SpaceMint

Overcoming Bitcoin's waste of energy

Georg Fuchsbauer

joint work with

S. Park, **A. Kwon**, **K. Pietrzak**, **J. Alwen** and **P. Gaži**

Journées nationales pré-GDR SI 31/05/17

Overview

1. **Bitcoin**
   - Transactions
   - Blockchain
   - Proof of work
   - Problems with PoW
2. **SpaceMint**
   - Proofs of space
   - Issues with PoSp
   - New blockchain format

Bitcoin

- Digital currency
- Decentralized (no bank issuing coins)
- Pseudonymous
- Controled Inflation

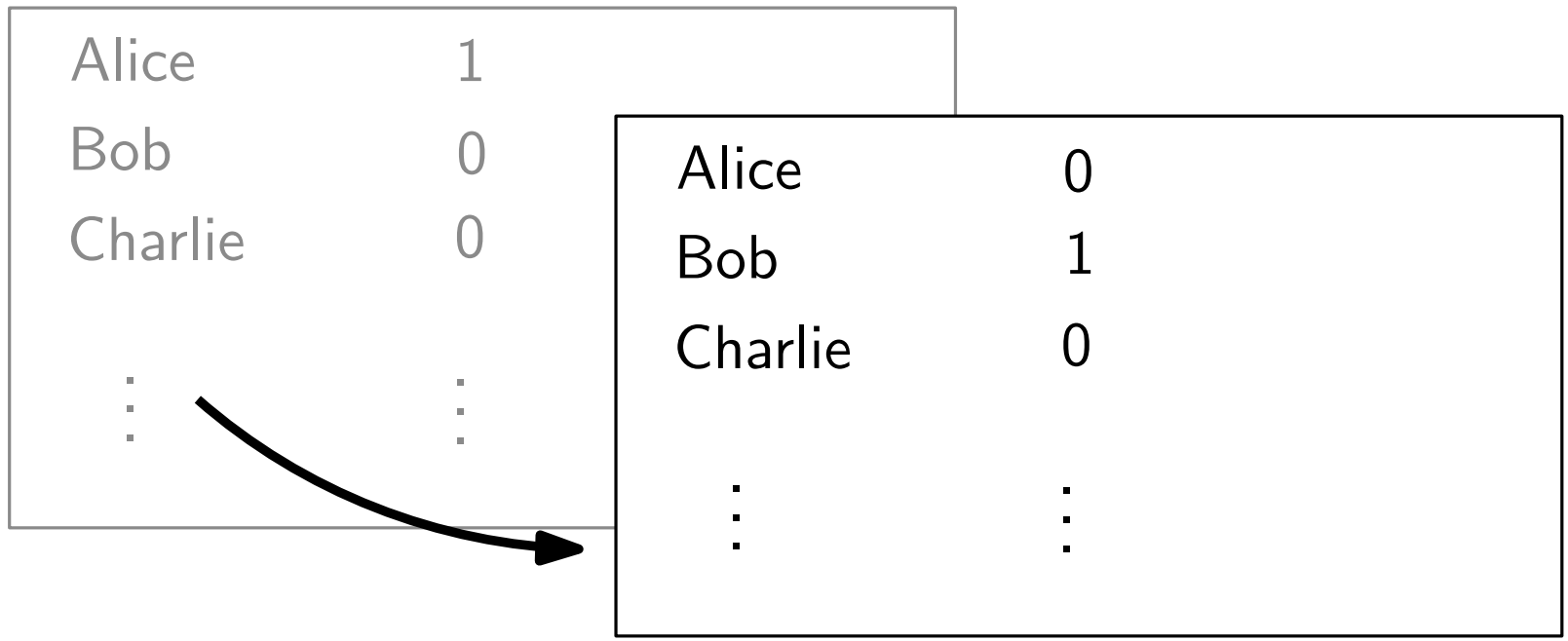
Ledger

Public ledger (maintained by authority)

Alice	1
Bob	0
Charlie	0
⋮	⋮

Ledger

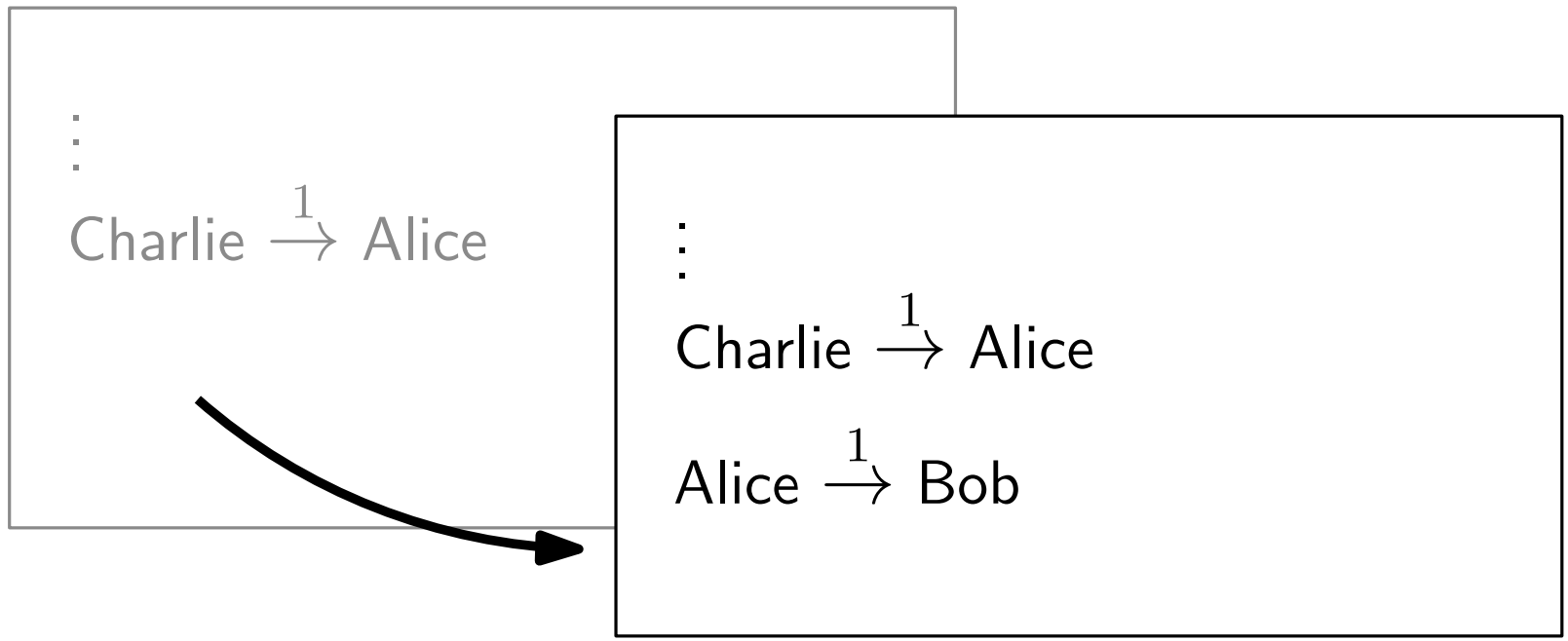
Public ledger



Alice: transfer 1 $\rightarrow$ Bob

Ledger

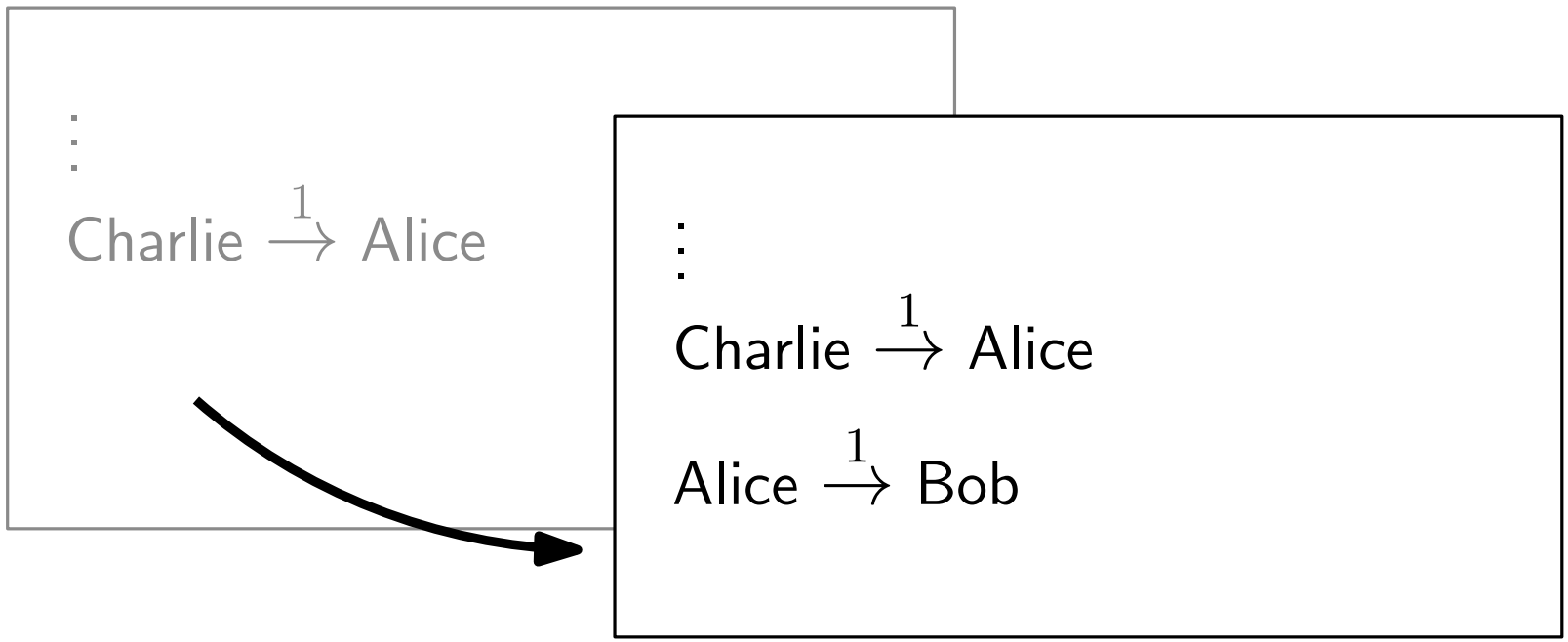
Public ledger (records all transactions)



Alice: transfer 1 $\rightarrow$ Bob

Ledger

Public ledger (records all transactions)



Alice: transfer 1 $\rightarrow$ Bob

how to identify?

Digital signatures

- Alice can create a **key pair**
  - **private key** used to sign messages
  - **public key** lets anyone verify signatures

Digital signatures

- Alice can create a **key pair**
  - **private key** used to sign messages
  - **public key** lets anyone verify signatures
- **Unforgeability**: no one can forge signature w/o knowing secret key

Digital signatures

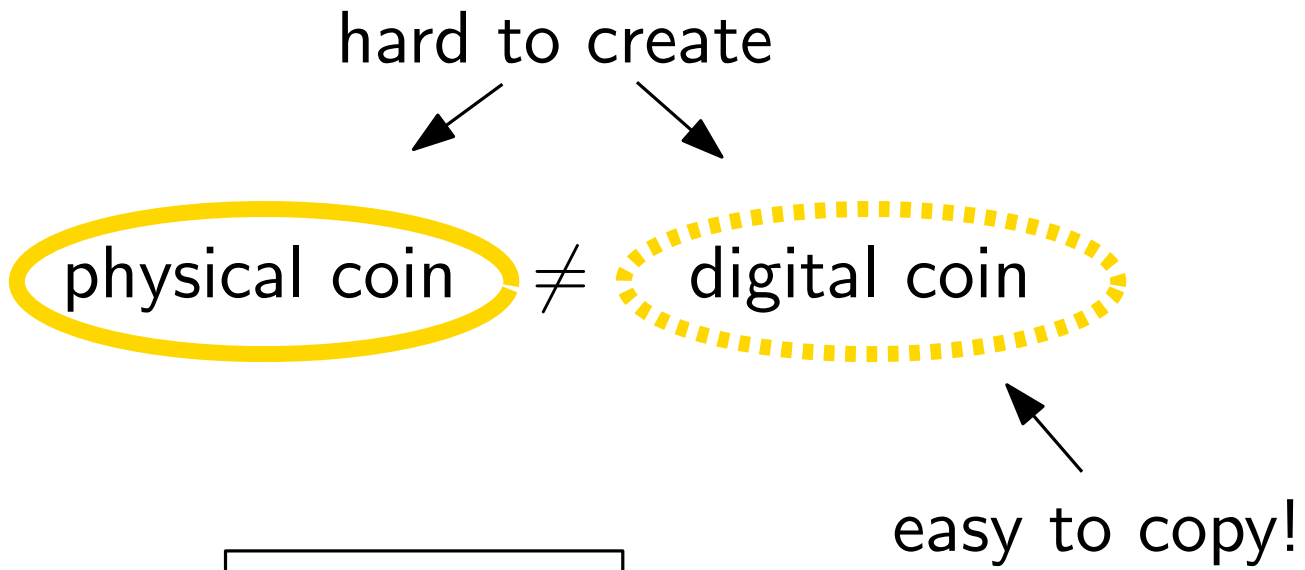
- Alice can create a **key pair**
  - **private key** used to sign messages
  - **public key** lets anyone verify signatures
- **Unforgeability**: no one can forge signature w/o knowing secret key

- Public key $\leftrightarrow$ coin
- Private key: enables spending of coin

Transactions

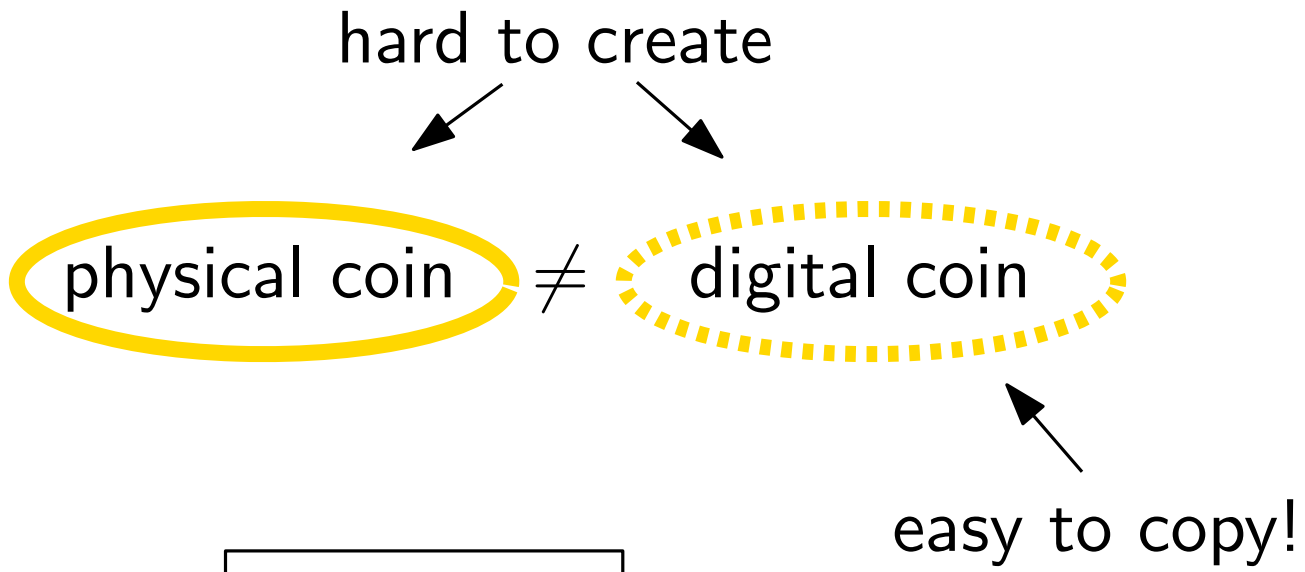
- Alice owns $\boxed{pk_A}$ i.e. it's in the ledger
- Bob creates $\boxed{pk_B}$
- Alice signs $\boxed{pk_A \rightarrow pk_B}$ and adds to ledger

Double-spending



- Alice signs $\boxed{pk_A \rightarrow pk_B}$
- Alice signs $\boxed{pk_A \rightarrow pk_C}$

Double-spending



- Alice signs $pk_A \rightarrow pk_B$
- Alice signs $pk_A \rightarrow pk_C$

Ledger only accepts if

- exists transaction $* \rightarrow pk_A$!
- no transaction ~~$pk_A \rightarrow *$~~

