DAYANANDA SAGAR COLLEGE OF ENGINEERING

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

DSCE

DEPARTMENT OF INFORMATION SCIENCE

BLOCKCHAIN
(19IS7DEBLC)

Faculty in charge:

Bindu Bhargavi S M
Asst. Professor, Dept. of ISE, DSCE

Module 1

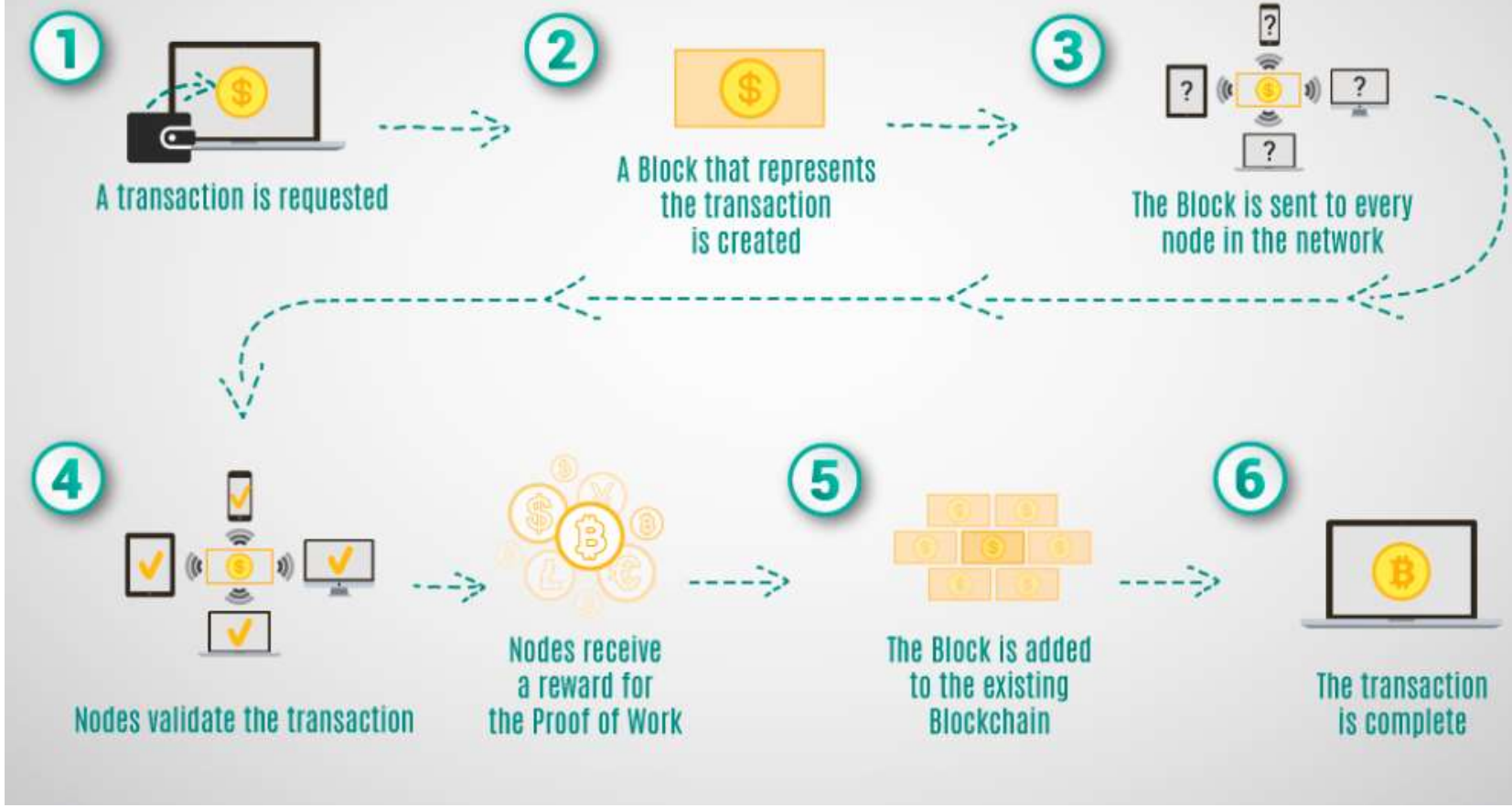
- **Blockchain (BC) 101:** Introduction, Distributed Systems, History of BC and Bitcoin – Electronic cash, BlockChain, Generic Elements of BC, Benefits and limitations of BC, Tiers and Features of BC, Types of BC
- **Decentralization:** Decentralization using BC, Methods of decentralization, Routes to decentralization, BC and ecosystem decentralization, Smart Contracts, Decentralized Organizations, Platforms for decentralization

Introduction

- Blockchain is a technology which permits transactions to be gathered into blocks and recorded, cryptographically chains the blocks in chronological order and allows the resulting ledger to be accessed by different servers.
- Application areas of blockchain are: Supply chain, government, energy, food, retail, healthcare, insurance, education sector, travel and hospitality
- Blockchain offers new tools for authentication and authorization in the digital world

