Bitcoin

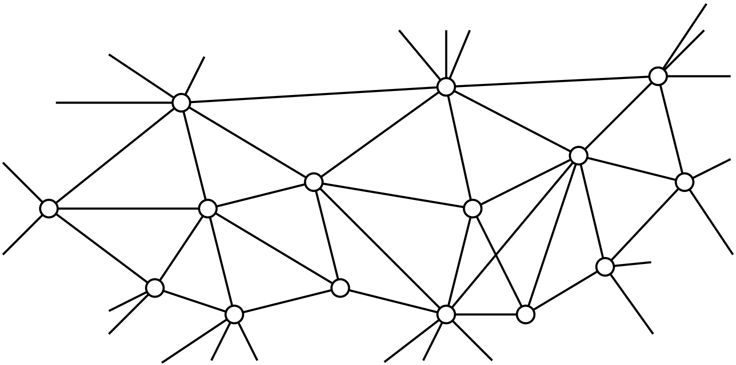
Saravanan Vijayakumaran

Department of Electrical Engineering
Indian Institute of Technology Bombay

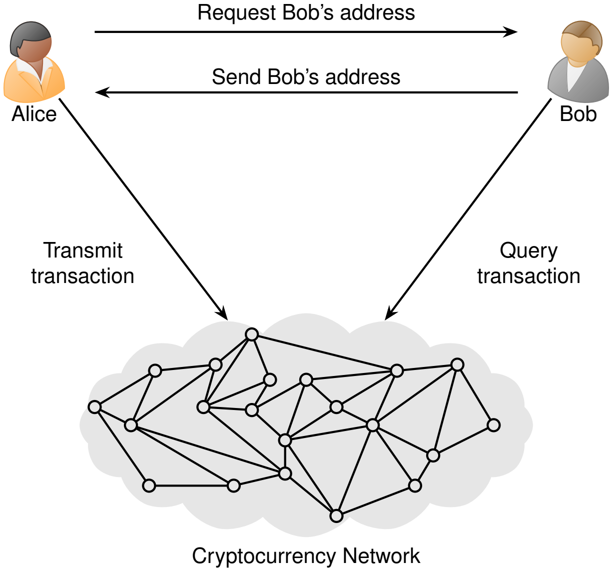
January 8, 2024

What is Bitcoin?

- Cryptocurrency
- Open source software
- Decentralized network

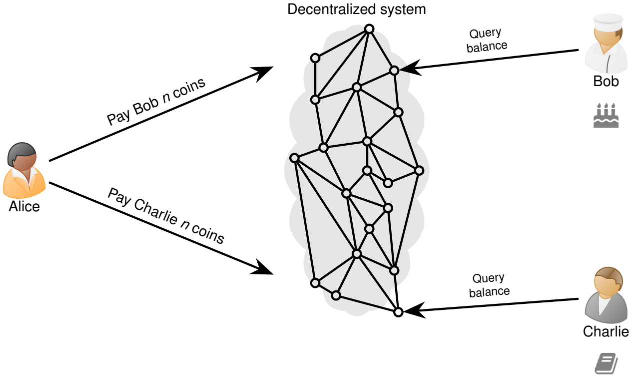


Cryptocurrency Transaction Workflow



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



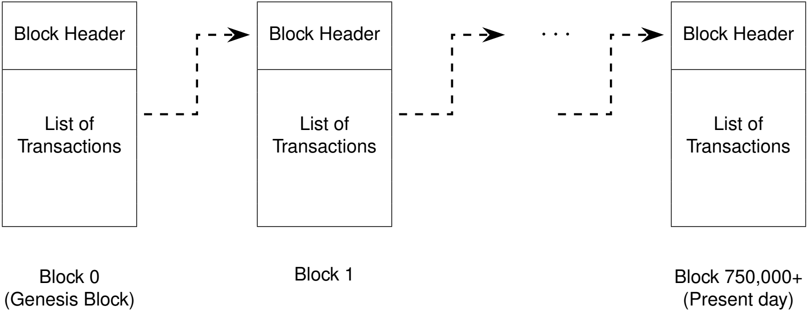
Solution without a central coordinator?

