Blockchain Technology

@iLabAfrica – Strathmore University

What is Blockchain?

Blockchain vs Bitcoin???

Discussion…

- Bitcoin – A digital currency invented (2009) with the intention of simplifying digital transactions by eliminating "middle men"
  - Middle men → Regulators control
  - How? By storing and transacting the currency over a built in network (a blockchain), rather than going through central monetary repository (intermediaries)
  - Bitcoin – NOT SYNONYMOUS TO blockchain. It is transacted over an open, public, anonymous blockchain network.

- Blockchain has taken a life of its own, permeating a broad range of applications and industries e.g. Finance (supply chain), government, health care, identity management, manufacturing and distribution.

Blockchain is like The operating system

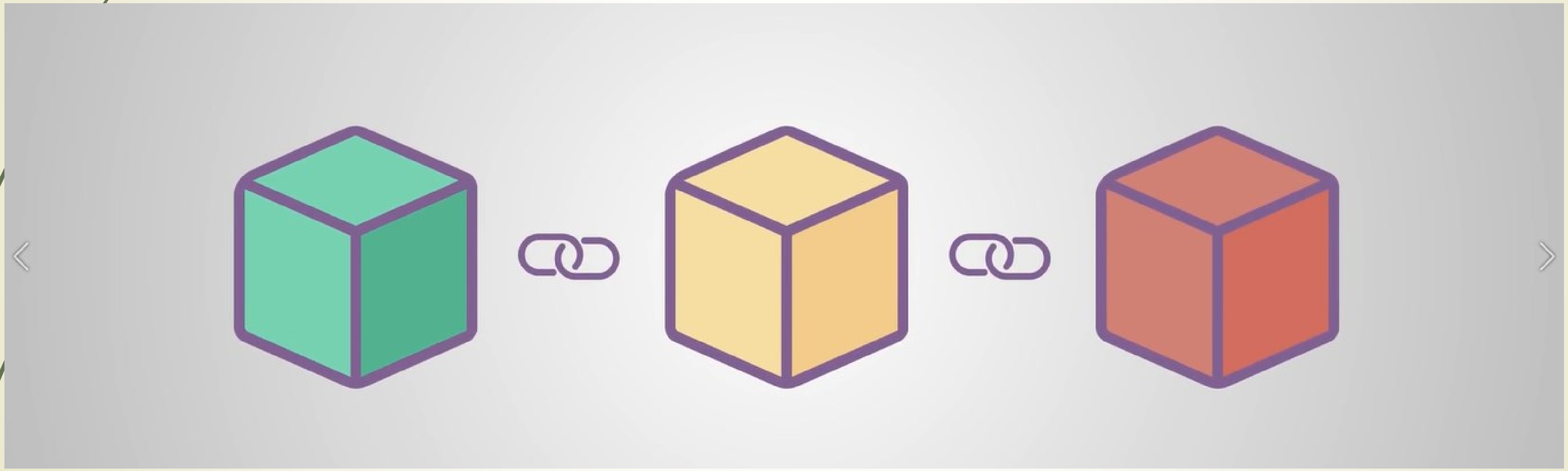
Bitcoin is like one more program running on the operating system

Course objectives

- Characteristics that define blockchain
- Important features of the Hyperledger blockchain platform
- Algorithms and techniques that enable a blockchain platform
- Method for realizing trust in a blockchain platform

