Blockchain technology and Smart Contracts

Carlos G. Oliver
Pericles Philippopoulos
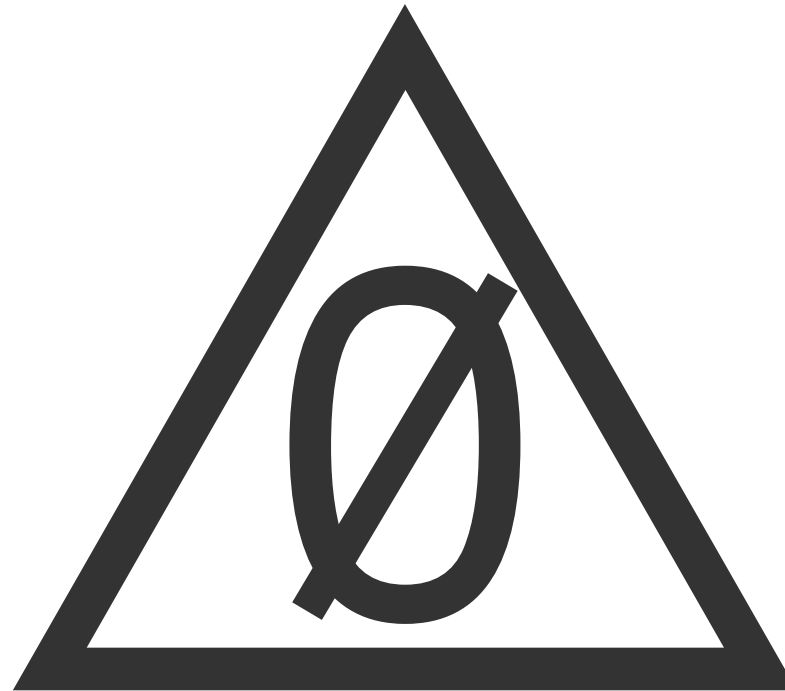
Local Logic: Lunch and Learn
February 2018

Ø
DELPHI

Delphi Crypto

Research

Education

Consultation

info@delphicrypto.com

delphicrypto.com

Outline

- Blockchain

- Decentralization

- Smart contracts

- Mining

DELPHI

Blockchain

- list of records

$$\boxed{record}$$

$$\boxed{record}$$

$$\boxed{record}$$

Blockchain

- list of records

- grouped in blocks

Block

| *record* |
| *record* |
| *record* |

...

DELPHI

Blockchain

- list of records

- grouped in blocks

- linked in a chain

$\longrightarrow$

ledger

- add to chain

- can't modify old blocks

Block	*Block*	*Block*
record	record	record
record	record	record
record	record	record
...	...	...

...

DELPHI
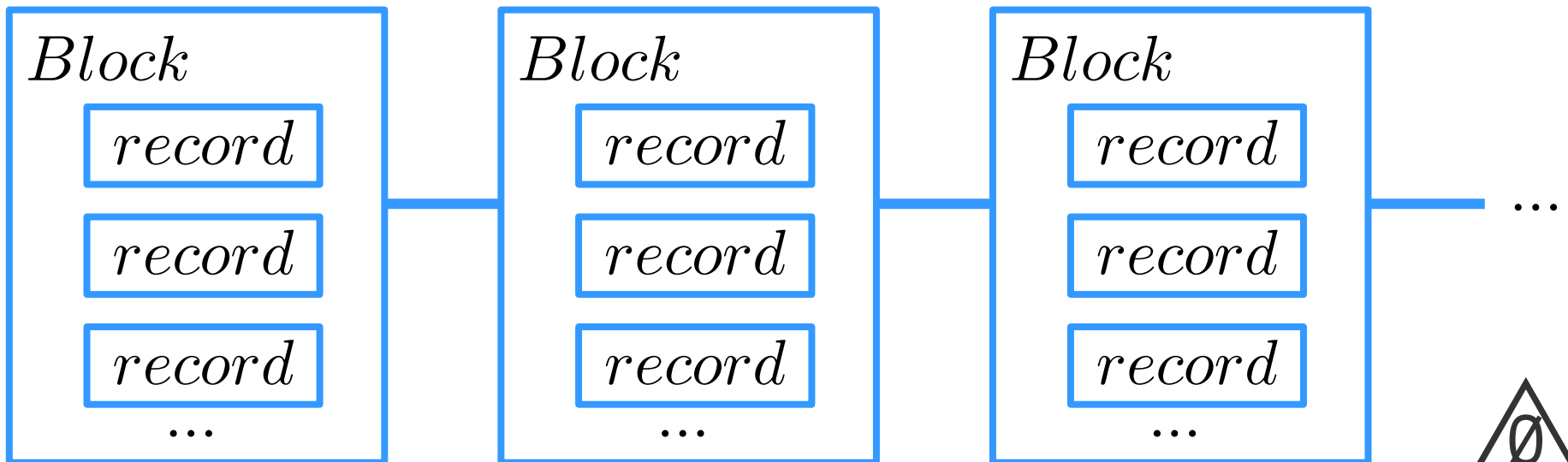
Who maintains the ledger?
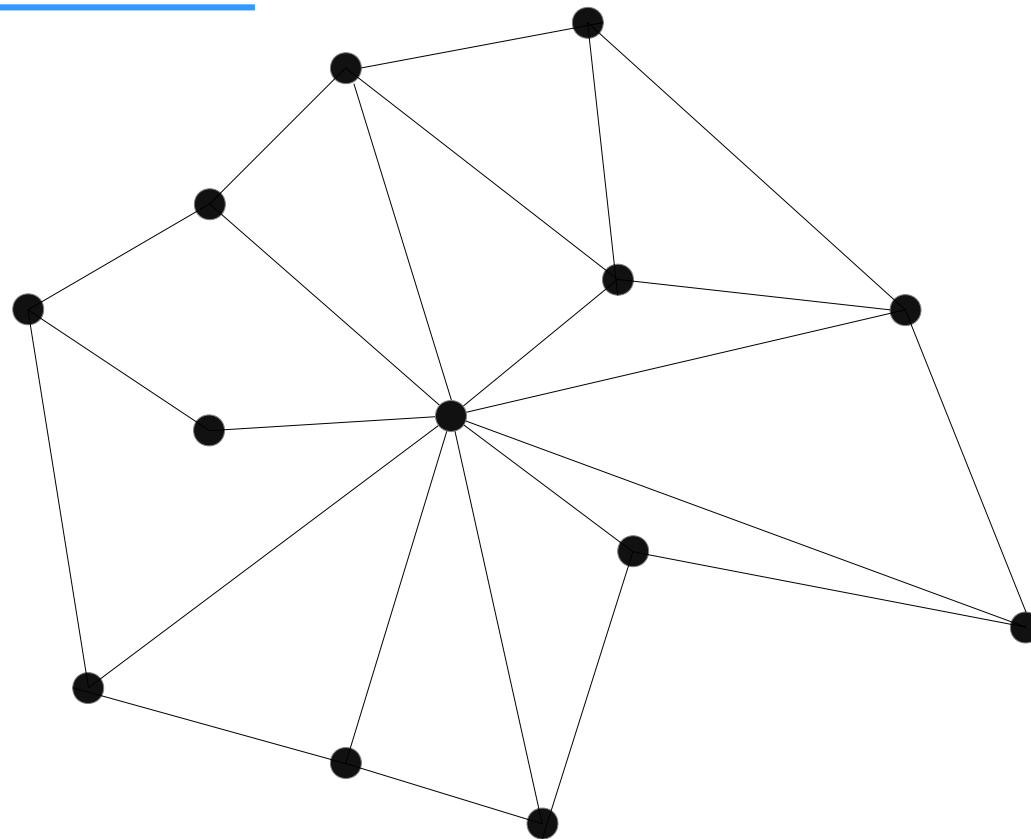
Centralized Ledger
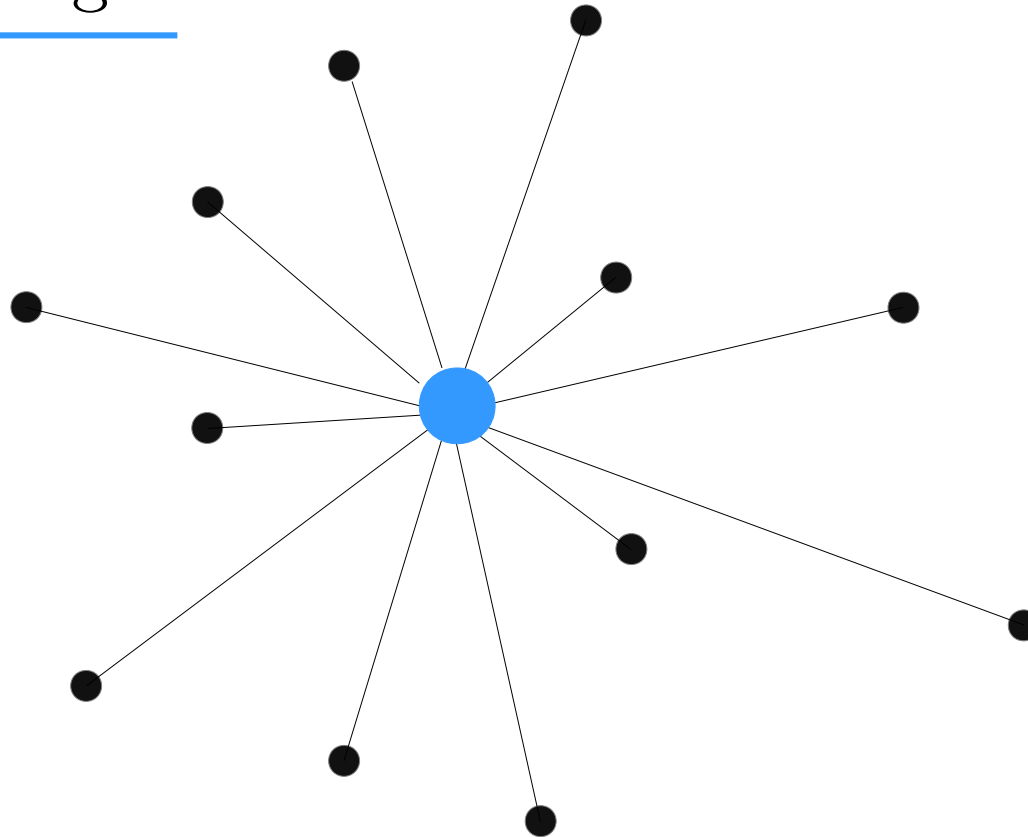
A trusted central authority maintains the ledger.