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

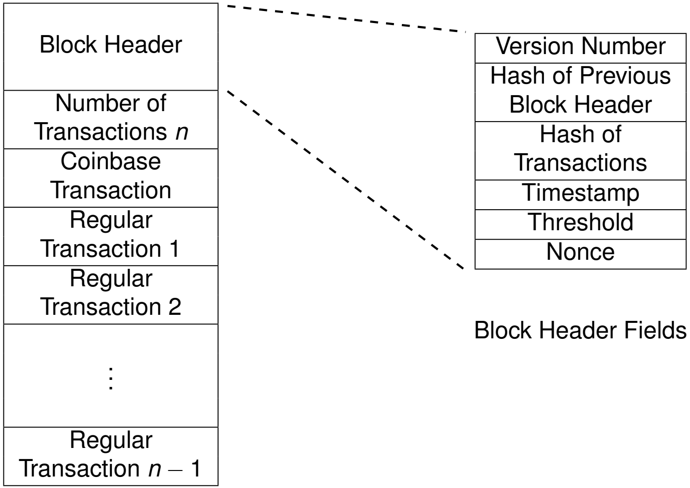
The Blockchain

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



How are the blocks linked?

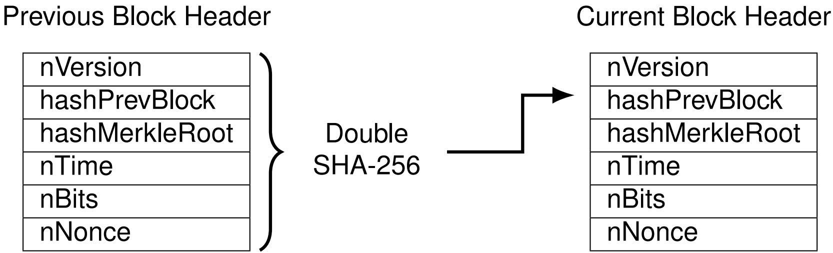
Bitcoin Block and Header Formats



- Hash = Output of cryptographic hash function

Block Header

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



Cryptographic Hash Functions

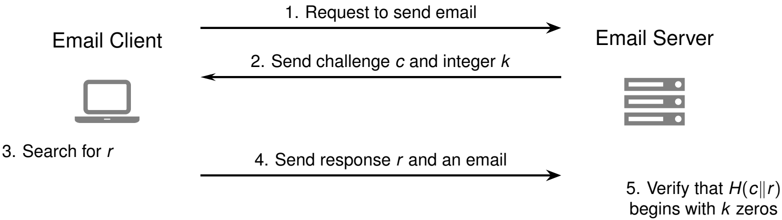
- Easy to compute but difficult to invert
- Collision-resistant
- Pseudorandom outputs
- SHA-256 = NIST approved CHF with 256-bit outputs

Input	SHA-256 Output
dec0	**0525bd43e7ba2917ebb5ff4893961fa6e6a3b5ccadbffd9bc520882168945a71**
dec1	**0740174f35ff7cb50b8417bdc50be191f8c5e5daaf4c4bdb8498b1fe3aa41d0d**
dec2	**dabc08efd0d2ae280fc0177c978ab7c82542cc67d3acafb62cbd913b5b73cf72**
dec3	**a2b2c10ec26b94298e07e0273c319686721d6c7f285756fb4400b2bb9014ff4c**
dec4	**5076f2f9de8dbc00ebc6c72b3d207cd7b985b91f634026fd746fe07dc19993c3**
dec5	**884466e61bd01d5282386b758313b44a424b6d9d890255770393f267664c64f9**
dec6	**f37095c5192a84934ba69db9de48ad52051321fe64efc5bd95074eaaa66d08a4**
dec7	**aed0913ad1fedc68e621b23c895f5c2aa24db2cce1cb82ef123a92351ef081c3**
dec8	**8bac240a6fccbf8ead9a913d9e65f8394728e2cfeb36f745d1f0142f6e7fd0b6**
dec9	**99e9d59894056331a3ebe12870d9eb7b245a11707334a97dfad58de16eac977e**

- At a billion outputs per second, 78 billion years required to calculate 2^{100} outputs

Hashcash

- A database you own where anyone in the world can add entries? Your email inbox
- Hashcash was proposed in 1997 to prevent spam
- Protocol
  - Suppose an email client wants to send email to an email server
  - Client and server agree upon a cryptographic hash function H
  - Email server sends the client a challenge string c
  - Client needs to find a string r such that $H(c \| r)$ begins with k zeros



- The r is considered **proof-of-work (PoW)**; difficult to generate but easy to verify
- Demo

Difficulty Increases with k

- Let hash function output length n be 4 bits

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Binary	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

