Sustainable Blockchains

Krzysztof Pietrzak

Institute of Science and Technology Austria

Public Lecture Series "Sustainability in Computer Science"

Nov. 3 2025

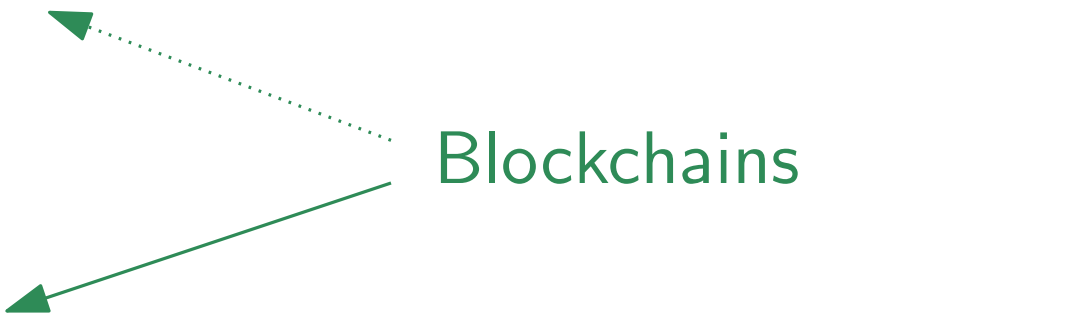
- Centralized (DigiCash)
  one party controls everything

- Decentralized but Permissioned (Hyperledger,. . .)
  fixed list of parties

- Fully Permissionless (Bitcoin, Chia, Ethereum,. . .)
  everyone can participate!

- Centralized (DigiCash)
  one party controls everything

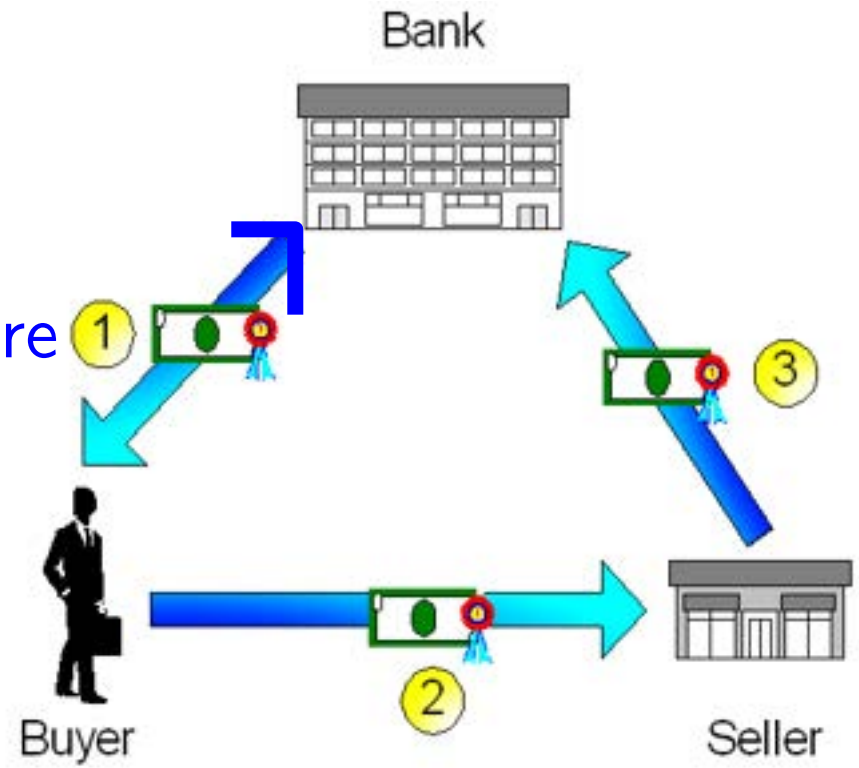
- Decentralized but Permissioned (Hyperledger,. . .)
  fixed list of parties



- Fully Permissionless (Bitcoin, Chia, Ethereum,. . .)
  everyone can participate!

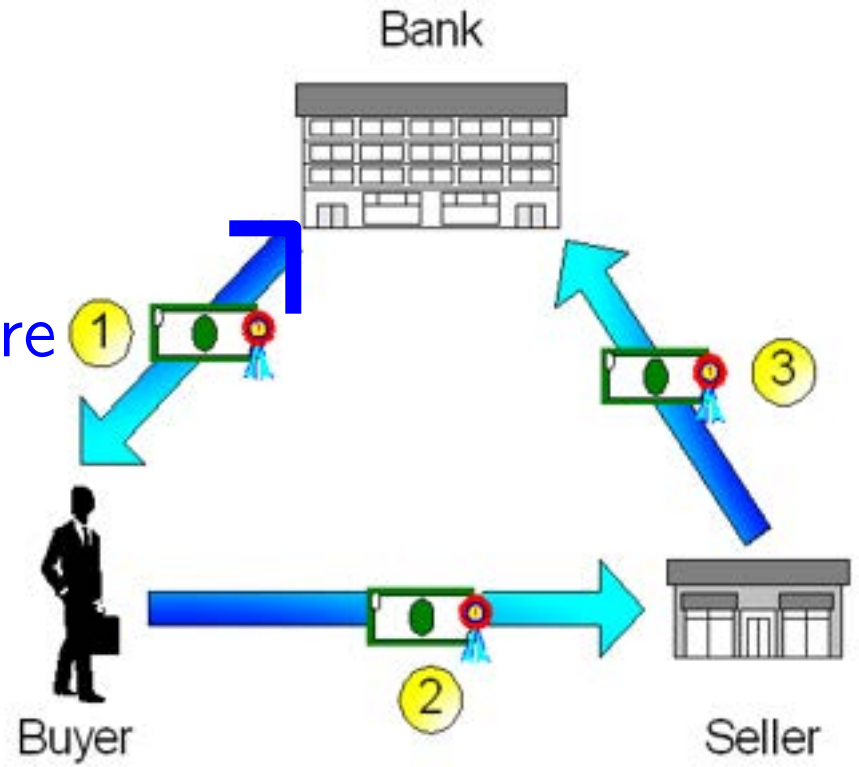
(Centralized) Anonymous E-Cash, 80-90's

Blind Signature

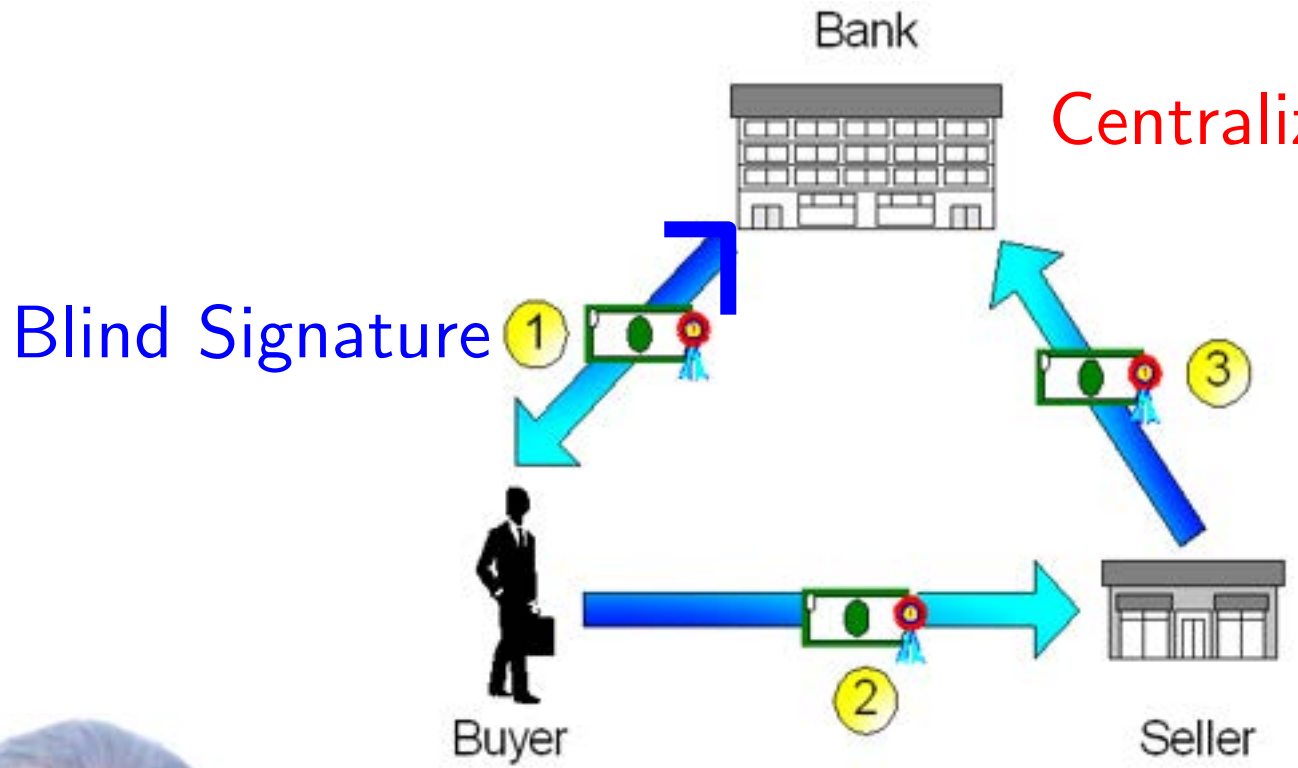


(Centralized) Anonymous E-Cash, 80-90's

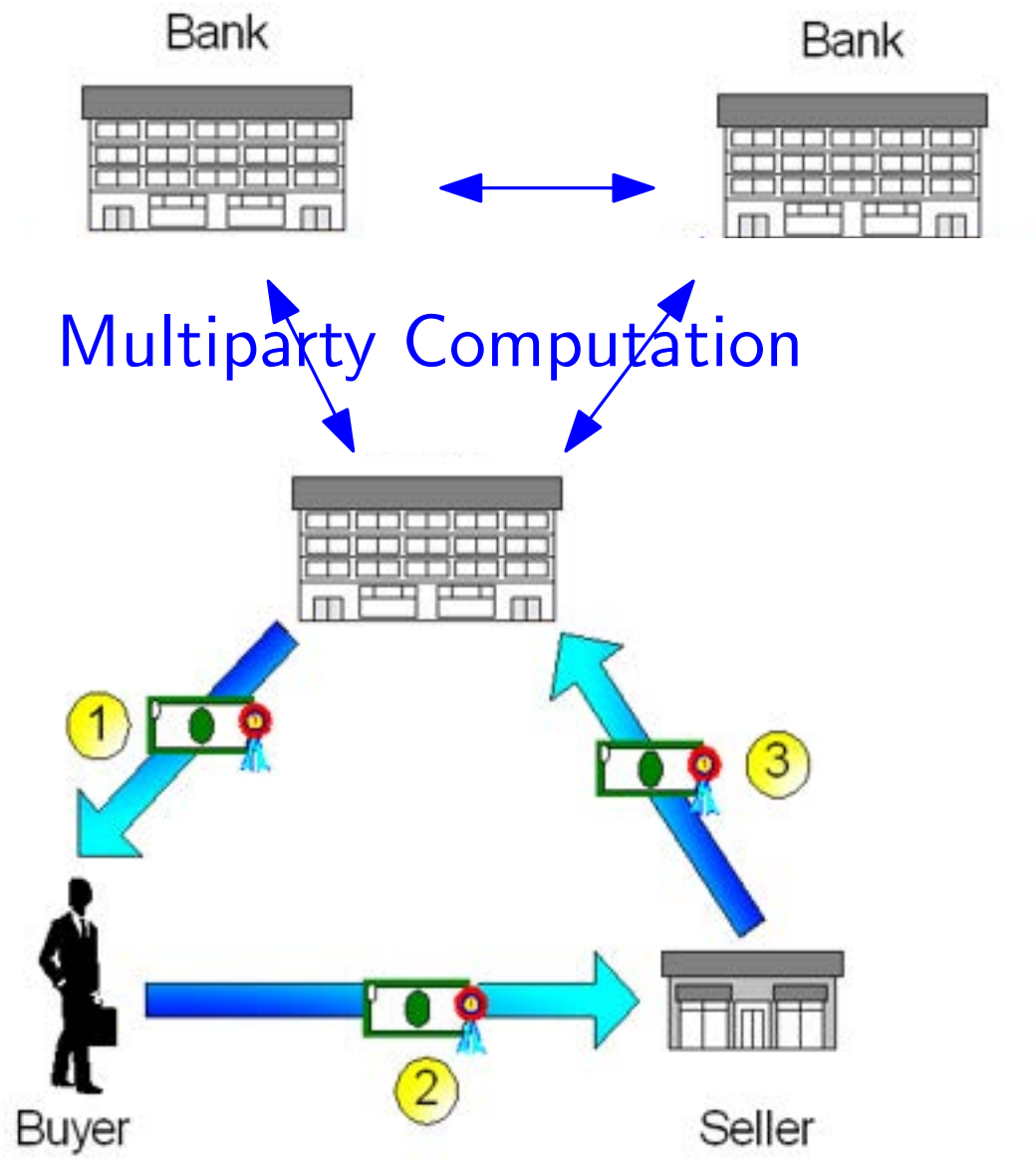
Blind Signature



(Centralized) Anonymous E-Cash, 80-90's

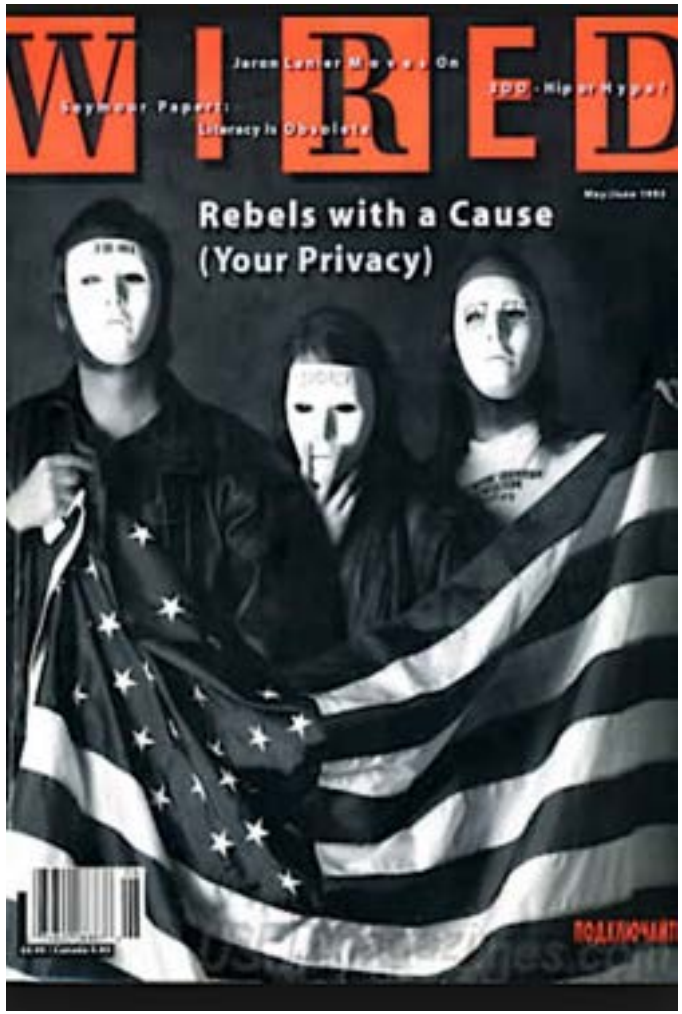


Decentralization using 80s Crypto



https://en.wikipedia.org/wiki/Cypherpunk

A **cypherpunk** is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.



Permissonless E-Cash / Nov. 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.

