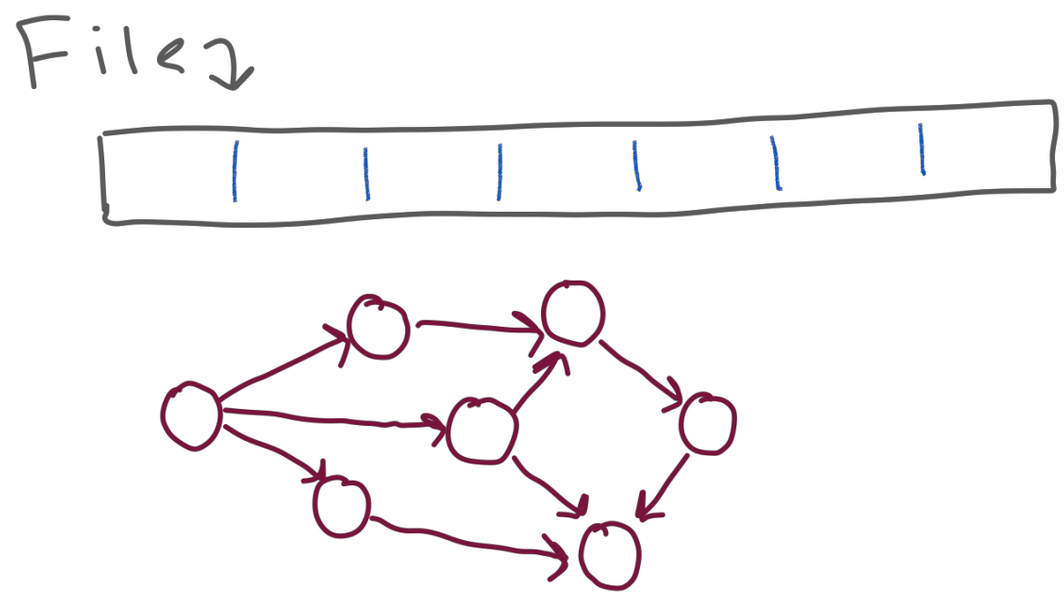
VDFs and Filecoin

Exploring how Filecoin might use Verifiable Delay Functions

Areas of Exploration

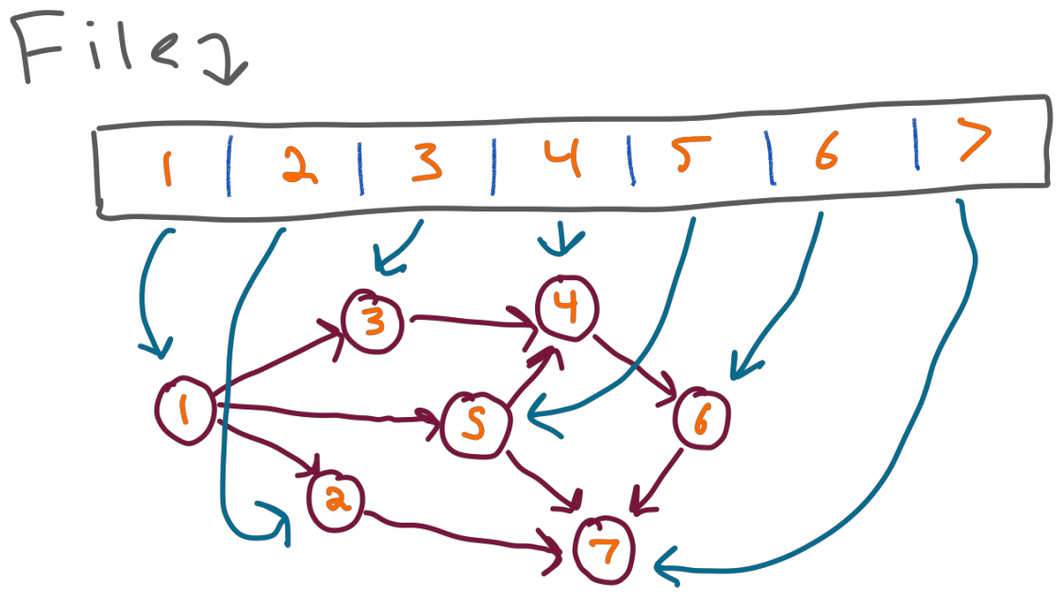
- Proof of Replication
- Proof of Space Time
- Expected Consensus

Proof of Replication



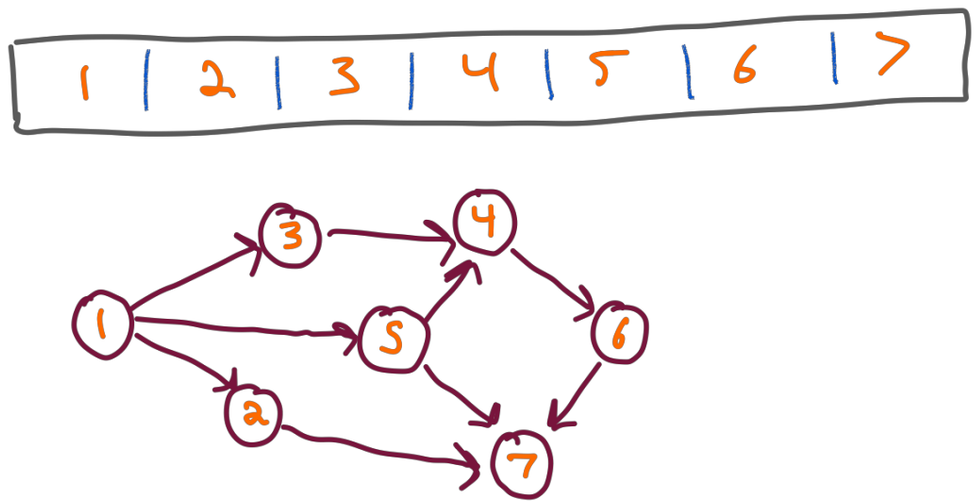
- A slow, unique encoding of some input data (any data!)
- Protects against deduplication ‘attacks’
- In context of PoSt, protects against generation attacks

Proof of Replication

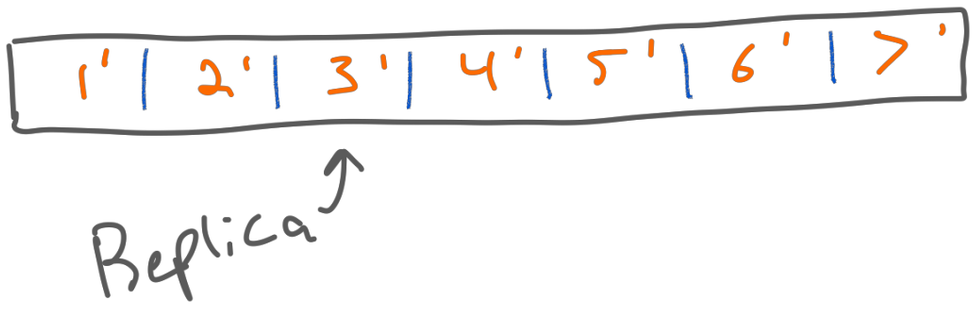


- A slow, unique encoding of some input data (any data!)
- Protects against deduplication ‘attacks’
- In context of PoSt, protects against generation attacks

Proof of Replication

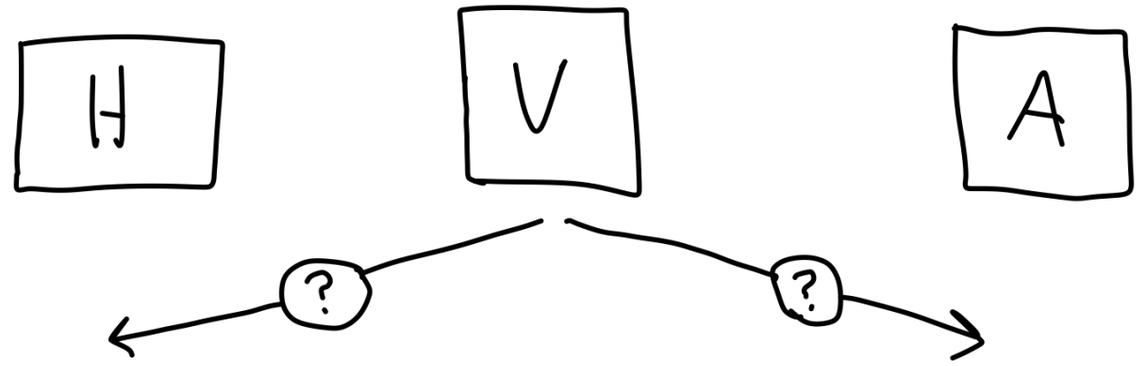


- A slow, unique encoding of some input data (any data!)
- Protects against deduplication ‘attacks’
- In context of PoSt, protects against generation attacks



