Bitcoin: Concepts, Practice, and Research Directions

Ittay Eyal, Emin Gün Sirer

Computer Science, Cornell University

DISC Bitcoin Tutorial, October 2014

Barter

Gold

Fiat

Barter

Gold

Fiat

Bitcoin

2008: The Bitcoin white paper

2009: Reference implementation

[Satoshi Nakamoto]

Barter Gold Fiat Bitcoin

- Decentralized control
- Decentralized minting
- Easy to transfer
- Novel tech, new applications

Barter

Gold

Fiat

Bitcoin

taxation is a crime!

Banks: criminals, who print money and lend it as debt.

Bitcoin or oligarchy?

Separate church and state?
Separate bank and state!

Great Success!

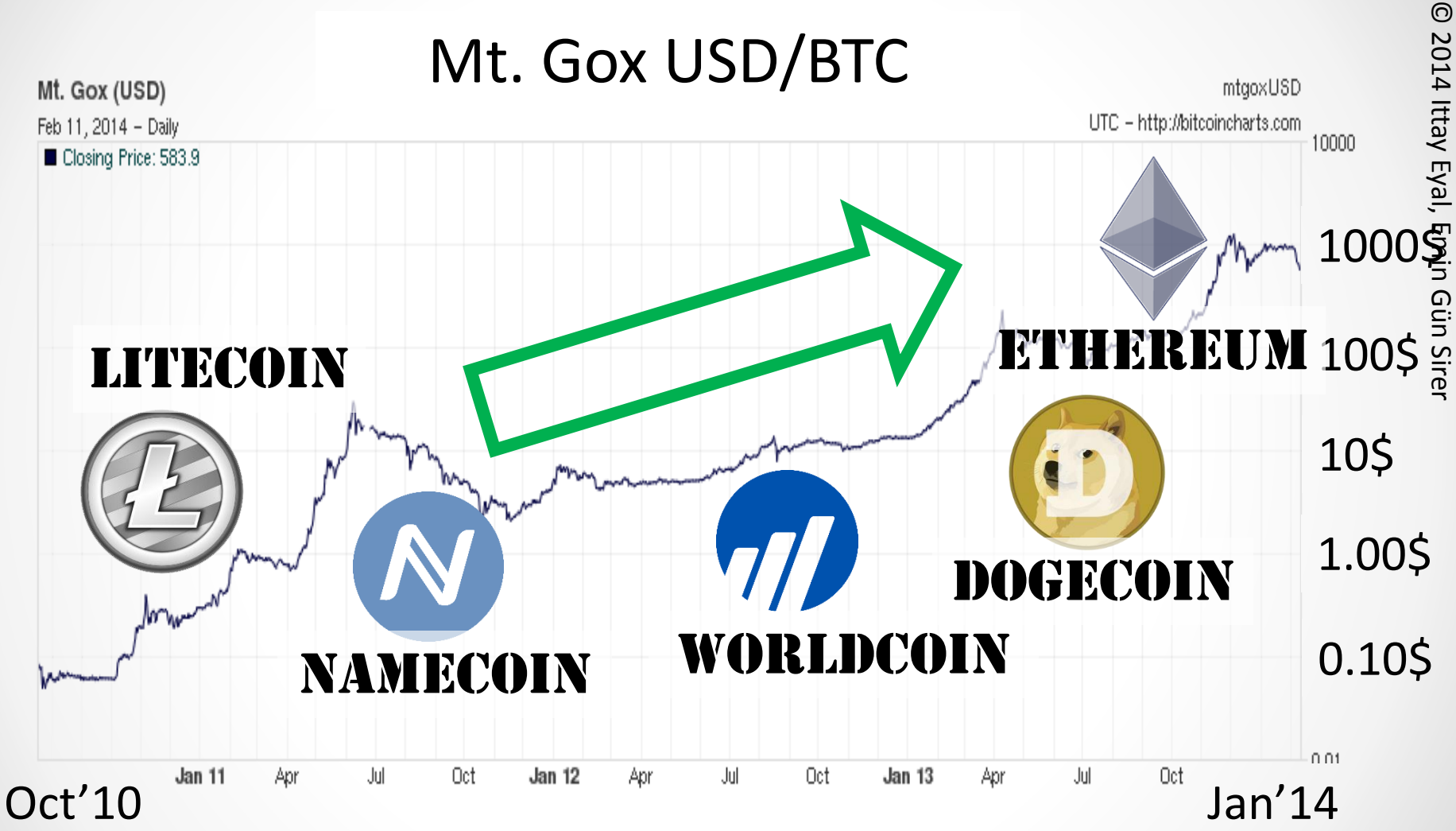
Mt. Gox USD/BTC

Oct'10

Jan'14

[http://bitcoincharts.com/]

Great Success!



[http://bitcoincharts.com/]

Mostly Great Success

[http://bitcoincharts.com/]

Acceptance

1 btc in usd

Web News Shopping Images Maps More Search tools

About 43,500,000 results (0.50 seconds)

1 Bitcoin equals

467.02 US Dollar

1 Bitcoin

467.02 US Dollar

Disclaimer

472.6 **USD** · Preev
preev.com/
DESC=
USD - GBP - Bitcoin to gold - Bitcoin to Euro

Bitcoin Charts
bitcoincharts.com/ Bitcoin Charts
So far, more then 10 **BTC** got donated, which is a lot, compared to the approx. 10 000€ donations (in German) ... 8 Apr 2014 Bitcoin Core version 0.9.**1** released

Acceptance

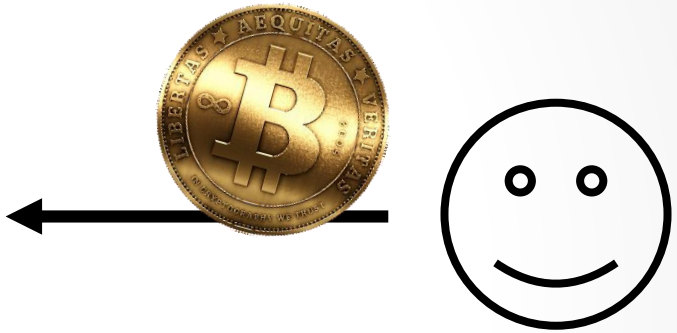
airBaltic

CheapAir.com

overstock.com

newegg.com

DELL



Acceptance

airBaltic

CheapAir.com

overstock.com

newegg.com

DELL

coinbase

CIRCLE

bitpay

Acceptance

Welcome! | Silk Road

http://ianxz6zefk72ulzz.onion/index.php

silk road darknet

Most Visited | Learn more about Tor | The Tor Blog

Are you using Tor? | list of TOR sites silkroad - Goo... | TORDIR - Link List | Welcome! | Silk Road

Silk Road
anonymous marketplace

Welcome
messages(0) | orders(0) | account(฿0) | settings | log out
(0)

Shop by category:
Cannabis(203)
Ecstasy(35)
Psychedelics(127)
Opioids(39)
Stimulants(68)
Dissociatives(9)
Other(197)
Benzos(43)


1 hit of LSD (blotter)
฿0.58


1/8 oz high quality cannabis
฿2.05


1 g pure MDMA (white)
฿1.28

recent feedback:

seller	rating	feedback	
1UP of Canada(97)	4 of 5	amazing weed. the flattened, which I	d that the product was item
CaliforniaSunrise	5 of 5	Fast shipping. Nice	item
Rook	5 of 5	all good! thanks so	item
illy	5 of 5	Very friendly. Fast	item
somatik	5 of 5	Order arrived quic	item
gamely54	5 of 5	No issue at all, I o	item
mellowyellow	5 of 5	Item arrived quick	item
dirtysouf(100)	5 of 5	looks good	item

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Many Players

- Farmers
- Payment services
- Investors
- Start-ups
- Venture Capital
- Miners
- Developers
- Researchers

Roadmap

- Protocol
- Security
- Research
- Non-technical

Bitcoin:
Concepts, Practice, and Research Directions

Part I
Protocol

Ittay Eyal, Emin Gün Sirer

Computer Science, Cornell University

DISC Bitcoin Tutorial, October 2014

Part 1 – Protocol

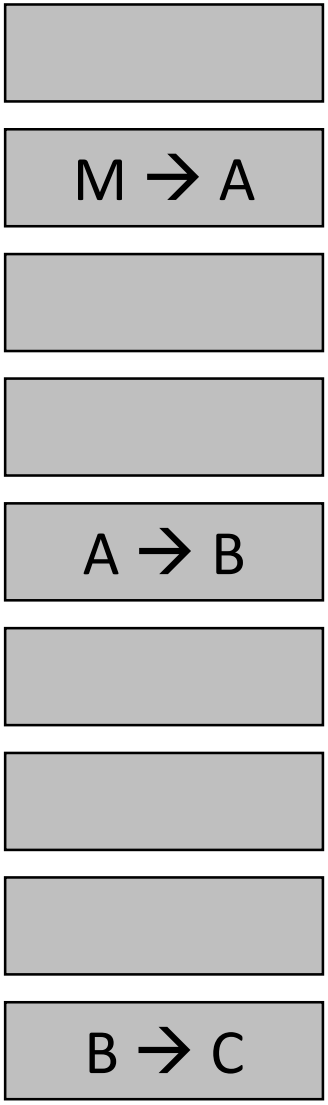
- Overview
- The Blockchain
- Block propagation
- Mining
- Transactions

