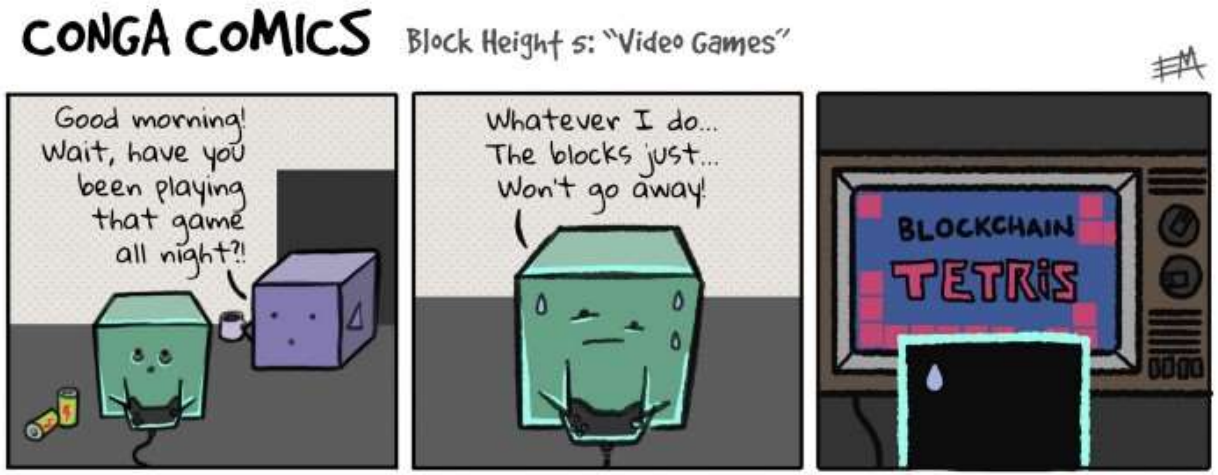
Cybersecurity Management
GCS 2.4 – Blockchain

