

Bitcoin and Energy

Understanding Proof of Work for a Sustainable Future

How Bitcoin can be part of the solution and not part of the problem

Pietro Speroni di Fenizio

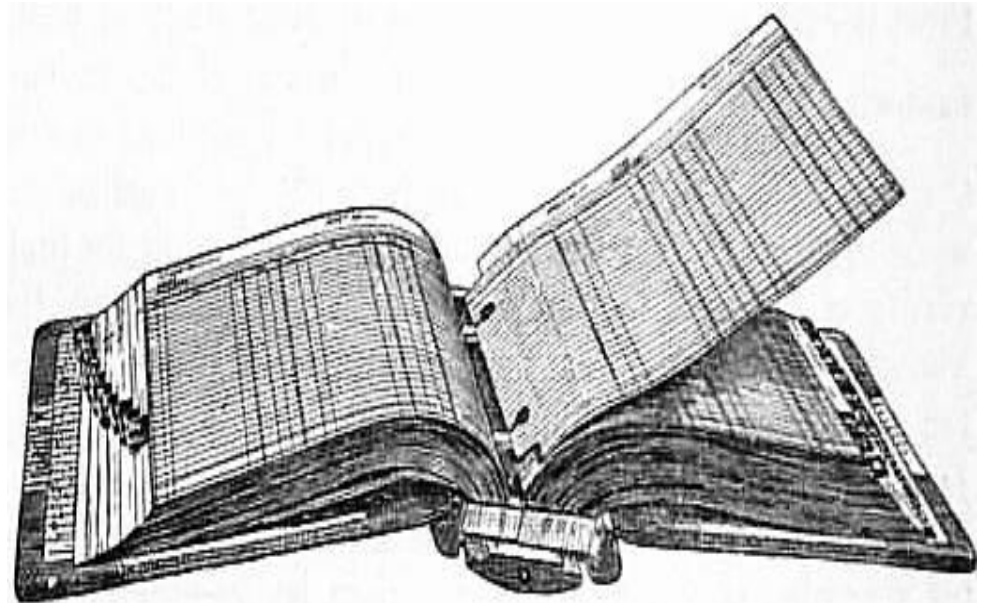
Plan of the Talk (details matter)

- Why Bitcoin is important
- How does proof of work function and why does Bitcoin use so much energy
- The positive elements of Bitcoin energy use