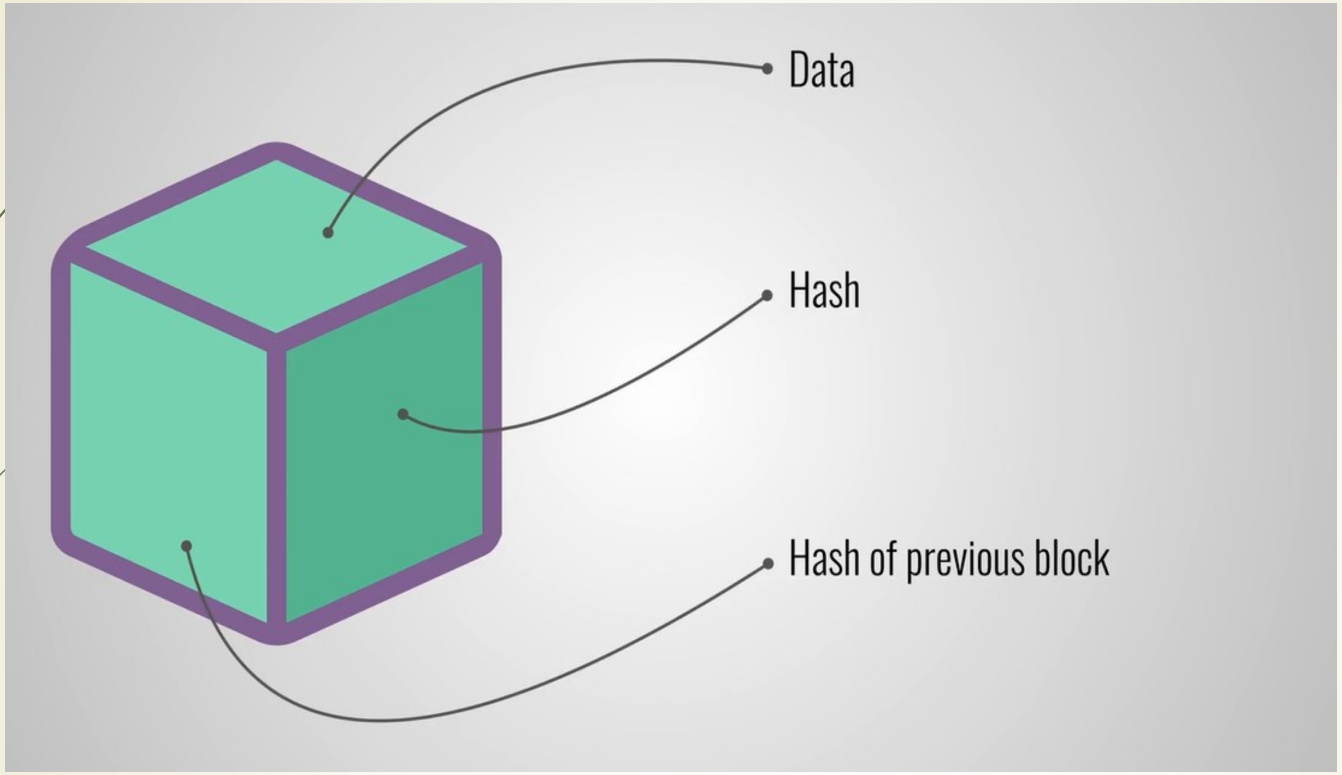
What is Blockchain?

- A chain of blocks that contains information



- A trusted distributed ledger with shared business processes.

The structure of A block



- Each block contains:
  - Data
  - The block’s hash and
  - The previous block’s hash

