Blockchain technology and Smart Contracts

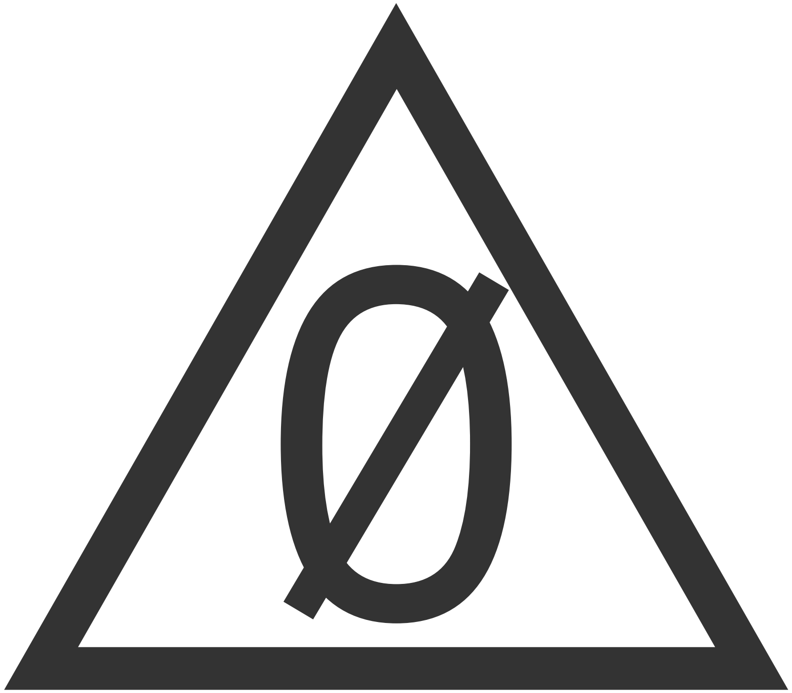
Carlos G. Oliver
Pericles Philippopoulos

Local Logic

February 2018

Delphi Crypto

Research



Education

Consultation

info@delphicrypto.com

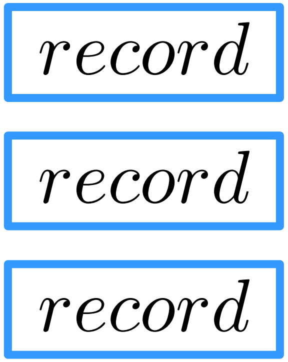
delphicrypto.com

Outline

- Blockchain
- Decentralization
- Smart contracts
- Mining

Blockchain

- list of records



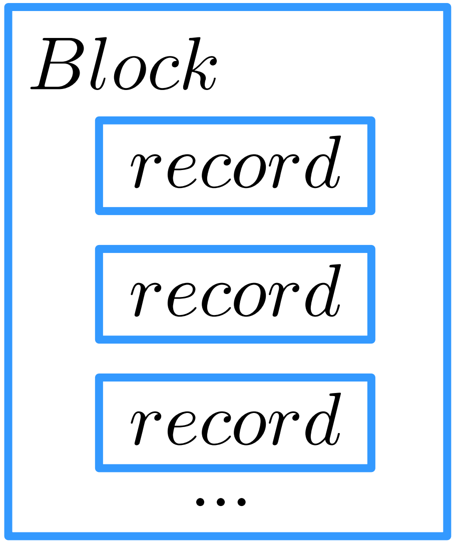
$record$

$record$

$record$

Blockchain

- list of records
- grouped in blocks



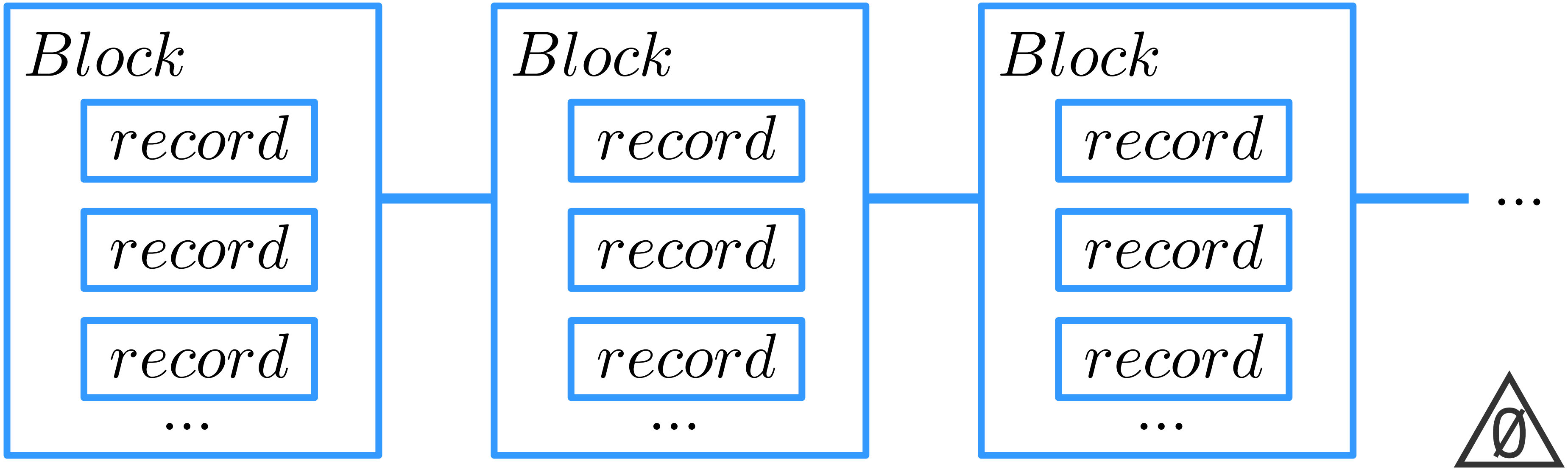
Blockchain

- list of records
- grouped in blocks
- linked in a chain

→

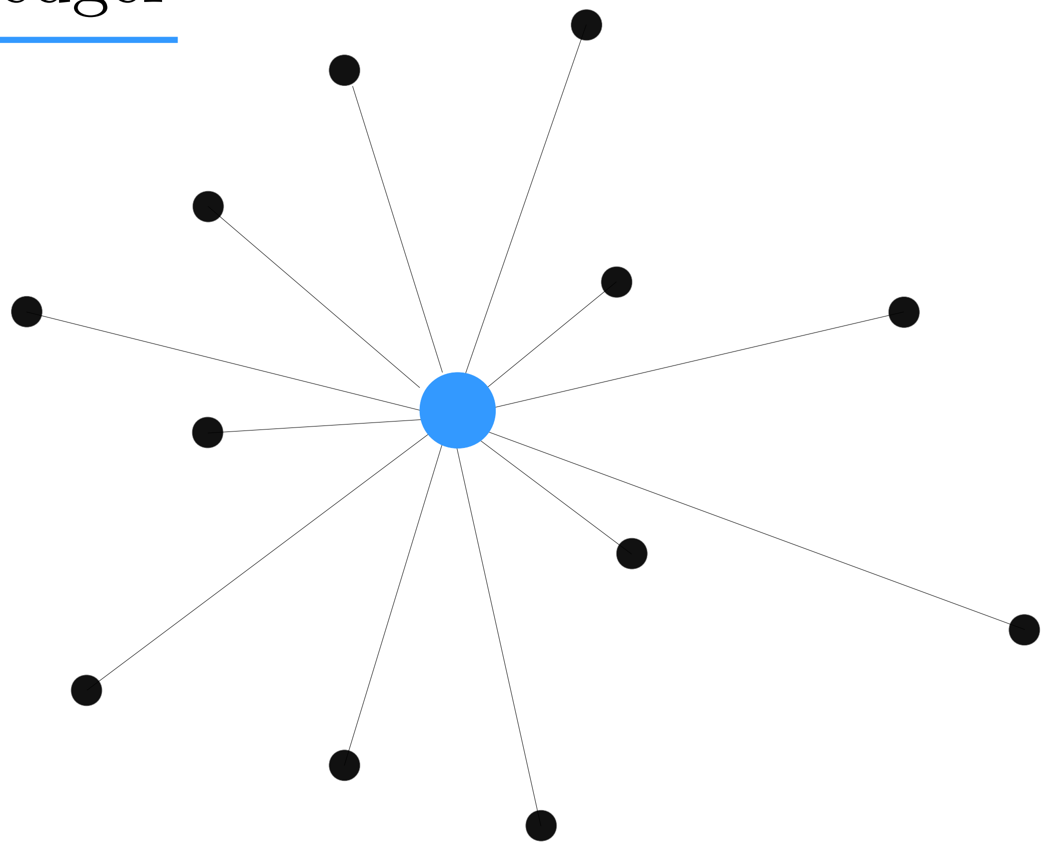
<u>ledger</u>

- add to chain
- can't modify old blocks



Who maintains the ledger?

