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

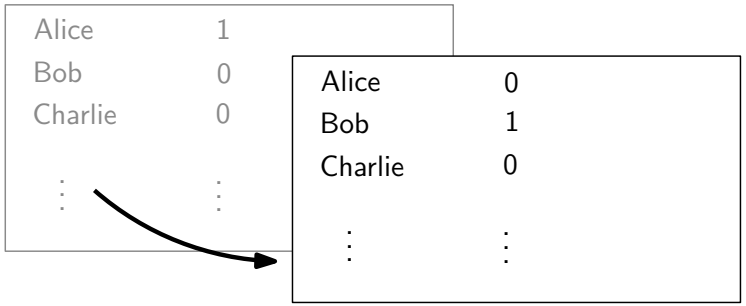
1. **Bitcoin**
   - Transactions
   - Blockchain
   - Proof of work
   - Problems with PoW
2. **SpaceMint**
   - Proofs of space
   - Issues with PoSp
   - New blockchain format

Bitcoin

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

Ledger

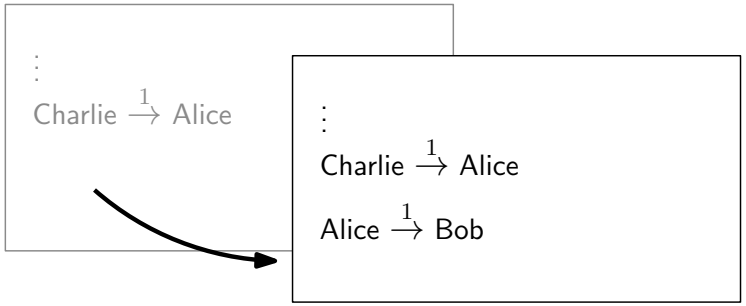
Public ledger



Alice: transfer 1 $\rightarrow$ Bob

Ledger

Public ledger (records all transactions)



Alice: transfer 1 $\rightarrow$ Bob

how to identify?

Transactions

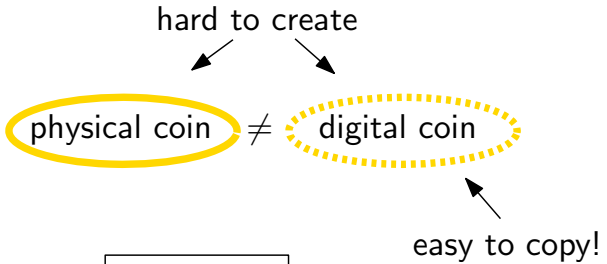
- Alice owns $\boxed{pk_A}$ i.e. it's in the ledger
- Bob creates $\boxed{pk_B}$
- Alice signs $\boxed{pk_A \rightarrow pk_B}$ and adds to ledger

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

Double-spending



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

Ledger only accepts if

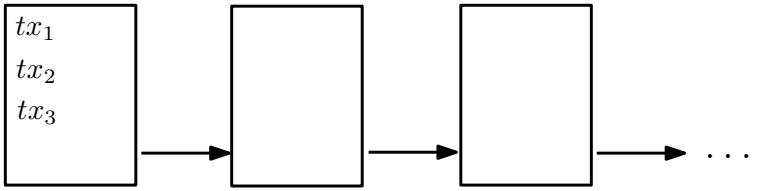
- exists transaction $\boxed{* \rightarrow pk_A}$!
- no transaction ~~$\boxed{pk_A \rightarrow *}$~~

Decentralization

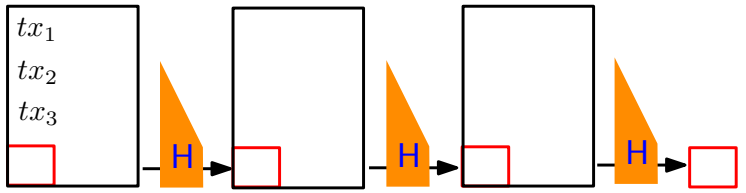
How to eliminate authority that

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

The Blockchain



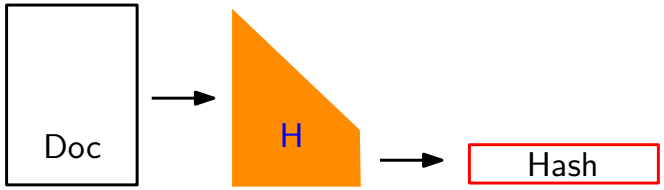
The Blockchain



- blocks linked by including hash of previous block
  ⇒ **cannot mofify block w/o changing everything after**

acts as fingerprint
for whole chain

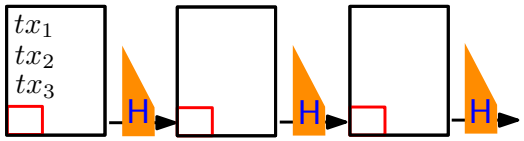
Cryptographic hash functions



- outputs look random
  ⇒ small modifs result in huge changes
  ⇒ hard to find preimage