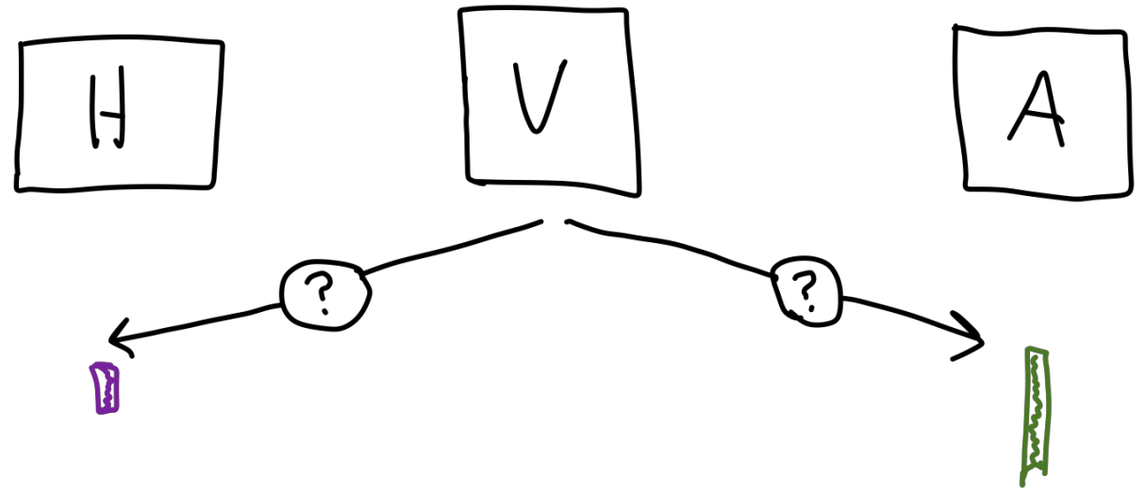
Proof of Replication

- VDFs in PoRep help protect against ‘generation attacks’ in PoSt



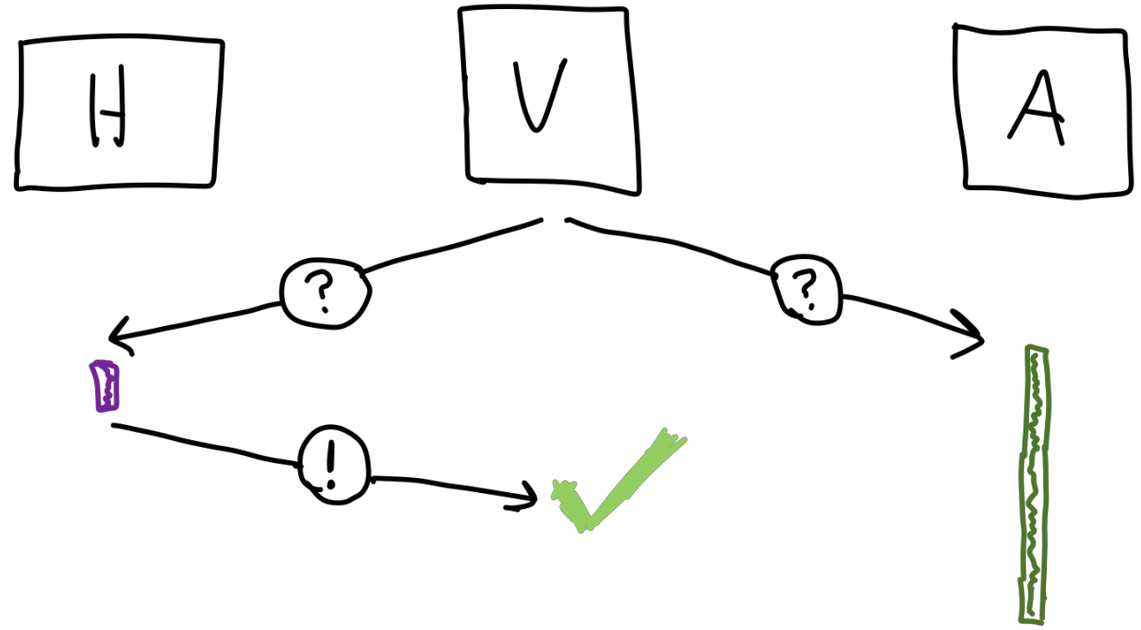
Proof of Replication

- VDFs in PoRep help protect against ‘generation attacks’ in PoSt



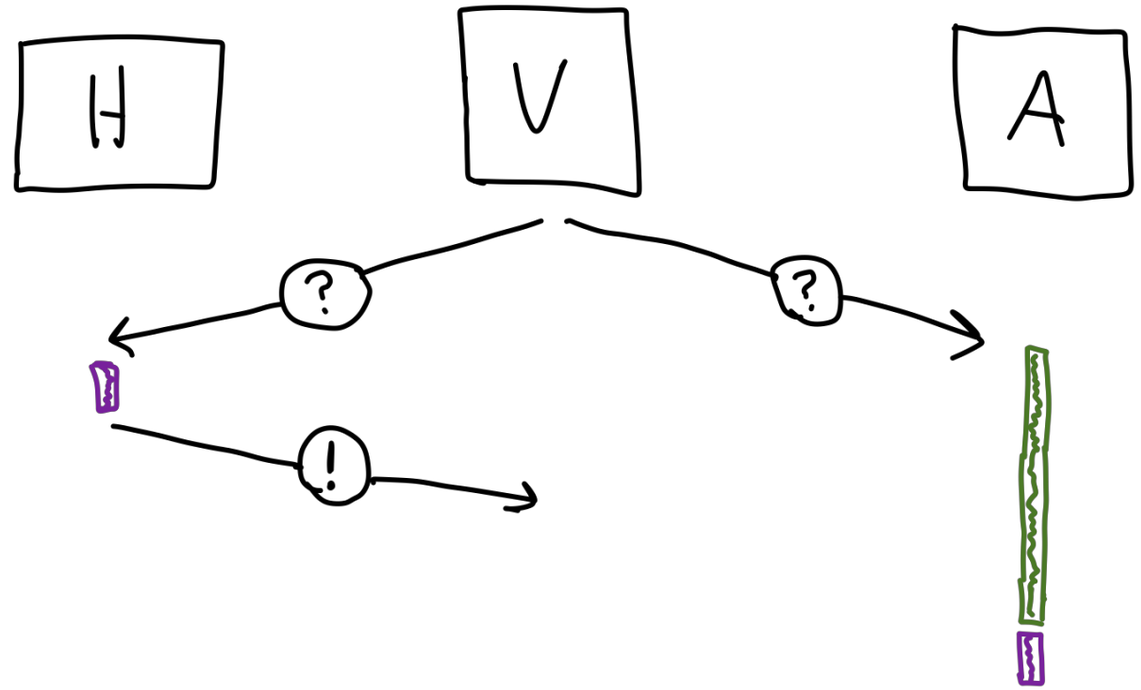
Proof of Replication

- VDFs in PoRep help protect against ‘generation attacks’ in PoSt



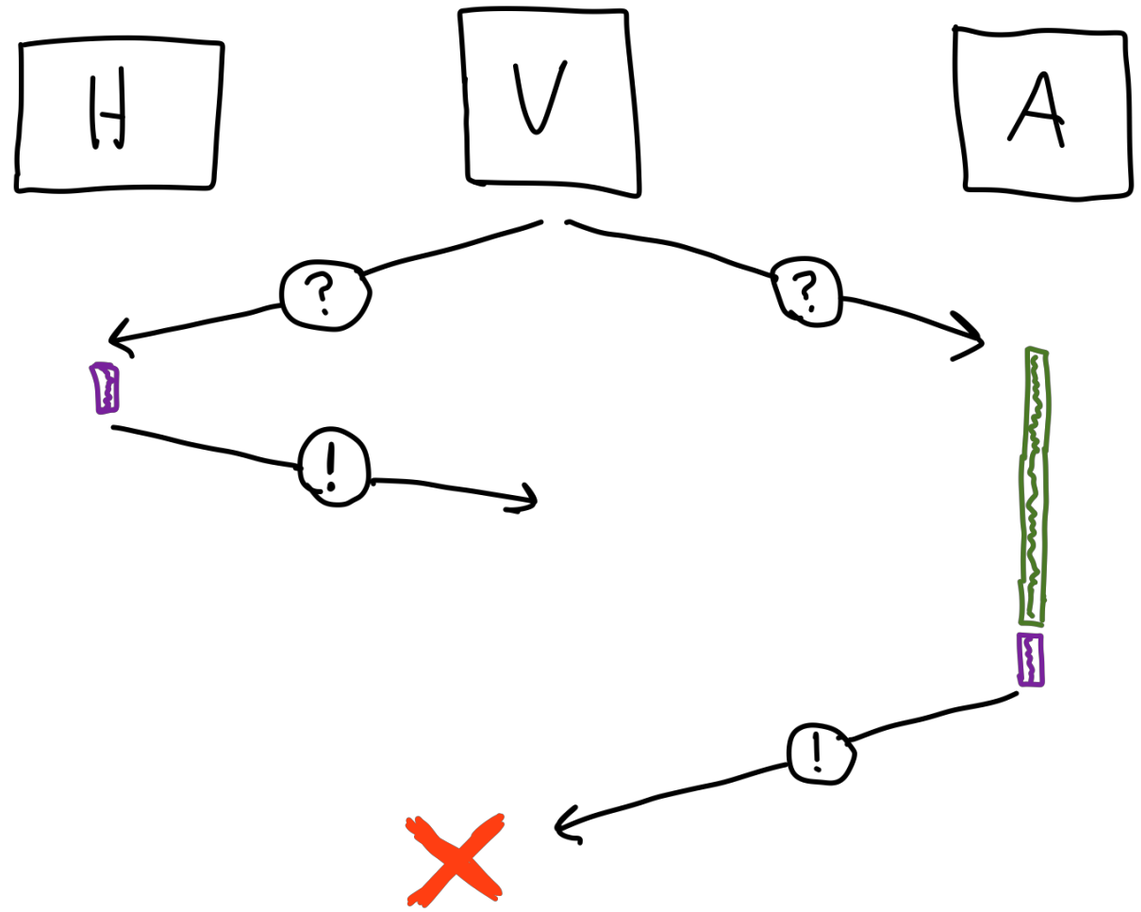
Proof of Replication

- VDFs in PoRep help protect against ‘generation attacks’ in PoSt



Proof of Replication

- VDFs in PoRep help protect against ‘generation attacks’ in PoSt



PoRep is a VDF

PoRep is a VDF

PoRep is a VDF

How?