Centralized Ledger

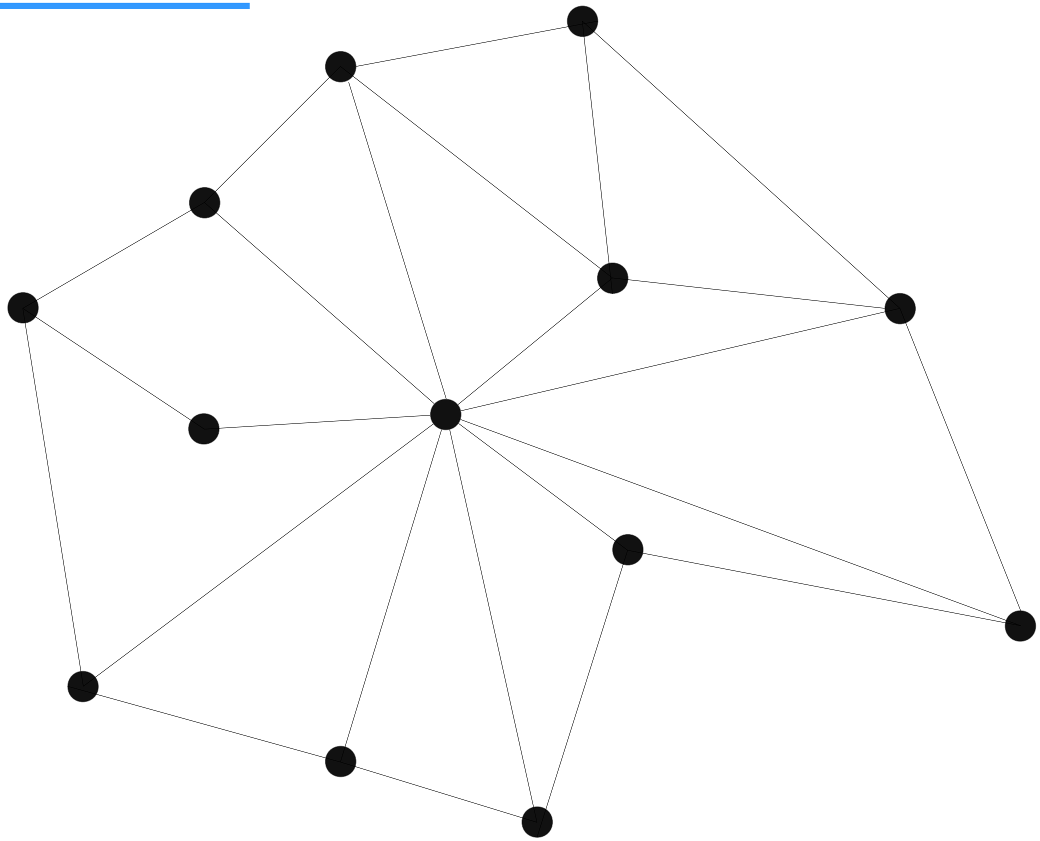


A trusted central authority maintains the ledger.

Blockchain

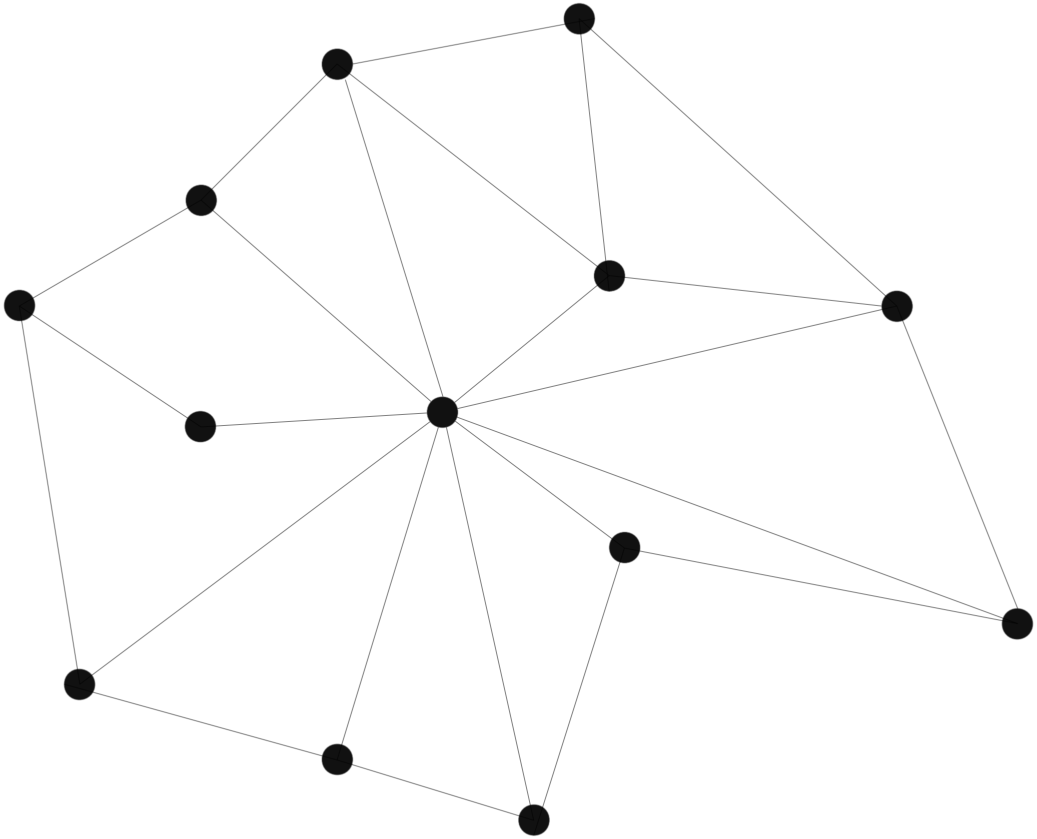
Decentralized Ledger

Distributed



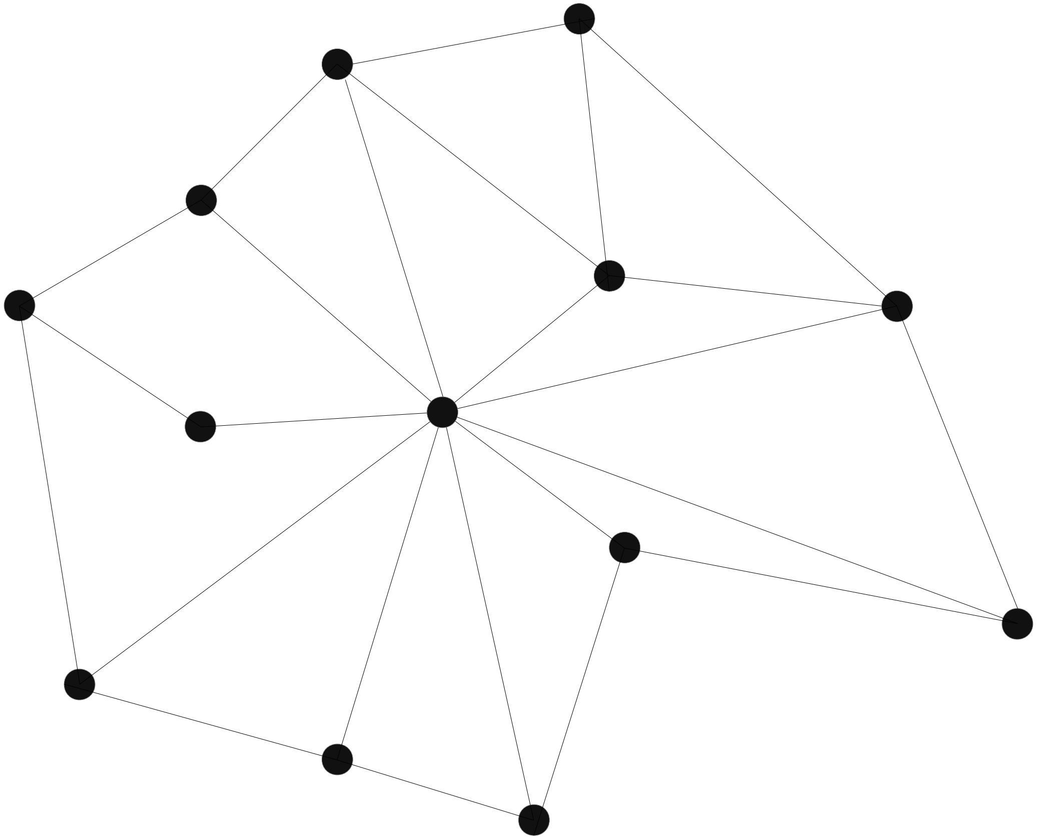
All peers in the network maintain the ledger.