  ⇒ **best way to find input with hash from some subset is randomly trying**

The Blockchain

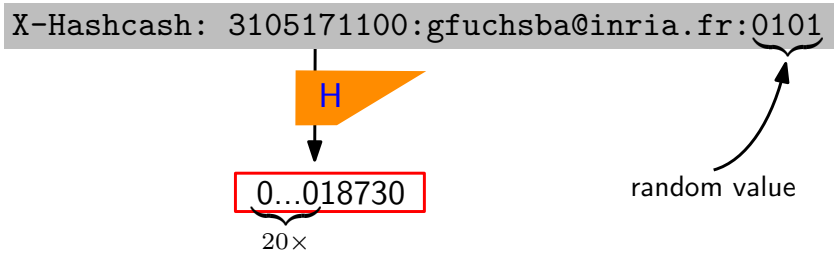


- transactions collected into block
- new block added & published every 10min
  ⇒ who adds block?

- assume mechanism chooses random user
  ⇒ user could be malicious
  ⇒ Sybil attacks? ⇒ Proof of work

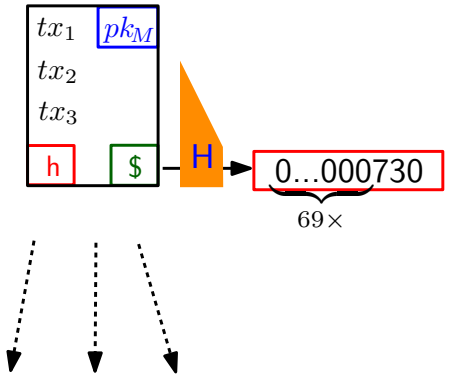
Proof of work

- 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

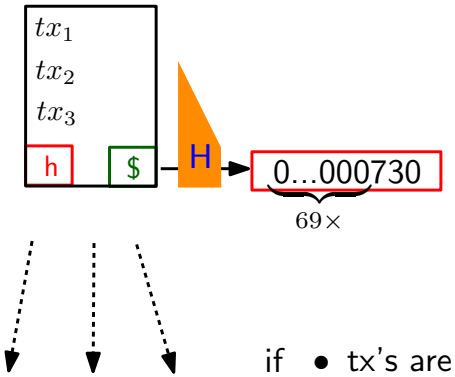


- Incentive?

  $\Rightarrow$ reward bitcoins!

  (all bitcoins created this way)

Mining

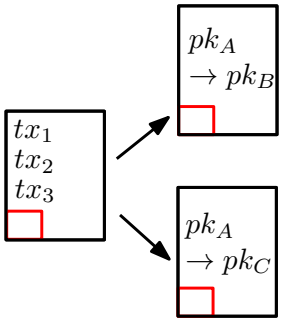


- collect transactions
- find value $ yielding small hash
- broadcast block

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

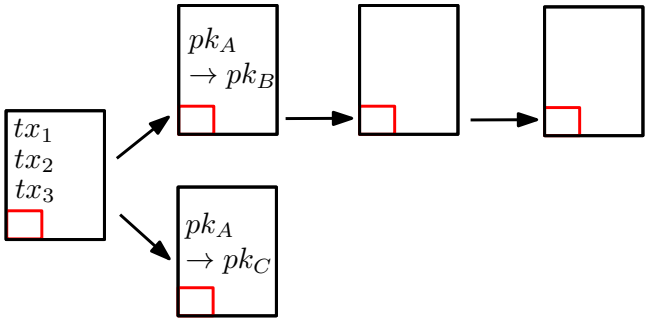
  $\Rightarrow$ add block to local copy of blockchain

Forks



- Double-spending!

