Fine-grained Space Complexity

Marshall Ball[1] Peter Fenteany[1] Tung Anh Vu[2]

[1]Courant Institute of Mathematical Sciences, New York University
[2]Faculty of Mathematics and Physics, Charles University

This research is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 823748.

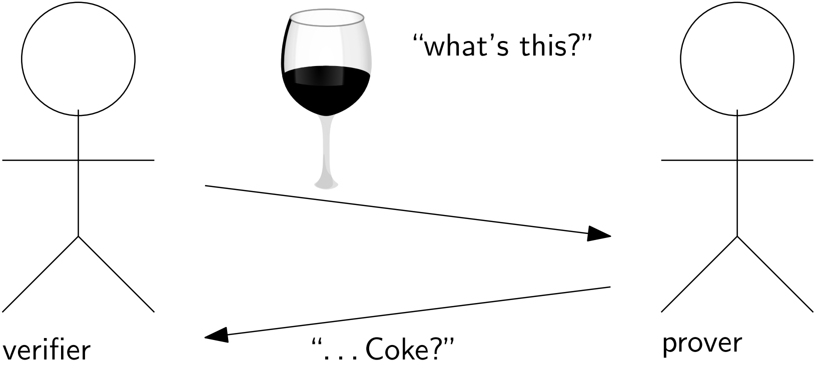
What is a proof?

What is a proof?

A proof is something that convinces me.

“I can distinguish Coke and Pepsi by taste.”

“I can distinguish Coke and Pepsi by taste.”



“what’s this?”

“. . . Coke?”

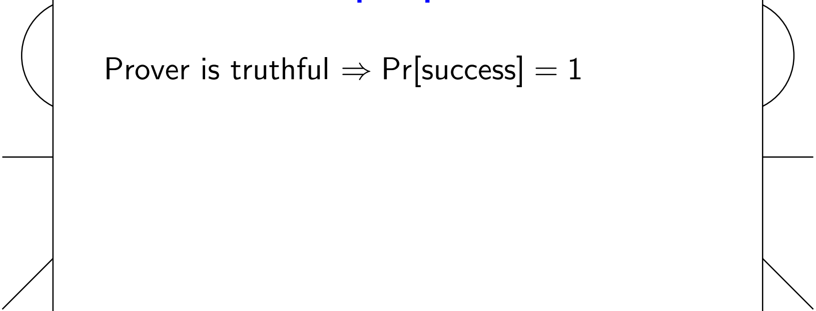
verifier

prover

“I can distinguish Coke

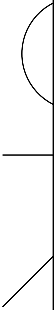
Protocol properties

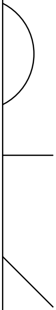
Prover is truthful $\Rightarrow \Pr[\text{success}] = 1$



veri

“I can distinguish Coke





Protocol properties

Prover is truthful $\Rightarrow \Pr[\text{success}] = 1$

Prover is lying $\Rightarrow \Pr[\text{success}] \leq 1/2$

veri

“I can distinguish Coke

Protocol properties

Prover is truthful ⇒ $\Pr[\text{success}] = 1$

Prover is lying ⇒ $\Pr[\text{success}] \leq 1/2$

Repeat protocol 300 times ⇒ dishonest prover succeeds with probability $\leq (1/2)^{300}$

verif

“I can distinguish Coke

Protocol properties

Prover is truthful $\Rightarrow$ Pr

$(1/2)^{300} \approx 10^{-90}$

Prover is lying $\Rightarrow$ Pr[su

Repeat protocol 300 times $\Rightarrow$ dishonest prover succeeds with probability $\leq (1/2)^{300}$

veri

“I can distinguish Coke

Protocol properties

Prover is truthful ⇒ Pr

Prover is lying ⇒ Pr[su

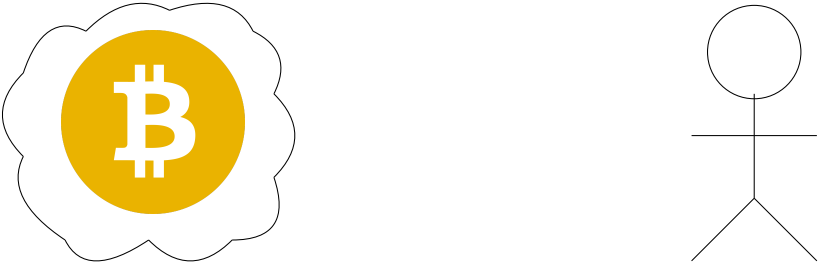
Repeat protocol 300 times ⇒ dishonest prover succeeds with probability $\leq (1/2)^{300}$

