Sustainable Blockchains

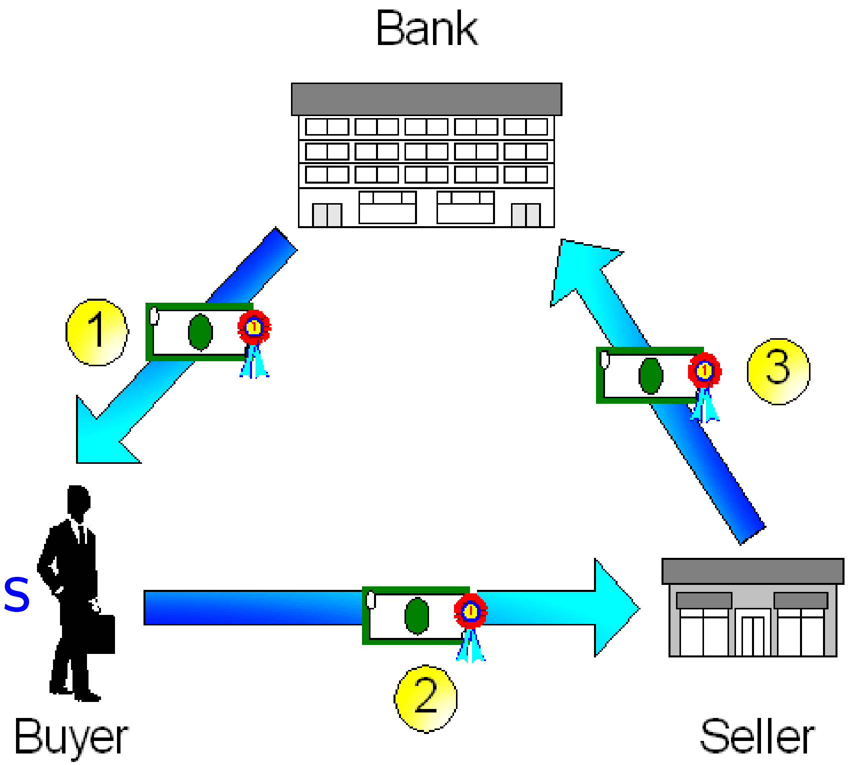
Krzysztof Pietrzak

ISTA Institute of Science and Technology Austria

Public Lecture Series “Sustainability in Computer Science”

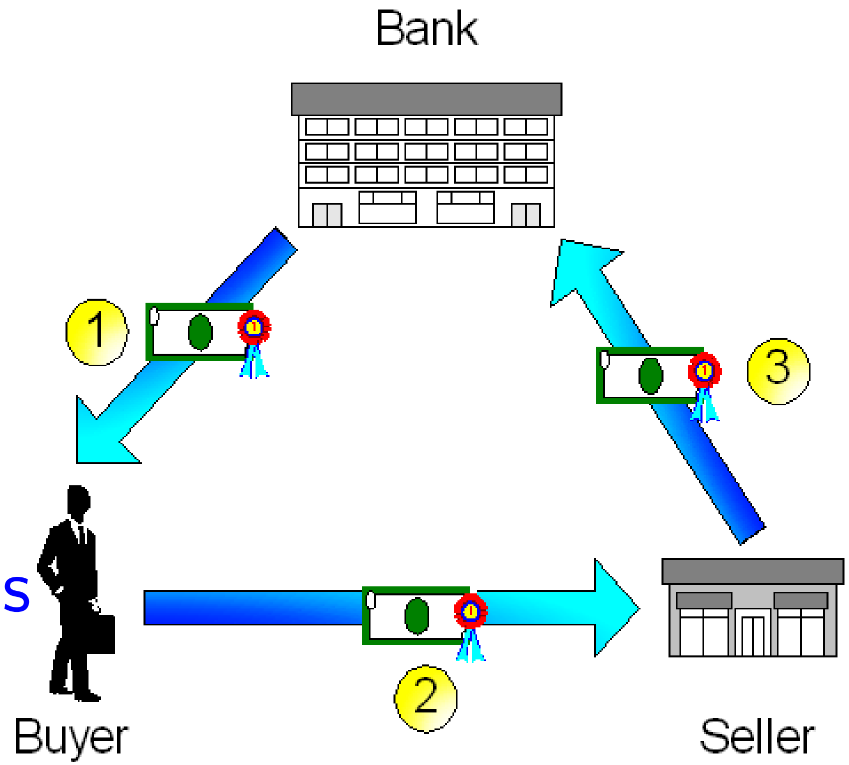
Nov. 13 2023

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



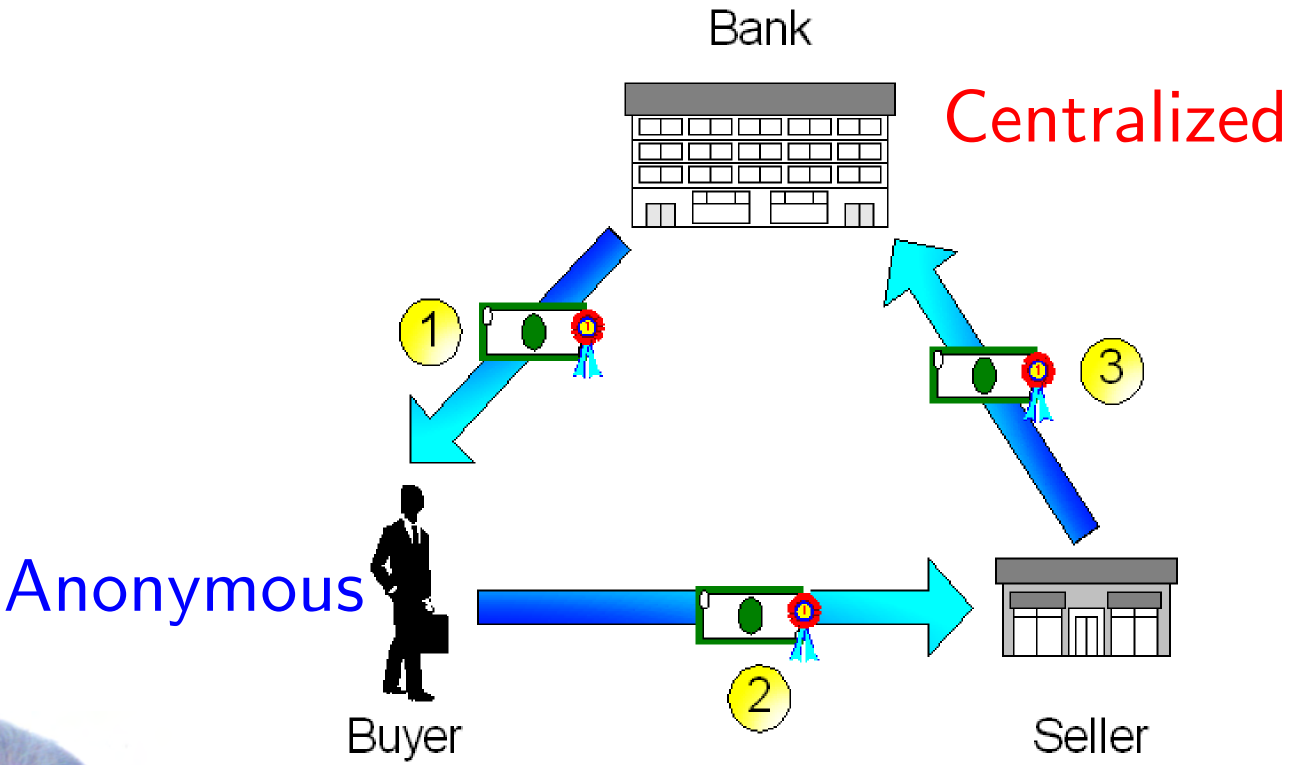
Anonymous

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



Anonymous

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

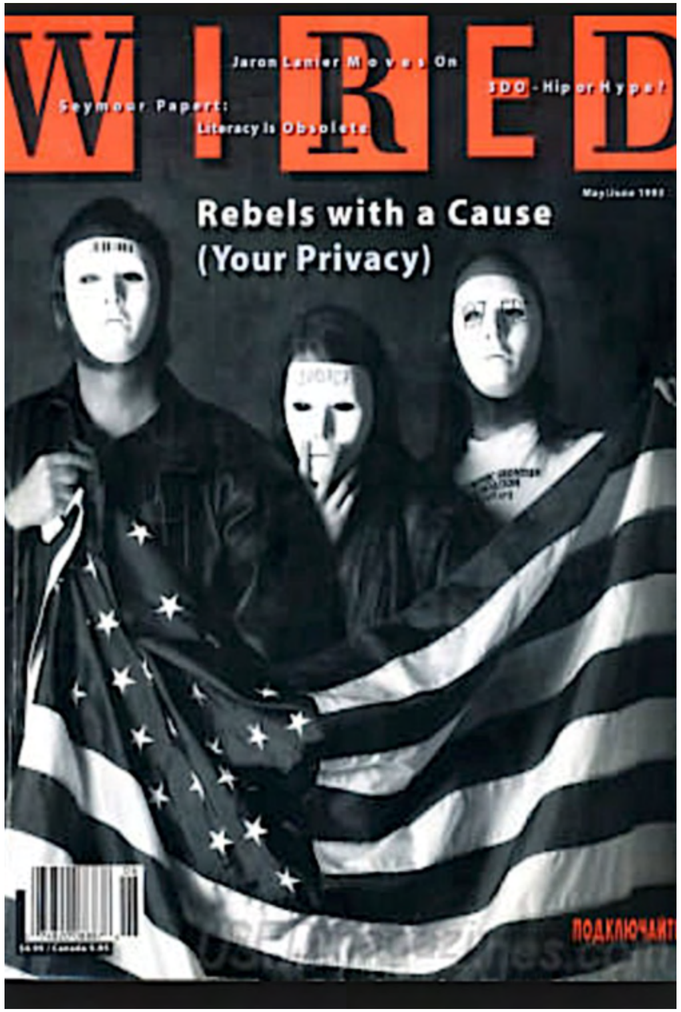


Centralized

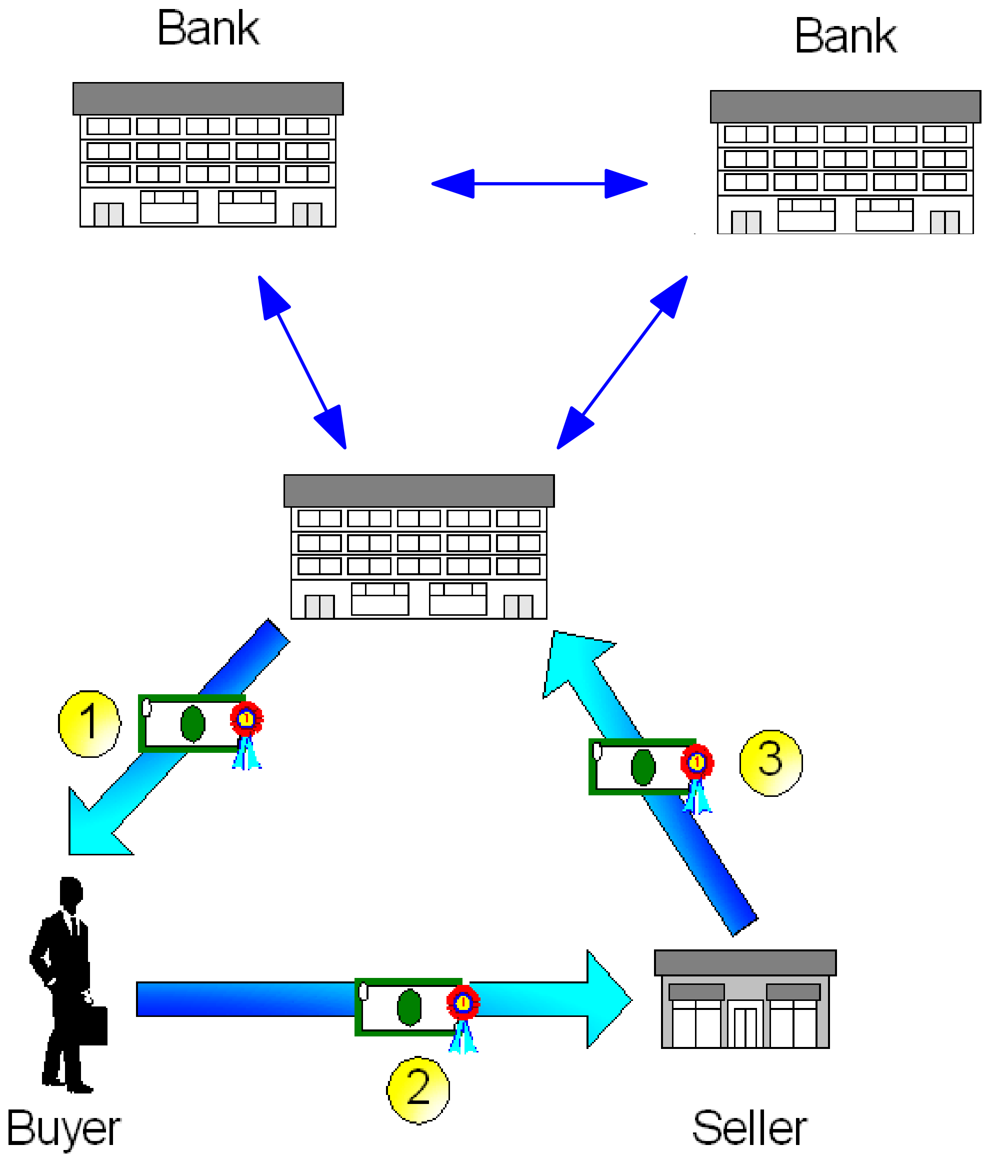
Anonymous

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

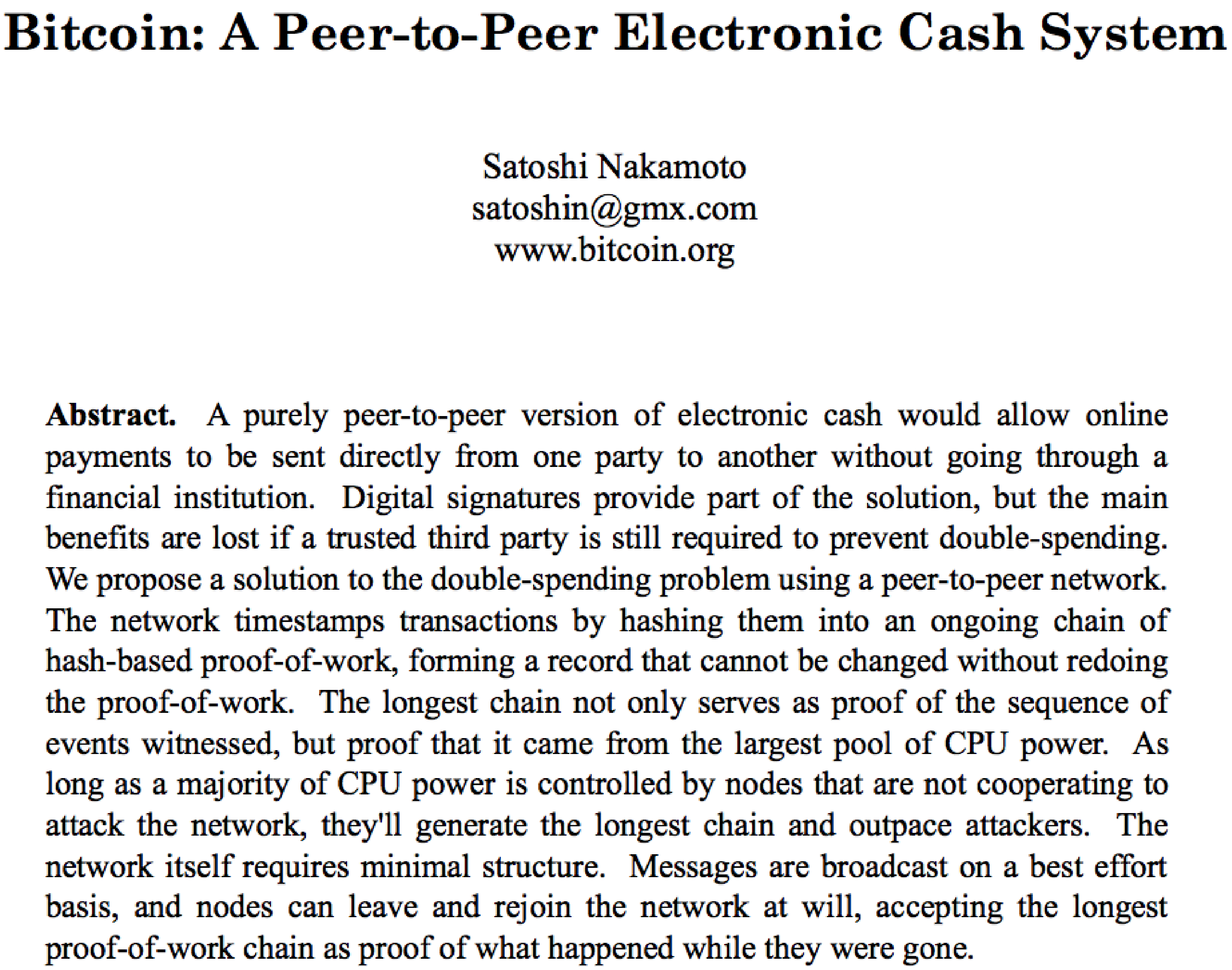
A **cypherpunk** is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.



Decentralization using 80s Crypto



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

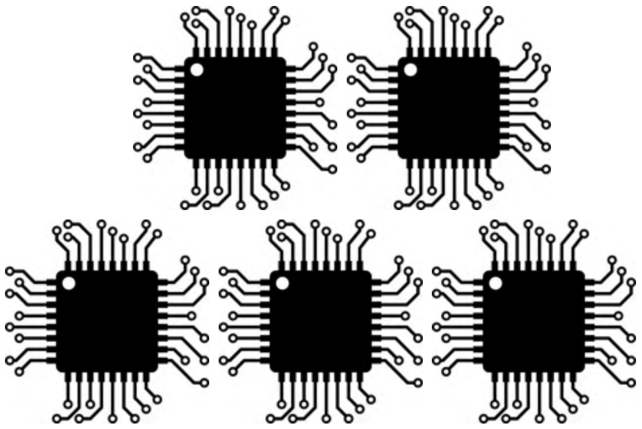
Bitcoin Consensus

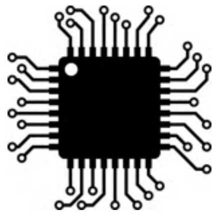
Consensus in a permissionless setting is impossible

Bitcoin Consensus

Nakamoto Consensus

Assumption: Majority of computing power controlled by honest parties

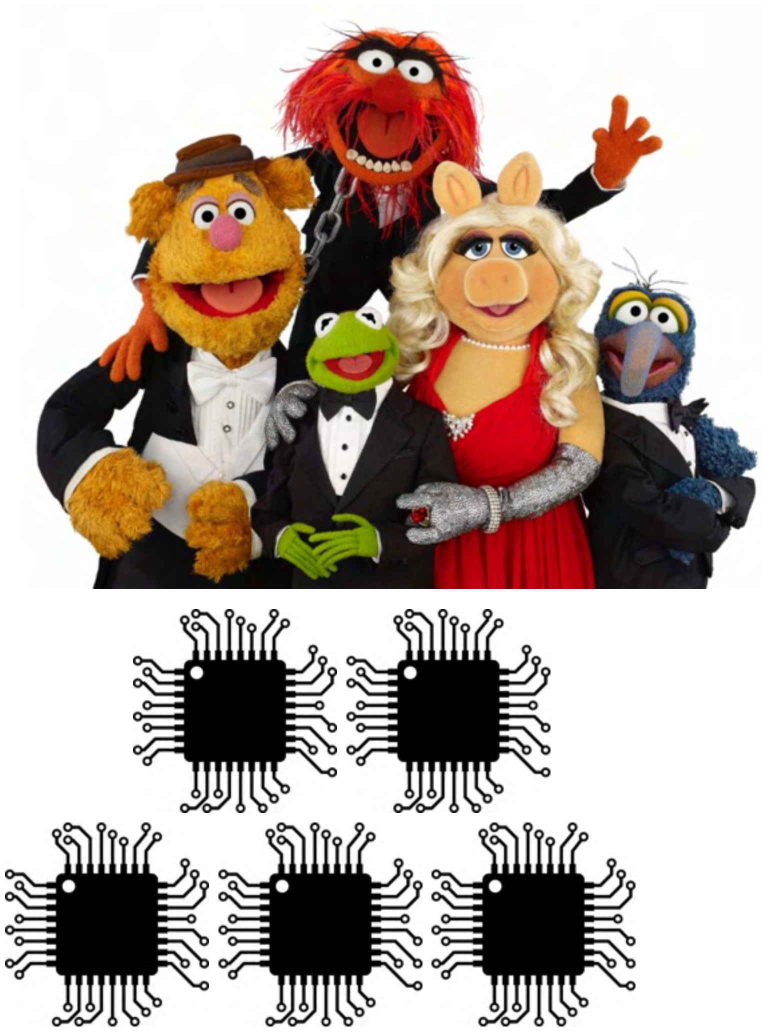


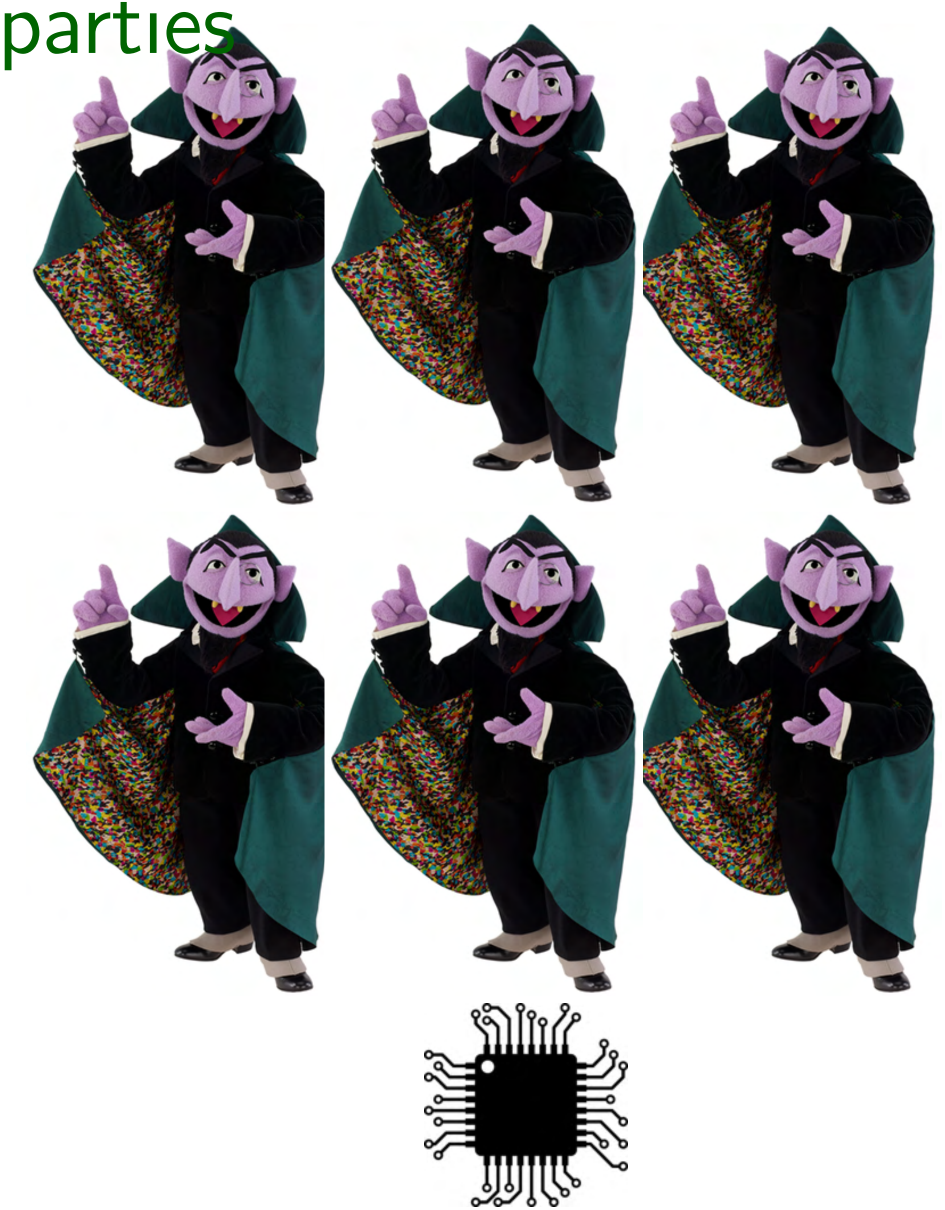


Bitcoin Consensus

Nakamoto Consensus

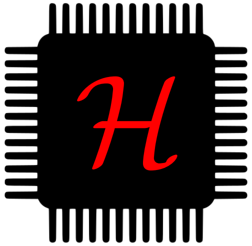
Assumption: Majority of computing power controlled by honest parties





