Blockchain Technology

22nd Nov 2019

G Jyostna

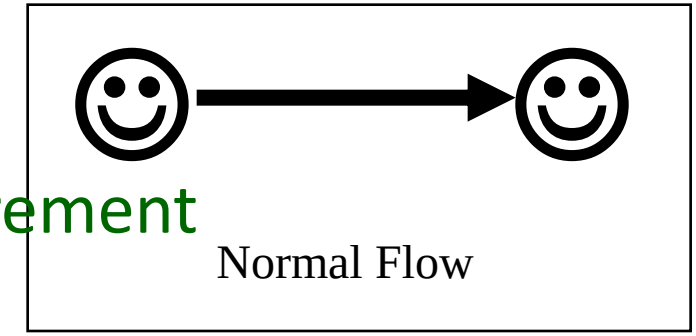
C-DAC Hyderabad

Agenda

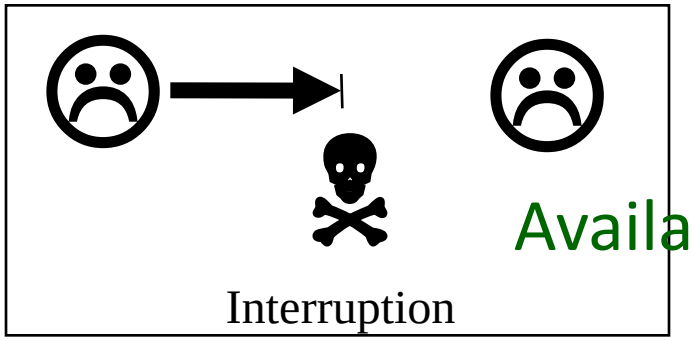
- Fundamentals
  - Cryptography
  - Merkle tree
  - Distributed Ledger
- Blockchain
  - Fundamentals
  - Types
  - Use cases

FUNDAMENTALS

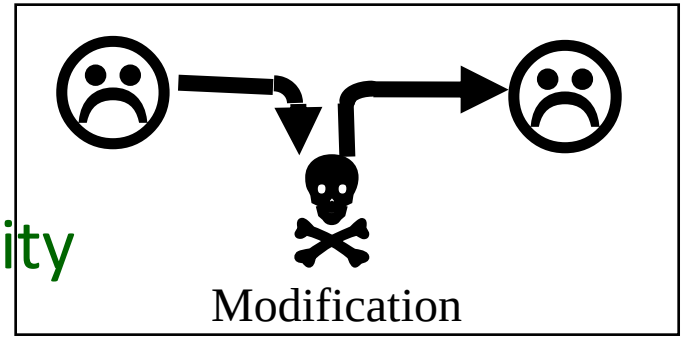
Network Security Issues & Requirements



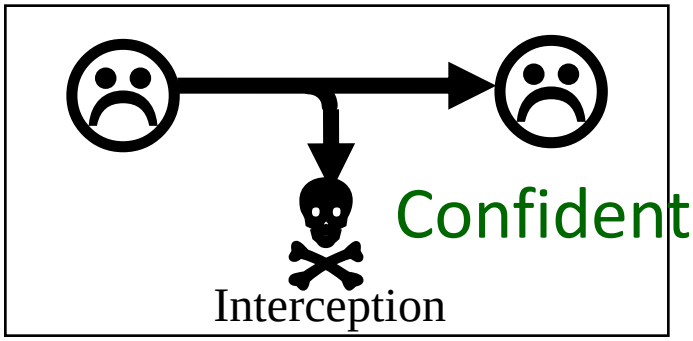
Requirement



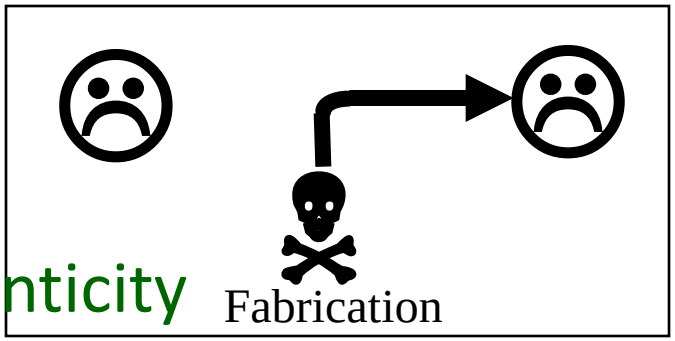
Availability



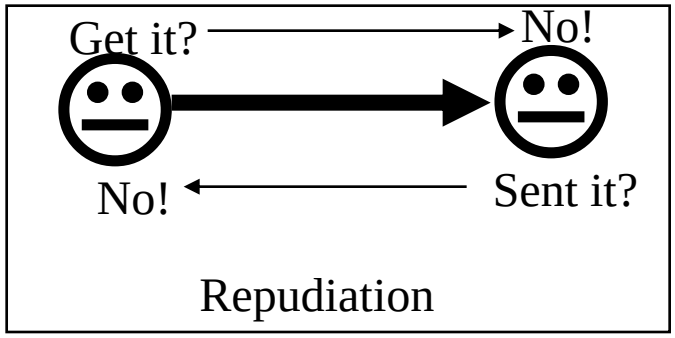
Integrity



Confidentiality



Authenticity



Non Repudiation

Security Mechanisms

- Confidentiality - Encryption
- Integrity - Hashing
- Non-Repudiation - Digital Signatures
- Authentication - Digital Certificates

Basic Cryptography Terminology

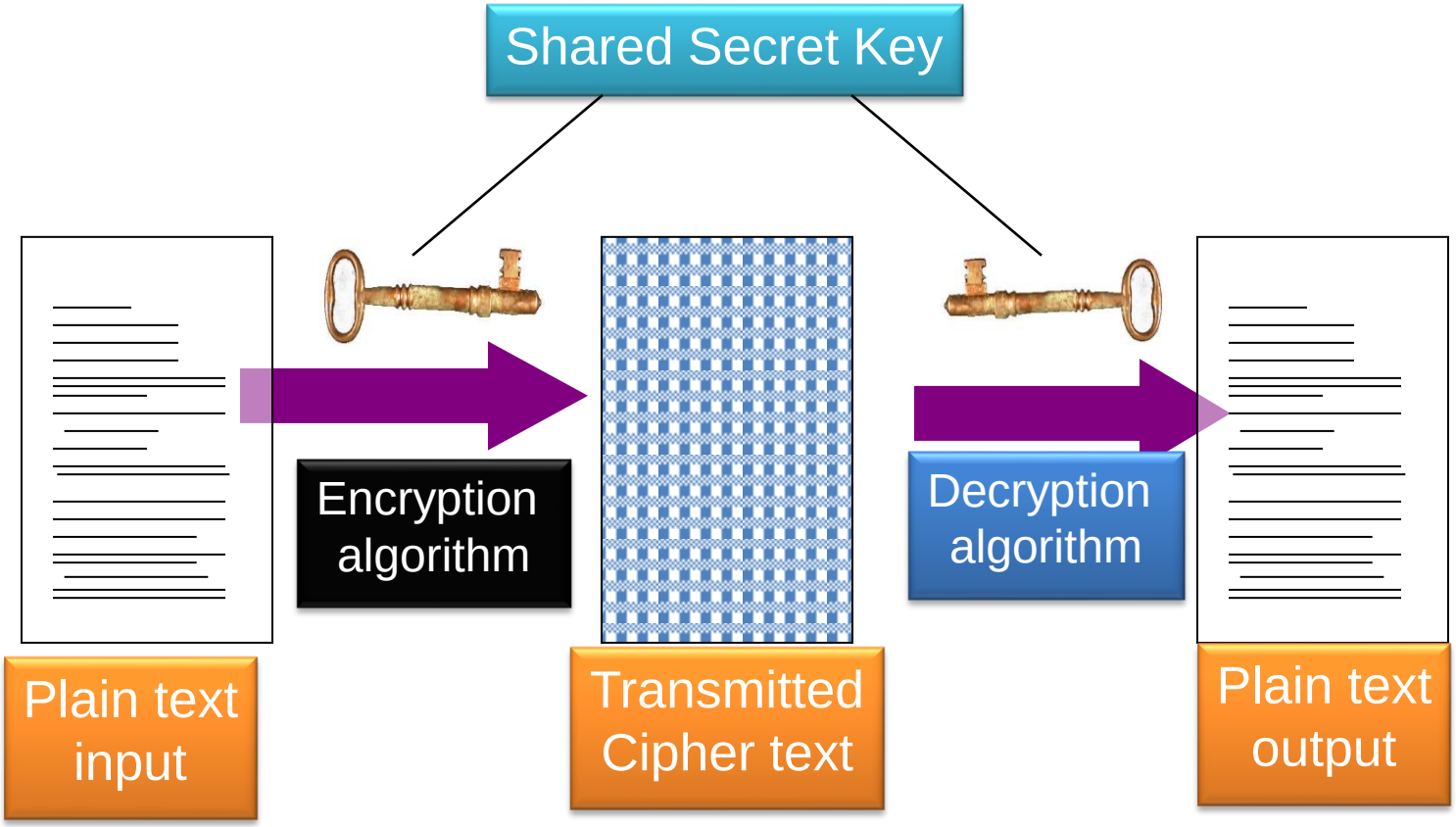
- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering plaintext from ciphertext
- **Cryptography** - study of encryption principles/methods

Cryptographic Algorithms

Types of Cryptographic Algorithms

- Secret key cryptography or Symmetric Key
- Public key cryptography or Asymmetric Key
- Hash functions