Decentralization

How to eliminate authority that

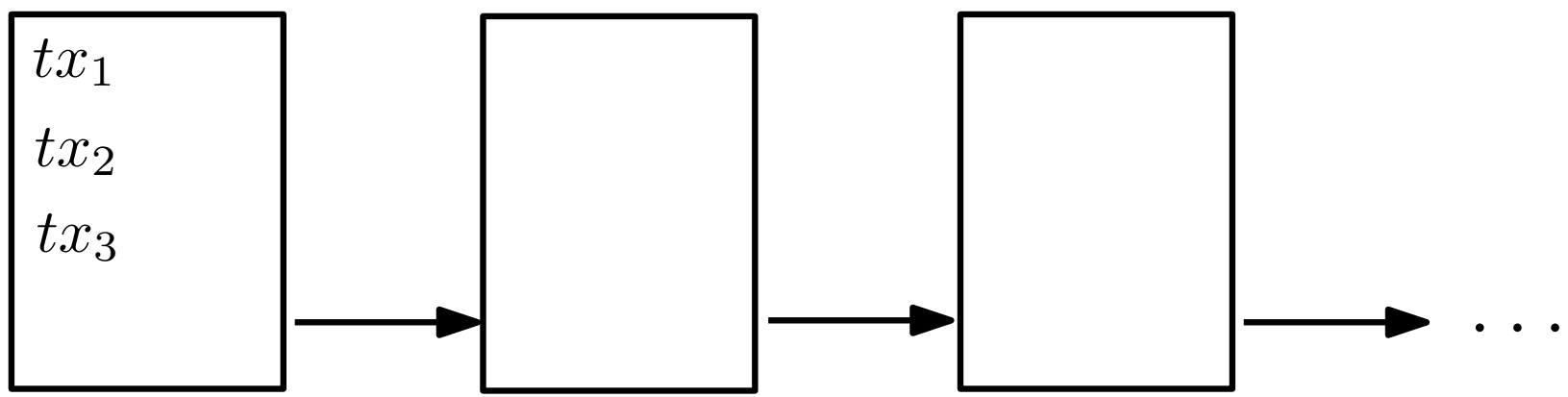
- checks validity of tx's
- publishes new tx's in ledger

Decentralization

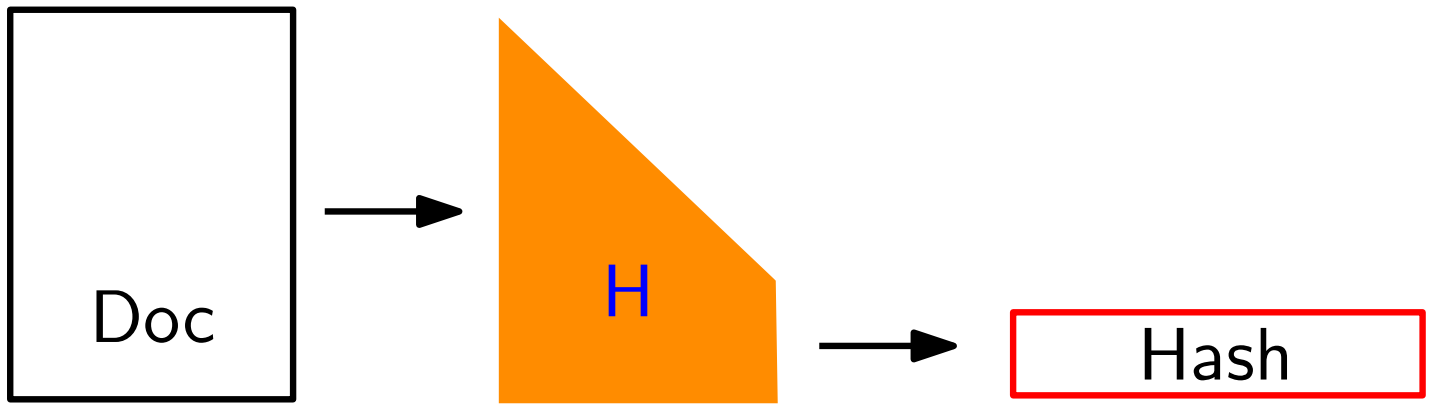
How to eliminate authority that

- checks validity of tx's
- publishes new tx's in ledger

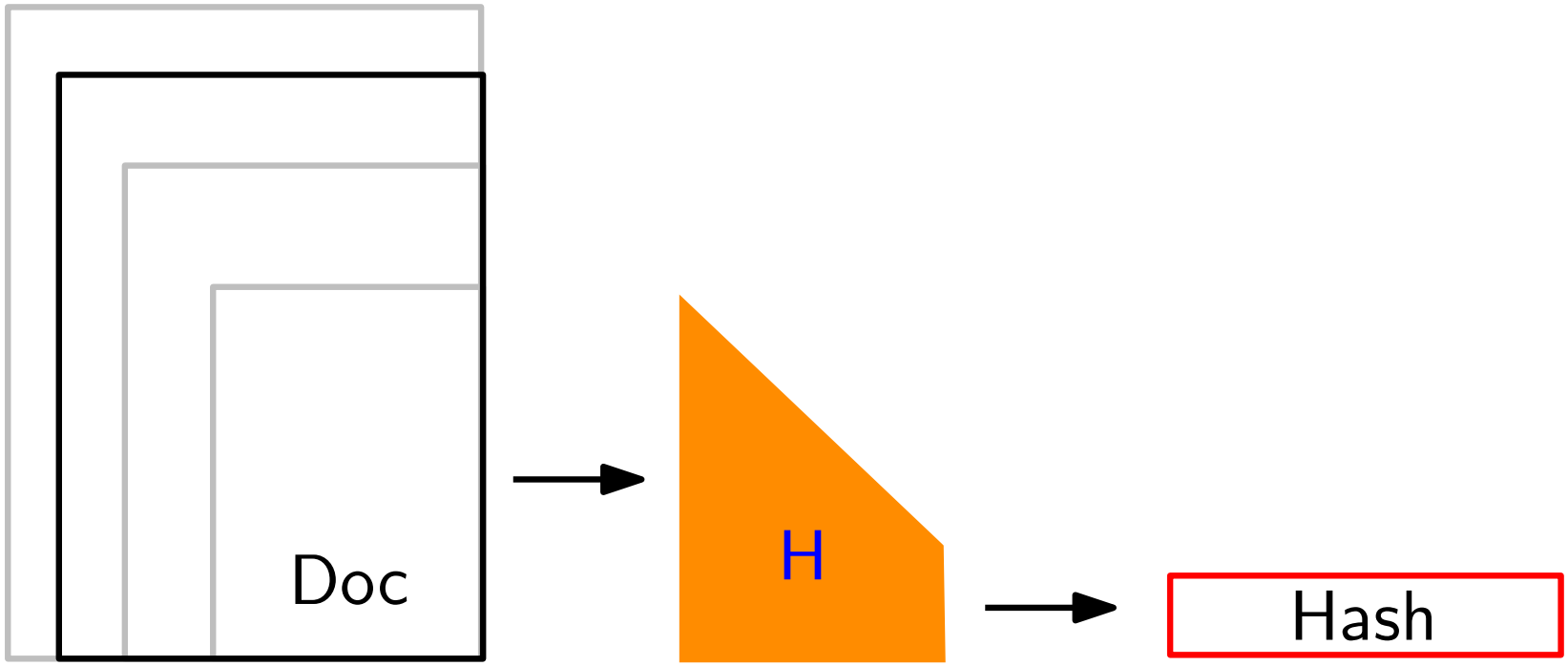
The Blockchain



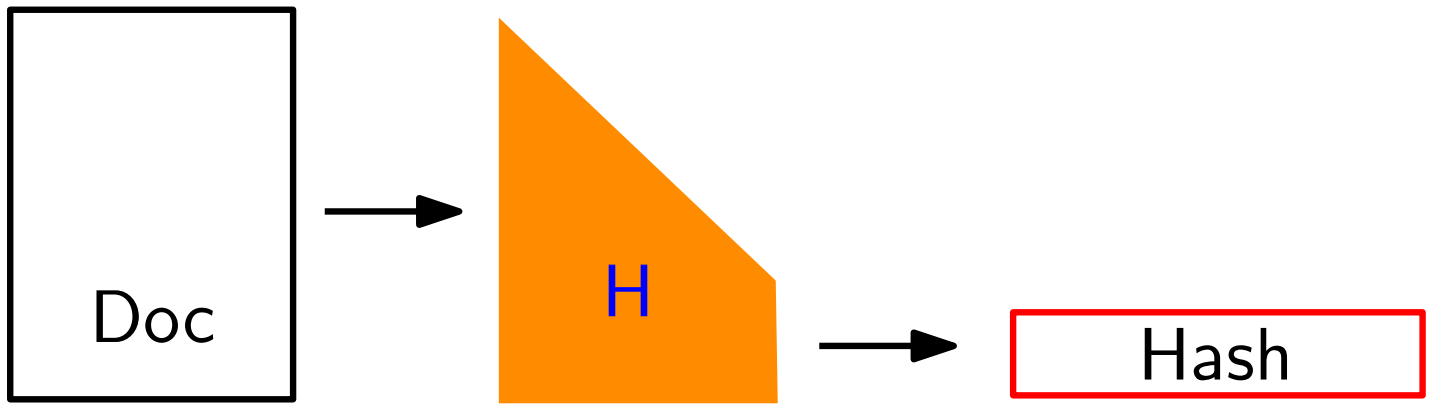
Cryptographic hash functions



Cryptographic hash functions



Cryptographic hash functions

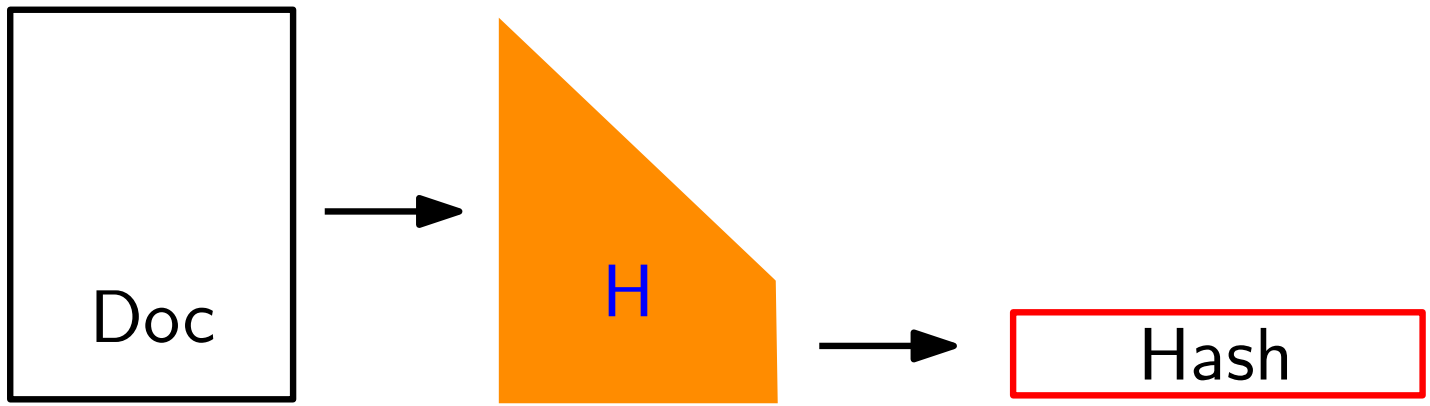


- outputs look random

  $\Rightarrow$ small modifs result in huge changes

  $\Rightarrow$ hard to find preimage

Cryptographic hash functions



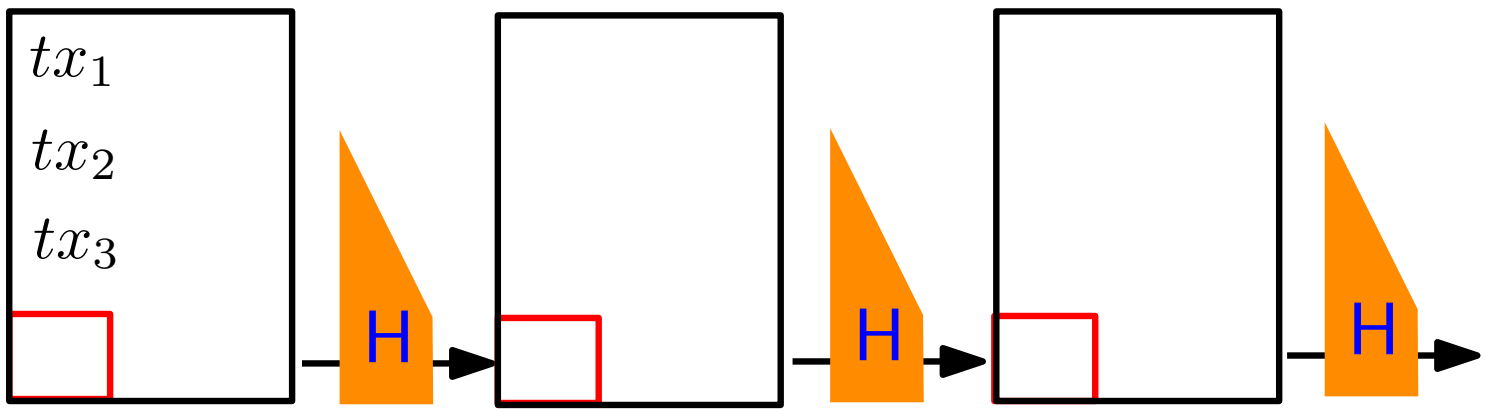
- outputs look random

  $\Rightarrow$ small modifs result in huge changes

  $\Rightarrow$ hard to find preimage

  $\Rightarrow$ **best way to find input with hash from some subset is randomly trying**

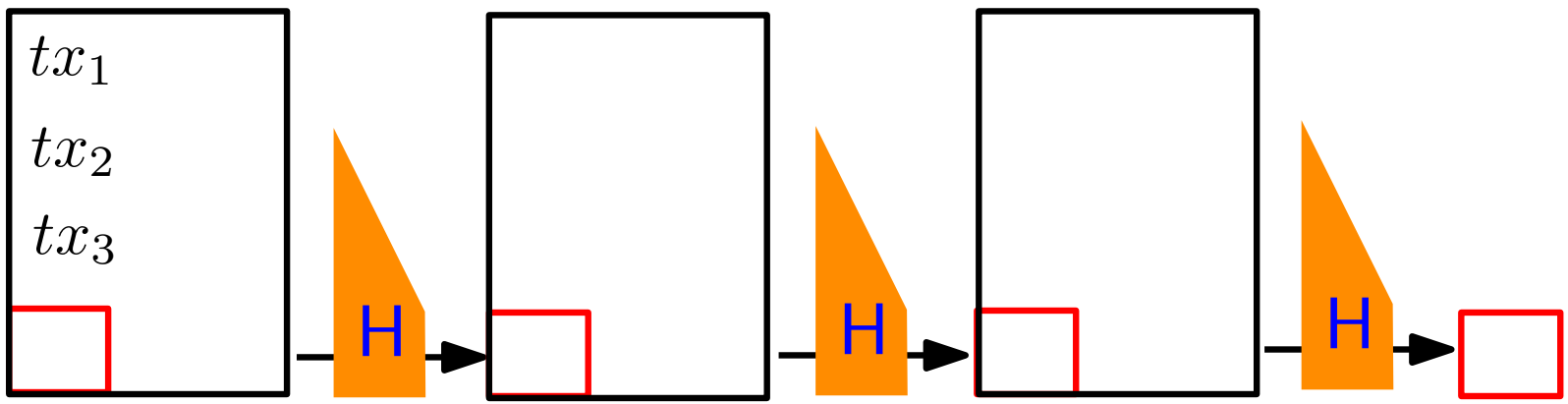
The Blockchain



- blocks linked by including hash of previous block

  $\Rightarrow$ **cannot mofify block w/o changing everything after**

The Blockchain

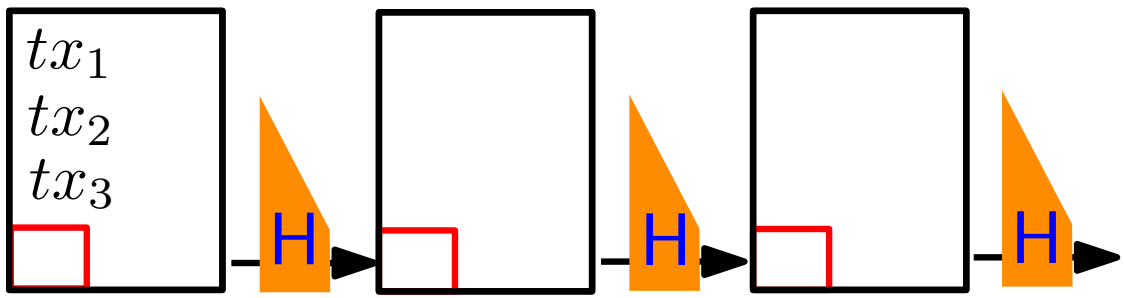


- blocks linked by including hash of previous block

  $\Rightarrow$ **cannot mofify block w/o changing everything after**

acts as fingerprint
for whole chain

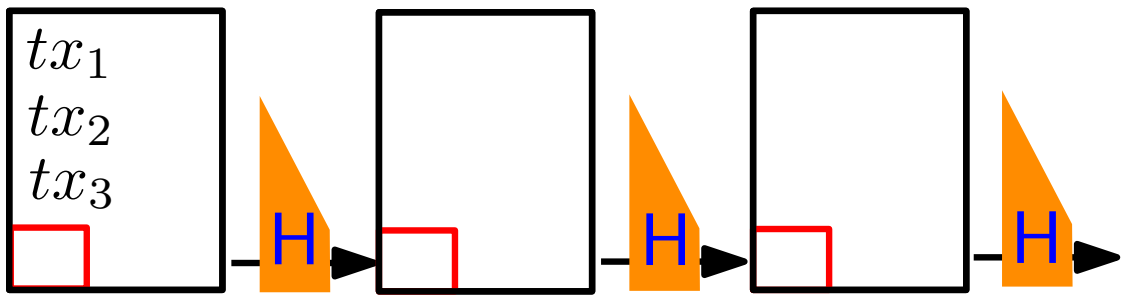
The Blockchain



- transactions collected into block
- new block added & published every 10min

  $\Rightarrow$ who adds block?

