Verifiable Delay Functions (VDFs) in Filecoin

Taosheng shi
IPFS原力区
价值　共建　共享　荣耀

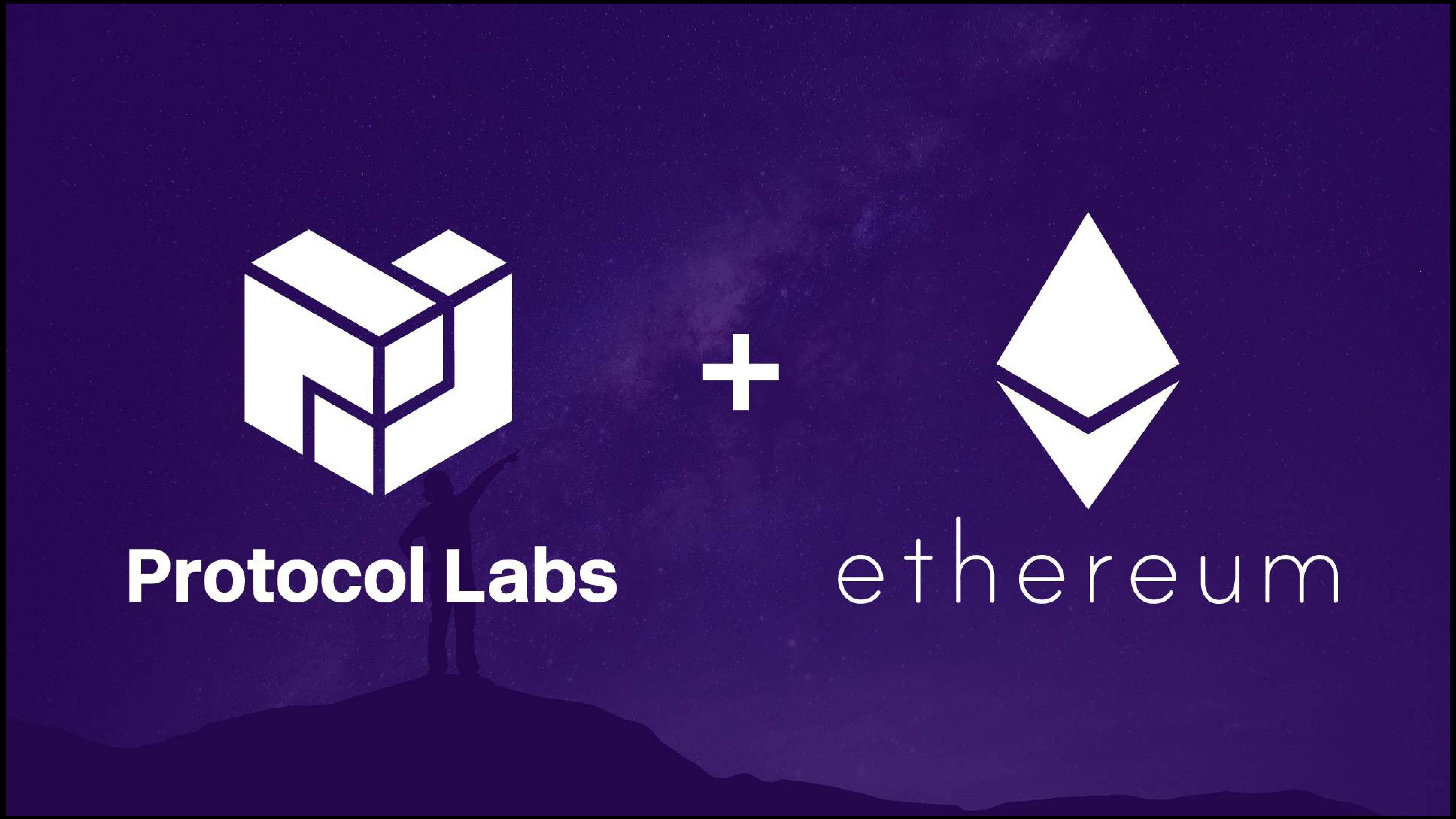
❑Five papers from June 2018:

1. “Verifiable Delay Functions”—Boneh, Bonneau, Bünz, Fisch
2. “Efficient Verifiable Delay Functions”—Wesolowski
3. “Simple Verifiable Delay Functions”—Pietrzak
4. “A Survey of Two Verifiable Delay Functions”—Boneh, Bünz, Fisch
5. “Verifiable Delay Functions from Supersingular Isogenies and Pairings”—De Feo, Masson, Petit, Sanso