- How energy is transported
- How the energy market works
- Suggestions for policy makers

What is Bitcoin

In its core:

a distributed censorship-resistant public ledger, with a fixed supply, that enables peer to peer transactions



Why Bitcoin is important

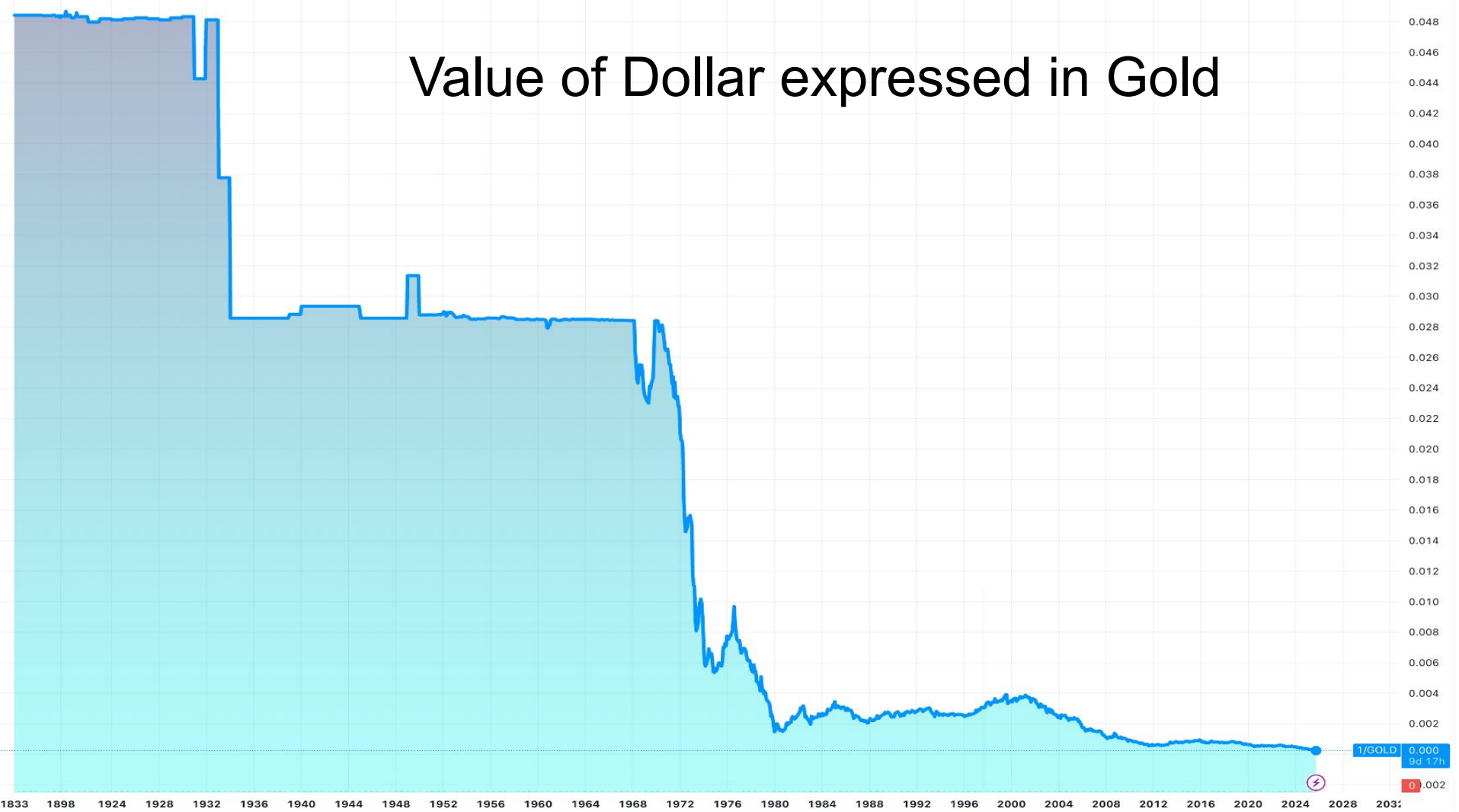
- It's money that cannot be printed away
- Let people push into the future the value of their work

