BLOCKCHAIN AND BITCOIN BASICS

FRIDAY MAR 23 2018, 12:00

IMORPHEUS.AI

BLOCKCHAIN OVERVIEW

A blockchain is a continuously growing list of records, which are linked and secured using cryptography.

- Decentralized, distributed digital ledger open to public
- Peer-to-peer network and distributed timestamping server
- Recorded transitions are very difficult to alter retroactively
- Authenticated by mass collaboration
- Removes infinite reproducibility of digital asset (double spending) in decentralized setting
- Used as value exchange protocol

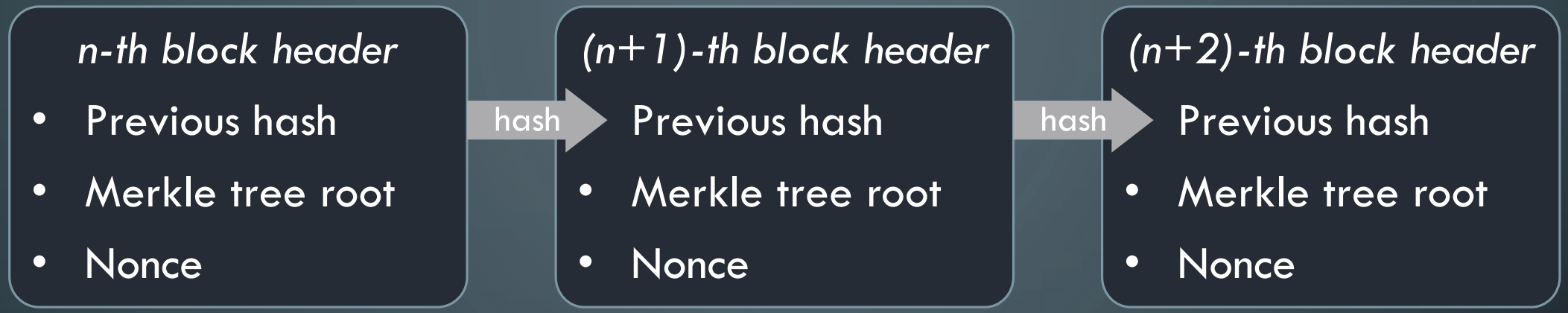
BITCOIN OVERVIEW

iMorpheus.ai

Bitcoin is a decentralized cryptocurrency and the first and best-known implementation of blockchain. It was invented by Satoshi Nakamoto.

- Bitcoin wallet uses asymmetric cryptography
- Transactions are authenticated by digital signature
- Blocks store transactions about every 10 minutes
- Network nodes compete to generate new blocks via proof of work
- Rewards for block generator are “free” bitcoins and transaction fee
- Total bitcoin circulation will be 21 million, currently about 17 million for a market capitalization of about 100-200 billion USD

BITCOIN BLOCK STRUCTURE



- Past: previous hash is compressed information of previous block
- Current: Merkle tree stores transactions in the current block
- Future: nonce is a the random number for proof of work
- Blocks are linked by cryptographic hash function in such a way that any change in one block will cause validation of following blocks to fail
- The longest chain agreed by the majority of nodes hold a complete history of all transactions

