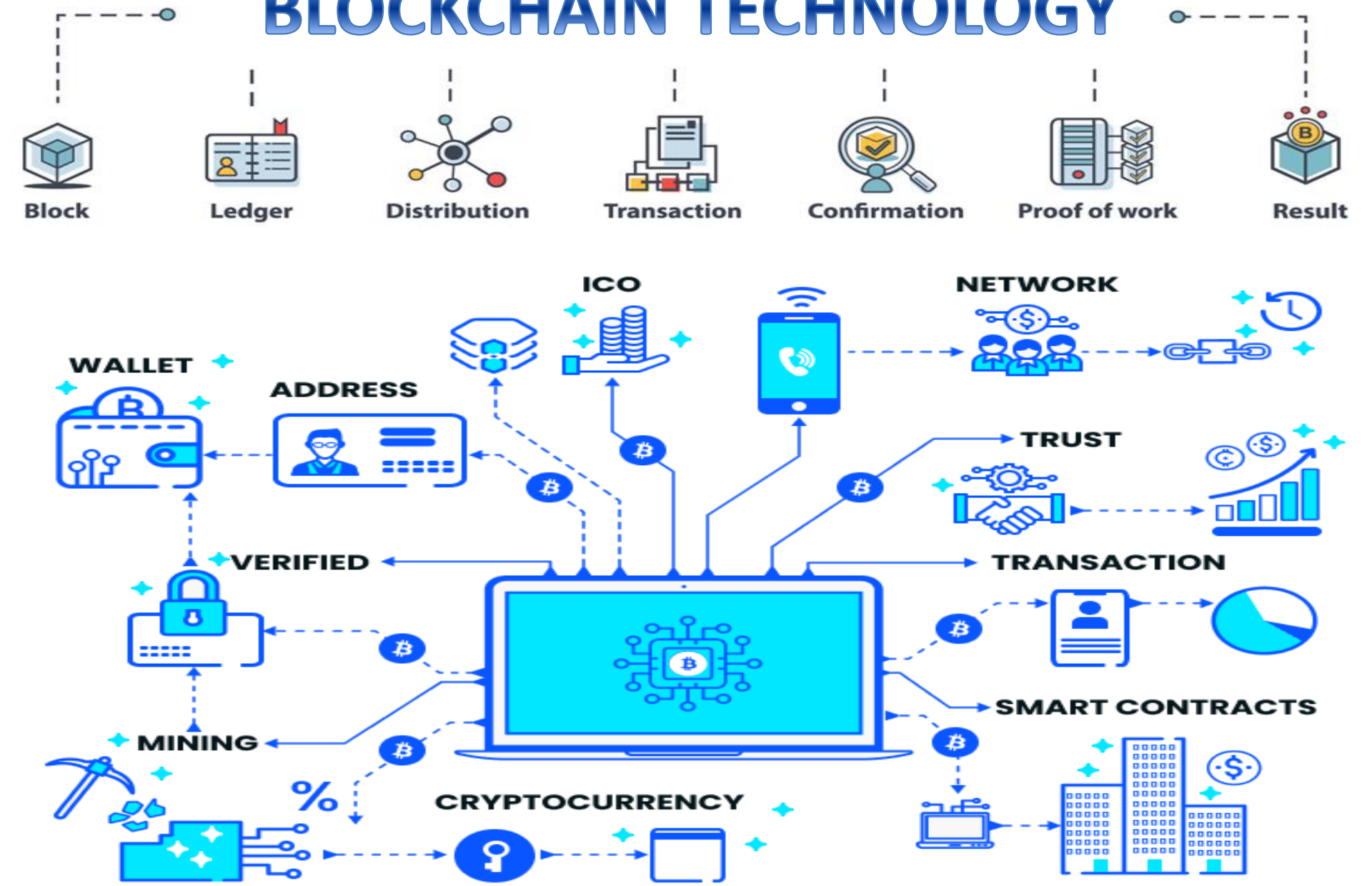
20CS4601C

BLOCKCHAIN TECHNOLOGY



Course Outcomes

- **CO1: Understand the key dimensions of Block chain Technology**
- **CO2: Apply the principles of Block chain for a given application.**
- **CO3: Apply the features of Ethereum and Hyperledger to develop various applications**
- **CO4: Analyze the given scenario and design a block chain based solution.**

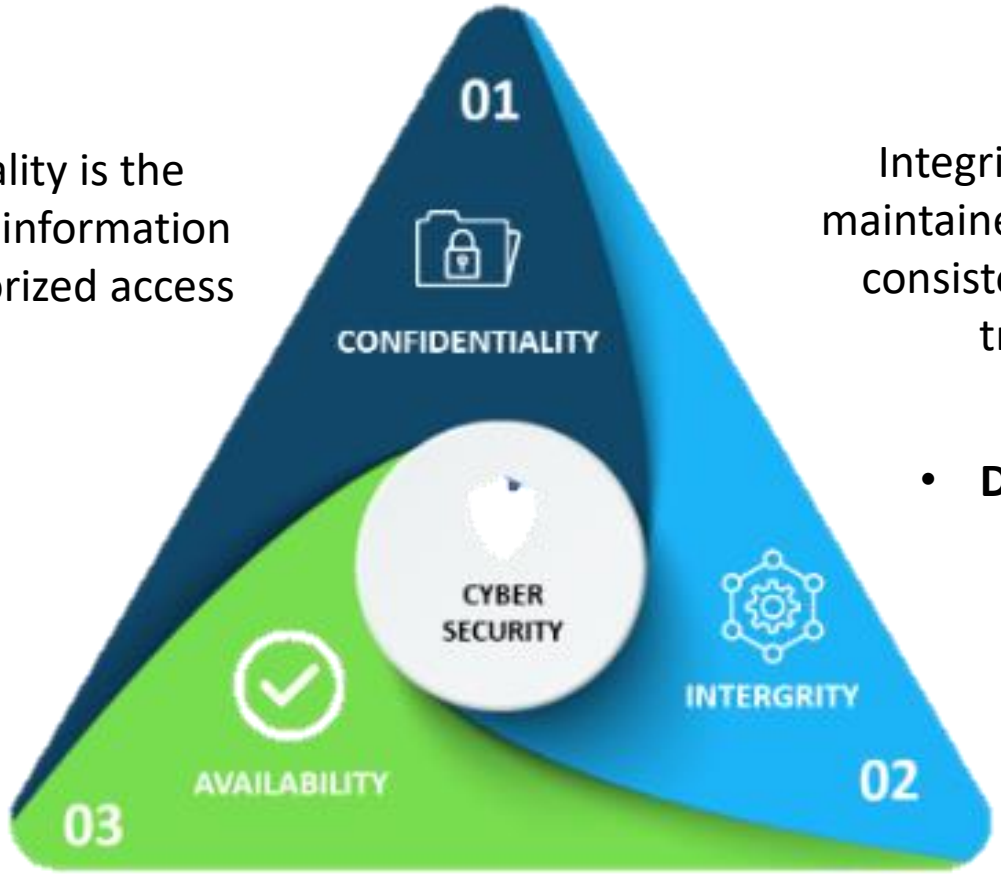
Perquisites:

Basic Concepts of Security & Distributed Computing

Security-CIA Triangle

Confidentiality is the protection of information from unauthorized access

- **Encryption**



Integrity of your data is maintained only if the data is consistent, accurate, and trustworthy.

- **Digital Signature (Hashing)**

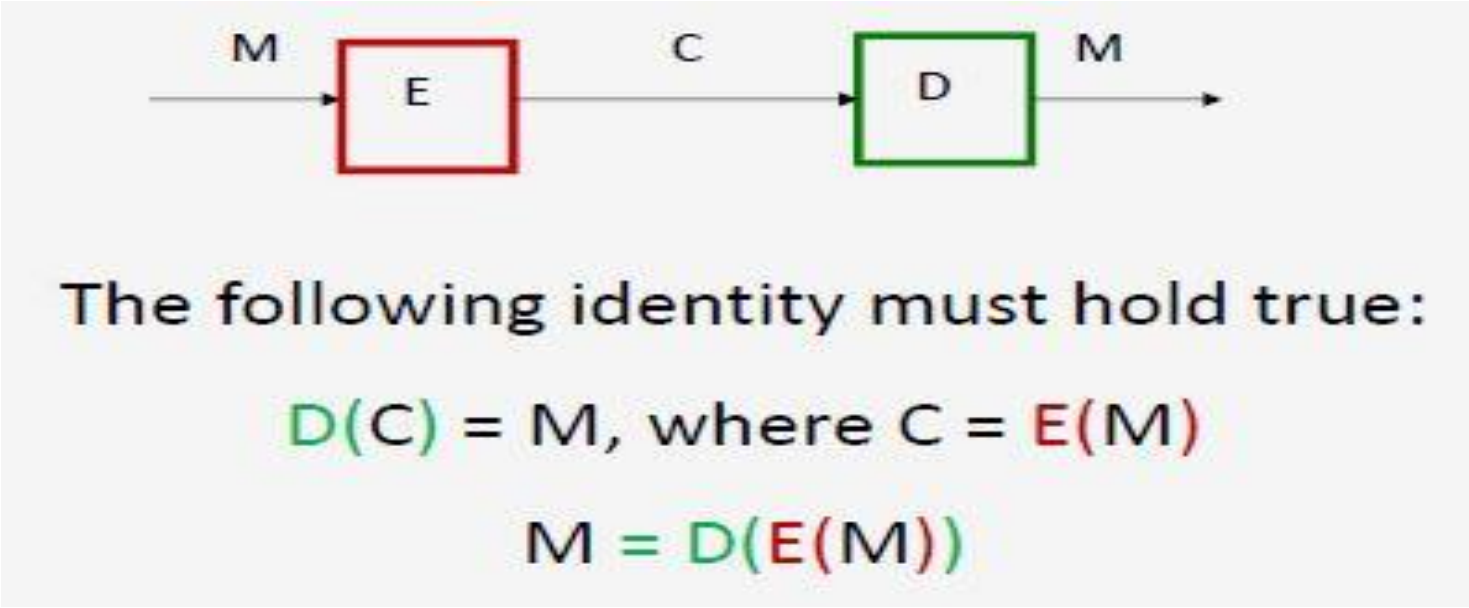
Availability means information should be readily accessible for authorized parties.