“The republic encourages and safeguards savings in all its forms”

Art 47. Italian Constitution

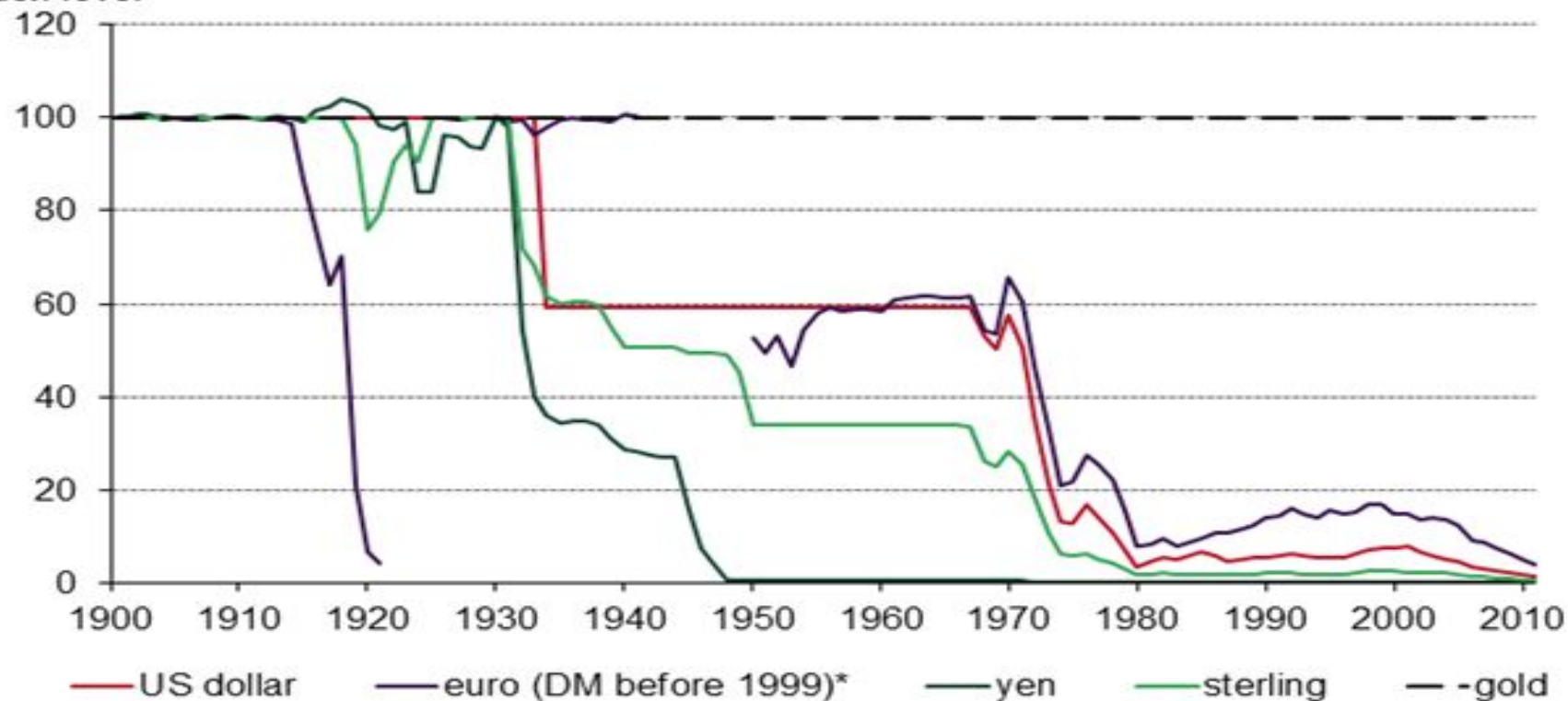
↖ Not necessarily productive

Value of Dollar expressed in Gold



Currencies in terms of gold (indexed: 1900=100)

Index level



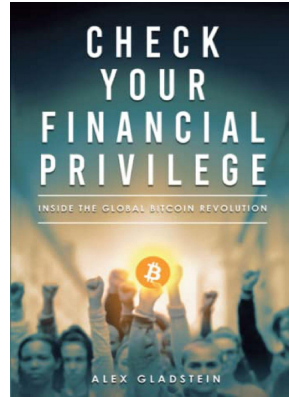
Source: IHS Global Insight, Thomson Reuters Datastream, World Gold Council

* The gaps in the deutschmark/euro line reflect hyperinflation in 1922 followed by the breakdown after WW2

Why Bitcoin is important

- It is easy to transport, making it useful for migrants
 - Also included
 - war migrants,
 - climate migrants,
- Cannot be confiscated, cannot be controlled by the state
 - Examples:
 - truck drivers in Canada during Covid,
 - feminists in Nigeria
 - palestinians in Gaza

Book: Check Your Financial Privilege



Why Bitcoin is important

it let you move value across space and time

How much energy does it cost to mine 1 bitcoin?

How much energy does it require to mine 1 bitcoin?

The question is ill-posed

How much energy does it cost to mine 1 bitcoin?

- Mining bitcoin is a side effect to another process:
 - Writing a page in a public ledger
 - Making sure each transaction is legal (no double-spending, for example)
 - Connecting the page to the previous page
 - Making sure no other copy of the public ledger is longer
 - Solving a *useless very difficult* mathematical problem

How much energy does it cost to mine 1 bitcoin?

- Mining bitcoin is a side effect to another process:

cost

- 0.0 % Writing a page in a public ledger
- 0.0 % Making sure each transaction is legal (no double-spending, for example)
- 0.0 % Connecting the page to the previous page
- 0.0 % Making sure no other copy of the public ledger is longer
- 99.9(9) % Solving a *useless very difficult* mathematical problem

Solving a *useless very difficult* mathematical problem ??

But why?

- To distribute new bitcoin in a random way
(not to the usual: rich people, the banks, the State...)
- To make sure no one can change with the ledger once it has been written
- To secure everything we did before

