Introduction to Blockchain and DLT

Griffith UNIVERSITY

Objectives

- To Give an Overall Introduction
- To Identify the Core Concepts & Mechanisms
- To Get a Basic Idea about Bitcoin Protocol
- To Compare Blockchain Technology & DLT

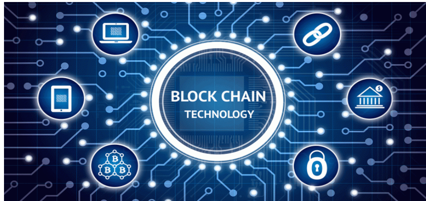
References

1) Satoshi Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, http://bitcoin.org/bitcoin.pdf, 2008

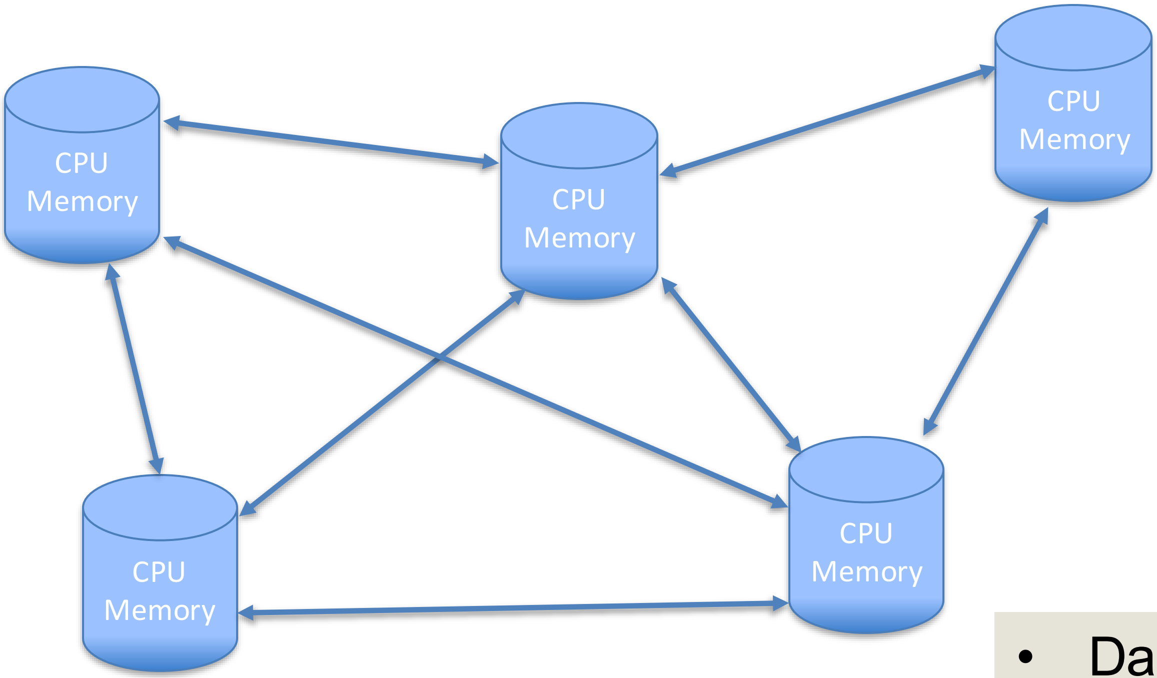
1) PGP Corporation, “An Introduction to Cryptography”, 2002, Chapter 1: https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf

Blockchain Technology

- One of the most promising technological innovations – **paradigm shift**
- **Distributed, peer-to-peer** technology
- Enables to build **Trust** from an untrusted environment
- Transactions & Records are **Tamper-evident (~ immutable)**
- Enables exchange of digital and physical assets even in an untrusted environment **preventing Double-spending**
- Internet of information ➔ **Internet of value** (Exchange of digital assets)
- Provides **Traceability (provenance)**

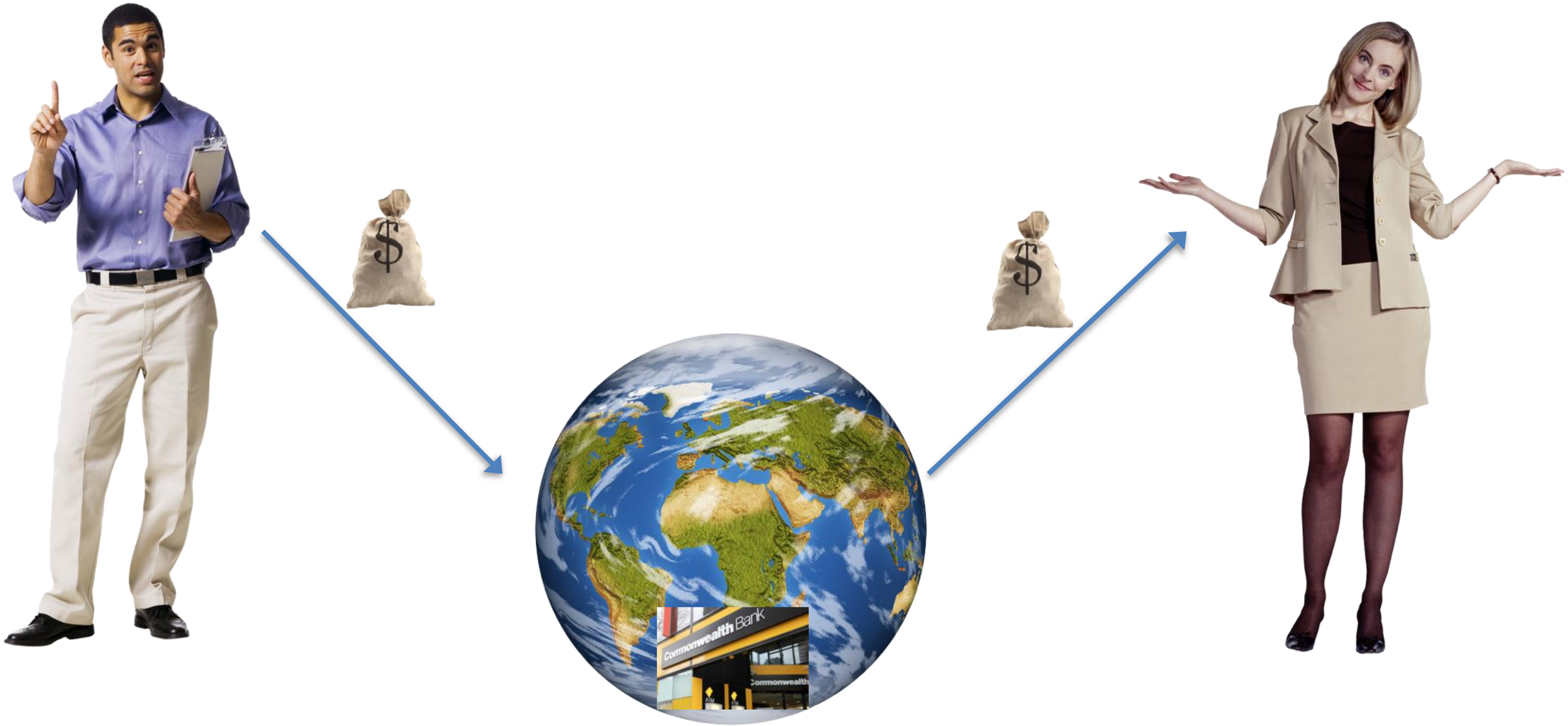


Distributed Peer-to-Peer Systems



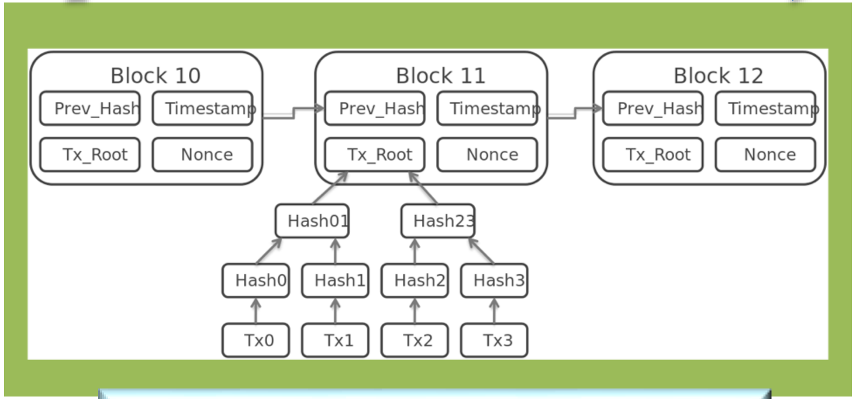
- Data Collection
- Data Flow
- Data Processing

Traditional Trust Environment



Centralised Trusted Authority

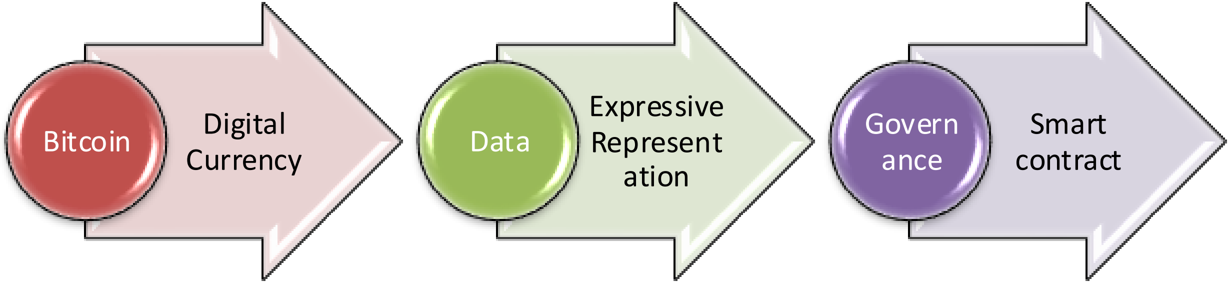
Trust via Distributed Ledger Technology



Distributed P2P Network

Characteristics

- Global reach
- Virtual/ Digital assets with no jurisdiction of residency
- Challenges for regulator to prosecute, while participants are vulnerable
- Proliferation of crypto currencies, Non-fungible tokens & Digital assets


