Decentralised storage in the blockchain era: solutions and challenges

Irene Giacomelli

CryptoNet

Protocol Labs

irene.giacomelli@protocol.ai

25th May 202
Torino

Protocol Labs

An open-source research, development, and deployment laboratory.

We aim to building the next generation of the internet with the focus on decentralisation!

Founded in 2014

Committed to Web 3

Many Different Projects

IPFS

libp2p

~200 Full Time Collaborators

100% Remote Organization

Protocol Labs

CryptoNet.org

Cryptonet is an open distributed research lab working on applied cryptography to improve crypto-networks.

Learn more →

30+

Research Collaborators

See all projects:

Projects

15+

Filecoin Protocol upgrades

Read work notes:

Cryptonet Notebook

$1M+

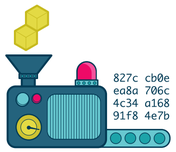
Available Research Grants

Apply for grants:

Grants [Paused]

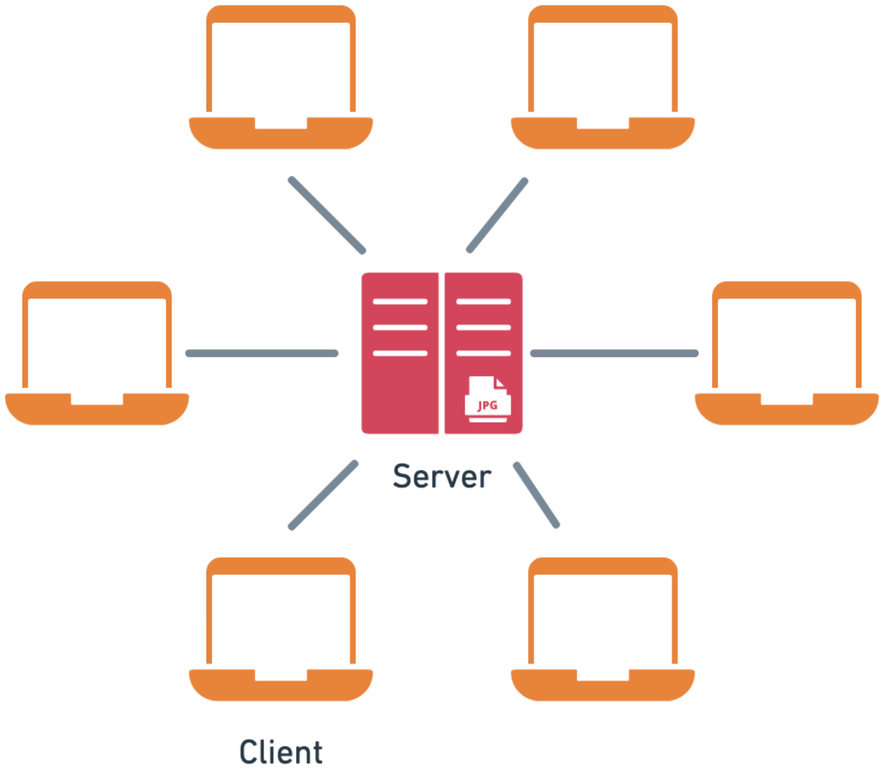
Talk Outline

Three Topics:

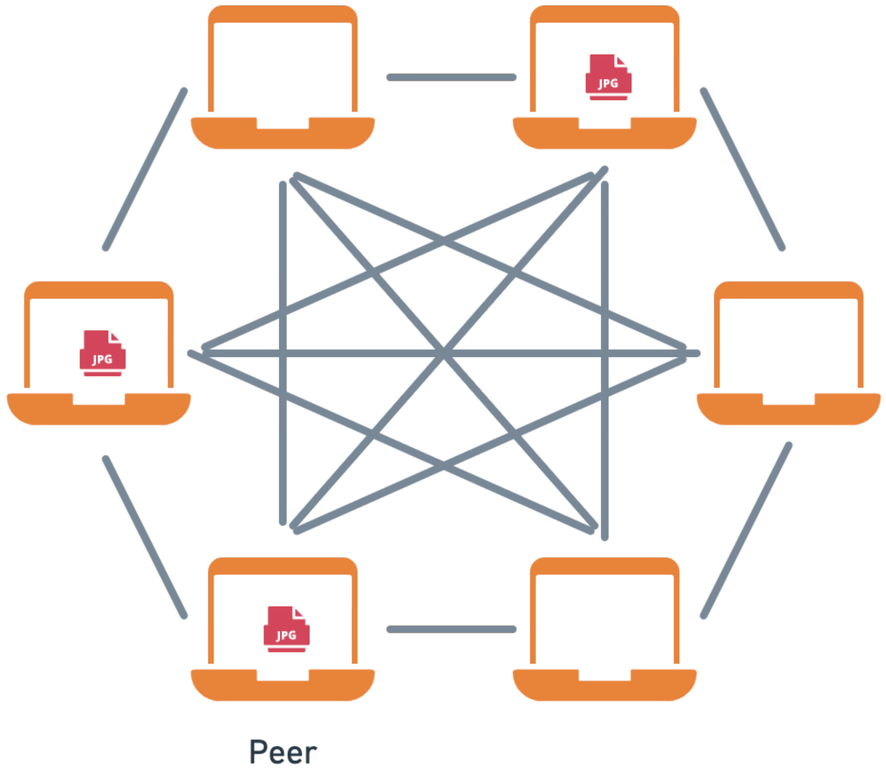
1. Decentralised storage 
2. Blockchain 

4. Filecoin: decentralised storage market power by a blockchain 

Decentralised Storage

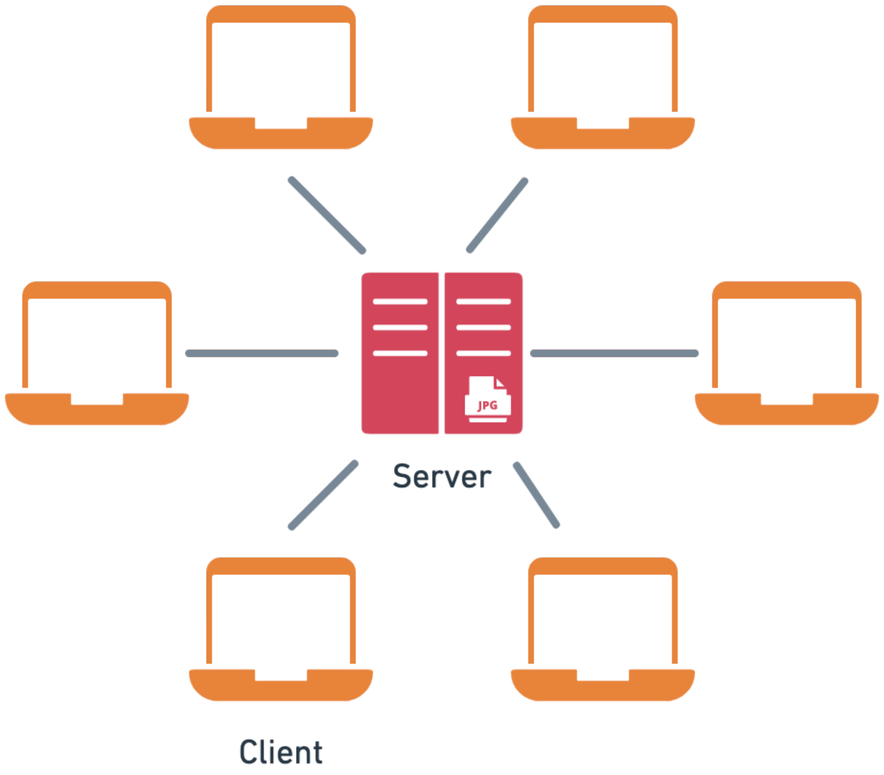


Client-Server model

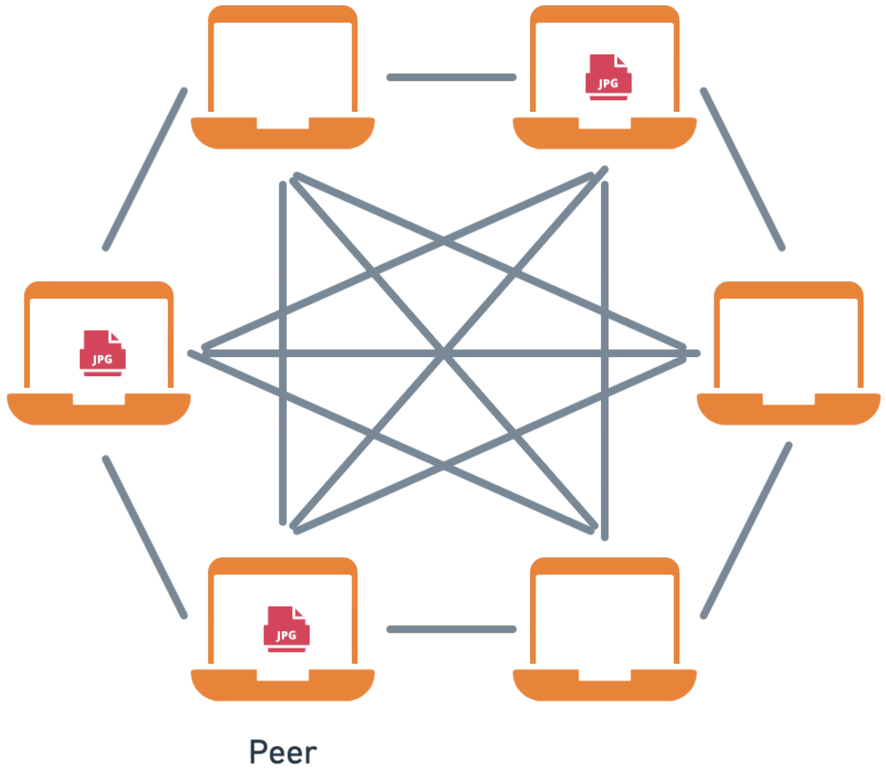


Peer-to-peer model

Decentralised Storage Market



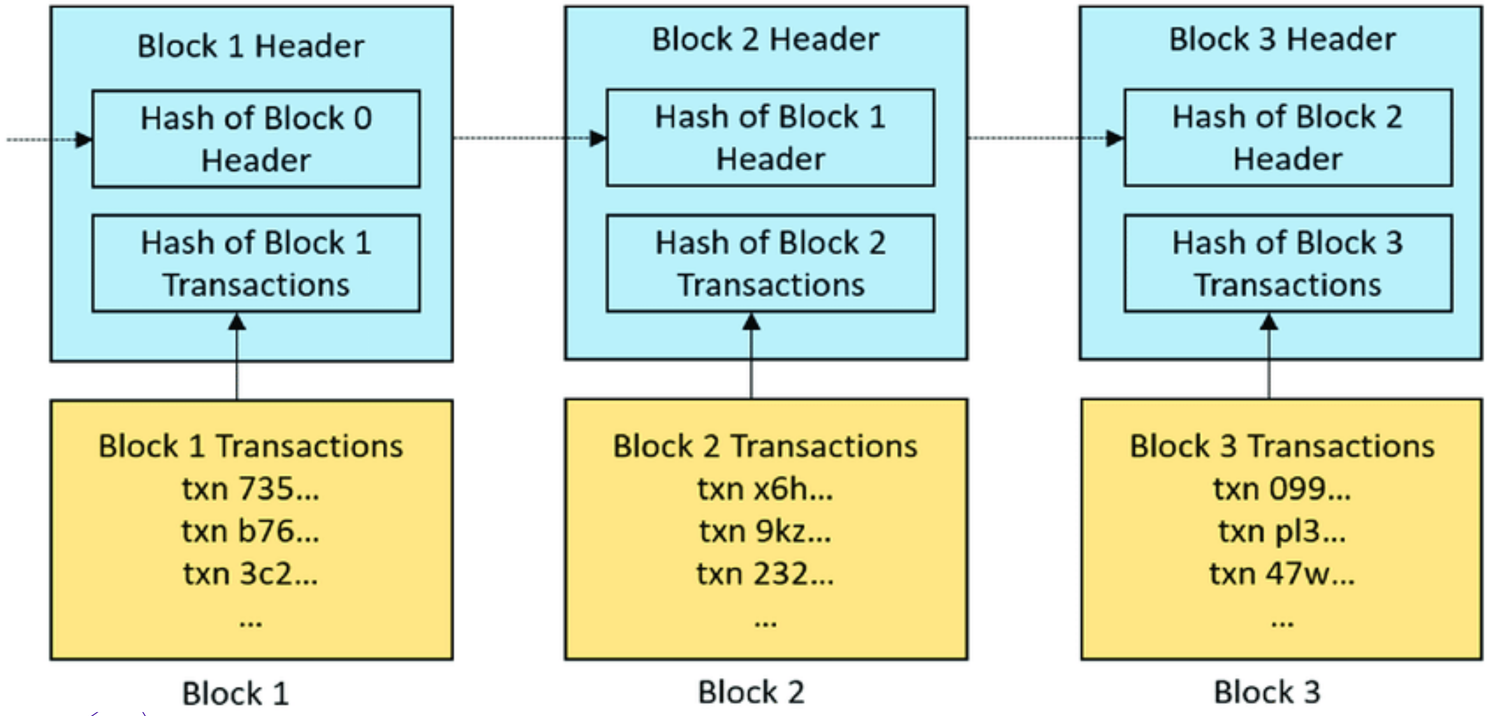
Client-Server model



Peer-to-peer model

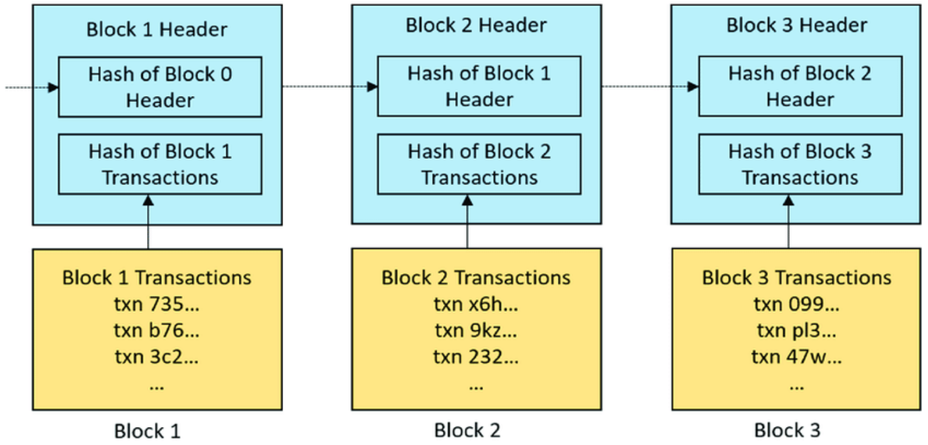
Blockchain preliminaries

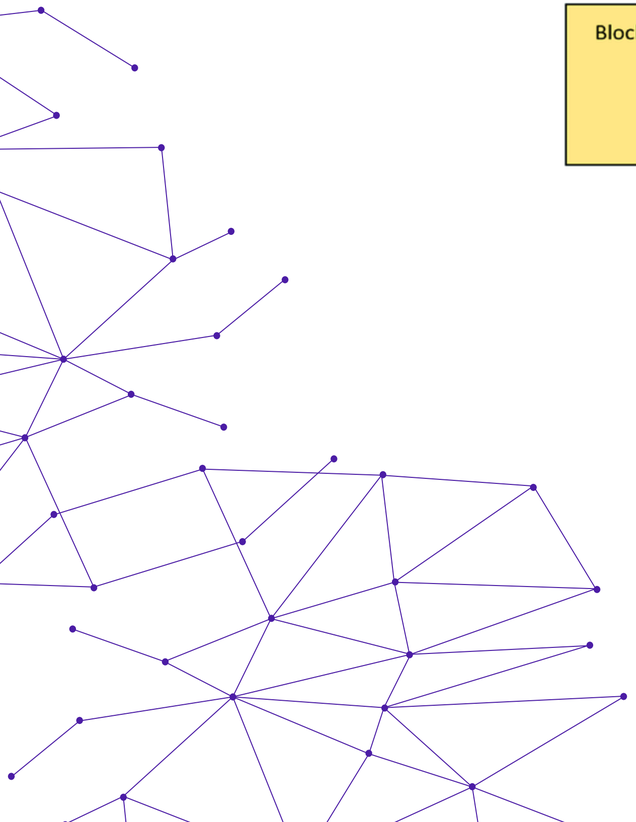
Blockchain = distributed (ie, maintained by a network) ledger, organised in blocks and irreversible



Blockchain preliminaries

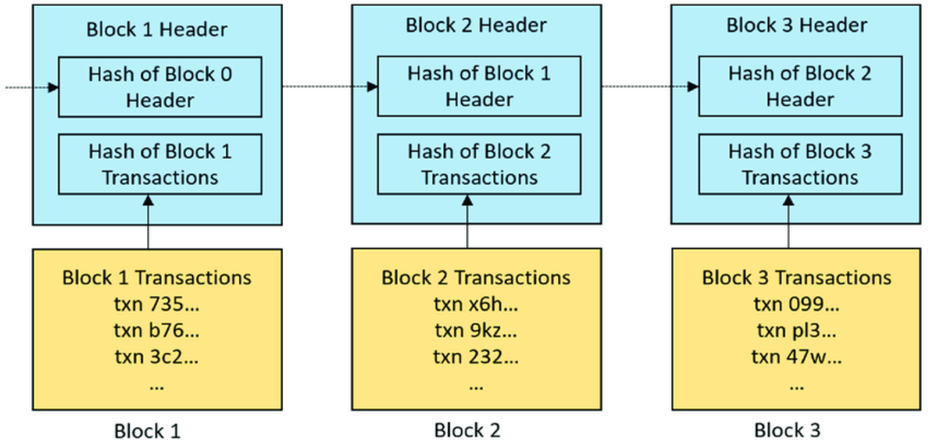
Critical problem: How do we agree on the next block?





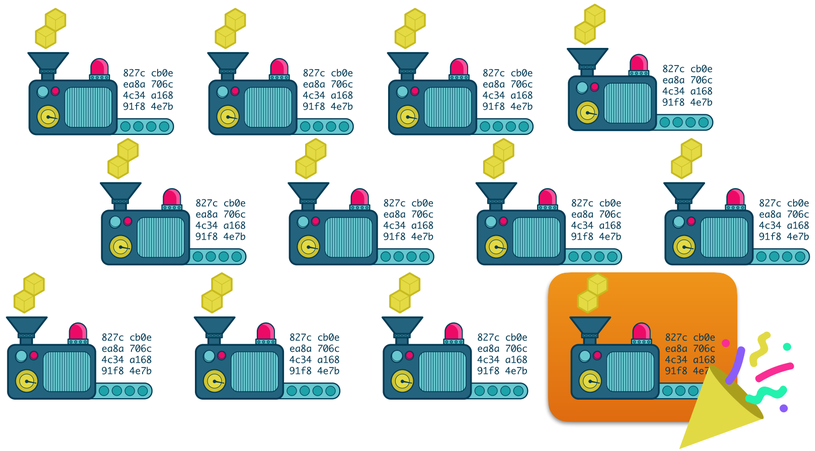
Blockchain preliminaries

Critical problem: How do we agree on the next block?

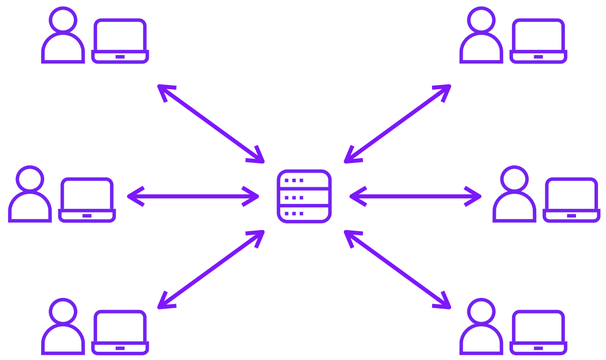


A **lottery** based on computational power chooses one node who creates the next block!

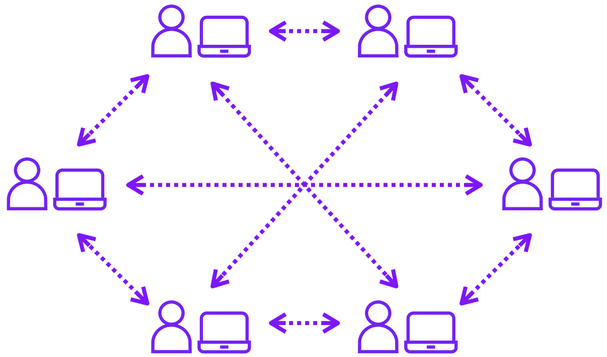
(**Nakamoto Consensus Protocol**)



Can a blockchain give decentralised storage market?