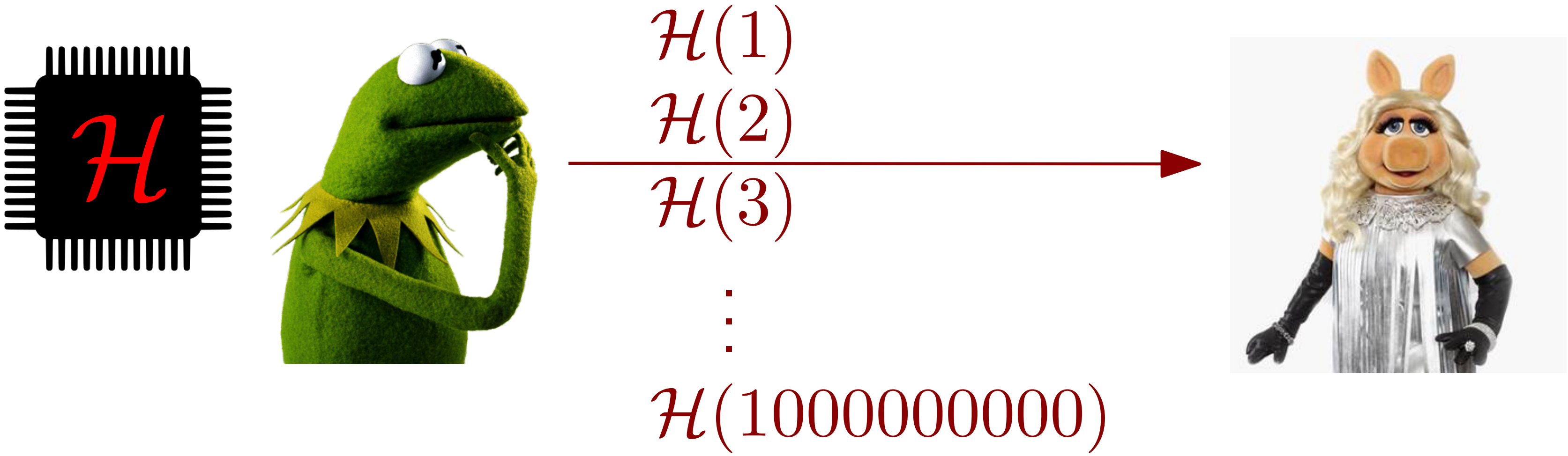
Proofs of Work [DworkNaor92]

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?



$\mathcal{H}(1)$

$\mathcal{H}(2)$

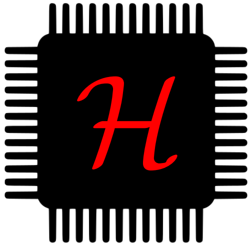
$\mathcal{H}(3)$

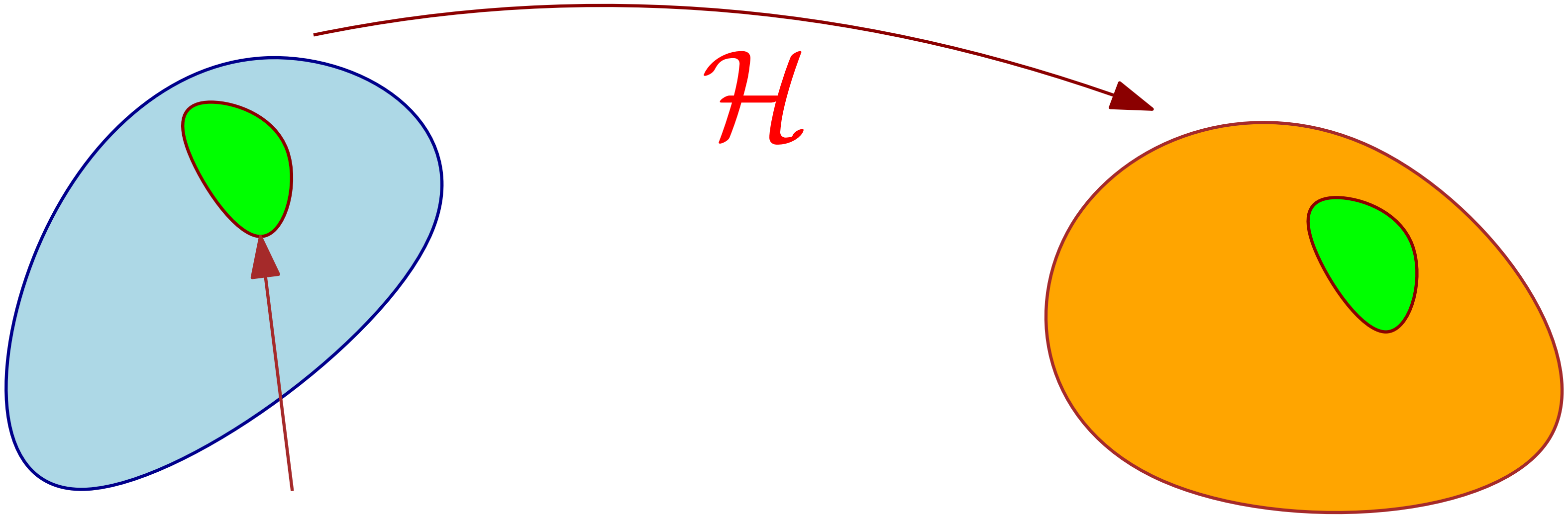
$\vdots$

$\mathcal{H}(1000000000)$

Proofs of Work [DworkNaor92]

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

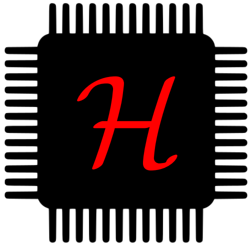


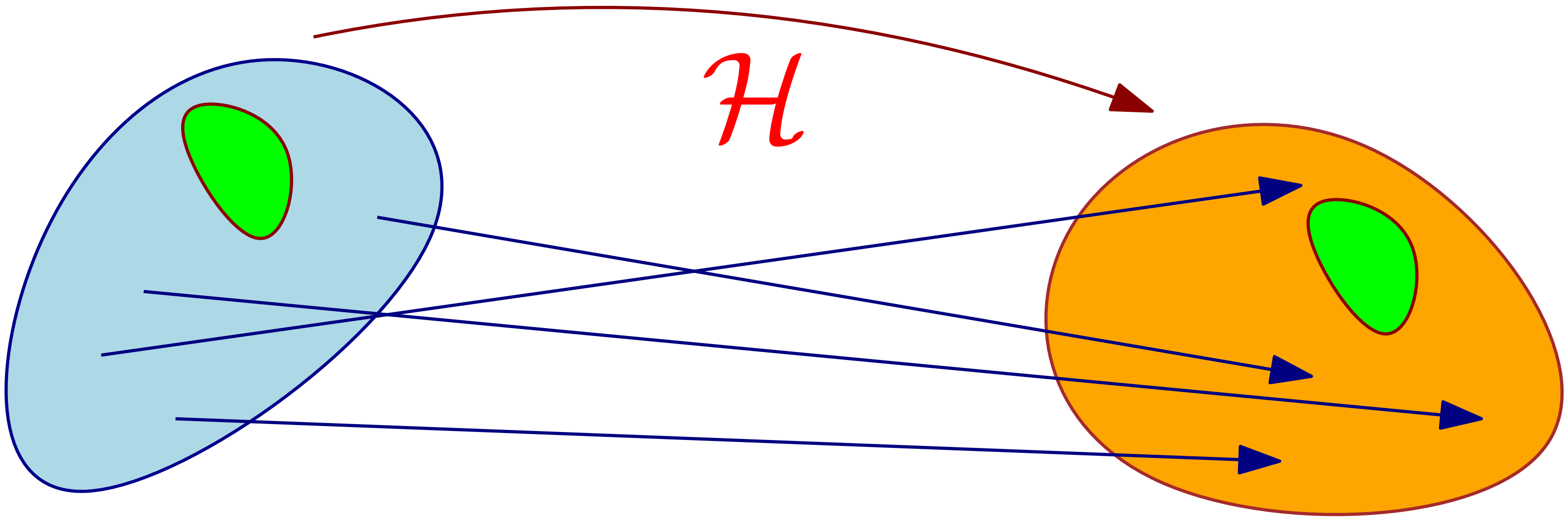


$$\{X \;:\; \mathcal{H}(X) = 000000000\ldots\}$$

Proofs of Work [DworkNaor92]

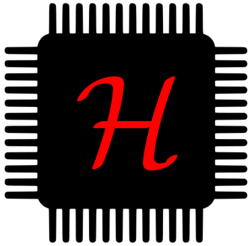
How can prove that it evaluated $\mathcal{H}$ 10^9 times?

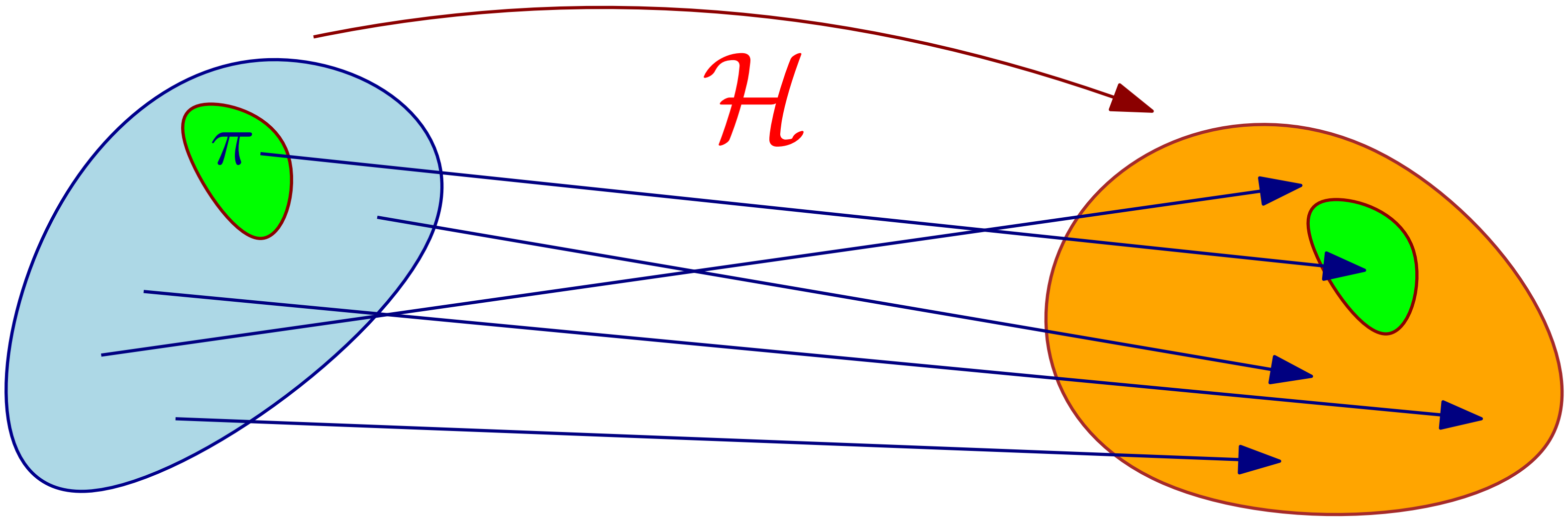




Proofs of Work [DworkNaor92]

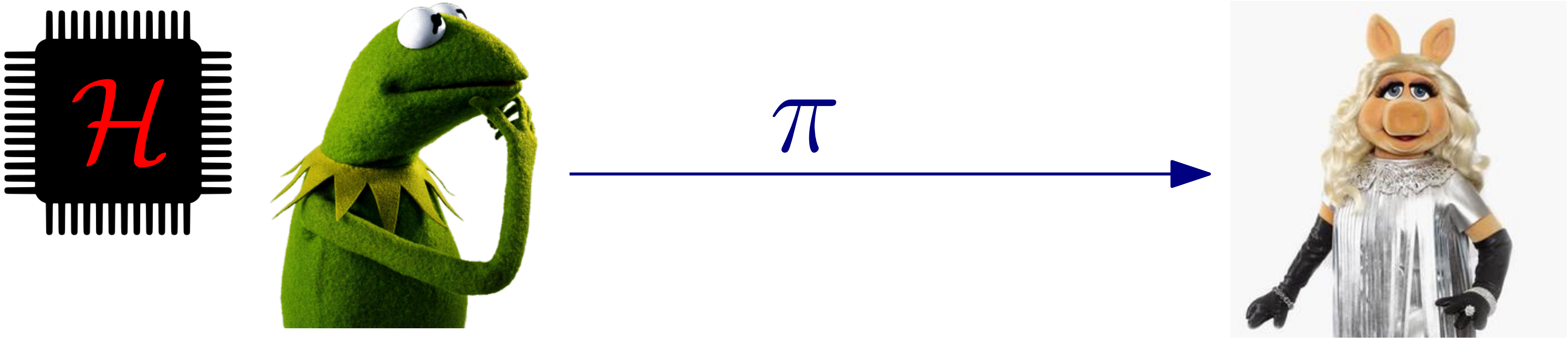
How can prove that it evaluated $\mathcal{H}$ 10^9 times?



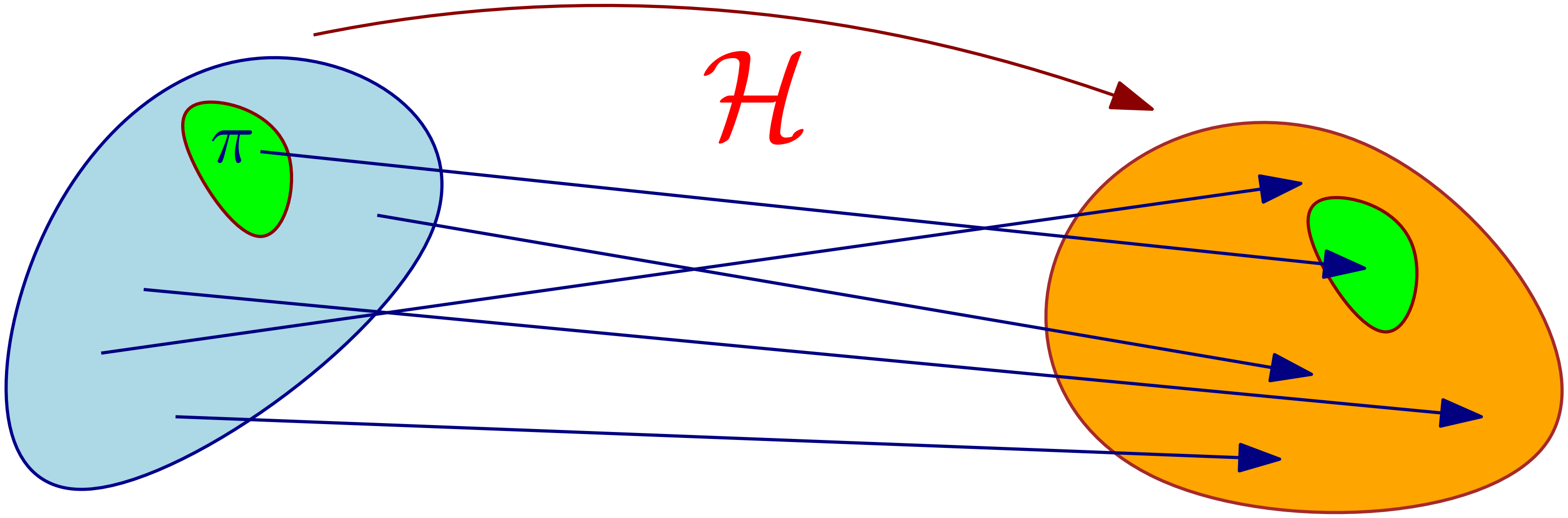


Proofs of Work [DworkNaor92]

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

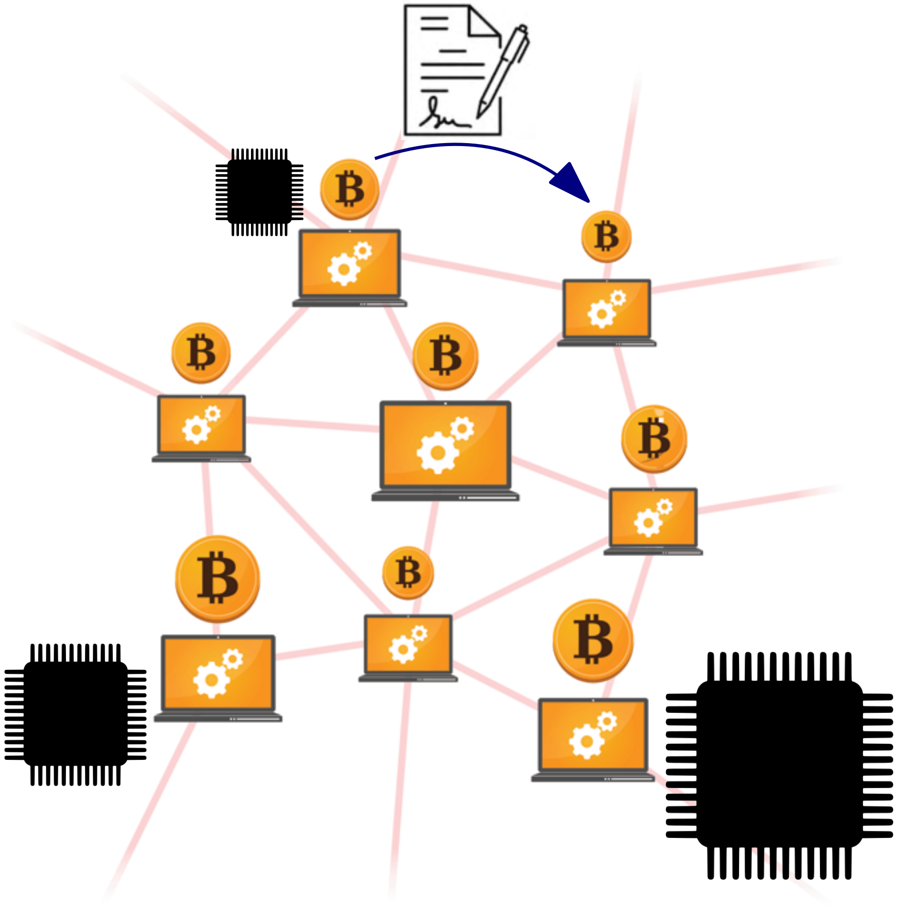


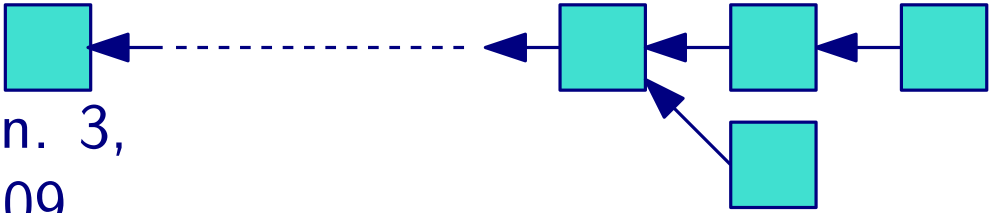
$$\mathcal{H}(\pi) \overset{?}{=} 000000000???????????$$



