PoM @ Breaking Bitcoin

Kevin Loaec

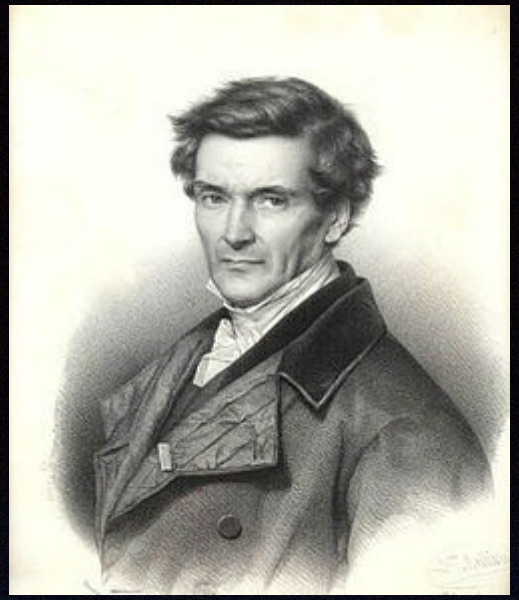
@kloaec
kevin@chainsmiths.com

breaking bitcoin

The Proof of Work Mechanism

A proof: no doubt possible

Work: defined in physics, S.I. unit is the Joule.



← Gaspard-Gustave Coriolis

The Proof of Work Mechanism

Electrical work (semiconductor junctions)

Has a cost in term of energy (also in Joule)

Practically: Reverse a Hash function

breaking bitcoin

The Proof of Work Mechanism

Why:

Economic countermeasure against spam and Sybil.

Problems:

- Economy of scale -> centralization (power, geography, supply chain...)
- Bad for the planet (and getting worse)

breaking bitcoin

What about PoS?

What law? -> hey the chain is immutable!

breaking bitcoin

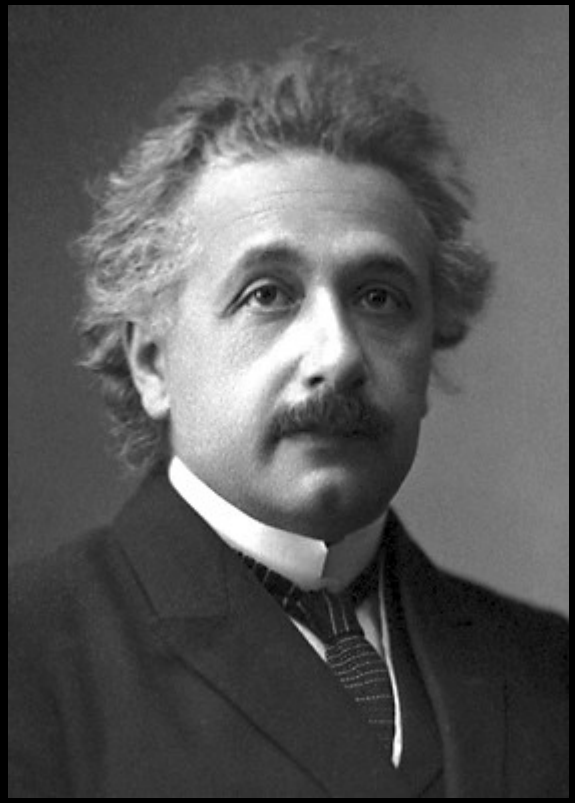
What about PoS?

- could work (maybe!) if based on Bitcoin
- feedback loop if removing the PoW. Still “immutable”?

...

breaking bitcoin

Proof of Moon



breaking bitcoin

Proof of Moon

- time only goes one way
- “c”, a limit at which information moves

breaking bitcoin

Proof of Moon

Back to our pre-requisite:

- a proof (verifiable and certain)
- hard to find/achieve, easy to verify

(- resist centralization)

Bonus:

- not as bad for our planet (less waste)
- Space-Pirate-resistant

breaking bitcoin

Looking at the sky

- things of the past
- that are still observable
- are “impossible” to fake
- are “impossible” to destroy

breaking bitcoin

Looking at the sky

Moons: around 50 unconfirmed in our Solar System. Too hard (for now)!

Quasars, Pulsars... been there for long.

New events: supernovae?

breaking bitcoin

Looking at the sky

How?

- hash the block header to get a “sky window” to search
- difficulty = size of the window
- decide an “observability” minimum requirement (hardcoded?)

Looking at the sky

Cool stuff:

- geographic decentralization.
- “useful” and not energy hungry
- cool name

breaking bitcoin

Looking at the sky

Problems:

- can’t be directly verified by smartphones/PCs
- can we find enough new events/corpses in 10min?
- how long is the verification process?
- “processing” problem

Thanks! Questions/ideas?

It’s not only PoW or PoS. Let’s research alternatives.