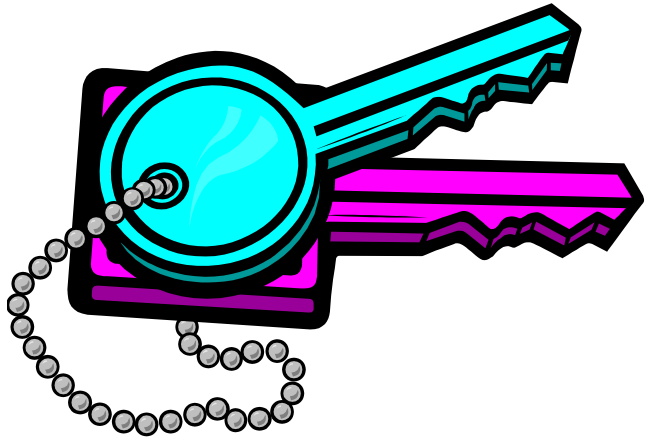
Secret Key Algorithms



Confidentiality

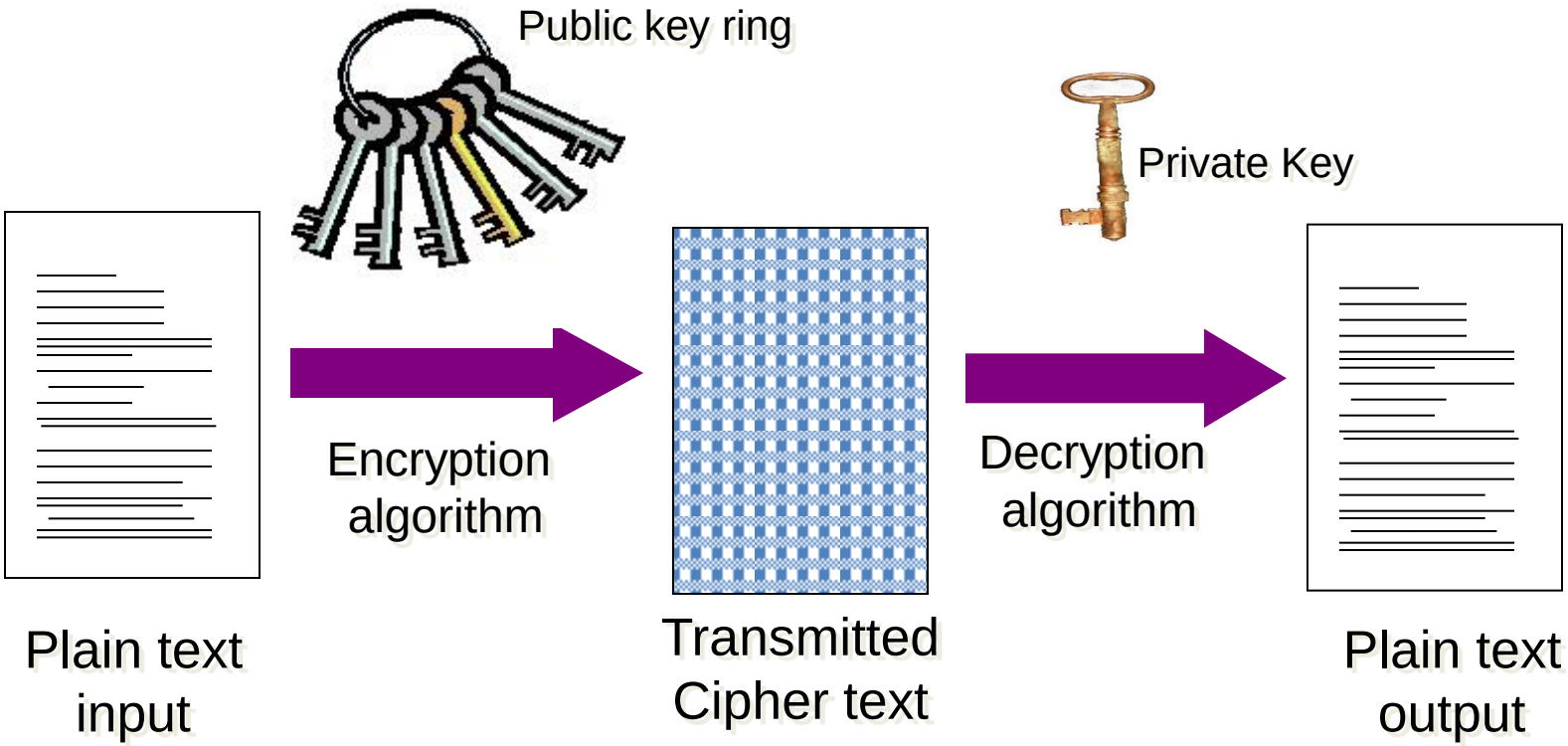
Public Key Cryptography

- Uses two keys: private & public
- Used for
  - Confidentiality
  - Authentication
  - Key distribution



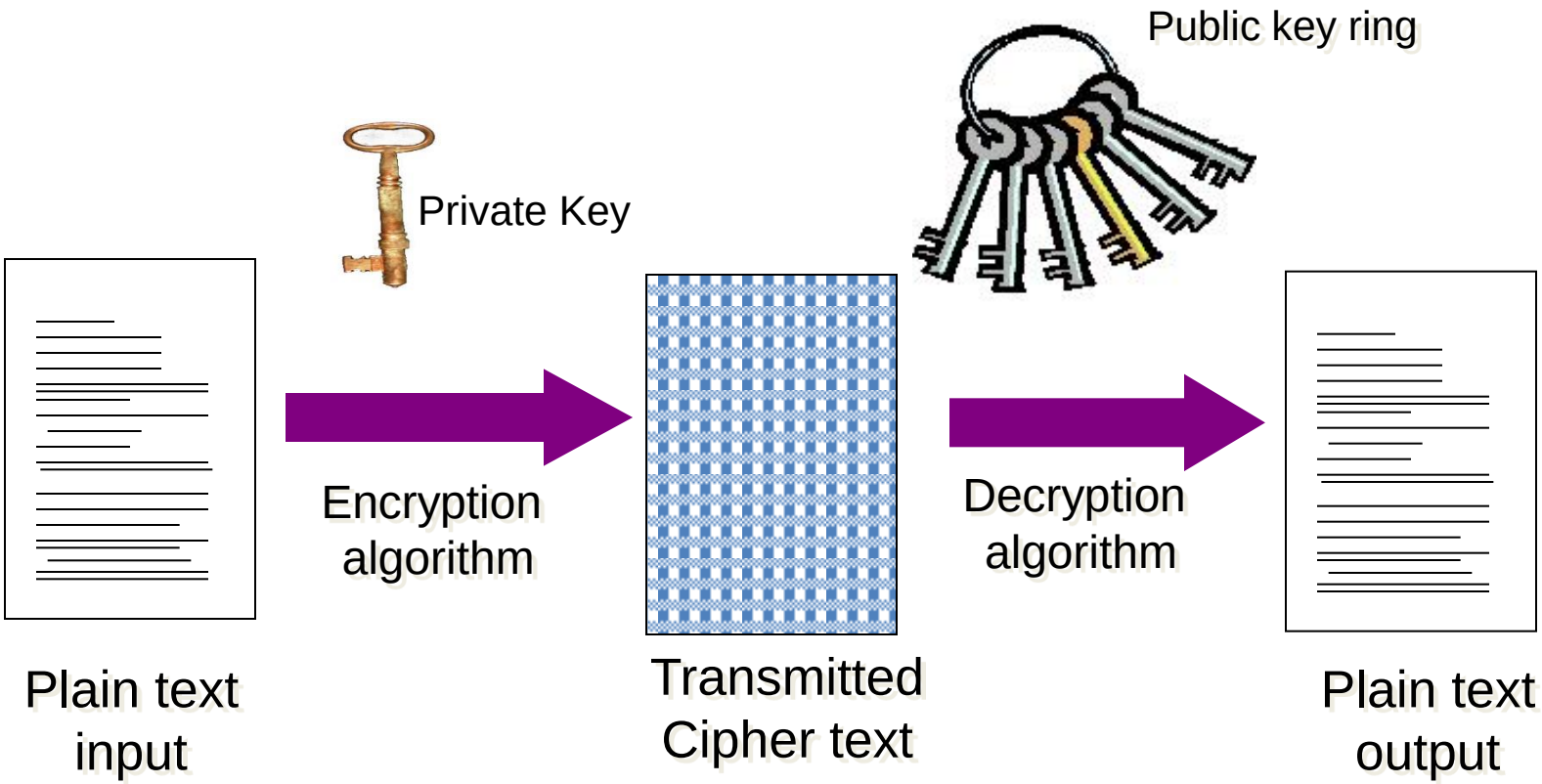
- Examples: RSA, Diffie Dellman, DSA etc

Public Key Algorithms



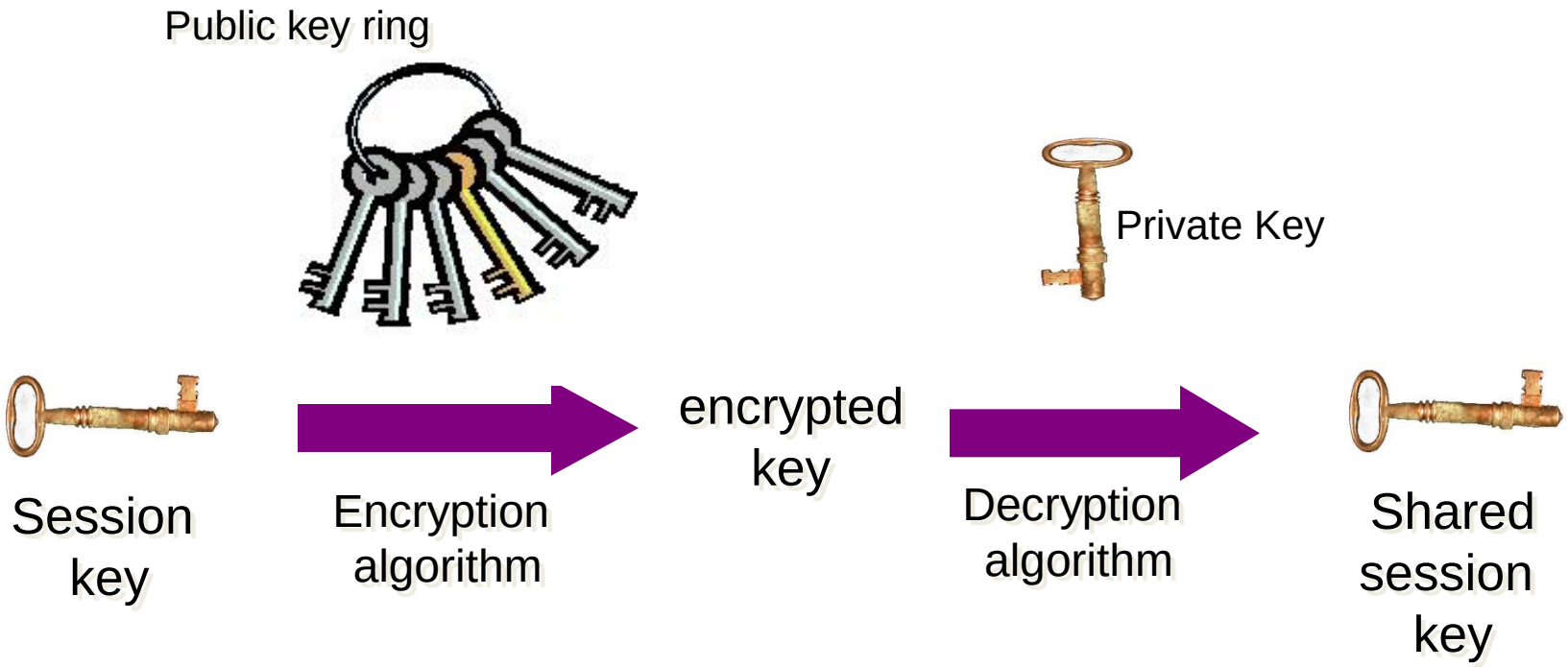
Confidentiality

Public Key Algorithms



Authentication

Public Key Algorithms



Key Exchange

The Hybrid Model

Very common practice: hybrid symmetric and asymmetric

- Asymmetric encryption is used to share a secret key, which is then used for symmetric encryption
- Advantages
  - Speed of symmetric, flexibility of asymmetric