Bitcoin Consensus

Consensus in a permissionless setting is impossible

Bitcoin Consensus

Consensus in a permissionless setting is impossible

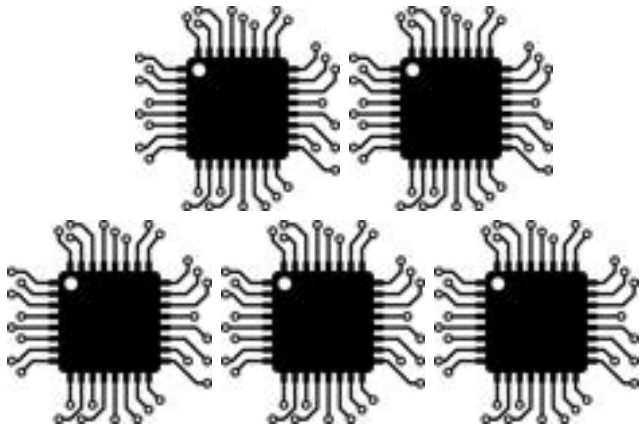
Bitcoin Consensus

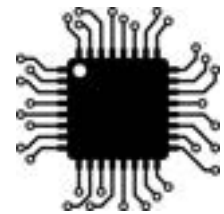
Consensus in a permissionless setting is impossible

Bitcoin Consensus

Nakamoto Consensus

Assumption: Majority of computing power controlled by honest parties

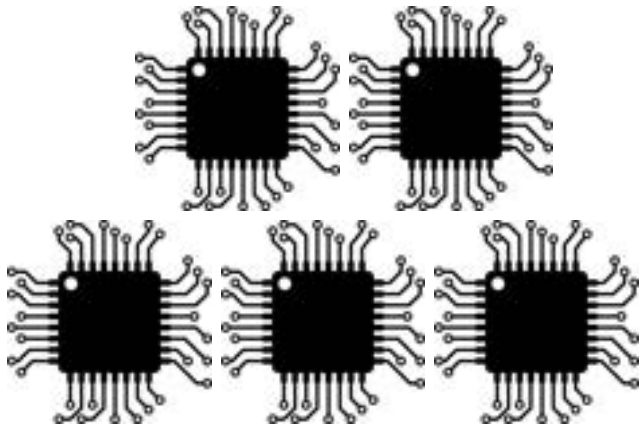


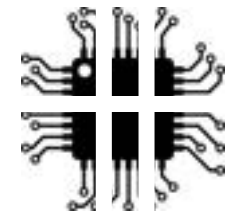


Bitcoin Consensus

Nakamoto Consensus

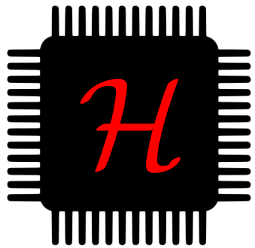
Assumption: Majority of computing power controlled by honest parties





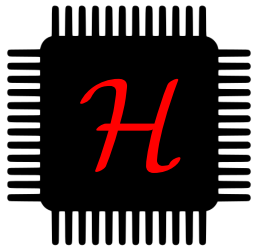
Proofs of Work [DworkNaor92]

How can  prove that it evaluated $\mathcal{H}$ 10^9 times?



Proofs of Work [DworkNaor92]

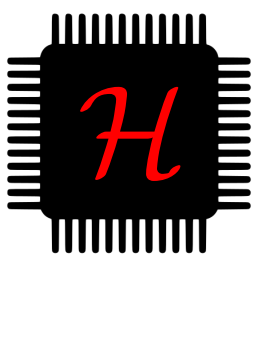
How can  prove that it evaluated $\mathcal{H}$ 10^9 times?



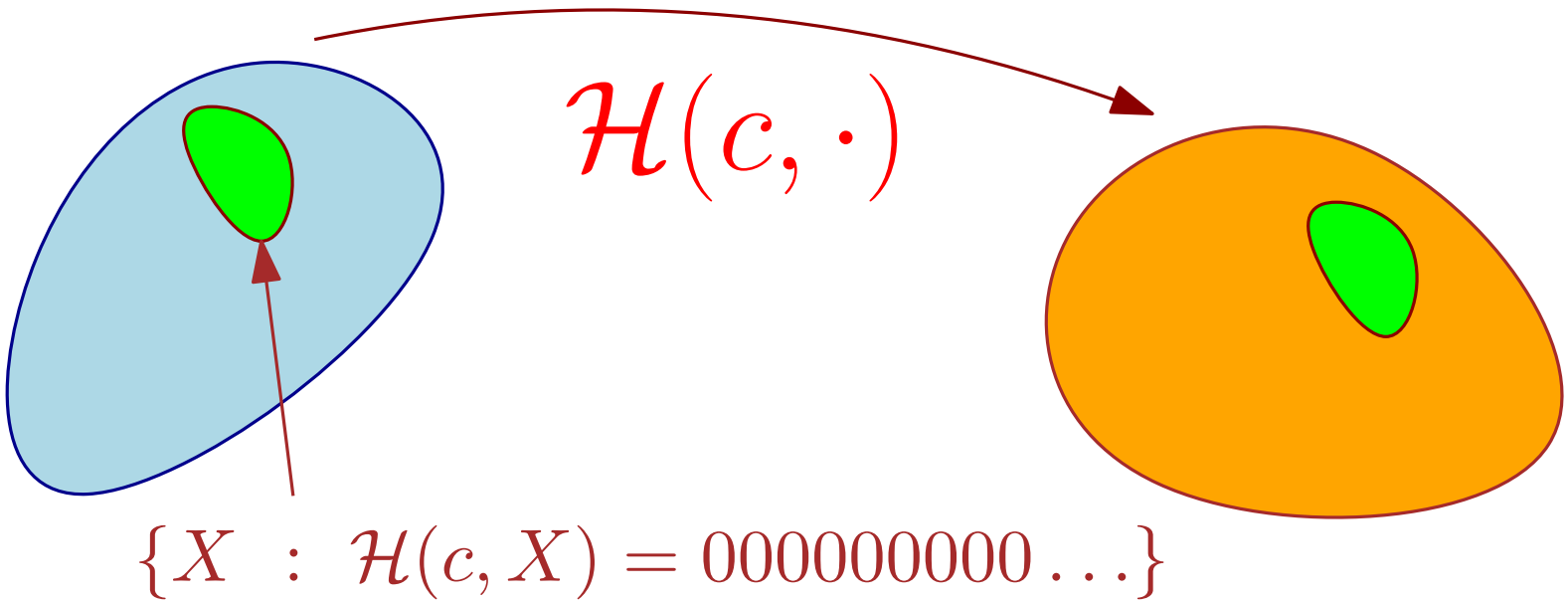
$\mathcal{H}(1)$
$\mathcal{H}(2)$
$\mathcal{H}(3)$
$\vdots$
$\mathcal{H}(1000000000)$

Proofs of Work [DworkNaor92]

How can  prove that it evaluated $\mathcal{H}$ 10^9 times?

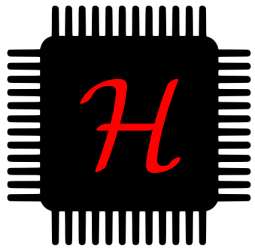


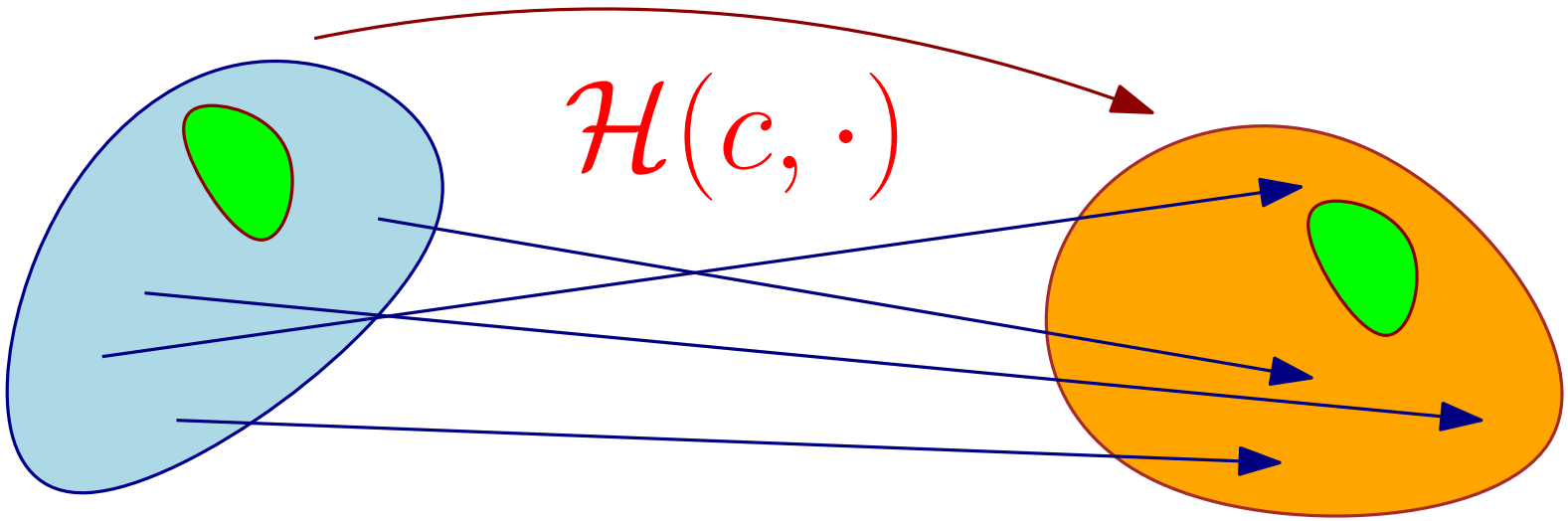
c



Proofs of Work [DworkNaor92]

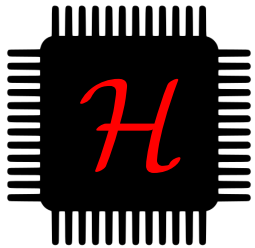
How can  prove that it evaluated $\mathcal{H}$ 10^9 times?

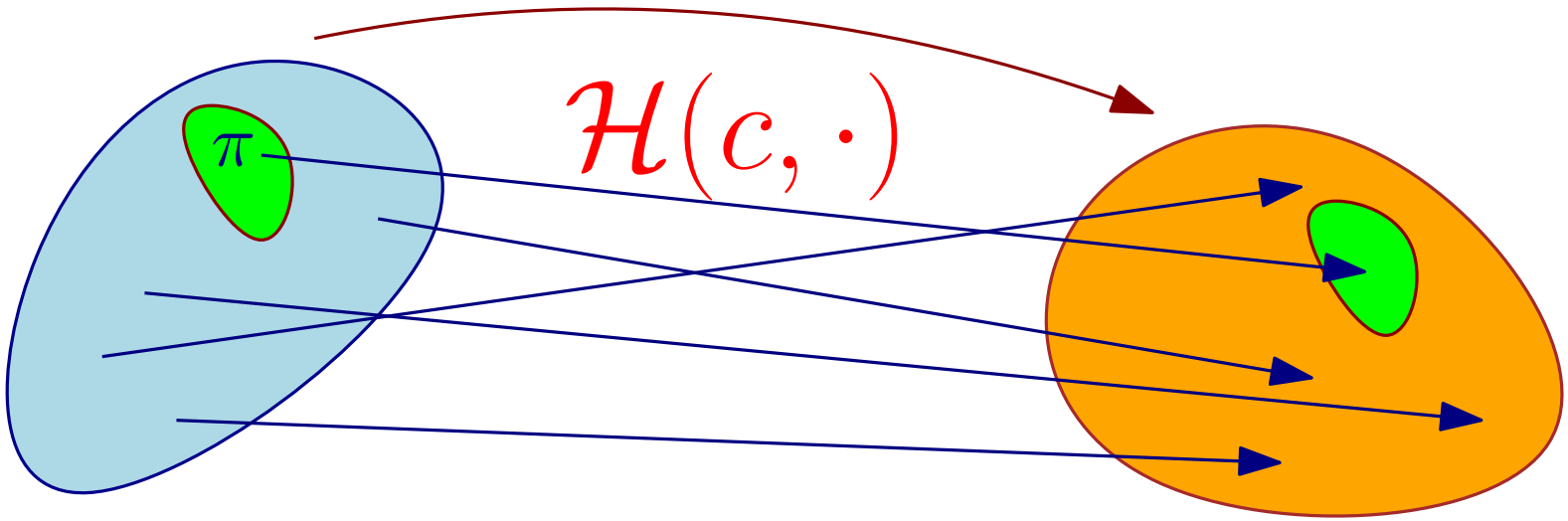




Proofs of Work [DworkNaor92]

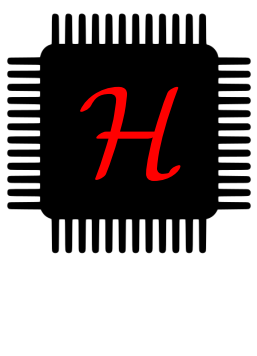
How can  prove that it evaluated $\mathcal{H}$ 10^9 times?





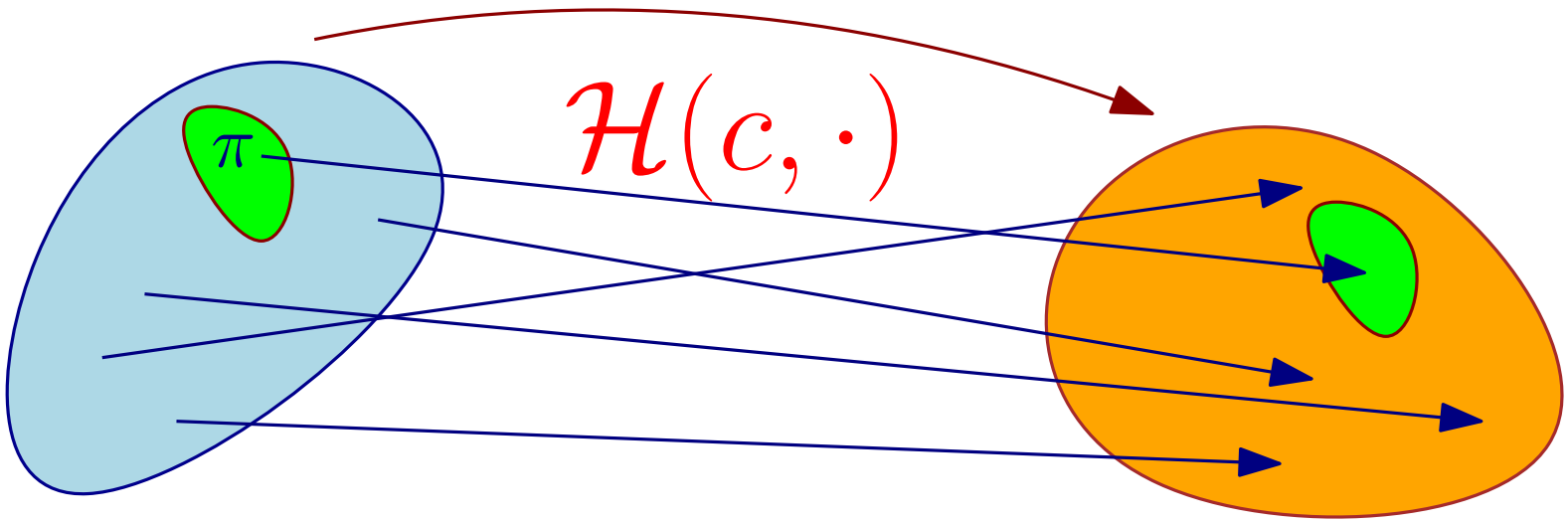
Proofs of Work [DworkNaor92]

How can  prove that it evaluated $\mathcal{H}$ 10^9 times?



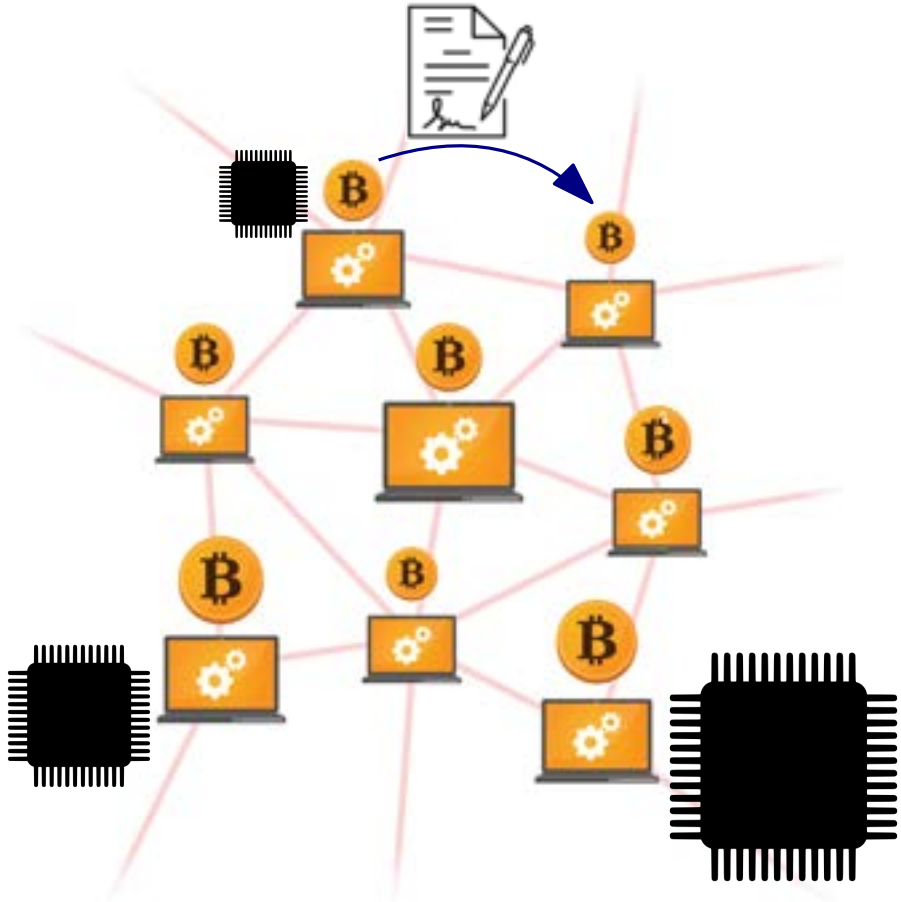
π

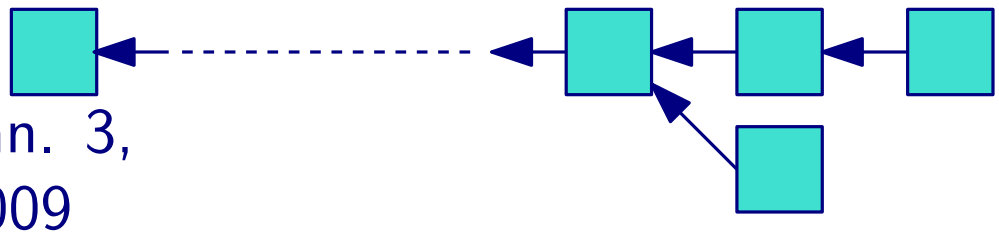
$\mathcal{H}(c, \pi) \stackrel{?}{=} 000000000 \star\star\star\star$