Why decentralization?



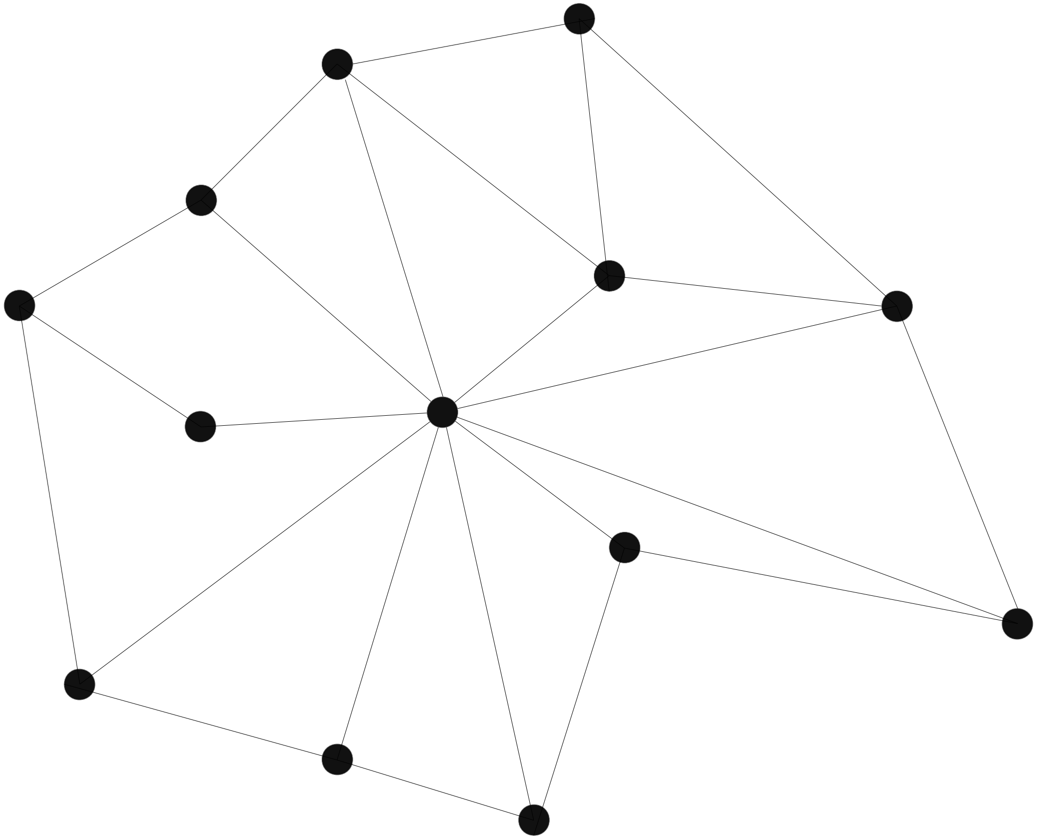
Why decentralization?

Transparency → all records fully traceable and immutable.



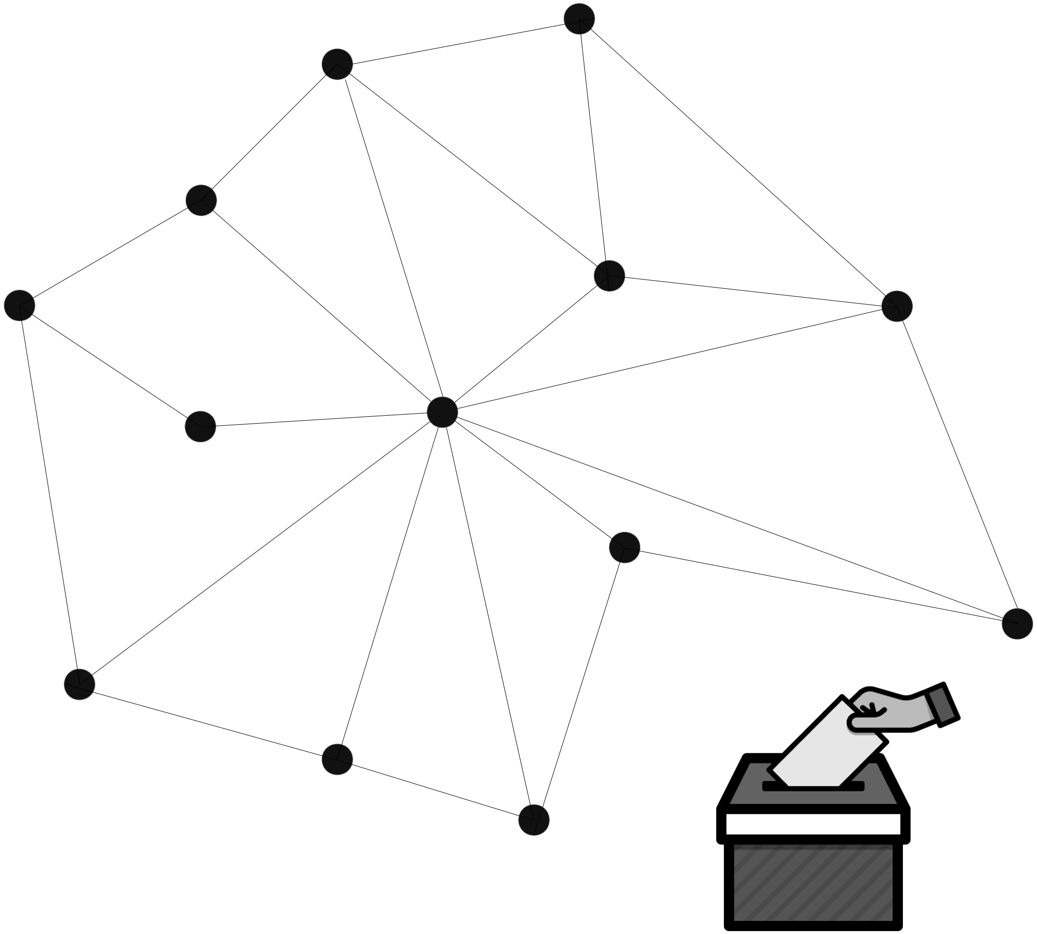
Why decentralization?

Security → Trustless, no single point of failure



Why decentralization?

Governance → Community-based decisions.