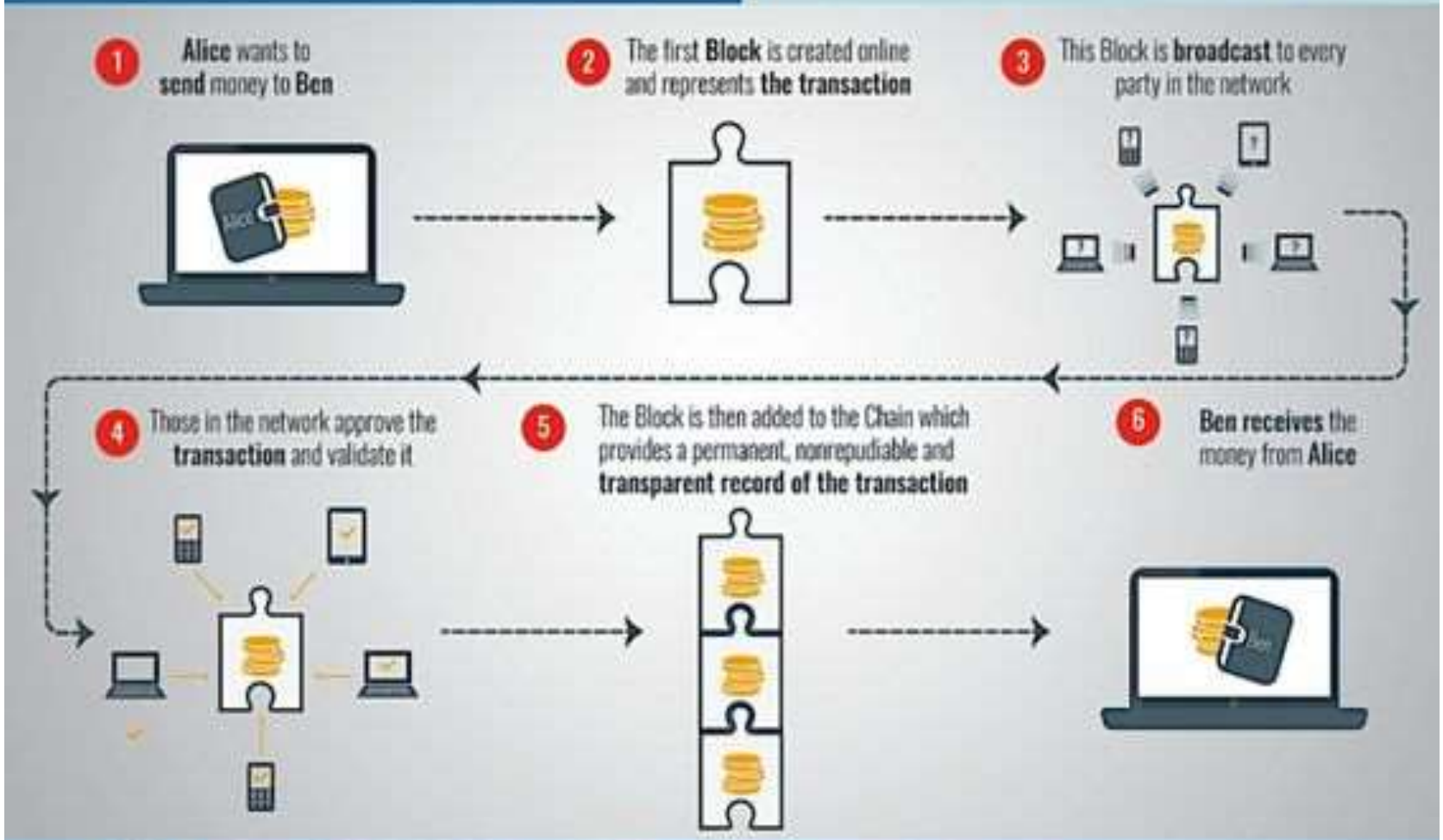

BLOCKCHAIN
NETWORK
VERIFIED
ICO
ADDRESS
WALLET
CRYPTOCURRENCY
TRUST
MINING
TRANSACTION
%
SMART CONTRACTS

HOW BLOCKCHAIN WORKS



HOW BLOCKCHAIN WORKS

"A Blockchain is a cloud based database shared by every participant in a given system, in the case of this exemplar, its a currency trade. The Blockchain contains the complete transaction of the cryptocurrency or other record keeping in other applications. Think of it as a cloud based peer to peer ledger."



Notes: Transactions are not valid until added to the Chain
Tampering is immediately evident

The Blockchain is regarded as safe as everyone in the network has a copy
The Source of any discrepancies are usually evident immediately

@PDForrest

Blockchain in Supply Chain

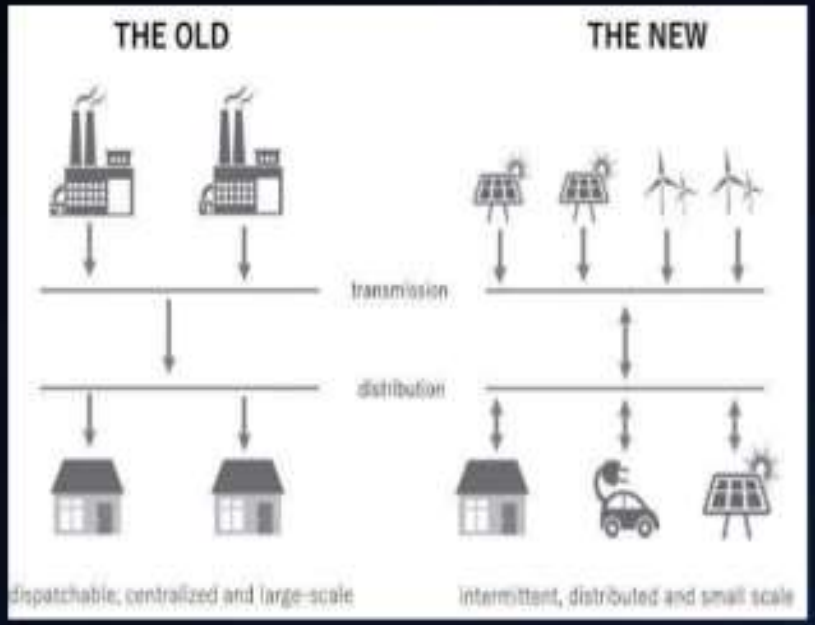
By utilizing a distributed ledger, companies within a supply chain gain transparency into shipment tracking, deliveries, and progress among other suppliers where no inherent trust exists.

Blockchain in Government

Blockchain offers promise as a technology to store personal identity information, criminal backgrounds, and "e-citizenship," authorized by biometrics.

Blockchain in Energy

Decentralized energy transfer and distribution are possible via micro-transactions of data sent to blockchain, validated, and re-dispersed to the grid while securing payment to the submitter.



Blockchain in Food

Using blockchain to store food supply chain data offers enhanced traceability of product origin, batching, processing, expiration, storage temperatures, and shipping.

Blockchain in Retail

Secure P2P marketplaces can track P2P retail transactions, with product information, shipment, and bills of lading input on the blockchain, and paying via Bitcoin.

Blockchain in Insurance

Assets

Business

When autonomous vehicles and other smart devices communicate status updates with insurance providers via the blockchain, premium costs decrease as the need for auditing and authenticating data vanishes.

Blockchain in Travel & Hospitality

Passengers store their authenticated "single travel ID" on the blockchain for use in lieu of travel documents, identification cards, loyalty program IDs, and payment data.

Blockchain in Education

Educational institutions could utilize the blockchain to store credentialing data around assessments, degrees, and transcripts eliminating chance of lost of results slips.

Applications

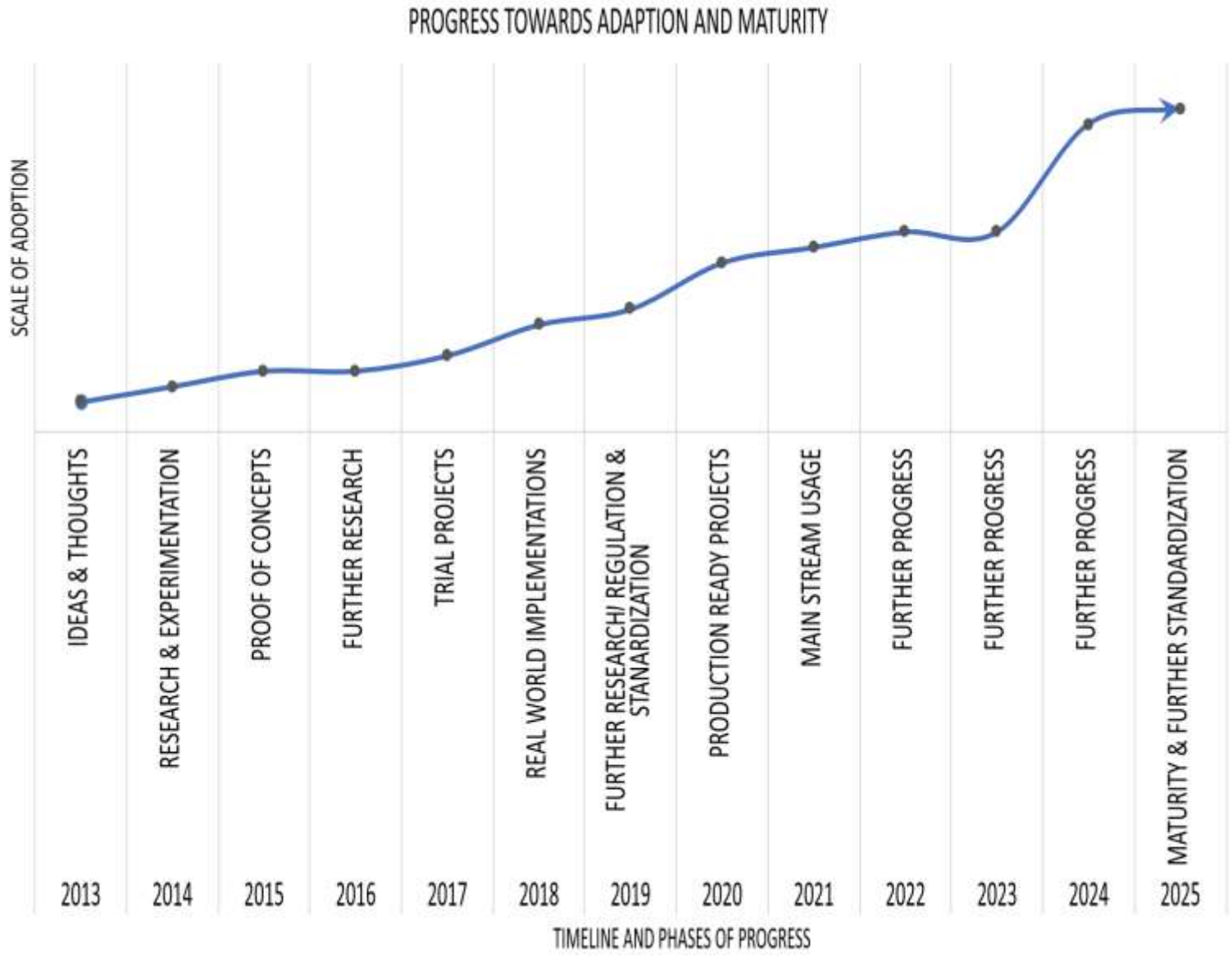
- Walmart
- DeBeers
- Amazon
- Blockchain and IOT
  - Continuity of information
  - Accessibility of information
  - Link between physical and information flows
  - Code of conduct violations and fraud detection
  - Effective fraud detection process

