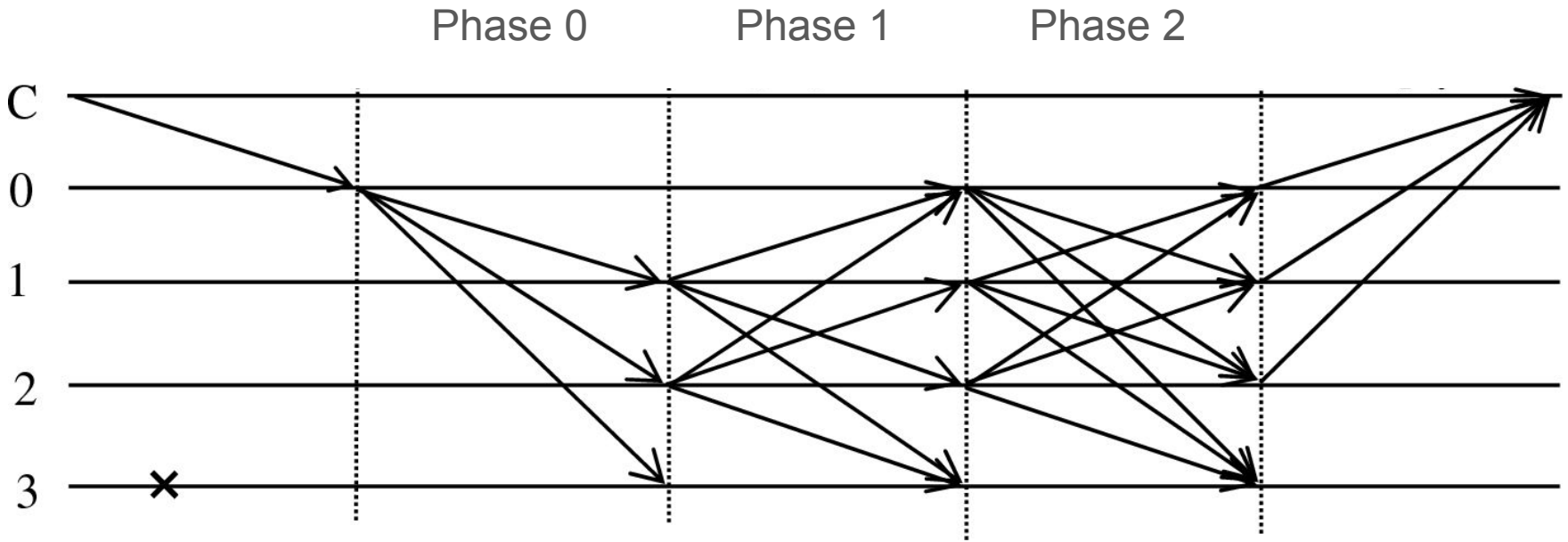
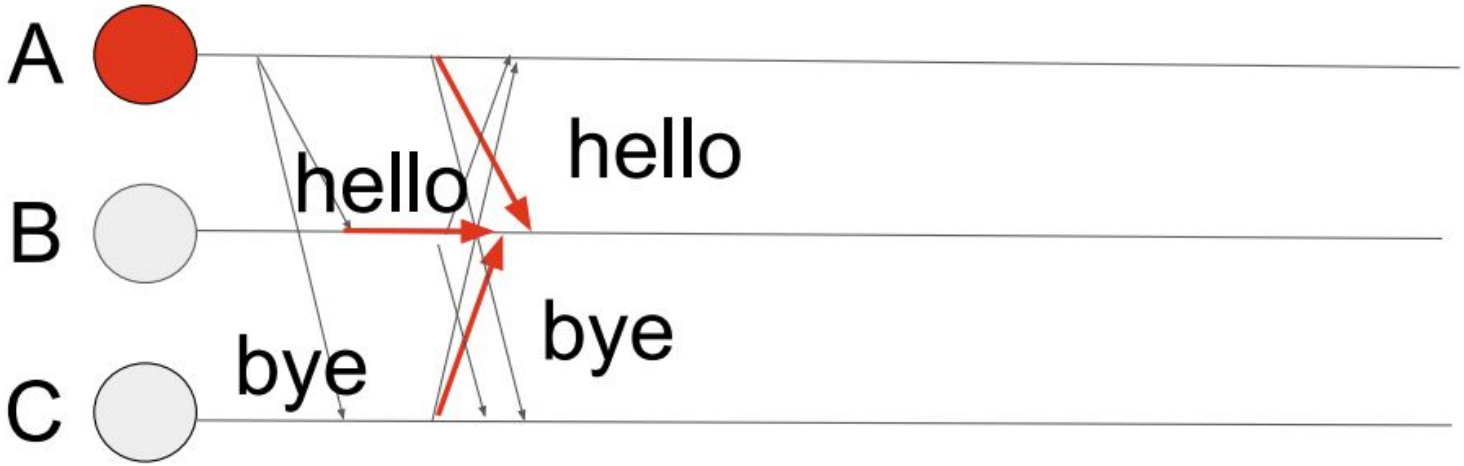
Why BFT consensus needs 3 phases？


