

Blockchain technology and Bitcoin

Pericles Philippopoulos – McGill University, Montreal, Canada

CONFETI
January 2018



Blockchain

- list of records

record

record

record

Blockchain

- list of records
- grouped in blocks

Block

record

record

record

...

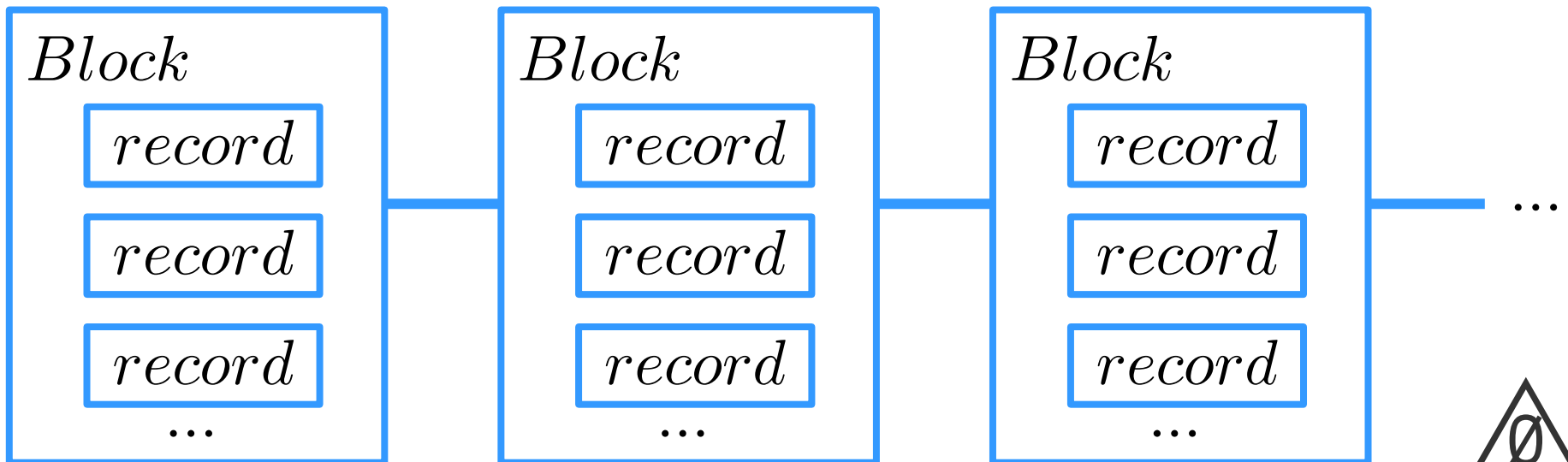
Blockchain