$(1/2)^{300} \approx 10^{-90}$

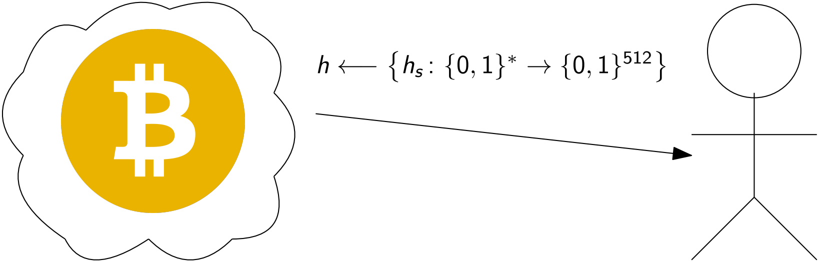
# particles in the universe $\approx 10^{80}$

veri

Proofs of Work, i.e. how does one mine Bitcoin?

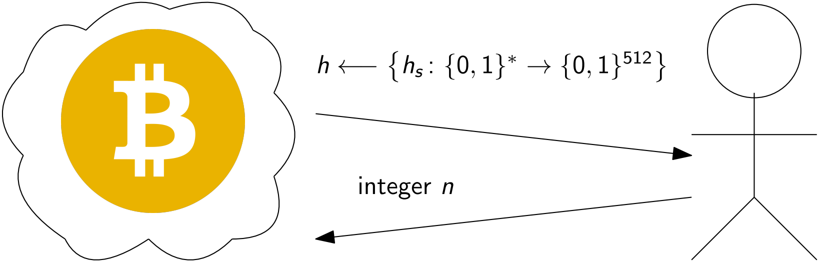


Proofs of Work, i.e. how does one mine Bitcoin?



$$h \longleftarrow \left\{ h_s \colon \{0,1\}^* \to \{0,1\}^{512} \right\}$$

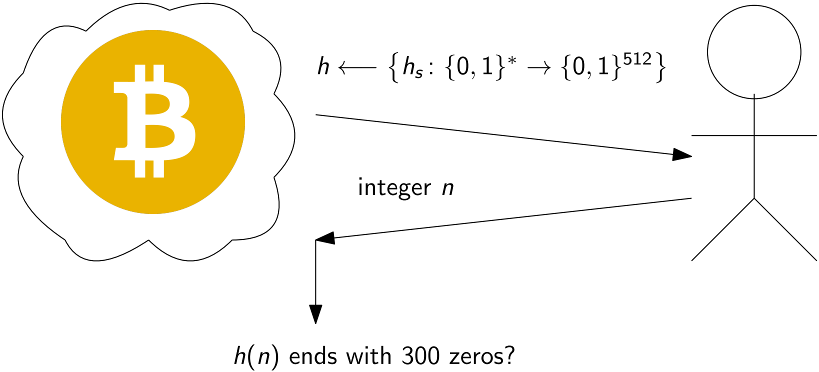
Proofs of Work, i.e. how does one mine Bitcoin?



$h \longleftarrow \left\{ h_s \colon \{0,1\}^* \to \{0,1\}^{512} \right\}$

integer n

Proofs of Work, i.e. how does one mine Bitcoin?