The Blockchain



- transactions collected into block
- new block added & published every 10min

  $\Rightarrow$ who adds block?

- assume mechanism chooses random user

  $\Rightarrow$ user could be malicious

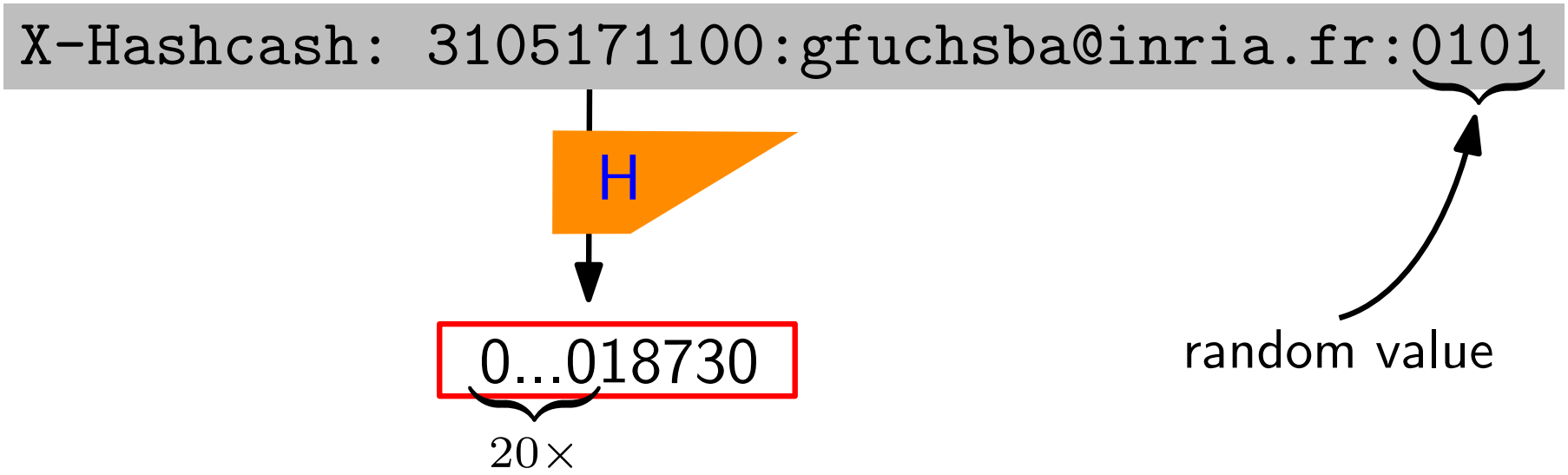
  $\Rightarrow$ Sybil attacks? $\Rightarrow$ Proof of work

Proof of work

- prove that you've performed work
- e.g. prevent spam: Hashcash

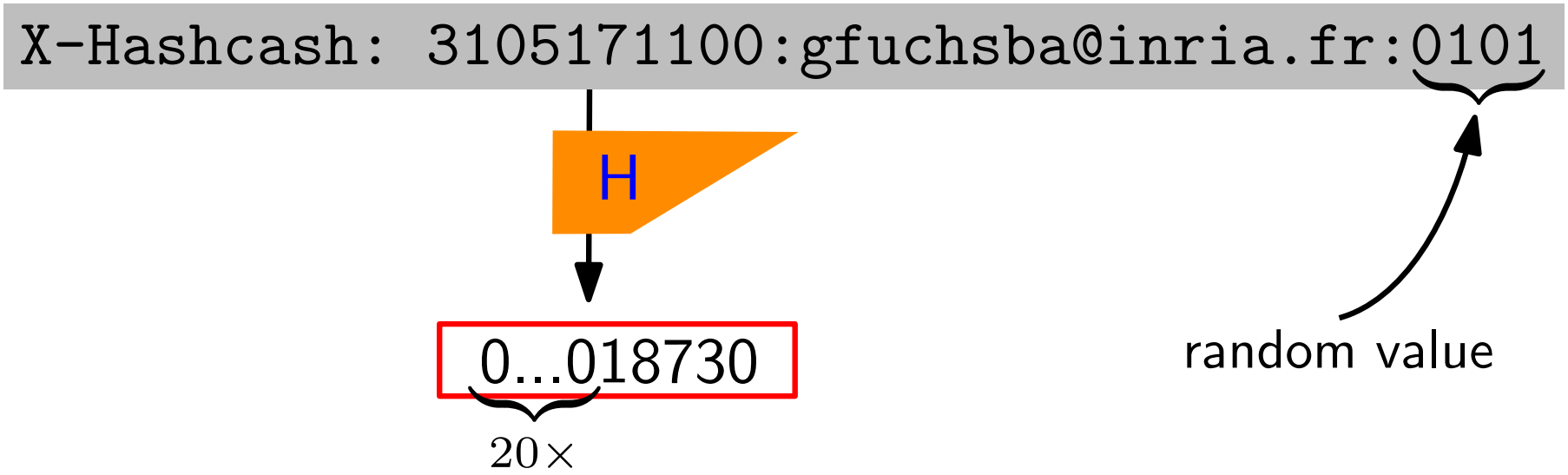
Proof of work

- prove that you've performed work
- e.g. prevent spam: Hashcash



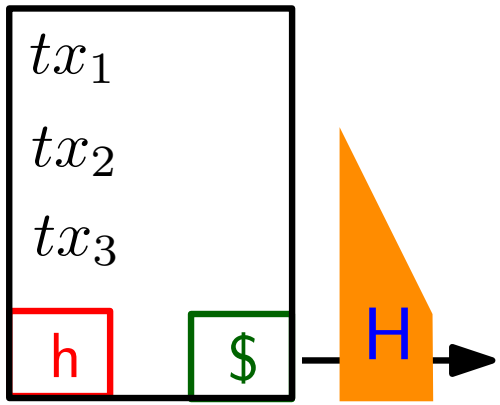
Proof of work

- prove that you've performed work
- e.g. prevent spam: Hashcash

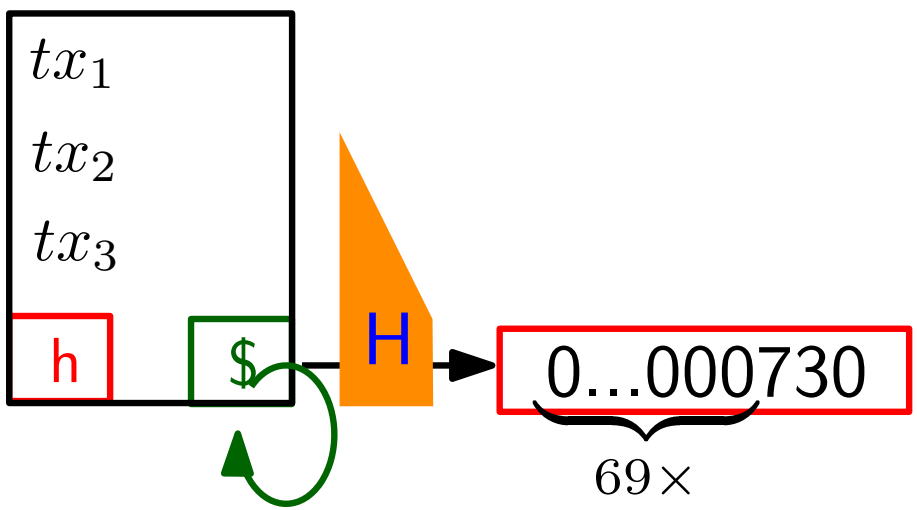


- try out $\approx 2^{20}$ values ($\sim$1s)
- easy to verify ($\sim 1\mu$s)

Mining

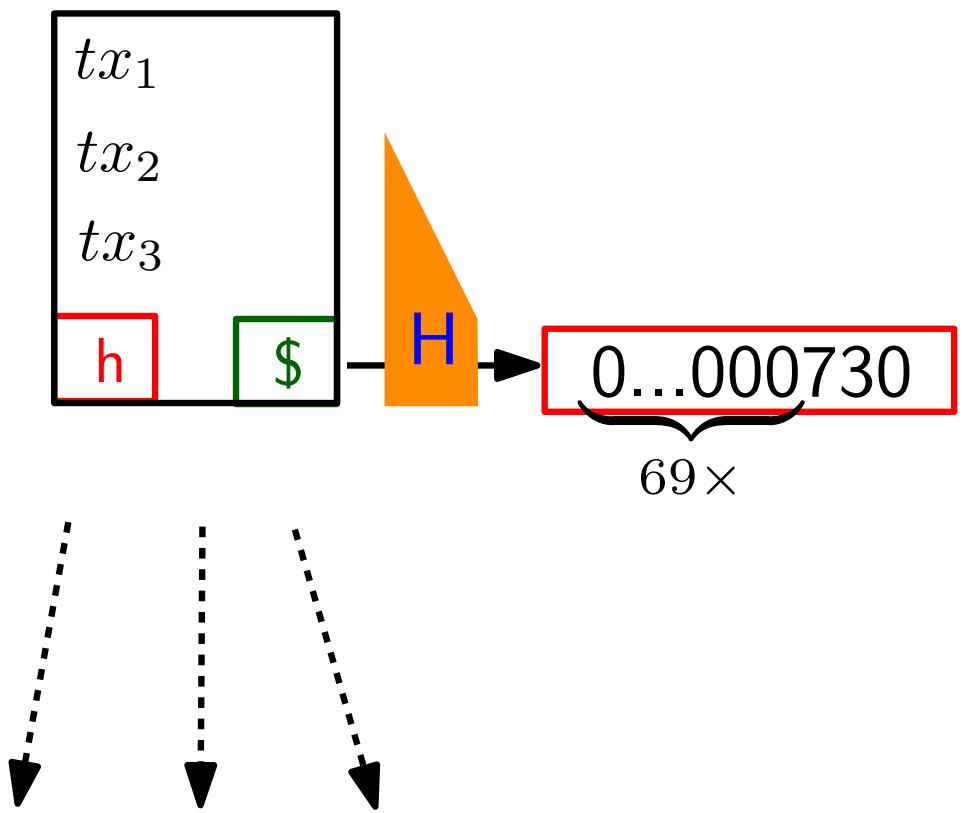


Mining



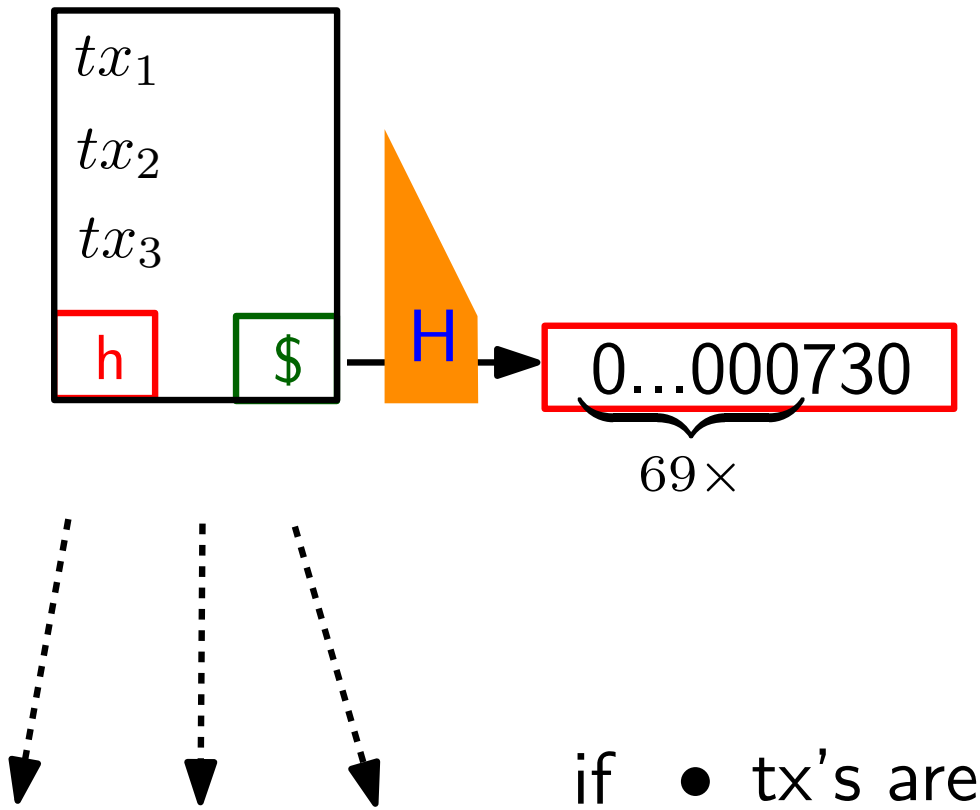
- collect transactions
- find value $ yielding small hash

Mining



- collect transactions
- find value $ yielding small hash
- broadcast block

Mining

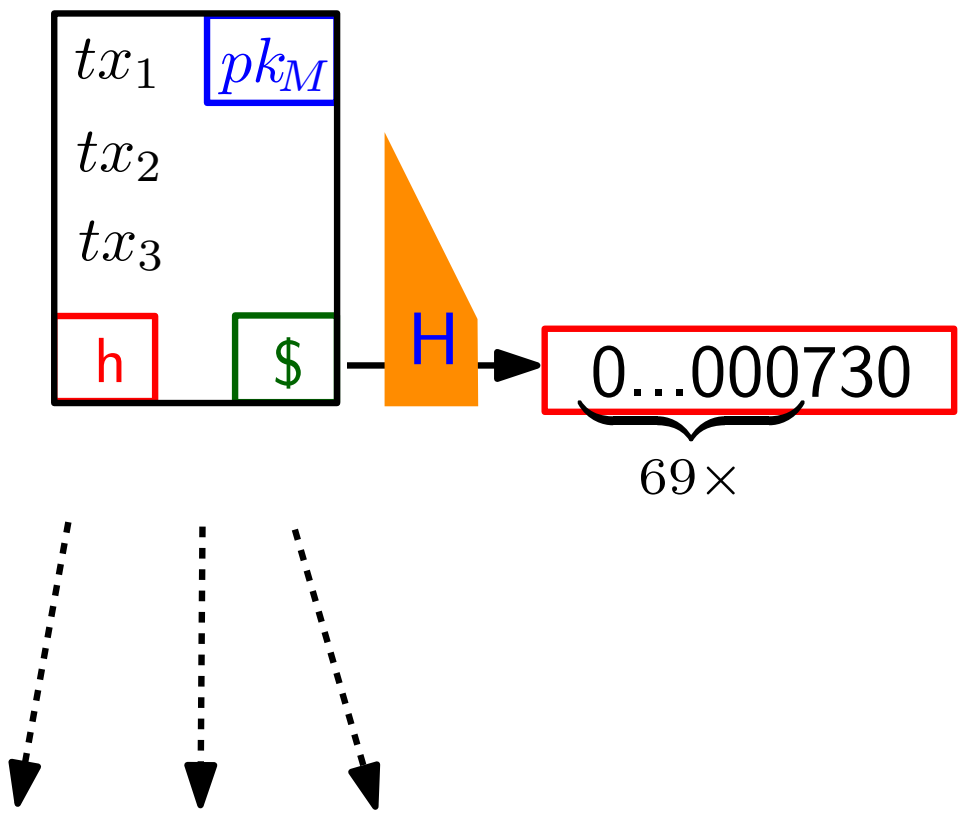


- collect transactions
- find value $ yielding small hash
- broadcast block

if
- tx's are valid
- hash is small enough

$\Rightarrow$ add block to local copy of blockchain

Mining

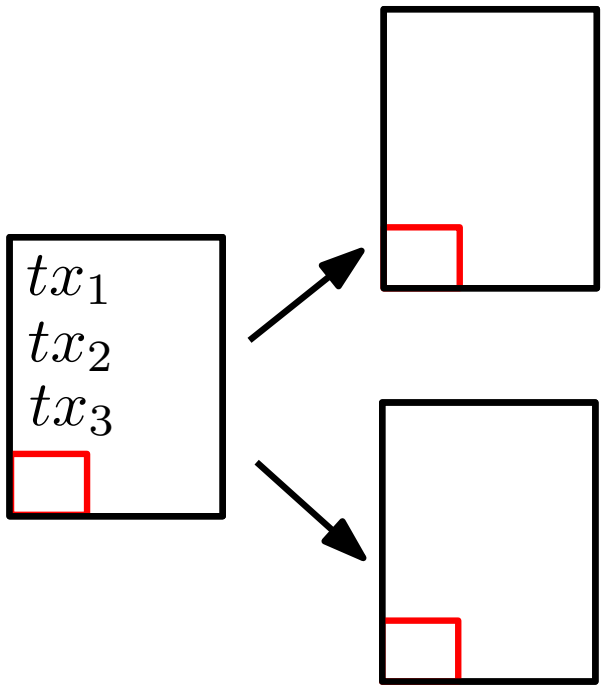


- Incentive?