10^9 required in expectation to find a proof π

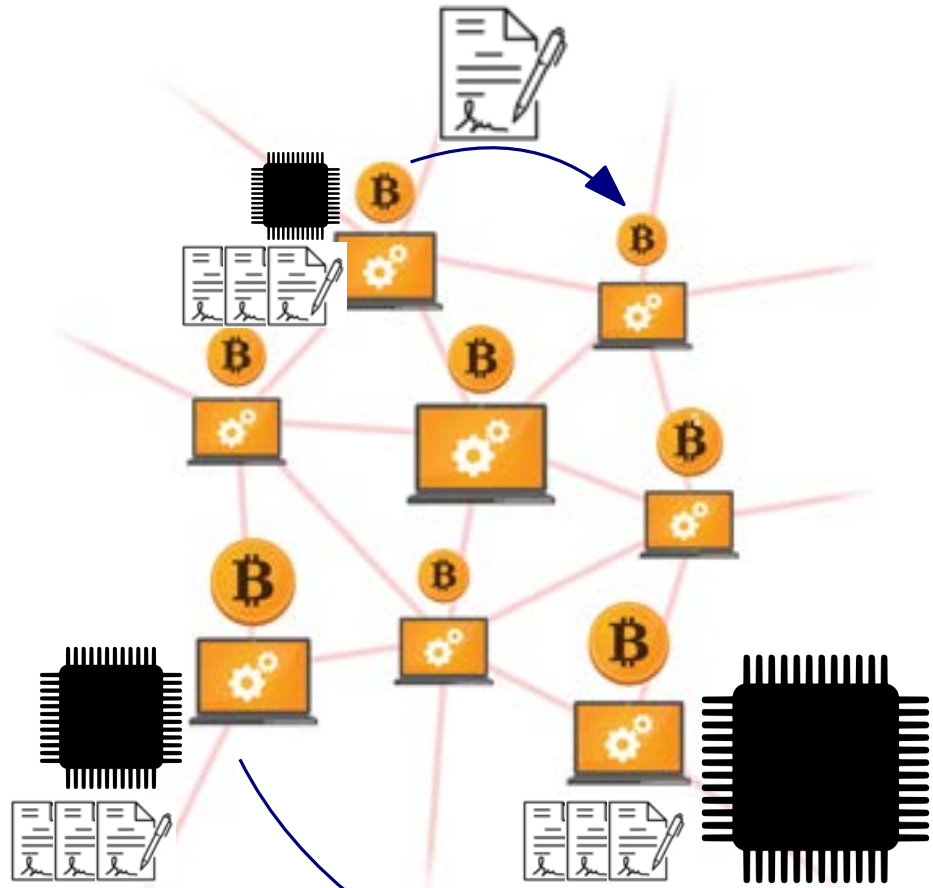
Proofs of Work in Bitcoin

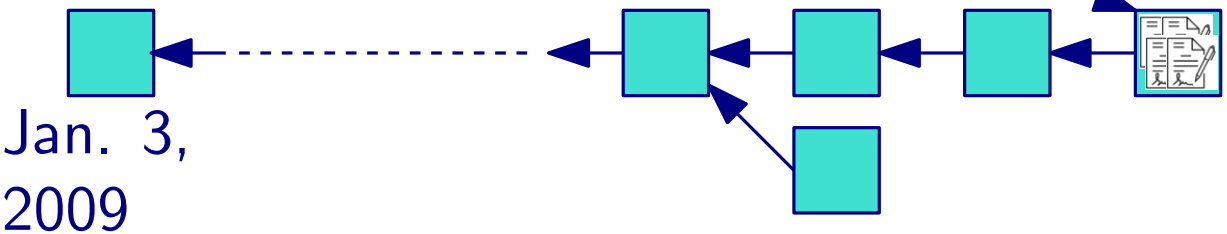




Jan. 3, 2009

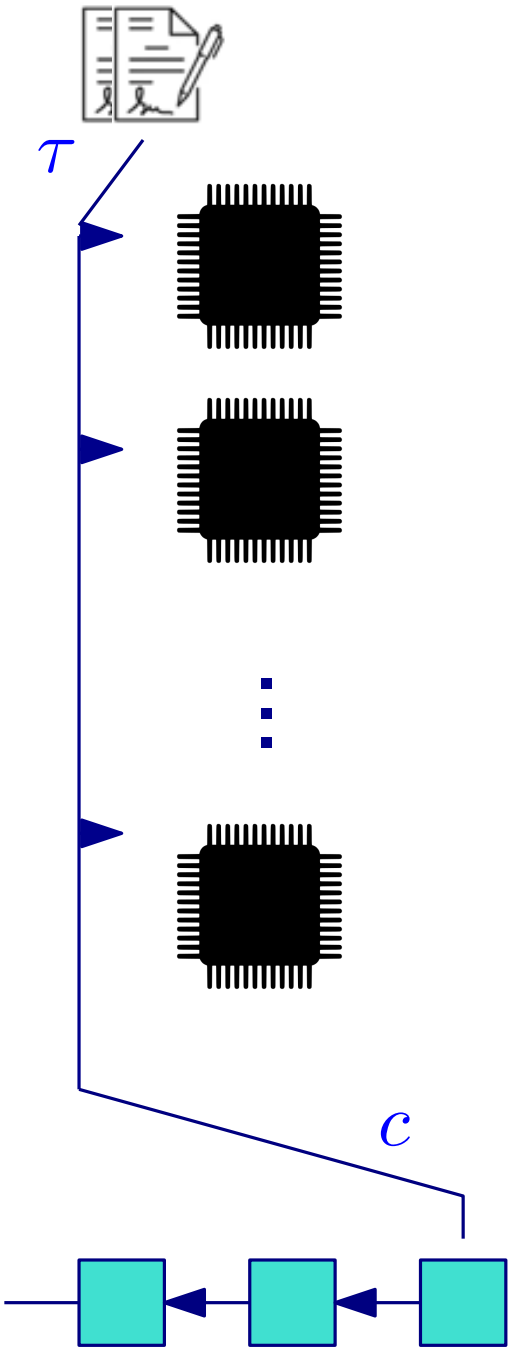
Proofs of Work in Bitcoin



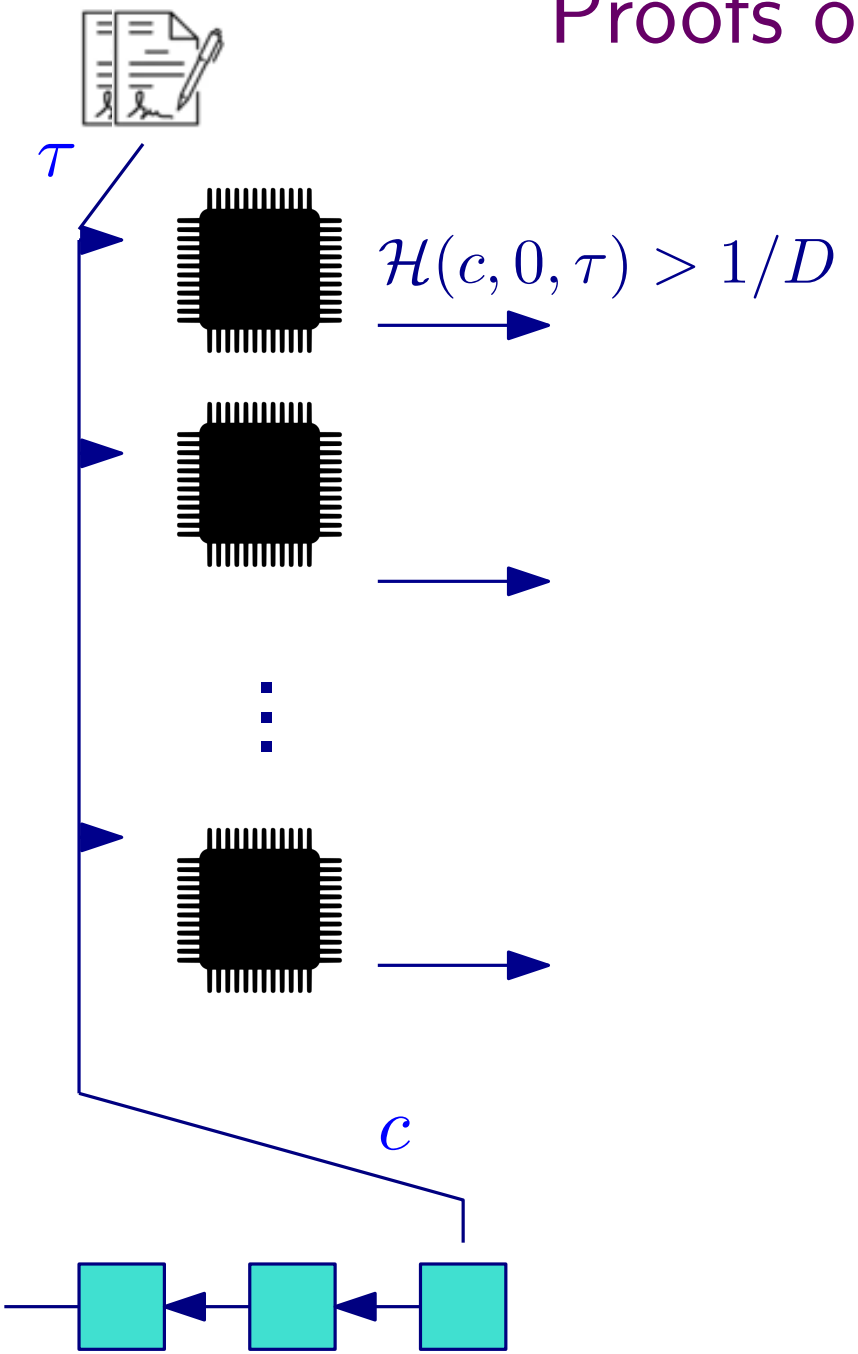


Jan. 3, 2009

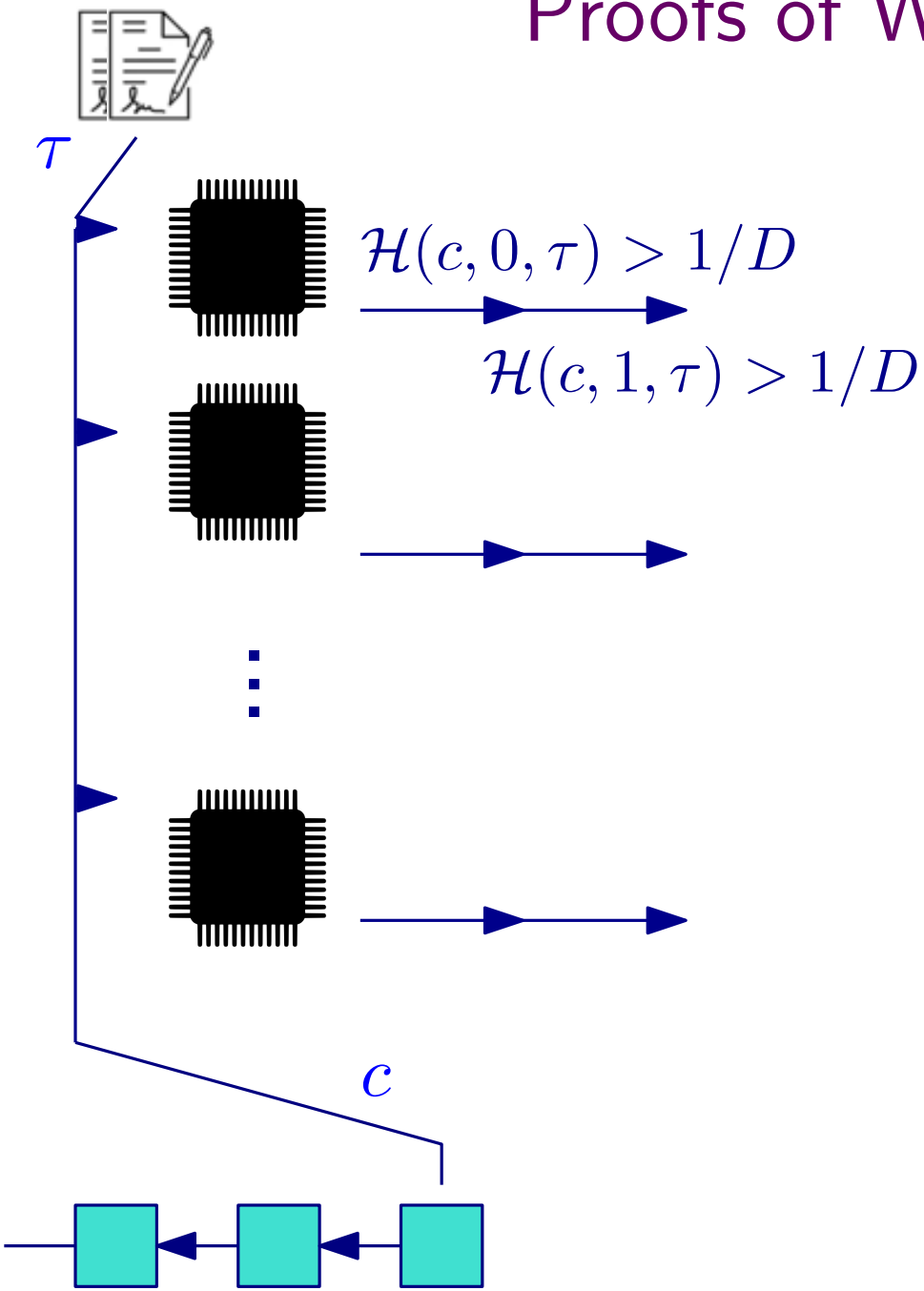
Proofs of Work in Bitcoin



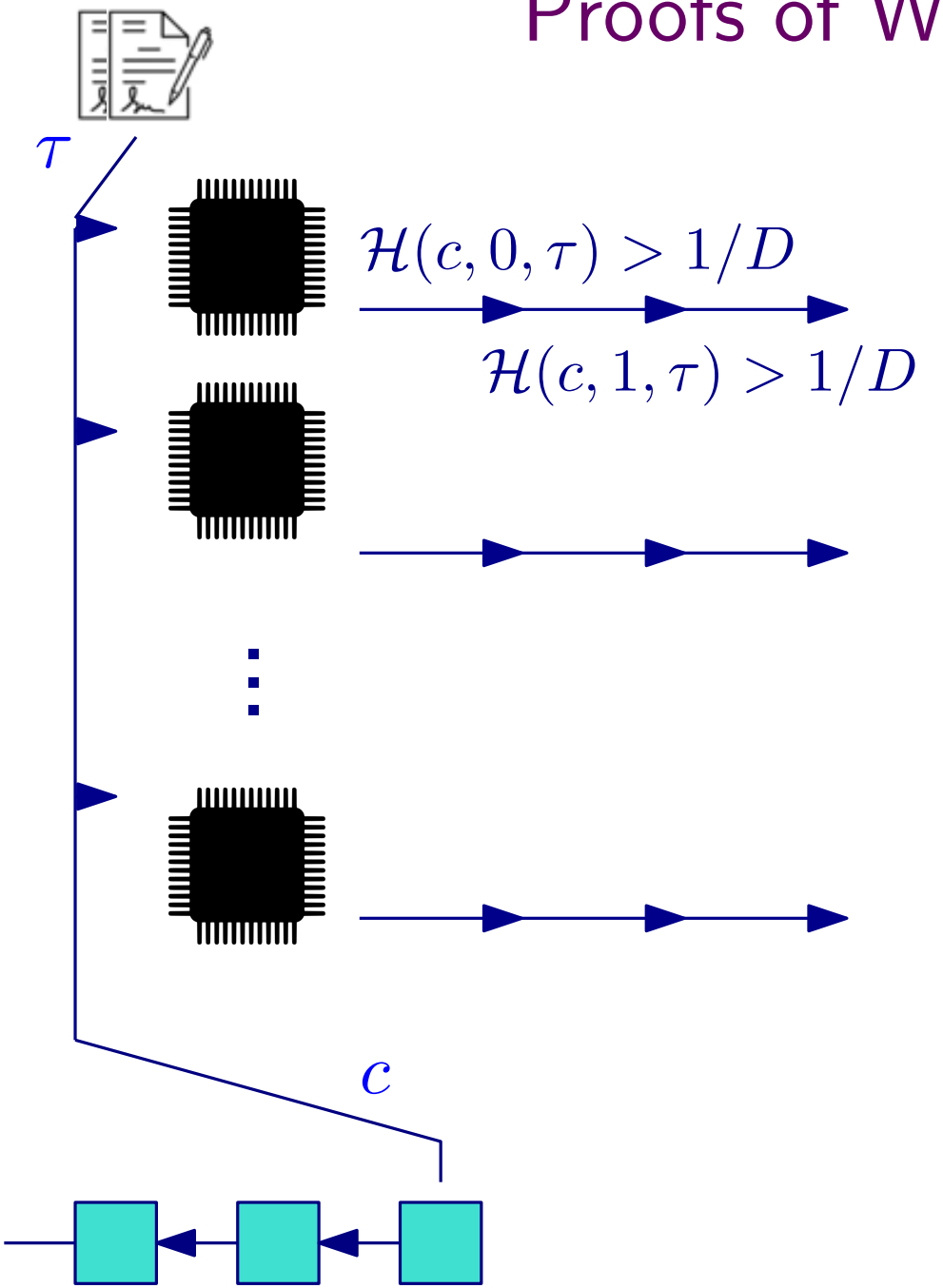
Proofs of Work in Bitcoin



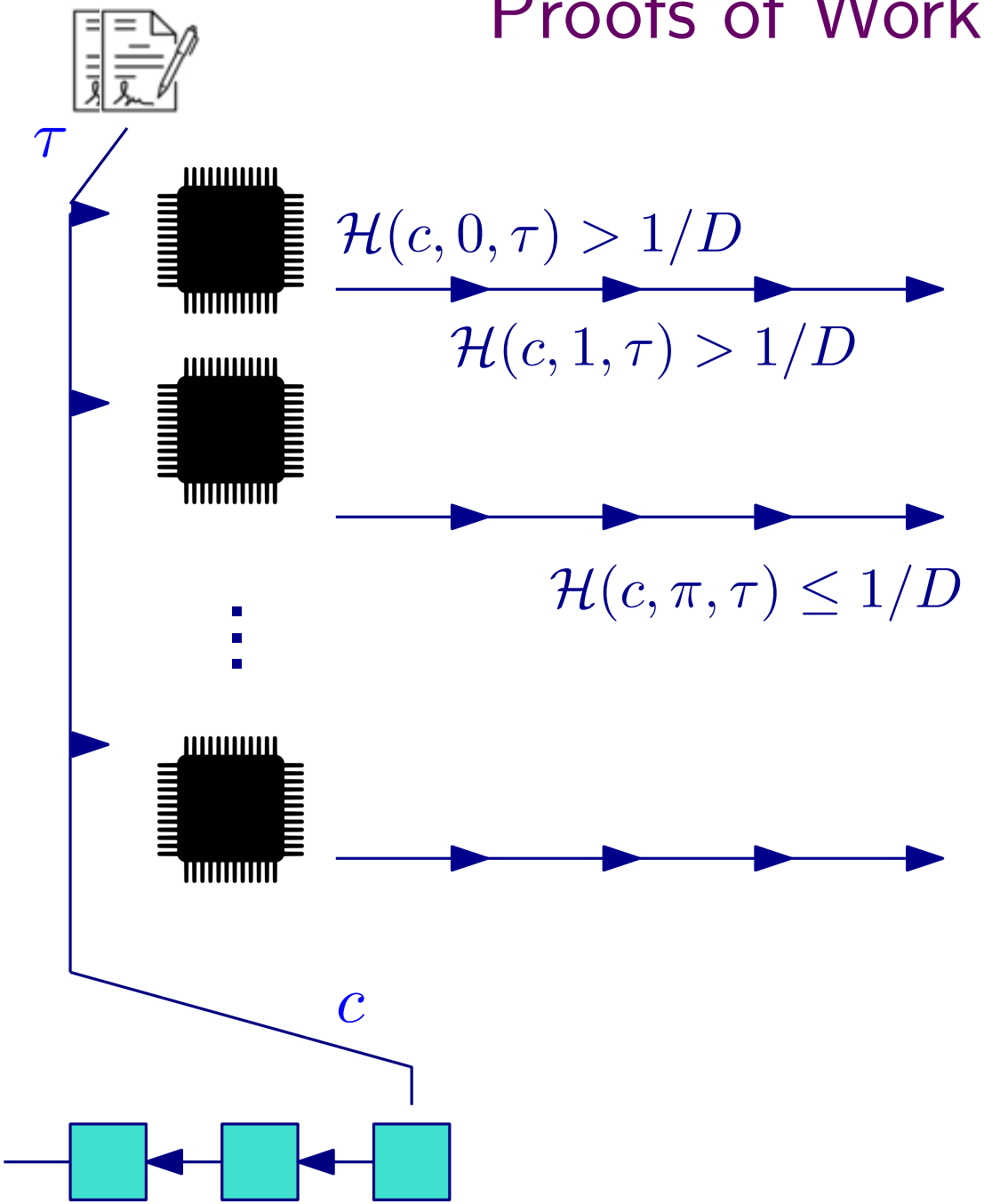
Proofs of Work in Bitcoin



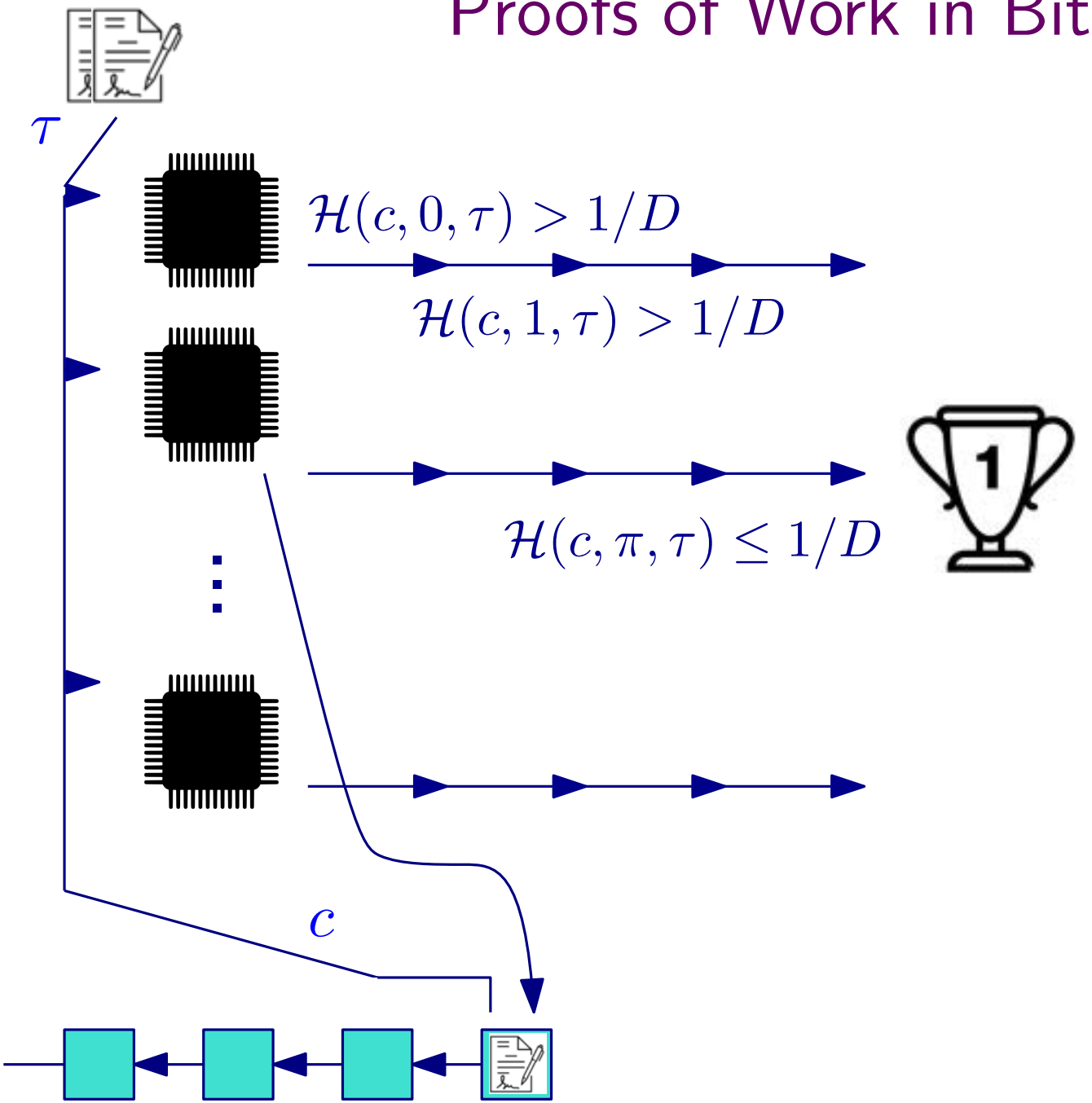
Proofs of Work in Bitcoin



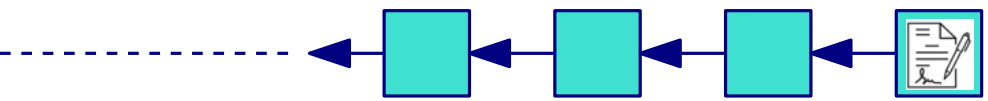
Proofs of Work in Bitcoin



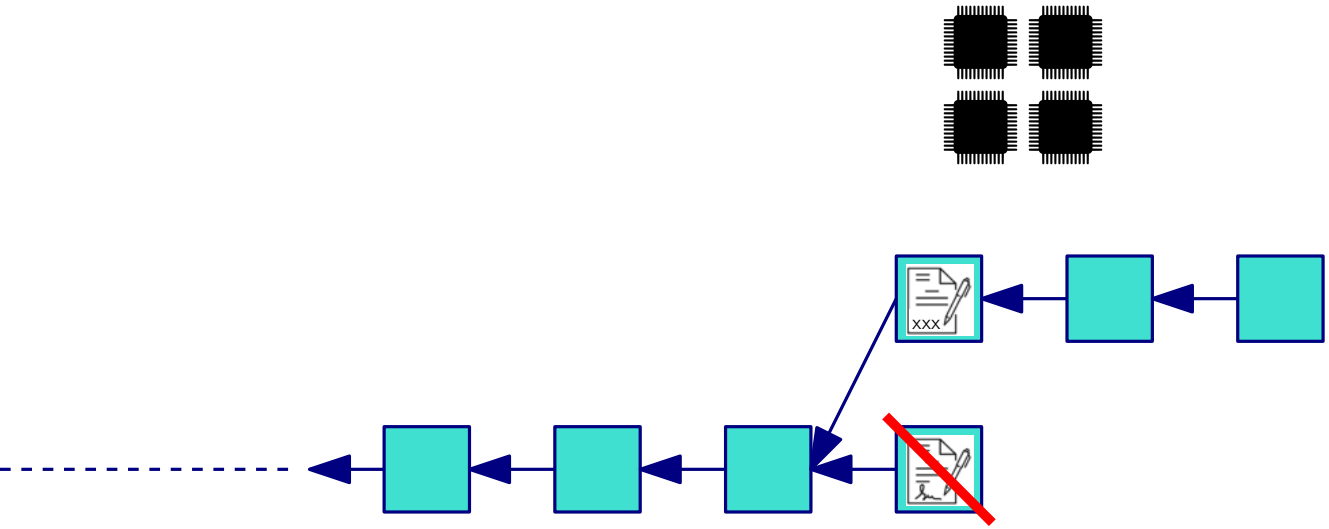
Proofs of Work in Bitcoin



Security of Bitcoin

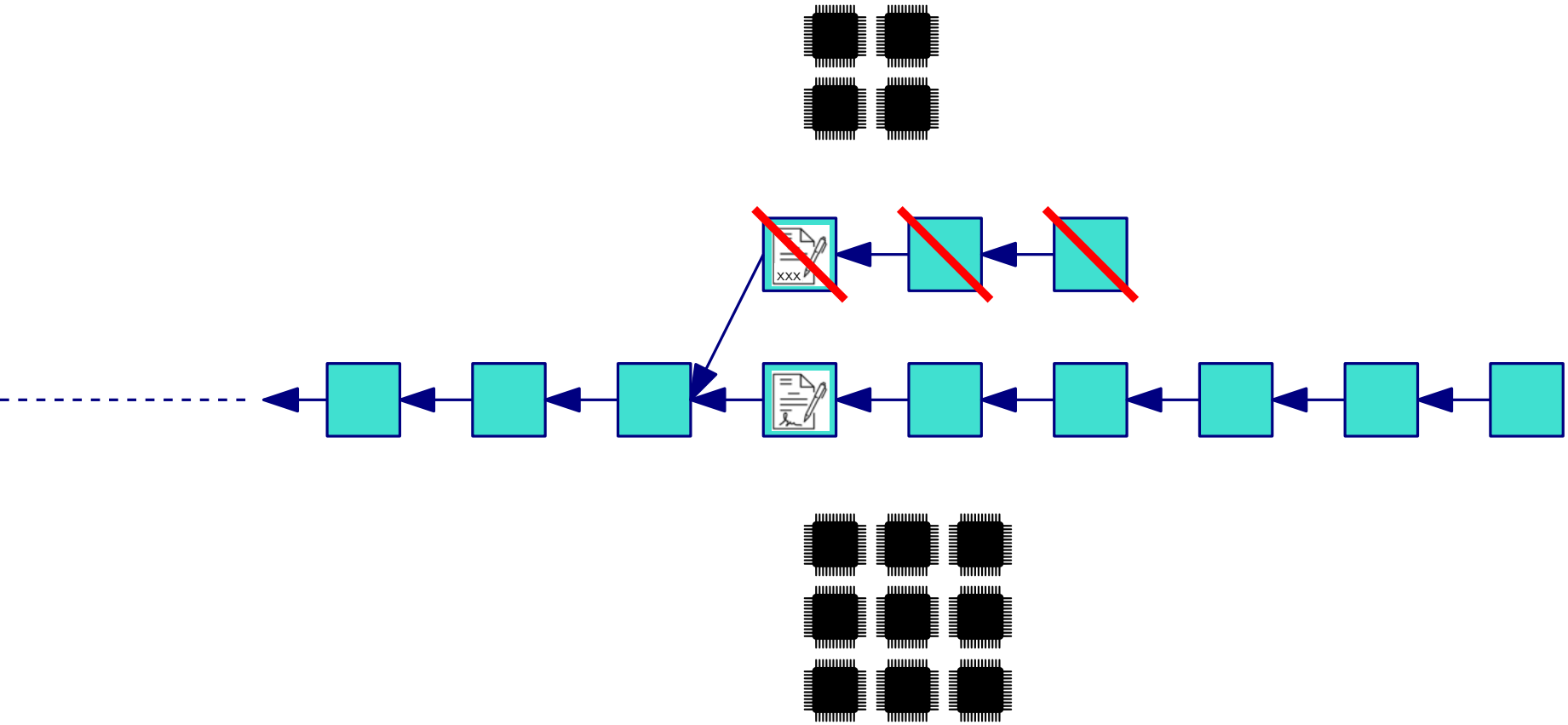


Security of Bitcoin



Security of Bitcoin

Security of Bitcoin



101 Blockchains

PERMISSIONED VS PERMISSIONLESS

PERMISSIONLESS BLOCKCHAIN

WHAT ARE PERMISSIONLESS BLOCKCHAINS?

Permissionless blockchains are blockchains that require no permission to join and interact with.

CHARACTERISTICS

- Truly decentralized
- Transparent network
- Immutability

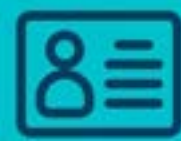
ADVANTAGES

- Open to all
- Brings trust to all users
- Offers high security

DISADVANTAGES

- Slow transaction speed
- Harder to scale
- Not energy efficient

USE CASES



- Digital Identity
- Voting
- Fundraising

PERMISSIONED BLOCKCHAIN

WHAT ARE PERMISSIONED BLOCKCHAINS?

Permissioned blockchains are blockchains that require permission to join and participate in consensus.

