Business Application – Acquisition, Development & Implementation

(Chapter - 5 : DISSA Course) - **Blockchain**

Arijit Chakraborty

July 18 , 2021

BC= architecture

- *Blockchain* = shared, immutable ledger that facilitates process of recording transactions & tracking assets in a business network.
- A*sset* = tangible (car, cash, land) or intangible (IPR, patents, copyrights, branding)
- BC network can track orders, payments, accounts, production.
- Members share single view = users see all details of a transaction end-to-end,
- **Features**

✓ *Decentralized , autonomy*

✓ *Immutability, security*

✓ *Hash-Identifier*

✓ *Distributed Ledger Technology (DLT)*

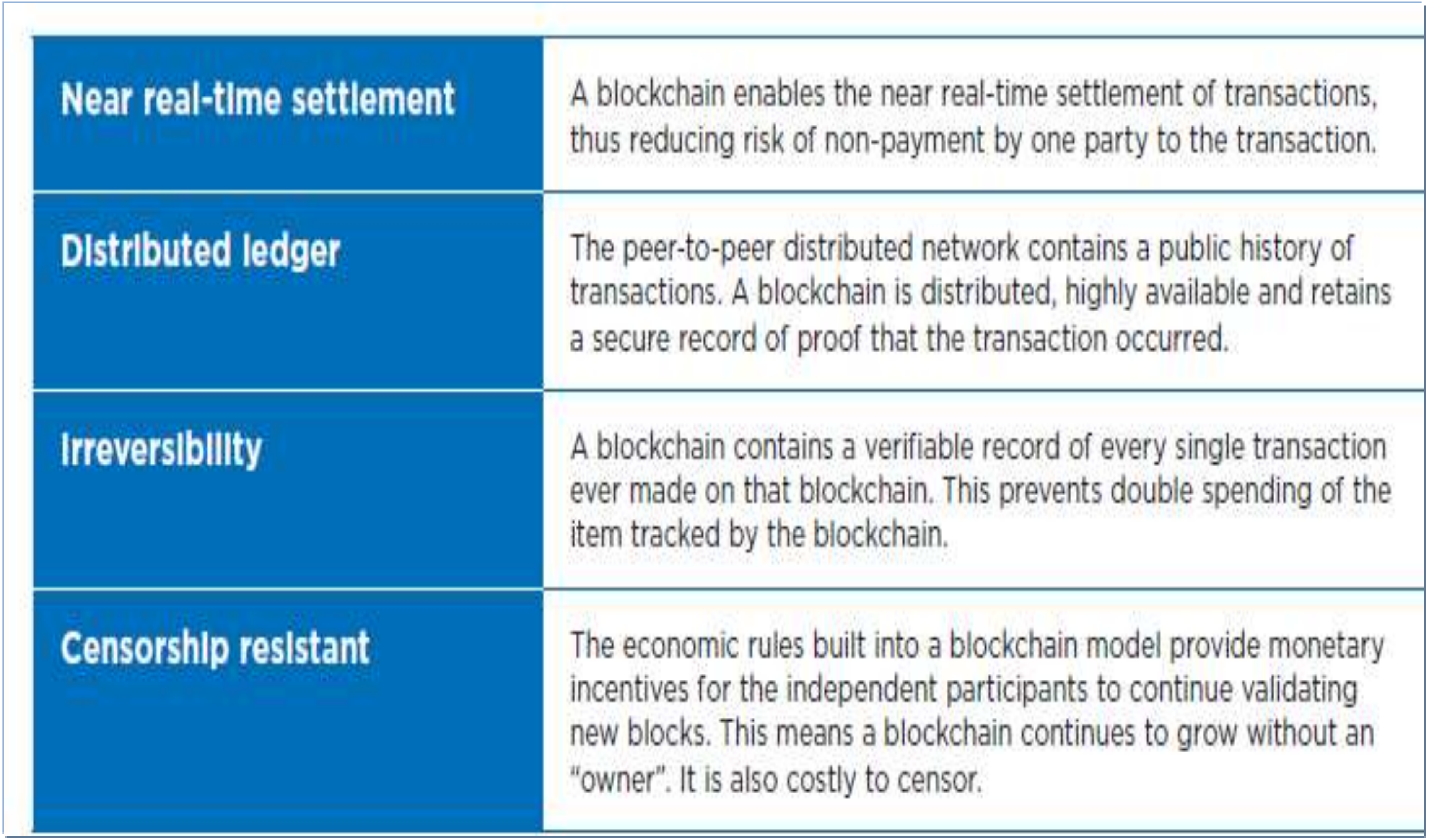
✓ **Consensus algorithm**

- No one node or server is responsible for approving transactions, leading to genuinely distributed transaction processing
- Each entry is validated & recorded on all ledgers across network
- **Blocks in a chain = pages in a book:**
- **A book = chain of pages.**

Blockchain

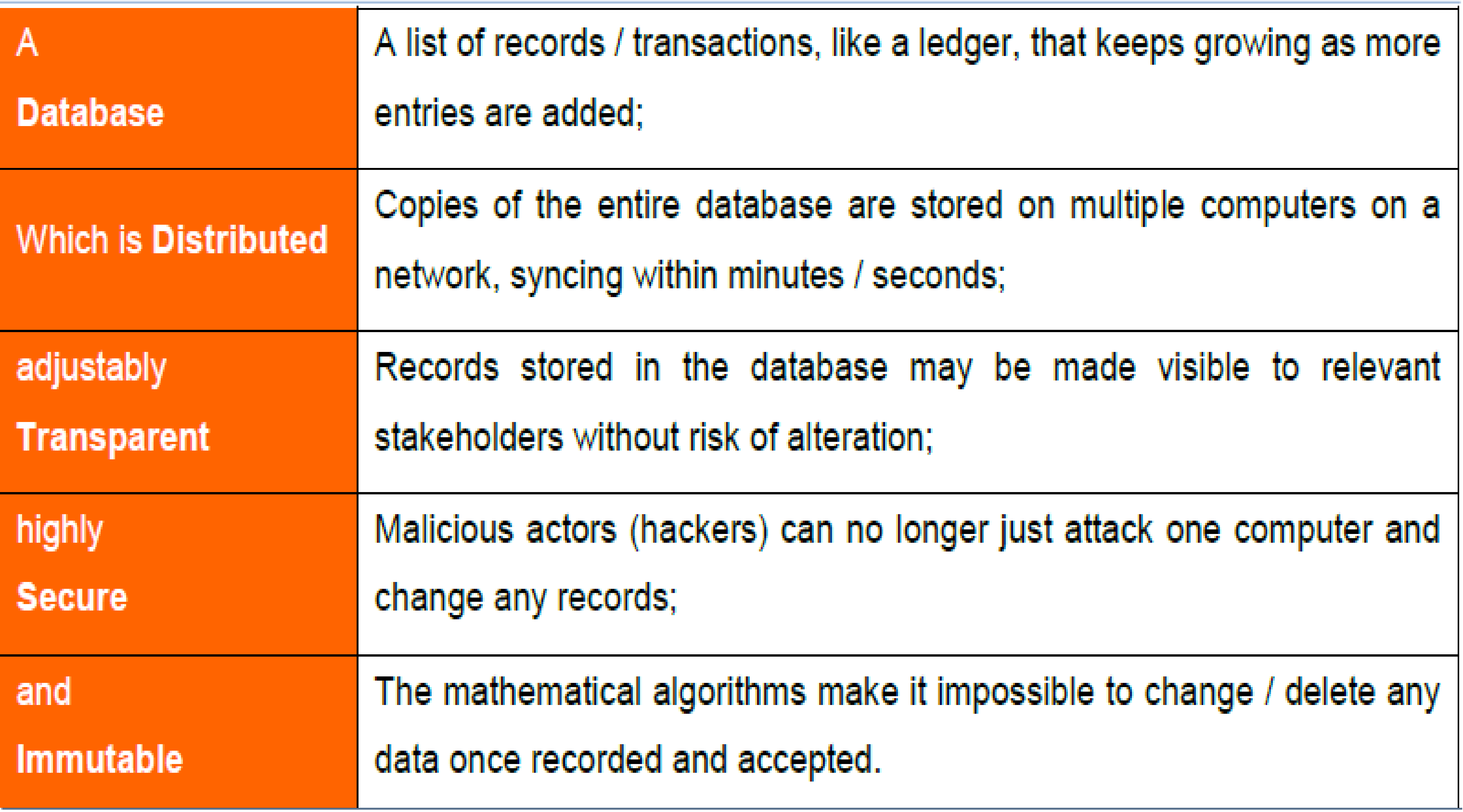
- Distributed database/ ledger = maintains continuously growing list of data records (public & private) put together in encrypted blocks.
- Transactions & details *(date, place, amount, anonymized participants & their encrypted signatures)* recorded & verified through **consensus algorithms**