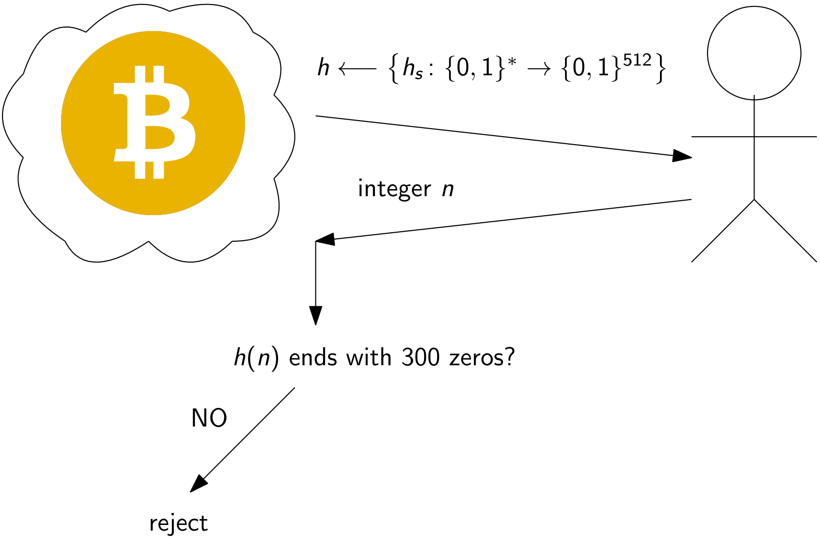


$h \longleftarrow \left\{ h_s \colon \{0,1\}^* \to \{0,1\}^{512} \right\}$

integer n

$h(n)$ ends with 300 zeros?

Proofs of Work, i.e. how does one mine Bitcoin?



$h \longleftarrow \left\{ h_s : \{0,1\}^* \to \{0,1\}^{512} \right\}$

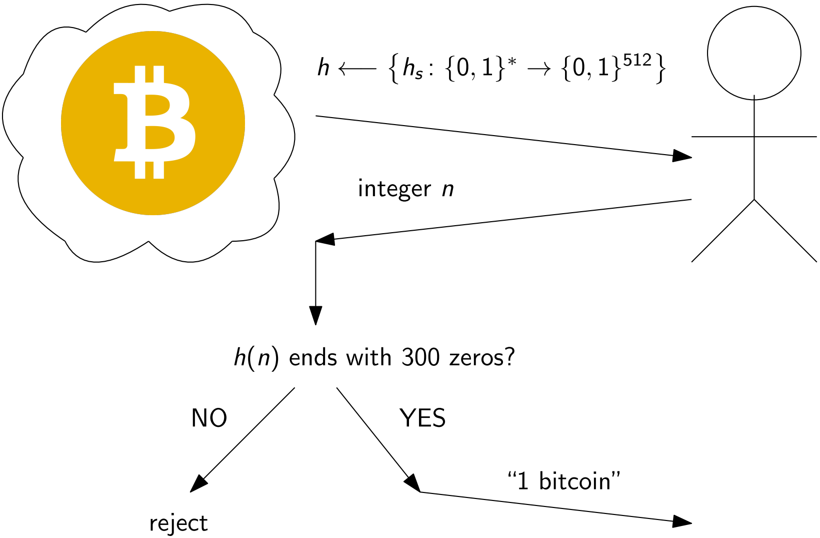
integer n

$h(n)$ ends with 300 zeros?

NO

reject

Proofs of Work, i.e. how does one mine Bitcoin?



$h \longleftarrow \left\{h_s\colon \{0,1\}^* \to \{0,1\}^{512}\right\}$

integer n

$h(n)$ ends with 300 zeros?