Bitcoin

Digital Currency

Data

Expressive Represent ation

Govern ance

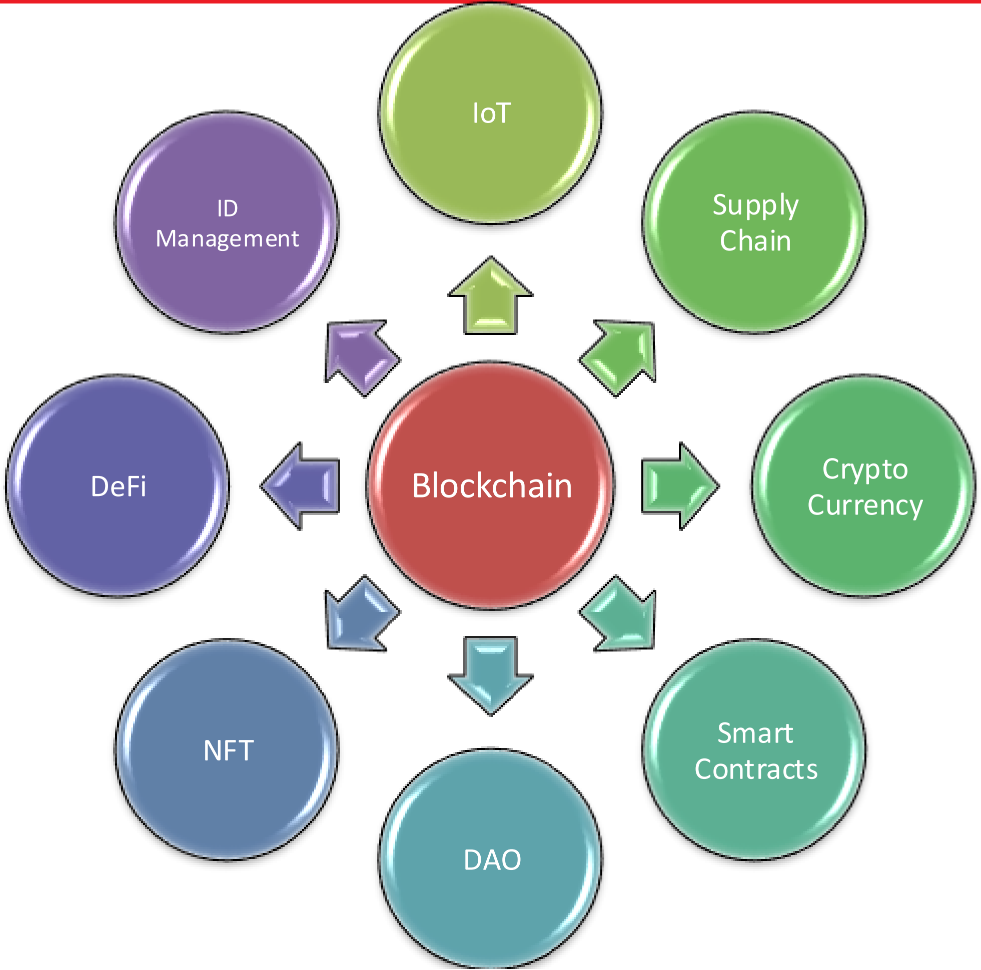
Smart contract

Data Driven Economy

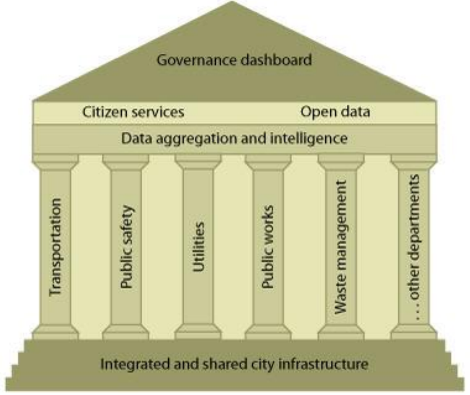
- Business intelligence and analytics
- IT was functional-level strategy and **was** to be aligned with business strategy
- But digital economy rewrites the rules and fundamentally transforms business strategies

Potential Blockchain Applications

Griffith UNIVERSITY



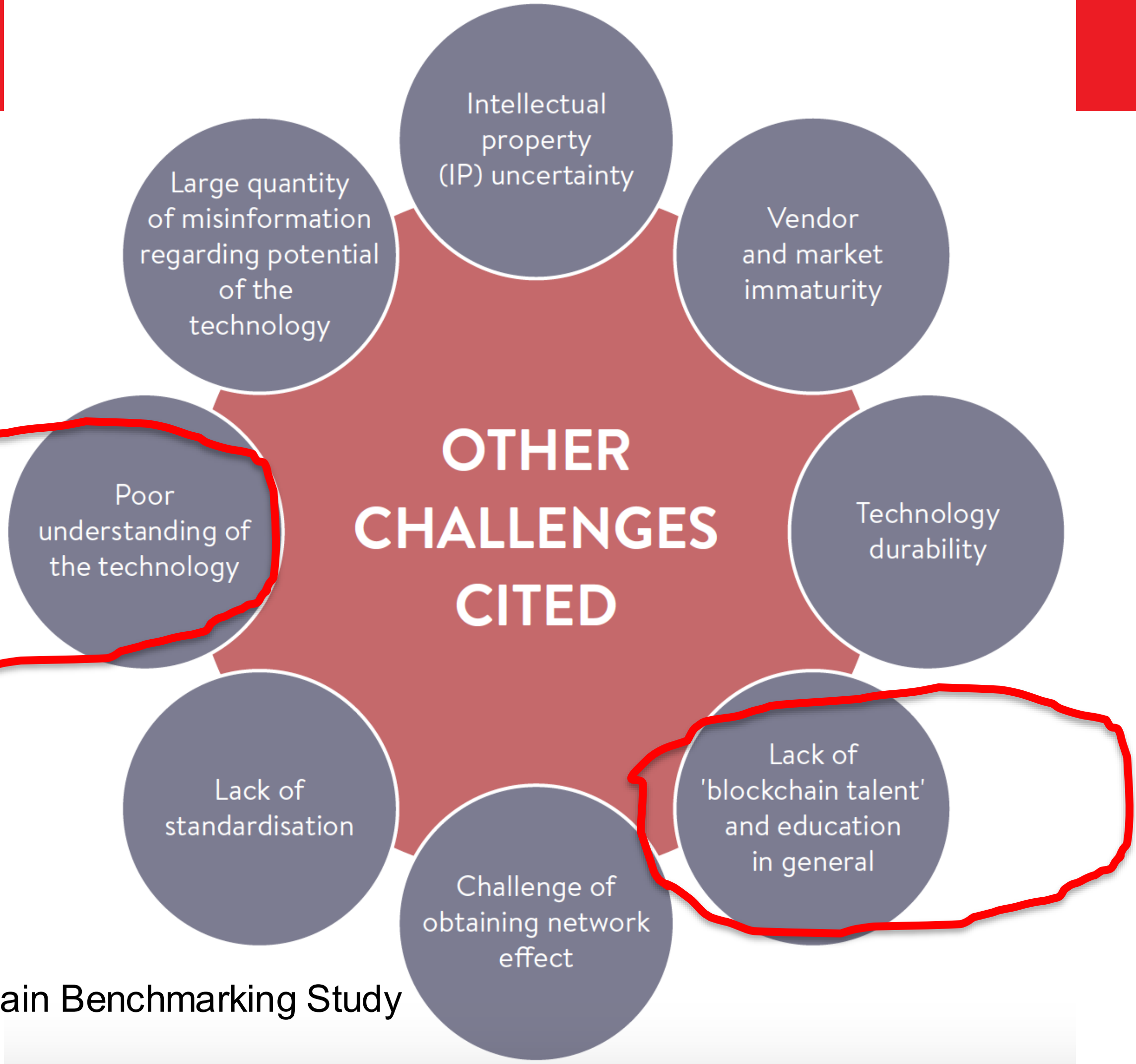
21st Century Smart Governance



- Potential for radical institutional and societal reforms
  - Provides **Transparency** and **Privacy**
  - **Engage the Citizens** & **Stakeholders** in the processes
  - Removes the need for **intermediary/ arbitration**
  - **Agree on a single source of truth**

Gold Coast 2018 XXI Commonwealth Games | Griffith UNIVERSITY
OFFICIAL PARTNER

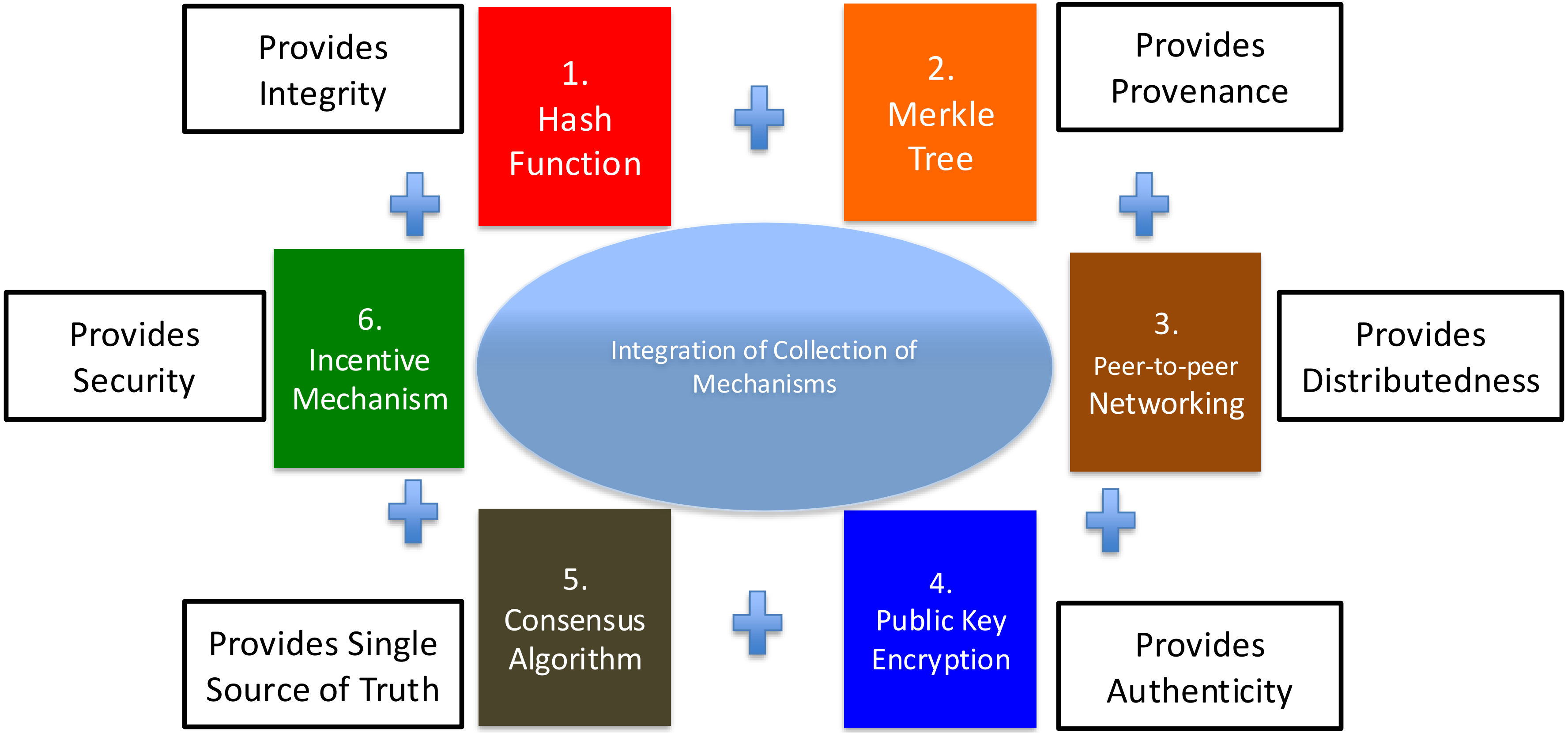
Griffith UNIVERSITY


OTHER CHALLENGES CITED
Intellectual property (IP) uncertainty
Vendor and market immaturity
Technology durability
Lack of 'blockchain talent' and education in general
Challenge of obtaining network effect
Lack of standardisation
Poor understanding of the technology
Large quantity of misinformation regarding potential of the technology