Blockchain

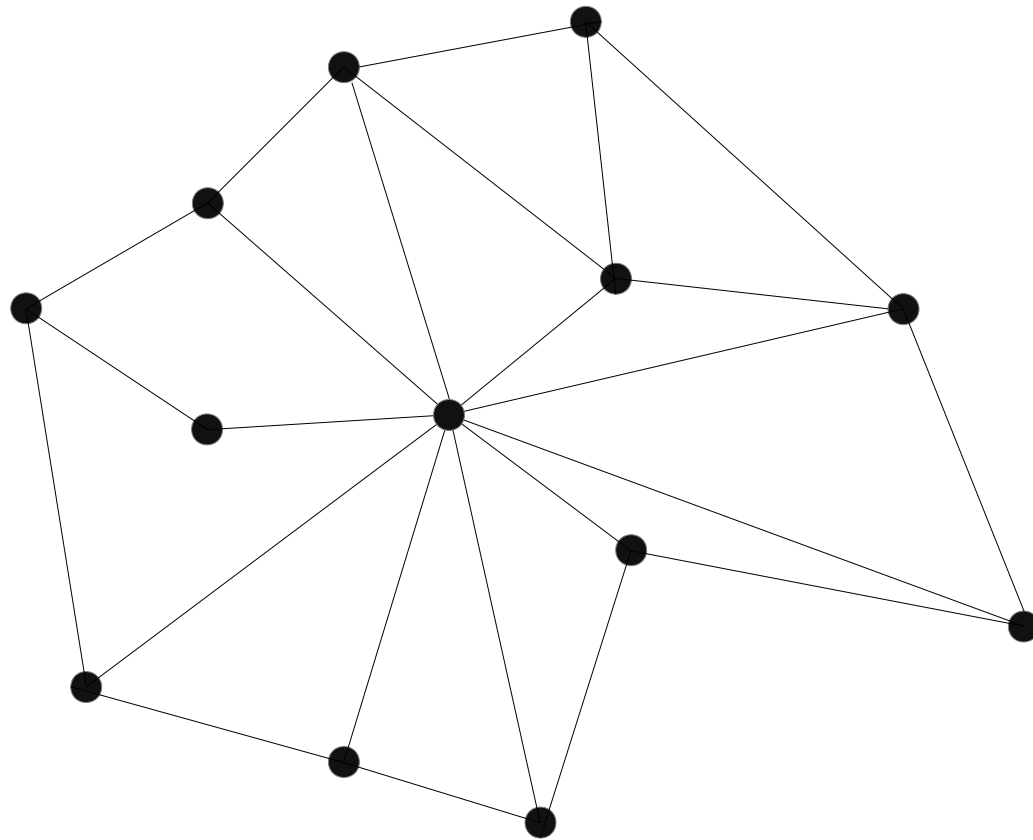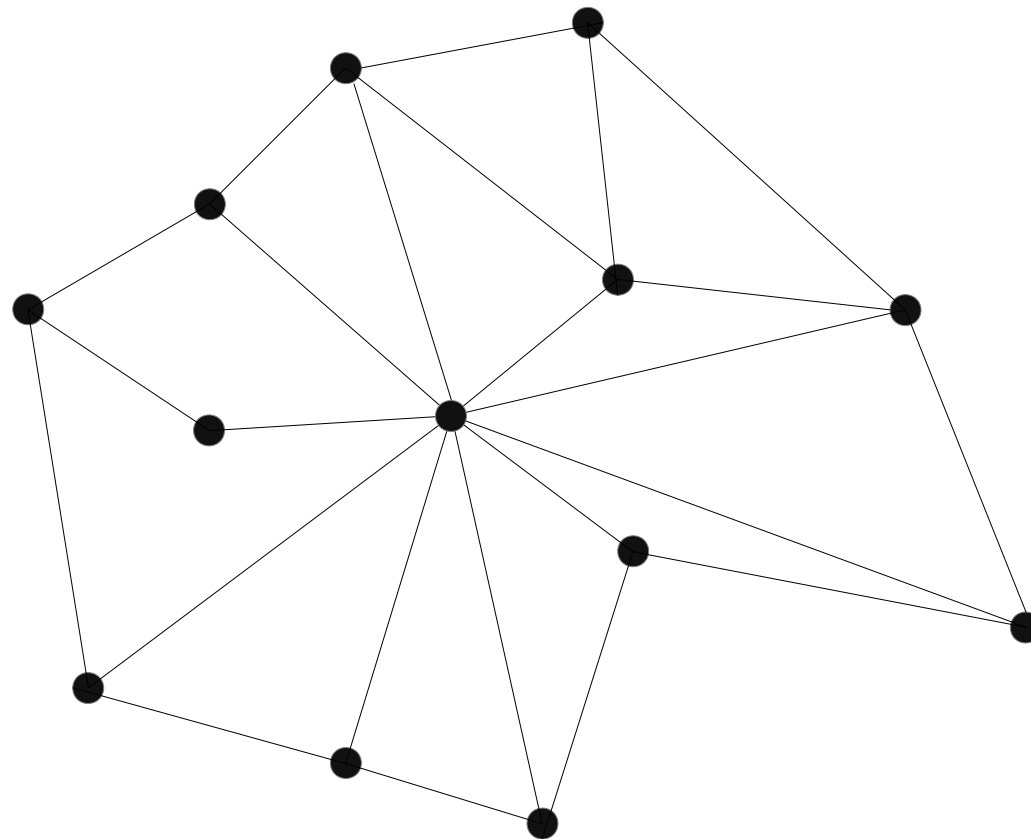**Decentralized Ledger**