Demo

- https://www.devglan.com/online-tools/aes-encryption-decryption

Integrity

- Encryption protects only against passive attack

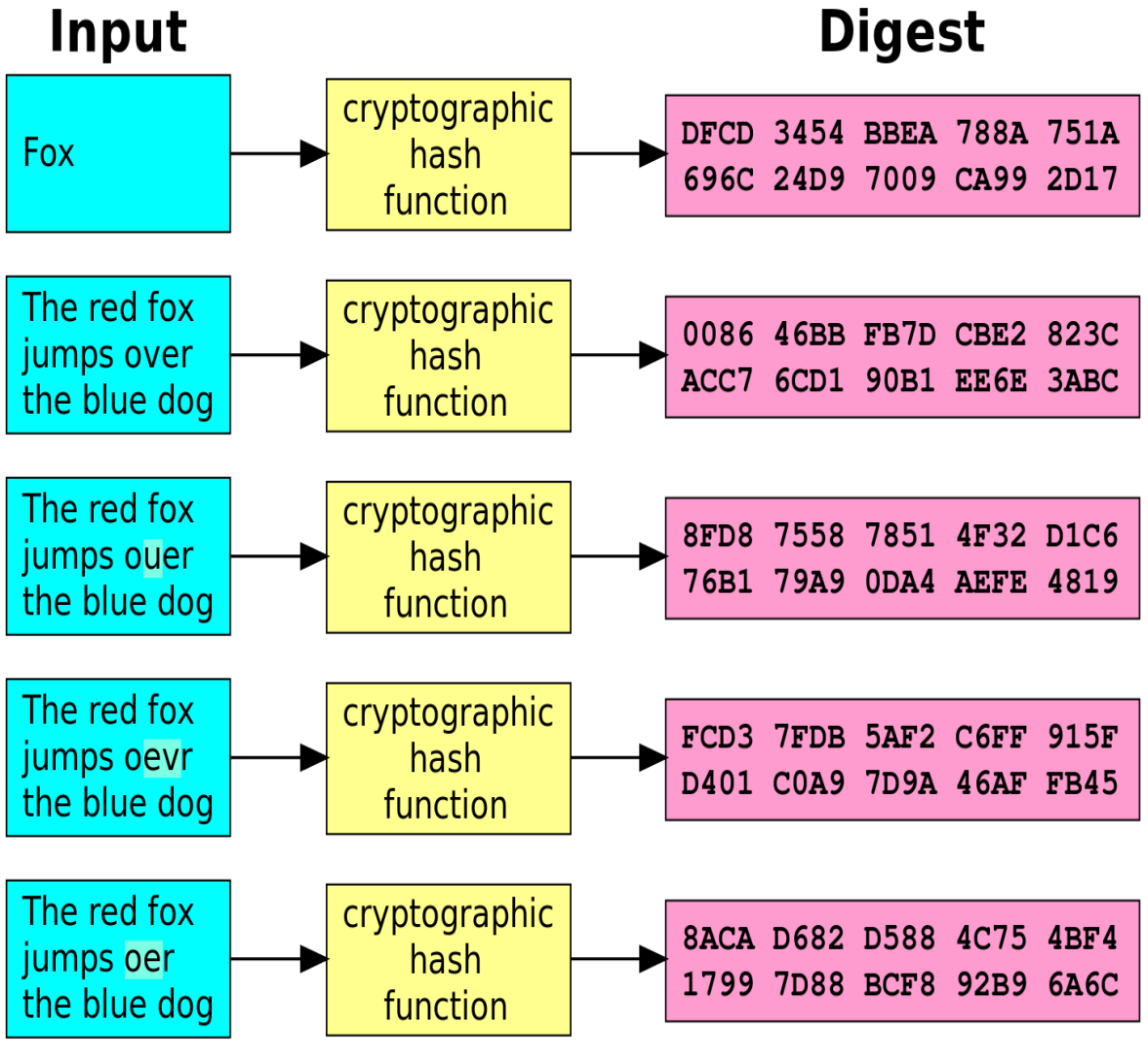
- Integrity
  - A message digest is computed which is appended to message using hash functions.
  - x is called the **message** and H(x) is called the **message digest**

Hash Functions

- Hash function **H** Map any sized data to a fixed size
- **x** can be of any arbitrary length, but **H(x)** is within the range **[0..n-1]**
- H is a function that map any sized data to a fixed size.

Cryptographically Secured Hash Functions

- Examples: MD5, SHA256
- x is called the **message** and H(x) is called the **message digest**
- A small change in the data results in a significant change in the output – called the **avalanche effect**



Source: https://en.wikipedia.org/wiki/Cryptographic_hash_function

Cryptographic Hash Function: Properties

- Collision-Free
- Hiding
- Puzzle-friendly

Demo

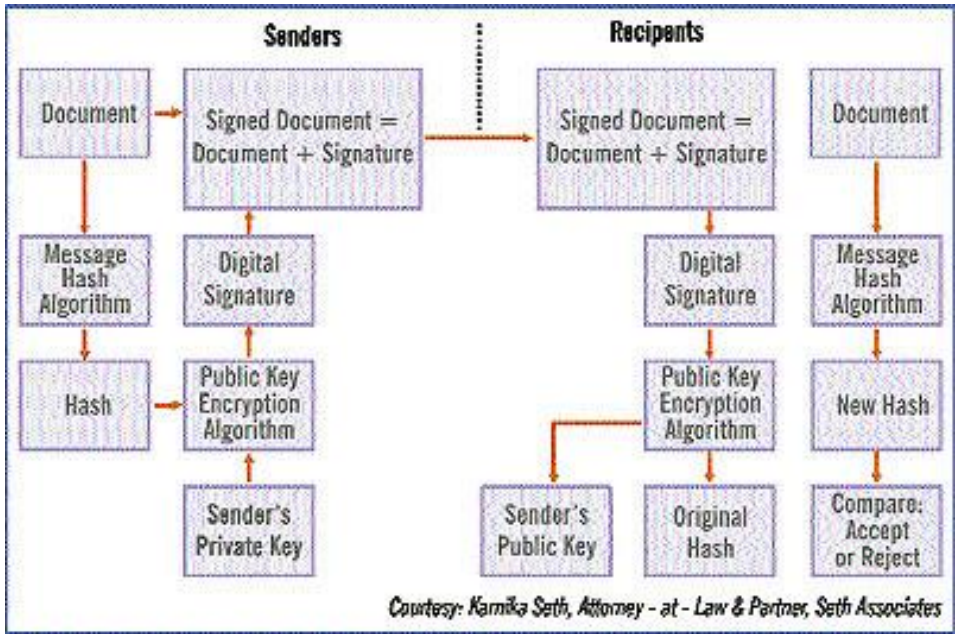
- https://www.tools4noobs.com/online_tools/hash/

Purpose of Digital Signature

- It is an authentication mechanism which enables the creator of a message to attach a code that acts as a signature
- Only the signing authority can sign a document, but everyone can verify the signature
- Signature is associated with the particular document
  - Signature of one document cannot be transferred to another document

How Digital Signature is Generated?

- Encrypt a small block of bits that is a function of the document (authenticator), using sender's private key.
- This serves as signature that verifies origin and content.
- SHA-1 or SHA-256 or other hash function can be used as this function.



