Cryptocurrencies
from technology to economy

Roger Wattenhofer

ETH Zurich – Distributed Computing Group

Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

Diebstahl Hacker erbeuteten bei einem Mitarbeiter der ETH Zürich 9222 Bitcoin. Heute sind die virtuellen Münzen 9 Millionen Franken wert. Der Fall liegt nun bei der Kantonspolizei.

VON CHRISTIAN BÜTIKOFER 06.12.2013

Cryptocurrencies

#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	$ 8,981,243,870	$ 574.31	15,638,375 BTC	$ 71,004,500
2	Ethereum	$ 1,172,919,101	$ 14.51	80,853,613 ETH	$ 9,933,140
3	Litecoin	$ 216,171,881	$ 4.68	46,149,551 LTC	$ 5,031,230
4	Ripple	$ 201,593,968	$ 0.005782	34,868,679,462 XRP *	$ 552,597
5	The DAO	$ 162,984,082	$ 0.138973	1,172,775,159 DAO *	$ 1,502,090
6	Dash	$ 51,232,986	$ 7.87	6,510,786 DASH	$ 248,316
7	Lisk	$ 46,560,900	$ 0.465609	100,000,000 LSK *	$ 2,472,480
8	Dogecoin	$ 27,584,159	$ 0.000263	104,686,099,387 DOGE	$ 506,232
9	MaidSafeCoin	$ 25,406,247	$ 0.056140	452,552,412 MAID *	$ 421,888
10	DigixDAO	$ 20,670,600	$ 10.34	2,000,000 DGD *	$ 65,517

What is Bitcoin?
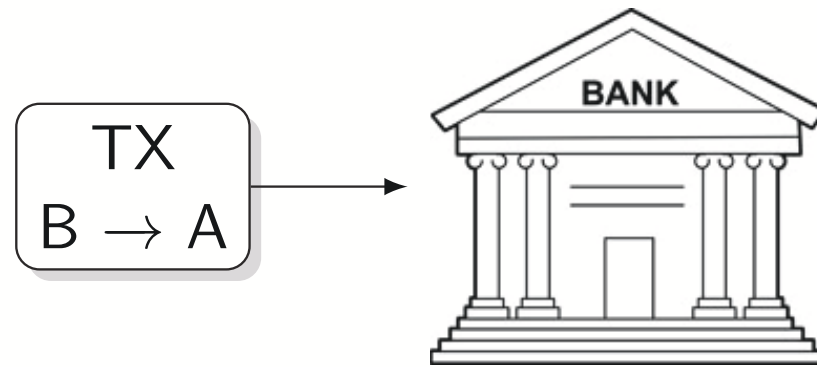
«Satoshi Nakamoto»
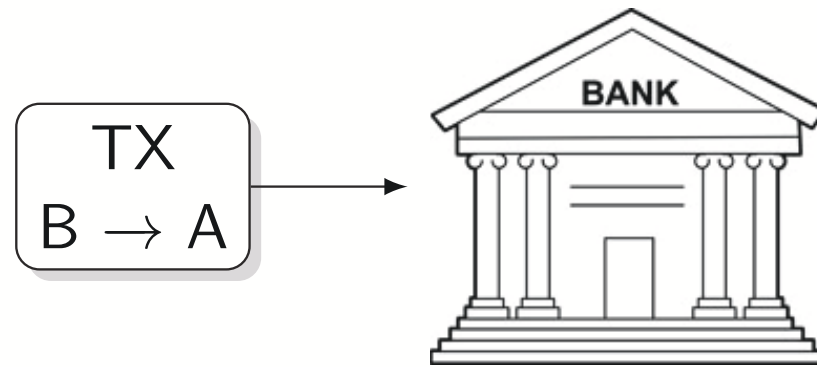
Technology