$k = 3$

$k = 2$

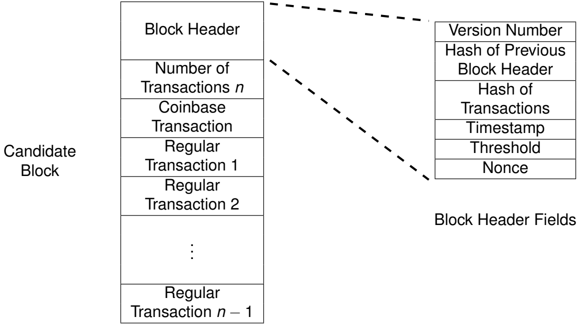
$k = 1$

- Since H has pseudorandom outputs, probability of success in a single trial is

$$\frac{2^{n-k}}{2^n} = \frac{1}{2^k}$$

Bitcoin Mining

- Mining = 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



- Threshold encodes a 256-bit value like 0x$\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{\text{48 times}}$
- Miner who can find Nonce such that

$$\text{SHA256(SHA256(}\underbrace{\text{Version Number} \parallel \cdots \parallel \text{Nonce}}_{\text{Candidate Block Header}}\text{))} \leq \text{Threshold.}$$

can add a new block

Mining is Hard

Target value T	Fraction of SHA256d outputs $\leq T$
$0x7\underbrace{\text{FFFF FFFF}\cdots\text{FFFF}}_{\text{63 times}}$	$\frac{1}{2}$
$0x0\underbrace{\text{FFFF FFFF}\cdots\text{FFFF}}_{\text{63 times}}$	$\frac{1}{16}$
$0x\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{\text{48 times}}$	$\frac{1}{2^{64}}$

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

Why should anyone mine blocks?

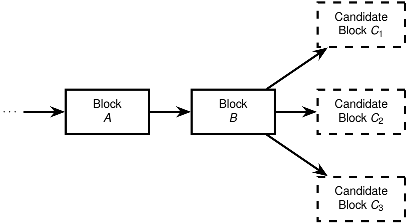
- Successful miner gets rewarded in bitcoins
- Every block contains a **coinbase transaction** which creates 6.25 bitcoins
- Each miner specifies his own address as the destination of the new coins
- Every miner is competing to solve their own PoW puzzle
- Miners also collect the transaction fees in the block

Mining Farms

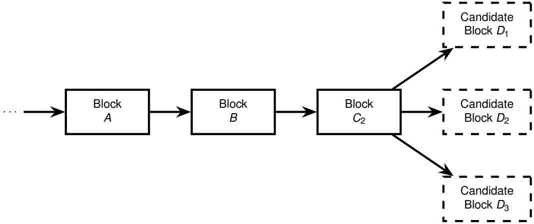
- Mining farms have thousands of mining rigs
- Each mining rig has dozens of mining chips
- Each chip has dozens of SHA256 mining cores
- Farms are located in places with cheap power and cooling

Block Addition Workflow

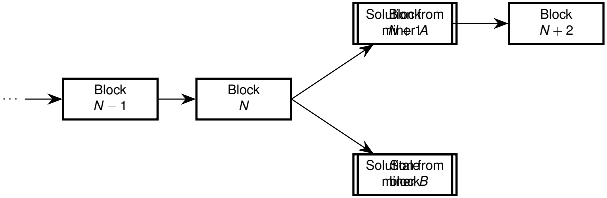
- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block



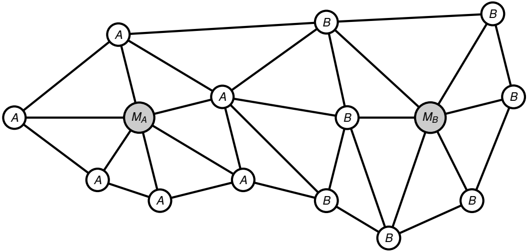
- Miners compete to solve the search puzzle and broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones



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
- This is called proof-of-work (PoW) 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

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

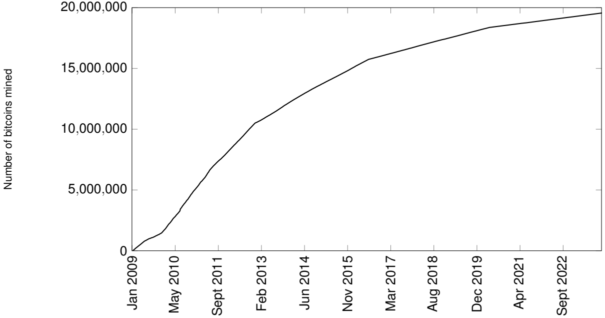
- Recall that probability of success in single trial is $\frac{T+1}{2^{256}}$
- If $t_{\text{sum}} = 2016 \times 8 \times 60$, then $T_{\text{new}} = \frac{4}{5}T$
- If $t_{\text{sum}} = 2016 \times 12 \times 60$, then $T_{\text{new}} = \frac{6}{5}T$
- Additionally, T_{new} is clipped to be in $\left[\frac{T}{4},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