Only 1 year old

chia
SOLANA
Filecoin
TEZOS
MARKET CAP
N
CØSMOS
POA
INJECTIVE
PROTOCOL
IoTeX
Harmony

Blockchain interest



VDF project management

SUPRA
NATIONAL

VDF project management

funded 50/50 by Protocol Labs and the Ethereum Foundation

LIGERO

VDF project management

funded 50/50 by Protocol Labs and the Ethereum Foundation

❑VDF Research Effort:

- https://vdfresearch.org/

❑Ethereum Research:

- https://ethresear.ch/

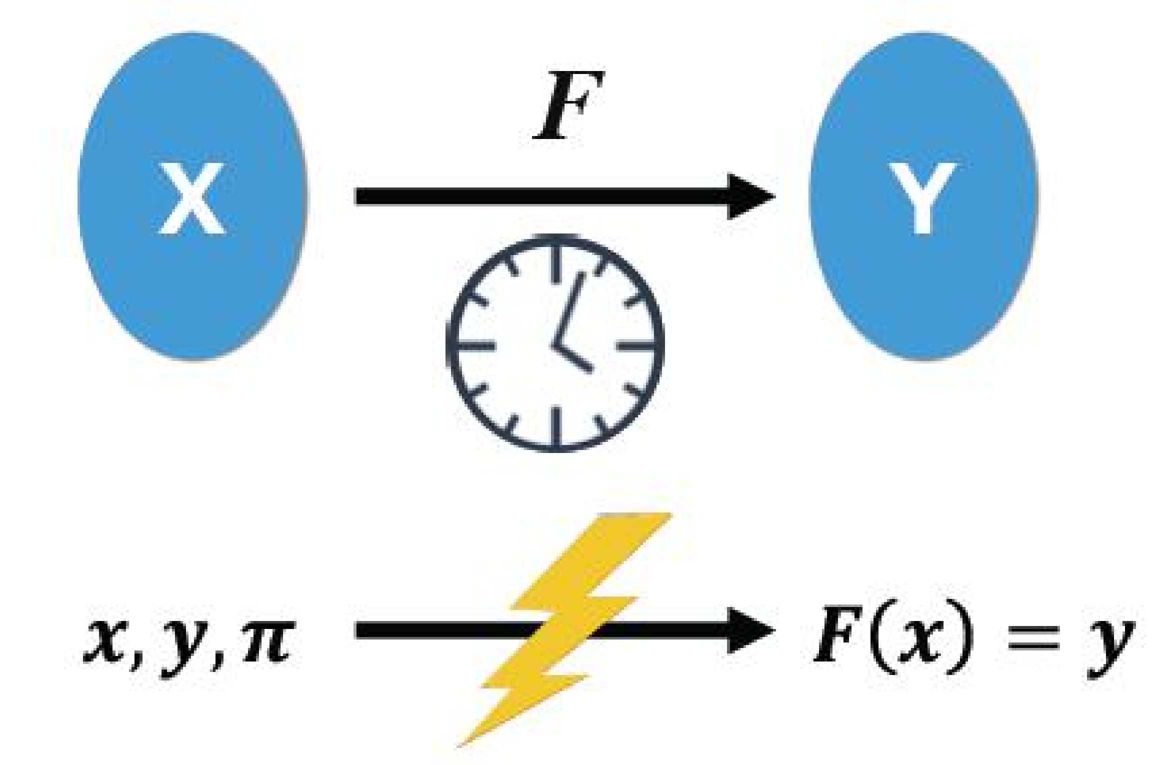
❑My github:

- github.com/taoshengshi

VDF project management

❑ **Function:**

- unique output for every input



❑ **Delay:**

- can be evaluated in time T
- can not be evaluated in time <T on parallel

❑ **Verifiable:**

- correctnees of output can be verified efficiently

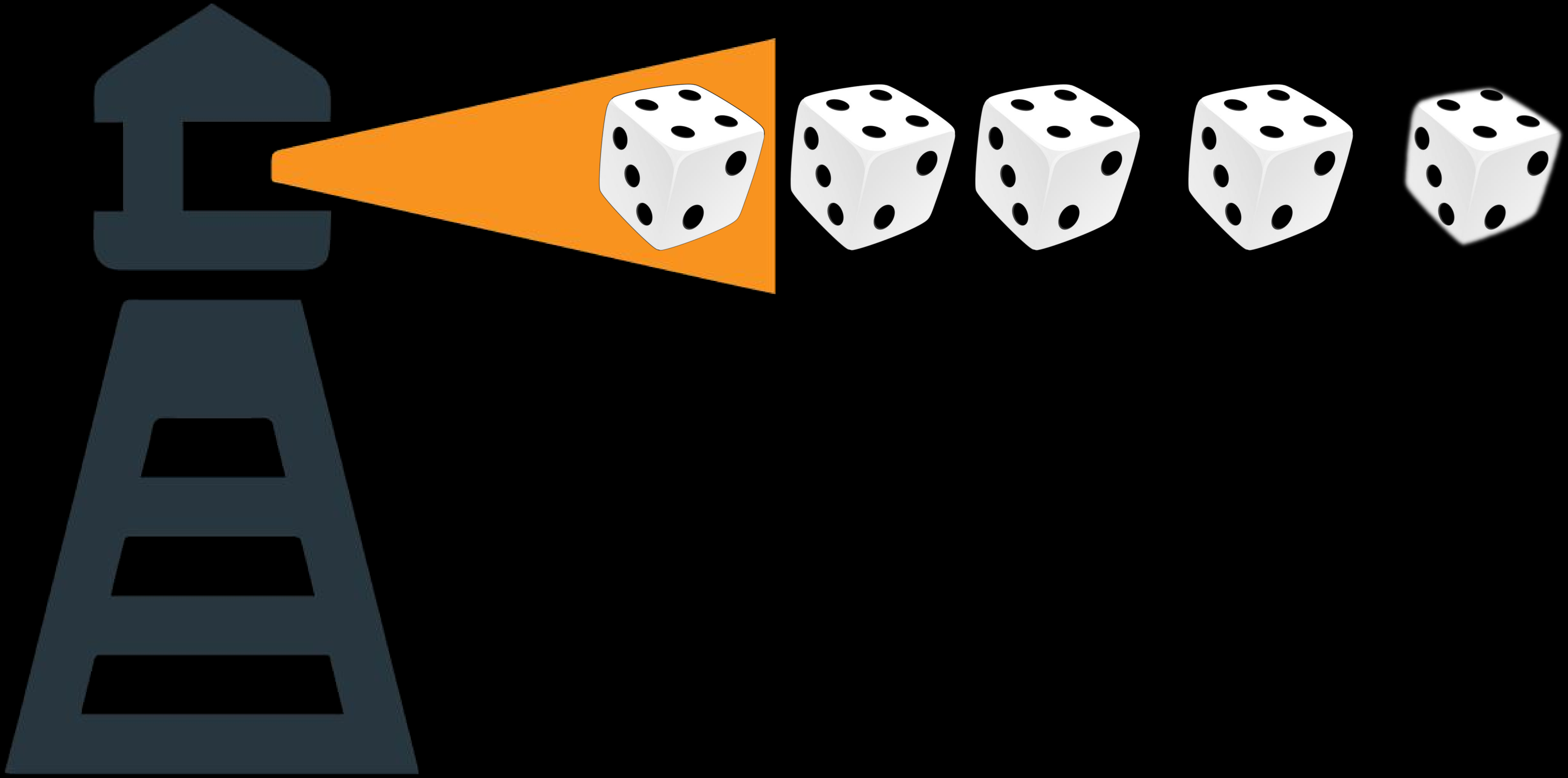
What is a VDF?