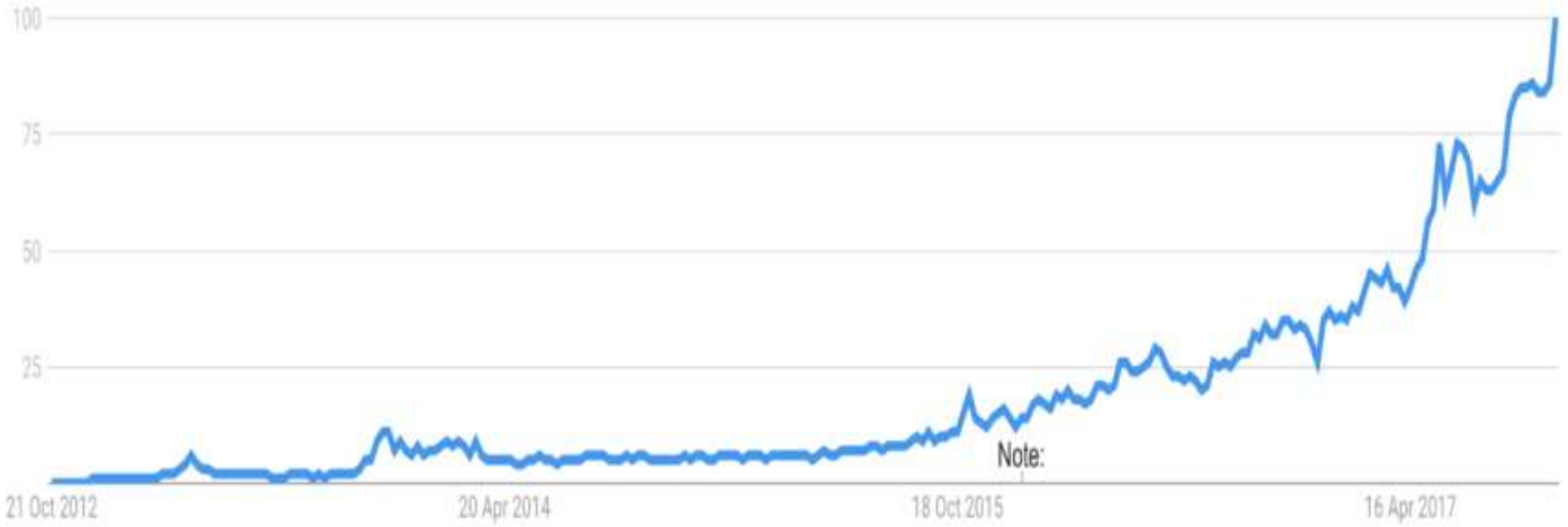
Technical requirements

- Identity and reputation of participants is central to the trust and must be exposed.
- Information generated is qualitative
- Controlled access to information is critical – smart contracts
- Usage of type of nodes and relative capabilities in the network
- Connectivity id intermittent and action must be taken when disconnected
- Actions must be reversible

Drawbacks of Blockchain

- Blockchain has an environmental cost
- Lack of regulation creates a risky environment
- More complex – hard to appreciate the benefits
- Blockchains can be slow and cumbersome.


PROGRESS TOWARDS ADAPTION AND MATURITY
SCALE OF ADOPTION
IDEAS & THOUGHTS
RESEARCH & EXPERIMENTATION
PROOF OF CONCEPTS
FURTHER RESEARCH
TRIAL PROJECTS
REAL WORLD IMPLEMENTATIONS
FURTHER RESEARCH/ REGULATION & STANARDIZATION
PRODUCTION READY PROJECTS
MAIN STREAM USAGE
FURTHER PROGRESS
FURTHER PROGRESS
FURTHER PROGRESS
MATURITY & FURTHER STANDARDIZATION
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
TIMELINE AND PHASES OF PROGRESS



Google trend graph for blockchain

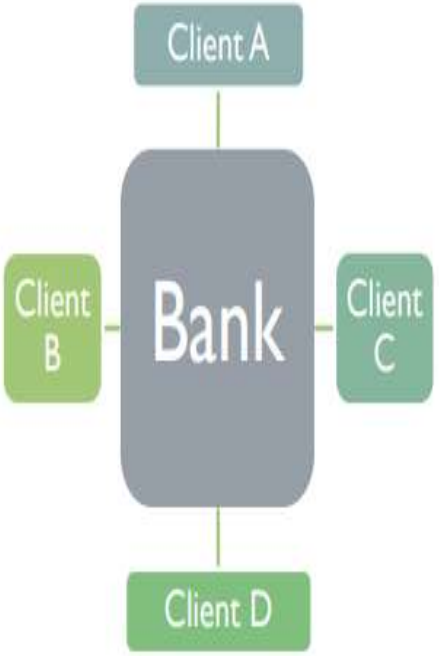
Revisiting the def

- Blockchain is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update
- Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.
- Blockchain is a system comprised of..
  - Transactions
  - Immutable ledgers
  - Decentralized peers
  - Encryption processes
  - Consensus mechanisms
  - Optional Smart Contracts

- **Peer-to-peer**
  - no central controller in the network
  - all participants talk to each other directly
  - **No** third-party involvement