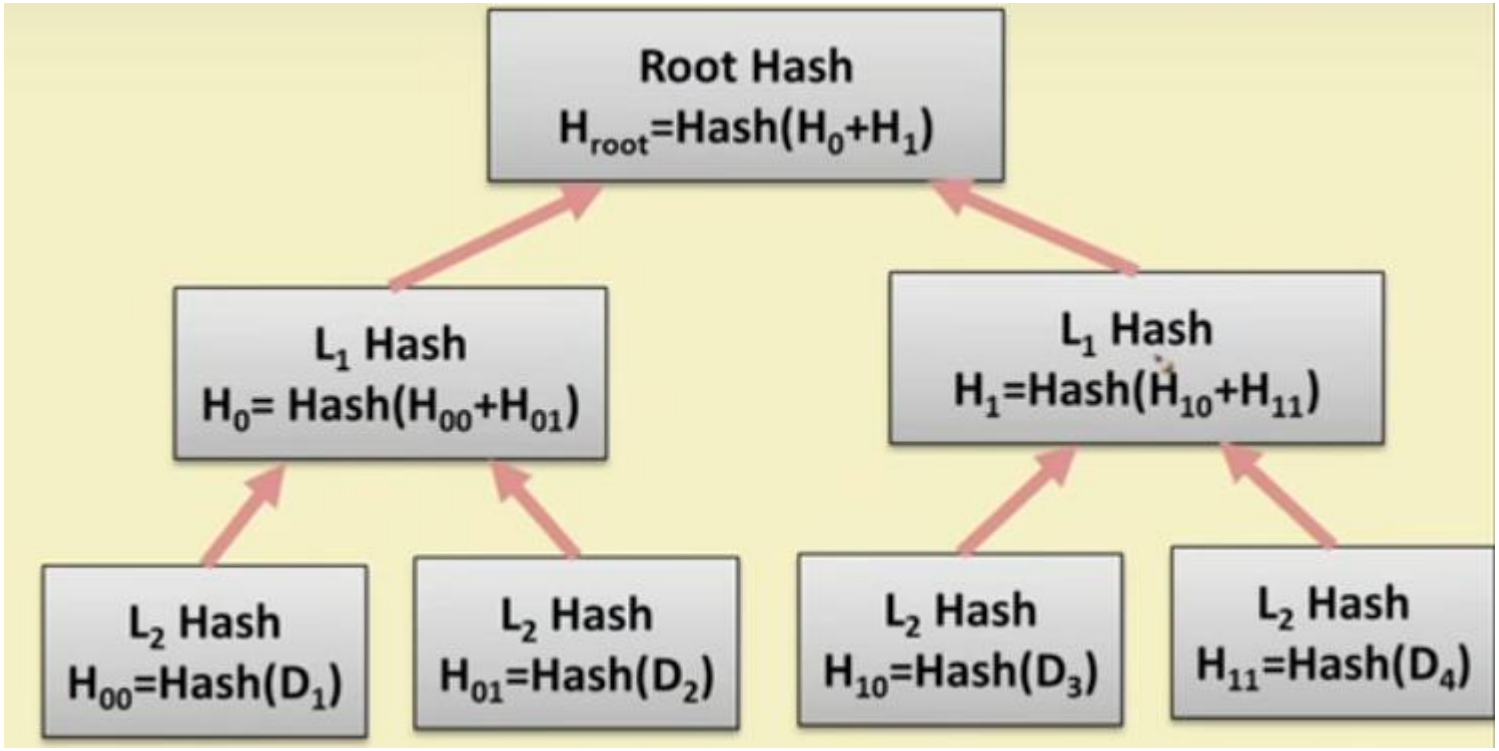
Digital Certificates – Manage Key

- Used for distribution of public keys.
- Public key certificate consisting of public key and user ID of key owner is signed by a trusted third party.
- The third party is called Certificate Authority(CA).

Digital Certificates

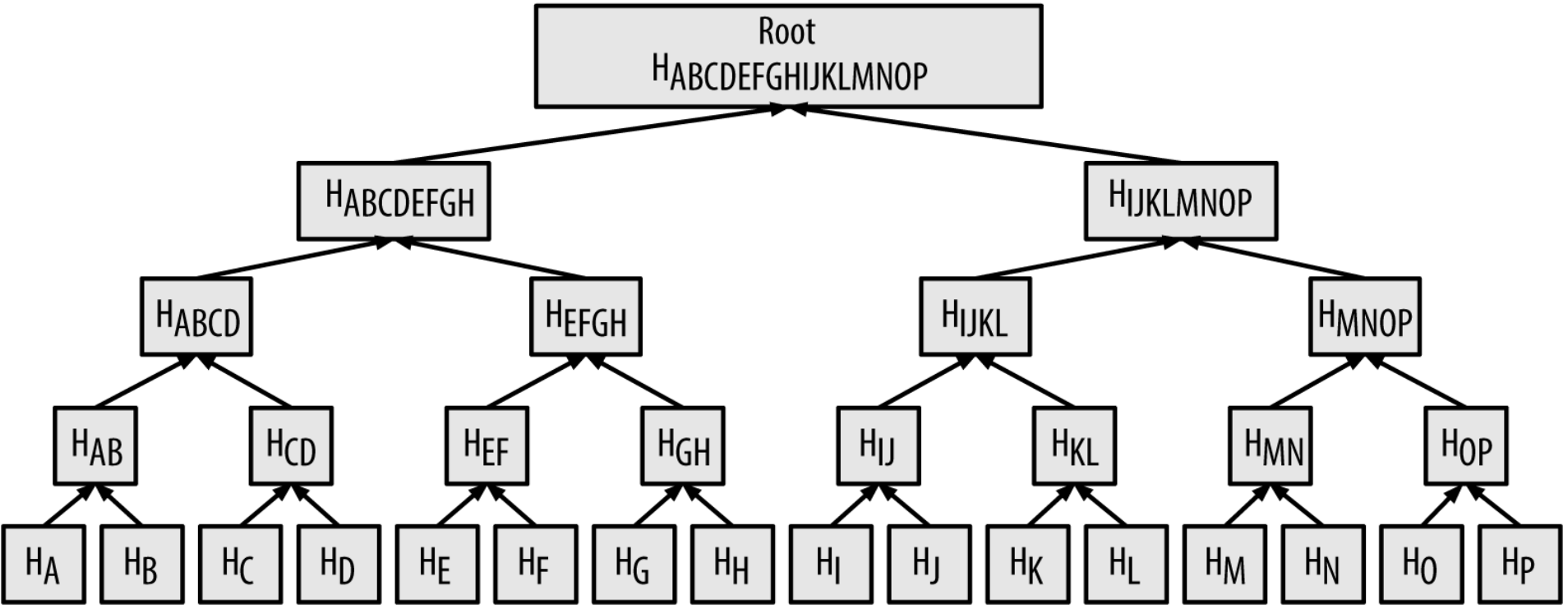
- A Digital Certificate typically contains
  - Owner's public key
  - Owner's name
  - Expiration date of the public key
  - Name of the issuer (CA that issued the Digital ID)
  - Serial number of the Digital ID
  - Digital signature of the issuer
  - X.509

Merkle Trees (Ralph Merkle, 1979)



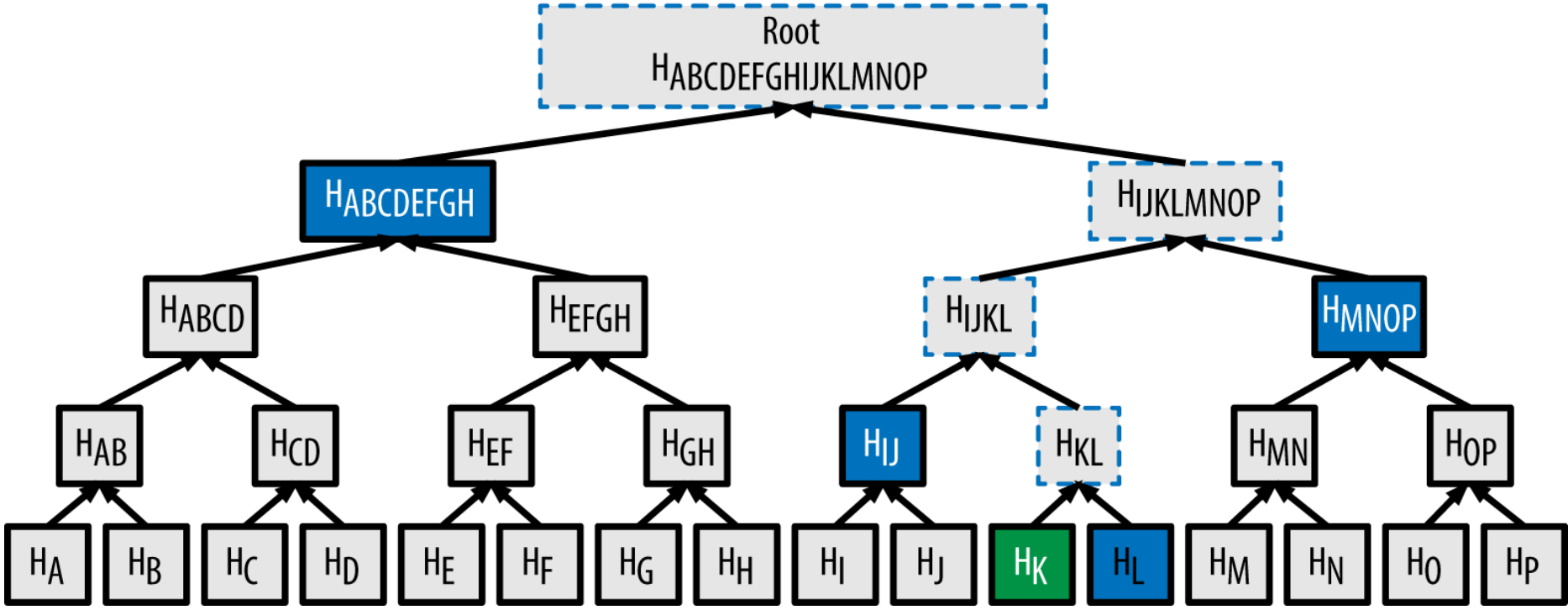
Source: NPTEL Course

Construction of Merkle tree



http://orm-chimera-prod.s3.amazonaws.com/1234000001802/images/msbt_0704.png

Transaction verification

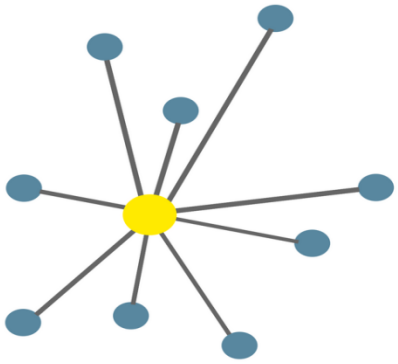


http://orm-chimera-prod.s3.amazonaws.com/1234000001802/images/msbt_0705.png

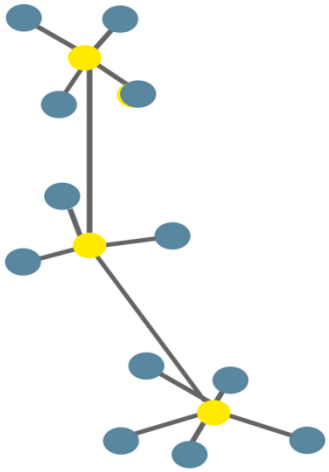
Why do we need a merkle tree

- Easy to check if transactions have been tampered with
- Uses fewer resources
- Easy to verify if a specific transaction has been added to the block

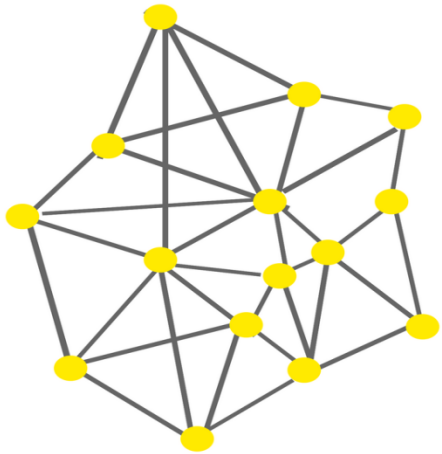
Three stages of computer network evolution



Centralized



Decentralized



Distributed

Source: Daxx.com

Pros
Simple deployment
Can be developed quickly
Affordable to maintain
Practical when data needs to be controlled centrally

Cons
Prone to failures
Higher security and privacy risks for users
Longer access times to data for users who are far from the server

Pros
Less likely to fail than a centralized system
Better performance
Allows for a more diverse and more flexible system