- Takes some inputs, produces an output after a prescribed time

How?

- Takes some inputs, produces an output after a prescribed time

- The same inputs should always produce the same output

How?

- Takes some inputs, produces an output after a prescribed time
- The same inputs should always produce the same output
- A verifier can efficiently check that the process was done correctly

Proof of SpaceTime

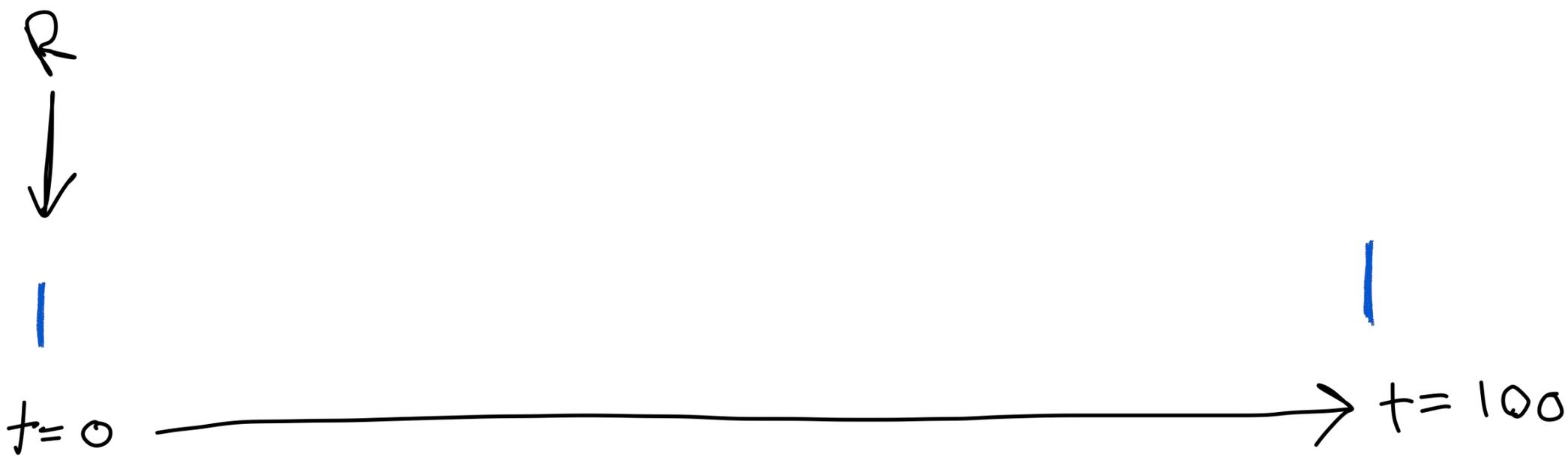
- Proves to the verifier that some known data was correctly stored over a given period of time.

- Ensures the space wasn’t used for storing anything else during the proof.

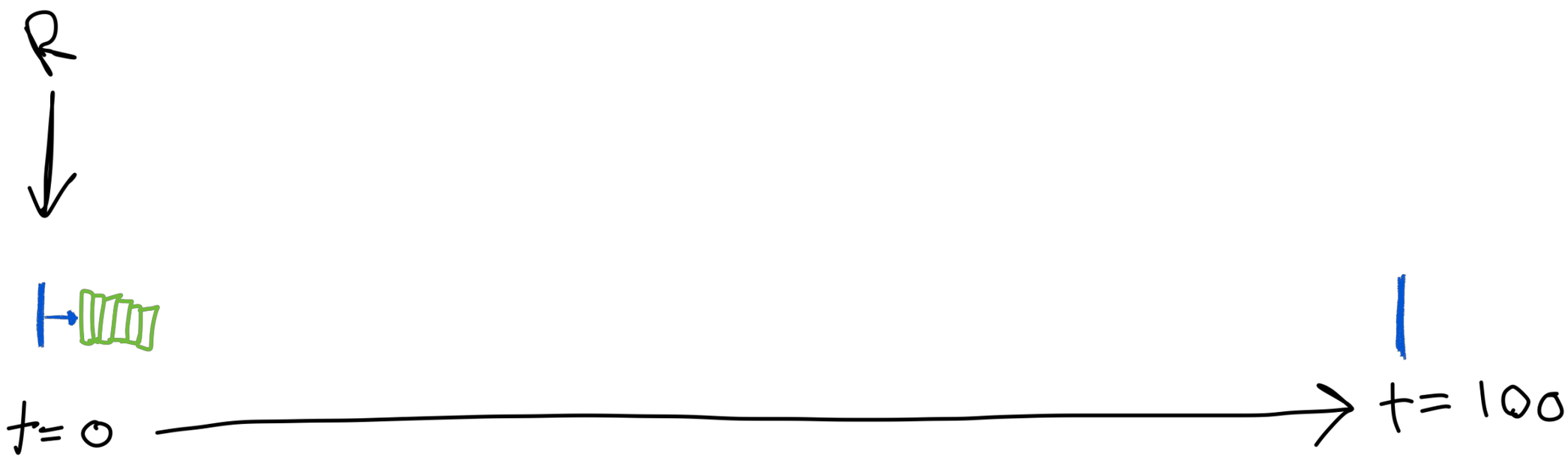
Proof of SpaceTime

- non-interactive, succinct output
- must not be computable too much faster than the expected duration