Forks



"Always mine on the longest chain"

Secure if majority of miners is honest

$\Rightarrow$ wait for 6 blocks before accepting payment

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

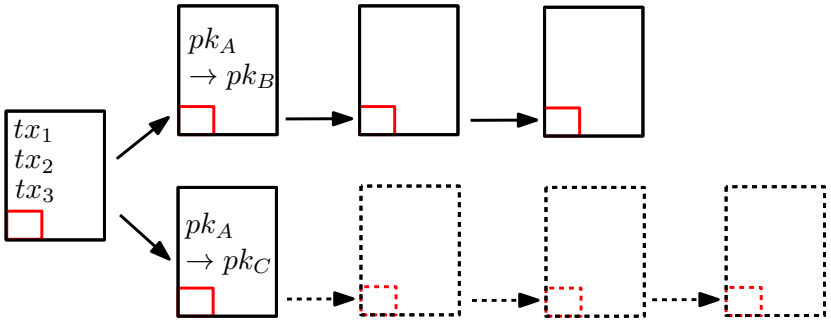
Problems

- 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?**

Forks



The "51%-attack"

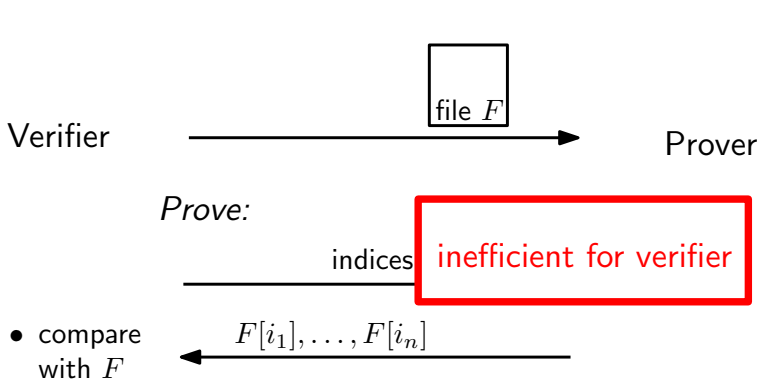
Proof of stake

- 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

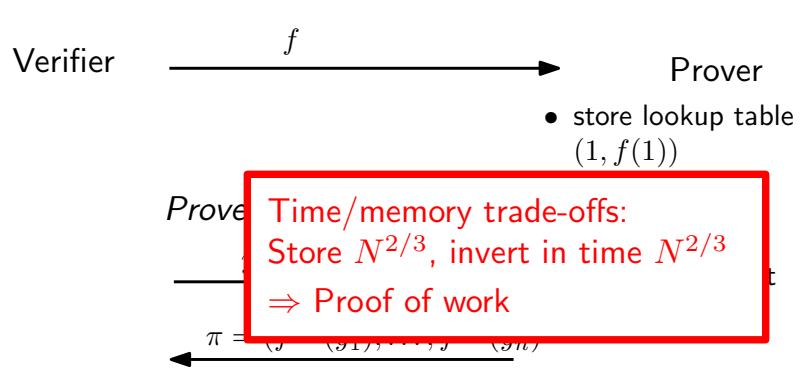