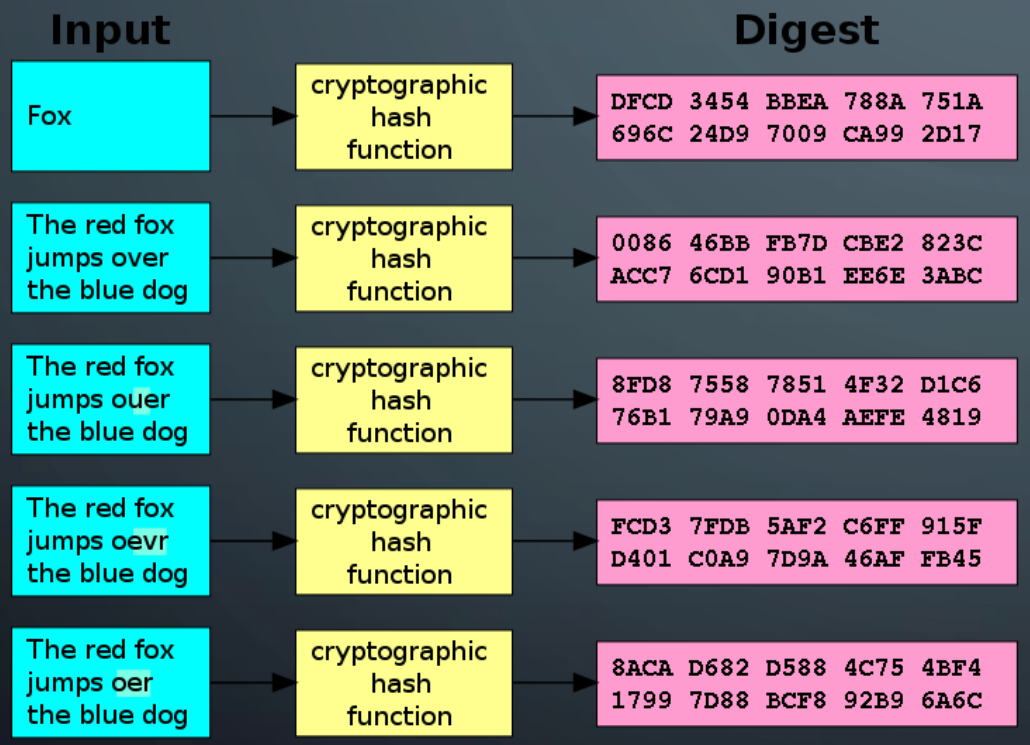
BITCOIN NETWORK

Nodes in Bitcoin run the following steps:

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. Each node works on finding a nonce (proof of work) for its block
4. When a mode finds a nonce, it broadcasts the complete block to all nodes
5. Other nodes verify the result by checking that all transactions are valid and that the calculated nonce gives hash value that satisfies certain condition
6. Nodes express their acceptance by working on creating the next block in the chain, using the hash of accepted block as previous hash

CRYPTOGRAPHIC HASH FUNCTION

A hash function maps data of arbitrary size to data of fixed size. A cryptographic hash function is a special hash function with certain properties.