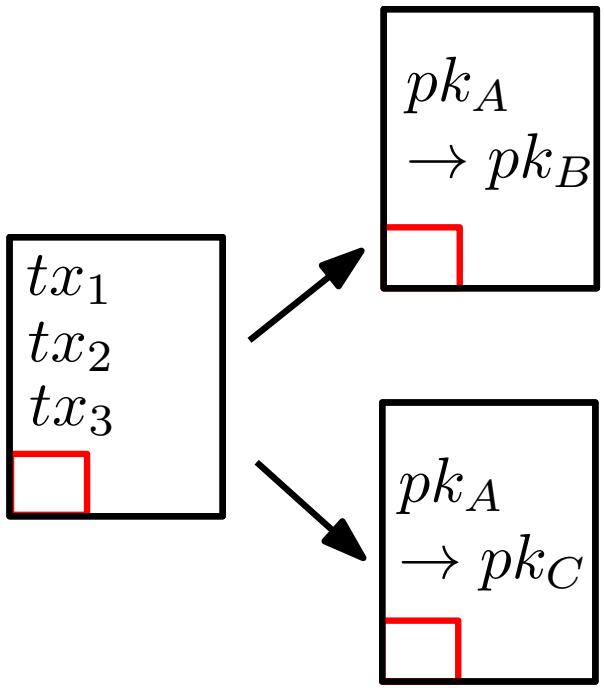
  $\Rightarrow$ reward bitcoins!

  (all bitcoins created this way)

Forks

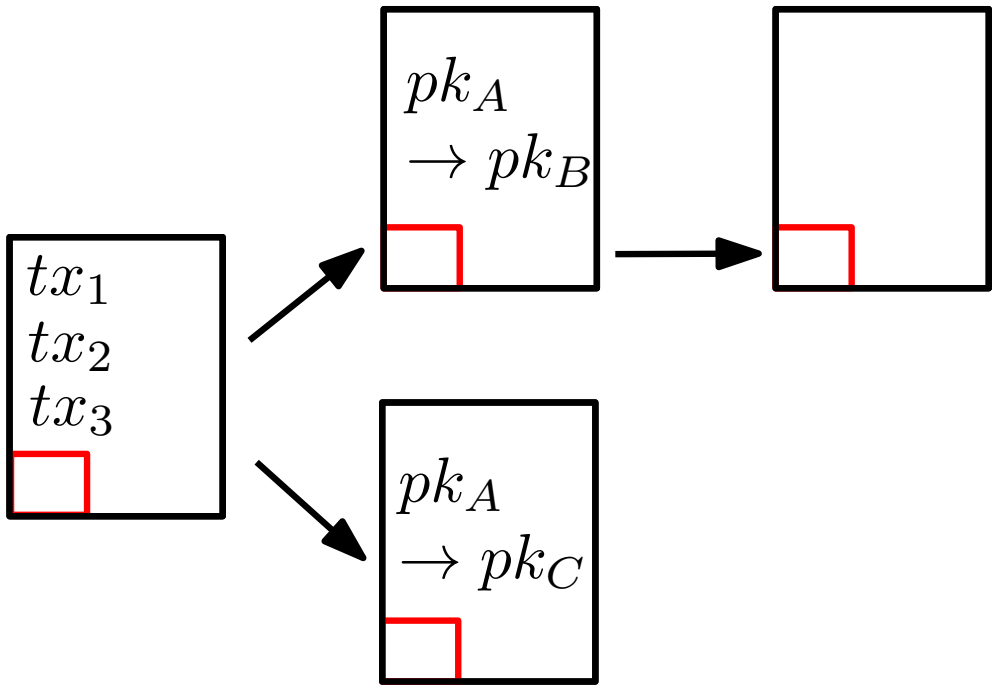


Forks



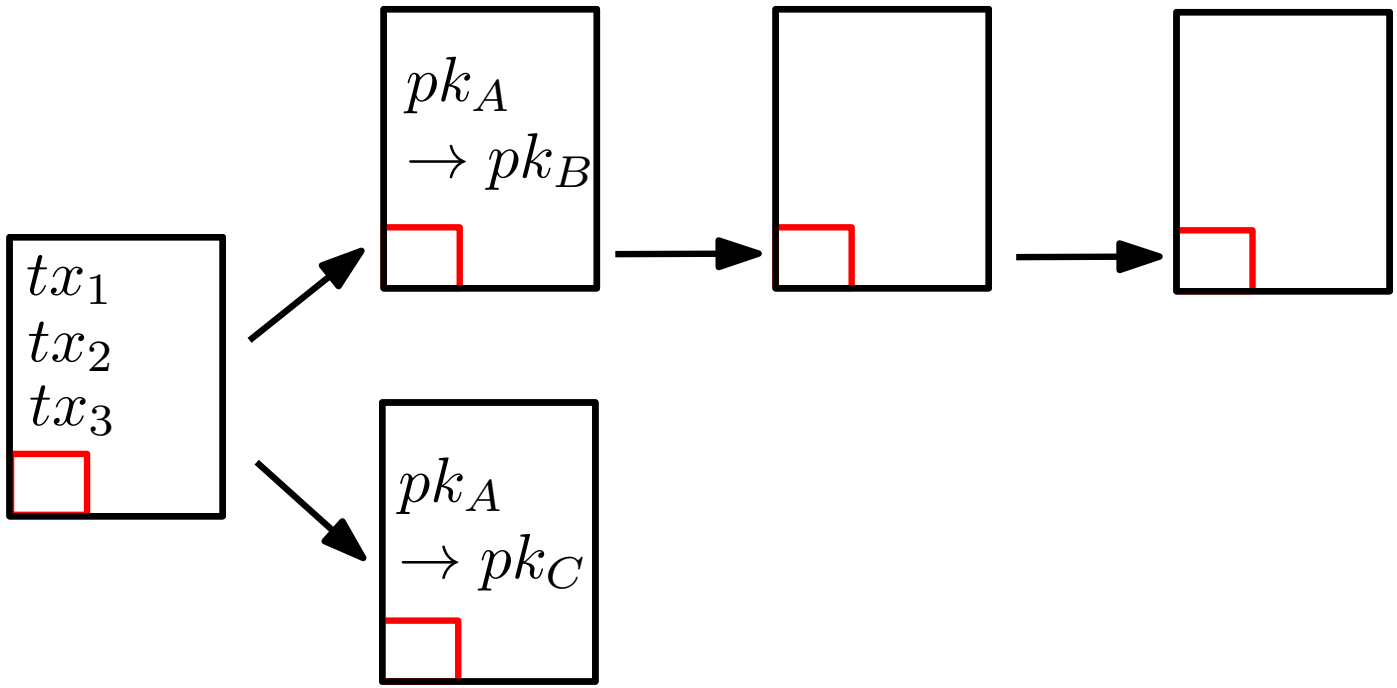
- Double-spending!

Forks



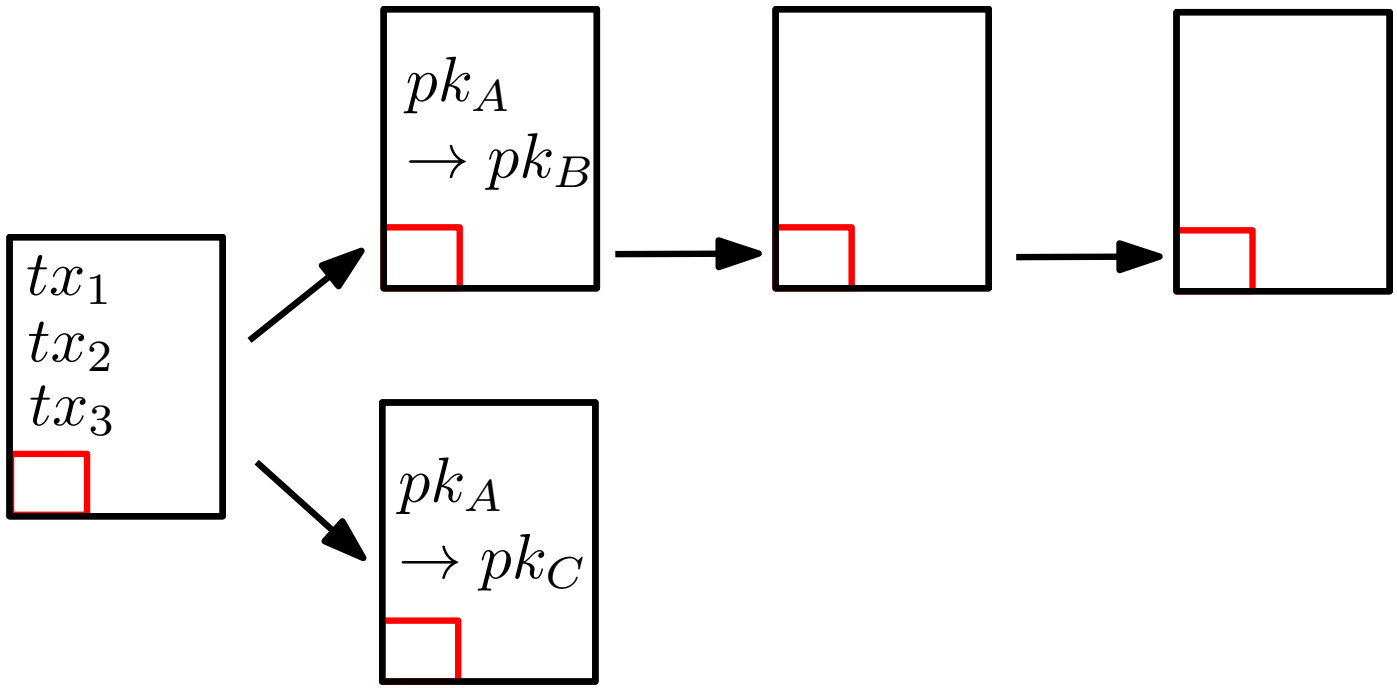
"Always mine on the longest chain"

Forks



"Always mine on the longest chain"

Forks

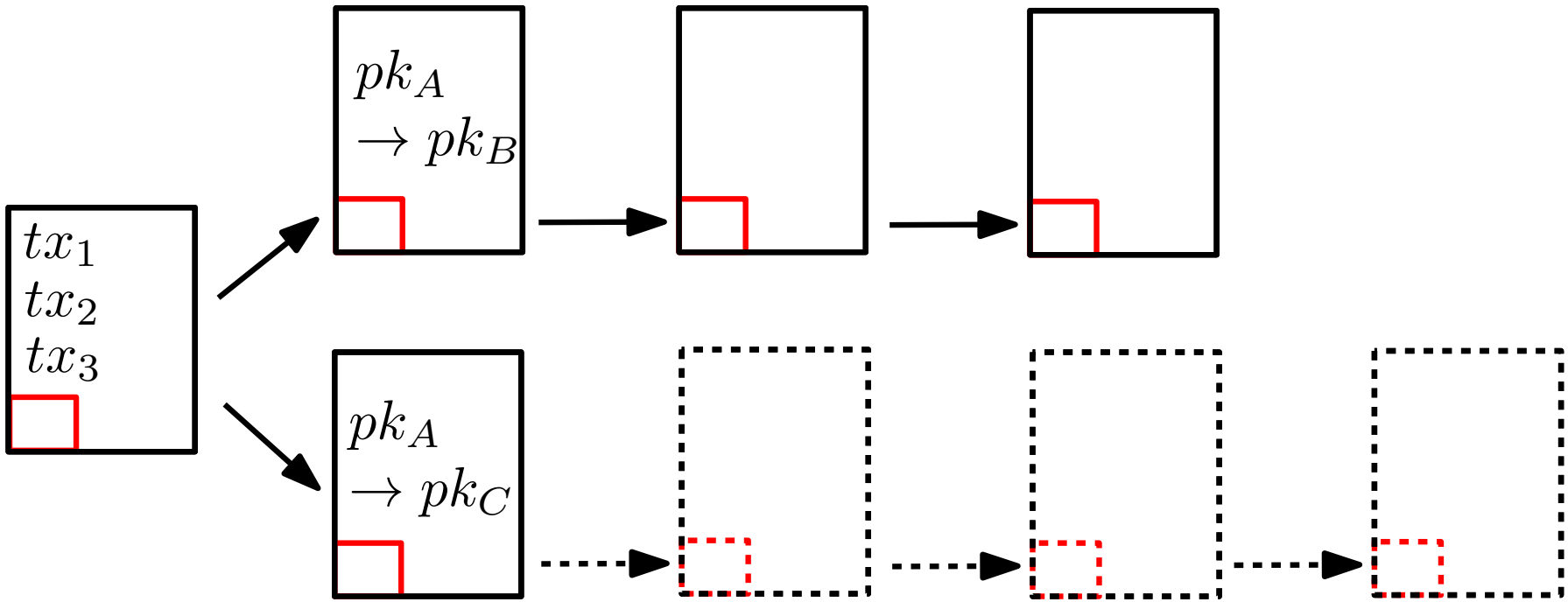


"Always mine on the longest chain"

Secure if majority of miners is honest

$\Rightarrow$ wait for 6 blocks before accepting payment

Forks



The "51%-attack"

Why does it work?

Why does it work?

- Miners incentivized by rewards
- Probability of mining block $\sim$ computing power

  $\Rightarrow$ no Sybil attacks!
- Rational to mine on longest chain

  $\Rightarrow$ quick consensus

Why does it work?

- Miners incentivized by rewards
- Probability of mining block $\sim$ computing power
  $\Rightarrow$ no Sybil attacks!
- Rational to mine on longest chain
  $\Rightarrow$ quick consensus

Problems

- specialized hardware + cheap electricity
  $\Rightarrow$ *mining oligarchy*
- Bitcoin consumes electricity like town of 100k population
  $\Rightarrow$ *polluting*

Why does it work?