Confidentiality

- Basic Terminology

Plaintext (or clear text)	:	The message.
Encryption (encipher)	:	Encoding of message.
Ciphertext	:	Encrypted message.
Decryption (decipher)	:	Decoding of ciphertext

- **Encryption / Decryption Model**



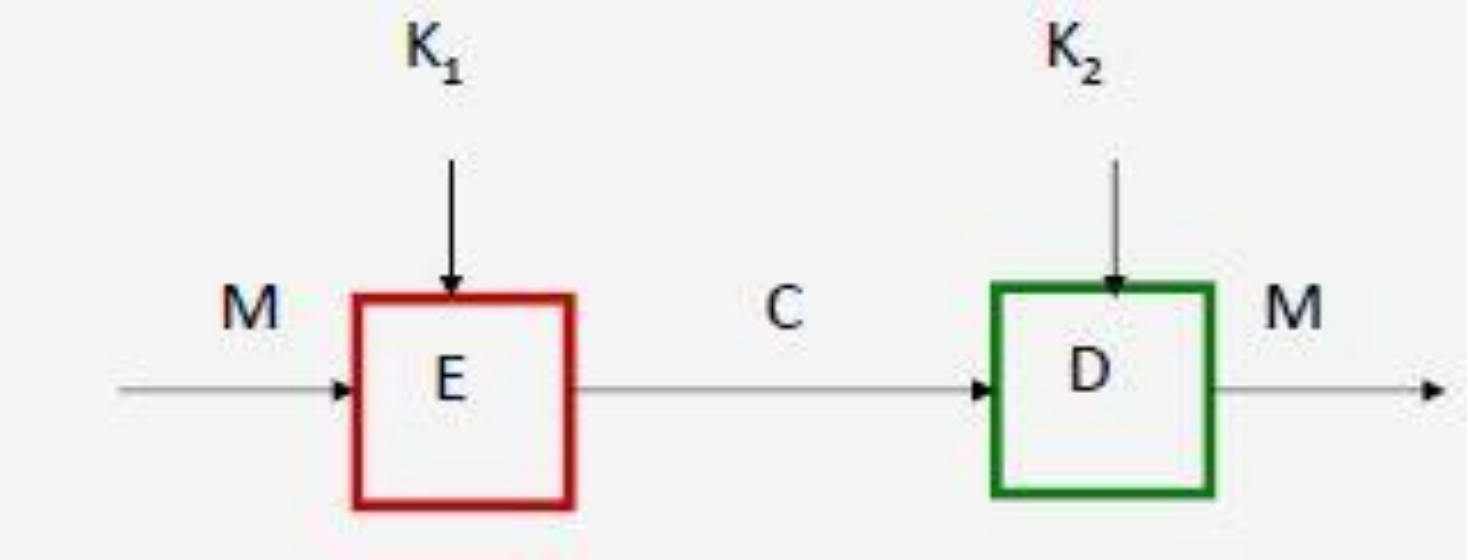
Key Based Encryption/Decryption

- **Symmetric Case**

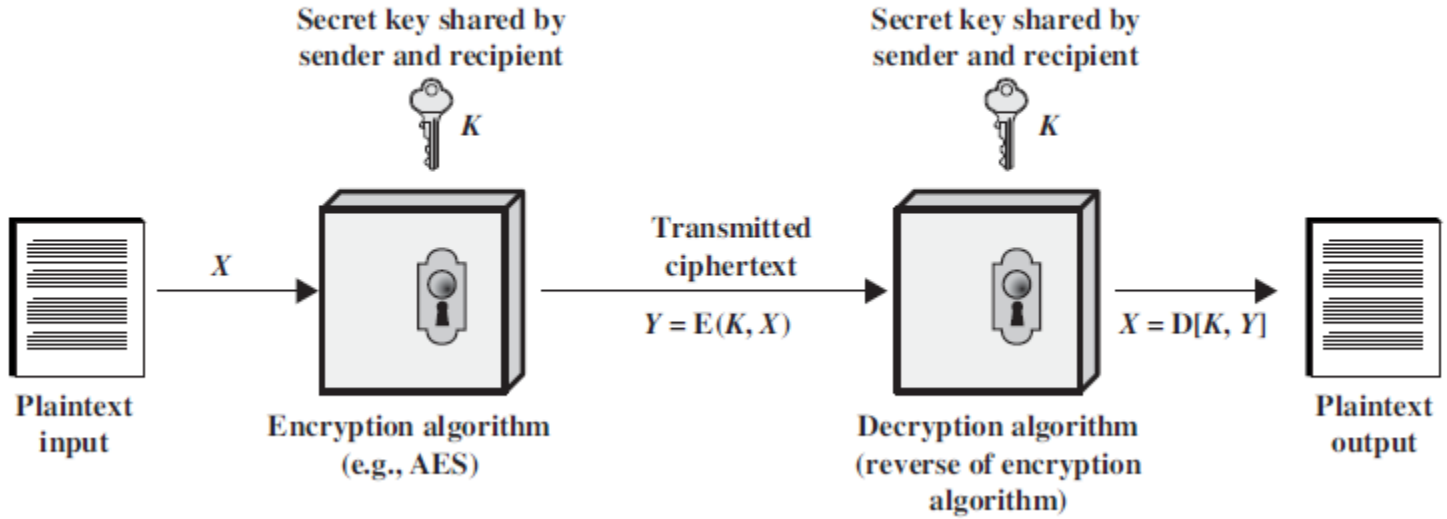
Both keys are the same or derivable from each other. K1 = K2.

- **Asymmetric Case**

keys are different and not derivable from each other. K1 != K2



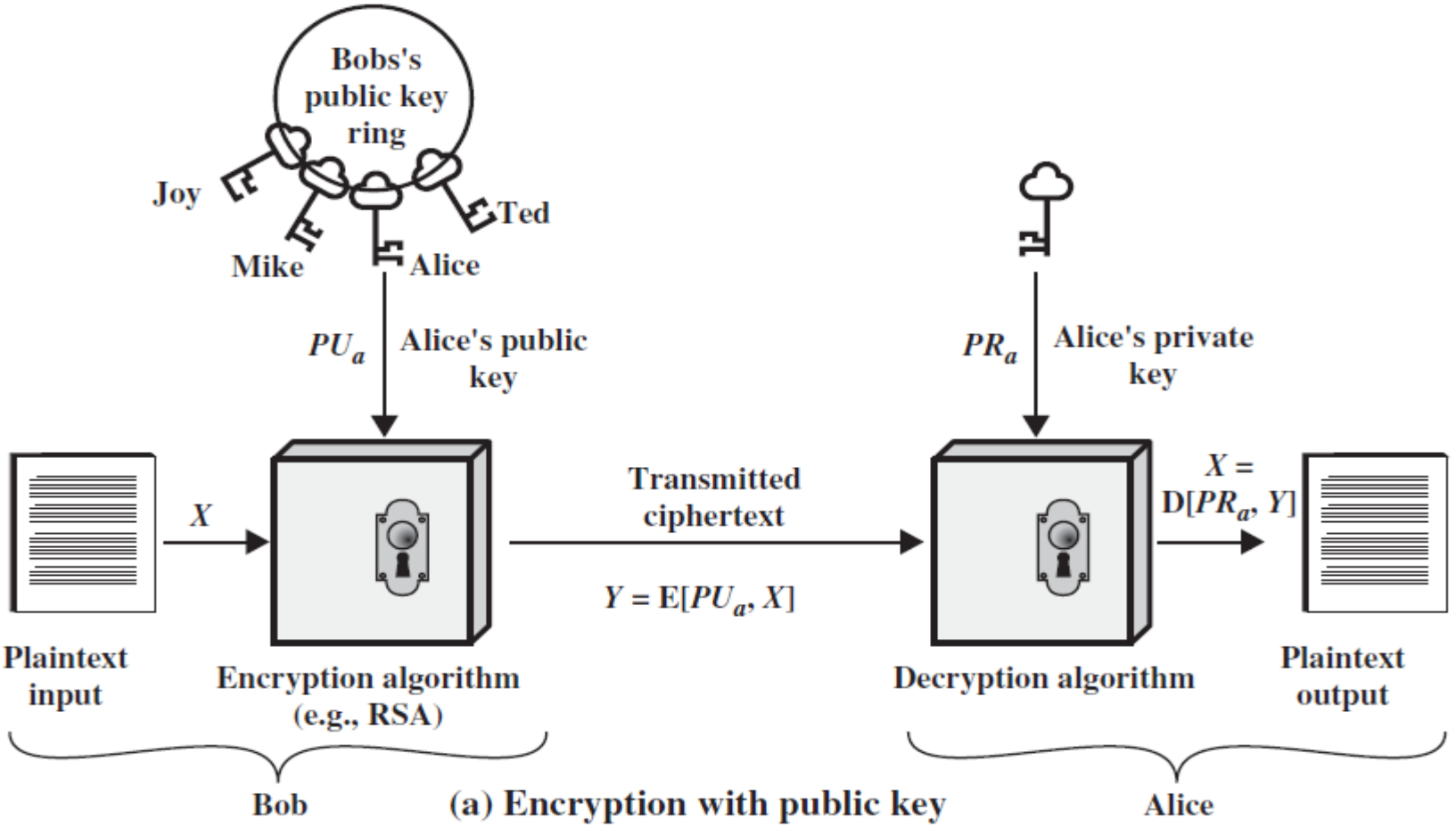
Symmetric Mechanism



- Substitution Mechanism
- Transposition Mechanism
- Steganography
- Rotor Mechanisms
  - DES, AES