Cons
Security and privacy risks to users
Higher maintenance costs
Inconsistent performance when not properly optimized

Pros
Fault-tolerant
Transparent and secure
Promotes resource sharing
Extremely scalable

Cons
More difficult to deploy
Higher maintenance costs

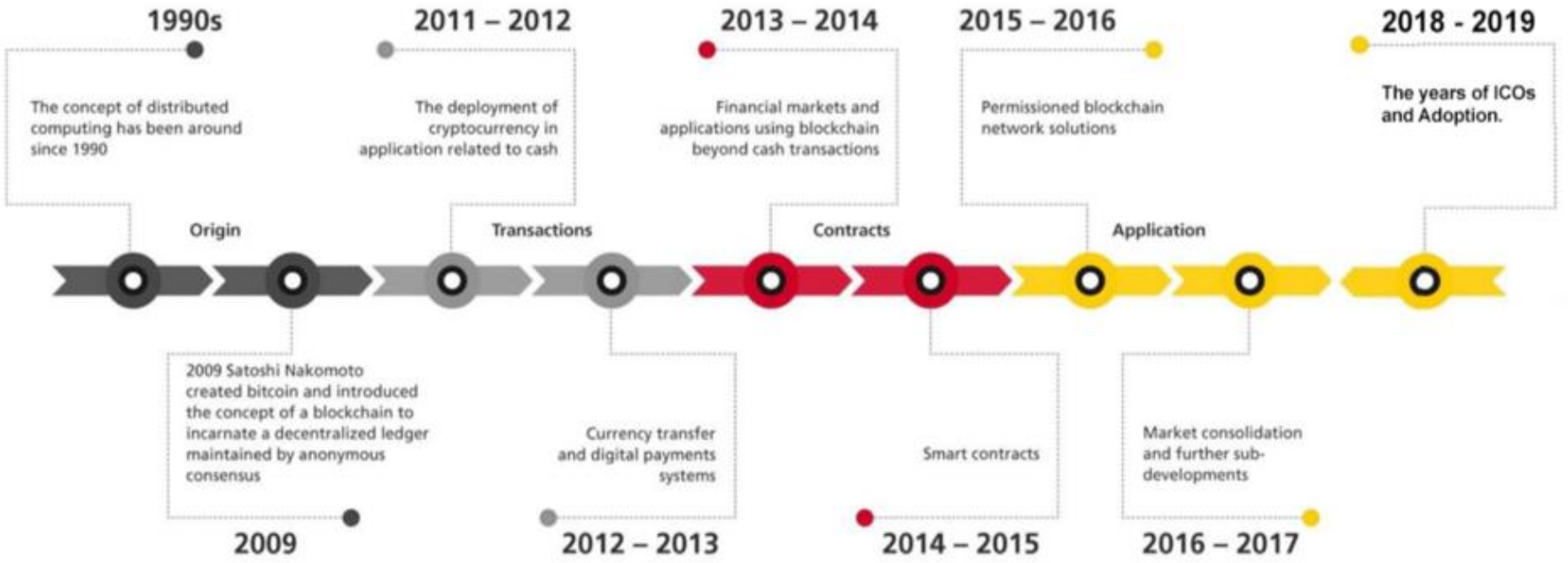
Crypto Nonce and Timestamp

- A **nonce** is an arbitrary number that can be used just once. It is often a random / pseudo random number issued in protocol messages to avoid replay attacks

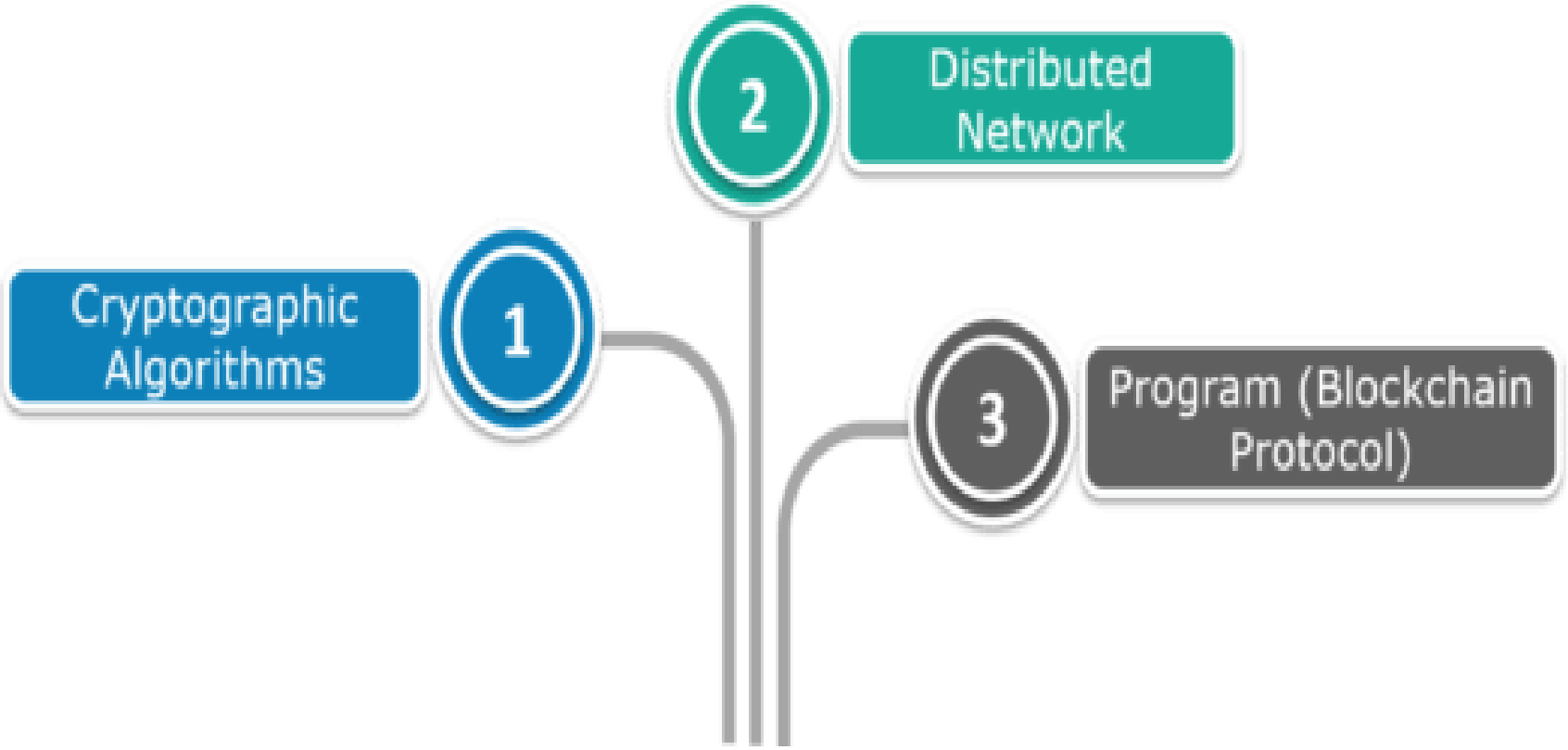
- A **Timestamp** is the time at which an event is recorded by a computer, it helps to prevent replay attacks

BLOCKCHAIN TECHNOLOGY

BLOCKCHAIN HISTORY



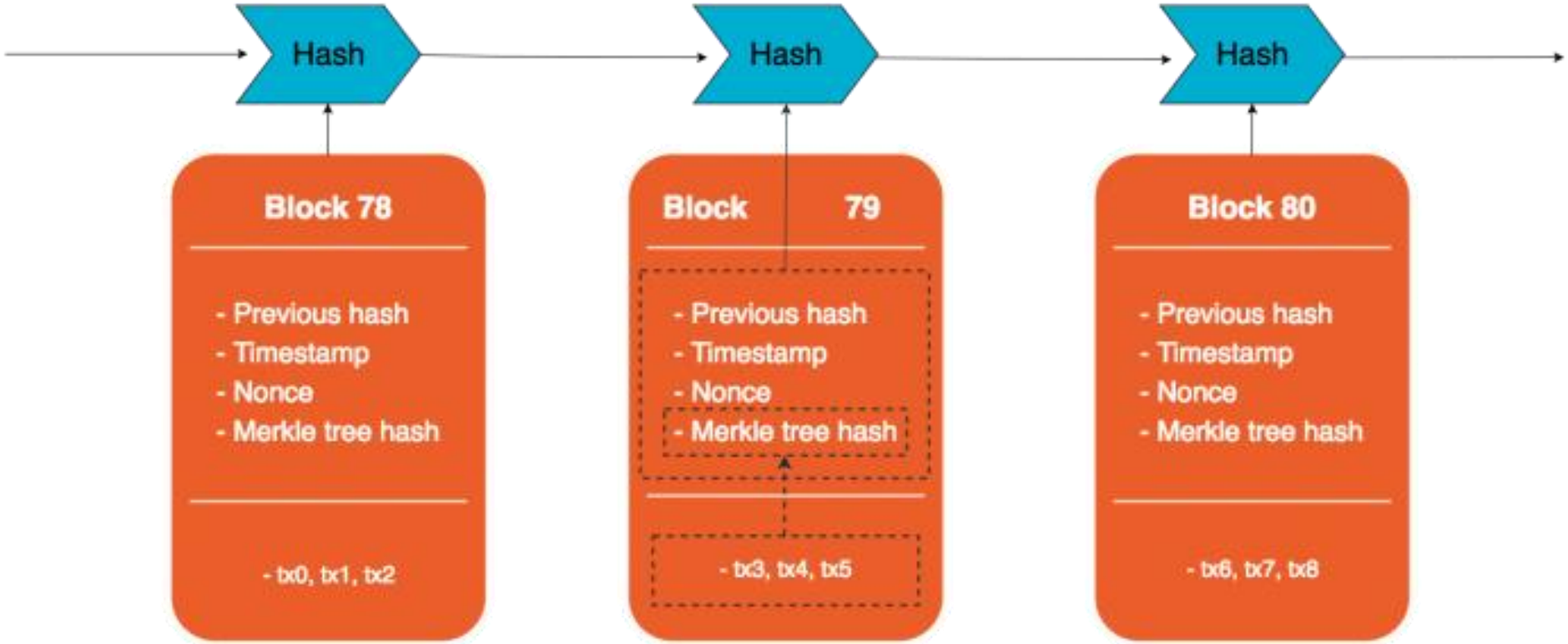
Blockchain Technology



Blockchain and use of technologies?