Phase 0
Phase 1
Phase 2
C
0
1
2
3

Phase 0 Phase 1

Malicious leader

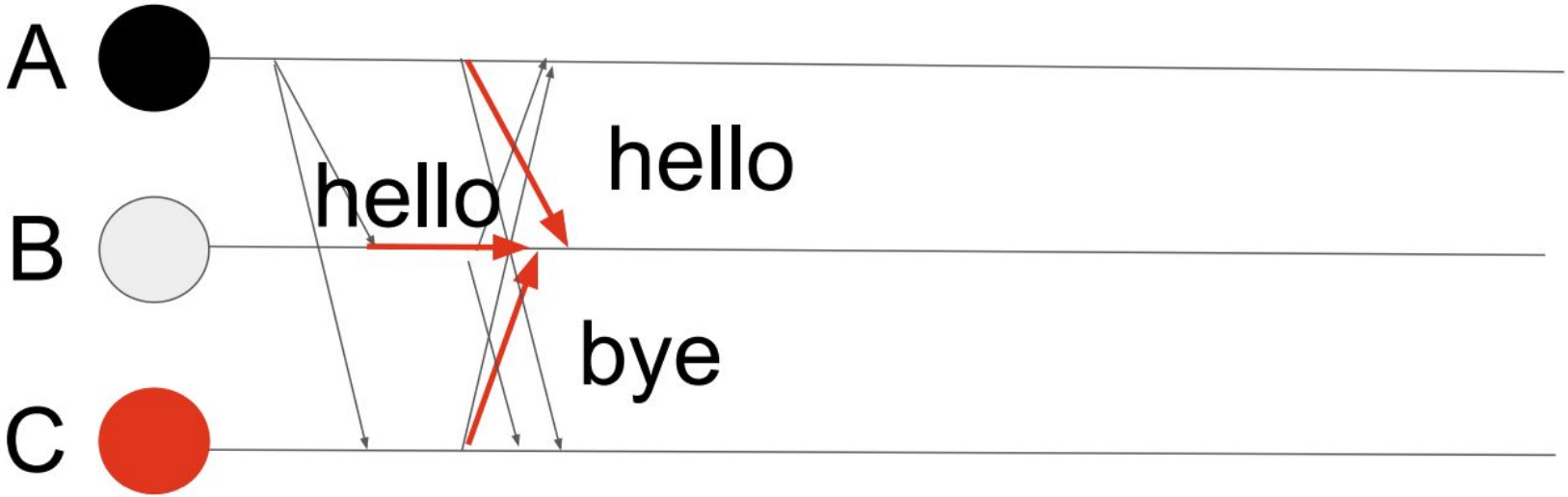


B: (hello), hello, bye

C: (bye), bye, hello

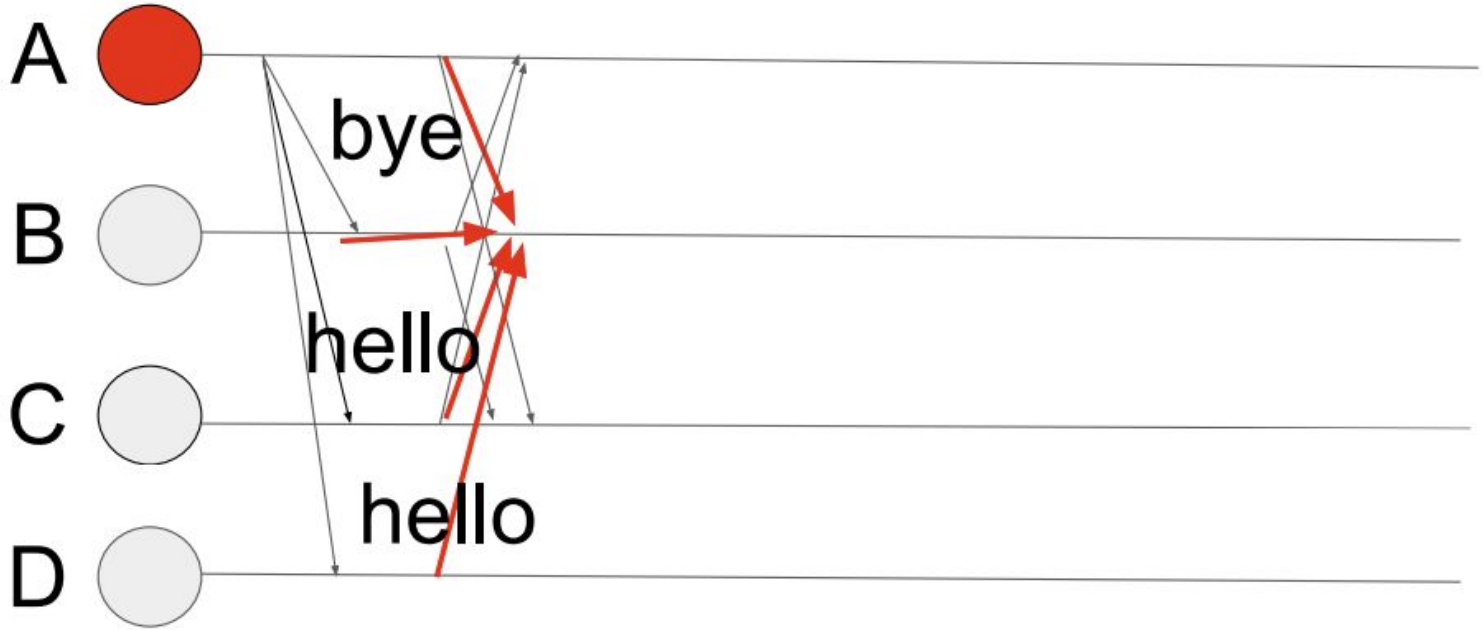
Phase 0 Phase 1

Malicious students



B: (hello), hello, bye

Phase 0 Phase 1



B: (bye), bye, hello, hello

And the final equation will be : $n >= 3f + 1$

faulty	total number
1	4
2	7
3	10
4	13
5	16
6	19
7	22
8	25
9	28
10	31
11	34
.....	
992	2977
993	2980
994	2983
995	2986
996	2989
997	2992
998	2995
999	2998
1000	3001