The Bank of Bitcoin

The Bank of Bitcoin

User	Balance
A	2
B	5
C	8

The Bank of Bitcoin

TX
B → A

BANK

User	Balance
A	2
B	5
C	8

The Bank of Bitcoin

User	Balance
A	~~2~~ 4
B	~~5~~ 3
C	8

Opening an Account in Bitcoin

$$\boxed{\text{Private Key}} \longrightarrow \boxed{\text{Public Key}} \longrightarrow \boxed{\text{Address}}$$

Transferring Bitcoins
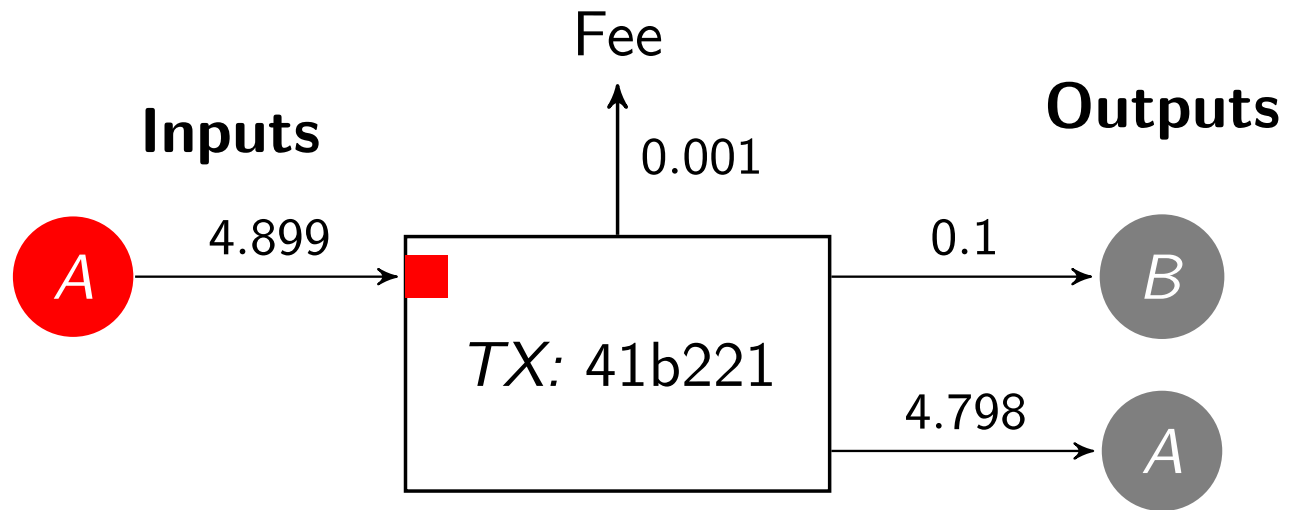
TX: 41b221

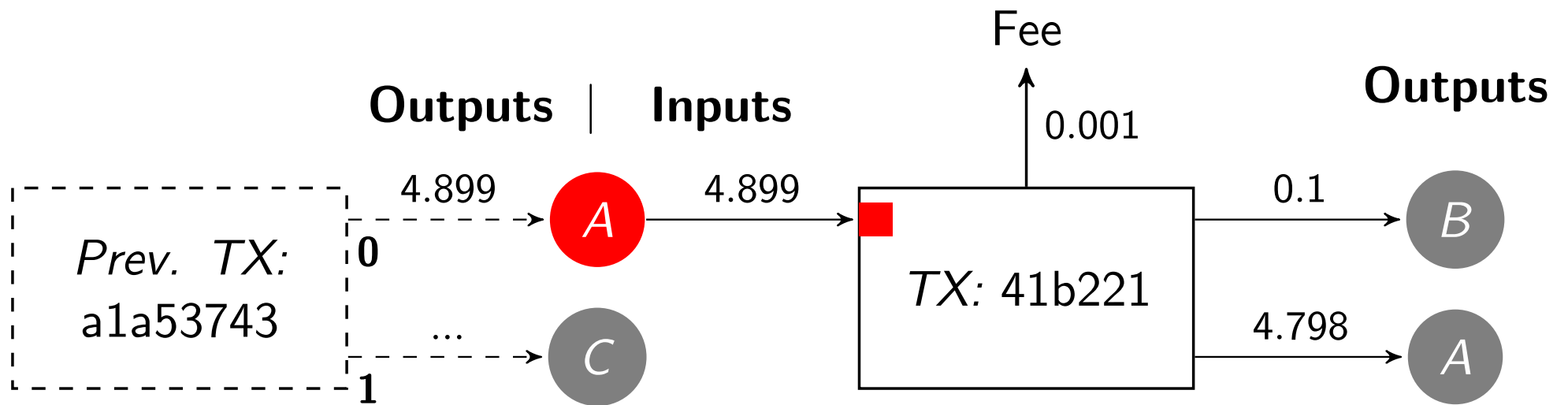# Transferring Bitcoins
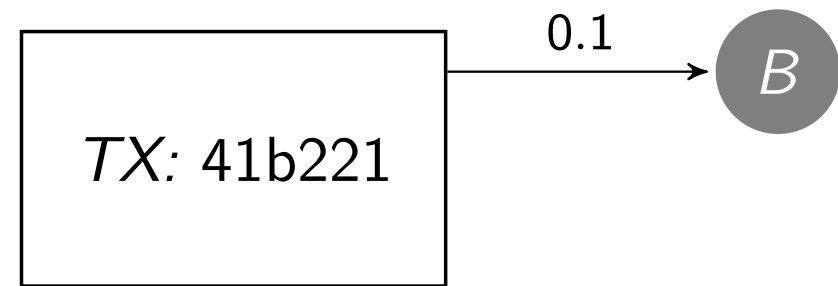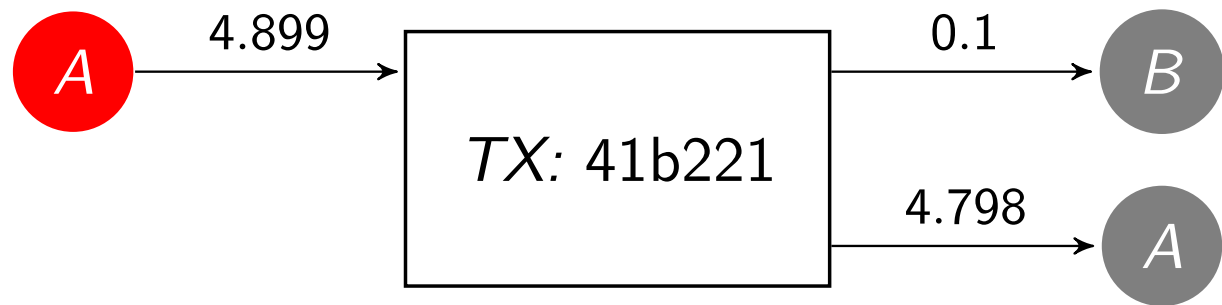
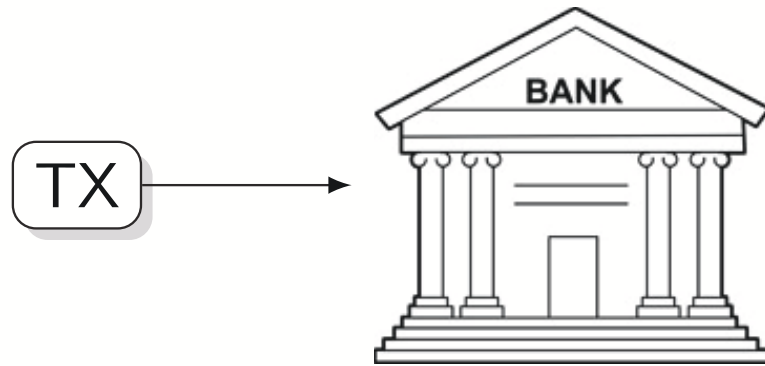# Transferring Bitcoins