Bitcoin Blockchain Explorers

- Web interfaces to view current blockchain state
  - `https://www.blockstream.info`
  - `https://www.blockchain.com/explorer`
- Demo checklist
  - List of transactions (coinbase, regular)
  - Address generation in `https://www.bitaddress.org`
  - Brainwallet generation at `https://brainwalletx.github.io`

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, 12.5 BTC in July 2016, 6.25 in May 2020, 3.125 in Apr 2024 (expected)
- Total Bitcoin supply is approx 21 million

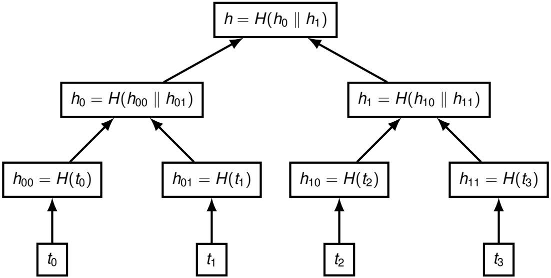


Data source: `https://www.blockchain.com/explorer/charts/total-bitcoins`

- The last bitcoin will be mined in 2140

Merkle Hash of Transactions

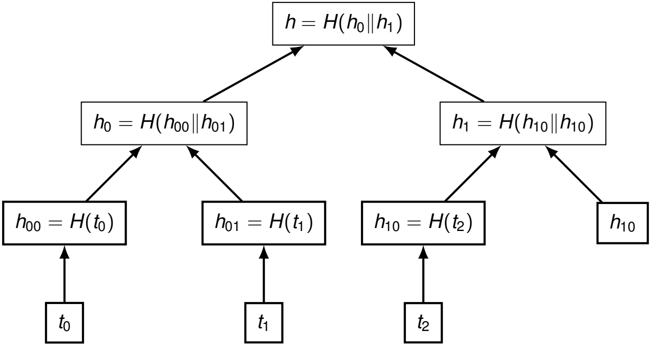
nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce



- Merkle hash of the transactions allows light clients

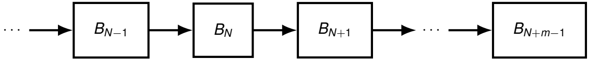
Padding the Merkle tree

- If the number of transactions is not a power of two, they are padded

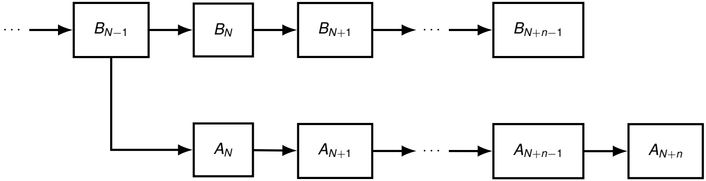


Tamper Resistance

- Suppose Alice wants to modify block B_N

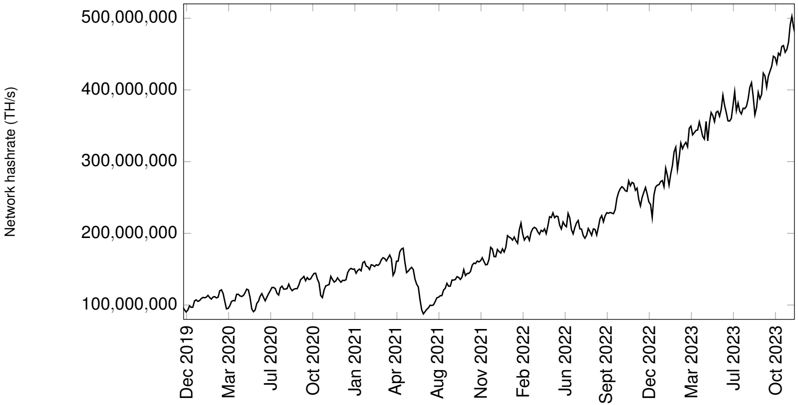


- Alice works on A_N branch; other miners work on B_N branch



- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate
- Current Bitcoin network hashrate $\approx$ 500 EH/s = 500×10^{18} H/s
- One mining unit costing \$4000 gives 200 TH/s
- Controlling 50% of hashrate = Controlling 5 billion USD worth of hardware

Bitcoin Hashrate



Data source: `https://www.blockchain.com/explorer/charts/hash-rate`

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`
- Chapter 7 of *Grokking Bitcoin*, Kalle Rosenbaum
- Bitcoin Charts
  - `https://www.blockchain.com/explorer/charts`
  - `https://data.bitcoinity.org/bitcoin/block_time`
- Bitmain Mining Rigs `https://shop.bitmain.com`