CHARACTERISTICS

- Governance structure
- Private transactions
- Authentication process

ADVANTAGES

- Extremely fast output
- Scalable network
- Offers energy efficiency

DISADVANTAGES

- Not truly decentralized
- Less transparent
- Partial immutability

USE CASES

- Food tracking
- Banking and payments
- Supply chain management

101 Blockchains

PERMISSIONED VS PERMISSIONLESS

PERMISSIONLESS BLOCKCHAIN

WHAT ARE PERMISSIONLESS BLOCKCHAINS?

Permissionless blockchains are blockchains that require no permission to join and interact with.

CHARACTERISTICS

- Truly decentralized
- Transparent network
- Immutability

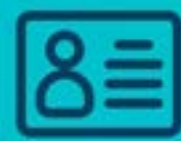
ADVANTAGES

- Open to all
- Brings trust to all users
- Offers high security

DISADVANTAGES

- Slow transaction speed
- Harder to scale
- Not energy efficient

USE CASES



- Digital Identity
- Voting
- Fundraising

PERMISSIONED BLOCKCHAIN

WHAT ARE PERMISSIONED BLOCKCHAINS?

Permissioned blockchains are blockchains that require permission to join and participate in consensus.

CHARACTERISTICS

- Governance structure
- Private transactions
- Authentication process

ADVANTAGES

- Extremely fast output
- Scalable network
- Offers energy efficiency

DISADVANTAGES

- Not truly decentralized
- Less transparent
- Partial immutability

USE CASES

- Food tracking
- Banking and payments
- Supply chain management

101 Blockchains

PERMISSIONED VS PERMISSIONLESS

PERMISSIONLESS BLOCKCHAIN

WHAT ARE PERMISSIONLESS BLOCKCHAINS?