Trivial solution



Proof of space

- prove that you've allocated disk space

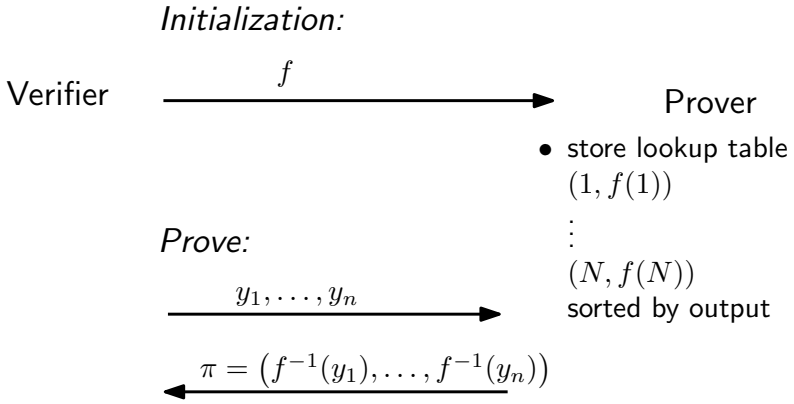
A better solution



Proof of space

- prove that you've allocated disk space

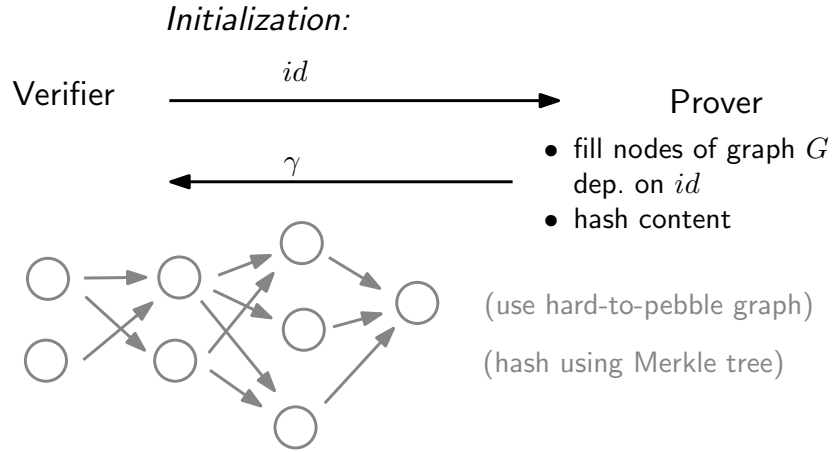
A better solution



Proof of space

- prove that you've allocated disk space

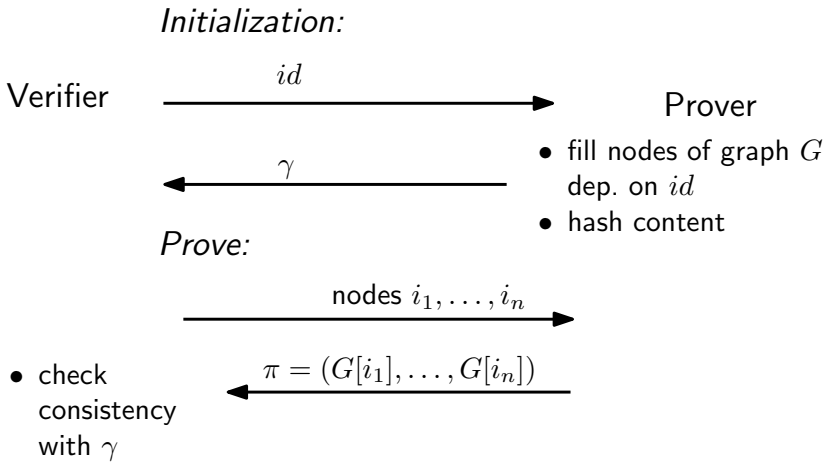
[DFKP'15]



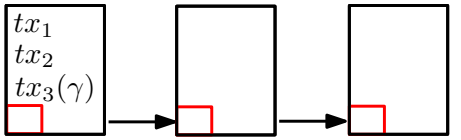
Proof of space

- prove that you've allocated disk space

[DFKP'15]