DELPHI

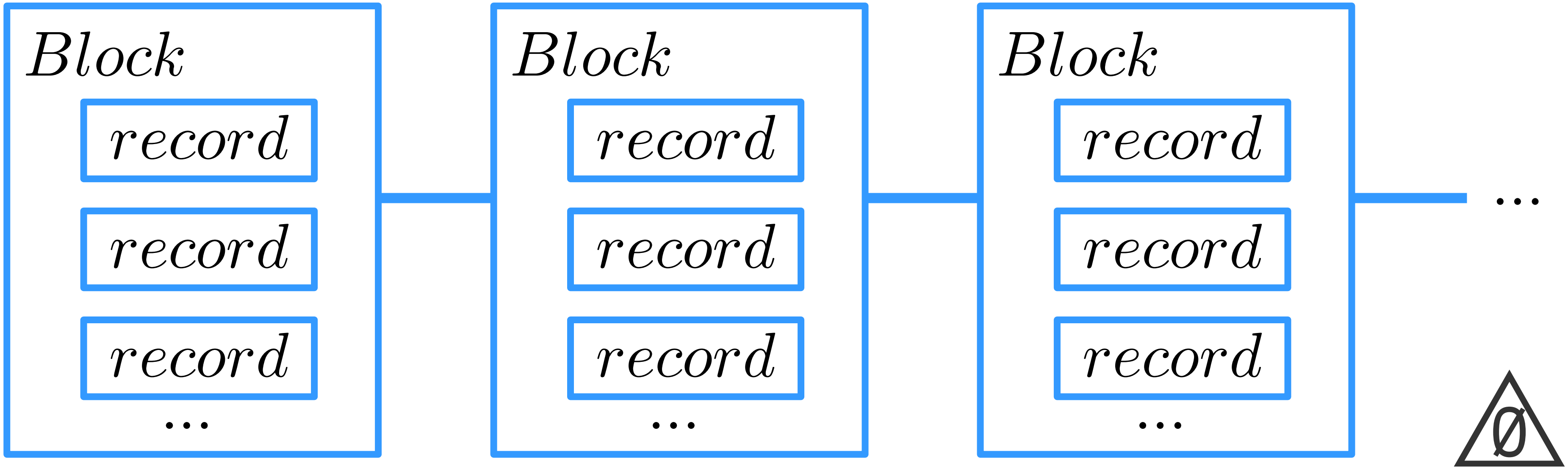
Public Blockchain: Bitcoin

‘Original Blockchain’

- cryptocurrency
  - → blockchain keeps track of wealth
- open source (Ex. Litecoin)
- trustless
- secured by miners
- whitepaper: bitcoin.org/bitcoin.pdf

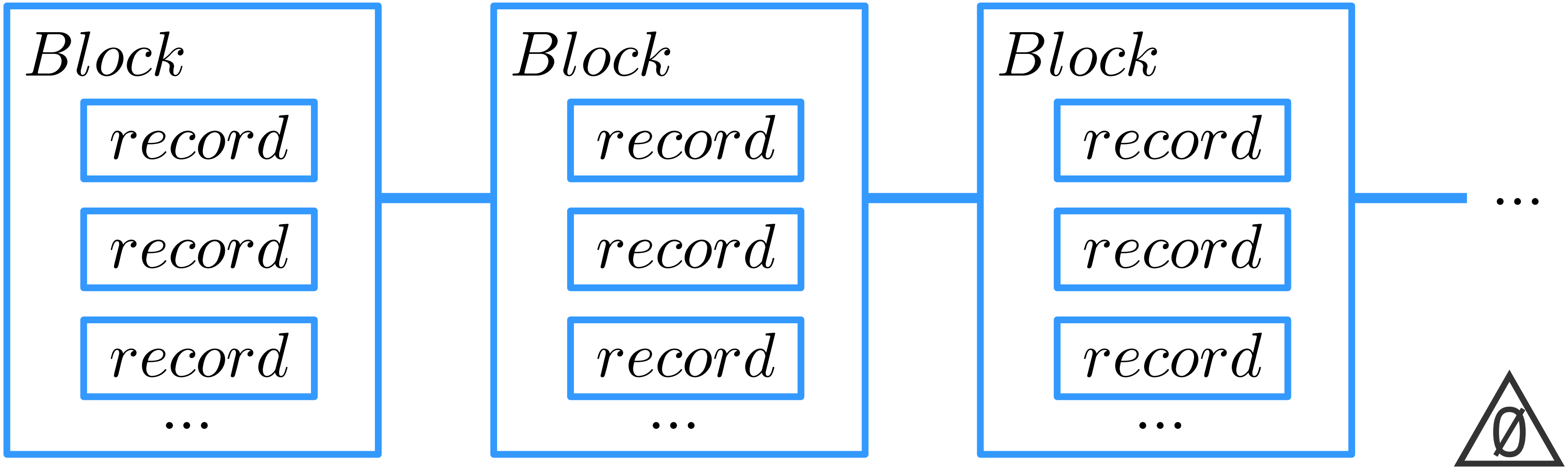
Records are “Smart Contracts”

- Piece of code



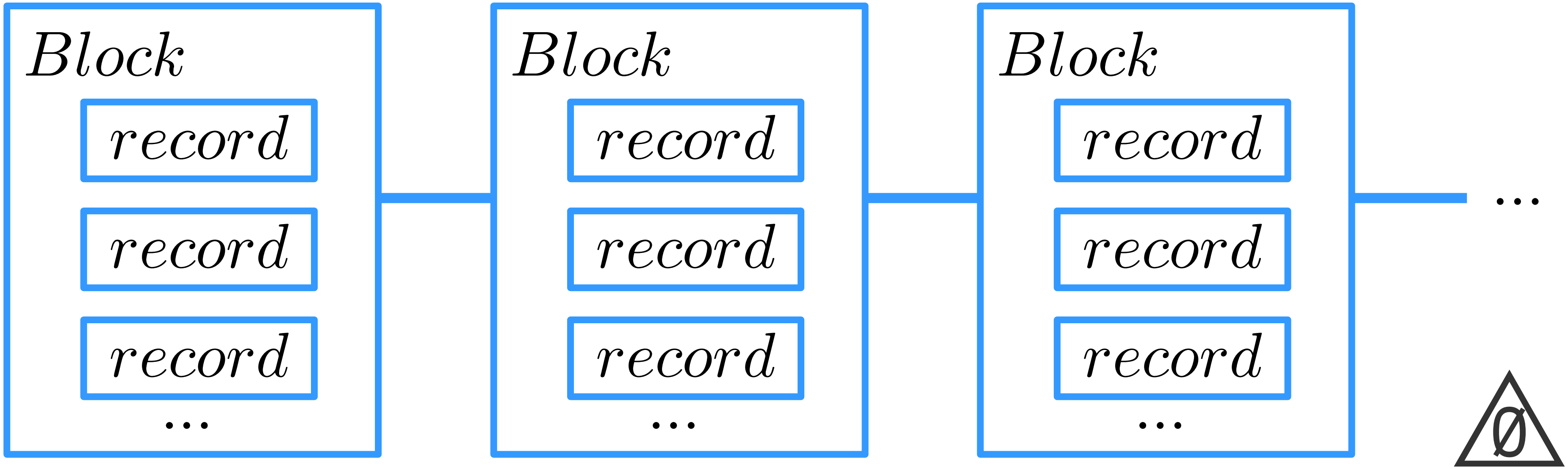
Records are “Smart Contracts”