If it was easy

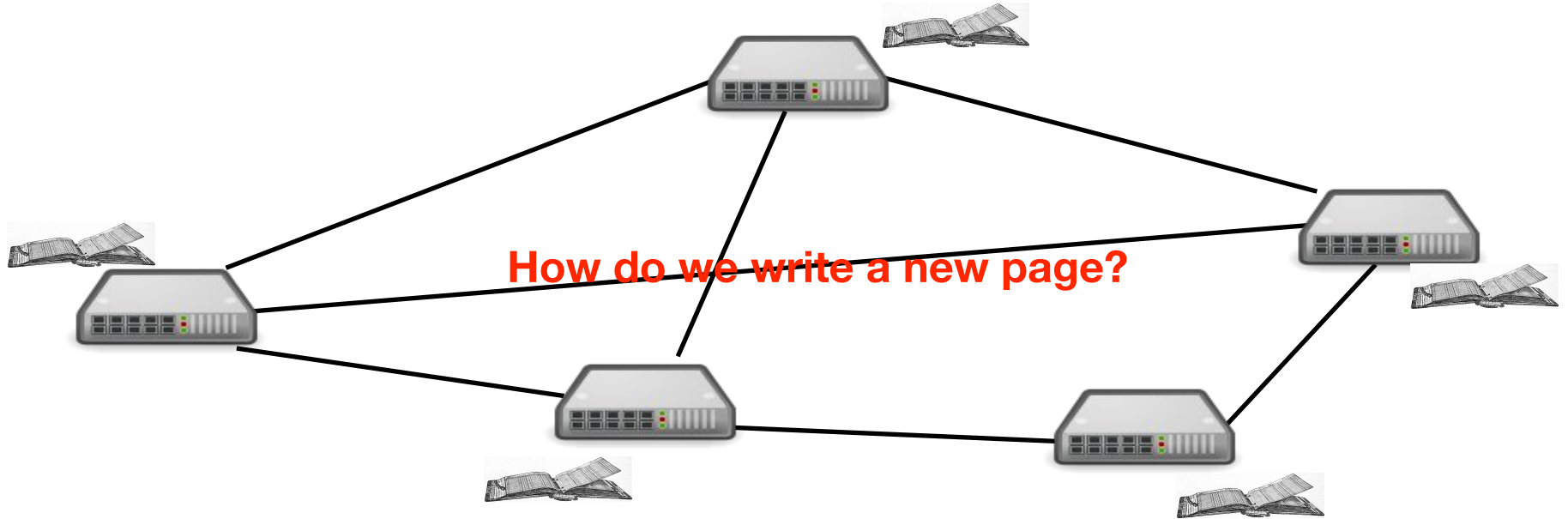
- Someone could generate a longer version of the ledger and take over
- To avoid this we would need a centralised version of the ledger
- We would be back at square one (*a monetary supply controlled by someone*)

Ergo

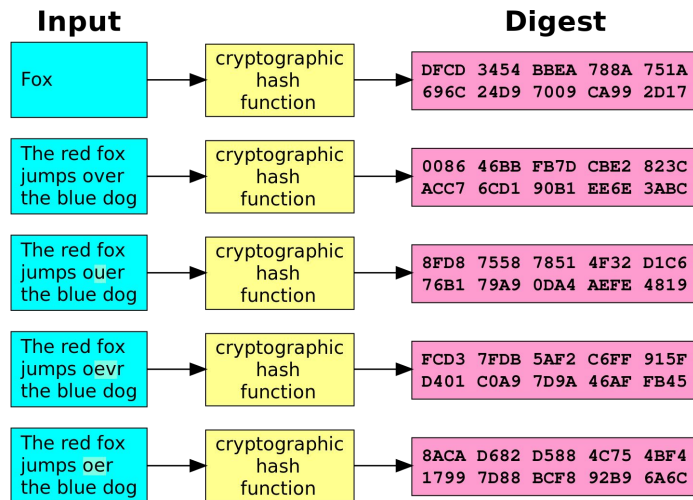
- We need to expensive process to have free money
- But the production of bitcoin is not the key element
- Making sure the network is secure *and* decentralised, is
- Bitcoin production is just a side effect

The right question:

- we have a network of computers with each having a copy of the public ledger



Hash Function for the Proof of Work

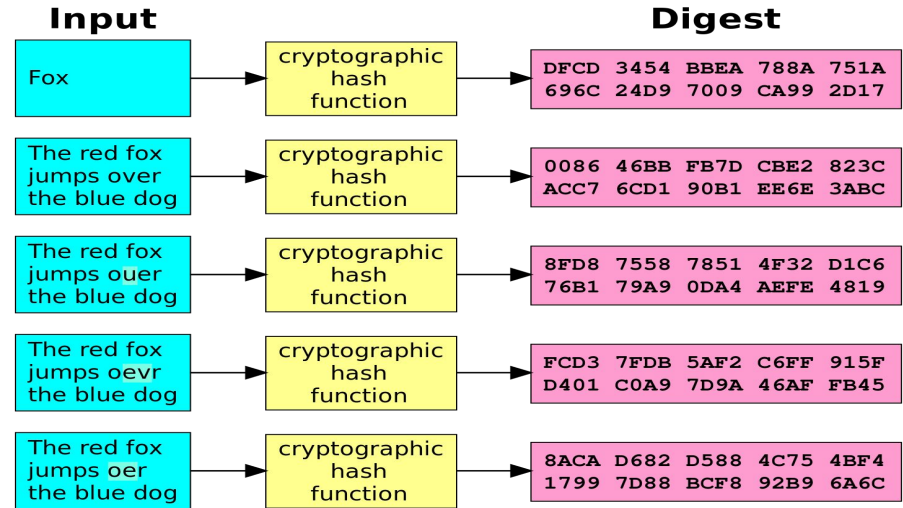


1. How Blockchain Works

- It is possible to have a problem with variable difficulty, which is easy to check if the solution is correct
 - Example:
 - Find an input in which the hash has 3 zero as the first 3 characters
 - Find an input in which the hash has 4 zero as the first 4 characters
 - Find an input in which the hash has 5 zero as the first 5 characters