Source: Global Blockchain Benchmarking Study

Six Core Concepts and Mechanisms

Griffith UNIVERSITY



Provides Integrity

1. Hash Function

2. Merkle Tree

Provides Provenance

Integration of Collection of Mechanisms

6. Incentive Mechanism

Provides Security

3. Peer-to-peer Networking

Provides Distributedness

5. Consensus Algorithm

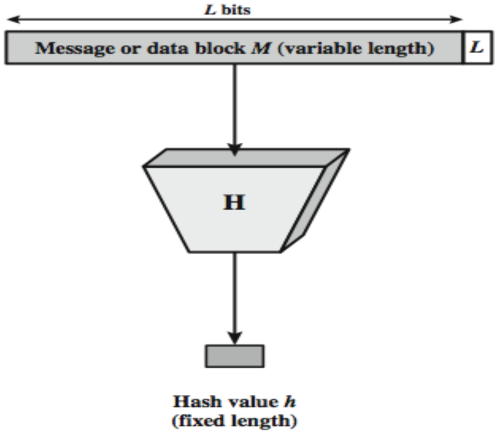
Provides Single Source of Truth

4. Public Key Encryption

Provides Authenticity

Hash Function Operation

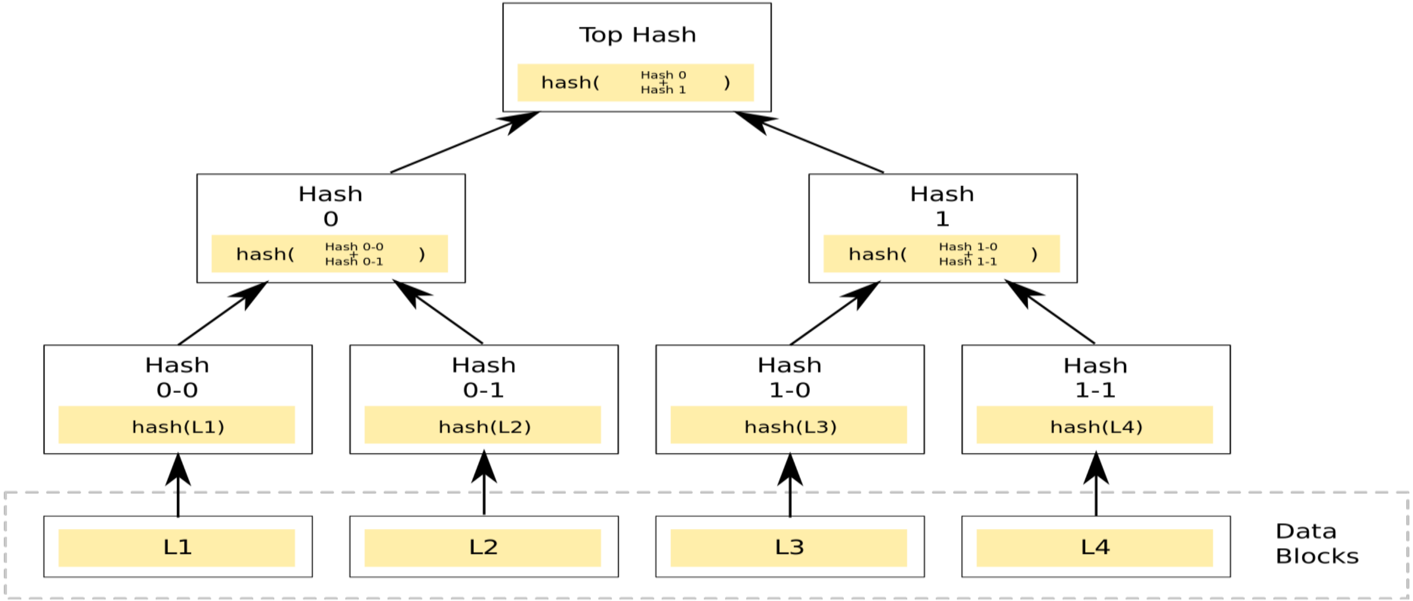
h = H(m)



1. **One-way property**
   - Given H(x), infeasible to find x
2. Given x, easy to compute hash value **H(x)**
3. **Weak collision resistance**
   - Given **`x`** is infeasible to find **`y`** such that **`H(y)=H(x)`**
4. **Strong collision resistance**
   - Is infeasible to find any **`x,y`** such that **`H(y)=H(x)`**

Merkle Tree: Method of Providing Digital Signature

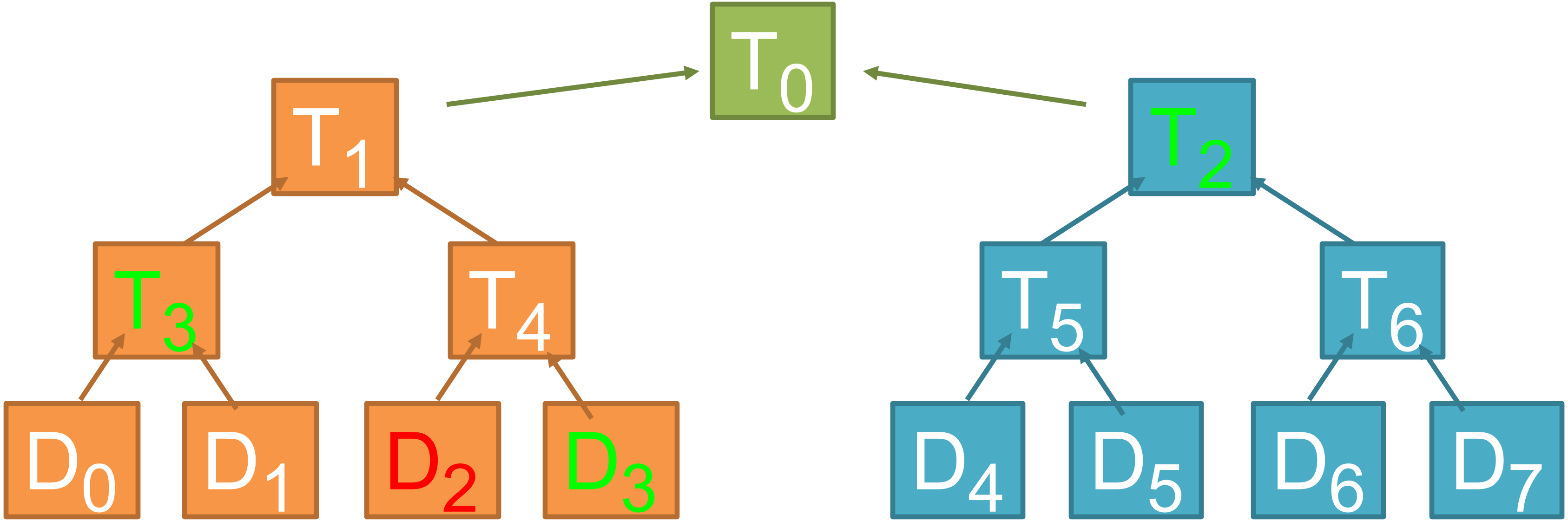
- A Merkle hash tree is a tree of hashes in which the leaves are hashes of data blocks in a file or set of files
- Nodes further up in the tree are the hashes of their respective children
- For example, *hash 0* is the result of hashing *hash 0-0* and *hash 0-1*



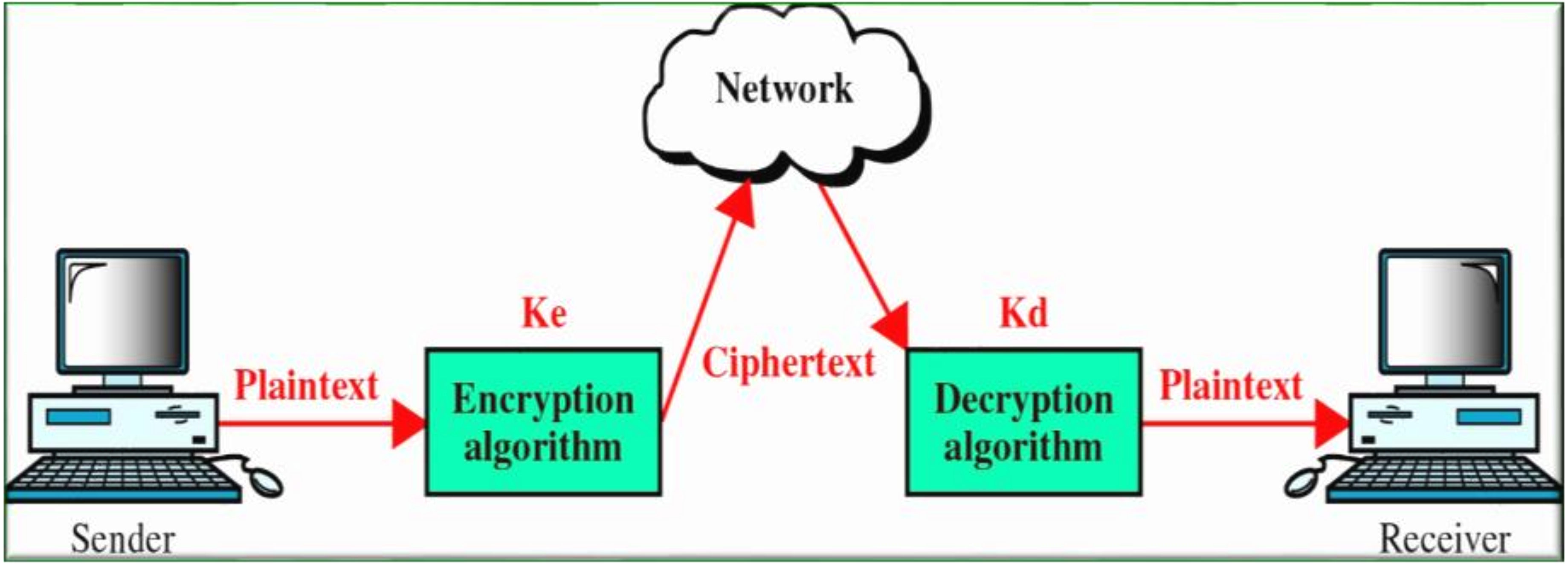
Ralph Merkle

Merkle Trees: Authentication

- Verifier knows T_0
- Suppose, you want to authenticate leaf **D_2**
- Sender gives D_3 T_3 T_2 ;   Re-compute T_0 using D_2
- Verify $T_0 = H(\ H(\ T_3\ ||\ H(\ D_2\ ||\ D_3\ ))\ ||\ T_2\ )$