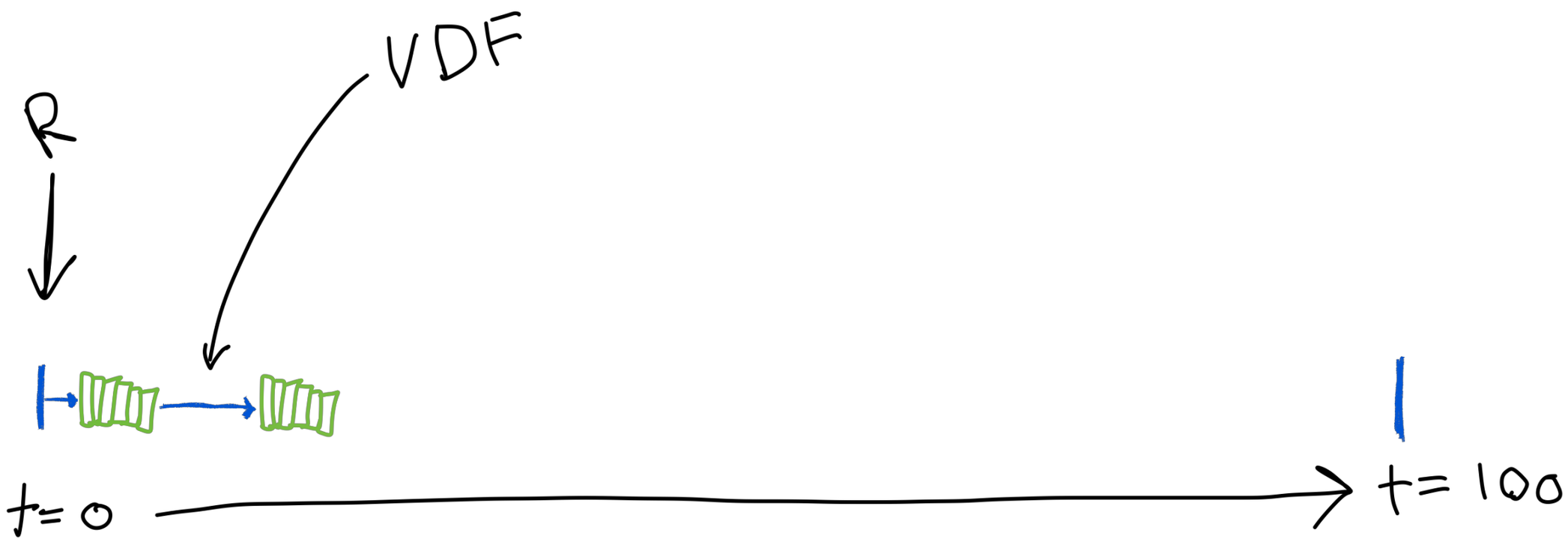
Proof of SpaceTime



Proof of SpaceTime

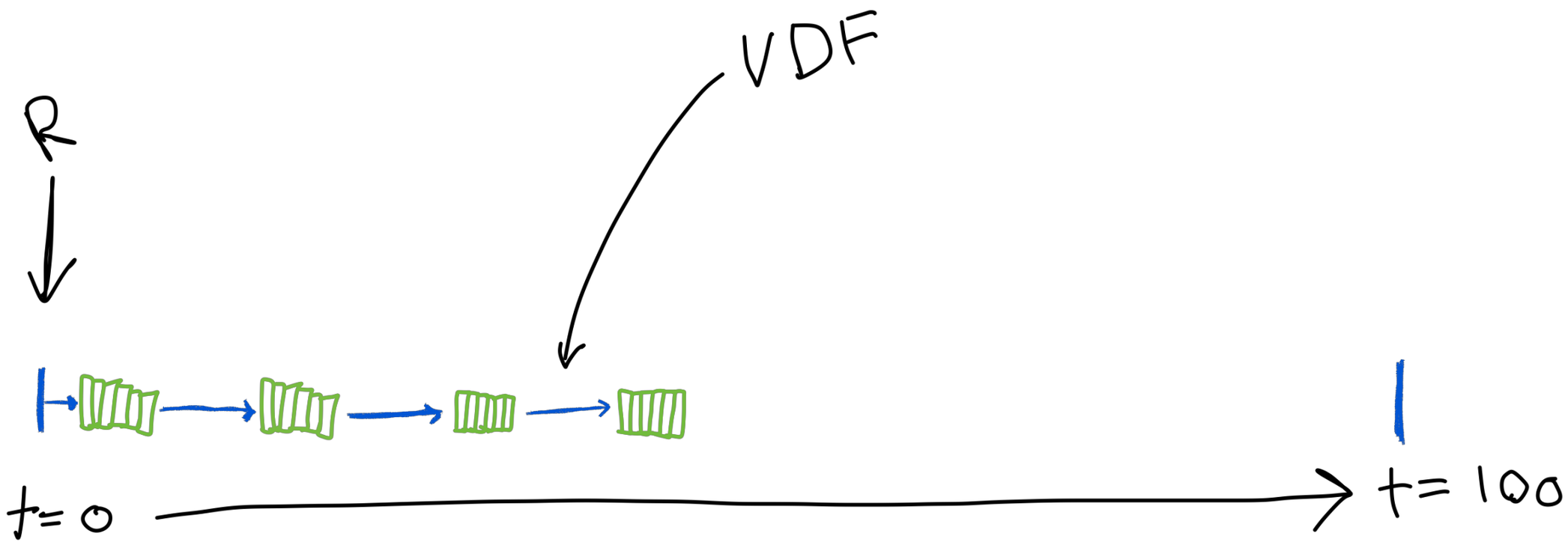


Proof of SpaceTime

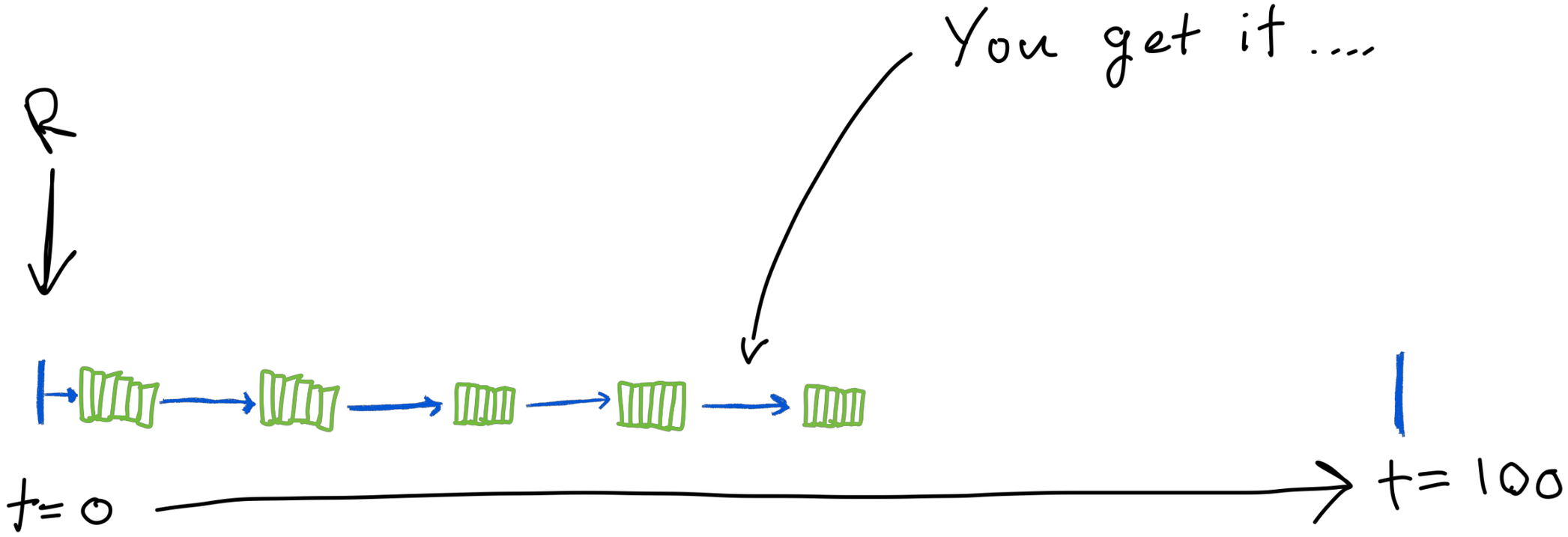


Proof of SpaceTime

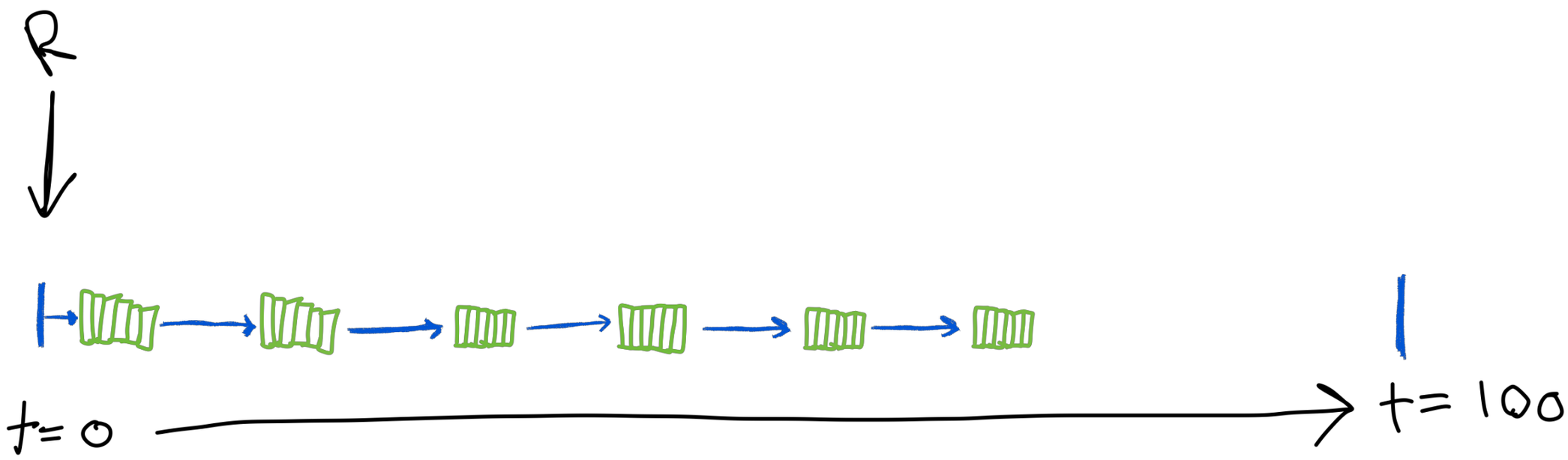
Proof of SpaceTime



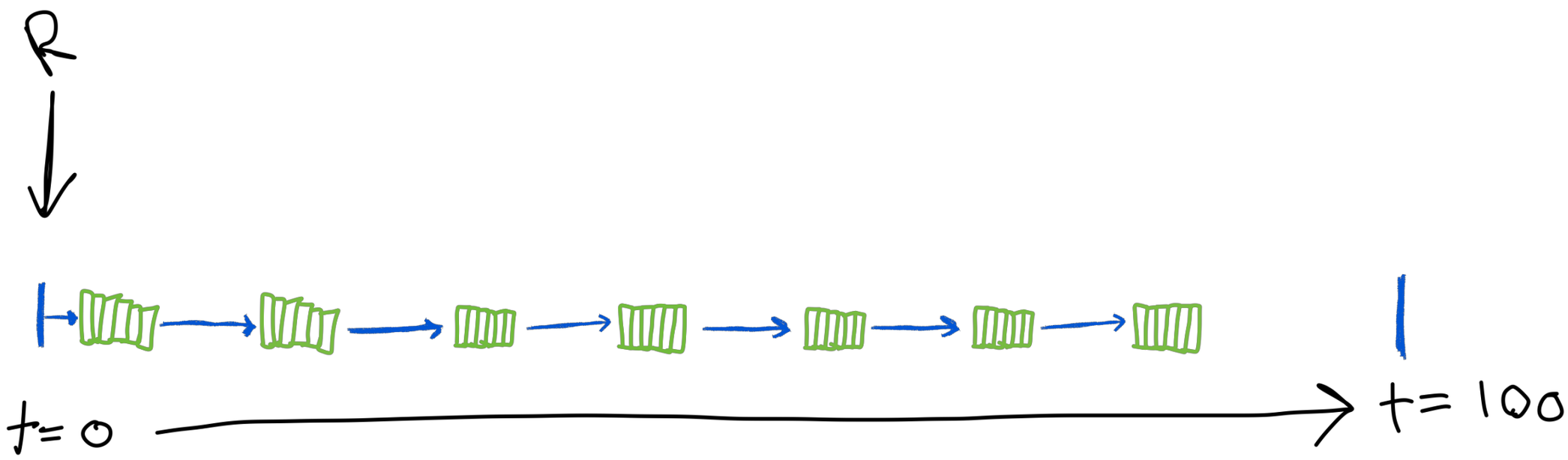