Tolerating rate = 1000 / 3001 = 0.333 = 33.3%

CSC 116: **Blockchain Overview / Proof of Work**

2008

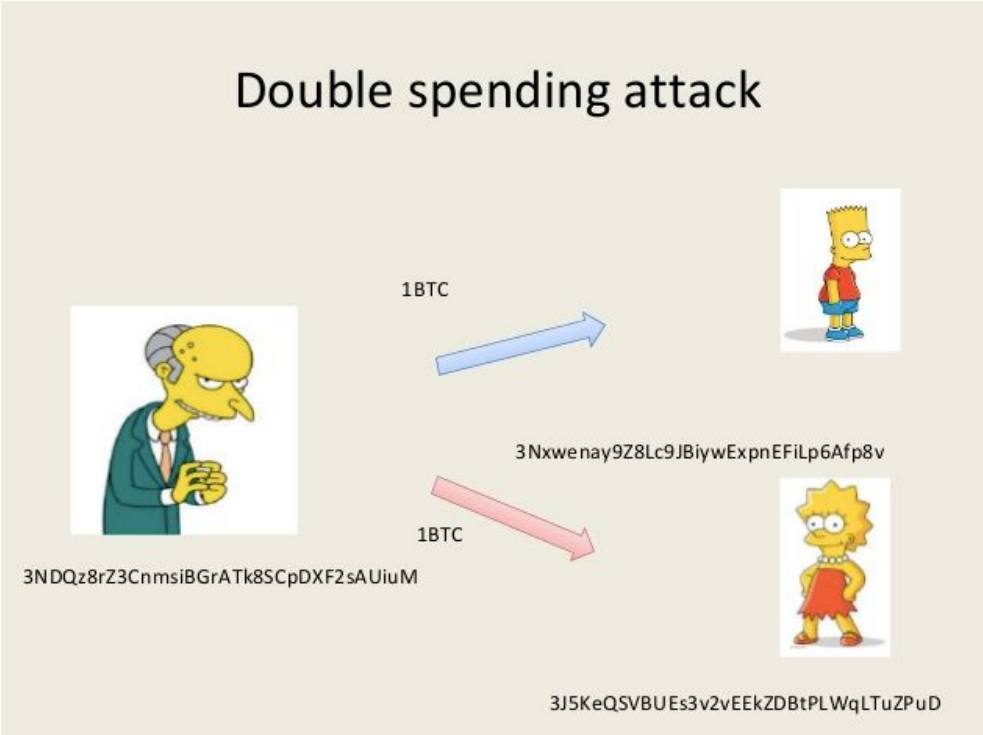
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Double Spending