VS



Filecoin: Decentralise the Storage Market

The **Blockchain** replaces the **Trusted Third Party** by keeping track of everything going on in the network

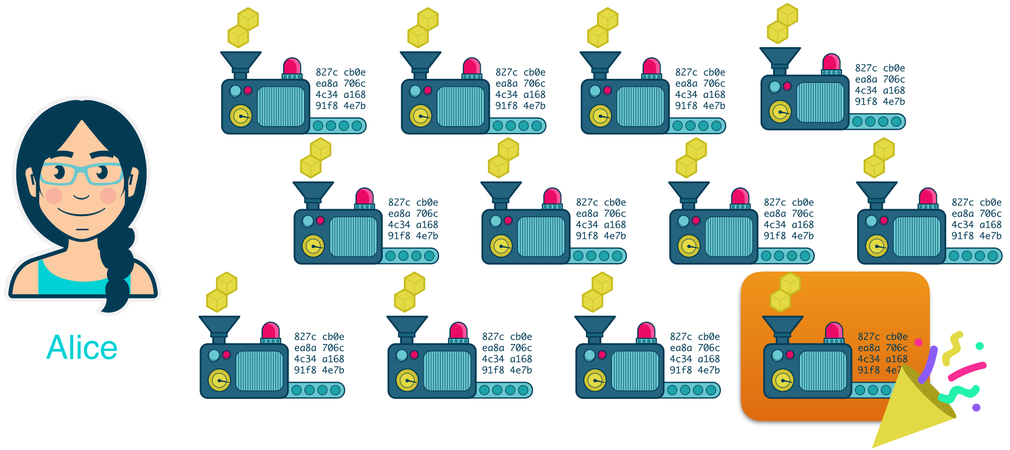
Blockchains and Storage

- Data availability: Store transactions data (from Ethereum}
  - Example: celestia.org 
- Data in the blockchain’s blocks
  - Example: ⓐ arweave.org
- Blockchain and smart contracts are used for deals and payments
  - Example: sia.tech
- Data Storage is the underlying resource for the blockchain consensus
  - Example: filecoin 

How PoS is different from PoW?

Proof of Space (PoS)

Proof of Work (PoW)



In PoS the underlying resource is (persistent) storage rather than computation.

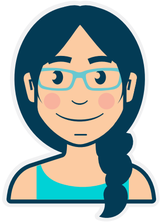
A more efficient and green alternative to PoW in Nakamoto-Style Consensus Protocols!

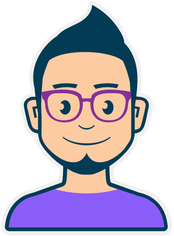
What is a Proof of (Useful) Space?

Proof of Space (PoS)

Alice

"I am storing data D of size N!"





Bob

"True/False!"

Security property:

Bob can check that Alice persistently stores the (incompressible) data D of size N!

What is a Proof of Space?

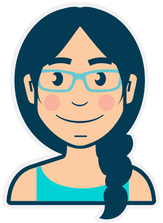
Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

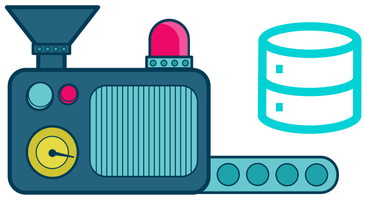
2. **Execution** (repeated audit phase)

Alice



Bob

Initialization:



Advice,
Enc(data)

What is a Proof of Space?

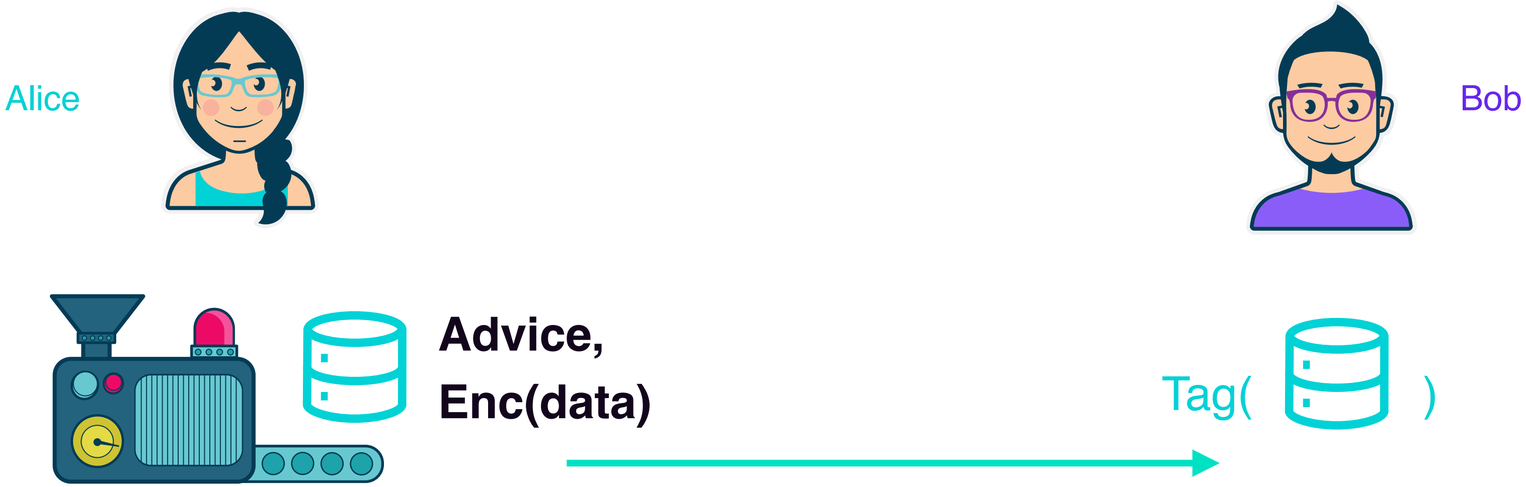
Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)

Initialization:



What is a Proof of Space?

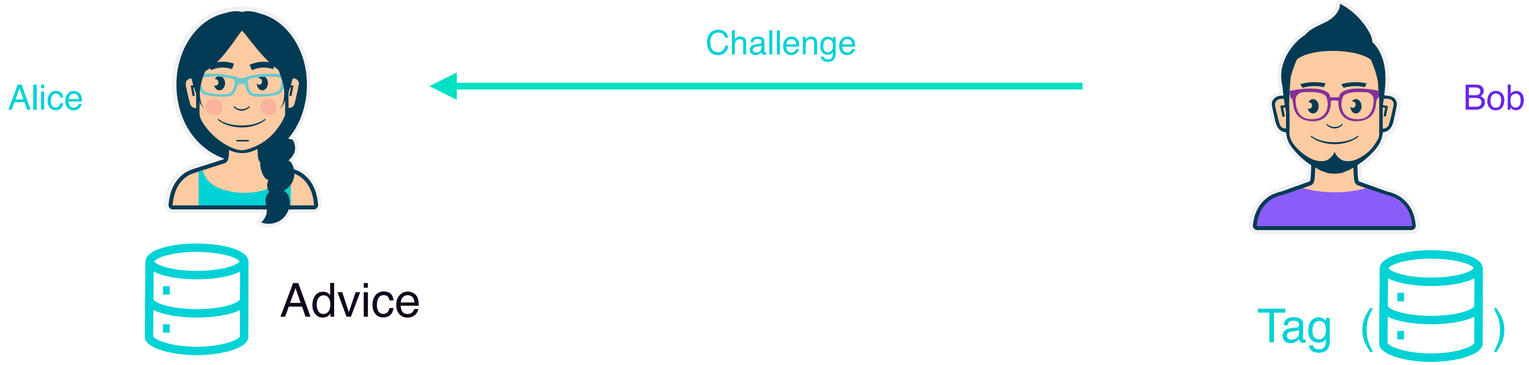
Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)

Execution:



What is a Proof of Space?

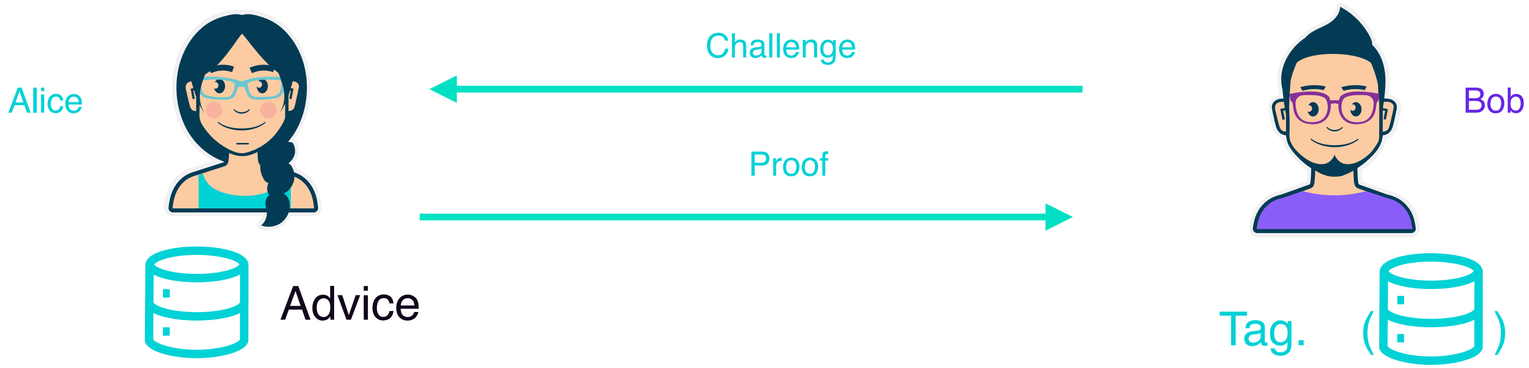
Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)

Execution:



What is a Proof of Space?

