extremely hard**" to make a change in the blockchain
  - Tampering the system becomes harder as the chain grows

- Example for permission-less network : Bitcoin

Cryptocurrency Applications using Blockchain

- Bitcoin
- Litecoin
- Bytecoin
- Peercoin
- Emercoin
- Ripple (XRP)
- Waves
- Omni (MSC)
- Gridcoin (GRC)

The Permissioned (Private) Model – Blockchain 2.0

- Blockchain can be applied just beyond cryptocurrency
- The underlying notions of consensus, security and distributed replicated ledgers can be applied to even closed or permissioned network settings
- Most **enterprise use cases** only involve a few ten to a few hundred known participants

Blockchain 2.0

- A decentralized platform - can be utilized to avoid intermediates (the middleman)

- **Smart Contracts:** An automated computerized protocol used for digitally facilitating, verifying or enforcing the negotiation or performance of a legal contract by avoiding intermediates and directly validating the contract over a decentralized platform - faster, cheaper and more secure

Permissioned Model

- A blockchain architecture where users are **authenticated apriory**
- Users know each other
- But, users may **not trust each other** – Security and Consensus are still required
- Run blockchain among **known and identified participants**

Permissioned Blockchain Applications

- Asset Movements and Tracking
  - Financial marketplace
  - Supplychain

Permissioned Blockchain Applications

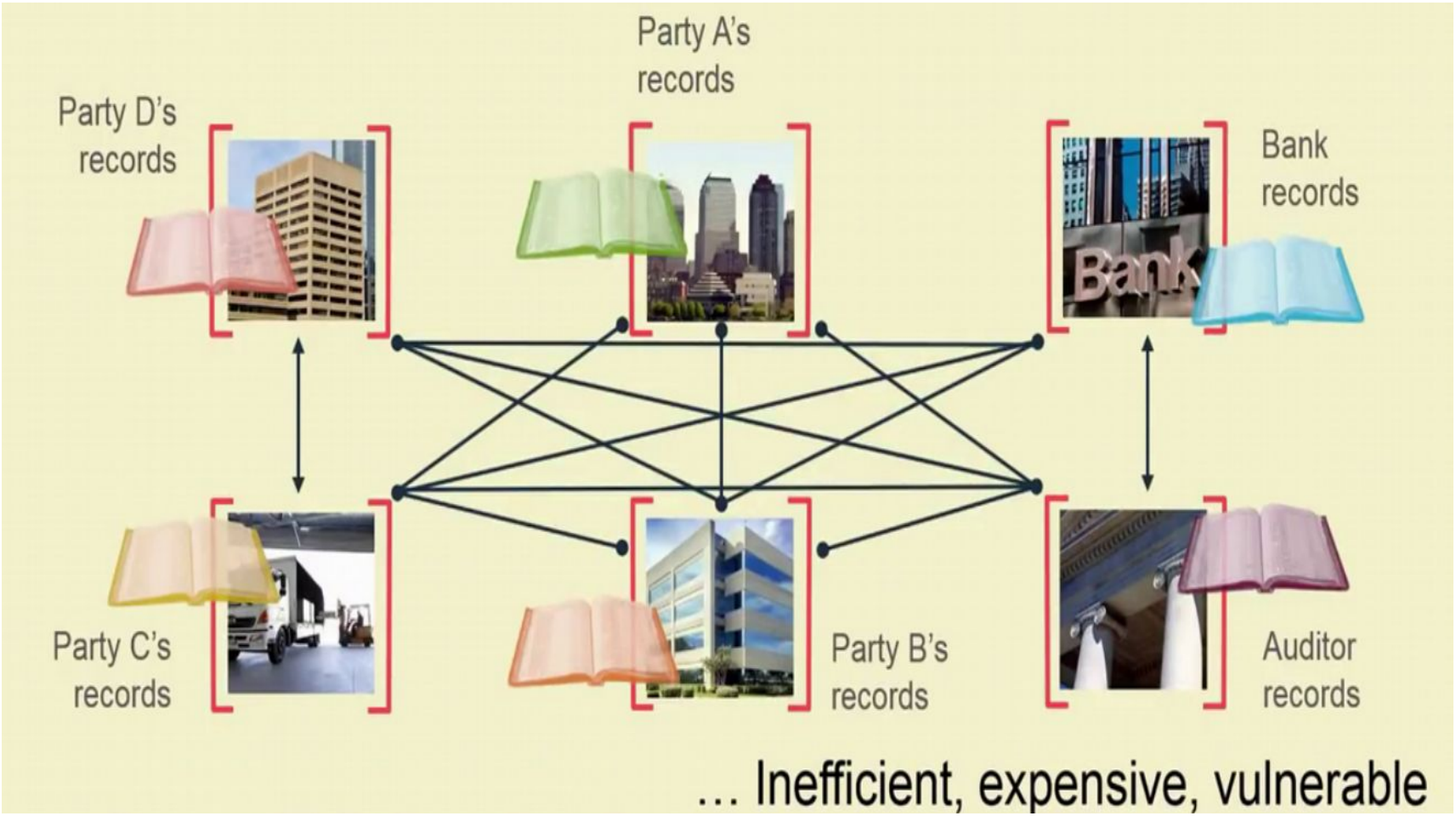
- Provenance tracking – tracking the origin and movement of high-value items across a supply chain, such as luxury goods, pharmaceuticals, cosmetics and electronics.
  - When the high-value item is created, a corresponding digital token is issued by a trusted entity, which acts to authenticate its point of origin
  - Every time the physical item changes hands, the digital token is moved in parallel-? The real-world chain of custody is precisely mirrored by a chain of transactions on the blockchain
  - The token is acting as a virtual “certficate of authenticity”, which is far harder to steal or forge than a piece of paper.