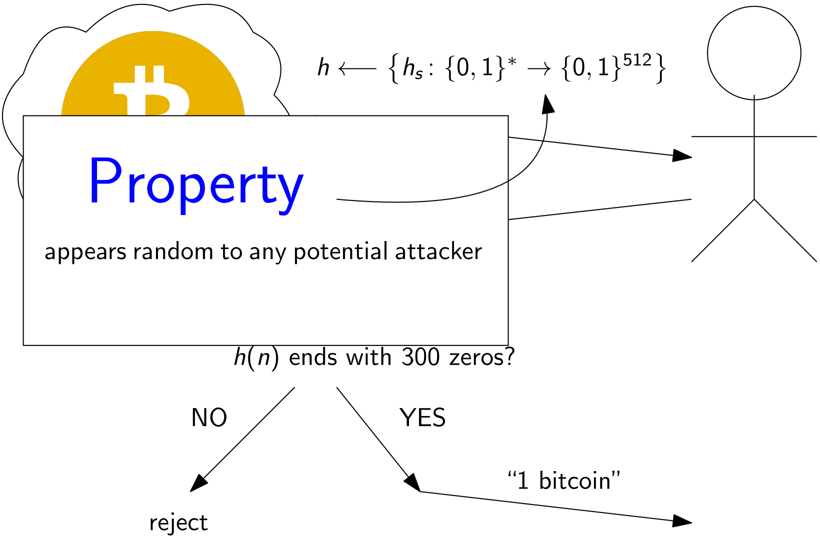
NO

YES

reject

“1 bitcoin”

Proofs of Work, i.e. how does one mine Bitcoin?



$h \longleftarrow \left\{ h_s \colon \{0,1\}^* \to \{0,1\}^{512} \right\}$

Property

appears random to any potential attacker

$h(n)$ ends with 300 zeros?

NO

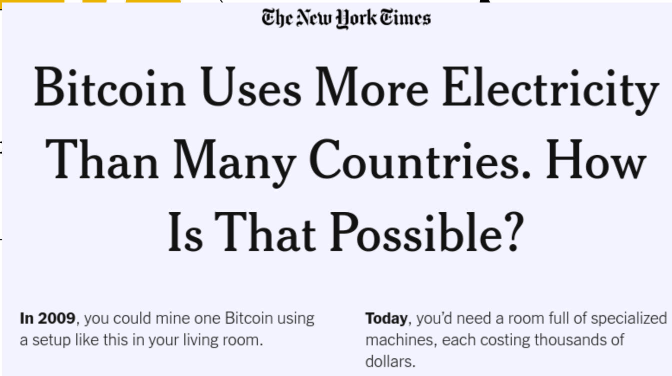
YES

reject

“1 bitcoin”

Proofs of Work, i.e. how does one mine Bitcoin?

$h \longleftarrow \{h_s \colon \{0,1\}^* \to \{0,1\}^{512}\}$



The New York Times

Bitcoin Uses More Electricity Than Many Countries. How Is That Possible?

In 2009, you could mine one Bitcoin using a setup like this in your living room.

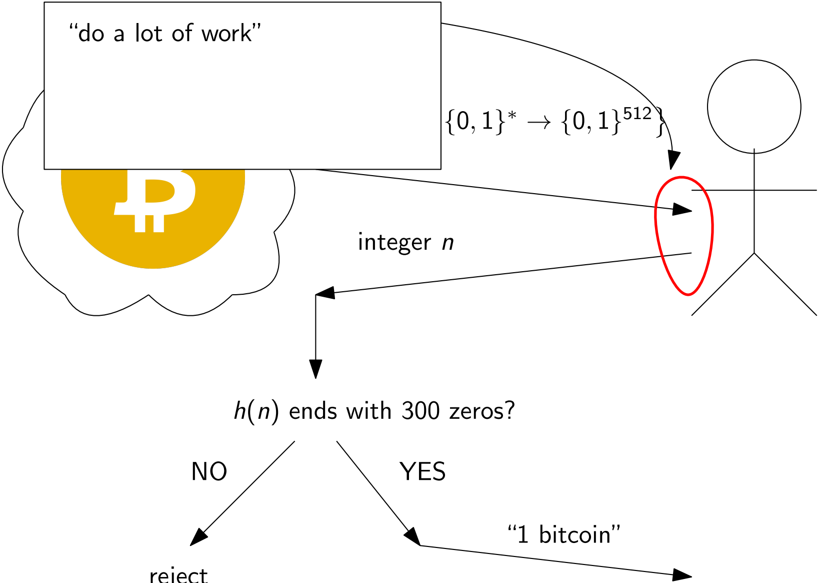
Today, you'd need a room full of specialized machines, each costing thousands of dollars.

ap

1 bitcoin

reject

Proofs of Sequential Work



“do a lot of work”

$\{0,1\}^* \to \{0,1\}^{512}$

integer n

$h(n)$ ends with 300 zeros?