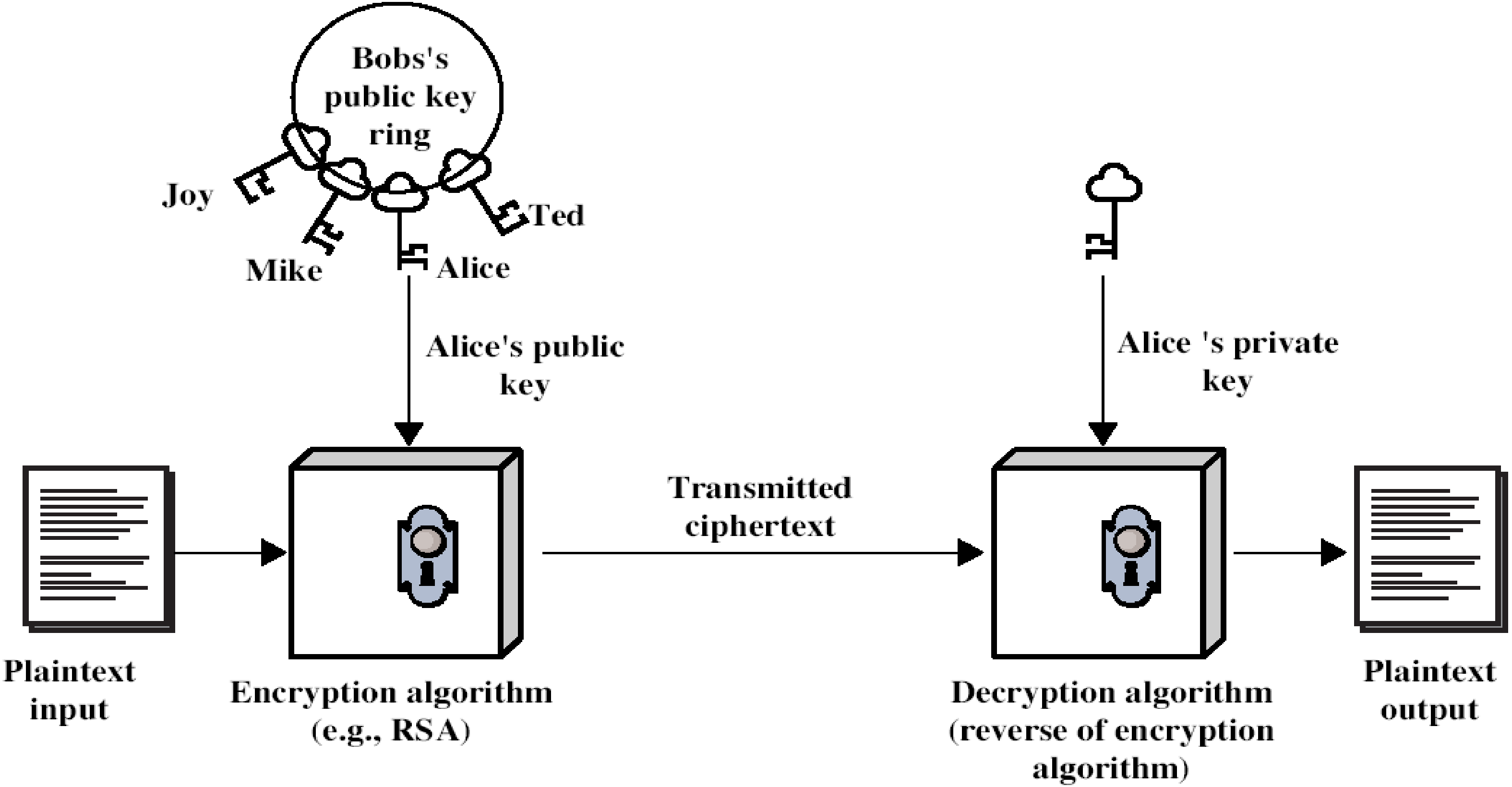
General Encryption Model



Ke: encryption key

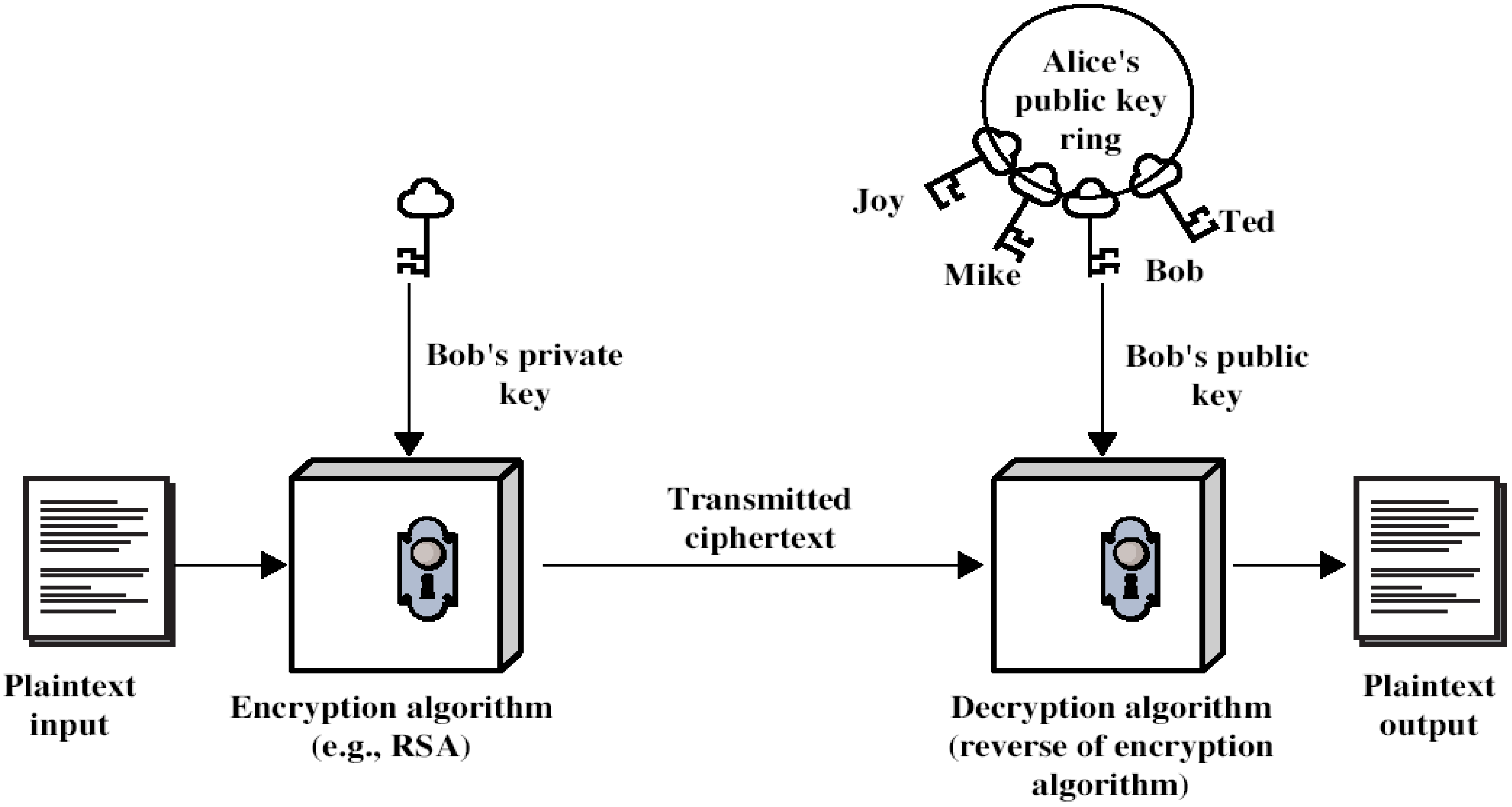
Kd: decryption key

Public-Key Encryption



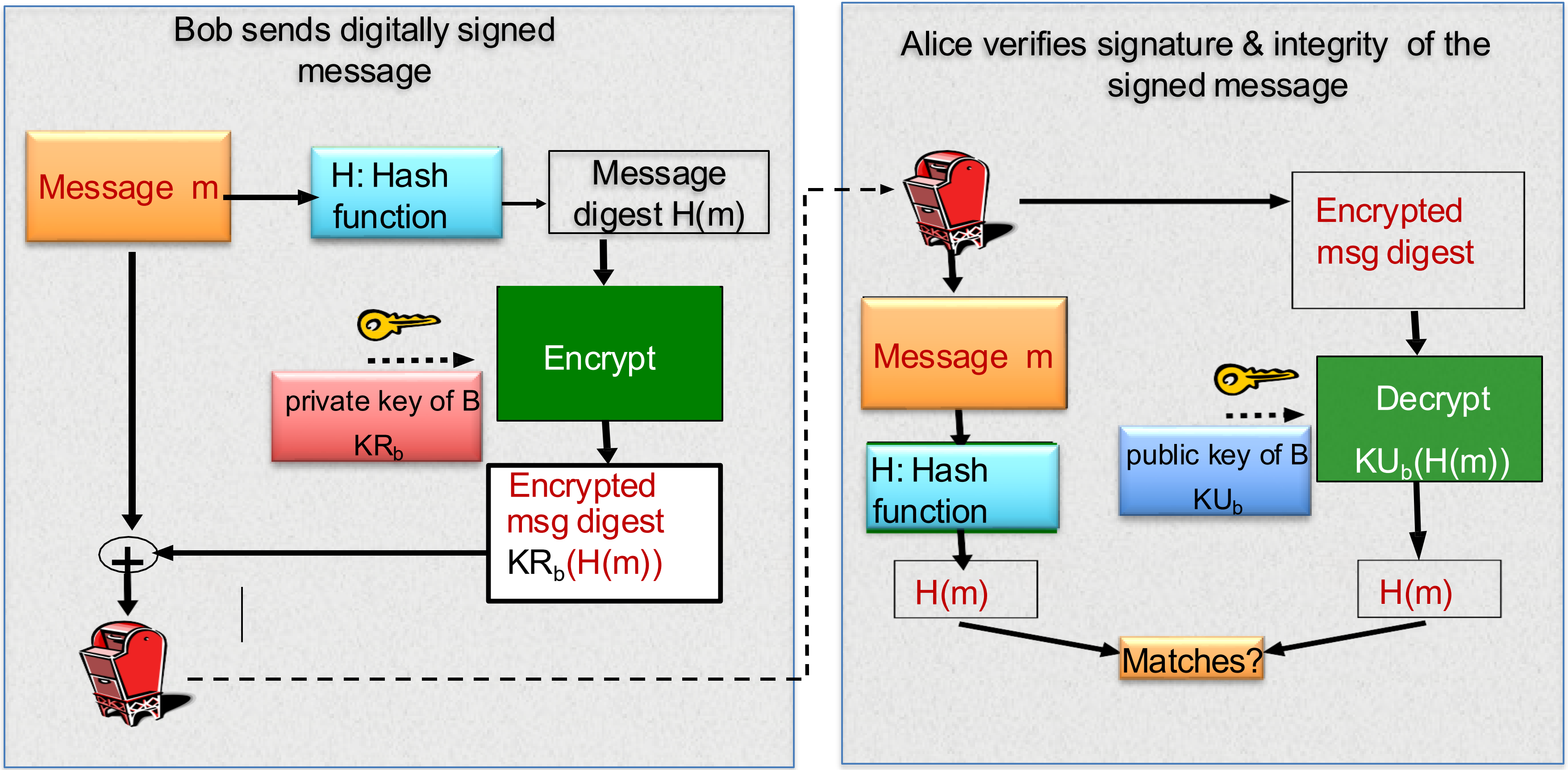
(Stallings Fig 9.1a)

Public-Key Authentication



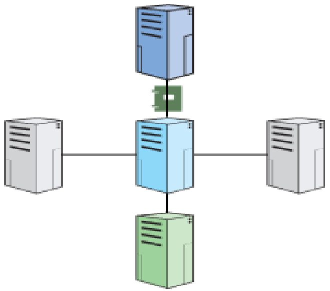
(Stallings Fig 9.1b)

Digital Signature and Verification

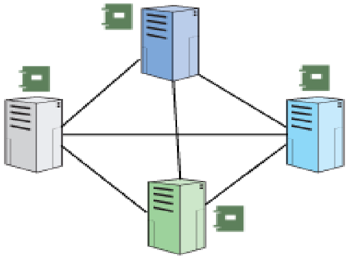


What is Peer-to-Peer Network?