Hash Function

1. How Blockchain Works



It is a deterministic function. The same input leads to the same output

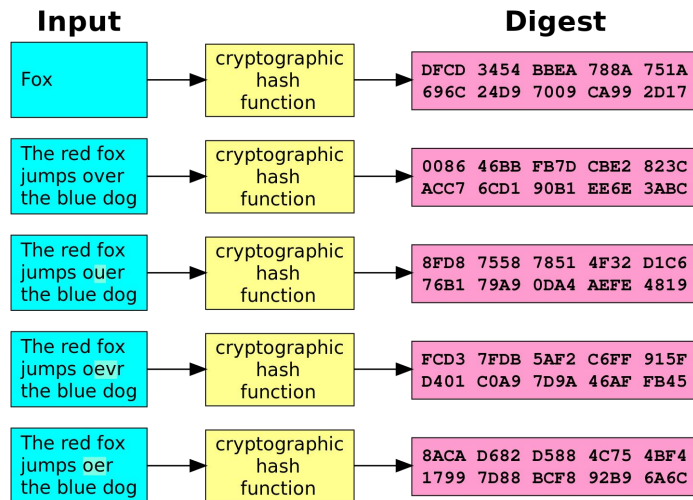
It is fast to calculate from the input the output

It is not possible to calculate the input from the output without checking all the possible input

A small difference in the input leads to a huge difference in the output. So huge to look uncorrelated.

It is not realistic to hope to find 2 input that have the same output.

Hash Function for the Proof of Work



1. How Blockchain Works

- It is possible to have a problem with variable difficulty, which is easy to check if the solution is correct
 - Example:
 - Find an input in which the hash has 3 zero as the first 3 characters
 - Find an input in which the hash has 4 zero as the first 4 characters
 - Find an input in which the hash has 5 zero as the first 5 characters

3. BLOCK

Block:

Nonce:

Data:

Una hash function prende una stringa e la trasforma in un numero esadecimale

Hash:

3. BLOCK

Block:

#1

Nonce:

12213

Data:

Una hash function prende una stringa e la trasforma in un numero esadecimale

Hash:

00003520e1ccfe2ebddf344d911165b9ddbaecd8d330225f3e0edd03d096aba8

Mine

2. HASH

Data:

112213Una hash function prende una stringa e la trasforma in un numero esadecimale

Hash:

00003520e1ccfe2ebddf344d911165b9ddbaecd8d330225f3e0edd03d096aba8

A blockchain is a series of blocks linked

[illegible]

Block:

#2

Nonce:

125389

Data:

in una blockchain prendiamo
l'hash del blocco precedente e
lo aggiungiamo alla stringa

Prev:

0000a895f194945b00d45d8d6f

Hash:

000053ea01622640a97bce3c2f

Mine

Block:

#3

Nonce:

12953

Data:

non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev:

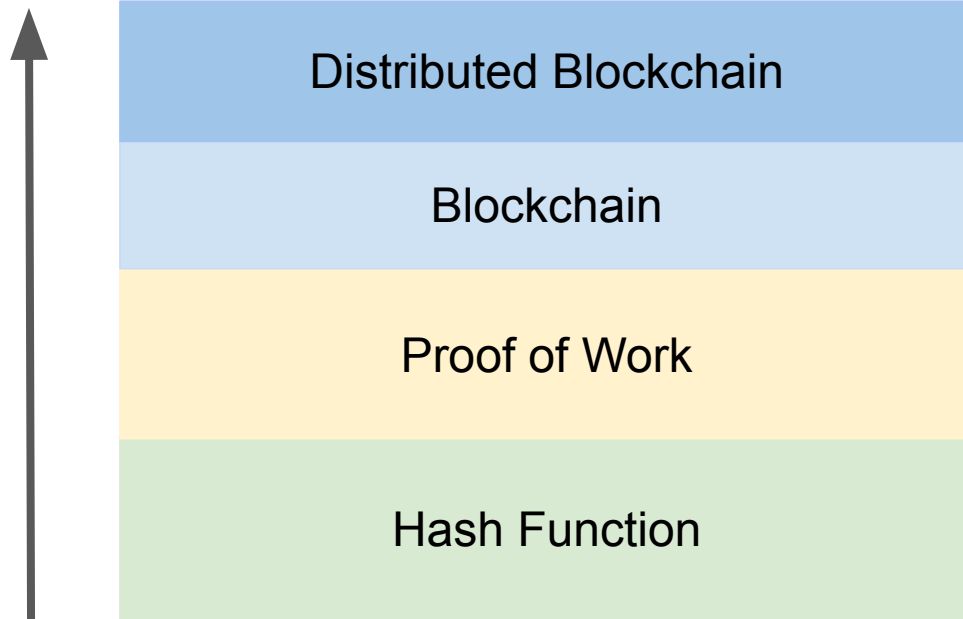
000053ea01622640a97bce3c2f

Hash:

0000124224a6277bb51ab1fb6f

Mine

Bitcoin Building Blocks



A blockchain is a series of blocks linked

[illegible]

Block:

#2

Nonce:

125389

Data:

in una blockchain prendiamo
l'hash del blocco precedente e
lo aggiungiamo alla stringa

Prev:

0000a895f194945b00d45d8d6f

Hash:

000053ea01622640a97bce3c2f

Mine

Block:

#3

Nonce:

12953

Data:

non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev:

000053ea01622640a97bce3c2f

Hash:

0000124224a6277bb51ab1fb6f

Mine

PEER A

Block: # 2

Nonce: 125389

Data: In una blockchain prendiamo l'hash del blocco precedente e lo aggiungiamo alla stringa

Prev: 3a6473ce3f60a104c2f7d8041

Hash: 000053ea01622640a97bce3c

Mine

Block: # 3

Nonce: 12937

Data: non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev: 000053ea01622640a97bce3c

Hash: 615722a3a6d81e174d670f7fe

Mine

Block: # 4

Nonce: 35990

Data:

Prev: 615722a3a6d81e174d670f7fe

Hash: 447ec02b241ea9860a38caa2

Mine

PEER B

Block: # 1

Nonce: 2325

Data: Una hash function prende una stringa e la trasforma in un numero esadecimale

Prev: 00000000000000000000000000000000c

Hash: 0000a895f194945b00d45d8d

Mine

Block: # 2

Nonce: 125389

Data: In una blockchain prendiamo l'hash del blocco precedente e lo aggiungiamo alla stringa

Prev: 0000a895f194945b00d45d8d

Hash: 000053ea01622640a97bce3c

Mine

Block: # 3

Nonce: 12953

Data: non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev: 000053ea01622640a97bce3c

Hash: 0000124224a6277bb51ab1fb

Mine

PEER C

Block: # 1

Nonce: 2325

Data: Una hash function prende una stringa e la trasforma in un numero esadecimale

Prev: 00000000000000000000000000000000c

Hash: 0000a895f194945b00d45d8d

Mine

Block: # 2

Nonce: 125389

Data: In una blockchain prendiamo l'hash del blocco precedente e lo aggiungiamo alla stringa

Prev: 0000a895f194945b00d45d8d

Hash: 000053ea01622640a97bce3c

Mine

Block: # 3

Nonce: 12953

Data: non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev: 000053ea01622640a97bce3c

Hash: 0000124224a6277bb51ab1fb

Mine

Block: # 3

Nonce: 12953

Data: non si può modificare un blocco di una blockchain senza ricalcolare tutti i successivi

Prev: 000053ea01622640a97bce3c2f

Hash: 0000124224a6277bb51ab1fb6!

Mine

How much energy does it cost to mine 1 bitcoin?

The question is ill-posed

How much energy does it cost to write a new page of the public ledger?

How much energy does it cost to write a new page of the public ledger?

Cost = $\sum$ energy used by every miner

Cost = f (expectation of the price of bitcoin, local cost of energy)

- If the (expectation of the) price of bitcoin goes down, miners turn off their machine
- If the local cost of energy goes up, miners turn off their machine
- Divided by the number of miners around the world