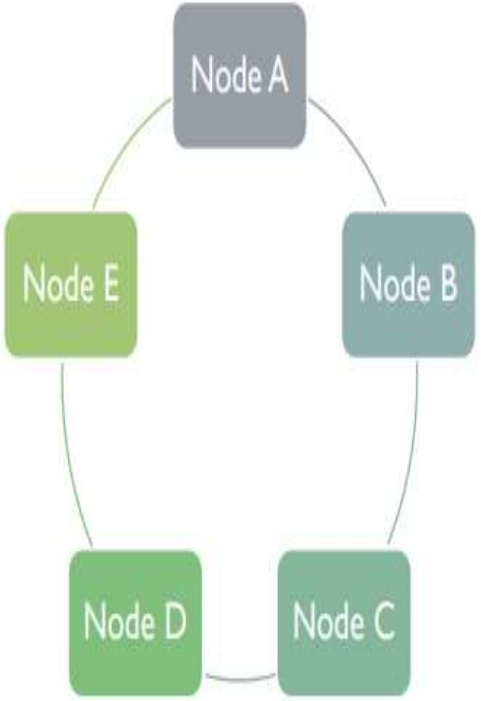
- **Distributed ledger**
  - ledger is spread across the network among all peers in the network
  - each peer holds a copy of the complete ledger

Centralized Ledger

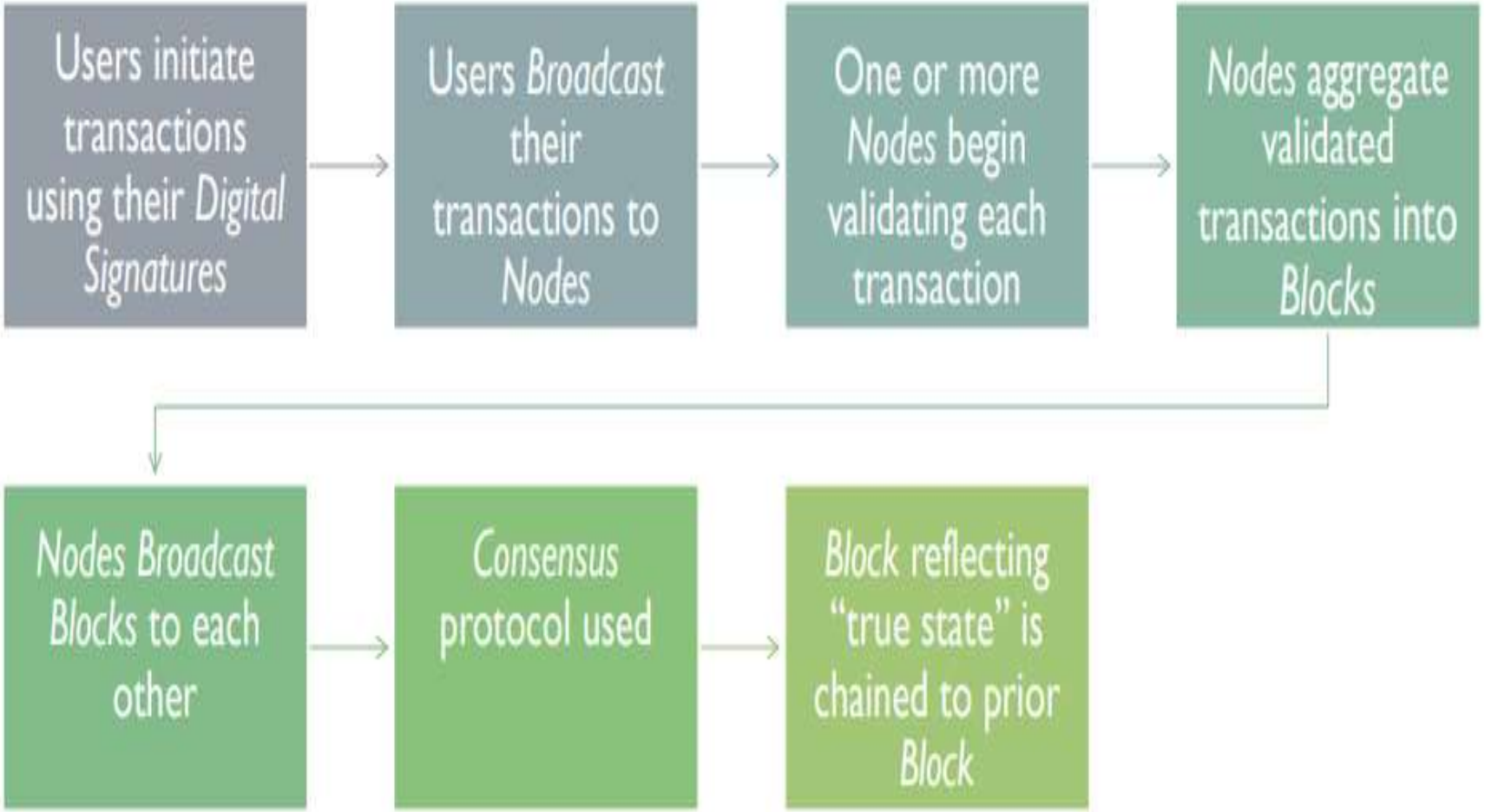


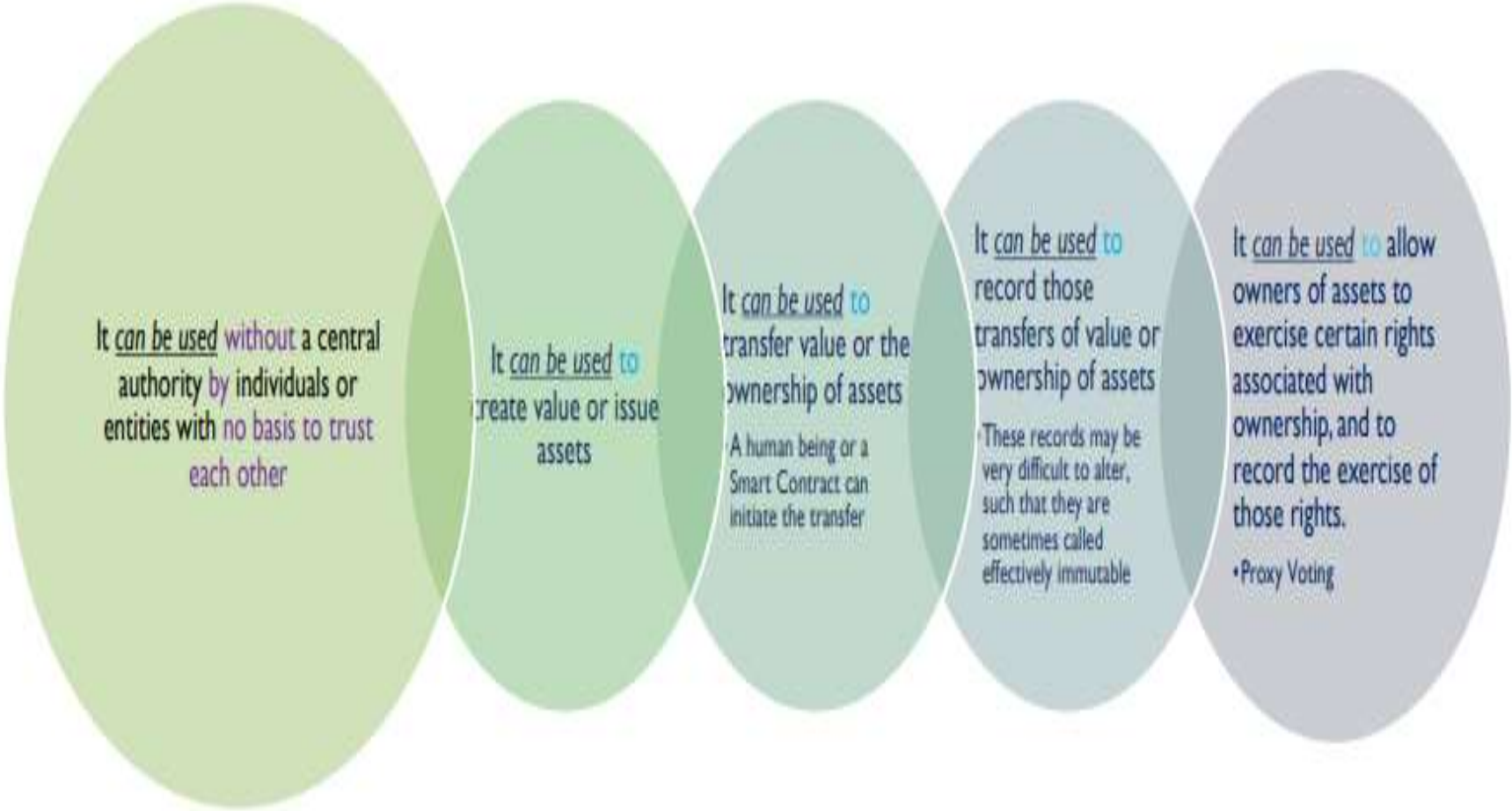
- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