Distributed

All peers in the network maintain the ledger.
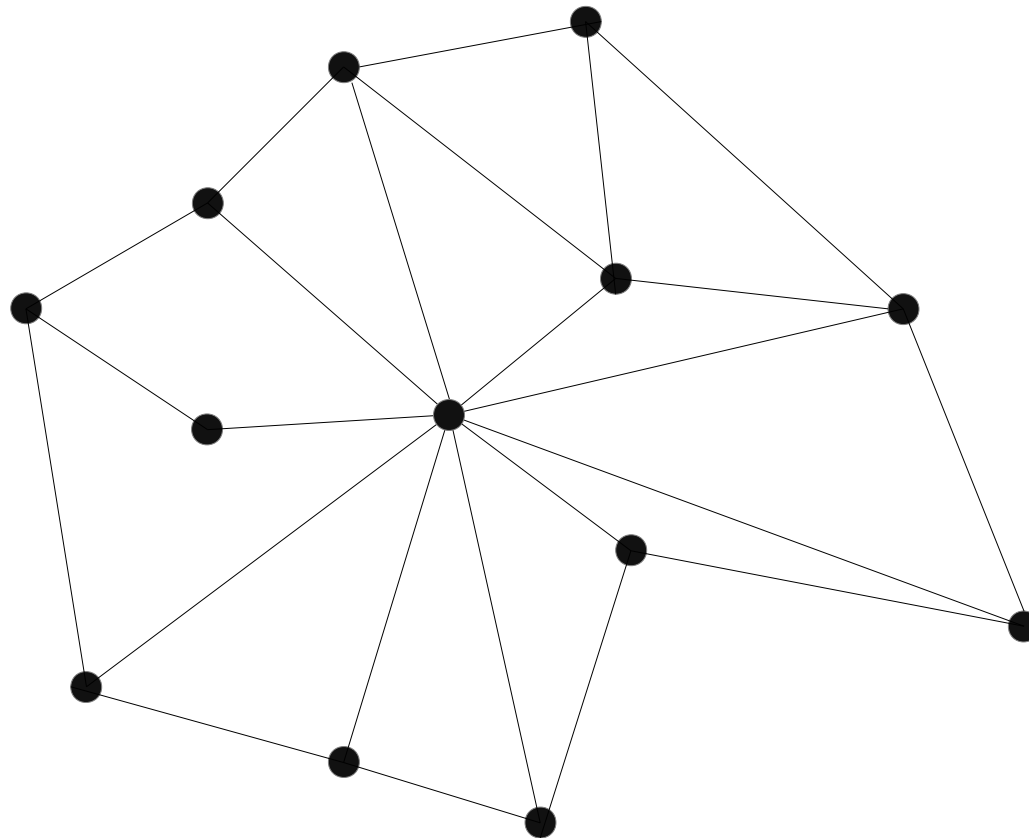
DELPHI

Why decentralization?

DELPHI

Why decentralization?

Transparent $\rightarrow$ all records fully traceable and immutable.

Why decentralization?

Secure $\rightarrow$ Trustless, no single point of failure

Why decentralization?

