Bitcoin

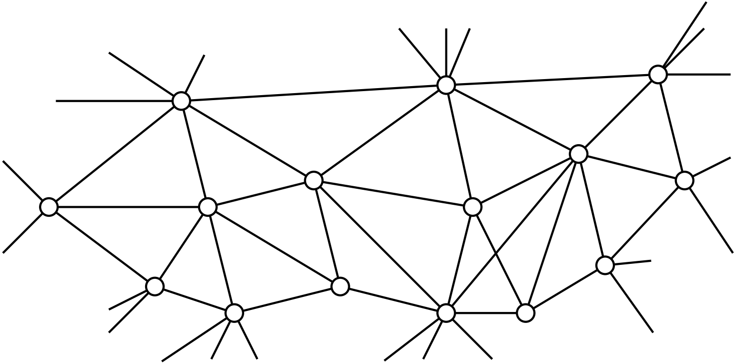
Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 31, 2018

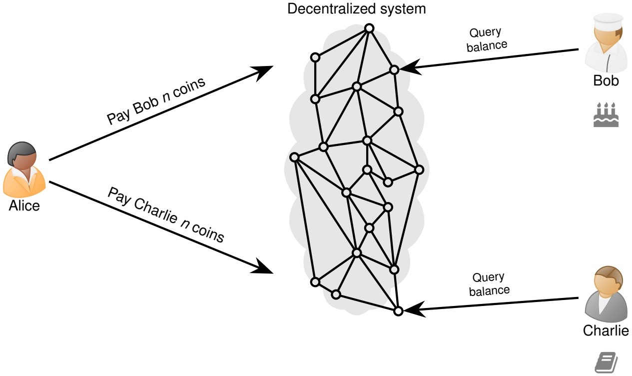
What is Bitcoin?

- 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



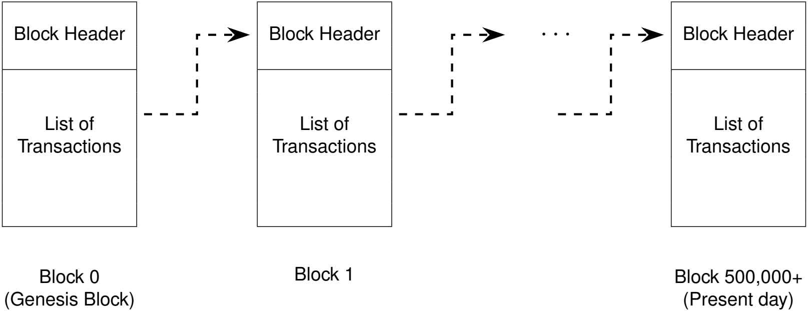
Solution without a central coordinator?

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

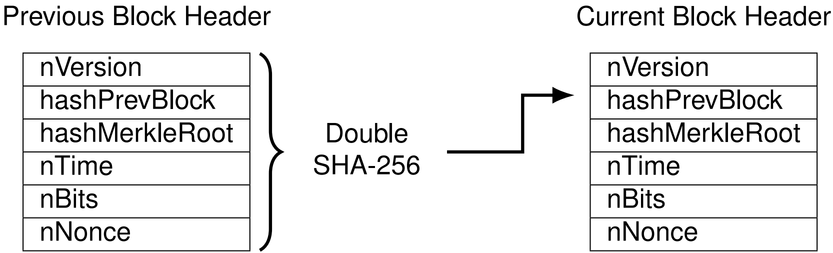
Blockchain: A public database to store all transactions which is replicated by many network nodes



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



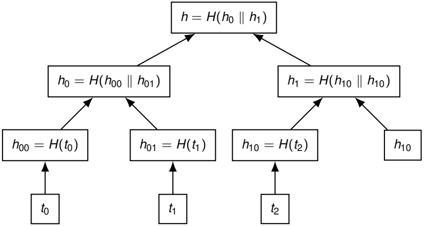
Bitcoin Mining (1/2)

- 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
⋮
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



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

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

  can add a new block
- Modifying any header field will require solving PoW puzzle again

Why is Mining Hard?

Target value T	Fraction of SHA256d outputs $\leq T$
$0x7\underbrace{FFFF\,FFFF\cdots FFFF}_{\text{63 times}}$	$\frac{1}{2}$
$0x0\underbrace{FFFF\,FFFF\cdots FFFF}_{\text{63 times}}$	$\frac{1}{16}$
$0x\underbrace{00\cdots 00}_{\text{16 times}}\underbrace{FFFFF\cdots FFFFF}_{\text{48 times}}$	$\frac{1}{2^{64}}$

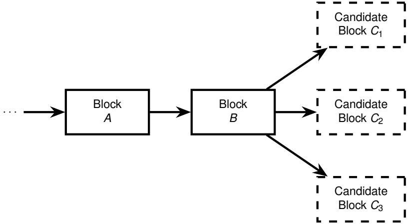
$$\Pr[\text{SHA256d output} \leq T] \approx \frac{T+1}{2^{256}}$$

Why should anyone mine blocks?