Distributed Ledger



- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."


Users initiate transactions using their *Digital Signatures*
Users *Broadcast* their transactions to *Nodes*
One or more *Nodes* begin validating each transaction
Nodes aggregate validated transactions into *Blocks*
Nodes Broadcast Blocks to each other
Consensus protocol used
Block reflecting "true state" is chained to prior *Block*



Degree of trust between the users determines the technological configuration of a distributed ledger

Participation	Open	Closed
Permission	Permissionless	Permissioned
Ledger Design	One ledger	One ledger or Segregated ledgers
Validation	Methodology depends on degree of trust between nodes. Where there is no basis for trust, may be achieved through proof of work, which requires the algorithmic solving of a cryptographic hash.	
Consensus Mechanism	Mechanism depends on degree of trust between nodes. Where there is no centralized authority, consensus may be determined algorithmically.	

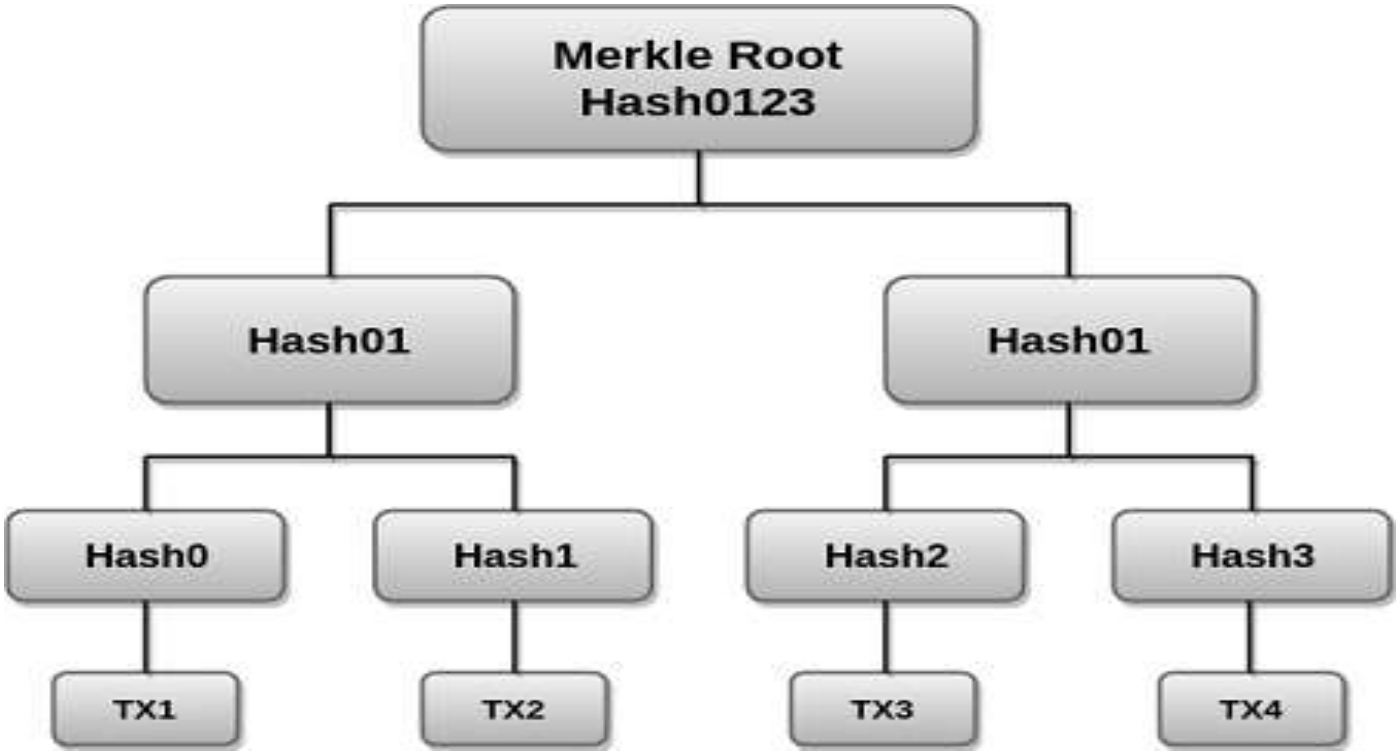
- Cryptographically secure
  - Use of cryptography to provide security services
  - Non repudiation, data integrity and data origin authentication
- Append only
  - data can only be added to the blockchain in *time-ordered sequential order*
  - General Data Protection (GDPR) ruling
  - immutable and cannot be changed.
- Updatable via consensus
  - Decentralization
  - Updates validated against blockchain protocol and added only after consensus have been reached.
  - distributed peer-to-peer network running on top of the internet