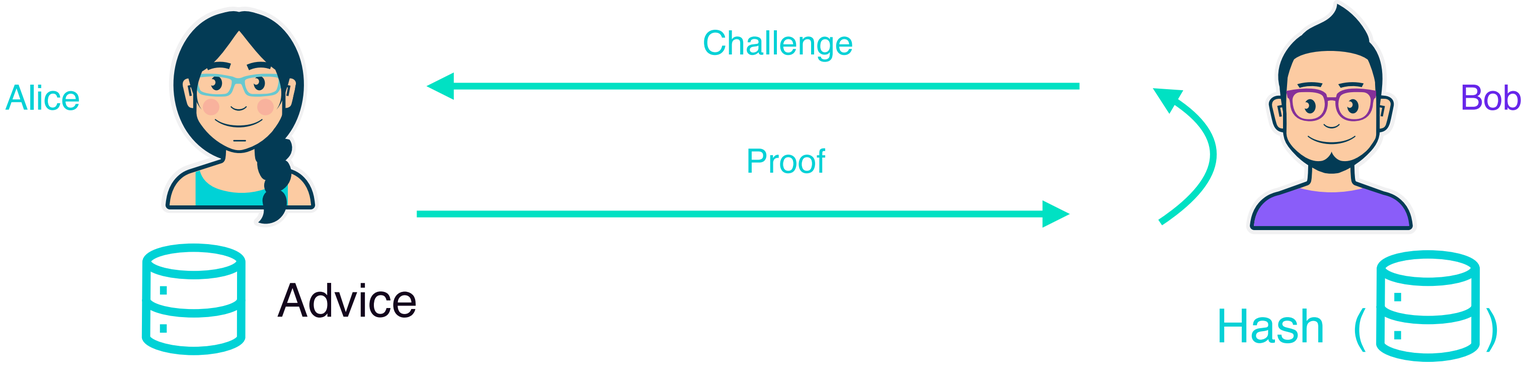
Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)

Execution:



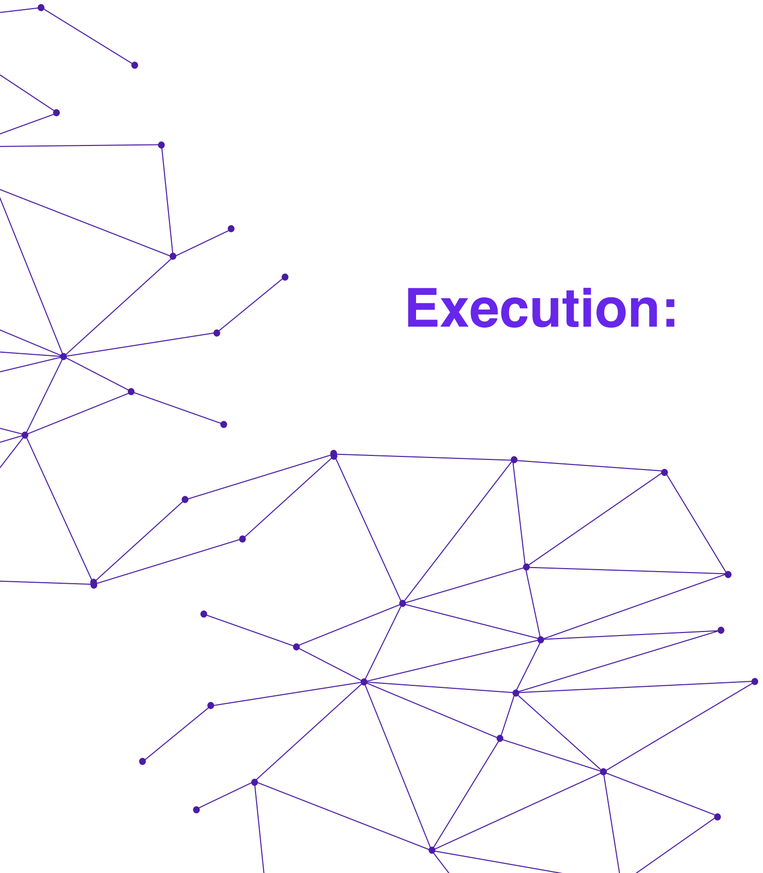
What is a Proof of Space?

Proof of Space (PoS)

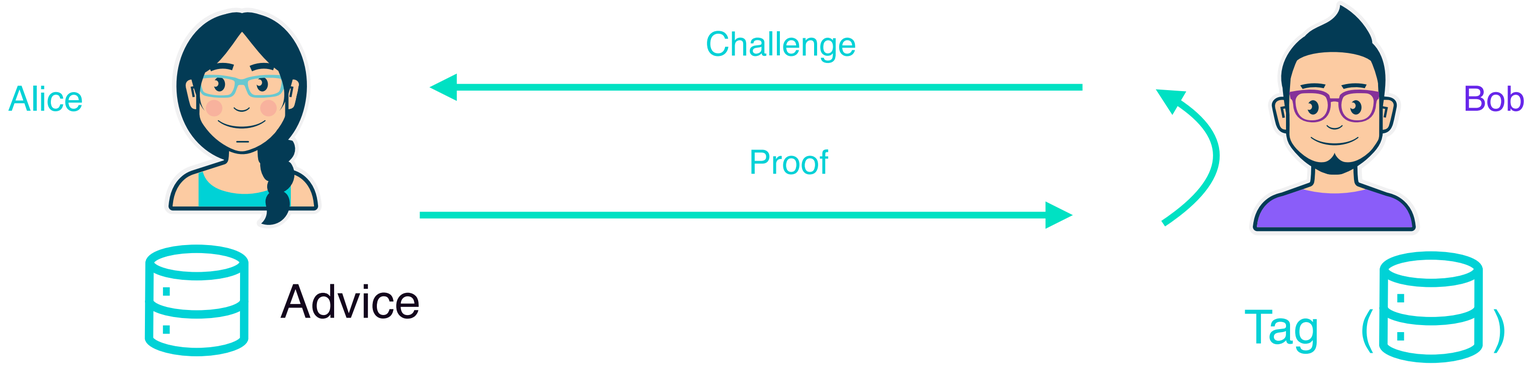
Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)



Execution:



Soundness (informal, fix eps)

if Alice stores N' then she must do a computation of T(N') steps in order to produce a convincing proof (for any N'< eps * N).

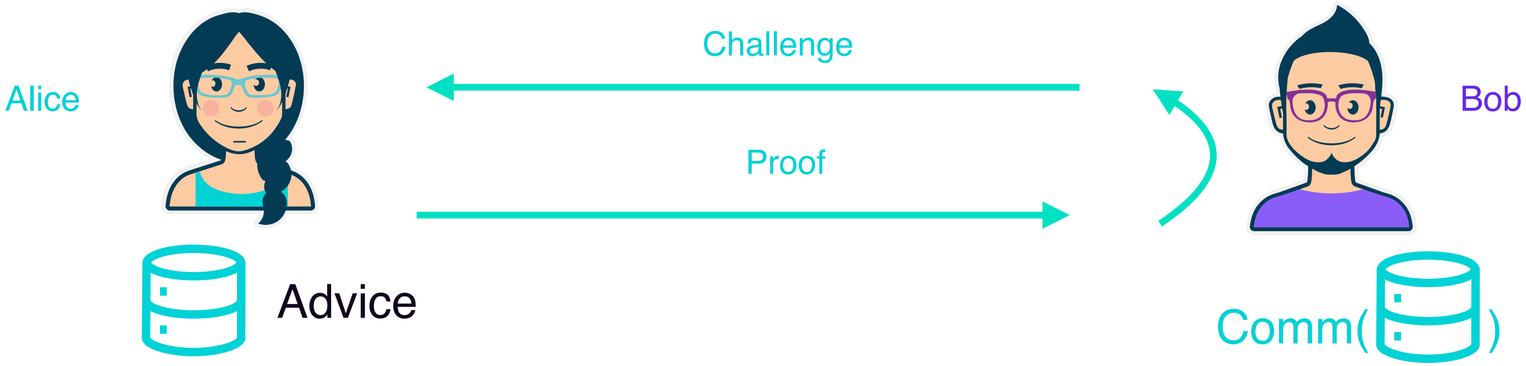
Question 1: What is a Proof of Space?

Proof of Space (PoS)

Two phases protocol:

1. **Initialization** (one-time setup)

2. **Execution** (repeated audit phase)



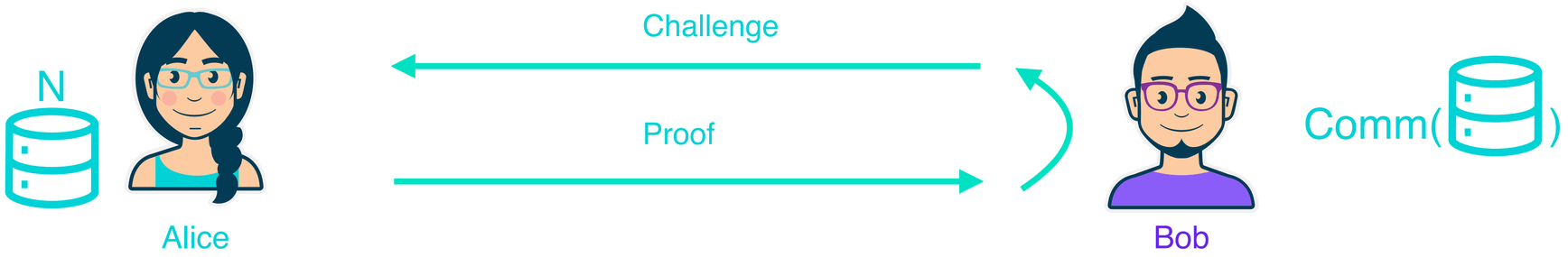
Execution:

The *"T-step computation"* is infeasible/irrational
=> Alice is persistently storing the advice

What is a Proof of Space?

Proof of Space (PoS)

Execution



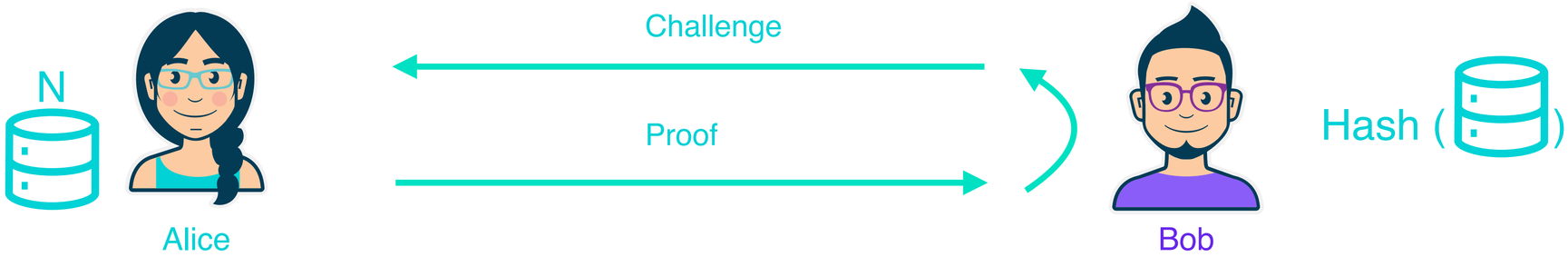
What does “T-step computation is infeasible” mean in practice?