Permissionless blockchains are blockchains that require no permission to join and interact with.

CHARACTERISTICS

- Truly decentralized
- Transparent network
- Immutability

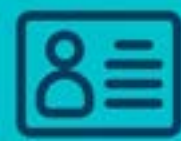
ADVANTAGES

- Open to all
- Brings trust to all users
- Offers high security

DISADVANTAGES

- Slow transaction speed
- Harder to scale
- Not energy efficient

USE CASES



- Digital Identity
- Voting
- Fundraising

PERMISSIONED BLOCKCHAIN

WHAT ARE PERMISSIONED BLOCKCHAINS?

Permissioned blockchains are blockchains that require permission to join and participate in consensus.

CHARACTERISTICS

- Governance structure
- Private transactions
- Authentication process

ADVANTAGES

- Extremely fast output
- Scalable network
- Offers energy efficiency

DISADVANTAGES

- Not truly decentralized
- Less transparent
- Partial immutability

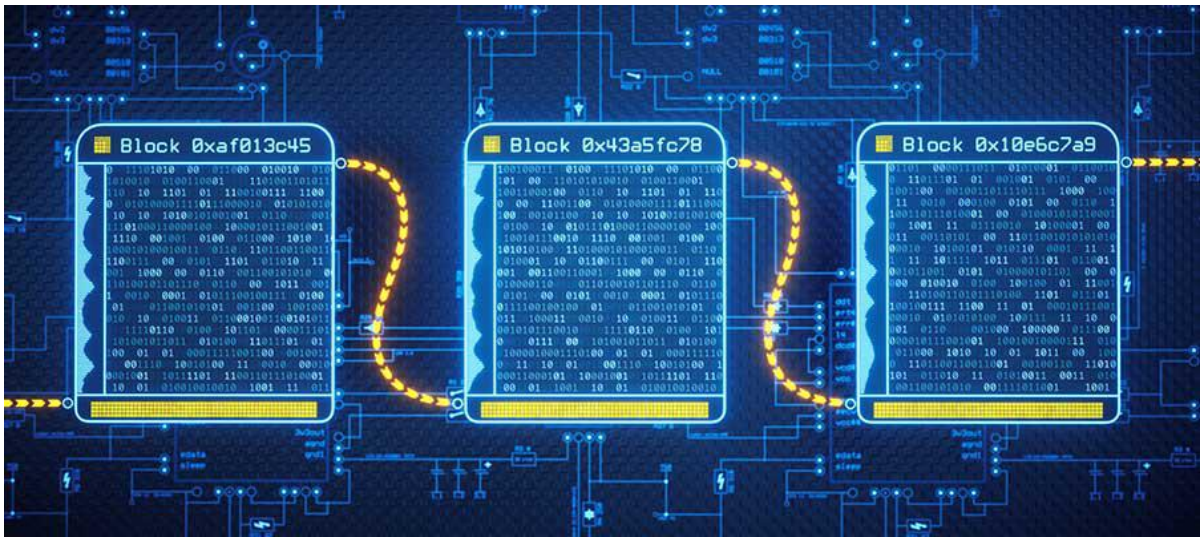
USE CASES

- Food tracking
- Banking and payments
- Supply chain management

Consnsus and Application Layer

Application layer

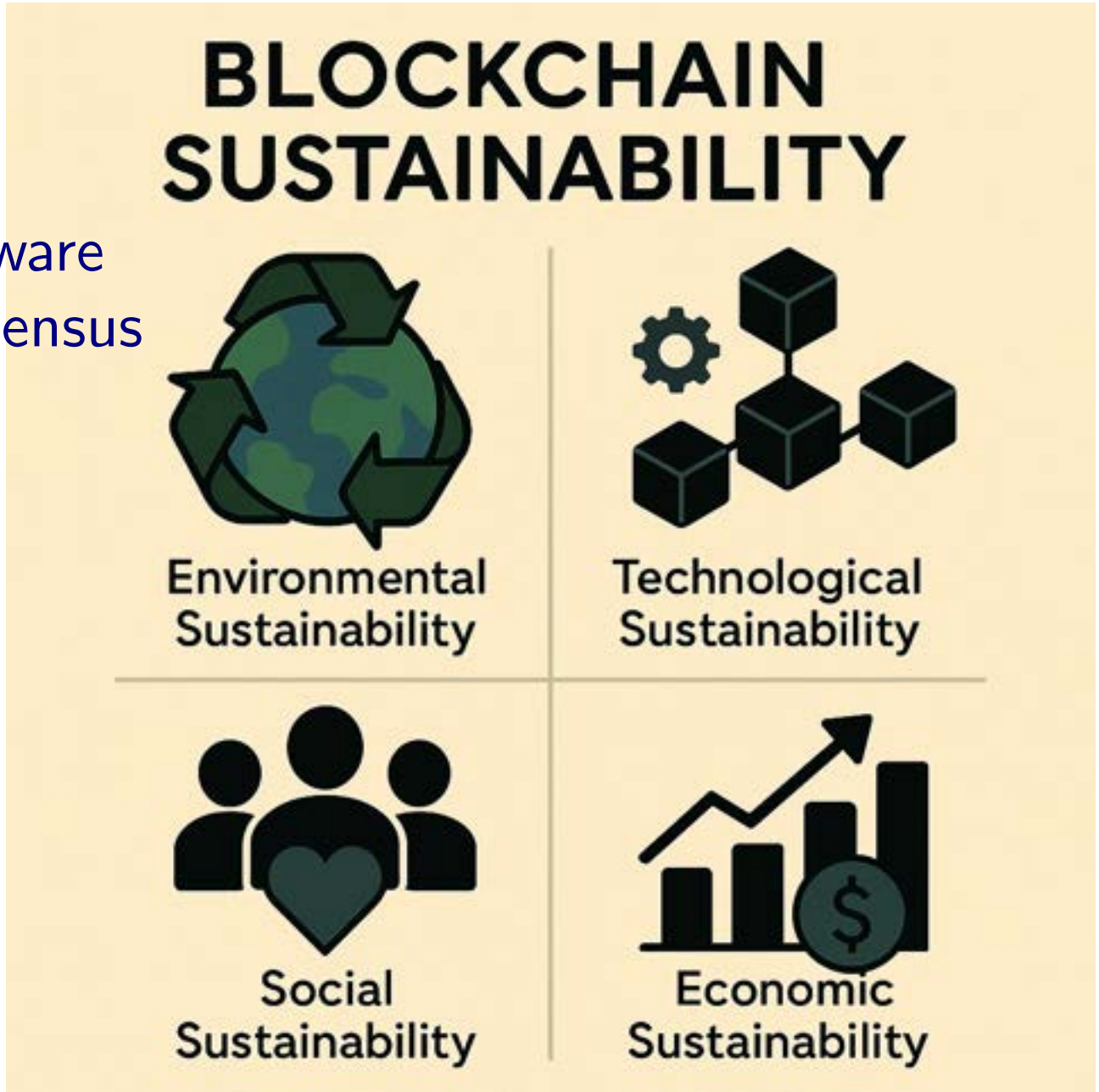
- UTXA/transactions (Bitcoin)
- Smart Contracts (Ethereum)