❑Randomness beacon

❑Expected Consensus

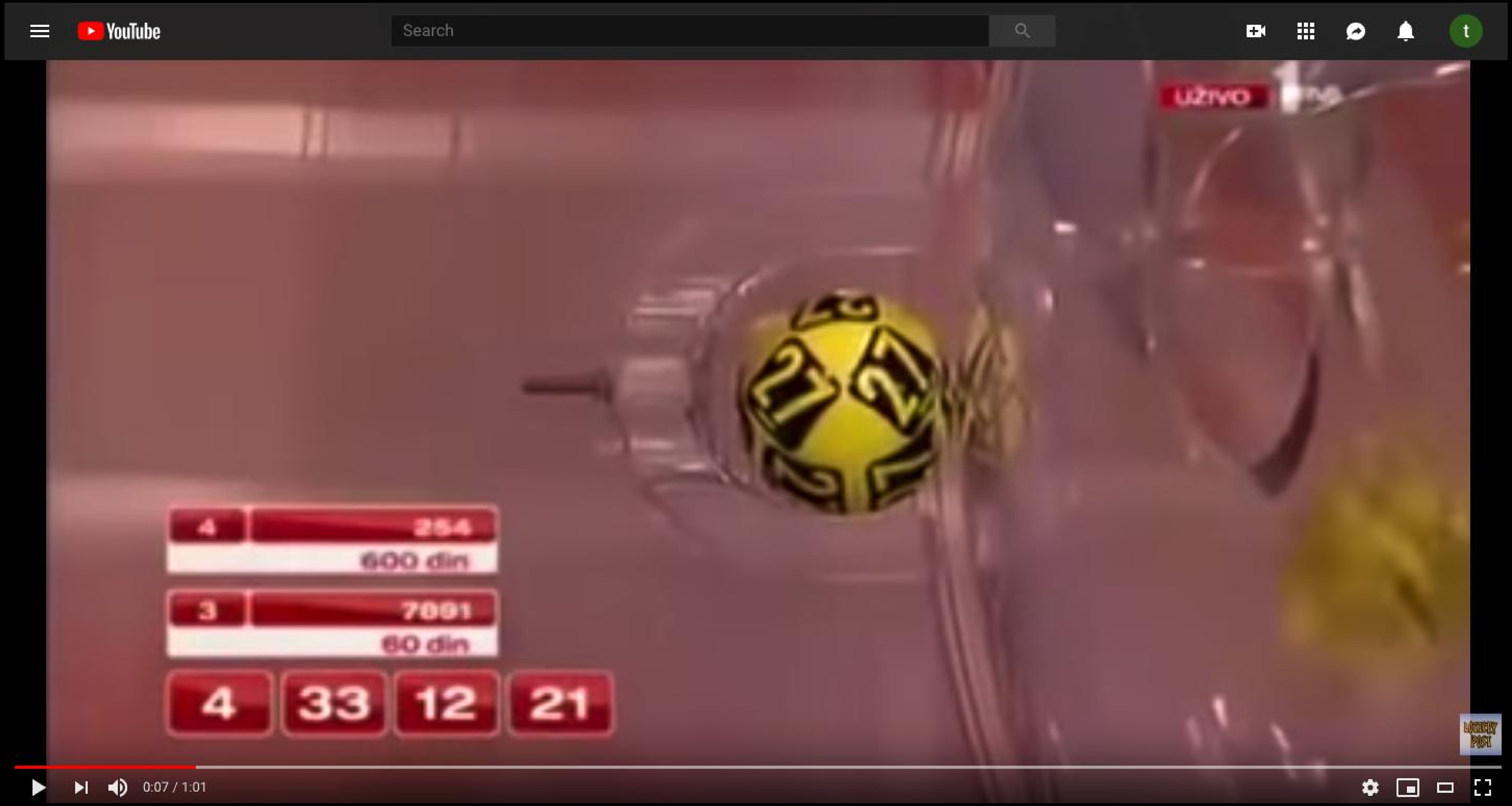
❑Proof of Spacetime

Applications of VDFs



part1: Randomness beacon

public randomness



2015 Serbian lottery

https://www.youtube.com/watch?v=Ls6zq9ibHpY

❑Unpredictable

- Before t0 the value of the beacon is unknown

❑Convincing

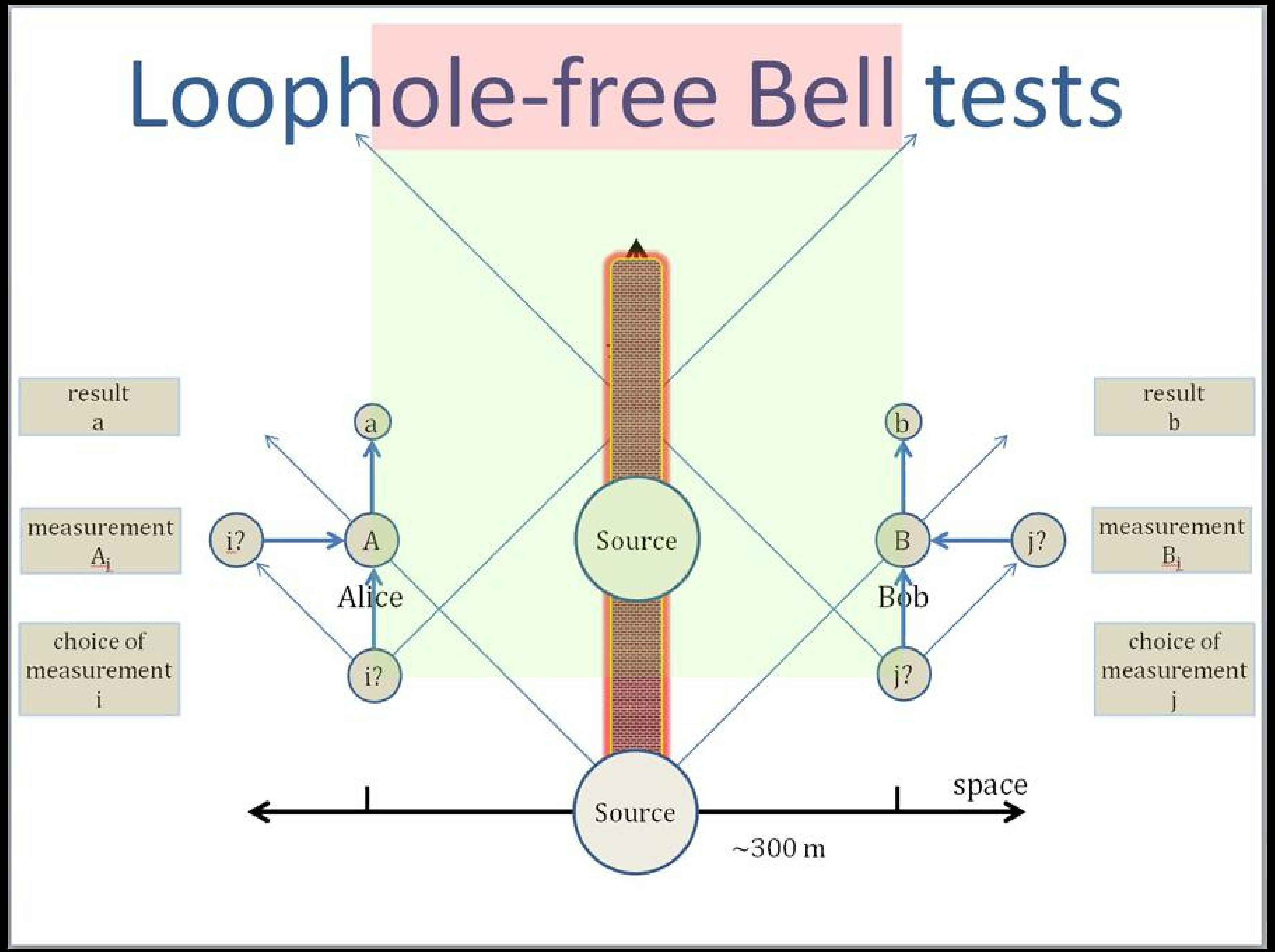
- At time t1>t0,an honest beacon provider can always convince an observer of the correct beacon value

❑Unforgeable

- An observer can distinguish a valid beacon from a forged beacon

secure beacons

service to regularly publish random data



Loophole-free Bell tests

NIST beacon

Pros: high-bandwidth, frequent quantum-mechanical randomness
Cons: completely centralized