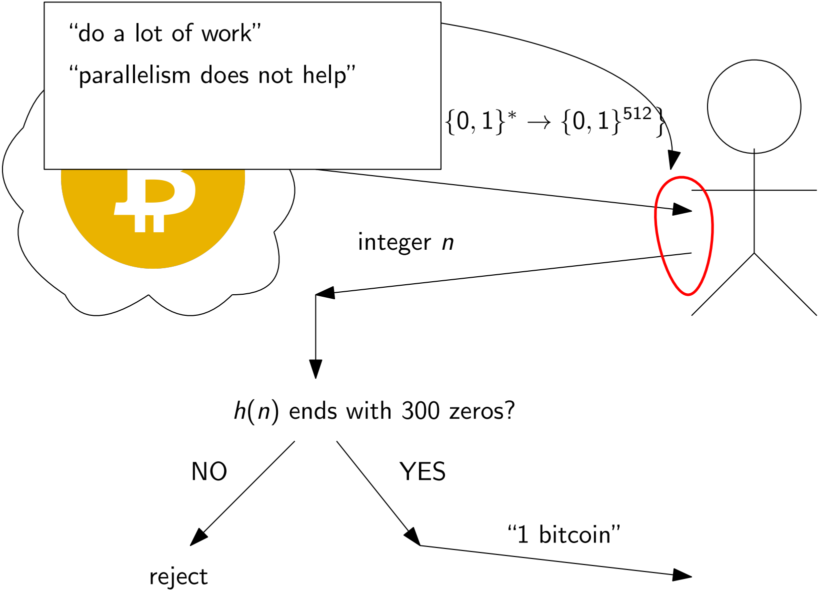
NO

YES

reject

“1 bitcoin”

Proofs of Sequential Work



“do a lot of work”

“parallelism does not help”

$\{0,1\}^* \rightarrow \{0,1\}^{512}$

integer n

$h(n)$ ends with 300 zeros?

NO

YES

reject

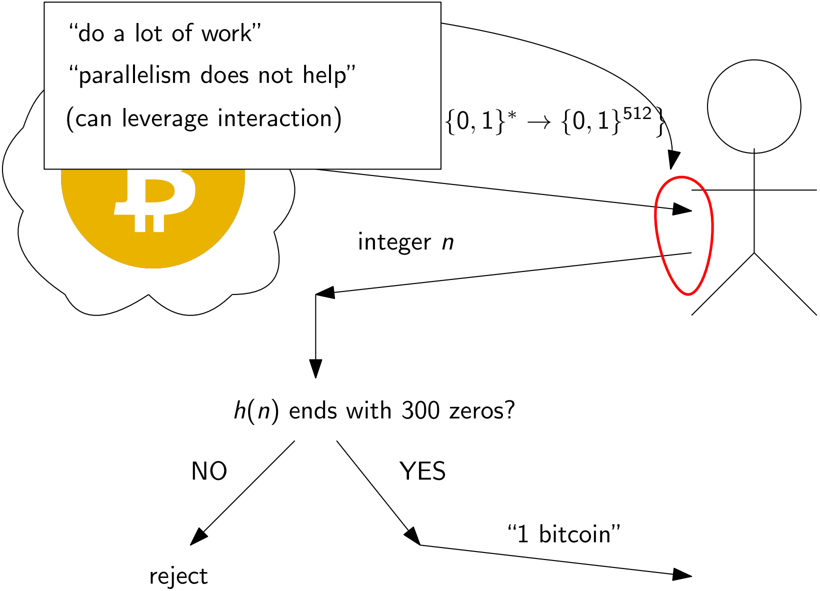
“1 bitcoin”

Proofs of Sequential Work

“do a lot of work”

“parallelism does not help”

(can leverage interaction)