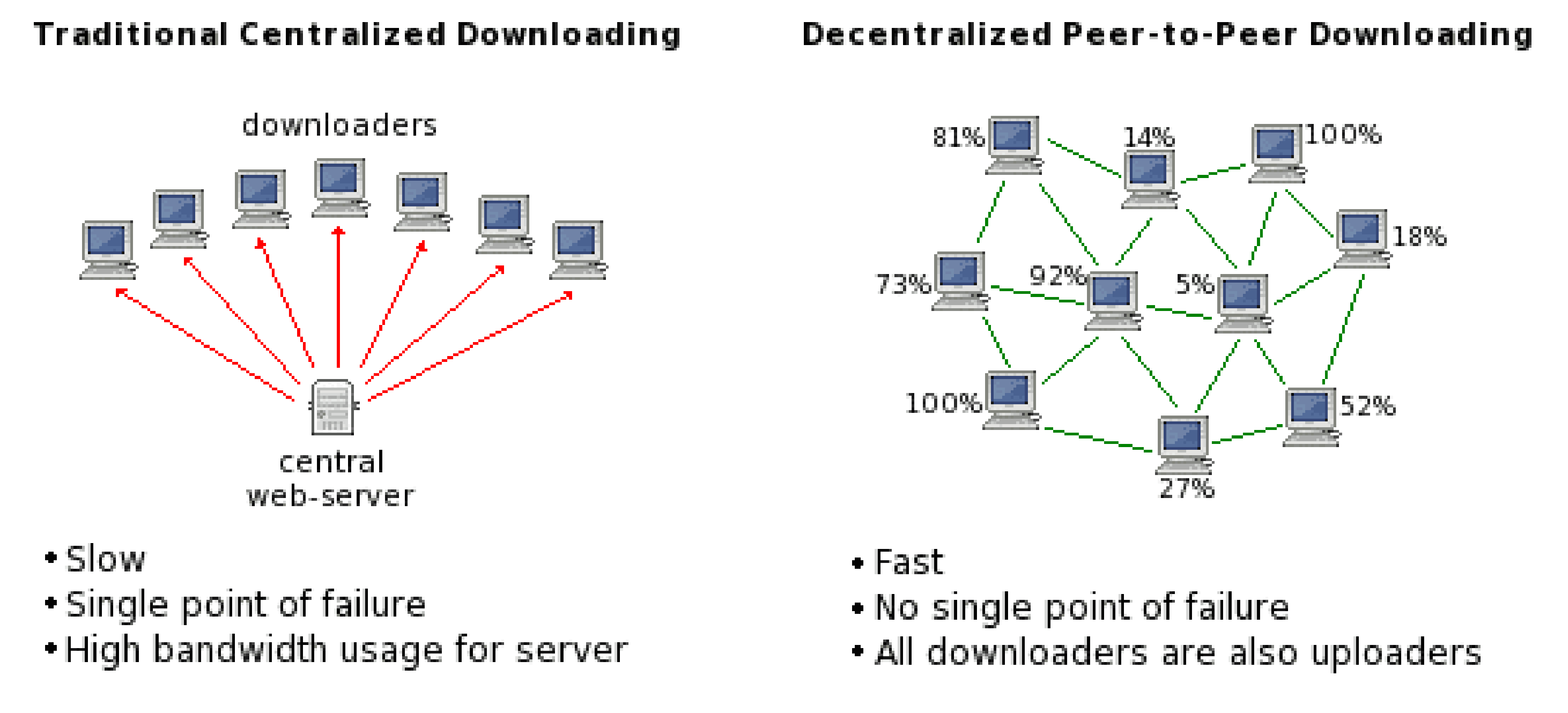
What is Blockchain?

- It enables peer to peer interaction (transfer of digital assets) in a decentralized network, (without need for any intermediaries).
- Establishing trust among unknown peers
- Recording the transaction in an immutable distributed ledger

Centralized vs. decentralized

- A purchase using a credit card
  - Credit card agency – visa, master card etc.
  - Customer bank
  - Credit card’s bank
  - Exchange
  - Merchants bank
  - Merchant
- *Compare this with a scenario where peers can transact with each other irrespective of location.*

Centralized vs. decentralized


Traditional Centralized Downloading
downloaders
central web-server
Decentralized Peer-to-Peer Downloading
81%
14%
100%
18%
73%
92%
5%
100%
52%
27%

Traditional Centralized Downloading

- Slow
- Single point of failure
- High bandwidth usage for server

Decentralized Peer-to-Peer Downloading

- Fast
- No single point of failure
- All downloaders are also uploaders

- *Compare this with a scenario where peers can transact with each other irrespective of location.*

Trust among unknown parties?

- How do we ensure this? By having processes in place to
  - Validate
  - Verify and
  - Confirm transactions
- *Functions of the intermediaries are shifted to the peripheries i.e. to the peers in the network*
  - Transaction is recorded in a distributed ledger
  - Create a tamperproof (immutable) chain of blocks
  - Consensus protocol (agreement on the block to be added to the chain)

Applications of Blockchain

- Goods transfer e.g. supply chain
- Digital media transfer e.g. sale of art
- Remote services delivery e.g. travel and tourism
- Distributed intelligence e.g. education credentials
- Distributed resources e.g. power generation and distribution
- Crowd funding e.g. start-up-fund raising
- Crowd operation e.g. electronic voting
- Identity management e.g. one ID for all ones life's functions
- Government public records and open governing

Blockchains can be:

- Permissioned
  - Best for the business scenario
- Permissionless
  - Like the bitcoin blockchain

Blockchain for business

The Bitcoin blockchain

- It is an example of an un-permissioned, public ledger
    - Public – anyone can join (permission-less)
    - Anonymity –Transactions not tied to user identity
- Due to the nature and requirements of businesses, their Blockchains need to be
    - Permissioned
    - Private
    - And they prioritize:
        - Identity over anonymity
        - Assets over cryptocurrency
        - Selective endorsement