Latency model: Alice must answer challenges in a limited window of time for the proof to be valid. We need a ***timing heuristic assumption*** to translate T-steps in t seconds!

What is a Proof of Space?

Proof of Space (PoS)

Execution

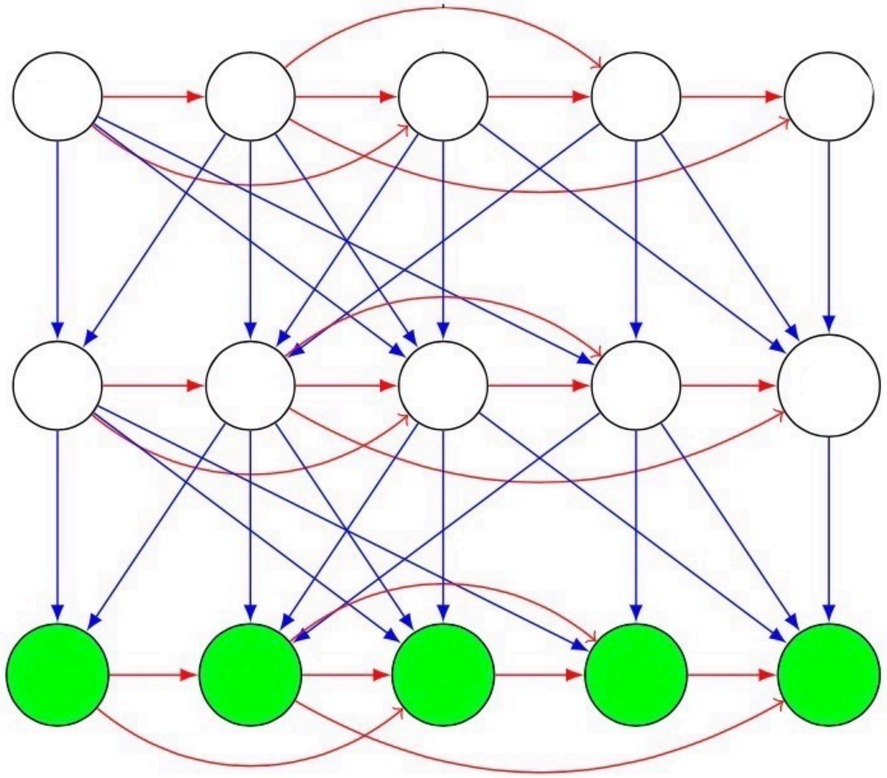


What does “T-step computation is irrational” mean in practice?

Cost Model: Alice chooses to store because T steps are more expensive than storing the advice for the time between two consecutive executions (rational prover). We need a ***cost heuristic assumption*** to translate T-steps in t dollars!

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)



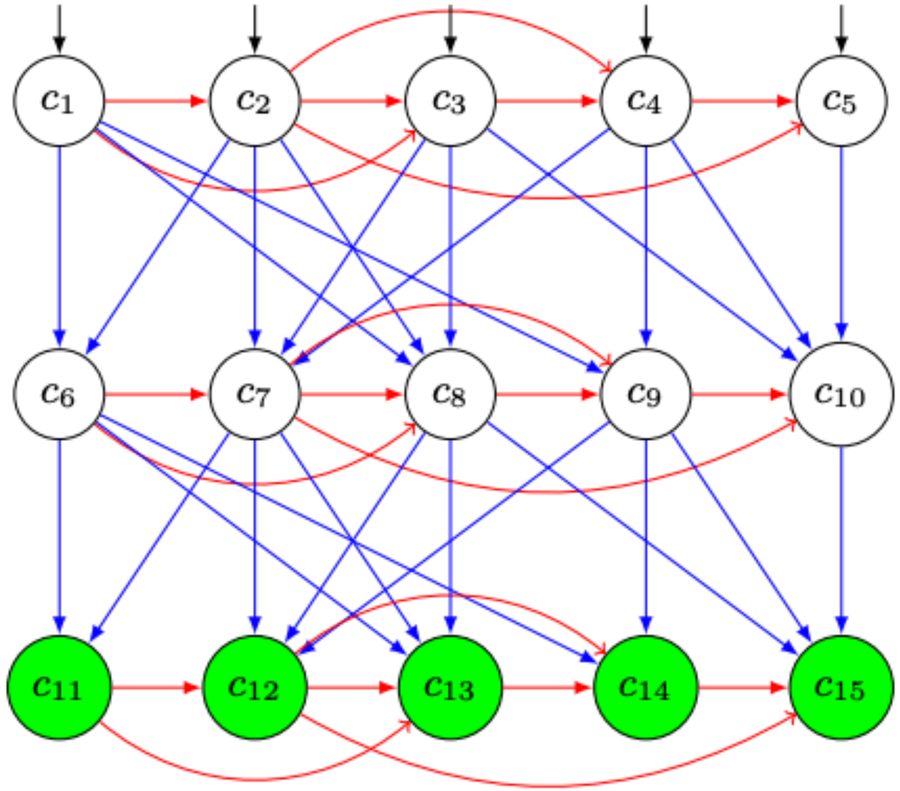
Each layer is a **depth-robust graph** (red edges)**:**
each set of 80% of the nodes has a long path (20%)

Each pair of layers is an **expander** (blue edges)**:**
an x fraction of nodes in the lower lever has a 2x of the nodes of the upper layer as parents (x < 1/3)

Ben Fish, Crypto19, “Tight Proofs of Space”

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)

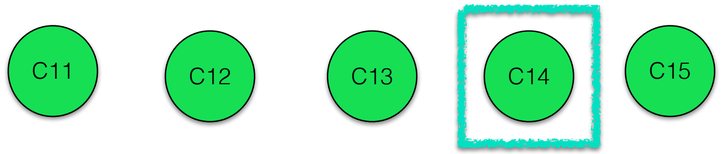


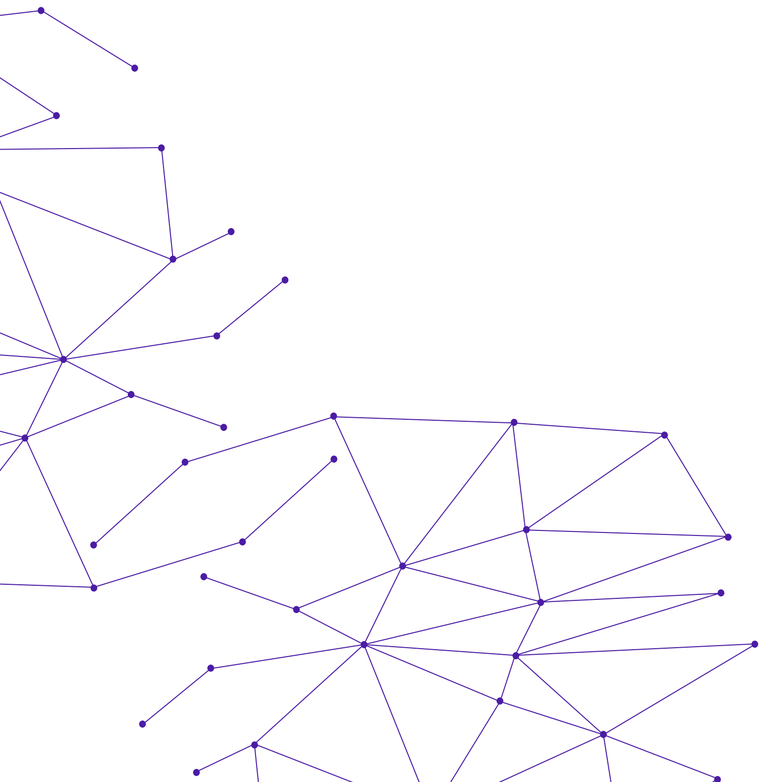
Label of a node:

c_i = Hash(i ll Hash(D) ll c_j if j is a parent of i)

Enc(D) = labels of green nodes + D

Graph-labelling based PoS





Execution

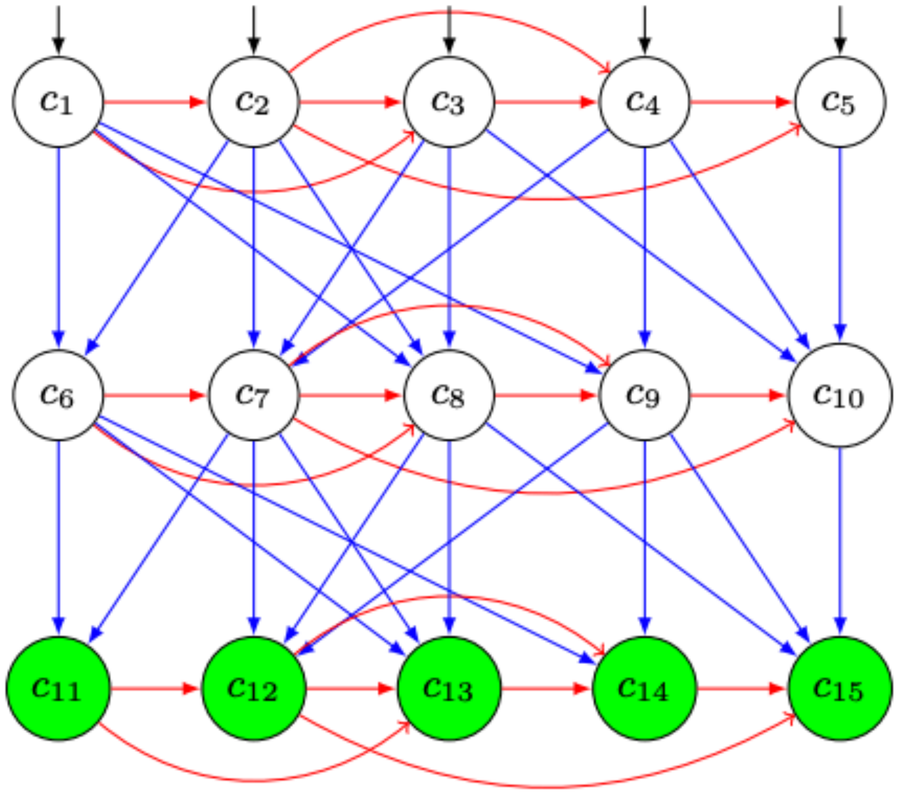
Bob periodically choses a random node

Alice answer with the label (and hash proof)

If she does not store it, must re-compute it!!