2023-2024

Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu



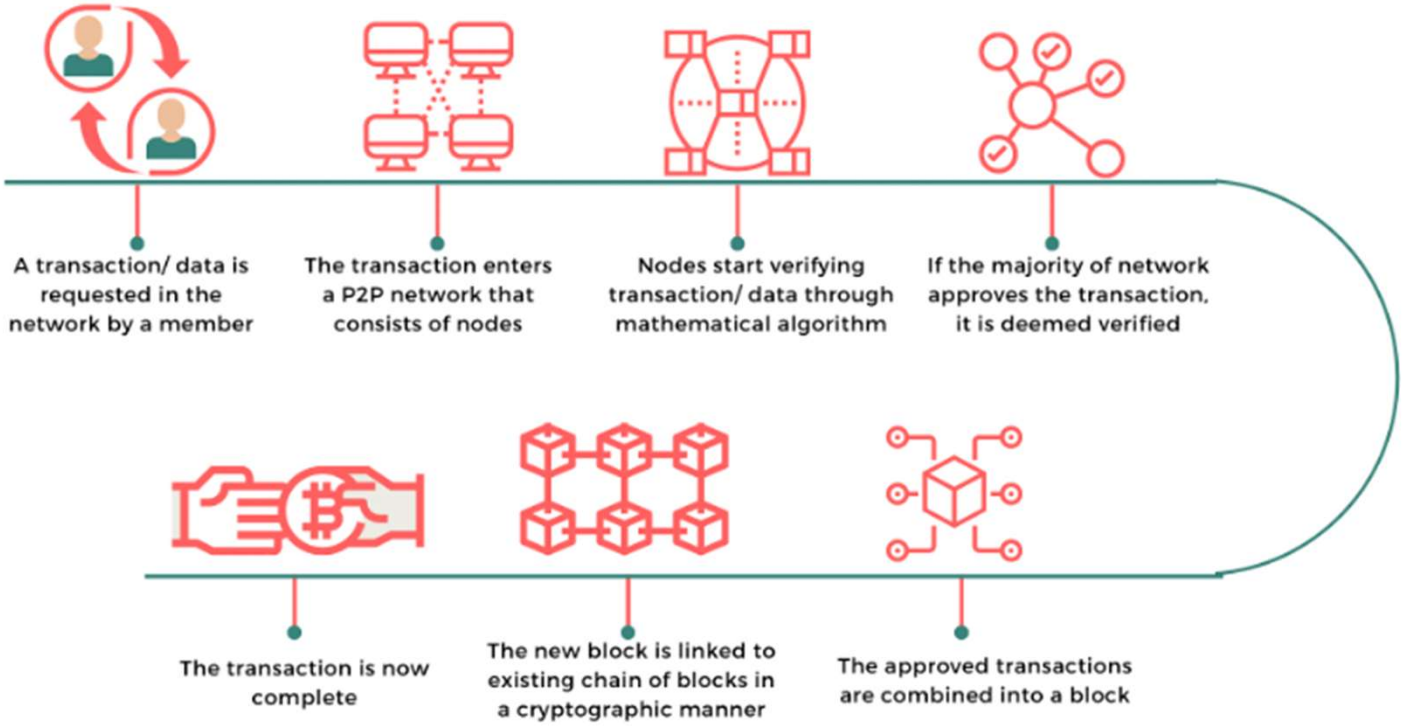
Blockchain 101

Definition

- Distributed and immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
  - Tangible assets: houses, cars, cash, land
  - Intangible assets: intellectual property, patents, copyrights, branding
- Blockchain is a unique system that allows the storing of data in a way that it becomes nearly impossible to tamper the existing data or cheat the system.

Source: IBM

How it works?



Source: https://freemanlaw.com

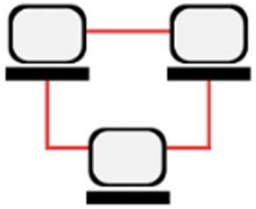
Main features

DECENTRALIZED

- The control/ power is not held by a single entity. Instead it is distributed among multiple participants.
- Even if one node is corrupted/ fails, the network repairs itself.

PEER TO PEER

- Direct peer to peer transaction of data or finance.
- Decentralized nature of blockchain instills trust in the process such that two unknown parties can directly interact/ transact with each other



DISTRIBUTED

- Data is distributed among the nodes(computers/ hard drives).
- Even if one node is tampered, the data does not get compromised.

Source: https://freemanlaw.com

Some use cases

- **Cryptocurrencies**
  - Blockchain originally designed to manage digital currencies like bitcoin. Given the anonymity of crypto coins, blockchain is the only way to keep track of transactions with accuracy and privacy for all parties concerned
- **Protection against money laundering**
  - The encryption that is crucial to the blockchain once again comes in handy when fighting money laundering
- **Trade finance**
  - Blockchain can digitize trade finance to make it more efficient, transparent, simple, affordable, and robust
- **Supply chain transparency**
  - Customers may have complete insight and transparency into the items they purchase using a blockchain-based technology that tracks items from the manufacturing point through the supply chain

Some use cases

- **Smart contracts**
  - Computer protocols that execute the terms of an agreement between peers without the need for third-party verification or approval
- **IoT**
  - Include supply chain management, asset tracking, and keep track of machine readings taken worldwide
- **Healthcare**
  - Managing electronic medical record data, preserving health information, safeguarding information, and monitoring disease and epidemics
- **Art**
  - Non-fungible tokens (NFTs) have enabled the creation of crypto art.
- **Gaming**
  - Offers new possibilities such as genuine asset ownership, consensus-driven updates, decentralized marketplaces, simplified tokens

Some use cases

- **Energy**
  - metering, billing, clearing procedures, asset management, origin guarantees, emission allowances, and renewable energy certificates
- **AI**
  - Immutability and the fact that every computer continuously verifies information on the network make it an ideal solution for big data
- **Electronic voting**
  - The government could tally votes more efficiently and effectively because each vote would be attributed to one ID
- **Security**
  - Self-sovereign identity, secure data transmission, private messaging
- **Cybersecurity**
  - Because of inherent and intrinsic Blockchain features

Key elements

- **Distributed ledger (DLT)**
  - Is the consensus of replicated, shared, and synchronized digital data that is geographically spread (distributed) across many sites, countries, or institutions.
  - Does not require a central administrator
  - Does not have a single (central) point-of-failure
- **Immutable records**
  - Once the transaction is recorded in the ledger, there's no way any blockchain participant can tamper with the data or make changes.
  - In case the transaction records an error, a new transaction must be added to reverse and eliminate the error
- **Smart contracts**
  - Set of rules stored in blockchain, which is automated.
  - This contract involves information like terms for travel insurance, conditions for corporate bond transfers, and so on.

Benefits

- **Greater Trust**
  - Data is 100% confidential in the blockchain records, that will only be shared with members the account holder grants permission to
- **Decentralised Structure**
  - No third-party involved or intermediaries included
- **Maximum Security**
  - Blockchain builds an unaltered ledger with end-to-end encryption.
  - The data is never stored in a single computer; eliminating the chances of unauthorized activities such as hacking
- **Reduced Cost**
  - Due to decentralisation

Benefits

- **Speed**
  - No intermediaries and fewer manual interventions, much faster and more reliable transactions
- **Individual Control Of Data**
  - Individuals and institutions have the power to decide with whom and for how long they want to share a piece of information or want to keep it confidential
- **Visibility And Traceability**
  - Manage inventory, confirm the history, respond to problems within time. Blockchain can easily track the origins of various items
- **Immutability**
  - Once the transaction is recorded on the blockchain, there is no way it can be changed or removed or tampered with.