- Piece of code
- Stored on the blockchain

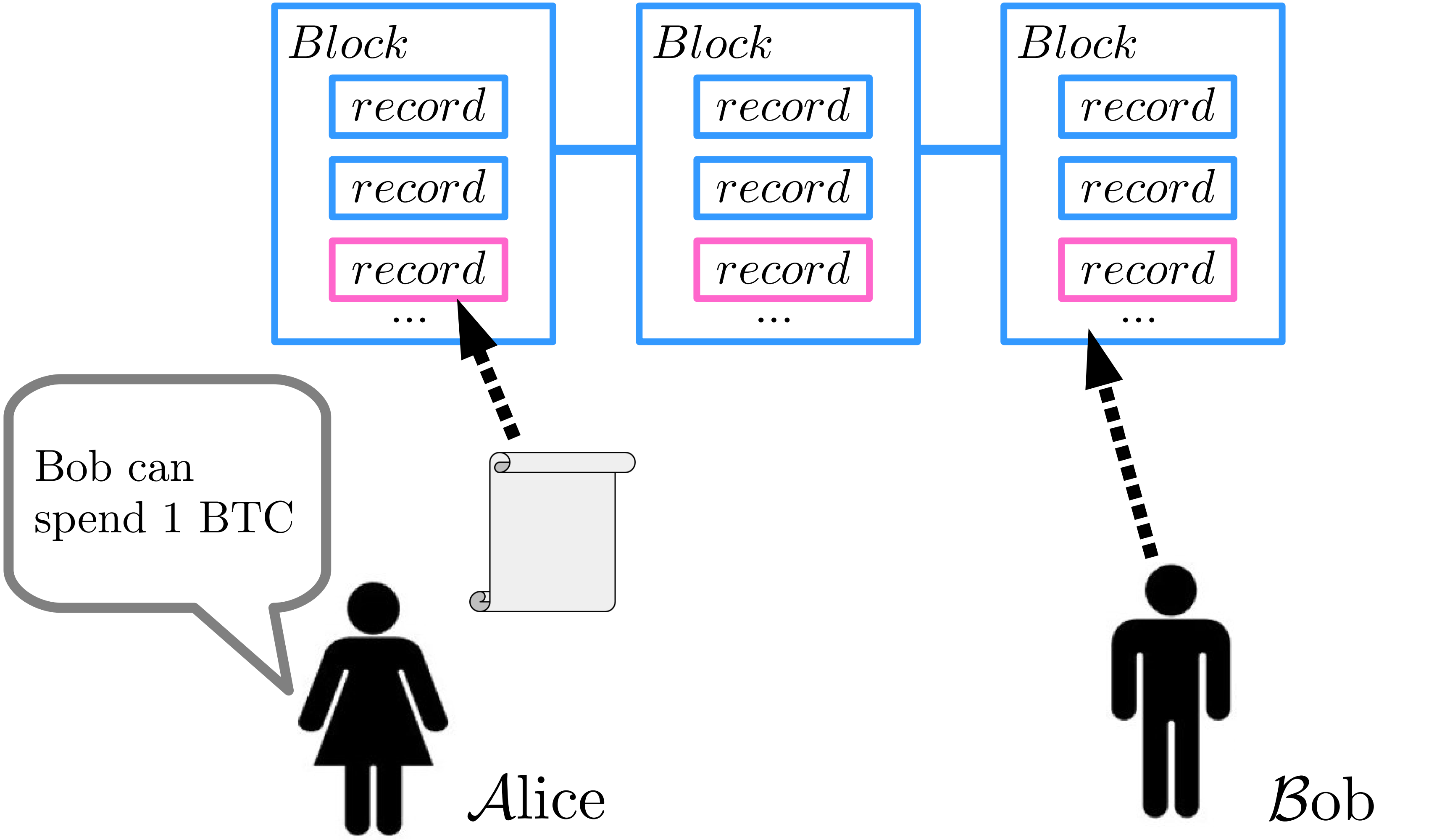


Records are "Smart Contracts"

- Piece of code
- Stored on the blockchain
- Execution state is validated by the network



Records are “Smart Contracts”



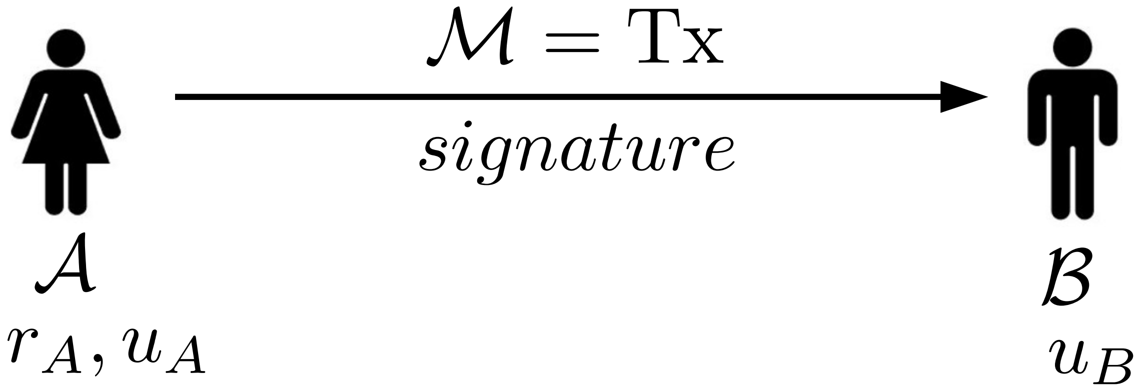
Bitcoin Transactions ₿

Cryptographic Signature

- public and private key pair generated
- only $\mathcal{A}$ knows private key, r_A
- public key, u_A, known by everyone

Signature

$$sig : r_A, \mathcal{M} \rightarrow signature$$



$\mathcal{M} = \mathrm{Tx}$

$signature$

$\mathcal{A}$

r_A, u_A

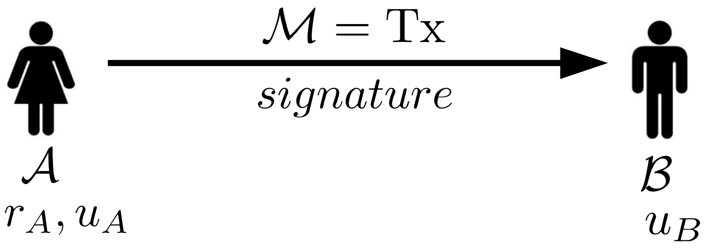
$\mathcal{B}$

u_B

Bitcoin Transactions

Cryptographic Signature

- public and private keys generated
- only $\mathcal{A}$ knows private key, r_A
- public key, u_A, known by everyone



Verification

$$check : u_A, \mathcal{M}, signature \rightarrow Yes/No$$

The $\mathcal{M}$essage can be verified by $\mathcal{B}$ob or anyone else

Bitcoin Transactions ₿

Overview

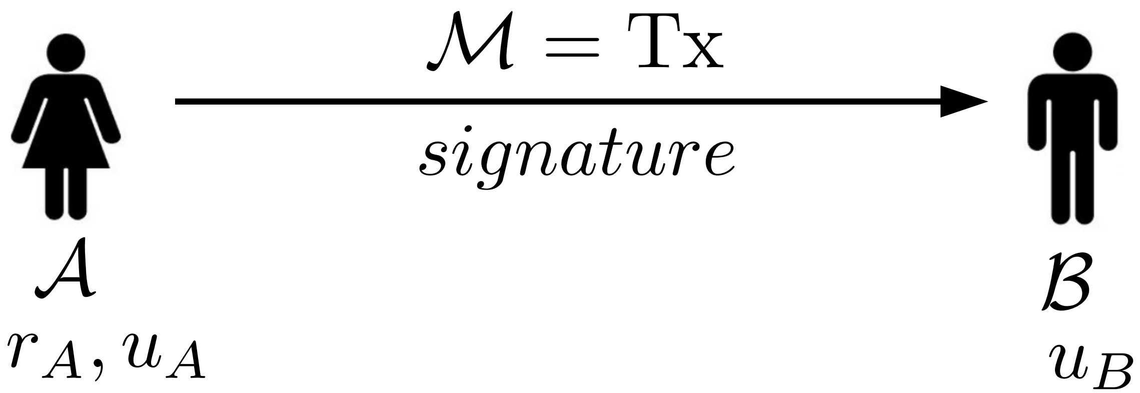
- participants in the network identified by public keys

  $\longrightarrow$ $\sim$ anonymity

- access to private key means access to funds

  $\longrightarrow$ $\sim$ access to ‘wallet’