Features



Near real-time settlement	A blockchain enables the near real-time settlement of transactions, thus reducing risk of non-payment by one party to the transaction.
Distributed ledger	The peer-to-peer distributed network contains a public history of transactions. A blockchain is distributed, highly available and retains a secure record of proof that the transaction occurred.
Irreversibility	A blockchain contains a verifiable record of every single transaction ever made on that blockchain. This prevents double spending of the item tracked by the blockchain.
Censorship resistant	The economic rules built into a blockchain model provide monetary incentives for the independent participants to continue validating new blocks. This means a blockchain continues to grow without an "owner". It is also costly to censor.

Essence of BC= New ”Trust System”



A **Database**	A list of records / transactions, like a ledger, that keeps growing as more entries are added;
Which is **Distributed**	Copies of the entire database are stored on multiple computers on a network, syncing within minutes / seconds;
adjustably **Transparent**	Records stored in the database may be made visible to relevant stakeholders without risk of alteration;
highly **Secure**	Malicious actors (hackers) can no longer just attack one computer and change any records;
and **Immutable**	The mathematical algorithms make it impossible to change / delete any data once recorded and accepted.

BC Operation

- BC store data in blocks -then chained together using cryptography.
- **Each block contains** = cryptographic hash of previous block, timestamp & transaction data. As new data comes in - entered into fresh block.
- Hash = mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length.
- Timestamp proves = transaction data existed when block was published
- *Person A transferred Rs 2500 to Person B (timestamp t=1)*
- *Person B transferred property LAND_XYZ to Person C (timestamp t=2)*
- *ABC Ltd transferred domain XYZ.com to DF Ltd (timestamp t=3)*
- BC= resistant to modification of data .
- Once recorded, data in any block cannot be altered retroactively without altering all subsequent blocks.
- **Bitcoin** = BC used in decentralized way = no single person or group has control— all users collectively retain control.
- Decentralized blockchains = immutable, data entered is irreversible.
- Bitcoin= transactions permanently recorded & viewable to anyone.
- **Nonce** = combination of 2 words, “n” means number & “once” means one time-arbitrary number that can be used just once in a cryptographic communication.

Technology overview - Example = Google Doc.

Google doc shared with group of people -- doc is distributed instead of copied

Creates decentralized distribution chain = gives everyone access to doc at same time.

No one is locked out awaiting changes from another party, modifications to doc being recorded real-time, making changes completely transparent.

BC = 2 important concepts: **blocks, nodes**

Blocks

Every chain consists of multiple blocks & each block has 3 basic elements:

1. The **data** in the block : 32-bit whole number called **nonce.** It is randomly generated when block is created, which then generates **block header hash.**

Hash = 256-bit number wedded to nonce. Starts with multiple zeroes (i.e., extremely small).

When first block of a chain icreated, a nonce generates the cryptographic hash.