Blockchain network types

- **Public**
  - Anyone can join and participate in, e.g. Bitcoin.
  - Substantial computational power required, little or no privacy for transactions, and weak security.
- **Private**
  - One organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger.
  - Significantly boost trust and confidence between participants

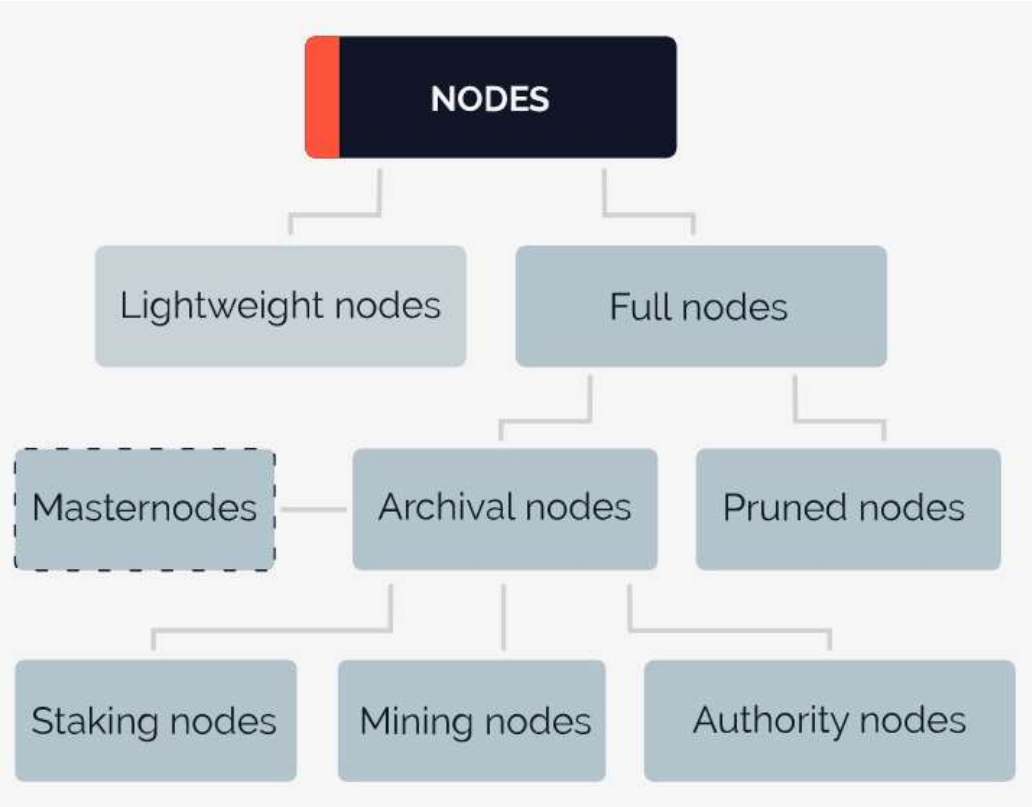
Blockchain network types

- **Permissioned**
  - Private blockchain will generally set up a permissioned blockchain network (also public can be)
  - Places restrictions on who is allowed to participate in the network and in what transactions.
  - Participants need to obtain an invitation or permission to join.

- **Consortium blockchains**
  - Multiple organizations can share the responsibilities of maintaining a blockchain.
  - Ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