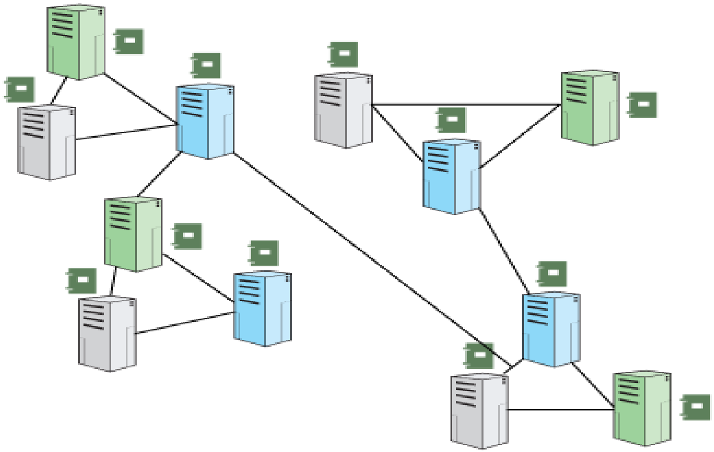
- Peer-to-Peer, distributed database of transactions
- Block contains hash values of previous transactions – for verification



Centralized ledger network

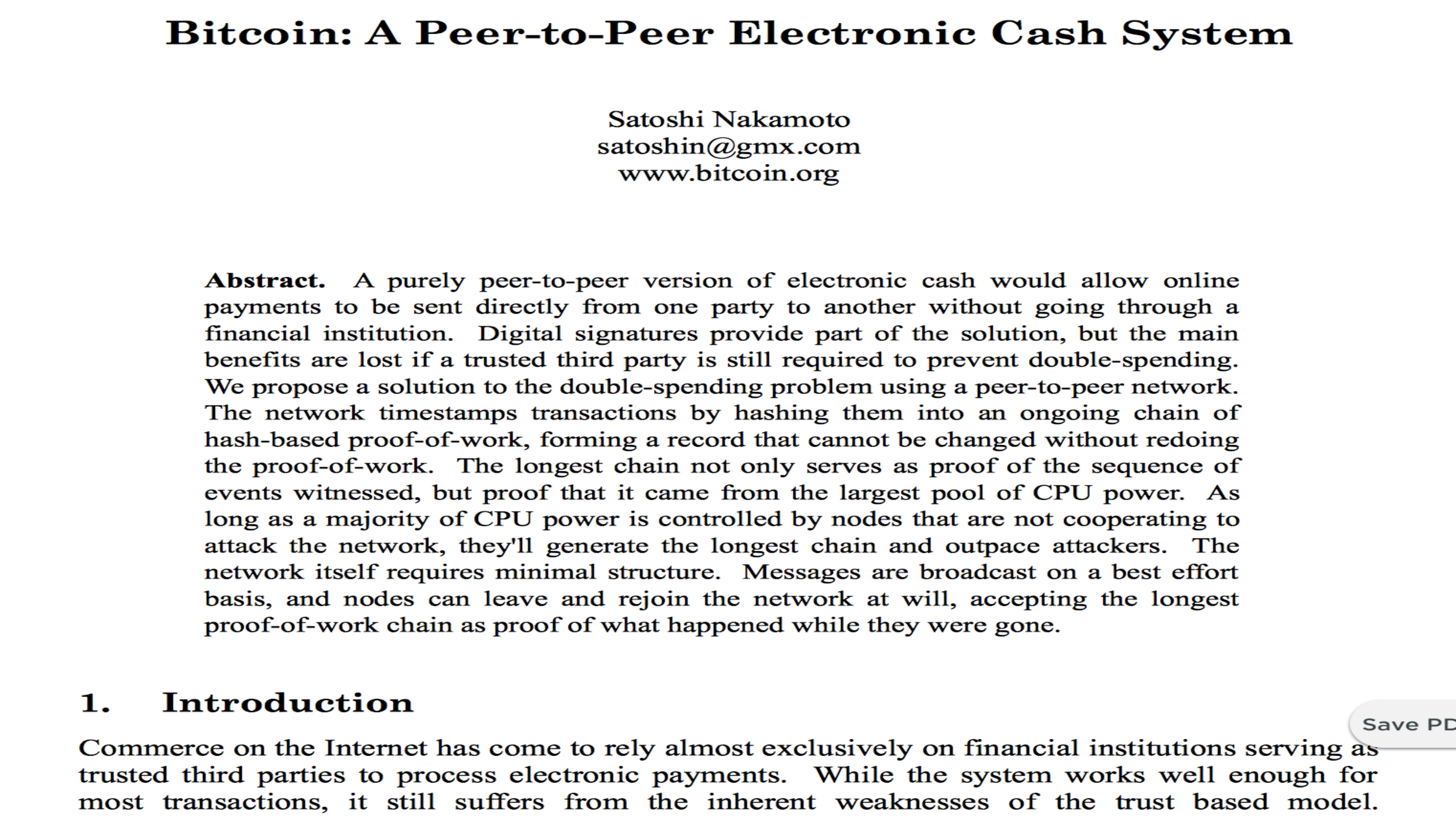


Distributed ledger network



Decentralized ledger network

www.ibm.com



Bitcoin: A Peer-to-Peer Electronic Cash System

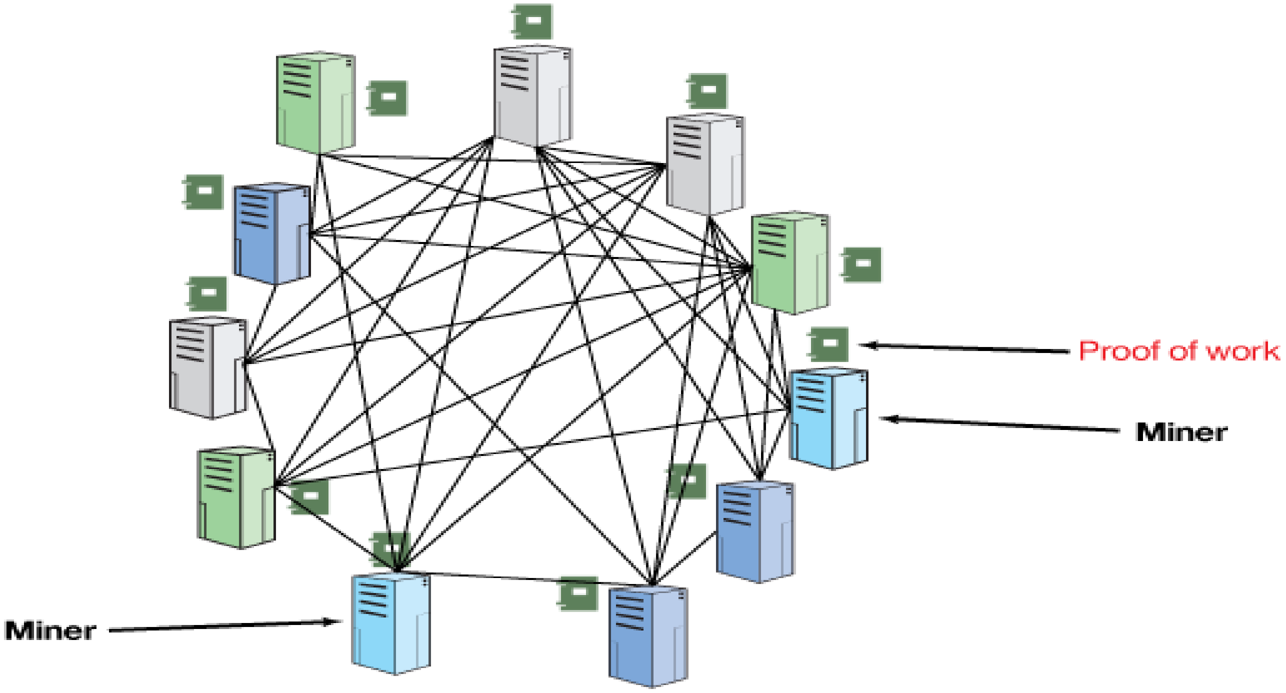
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

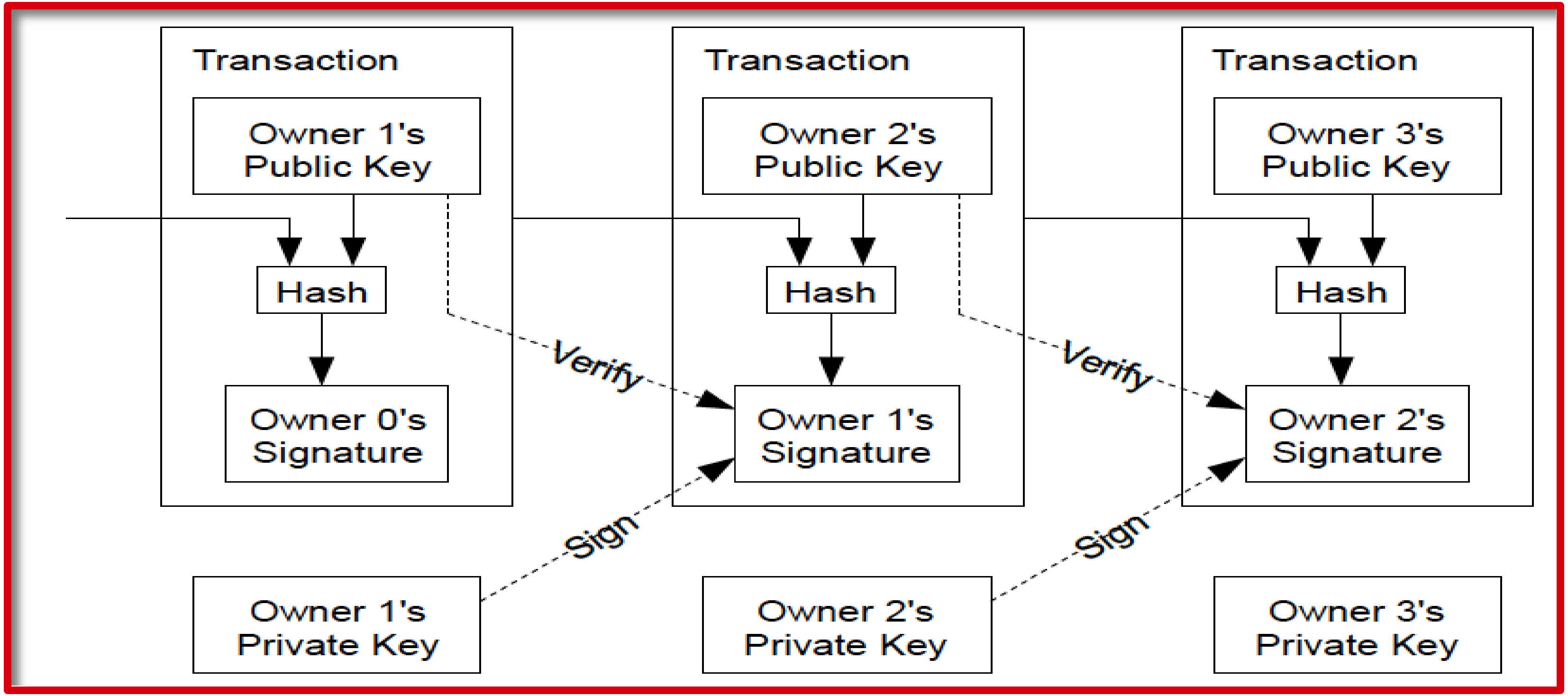
Bitcoin: Miner



Decentralized blockchain ledger network consensus

www.ibm.com

Bitcoin: Connected Series



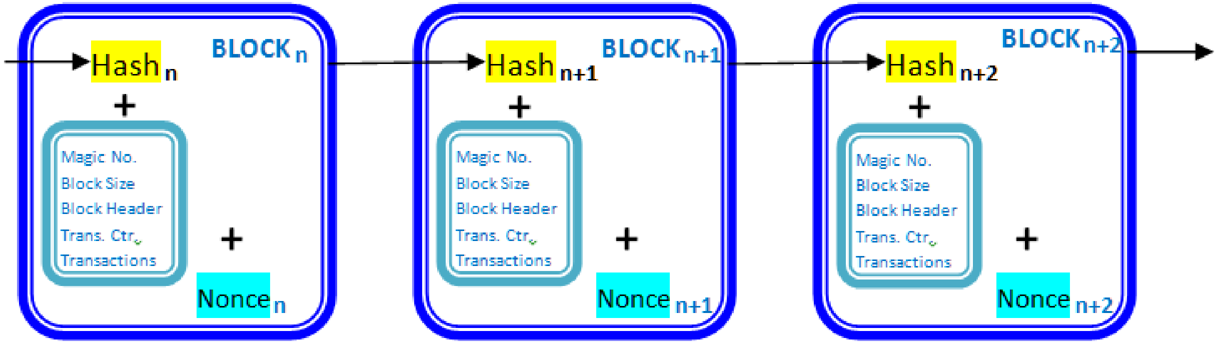
Block Generation

- **Cryptographic proof** instead of the traditional trust in the 3rd party
- Each transaction is protected through a **digital signature**
  - (previous hash + receiver’s public key) is signed with the private key of the sender
- Sender needs to prove the ownership of the private key