10^9 required in expectation to find a proof π

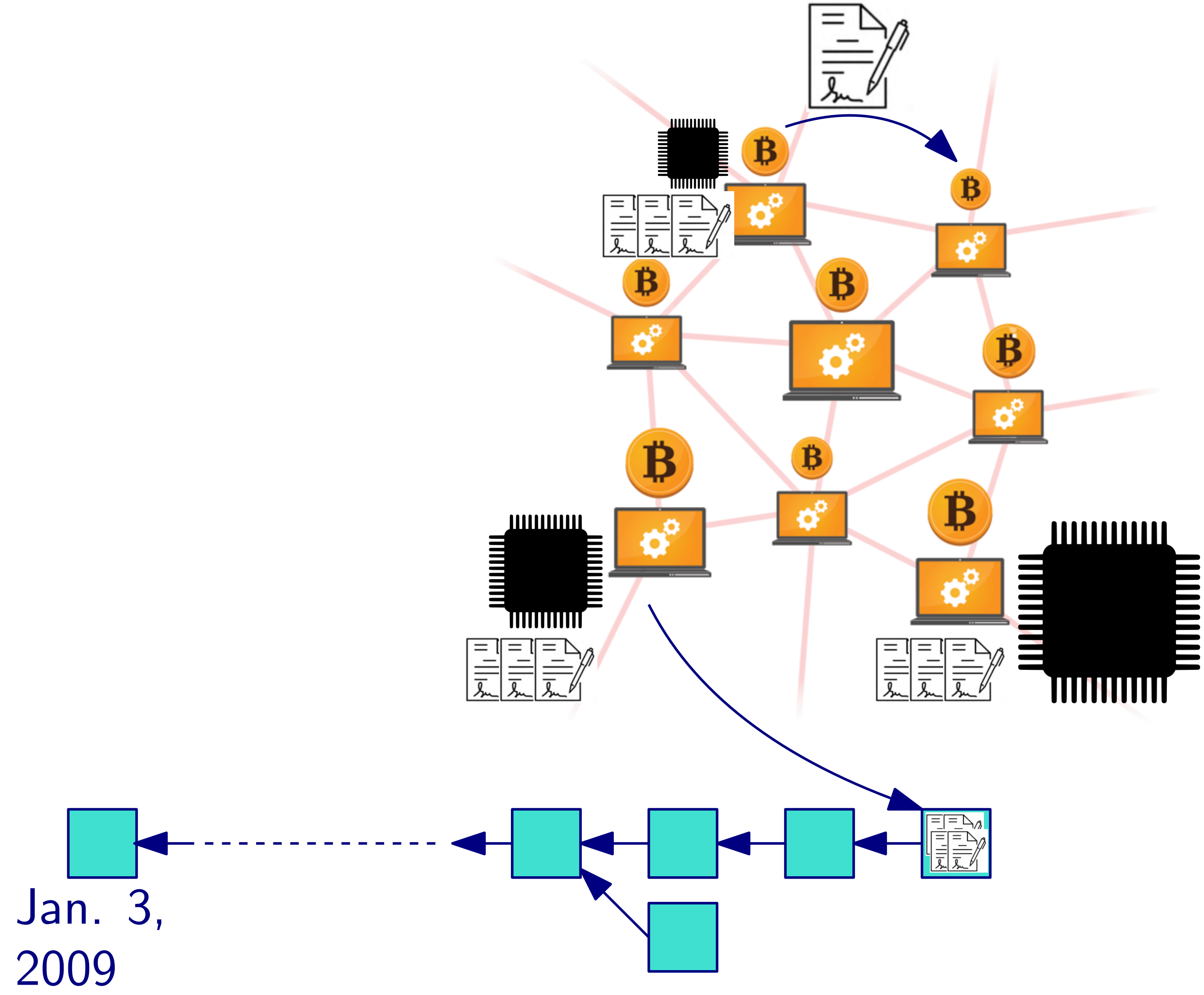
Proofs of Work in Bitcoin



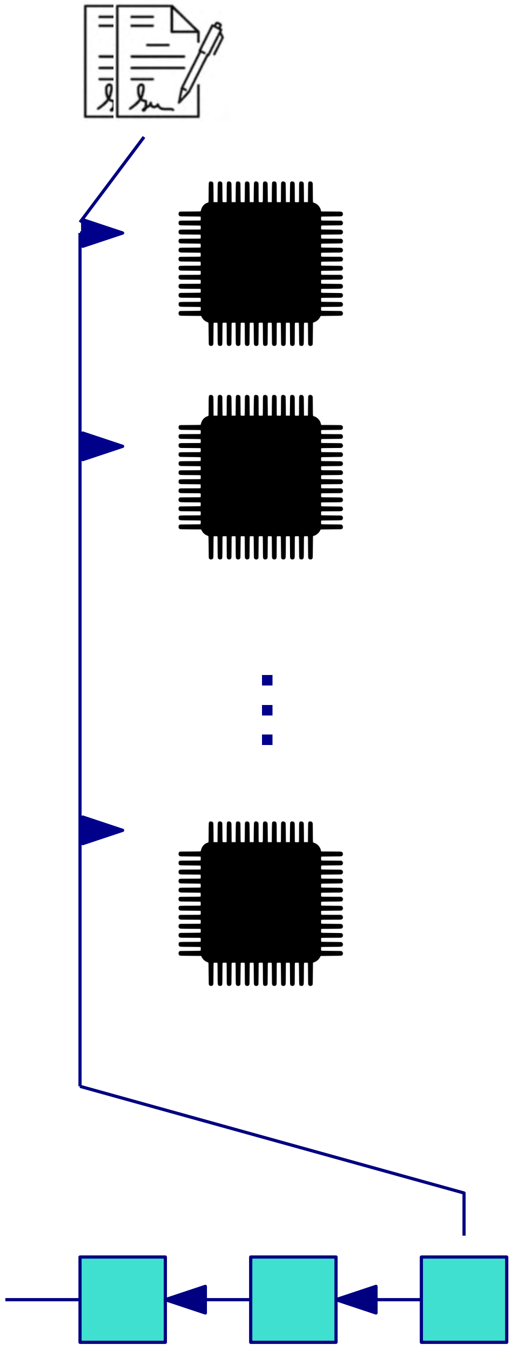


Jan. 3,
2009

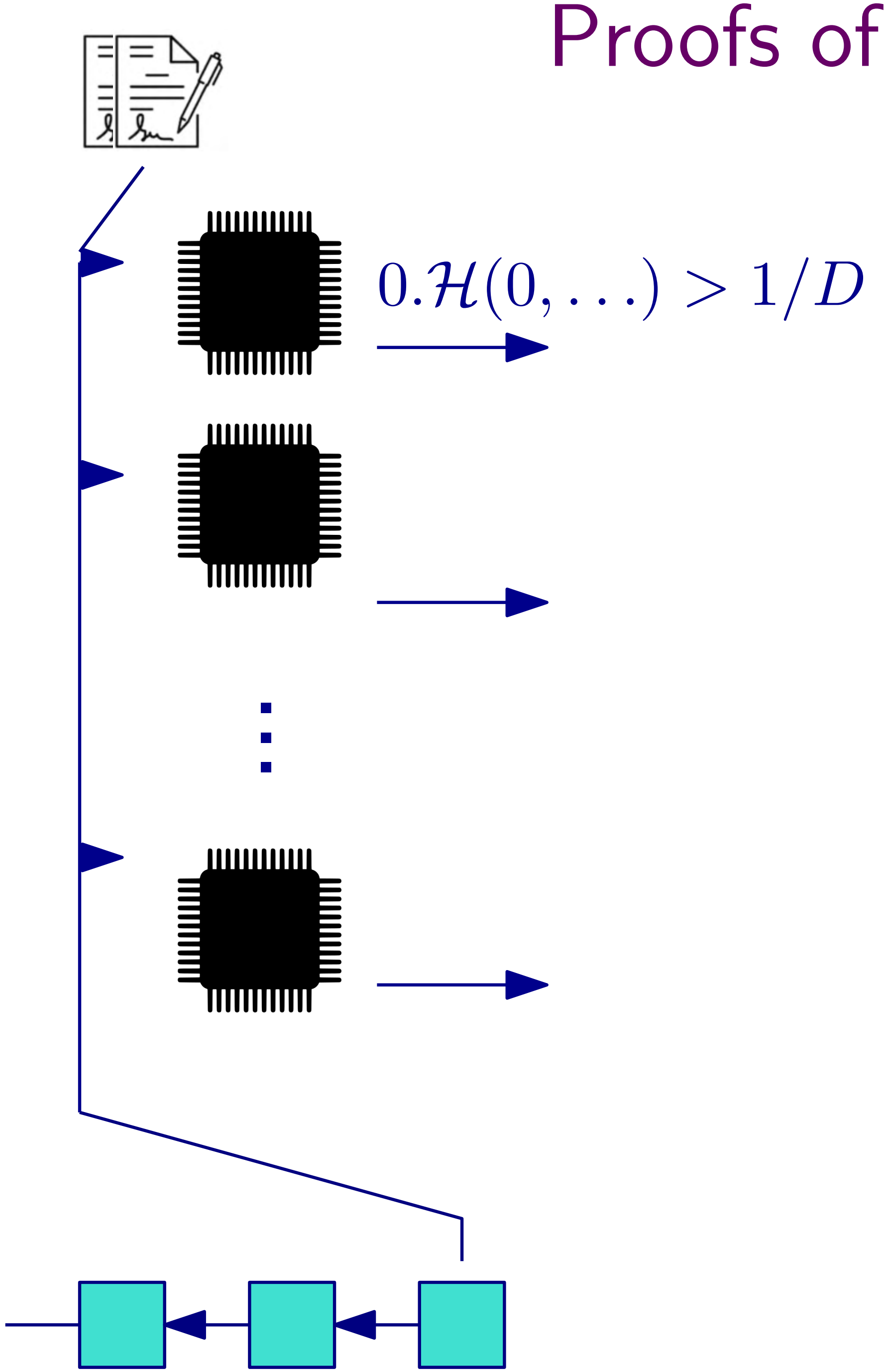
Proofs of Work in Bitcoin



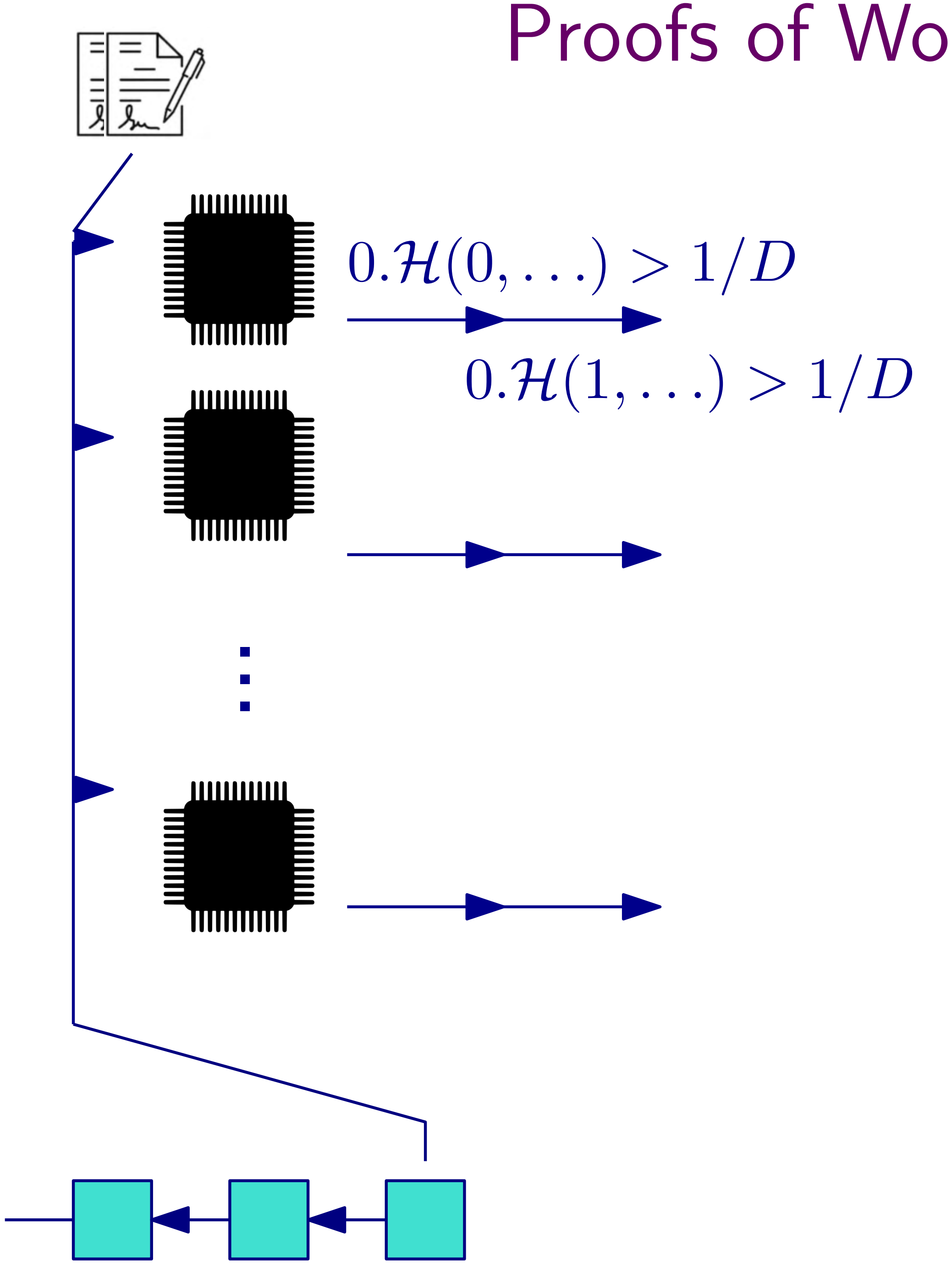
Proofs of Work in Bitcoin



Proofs of Work in Bitcoin



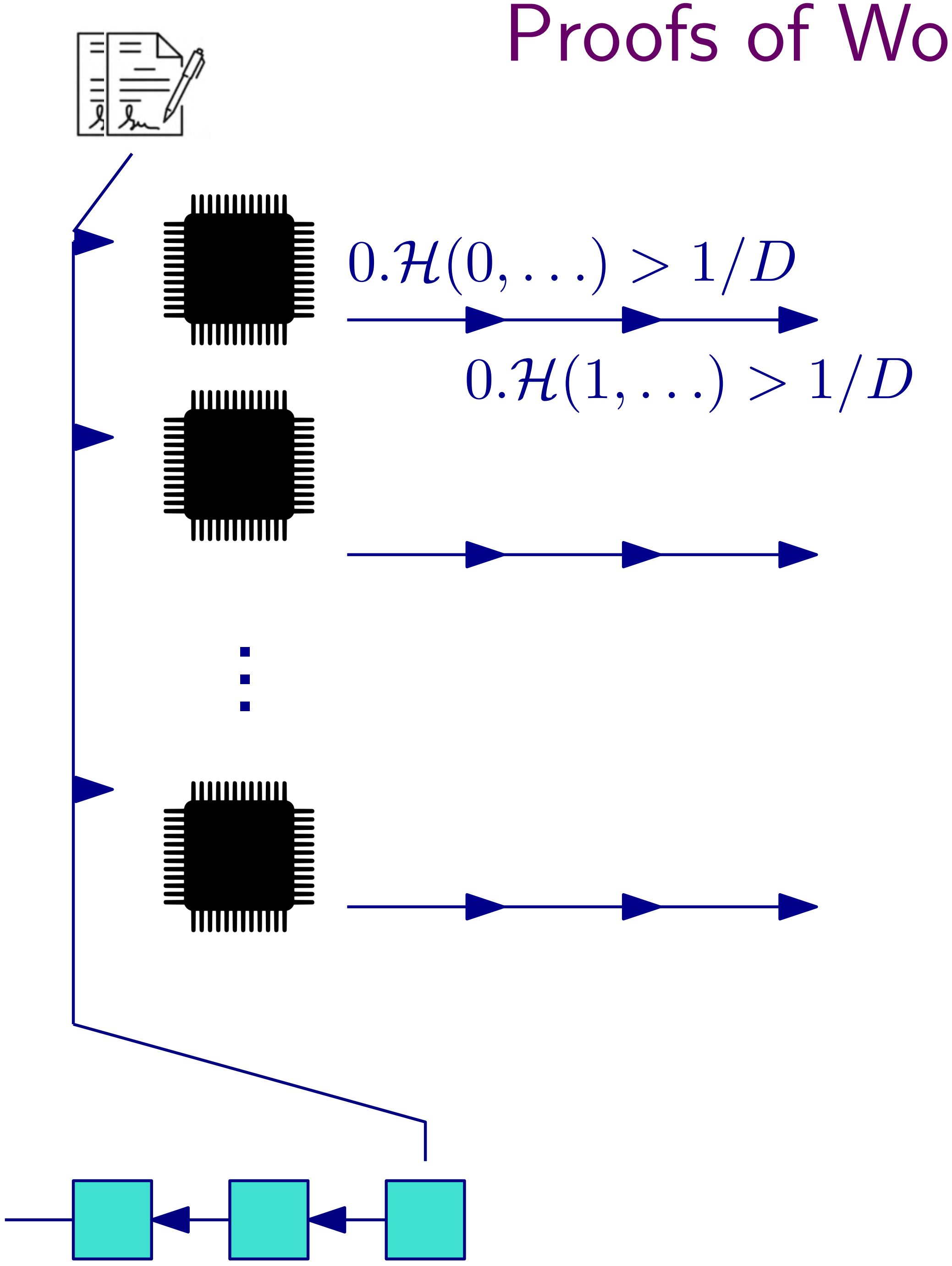
Proofs of Work in Bitcoin



$0.\mathcal{H}(0, \ldots) > 1/D$

$0.\mathcal{H}(1, \ldots) > 1/D$

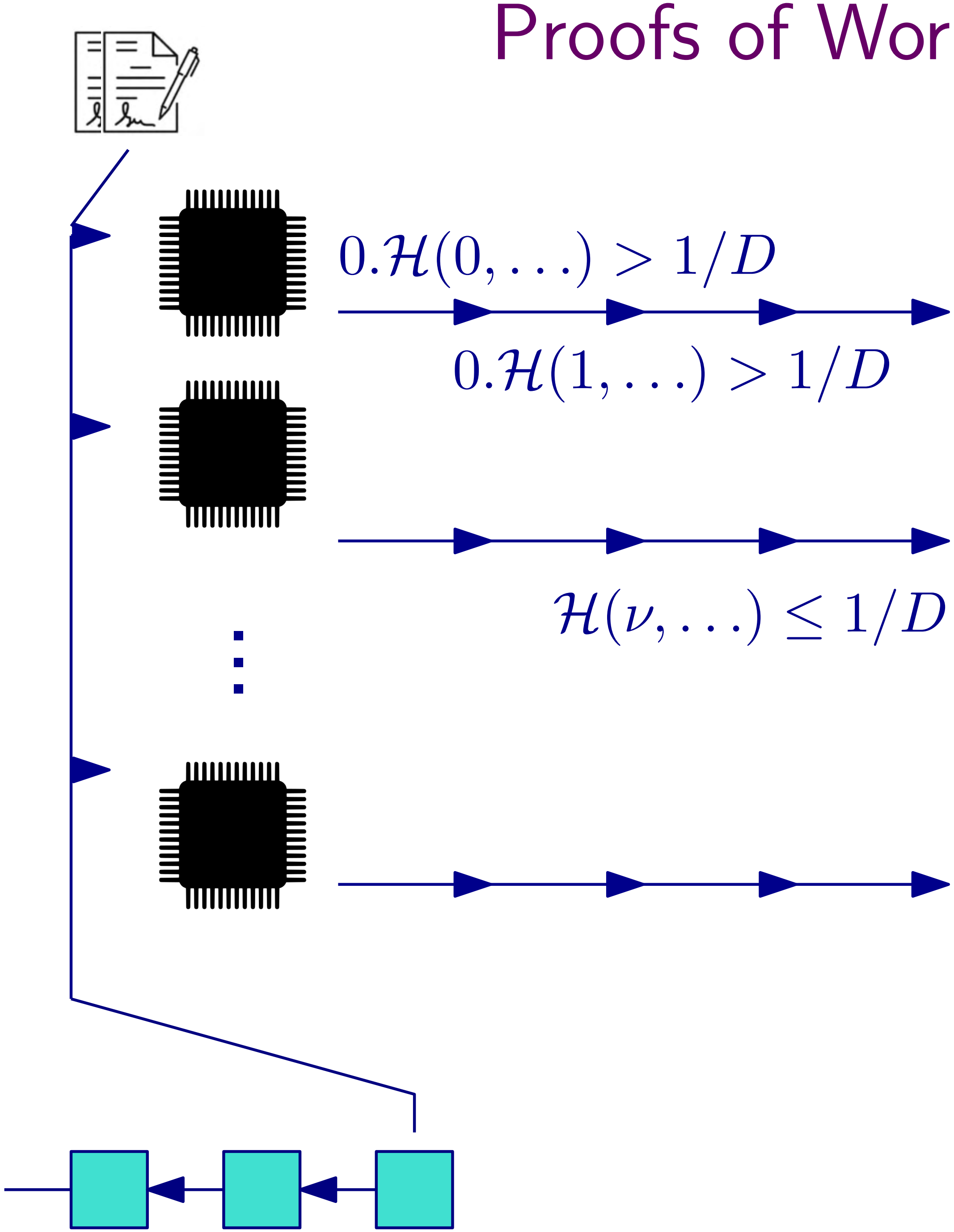
Proofs of Work in Bitcoin



$0.\mathcal{H}(0,\ldots) > 1/D$

$0.\mathcal{H}(1,\ldots) > 1/D$

Proofs of Work in Bitcoin

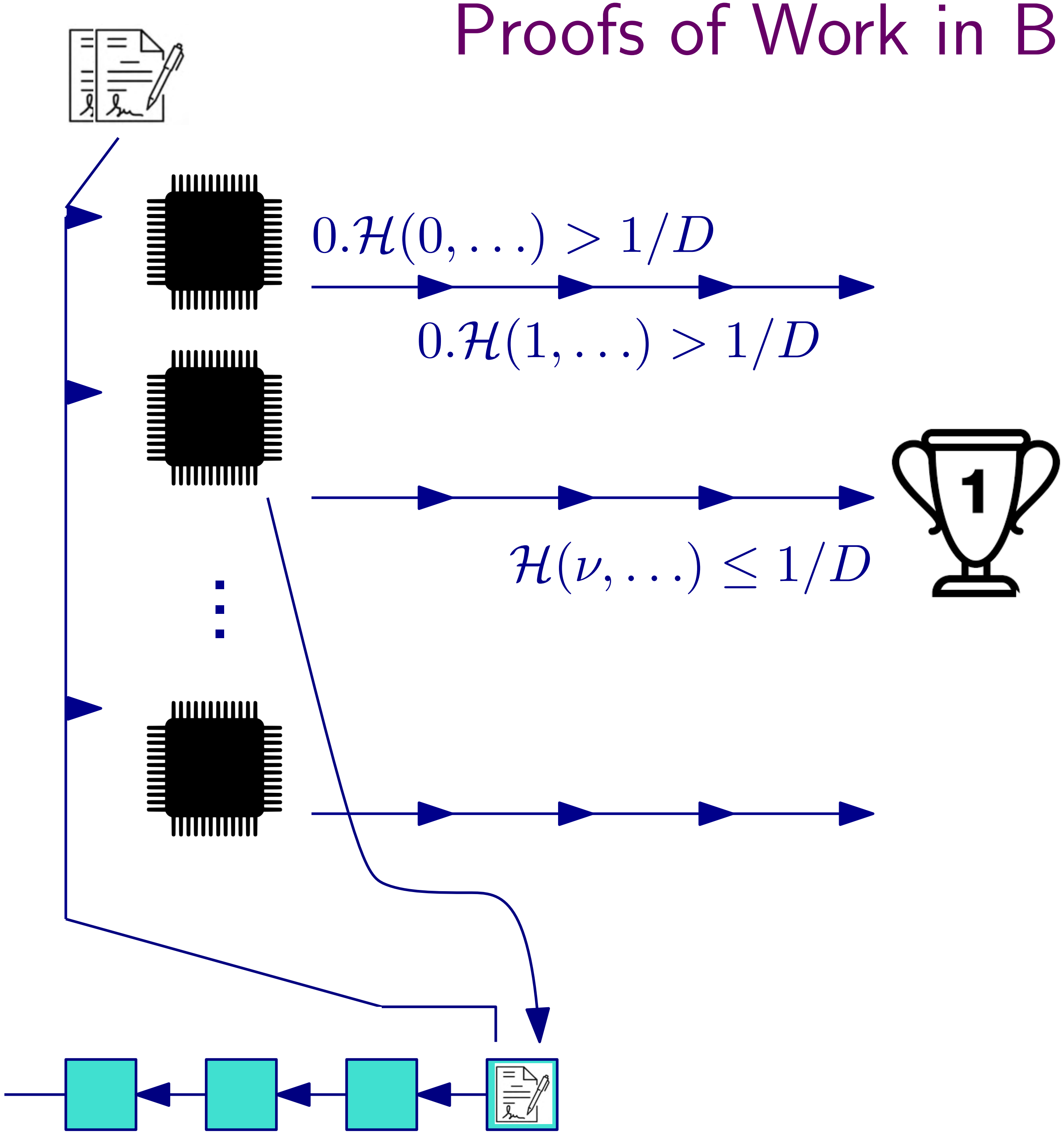


$0.\mathcal{H}(0, \ldots) > 1/D$

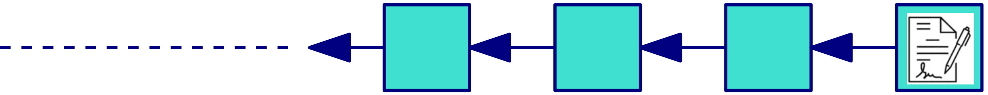
$0.\mathcal{H}(1, \ldots) > 1/D$

$\mathcal{H}(\nu, \ldots) \leq 1/D$

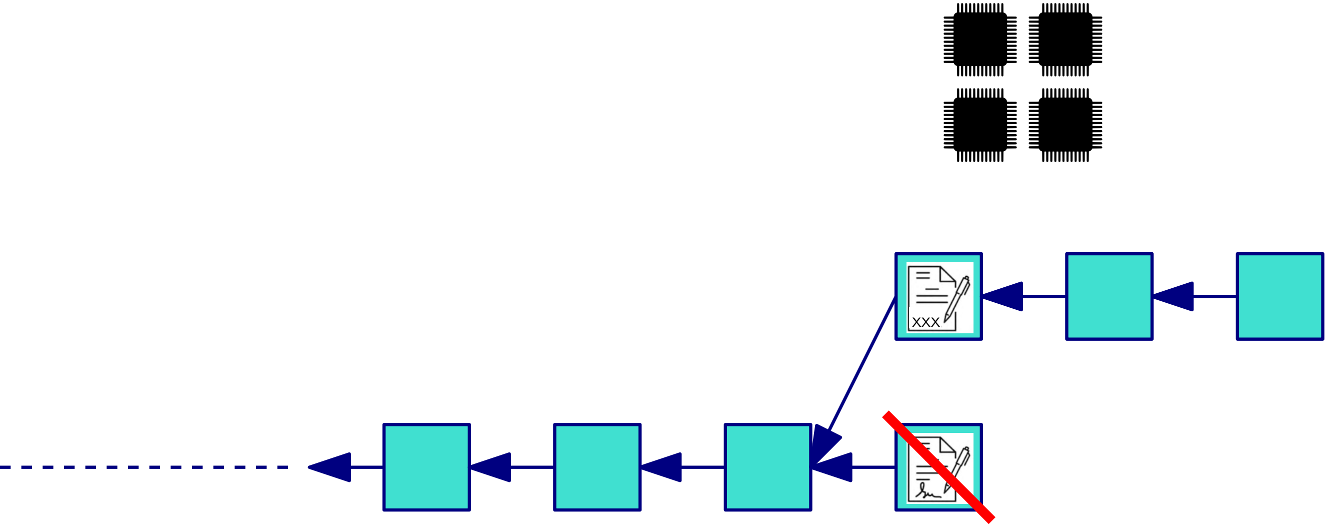
Proofs of Work in Bitcoin


$0.\mathcal{H}(0,\ldots) > 1/D$
$0.\mathcal{H}(1,\ldots) > 1/D$
$\mathcal{H}(\nu,\ldots) \leq 1/D$
1