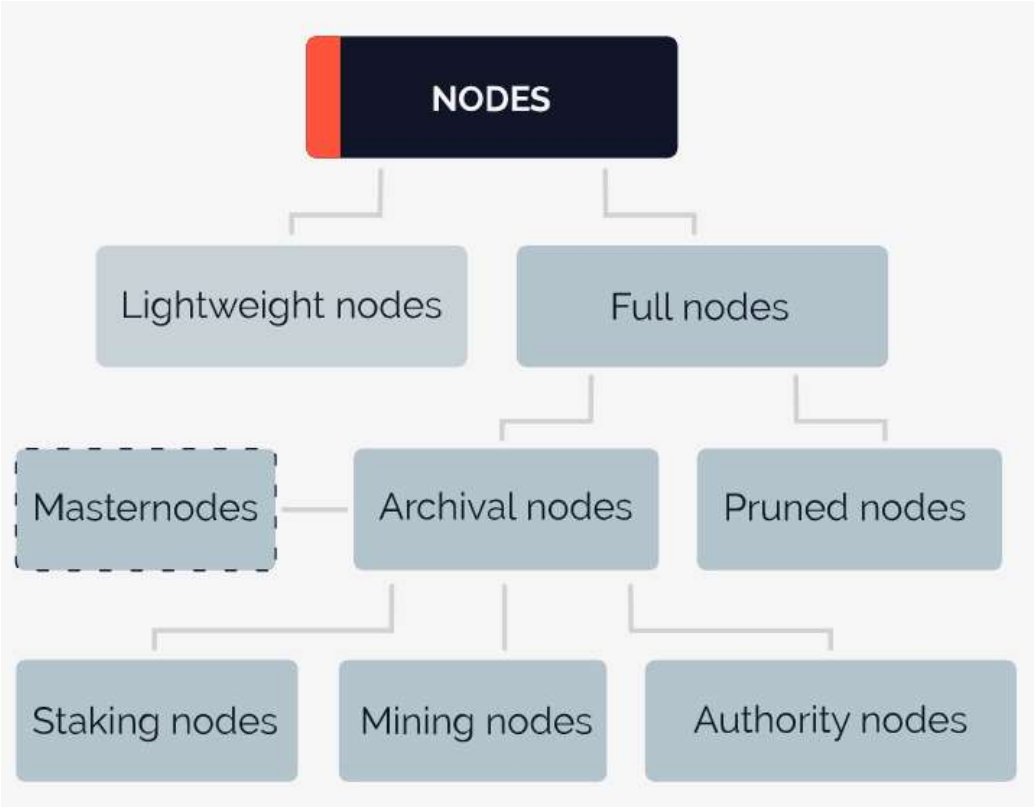
Types of nodes

- **Full node**
  - Act as Servers
  - Preserve a blockchain's transaction history, sync, store, copy and distribute data while also validating new blocks
  - Can be "pruned" (contain metadata of all blocks + only recent blocks) or "archival" (contain the entire blockchain ledger)



Types of nodes

- **Authority nodes**
  - Act as Moderators of a private or partially centralized blockchain.
- **Mining nodes**
  - Verify transactions using a proof-of-work consensus model unlock tokens and add new blocks to a blockchain.
  - Miners are computers, typically working in a group, that are owned by an entity, such as an individual or company
- **Master Nodes**
  - Validate transactions and maintain records. They do not generate new blocks.

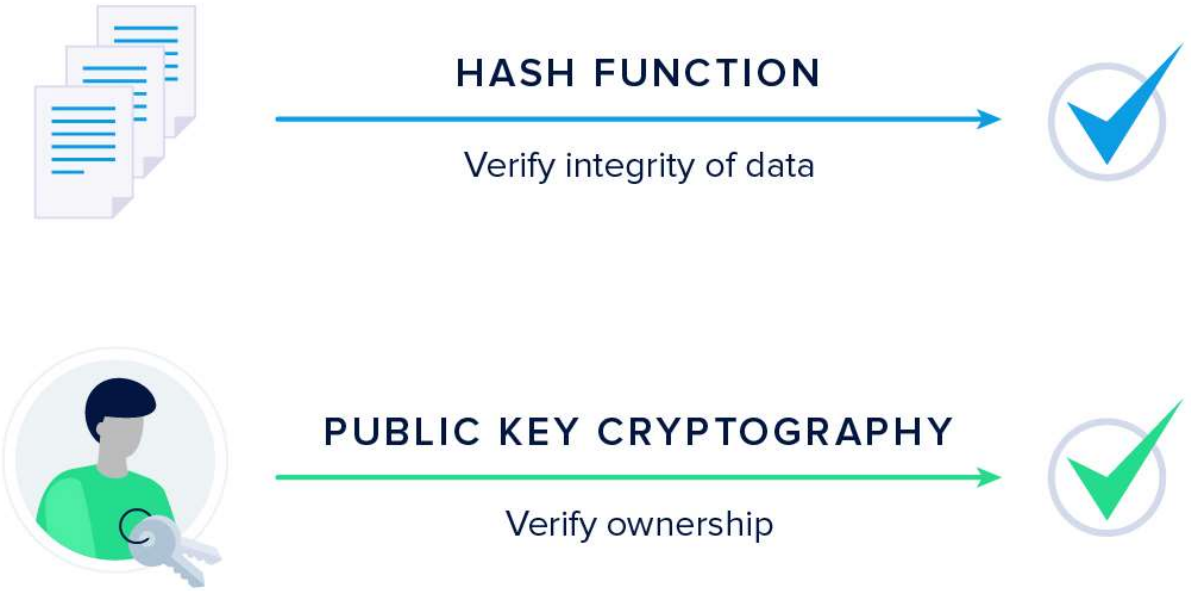


Platforms

- IBM Blockchain Platform
  - https://www.ibm.com/products/blockchain-platform/demos/build-your-blockchain-network/now-any-developer-can-become-a-blockchain-developer
- Ethereum
  - https://ethereum.org/en/learn/
- Hyperledger
  - https://www.hyperledger.org/use/tools