Democratic $\rightarrow$ Community-based decisions.
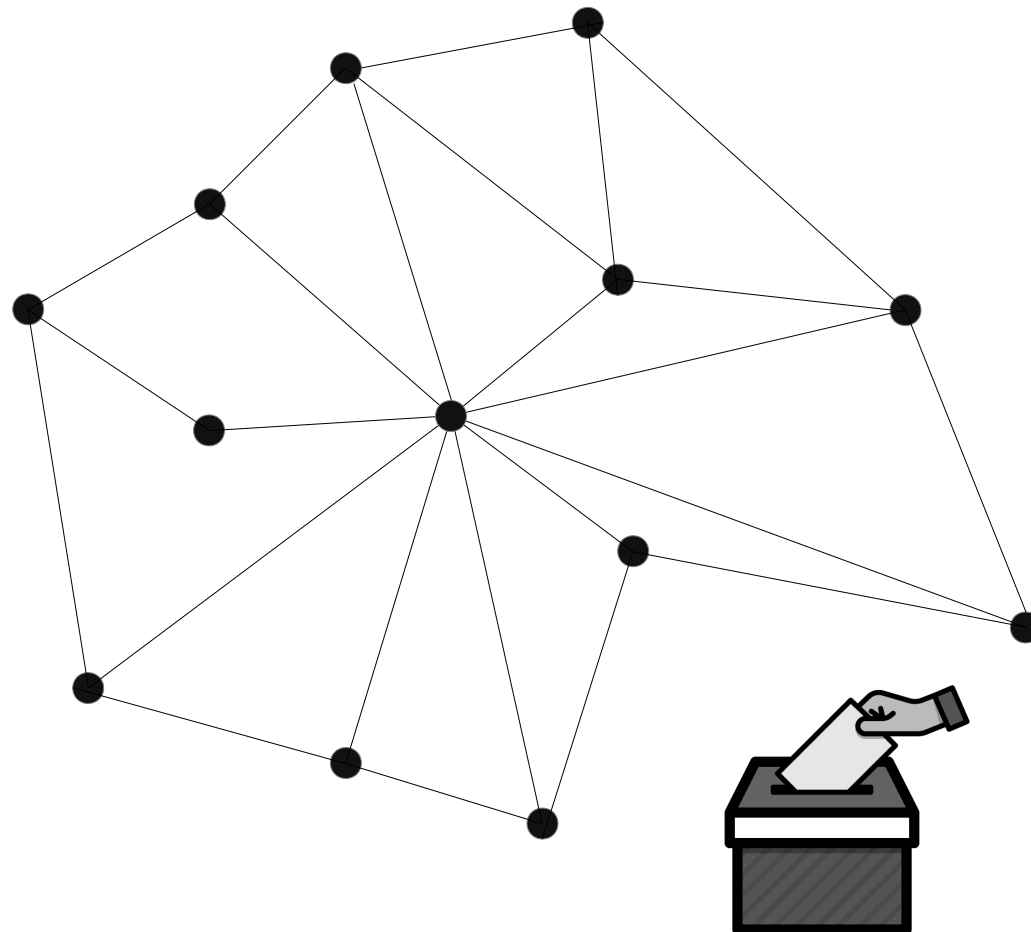
Public Blockchain: Bitcoin

'Original Blockchain'

- cryptocurrency

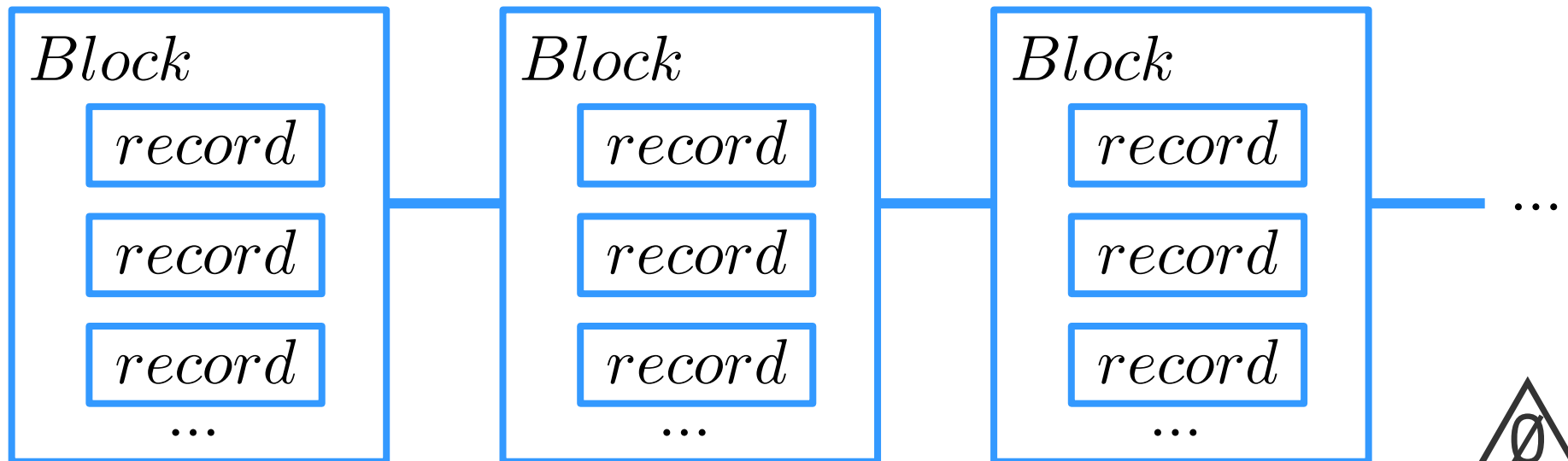 $\longrightarrow$ blockchain keeps track of wealth

- 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
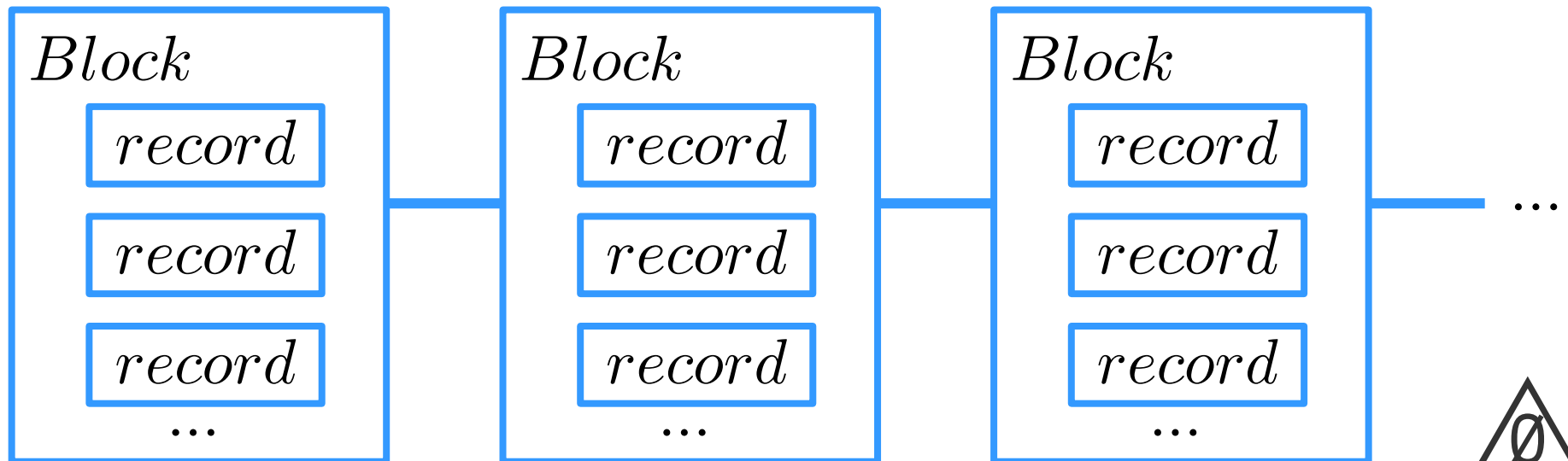
Records are "Smart Contracts"