Data in block considered signed & forever tied to the nonce and hash unless it is mined.

Mathematical functions that convert data of indeterminate length to ‘fingerprint’ of fixed length.

2. Nodes

Decentralised = No one computer or organization can own the chain.

Distributed ledger via nodes connected to the chain.

Nodes :any kind of electronic device = maintains copies of BC & keeps network functioning.

Blockchain mining = used to secure & verify & authenticate transactions

Blocks secured by **Blockchain miners** & connected to each other forming a chain.

Mining = adding new transactions to BC by solving algorithmic problems with computing resources.

"Blockchain" technology

- Each completed transaction encrypted,
- Involved participants identified by string of characters
- After certain time, transaction becomes part of block.
- **Block =** group of transactions linked to previous block,
- It is distributed to all parties associated with this network.
- User (a "**node**") has file of transactions in computer (a **"ledger"**).
- 2 accountants (**"miners"**) have **same file** on theirs (**"distributed"**).
- As user transacts, his computer sends e-mail to each accountant to inform them.
- Each accountant checks.
- The first to check & validate hits “REPLY ALL”, attaching their logic for verifying the transaction (**"proof of work"**).
- If other accountant agrees, everyone updates their file
- Provides reliable audit trail = authenticity & validity of transactions can be verified
- **Companies incorporated BC** = *Walmart, Pfizer, AIG, Siemens, Unilever, Tata Steel, ICICI Bank etc*

BC = storage of data

- Usually contains financial transactions;
- Is replicated across several systems in almost real-time;
- Usually exists over a peer-to-peer network;
- Uses cryptography & digital signatures to prove identity, authenticity & enforce read/write access rights;
- Can be **written b**y certain participants;
- Can be **read by** certain participants, or a wider audience;
- Have mechanisms to make it hard to change historical records,
- Make it easy to detect when someone is trying to do so.
- BC technology = backbone of cryptocurrency network Bitcoin
- **Consensus Algorithm= Mechanism**
- When 1 participant wants to send value to other, all other nodes in network communicate with each other using pre-determined mechanism to check that new transaction is valid.
- Blocks in chain validated by nodes to maintain single version of truth
- Computer algorithms = define modality of how BC based system defines what is the correct updated state of database. = simple majority amongst nodes.