Transferring Bitcoins

Transferring Bitcoins

Inputs

Outputs

A —— 4.899 ——→ ☐ **TX:** 41b221 —— 0.1 ——→ B

—— 4.798 ——→ A

Transferring Bitcoins

Inputs

Fee

Outputs

4.899

0.001

A

TX: 41b221

0.1

B

4.798

A
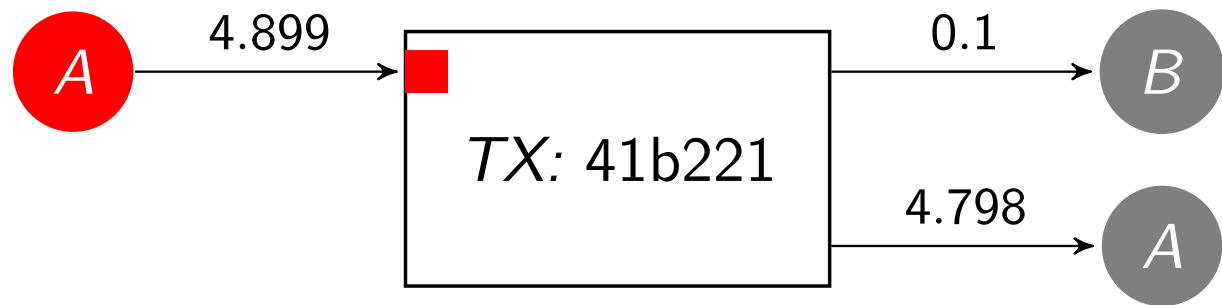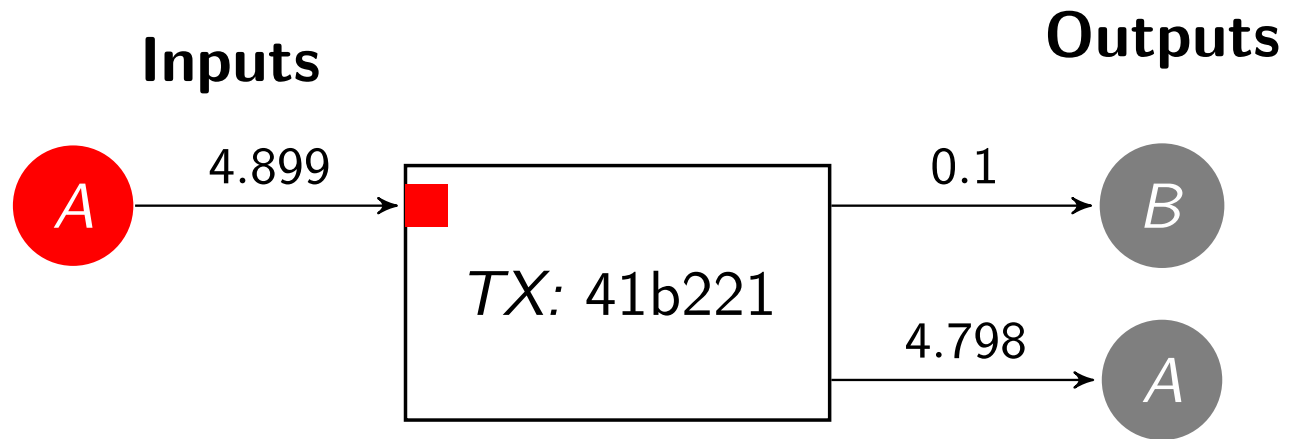
Transferring Bitcoins