Block Validation

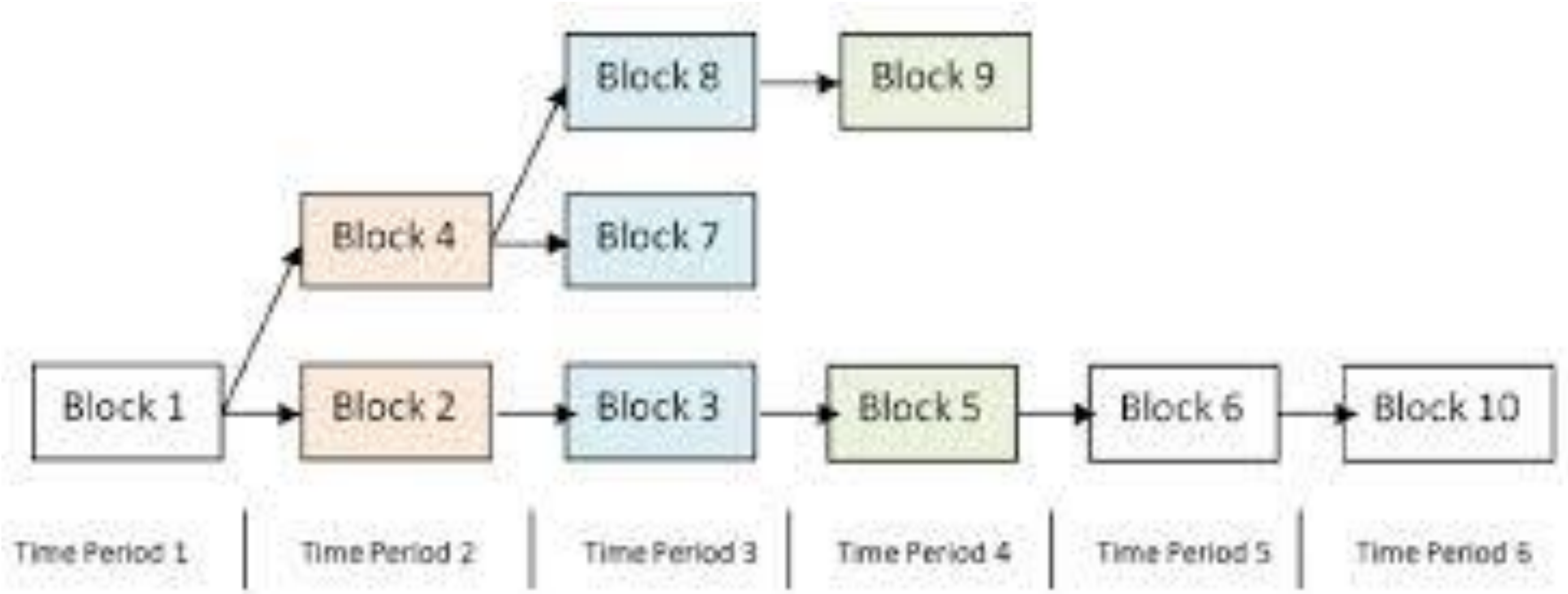
- This is verified by the public key of the sender
- Each transaction is broadcast to every node and is then recorded in a public ledger (after verification)
- All other nodes can act as ‘miners’ to solve the crypto problem

Proof of Work



- The ‘miner’, who 1st generates the correct pseudorandom number **gets rewarded** for the ‘proof-of-work’
- Proof-of-work and broadcasting to all prevent ‘double spending’
- Verification is easy

Verification – Forking

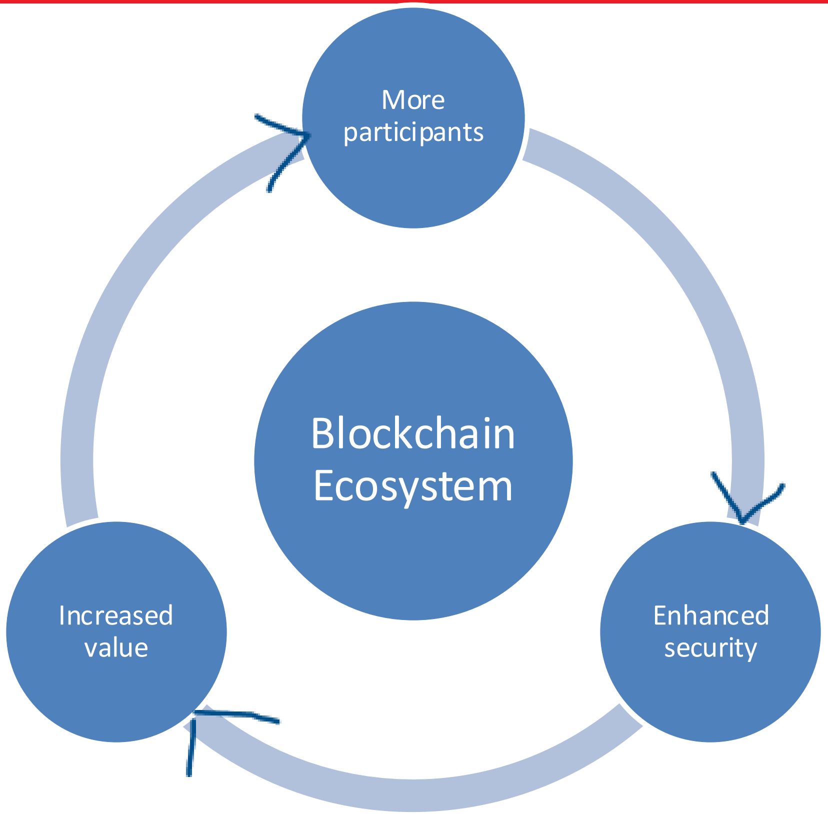


- Longest proof-of-work chain is used

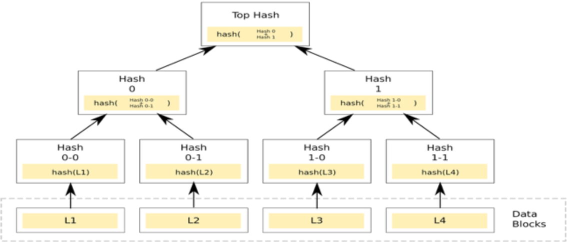
Security

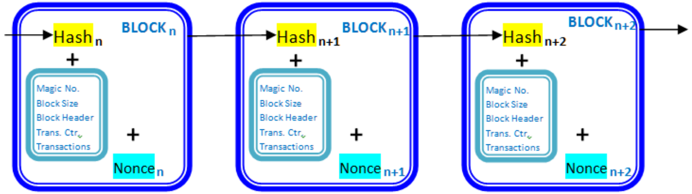
- Blockchain security is as good as the way the system is designed
- In general, good integrity but poor in other characteristics (confidentiality)
- Implementation gaps are the main vulnerabilities at the initial phase
- Not much work has been done on formal verification of protocols and the Architecture of DLT systems