- Miners incentivized by rewards
- Probability of mining block $\sim$ computing power

  $\Rightarrow$ no Sybil attacks!
- Rational to mine on longest chain

  $\Rightarrow$ quick consensus

Problems

- specialized hardware + cheap electricity

  $\Rightarrow$ *mining oligarchy*

Bitcoin consumes electricity like town of 100k population

$\Rightarrow$ *polluting*

$\Rightarrow$ **Can proof of work be replaced by something else?**

Proof of stake

- prob. of mining $\sim$ number of coins owned
- **Problems:**
  - *Nothing-at-stake problems*
  - *Participation: miners = holders*

Proof of space

- prove that you've allocated disk space

Trivial solution

Verifier

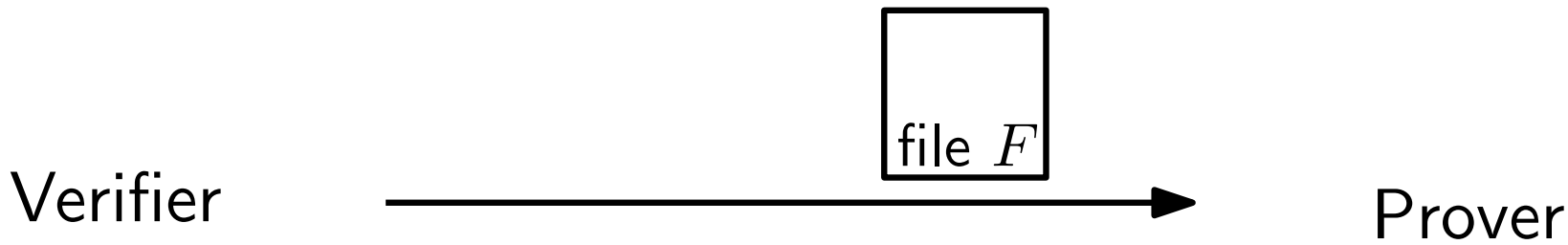
Prover

Proof of space

- prove that you've allocated disk space

Trivial solution

Initialization:

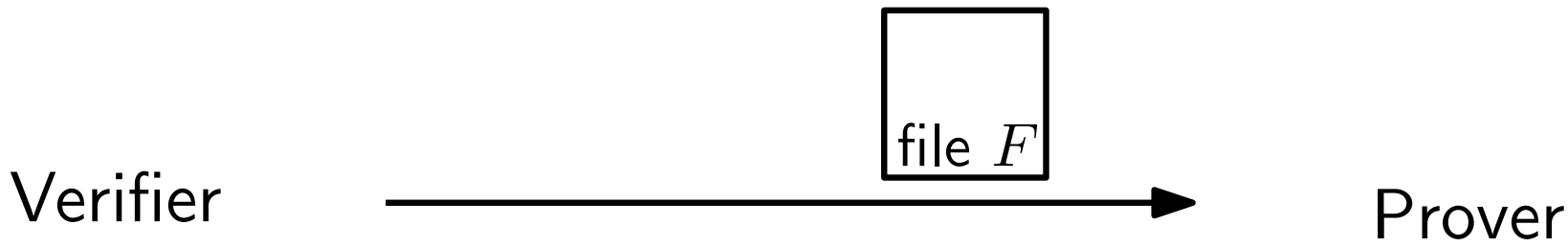


Proof of space

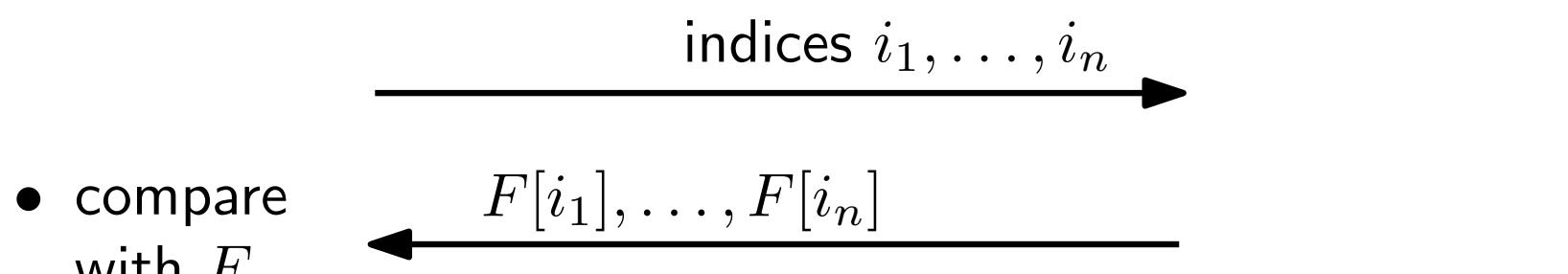
- prove that you've allocated disk space

Trivial solution

Initialization:



Prove:

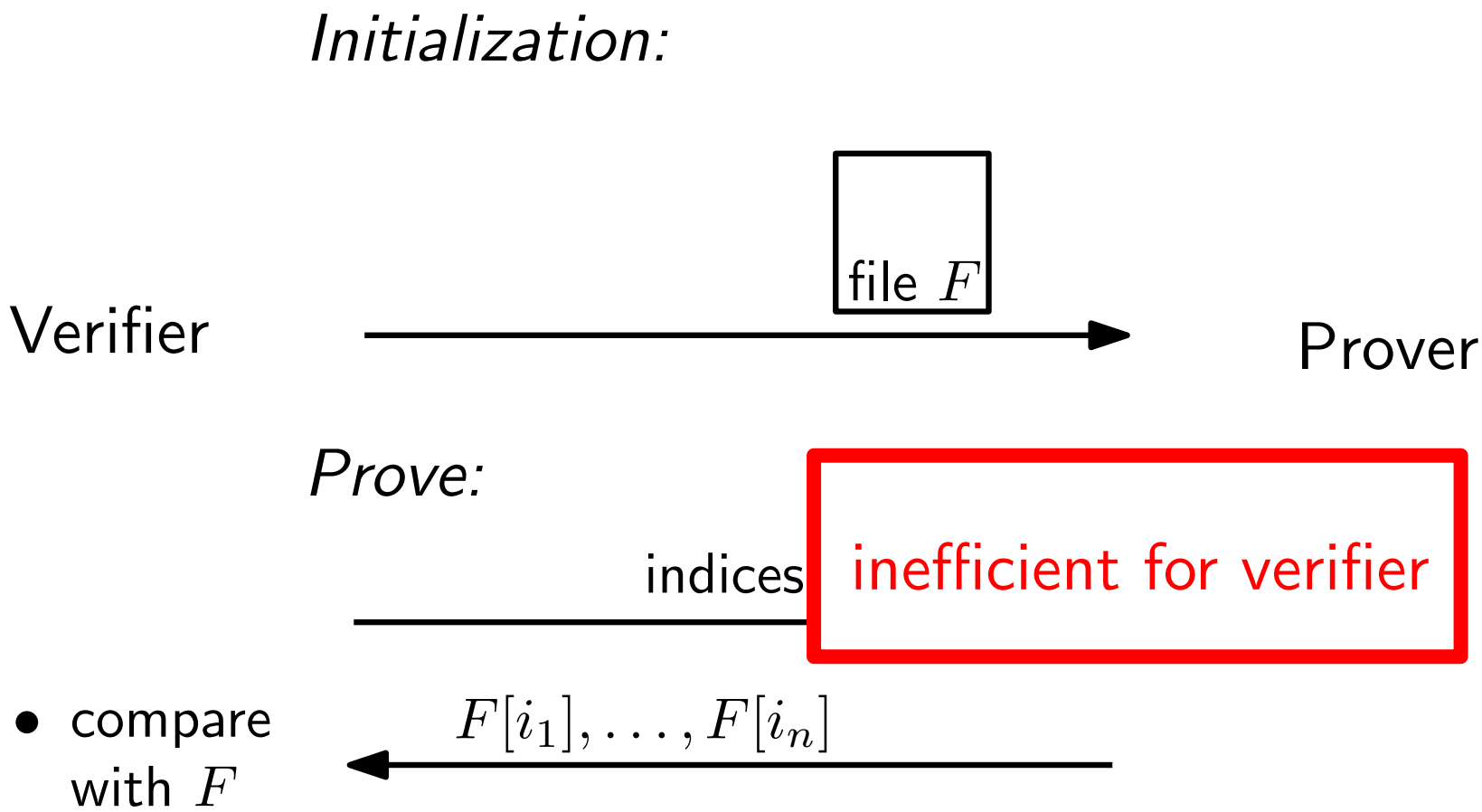


- compare with F

Proof of space

- prove that you've allocated disk space

Trivial solution

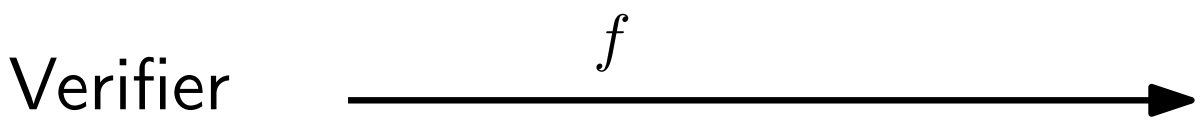


Proof of space

- prove that you've allocated disk space

A better solution

Initialization:

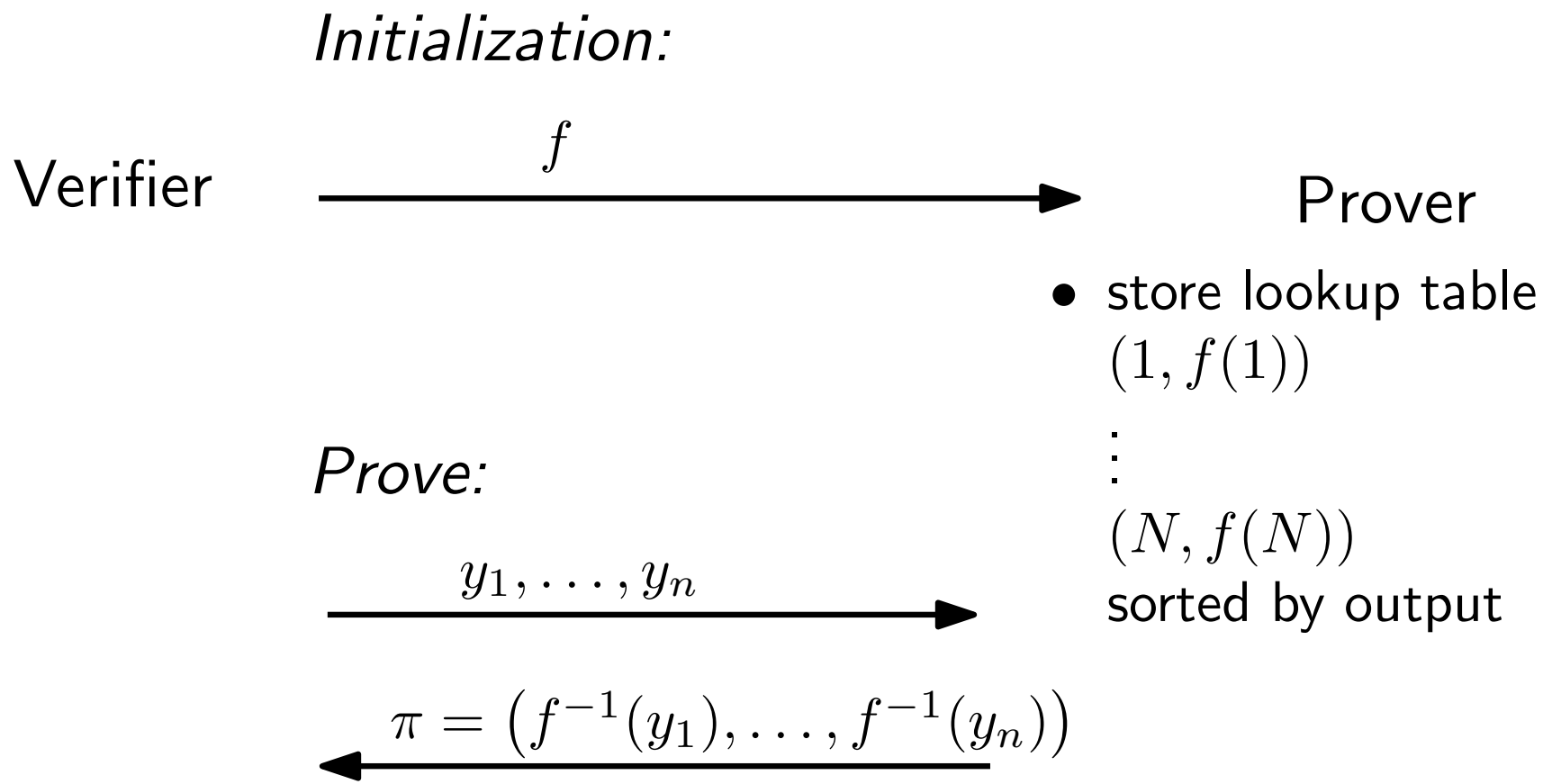


- store lookup table
  $(1, f(1))$
  $\vdots$
  $(N, f(N))$
  sorted by output

Proof of space

- prove that you've allocated disk space

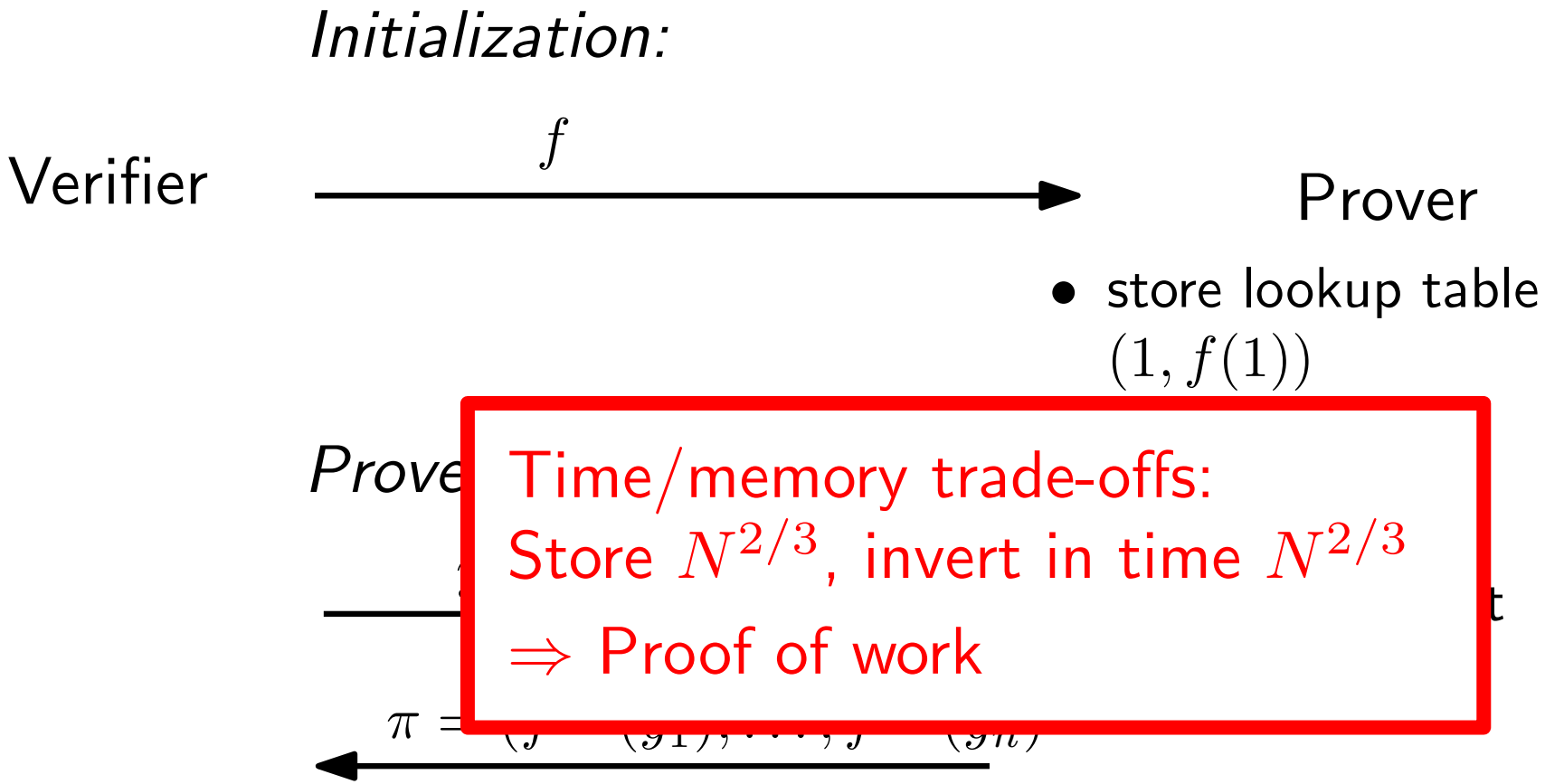
A better solution



Proof of space

- prove that you've allocated disk space

A better solution



Proof of space

- prove that you've allocated disk space

[DFKP'15]

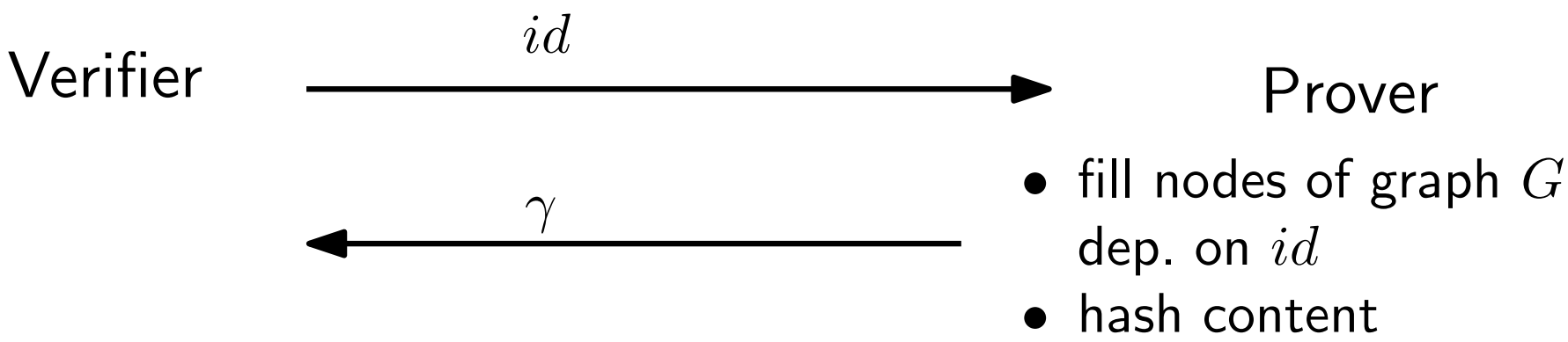
Initialization:

Proof of space

- prove that you've allocated disk space

[DFKP'15]

Initialization:



Proof of space

- prove that you've allocated disk space

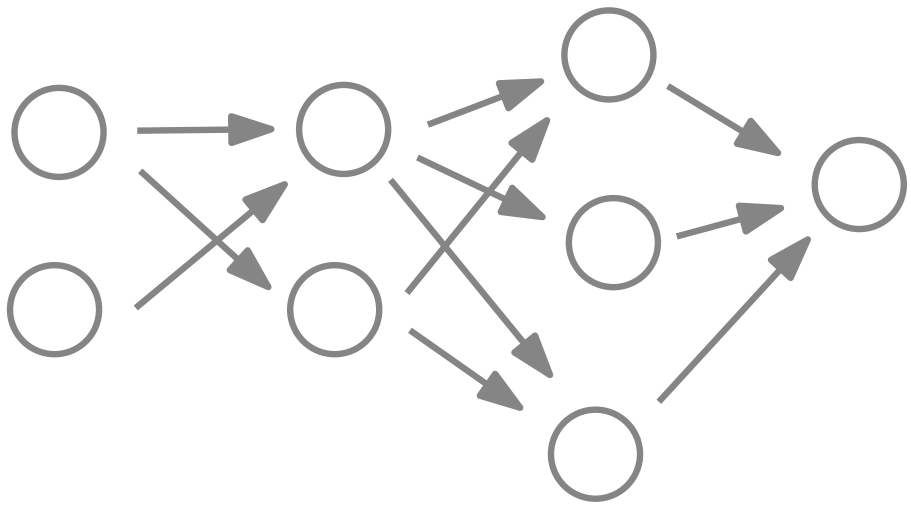
[DFKP'15]

Initialization:

Verifier $\xrightarrow{id}$ Prover

Verifier $\xleftarrow{\gamma}$ Prover

- fill nodes of graph G dep. on id
- hash content



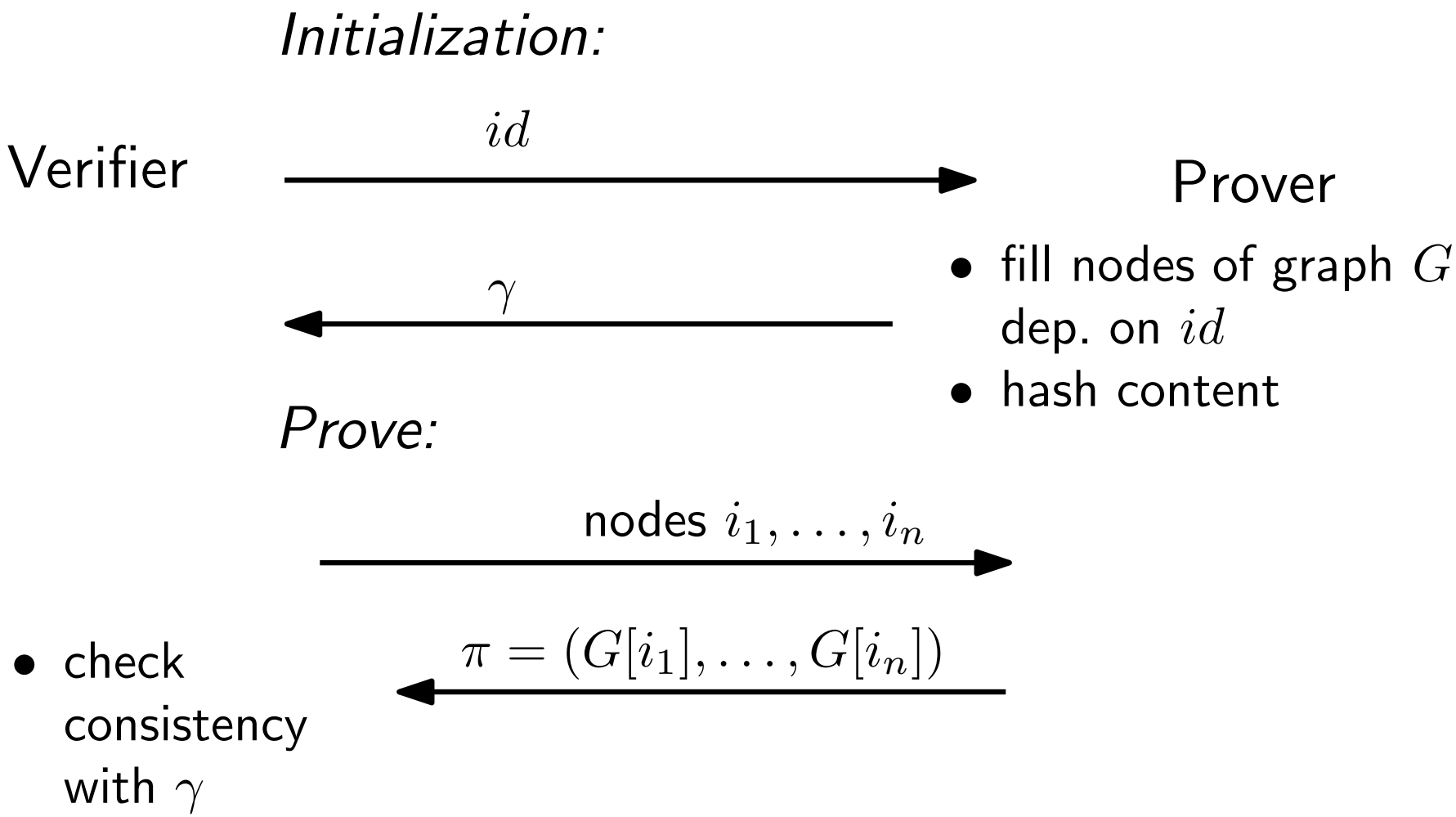
(use hard-to-pebble graph)

(hash using Merkle tree)

Proof of space

- prove that you've allocated disk space

[DFKP'15]



SpaceMint

- replace proof of **work** by proof of **space**
- **Advantages:**
  - *green:* low electricity; reusable hardware
  - *decentralized*

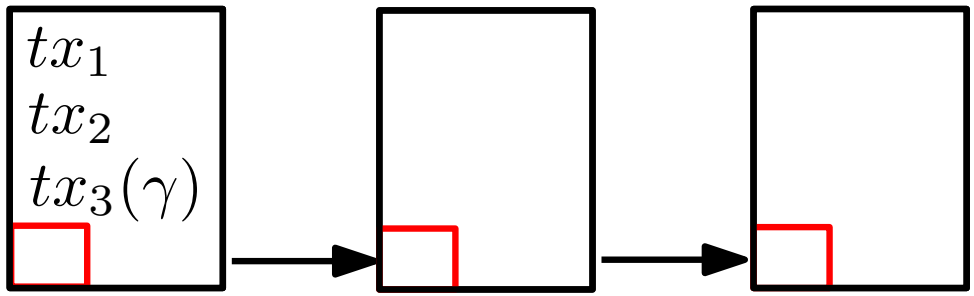
SpaceMint

- replace proof of **work** by proof of **space**
- **Advantages:**
  - *green:* low electricity; reusable hardware
  - *decentralized*
- **Challenges:**
  - PoS is *interactive*
  - *Nothing-at-stake problems*

SpaceMint

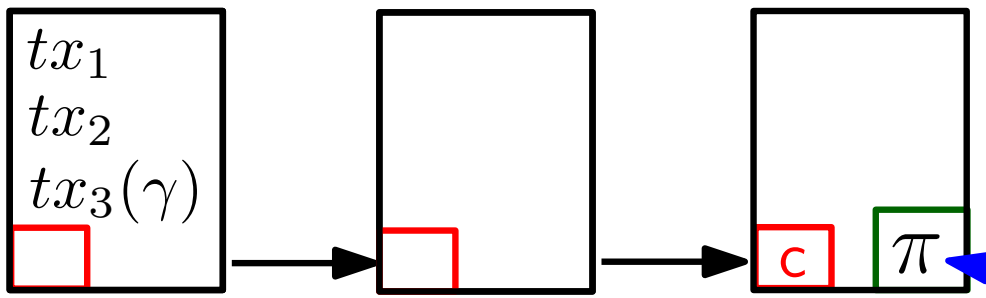
- replace proof of **work** by proof of **space**
- **Advantages:**
  - *green:* low electricity; reusable hardware
  - *decentralized*
- **Challenges:**
  - PoS is *interactive*
  - *Nothing-at-stake problems*
    - Mining multiple chains
    - Grinding blocks

SpaceMint



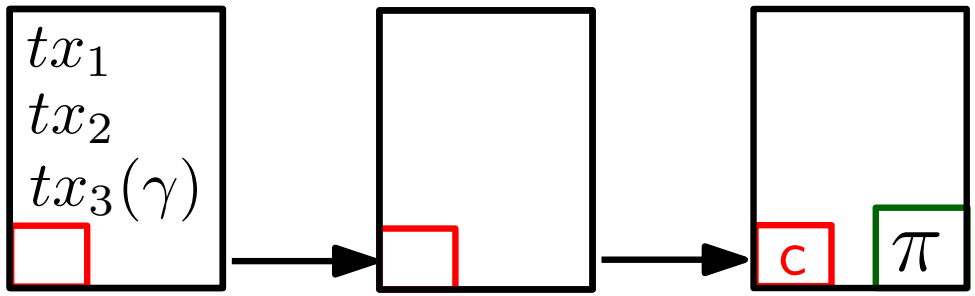
- Miner initializes space with $id = pk$
- broadcasts γ
- γ gets added to chain

SpaceMint



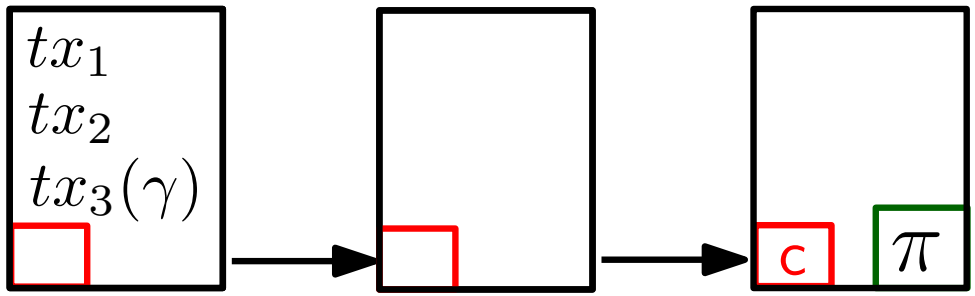
proof π
for hash γ
with challenge c

SpaceMint



Who gets to add the block?

SpaceMint



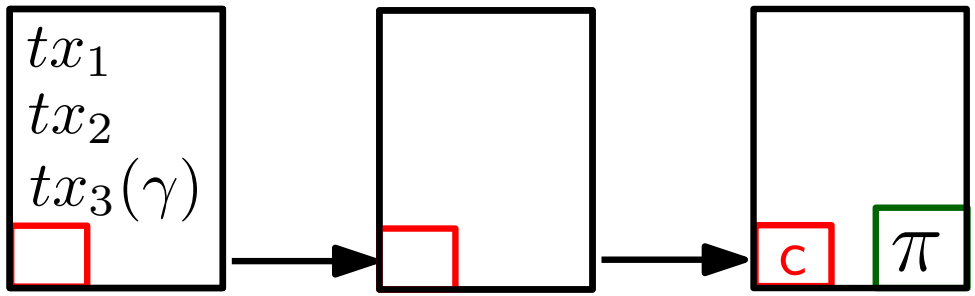
Who gets to add the block?

- **Quality** of proof?

  $\Rightarrow$ define fct. of proof π: quality $\sim$ space allocated

  $\Rightarrow$ block with *best* proof gets added to chain

SpaceMint



Who gets to add the block?

- **Quality** of proof?

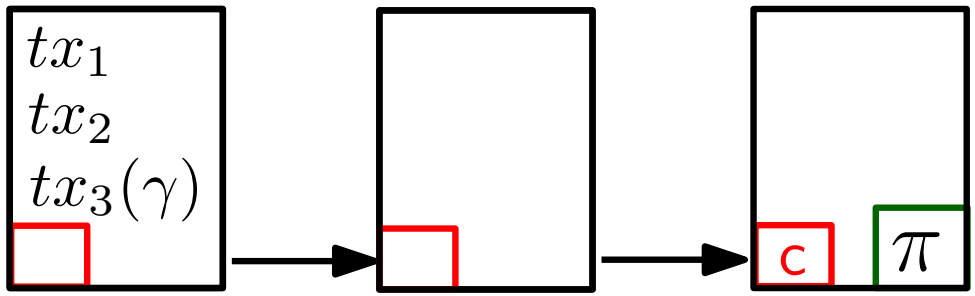
  $\Rightarrow$ define fct. of proof π: quality $\sim$ space allocated

  $\Rightarrow$ block with *best* proof gets added to chain

- Blocks define **quality of chain**

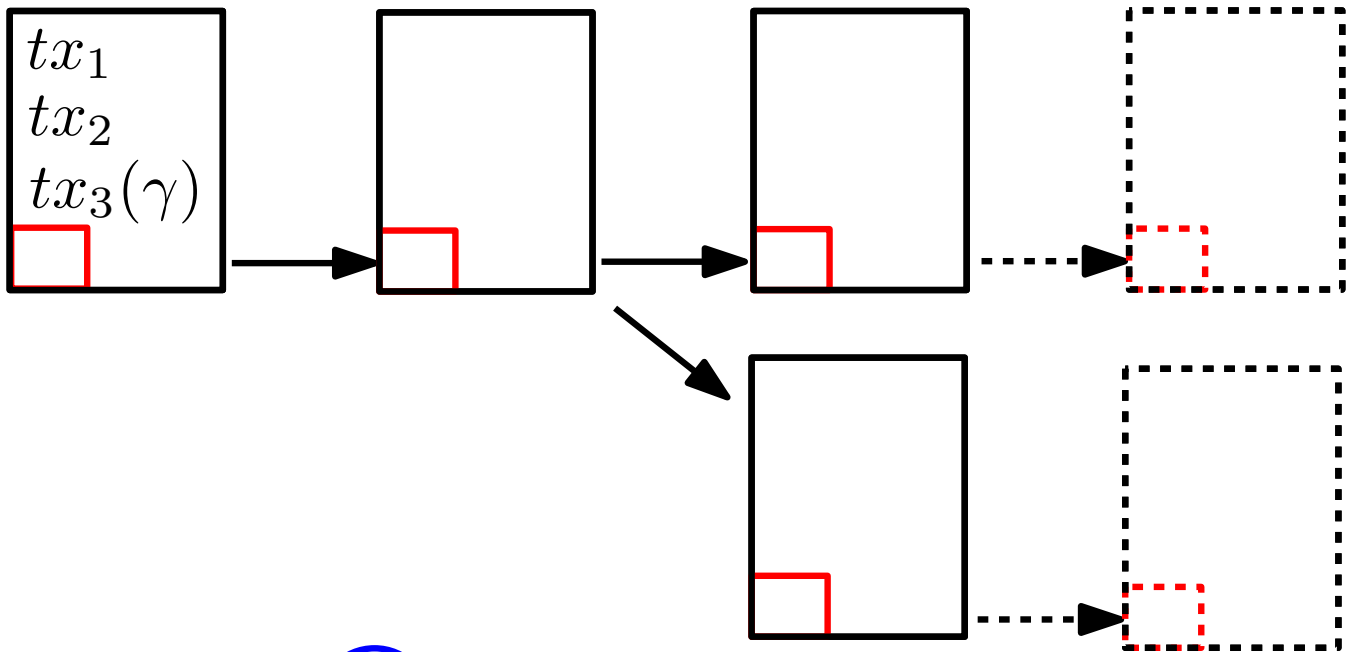
  $\Rightarrow$ always mine on *best* chain

SpaceMint



Does this work?