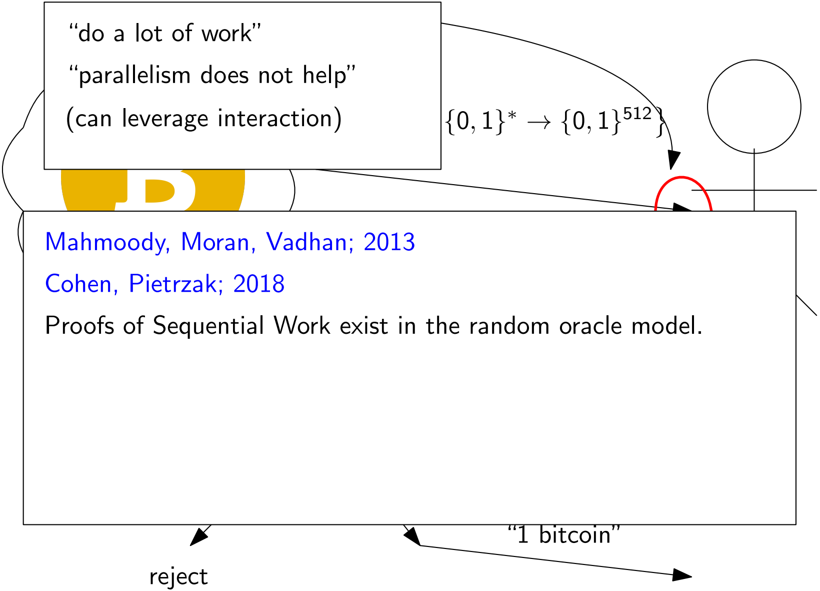

$\{0,1\}^* \rightarrow \{0,1\}^{512}$
integer n
$h(n)$ ends with 300 zeros?
NO
YES
reject
“1 bitcoin”

Proofs of Sequential Work

“do a lot of work”

“parallelism does not help”

(can leverage interaction)

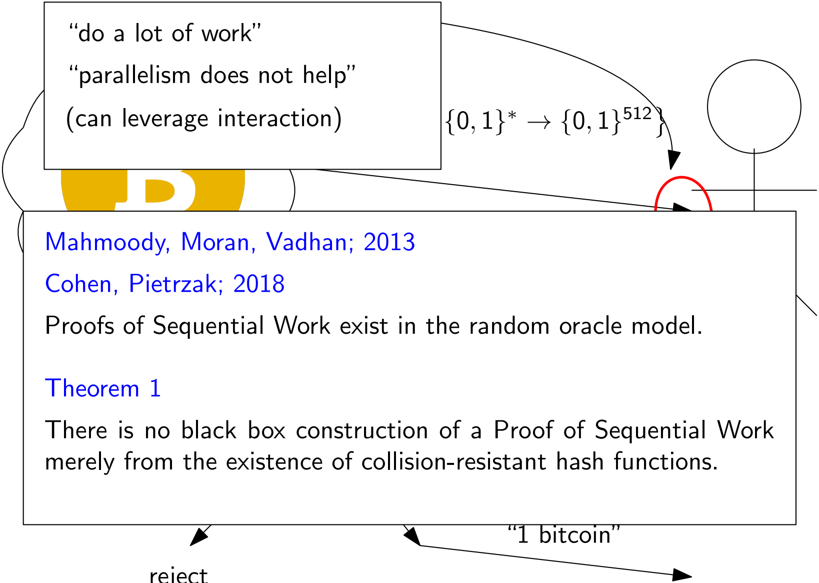


Mahmoody, Moran, Vadhan; 2013

Cohen, Pietrzak; 2018

Proofs of Sequential Work exist in the random oracle model.

Proofs of Sequential Work



"do a lot of work"

"parallelism does not help"

(can leverage interaction)

Mahmoody, Moran, Vadhan; 2013

Cohen, Pietrzak; 2018

Proofs of Sequential Work exist in the random oracle model.

Theorem 1

There is no black box construction of a Proof of Sequential Work merely from the existence of collision-resistant hash functions.

Thank you for your attention.

Questions, comments, . . . ?