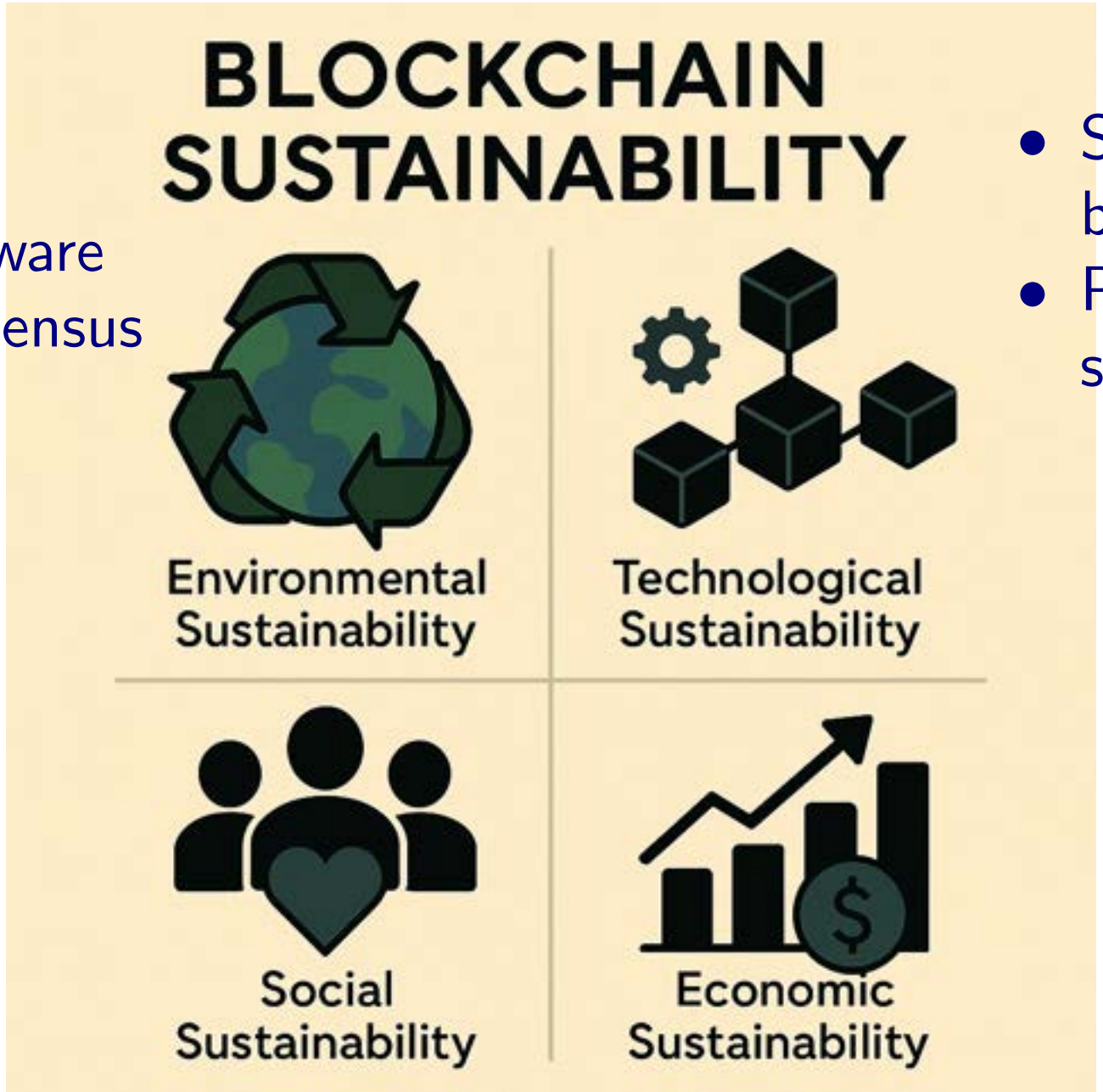
Consensus Layer

- Throughput
- Finality/Latency
- Proof of Work vs. Proof of Stake

Energy/Hardware
waste of consensus



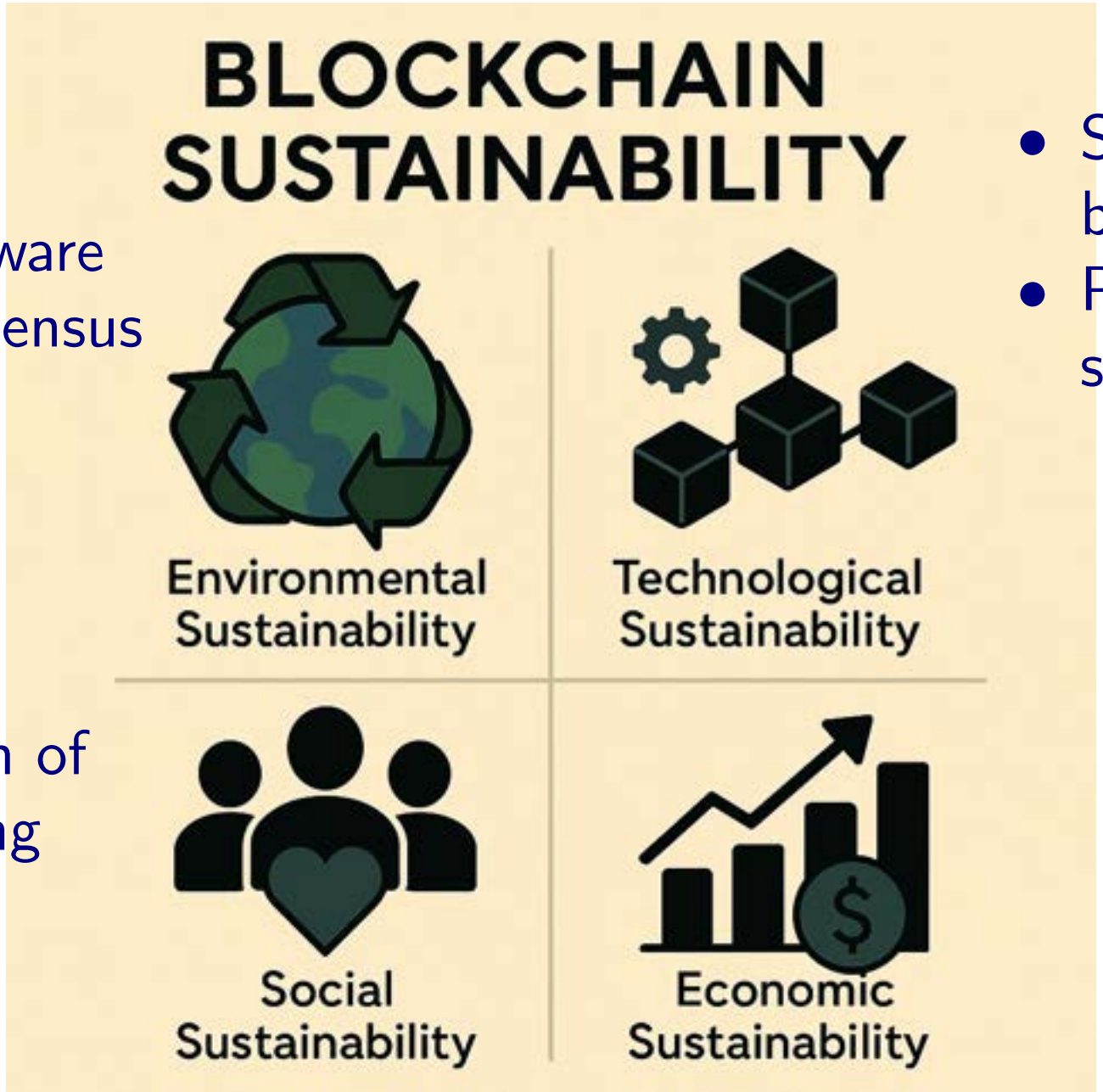
Energy/Hardware waste of consensus



- Scalability bottlenecks
- Postquantum security

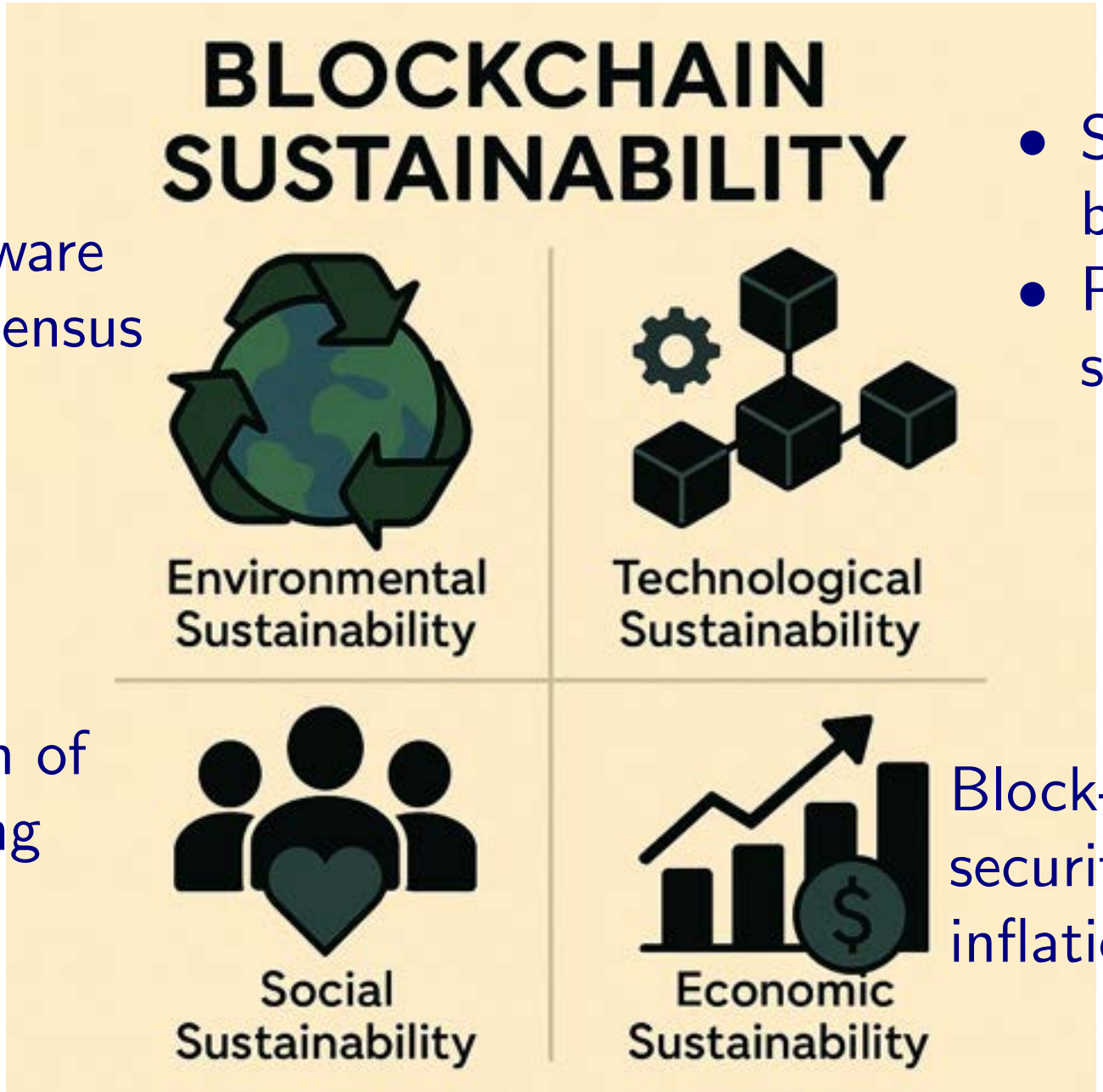
Energy/Hardware waste of consensus

Concentration of mining/staking power



- Scalability bottlenecks
- Postquantum security

Energy/Hardware waste of consensus



- Scalability bottlenecks
- Postquantum security

Concentration of mining/staking power

Block-rewards security vs. inflation

BLOCKCHAIN FOR SUSTAINABILITY

Carbon Credit Trading

Supply Chain Transparency

Renewable Energy Certificates

Verifiable Sustainability Claims

BLOCKCHAIN SUSTAINABILITY

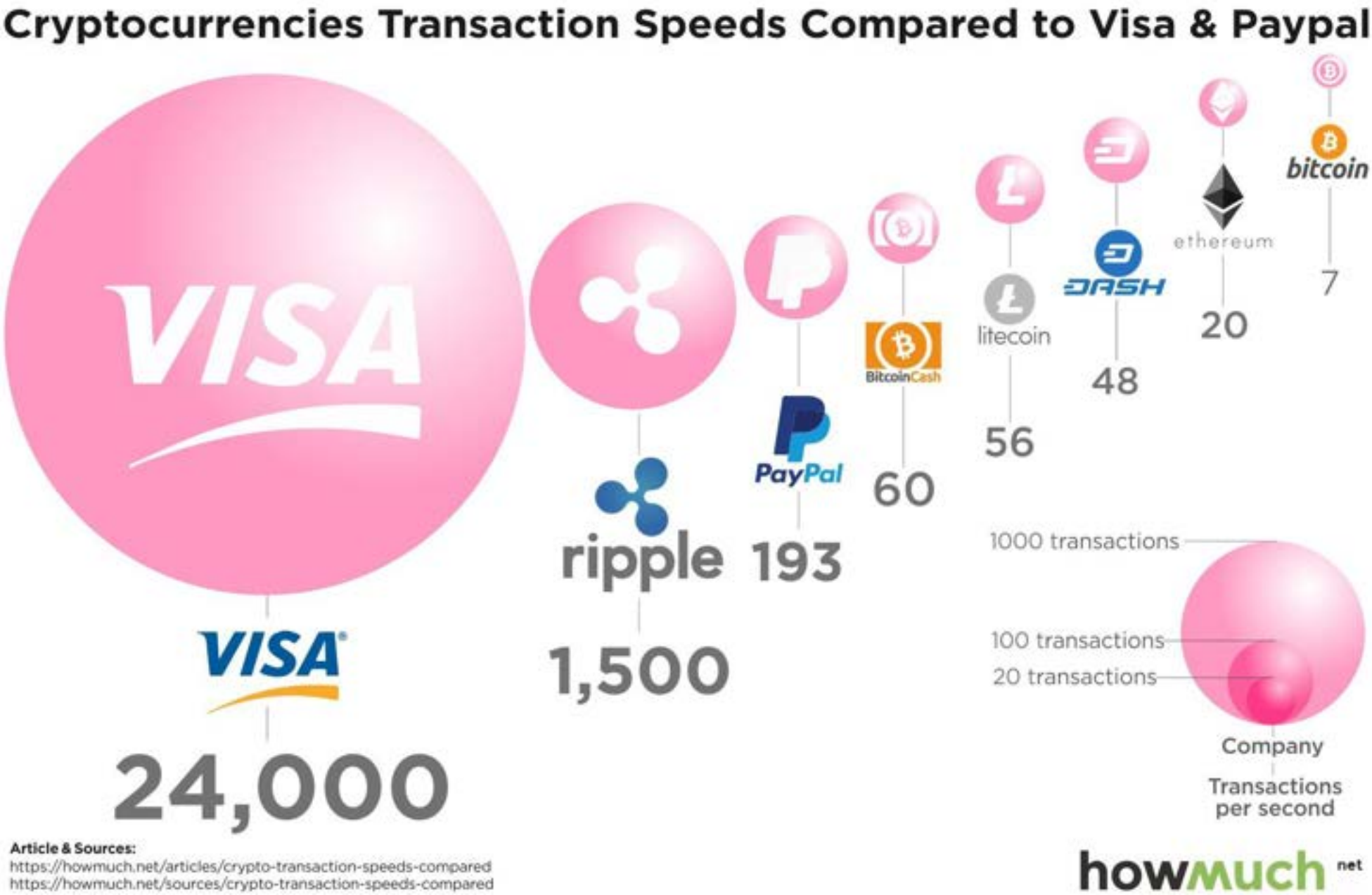
Environmental Sustainability

Technological Sustainability

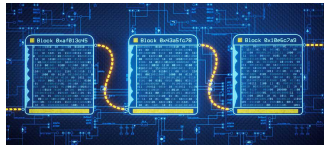
Social Sustainability

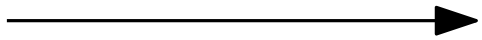
Economic Sustainability

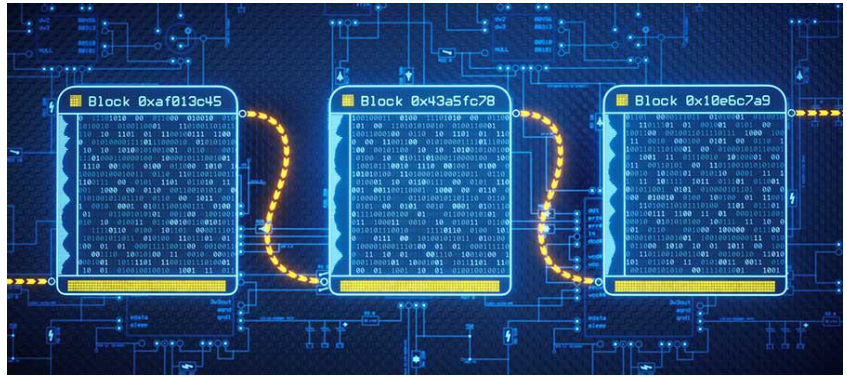
Scalability / Transactions per second



Scaling Blockchains

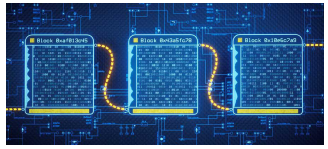




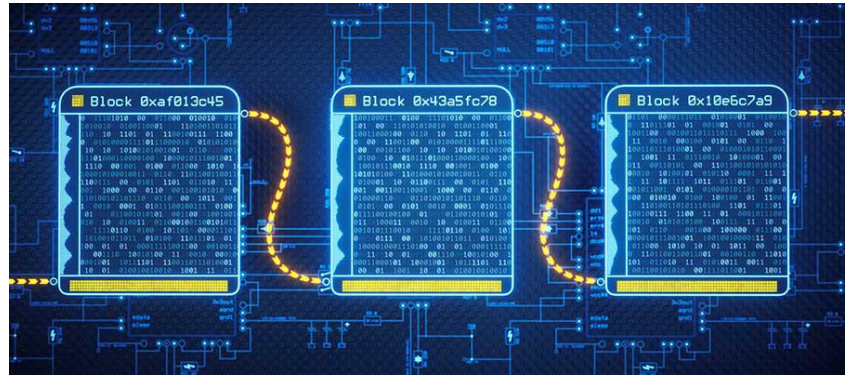


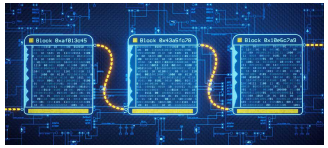
Increase block size and/or rate

Scaling Blockchains

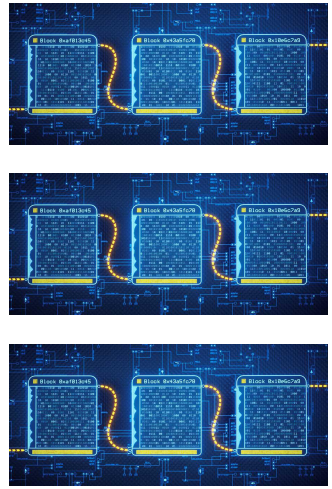


Increase block size and/or rate



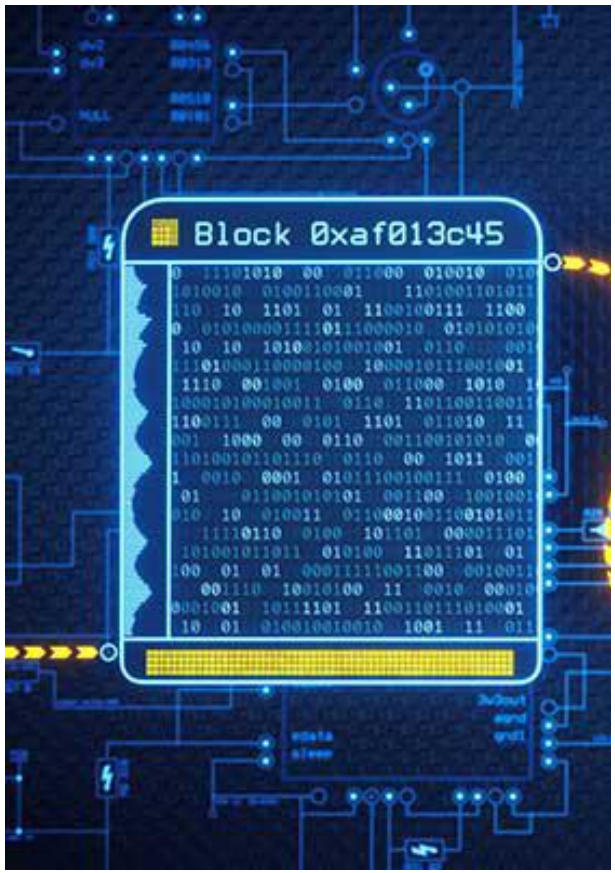


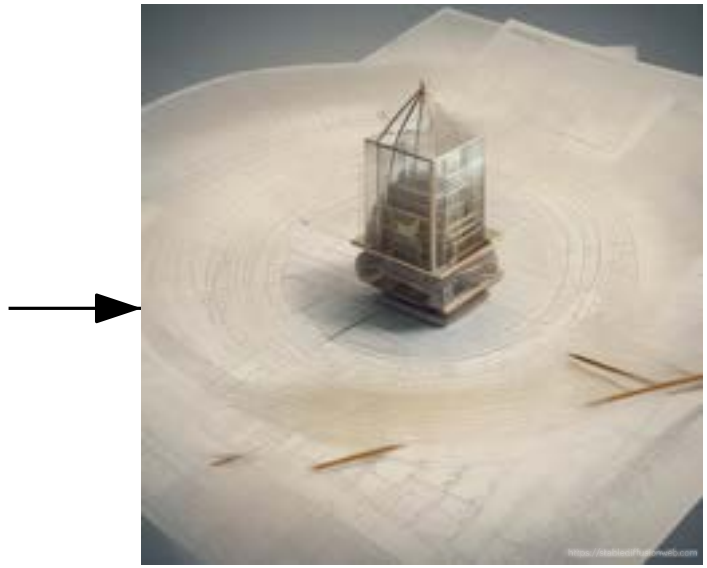
Sharding



Scaling Blockchains

Layer 2 Solution: Rollups





crypto magic
ZK-SNARKs[a]

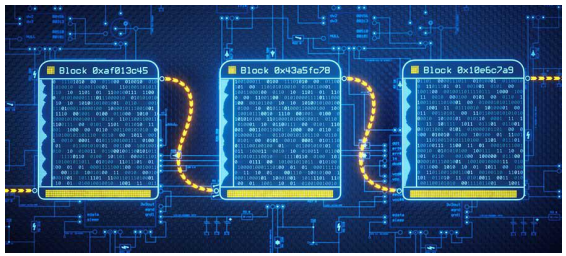
---

[a] Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Scaling Blockchains

Layer 2 solution: Payment Networks

Payment network, e.g. Lightning



Layer 1: Blockchain, e.g. Bitcoin

BLOCKCHAIN SUSTAINABILITY

Environmental Sustainability

Technological Sustainability

Social Sustainability

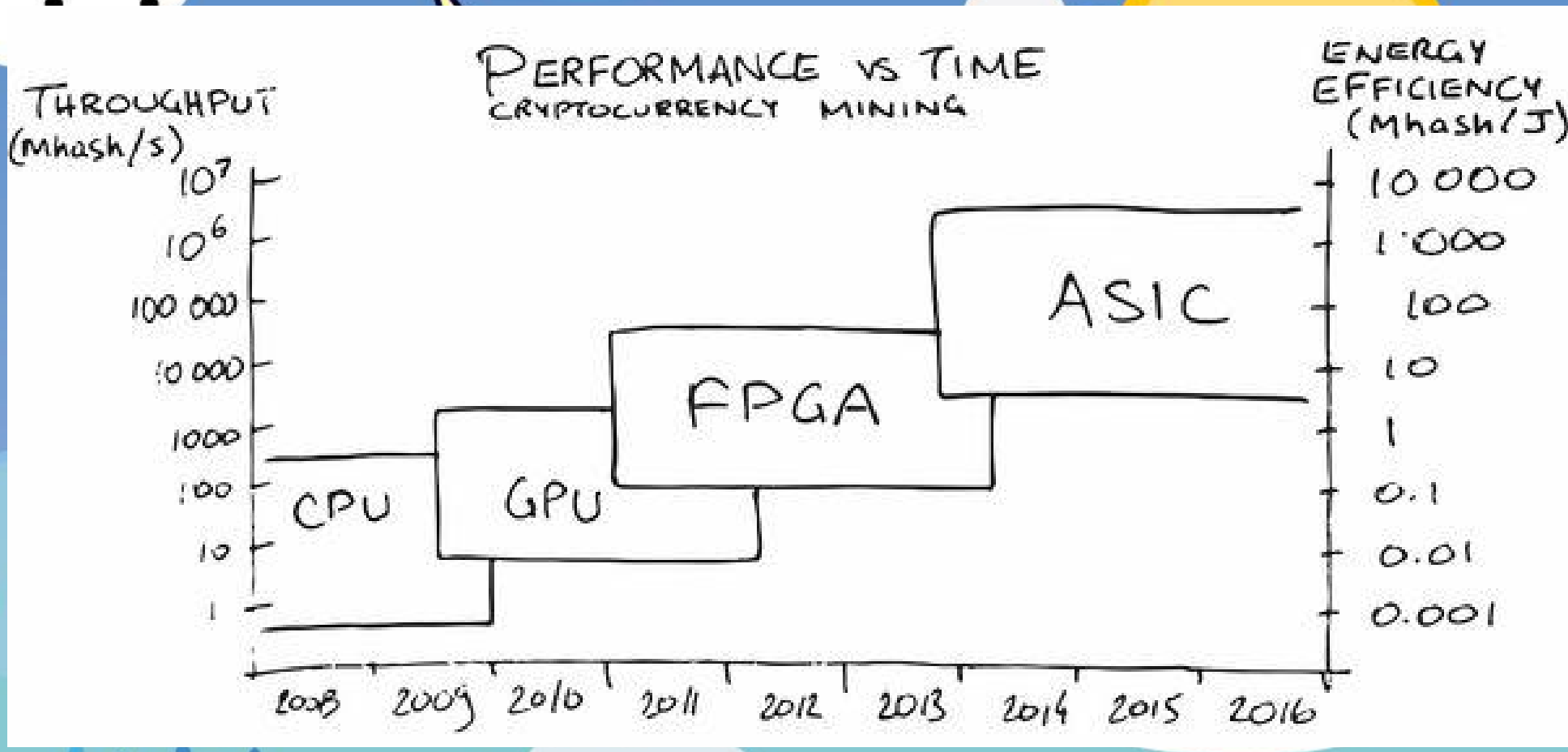
Economic Sustainability

Bitcoin Mining

Nakamoto's vision: spare CPU cycles used for mining

Bitcoin Mining

Nakamoto's vision: spare CPU cycles used for mining



Bitcoin Mining

Bitcoin Sustainability

https://digiconomist.net/bitcoin-energy-consumption

Single Bitcoin Transaction Footprints

Carbon Footprint

462.90 kgCO2

Equivalent to the carbon footprint of 1,025,937 VISA transactions or 77,149 hours of watching Youtube.