Protocol Overview

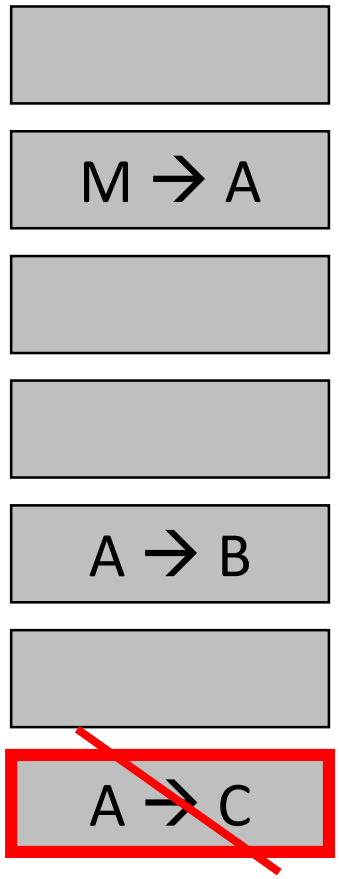
Key Issues

1. Stealing
2. Double-spending → Not a local solution

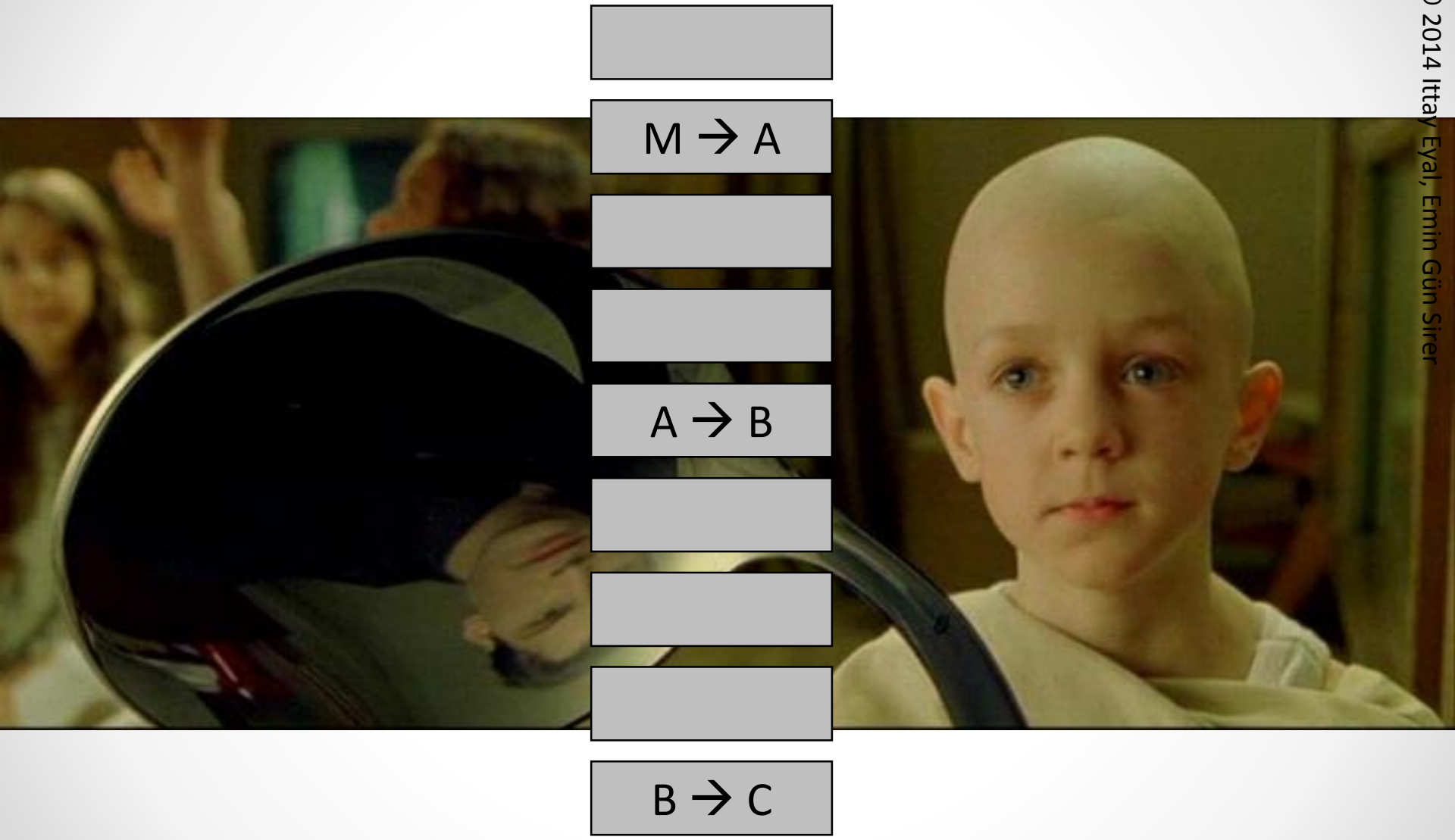
Global Ledger



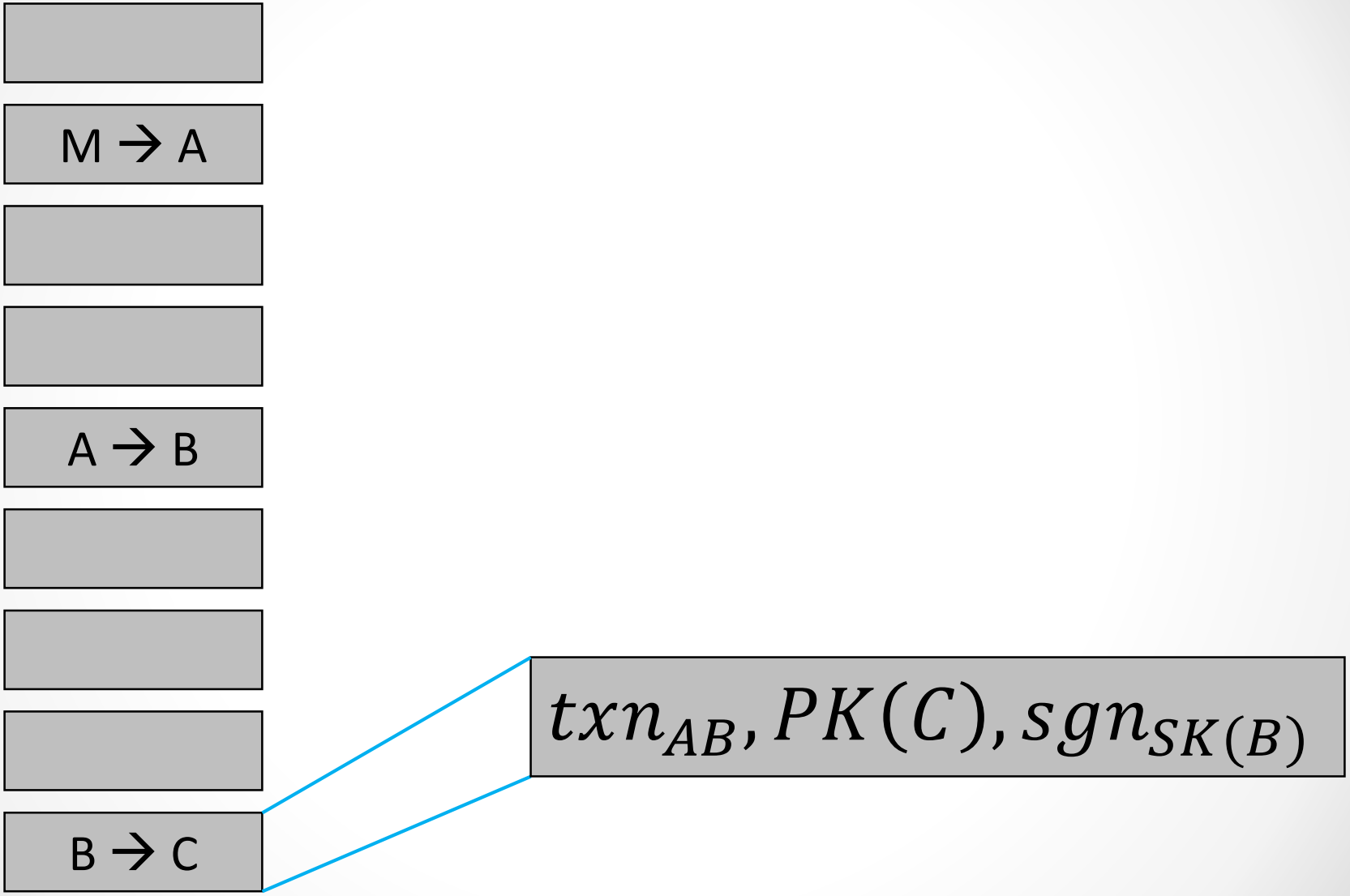
Global Ledger



Global Ledger

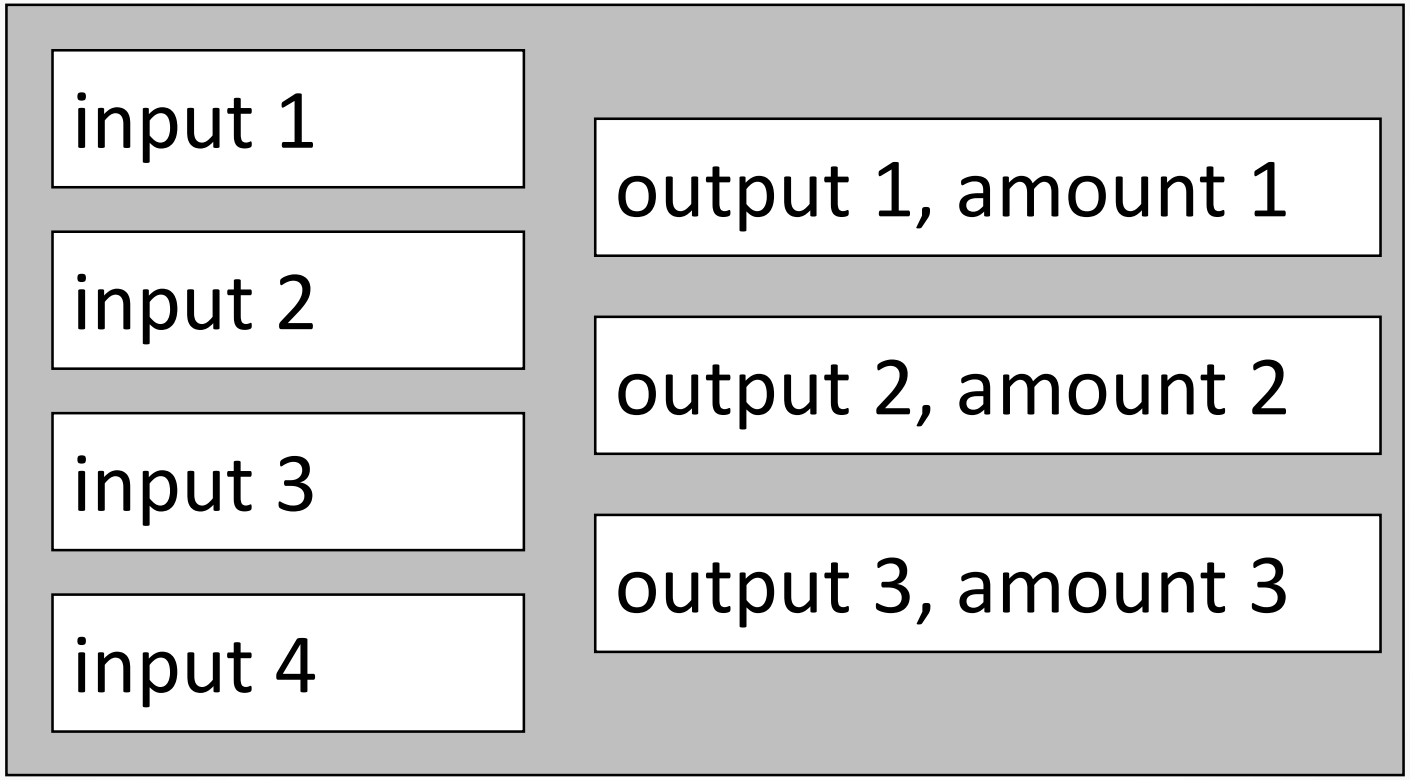


Addresses and Transactions



Addresses and Transactions

Transaction structure (roughly):



Inputs are fully spent.

Goal

1. No stealing
2. No double-spending

The Blockchain

Global Ledger

Global Ledger of all transactions

Requirements

1. No central control
2. High availability, security
3. Impossible to manipulate
4. Distributed minting

Global Ledger

Sounds like my bank!

Global Ledger of all transactions

Requirements

1. No central control
2. High availability, security
3. Impossible to manipulate
4. Distributed minting

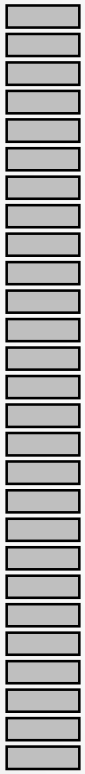
Doesn't sound like my bank.

Global Ledger

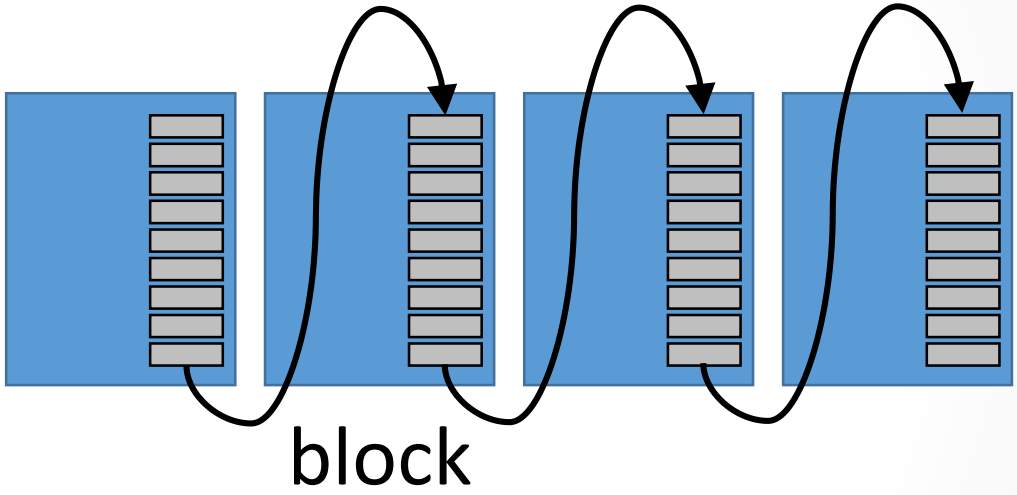
- Distributed system
- Open
- Consensus (not exactly)
- Byzantine model