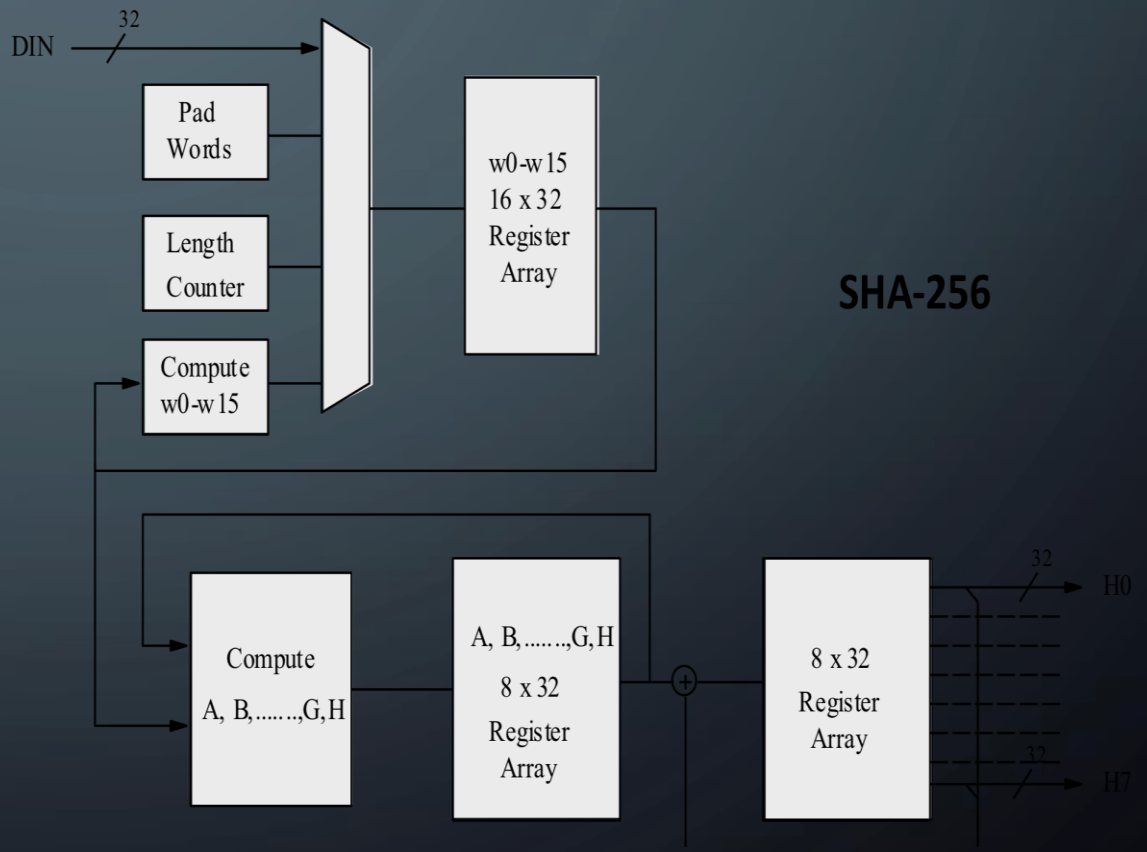


- Deterministic and quick to compute
- Infeasible to invert except by brute force attack (trying all inputs)
- Infeasible to find two different messages with the same hash value
- Small change to message makes unpredictable change in output

SECURE HASH ALGORITHM (SHA)

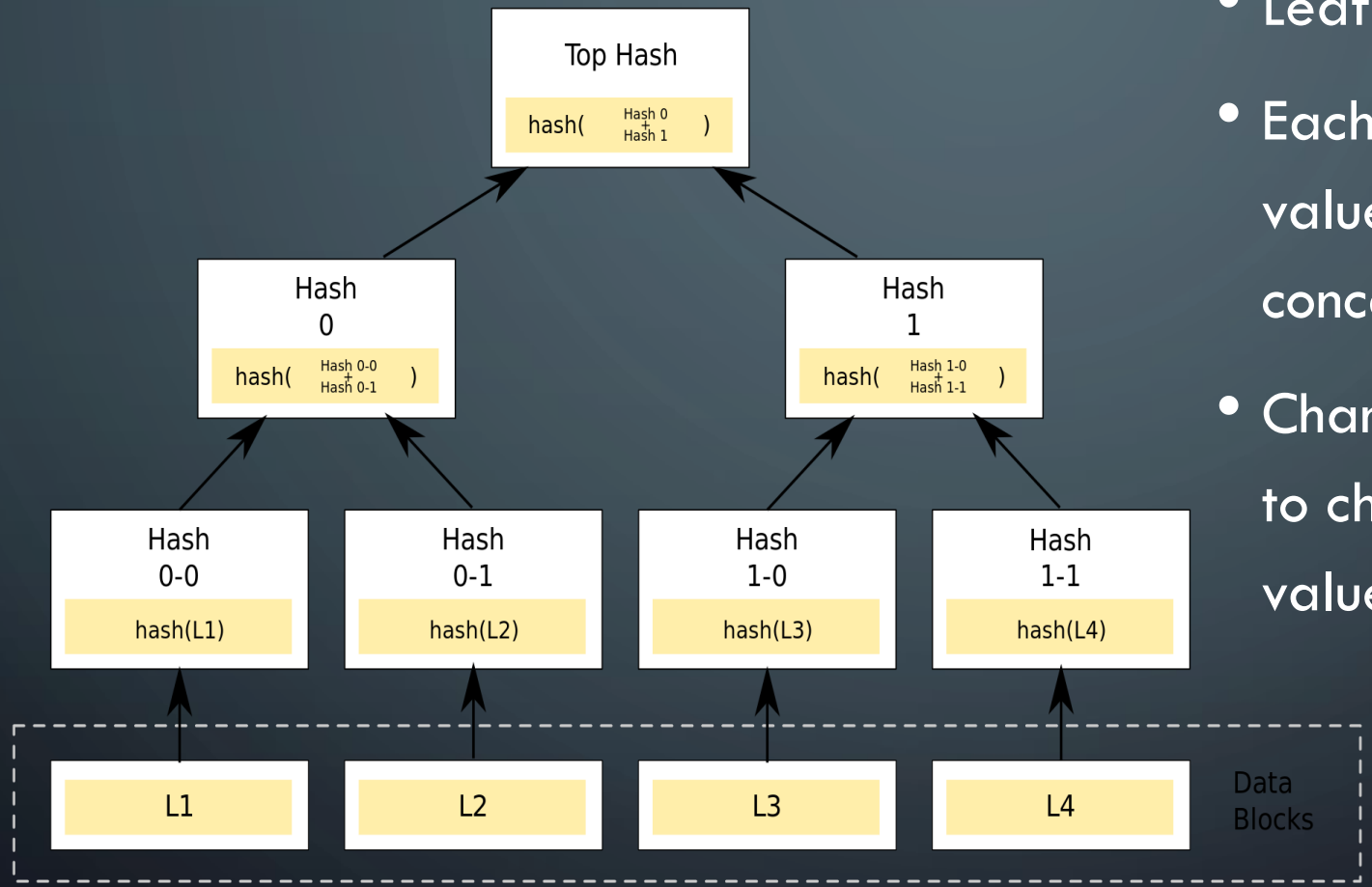
A family of cryptographic hash functions published by National Institute of Standards and Technology, designed by National Security Agency.