Blockchain Security

Cornerstones

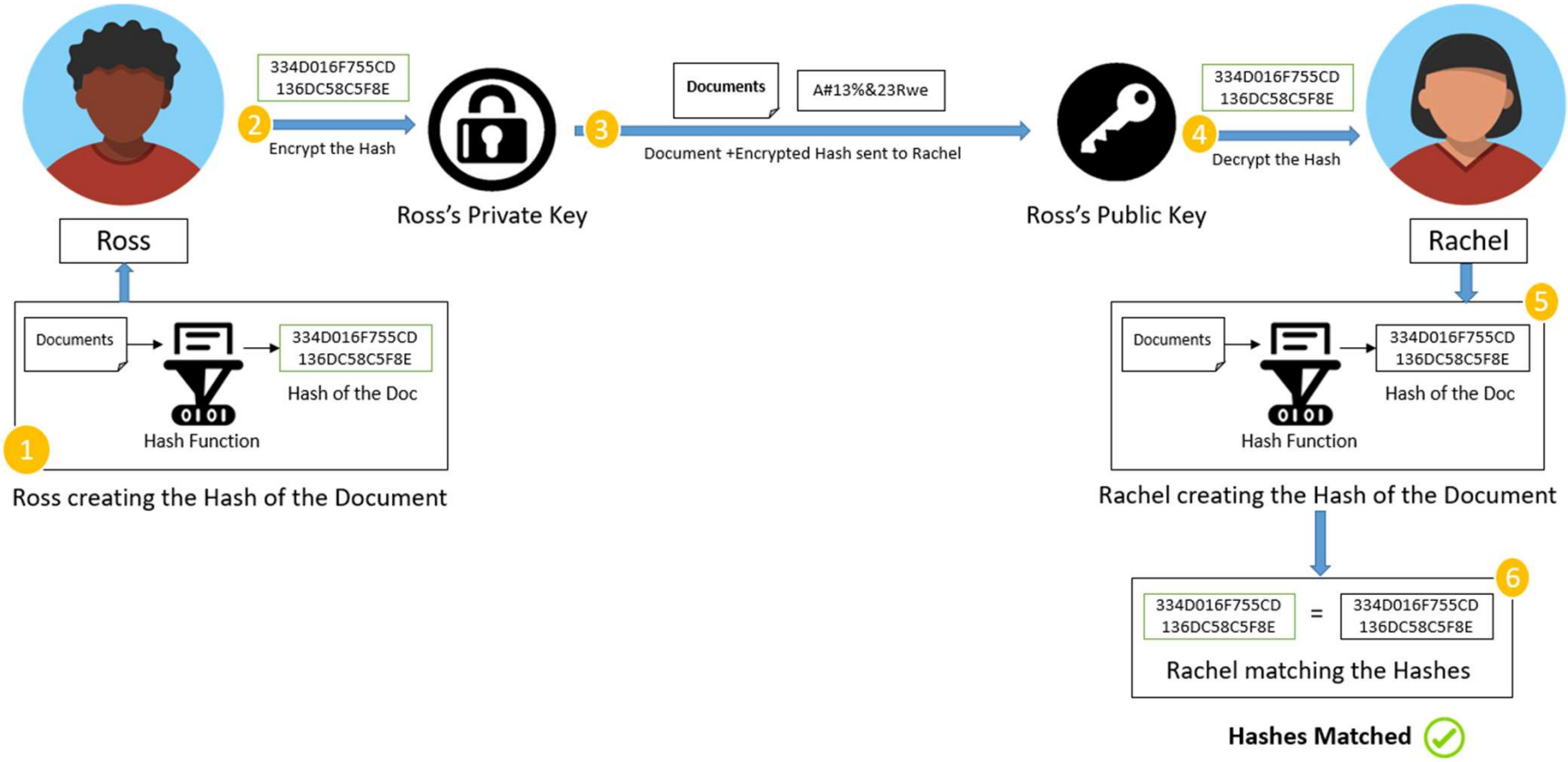


Source: https://www.horizen.io/

Public Key Cryptography

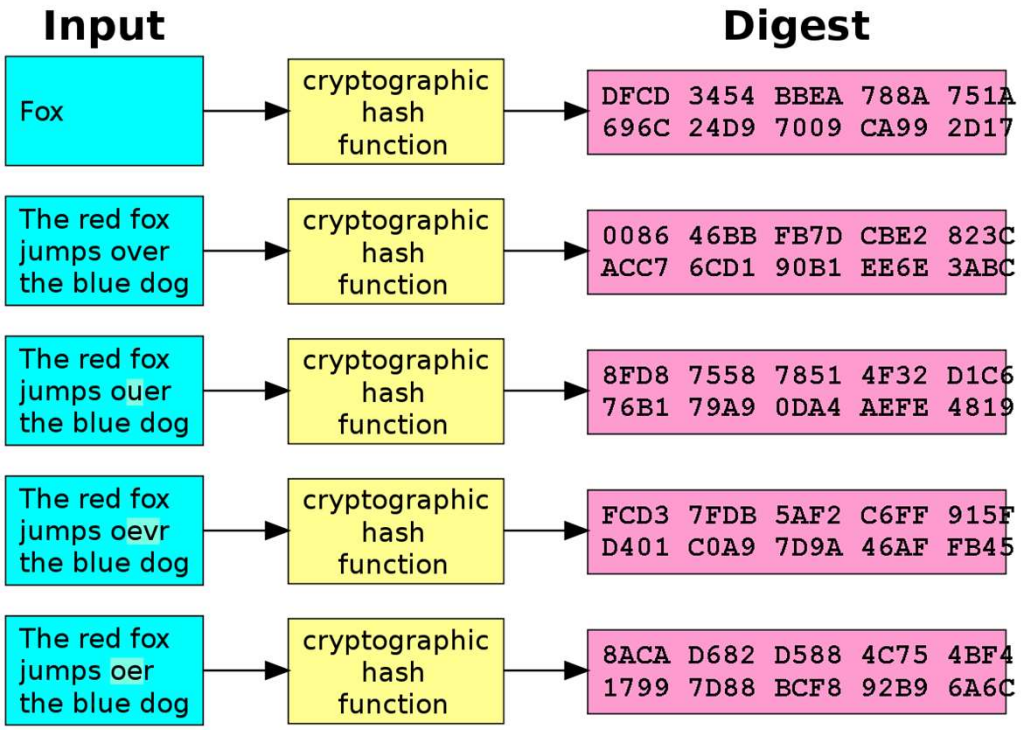
- Asymmetric cryptography, to verify ownership.
- Every user creates two keys when he/she joins the network: a public, and a private key.
- Public key -> “address” -> shared, known between peers
- Private key -> “password” -> never leave from owner