Initiating and Broadcasting of transactions	• Digital Signatures • Public / Private keys
Validation of Transactions	• Proof of Work or its derivatives • Other mechanisms
Chaining Blocks	• Hash function • Merkle tree

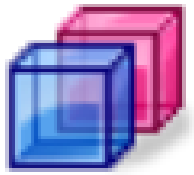
Glimpse of Blocks



What is a Blockchain?

- A blockchain is a continuously growing list of records, called blocks
- Blocks are linked and secured
- Block typically contains
  - a hash pointer as a link to a previous block
  - a timestamp and
  - transaction data
- Inherently resistant to modification of the data by design
- It can serve as an open, distributed ledger that can record transactions between two parties in a verifiable and permanent way
- As a distributed ledger it is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.
- Once recorded, the data in any given block cannot be altered without the alteration of all subsequent blocks

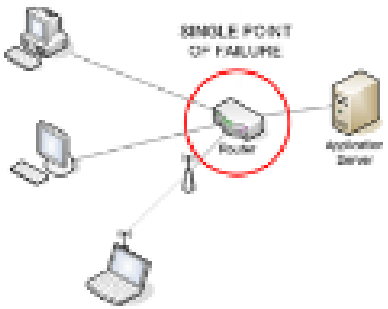
Blockchain benefits



Transparency

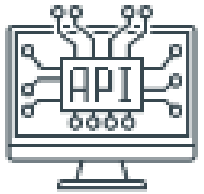
Timestamped

Immutable



No Single Point of Failure

Irrevokable



Programmable

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

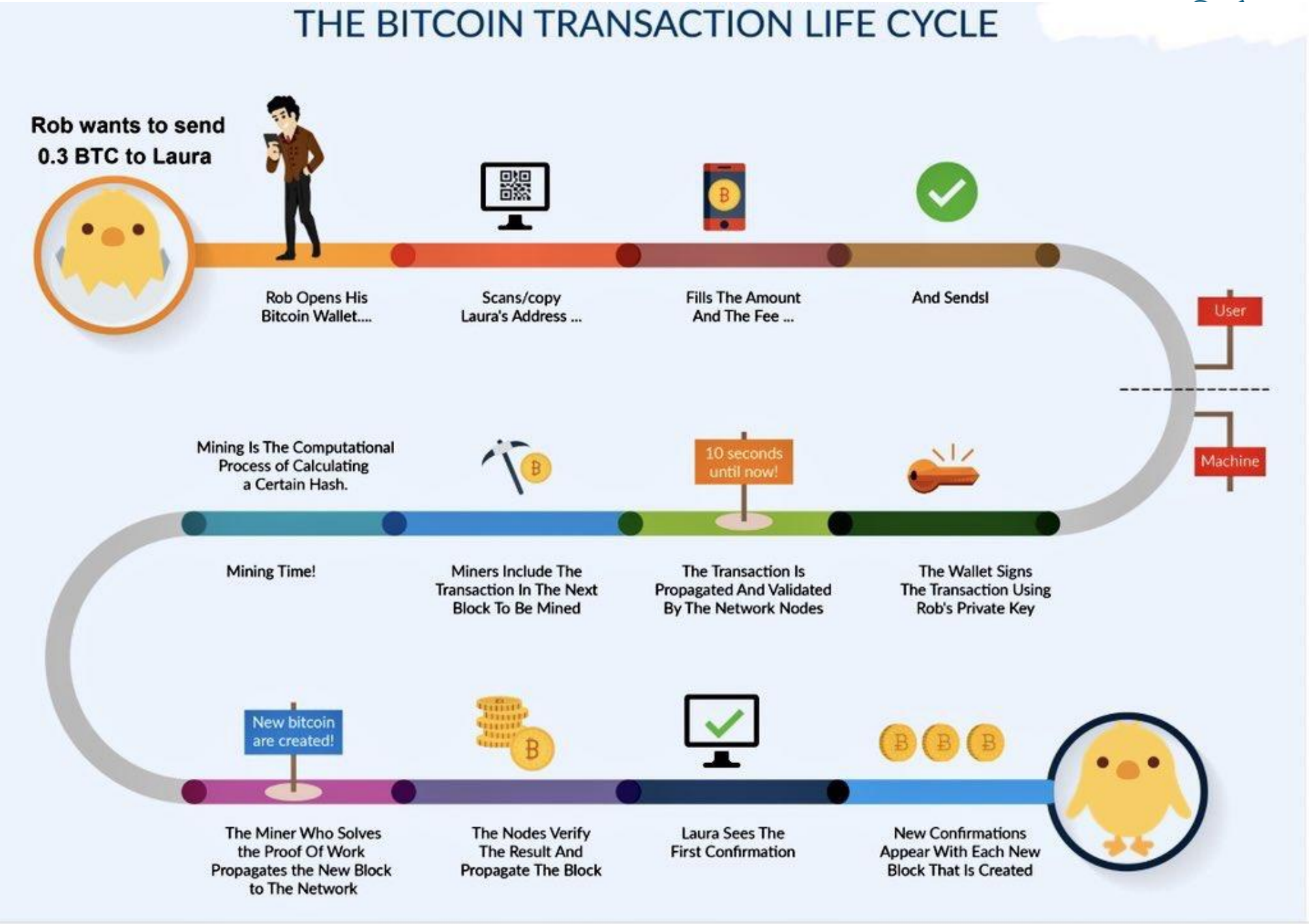
What is Bitcoin?

- Bitcoin is a completely decentralized, peer-to-peer, permissionless cryptocurrency put forth is 2009
  - No central party for ordering or recording anything
  - Software that runs on machines of all stakeholders to form the system
  - **No identity**; no need to signup anywhere to use; no access control - anyone can participate in any role

Peer Addresses (Ref: Bitcoin)

- For Bitcoin, the transactions are pseudo-anonymous
  - Transactions are sent to public key addresses, - cryptographically generated addresses, computed by the wallet applications
- Address in bitcoin is synonymous to an “Account” in a bank
- The wallet listens for transactions addressed to an account
  - Encrypts the transactions by the public key of the target address
  - Only the target code can decrypt the transaction and accept it
- However the actual transaction amount is open to all for validation

THE BITCOIN TRANSACTION LIFE CYCLE



Source: https://twitter.com/btc/status/1009159861379260416

The Bitcoin Transaction Life Cycle - The Network

Step 1) The wallet constructs the transactions, sign using senders private key, broadcasts it to the network

Step 2) The network nodes validate the transactions based on the existing Blockchain, and propagate the transaction to the miners

Step 3) The **miners include the transaction** to the next block to be mined

The Bitcoin Transaction Life Cycle - The Miners

Step 1) The miners collect all the transactions for a time duration, say for 5 mins

Step 2) Miners construct a new block and tries to connect it with the existing blockchain, through a cryptographic hash computation - The mining Procedure

Step 3) Once the mining is over and the hash is obtained, the block is included in the existing blockchain - The updated blockchain is propagated in the network

The Bitcoin Transaction Life Cycle - The Receiver

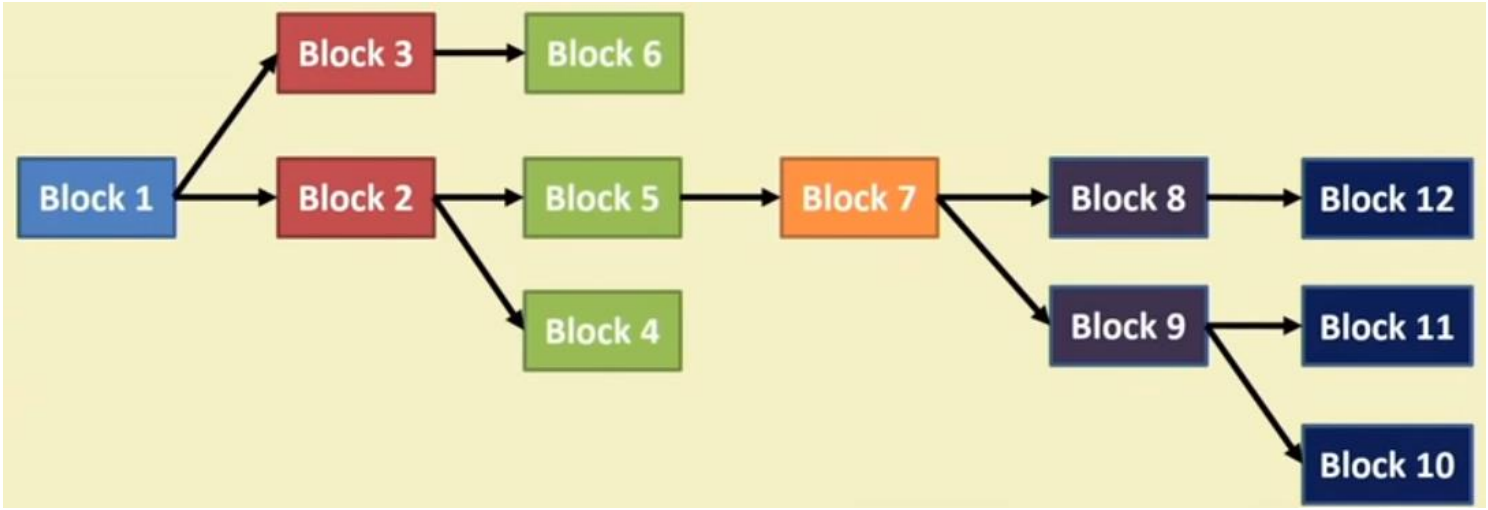
Step 1) Sender opens his Bitcoin Wallet and refreshes, the Blockchain gets updated