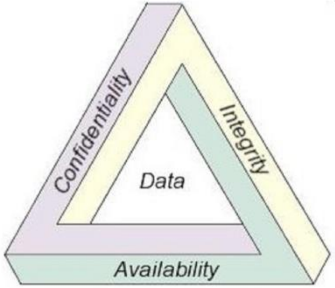
Security and Value Creation

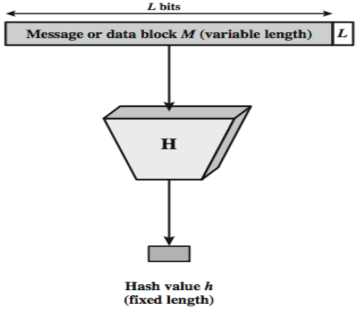


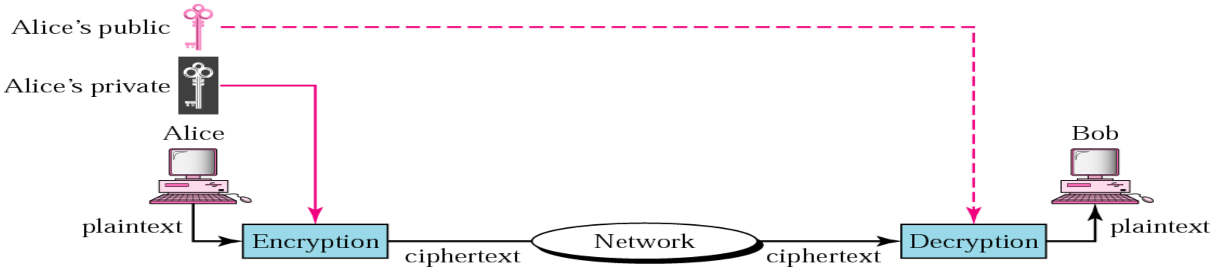
Summary of Security Mechanisms

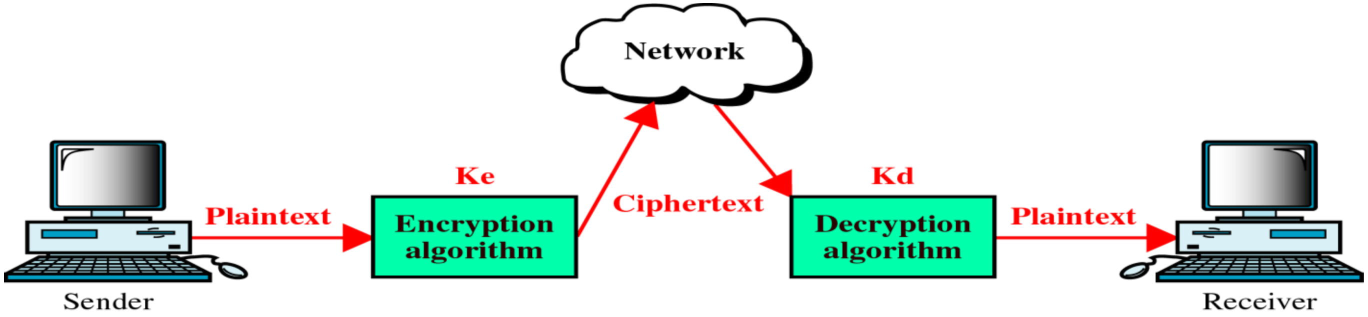








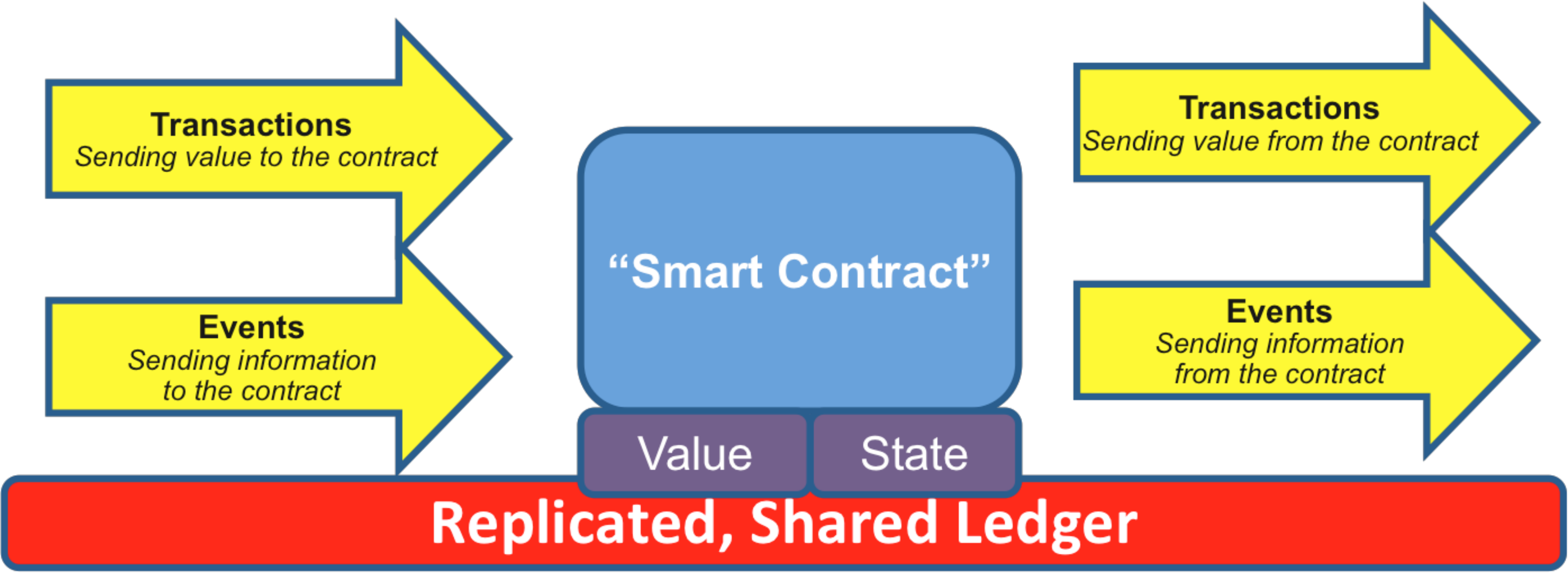




Blockchain Technology

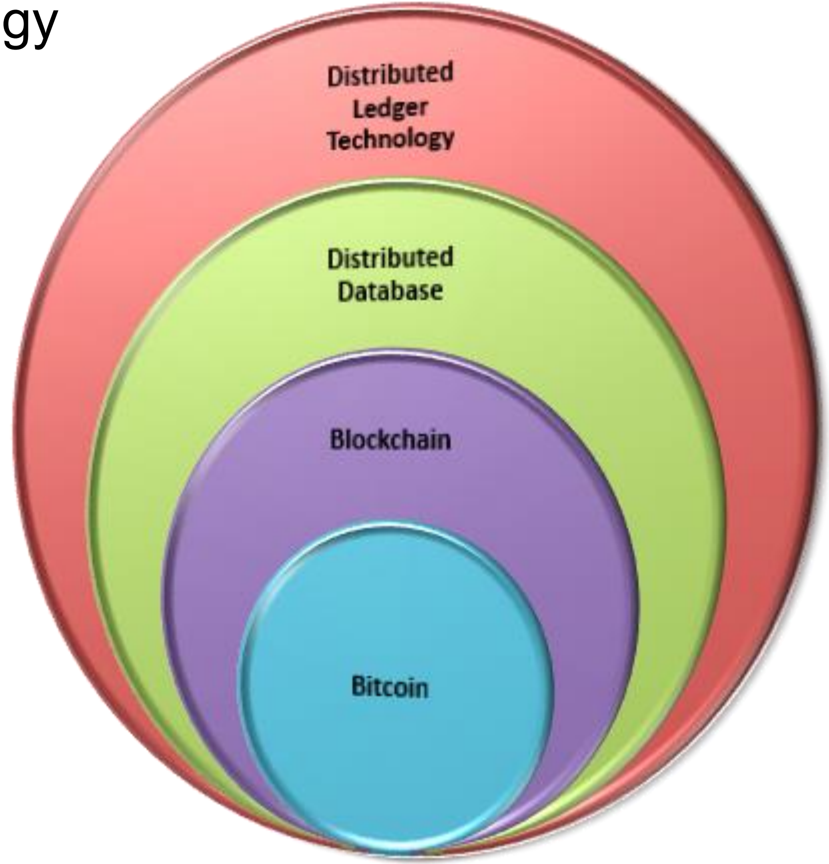
- Distributed database for recording transactions/ storing digital assets
- Enabling transfer of digital assets
- Execute Smart Contracts and run different consensus mechanisms
- Can develop applications on a programmable platforms to run bitcoin like protocols
- Can operate at different levels of decentralisation

Smart Contract [Richard Brown]

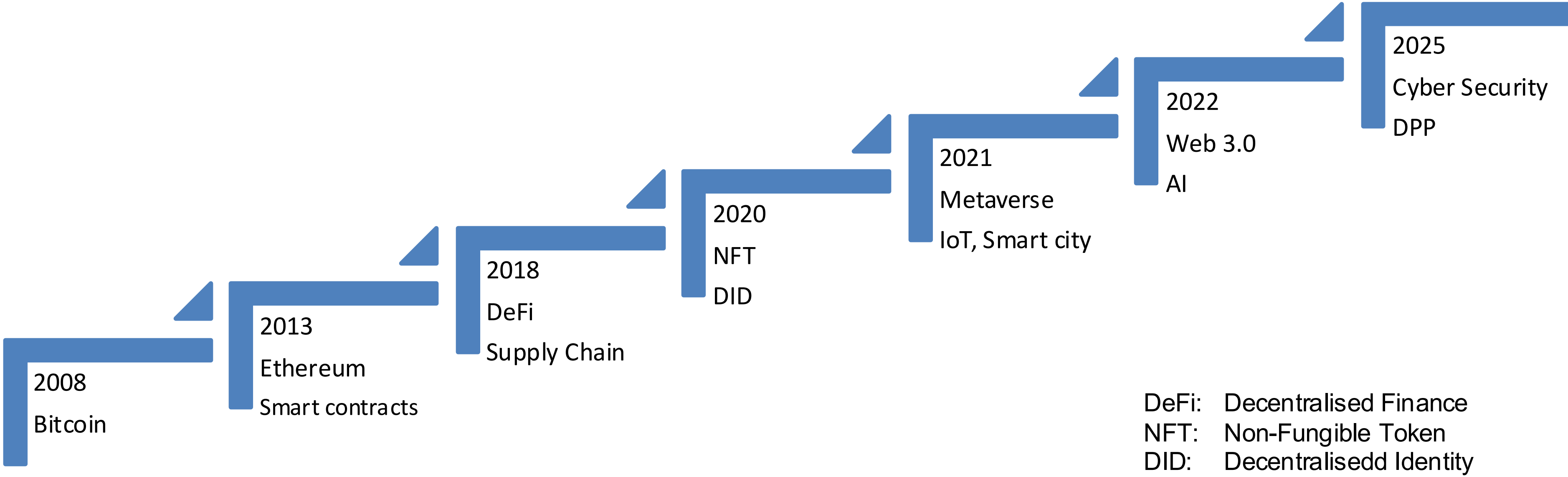

Transactions
Sending value to the contract
Events
Sending information to the contract
"Smart Contract"
Value
State
Transactions
Sending value from the contract
Events
Sending information from the contract
Replicated, Shared Ledger