Distributing the Bank

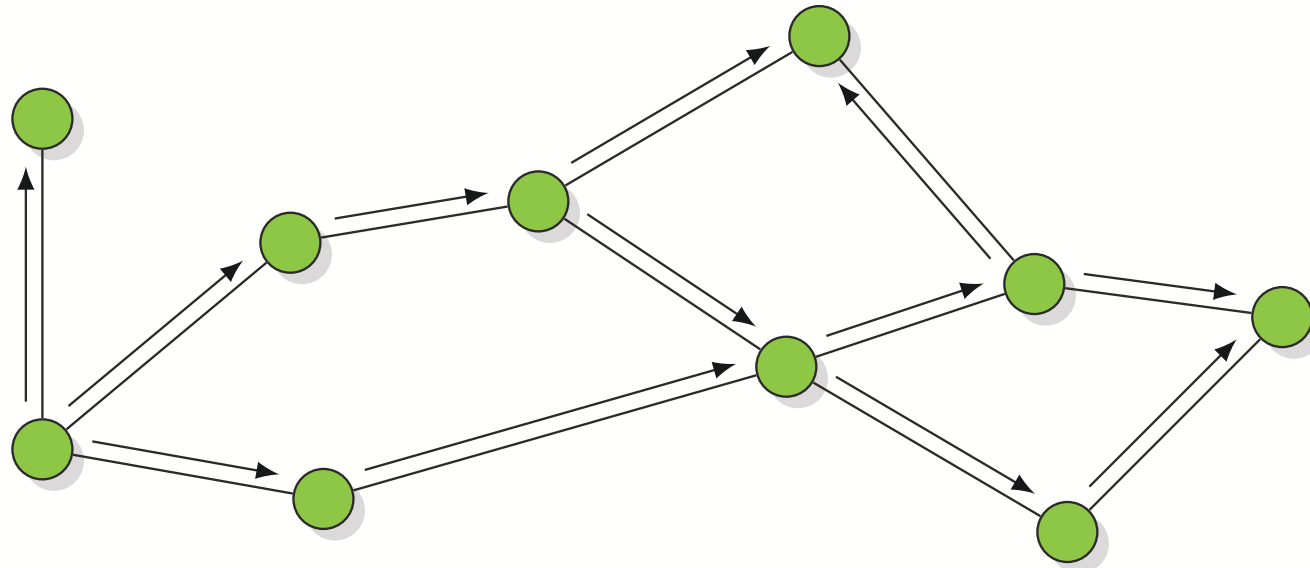| User	Balance
A	2
B	5
C	8