- Elliptic Curve Cryptography is widely used

Digital Signature



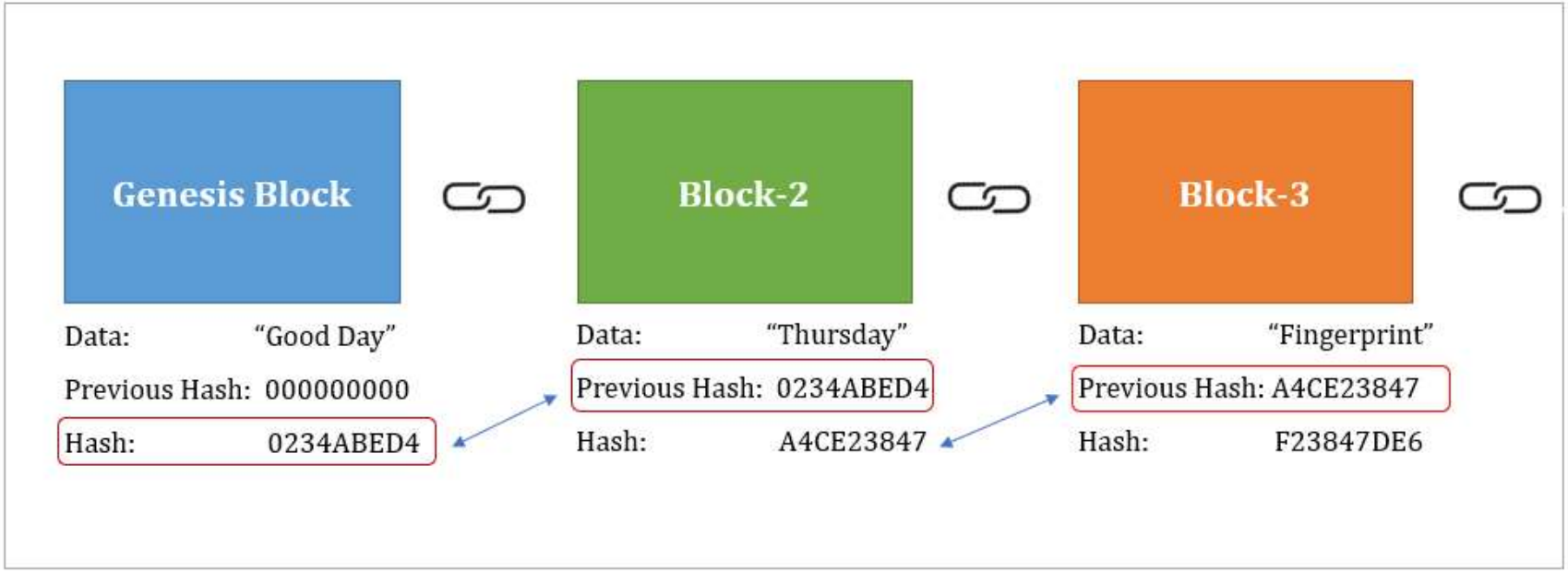
Hash Function

- Transform a variable size input message into a fixed size output hash (digest)
- Deterministic : one input -> same hash
- Two different message do not have same hash
- Quick to compute and infeasible to reverse the process
- Small change in the message change drastically hash (avalanche effect)