- SHA-2 is widely used, including bitcoin (SHA-256)
- Maps message of maximum size $(2^{64} - 1)$ bits into 256-bit digest, using simple bit operations
- Padding → blocks → initial hash value → loop rounds → result



SHA-256

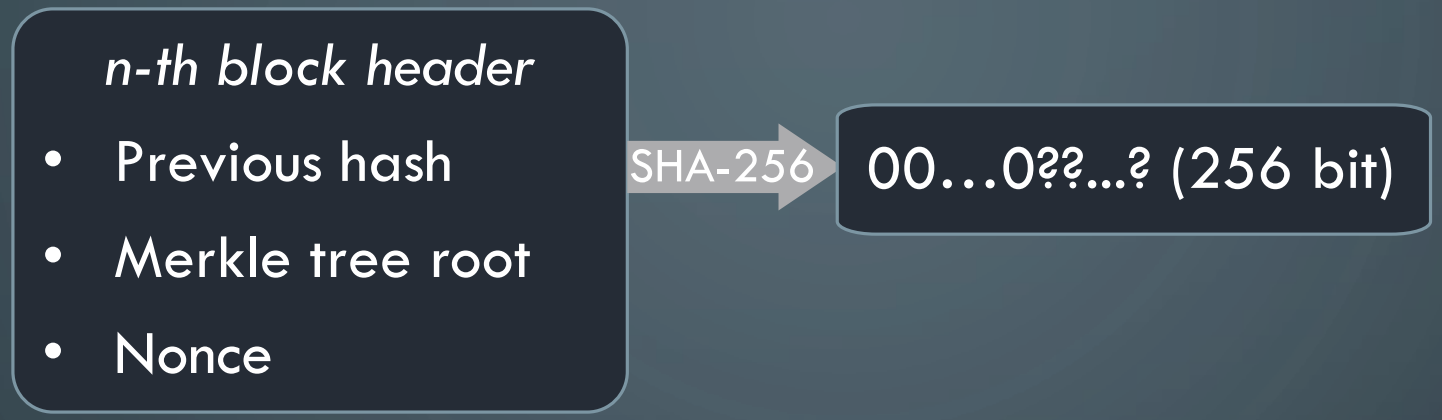
MERKLE TREE



- Leaf nodes are data blocks
- Each non-leaf node is hash value of its child nodes by concatenation
- Change in any data will lead to chain of change in hash value up to root

iMorpheus.ai

PROOF OF WORK



- To generate a new block, each node competes to find a random number (nonce) such that the block hash value (256 bit) starts with a bunch of 0
- The difficulty of this partial hash inversion problem is controlled by number of zeros required (difficulty target), which is adjusted every 2016 blocks so that blocks are generated once every ten minutes on average
- Every node can quickly verify whether the problem (nonce) has been solved