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)



Layer 1

Layer 2

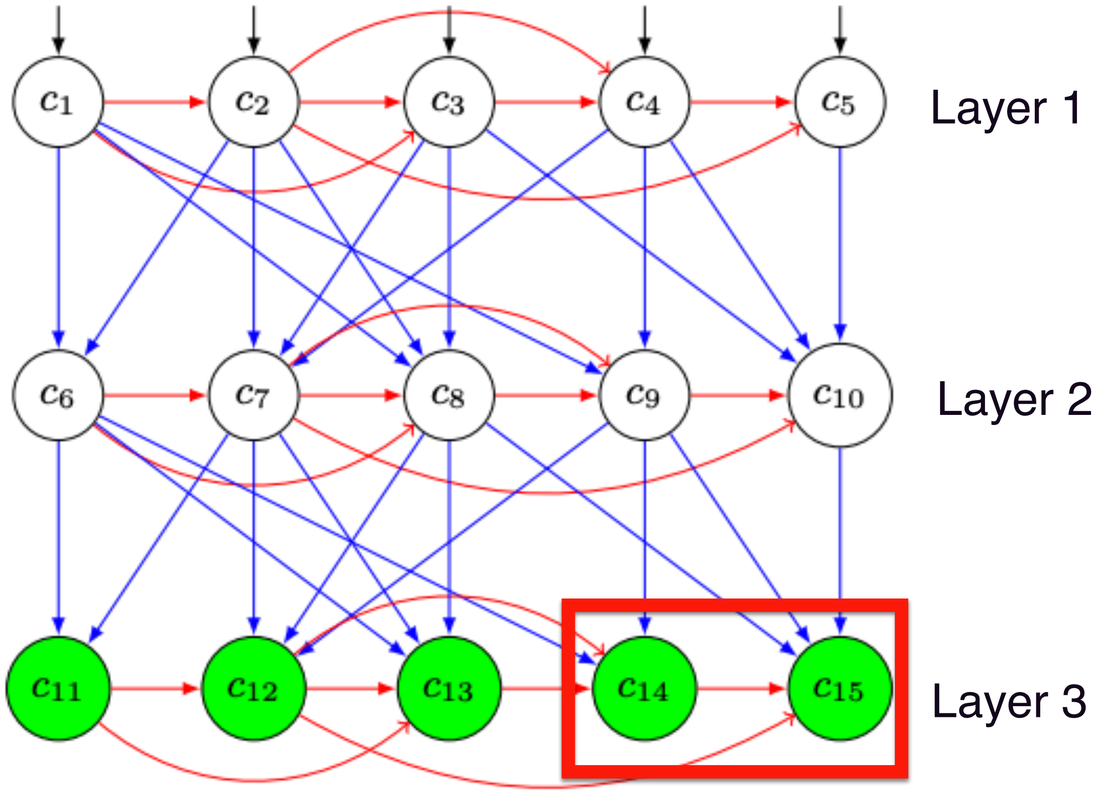
Layer 3

Security property:

- Re-computing from scratch is slow/expensive because:
  a random node has “many many” parents (with high prob.)

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)



Layer 1

Layer 2

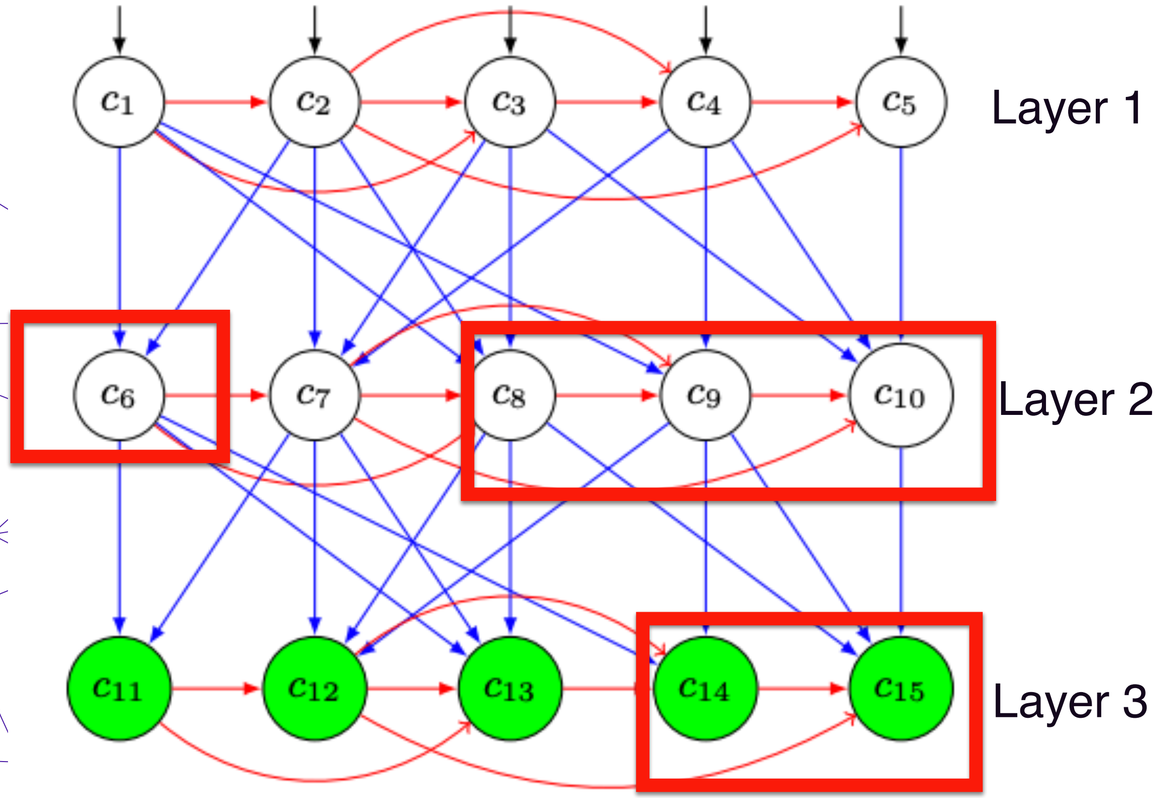
Layer 3

Malicious Alice:

Store only c11, c12, c13
(Delete c14, c15)

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)



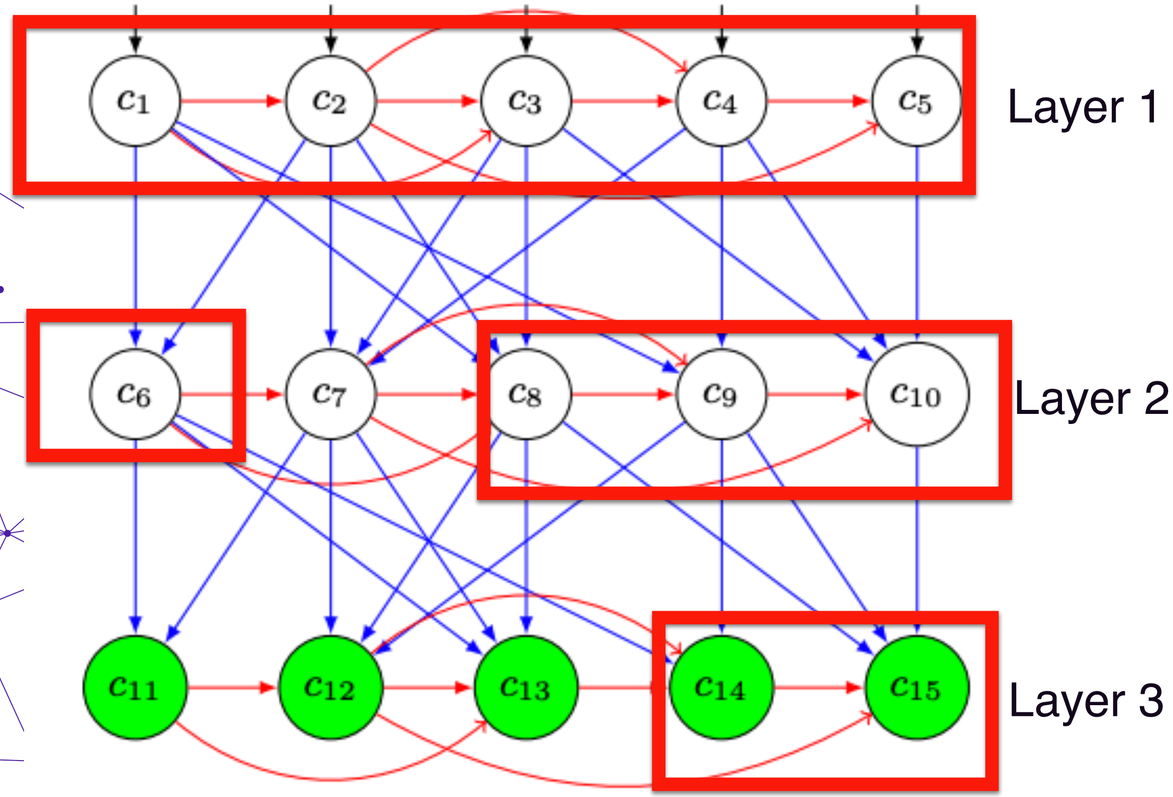
Security argument:

Recomputing c14, c15

- 4 parents in layer 2 (because of the expander graph)

Graph-labelling based PoS

Stacked-DRGs graph (aka “SDR”)



Security argument:

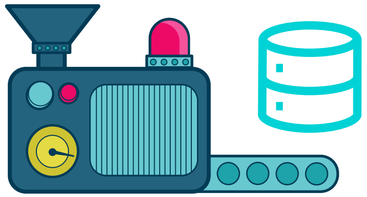
Recomputing c14, c15
- 80% of the final layer => long path!!
(because of the depth-robust graph)