Distributing the Bank
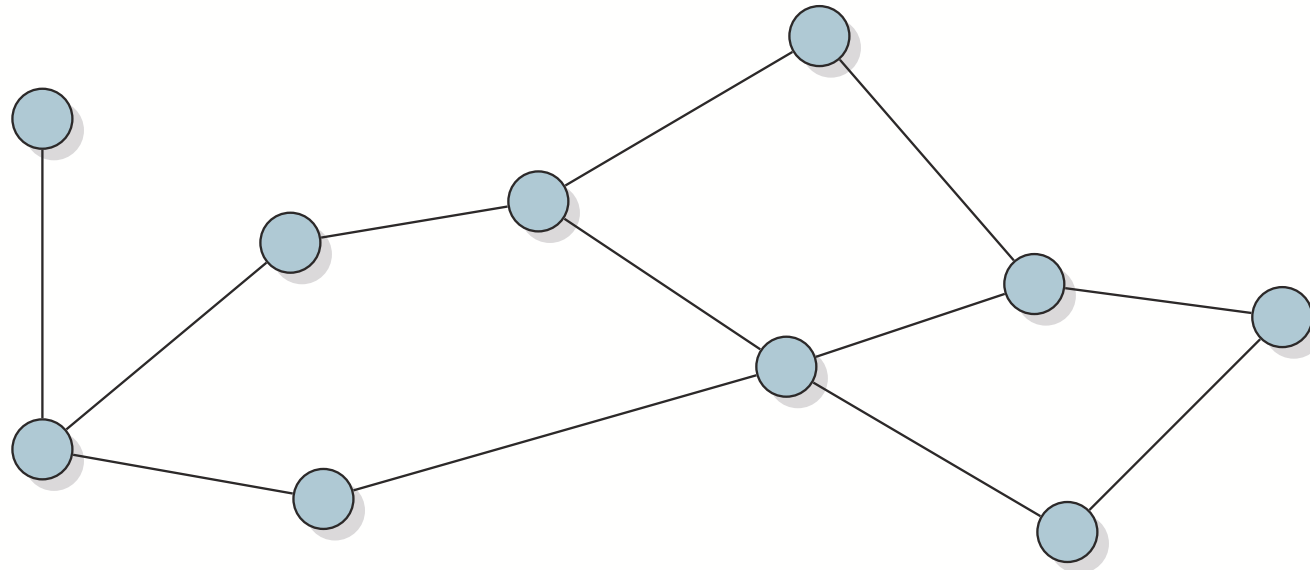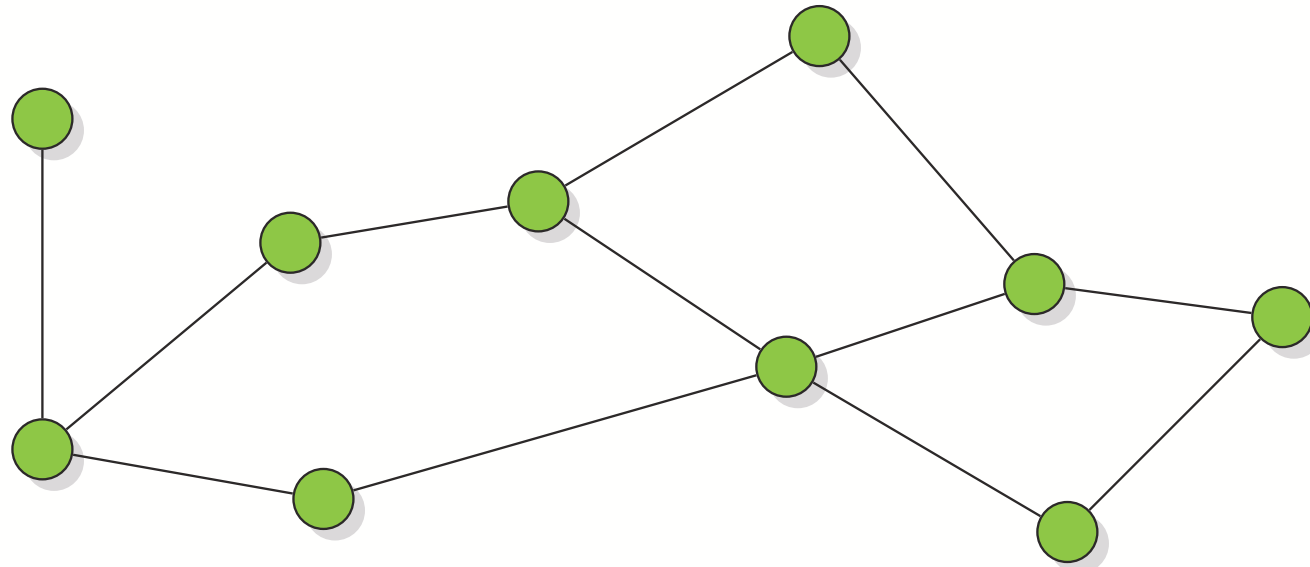