The Blockchain

Ledger



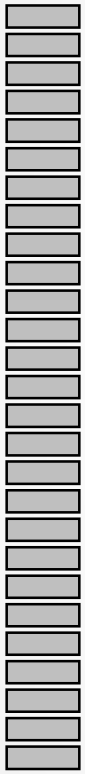
Blockchain



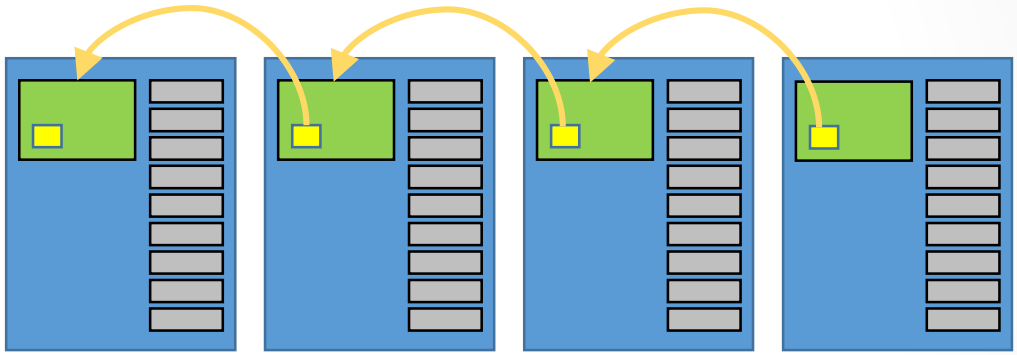
block

The Blockchain

Ledger



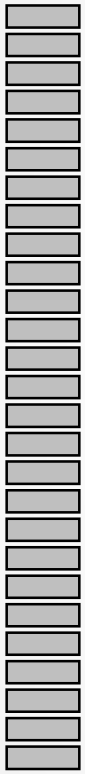
Blockchain



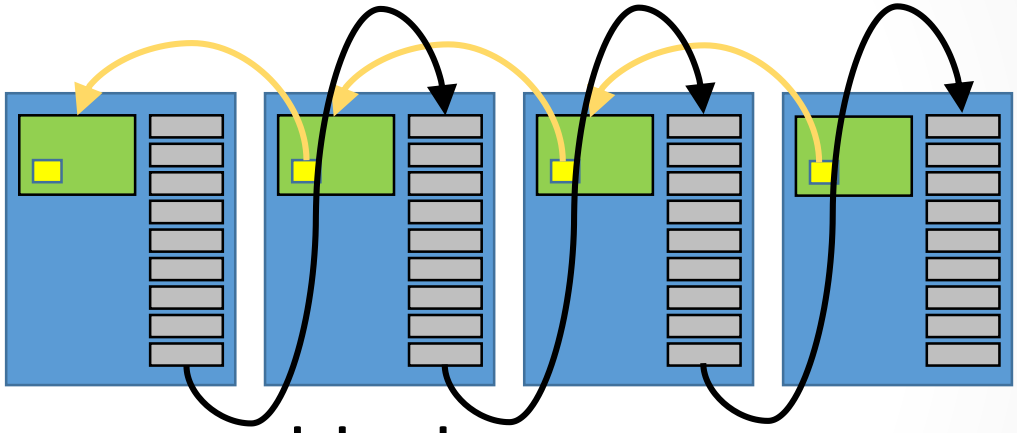
block

The Blockchain

Ledger

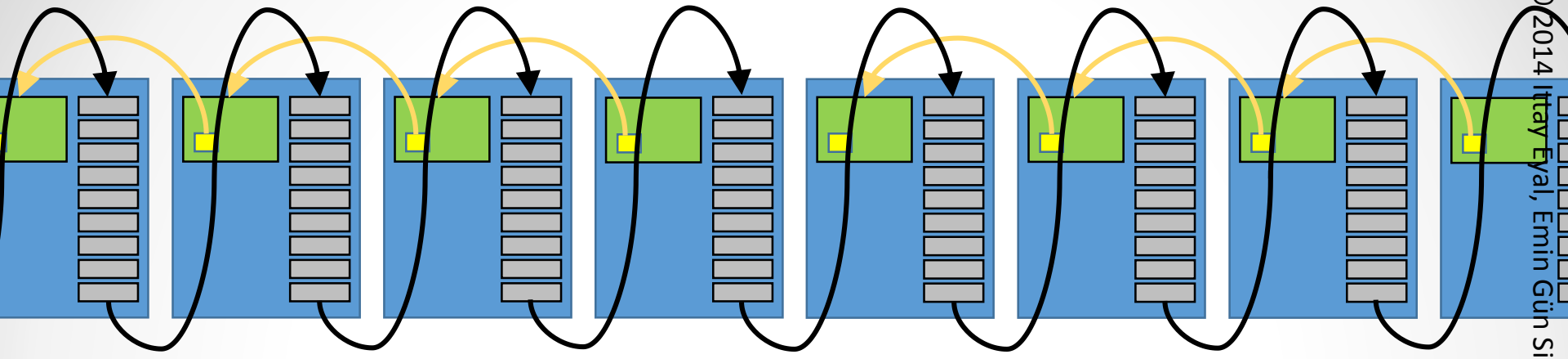


Blockchain



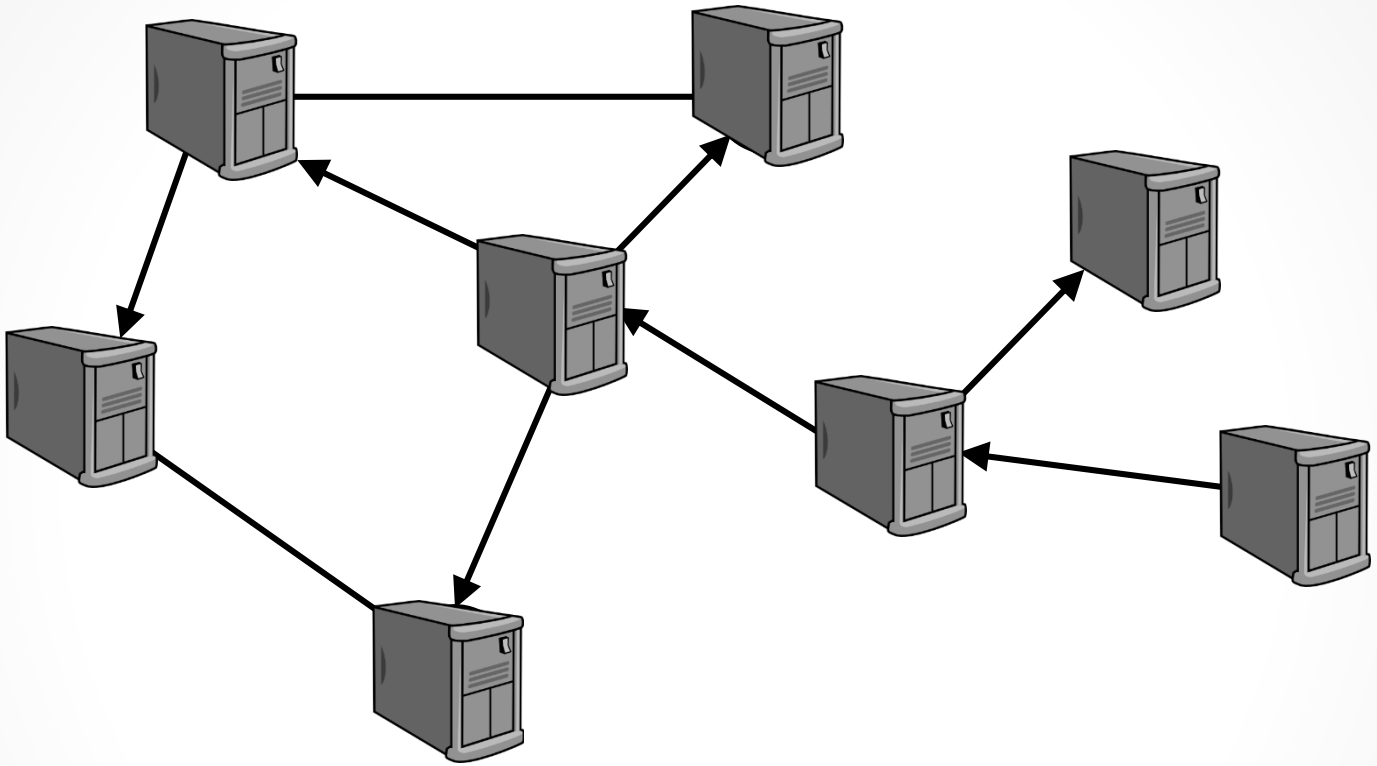
block

The Blockchain

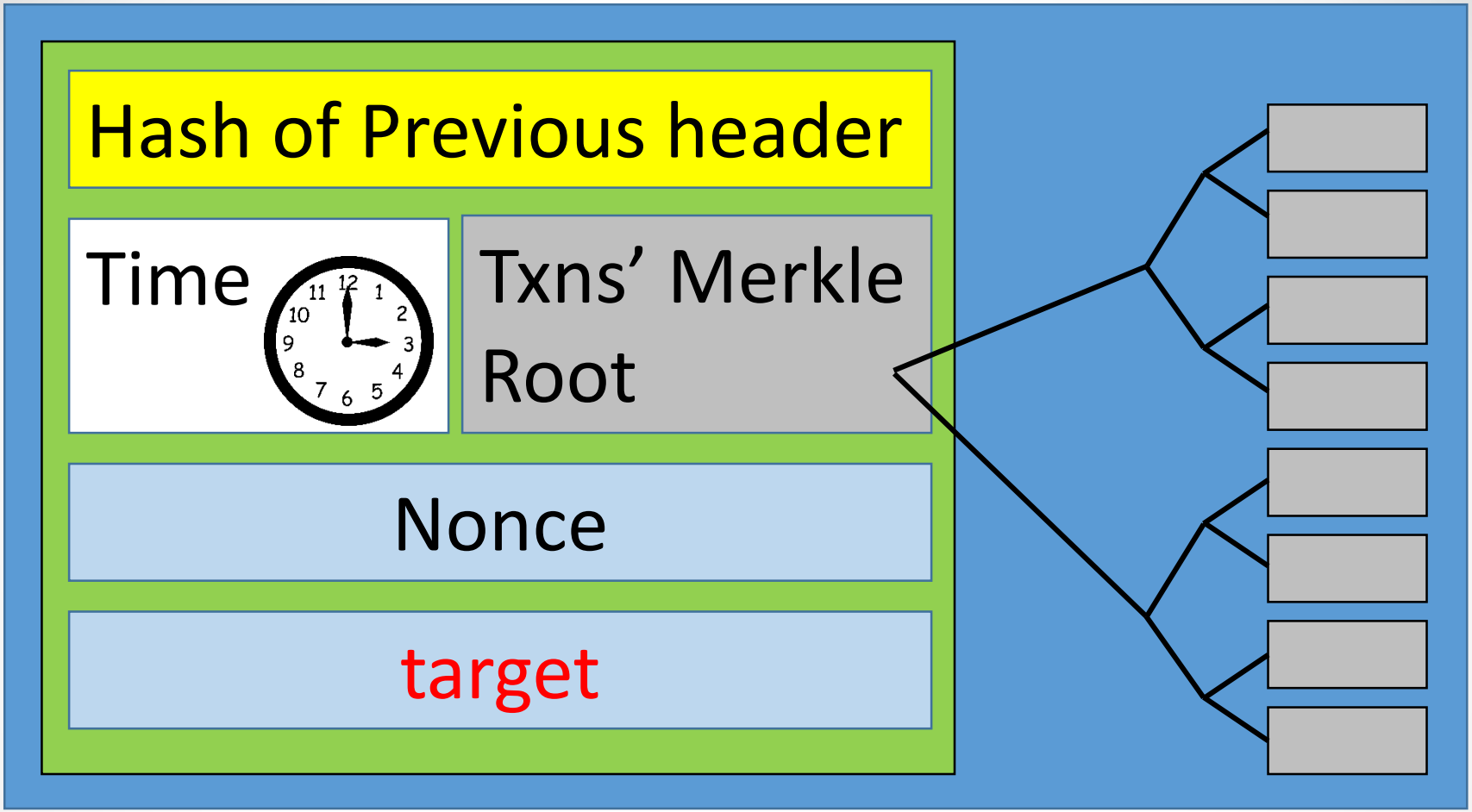


- Clients issue unforgeable transactions.
- Miners collate transactions and …
- add them to blockchain by solving cryptopuzzles,
- for which they receive a reward (minted coins).