- Piece of code

- Stored on the blockchain

- Execution state is validated by the network
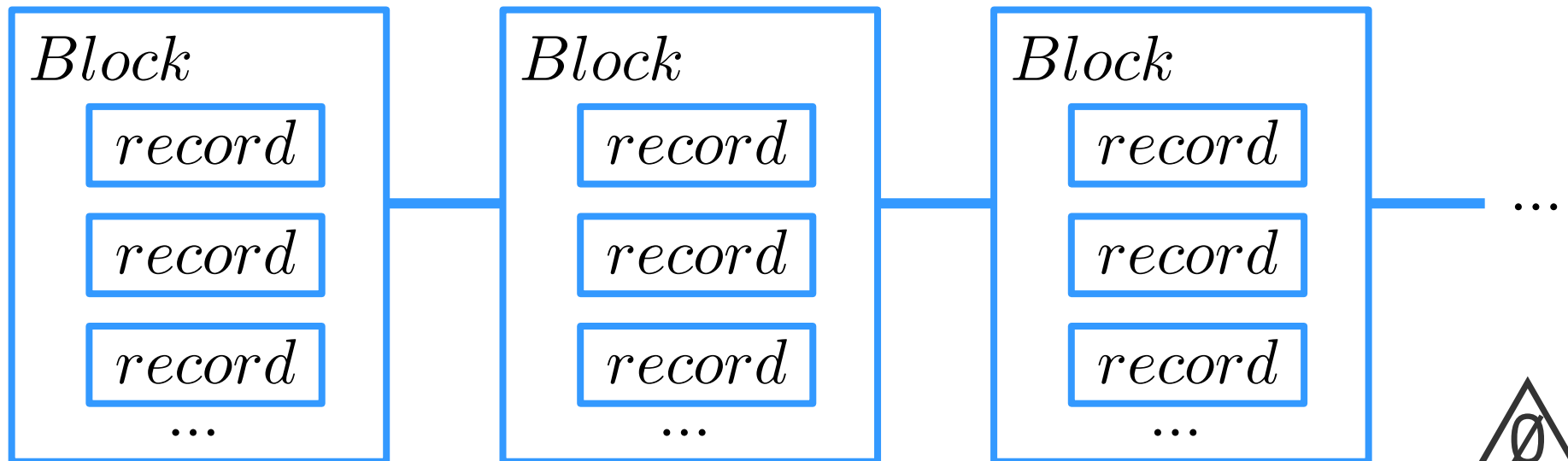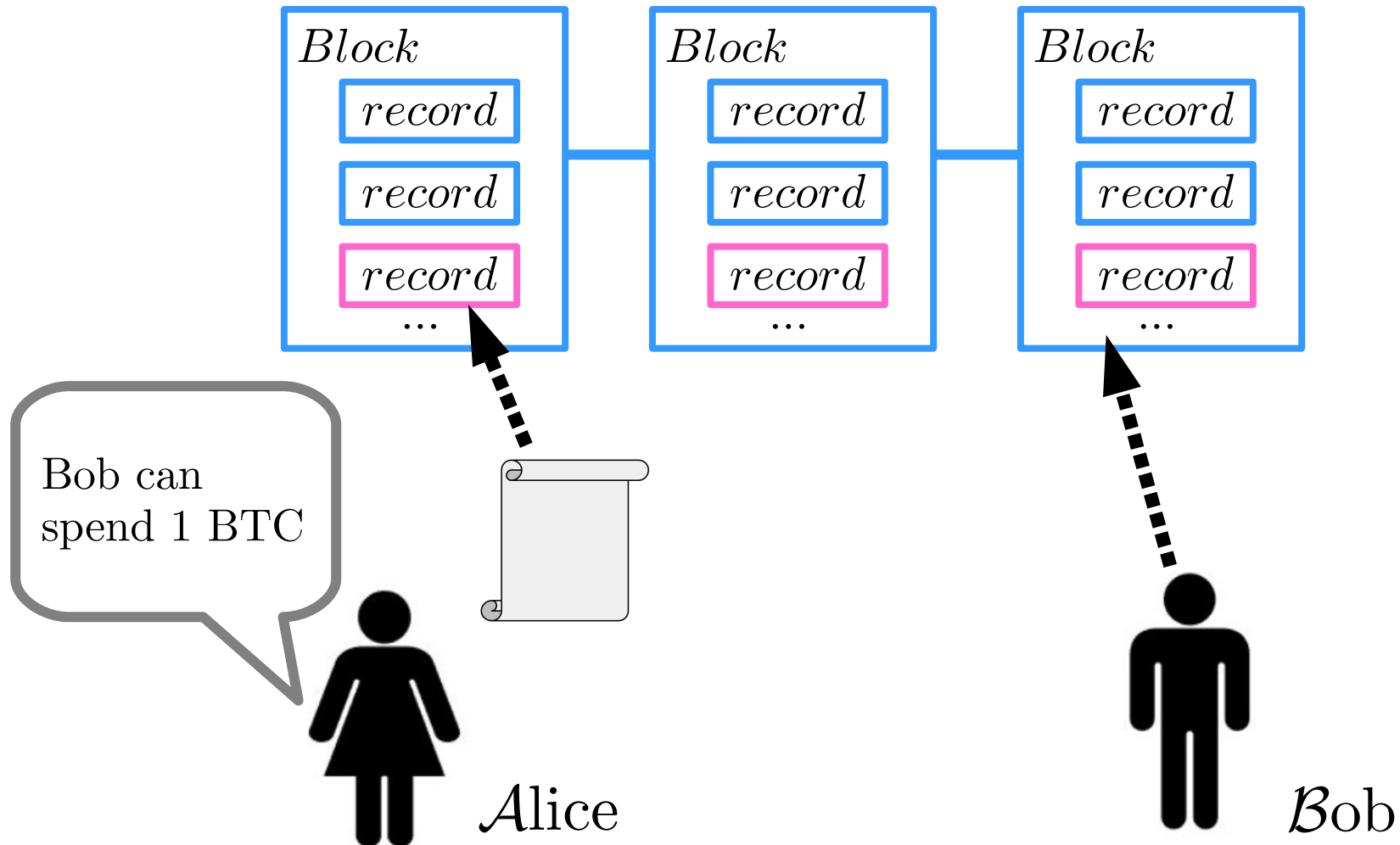
Bitcoin Transactions ₿

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

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

$signature$

$\mathcal{A}$

r_A, u_A

$\mathcal{B}$

u_B

DELPHI
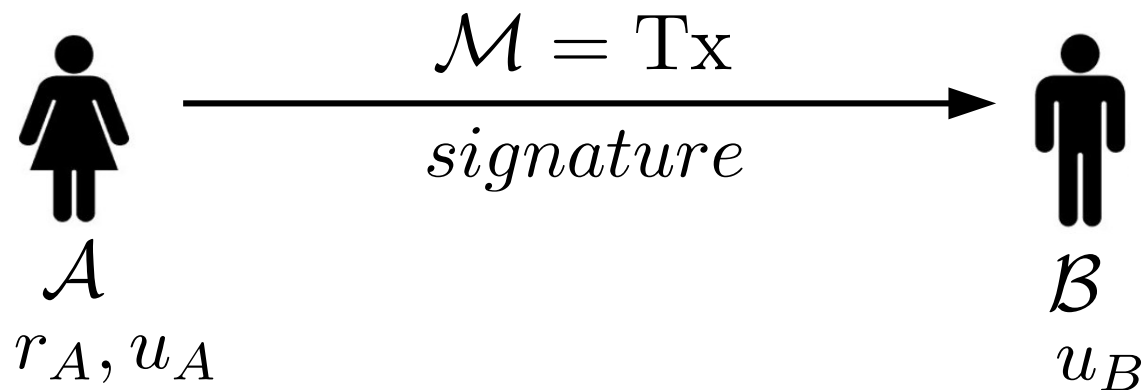
Bitcoin Transactions ₿

Cryptographic Signature

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

Signature

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

$$\mathcal{A} \xrightarrow[\quad signature \quad]{\mathcal{M} = \text{Tx}} \mathcal{B}$$