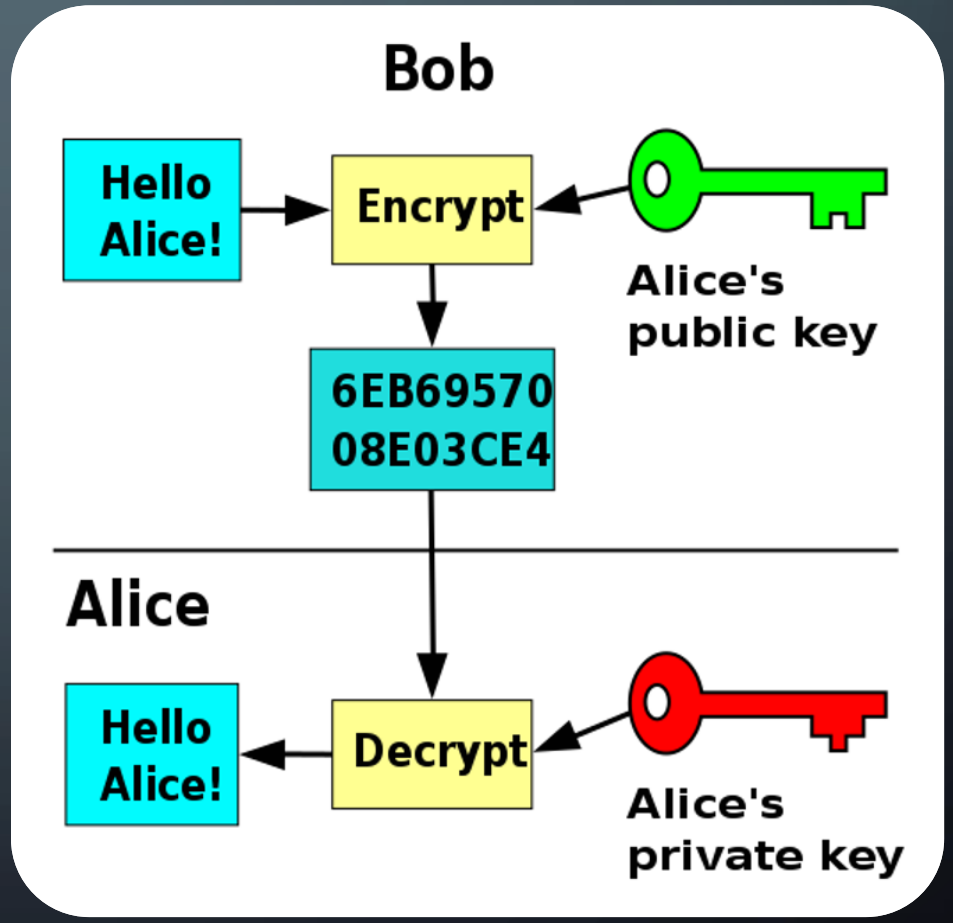
MINING

For each successful block mined, reward of certain amount of newly created bitcoin is added to miner. The reward is halved every 210,000 blocks (about four years), currently 12.5 bitcoins. This gives incentive to mining as well as keeps a steady flow of new bitcoins into circulation, much like gold mining.