Transaction and Block Propagation



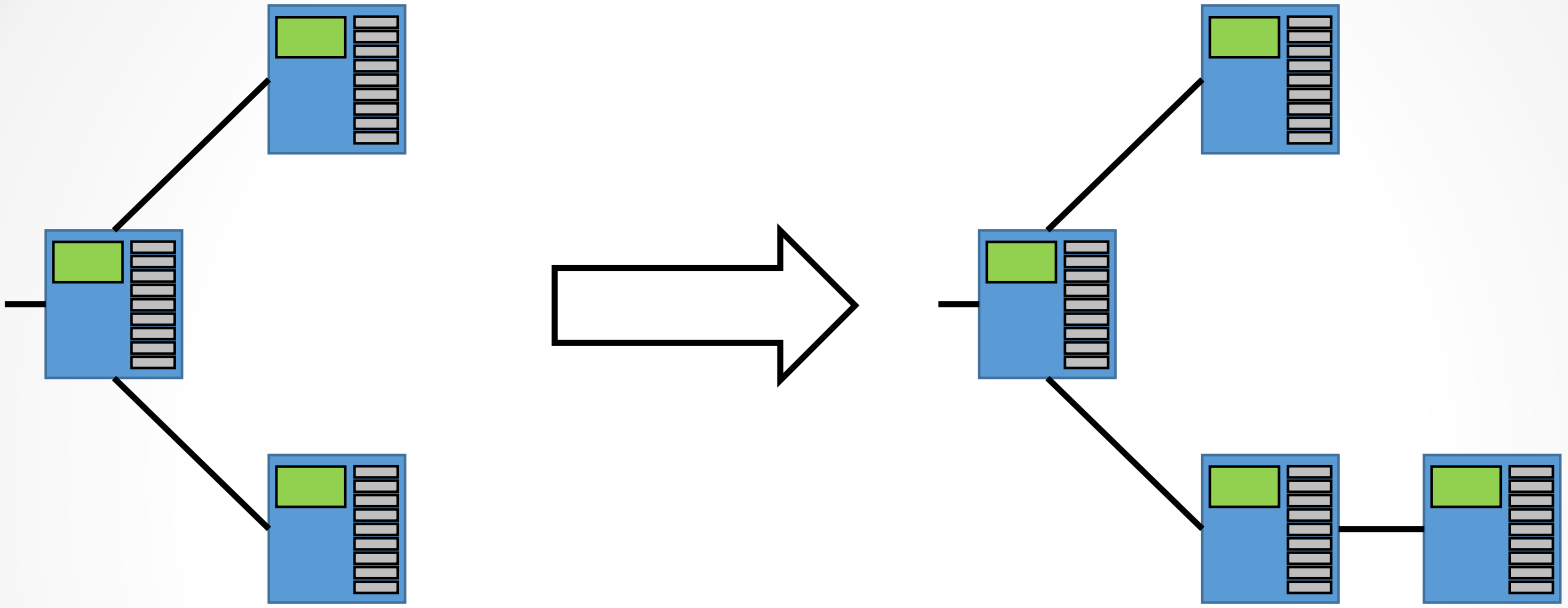
- Nodes propagate legal transactions and blocks.
- Blocks are difficult to create



Auto-adjusting difficulty cryptopuzzle:

SHA256(**SHA256**(block-header)) < target

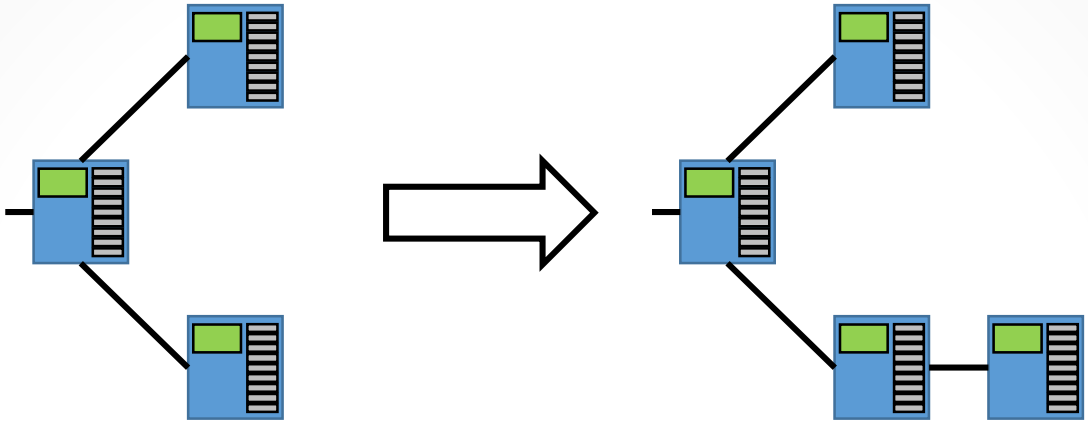
Forks



- Longest chain of blocks
  - Tiebreaker: earliest

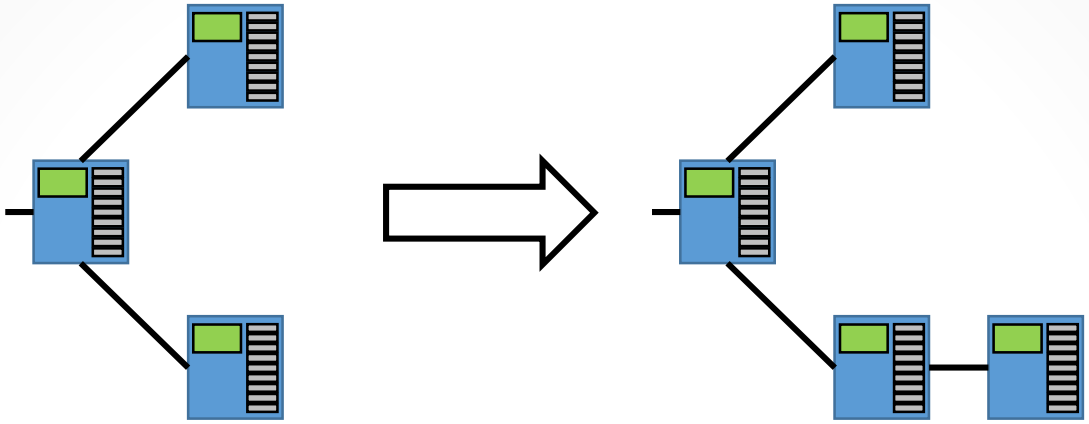
A weak form of consensus

Fork Resolution



- Requirement: **compute majority is honest**
- **Hardest** chain of blocks (aggregate difficulty)
  - Or the one you heard of first.

Fork Resolution



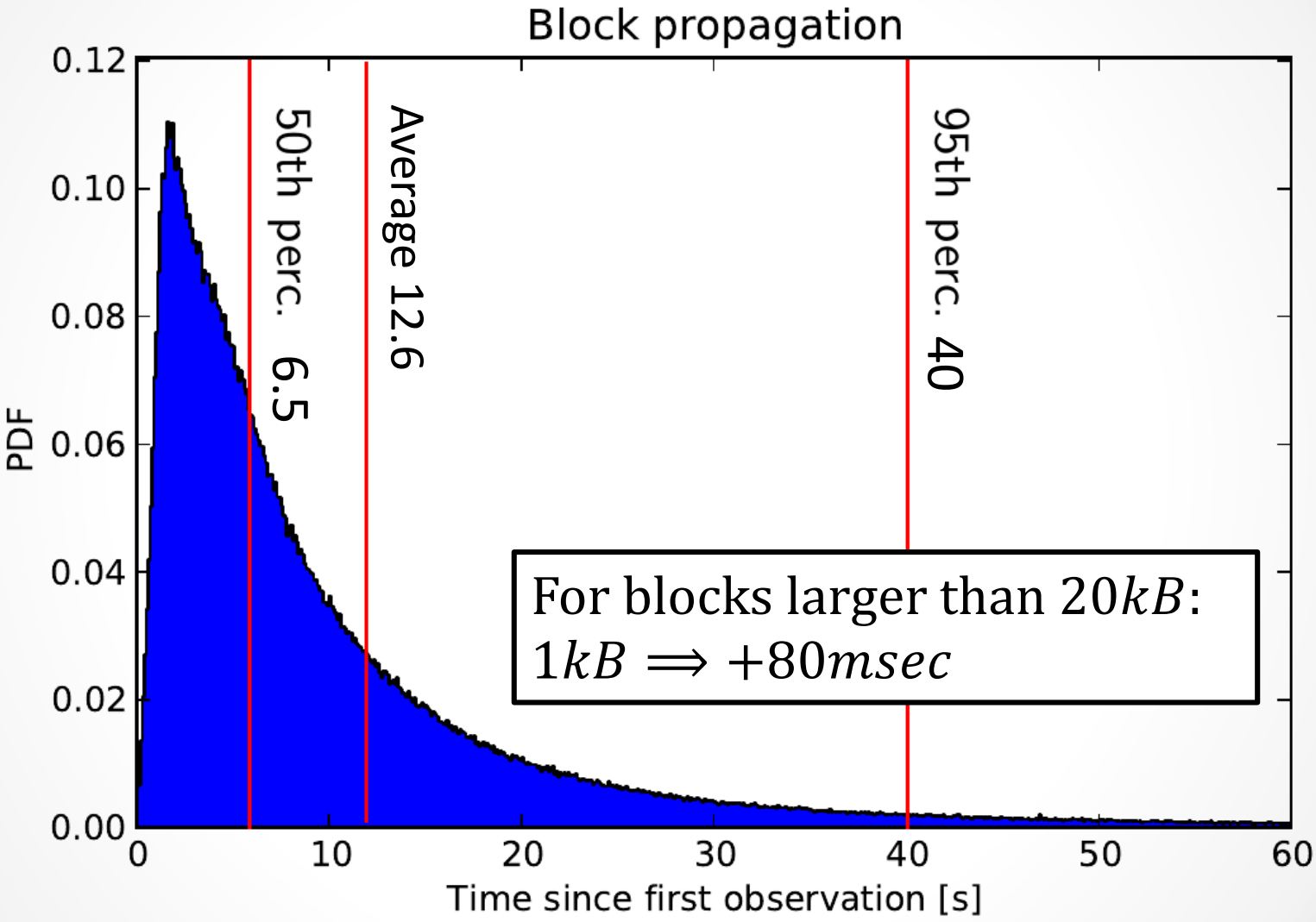
- Requirement: **compute majority is honest**
- **Hardest** chain of blocks (aggregate difficulty)
  - Or the one you heard of first.

Dishonest majority controls blockchain

(More on that later)

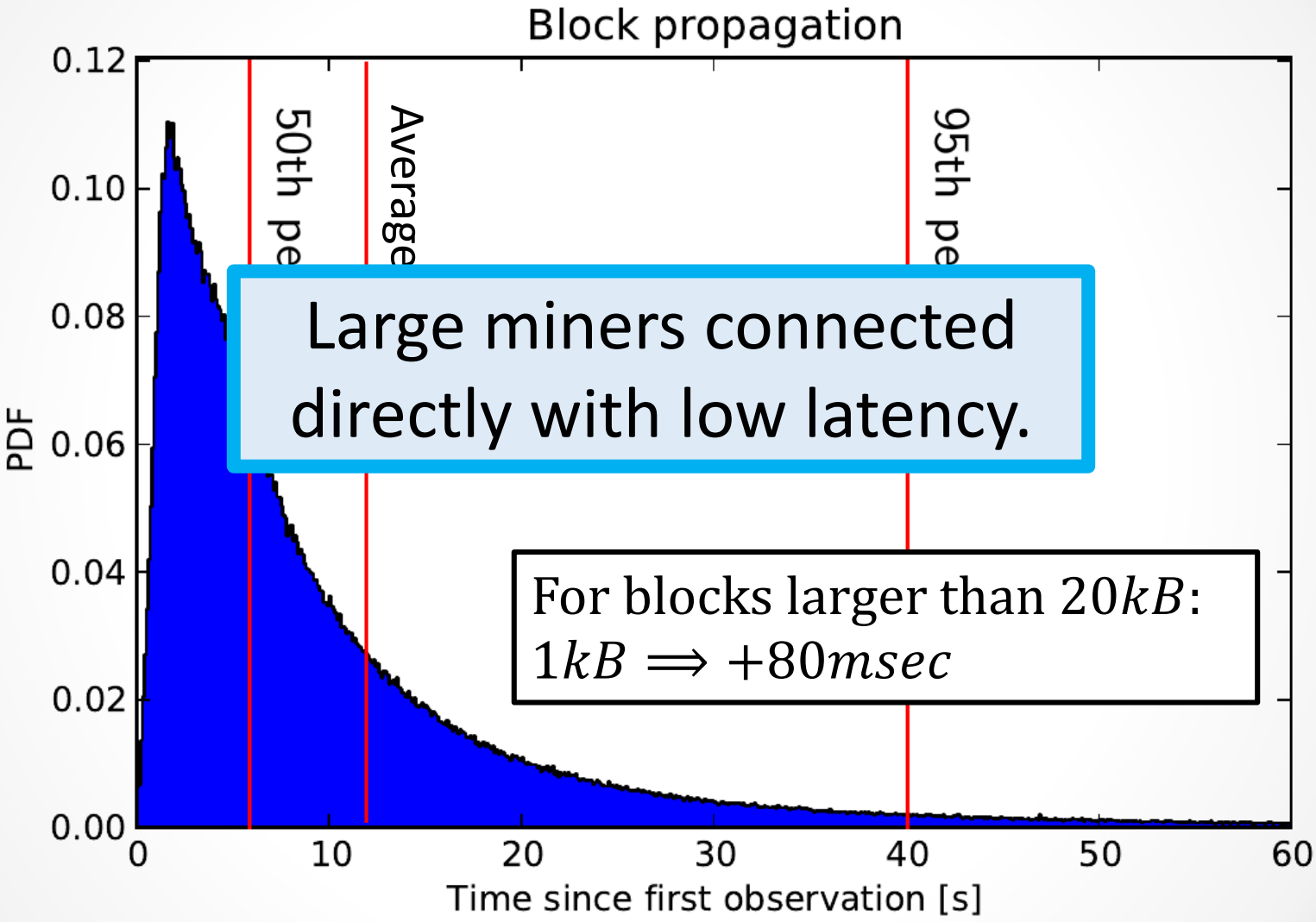
Block Propagation

Block Propagation



[Decker and Wattenhofer '13]