$\mathcal{A}$
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

$$\mathcal{A} \xrightarrow[signature]{\mathcal{M} = \text{Tx}} \mathcal{B}$$

$$\mathcal{A} \quad\quad\quad\quad\quad\quad\quad \mathcal{B}$$
$$r_A, u_A \quad\quad\quad\quad\quad\quad u_B$$

Verification

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

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

DELPHI

Bitcoin Transactions ₿

Cryptographic Signature

- public and private keys generated

- only $\mathcal{A}$ knows private key, r_A

- public key, u_A, known by everyone

$$\mathcal{A} \xrightarrow[\text{signature}]{\mathcal{M} = \text{Tx}} \mathcal{B}$$

$\mathcal{A}$
r_A, u_A

$\mathcal{B}$
u_B

Verification

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

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

DELPHI

Other smart contracts

Distributed File Storage

Smart Contract

🔒 data to store

🔓 data is properly stored

DELPHI

Other smart contracts

File Storage

Ethereum

- Cryptocurrency

- Turing-complete language

- Less limited

  $\rightarrow$ decentralized applications (dApps)

Other smart contracts

Distributed Computing

DELPHI
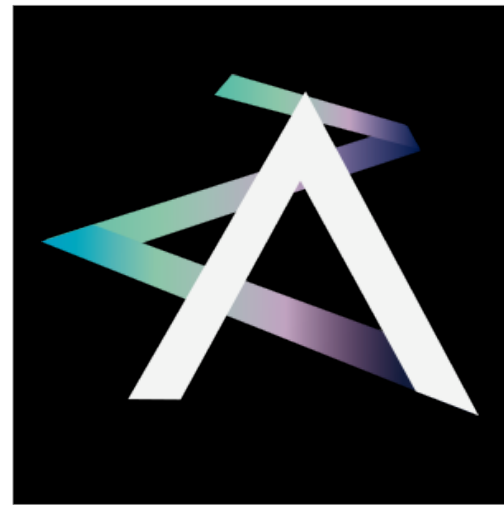
Other smart contracts

- games: Cryptokitties

- gambling: Etheroll, Funfair, ...

- insurance

- voting

- auctions

Summary

- Blockchain is a ledger

- Records are smart contracts

- Decentralized networks guarantee the state of records

- Recent smart contracts can provide real world applications:

  - Transparent

  - Secure

  - Democratic

DELPHI

Delphi Crypto

Thank you!

delphicrypto.com

info@delphicrypto.com

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

IOTA

Bitcoin Mining ₿

No central authority

Who keeps track of which transactions are valid?
double spending?
why?

DELPHI

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'

$H(\text{bank}) = 4381\text{dc}2\text{ab}14285160\text{c}808659\text{aee}005\text{d}51255\text{add}7264\text{b}318\text{d}07\text{c}7417292\text{c}7442\text{c}$

$H(\text{Bank}) = 676\text{c}471\text{bc}8\text{dc}3\text{d}1324133\text{cf}087\text{c}20\text{aa}0137\text{fc}02348811\text{e}4162\text{c}79\text{e}560298\text{fb}11$

$H(\text{the bank}) = \text{b}3\text{d}0\text{b}18\text{e}01647\text{cc}301\text{a}5\text{dc}022784\text{fd}1\text{e}5\text{b}85475\text{a}4\text{dbb}14140\text{b}983\text{dbf}1\text{c}5\text{a}7\text{be}1$

$H(\text{thebank}) = \text{fc}4\text{cb}9\text{f}881175\text{d}7\text{b}5\text{ac}02906947\text{f}288\text{b}9998\text{bd}9354\text{ea}06\text{ddf}13\text{fc}21\text{fa}5\text{c}12\text{c}4\text{d}$

DELPHI

Bitcoin Mining ₿

Cryptographic Hash Function (H)

- maps any input to fixed size output

- not invertible

- not 'continuous'

