Bitcoin

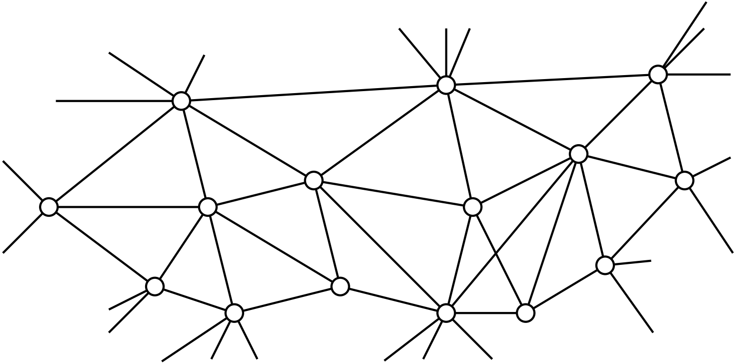
Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 31, 2018

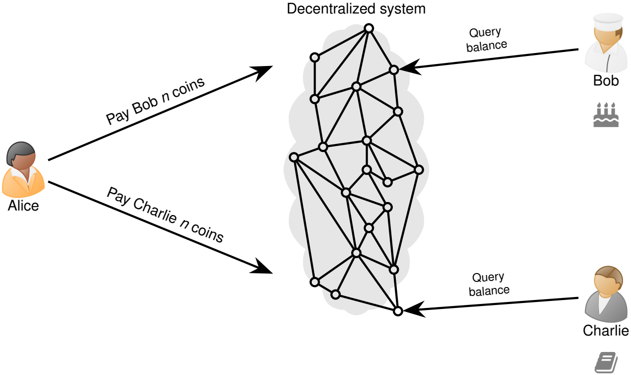
What is Bitcoin?

- Cryptocurrency
- Open source
- Decentralized network



Decentralization Challenges

- Counterfeiting
- Currency creation rules
- Double spending
  - Alice pays Bob *n* digicoins for a cake
  - Alice uses the **same** *n* digicoins to pay Charlie for a book



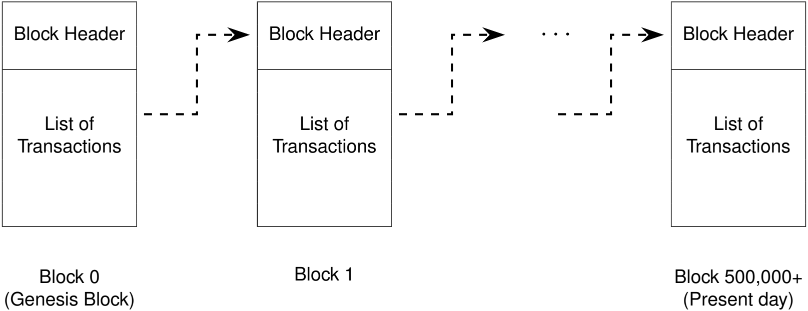
Solution without a central coordinator?

Double Spending

- Familiar to academics
- Submitting same paper to two conferences
- **Possible solution**
  Reviewers google paper contents to find duplicates
- Solution fails if
  - Conferences accepting papers at same time
  - Conference proceedings not published/indexed
- **Better solution**
  A single public database to store all submissions to all conferences

The Blockchain

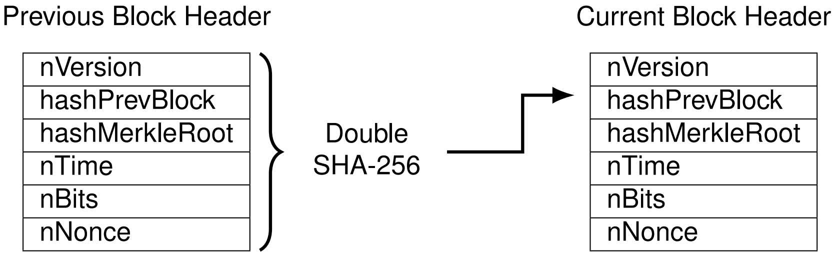
Blockchain: A public database to store all transactions which is replicated by many network nodes



How are the blocks linked?

Block Header

nVersion	4 bytes
hashPrevBlock	32 bytes
hashMerkleRoot	32 bytes
nTime	4 bytes
nBits	4 bytes
nNonce	4 bytes



Previous Block Header

nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

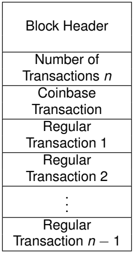
Double SHA-256

Current Block Header

nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

Bitcoin Mining (1/2)

- Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



Block Header

Number of Transactions n

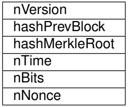
Coinbase Transaction

Regular Transaction 1

Regular Transaction 2

$\vdots$

Regular Transaction $n-1$



nVersion

hashPrevBlock

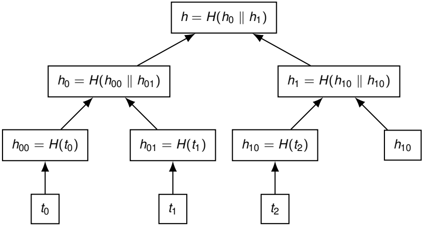
hashMerkleRoot

nTime

nBits

nNonce

- hashPrevBlock contains double SHA-256 has of previous block's header
- hashMerkleRoot contains root hash of transaction Merkle tree



$h = H(h_0 \parallel h_1)$

$h_0 = H(h_{00} \parallel h_{01})$

$h_1 = H(h_{10} \parallel h_{10})$

$h_{00} = H(t_0)$

$h_{01} = H(t_1)$

$h_{10} = H(t_2)$

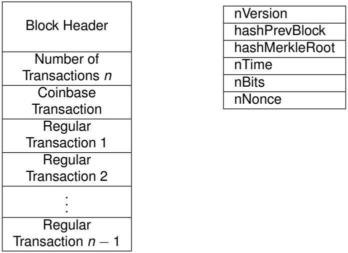
h_{10}

t_0

t_1

t_2

Bitcoin Mining (2/2)



Block Header

Number of Transactions n

Coinbase Transaction

Regular Transaction 1

Regular Transaction 2

$\vdots$

Regular Transaction $n-1$

nVersion

hashPrevBlock

hashMerkleRoot

nTime

nBits

nNonce

- nBits encodes a 256-bit target value T, say

$$T = \text{0x}\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{\text{48 times}}$$

- Miner who can find nNonce such that

  $$\text{SHA256}\left(\text{SHA256}\left(\text{nVersion} \,\|\, \text{hashPrevBlock} \,\|\, \ldots \,\|\, \text{nNonce}\right)\right) \leq T$$

  can add a new block

- Modifying any header field will require solving PoW puzzle again

References

- Chapter 4 of *An Introduction to Bitcoin*, S. Vijayakumaran, `www.ee.iitb.ac.in/~sarva/bitcoin.html`