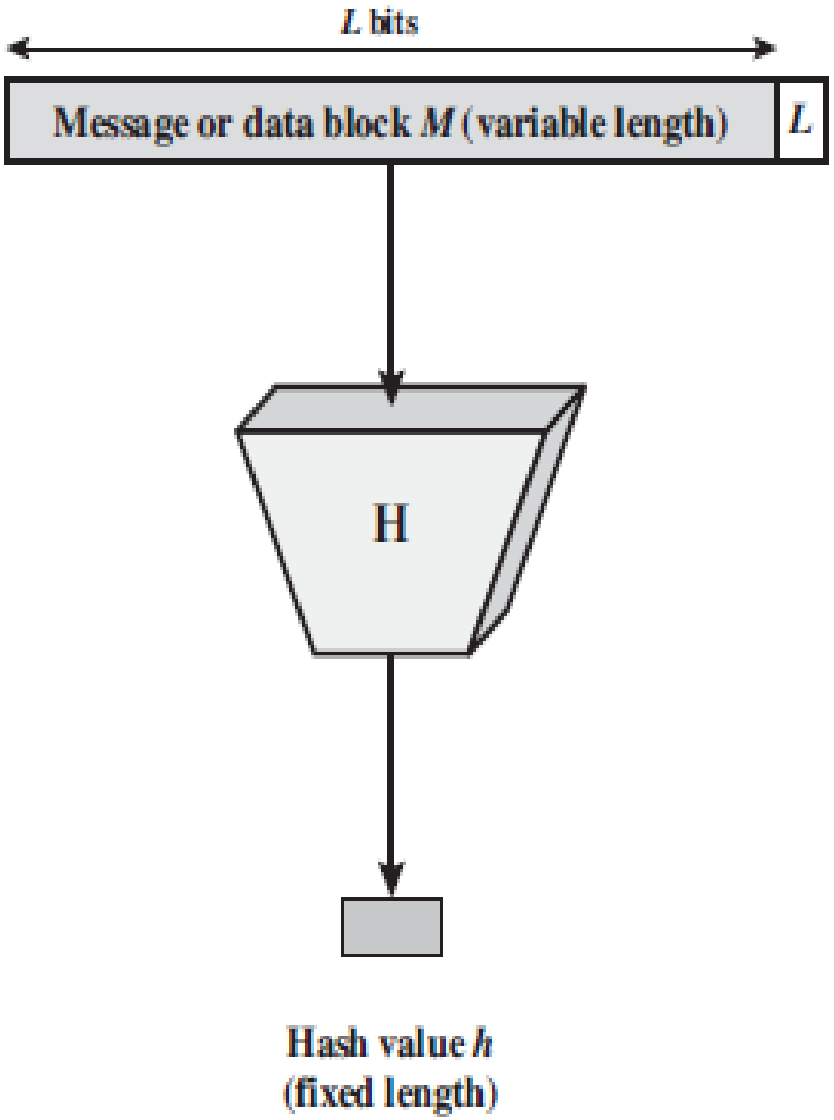
Asymmetric Mechanism

- Public Key
- Private Key

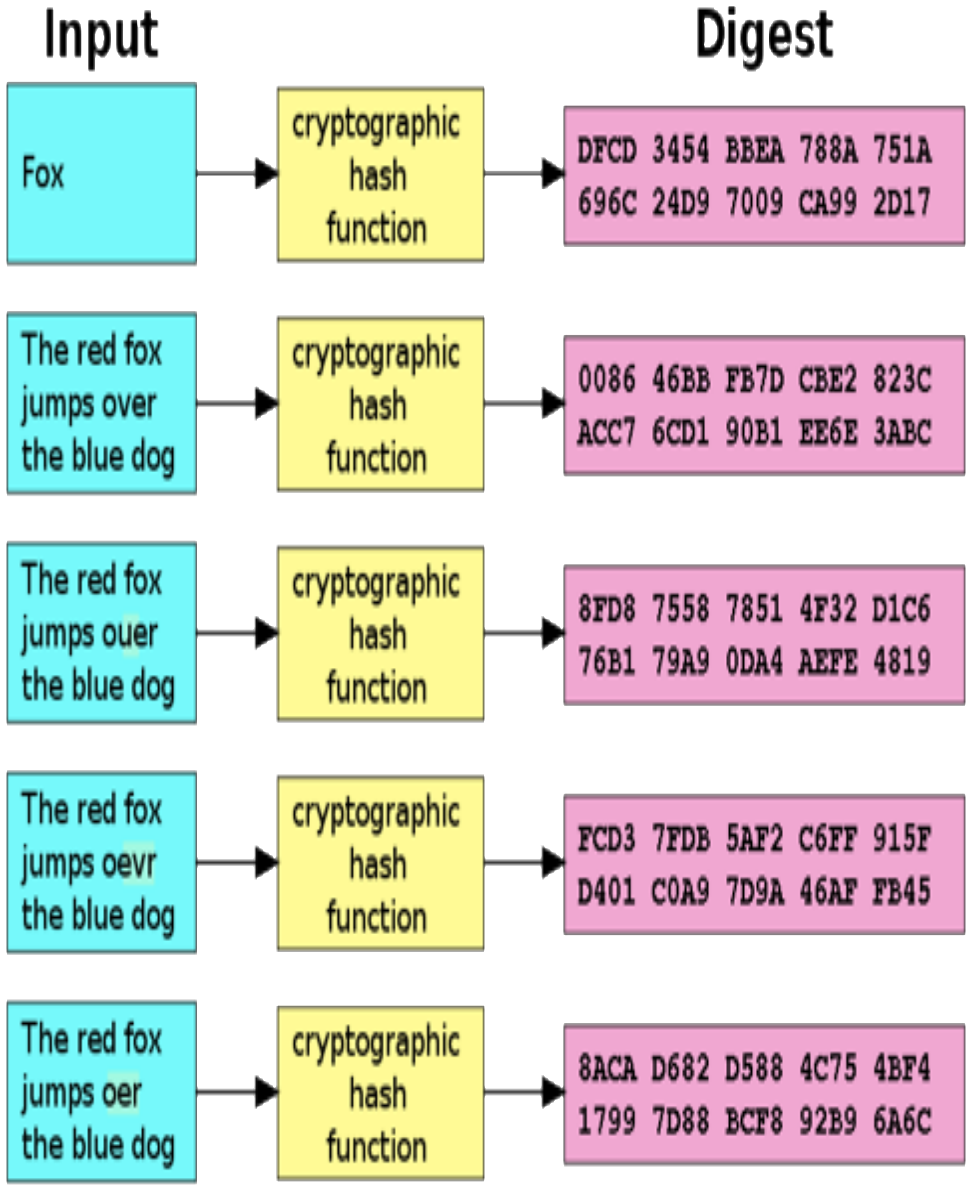


Integrity

- Achieved through Hashing Mechanism
- A **hash function** H accepts a variable-length block of data 'M' as input and produces a fixed-size hash value h=H(M).
- Easy to compute
- Almost impossible to reverse-No deterministic algorithm can find
- Used as Digital Signature