Distributing the Bank
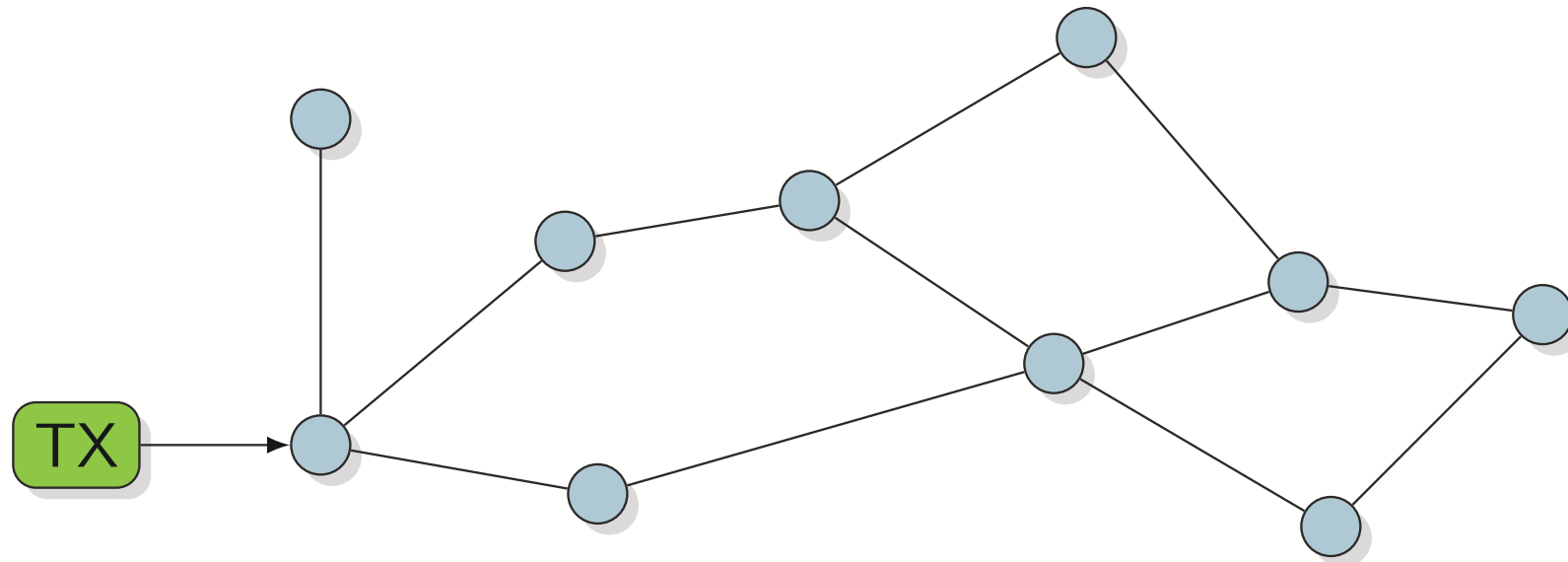
Distributing the Bank