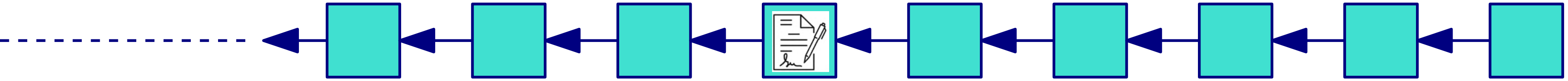
Security of Bitcoin



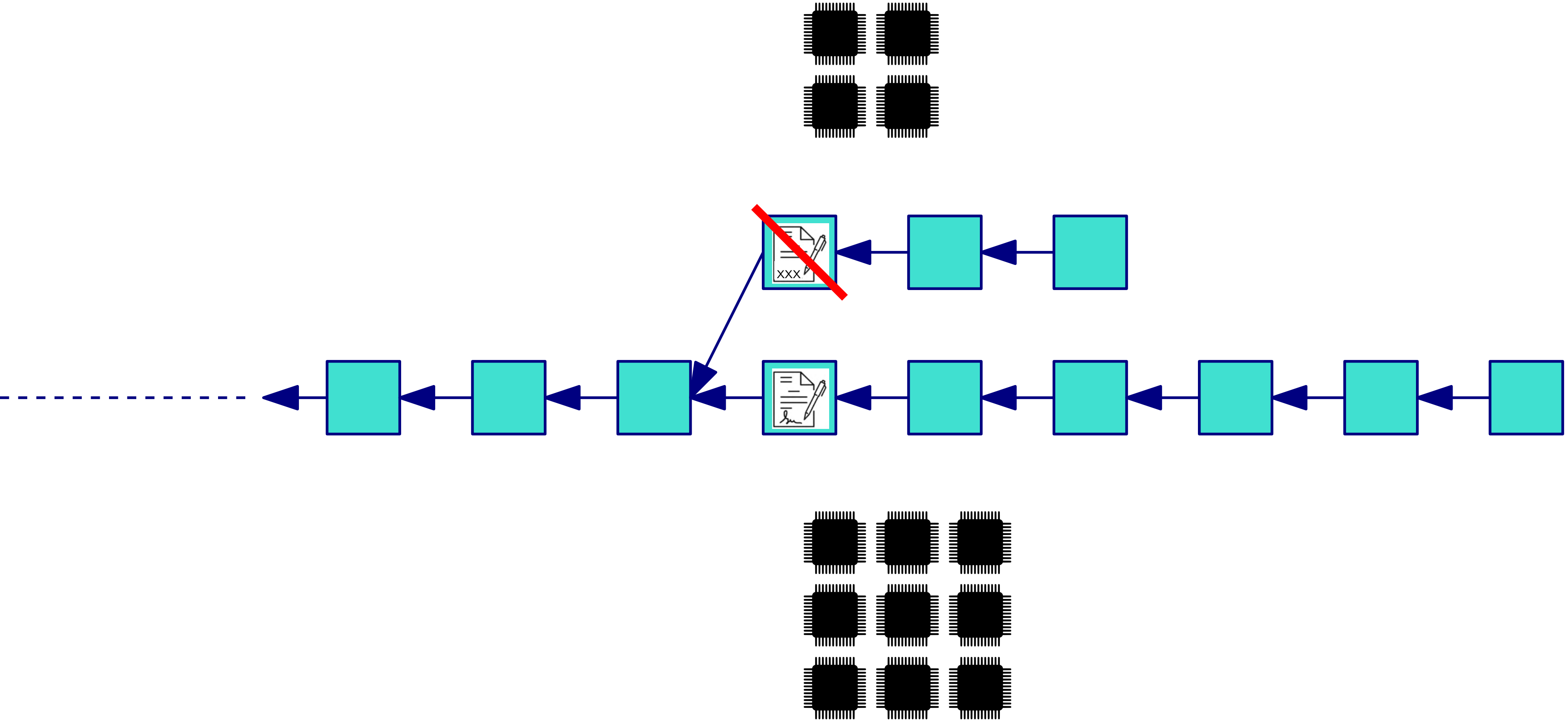
Security of Bitcoin



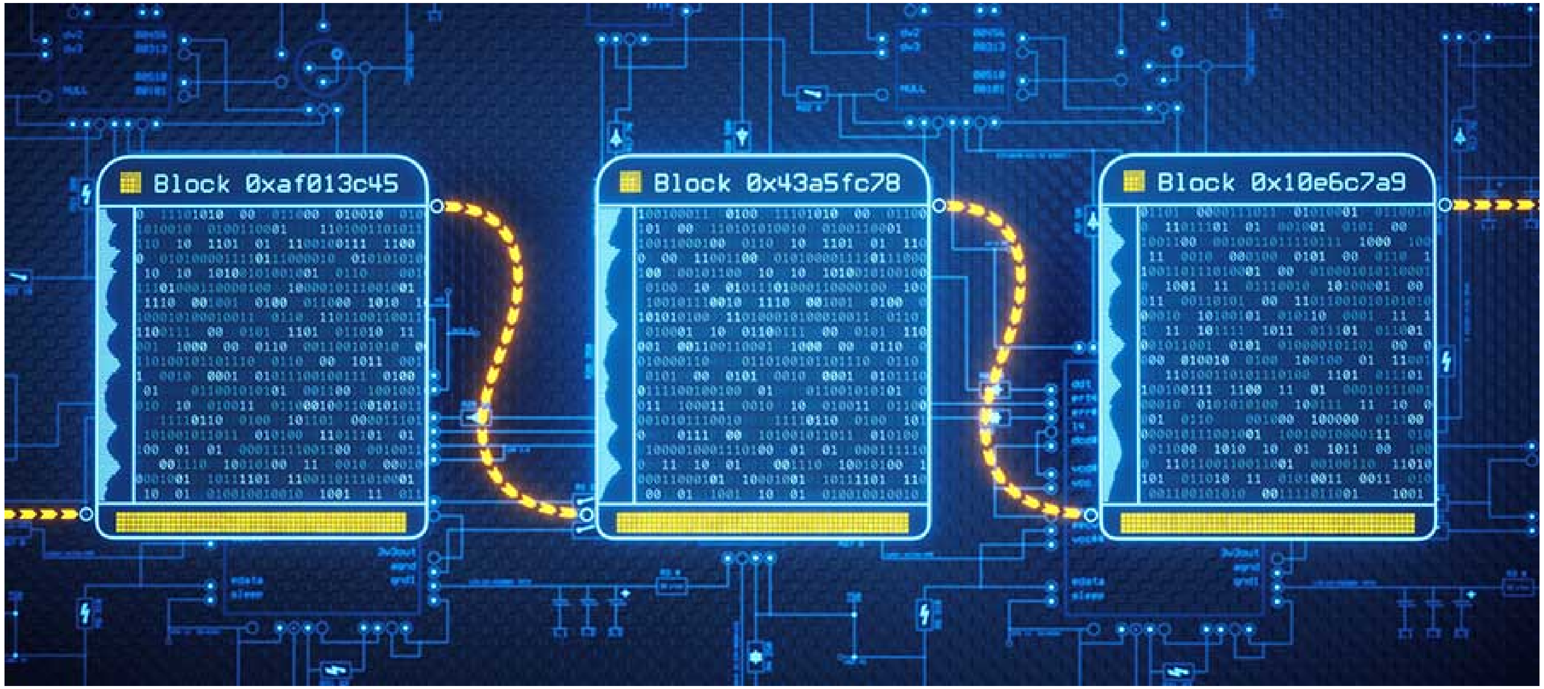
Security of Bitcoin



Security of Bitcoin



Consensus and Application Layer

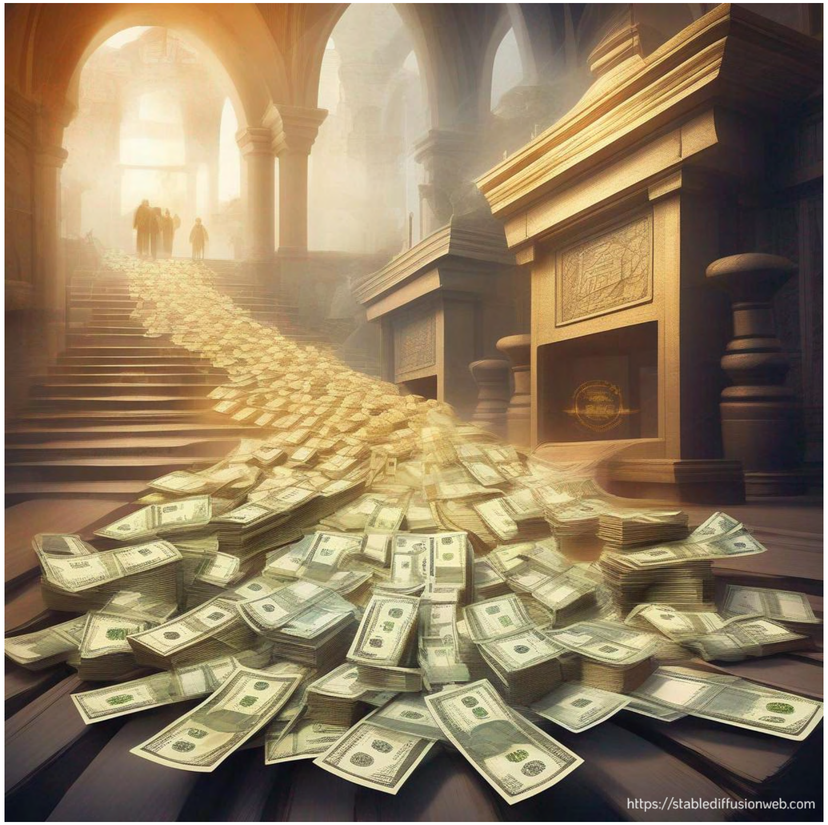


Sustainability of Blockchains

Ecological footprint from mining

Sustainability of Blockchains

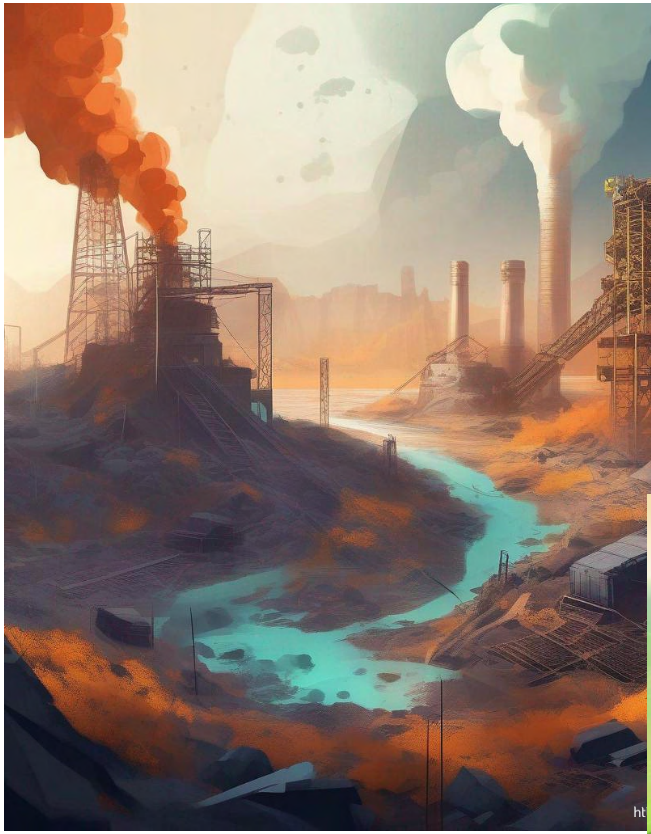
Ecological footprint from mining



Scalability

Sustainability of Blockchains

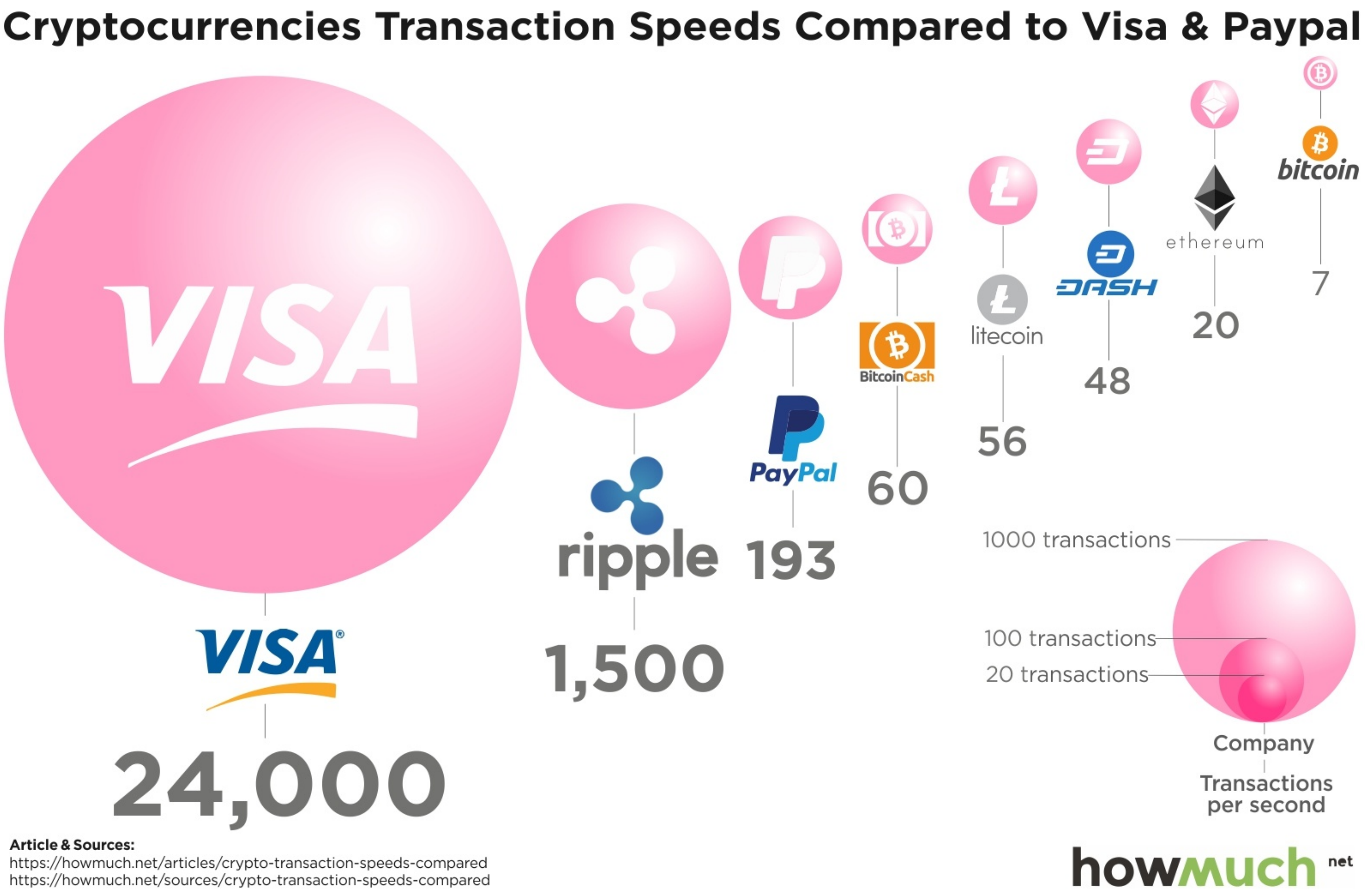
Ecological footprint from mining



Scalability

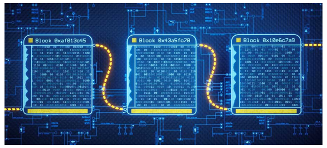
Blockchains **for** sustainability

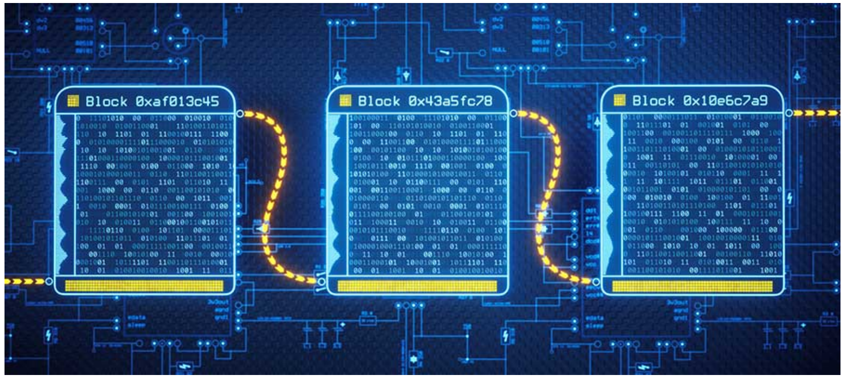
Transactions per second



Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

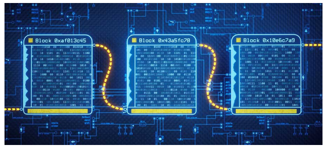
Scaling Blockchains

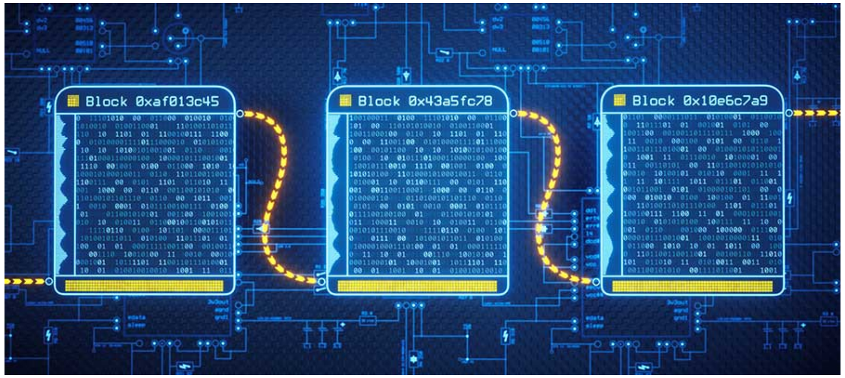




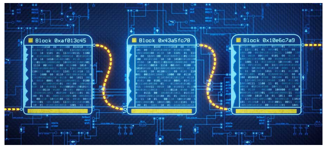
Increase block size and/or rate

Scaling Blockchains

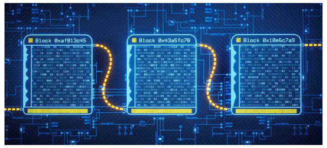


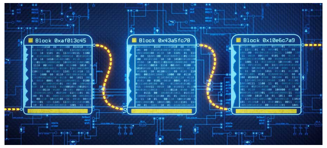


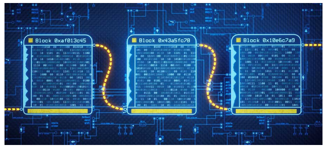
Increase block size and/or rate



Sharding

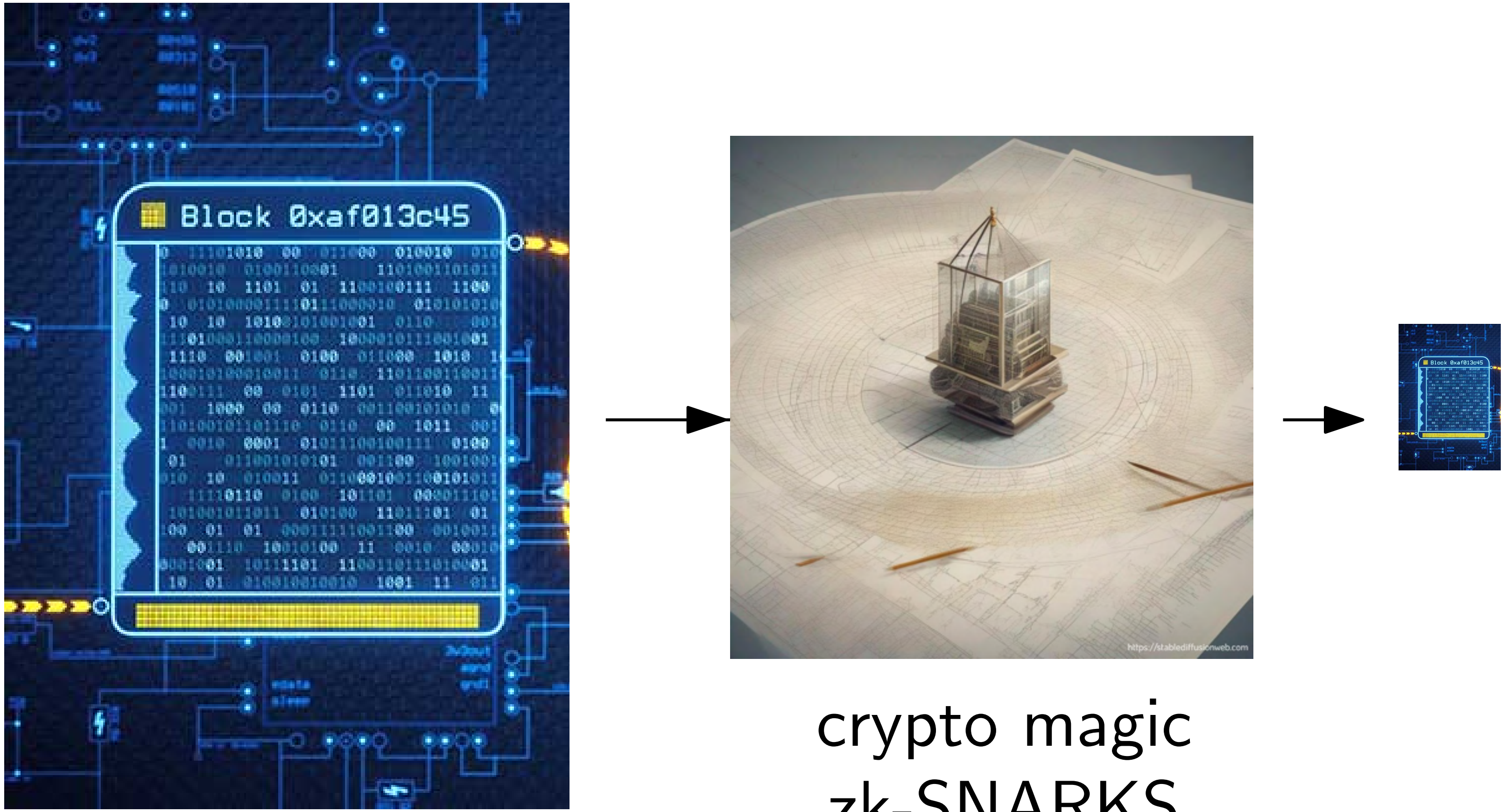






Scaling Blockchains

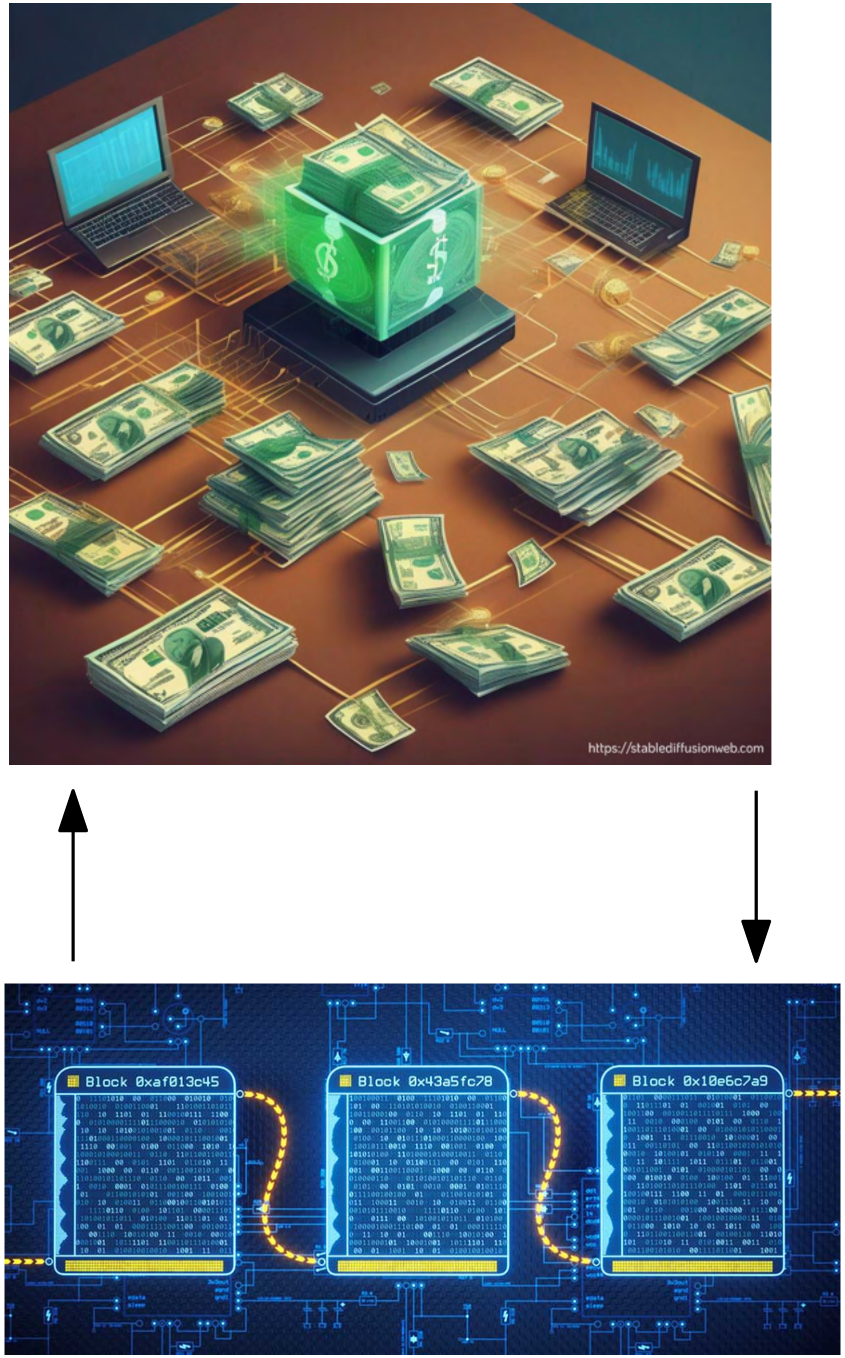