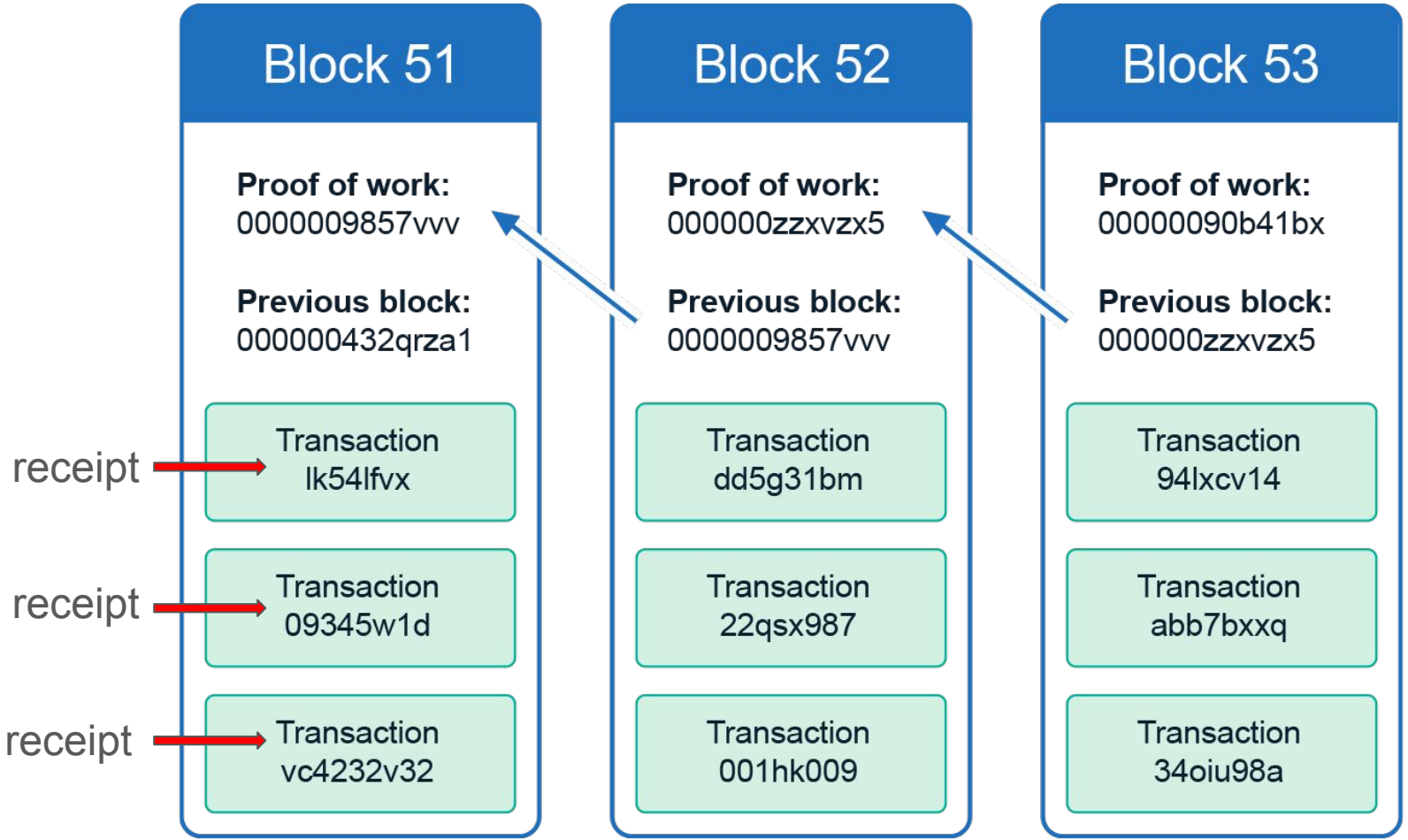
Imagine you have a $10 bill, and you give it to a friend to buy coffee. Once you give away the bill, you no longer have it—you can't use it again.