Block Propagation

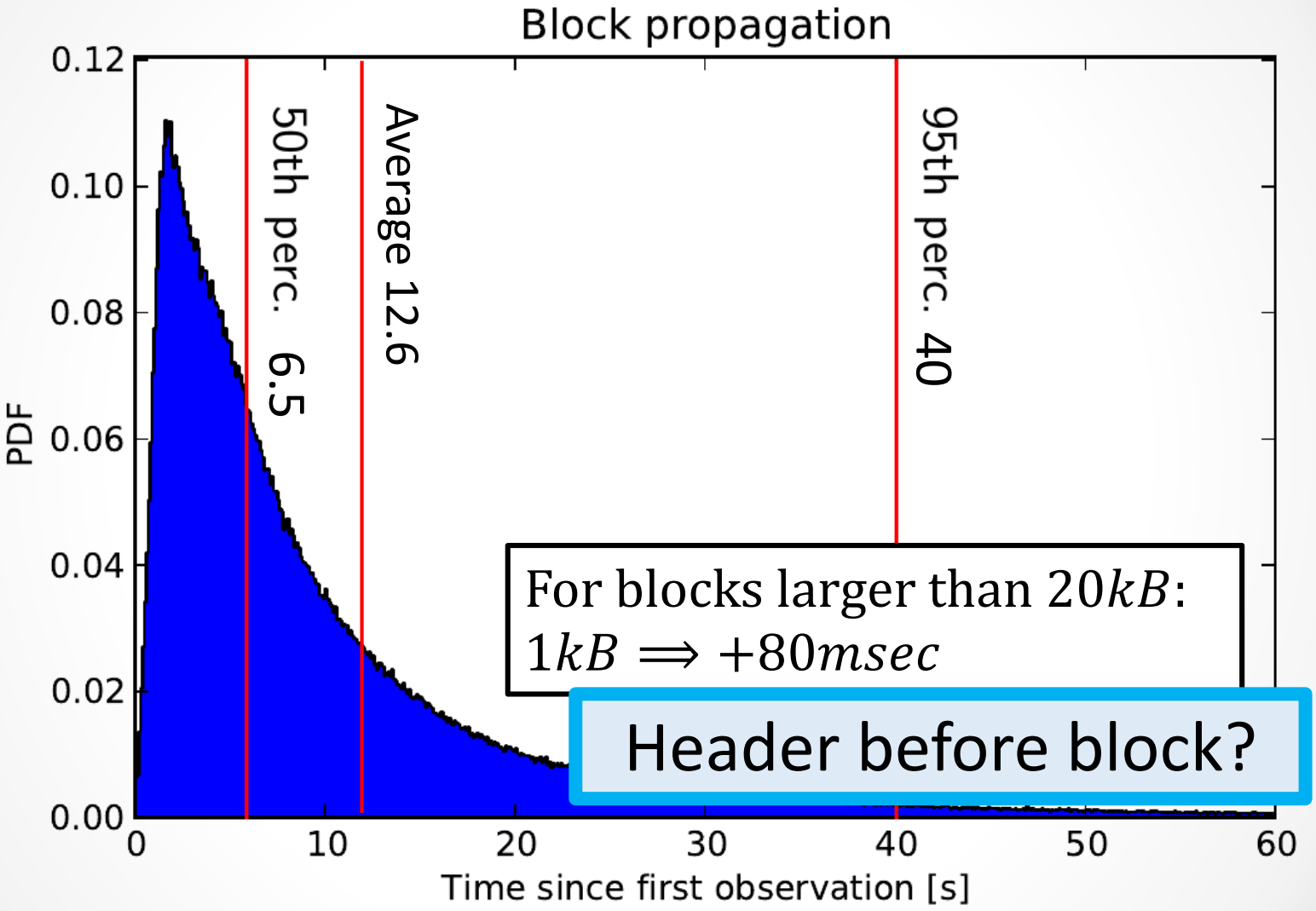


Large miners connected directly with low latency.

For blocks larger than $20kB$:
$1kB \Longrightarrow +80msec$

[Decker and Wattenhofer '13]

Block Propagation



For blocks larger than $20kB$:
$1kB \Longrightarrow +80msec$

Header before block?

[Decker and Wattenhofer '13]

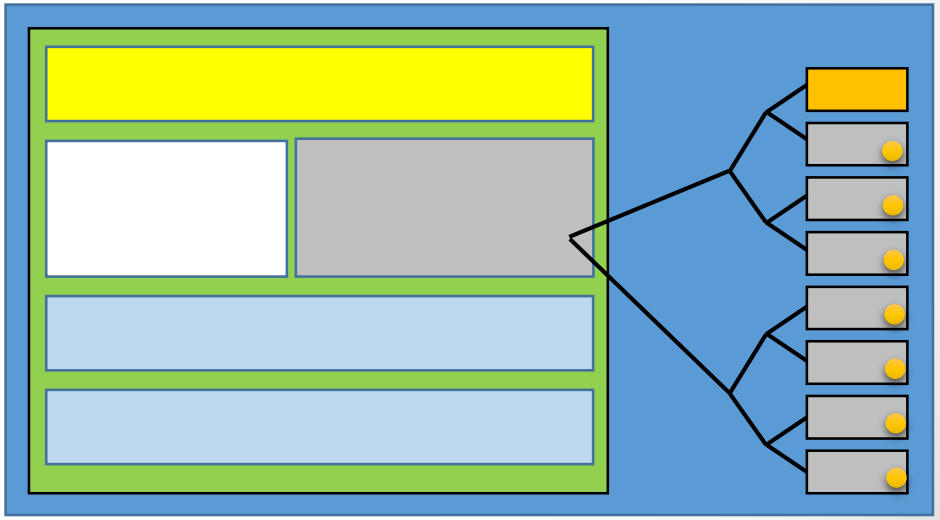
Mining

Motivation?

- Prize:
  - Mining: Newly minted coins (today 25฿, total 21 million at 2140)
  - Transaction fees (up to ~10^{-4}฿/1KB).

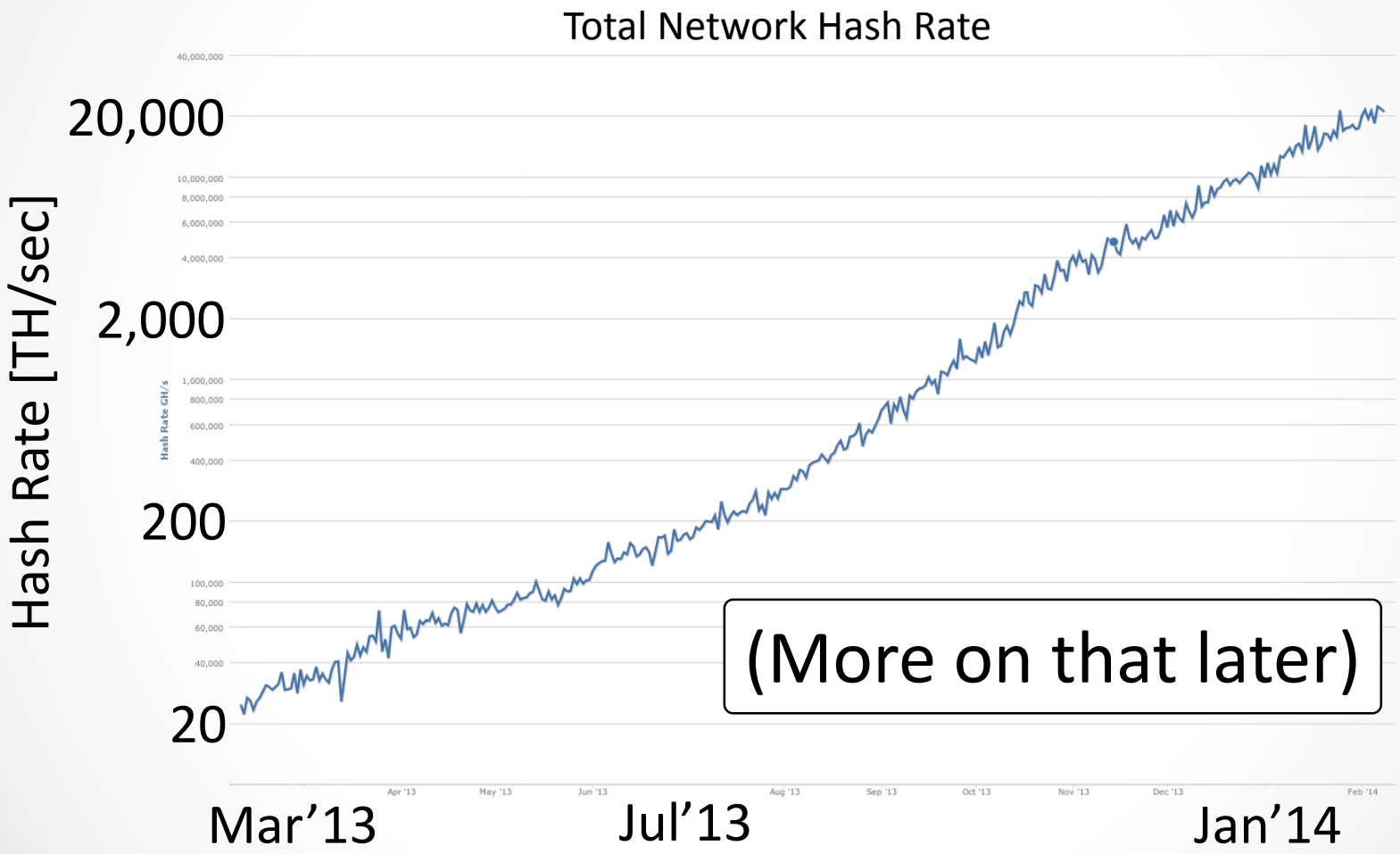
How?