natural phenomena

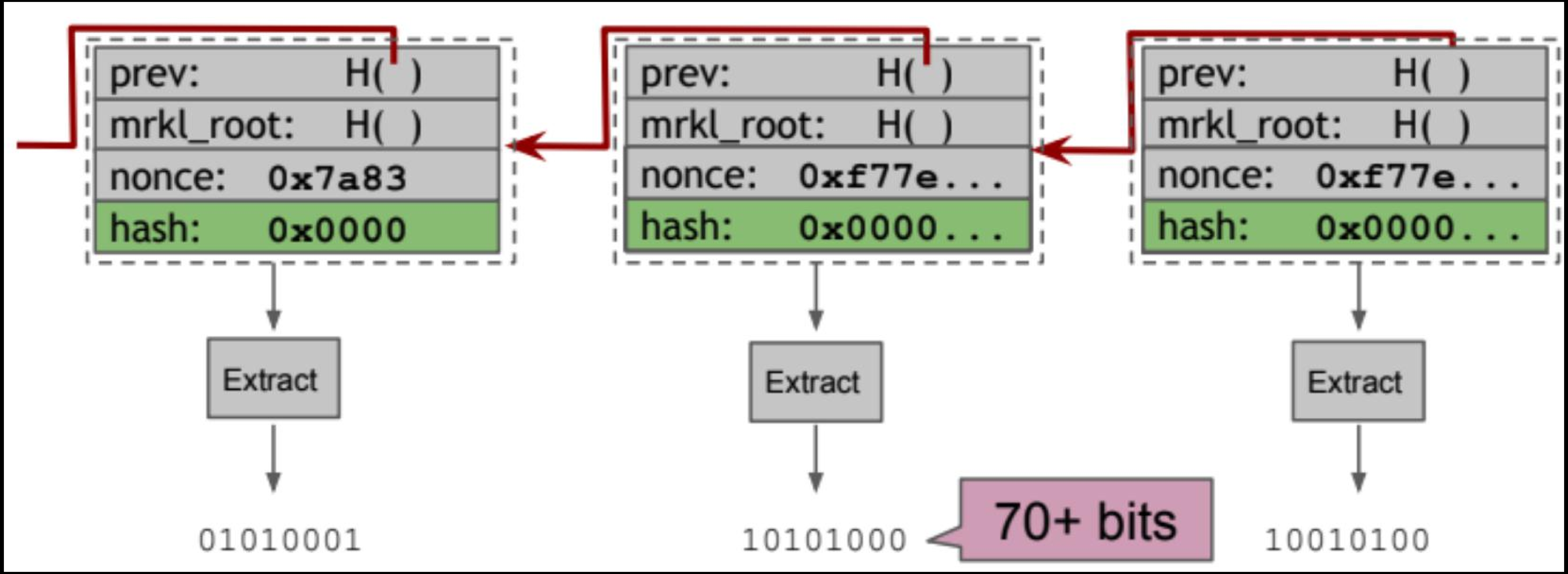
Use natural phenomena as randomness source
one trusted party that does the measurements, that can cheat as anyone else