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



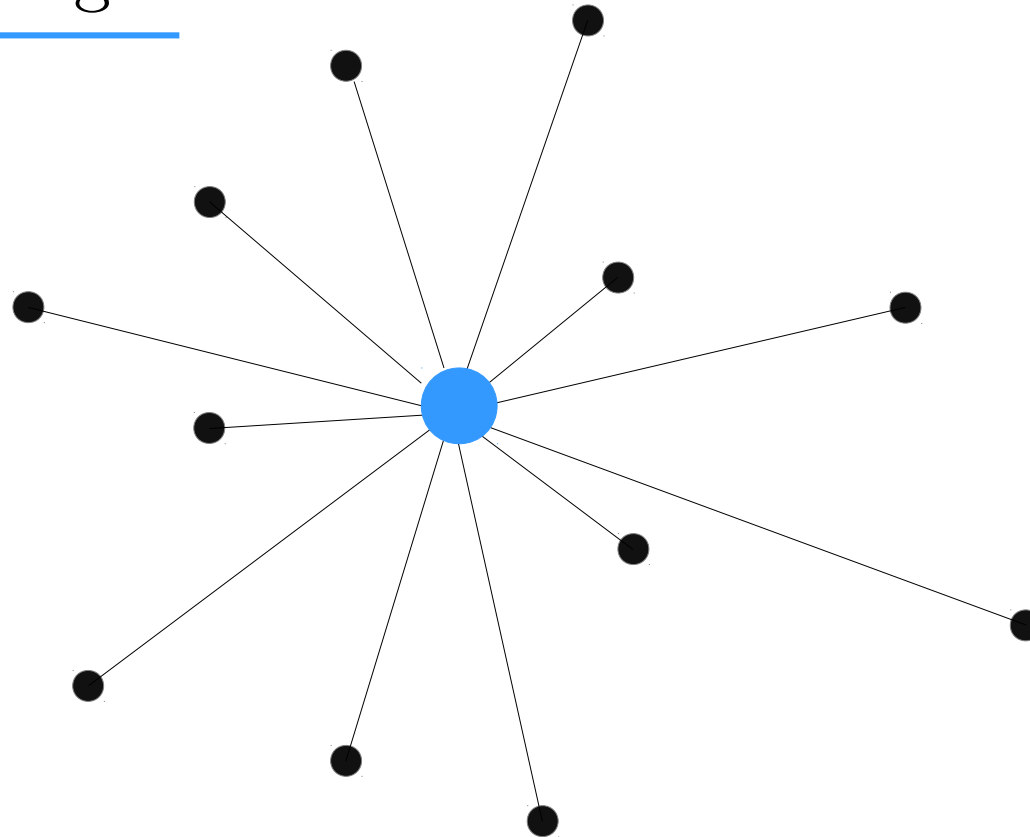
ledger

- add to chain
- can't modify old blocks



Blockchain

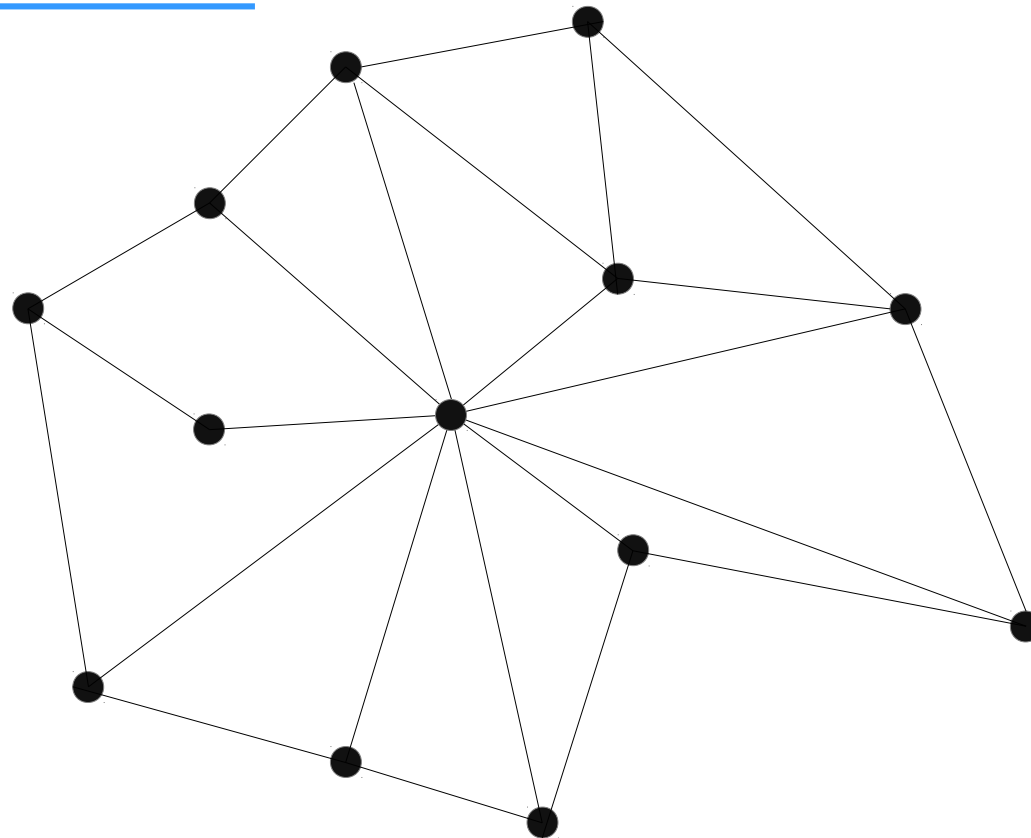
Centralized Ledger



Blockchain

Decentralized Ledger

Distributed



reduce, track down errors, corruption...

Public Blockchain: Bitcoin

‘Original Blockchain’