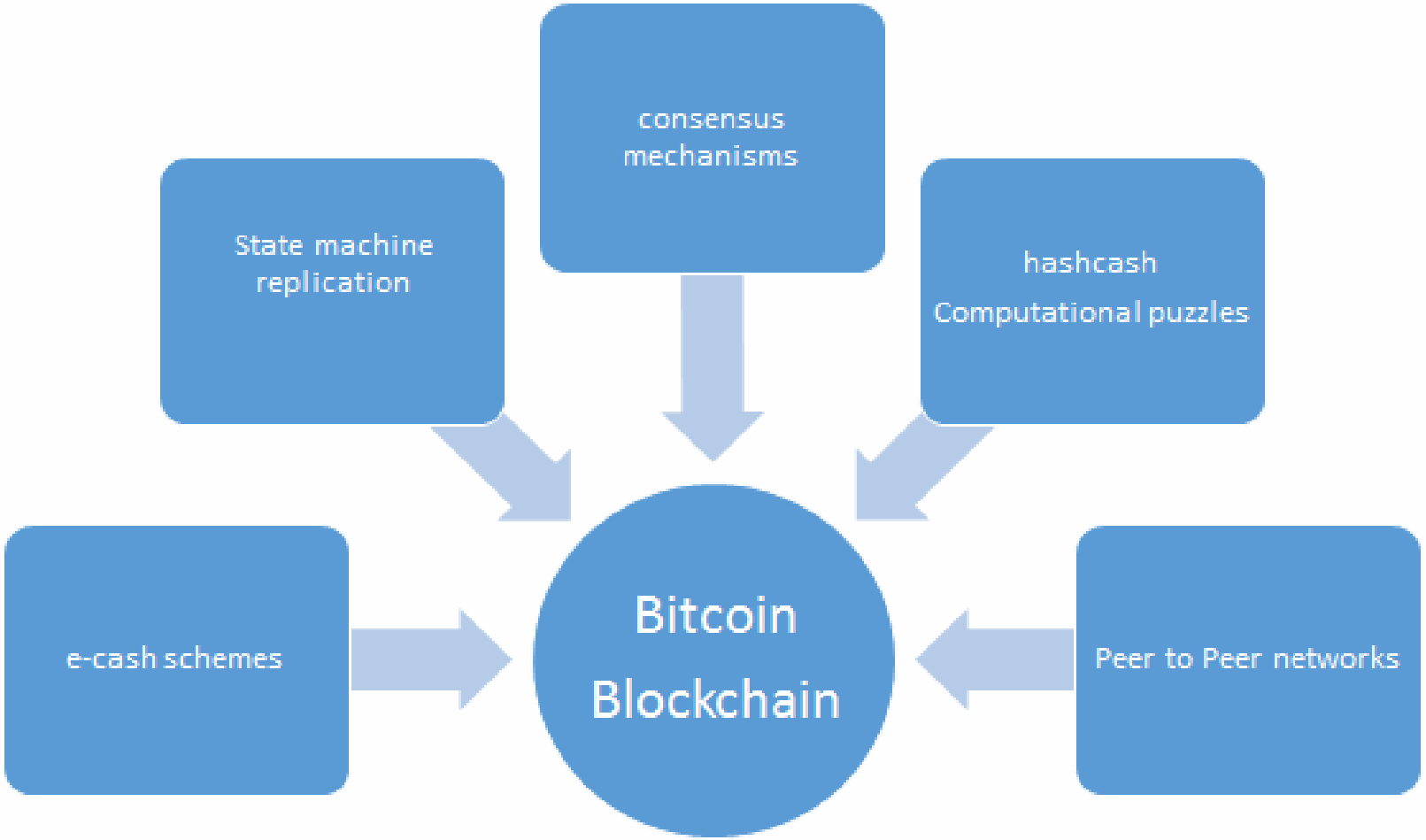
History of Blockchain

- Blockchain was introduced with the invention of Bitcoin in 2008
- Electronic cash
  - Accountability and anonymity
  - Use of blind signatures and secret sharing
- Crypto currency – solved the problem of distributed consensus in a trustless network
- Public key cryptography – with Proof of Work mechanism
- Secure, controlled and decentralized method of mining digital currency
- Bitcoins – Merkle trees, hash functions and hash chains.

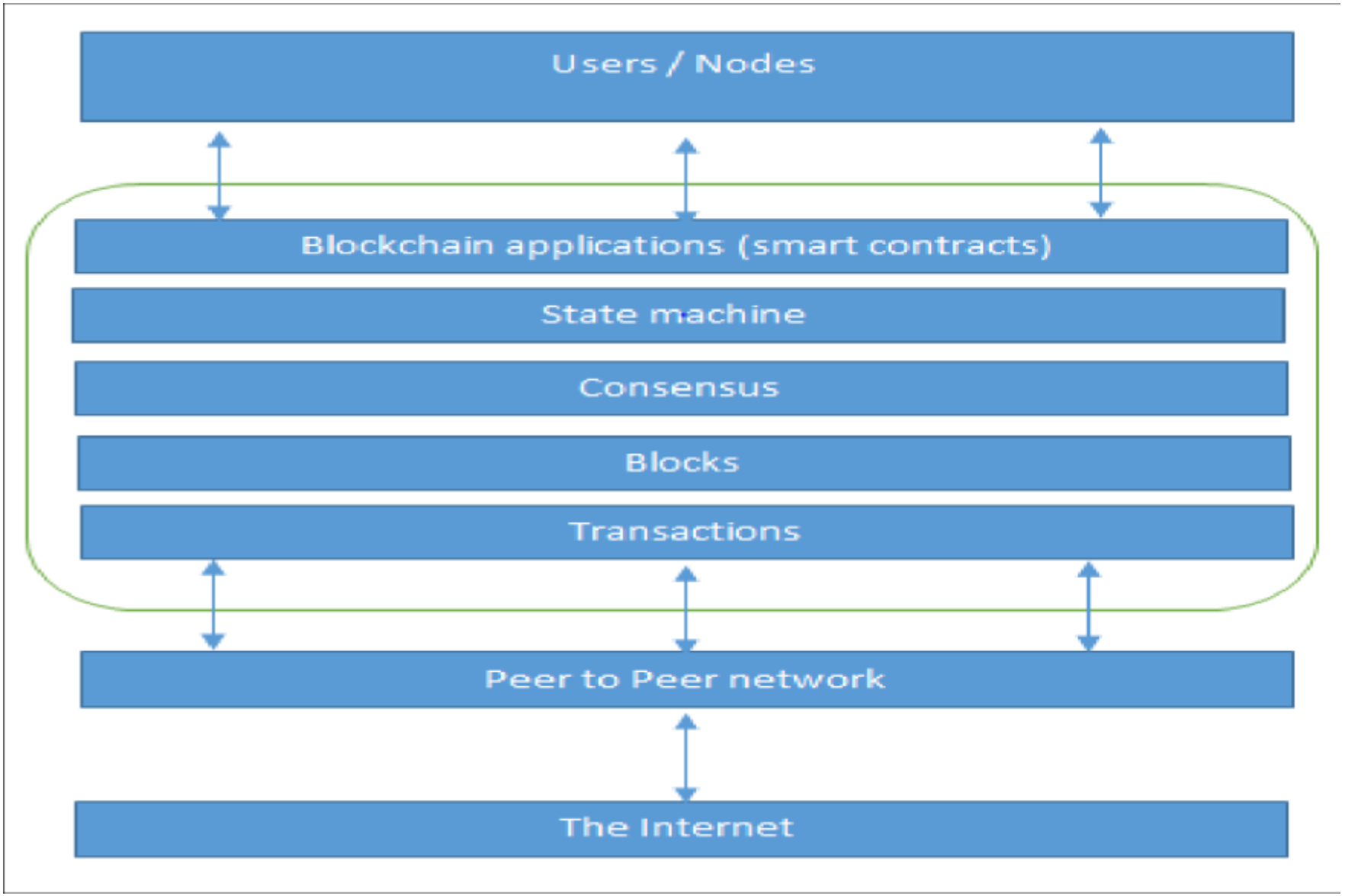
- Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system

- Merkle tree is a fundamental part of blockchain technology. It is **a mathematical data structure composed of hashes of different blocks of data**, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data