SpaceMint

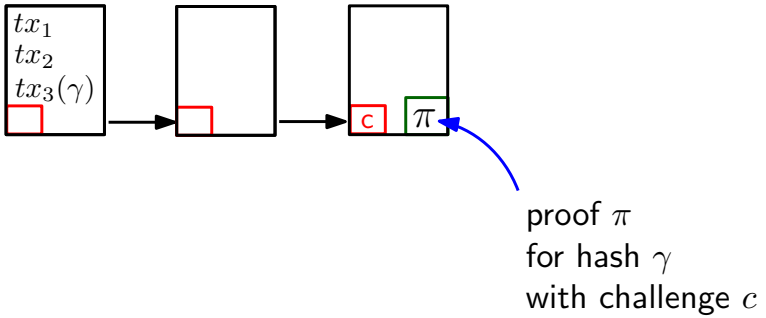


- Miner initializes space with $id = pk$
- broadcasts γ
- γ gets added to chain

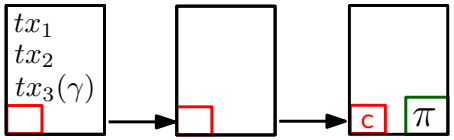
SpaceMint

- 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



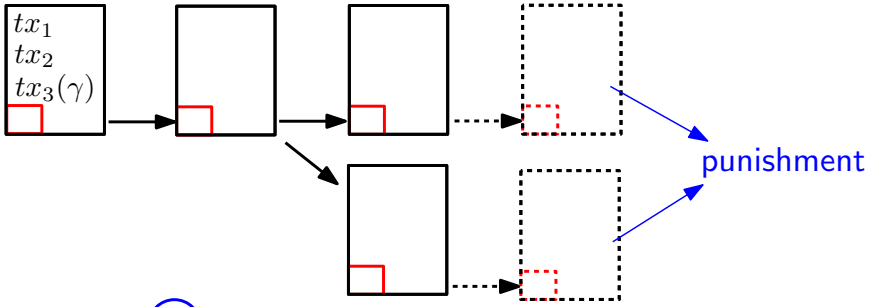
SpaceMint



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

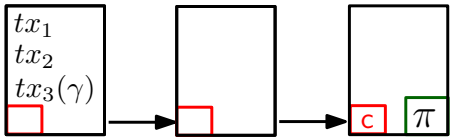


$\neq$ Bitcoin: (1)

- *easy* to generate proofs!
  - $\Rightarrow$ **miners try to extend every chain**
  - $\Rightarrow$ no consensus!

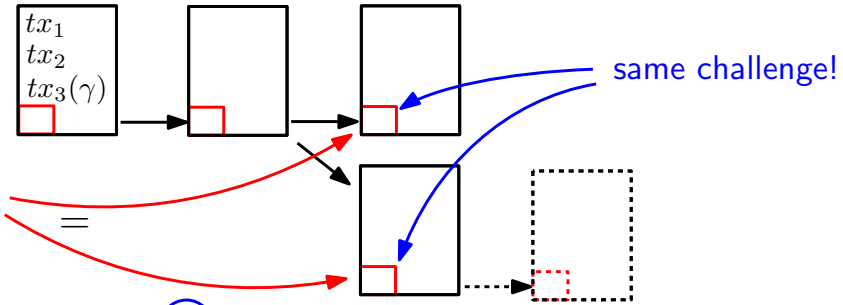
Forbid extending 2 chains

SpaceMint



Does this work?

SpaceMint

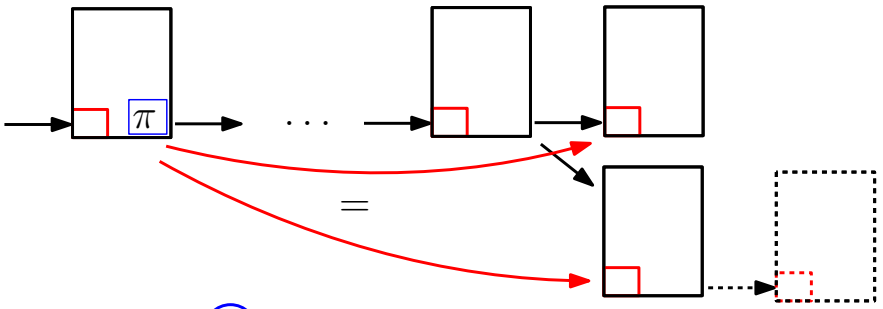


$\neq$ Bitcoin: (2)

- *easy* to check if good solution!
  - $\Rightarrow$ **miners might not extend best chain**
  - $\Rightarrow$ no consensus!

Take challenge from past

SpaceMint



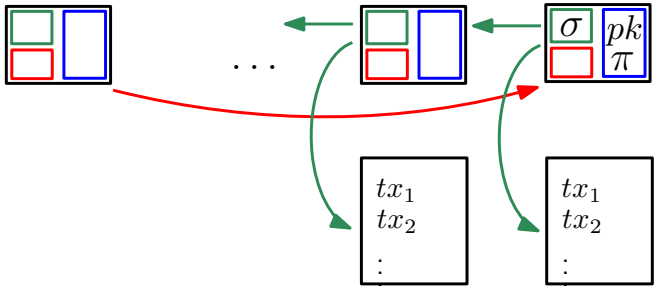
$\neq$ Bitcoin: (3)

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

$\Rightarrow$ proof of work

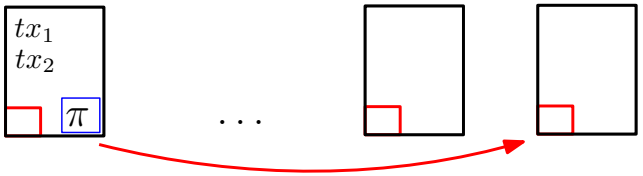
Make challenge hash of π only

SpaceMint



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

SpaceMint



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

New blockchain structure

SpaceMint

More ecological?

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