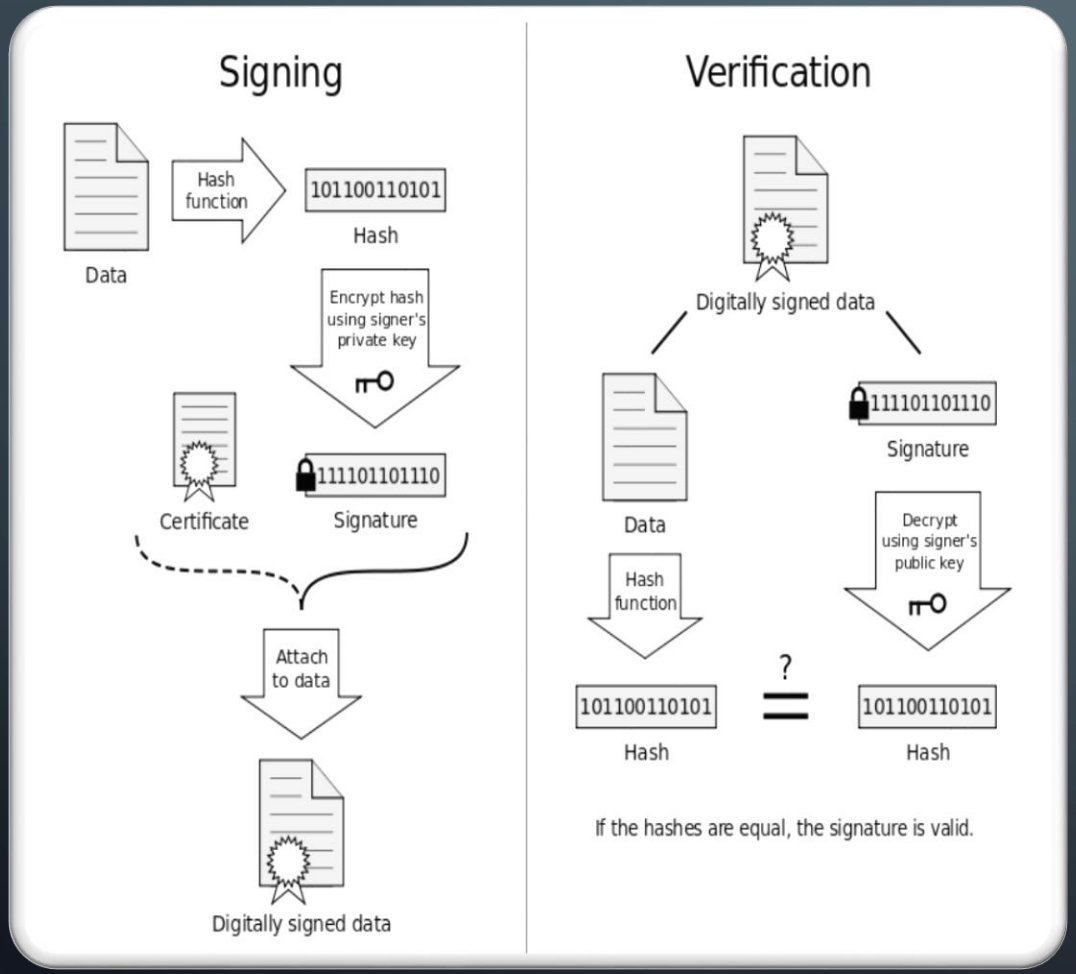
Miners use processing power to keep blockchain running. It was intended by Satoshi that distributed CPU power will help decentralize bitcoin system. Now most processing power comes from specifically built mining pools with many ASICs that consumes huge amount of electricity.

ASYMMETRIC CRYPTOGRAPHY

- A pair of keys (parameter for encryption and decryption algorithms) that are mathematically bounded:
  - Public key is open to every one
  - Private key is only known to the owner
- Information can be encrypted by public key and decrypted by private key, and vice versa
- Two major applications
  - Public key encryption: Bob encrypts a message by Alice's private key; only Alice can decrypt this message using her private key
  - Digital signature