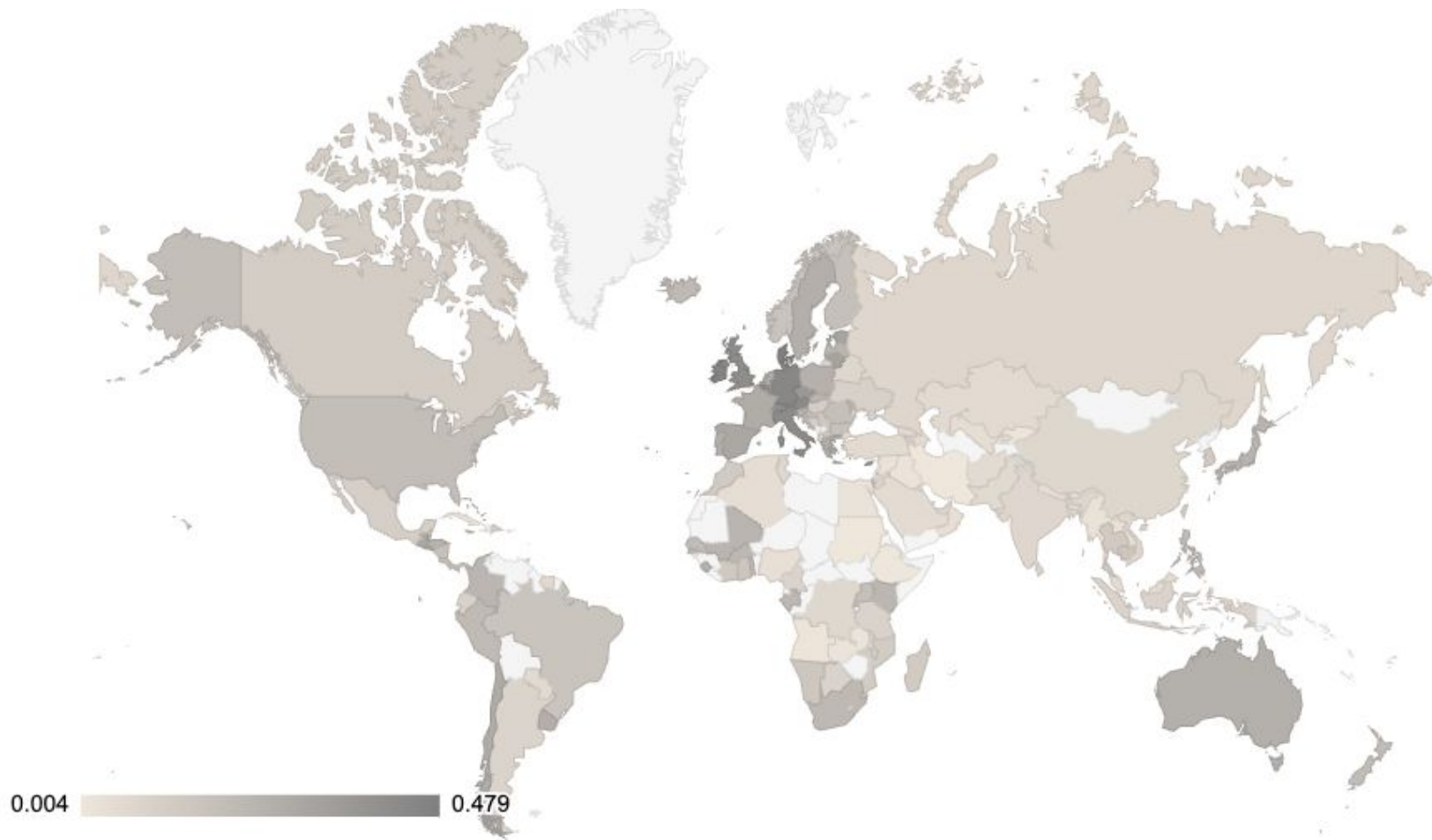
Mining is a massive, decentralized energy price discovery and arbitrage system, where the total energy cost depends on the entire global distribution of energy prices.

Miners automatically find and consume the cheapest available energy globally

The positive elements of Bitcoin energy use

- Can be done anywhere in the World
- Can be turned on or off nearly instantly
- Can be tweaked to use exactly the energy you want
- Pays you back
- Produces heat as a byproduct

Map of average Energy Price for Household



Transporting energy is hard

- Energy Loss as electricity travels through the cable
- Massive cost upfront (in money and energy)
- Fragility of the infrastructure
- Cheaper to move goods than energy
- Even cheaper to move bits



The Alternatives

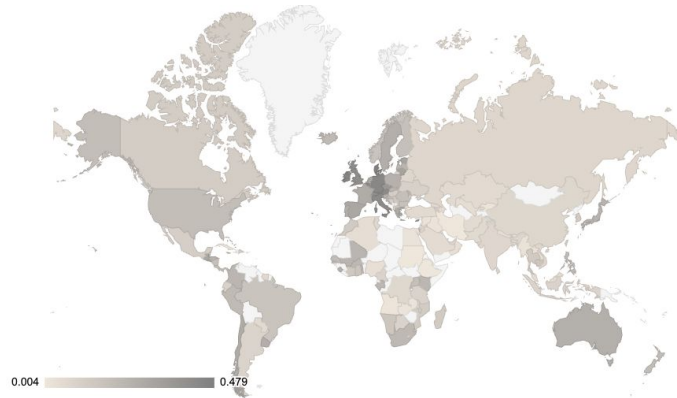
- Use electricity for energy costly industries (example Aluminium in Iceland)
- Lower the electrical bill
- Chemical batteries
 - Ammonia (ammoniac NH_3)
 - Hydrogen
 - Synthetic methane
 - Methanol
 - ...