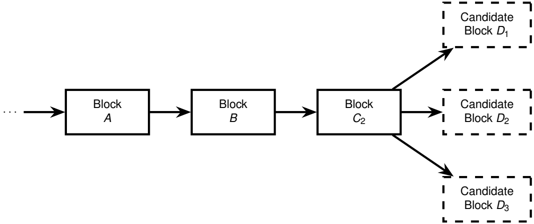
- Successful miner gets rewarded in bitcoins
- Every block contains a **coinbase transaction** which creates 12.5 bitcoins
- Each miner specifies his own address as the destination of the new coins
- Every miner is competing to solve their own PoW puzzle
- Miners also collect the transaction fees in the block

Block Addition Workflow

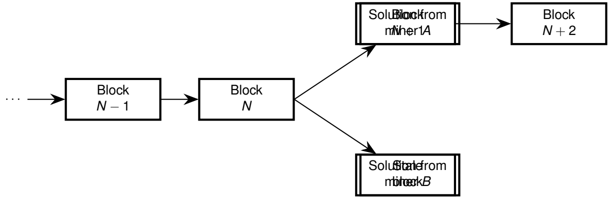
- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block



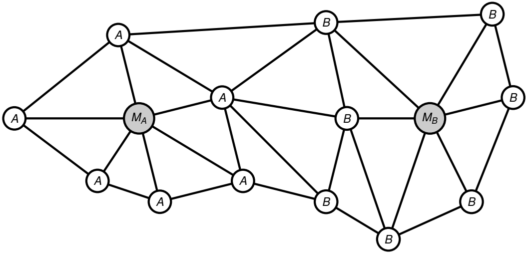
- Miners compete to solve the search puzzle and broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones



What if two miners solve the puzzle at the same time?



- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others



- Nodes always switch to the chain which was more difficult to produce
- Eventually the network will converge and achieve consensus

How often are new blocks created?

- Once every 10 minutes

nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

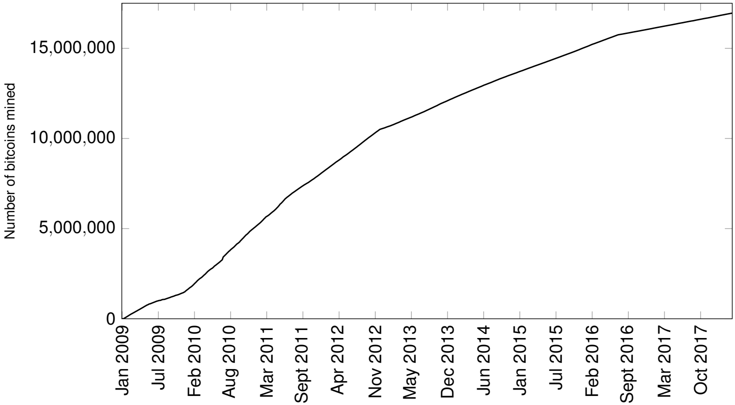
- Every 2016 blocks, the target T is recalculated
- Let t_{sum} = Number of seconds taken to mine last 2016 blocks

$$T_{\text{new}} = \frac{t_{\text{sum}}}{2016 \times 10 \times 60} \times T$$

- Recall that probability of success in single trial is $\frac{T+1}{2^{256}}$
- If $t_{\text{sum}} = 2016 \times 8 \times 60$, then $T_{\text{new}} = \frac{4}{5} T$
- If $t_{\text{sum}} = 2016 \times 12 \times 60$, then $T_{\text{new}} = \frac{6}{5} T$

Bitcoin Supply

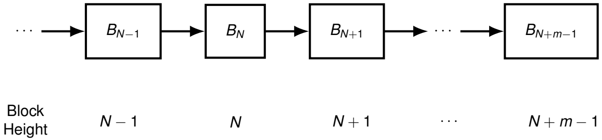
- The block subsidy was initially 50 BTC per block
- Halves every 210,000 blocks $\approx$ 4 years
- Became 25 BTC in Nov 2012 and 12.5 BTC in July 2016
- Total Bitcoin supply is 21 million



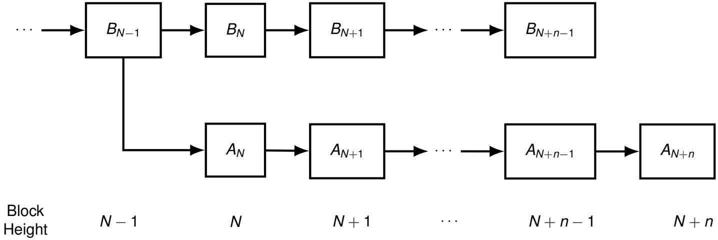
- The last bitcoin will be mined in 2140

Tamper Resistance

- Suppose Alice wants to modify block B_N



- Alice works on A_N branch; other miners work on B_N branch



- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate

Key Takeaways

- Bitcoin's blockchain prevents double spending and tampering
- Secure only if nobody controls 50% or more of network hashrate
- Mining difficulty adjusted to regulate coin supply
- Miners incentivized by block reward
- Block subsidy halves every four years to cap total coin supply

References

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