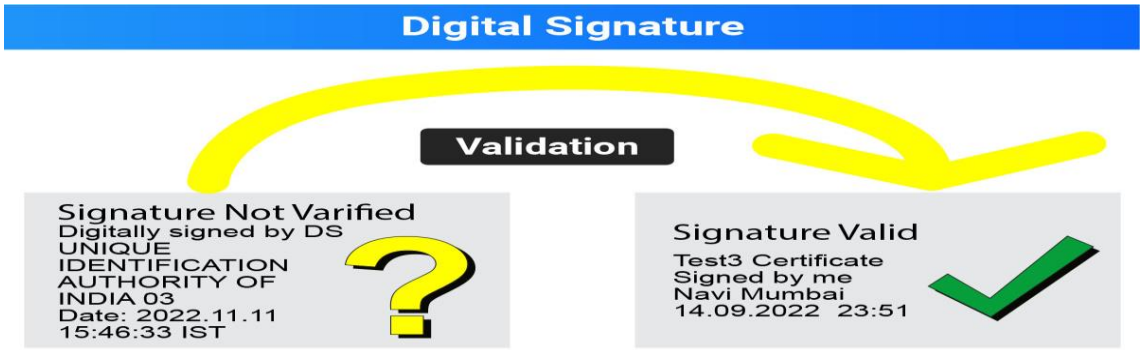
- Hashing Techniques
  - Message Digest (MD5)
  - Secure Hash Algorithm (SHA256)



https://emn178.github.io/online-tools/sha256.html

Digital Signature

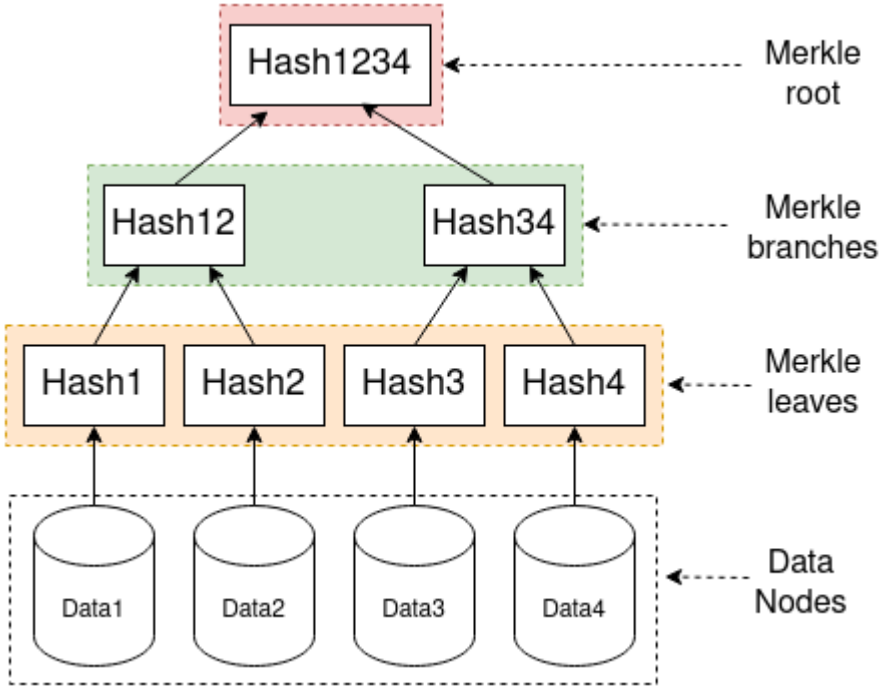
- A digital code, which can be included with an electronically transmitted document to verify
  - The content of the document is authenticated
  - The identity of the sender
  - Prevent non-repudiation – sender will not be able to deny about the origin of the document
- Only the signing authority can sign a document, but everyone can verify the signature
- A small change in the data results in a significant change in the output – called the **avalanche effect**(Butterfly Effect)
- Signature is associated with the particular document
- Signature of one document cannot be transferred to another document
- Use Hashing Algorithms (Mostly Certificate Authorities-ex:eMudra)



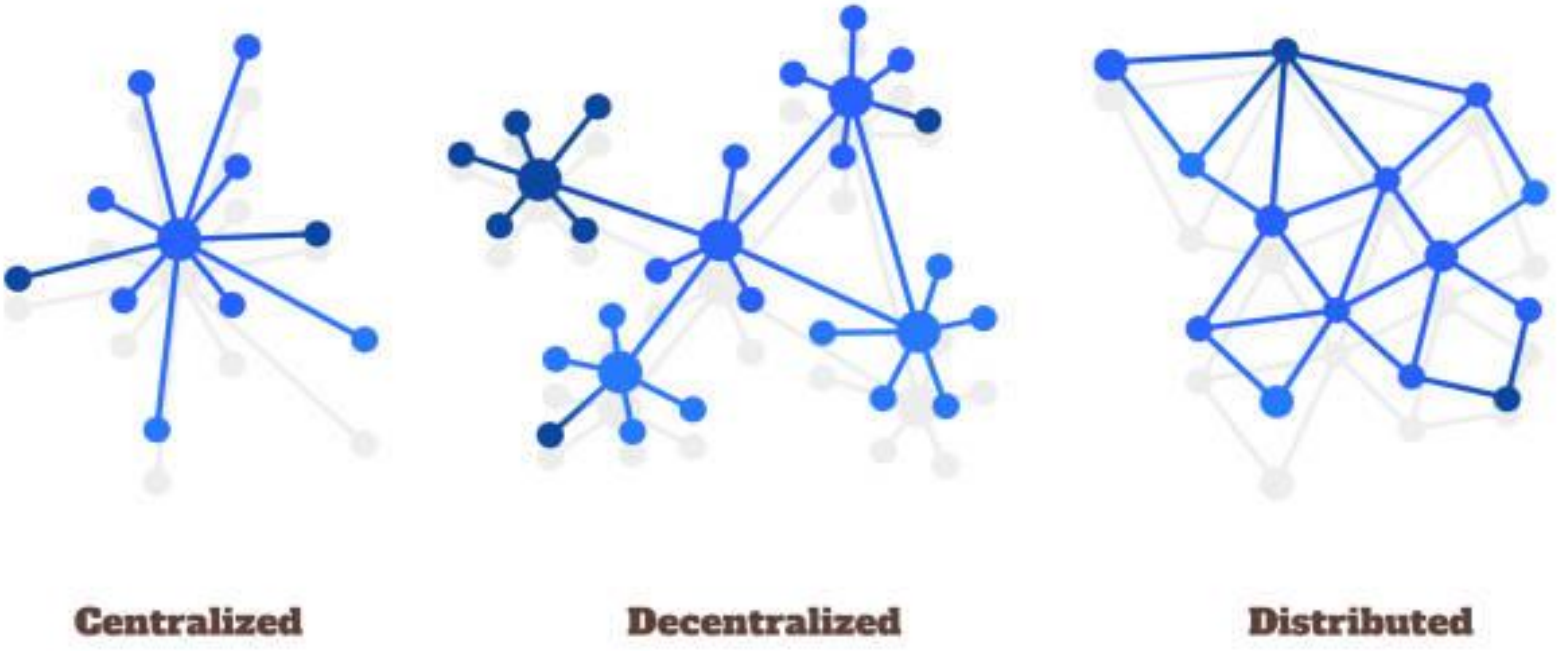
Merkle Trees (Ralph Merkle, 1979)

- Also known as **hash tree**
  - ***every leaf node*** is labelled with the hash of a data block
  - ***every non-leaf node*** is labelled with the cryptographic hash of the labels of its child nodes
- Bayer, Harber and Stornetta used Merkle Tree in 1992 for timestamping and verifying a digital document - improved the efficiency by combining timestamping of several documents into one block

- Uses of Merkle Tree
  - Peer to Peer Networks: Data blocks received in undamaged and unaltered; other peers do not lie about a block
  - **Blockchain** implementation – shared information are unaltered; no one can lie about a transaction



Centralized V/s Decentralized V/s Distributed Architectures



Centralized System

- Centralized systems are conventional (client-server) IT systems in which there is a single authority that controls the system, and who is solely in charge of all operations on the system.
- All users of a centralized system are dependent on a single source of service.
- The majority of online service providers, including Google, Amazon, eBay, and Apple's App Store, use this conventional model to deliver services.

Advantages	**Disadvantages**
✓ Command chain	Not 100% Trustable
✓ Reduced Costs	Single point of Failure
✓ Consistent Output	Scalability Limitation

Decentralized System

- A decentralized system is a type of network where nodes are not dependent on a single master node; instead, control is distributed among many nodes.
- This is analogous to a model where each department in an organization is in charge of its own database server, thus taking away the power from the central server and distributing it to the sub-departments, who manage their own databases.

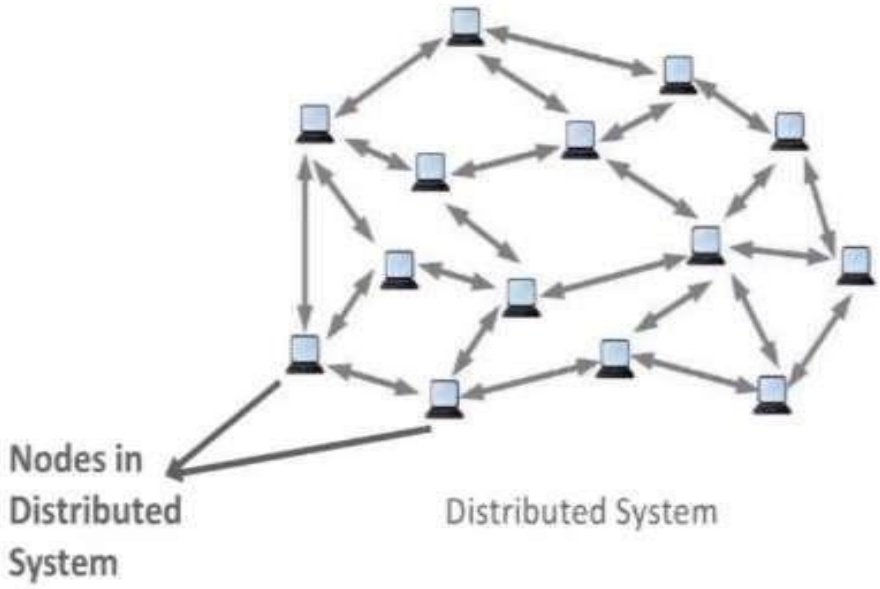
Advantages	Disadvantages
✓ Full Control	Costly
✓ Immutable Data	Misuse of Authority
✓ High Security	Volatility