- ***Coinbase*** transaction
- Transactions ***fees***



Mining

Difficulty rise:



[Blockchain.info]

Mining

Difficulty rise

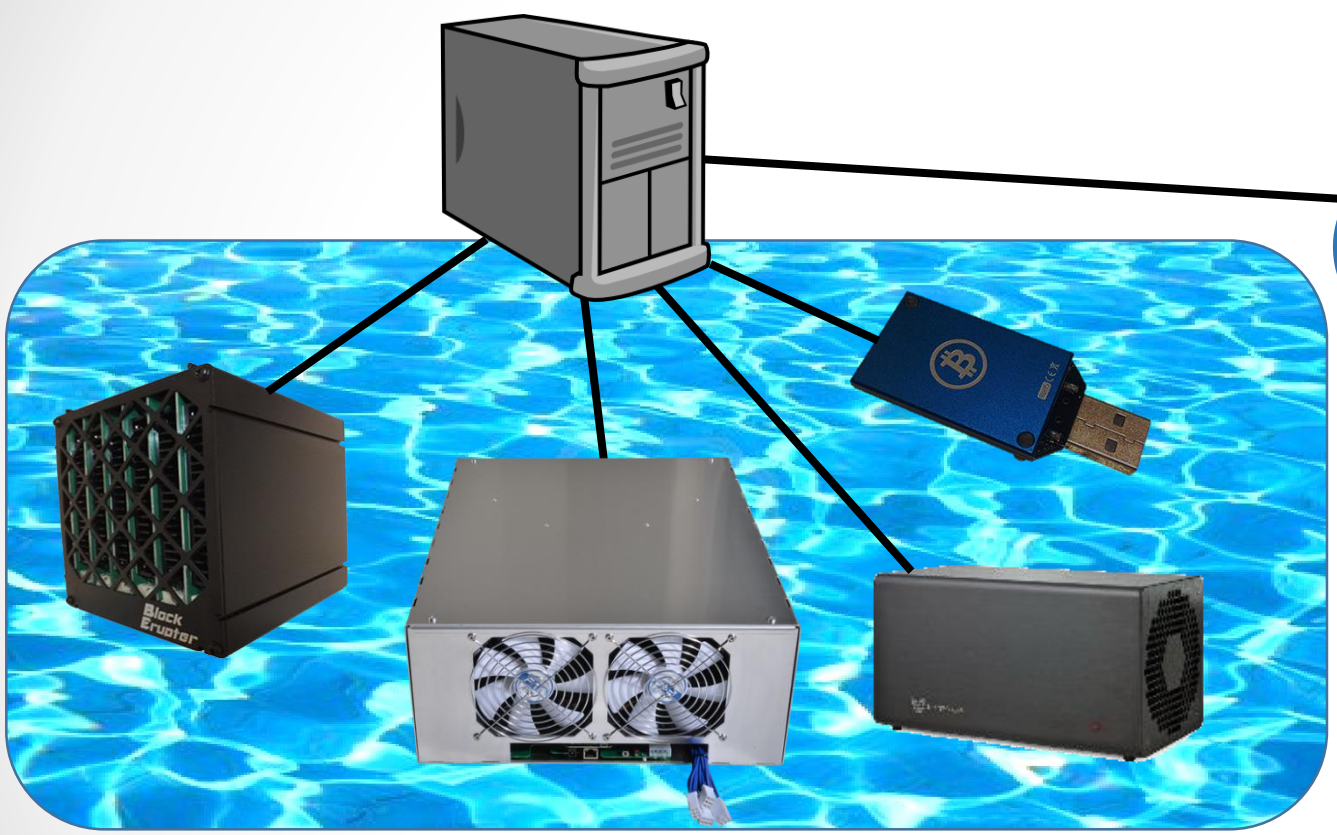
[Blockchain.info]

Mining Pools

Example:
(700 USD/BTC)

- **Avg revenue**: 6.71$ / day
- **HW break even**: ~1.5 years (w/ free power)
- **Time to block**: over 7 years

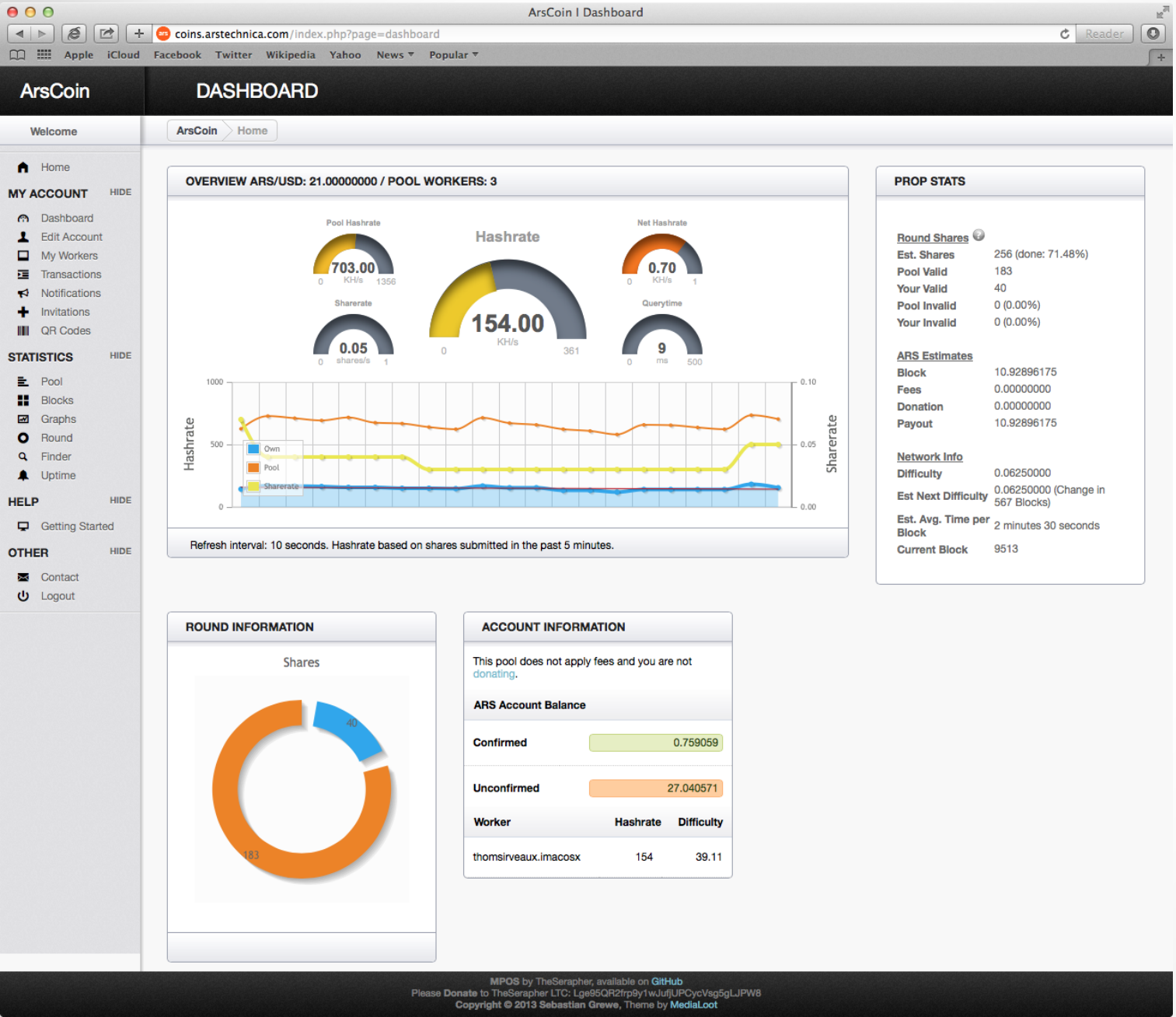
Mining Pools



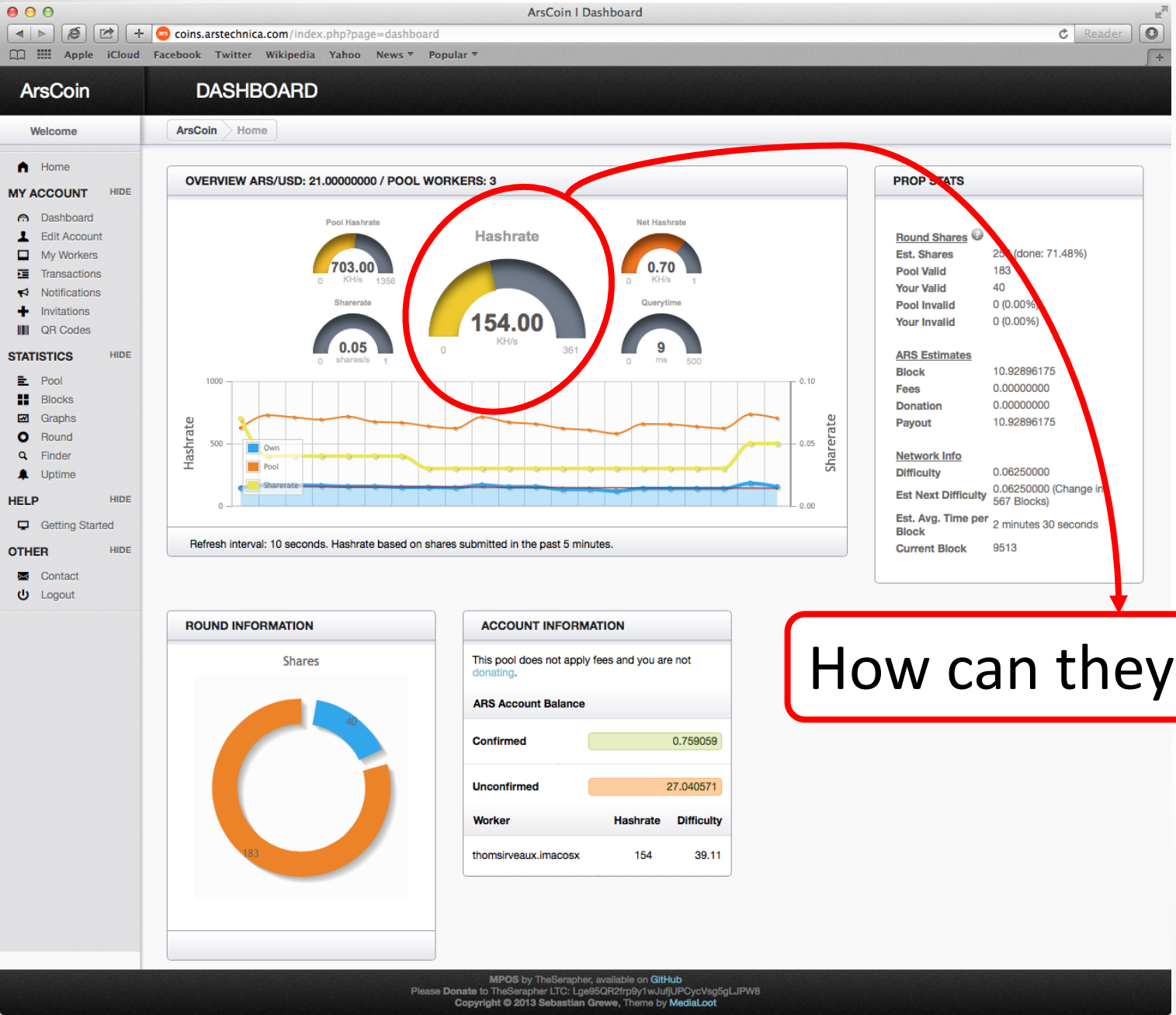
Bitcoin Network

- Pool with power α gets α of blocks
- Each miner makes the average (- pool fee)