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



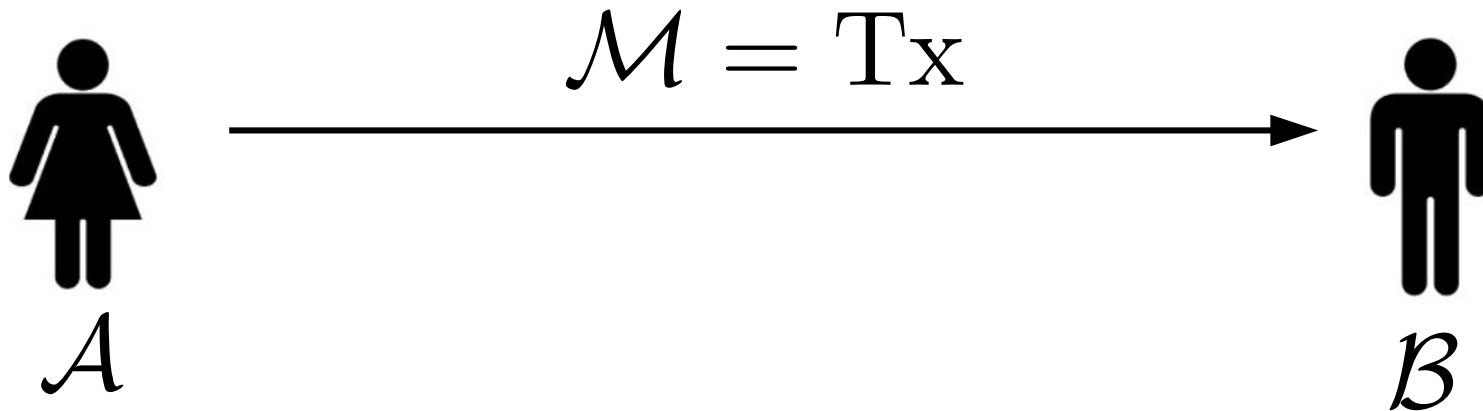
Public Blockchain: Bitcoin

‘Original Blockchain’

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



Bitcoin Transactions



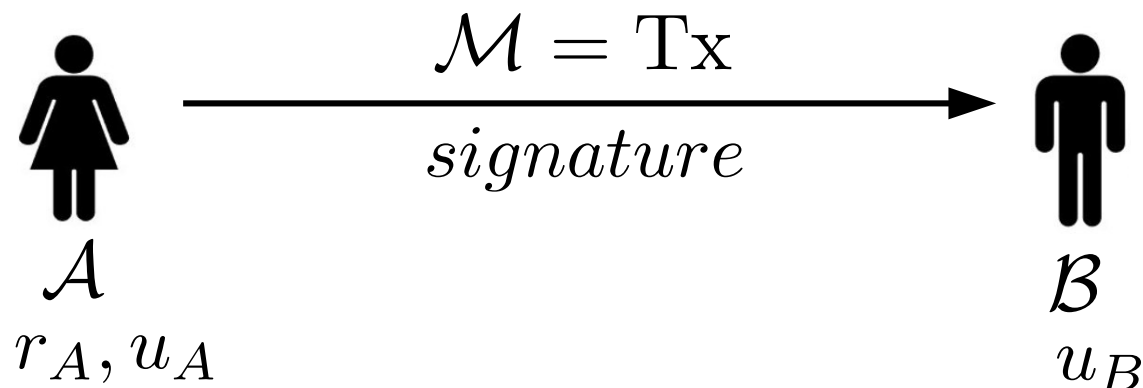
How do you prove Alice sent the \mathcal{M} essage to Bob ?

Bitcoin Transactions

Cryptographic Signature

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

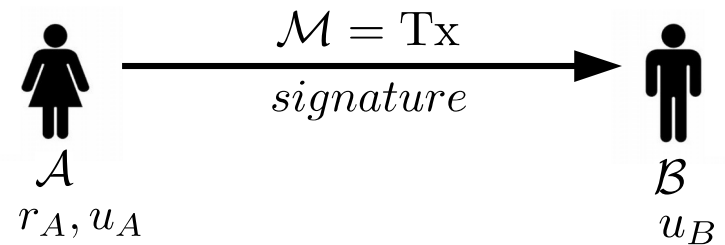
Signature



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

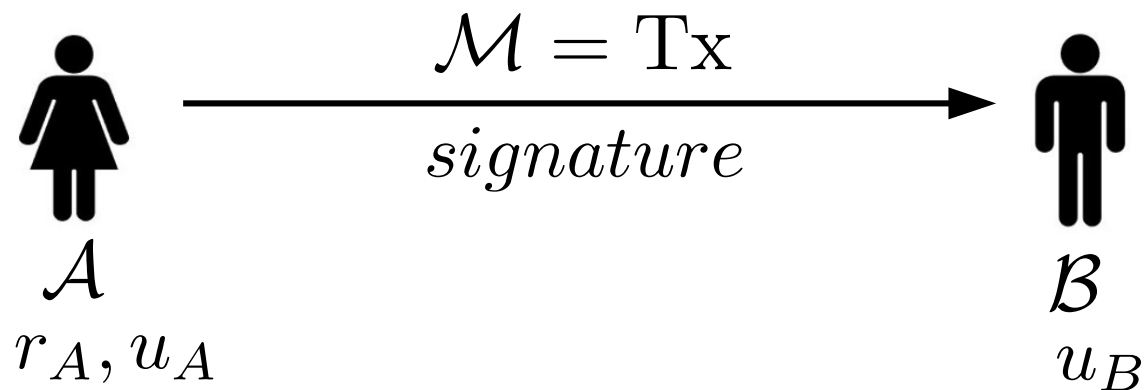
$check : u_A, \mathcal{M}, signature \rightarrow Yes/No$