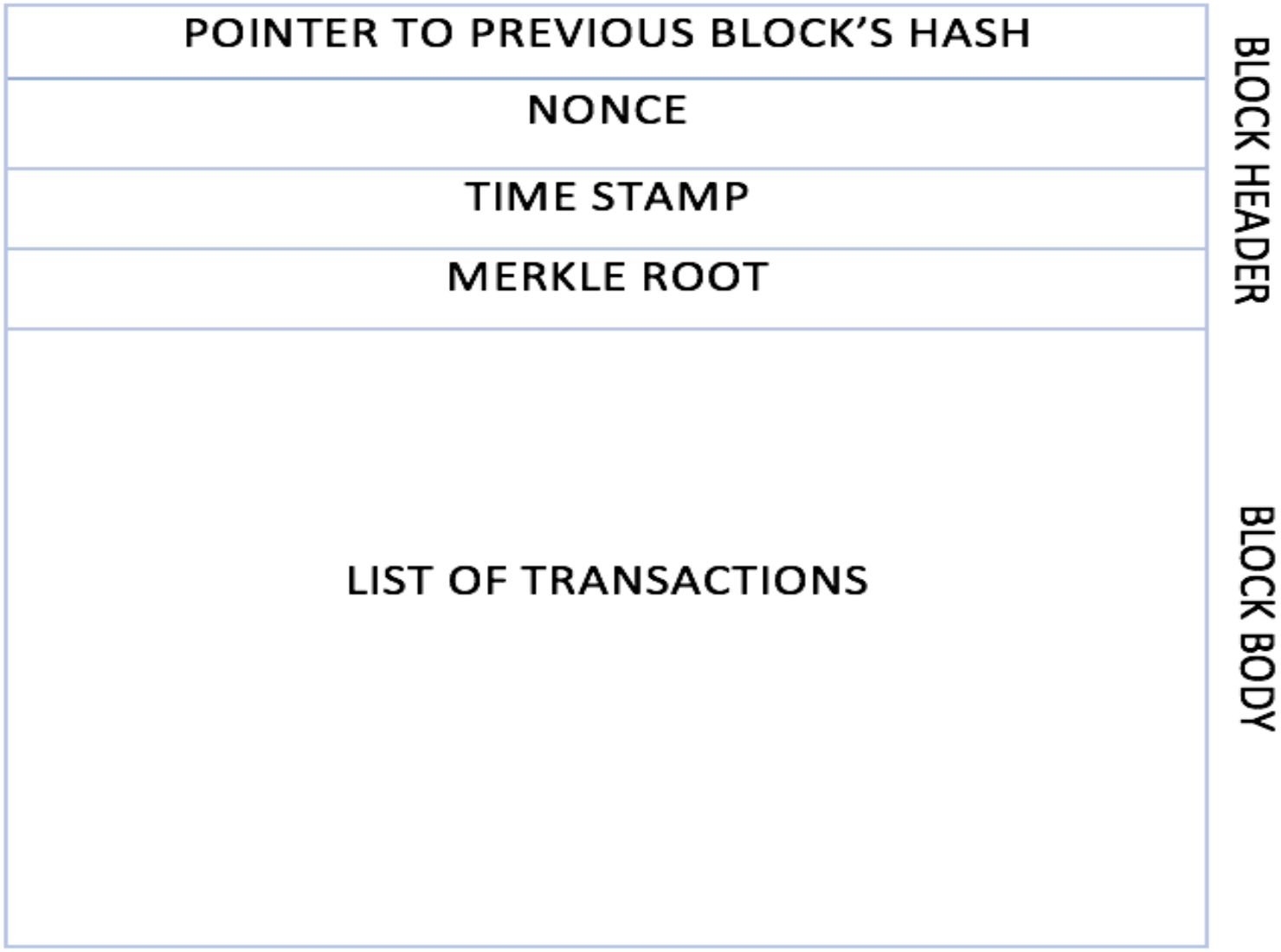
State machine replication: Fault tolerance and transperancy



Network view of a blockchain

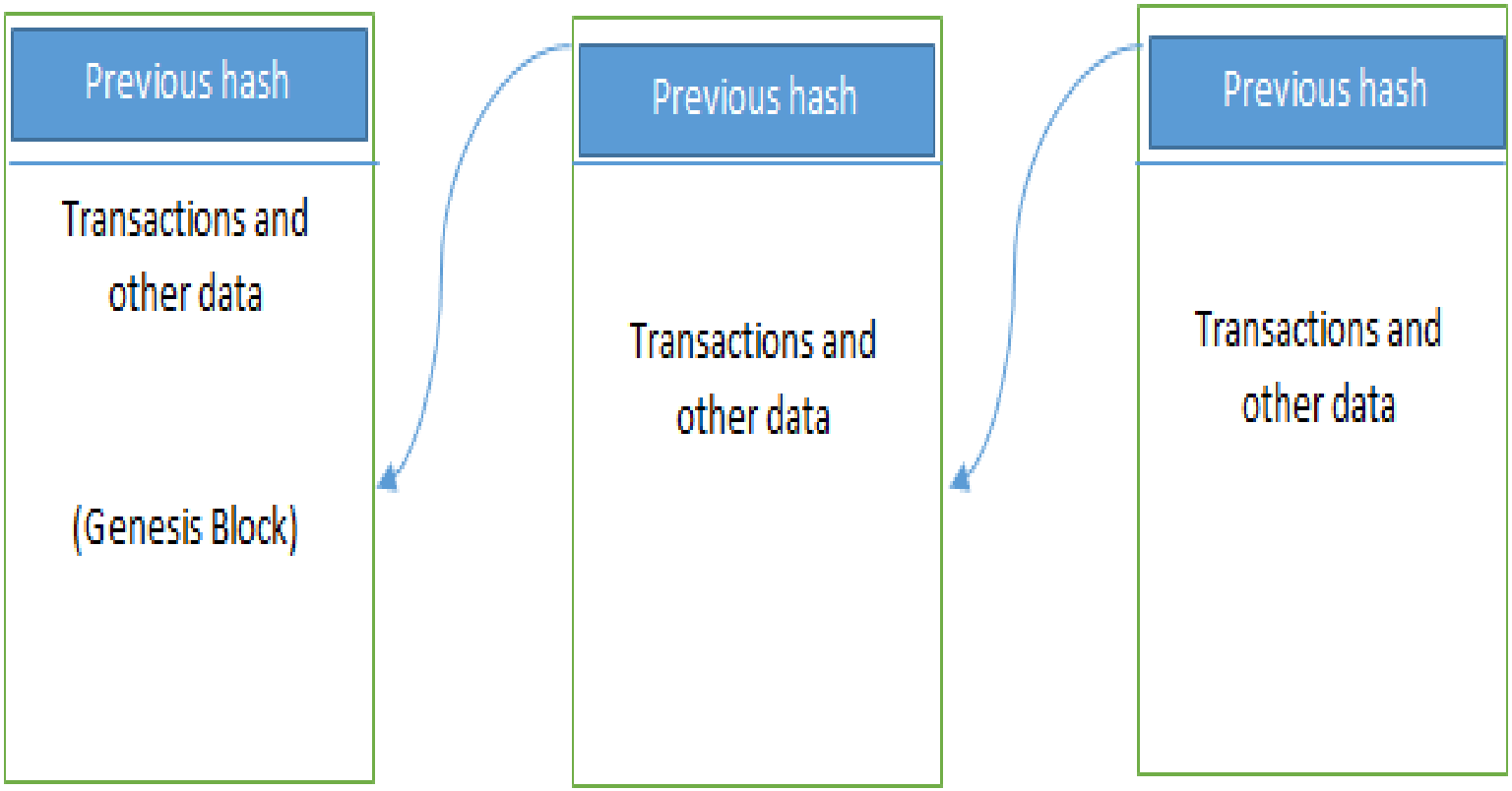
- Internet – provides the basic communication layer
- Peer – to – peer network : runs on top of the internet, hosts a layer of blockchain
- Blockchain – transactions, blocks, consensus mechanisms, state machines, blockchain smart contracts.
- Users/ Nodes – carrying out transaction verification, consensus and processing

- Block: a selection of transactions organized logically
- Transaction: record of an event
- Genesis block: first block which is hardcoded at the starting of the blockchain
- Nonce: number that is generated and used only once
- Merkle Root: hash of all nodes of a Merkle tree
  - Mathematical data structures composed of hashes of different blocks of data
  - Serves as a summary of all transactions in a block
- Functional attributes of a block are: block header, timestamp, nonce, Merkle root and block body which is composed of transactions.