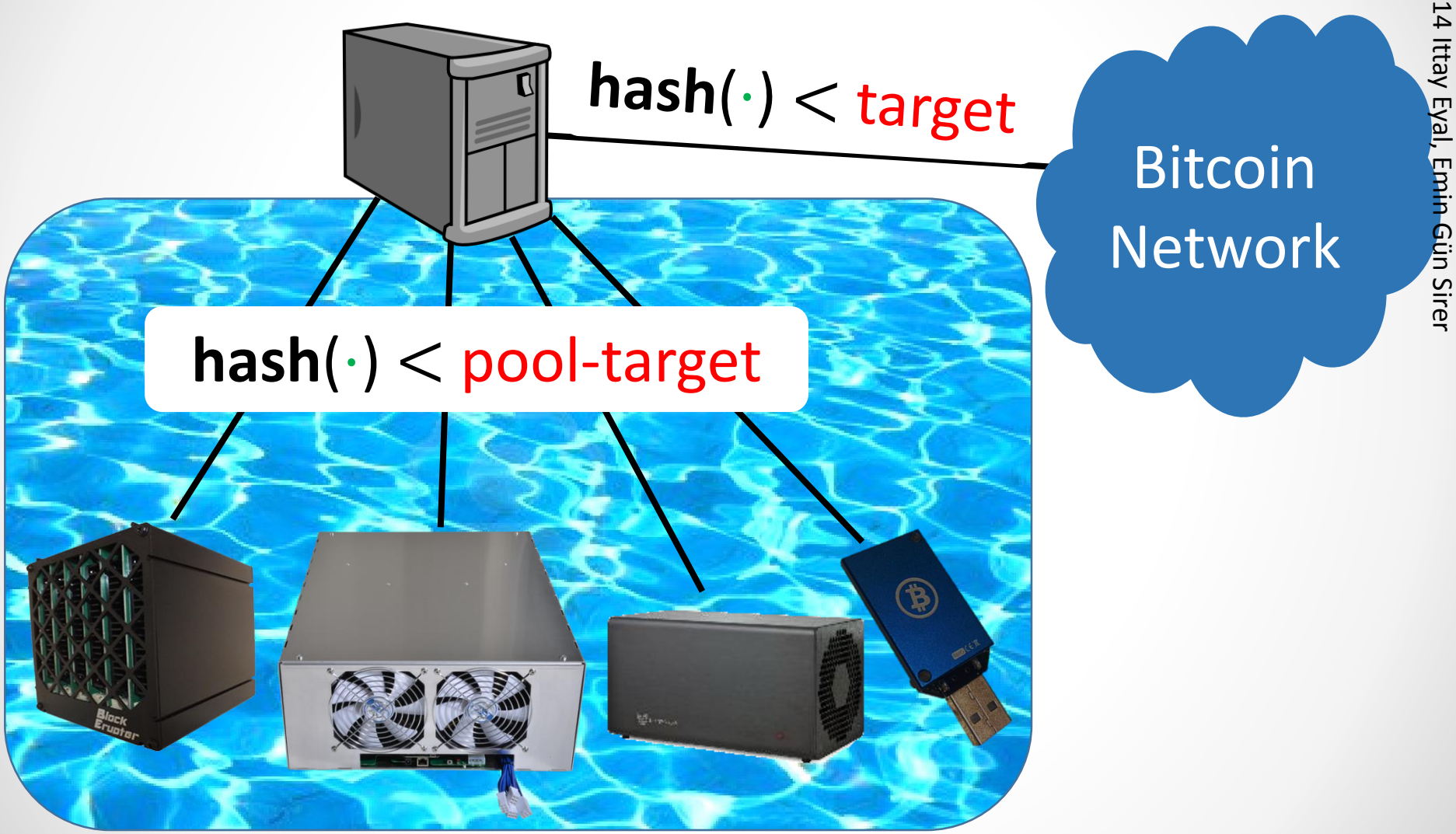
Mining Pools



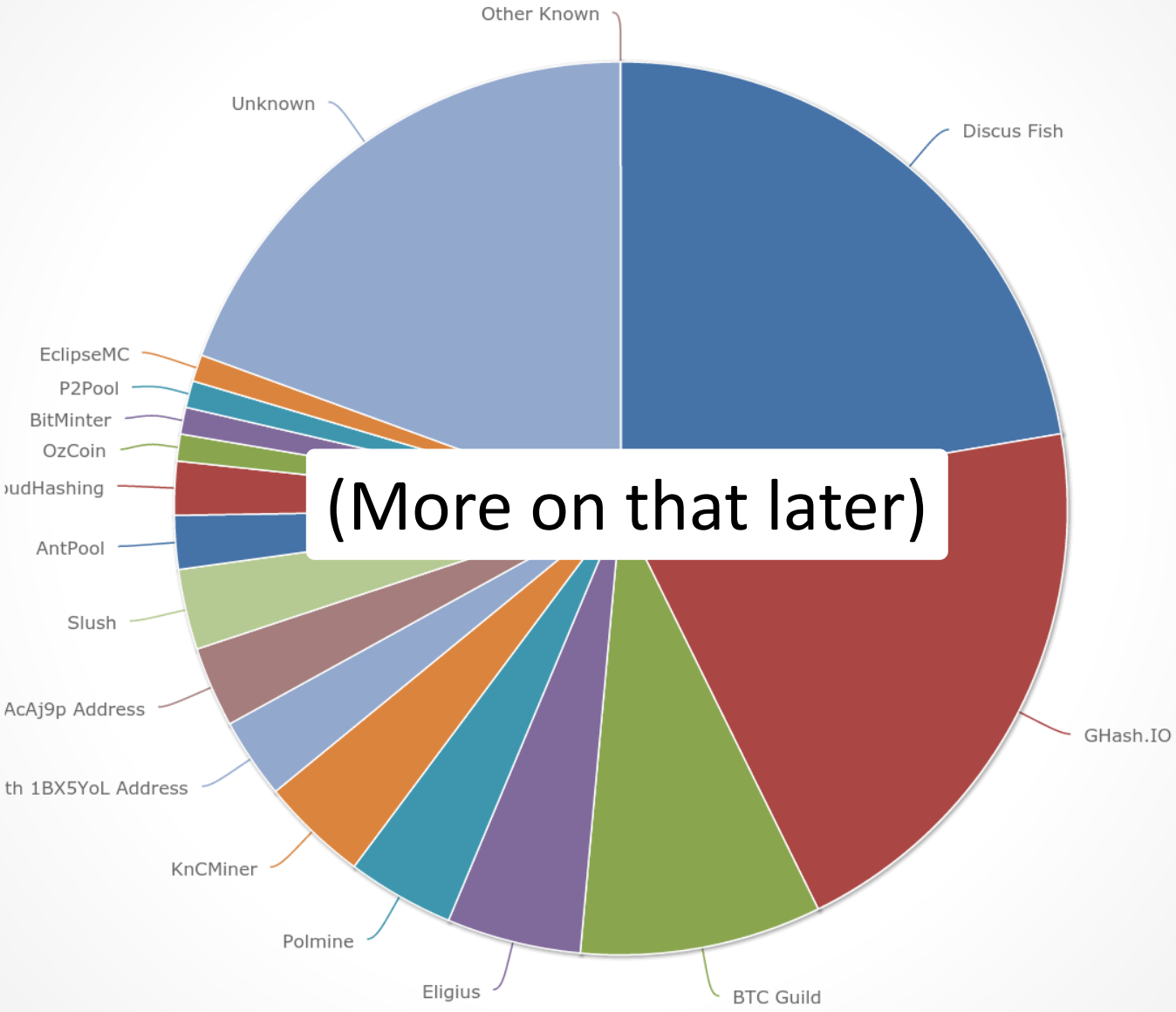
Mining Pools



Mining Pools



Mining Pools

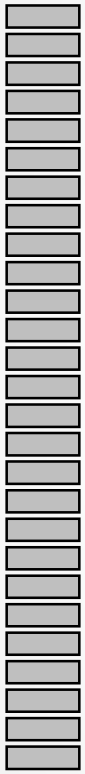


[Blockchain.info, February 2014]