Bitcoin mining

- Why must mining happen?
  1. It is the process by which verification of transactions between users is done so that they can be added into the blockchain (public ledger)
     - To ensure no double spending – digital assets can easily be duplicated
       - Use of public key encryption to ensure one owns the coins they are transacting
       - Any value transferred must be able to be traced from a previous source
     - No central authority – verification is delegated to peers in the network
     - The pool of miners must not all be there for verification to happen
  2. It is also a process by which new coins are introduced into the network

Mining…

- What exactly is mining?
  - Collection of transactions and organizing them into blocks
    - Miner nodes receive and verify transaction whenever they are made, add them into a memory pool & assemble them into a block
  - Miner adds the coinbase transaction
    - New coins are made
  - Hash each transaction
  - A merkle tree of the hashes (up to the root hash)
  - Root hash+ previous block's hash + nonce hashed: **Block hash**
  - Hash difficulty: Compare hash to the target value
  - Repeat this with random nonce until the valid hash is obtained
  - Broadcast the valid hash
  - All other nodes check if hash is valid & add it to the blockchain

Mining...

- If 2 valid hashes are broadcasted?
  - Orphaned/ stale block
- Mining pools
  - Combining forces then the reward is shared
- Watch binance video: https://www.youtube.com/watch?v=2VtH-XAOjXw

Examples of crypto-currencies

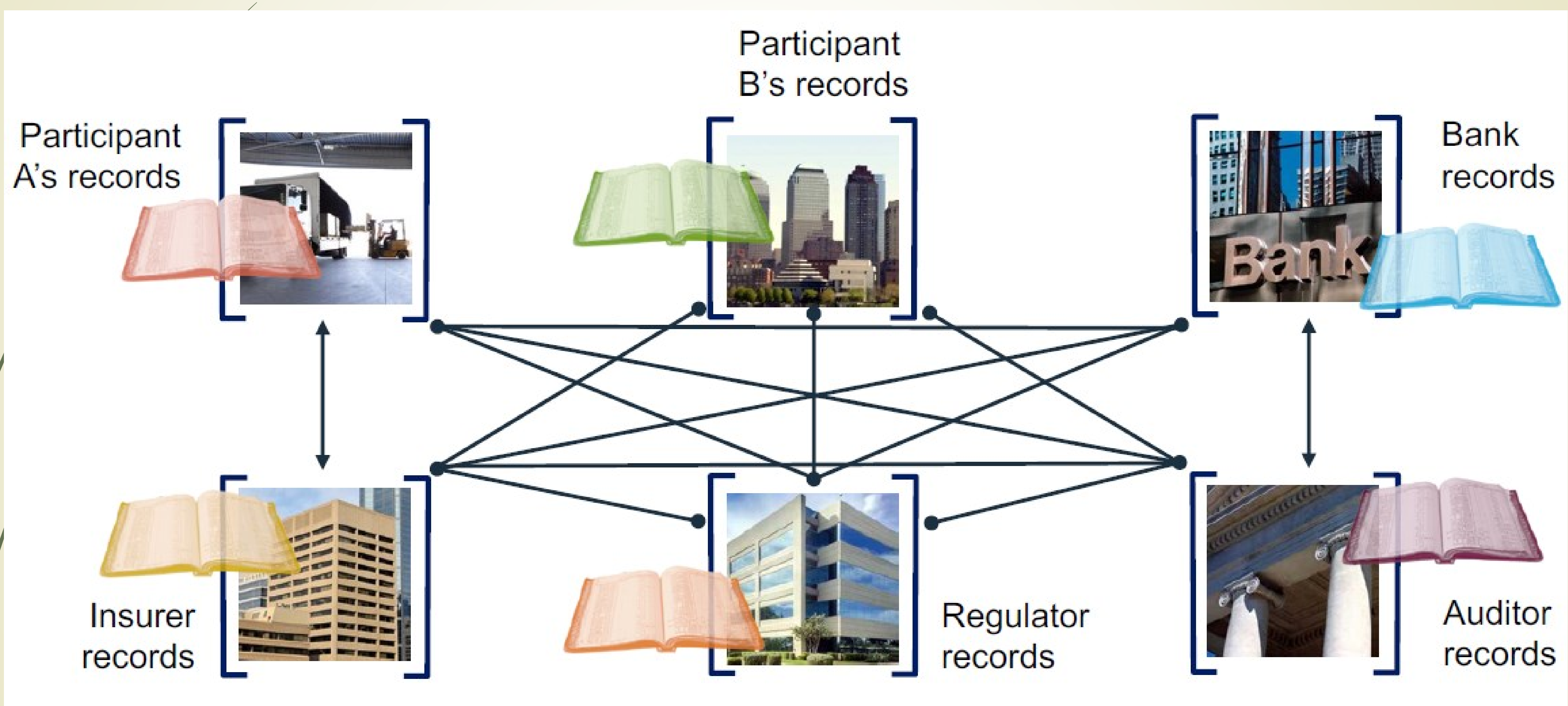
ethereum
Bitcoin
Ethereum
Litecoin
Dogecoin
Monero
Zcash