Rollups



crypto magic
zk-SNARKS

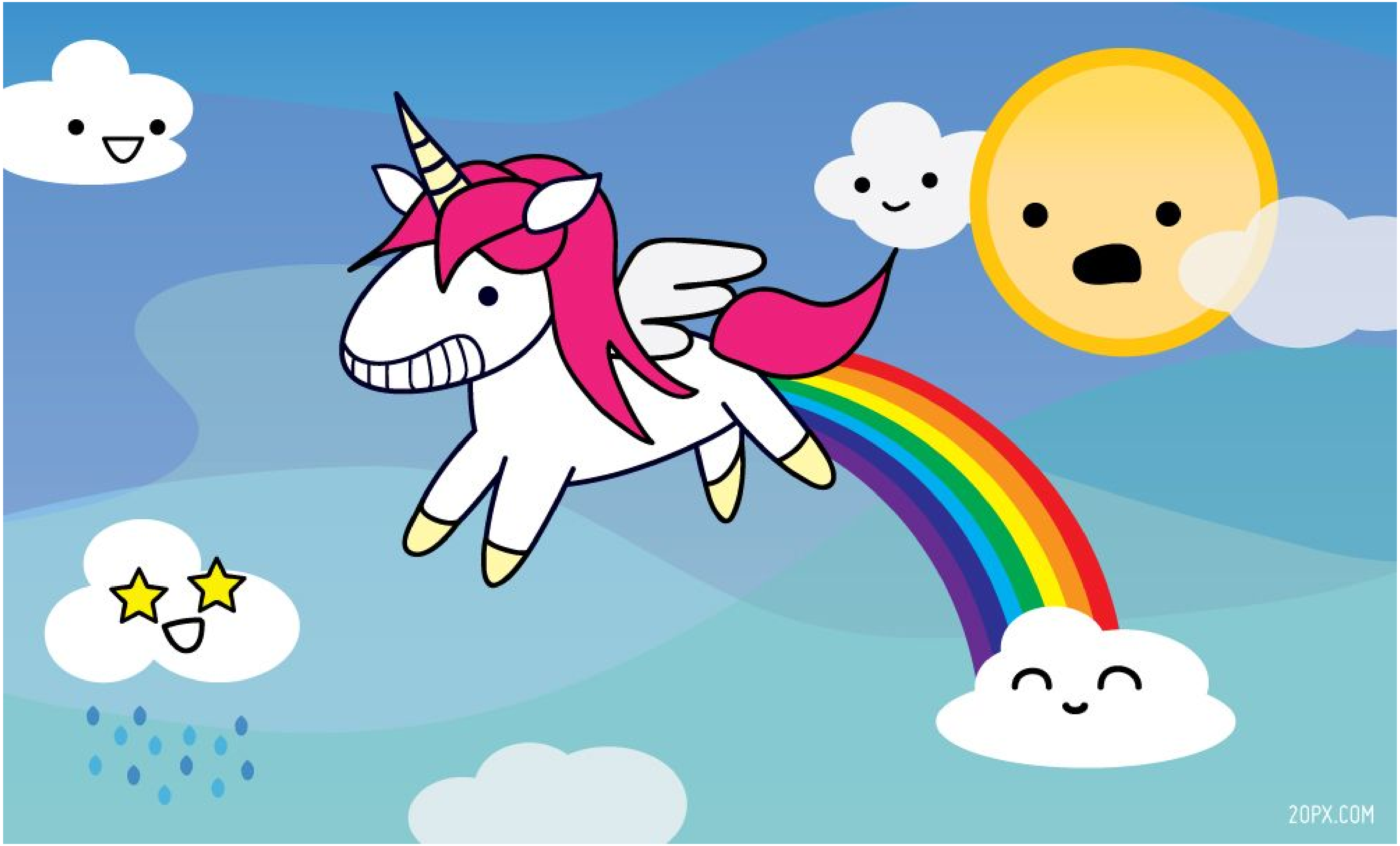
Scaling Blockchains

Layer 2 solutions:
Payment channels



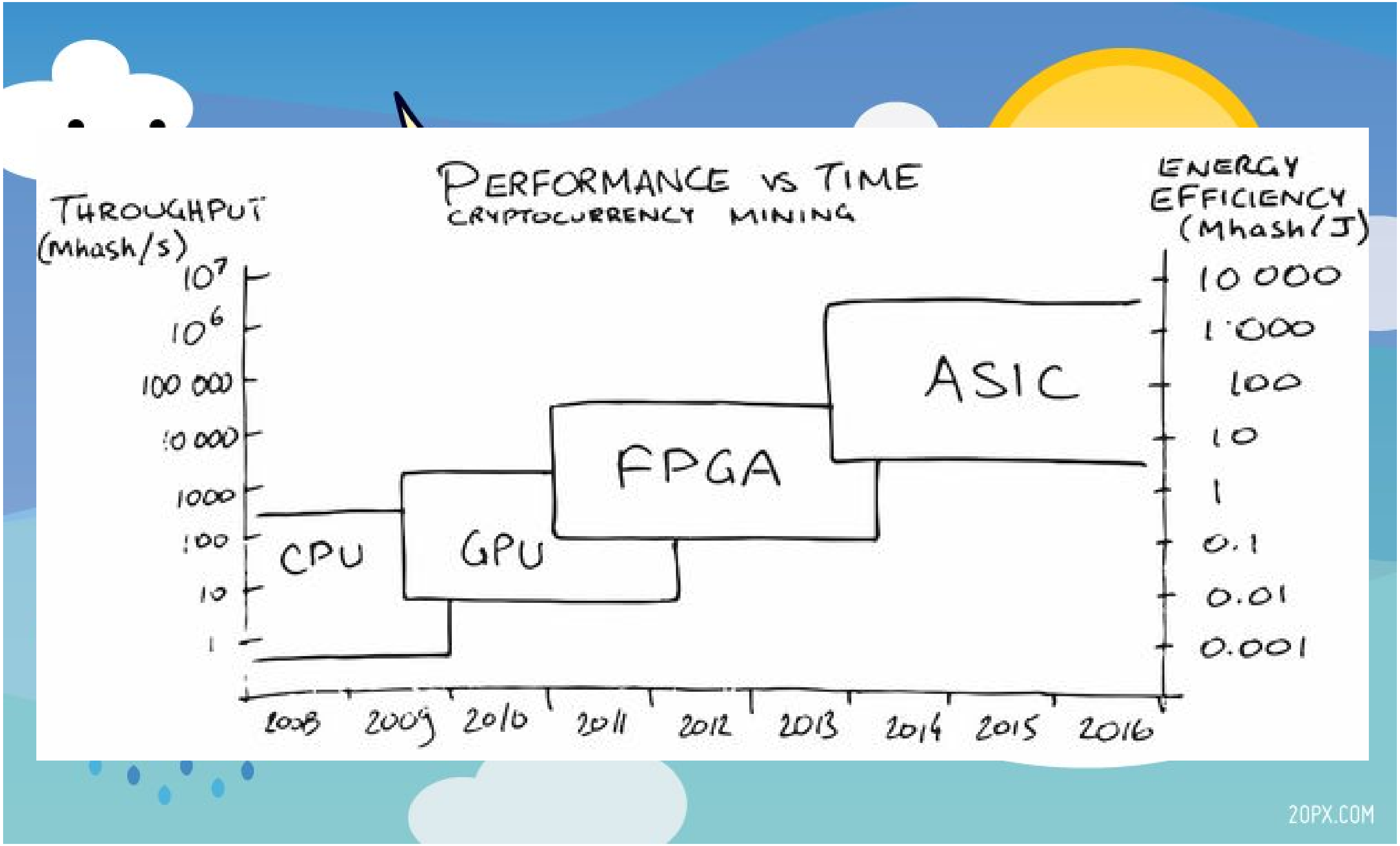
Bitcoin Mining

Nakamoto's vision: spare CPU cycles used for mining



Bitcoin Mining

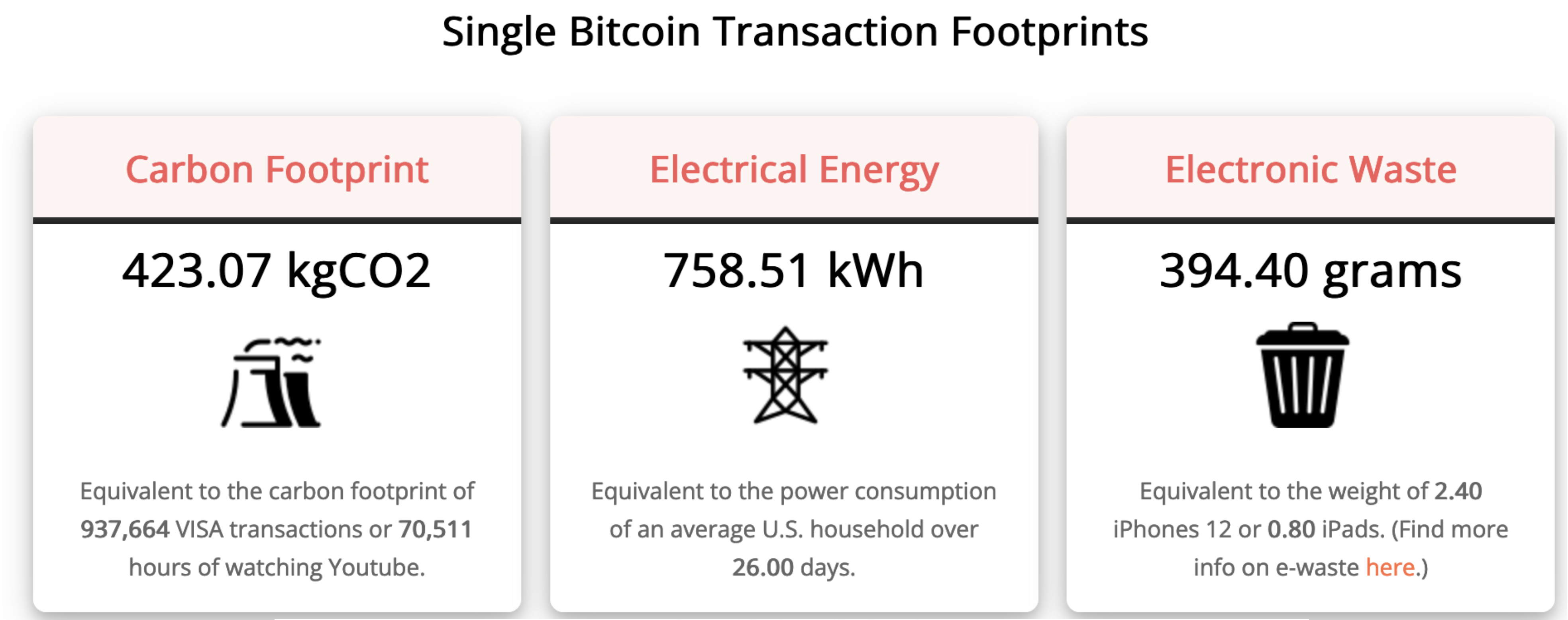
Nakamoto's vision: spare CPU cycles used for mining



Bitcoin Mining

Bitcoin Sustainability

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



Single Bitcoin Transaction Footprints

Carbon Footprint

423.07 kgCO2

Equivalent to the carbon footprint of **937,664** VISA transactions or **70,511** hours of watching Youtube.

Electrical Energy

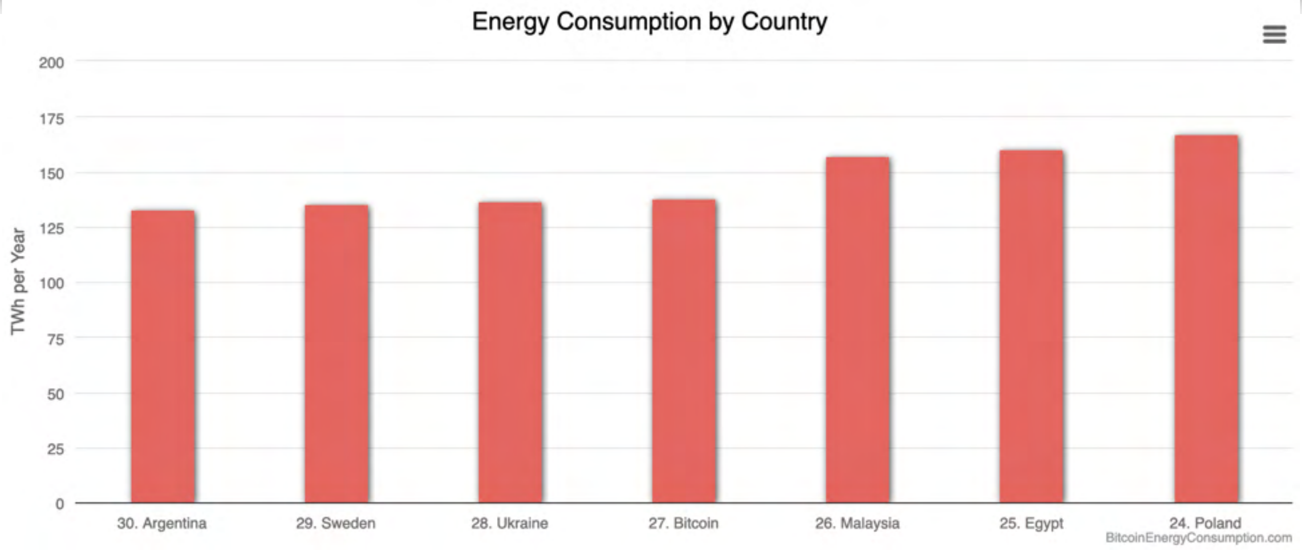
758.51 kWh

Equivalent to the power consumption of an average U.S. household over **26.00** days.

Electronic Waste

394.40 grams

Equivalent to the weight of **2.40** iPhones 12 or **0.80** iPads. (Find more info on e-waste here.)



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

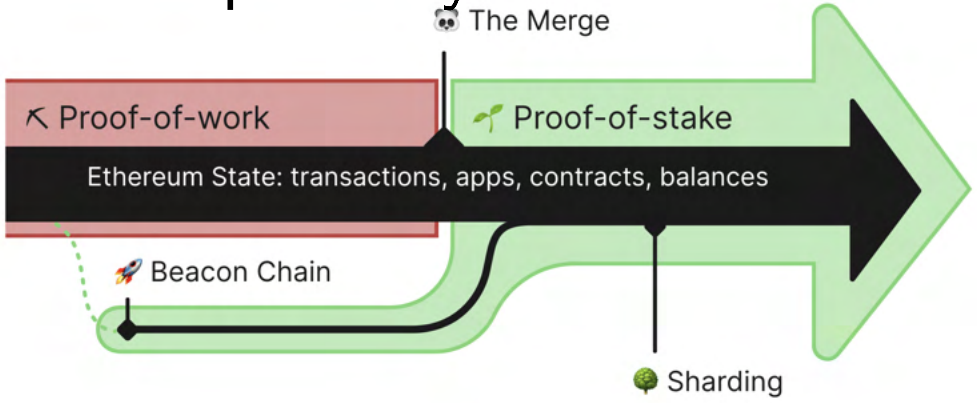
Alternatives to Proof of Work Mining?

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,. . .)

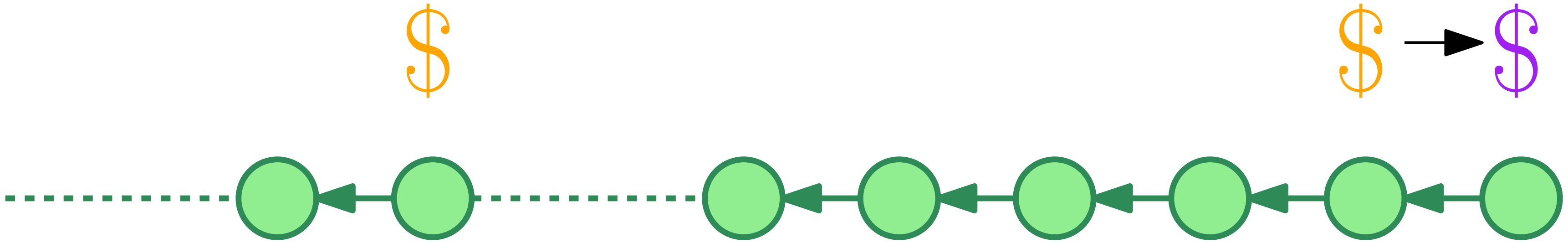
mining resource: (staked) coins

PoW vs PoS

PoStake no longer permissonless?