The \mathcal{M} essage can be verified by Bob or anyone else

Bitcoin Transactions

Overview

- participants in the network identified by public keys
—▶ \sim anonymity
- access to private key means access to funds
—▶ \sim access to ‘wallet’
- transaction broadcasted and added to the ledger



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

$H(a) = \text{ca978112ca1bbdcafacc231b39a23dc4da786eff8147c4e72b9807785afee48bb}$

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

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'

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

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

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

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

Bitcoin Mining

Cryptographic Hash Function (H)

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

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

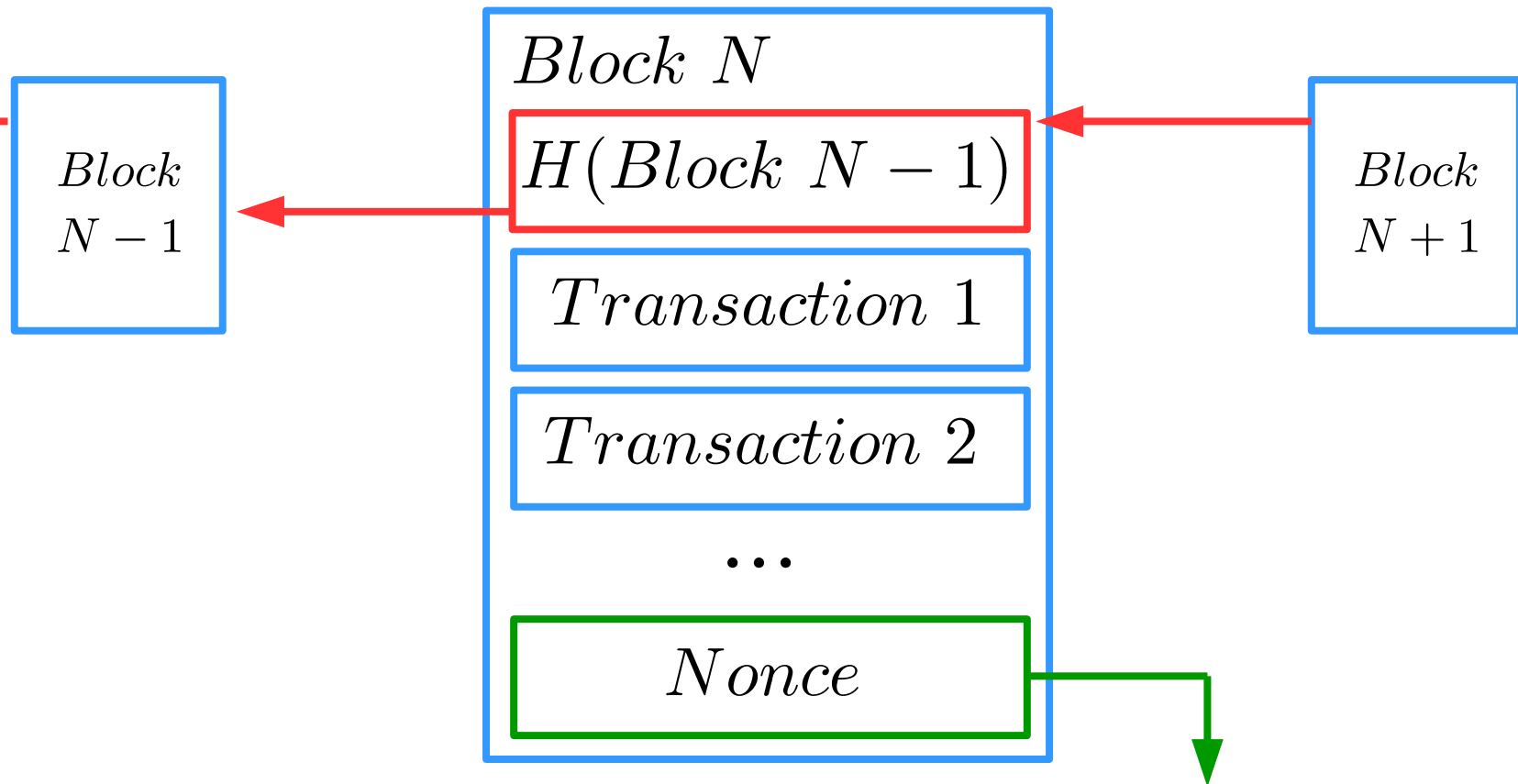
Bitcoin Mining

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

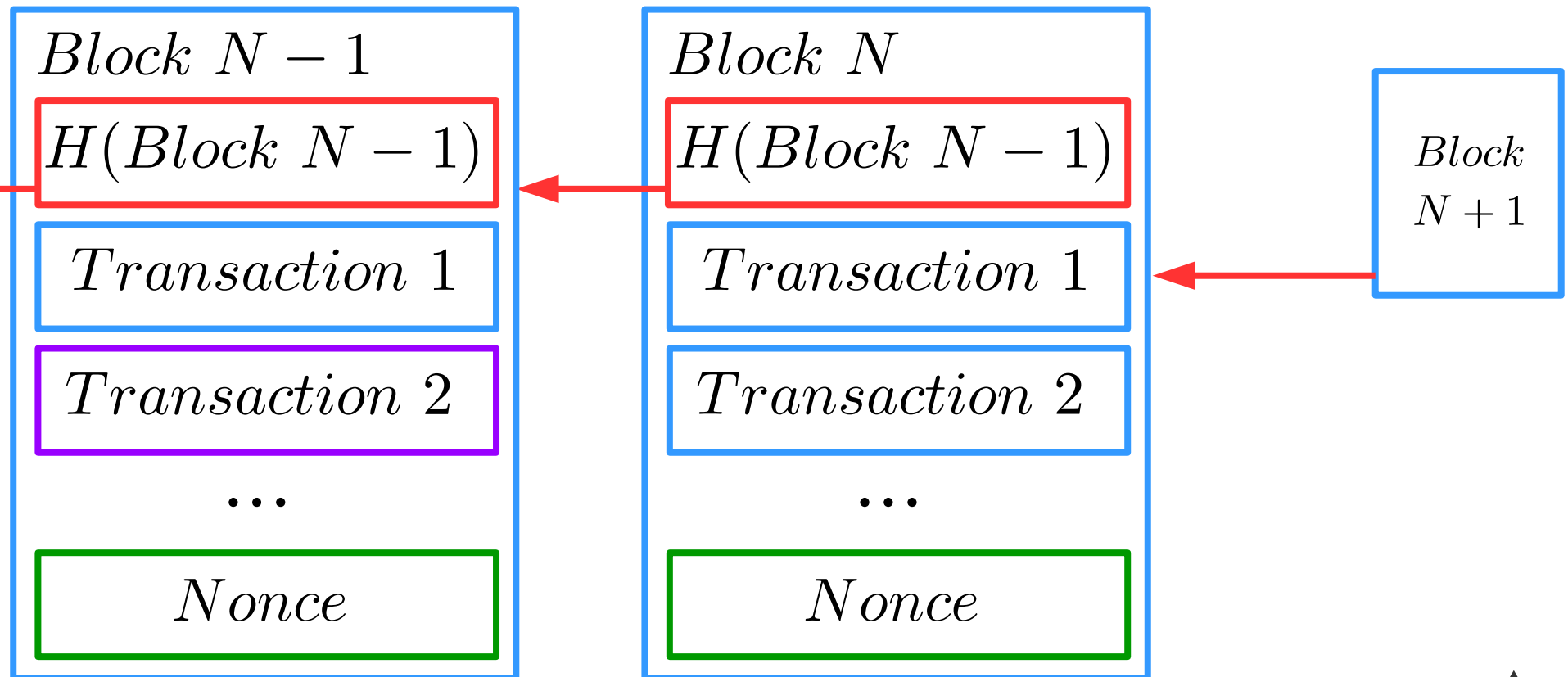
How does mining work?