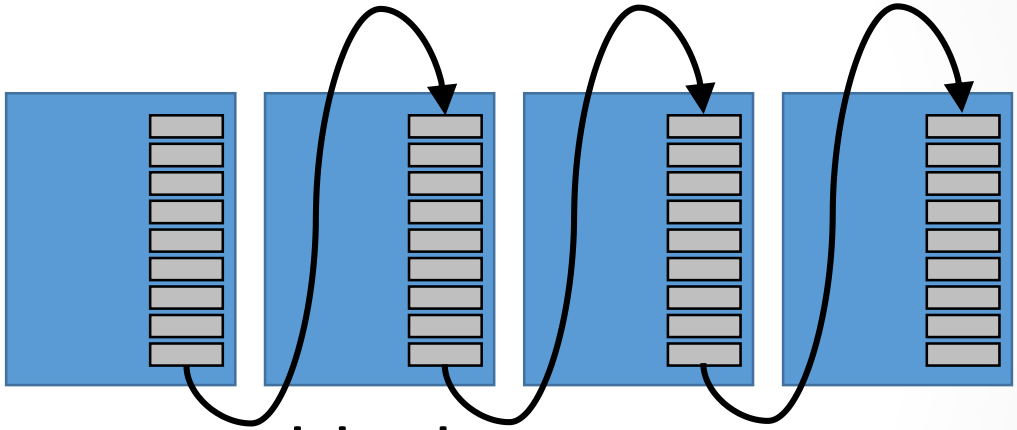
Transactions

Transactions

Ledger

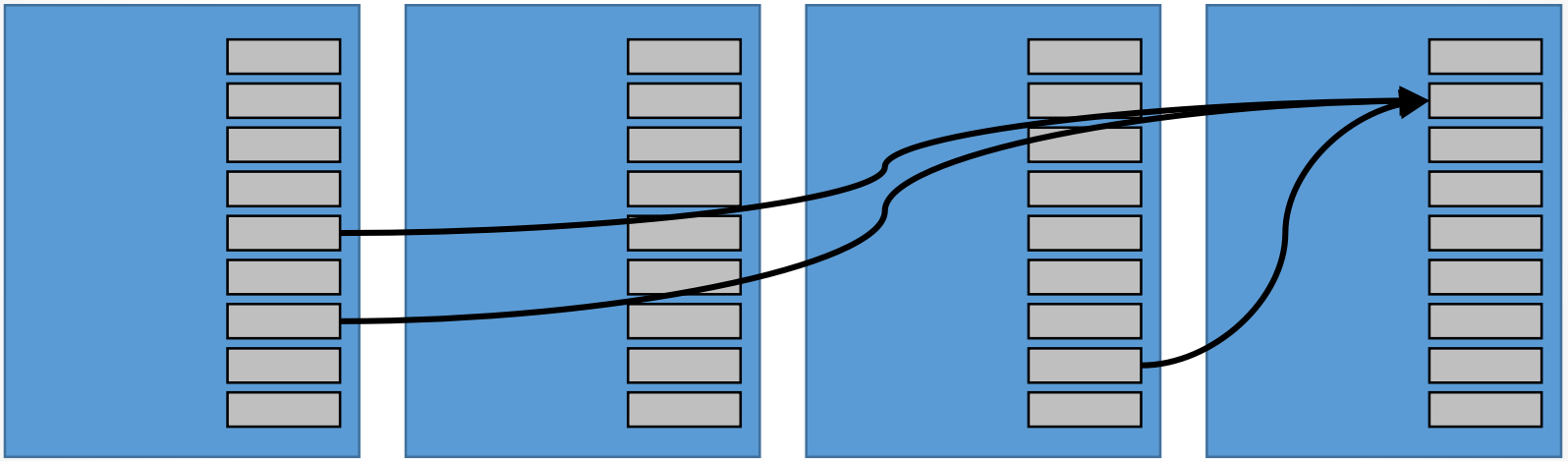


Blockchain

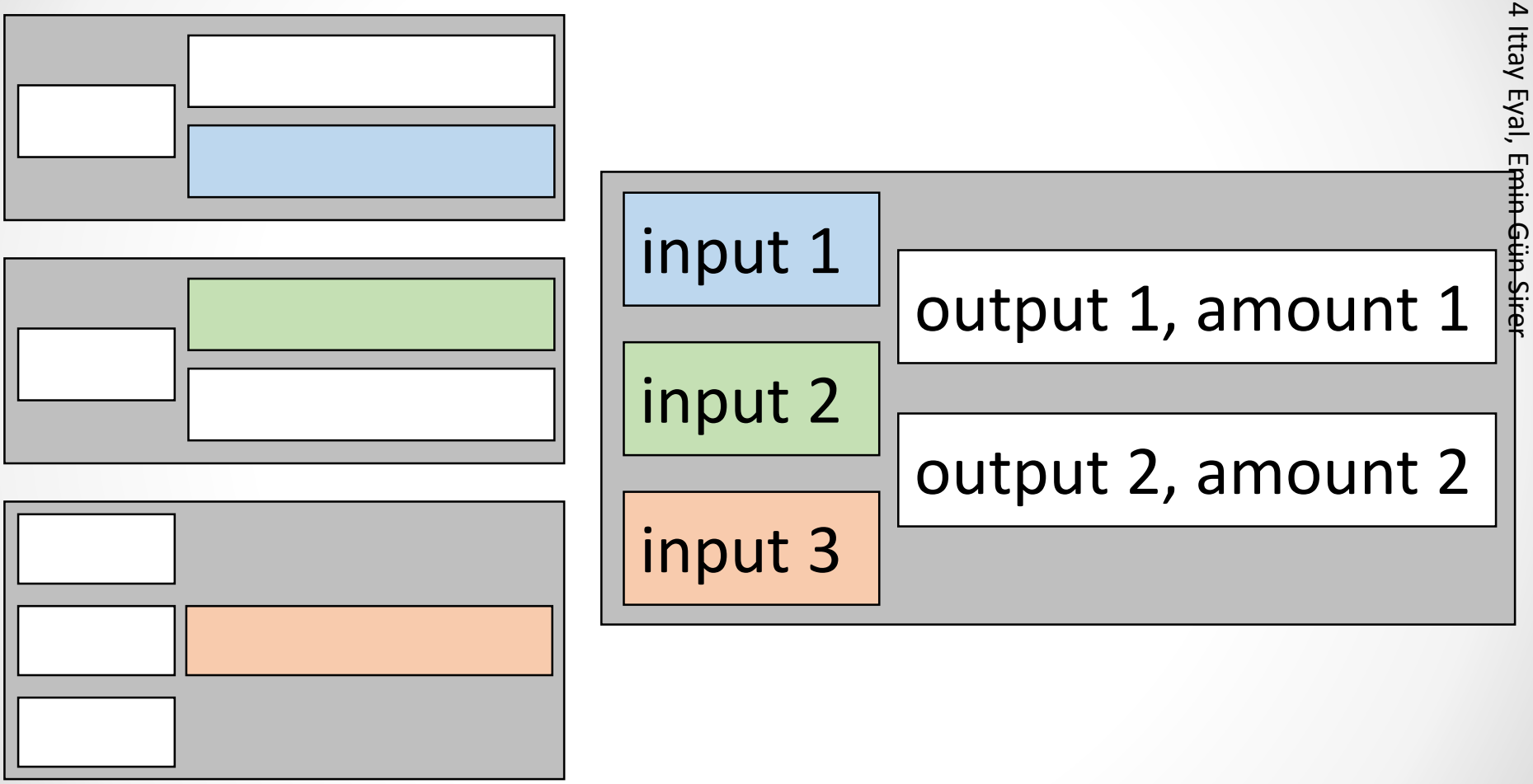


block

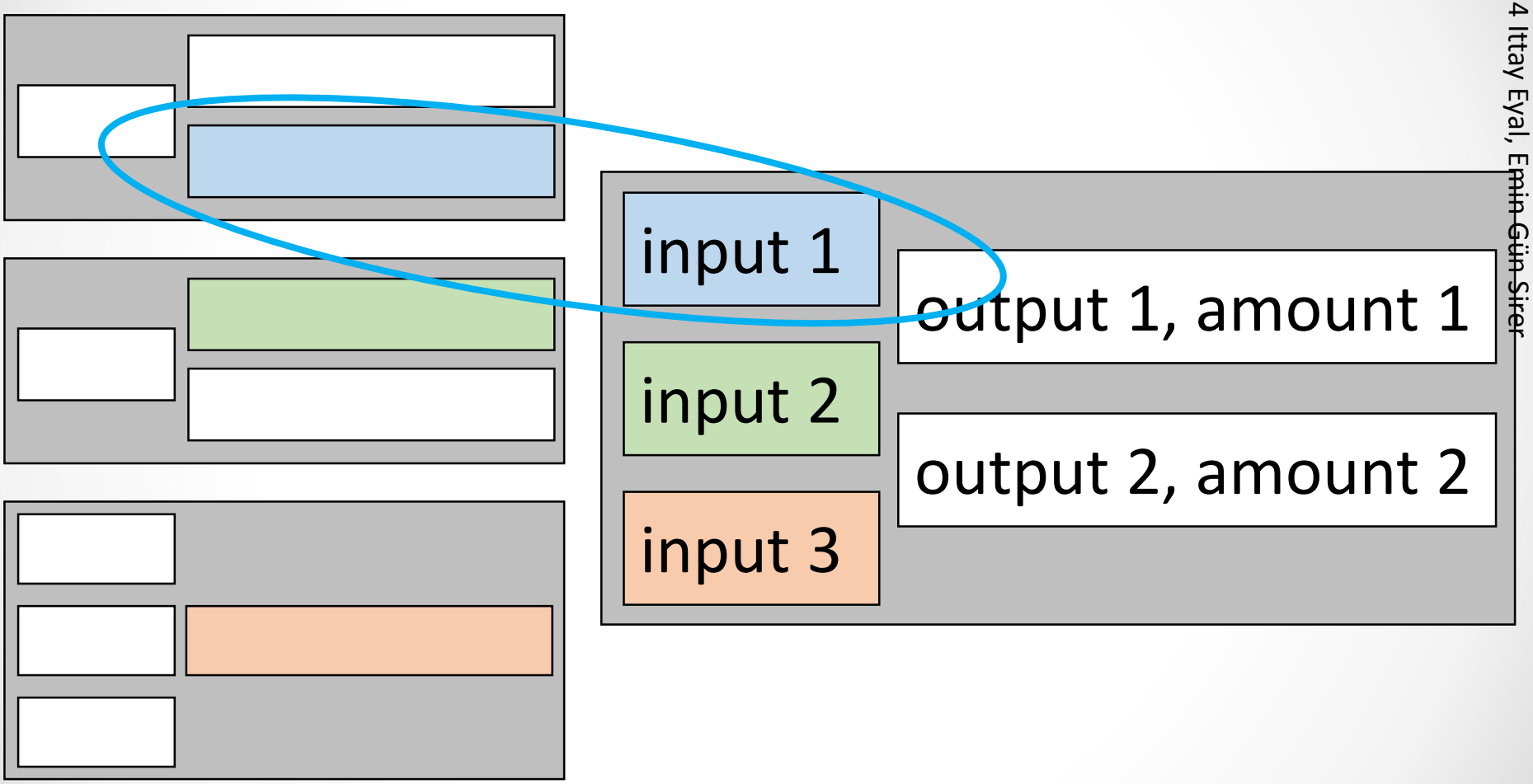
Transactions



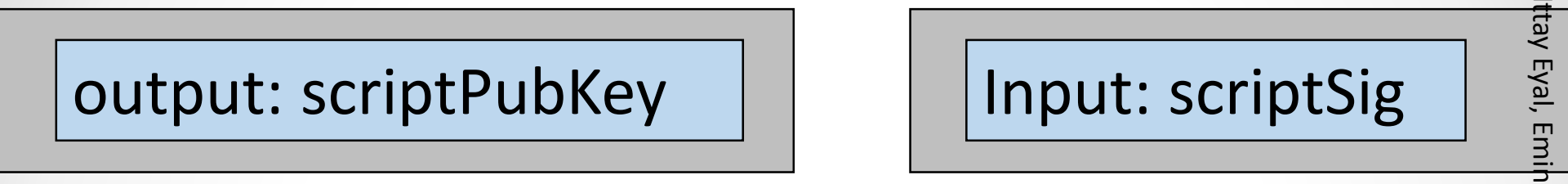
Transactions



Transactions



Pay-to-PubkeyHash



Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

output: scriptPubKey

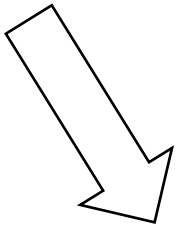
Input: scriptSig

Address is the public key hash.

Owner signs with matching private key.

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`



Stack

Verification script

`<sig>`
`<pubKey>`
`OP_DUP`
`OP_HASH160`
`<pubKeyHash>`
`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

`<sig>`

Verification script

`<pubKey>`
`OP_DUP`
`OP_HASH160`
`<pubKeyHash>`
`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

`<pubKey>`
`<sig>`

Verification script

`OP_DUP`
`OP_HASH160`
`<pubKeyHash>`
`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

`<pubKey>`
`<pubKey>`
`<sig>`

Verification script

`OP_HASH160`
`<pubKeyHash>`
`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

`hash160(<pubKey>)`
`<pubKey>`
`<sig>`

Verification script

`<pubKeyHash>`
`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

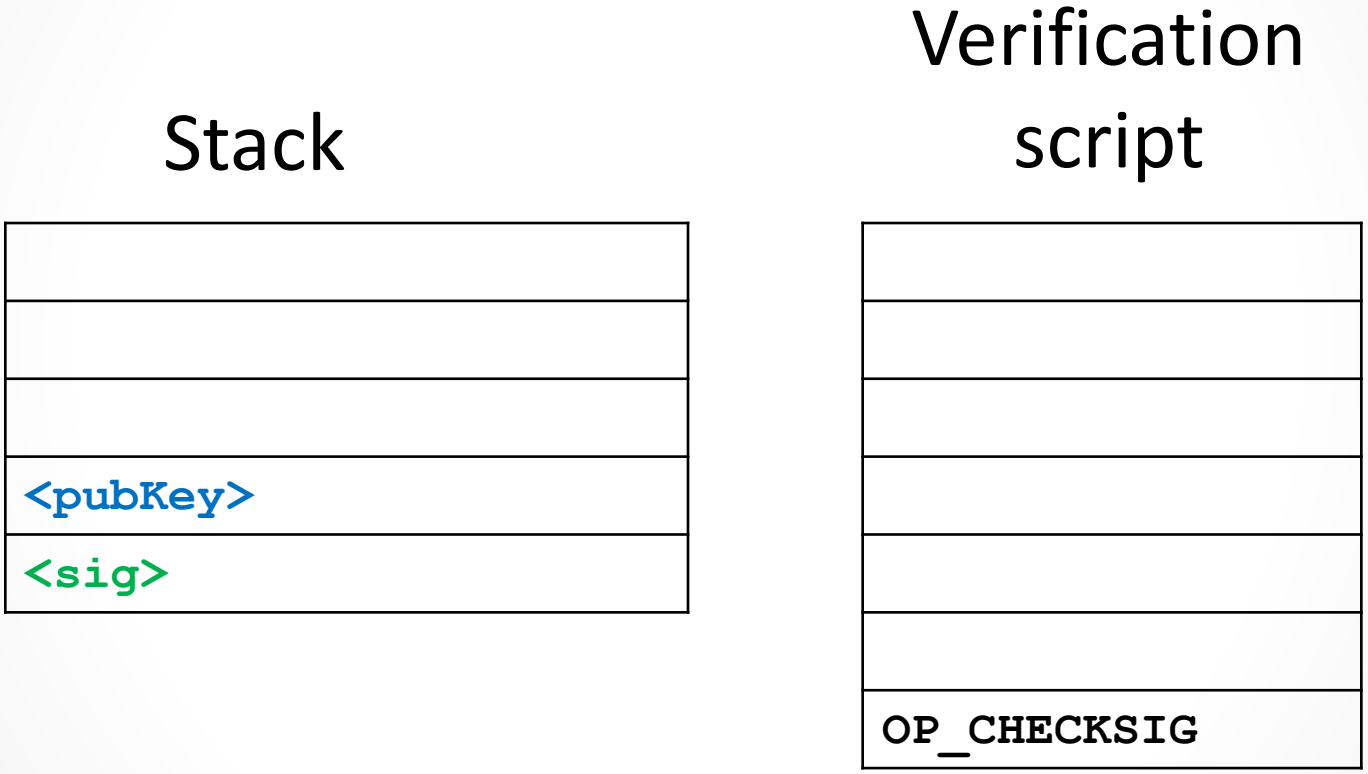
`<pubKeyHash>`
`hash160(<pubKey>)`
`<pubKey>`
`<sig>`

Verification script

`OP_EQUALVERIFY`
`OP_CHECKSIG`

Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

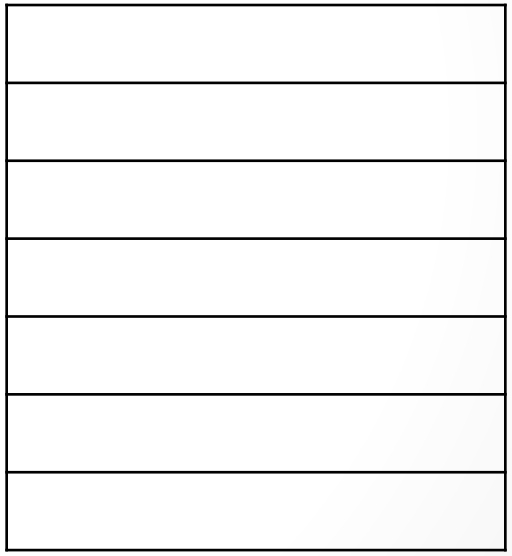


Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
scriptSig: `<sig> <pubKey>`

Stack

Verification script



Return true.

Other Transaction Types

- **Coinbase**
  No input
- **Pay to Script Hash (P2SH)**
  Script in signature (receiver side)
- **Multisig**
  Require k/n signatures