Use Cases

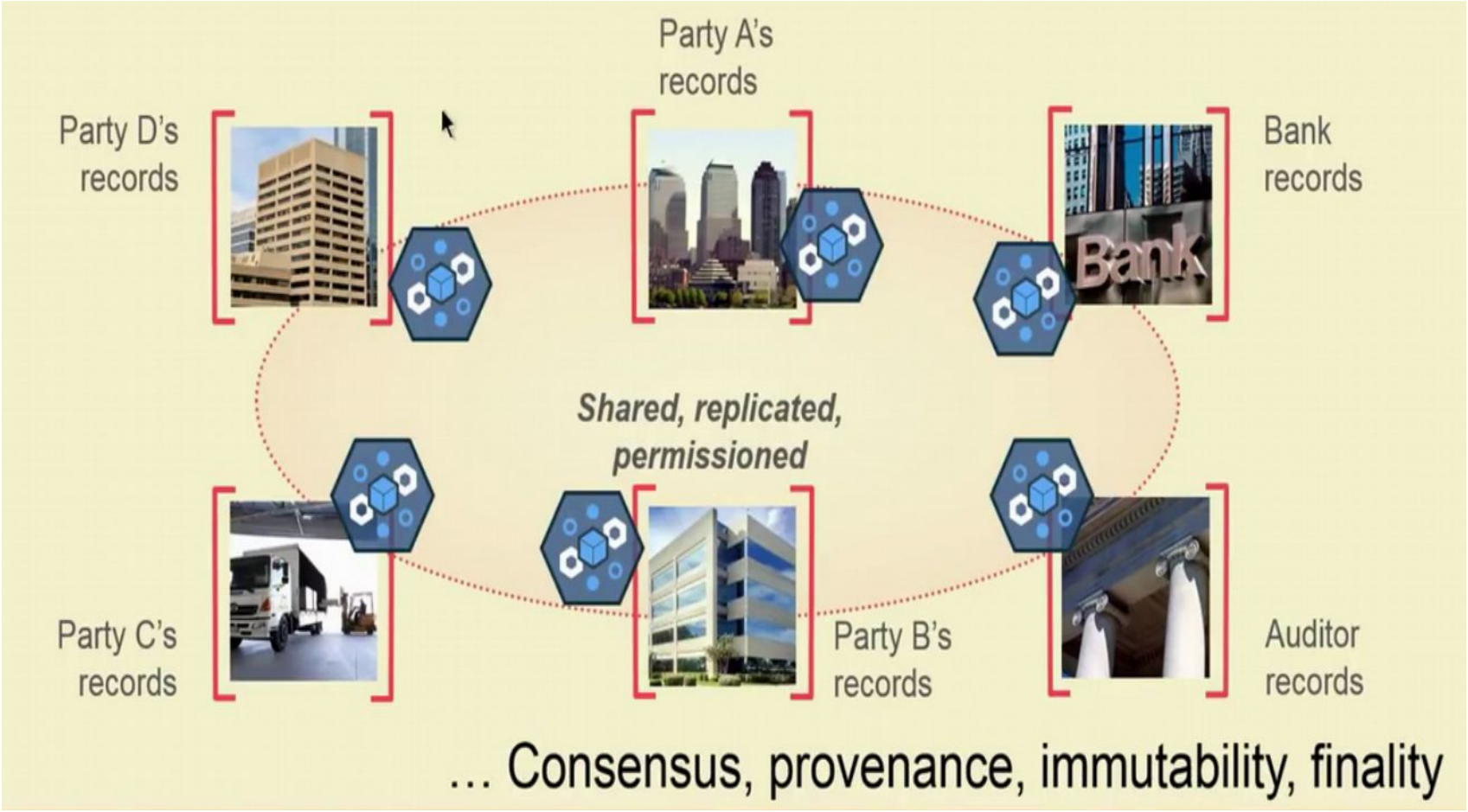
- Particularly interesting for business applications – execute contracts among a closed set of participants

- Example: Supply chain, payments, custody, credit swaps, commodities, micro lending, escrow, charity, music publishing Provenance tracking of assets and much more

Difficult to Track Asset Transfers in a Business Network



Solution – Shared, Replicated and Permissioned Ledger



Hyperledger Fabric

- A Permissioned blockchain framework that provides an enterprise-grade foundation for transactional applications
- A shared ledger that supports smart contracts – ensures security and integrity of recorded transactions
- Unlike Bitcoin and Ethereum, Hyperledger Fabric supports privacy and confidential transactions

Permission-less vs Permissioned Blockchains

	Permission-less	Permissioned
Access	Open read/write access to database	Permissioned read/write access to database
Scale	Scale to a large number of nodes, but not in transaction throughput	Scale in terms of transaction throughput, but not to a large number of nodes
Consensus	Proof of work/ proof of stake	Closed membership consensus algorithms
Identity	Anonymous/pseudonymous	Identities of nodes are known, but transaction identities can be private/anonymous/pseudonymous
Asset	Native assets	Any asset/data/state

References

- NPTEL Course Material
- https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

futureskills prime
A MeitY - NASSCOM Digital Skilling Initiative

प्रगत संगणन विकास केंद्र
सी डैक CDAC
॥ ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

cdacchain@cdac.in

THANK YOU