- no collisions

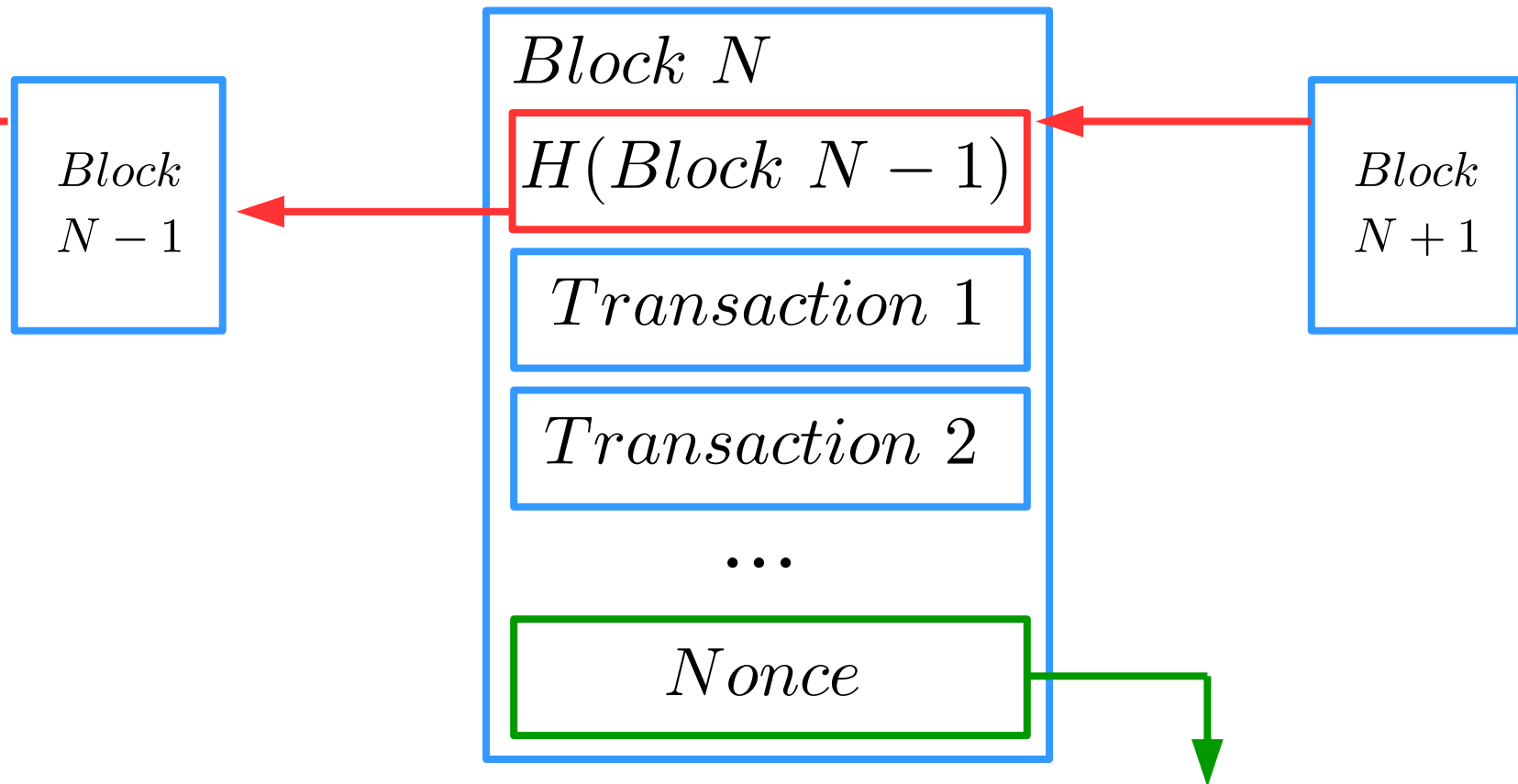$$x \neq y \implies H(x) \neq H(y)$$

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

DELPHI
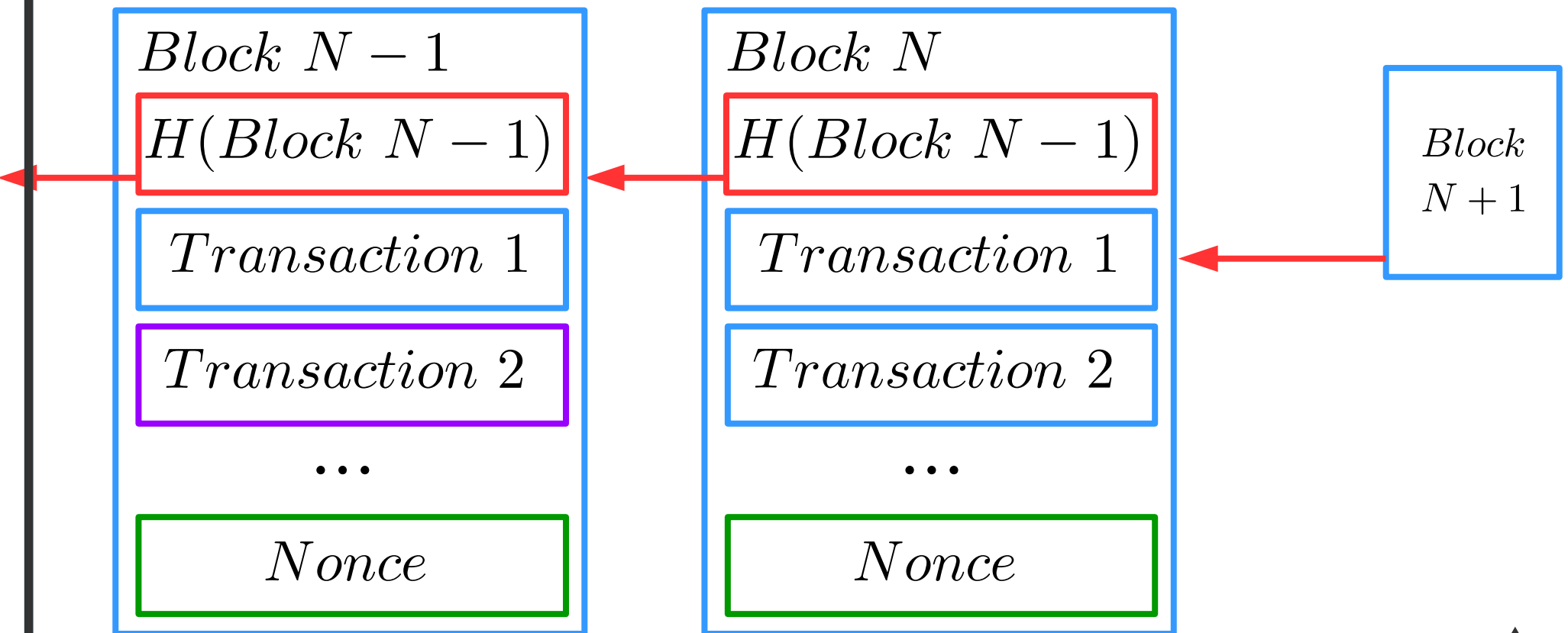
Bitcoin Mining ₿

How does mining work?

Block N

$H(Block\ N-1)$

Transaction 1

Transaction 2

...

Nonce

Block N − 1

Block N + 1

picked so hash has correct amount of 0's

DELPHI

Bitcoin Mining ₿

What if someone cheats?

Block N − 1	Block N	
H(Block N − 1)	H(Block N − 1)	
Transaction 1	Transaction 1	Block N + 1
Transaction 2	Transaction 2	
...	...	
Nonce	Nonce	

DELPHI

Bitcoin Mining ₿

What if someone cheats?