cryptographic beacons

service to regularly publish random data

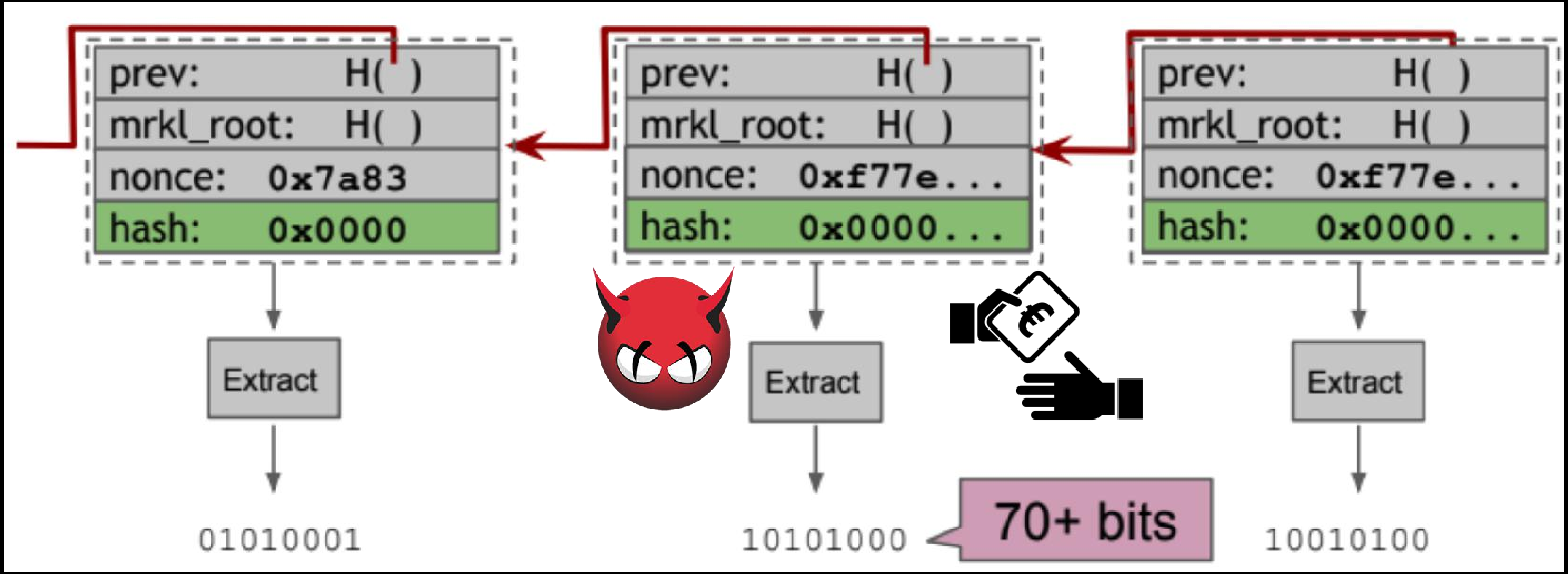
Bitcoin beacon

Decentralized,Continuously publishing,Inherent broadcast mechanism
PoW solutions inherently unpredictable



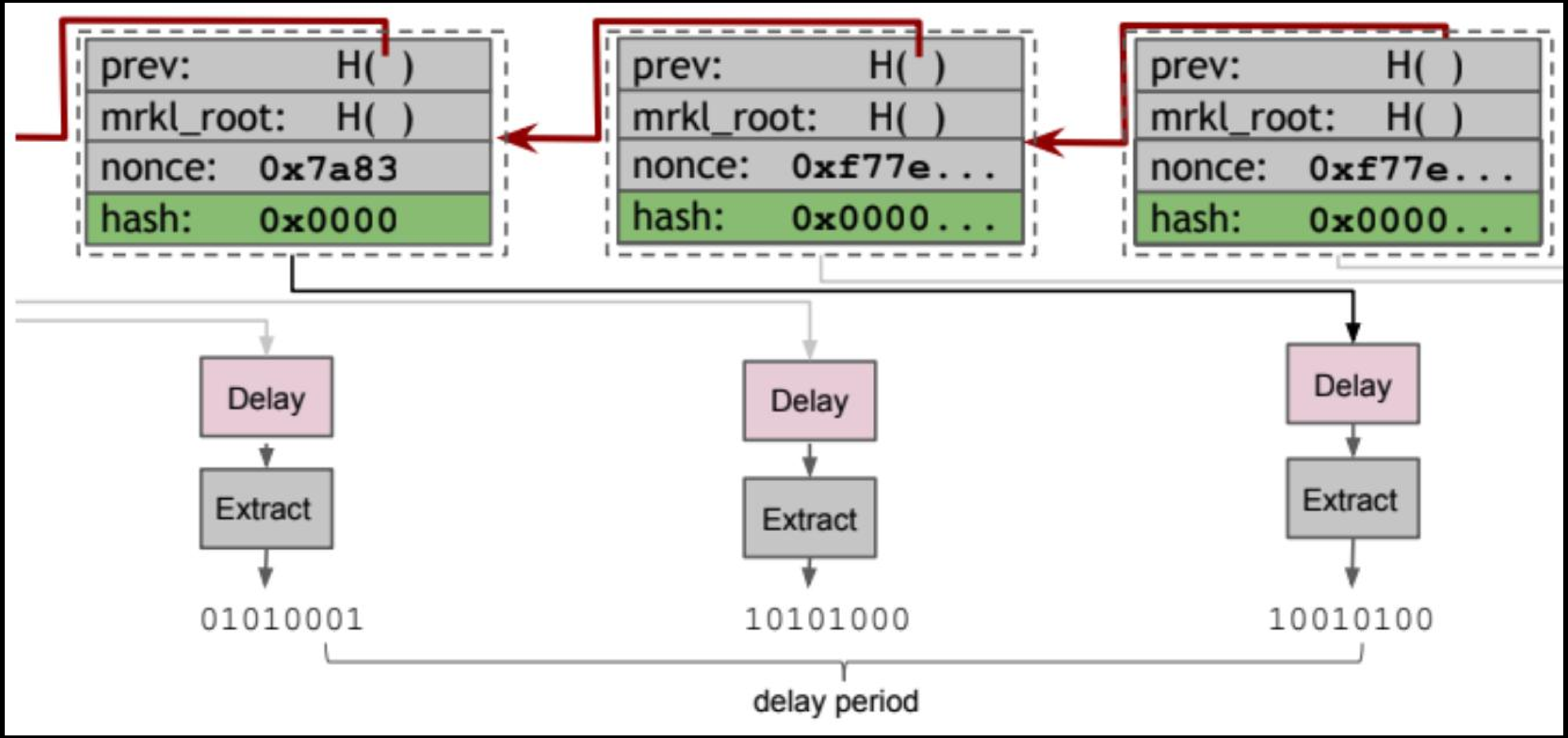
is blockchain beacon secure?

leading zero : min-entropy bound make sure secure
Assuming miners follow the default protocol



No! miners can withhold blocks

rational attacker and bribery attacking
Can we bound the cost of manipulation?