Distributed Systems

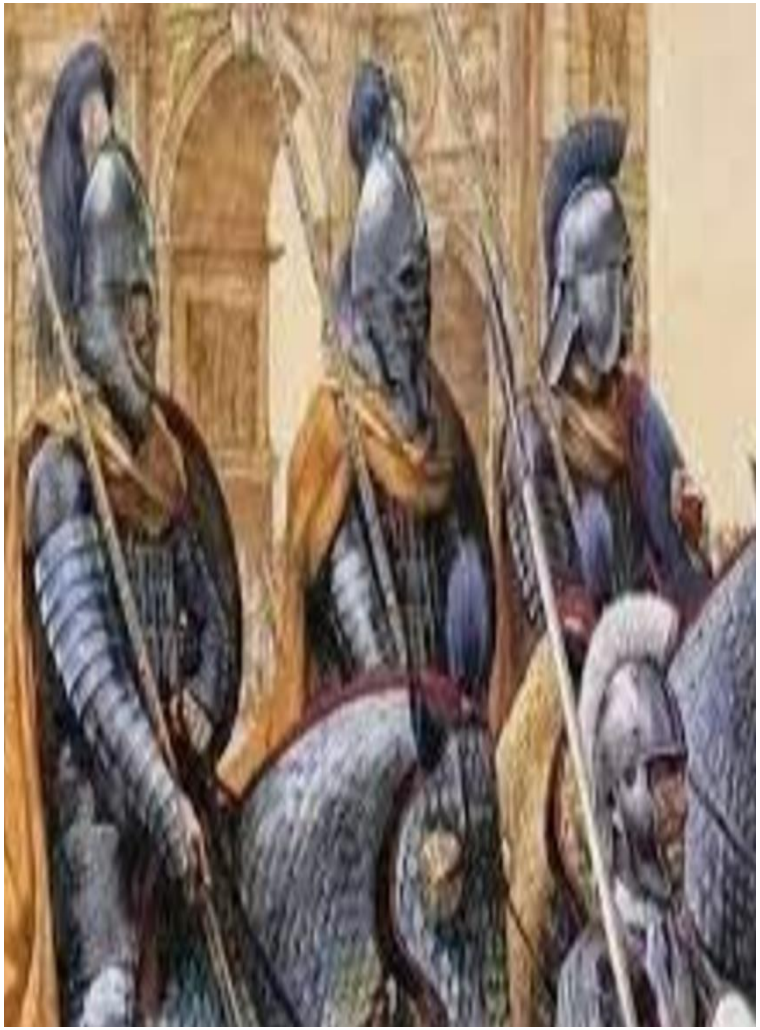
- A System where two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome
- It's modeled in such a way that end users see it as a single logical platform
- For example, Google's search engine is based on a large distributed system; however, to a user, it looks like a single, coherent platform.

Digital Ownership

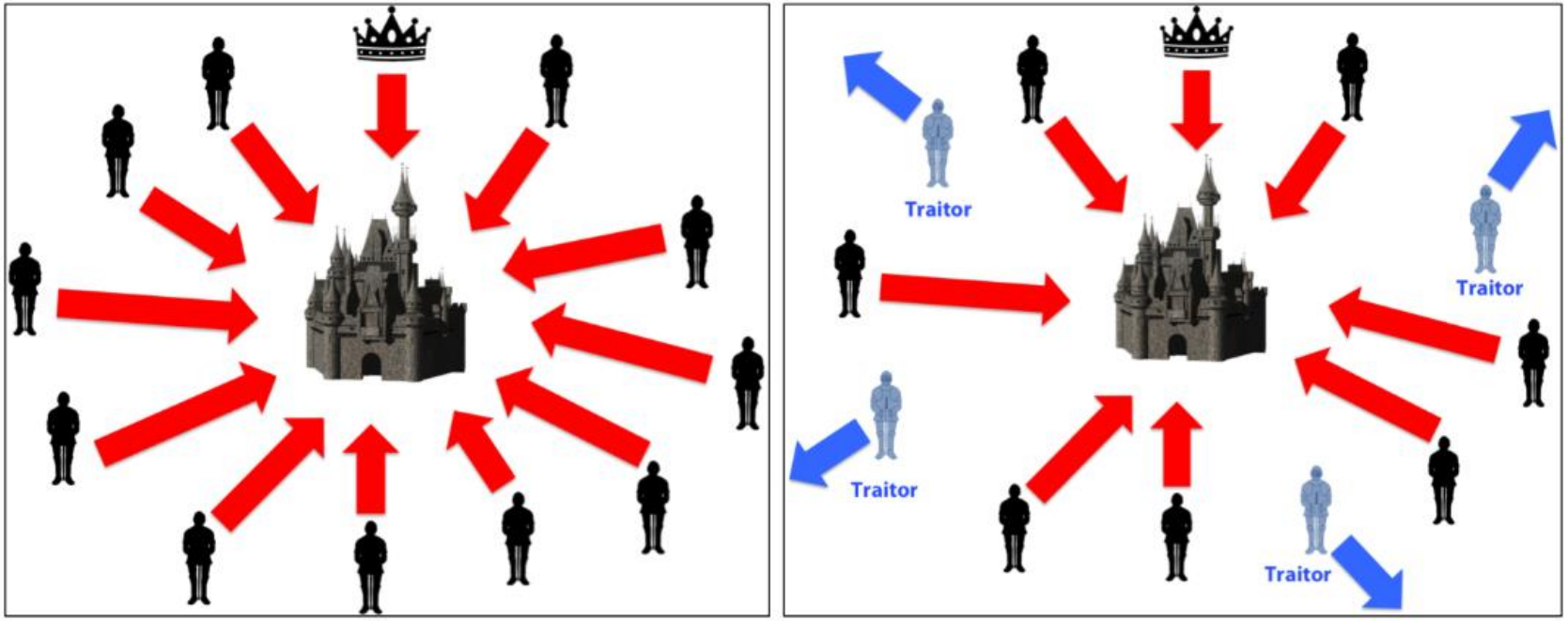
- "Digital ownership" describes the legal rights and authority a person or organization has over a digital asset or piece of property.
- Democratizing ownership could open new avenues for value production and trade in the digital economy. Blockchain technology allows people to own and control their digital assets without intermediaries



The Byzantine Generals' Problem



- A group of Generals, each commanding a portion of the Byzantine Army, encircle a City with the aim of conquering it. They must decide whether to attack or retreat.
- However, whatever they decide, the most important thing is that they all reach a consensus i.e. they all attack or they all retreat.
- The reason for this is that the City can only be taken with the full might of the collective army. If even one General decides not to attack, then there will not be enough force to overthrow the City and all attacking soldiers will die.
- Consensus however is not a simple thing to achieve, especially because within this Army, the Generals do not trust each other, just as we cannot trust each other online. A General might say they plan to attack, when in fact they plan to secretly retreat.



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

- With the Byzantine Generals, if each of their orders were recorded and shared across the army, every General would have a copy of every other General's orders, always up-to-date and 100% verified.
- i.e in distributed systems, the maintenance of the ledger takes a lot of work (as does the function of a central authority), but the difference with the distributed ledger is that it has no single person/authority responsible for this.
- Instead, incentives are given to those who choose to do the work by using one of the various consensus protocol mechanisms (proof-of-work, proof-of-stake etc). Therefore the network of individuals choosing to maintaining the network arrive at the consensus.

History & Evolution of Blockchain Technologies

Characteristics of Money

- Durability
- Portability
- Divisibility
- Uniformity
- Limited supply
- Acceptability

- Ways to create a Monitory system
  - Credit–Debt based system
  - Cash based system: External medium of exchange (ex: Gold, Silver, or banking system mode like Cash)
- Each has its merits and demerits
- Different societies use different mechanisms

Digital Credit to Digital Cash

- Cash need to be bootstrapped, but…
  - Has no risk of default
  - Credit is by its nature not anonymous , its trackable
  - Credit based system -you need to be online (checking with central authority) and need to deal with swindlers….
- Credit based system was easy to digitize- just by keeping track of who owes whom
  - 90's -> SET(Secure Electronic Transactions) Architecture
    - Ex: Credit/Debit card mechanism (buyer, seller, & intermediary)
    - Getting a Certificate from an authority was an issue

Digital Money

- 1983- cryptographer David Chaum - Proposed Blind Signatures
- Blind Signature allowed someone to sign a document and prove their ownership while at the same time hiding the information in the document.
- You can prove that you owned some money (stored at bank) by signing a transaction (credit based)
- Anonymous but still required centralization
- Commercialized as DigiCash – tried out at a bank – later went bankrupt

Double Spending Problem

- A has eCash note with serial number(Hash value) ex: 0x86A54399B01738
- A can use his eCash more than once to B & C.
- This is called 'Double Spend Problem'

Sol:

  - Use centralized source of truth
  - Buyers are anonymous, but merchants were not
  - Acted as Pseudo cash
- 5th property of money- limited in supply
- Computers can do computation work-as a backing for our currency
- This led to the idea of 'Computational Banking'