PoW vs PoS

Long range attack using “old keys”



staked coins

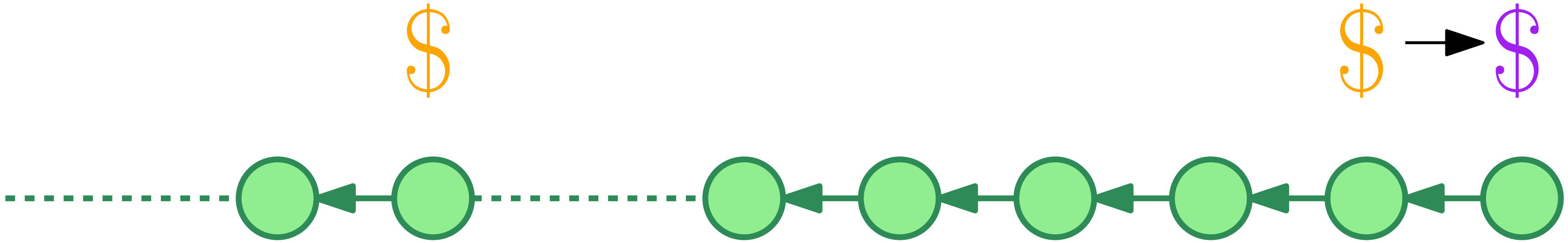
staked coins transferred to new addresses

PoW vs PoS

Long range attack using “old keys”

staked coins transferred to new addresses

staked coins



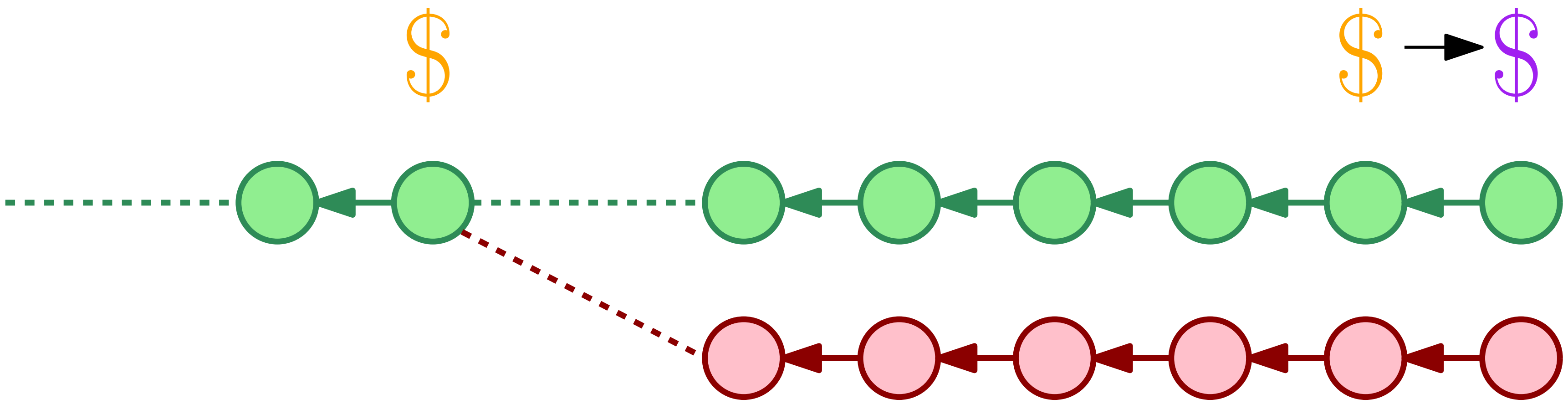
Adversary cheaply aquries $

PoW vs PoS

Long range attack using “old keys”

staked coins transferred to new addresses

staked coins

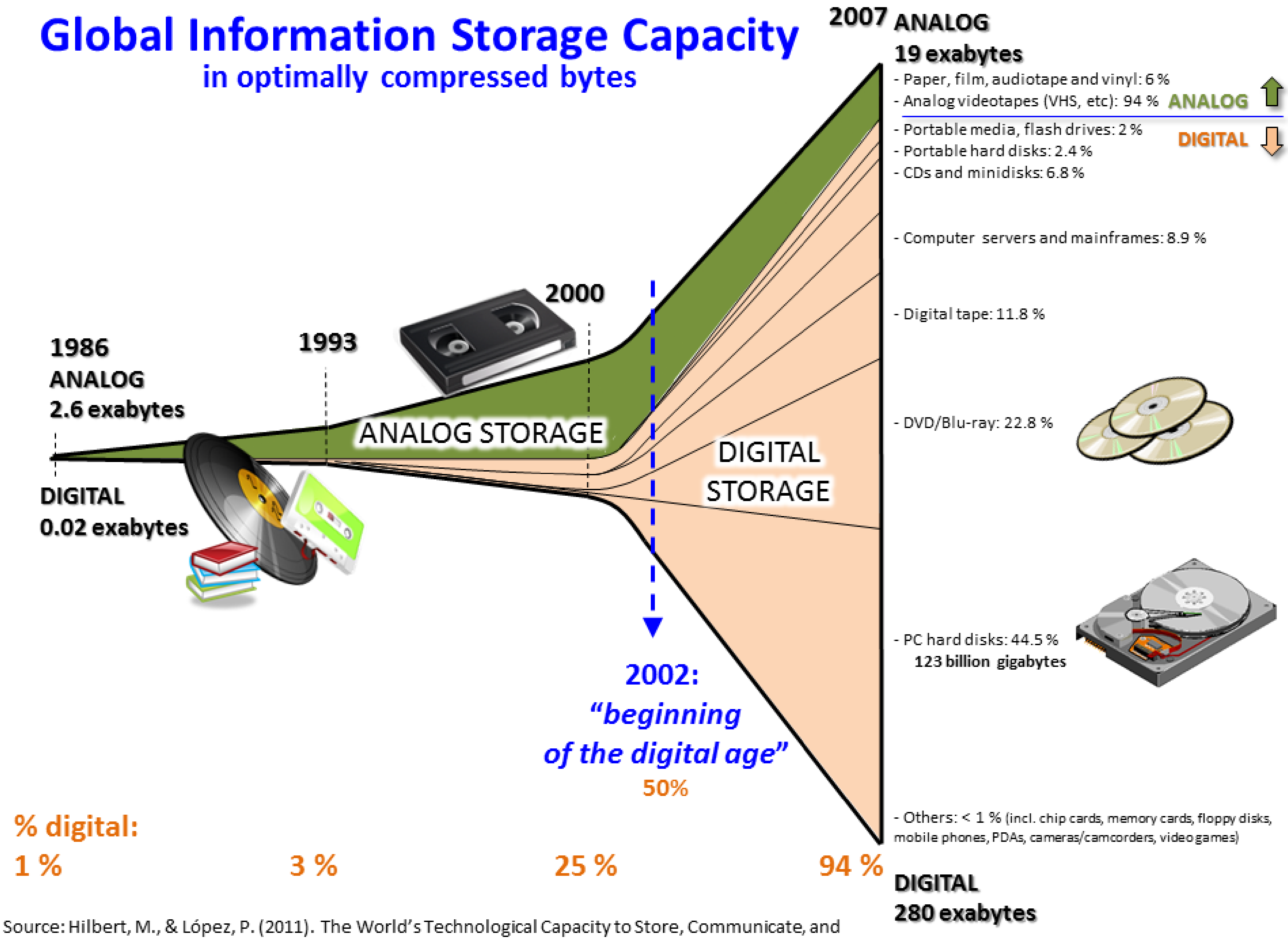


Adversary cheaply aquries $

Adversary bootstraps heavier chain using $

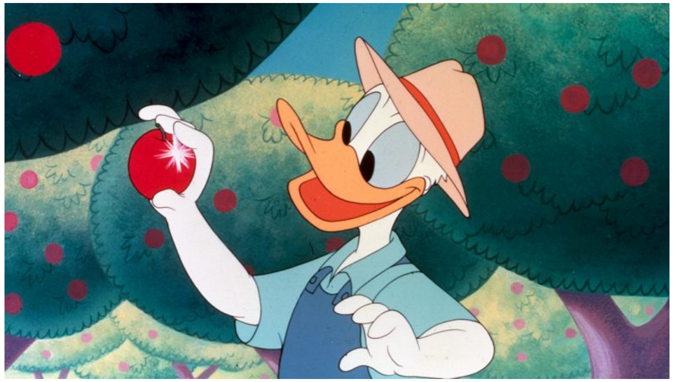
Global Information Storage Capacity

in optimally compressed bytes

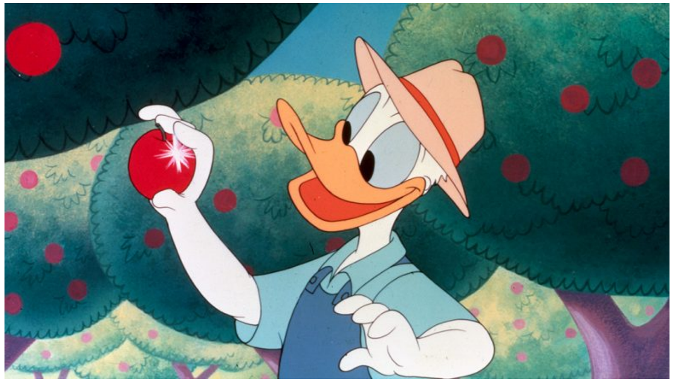


Source: Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332(6025), 60 –65. http://www.martinhilbert.net/WorldInfoCapacity.html

Work vs. Space vs. Stake Mining/Farming



Work vs. Space vs. Stake Mining/Farming



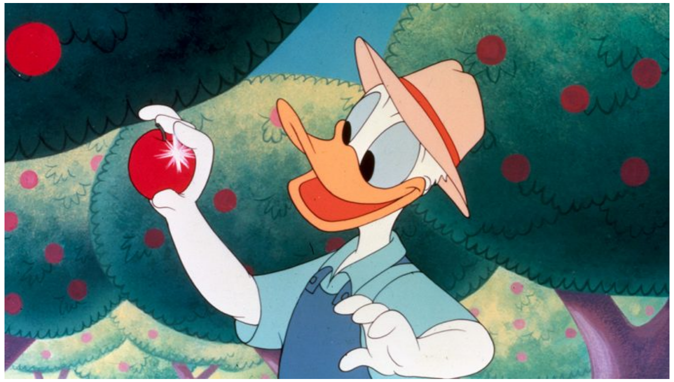
Resource is

External

External

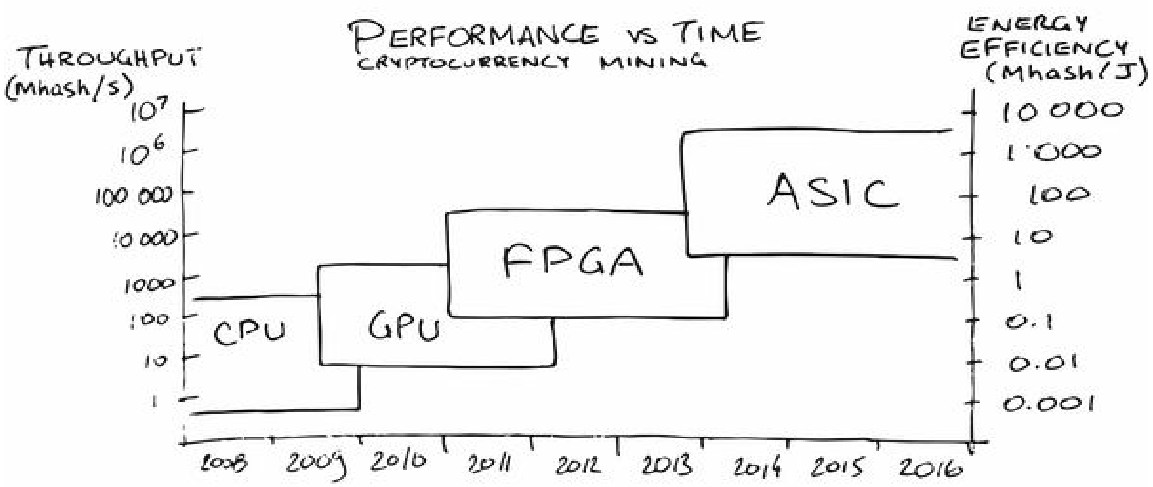
Internal

Work vs. Space vs. Stake Mining/Farming



	Resource is	Power consumption
	External	Huge
🖴	External	Tiny
	Internal	Tiny

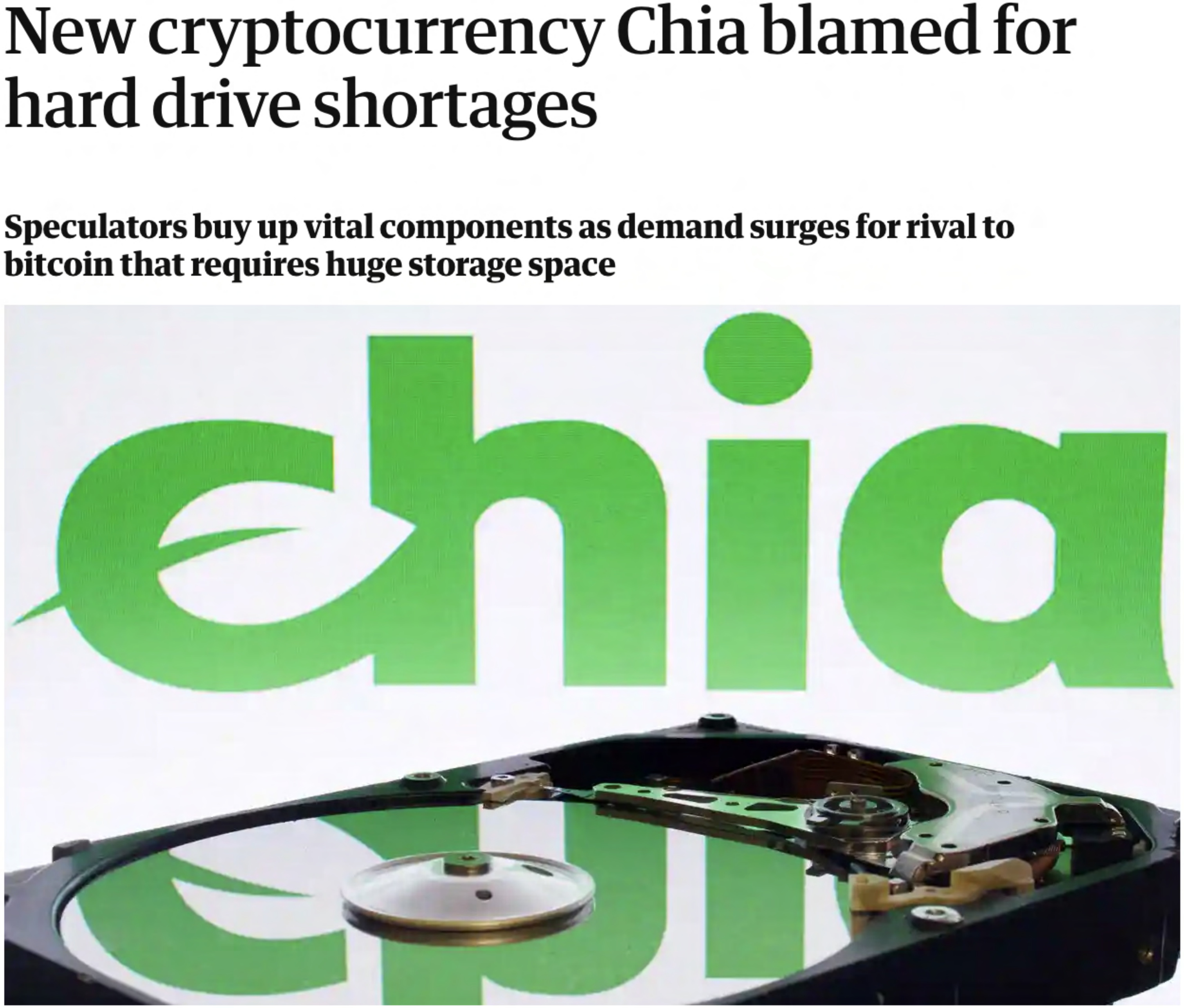
Work vs. Space vs. Stake Mining/Farming



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

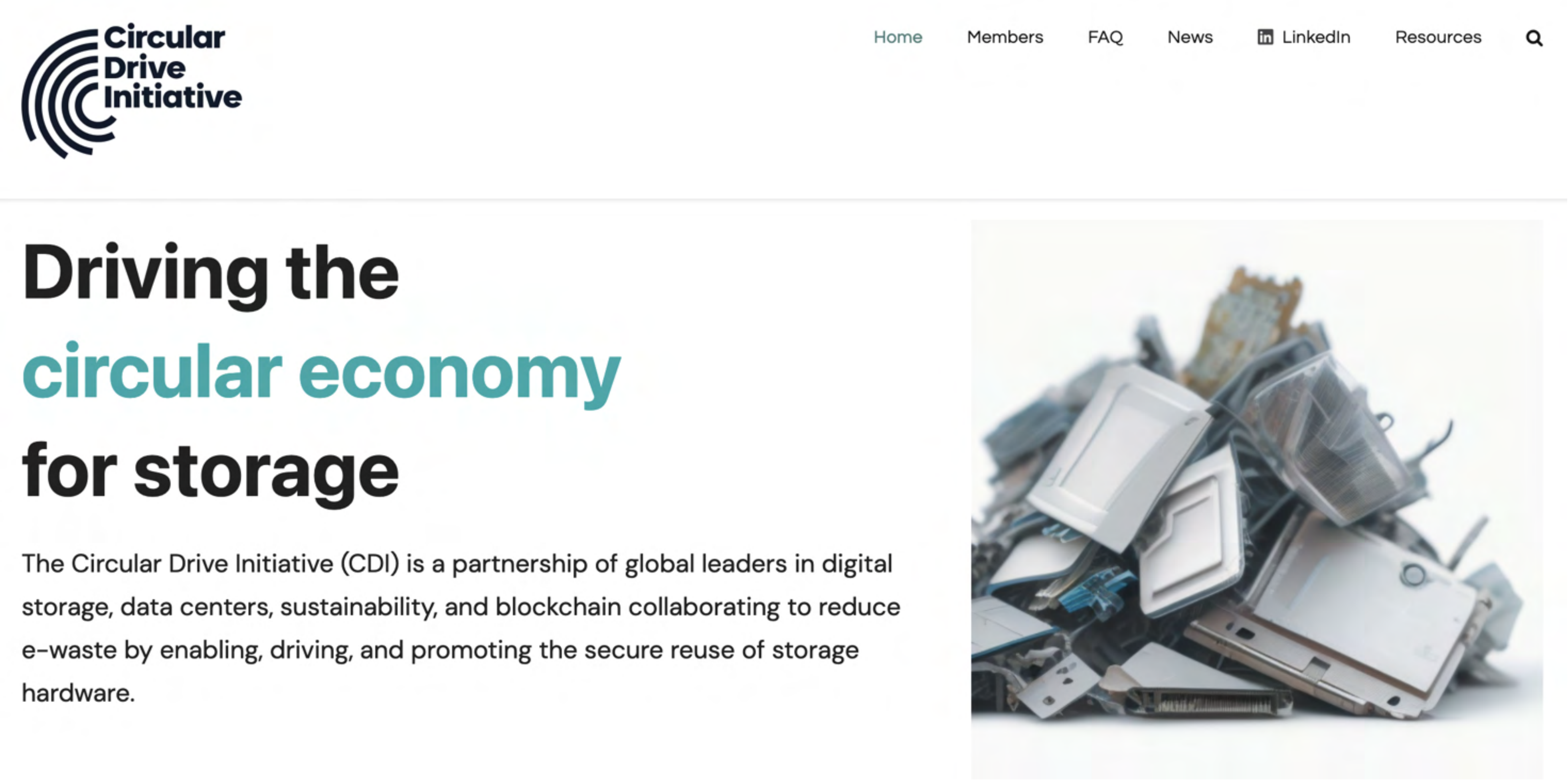
founded in 2017, launched 2021

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



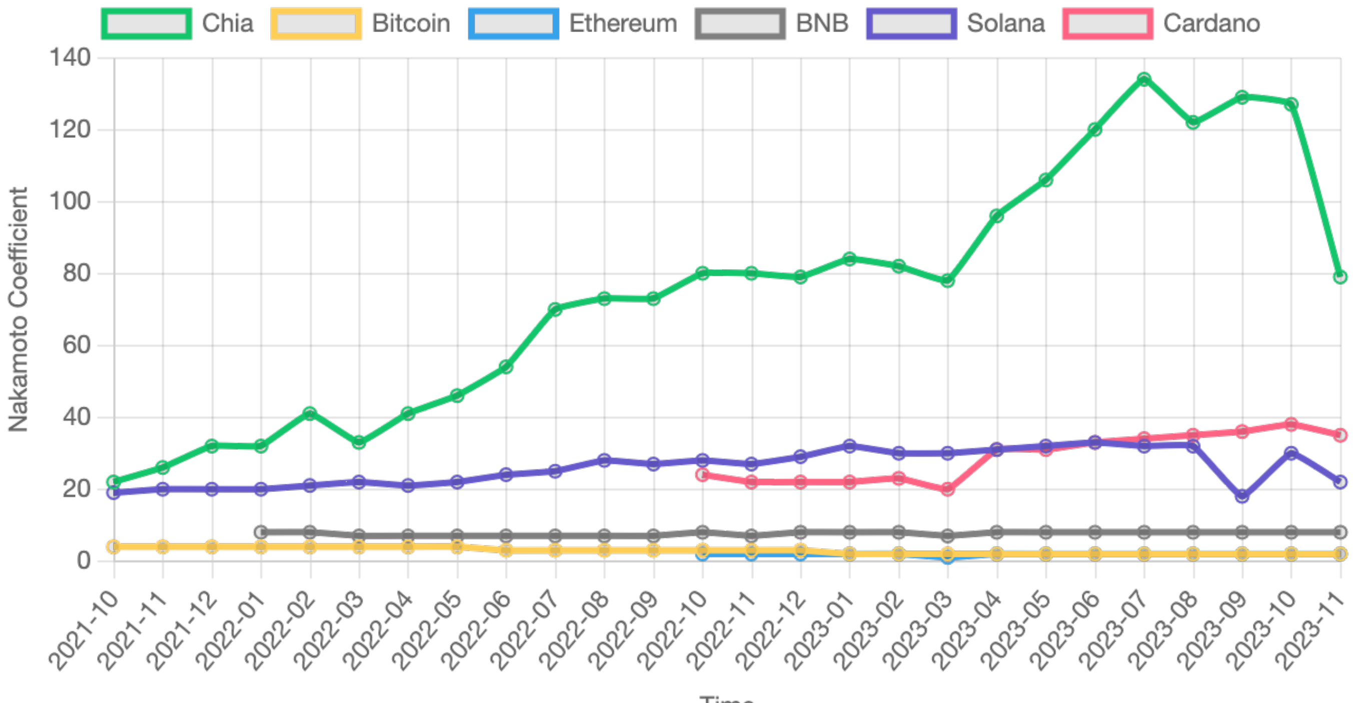
Circular Drive Initiative

Home Members FAQ News LinkedIn Resources

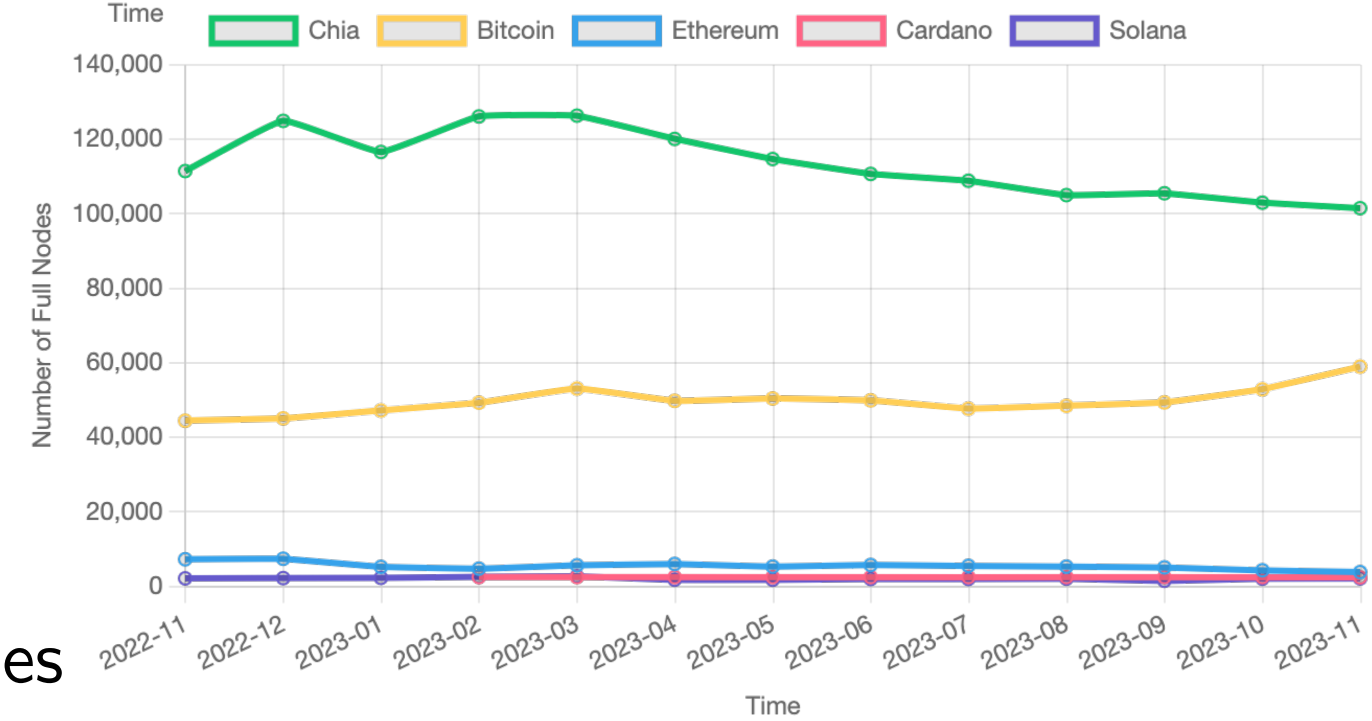
Driving the circular economy for storage

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.