picked so hash has correct amount of 0's

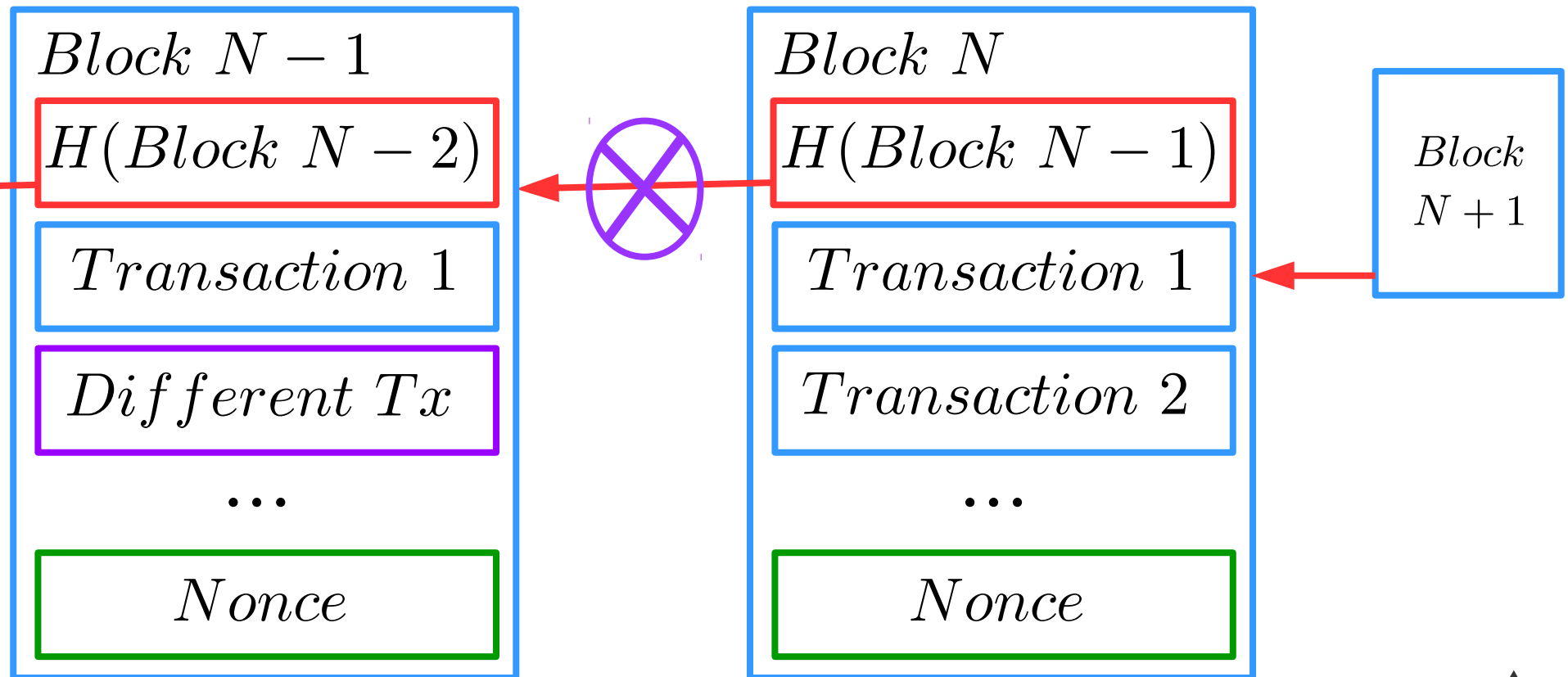
Bitcoin Mining

What if someone cheats?



Bitcoin Mining

What if someone cheats?



→ 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 (~ 21 million coins)