SpaceMint



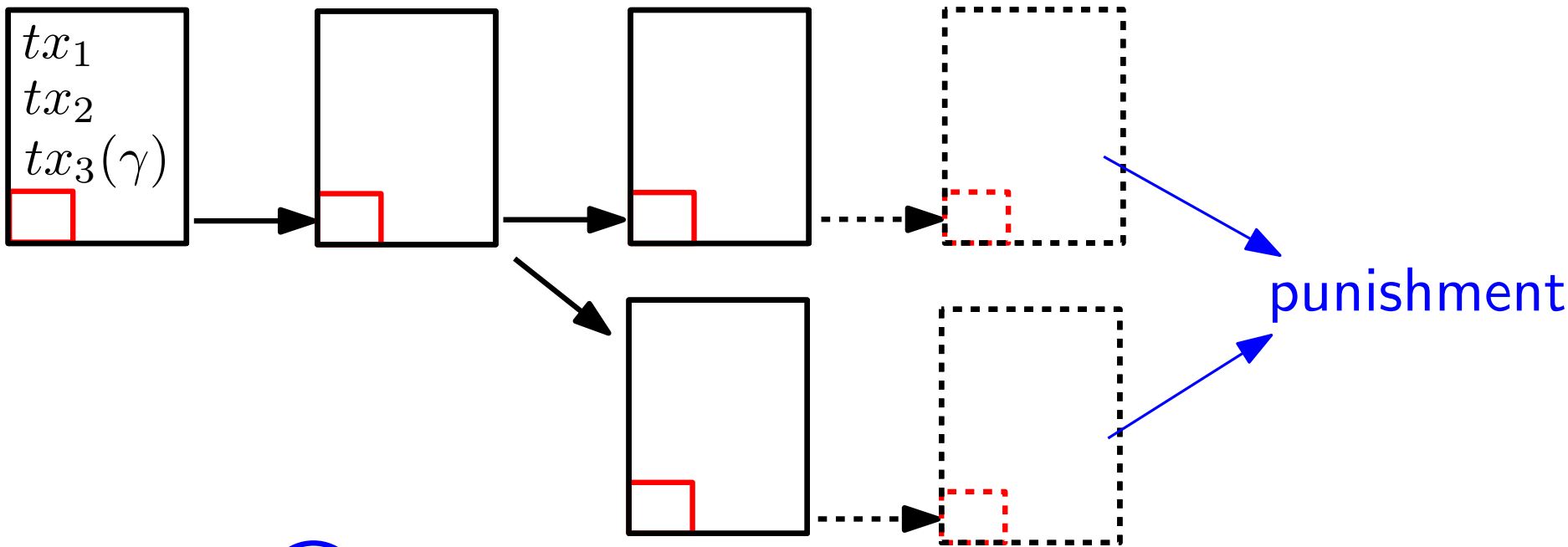
$\neq$ Bitcoin: (1)

- *easy* to generate proofs!

  $\Rightarrow$ **miners try to extend every chain**

  $\Rightarrow$ no consensus!

SpaceMint



$\neq$ Bitcoin: (1)

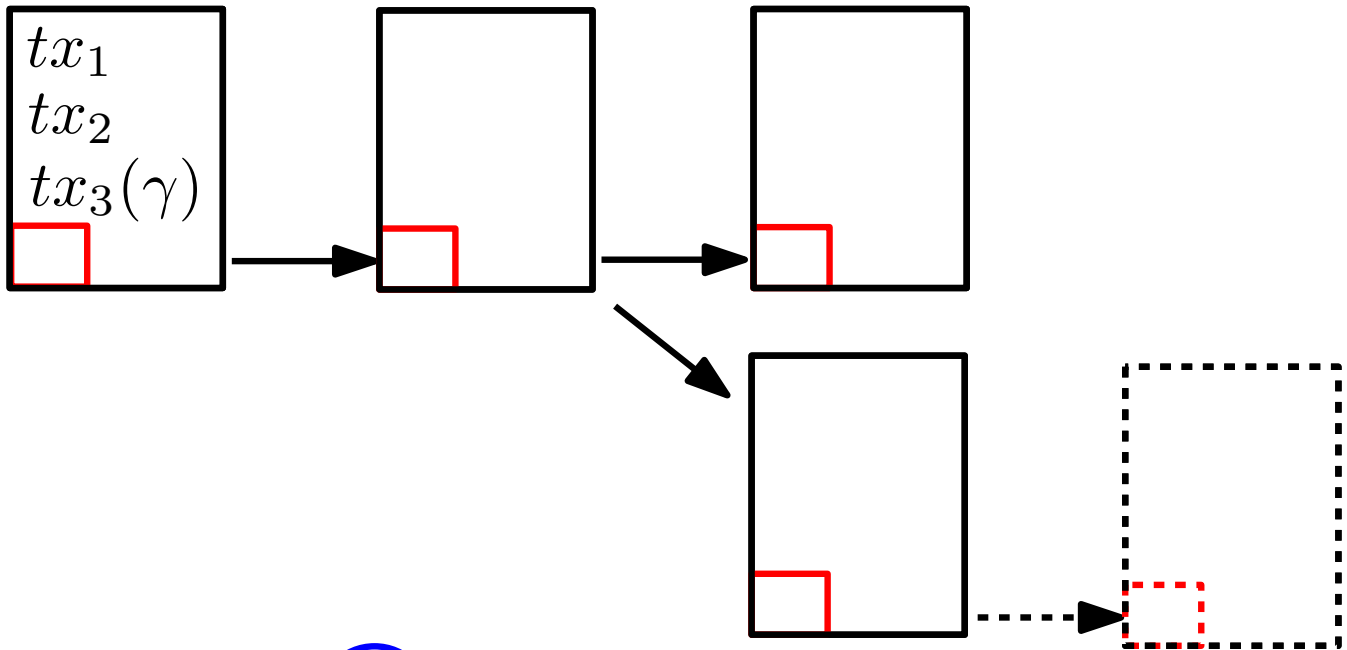
- *easy* to generate proofs!

  $\Rightarrow$ **miners try to extend every chain**

  $\Rightarrow$ no consensus!

Forbid extending 2 chains

SpaceMint



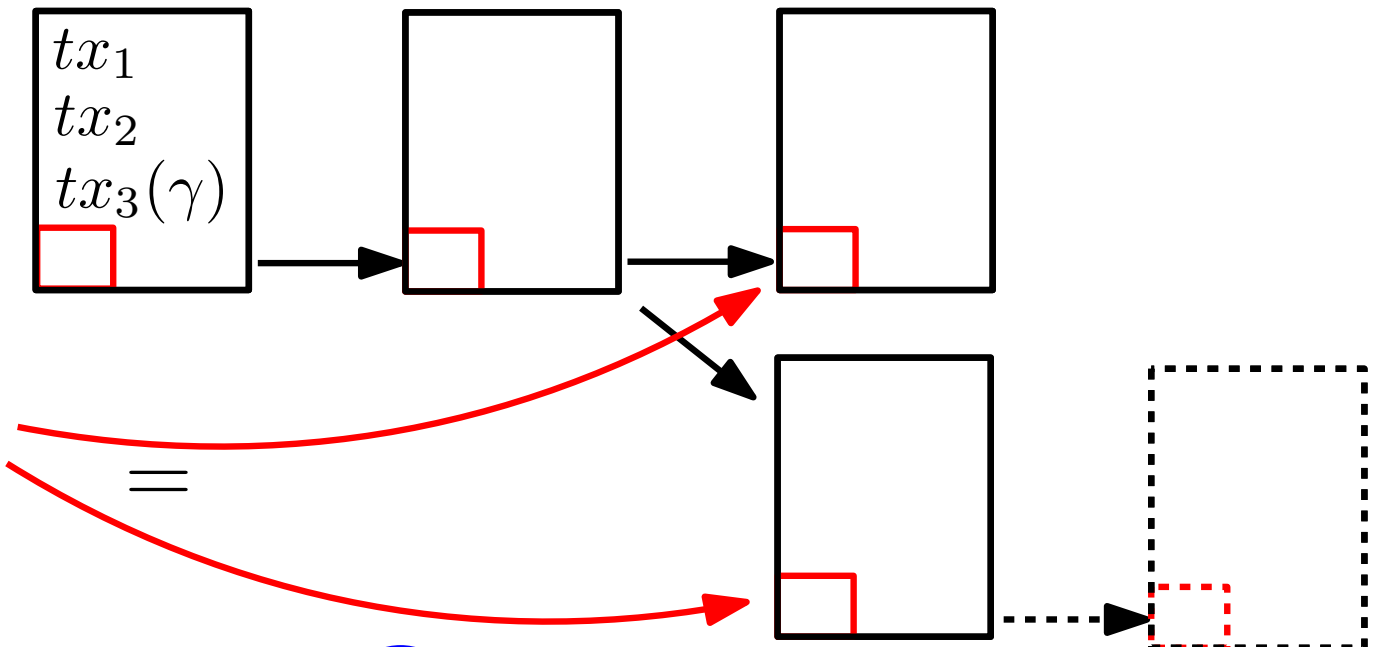
$\neq$ Bitcoin: (2)

- *easy* to check if good solution!

  $\Rightarrow$ **miners might not extend best chain**

  $\Rightarrow$ no consensus!

SpaceMint



$\neq$ Bitcoin: (2)

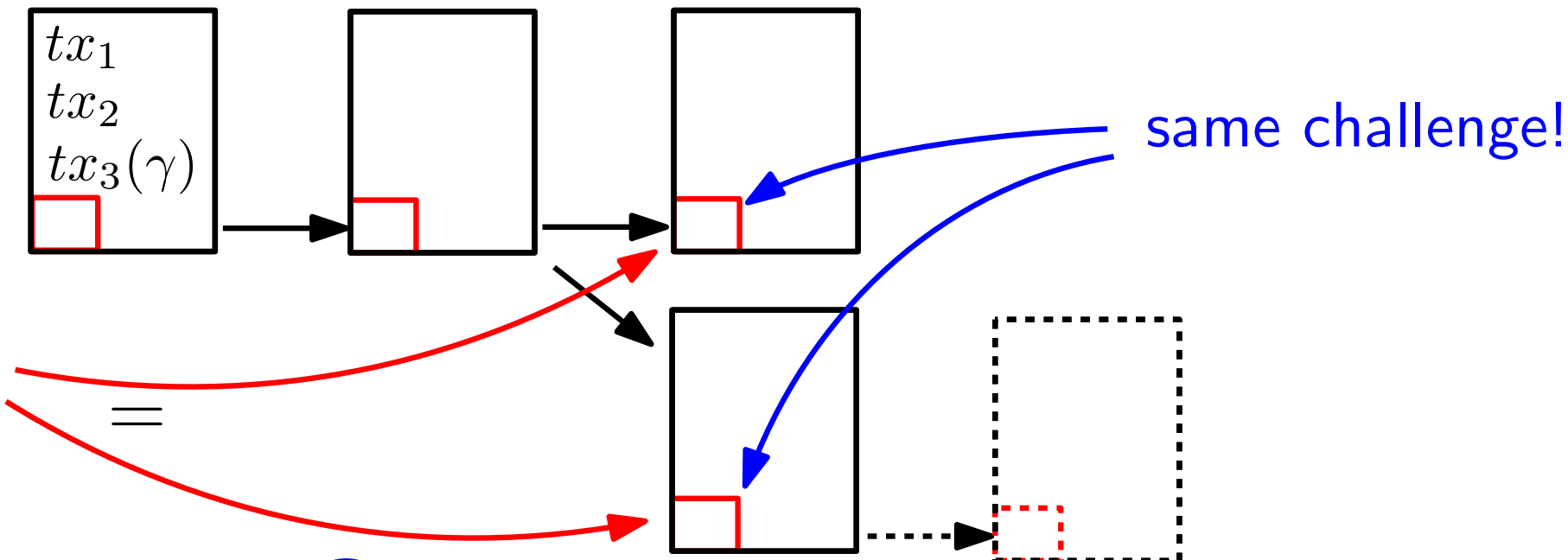
- *easy* to check if good solution!

  $\Rightarrow$ **miners might not extend best chain**

  $\Rightarrow$ no consensus!

Take challenge from past

SpaceMint



$\neq$ Bitcoin: (2)

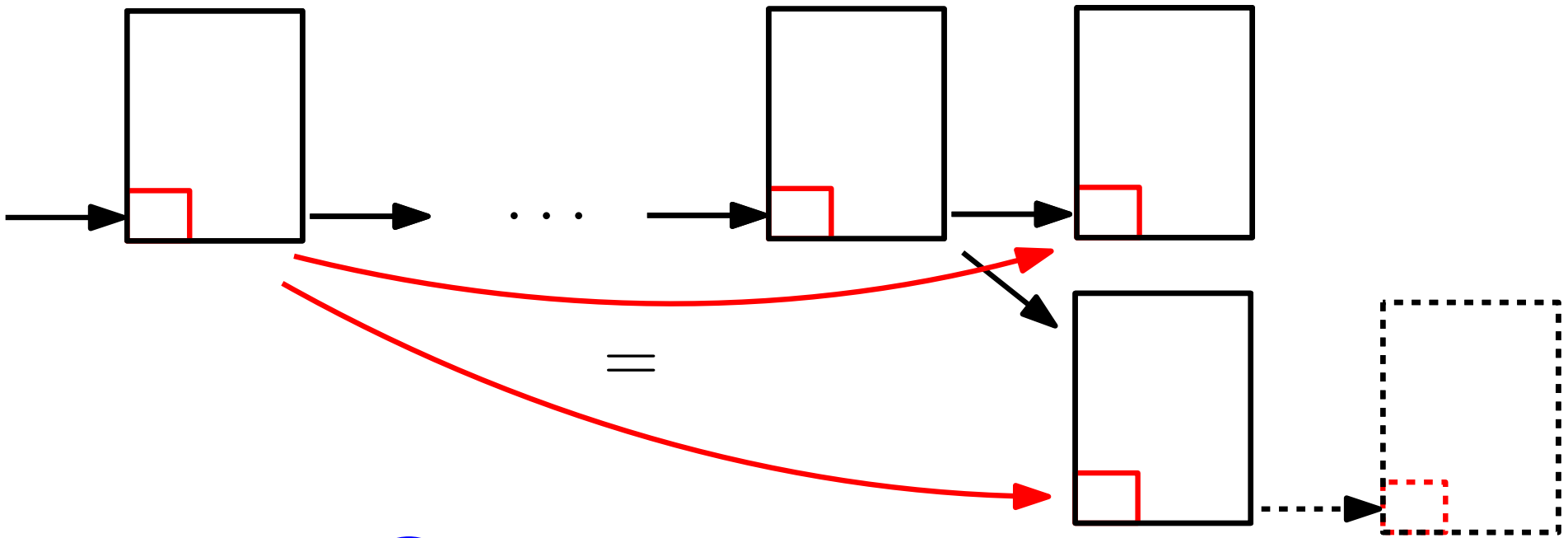
- *easy* to check if good solution!

  $\Rightarrow$ **miners might not extend best chain**

  $\Rightarrow$ no consensus!

Take challenge from past

SpaceMint



$\neq$ Bitcoin: (2)

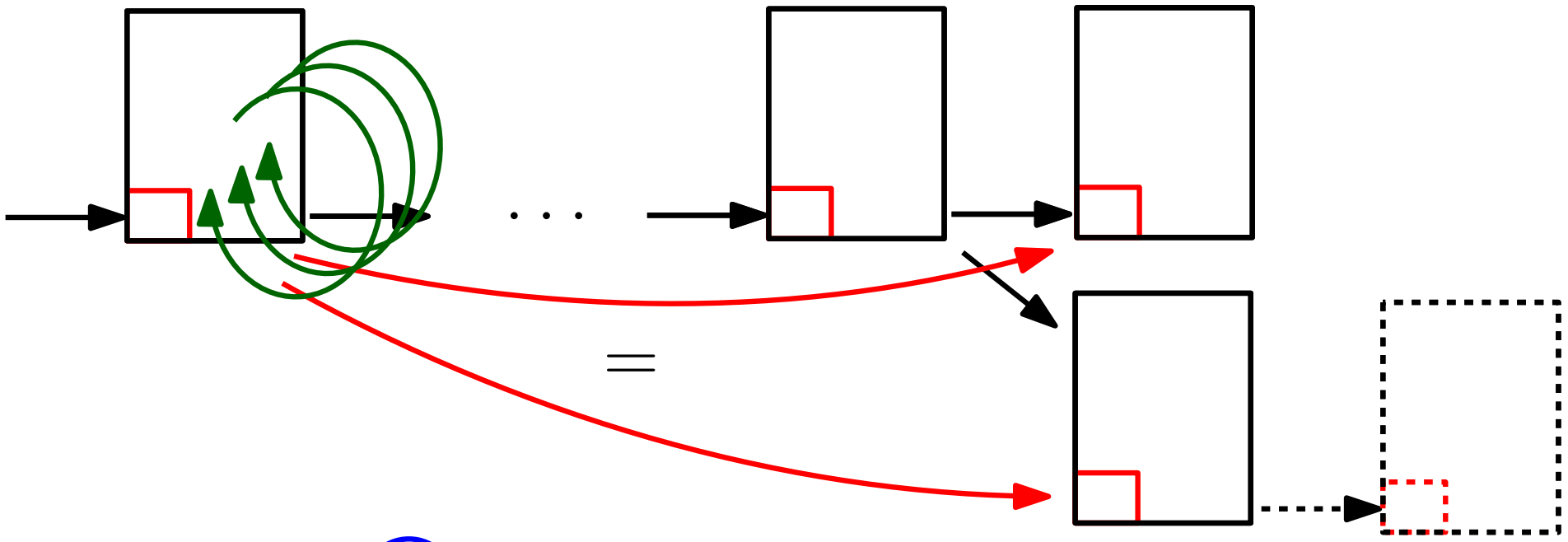
- *easy* to check if good solution!

  $\Rightarrow$ **miners might not extend best chain**

  $\Rightarrow$ no consensus!