Computational Banking

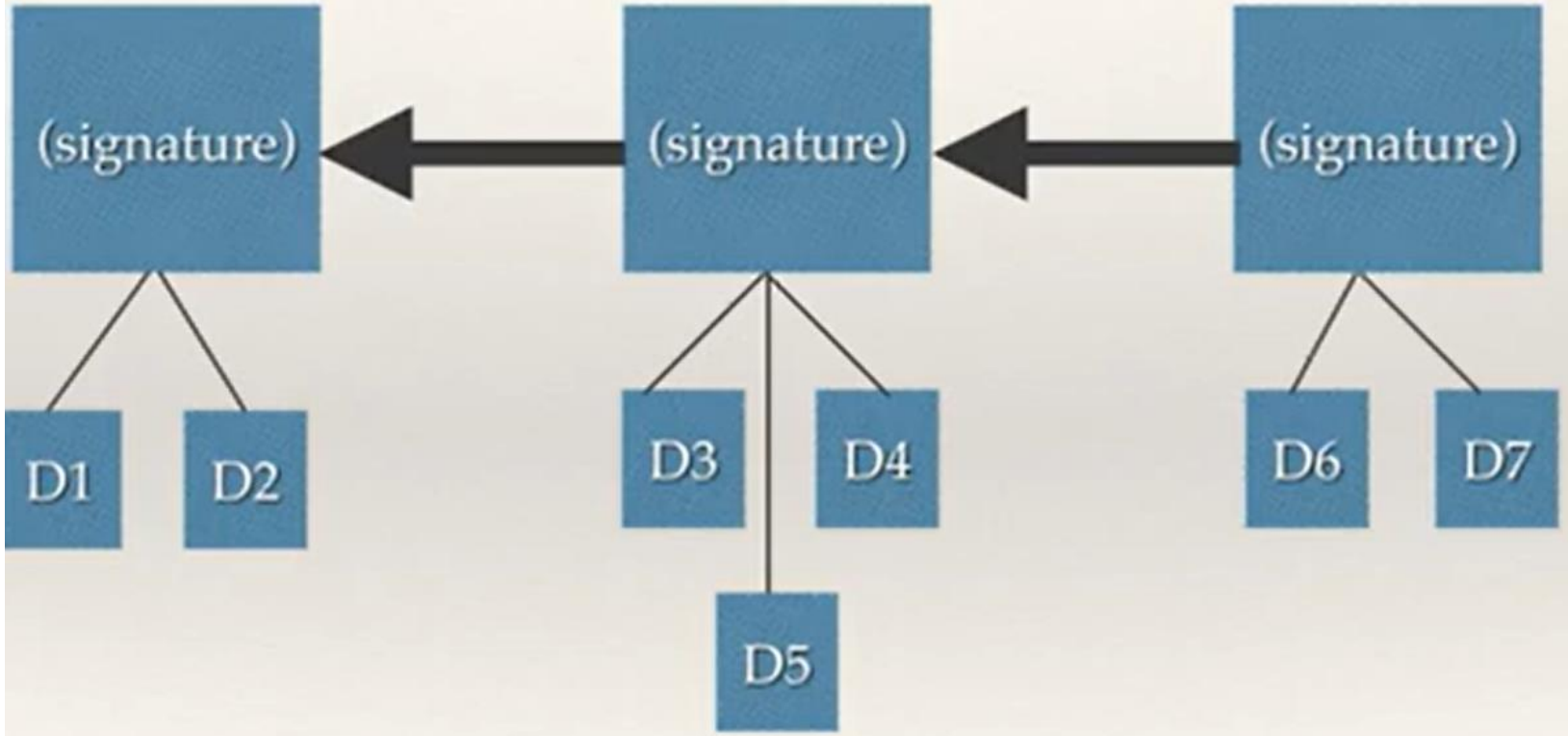
- 1992-Idea was proposed by Dwork, Naor's paper
- Later implemented as Adam Black's HashCash
- Similar to CAPTCHA mechanism-get some reward for solving it

Ledger's

- How to determine the order / timestamp of documents in a decentralized manner?
- If we know D1 was written before D2, D2 was written before D3, etc.. We can have a good idea of when the document was written.
- How to enforce the order? links to previous document!
- This makes a chain of documents…
- 1991: "How to Timestamp a Digital Document" by Haber, Stuart, Scott Stornetta

- Very inefficient with large number of documents
- Improvement: collect documents into groups (“blocks”), and only have signature link from going from block to block.
- In other words Block Chain

A "Block Chain"



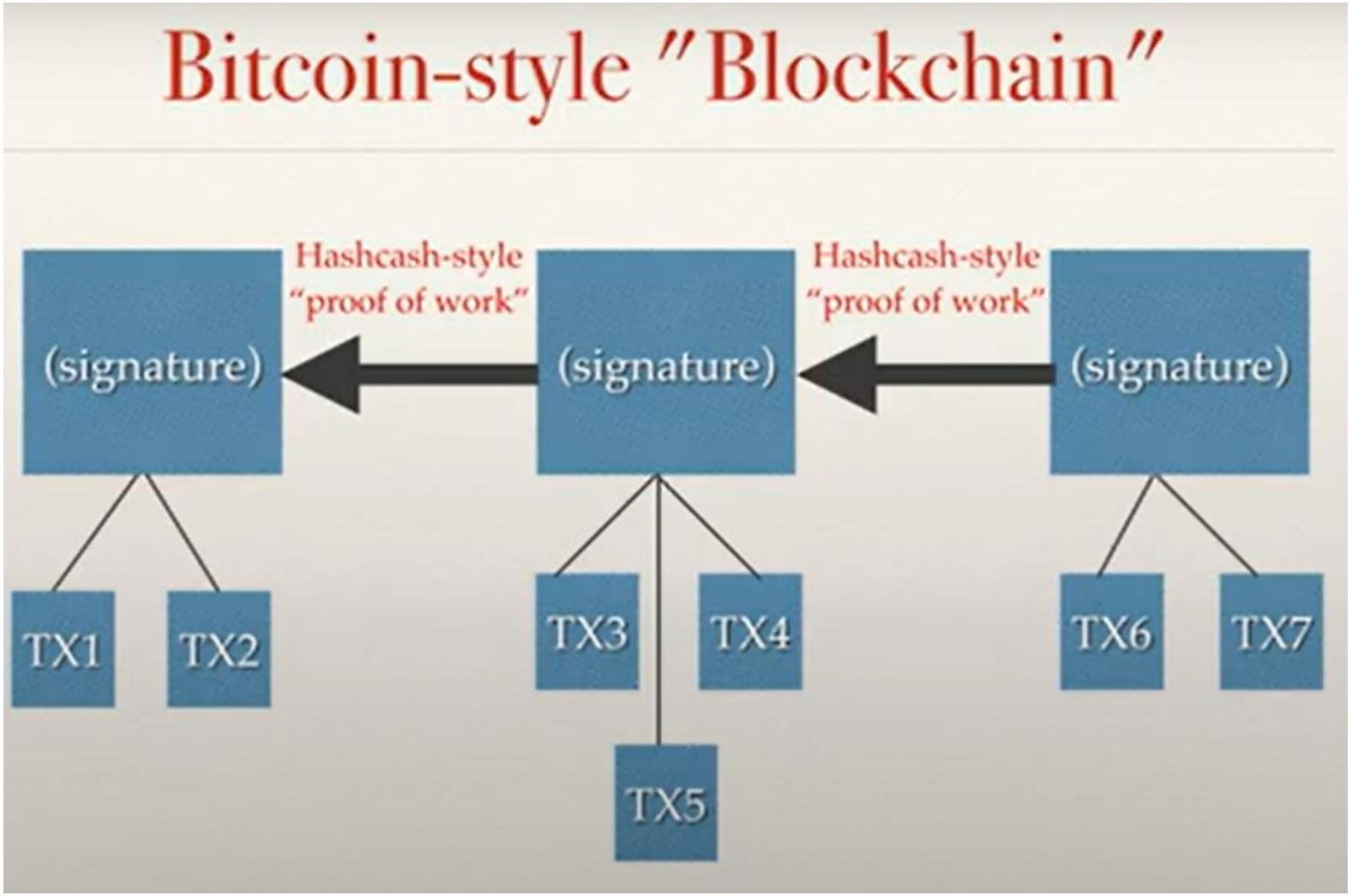
Reusable Proof Of Work

Hal Finney

- 2004: Rusable Proof of Work(RPoW)
- The unique feature of the RPOW system is its approach to security.
- RPOW is the first public implementation of a server designed to allow users throughout the world to verify its correctness and integrity in real time.
- Based on principles similar to those proposed for so-called "Trusted Computing", RPOW allows third parties to dynamically and remotely verify what program is running on the RPOW server.