Bitcoin Mining

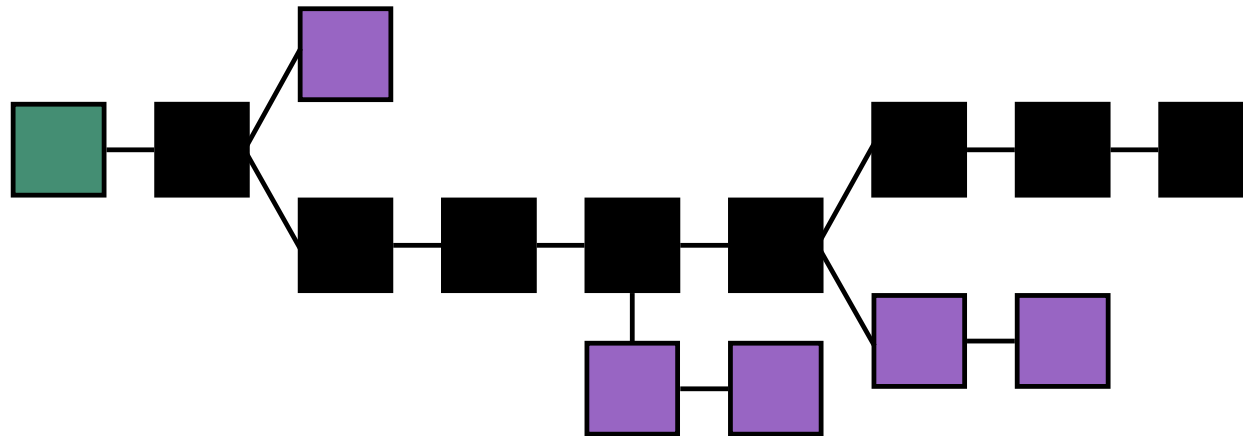
Consumption

- 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

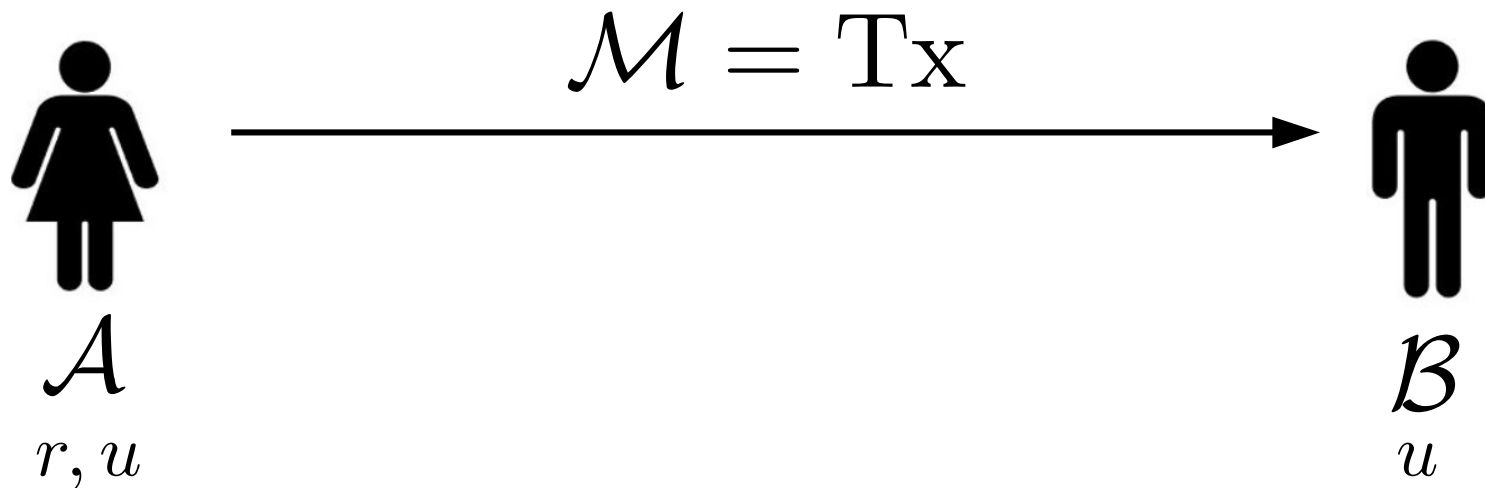
Bitcoin Mining

Longest Valid Chain

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



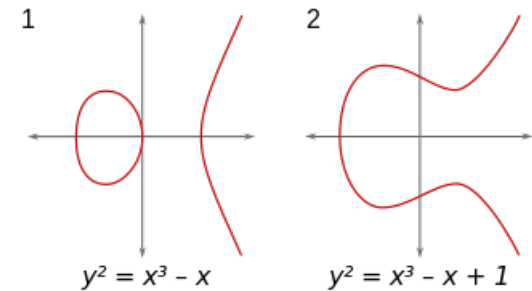
Bitcoin Transactions



Quantum Computers

Transactions

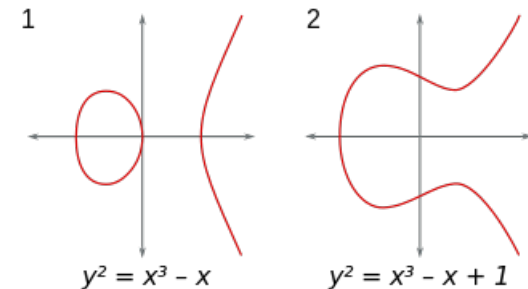
- public-key cryptography - elliptic curves
- discrete-log problem