Step 2)The transaction reflects at Senders wallet

Challenge-Response to Permission-less Consensus

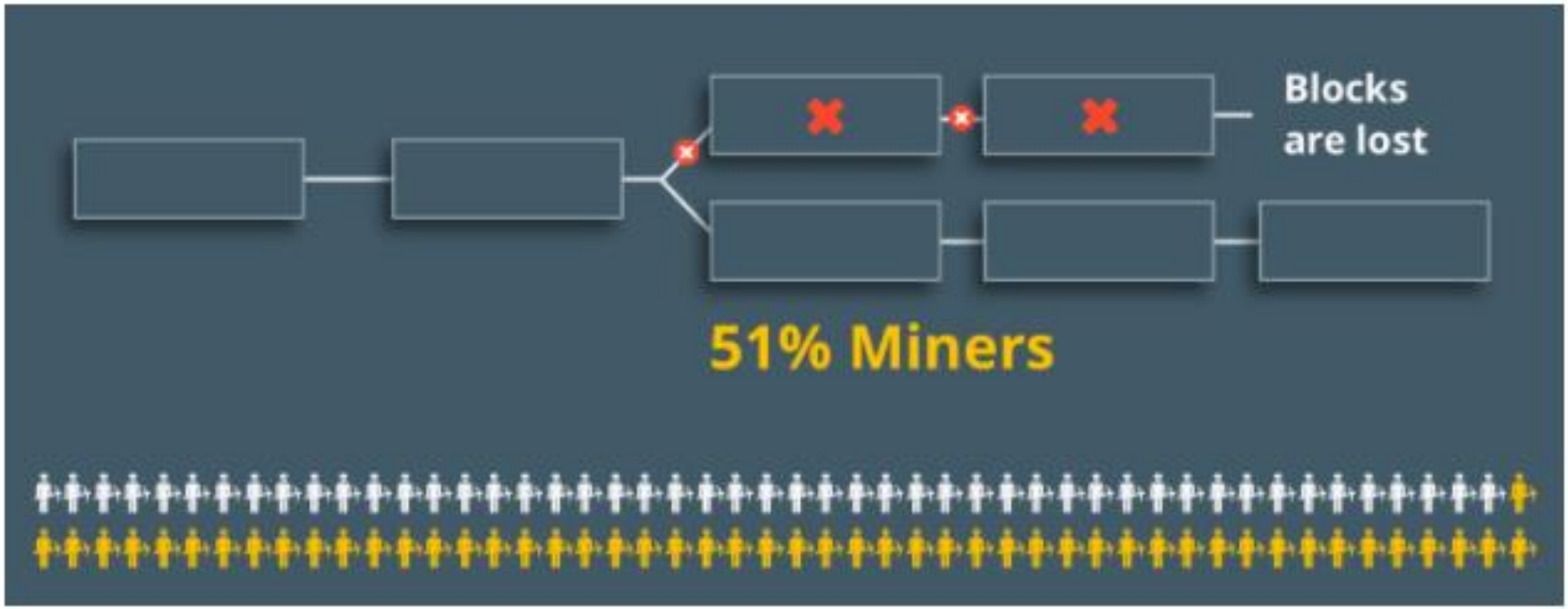
- The Challenge-response protocol: The nodes in the network tries to solve the challenge posed by the network
  - The nodes or the participants do not need to reveal their identity
- The node that is able to solve the challenge first, would get to dictate what the next set of data or state elements to be added should be
- This will continue iteratively at different rounds
- Bitcoin - PoW - Works on Challenge-Response
  - To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync.

Blockchain (at Permission-less Model) as a Tree



- Fork – Which one to accept?
  - accepting the chain with the most proof-of-work
- 51% attack and the double spend
- Finality?
  - *how long one has to wait to be given a reasonable guarantee the transaction written in blockchain is irreversible*

51% attack



Source: https://thebitcoin.pub/t/proof-of-work-pow-explained/24952

Demo

- https://blockchaindemo.io/

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 Blockchain

- Can realize various benefits like
  - Strict notion of security and privacy
  - Greater transactional throughput based on the traditional notions of distributed consensus
    - Raft Consensus
    - Paxos Consensus
    - Byzantine Fault Tolerance (BFT) algorithms
  - Finality can be reached immediately

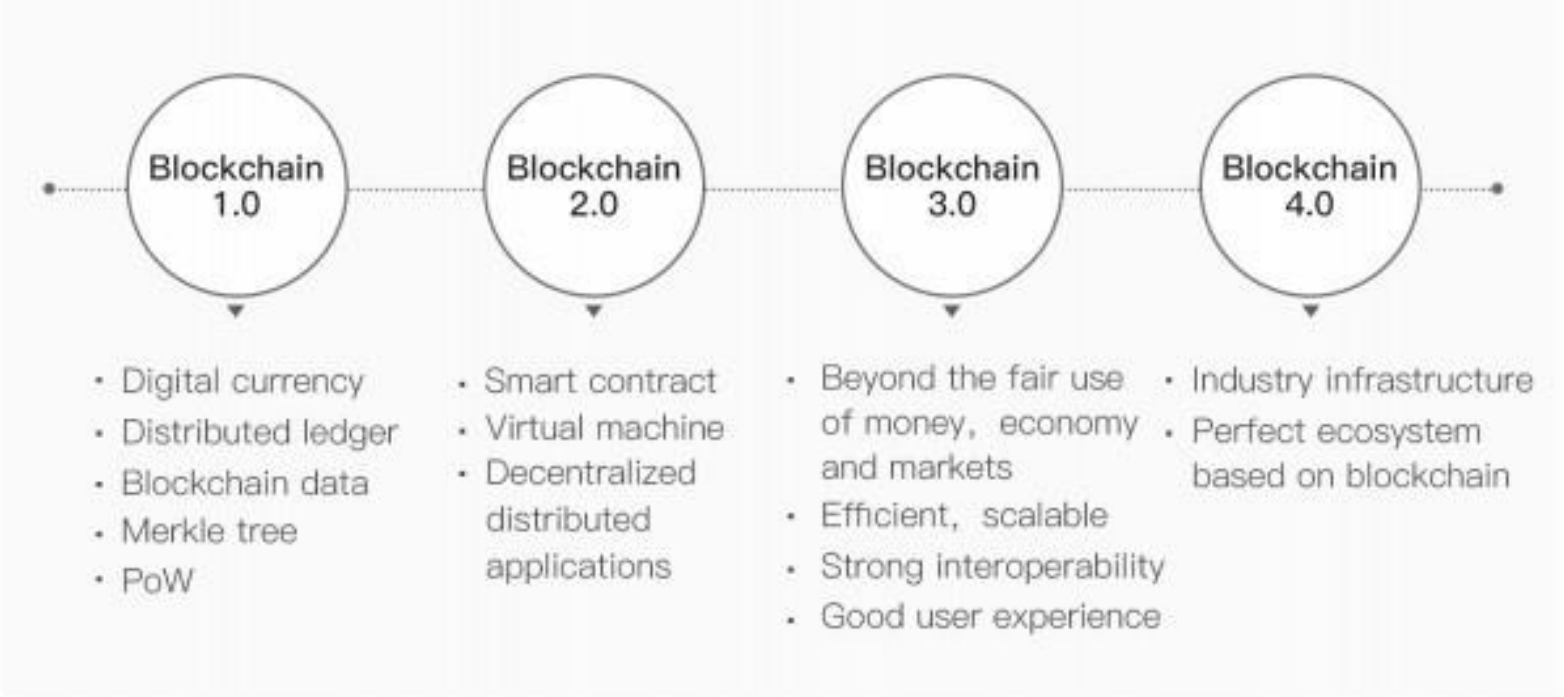
Permissioned Model

- 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

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

Evolution of Blockchain



CHOOSING AN USE CASE

Auditing and Compliance

- Put the date in Blockchain
  - Collects transaction records from diverse set of divisions
  - No one can tamper the date, but everyone can verify
- Blockchain is append-only
  - Once a transaction has been recorded, it cannot be removed without changing the view of others
- Blockchain has multiple advantages
  - Reduces the cost of auditing - you do not need to talk individually to every division
  - Auditors have global view of the data
  - Compliance becomes passive to active
    - Can be checked and validated immeidately when the transaction is recorded

Blockchain for voting

The Switch

West Virginians abroad in 29 countries have voted by mobile device, in the biggest blockchain-based voting test ever

Building a workable, scalable, and inclusive online voting system is now possible, thanks to blockchain technologies," writes Alex Tapscott, whom the Times describes as co-founder of the Blockchain Research Institute.

Blockchain and Perishable goods

BITCOIN (BTC), COMPANIES, CRYPTOCURRENCIES, NEWS

Bitcoin Finds its Way to Walmart Store Shelves

BY SOFIKO ABESLAMIDZE ON WEDNESDAY, SEPTEMBER 5TH, 2018 12:48PM UTC | LEAVE A COMMENT

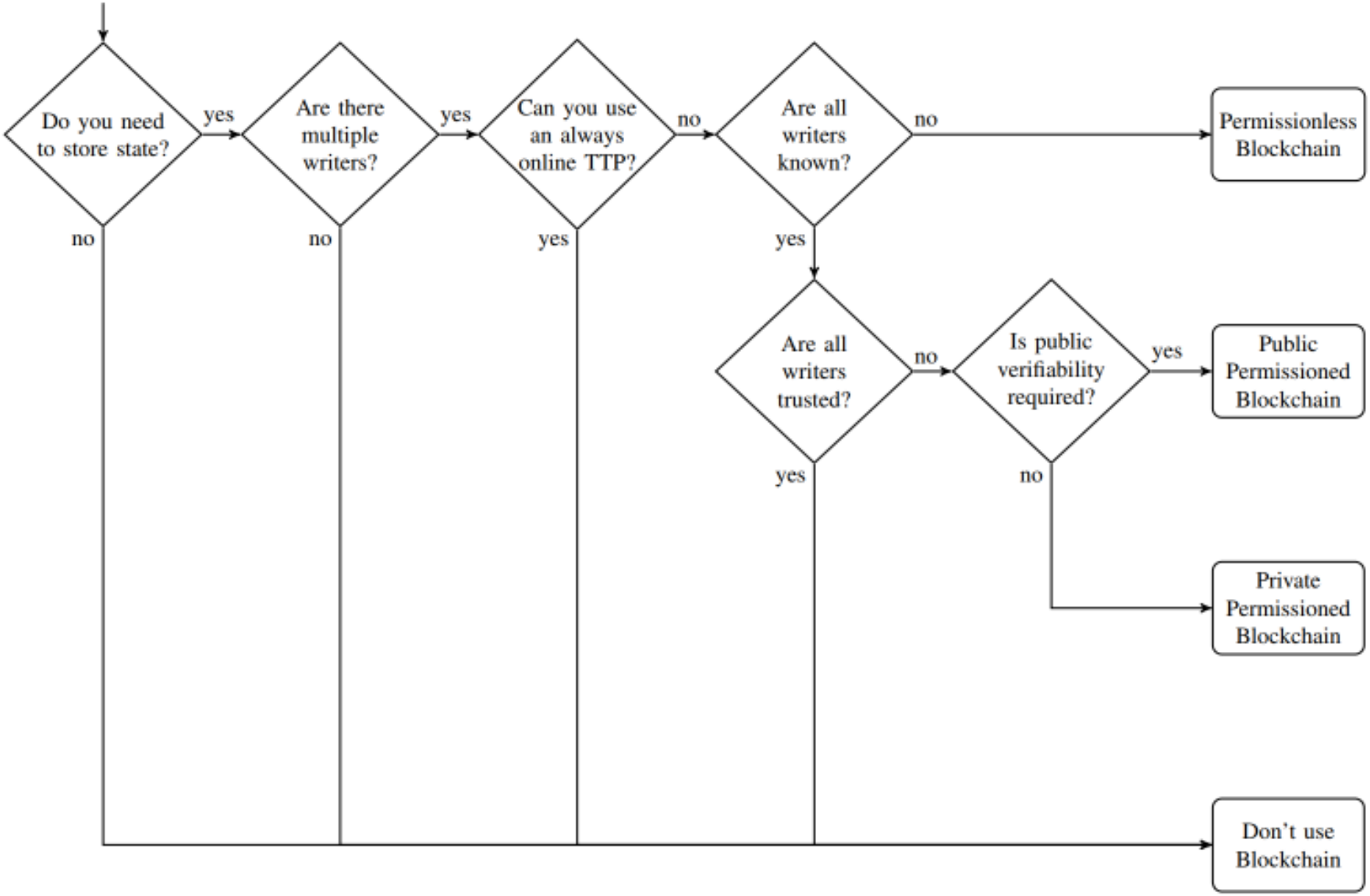
Bitcoin is entering the stores of American retail giant Walmart, but for now it is available only in the form of chocolate candy wrapped in a gold foil.