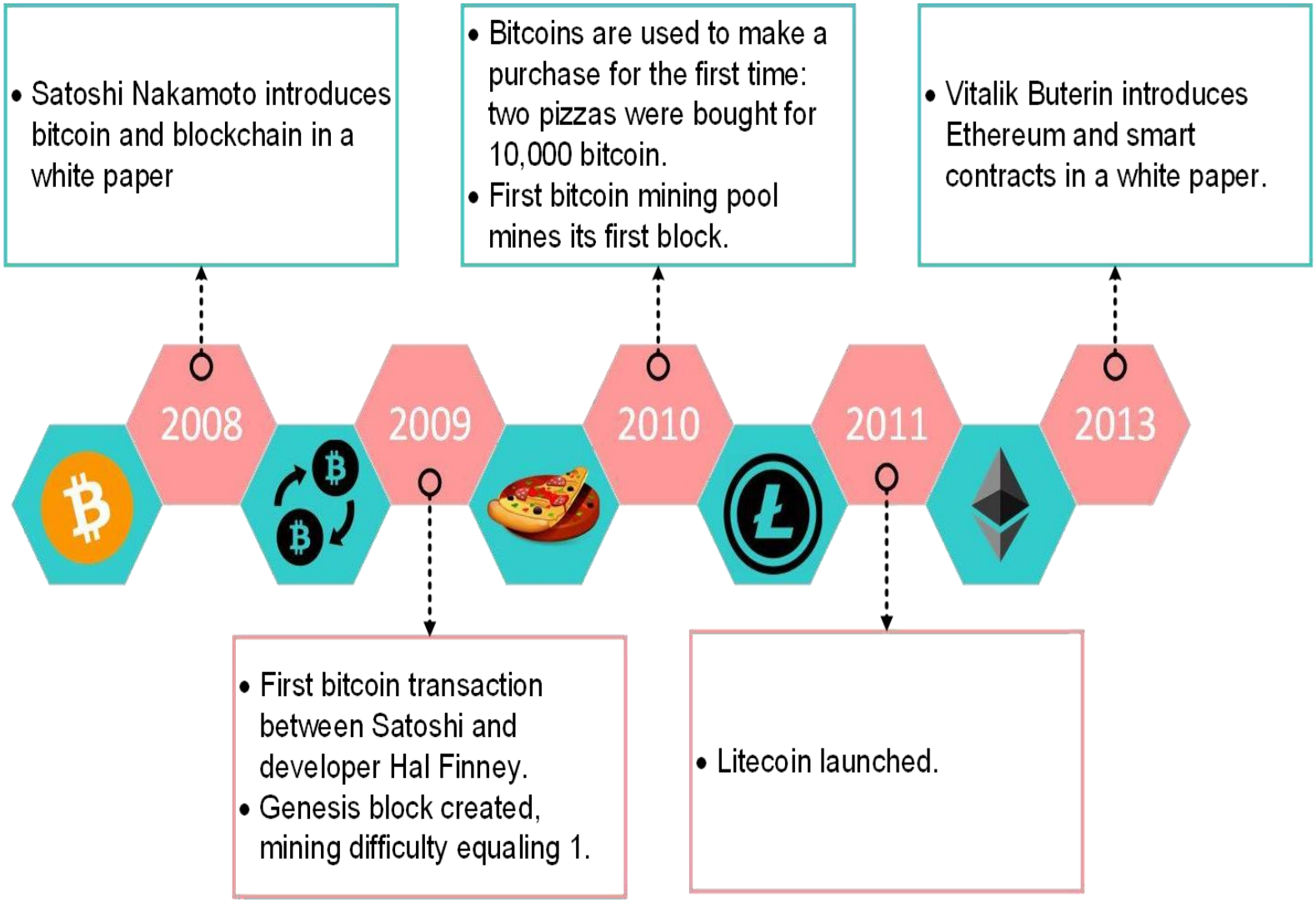
Bitcoin

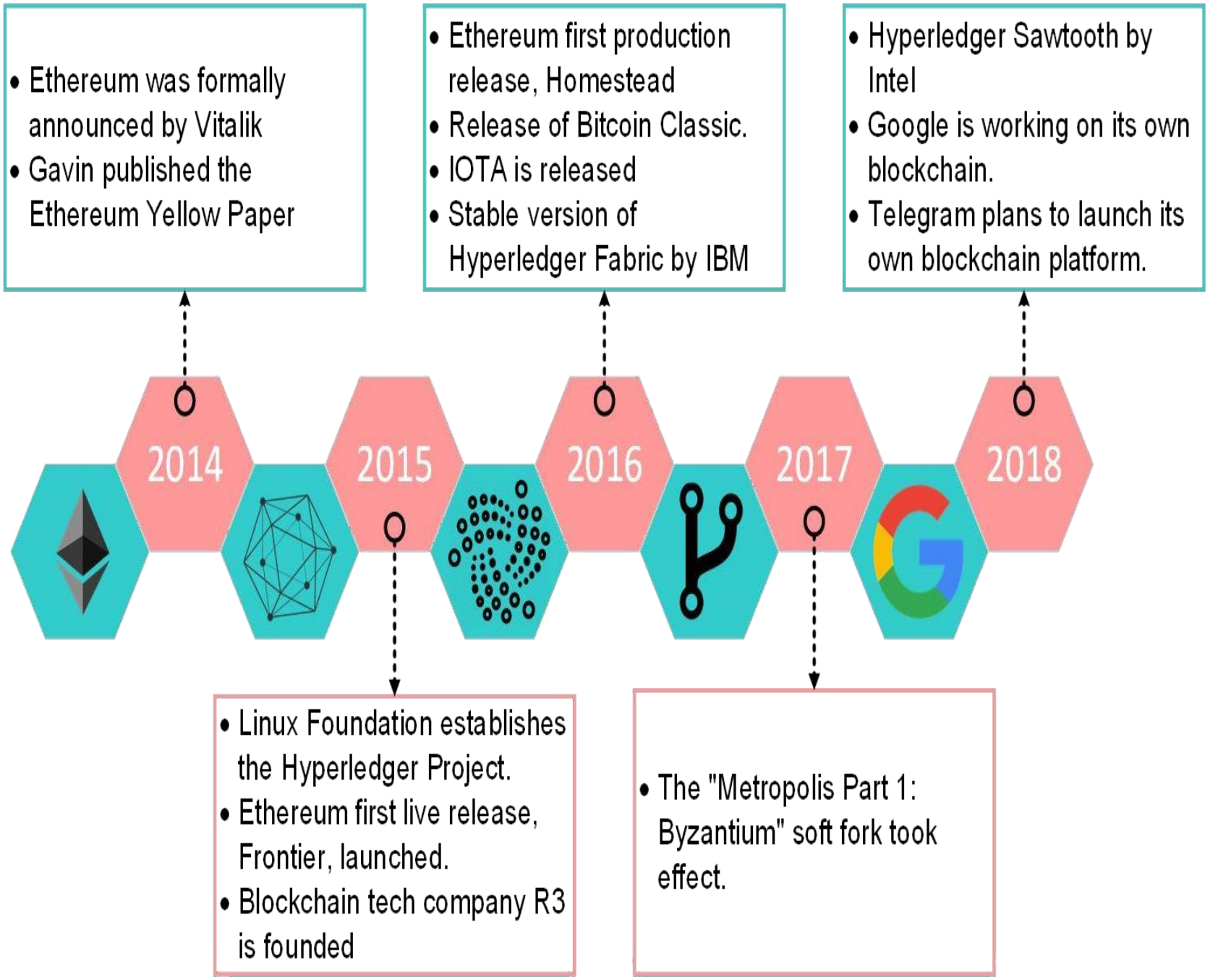
- The first modern Cryptocurrency
- Decentralized-no central arbiter and no easy way to censor transactions
- Transactions signed cryptographically
- Blocks added to a blockchain with proof of work, and those who add them are rewarded with bitcoins.
- "Bitcoin: A Peer to Peer Electronic Cash System" - **Satoshi Nakomoto**
- Bitcoin was created by the pseudonymous "Satoshi Nakomoto"
- Satoshi interacted with people online for several years, then went dark immediately
- The Concept behind it was used for the advent of new technology called "Blockcahin"



- Using transactions instead of documents, and rewarding them

Blockchain Evolution




• Ethereum was formally announced by Vitalik
• Gavin published the Ethereum Yellow Paper
• Ethereum first production release, Homestead
• Release of Bitcoin Classic.
• IOTA is released
• Stable version of Hyperledger Fabric by IBM
• Hyperledger Sawtooth by Intel
• Google is working on its own blockchain.
• Telegram plans to launch its own blockchain platform.
2014
2015
2016
2017
2018
• Linux Foundation establishes the Hyperledger Project.
• Ethereum first live release, Frontier, launched.
• Blockchain tech company R3 is founded
• The "Metropolis Part 1: Byzantium" soft fork took effect.