- transaction broadcasted and added to the ledger



$\mathcal{M} = \mathrm{Tx}$

signature

$\mathcal{A}$

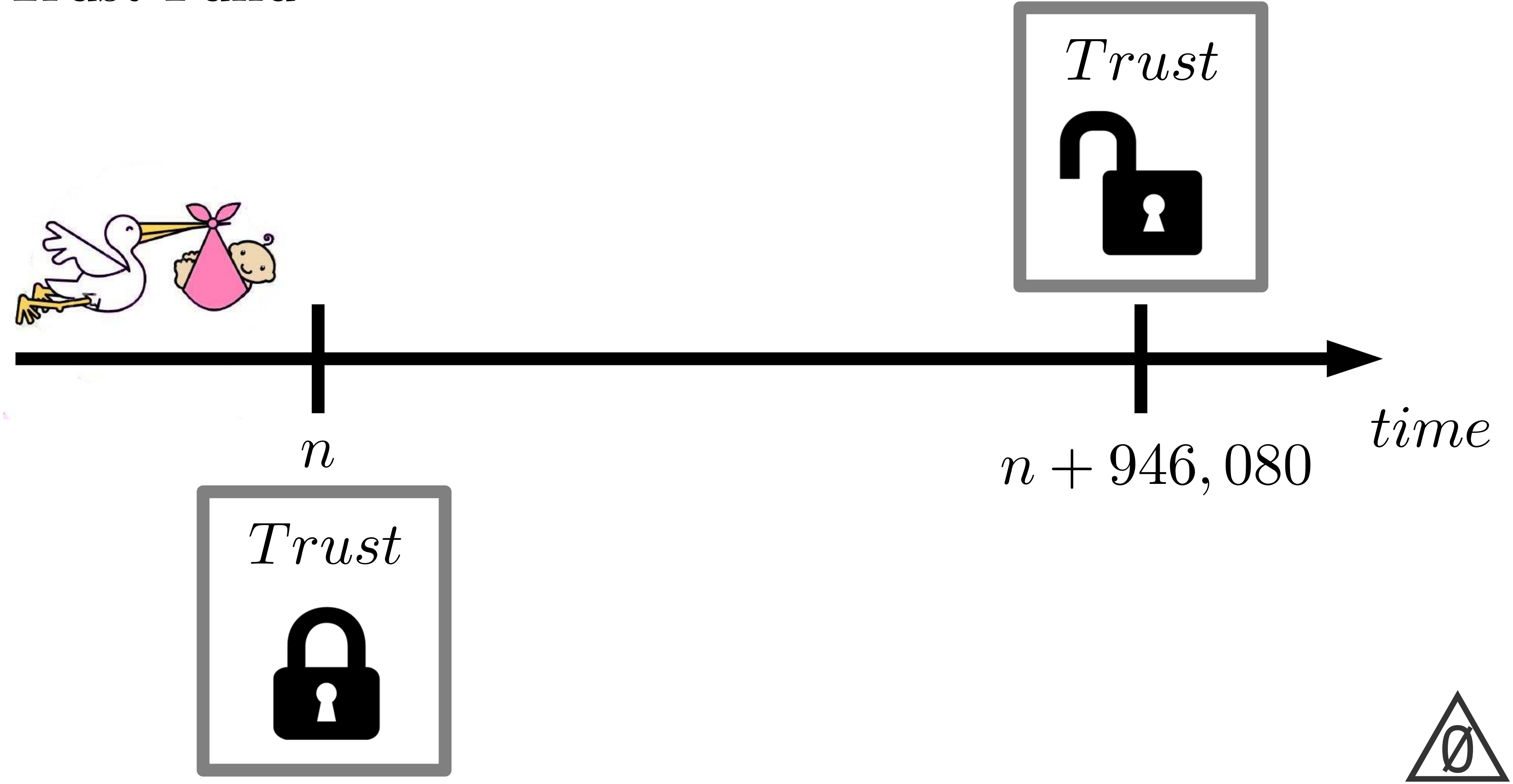
r_A, u_A

$\mathcal{B}$

u_B

Simple smart contract

Trust Fund



$Trust$

n

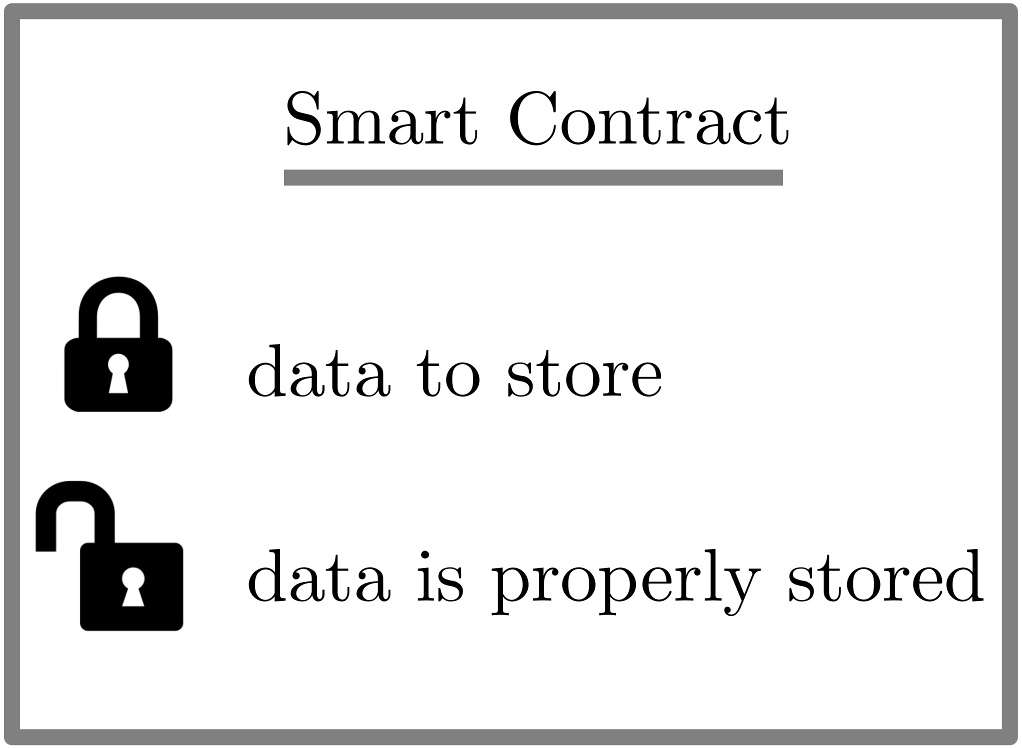
$n + 946,080$

$time$

$Trust$

Other smart contracts

File Storage



Smart Contract

🔒 data to store

🔓 data is properly stored

Other smart contracts

File Storage

STORJ.IO

sia

MaidSafe

Filecoin

Ethereum

- cryptocurrency
- Turing-complete language
- more complicated smart contracts

  → decentralized applications (dApps)

Other smart contracts

Distributed Computing

Smart Contract

🔒 computation to run

🔓 computation properly executed

Other smart contracts

Distributed Computing

Other smart contracts

- games: Cryptokitties
- gambling: Etheroll, Funfair, ...
- insurance
- voting
- auctions

Data Marketplace

- tangle (DAG) not blockchain
- sensors around the world - IOT
- data stored on tangle, cannot be corrupted
- all data can be bought or sold

IOTΛ

Delphi Crypto

Thank you!

delphicrypto.com

info@delphicrypto.com

DELPHI

Bitcoin Mining ₿

No central authority

Who keeps track of which transactions are valid?

double spending?

why?

Bitcoin Mining

Cryptographic Hash Function (H)

- maps any input to fixed size output

$$H(\text{a}) = \text{ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb}$$

$$H(\text{``Bible''}) = \text{47f63b8cd8470051acd3a3c0bd5c77c4aa9574d79cf5bfb3e576facabbc11491}$$

Bitcoin Mining ₿

Cryptographic Hash Function (H)

- maps any input to fixed size output
- not invertible

Bitcoin Mining

Cryptographic Hash Function (H)

- maps any input to fixed size output
- not invertible
- not ‘continuous’

$H(\text{bank}) = \text{4381dc2ab14285160c808659aee005d51255add7264b318d07c7417292c7442c}$

$H(\text{Bank}) = \text{676c471bc8dc3d1324133cf087c20aa0137fc02348811e4162c79e560298fb11}$

$H(\text{the bank}) = \text{b3d0b18e01647cc301a5dc022784fd1e5b85475a4dbb14140b983dbf1c5a7be1}$

$H(\text{thebank}) = \text{fc4cb9f881175d7b5ac02906947f288b9998bd9354ea06ddf13fc21fa5c12c4d}$

DELPHI

Bitcoin Mining ₿

Cryptographic Hash Function (H)

