FACULTY OF AUTOMATIC CONTROL AND COMPUTERS

POLITEHNICA BUCUREȘTI 1818

Session 03
Bitcoin

Blockchain Protocols and Decentralized Applications

Evolution of Ledgers

timestamped
append-only log

auditable database

Secured via cryptography
- Hash functions for **tamper resistance** and **integrity**
- Digital signatures for **consent**

Consensus for **agreement**

network consensus protocol

Addresses '**cost of trust**' (Byzantine Generals problem)
- Permissioned
- Permissionless

Discussions

- Paper: https://bitcoin.org/bitcoin.pdf
- Hashing
- Cryptography
- Signatures
- Timestamped Append-only Logs (Blocks)
- Merkle Trees
- Consensus through Proof of Work
- Network of Nodes
- Bitcoin

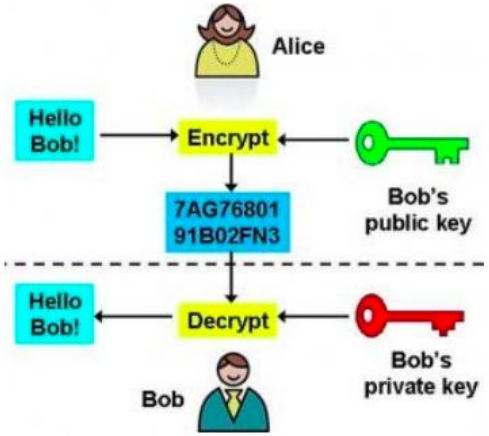
Cryptography

- Communication in presence of adversaries

Scytale Cipher
Ancient Times

Enigma Machine
1920s - WWII

Image by the CIA and is in the public domain via Wikimedia Commons.



Asymmetric Cryptography
1976 to today

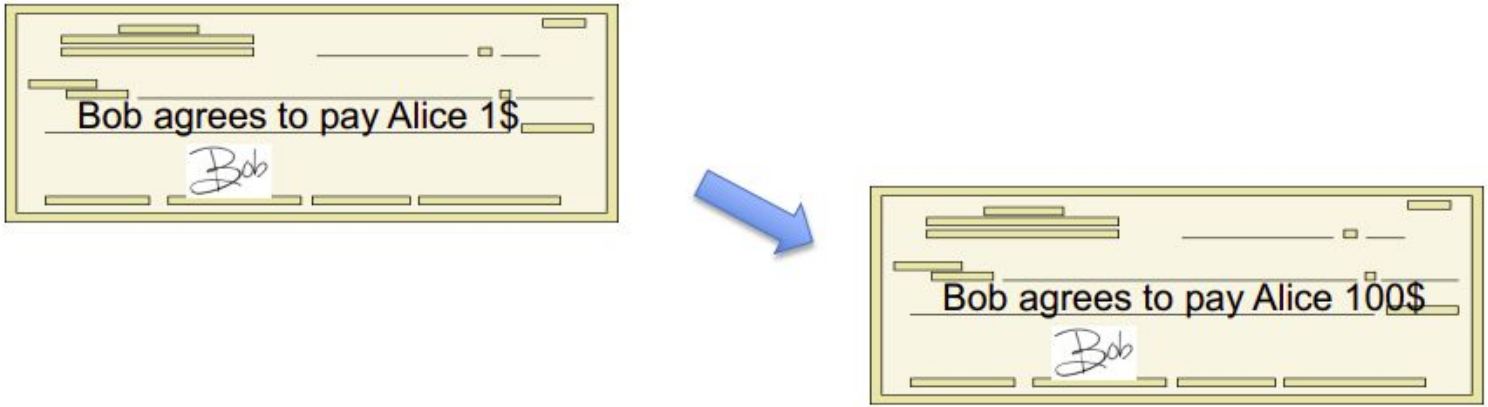
Image is in the public domain via Wikipedia.