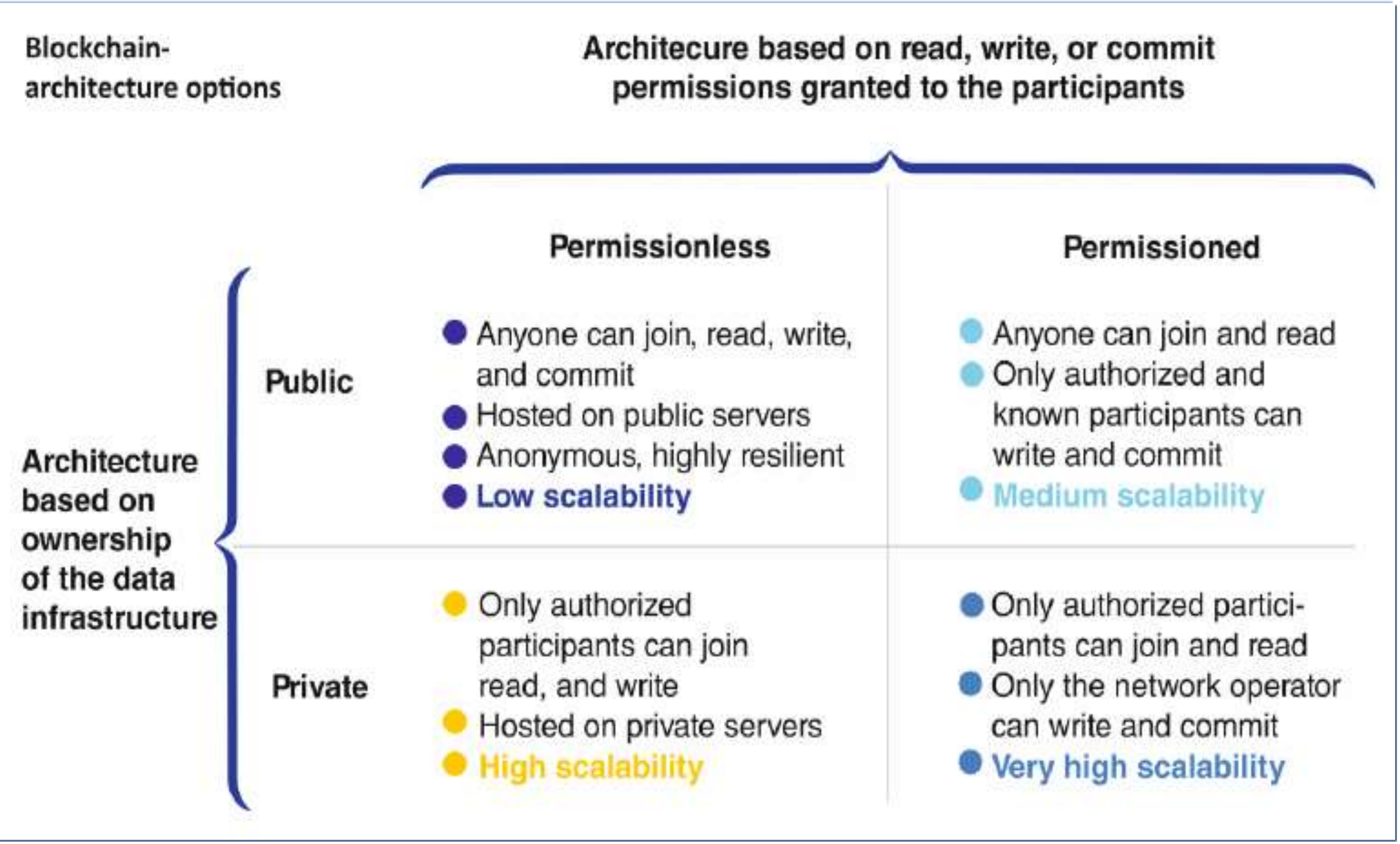
Smart Contracts

- Smarts contracts = automated contracts = embedded in block chain
- self-executing contracts with terms of agreement between buyer & seller directly written into lines of code.
- Code & agreements exist across distributed, decentralized BC network.
- Code controls the execution, transactions are trackable & irreversible.
- Help exchange money, property, shares, Avoids a middle man
- Transactions can be sent with rules attached
- **Benefits**
- Immutable
- Distributed ledger
- Efficient & Reliable
- Lacks single point of failure
- **Consensus Algorithm levels**

Participants & their roles

- ! **Blockchain user:** Participant (business user) with permissions to join Blockchain network, conducts transactions with other network participants.
- ! **Regulator:** Blockchain user with special permissions to oversee transactions happening in network. Regulators may be prohibited from conducting transactions.
- ! **Blockchain developer:** Programmers who create applications & smart contracts -enable BC users to conduct transactions on BC network.
- ! **Blockchain network operator:** Individuals - special permissions & authority to define, create, manage, monitor BC network.
- ! **Certificate authority:** Individual who issues & manages different types of certificates required to run a permissioned BC

BC Types



Blockchain-architecture options

Architecure based on read, write, or commit permissions granted to the participants

		Permissionless	Permissioned
Architecture based on ownership of the data infrastructure	Public	● Anyone can join, read, write, and commit ● Hosted on public servers ● Anonymous, highly resilient ● **Low scalability**	● Anyone can join and read ● Only authorized and known participants can write and commit ● **Medium scalability**
	Private	● Only authorized participants can join read, and write ● Hosted on private servers ● **High scalability**	● Only authorized participants can join and read ● Only the network operator can write and commit ● **Very high scalability**

BC - types

- **Permissionless Blockchain**
- open to any potential user. Ex- Bitcoin blockchain - public or permissionless blockchain; anyone can participate as a node in the chain by agreeing to relay & validate transactions on network thereby offering their computer processor as a node.
- **Joining blockchain** = downloading software & bitcoin ledger from Internet.
- Blockchain maintains list of every transaction performed, reflects full transaction history & account balances of all parties
- **Permissioned Blockchain**
- Participation in BC network to participants who have already been given permission by agreed-upon administrators.
- Example - supply chain network may use blockchain to track movement of goods.