Take challenge from past

SpaceMint

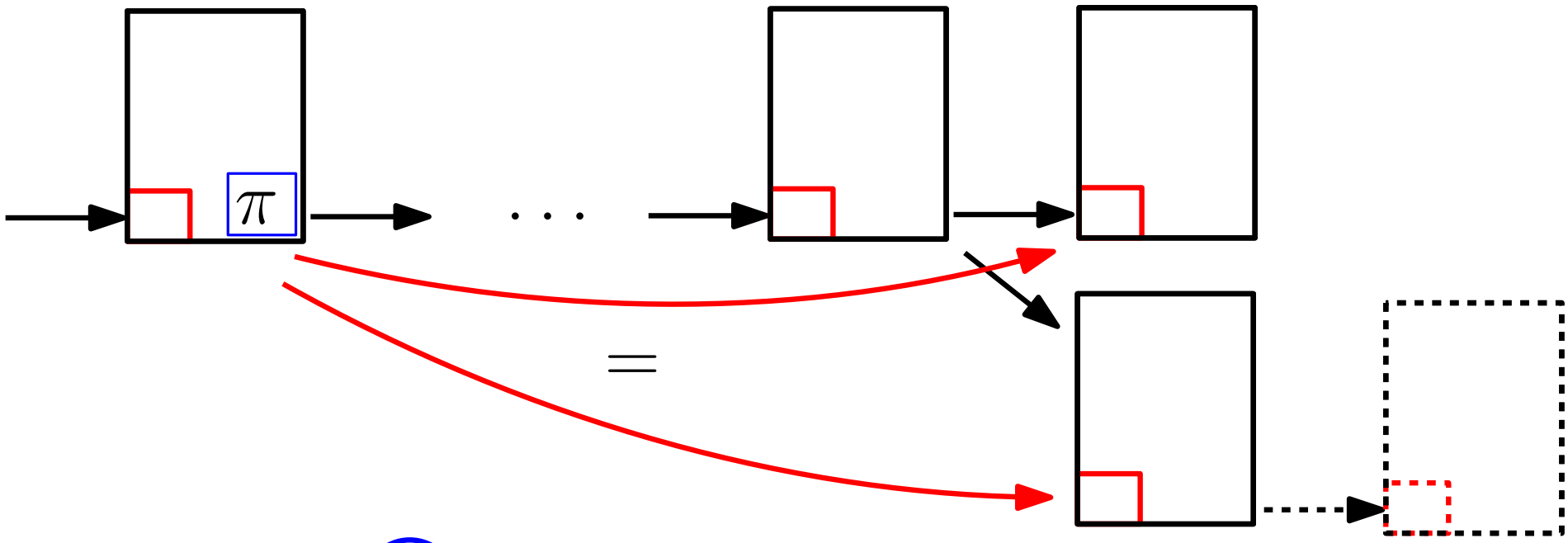


$\neq$ Bitcoin: (3)

$\Rightarrow$ **miners might grind blocks leading to good challenge in future**

$\Rightarrow$ proof of work

SpaceMint



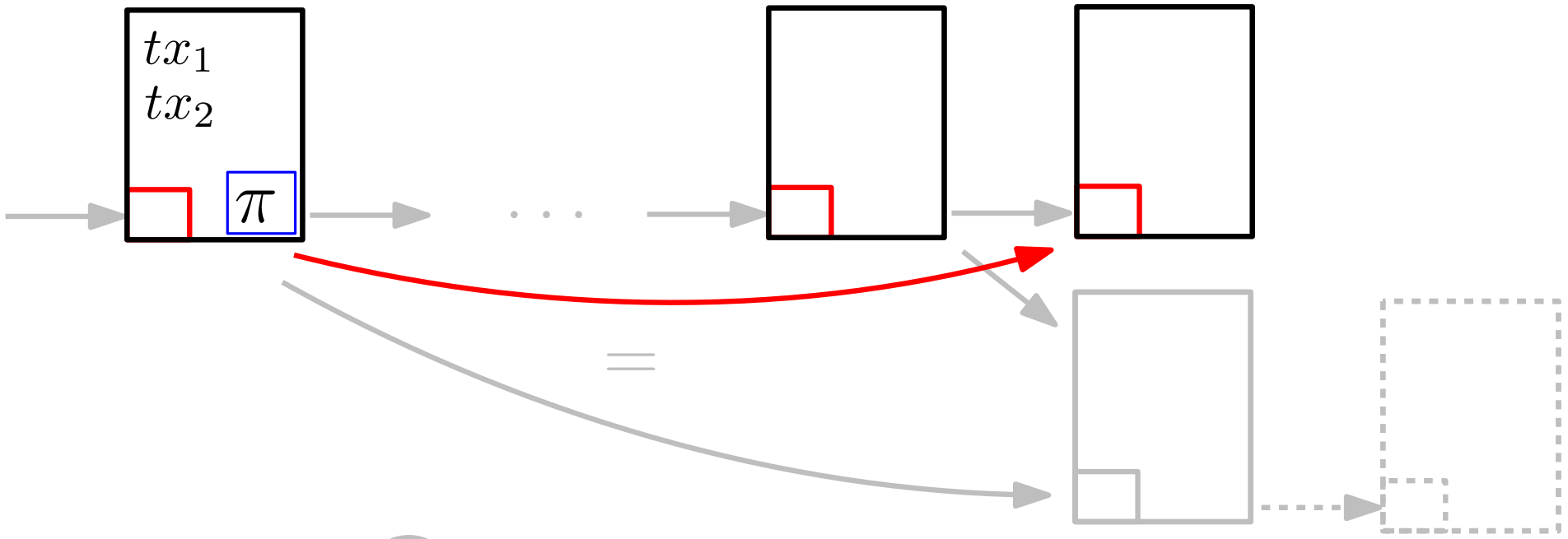
$\neq$ Bitcoin: (3)

$\Rightarrow$ **miners might grind blocks leading to good challenge in future**

$\Rightarrow$ proof of work

Make challenge hash of π only

SpaceMint



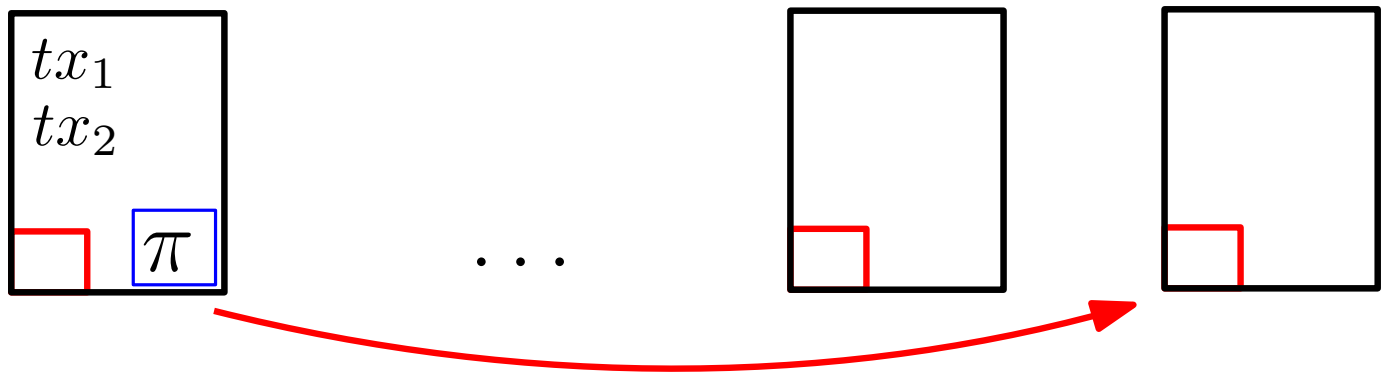
$\neq$ Bitcoin: (3)

$\Rightarrow$ **miners might grind blocks leading to good challenge in future**

$\Rightarrow$ proof of work

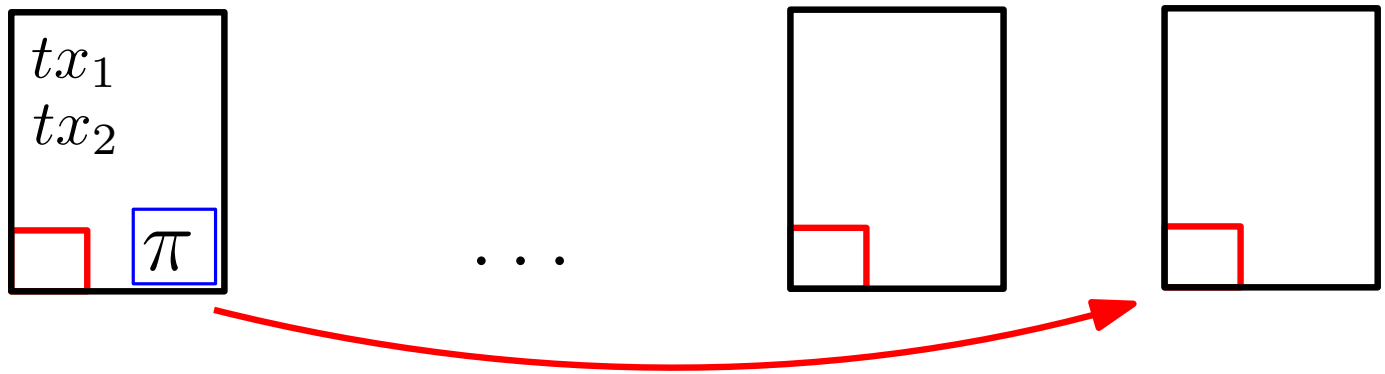
Make challenge hash of π only

SpaceMint



- Transactions not hashed
  $\Rightarrow$ not consolidated in chain!
- Blocks not linked to previous block
  $\Rightarrow$ consensus??

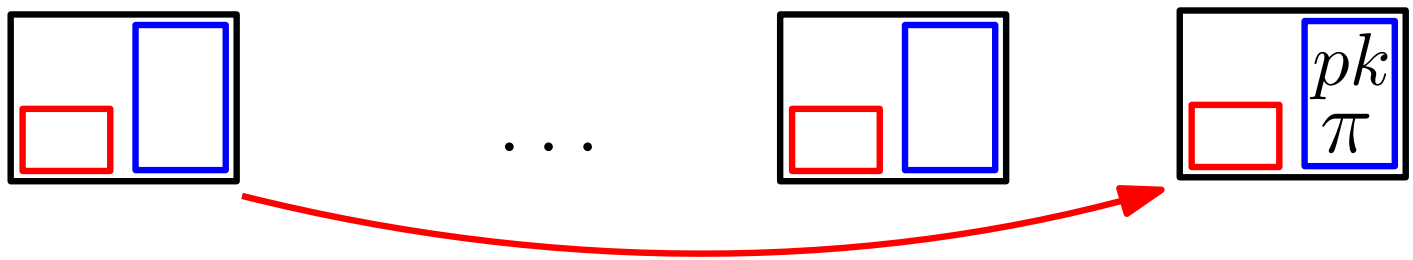
SpaceMint



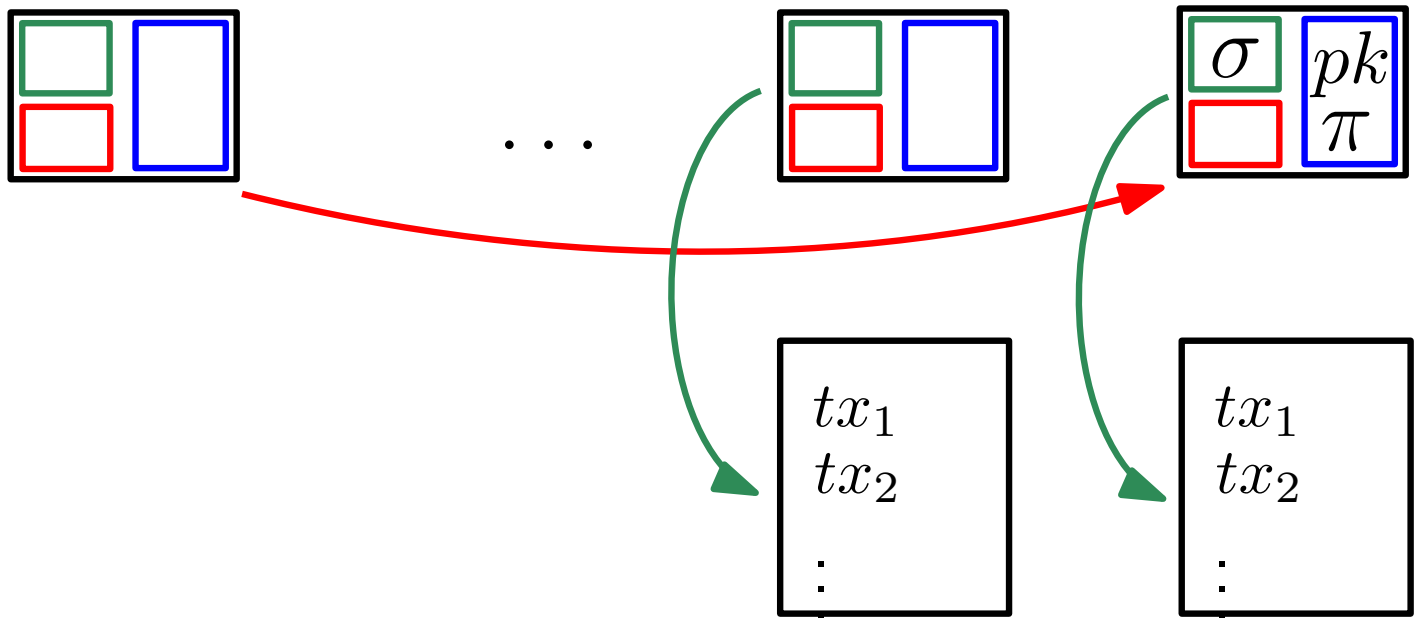
- Transactions not hashed
  $\Rightarrow$ not consolidated in chain!
- Blocks not linked to previous block
  $\Rightarrow$ consensus??

New blockchain structure

SpaceMint

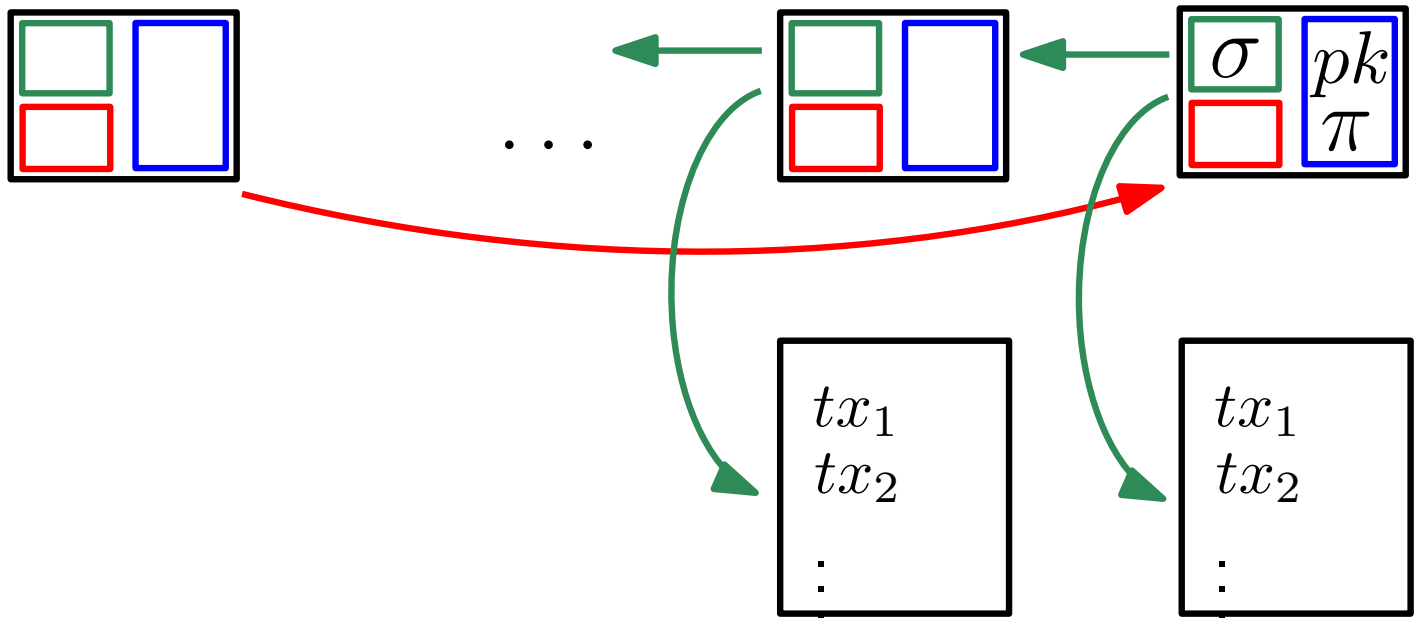


SpaceMint



Use **signatures** (tied to proof) to link blocks

SpaceMint



Use **signatures** (tied to proof) to link blocks

SpaceMint

More ecological?

- no ongoing cost
- resources recyclable
- unused disk space $\Rightarrow$ decentralized

Y a-t-il des questions?