Electrical Energy

829.92 kWh

Equivalent to the power consumption of an average U.S. household over 28.45 days.

Electronic Waste

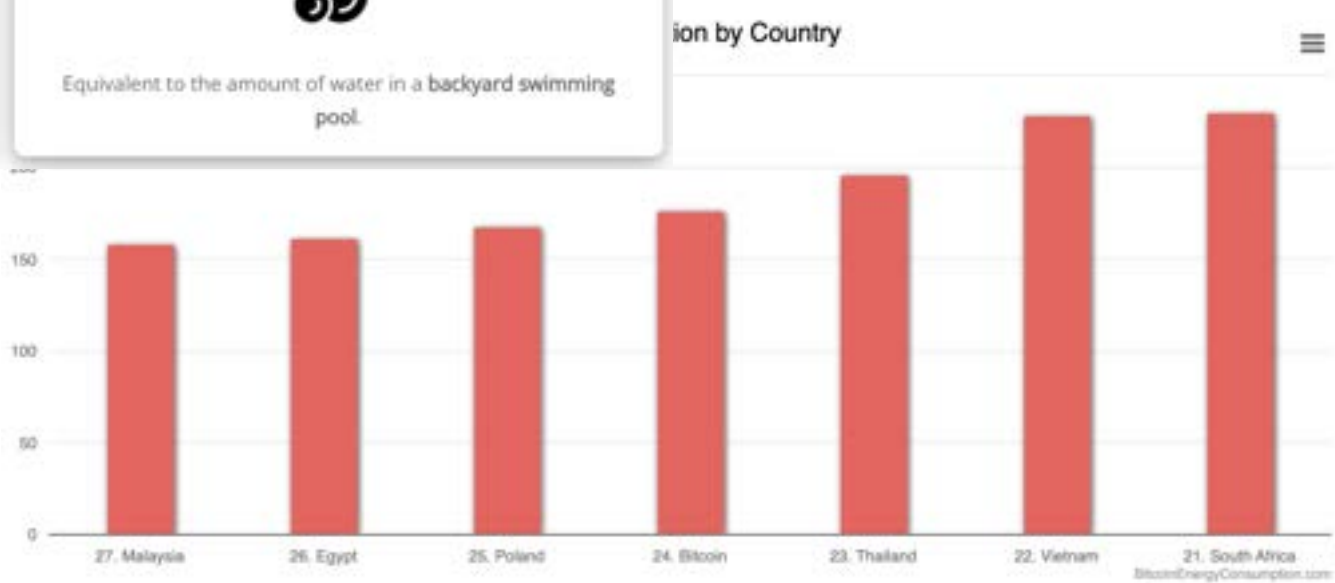
194.10 grams

Equivalent to the weight of 1.18 iPhones 12 or 0.40 iPads. (Find more info on e-waste here.)

Fresh Water Consumption

13,080 liters

Equivalent to the amount of water in a backyard swimming pool.



Can we have a more sustainable Blockchain?

Alternatives to Proof of Work Mining?

Proofs of (Useful) Work

(Bitcoin,old Ethereum, Primecoin. . .)

mining resource: work

Alternatives to Proof of Work Mining?

Proofs of (Useful) Work

(Bitcoin,old Ethereum, Primecoin. . .)

mining resource: work

Proofs of Stake

(Ethereum, Algorand, Ourboros,. . .)

mining resource: (staked) coins

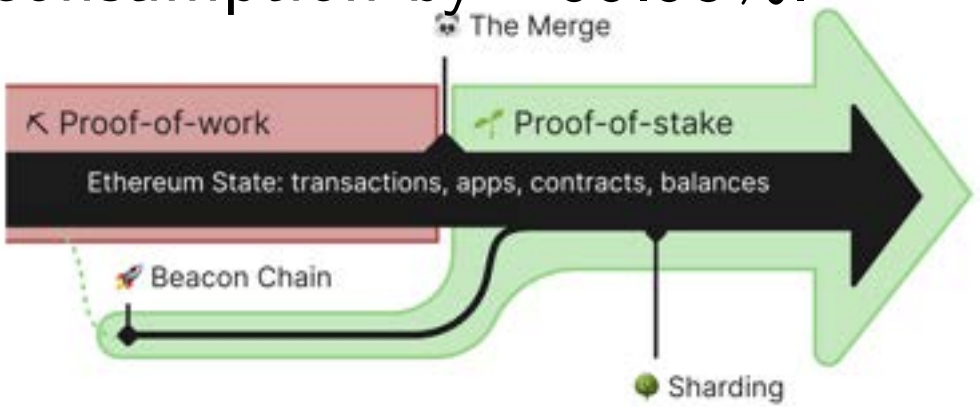
Alternatives to Proof of Work Mining?

Proofs of (Useful) Work

(Bitcoin,old Ethereum, Primecoin. . .)

mining resource: work

September 2022, "the Merge" reduced Ethereum's energy consumption by ≈99.95%.



Proofs of Stake

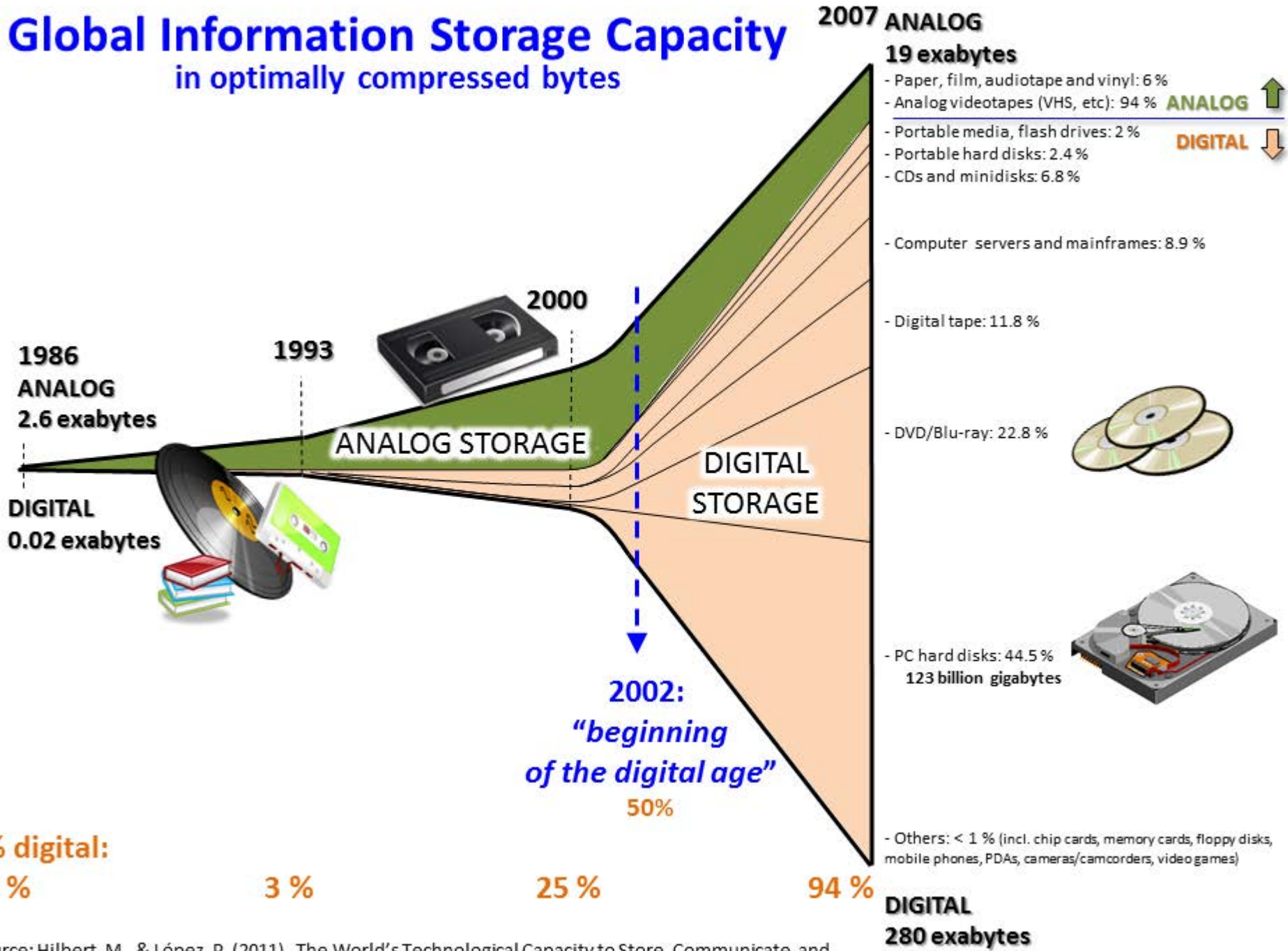
(Ethereum, Algorand, Ourboros,. . .)

mining resource: (staked) coins

Proof of Stake Issues

Global Information Storage Capacity

in optimally compressed bytes



Source: Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332(6025), 60 –65. http://www.martinhilbert.net/WorldInfoCapacity.html

Work vs. Space vs. Stake Mining/Farming

Work vs. Space vs. Stake Mining/Farming

Resource is

External

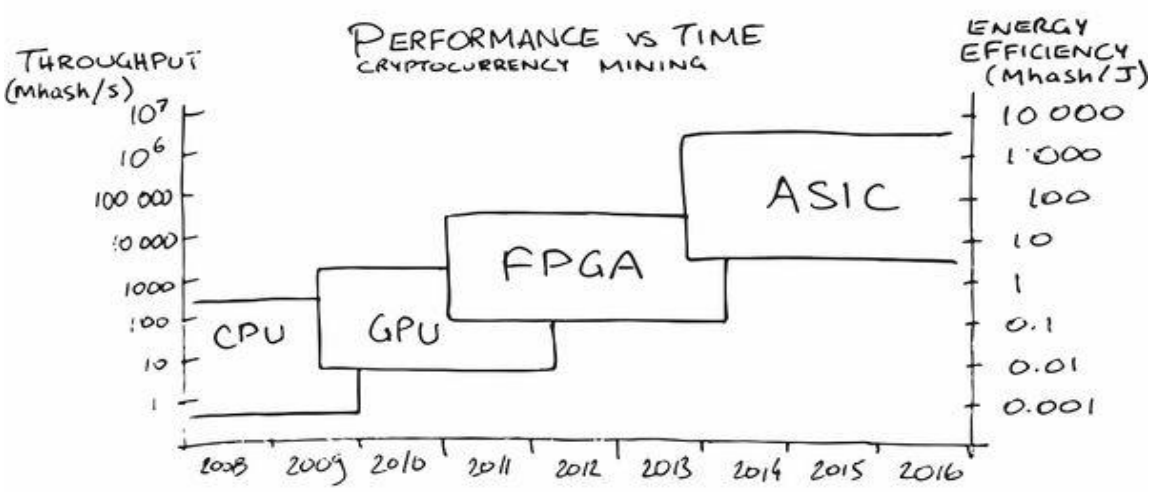
External

Internal

Work vs. Space vs. Stake Mining/Farming

	Resource is	Power consumption
	External	Huge
	External	Tiny
	Internal	Tiny

Work vs. Space vs. Stake Mining/Farming



Resource is	Power consumption	Hardware
work	External	Huge	Application Specific Integrated Circuits (ASIC)
space	External	Tiny	General Purpose Disk Storage
stake	Internal	Tiny	None

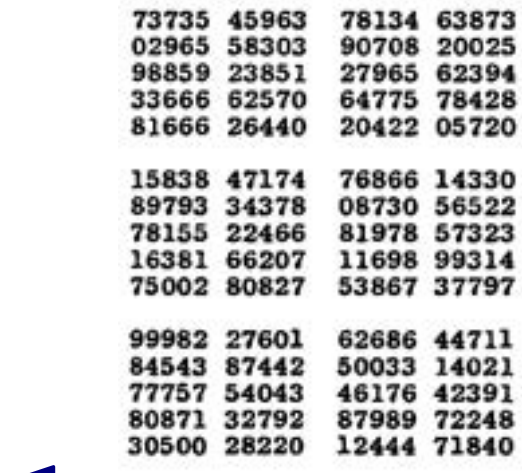
Proofs of Space [DFKP'15]

Proofs of Space [DFKP'15]

73735 45963 78134 63873
02965 58303 90708 20025
98859 23851 27965 62394
33666 62570 64775 78428
81666 26440 20422 05720

15838 47174 76866 14330
89793 34378 08730 56522
78155 22466 81978 57323
16381 66207 11698 99314
75002 80827 53867 37797

99982 27601 62686 44711
84543 87442 50033 14021
77757 54043 46176 42391
80871 32792 87989 72248
30500 28220 12444 71840



73735 45963 78134 63873
02965 58303 90708 20025
98859 23851 27965 62394
33666 62570 64775 78428
81666 26440 20422 05720

15838 47174 76866 14330
89793 34378 08730 56522
78155 22466 81978 57323
16381 66207 11698 99314
75002 80827 53867 37797

99982 27601 62686 44711
84543 87442 50033 14021
77757 54043 46176 42391
80871 32792 87989 72248
30500 28220 12444 71840

Proofs of Space [DFKP'15]

73735 45963 78134 63873
02965 58303 90708 20025
98859 23851 27965 62394
33666 62570 64775 78428
81666 26440 20422 05720

15838 47174 76866 14330
89793 34378 08730 56522
78155 22466 81978 57323
16381 66207 11698 99314
75002 80827 53867 37797

99982 27601 62686 44711
84543 87442 50033 14021
77757 54043 46176 42391
80871 32792 87989 72248
30500 28220 12444 71840

33666 62570 64775 78428
81666 26440 20422 05720

15838 47174 76866 14330
89793 34378 08730 56522
78155 22466 81978 57323
16381 66207 11698 99314
75002 80827 53867 37797

99982 27601 62686 44711
84543 87442 50033 14021
77757 54043 46176 42391
80871 32792 87989 72248
30500 28220 12444 71840

Proofs of Space [DFKP'15]

random index

37797

73735	45963	78134	63873
02965	58303	90708	20025
98859	23851	27965	62394
33666	62570	64775	78428
81666	26440	20422	05720
15838	47174	76866	14330
89793	34378	08730	56522
78155	22466	81978	57323
16381	66207	11698	99314
75002	80827	53867	37797
99982	27601	62686	44711
84543	87442	50033	14021
77757	54043	46176	42391
80871	32792	87989	72248
30500	28220	12444	71840

33666	62570	64775	78428
81666	26440	20422	05720
15838	47174	76866	14330
89793	34378	08730	56522
78155	22466	81978	57323
16381	66207	11698	99314
75002	80827	53867	37797
99982	27601	62686	44711
84543	87442	50033	14021
77757	54043	46176	42391
80871	32792	87989	72248
30500	28220	12444	71840

Proofs of Space [DFKP'15]

73735 45963 78134 63873
02965 58303 90708 20025
98859 23851 27965 62394
33666 62570 64775 78428
81666 26440 20422 05720

TOO MUCH COMMUNICATION

99982 27601 62686 44711
84543 87442 50033 14021
77757 54043 46176 42391
80871 32792 87989 72248
30500 28220 12444 71840

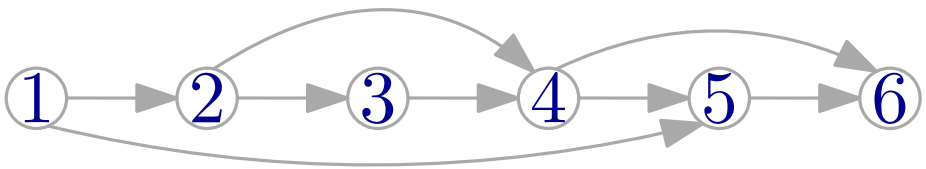
Proofs of Space [DFKP'15]




Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak: Proofs of Space. CRYPTO 2015

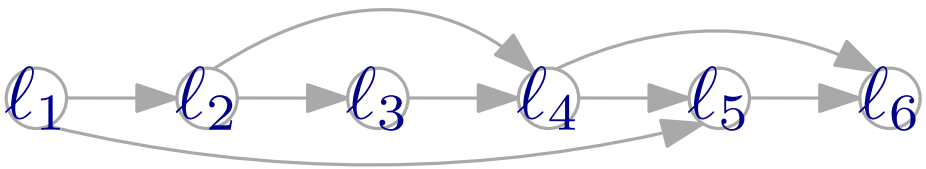
Proofs of Space [DFKP'15]

https://www.pebbling-game.at/



Proofs of Space [DFKP'15]