Cryptographic Hash functions

- Maps any data (from one string to an entire hard disk) to an Output called “HASH” with fixed size
- Properties
  - Deterministic - same result every time
  - Efficient - fast computation
  - Preimage resistant (One way): infeasible to determine x from Hash(x)
  - Collision resistant: infeasible to find and x and y where Hash(x) = Hash(y)
  - Avalanche effect: Change x slightly and Hash(x) changes significantly
- Used in blocks, addresses

Signatures

- Physical signatures: bind transaction to author
- Problem in the digital world
  - anyone can copy Bob's signature from one doc to another



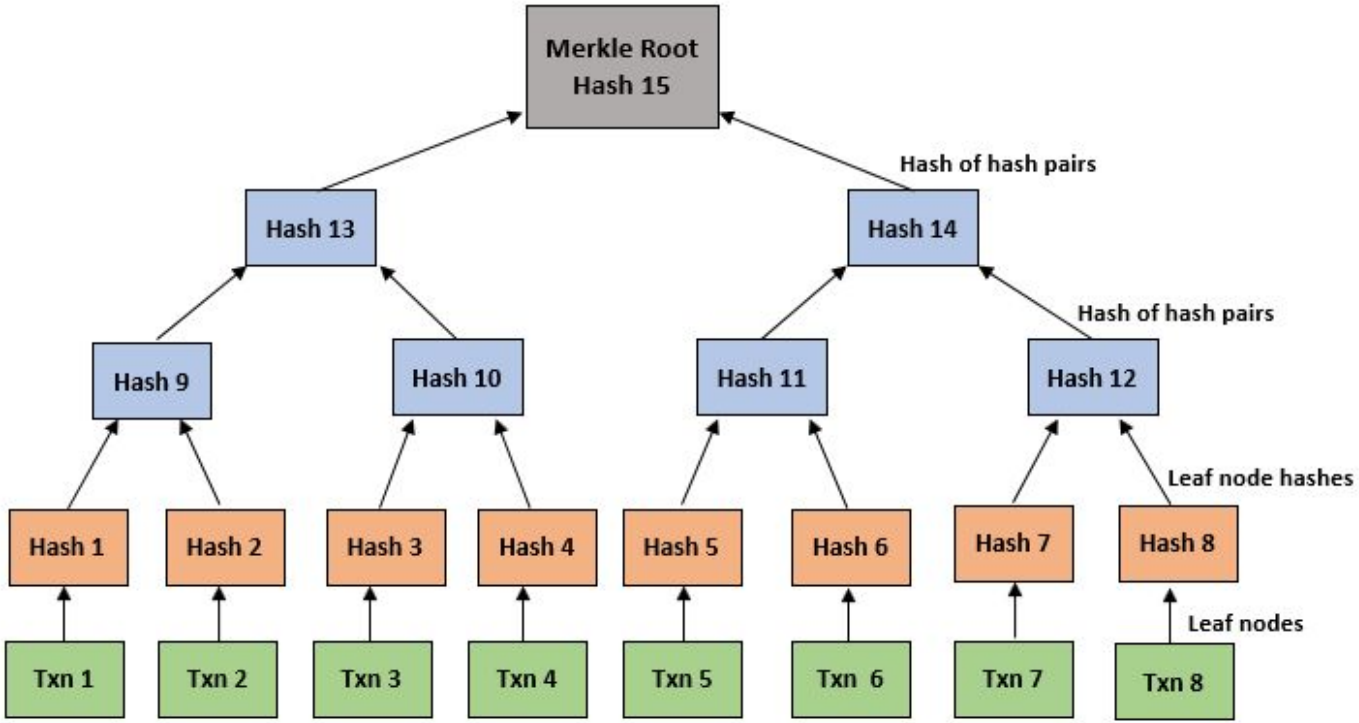
Digital Signatures

- Prove that **private key** match **public key**

Digital Signatures (2)

- RSA
- DSA
- Elliptic Curve Digital Signature Algorithm (EDCSA) - Bitcoin
    - significantly shorter private and public keys to achieve the same level of security

Merkle Trie



https://arxiv.org/abs/2209.13431

Bitcoin

- Electronic cash
- Online payments
- No financial institution
- Prevent double-spending
  - Using peer-to-peer
- Proof-of-work
- Nodes can leave and rejoin the network
- Whitepaper

Whitepaper discussions