- maps any input to fixed size output
- not invertible
- not ‘continuous’
- no collisions

$$x \neq y \implies H(x) \neq H(y)$$

DELPHI

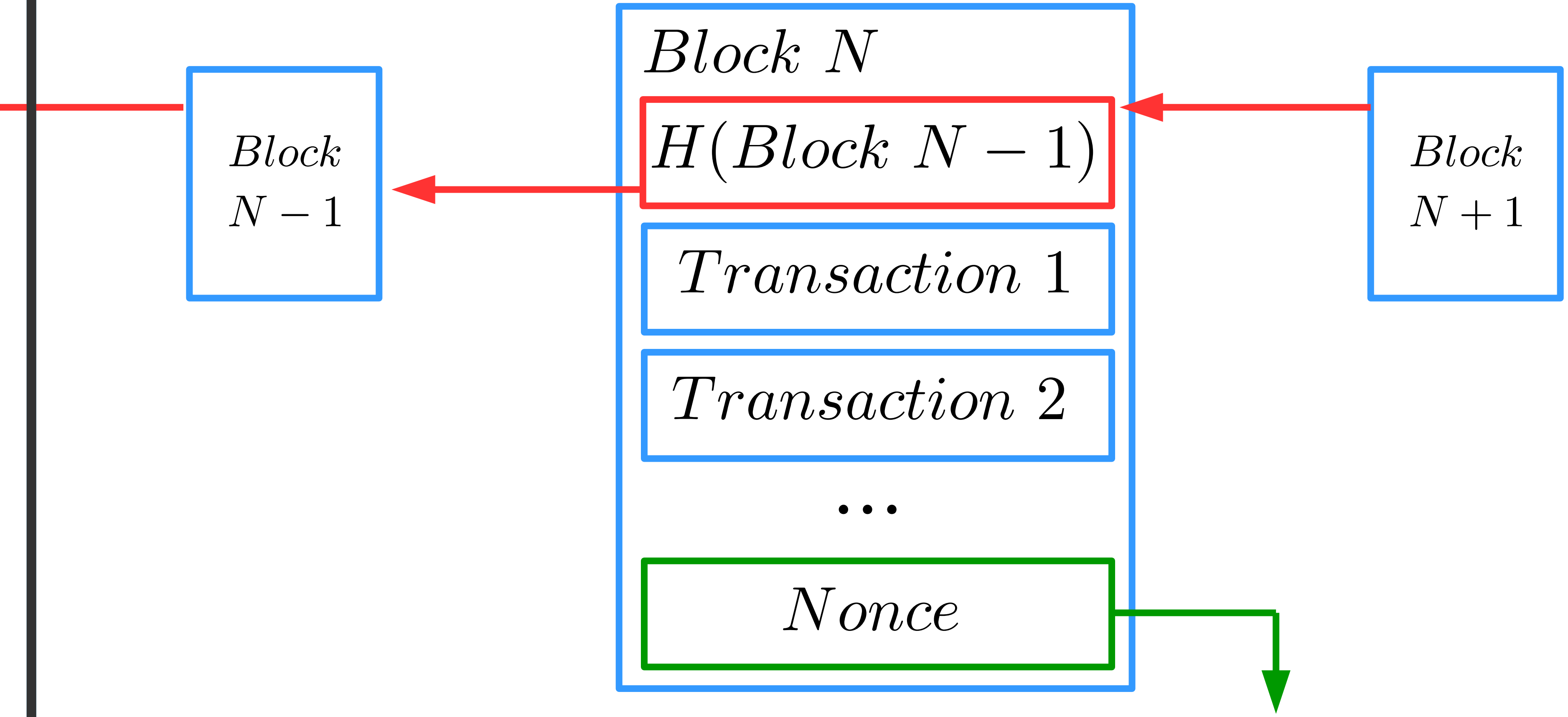
Bitcoin Mining ₿

How does mining work?

- anyone in the network can add block
- hash of the block must start with a certain number of 0's
  - ⟶ determined by a difficulty parameter
  - ⟶ $H(Block) = 00000....ab142a1...$
- blocks contain:
  - ⟶ hash of last block
  - ⟶ valid transactions

Bitcoin Mining

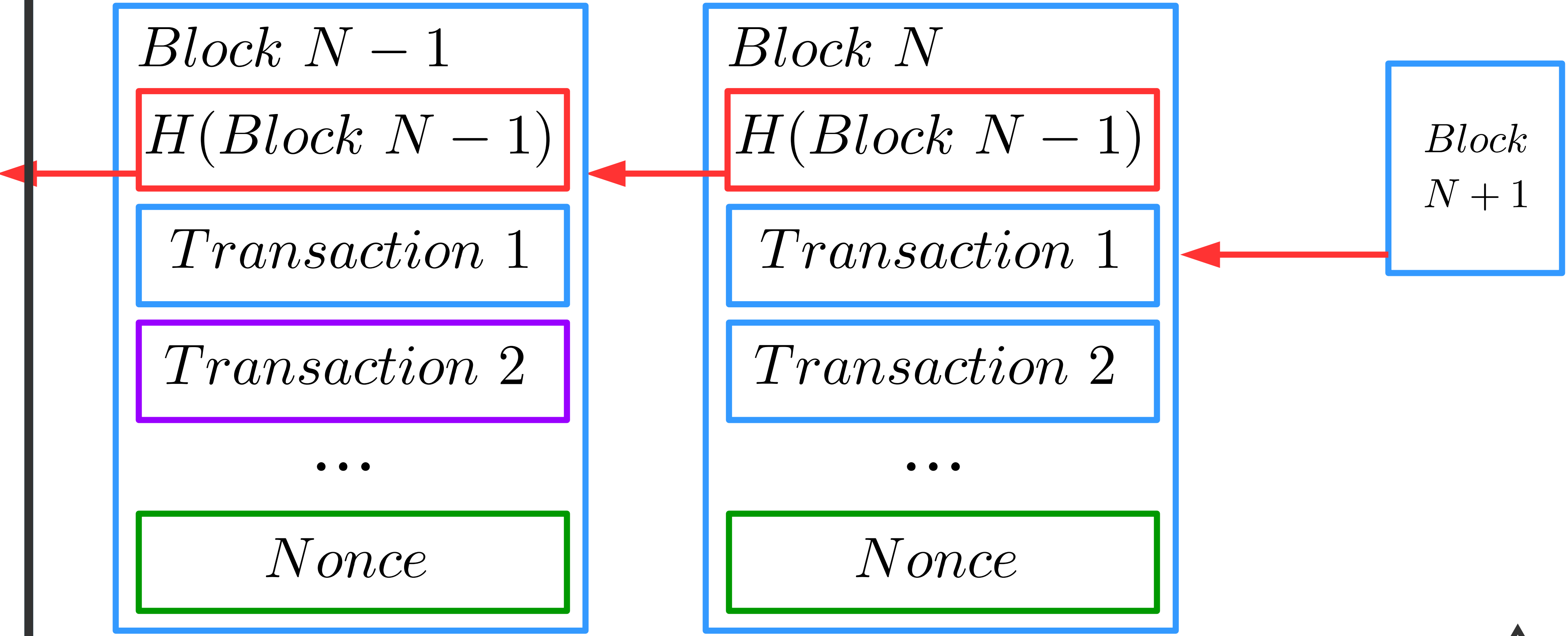
How does mining work?