Walmart announced an initiative to improve food safety by utilizing blockchain tech to provide **better food tracking and consumer safety**. The project was launched in collaboration **with IBM and Tsinghua University.**

Five Blockchain Product Use Cases To Follow This Year - Forbes

- Streamlined supply chains
- Forming smarter predictions
- Building decentralized apps
- Simplifying the Internet of Things
- Fortifying identity management

Do you need a Blockchain?



BLOCKCHAIN AND C-DAC

C-DAC Hyd in Blockchain Technology

- MeitY funded project
- Building applications in the field of e-Governance, education domains
- Proof of Existence framework

Developed applications

- Property Management Application
  - Support from Telangana State Government
- CKYC application - ongoing
- ACTS certificates application
- PoE as a Service

Proof-of-Existence

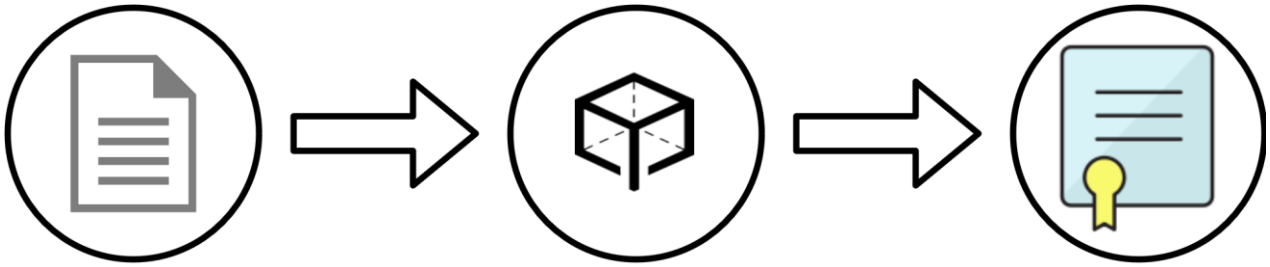
Motivation

- Number of digital artefacts are generated by ICT systems
- Fake or fabricated documents is a major issue (degree certificates, property records etc)
- Many document management systems lack
  - Transparency
  - Security
  - Efficiency
- How the problem can be solved?
  - Temporal existence
  - Verify Origin
  - Verify Content Authenticity

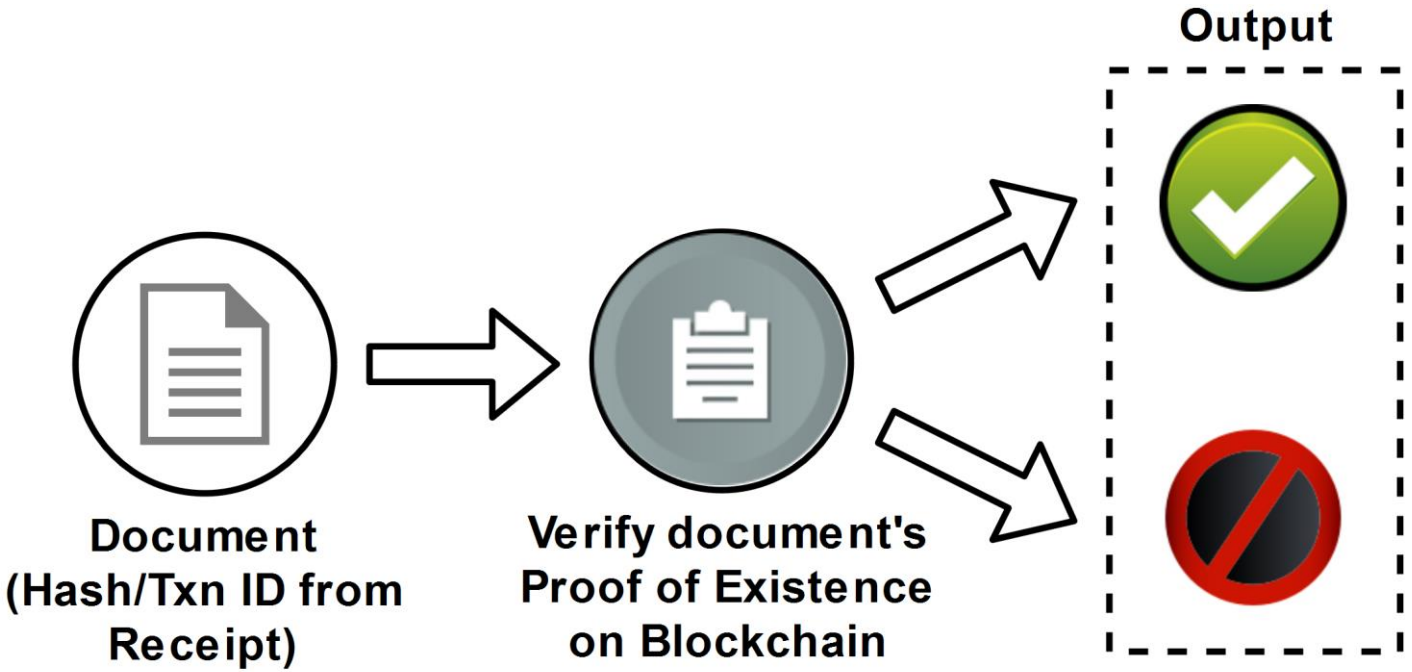
PoE

- Records the following details on Blockchain
  - hash of digital artefact
  - timestamp
- Allows verifying
  - digital artefact hash not tampered
  - digital artefact existed at a point in time when it was recorded on Blockchain

Record



Verify



PoE Benefits

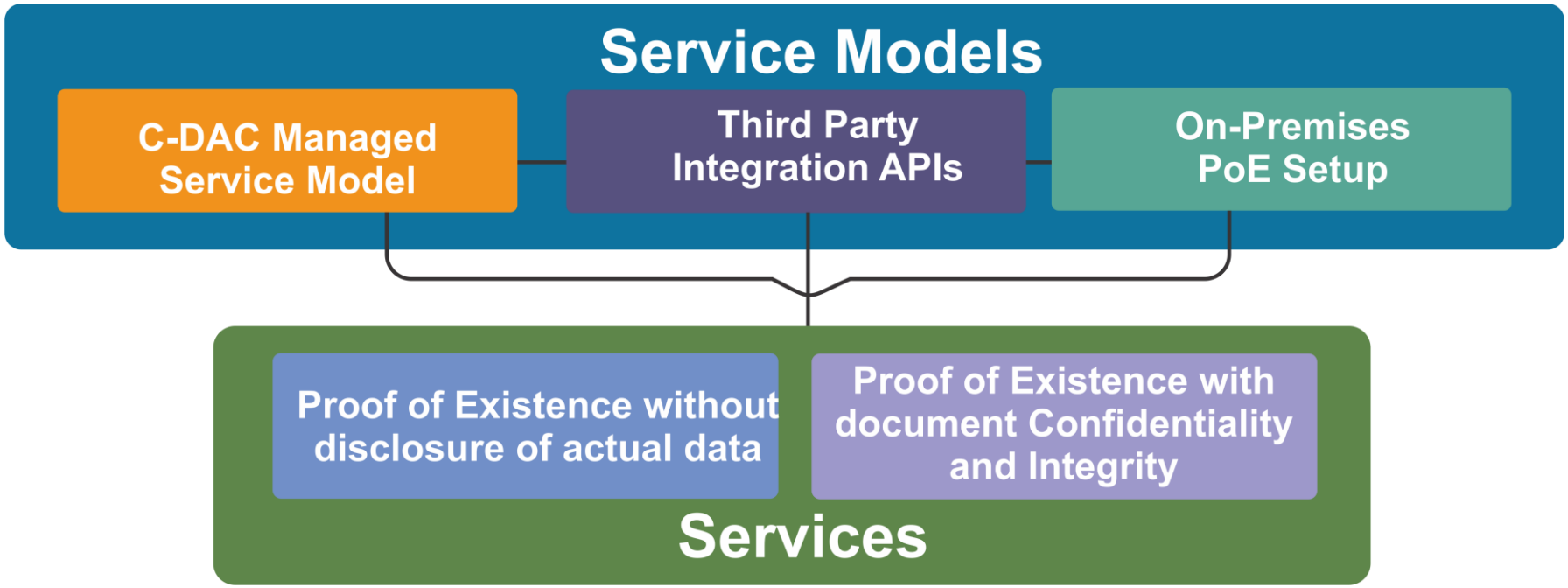
1. Proves document ownership without revealing actual data
2. Records time stamp & proves certain data exists at a certain moment of time.
3. Certify the existence of document without the need of a Central Authority
4. Ensures document Integrity
5. Ensures that timestamp and hash of the documents cannot be tampered retroactively

PoE Applications

Target Users

- e-Governance applications
- Educational Institutes / Universities
- Government Departments
- Organizations related IPR
- Citizens (personal important documents)

Service Models



References

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

gjyostna@cdac.in

THANK YOU