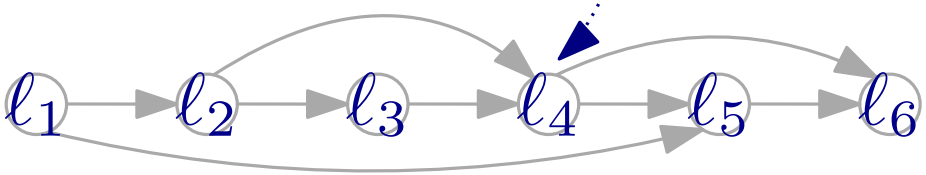
$$\ell_4 := hash(\ell_2, \ell_3)$$



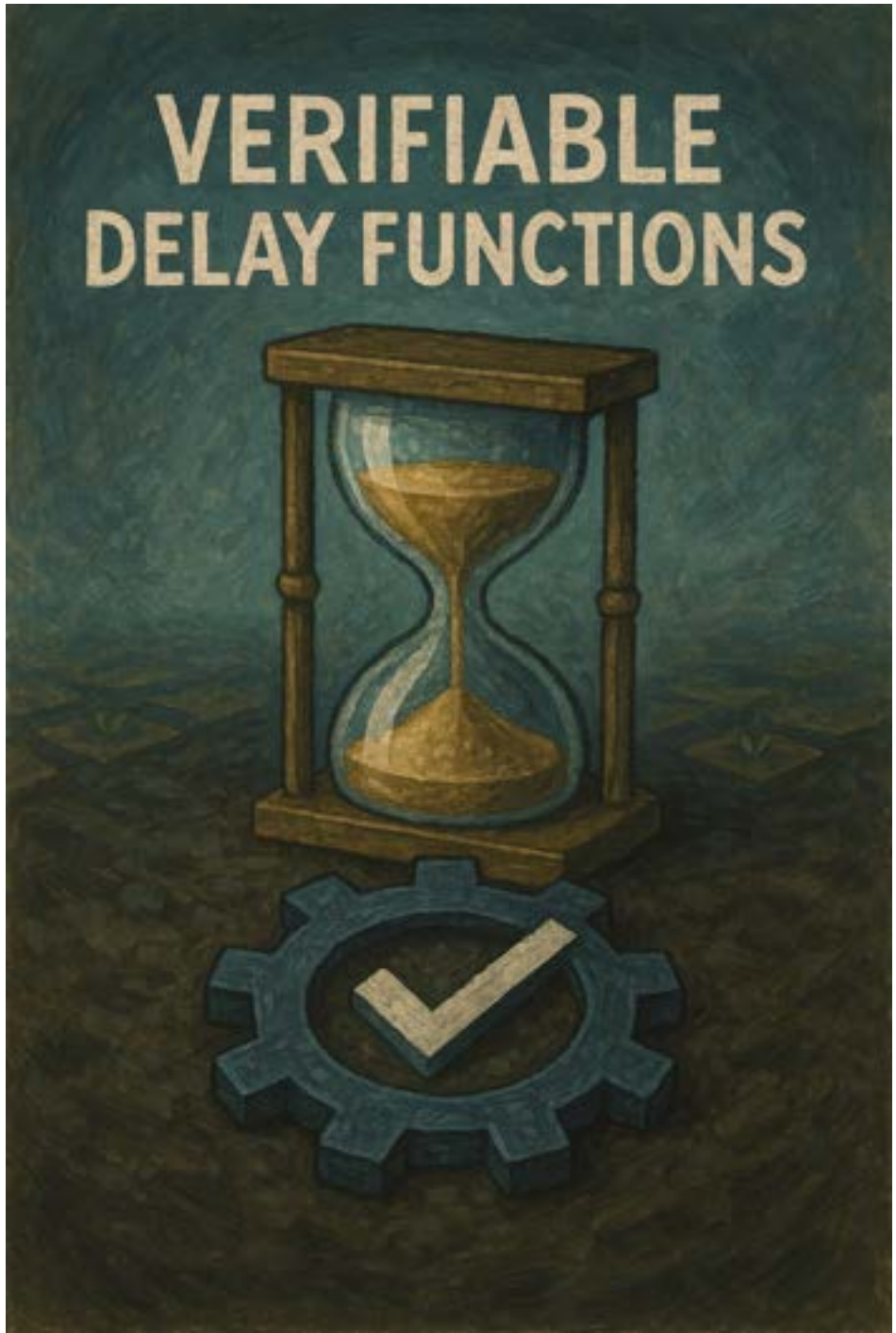
Proofs of Space [DFKP'15]

4

ℓ_4



Sustainable Blockchains at ISTA



Sustainable Blockchains at ISTA

The Guardian, May 26, 2021

New cryptocurrency Chia blamed for hard drive shortages

Speculators buy up vital components as demand surges for rival to bitcoin that requires huge storage space

Circular Drive Initiative

Driving the circular economy for storage

The Circular Drive Initiative (CDI) is a partnership of global leaders in digital storage, data centers, sustainability, and blockchain collaborating to reduce e-waste by enabling, driving, and promoting the secure reuse of storage hardware.

BLOCKCHAIN SUSTAINABILITY

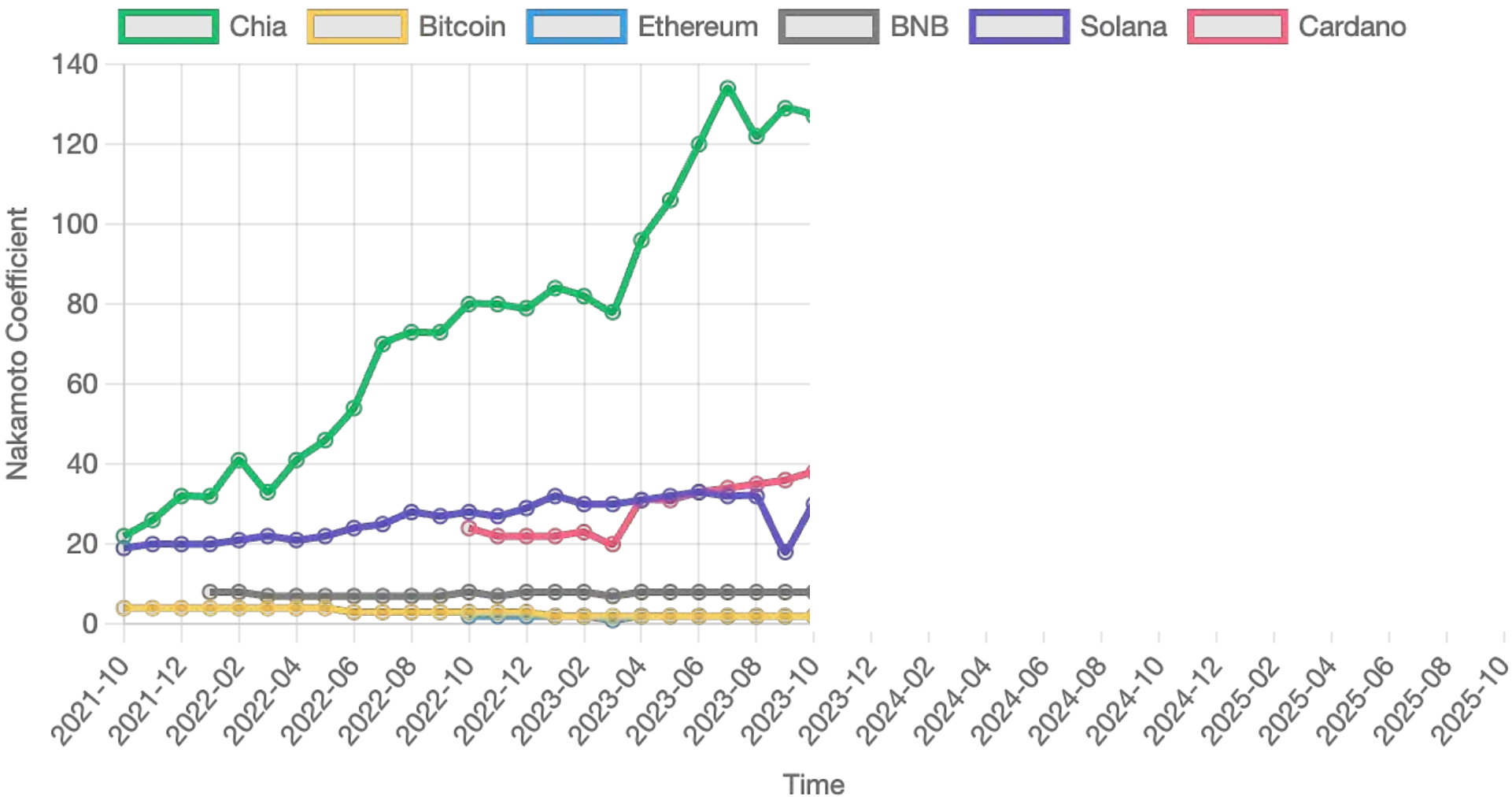
Environmental Sustainability

Technological Sustainability

Social Sustainability

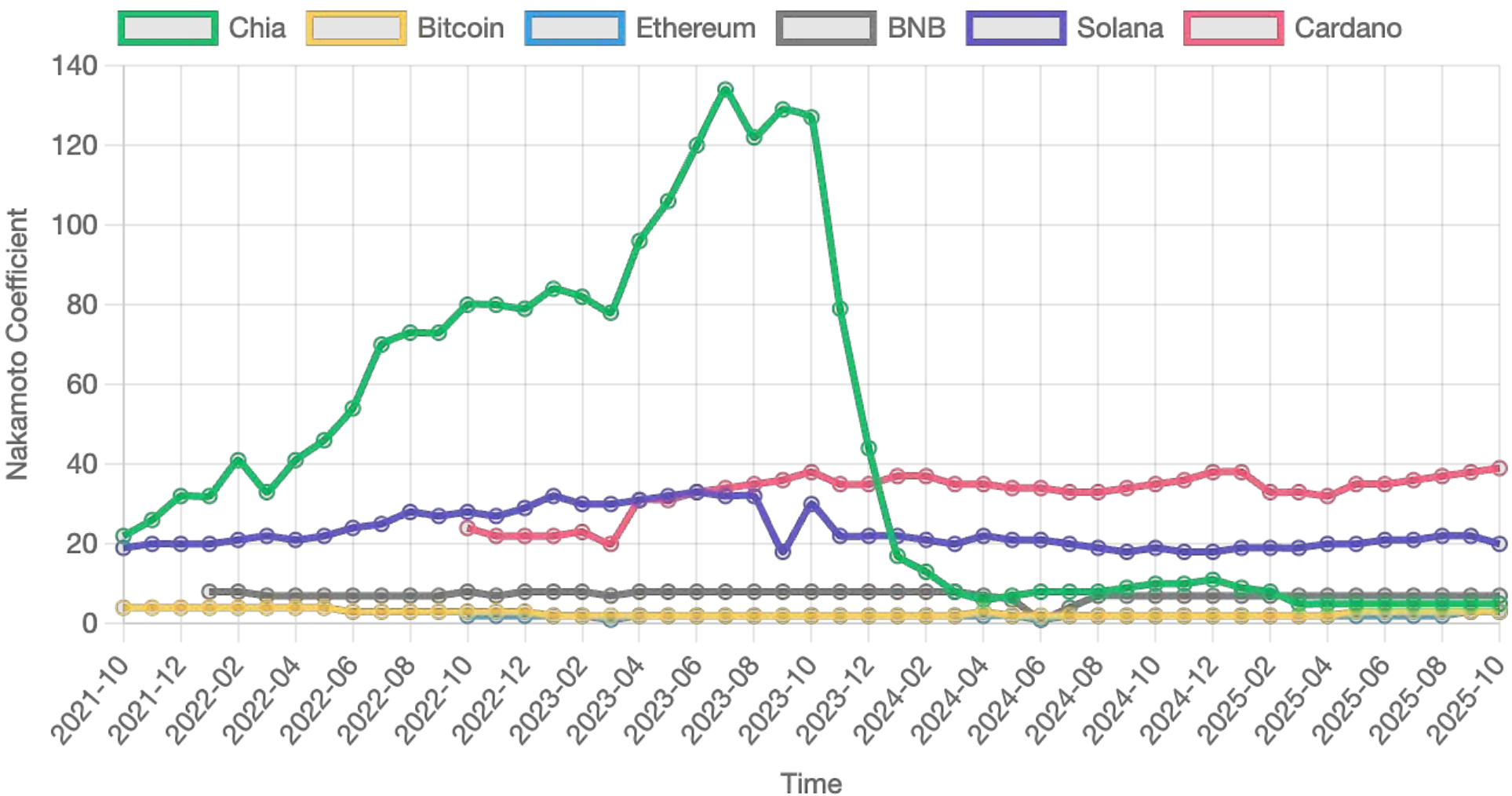
Economic Sustainability

The **Nakamoto coefficient** is the minimum number of entities (e.g., miners, validators, or nodes) that together control enough of the system to disrupt consensus or compromise its integrity.



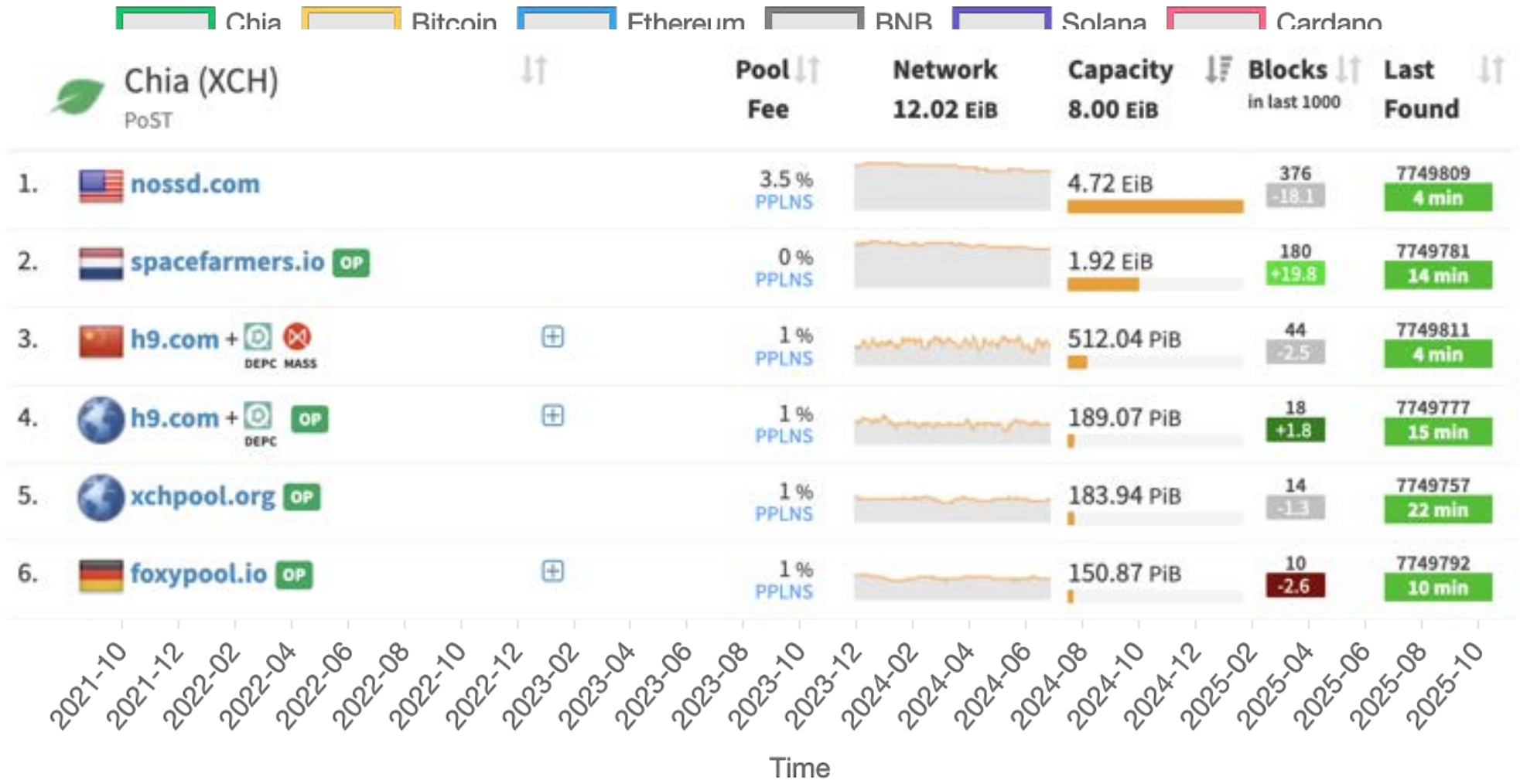
https://xch.farm/decentralization/

The **Nakamoto coefficient** is the minimum number of entities (e.g., miners, validators, or nodes) that together control enough of the system to disrupt consensus or compromise its integrity.



https://xch.farm/decentralization/

The **Nakamoto coefficient** is the minimum number of entities (e.g., miners, validators, or nodes) that together control enough of the system to disrupt consensus or compromise its integrity.



https://xch.farm/decentralization/

BLOCKCHAIN FOR SUSTAINABILITY

Carbon Credit Trading

Supply Chain Transparency

Renewable Energy Certificates

Verifiable Sustainability Claims

https://www.youtube.com/watch?v=cXwTV2bAnvI

BLOCKCHAIN FOR SUSTAINABILITY

Carbon Credit Trading

Supply Chain Transparency

DePIN

Renewable Energy Certificates

Verifiable Sustainability Claims