Block N − 1		Block N		Block N + 1
H(Block N − 2)		H(Block N − 1)		
Transaction 1		Transaction 1		
Different Tx		Transaction 2		
...		...		
Nonce		Nonce		
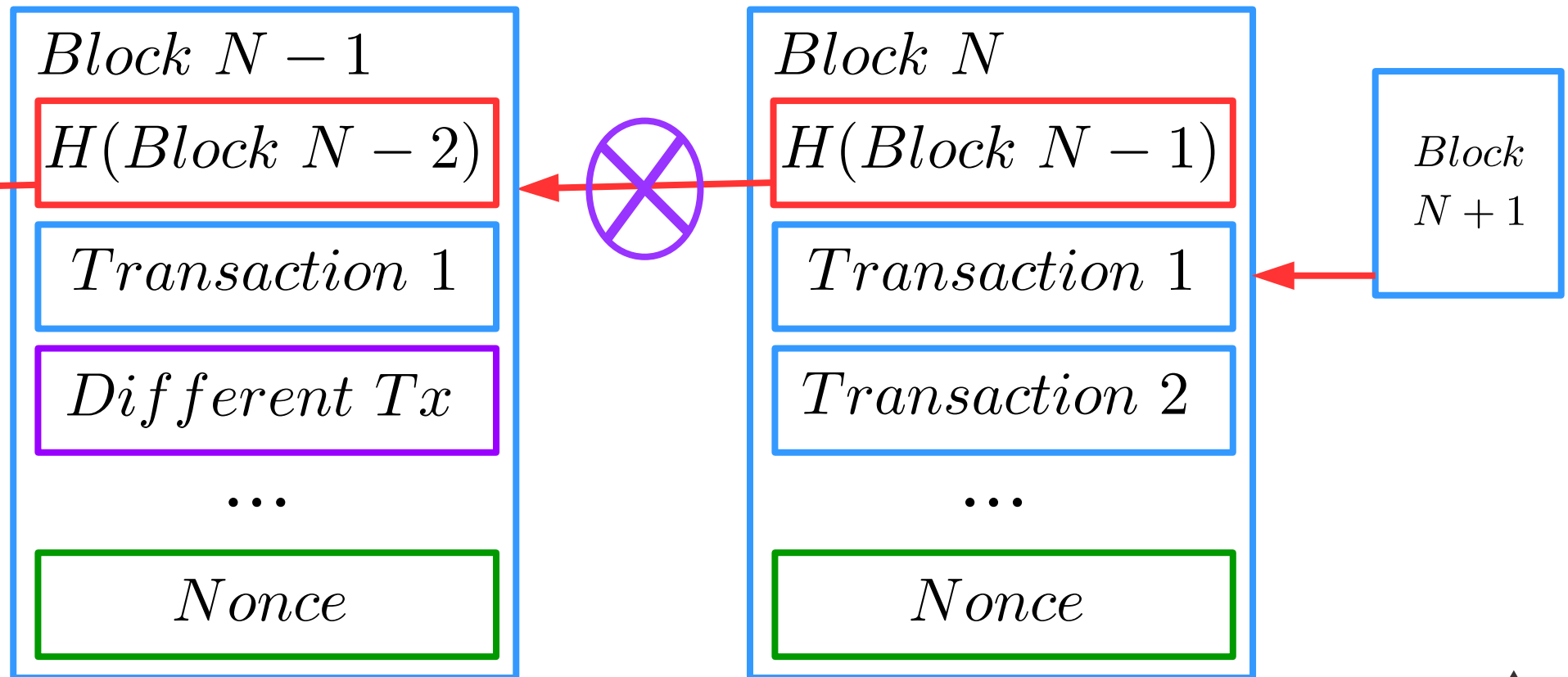
→ Error gets propagated

DELPHI

Bitcoin Mining ₿

Overview

- miners add 1 MB blocks respecting current difficulty

- network accept valid blocks by adding blocks on the chain

    → add blocks to <u>longest</u> 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)

DELPHI

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

DELPHI

Bitcoin Mining ₿

Longest Valid Chain

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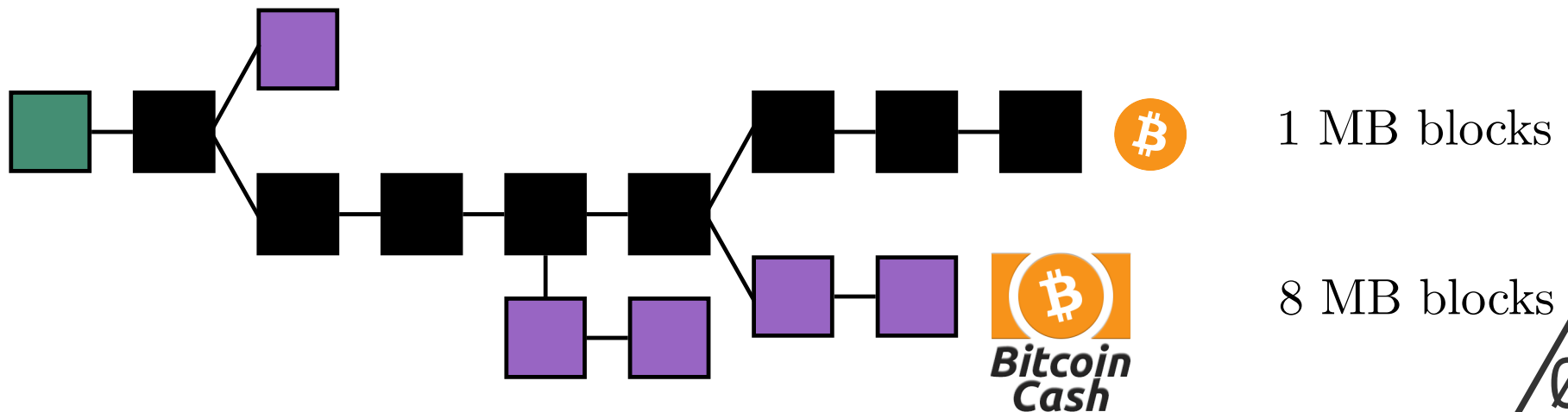
- 51 % attack

DELPHI
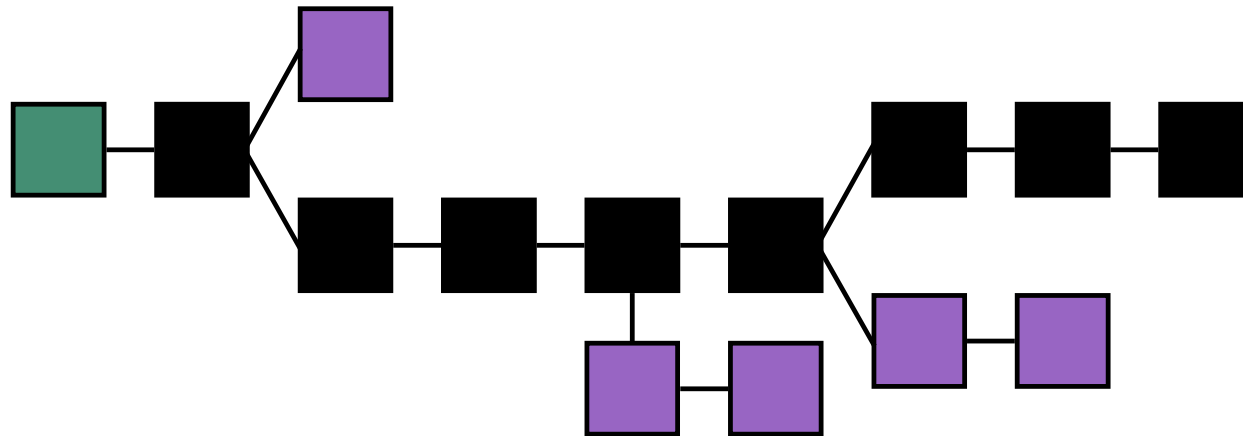
Forking and Bitcoin Cash

Resolution of the conflict

- fork the ledger

- same past, different future

- different miners agree to work on different chains

1 MB blocks

8 MB blocks

Other Ideas

Cryptocurrencies

- Bitcoin is first, is it best?

- Ethereum: smart contracts

- Iota: tangle

- Quantum Resistant Ledger: 'resistant' to quantum computers

Other Ideas

Smart Contracts

- decentralized applications - dApps

- Ex. Pear: decentralized journal

  ⟶ https://github.com/delphicrypto/Pear

PEAR