Quantum Computers

Transactions

- public-key cryptography - elliptic curves
- discrete-log problem



Find k , such that $b^k = a$

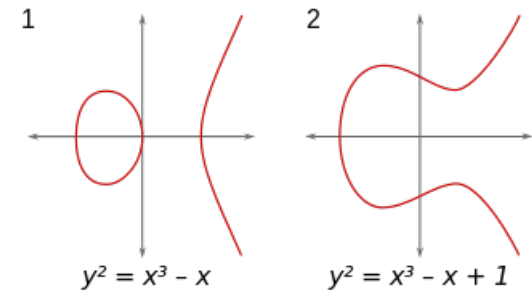
$$a, b \in G$$

G is a group

Quantum Computers

Transactions

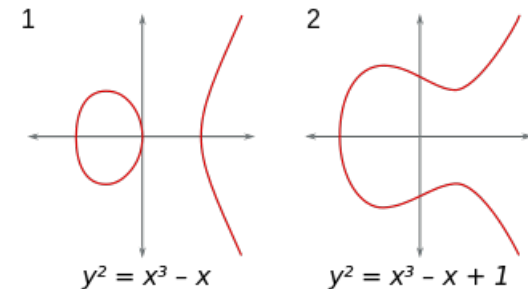
- public-key cryptography - elliptic curves
- discrete-log problem
 - Inefficient classically



Quantum Computers

Transactions

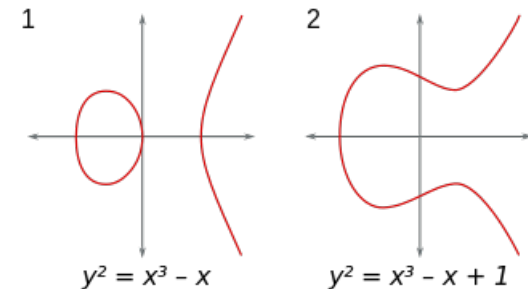
- public-key cryptography - elliptic curves
- discrete-log problem
 - Inefficient classically
- quantum computer: Shor's algorithm
 - Efficient
- private key can be found from public key
 - Funds are not secure



Quantum Computers

Transactions

- public-key cryptography - elliptic curves
- discrete-log problem
 - Inefficient classically
- quantum computer: Shor's algorithm
 - Efficient
- private key can be found from public key
 - Funds are not secure
- a lot of the encrypted communication breaks
 - ways to fix this



Quantum Computers

Mining

- Classically: trial and error
→ $O(2^d)$
- Quantum: Grover's Algorithm
→ $O(2^{d/2})$
- better at mining than the rest of the network
→ $d \sim 60$
- eventually everyone has a quantum computer
→ difficulty readjusted

Forking and Bitcoin Cash



Disagreement about the future

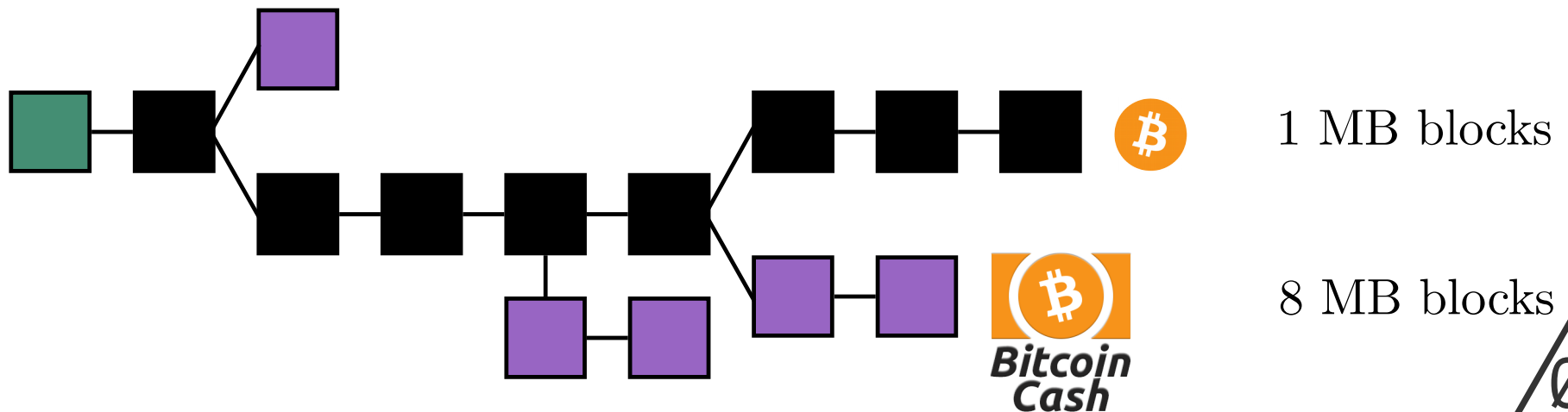
- issue: not enough transactions/block
 - ▶ scaling problem
- Bitcoin: segwit
 - ▶ restructure blocks
- Bitcoin Cash: Larger blocks

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



Other Ideas

Smart Contracts

- decentralized applications - dApps
- Ex. Pear: decentralized journal
 - <https://github.com/ricott1/Pear>