Proof of SpaceTime



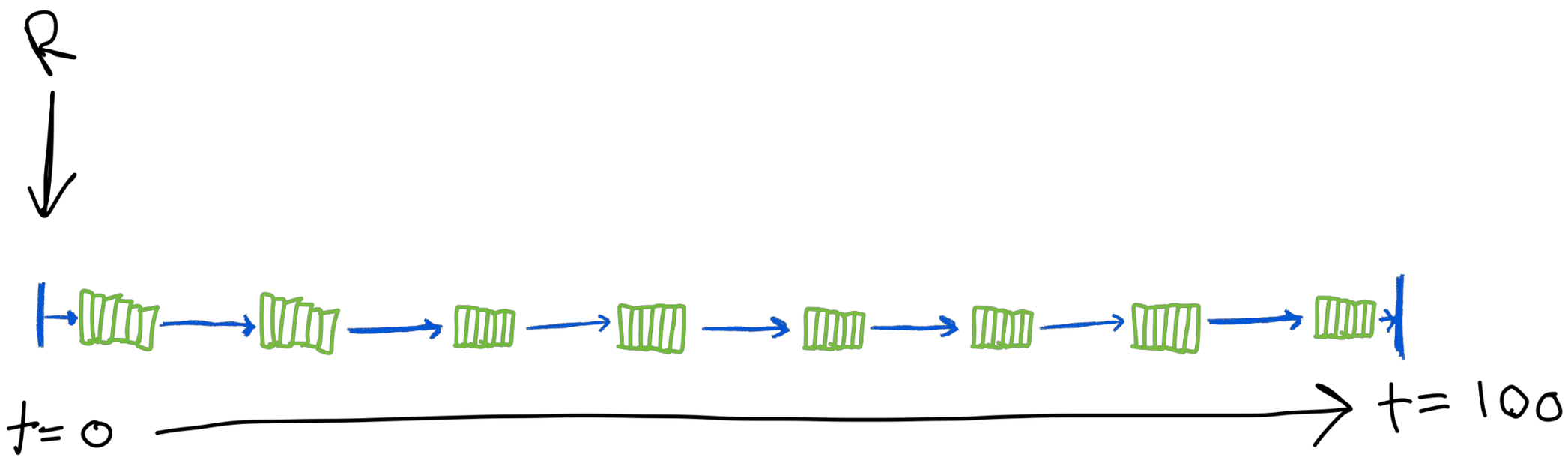
Proof of SpaceTime



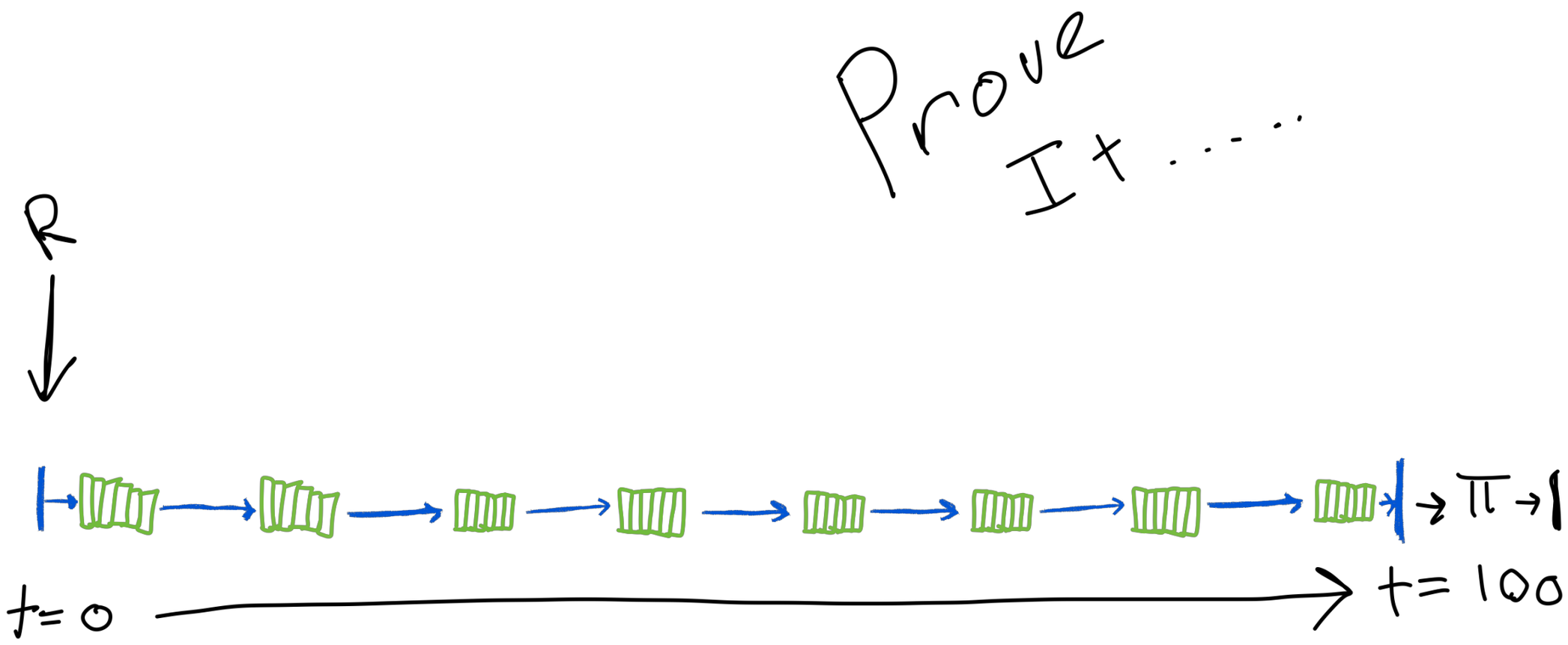
Proof of SpaceTime



Proof of SpaceTime

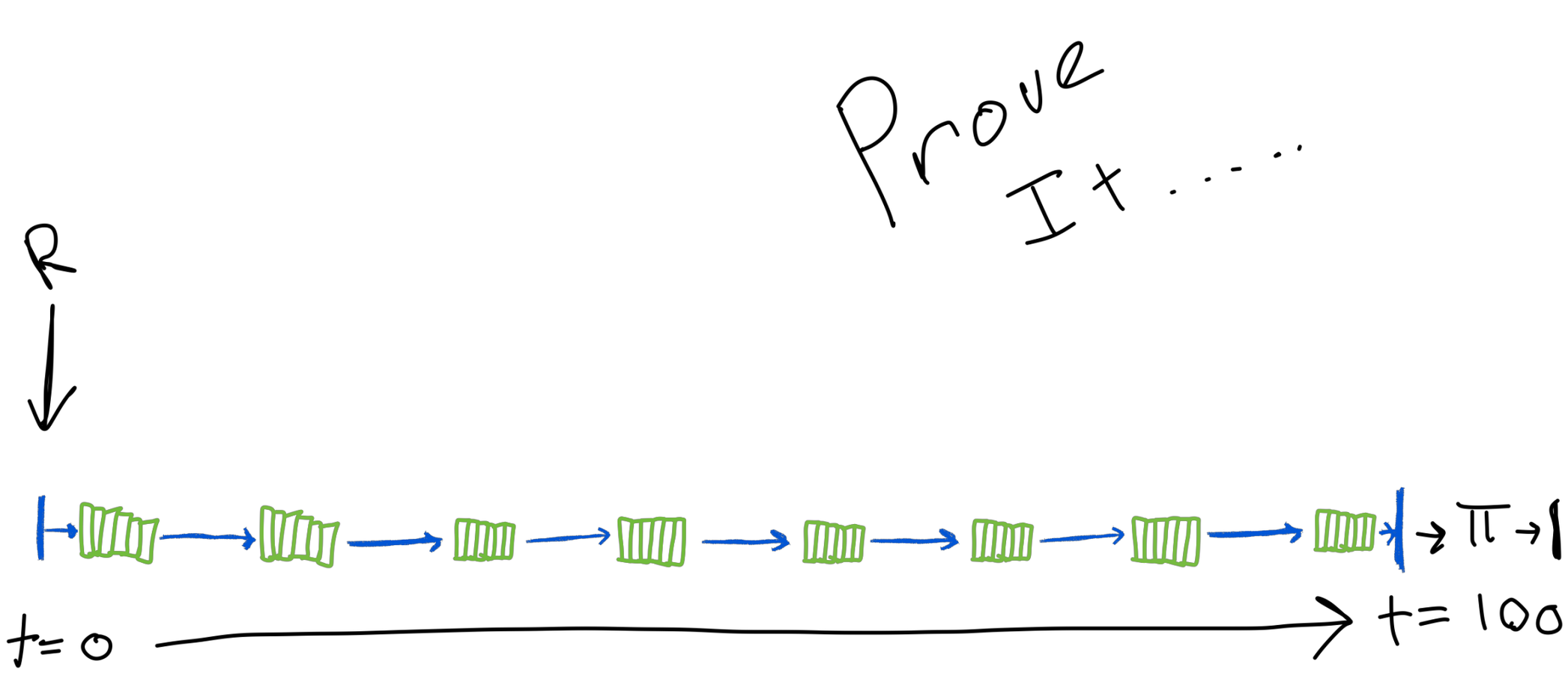


Proof of SpaceTime

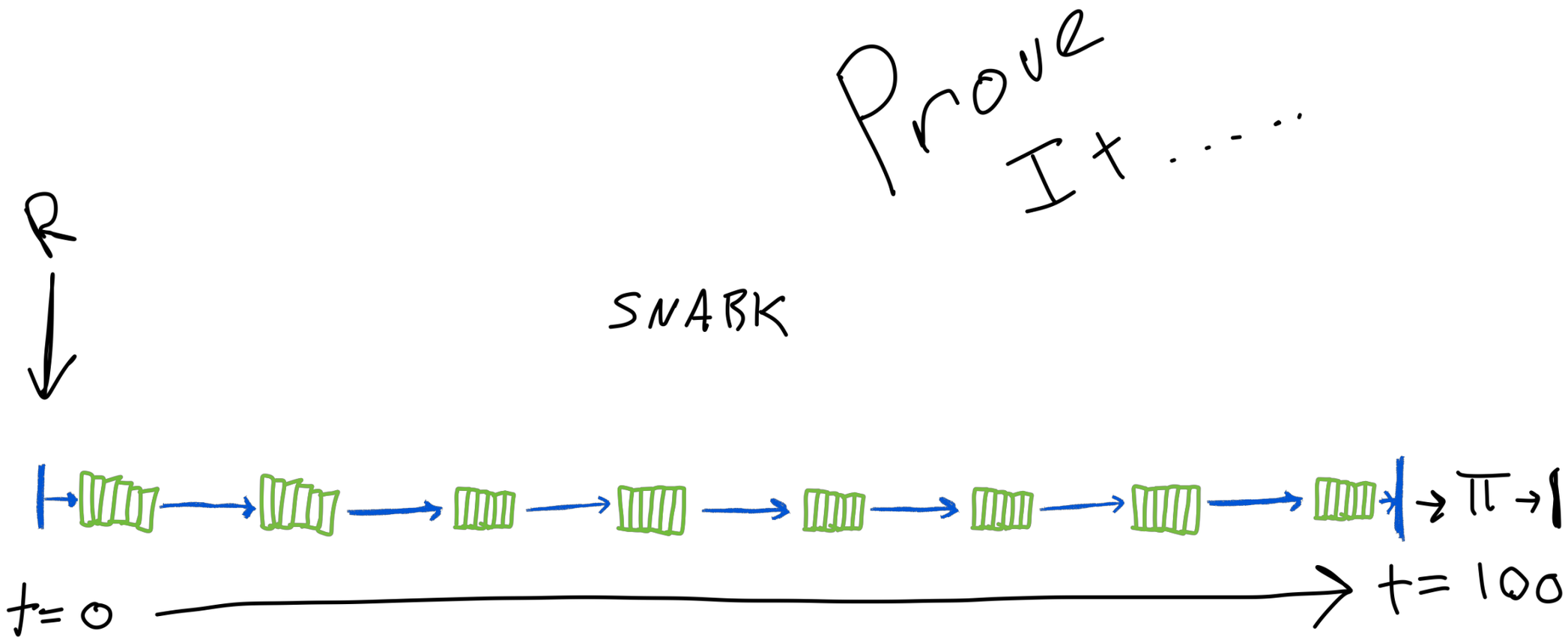


Proof of SpaceTime