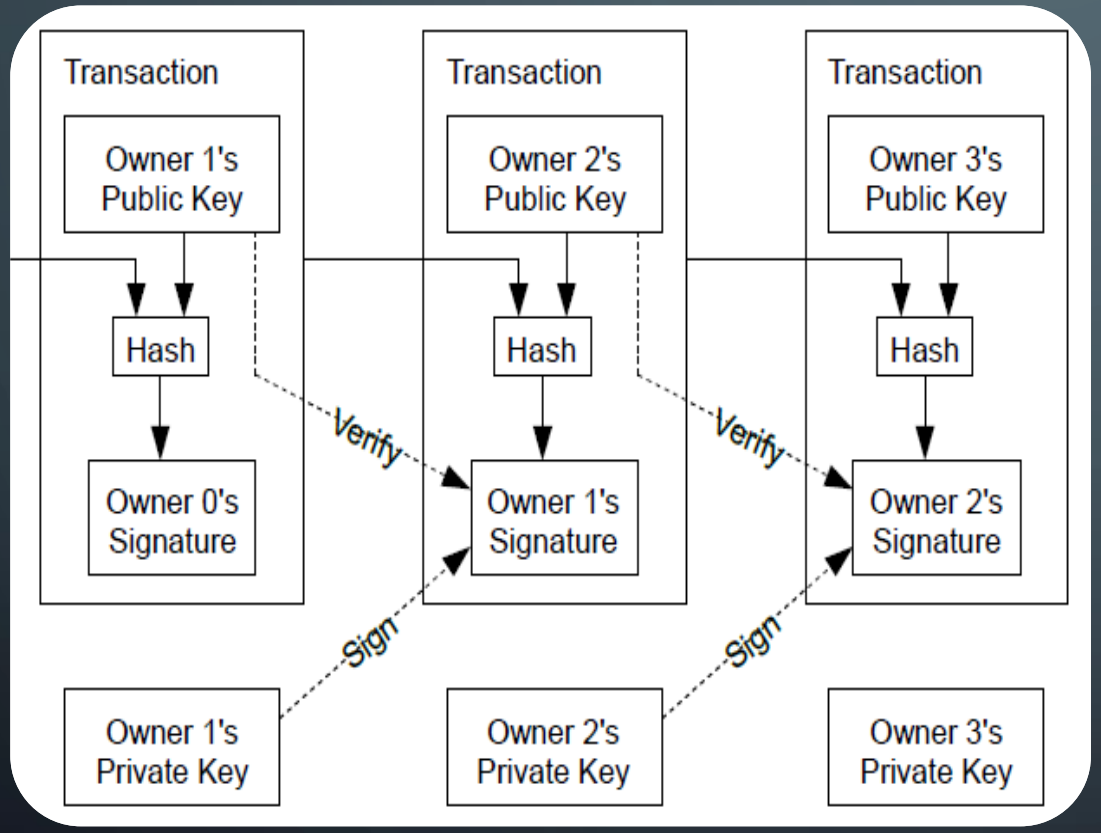


DIGITAL SIGNATURE



- Sender calculates hash value of message and attaches it to message, which becomes digitally signed message
- Receiver (anyone with public key) decrypts hash value and compares with message hash value; message is valid if hash values are equal
- Integrity of message
- Non-repudiation of signature