Current status

Multiple ledgers for multiple business networks

- Ineffective
- Expensive
- Vulnerable

Problem

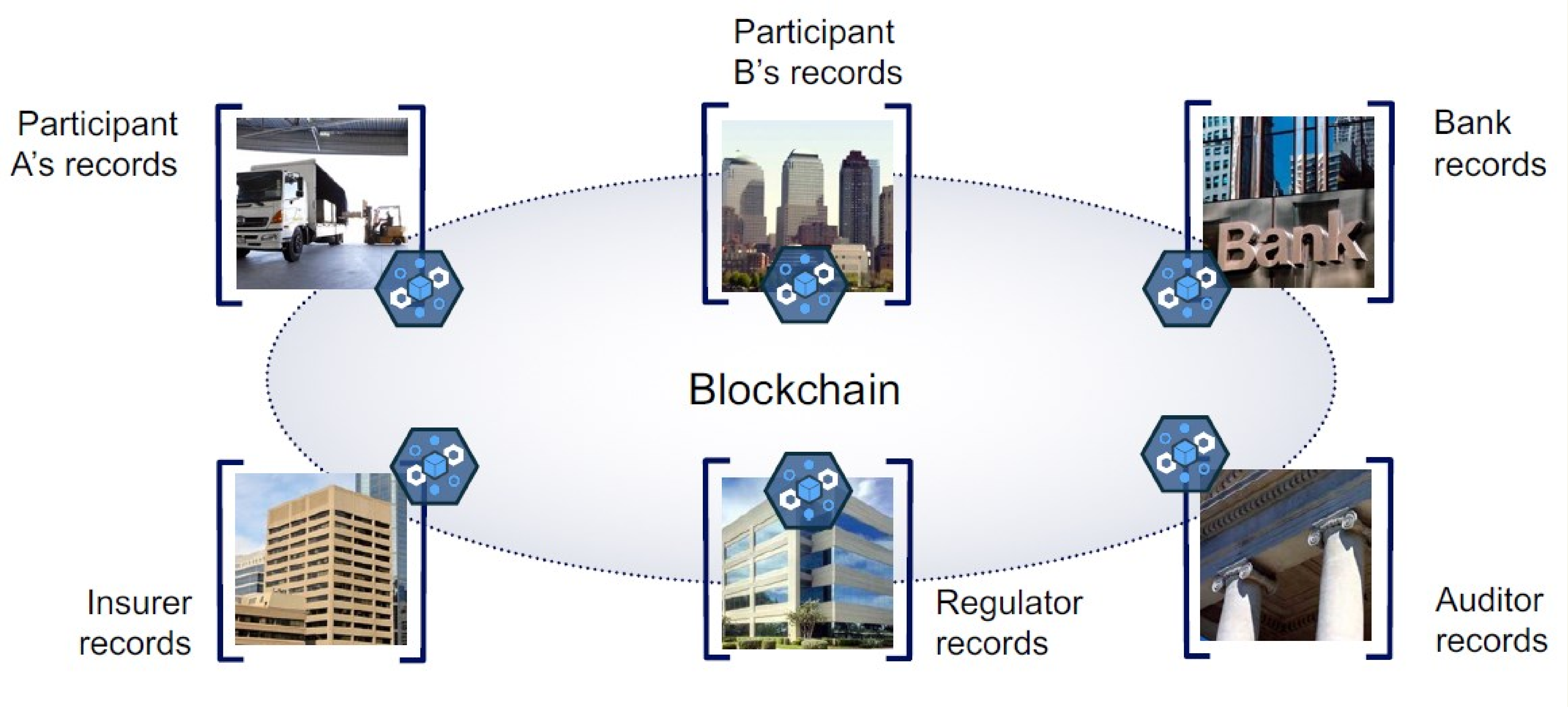

Participant B's records
Participant A's records
Bank records
Insurer records
Regulator records
Auditor records
Bank

Blockchain features

- **Distributed (shared)**
- Permissioned (for permissioned Blockchains)
- Provenance
- Immutability

Blockchain brings..