https://xch.farm/decentralization/



Nakamoto Coefficient

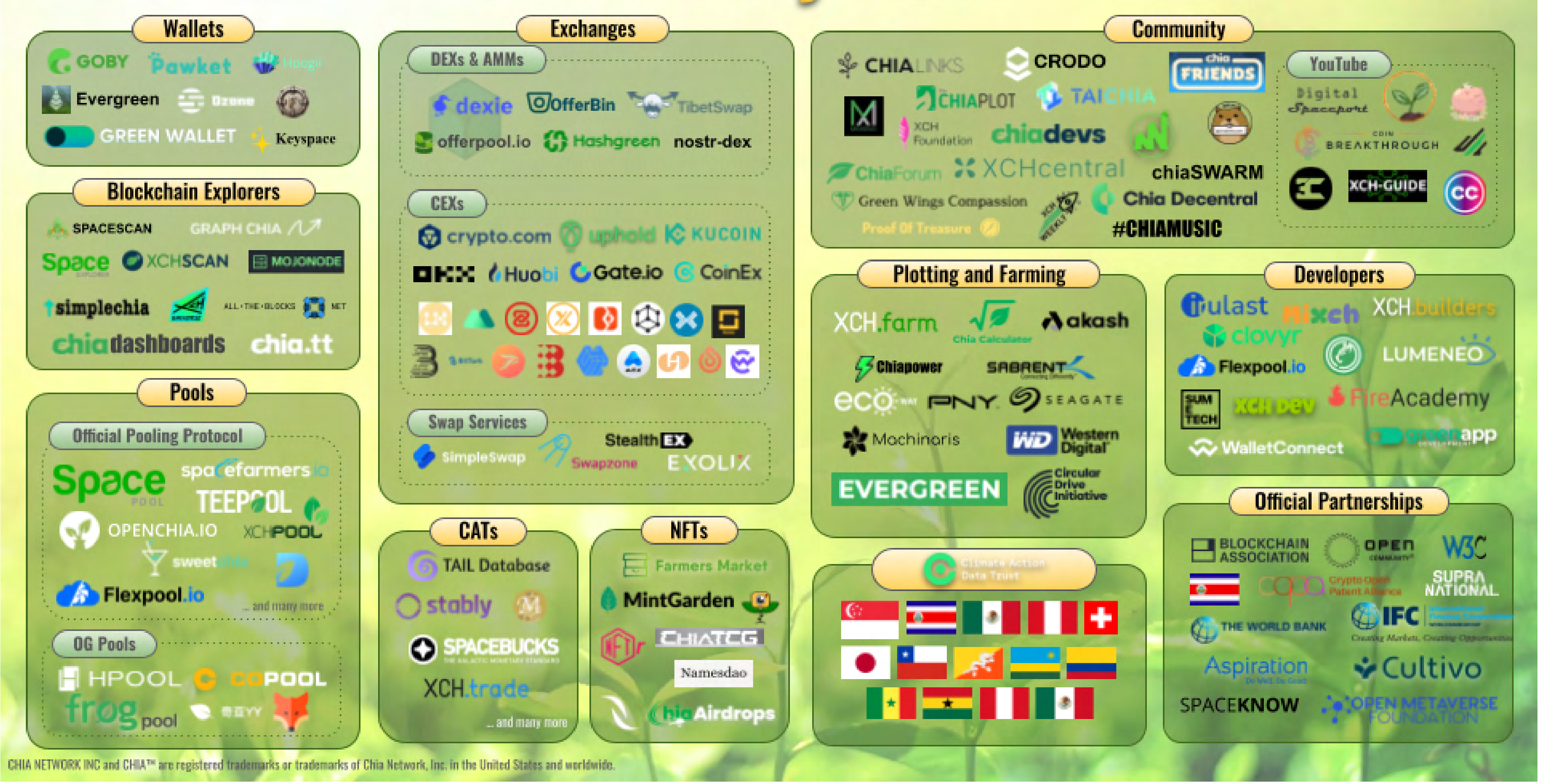


Number of Full Nodes

https://stablediffusionweb.com

chiaecosystem

June 2023
@SlowestTimelord



Wallets

GOBY
Pawket
Hoogii
Evergreen
Ozone
GREEN WALLET
Keyspace

Blockchain Explorers

SPACESCAN
GRAPH CHIA
Space EXPLORER
XCHSCAN
MOJONODE
simplechia
ALL · THE · BLOCKS .NET
chiadashboards
chia.tt

Pools

Official Pooling Protocol

Space POOL
spacefarmers.io
TEEPOOL
OPENCHIA.IO
XCHPOOL
sweetchia
Flexpool.io
... and many more

OG Pools

HPOOL
COPOOL
frog pool

Exchanges

DEXs & AMMs

dexie
OfferBin
TibetSwap
offerpool.io
Hashgreen
nostr-dex

CEXs

crypto.com
uphold
KUCOIN
OKX
Huobi
Gate.io
CoinEx

Swap Services

SimpleSwap
Swapzone
StealthEX
EXOLIX

CATs

TAIL Database
stably
SPACEBUCKS
THE GALACTIC MONETARY STANDARD
XCH.trade
... and many more

NFTs

Farmers Market
MintGarden
CHIATCG
Namesdao
ChiaAirdrops

Community

CHIALINKS
CRODO
chia FRIENDS
CHIAPLOT
TAICHIA
XCH Foundation
chiadevs
ChiaForum
XCHcentral
chiaSWARM
Green Wings Compassion
Chia Decentral
Proof Of Treasure
XCH WEEKLY
#CHIAMUSIC

YouTube

Digital Spaceport
COIN BREAKTHROUGH
XCH-GUIDE
CC

Plotting and Farming

XCH.farm
Chia Calculator
akash
Chiapower
SABRENT
eco
PNY
SEAGATE
Machinaris
WD Western Digital
EVERGREEN
Circular Drive Initiative

Developers

ulast
Mixch
XCH.builders
clovyr
Flexpool.io
LUMENEO
SUM TECH
XCH DEV
FireAcademy
WalletConnect
greenapp DEVELOPMENT

Official Partnerships

BLOCKCHAIN ASSOCIATION
OPEN COMMUNITY
W3C
copa Crypto Open Patent Alliance
SUPRA NATIONAL
THE WORLD BANK
IFC International Finance Corporation
Creating Markets, Creating Opportunities
Aspiration Do Well. Do Good.
Cultivo
SPACEKNOW
OPEN METAVERSE FOUNDATION

Climate Action Data Trust

CHIA NETWORK INC and CHIA™ are registered trademarks or trademarks of Chia Network, Inc. in the United States and worldwide.

Climate Warehouse: Helping Countries Leverage Climate Markets and Carbon Pricing

https://youtu.be/7k9U60scEK4

Proofs of Space

Proofs of Space

```
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
```

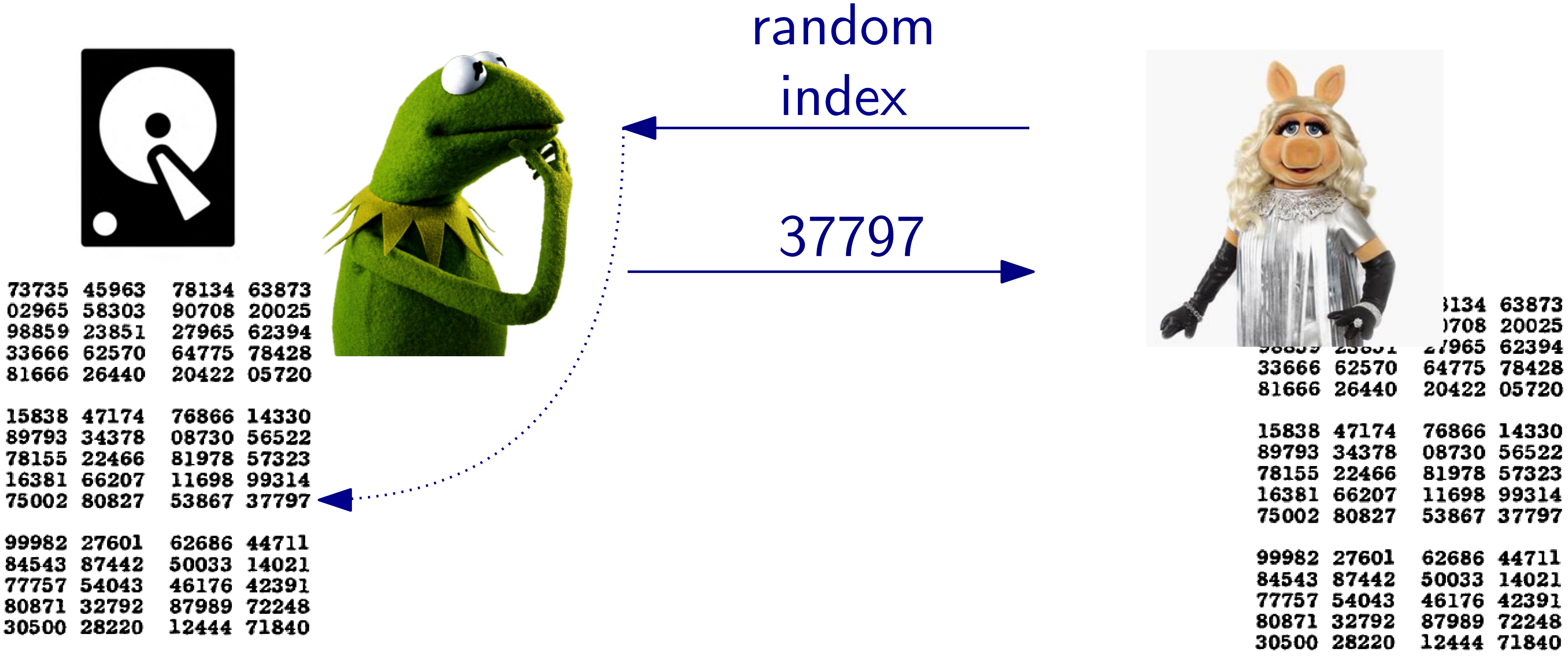
```
              134 63873
              708 20025
              7965 62394
33666 62570   64775 78428
81666 26440   20422 05720

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

```
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
```

```
               134 63873
               708 20025
               7965 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



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
```

```
              134 63873
              708 20025
              7965 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

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

TOO MUCH COMMUNICATION

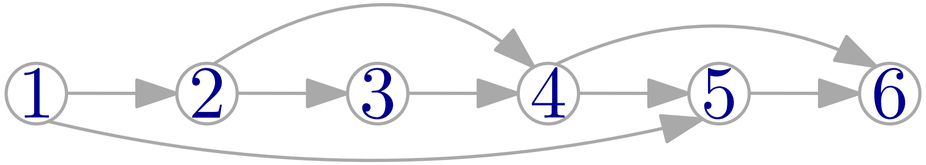
```
99982 27601  62686 44711
84543 87442  50033 14021
77757 54043  46176 42391
80871 32792  87989 72248
30500 28220  12444 71840
```

Proofs of Space

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

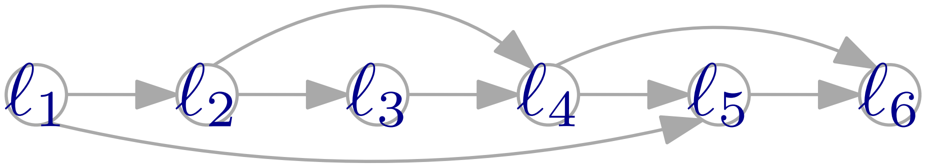
Proofs of Space

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

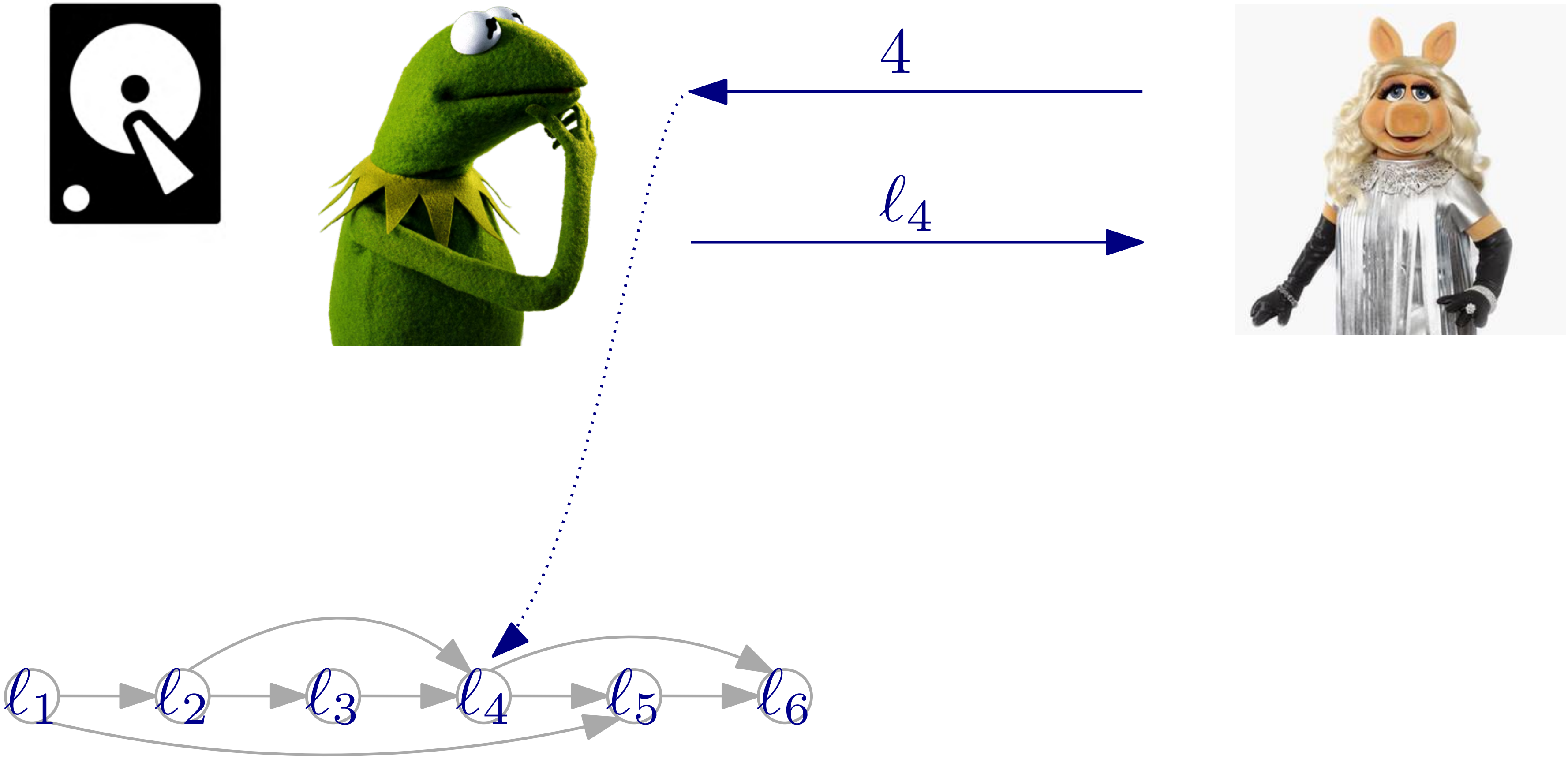


Proofs of Space

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



Proofs of Space



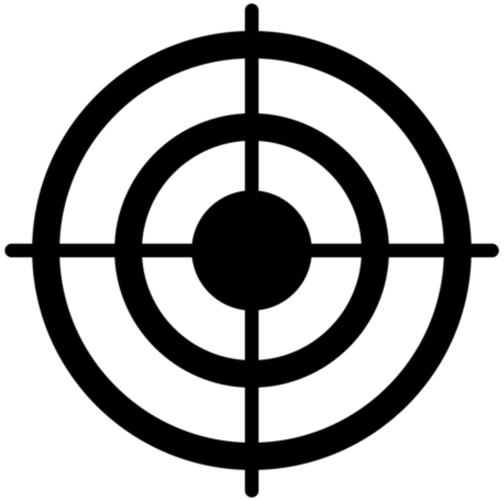
The Main Problem with Efficient Proof Systems

N Proofs of Work N times as costly as one

N Proofs of Space/Stake/. . . as cheap as 1

The Main Problem with Efficient Proof Systems

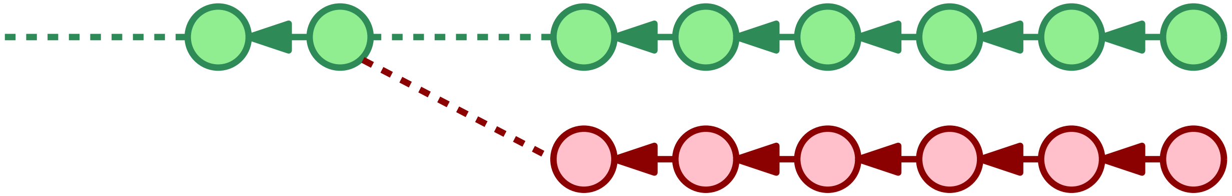
N Proofs of Work N times as costly as one



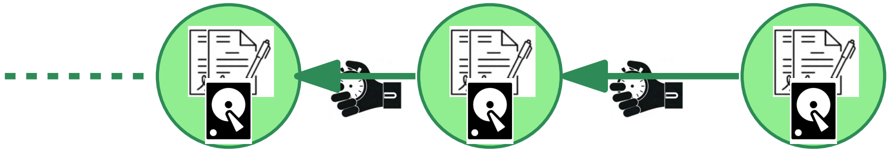
N Proofs of Space/Stake/. . . as cheap as 1

The 3 Issues with Efficient Proofs

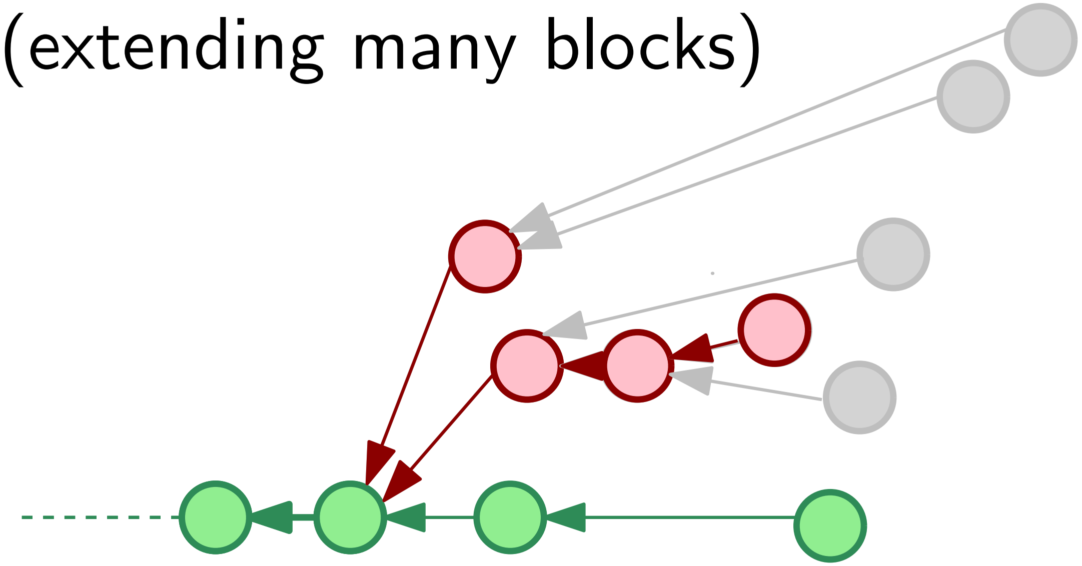
1) Bootstrapping (Long range forks, seeing the future)



2) Digging (grinding block)

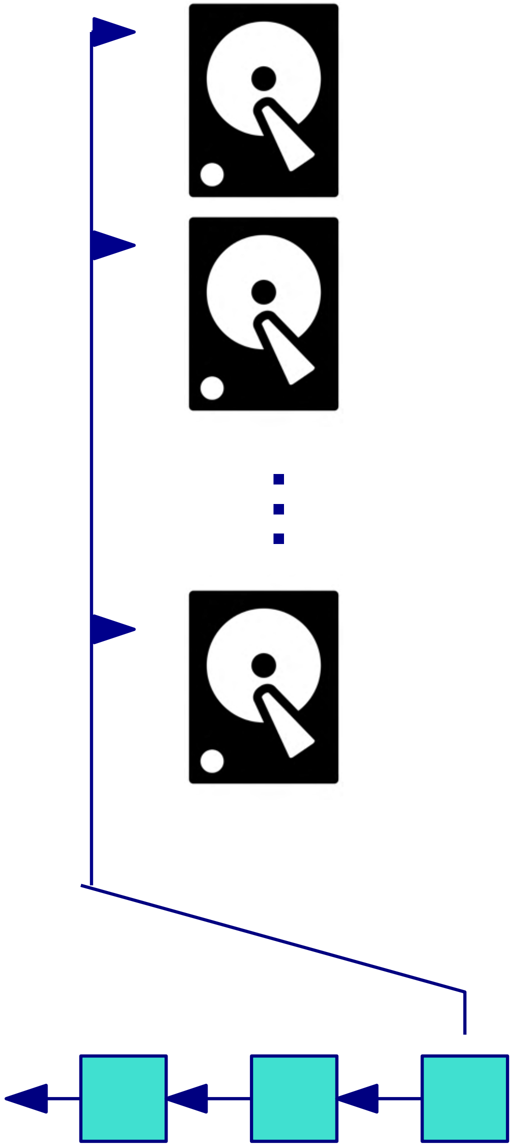


3) Double dipping (extending many blocks)

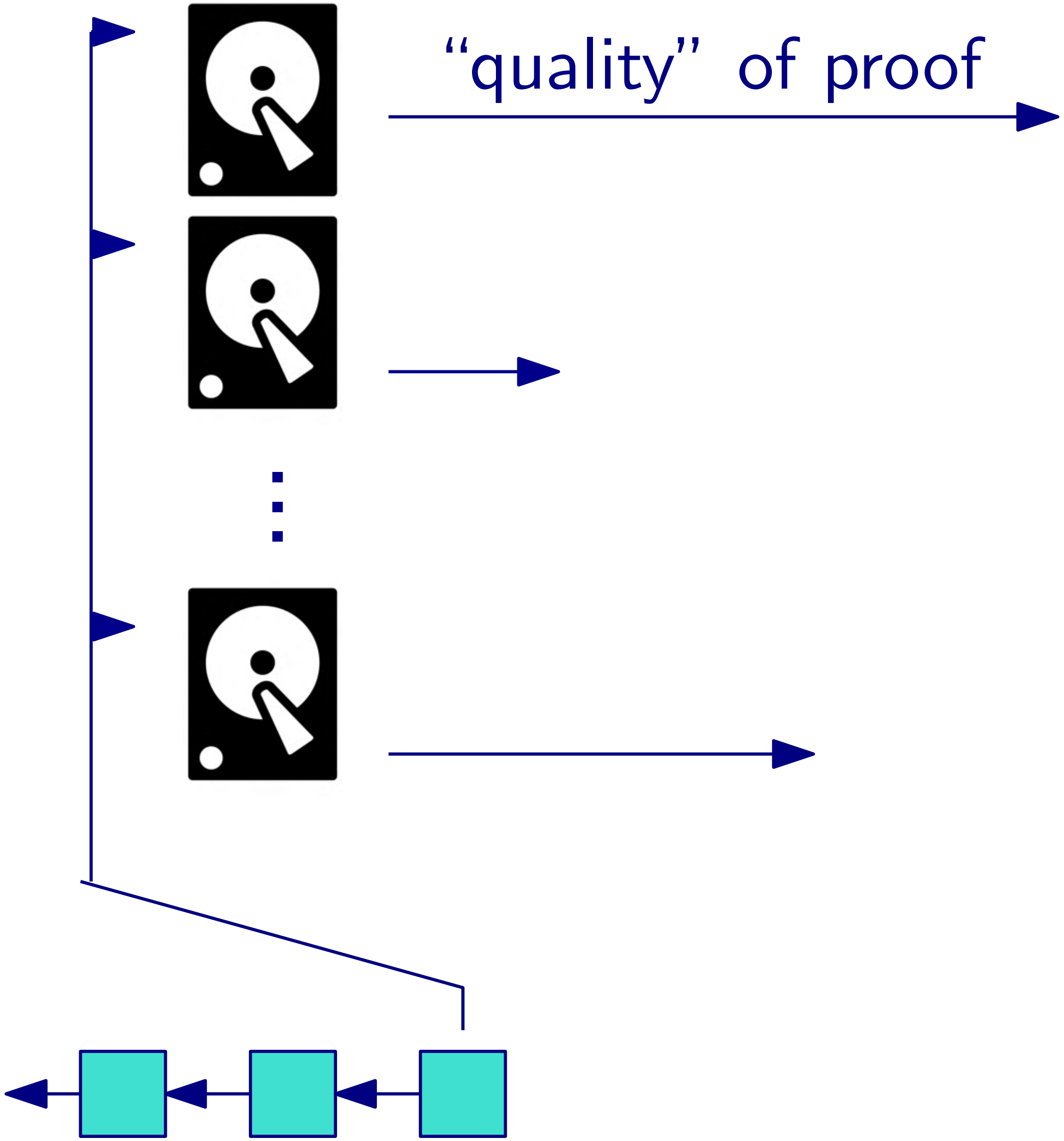


Proofs of Space and Time (early Chia proposal)