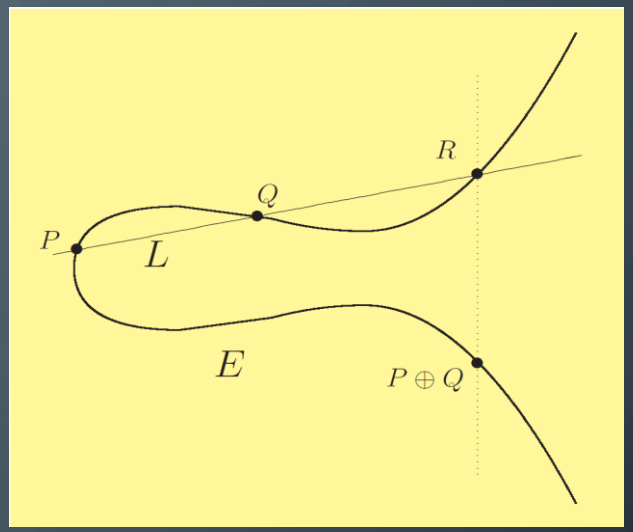
WALLET AND TRANSACTION

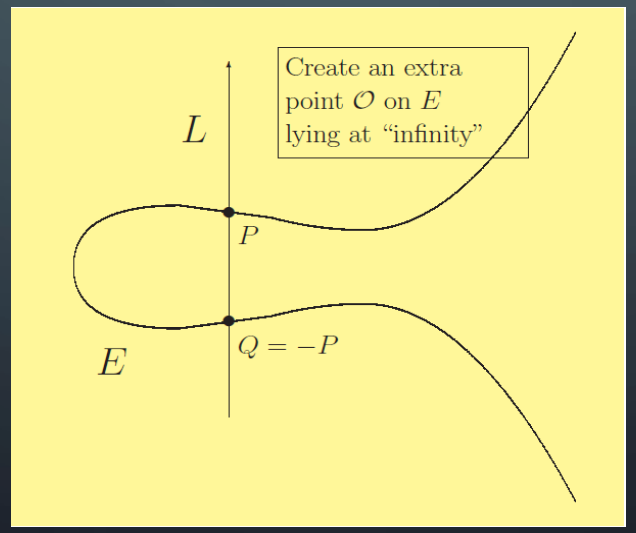


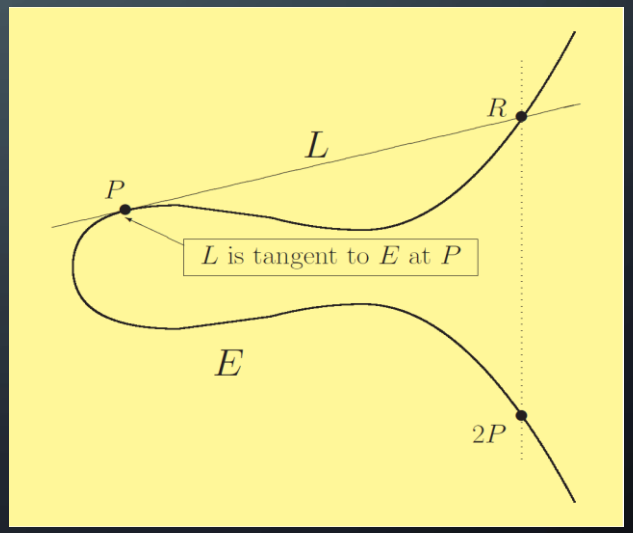
- Bitcoin wallet is a pair of public (address) and private (seed or password) keys
- In each transaction, sender uses private key to sign hash of receiver's public key and previous transaction
- Ownership verified by public key
- Each bitcoin is a chain of digitally signed transactions

ELLIPTIC CURVE ON FINITE FIELD

- Finite field $\mathbf{F}_p$ is integers $0,1,\ldots,p-1$ with addition and multiplication under module p
- Points on elliptical curve $E: y^2 = x^3 + Ax + B$ with coordinates in $\mathbf{F}_p$ plus infinity point (group identity) form a group $E(\mathbf{F}_p)$ under $\oplus$
- $\oplus$ can be defined by geometry (pictures) or algebra (formula omitted here)







DISCRETE LOGARITHM PROBLEM

- Given $E(\mathbf{F}_p)$ and S, T $\in E(\mathbf{F}_p)$, find smallest integer m such that $T = mS$; m is called discrete logarithm $m = \log_S T$
- Find such m turns out to be very difficult for general $E(\mathbf{F}_p)$ with $p = 2^n$, without specific knowledge of group structure
- Best known algorithm is Pollard's ρ method, whose time complexity is $O(\sqrt{p}) = O(2^{n/2})$
- For $n = 160$, ECDLP complexity is about the same as factoring 2^{1000} bit number, which is the basis for RSA algorithm
- RSA has its difficulty in factoring product of two large prime numbers

MORE TOPICS

- Fork - when rule changes make validity change in blocks
- Scalability - limited block size and block generating frequency
- Volatility - cryptocurrency tends to be very volatile
- Distributed data storage - on peer network nodes
- Proof of stake - instead of solving hash partial inversion, block generator is selected randomly based on coin amount, coin age, etc.
- Smart contract - programmed, self-executing digital contract
- Real world application - other than cryptocurrency

iMorpheus.ai

REFERENCES

1. Bitcoin “White Paper” - Satoshi Nakamoto
2. Ethereum “White Paper” - Vitalik Buterin
3. Secure Hash Signature Standard (SHS) (FIPS PUB 180-2)
4. An Introduction to the Theory of Elliptic Curves - Joseph H. Silverman
5. English Wikipedia pages on related topics

iMorpheus.ai

iMorpheus.ai Weekly Journal Club

Next Thursday, 29/03/2018

Principles of GNSS Positioning

Website : **http://imorpheus.ai**
Email Address : **live@imorpheus.ai**

iMorpheus.ai