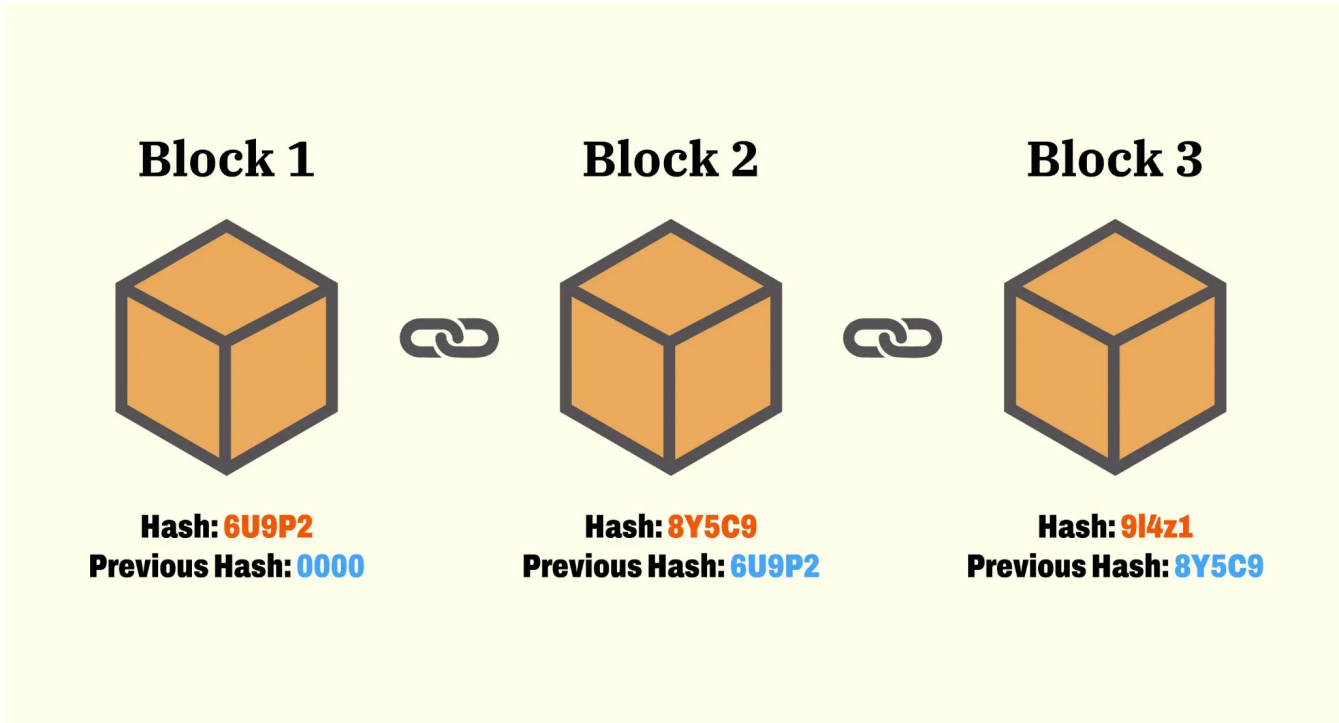


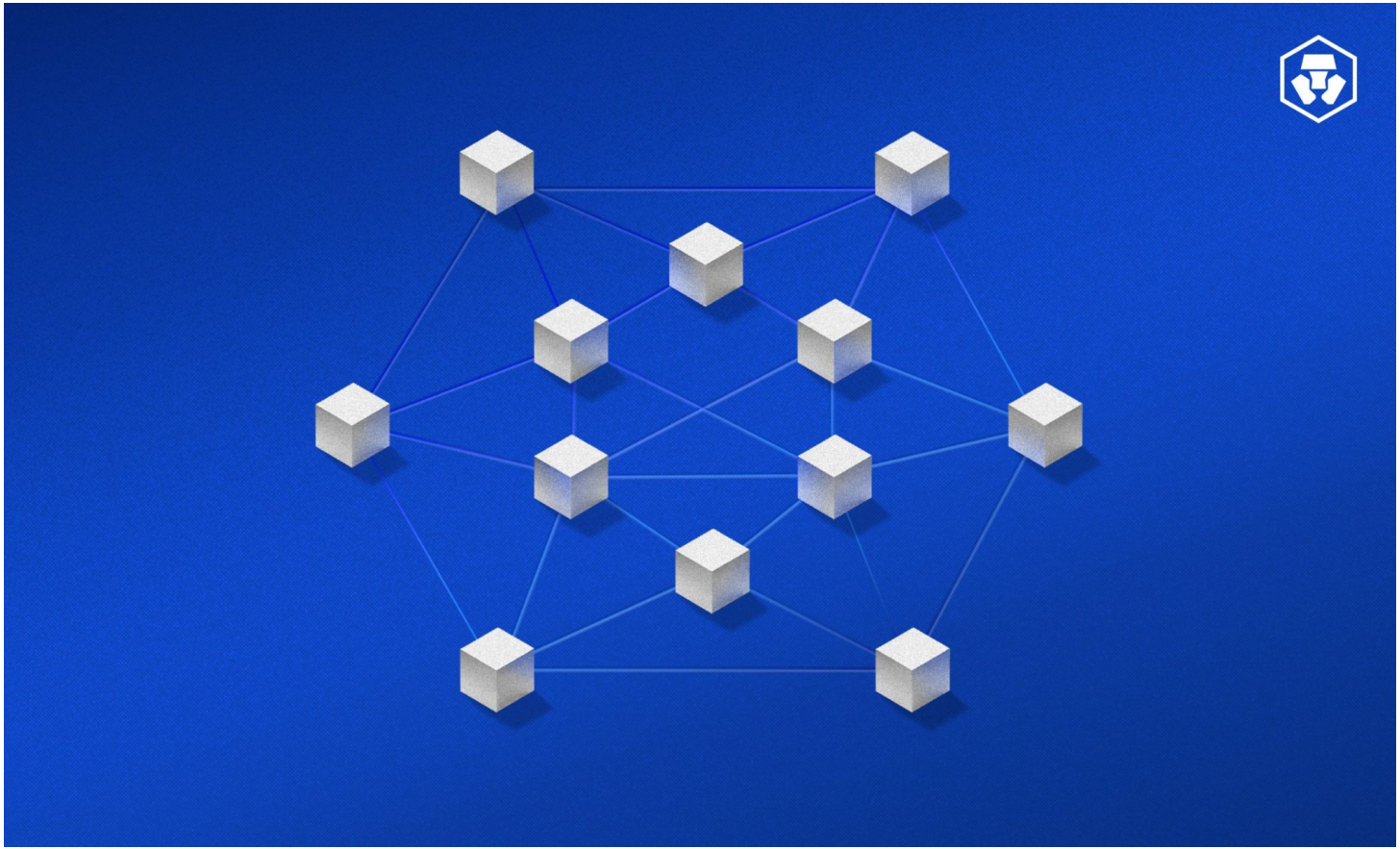
Now, think about digital money, like Bitcoin. Since it's just data, you could try to send the same Bitcoin to two different people at the same time. This is called **double spending**—it's like copying your digital money and using it twice, which is a problem because it would make the money worthless.