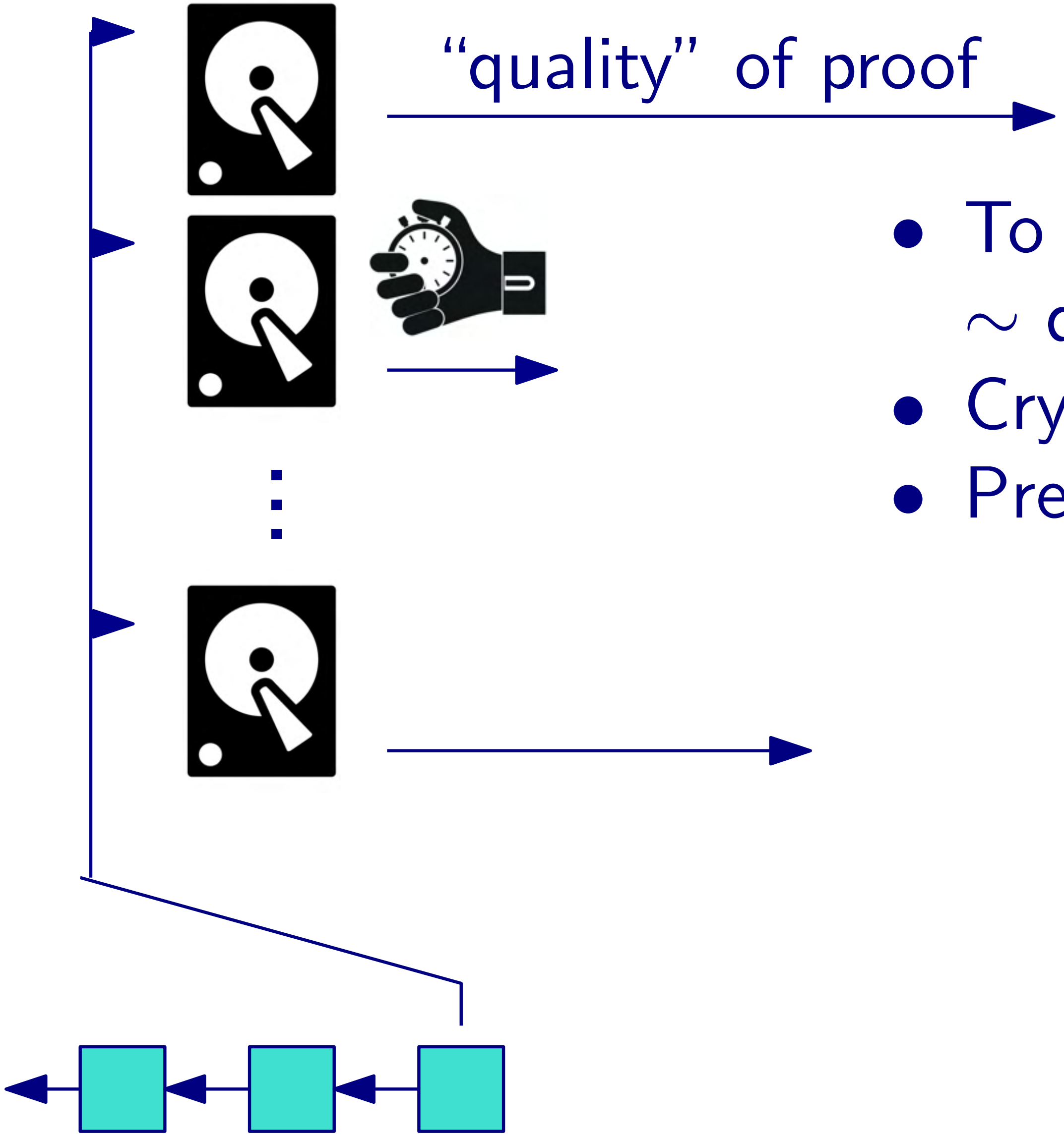
Proofs of Space and Time (early Chia proposal)



Proofs of Space and Time (early Chia proposal)

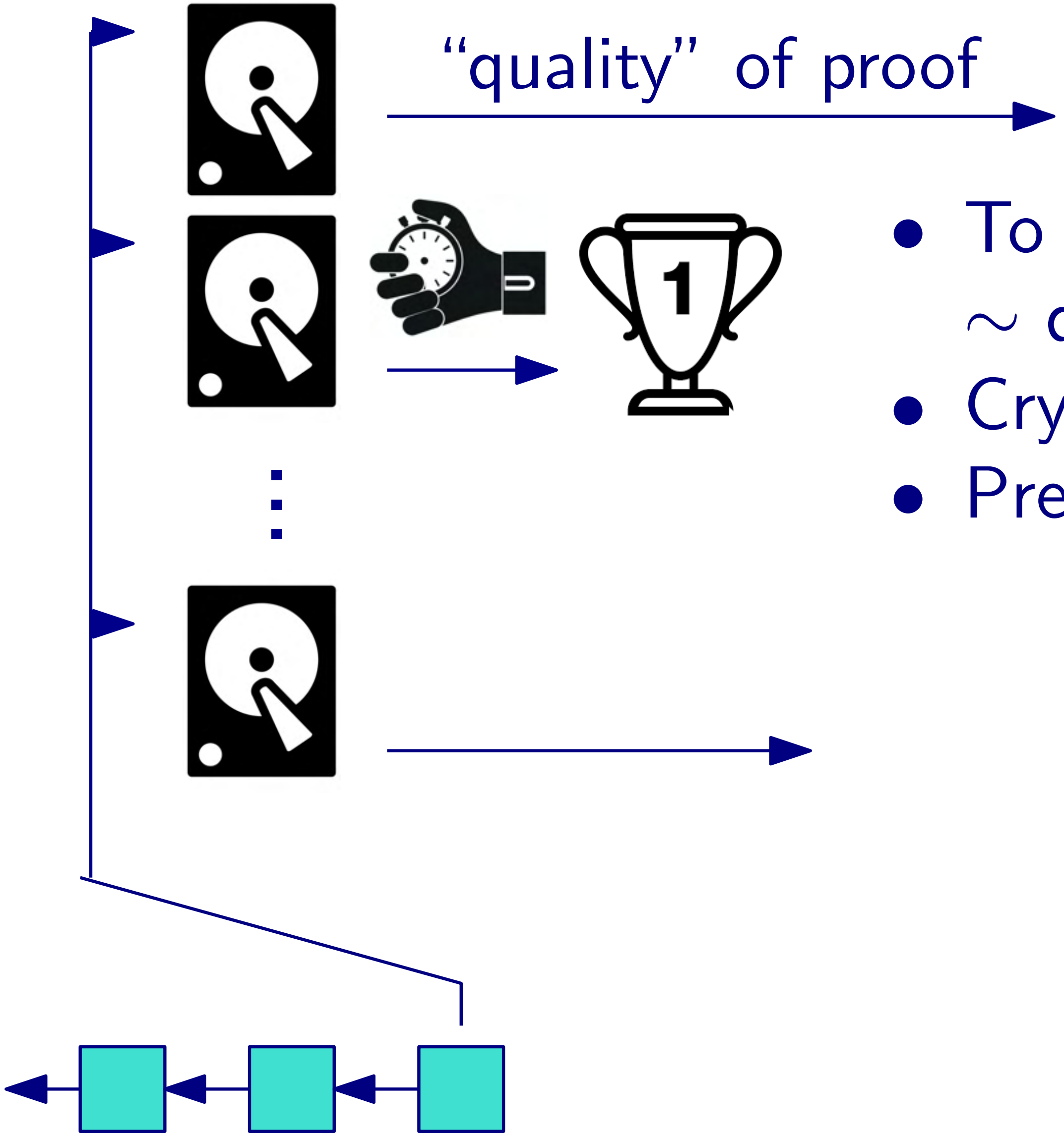


Proofs of Space and Time (early Chia proposal)



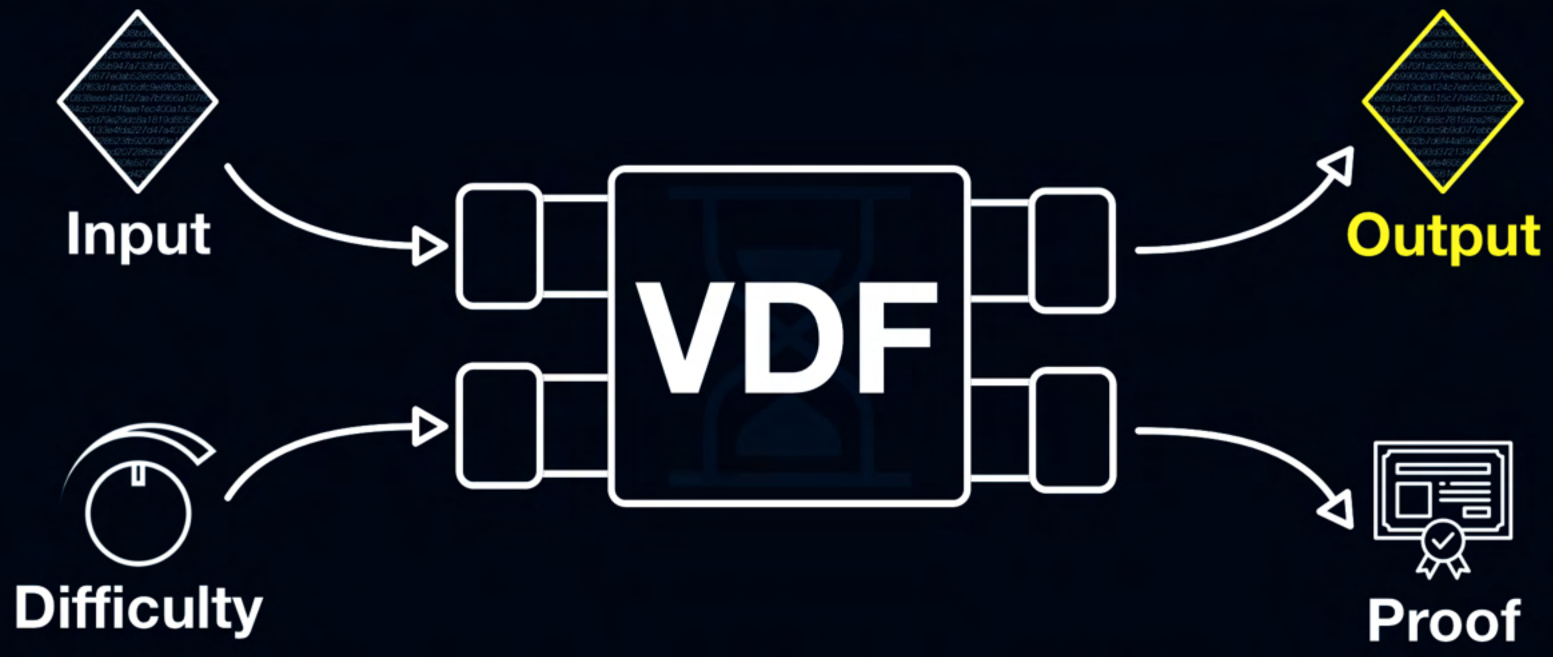
- To complete block wait for $\sim$ quality time
- Cryptographically enforced
- Prevents bootstrapping

Proofs of Space and Time (early Chia proposal)



- To complete block wait for $\sim$ quality time
- Cryptographically enforced
- Prevents bootstrapping

Verifiable Delay Function



A VDF is a function that requires a large amount of time to compute

The difficulty input controls how long the VDF takes to solve

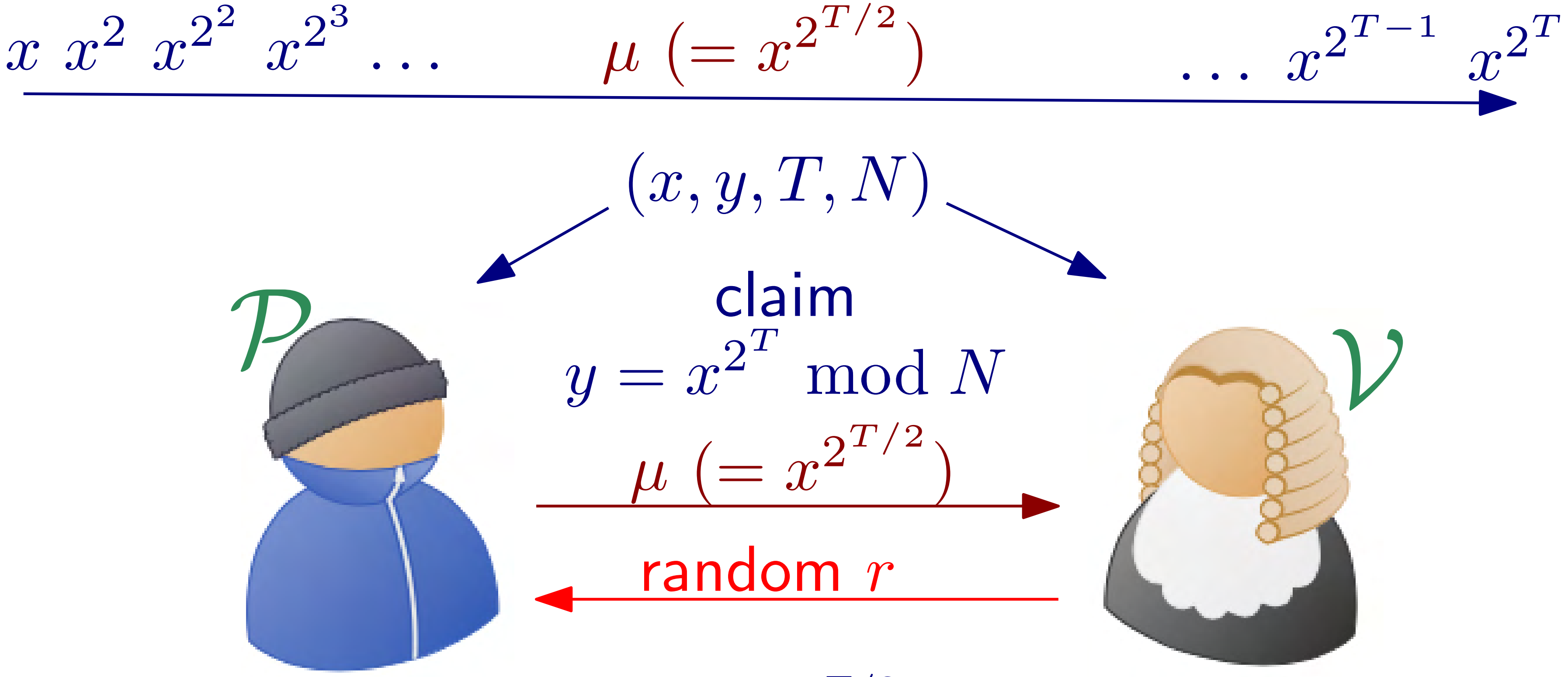
Verification(◇ , ◇ , 🗎)

A proof is used to quickly verify the output came from a given input

Simple Verifibale Delay Function [ITCS'19]

VDF$(x, T) = x^{2^T}$ in a group of unknown order

Proving $\sigma = x^{2^T}$ in RSA group $\mathbb{Z}_N^*, N = p \cdot q$



$x \ x^2 \ x^{2^2} \ x^{2^3} \ldots$ $\mu \ (= x^{2^{T/2}})$ $\ldots \ x^{2^{T-1}} \ x^{2^T}$

(x, y, T, N)

$\mathcal{P}$

$\mathcal{V}$

claim

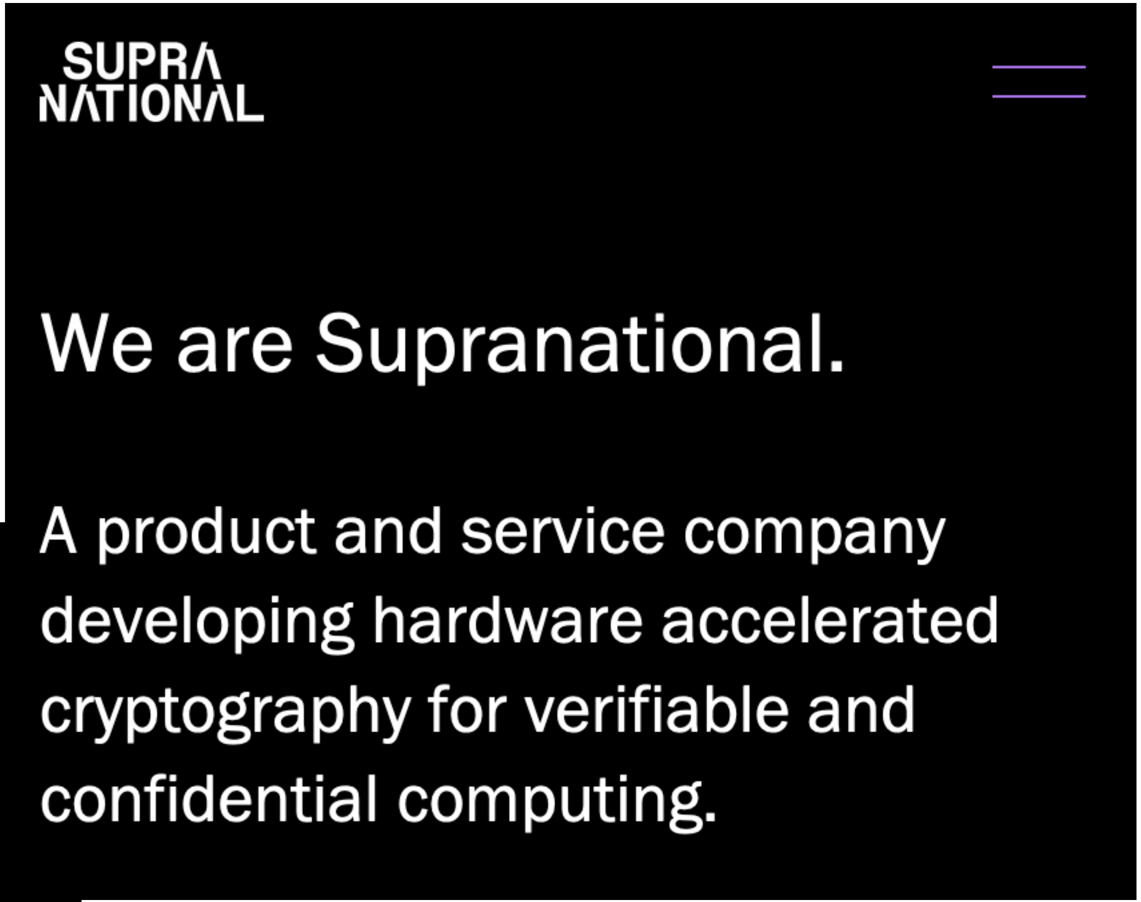
$y = x^{2^T} \mod N$

$\mu \ (= x^{2^{T/2}})$

random r

new claim $y' = x'^{2^{T/2}} \mod N$ where

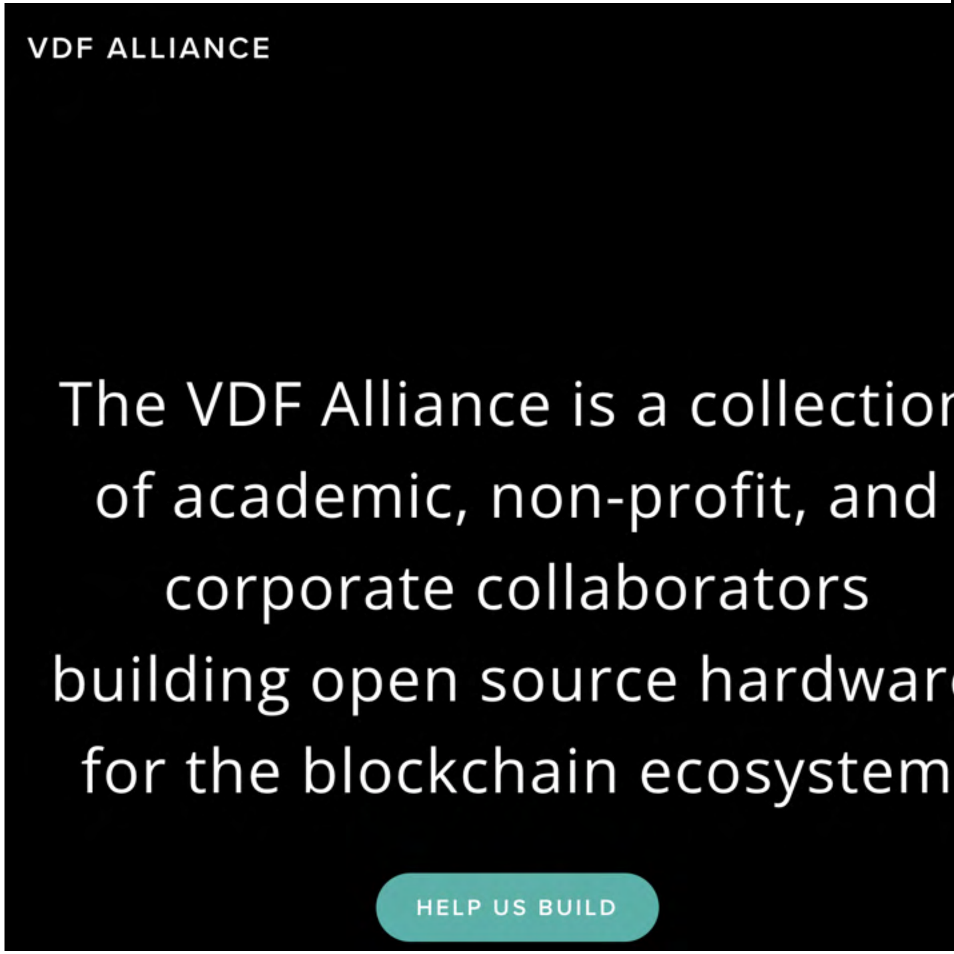
$x' := \mu^r \cdot y \qquad y' := (x^r \cdot \mu)^{2^{T/2}}$



SUPRA NATIONAL

We are Supranational.

A product and service company developing hardware accelerated cryptography for verifiable and confidential computing.



VDF ALLIANCE

The VDF Alliance is a collection of academic, non-profit, and corporate collaborators building open source hardware for the blockchain ecosystem