ICELAND: ALUMINUM POWERED BY EXCESS RENEABLES

Thus

Using energy for Bitcoin mining
in a place where there is an excess of renewable energy
is **sustainable**



How Italy's electricity market clears

- Generators submit offers for each hour: quantity (MWh) + price (€/MWh)
- Retailers/traders submit demand bids
- GME orders supply from lowest to highest price and matches it with demand
- The last accepted offer in each zone sets that zone's clearing price
- All accepted generators in the zone are paid the clearing price

Example: buying 1000 MWh at 75 €/MWh

Rank	Unit / Tech	Price (€/MWh)	Qty (MWh)	Cum. (MWh)	Accepted?	
1	Nuclear NPP (hypothetical)	-10	400	400	Yes	}
2	Waste-to-Energy	-5	50	450	Yes	
3	Solar Utility B	0	150	600	Yes	
4	Hydro C	40	200	800	Yes	
5	CCGT D (gas)	75	300	1,100	Partial (200/300)	
6	CCGT E (gas)	90	250	1,350	No	
7	Peaker F (oil)	150	150	1,500	No	

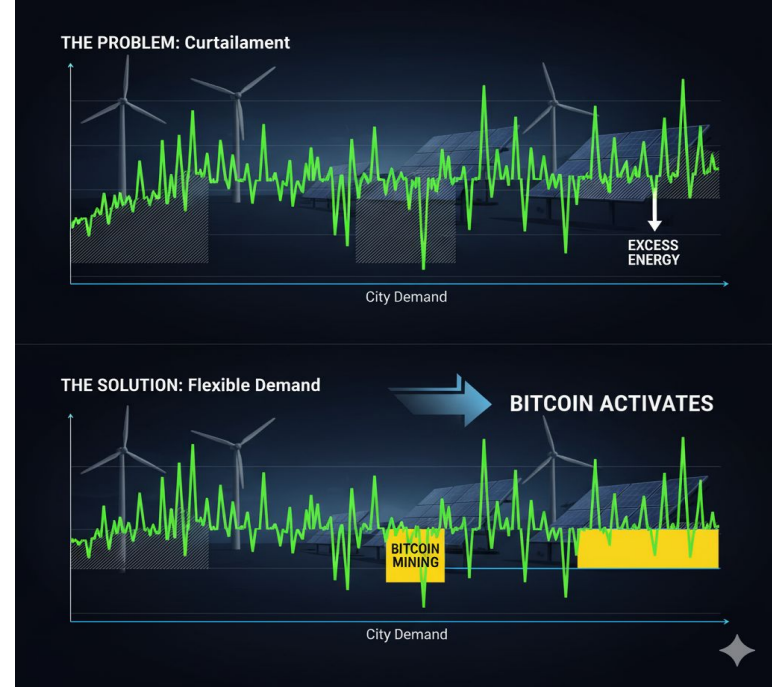
Negative cost: a bug, not a feature

- Occurs when inflexible or subsidized supply

Is bigger than the demand for that interval

- Generators bid negative to
 - avoid costly shutdown/start
 - capture production-linked incentives

- Consumers are effectively paid to take energy (price $< \text{€}0/\text{MWh}$), it hinders production
- System operators restore balance via curtailment, storage, or flexible demand
- A bitcoin mining rig that turns on only when the price is low and the production is only from renewable can be helpful



Suggestions for policy makers

- Policymakers **must** legislate Bitcoin mining
 - It is too dangerous to be left unchecked
- Bitcoin mining is not dangerous **where** there is an excess of energy
- Bitcoin mining is not dangerous **when** there is an excess of energy
- Bitcoin mining is not dangerous when we are only using **renewable sources**
- Bitcoin mining is **very dangerous otherwise**

Solutions:

- Bitcoin Mining Rig connected with a renewable facility that operates only when the mining rig is curtailed (slowed down) (**where**)
- A Bitcoin Mining Rig that only activates when the market price is below a certain level and the percentage of non-renewables is low enough (**when**)
- This would also encourage renewable technology as it would help pay for it

Suggestions for policy makers

**You are only allowed to mine if
you have a system that turns off the computers
if the cost is so high to be using non renewable energies**

The effect will be

- Stabilising the grid
- Enriching the nation
- Optimising the use of renewable energies

Suggestions for policy makers

The effect will be

- Stabilising the grid
- Enriching the nation
- Optimising the use of renewable energies

In short

- Bitcoin should be mined only with renewables
- When using renewables it is really good to
 - stabilise the grid
 - Help make renewable be profitable
- Legislations must align with this