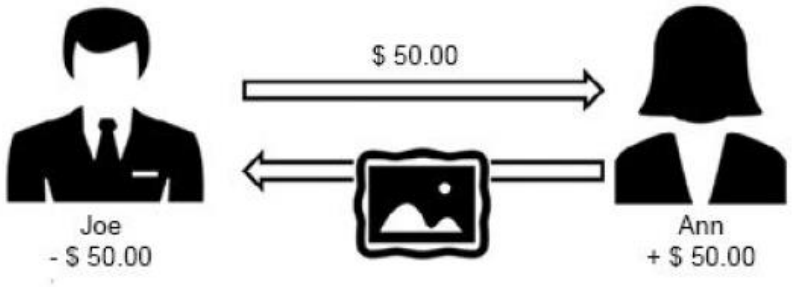
Generations of Blockchain

- First Generation Blockchain 1.0 (2008-2013): The Origin of Bitcoin
- Second Generation Blockchain 2.0 (2013-2015): Transactions with Smart Contracts
- Third Generation Blockchain 3.0 (2015-2018): Distributed Applications
- Fourth Generation Blockchain 4.0 (2018-Future): New Innovations,Applications

Traditional vs. Blockchain Transactions

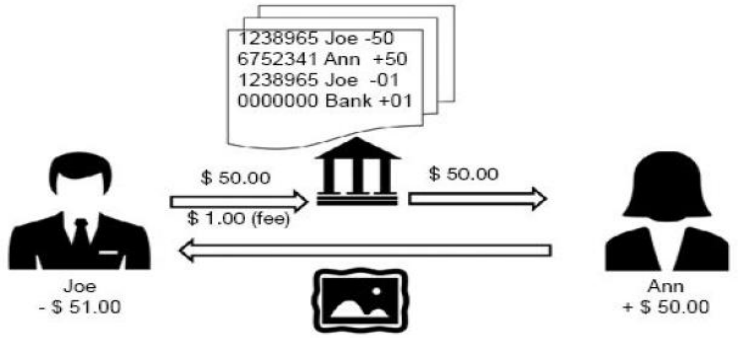
Scenario-1:

Physical transaction



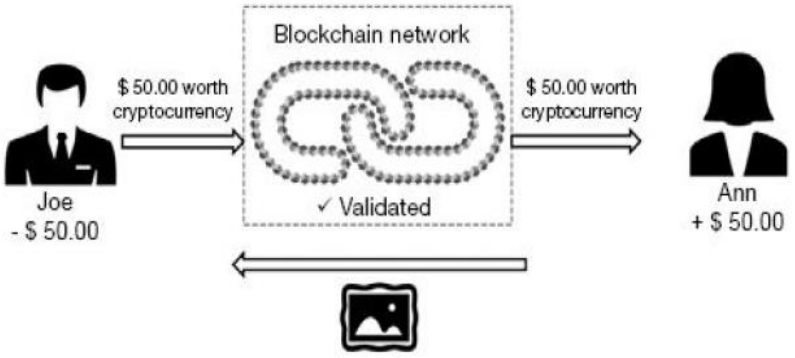
Scenario-2:

Traditional online transaction



Scenario-3:

Blockchain transaction



Introduction to BLOCKCHAIN

Definition

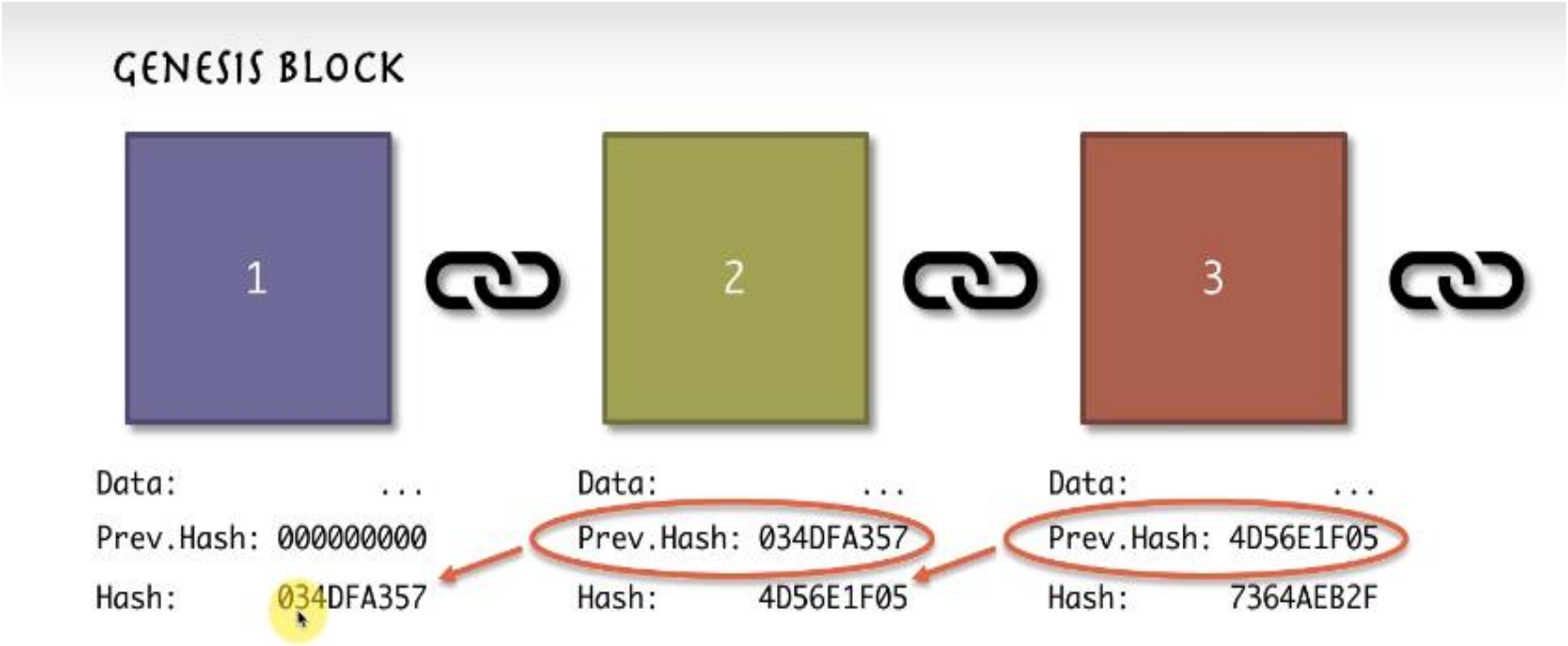
- **Layman's definition**:

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.

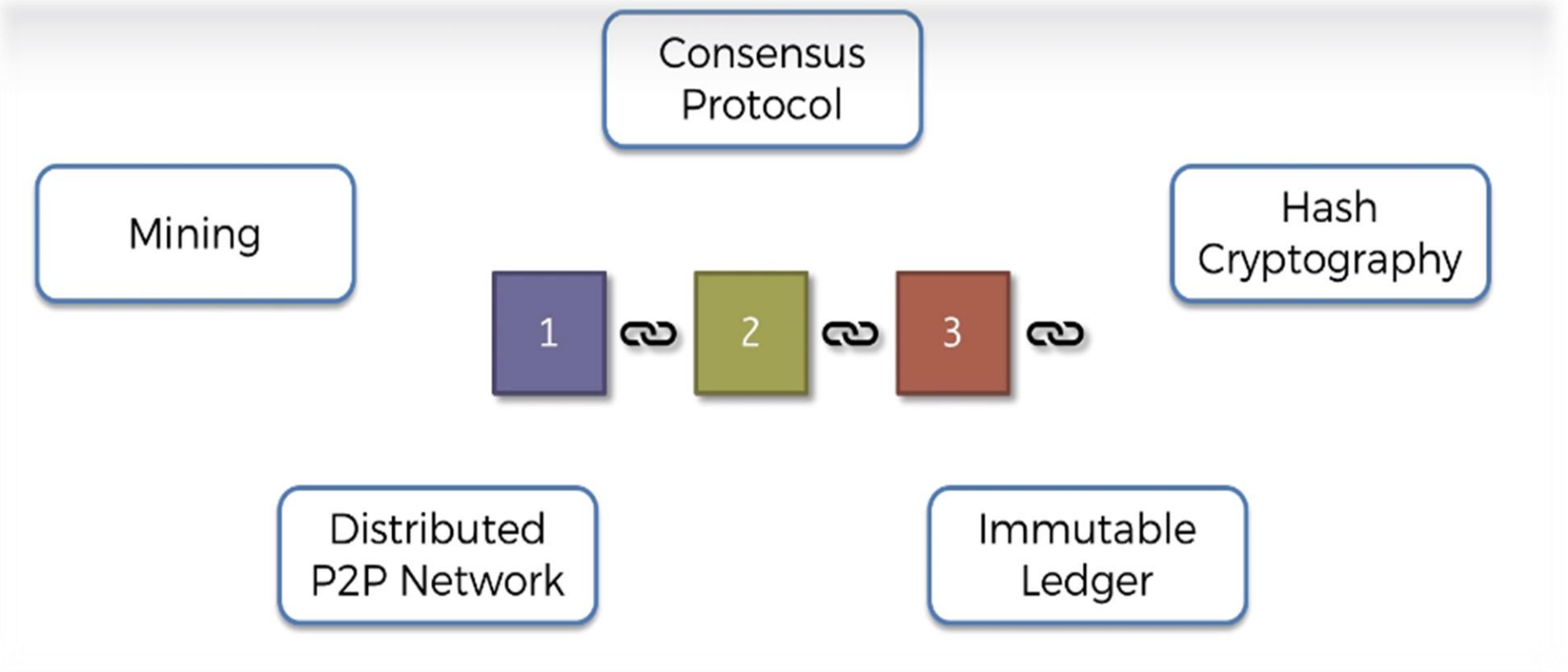
- **Technical definition**:

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


GENESIS BLOCK
1
2
3
Data: ...
Prev.Hash: 000000000
Hash: 034DFA357
Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05
Data: ...
Prev.Hash: 4D56E1F05
Hash: 7364AEB2F

Blockchain


Consensus Protocol
Mining
Hash Cryptography
1
2
3
Distributed P2P Network
Immutable Ledger