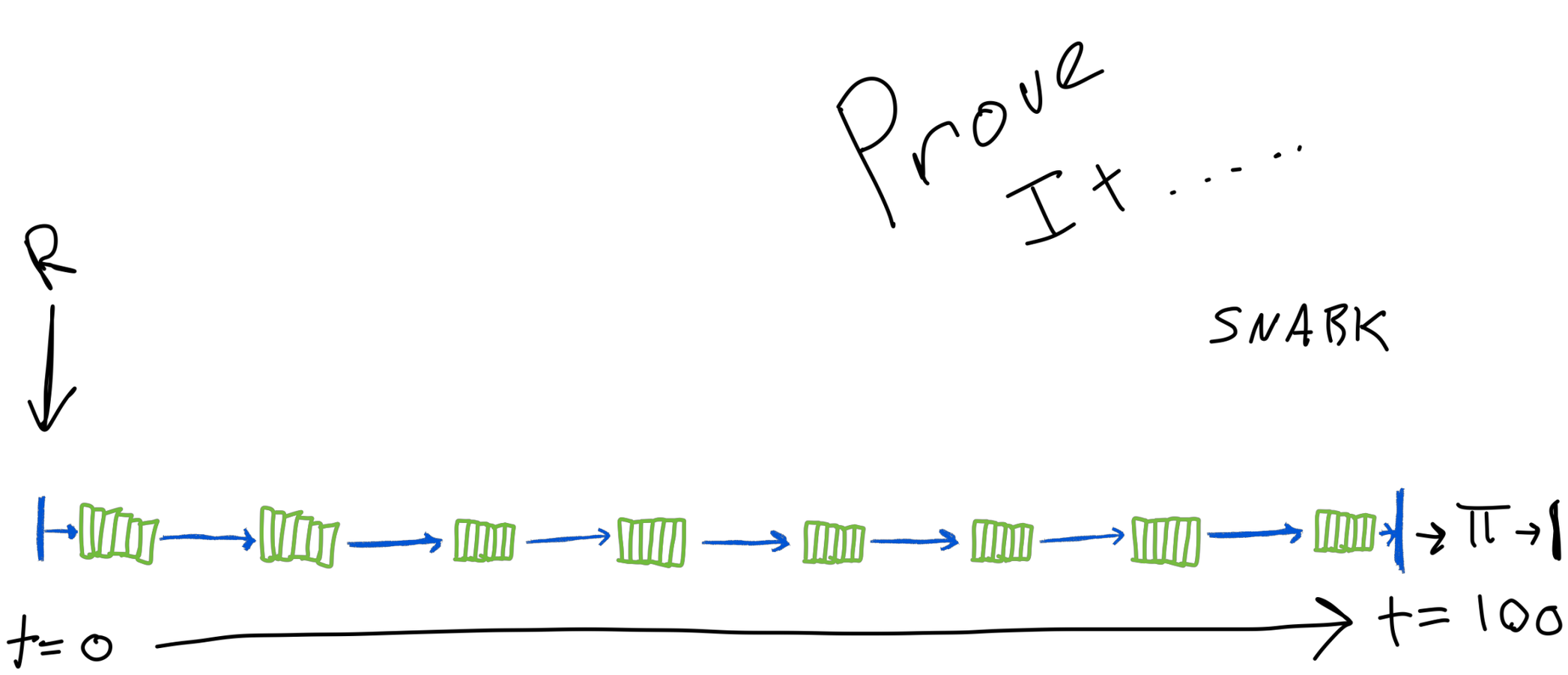
SNARK



Proof of SpaceTime

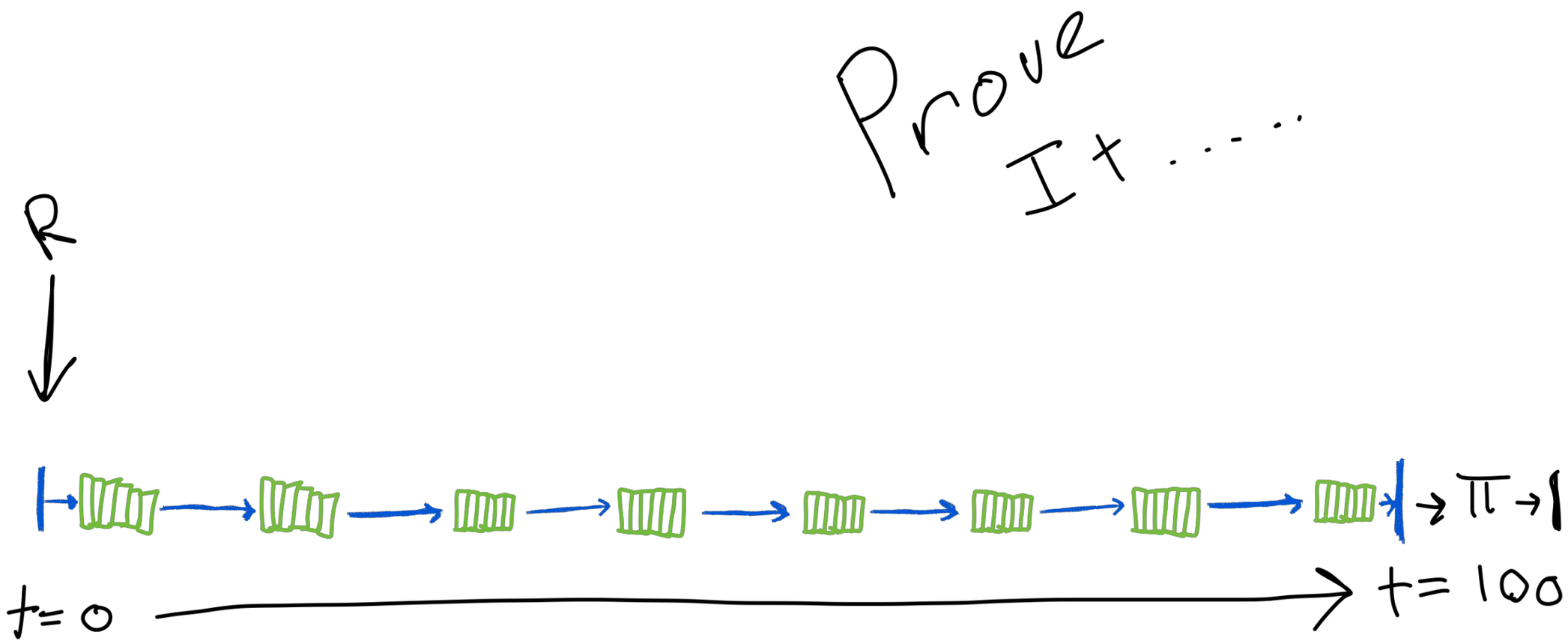


Proof of SpaceTime

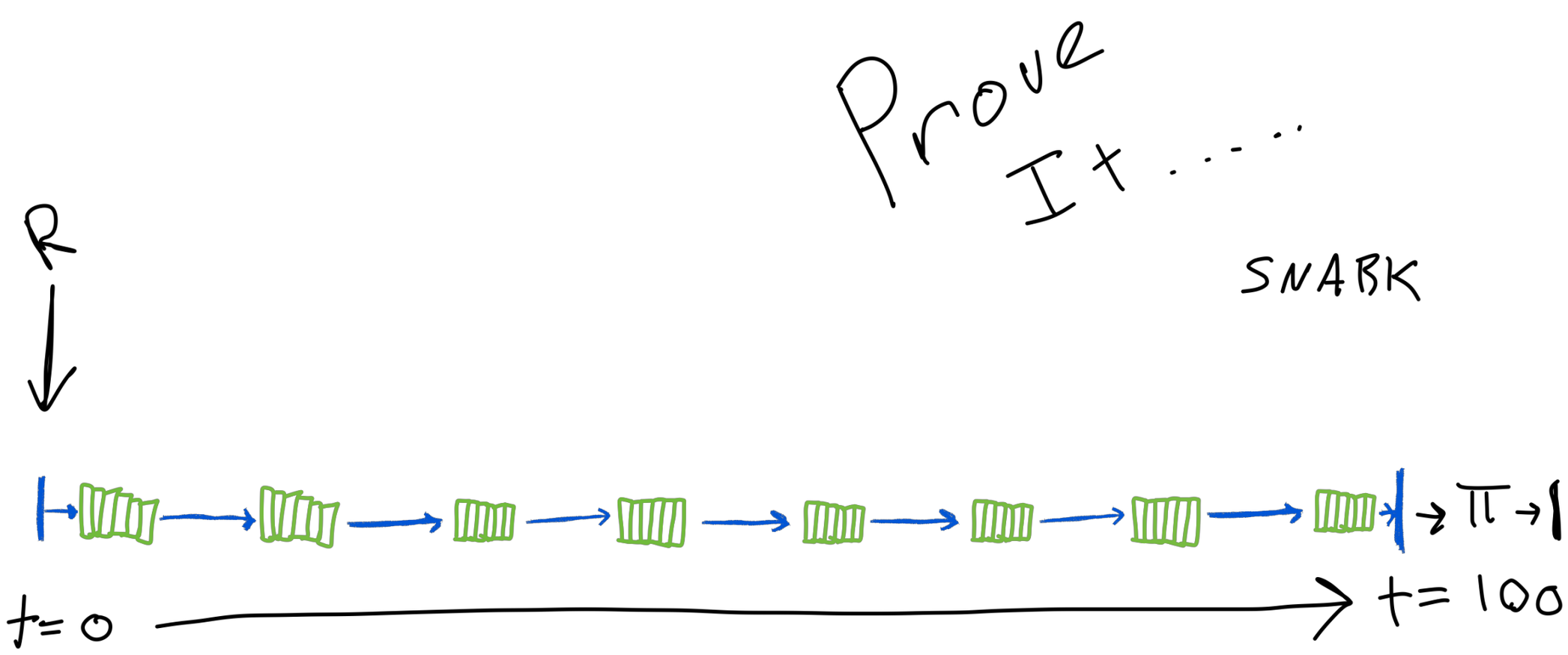


Proof of SpaceTime

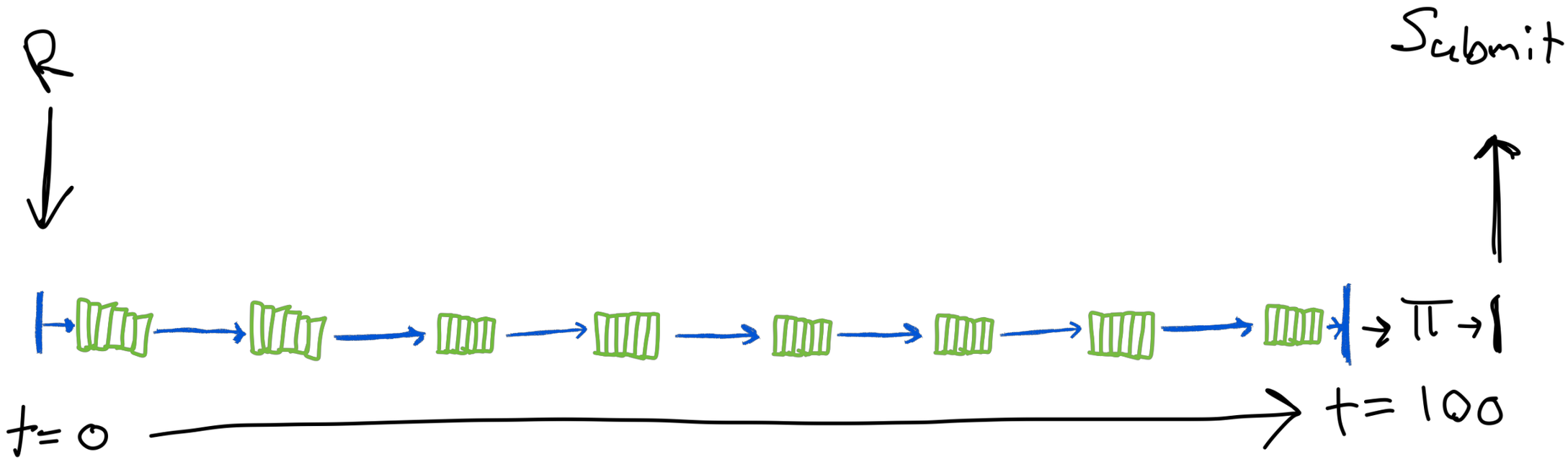
SNARK



Proof of SpaceTime

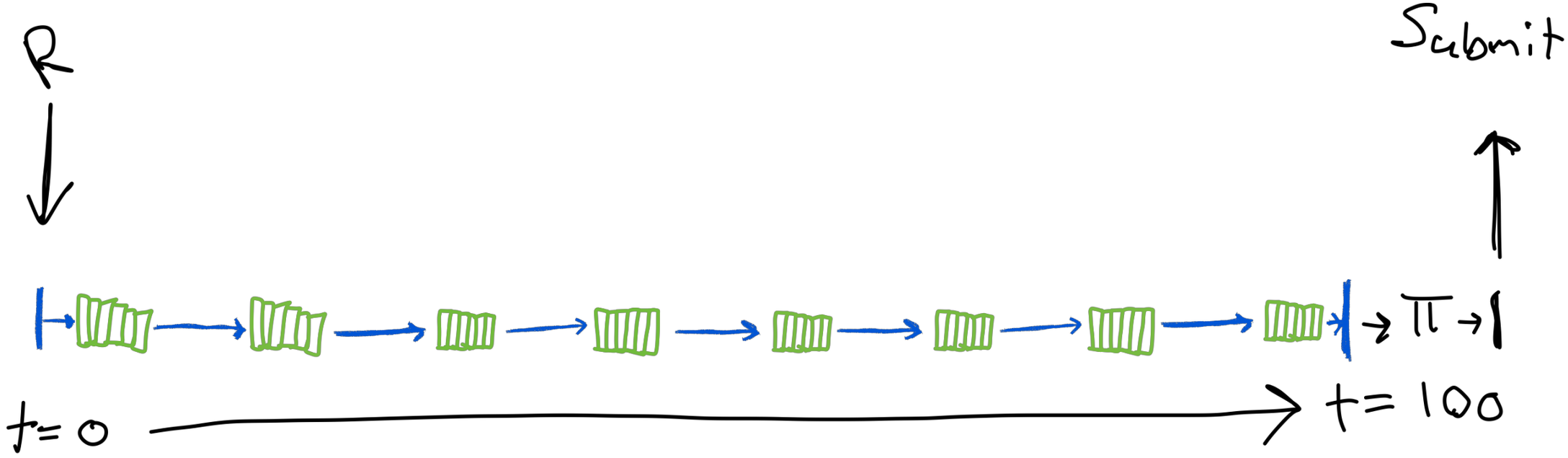