Long path => slow computation in the latency model

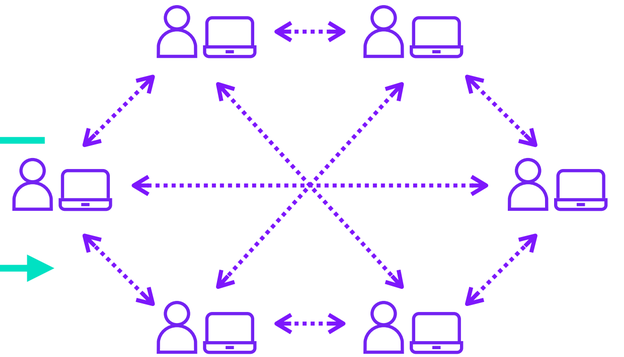
NOTE: We can also get a cost bound about the long path => cost model

PoS in Filecoin

Storage Provider



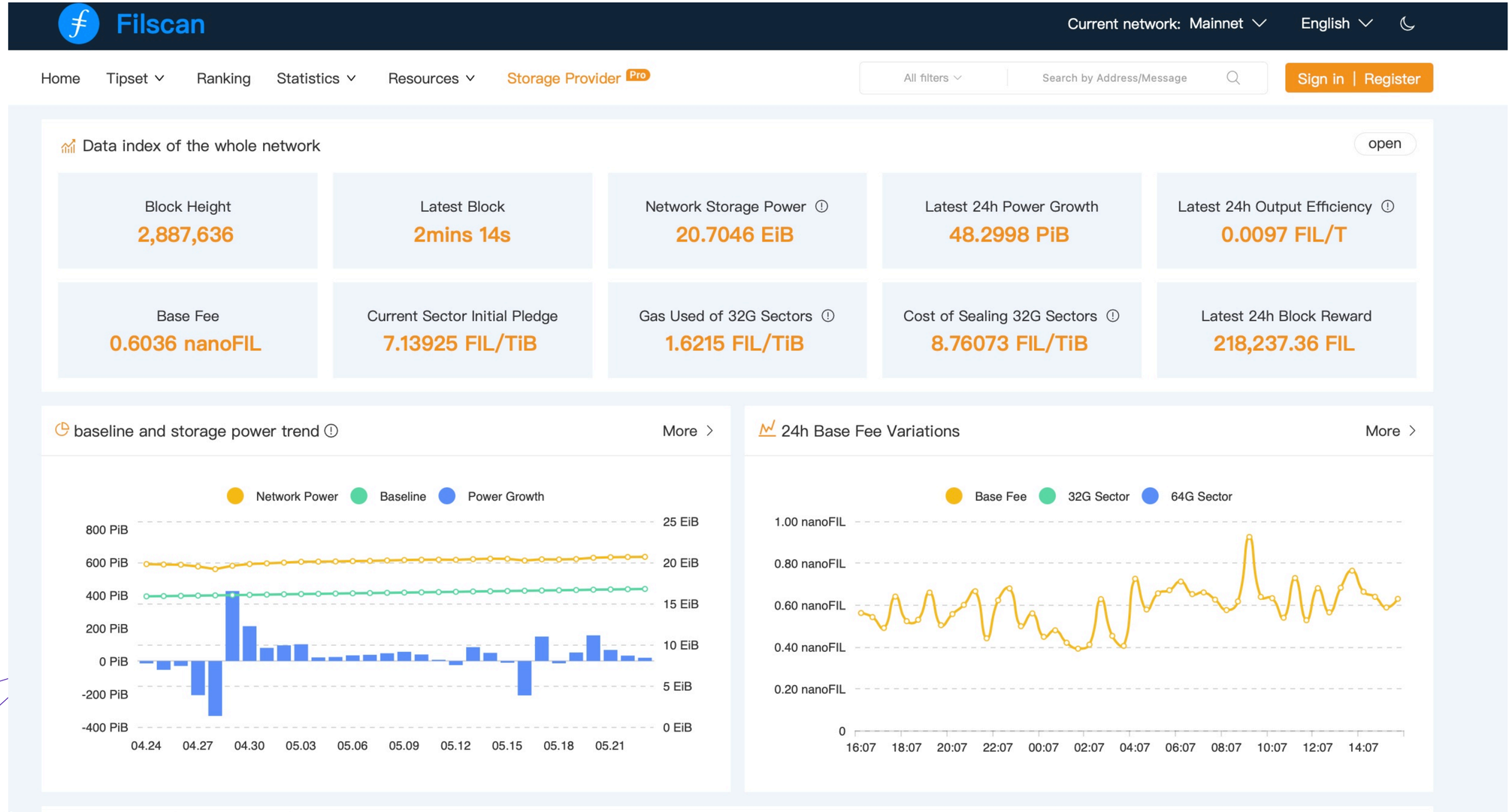
Advice,
Enc(D)



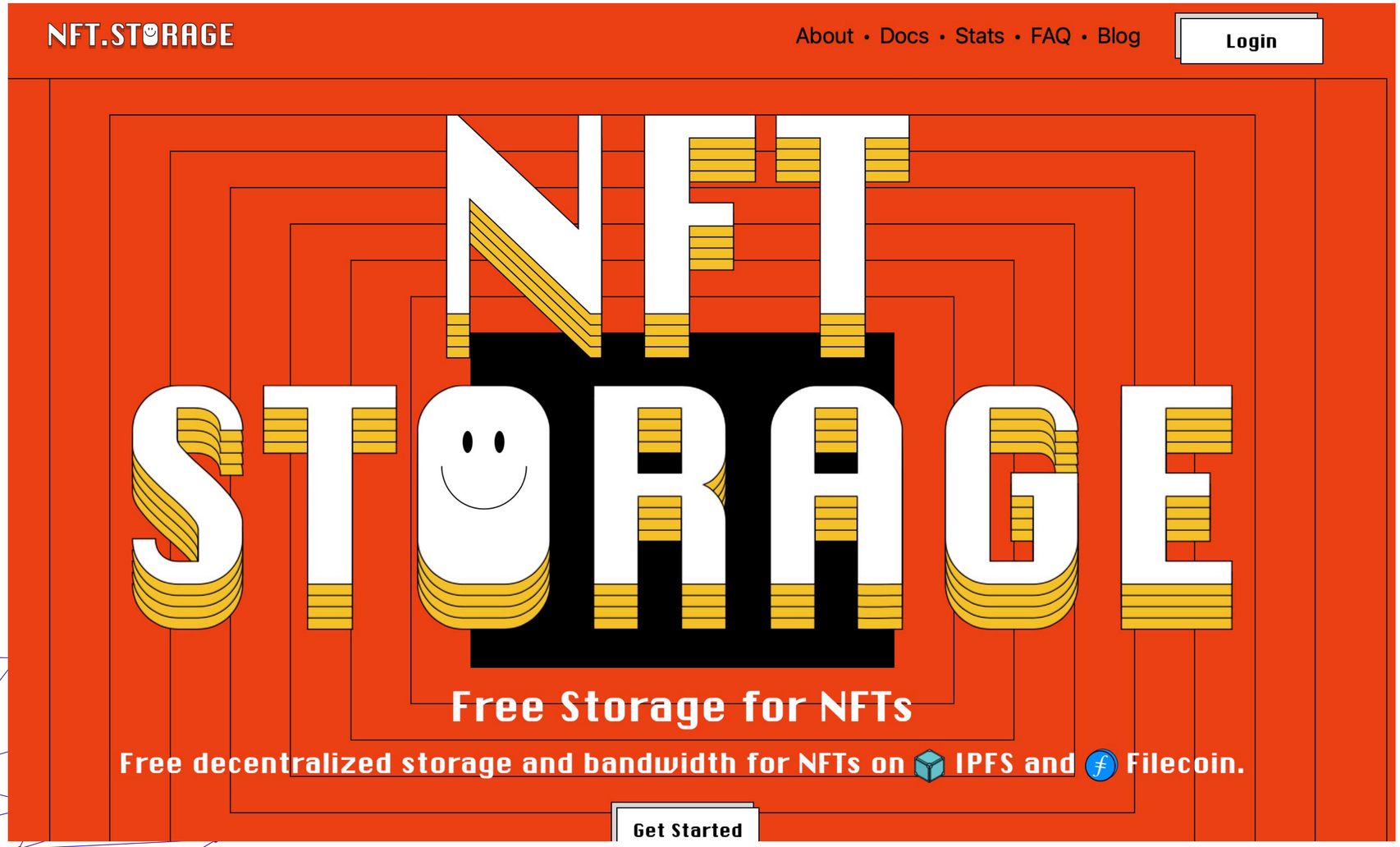
Blockchain

Hash ()

PoS in Filecoin



PoS in Filecoin



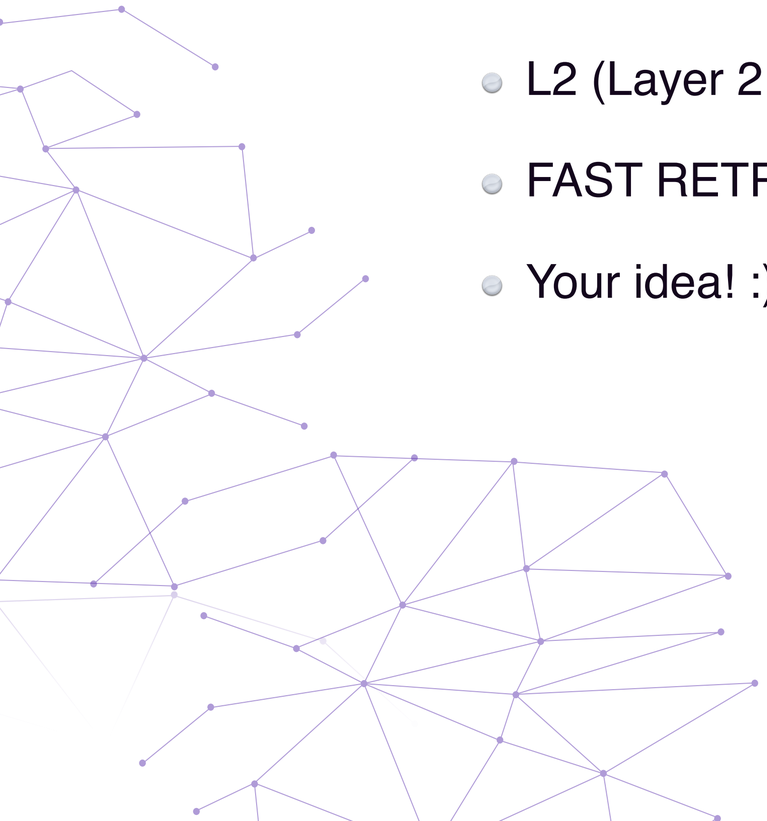
PoS in Filecoin

Is that all? Nope….