Shared, Permissioned, Replicated ledger



Blockchain for business

- Businesses manage the maintenance and exchange of Assets (tangible and intangible).
  - Tangible e.g. A house
  - Intangible
    - Financial e.g. A mortgage
    - Intellectual e.g. patents
    - Digital e.g. music
- Ledgers – the system of record for businesses.

Blockchain for business

- What does a business need?
  - Trust – not just anyone is on the network & can see everything
  - Privacy - not everyone sees everything – information is shared on a need to know basis
  - Proof/ evidence

Blockchain for business

- Due to the nature and requirements of businesses, their Blockchains need to be
  - Permissioned
  - Private
  - And they prioritize:
    - Identity over anonymity
    - Assets over cryptocurrency
    - Selective endorsement

Blockchain for business

- To ensure trust, we have:
  - Shared ledger
    - Distributed system of records shared across business networks (append–only)
    - Permissioned- users see only what they need to
  - Smart contracts
    - Verifiable and signed contractual conditions
    - Business terms executed with transactions
    - Encoded in programing language

- Privacy
  - Appropriate confidentiality between subsets of participants
  - Identity not linked to a transaction (shared ledger but users need confidentiality)
  - Cryptography is employed in ensuring privacy and also in transaction authentication
- Proof
  - Provable endorsement by relevant trusted participants
  - Endorsed transactions are added to the ledger
  - Verifiable audit trail – transactions can't be modified, inserted or deleted

Features of blockchain

- Consensus
- Provenance
- Immutability/ Finality

Consensus

- The process of keeping ledger transactions synchronized across the network (agreement on what is posted).
- Ensures that ledgers are only updated when transactions are approved by the appropriate participants and that ledgers update with the same transaction in the same order.
- There are varied algorithms that are used to achieve consensus on different blockchain platforms.

Consensus

- Proof of work (PoW): PoW was the first consensus algorithm to be created. It is employed by Bitcoin and many other crypto currencies.
- It involves numerous hashing attempts, so more computational power means more trials per second. Therefore, miners with a high hash rate have better chances to find a valid solution for the next block (aka. block hash).
- PoW consensus algorithm makes sure that miners are only able to validate a new block of transactions and add it to the blockchain if the distributed nodes of the network reach consensus and agree that the block hash provided by the miner is a valid proof of work.
- Proof of work is useful on a public blockchain, such as the one used for Bitcoin where participants are anonymous. Commitment here is expensive.

Consensus

- Proof of stake: Proof of Stake consensus algorithm replaces the PoW mining with a mechanism where blocks are validated according to the stake of the participants. The validator of each block (also called forger or minter) is determined by an investment of the cryptocurrency itself and not by the amount of computational power allocated. Each PoS system may implement the algorithm in different ways, but in general, the blockchain is secured by a pseudo-random election process that considers the node's wealth and the coins age (how long the coins are being locked or staked) - along with a randomization factor.
- The Ethereum blockchain is currently based on a PoW algorithm, but the Casper protocol will eventually be released to switch the network from PoW to PoS in an attempt to increase the network's scalability.

Consensus

- Multi-signature: A majority of validators (for example, three out of five) must agree that a transaction is valid.
- Practical Byzantine Fault Tolerance (PBFT): PBFT is an algorithm designed to settle disputes among computing nodes (network participants) when one node in a set of nodes generates different output from the others in the set.

Smart contract

A smart contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as part of a transaction

Other Consensus protocols

- Delegated proof of stake
- Proof of stake (Casper)- Ethereum
- Proof of importance
- Proof of Burn
- Proof of Authority
- Proof of Elapsed Time
- Proof of Capacity

Immutability/ Finality

Blockchain research: @iLabAfrica

- Assistance on blockchain research projects
- Working with the team on the projects that they have
  - Academic certificate digitization
  - Mining Crypto using solar energy
  - Road safety – traffic offense monitoring system

Evaluation

- Online test – Discuss the dates to share it
  - Smiley coin – Motivating learners by rewarding them using crypto
- Digital badge on DNA

IBM and Blockchain

- DNA
  - Earn digital badges
    https://developer.ibm.com/africa