Proof of SpaceTime

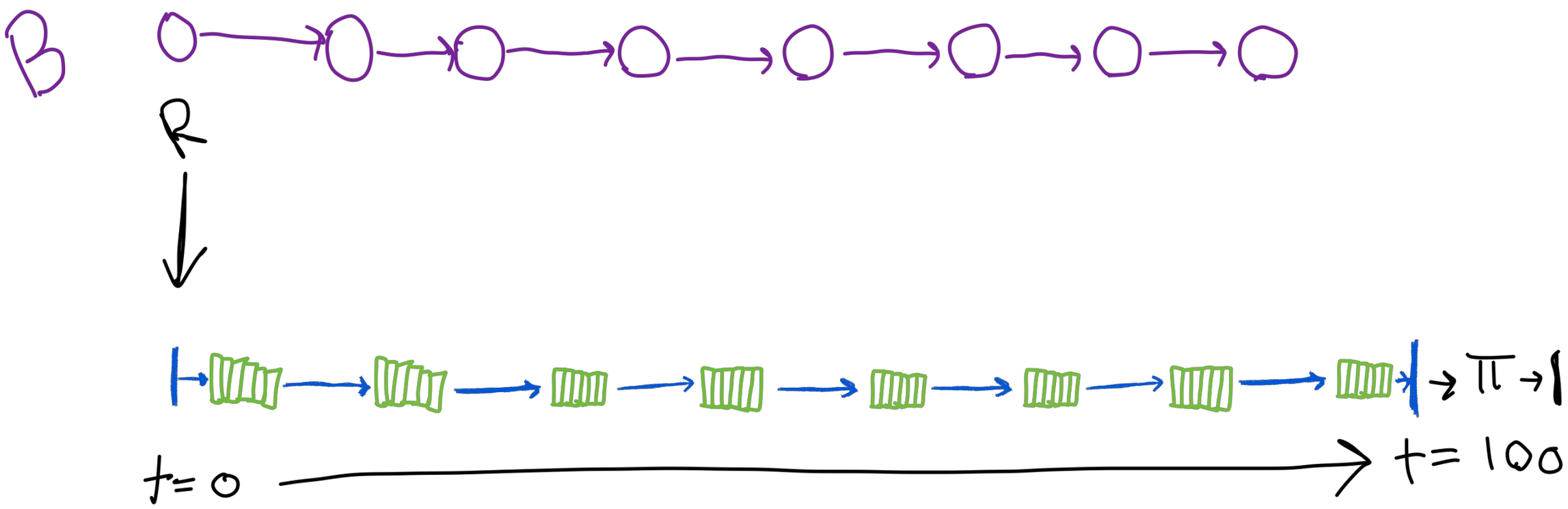


Proof of SpaceTime

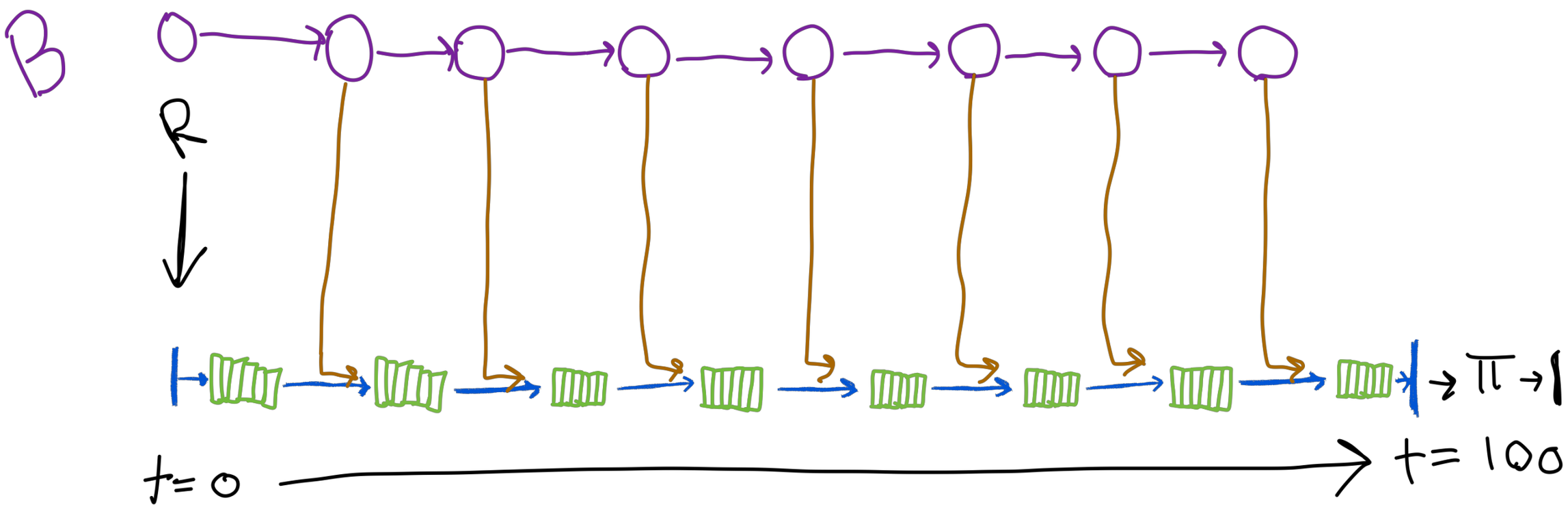
What Else?



Proof of SpaceTime



Proof of SpaceTime



Expected Consensus

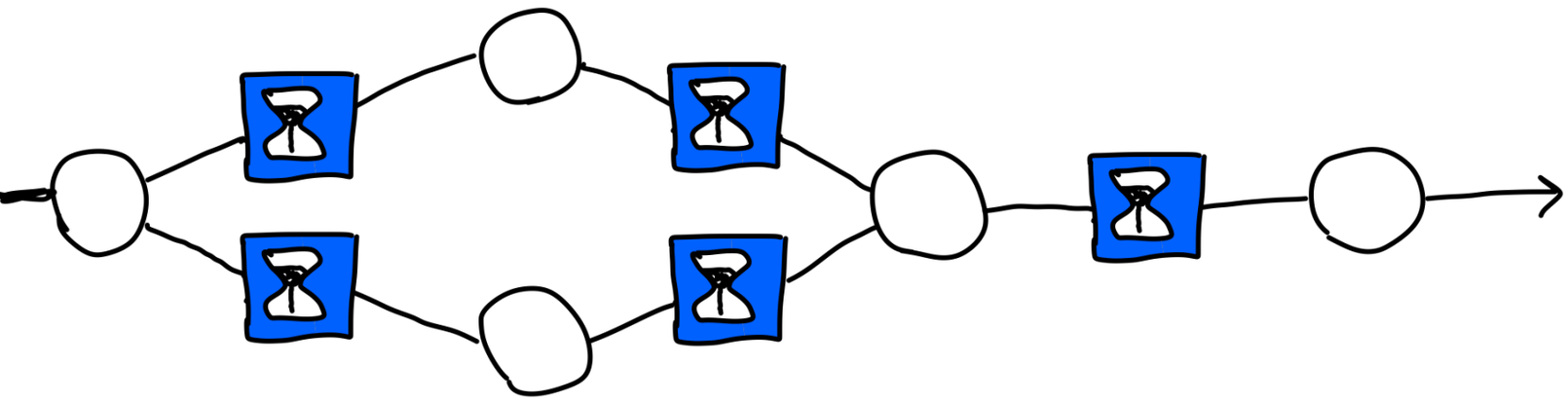
- Filecoin Consensus Mechanism