BC – Implementation cases

- **Adopting trade finance solution to facilitate paperless trade & transparency**
- BC digitises & automates paperwork filings for import & export of goods by enabling end users to securely submit, stamp & approve documents across national & organisational boundaries.
- Supply chain visibility = all parties involved i.e. *network - shippers, freight forwarders, ocean carriers, ports & customs authorities in a global shipping transaction*
- View real time= status of customs documents or view bills of lading.
- **Telecommunication**
- streamline internal operations of telecom industry -billing, roaming, network function, digital asset transactions, mobile money
- **Healthcare**
- to improve electronic medical records, & facilitating new drug development , medical innovation

- **Banking**
- used for derivative trading to connect potential buyers & sellers on decentralised network to update information on continuous basis.
- Crypto assets - just one type of digital asset exchanged on BC
- **Media**
- maintaining database of digital rights to avoid copyright issues, use smart contracts for payment of media owners
- **Retail**
- Food safety – BC = allow consumers to track origin of food items & enforce transparency in food supply chain from farm origination details to storage of food in retail stores.
- **Automotive**
- product life cycle management = tracking full history of vehicle from pre-production to sale.

BC – Major Risks

- Misconfigured access permissions, consensus & proof of stake mechanisms leading to transaction trust issues
- Lack of governance mechanisms leading to non compliance of transactions & regulatory penalties
- Concerns = unencrypted personal & confidential information contained in global transactions leading to regulatory concerns
- Challenges in interconnecting different blockchain protocols & data formats creating solution implementation roadblocks
- Challenges in securely maintaining cryptographic keys or weak encryption leading to permanent loss of whole data

IS Audit aspects

- Transaction recorded in a blockchain may still be:
- • unauthorized, fraudulent or illegal
- • executed between related parties
- • linked to a side agreement that is “off-chain”
- **IS auditor will :**
- need to extract data from BC & consider whether it is reliable.
- Review ITGC related to blockchain environment.
- IS auditor to understand & assess reliability of consensus protocol
- Review protocol could be manipulated
- **Role as Advisors**
- Providing advise on weighing costs & advantages of new system, etc.
- **Audit of Smart Contacts**
- **Service Auditor of Consortium Blockchain**
- **Central Access Granting Administrator**
- **Arbitration Function**

Blockchain , internal audit & IS Audit

- IA = Consider change in the way that information is accessed in new formats. (BC Technology)
- BC adoption requires framework to identify risk of exposure associated with transactions
- **ISACA-AICPA & CIMA Joint Blockchain Working Group**
- *Mission* : to identify & document risk with private blockchains
- **IIA Guidelines** = New methods to develop audit plans - identify BC threats & risks.
- **US AICPA** = outlined new roles for auditors - BC ecosystem
- **CIMA**
- **ISACA** = Blockchain Technology Audit Preparation Program
- **ISACA =** Cloud Access Security Broker (CASB) Audit Program.
- **Key Risks to be identified by IA Function**
- **1. Governance/design risk:** Lack of protocols for unconfirmed transactions can allow processing of fraudulent transactions that were previously rejected= network threat
- **2. Infrastructure/protocol management risk:** Conditional instructions in protocol or smart contract code can allow infinite loops putting ongoing operation & integrity of network at risk.
- **3. Key management:** Keys for storing & transacting in crypto assets at risk. Keys can be brute forced or guessed= loss of assets.