Solution: use a Delay Function

no way of knowing if this is a good randomnees beacon for him
enforce it take an hour to compute what the actual value of beacon
long and slow computaion that take an hour and only then you know the value of the beacon

part2: Proof of Spacetime

- ❑ VDF-PoSt:
    - a Proof-of-Spacetime using VDFs
- ❑ An Extension to PoSt to support multiple sectors
- ❑ An Extension to PoSt to support challenges taken from a Random Beacon

VDF in Filecoin PoSt

❑ *Step 1*: Generate `POST_EPOCHS` proofs:
  - `mix = challenge_seed`
  - `challenge_stream =
NewChallengeStream(PublicParams)`

VDF in Filecoin PoSt

Step 1:

❑Repeat `POST_EPOCHS` times:

- `(challenges, challenged_sectors) = challenge_stream(mix)`
- Generate proof: `porep_proof = OnlinePoRep.prove(challenges, challenged_sectors, commR, replica)`
  - Note: you can have the tree cached in memory
- append `porep_proof` to `porep_proofs[]`
- Add `porep_proof` to `porep_proofs`

VDF in Filecoin PoSt

Step 2

- Slow challenge generation from previous proof `porep_proof`:
    - Run VDF and generate a proof
        - `x = ExtractVDFInput(porep_proof))`
        - `y, vdf_proof = VDF.eval(x)`
        - Add `vdf_proof` to `vdf_proofs`
        - Add `y` to `ys`
        - `mix = y`

VDF in Filecoin PoSt

Step 2

❑Step 3: Output `porep_proofs`, `vdf_proofs`, `ys`

VDF in Filecoin PoSt

step3

Different VDF hardware run at different speed. A small percentage of gain in a `PoSt Epoch` would result in a large time difference in `Total Proving Time` between the fastest and the slowest prover. We call the difference between fastest and average prover `VDF speedup gap`. We define a VDF Speedup gap as a percentage (0-1) and we assume a concrete gap for a PoSt Period between the assumed fastest and the best known prover. We define this gap as `VDF_SPEEDUP_GAP`.

VDF in Filecoin PoSt

Problem with large `POST_EPOCH_COUNTS`

We break up a PoSt into multiple PoSt Periods. Each period must take challenges from a Random Beacon which outputs randomness every interval `MIN_POST_PERIOD_TIME` . In this way, the faster prover can be `VDF_SPEEDUP_GAP` faster in each PoSt Period, but cannot be `VDF_SPEEDUP_GAP` faster over the Total Proving Period.

In other words, the fastest prover cannot accumulate the gains at each PoSt period because, they have to wait for the new challenges from the Random Beacon. In the case of Filecoin, the blockchain acts as a Random Beacon).

VDF in Filecoin PoSt

Mitigating VDF Speedups

part3: Expected Consensus

- ❑Expected Consensus is a probabilistic Byzantine fault-tolerant consensus protocol.

- ❑At a highlevel, it operates by running a leader election every round in which, on expectation, oneparticipant may be eligible to submit a block.

Expected Consensus

❑Proof of resource: proves miner owns X% of total resources

❑Miner with X% of resource should in expectation mine X% of blocks in any chain window(chain quality).

consensus from any proof of resource

❑Proof of resource: proves miner owns X% of total resources

❑Break into X proofs of 1% of resources

- proofs x1,...,xn have distinct values
- each x1 gives one independent random trial :
  Ri = HASH(xi) (0,N)
- Miner finds R=Min(R1,...,Rn)
- Miner the evaluates a VDF with a time delay proportional to R on unpredictable challenge derived from x and previous block

consensus from any proof of resource

BREAK
THROUGH

Perhaps more importantly, the design and development of a secure and usable VDF construction would be a major breakthrough in applied cryptography and distributed systems, with applicability even beyond blockchains.

paxos -> bitocin ->VDF: 十年Paxos，十年VDF

a major breakthrough

❑set up “VDF China” Community

❑build ecosystem

- to research: github.com/taoshengshi
- combine hardware and software vendors
- explore new application areas

❑ regular meetup

My proposal

service to regularly publish random data

谢谢大家！