- Elects on ***expectation*** one leader per round

- Include all blocks from previous round as parents

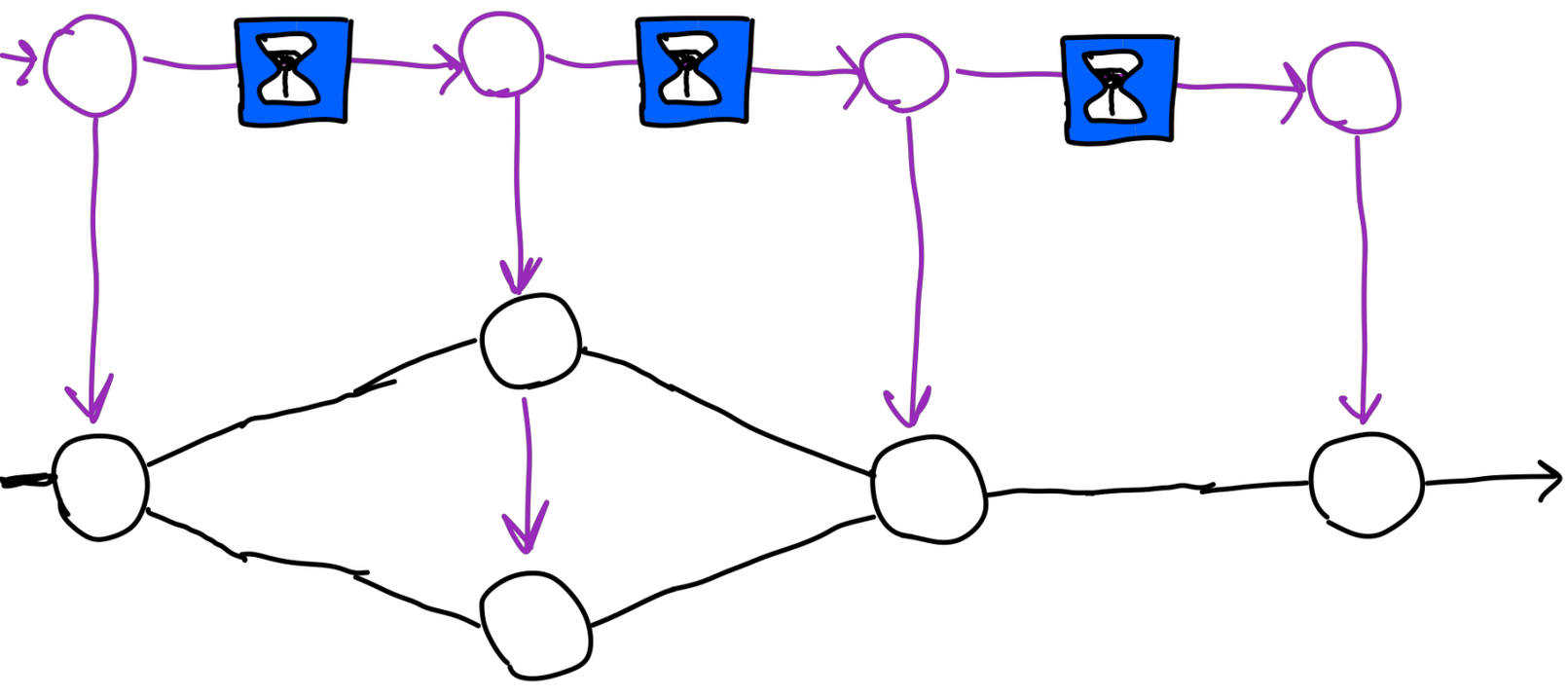
Expected Consensus

- Maybe use VDF for enforcing block delays



Expected Consensus

- Alternatively... Use a random beacon for enforcing delay



Thank You!

@whyrusleeping