Blockchain

https://guggero.github.io/blockchain-demo/#!/blockchain


Block 51
Proof of work:
0000009857vvv
Previous block:
000000432qrza1
Transaction
lk54lfvx
Transaction
09345w1d
Transaction
vc4232v32
Block 52
Proof of work:
000000zzxvzx5
Previous block:
0000009857vvv
Transaction
dd5g31bm
Transaction
22qsx987
Transaction
001hk009
Block 53
Proof of work:
00000090b41bx
Previous block:
000000zzxvzx5
Transaction
94lxcv14
Transaction
abb7bxxq
Transaction
34oiu98a
receipt
receipt
receipt


Block 1
Block 2
Block 3
Hash: 6U9P2
Previous Hash: 0000
Hash: 8Y5C9
Previous Hash: 6U9P2
Hash: 9l4z1
Previous Hash: 8Y5C9



https://mempool.space/graphs/lightning/nodes-map

Everyone in Bitcoin has a copy of the blockchain

10 years ago,
it is easy to
win bitcoins

Now! You need to buy whole building of GPUs to win

Why these crazy people (Miners) buy so many GPUs?

They want to make money!!!

They want to win bitcoin, it is a competition!!!

1 A Miner first creates a block!
2 Collecting all the transactions from different users.
3. This miner needs to prove its ability to store the datasets.
4. All the miners start their hard working on calculating puzzles.

What is the puzzle?

Hash function SHA-256

0000000000000000000 8af93b8a4c68e5

8a2e4a234b2bd2d09c2f0bbff7f2f01

5, Broadcast this block to every nodes, and attached to the last position of the blockchain.

6, These nodes verify the block:
Is the Proof of Work valid?
Are the transactions valid? (No double spending, correct signatures, etc.)
Is the block properly linked to the previous block? If valid, the node forwards the block to other nodes By Gossip protocol.

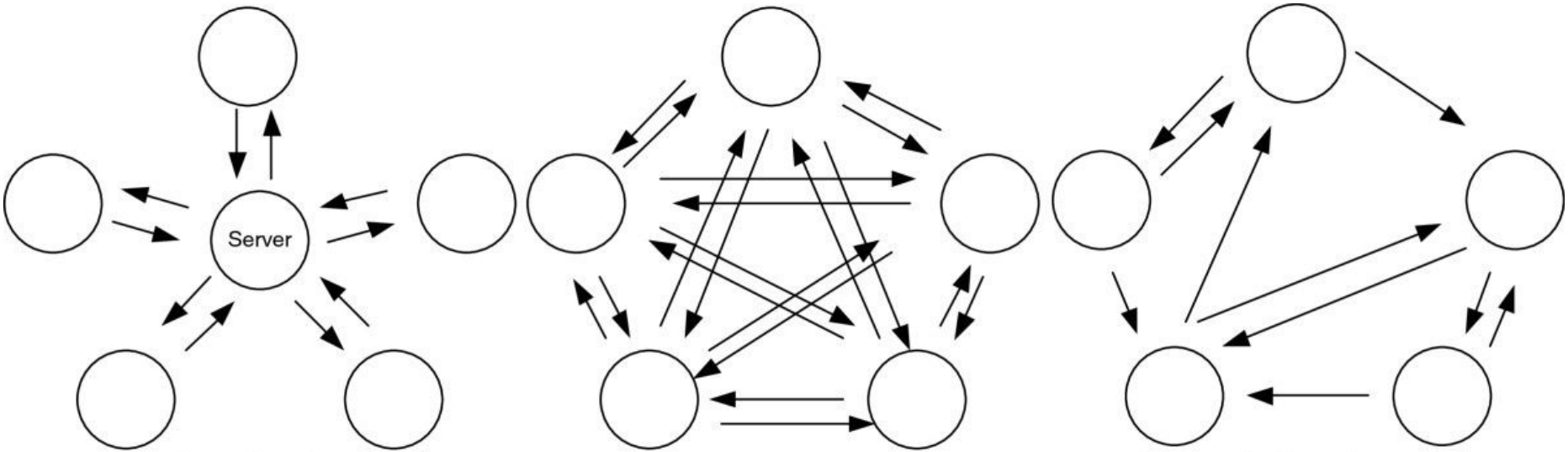
7, This miner will get 3.125 Bitcoin reward.

Alice has 1 BTC in her wallet (UTXO = 1 BTC).

She sends 0.3 BTC to Bob.
The transaction will consume her 1 BTC UTXO and create:
0.3 BTC → Bob (new UTXO)
0.7 BTC → Alice (change UTXO)

👉 The original 1 BTC UTXO is now fully spent and **no longer** valid.

Gossip protocol



(a) Centralized approach, which uses a centralized server for forwarding and mixing of multimedia streams

(b) Fully connected overlay approach, where all peers are in direct contact with one another

(c) Gossip-based approach, where peers operate in parallel, and each peer communicates with one or more randomly selected partner

Gossip protocol vs Broadcast

Feature	Gossip Protocol 🗣️	Broadcast 📡
How It Spreads	Nodes forward messages to a few peers, which continue spreading.	A node directly sends to **all** other nodes.
Scalability	✅ **Highly scalable** (works in large networks).	❌ **Not scalable** (network congestion in large systems).
Efficiency	✅ Less network traffic per node.	❌ High bandwidth usage (each node must handle all messages).
Speed	❌ Slower (takes multiple hops to spread).	✅ Faster (all nodes receive the message at once).
Fault Tolerance	✅ Works even if some nodes fail.	❌ If sender fails, message may not reach all nodes.
Redundancy	❌ Some nodes receive duplicate messages.	✅ No duplicates (one-time send to all).

Every 4 years, Miners will lose half reward.

1st	2012	50 → 25
2nd	2016	25 → 12.5
3rd	2020	12.5 → 6.25
4th	2024	6.25 → 3.125
5th (Next)	**2028**	**3.125 → 1.5625**
6th	2032	1.5625 → 0.78125
...	...	...
~33rd (Final Halving)	~2140	**0 BTC**

Market Summary > Bitcoin

95,783.57 USD

+278.23 (0.29%) ↑ today

Feb 19, 2:59 PM UTC · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

1	BTC	95783.57	USD

Feedback

More about Bitcoin →

Important Roles:

Wallets: Everyone registered has a global wallet
Miners: Want to make money
Regular Users: Buy products off-networks and pay the bitcoin on-line.

https://www.blockchain.com/explorer/addresses/btc/1XPTgDRhN8RFnzniWCddobD9iKZatrvH4

The main feature of Blockchain is transparency and immutability.

No any privacy!!!

Bitcoin like a virus spreading your data to every corners on the earth.

It is secure because everyone have your datasets

Drawbacks of Bitcoin:

Harm to the environment !
Wasting electricity!

10 mins genearting a block,
there are 10,000 nodes, more than 20,000 miners all over the world, only 1 winner.

Most of the miners are wasting their money and resources.

Harm to the environment

https://www.youtube.com/watch?v=rujSxh_TdP8

Some countries banned Cryptocurrency:

They afraid of money laundering.
Government can not control your money.

https://mempool.space/graphs/lightning/nodes-map

Difference of Bitcoin and Blockchain

1, Bitcoin is an application.

2, Blockchain is an algorithm.

Difficienty to attack blockchain

You need to **control** 51% precentage of nodes. Randonly attack is not meaningful.

Miners will try hard to protect the data because they want to make money.

Conclusion for PoW

Proof of Work (PoW) is a **consensus mechanism** used in Bitcoin and many other blockchains to ensure that all transactions are valid and that new blocks are added securely.

In simple terms, **miners must solve a difficult mathematical puzzle to add a new block to the blockchain**. This process requires **computational power**, which prevents spam, fraud, and malicious attacks.

Feature	Proof of Work (PoW) ⛏️	Byzantine Fault Tolerance (BFT) 🏛️
Security	✅ Very high (51% attack is costly)	✅ Secure but only tolerates up to 33% bad nodes
Energy Usage	❌ Very high	✅ Low (energy-efficient)
Decentralization	✅ Highly decentralized	❌ Less decentralized (limited validators)
Transaction Speed	❌ Slow (minutes per block)	✅ Fast (seconds)
Scalability	❌ Low (~7-30 TPS)	✅ High (~1000+ TPS)
Finality	❌ Probabilistic (longest chain wins)	✅ Instant finality
Resistance to Sybil Attacks	✅ Strong	✅ Strong (validators are known)
Best For	Public blockchains (Bitcoin, Ethereum)	Private blockchains (Hyperledger, Cosmos)

Thanks!

yxw1259@miami.edu