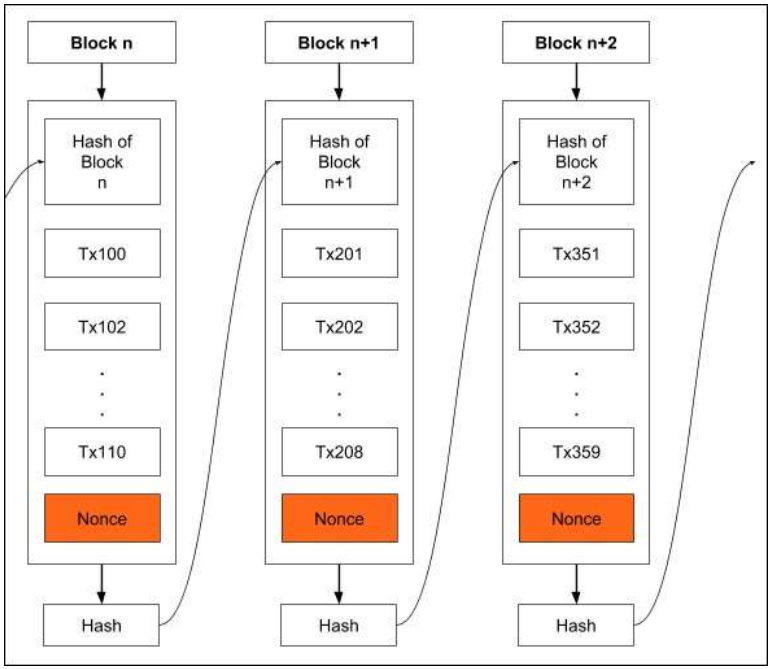
Hashing in block chain

- Basic cryptographic technique used in blockchain
  - SHA256 algorithm: https://sha256algorithm.com/
- Fingerprint of transactions/blocks added in a chain
- Allow easily checking if something has been changed in the transactions history.