Distributed Ledger Technology

- A generalised technology



Evolution of Blockchain Technology



2008
Bitcoin

2013
Ethereum
Smart contracts

2018
DeFi
Supply Chain

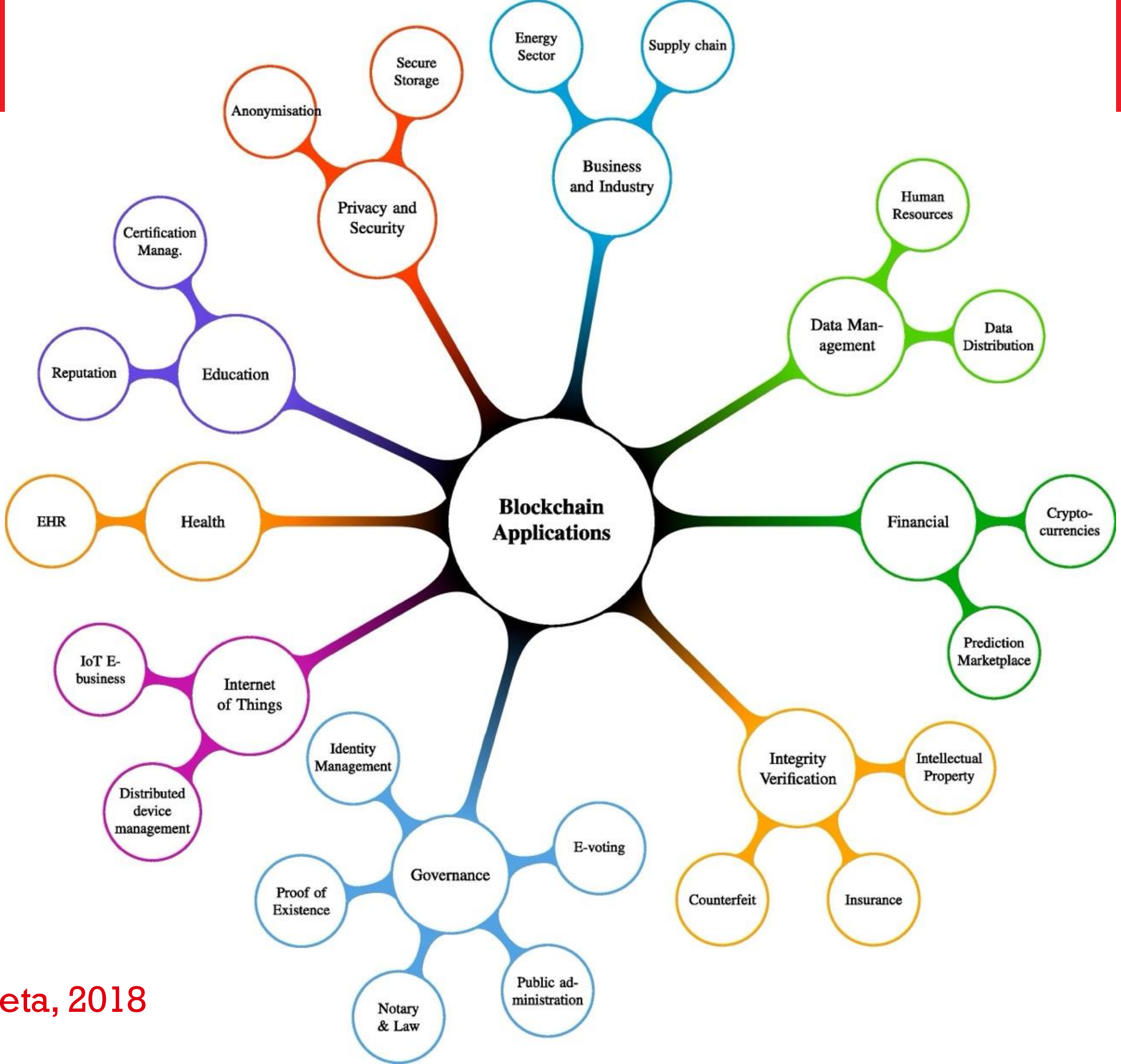
2020
NFT
DID

2021
Metaverse
IoT, Smart city

2022
Web 3.0
AI

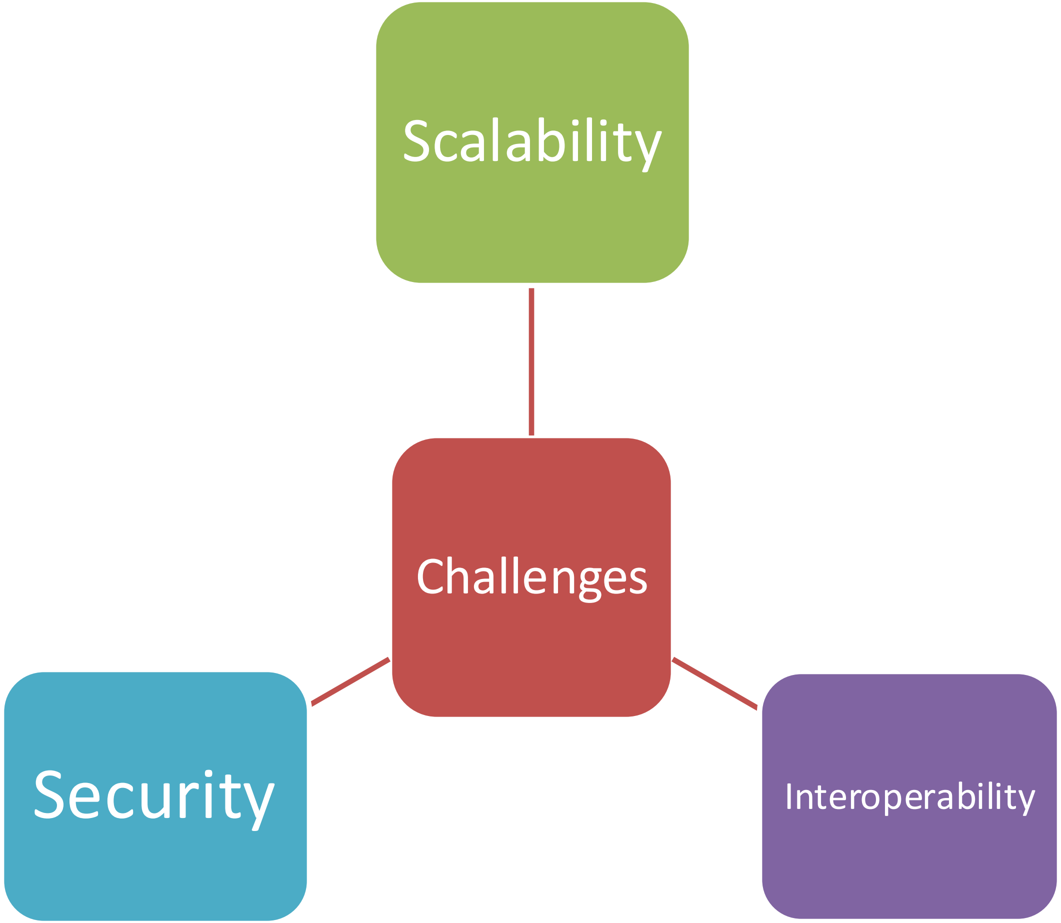
2025
Cyber Security
DPP

DeFi:	Decentralised Finance
NFT:	Non-Fungible Token
DID:	Decentralisedd Identity
IoT:	Internet of Things
AI:	Artificial Intelligence
DPP:	Digital Product Passport



Source: Fran Casino eta, 2018

Challenges in Blockchain Technology



Scalability

Challenges

Security

Interoperability

Attacks

- Denial of Service: overloading nodes with lots of transactions.
- 51% Attack: controlling more than 50% of nodes, can create fork longer than the main chain.
- Sybil attacks: when one node tries to represent multiple identities.
- Cryptographic attacks that break the underlying cryptography (Quantum).

The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application.

Each consensus algorithm has its own application scenario. There is no absolute good or bad. The choice of which consensus to use for implementing the blockchain depends on the type of network and data.

For a transaction to be valid on most cryptocurrency networks, the transaction needs to collect a certain number of confirmations (often equals to an inclusion in a block of a blockchain) from the network.

The CAP Theorem

States that in case of a partition, a distributed system can only preserve either consistency or availability.

CONSISTENCY
All clients see current data regardless of update/ delete

AVAILABILITY
system continue to operate even with node failures

CA

N/ A

CP

AP

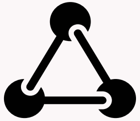
PARTITION TOLERANCE
the system continues to operate despite network failures

The trilemma

claims that blockchain systems can only at most have two of the following three properties

Decentralization

defined as the system being able to run in a scenario where each participant only has access to O(c) resources,



Scalability

defined as being able to process O(n) > O(c) transactions

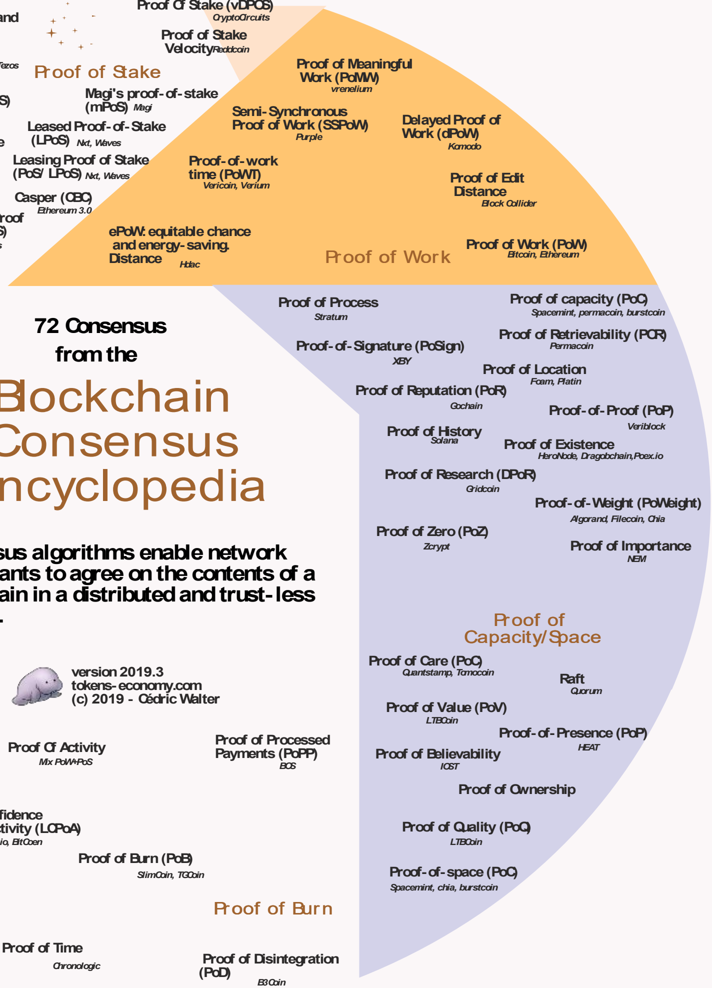
Security

defined as being secure against attackers with up to O(n) resources

72 Consensus from the Blockchain Consensus Encyclopedia

Consensus algorithms enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.

version 2019.3
tokens-economy.com
(c) 2019 - Cédric Walter



Proof of Stake

Variable Delayed Proof Of Stake (vDPOS) *CryptoCircuits*

Proof of Stake Velocity *Reddcoin*

Hybrid PBFT/ Aurand *Polkadot*

Proof of stake (PoS) *Ethereum, Nxt, Waves, Tezos*

Delegated proof-of-stake (DPoS) *Steemit, EOS, Bitshares*

Magi's proof-of-stake (mPoS) *Magi*

Leased Proof-of-Stake (LPoS) *Nxt, Waves*

Proof-of-Stake-Time (PoST) *PostCoin, Vericoin*

Leasing Proof of Stake (PoS/ LPoS) *Nxt, Waves*

Proof of stake Boo *Shield*

Casper (CBC) *Ethereum 3.0*

High Interest Proof of Stake (HiPoS) *EdgeCoin, GravityBits*

Tiered Proof Of Stake (TPOS) *XSN*

Casper (FFG) *Ethereum 2.0*

Proof of Work

Proof of Meaningful Work (PoMW) *vrenelium*

Semi-Synchronous Proof of Work (SSPoW) *Purple*

Delayed Proof of Work (dPoW) *Komodo*

Proof-of-work time (PoWT) *Vericoin, Verium*

Proof of Edit Distance *Block Collider*

ePoW: equitable chance and energy-saving. Distance *Hdac*

Proof of Work (PoW) *Bitcoin, Ethereum*

Proof of Capacity/Space

Proof of Process *Stratum*

Proof of capacity (PoC) *Spacemint, permacoin, burstcoin*

Proof-of-Signature (PoSign) *XBY*

Proof of Retrievability (POR) *Permacoin*

Proof of Location *Foam, Platin*

Proof of Reputation (PoR) *Gochain*

Proof-of-Proof (PoP) *Veriblock*

Proof of History *Solana*

Proof of Existence *HeroNode, Dragobchain,Poex.io*

Proof of Research (DPoR) *Gridcoin*

Proof-of-Weight (PoWeight) *Algorand, Filecoin, Chia*

Proof of Zero (PoZ) *Zcrypt*

Proof of Importance *NEM*

Proof of Care (PoC) *Quantstamp, Tomocoin*

Raft *Quorum*

Proof of Value (PoV) *LTBCoin*

Proof-of-Presence (PoP) *HEAT*

Proof of Believability *IOST*

Proof of Ownership

Proof of Quality (PoQ) *LTBCoin*

Proof-of-space (PoC) *Spacemint, chia, burstcoin*

DAG

Direct Acyclic Graph Tangle (DAG) *Iota*

Hashgraph *Hashgraph*

Block-lattice - Directed Acyclic Graphs (DAGs) *Nano*

BFT-based

Practical Byzantine Fault Tolerance *Hyperledger Fabric*

Federated Byzantine Agreement *Stellar, Ripple*

Delegated Byzantine Fault Tolerance *neo, byteBall*

Byzantine Fault Tolerance (BFT) *Dispath, Ripple*

asynchronous BFT protocol *HoneyBadgerBFT*

Modified Federated Byzantine Agreement (mFBA) *BOS*

Ouroboros *Cardano*

Hybrid models

Proof-of-Activity *Decred, Espers, Coinbureau*

Proof-of-authority (PoA) *Ethereum on azure*

Proof Of Activity *Mix PoW+PoS*

Proof Of Care (PoC) *Tamaguchi*

Limited Confidence Proof-of-Activity (LCPoA) *izzz.io, BitCoen*

High Interest Proof of Stake *EdgeCoin*

Proof of Processed Payments (PoPP)

Proof of Burn

Proof of Processed Payments (PoPP) *BOS*

Proof of Burn (PoB) *SlimCoin, TGCoin*

Proof of Time *Chronologic*

Proof of Disintegration (PoD) *B3Coin*

Legends

Stakeholders are those having coins or smart contracts on the blockchain. Only they can participate. Those with high stakes are chosen to validate new blocks.

Each participant on the network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or proof, to a specific computational challenge.

Proof-of-space, also called Proof-of-capacity, is a means of showing that one has a legitimate interest in a service by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.

Participants should show proof that they burned someething (coin, time,..) - e.g for a coin that they are sent to a verifiably unspendable address.

Most of the time a combination of existing consensus algorithm, e.g PoW+PoS but not always...

Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. ... and work as long as the number of traitors do not exceed one third of the generals.

In order to send a new transaction, you need to validate two previous transactions you're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.

SUMMARY

- We have learned:
  - An overall Introduction
  - Identified the Core Concepts & Mechanisms
  - Got a Basic Idea about Bitcoin Protocol
  - Compared Blockchain & DLT
  - Potential Applications of Blockchain

Next Week..

- Fundamental Mechanisms of DLT

Q&A