- SNARKs (“Succinct Non-interactive Argument of Knowledge")
- VECTOR COMMITMENTS (ie, Merkle Trees)
- LEADER ELECTION via VRF (“verifiable random function”)
- Different HASH functions
- Threshold Encryption (for the random bacon, drand)
- Digital Signatures

What’s next? —>

- FVM—> Filecoin Virtual Machine and Smart Contract Capability
- L2 (Layer 2 Applications)
- FAST RETRIVABILITY
- Your idea! :)



Thank you!

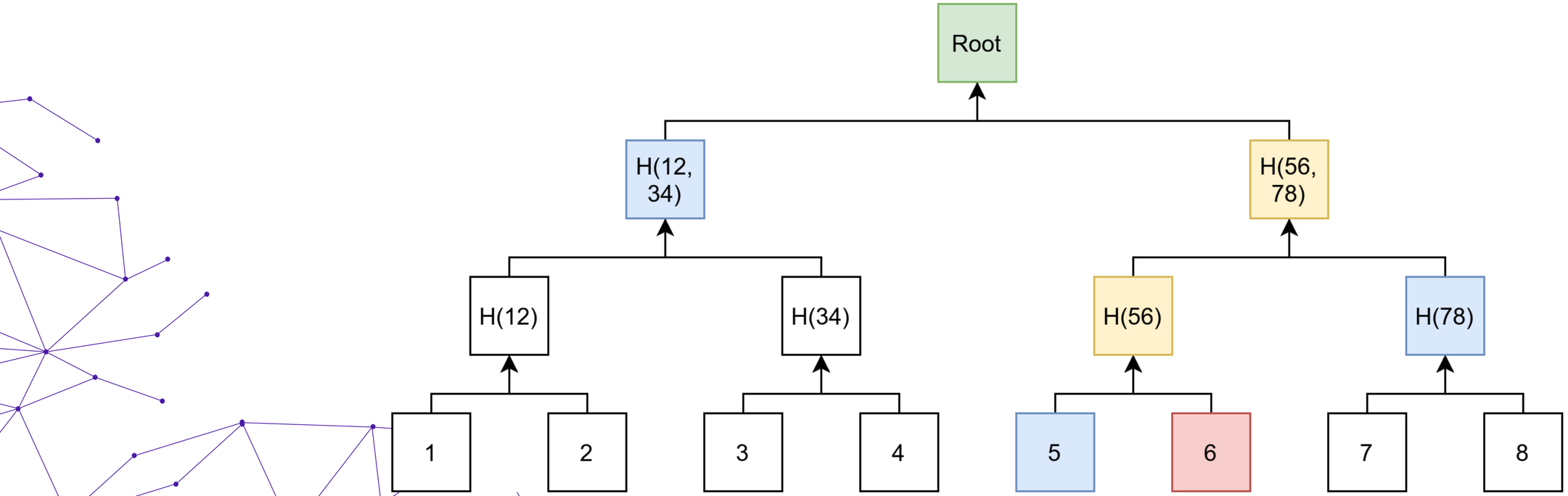
Questions?

irene.giacomelli@protocol.ai
cryptonet.org

Recall: commitment scheme used in Filecoin

How do we commit? Using Merkle-Trees (MT)

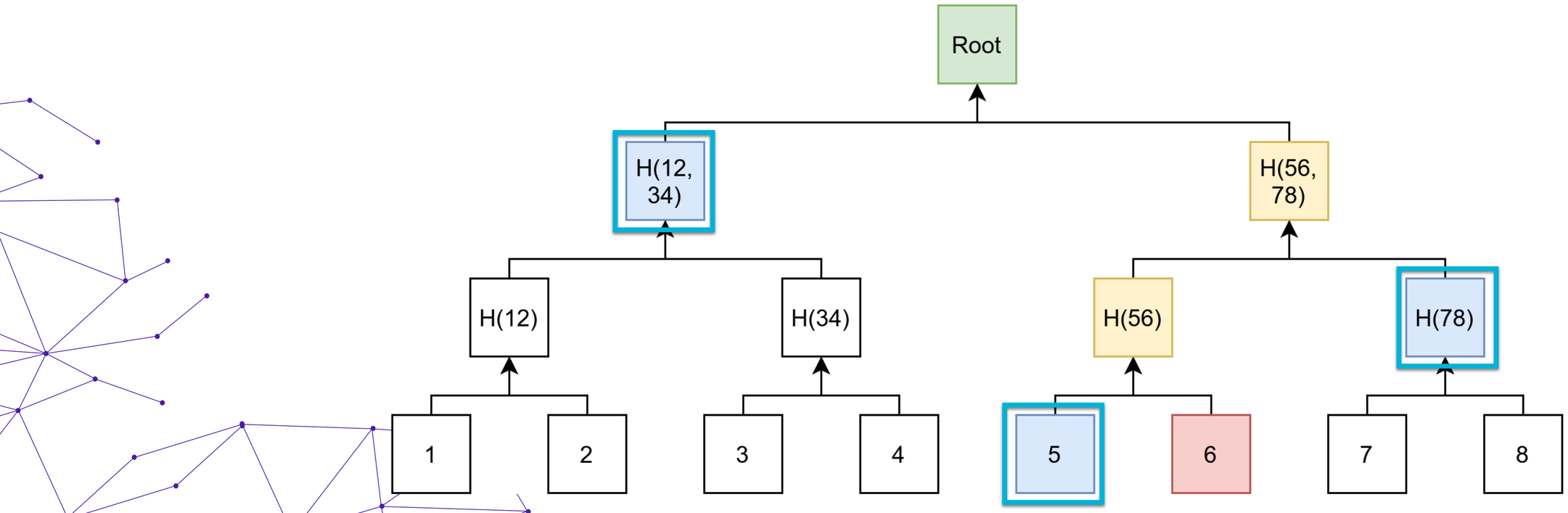
Root = Commitment (eg, Com(D) or Com(R))



Recall: commitment scheme used in Filecoin

How do we commit? Using Merkle-Trees (MT)

Root = Commitment (eg, Com(D) or Com(R))



Blue values = proof that 6th value is correct respect to the commitment

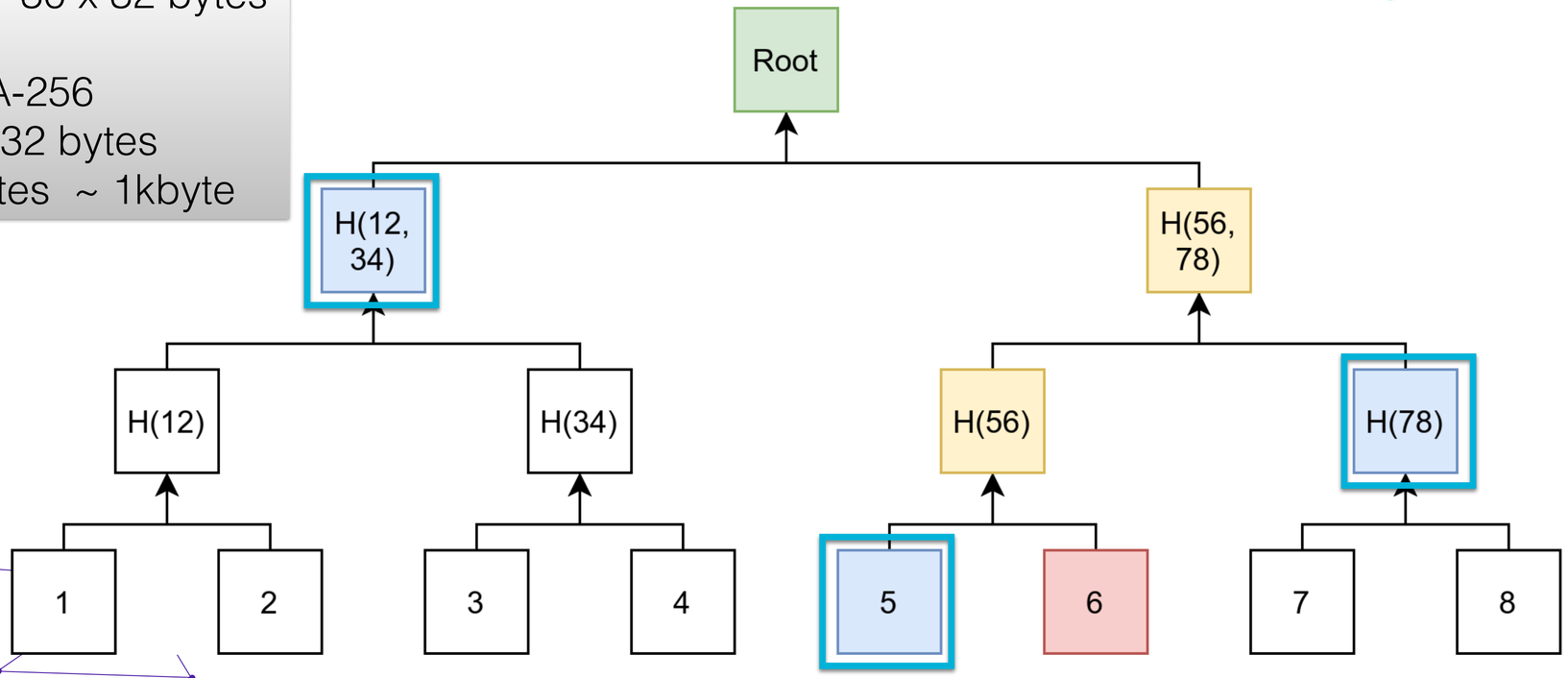
Recall: commitment scheme used in Filecoin

How do we commit? Using Merkle-Trees (MT)

Size of D = 32 GiB = 2^30 x 32 bytes

Take H = SHA-256
1 commitment = 32 bytes
1 proof = 30 x 32 bytes ~ 1kbyte

Root = Commitment (eg, Com(D) or Com(R))



Blue values = proof that 6th value is correct respect to the commitment