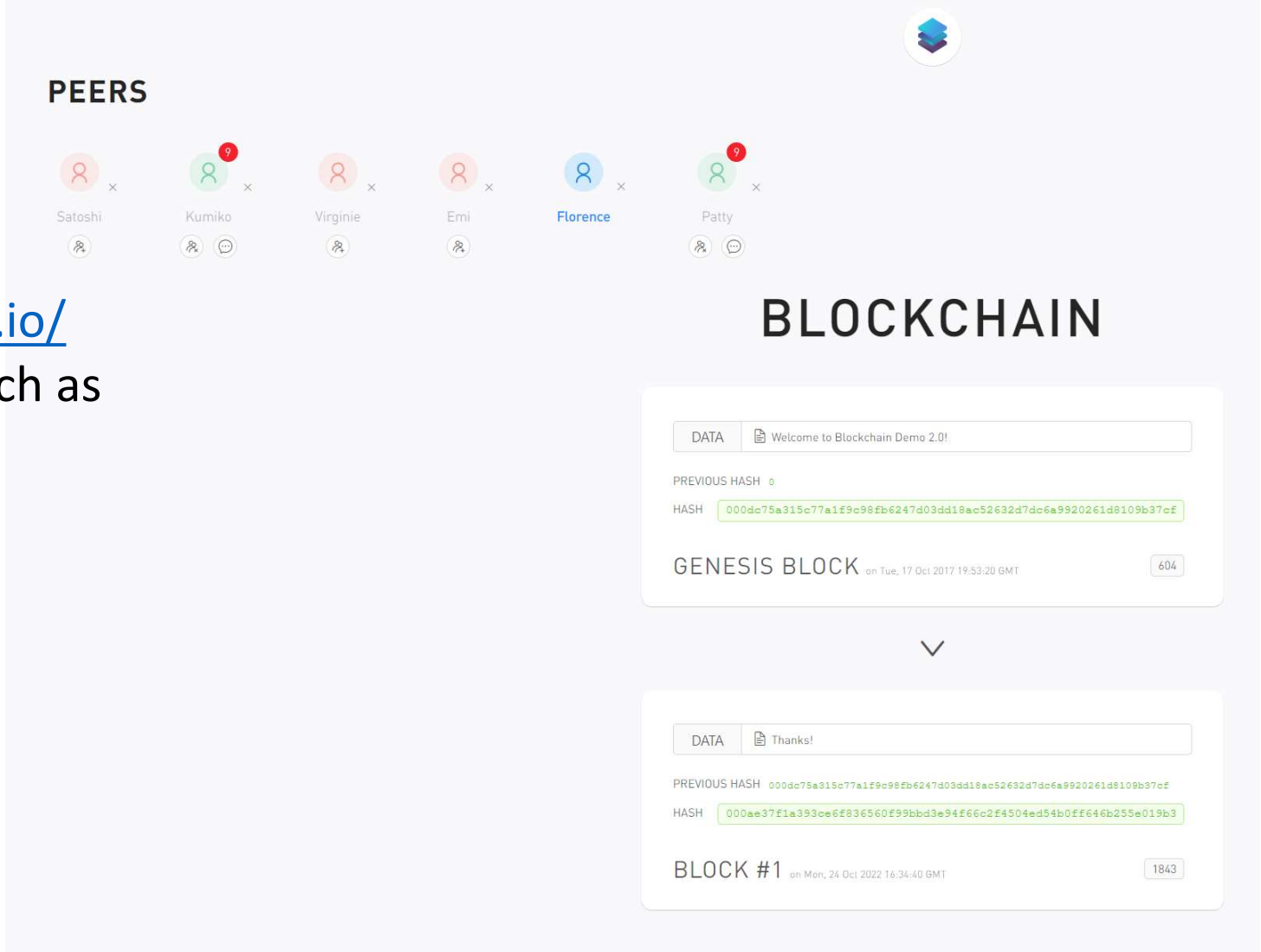
Valid blocks

- Setting an arbitrary number of consecutive zeros is a proof of validation, i.e., the block is signed.
  - Part of the contract
- A “nonce” (number user only once) needs to be appended to transactions in order to obtain hash messages with the target number of zeros
- Mining nodes are responsible of finding the nonce that accomplishes



Demos

- https://blockchaindemo.io/
- Useful to fix concepts such as hashing, avalanches, …



Exercise 1: Follow the guided demo

Exercise 2: Watch this video…very clever!

https://youtu.be/_160oMzblY8

Common Attacks

- **Phishing**
- **Sybil Attack**
  - Manipulate P2P networks creating multiple fake identities
  - A single entity controls all these fake entities (impact on voting)
- **51% attack** (endemic attack)
  - If a participant has more than 51% of the network, he could out-mine the network and hack the blockchain.
  - More miners in the network -> more distributed -> no one has majority power.
- Other attacks:
  - Byzantine Generals Problem
  - DDOS

Exercise 3: Lightreading “Attacks on blockchain”

https://www.horizen.io/blockchain-academy/technology/advanced/attacks-on-blockchain/

Good Practices

- **Governance specific to blockchain.**
  - Determine how new users or organizations join or leave the network
  - Enable mechanisms to remove bad actors, manage errors, protect data and address conflicts between parties
- **Data security**
  - Data minimization is a general best practice for determining what data is stored on-chain
  - Additional security measures should be applied to sidechains (off chain), hash data, data in transit, cloud storage
- **Network security**
  - Network connections from multiple parties beyond a single corporate network must interact, including IT and networking infrastructure, databases, servers and more, all of which introduce potential for security flaws or exploits

Good Practices

- **Application security**
  - Critical point of vulnerability (access to the blockchain)
  - Need strong user authentication and endpoint protections
- **Smart contracts security**
  - Another point of vulnerability because their integrity determines the reliability of the operation and trustworthiness of the results
- **Interoperability**
  - How data, identities and interactions occur across networks, applications and smart contracts at scale
  - Threats increase as interfaces and systems complexity expand
- **Use of trusted auditors and third parties**
  - Security assessments, penetration tests, and audits of smart contracts, source code and blockchain infrastructure should only be conducted by trusted parties

ENISA & Blockchain

- **Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies**
  - **Released February 2021**
  - This report aims to increase the understanding of blockchain technologies. It aims to explain the underlying technical concepts and how they relate to each other.
  - The goal is to explain the components, and illustrate their use by pointing to deployed instances where the ideas are utilized.

https://www.enisa.europa.eu/publications/crypto-assets-introduction-to-digital-currencies-and-distributed-ledger-technologies

References

- https://www.ibm.com/topics/what-is-blockchain
- https://www.horizen.io/blockchain-academy/technology/advanced/
- Blockchain 101: A visual demo
  - https://www.youtube.com/watch?v=_160oMzblY8
- https://www.infosys.com/insights/cyber-security/cybersecurity-blockchain.html

Cybersecurity Management
GCS 2.4 – Blockchain

2023-2024

Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu