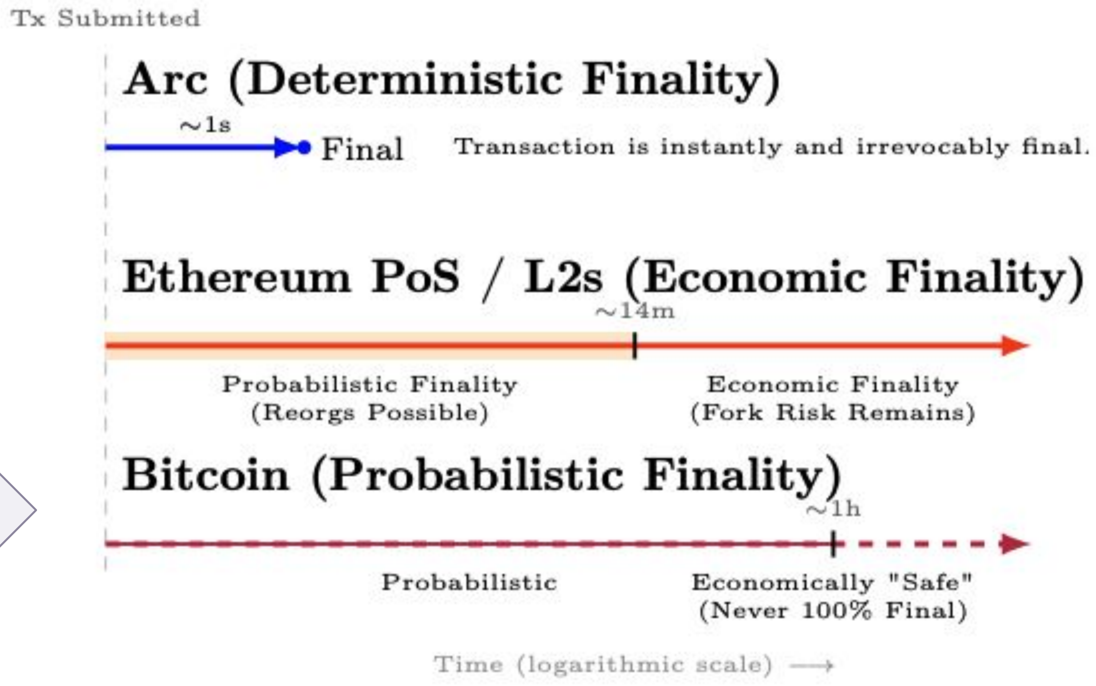
Bitcoin & Arc

Crypto fundamentals and future

Preston Vander Vos, Circle Research

How much do you know about crypto?

- Activities
    - Bought/Sold
    - Written a smart contract
    - Mined/Validated
- Terms
    - UTXO
    - dPoS
    - RWA



Tx Submitted

Arc (Deterministic Finality)

~1s

Final

Transaction is instantly and irrevocably final.

Ethereum PoS / L2s (Economic Finality)

~14m

Probabilistic Finality
(Reorgs Possible)

Economic Finality
(Fork Risk Remains)

Bitcoin (Probabilistic Finality)

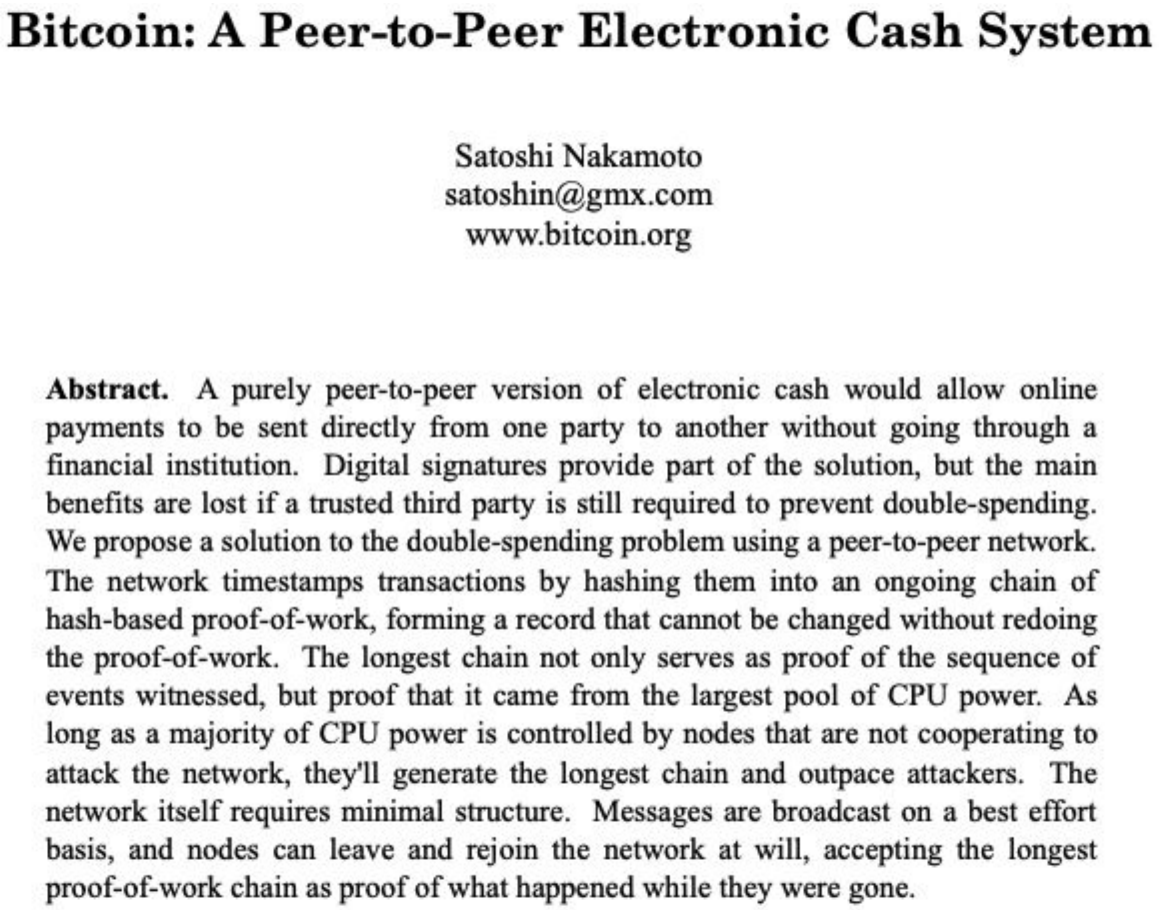
~1h

Probabilistic

Economically "Safe"
(Never 100% Final)

Time (logarithmic scale) ⟶

Figure 2: A timeline comparison of finality models.



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.

Bitcoin’s Origin

- The 9 page paper was released on Halloween 2008 🎃
- First block mined January 3, 2009
- Bitcoin built off of previous ideas
    - As Bitcoin’s Academic Pedigree discusses in depth
- Conceived during the Cypherpunk movement which worried about government oversight with the rise of the internet
- What surprised you about the Bitcoin paper?

Let’s Begin: Bitcoin Blocks

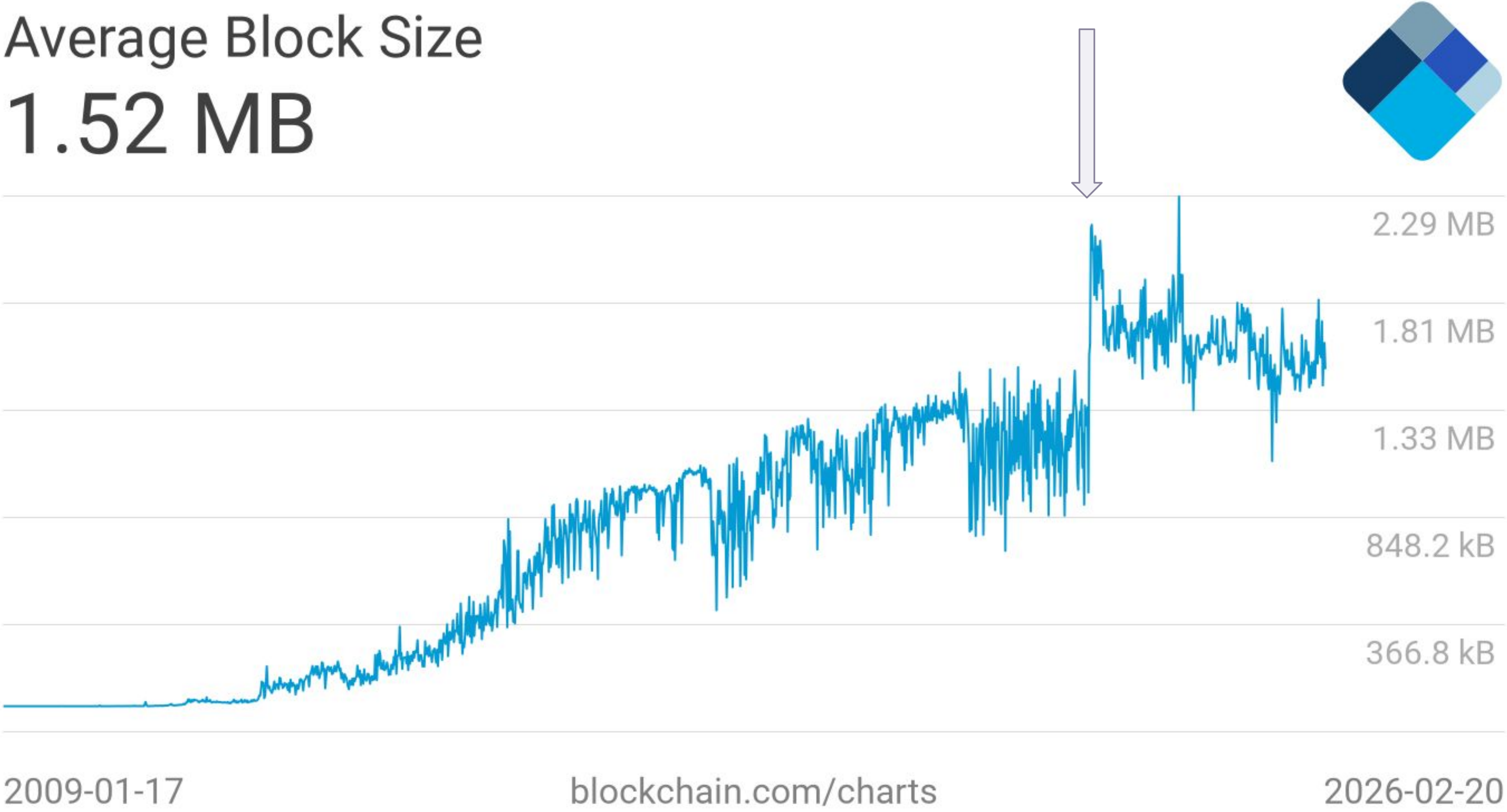
- Blocks include
  - Version number
  - Previous block’s identifier
  - Time
  - Difficulty
  - Nonce (number used only once)
  - Transaction Count
  - List of transactions
- What data structure does this remind you of? Linked list

Actual Blocks

- https://learnmeabitcoin.com/technical/block/

Average Block Size

1.52 MB



Proof of Work (PoW)

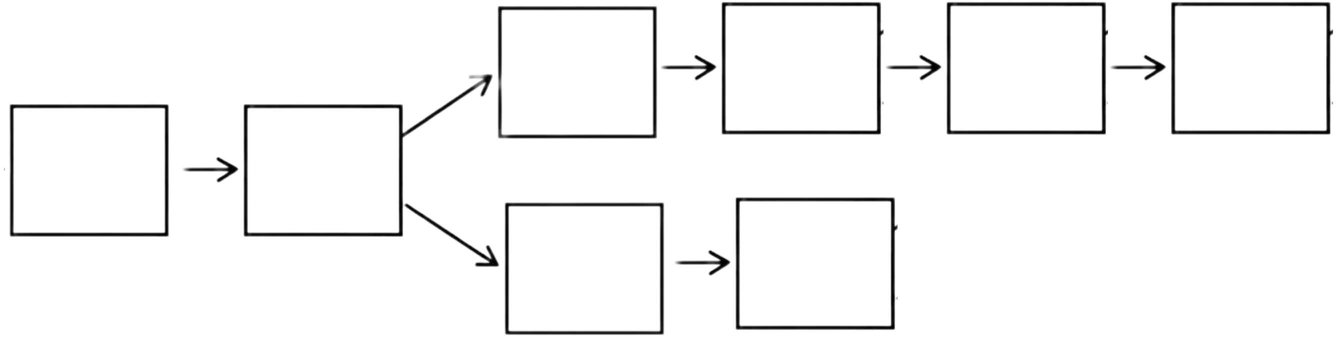
- A sybil resistance technique
  - “If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote.” -Bitcoin whitepaper
- Search for a nonce so that the SHA256 hash of the block header is small enough
  - Small enough is set by the difficulty (roughly equal to how many leading 0s are needed)

Game time!

- Let’s simulate PoW
- Go to https://emn178.github.io/online-tools/sha256.html
    - Likely the top result when you Google “sha256”

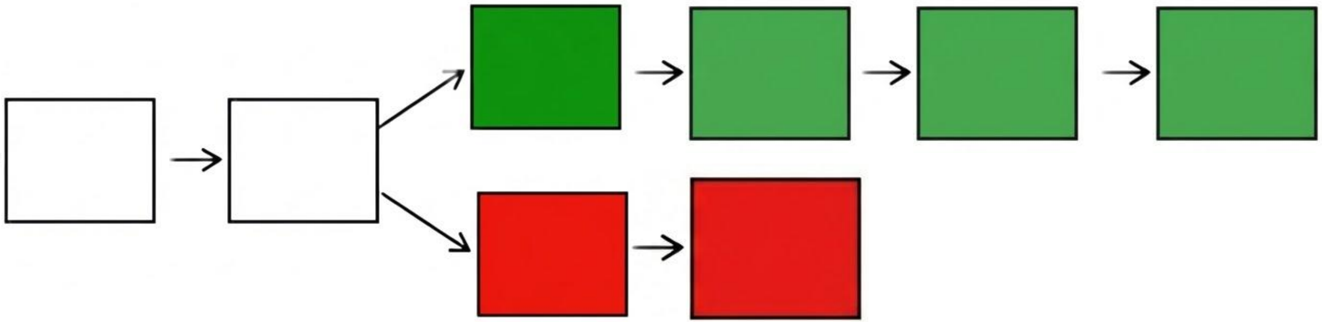
Bitcoin is Probabilistic

- What if two miners find a valid nonce at the same time?
- They both have the same previous block hash…
- A fork occurs!



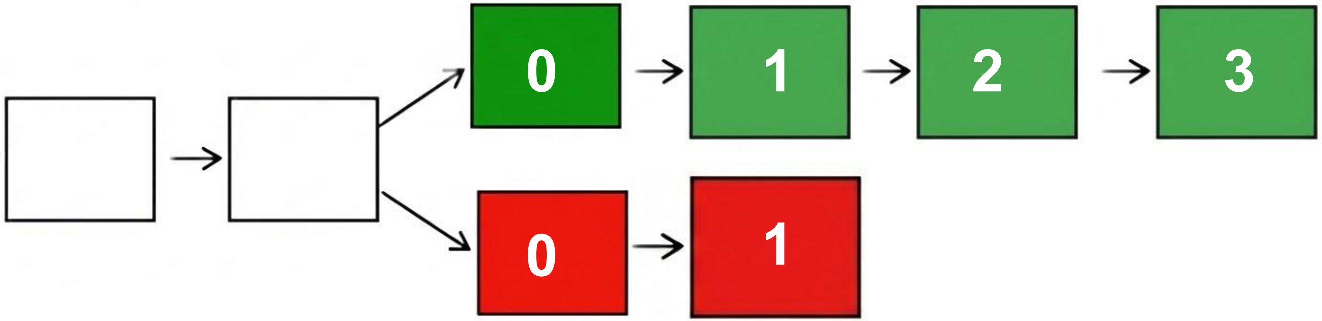
Bitcoin is Probabilistic

- What if two miners find a valid nonce at the same time?
- They both have the same previous block hash…
- A fork occurs!
- Eventually one side will win



Implications

- Since inclusion in a block does not guarantee finality, people wait
- Confirmation: the number of blocks built on top of a particular block
- Rule of thumb is to wait 6 confirmations
  - At ~10 mins per block, that's 1 hour!



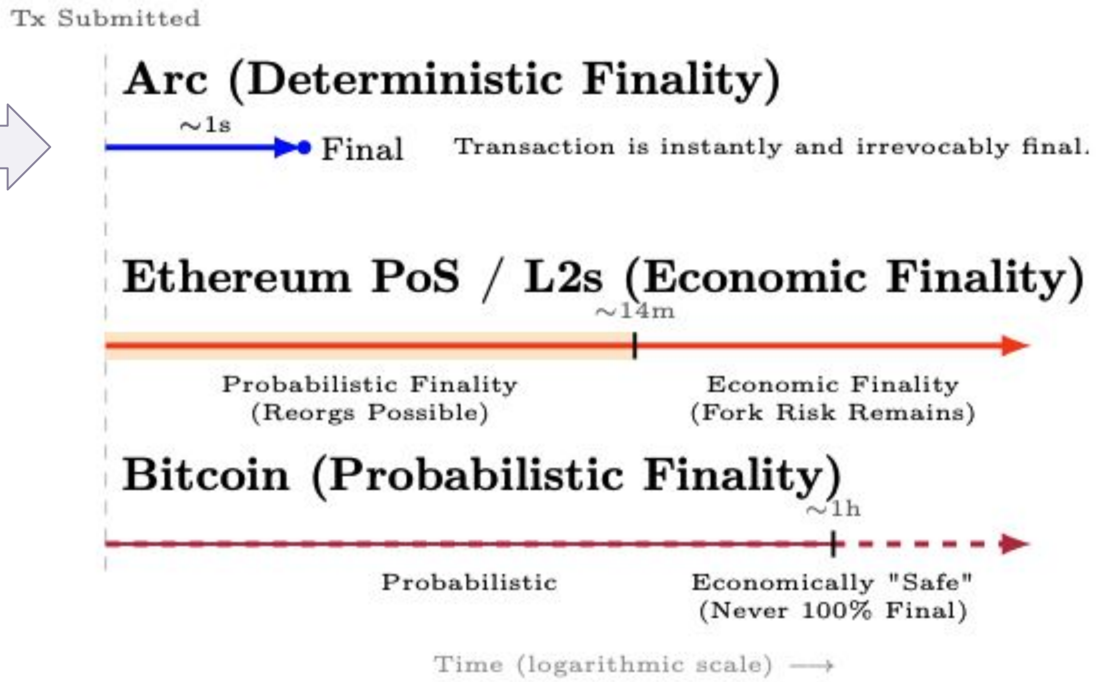

Tx Submitted
Arc (Deterministic Finality)
∼1s
Final
Transaction is instantly and irrevocably final.
Ethereum PoS / L2s (Economic Finality)
∼14m
Probabilistic Finality
(Reorgs Possible)
Economic Finality
(Fork Risk Remains)
Bitcoin (Probabilistic Finality)
∼1h
Probabilistic
Economically "Safe"
(Never 100% Final)
Time (logarithmic scale) ⟶

Figure 2: A timeline comparison of finality models.

Introducing a leader

- Bitcoin allows for multiple miners to create blocks at the same time
    - Problematic since forks will occur
- Idea: Only allow one miner to make a block
    - This miner is the leader
- Problems?
    - How is the leader role assigned?
    - What if the leader is offline?

Assigning leader roles

- The leader role must rotate, otherwise it’d be a centralized network
- Proof of Stake (PoS), like PoW, is a sybil resistance technique
    - We don’t want attackers to flood the network to gain lots of leader roles
- In PoW, miners demonstrate their commitment via hashing power
- In PoS, “validators” demonstrate their commitment via locking up money
    - This money is the native coin of the network (ex. ETH in Ethereum)
- Leaders are assigned based on a validators proportion of locked up money
    - If Alice locks away 100 ETH and the network at large locks away 5,000 ETH, then she will be the leader 100 / 5000 = 2% of the time

Offline leaders

- If a leader is offline, then they cannot make the block
- No one else can make the block
- The block is never created and the network will progress on to the next block
    - The progression happens after a timeout is reached
- Attackers can at most slow down block production by the length of the timeout

Tendermint

- A Byzantine Fault Tolerance (BFT) protocol
- The Tendermint protocol (2018) is a three round process
  - First, the leader tells fellow validators about their block
  - Second, the validators vote on the proposed block (66% threshold)
  - Third, the validators re-vote on the proposed block (66% threshold)
- If a block passes both rounds of voting, then it in included in the chain
- This is really fast! https://testnet.arcscan.app/

Deterministic Finality

- Blocks included in the chain will always be in the chain
- The leader role schedule is known to all participants
- Each leader “slot” is either a block that is included in the chain or skipped
  - Skips come from leaders being offline (as discussed), the block being invalid, or the block failing to collect sufficient votes
- No forks are possible, thus there is no need to wait for additional blocks

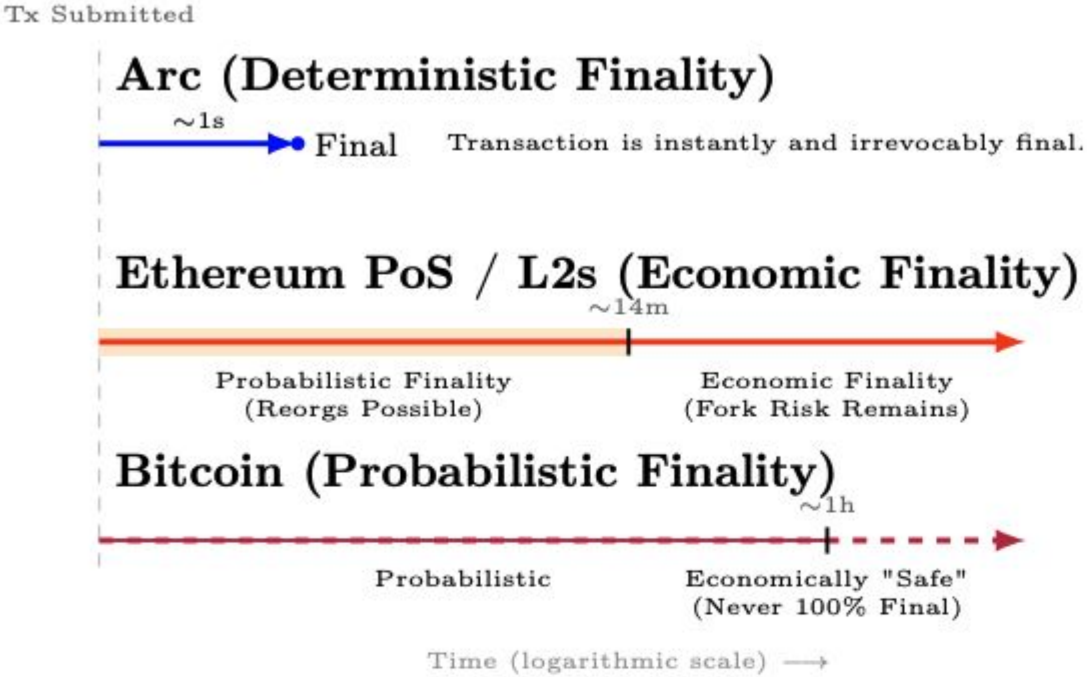
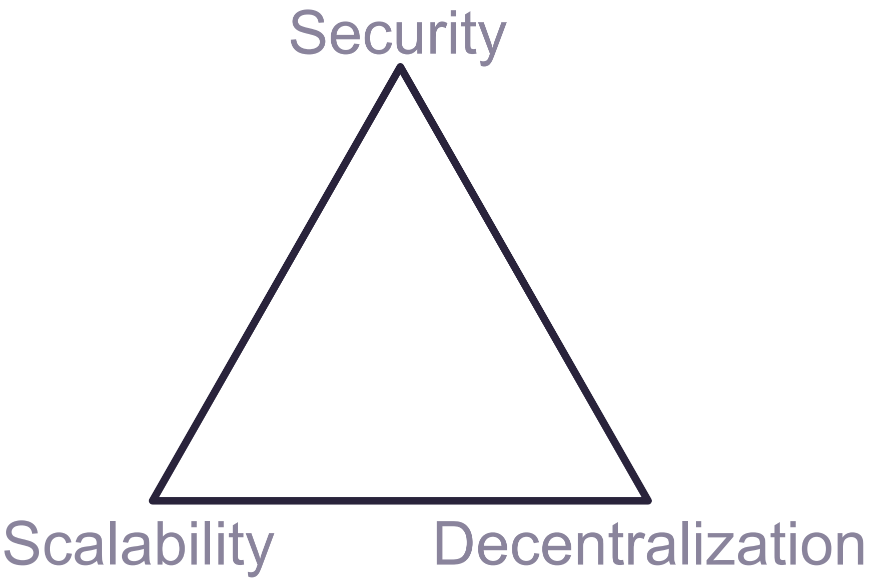

Tx Submitted
Arc (Deterministic Finality)
∼1s
Final
Transaction is instantly and irrevocably final.
Ethereum PoS / L2s (Economic Finality)
∼14m
Probabilistic Finality
(Reorgs Possible)
Economic Finality
(Fork Risk Remains)
Bitcoin (Probabilistic Finality)
∼1h
Probabilistic
Economically "Safe"
(Never 100% Final)
Time (logarithmic scale) ⟶

Figure 2: A timeline comparison of finality models.

Trade offs

- There is a well known trilemma in blockchains
- Where is Bitcoin?
- Where is Arc?



Thank you! Questions?

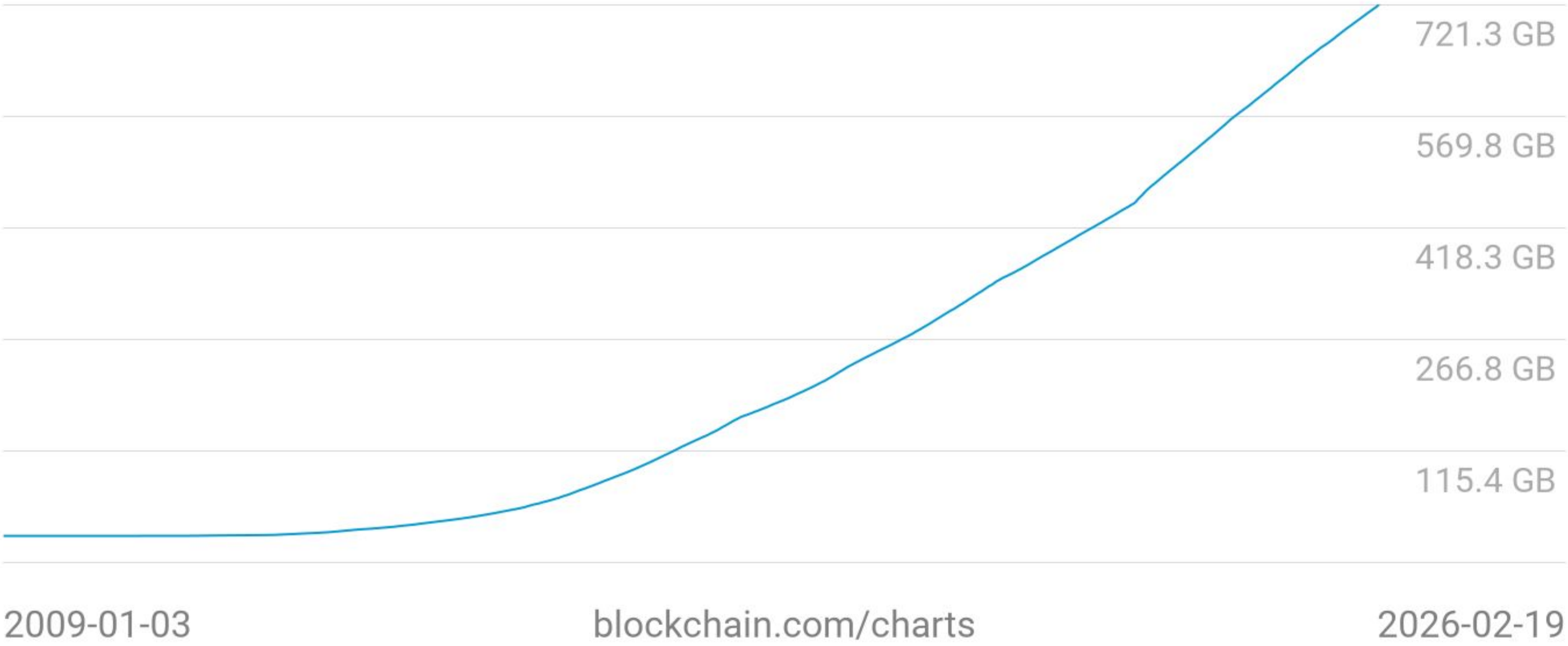
Resources

- https://learnmeabitcoin.com/
- https://satoshi.nakamotoinstitute.org/
- Good reads
  - https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared
  - https://blog.lopp.net/history-bitcoin-transaction-dust-spam-storms/
- Tendermint paper: https://arxiv.org/pdf/1807.04938
- Malachite: https://github.com/circlefin/malachite
  - Tendermint variant used by Arc
- Arc website: https://www.arc.network/

Bitcoin Appendix

Blockchain Size

721.4 GB



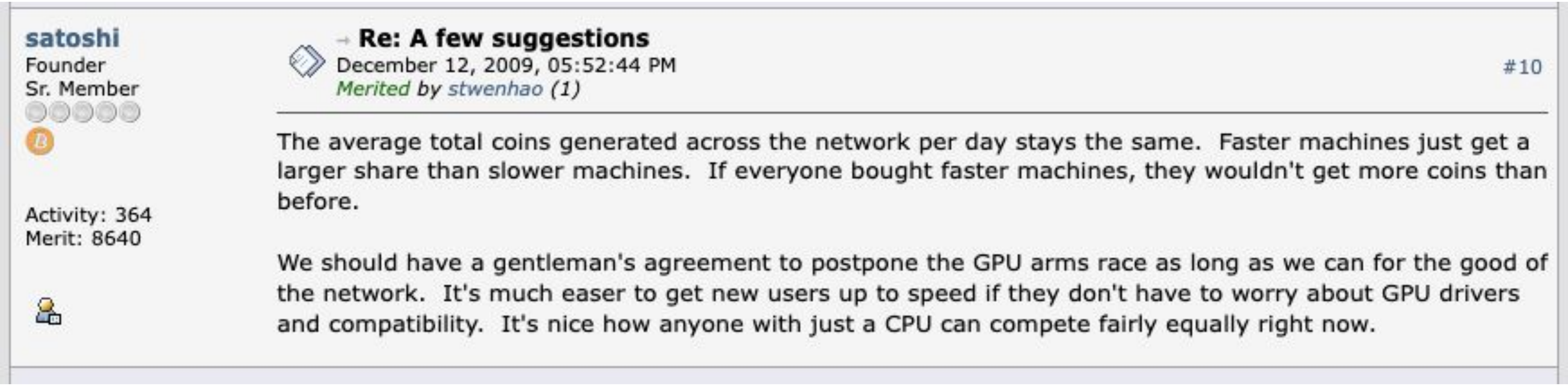
blockchain.com/charts

Headers only…

- Size of header: 80 bytes
- # blocks: ~938,000
- Size of blockchain headers only: ~75 MB
    - Much more manageable!

Industrialization of Mining

- PoW is hard, so people naturally gravitated towards more powerful machines
- CPU -> GPU -> ASIC (Application-Specific Integrated Circuit)
- Satoshi wasn't a fan…



satoshi
Founder
Sr. Member

Activity: 364
Merit: 8640

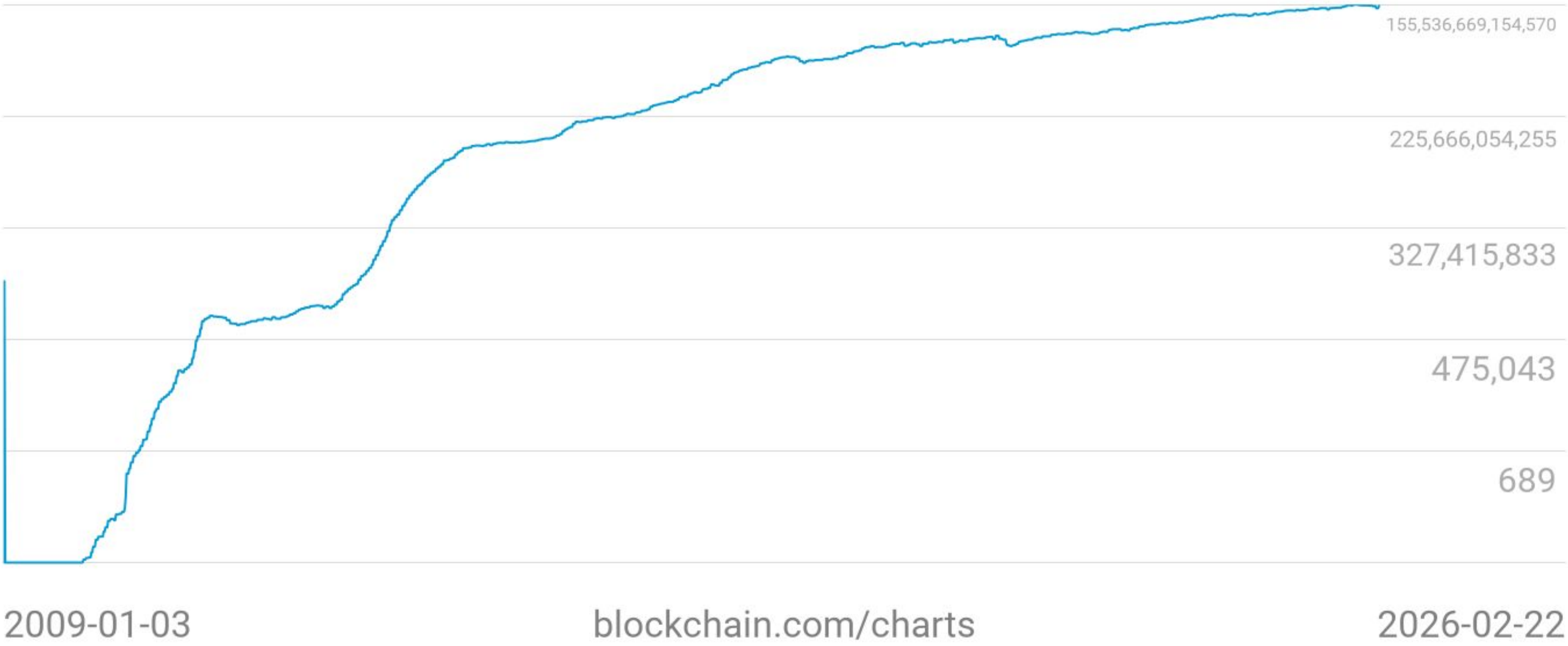
Re: A few suggestions
December 12, 2009, 05:52:44 PM
Merited by stwenhao (1)
#10

The average total coins generated across the network per day stays the same. Faster machines just get a larger share than slower machines. If everyone bought faster machines, they wouldn't get more coins than before.

We should have a gentleman's agreement to postpone the GPU arms race as long as we can for the good of the network. It's much easer to get new users up to speed if they don't have to worry about GPU drivers and compatibility. It's nice how anyone with just a CPU can compete fairly equally right now.

Difficulty

144,398,401,518,100



blockchain.com/charts