Generic structure of a block

Generic Elements of Blockchain



- Elements of a blockchain
  - Address
  - Transaction
  - Block
  - Peer to peer network
  - Scripting or Programming language
  - Virtual machine
  - State machine
  - Node
  - Smart Contract

Working of a Blockchain

- Nodes also called as miners create new blocks and mint crypto currencies
- Block signers validate and digitally sign the transactions
- Decision is made in the blockchain network regarding which node will append the next block to the blockchain – consensus mechanism

Accumulation of blocks in blockchain

- Transaction is started at the node by creating and digitally signing the node with private key
  - Transaction data structure consists of logic, relevant rules, source and destination address and other validation information
- Transaction is propagated in the blockchain network using flooding protocol – Gossip Protocol
- Validated transactions are included in the block and then propagated on to the network; along with confirming the transaction
- Newly created block becomes a part of the ledger – next block links itself cryptographically to this block – link is a hash pointer
  - Second confirmation of the transaction and first confirmation of the block
- Transactions are reconfirmed every time a new block is created.
  - Six confirmations are required for a transaction to be considered final in a Bitcoin network

Benefits and Limitations

- Benefits
  - Decentralization
  - Transparency and Trust
  - Immutability
  - High availability
  - Highly secure
  - Faster Dealings
  - Cost Saving
  - Simplification of current paradigms

- Limitations
  - Scalability
  - Adaptability
  - Regulation
  - Relatively immature technology
  - Privacy

Tiers of Blockchain Technology

- Blockchain 1.0
  - Cyrptographic currencies
  - Payments and applications
  - 2009 - 2010
- Blockchain 2.0
  - Financial services and smart contracts
  - Financial assets – derivatives, options, swaps, bonds
  - Ethereum, Hyperledger
  - 2010
- Blockchain 3.0
  - Used in government, health, media, arts and justice sectors
  - 2012
- Blockchain X.0
  - Represents a vision of blockchain singularity – public, open, with general purpose rational agents

Features of Blockchain

- **Distributed Consensus**
  - present a single version of the truth, which is agreed upon by all parties without the requirement of a central authority
- **Transaction verification**
  - valid transactions are selected for inclusion in a block
- **Platform for smart contracts**
  - These are automated, autonomous programs that reside on the blockchain network and encapsulate the business logic and code needed to execute a required function when certain conditions are met.
- **Generation of Crypto currency**
  - incentive to its miners who validate the transactions and spend resources to secure the blockchain
- **Transferring value between peers**
  - transfer of value between its users via tokens

- **Smart Property**
  - link a digital or physical asset to the blockchain in such a secure and precise manner that it cannot be claimed by anyone else – Digital Rights Management
- **Provider of Security**
  - integrity, availability of data, confidentiality and transparency, non repudiation and authentication – private keys and digital signatures
- **Immutability**
  - remote possibility of rolling back changes
- **Uniqueness**
  - Every transaction is unique, detection and avoidance of double spending is important

Types of Blockchain

- Distributes Ledgers
- Distributed Ledger Technology
- Blockchains
- Ledgers

- Distributed Ledgers
  - Distributed among the participants and spread across multiple sites or organizations
  - records are stored contiguously instead of being sorted into blocks
  - Corda - to record and manage agreements – financial services industry
  - Ripple – global payment network

- Distributed Ledger Technology
  - DLTs are permissioned blockchains that are
  - shared and used between known participants.
  - Shared database, with all participants known and verified.
  - Do not have cryptocurrency and does not require mining to secure the ledger

- Public blockchains
  - Open to public
  - Anyone can participate as a node in the decision making process
  - Rewards are not guaranteed
  - Users of these ledgers maintain a copy of the ledger on their local nodes
  - Use a distributed consensus mechanism to decide the state of the ledger
  - Eg: bitcoin, Ethereum

- Private Blockchains
  - Open only to a group of individuals/consortium/organizations who have decided to share the ledger among themselves
  - Can run in public mode if required
  - Eg: HydraChain and Quorum

- Permissioned ledger
  - Participants are already known and trusted with regulated access control
  - Does not require distributed consensus mechanism
  - Agreement protocol is used to maintain the shared version of the records
- Shared ledger
  - shared by the public or a consortium
- Fully private and proprietary blockchains
  - Need to share the data and provide the guarantee of authenticity.
- Tokenized blockchains
  - Generation of crypto currency as a result of consensus process through mining or initial distribution.
- Tokenless blockchains
  - Similar to private blockchains without tokens and shared distributed ledgers.

Consensus

- Consensus is a process of agreement between distrusting nodes on the final state of data
- developed to deal with faults in a distributed system and to allow distributed systems to reach a final state of agreement
- Distributed consensus
- Consensus algorithm depends on the type of application
- Types:
  - BFT based
  - Leader Election based

- Byzantine Fault Tolerance based
  - Consortium or permissioned type
  - No compute-intensive operations
  - Uses publisher signed messages
  - Agreement is reached based on the number of messages received
- Leader election based
  - Fully decentralized or permission less type
  - Leader-election lottery method
  - Winning node proposes a final value
  - Ex: PoW
- Paxos
  - Nodes – Proposer, Acceptor and Learner
  - Consensus is achieved in the presence of faulty nodes
- RAFT
  - Selection of the leader node
  - Leader commits proposed changes based on the replication on the majority of the follower nodes

Consensus Algorithms

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake (DPoS)
- Proof of Elapsed Time (PoET)
- Proof of Deposit (PoD)
- Proof of Importance (PoI)
- Federated consensus or federated Byzantine consensus
- Reputation-based mechanisms
- PBFT
- Proof of Activity (PoA)
- Proof of Capacity (PoC)
- Proof of Storage (PoS)

- **Proof of Work (PoW)**
  - Requires adequate computational resources for proposing a value for acceptance by the network
  - Bitcoin, Litecoin
  - Sybil Attack
- **Proof of Stake (PoS)**
  - Node or user should have adequate stake in the system
  - Coin age
  - Chances of proposing and signing the next block increases with coin age
- **Delegated Proof of Stake (DPoS)**
  - each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting
  - Bitshares blockchain

- **Proof of Elapsed Time (PoET)**
  - Trusted Execution Environment – provides randomness and safety in leader election process
  - Software Guard Extensions
  - *Hyperledger*
- **Proof of Deposit (PoD)**
  - nodes that wish to participate in the network have to make a security deposit before they can mine and propose blocks
- **Proof of Importance (PoI)**
  - monitors the usage and movement of tokens by the user in order to establish a level of trust and importance
  - NEM coin blockchain

- **Federated consensus**
  - stellar consensus protocol
  - Transactions - validated by the majority of trusted nodes.
- **Reputation-based mechanisms**
  - leader is elected by the reputation it has built over time on the network
  - based on the votes of other members
- **PBFT**
  - State machine replication
- **Proof of Activity (PoA)**
  - Combination of PoS and PoA
  - Stakeholder is selected in pseudorandom but uniform fashion

- **Proof of Capacity (PoC)**
  - uses hard disk space as resource to mine the blocks
  - hard drive mining
  - Burstcoin crypto currency
- **Proof of Storage (PoS)**
  - outsourcing of storage capacity
  - Piece of data stored by a node serves as a means to participate in the consensus mechanism