picked so hash has correct amount of 0's

Bitcoin Mining

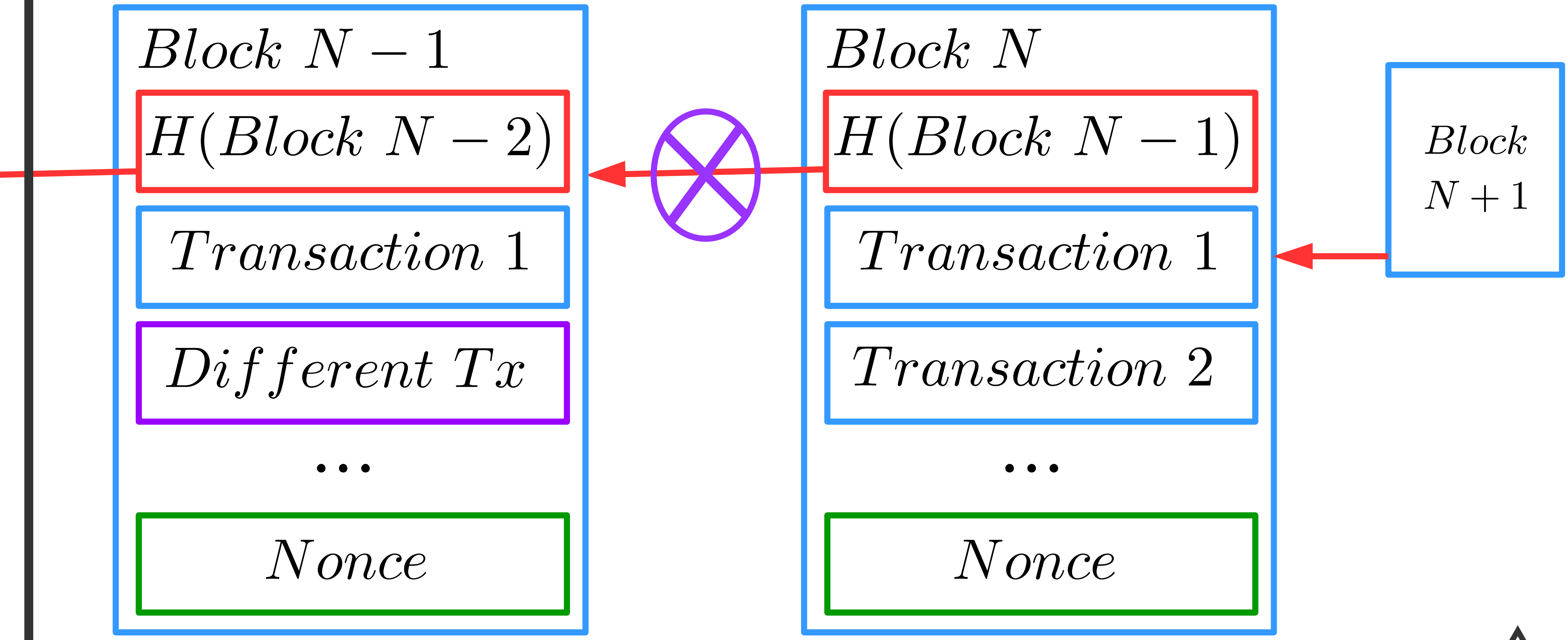
What if someone cheats?



DELPHI

Bitcoin Mining ₿

What if someone cheats?



$Block\ N-1$

$H(Block\ N-2)$

$Transaction\ 1$

$Different\ Tx$

$\cdots$

$Nonce$

$Block\ N$

$H(Block\ N-1)$

$Transaction\ 1$

$Transaction\ 2$

$\cdots$

$Nonce$

$Block$
$N+1$

→ Error gets propagated

Bitcoin Mining

Overview

- miners add 1 MB blocks respecting current difficulty
- network accept valid blocks by adding blocks on the chain
  - ⟶ add blocks to longest valid chain (most work)
- blocks can only be added not modified
- new block is added every 10 minutes (on average)
  - ⟶ difficulty readjusted every 2 weeks
- miners are rewarded for adding blocks
  - ⟶ current reward: 12.5 BTC + fees
  - ⟶ first transaction in the block
  - ⟶ total number of bitcoins is capped ($\sim$ 21 million coins)

Bitcoin Mining ₿

Consumption

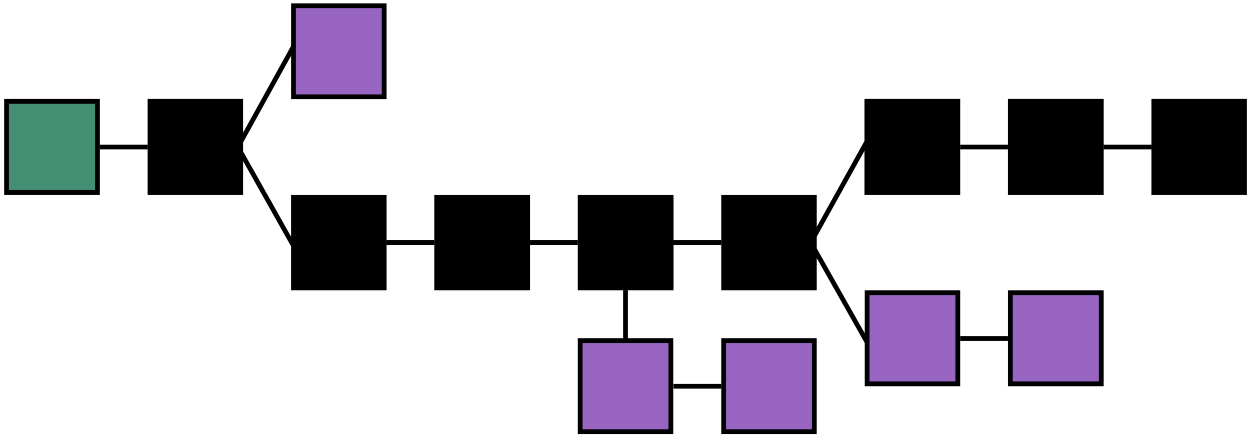
- in the beginning, mining could be done on a PC
- now, there are ‘BTC mining farms’
- hashing electricity consumption
  - ⟶ 0.09% of world’s power
  - ⟶ as much electricity as Syria
  - ⟶ enough to power 1,740,000 US households
  - ⟶ 1 tx ∼ powering 7 houses for a day
- Proposal for a fully decentralized blockchain and proof-of-work algorithm for solving NP-complete problems - arXiv:1708.09419v2

source: https://digiconomist.net/bitcoin-energy-consumption

Bitcoin Mining

Longest Valid Chain

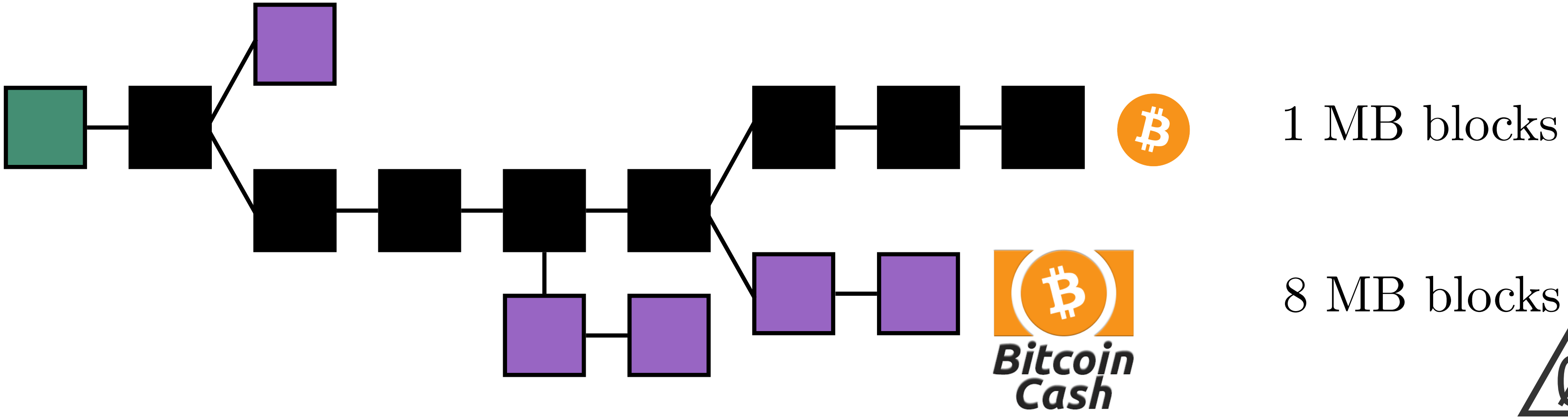
- longest chain will have the most valid transactions
- 51 % attack



Forking and Bitcoin Cash

Resolution of the conflict

- fork the ledger
- same past, different future
- different miners agree to work on different chains



Other Ideas

Cryptocurrencies

- Bitcoin is first, is it best?
- Ethereum: smart contracts
- Iota: tangle
- Quantum Resistant Ledger: ‘resistant’ to quantum computers

IOTA

QRL

The Quantum-Resistant Ledger

Other Ideas

Smart Contracts

- decentralized applications - dApps
- Ex. Pear: decentralized journal
  - ⟶ https://github.com/delphicrypto/Pear

PEAR