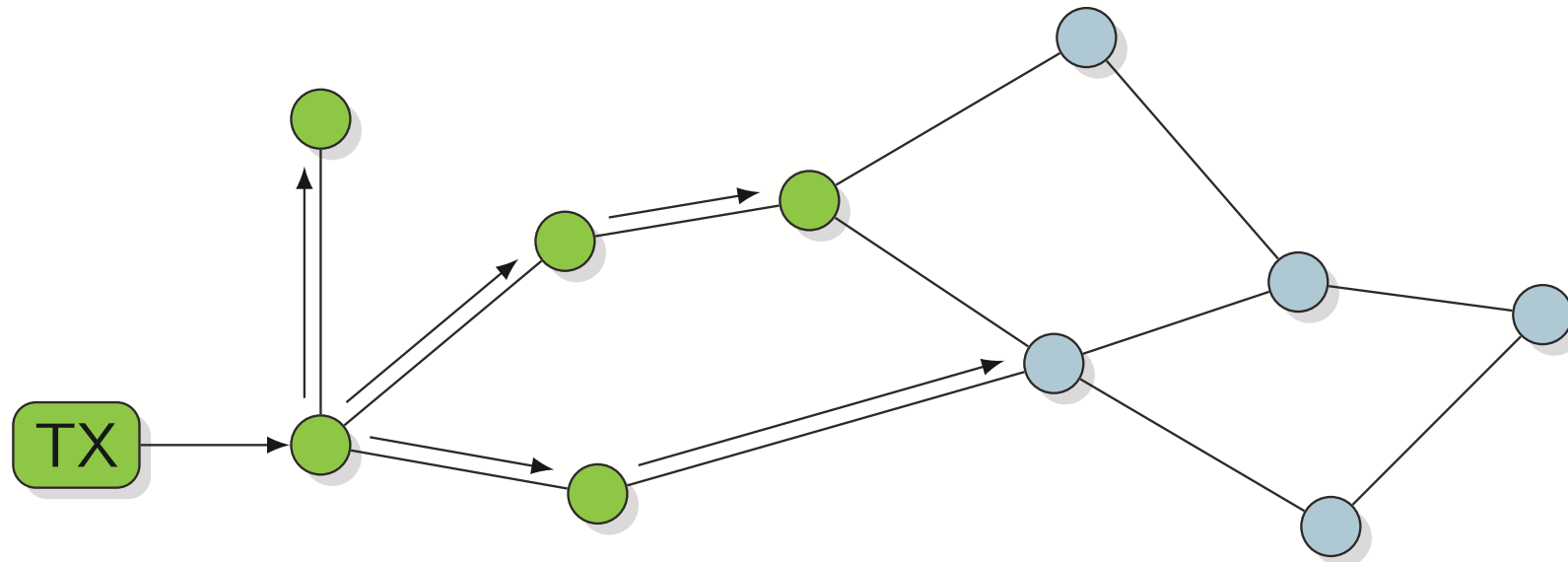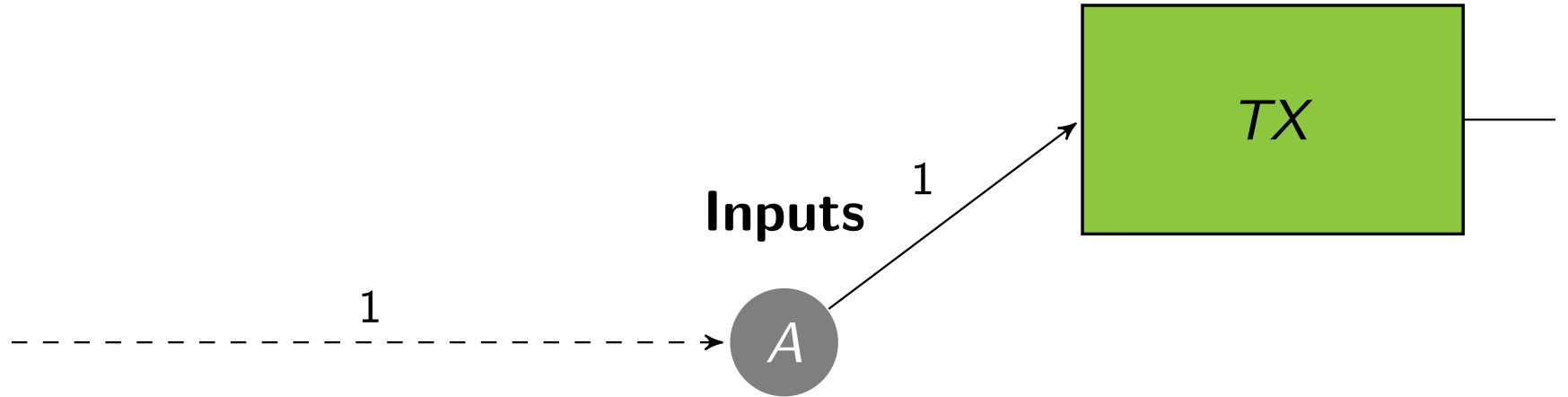
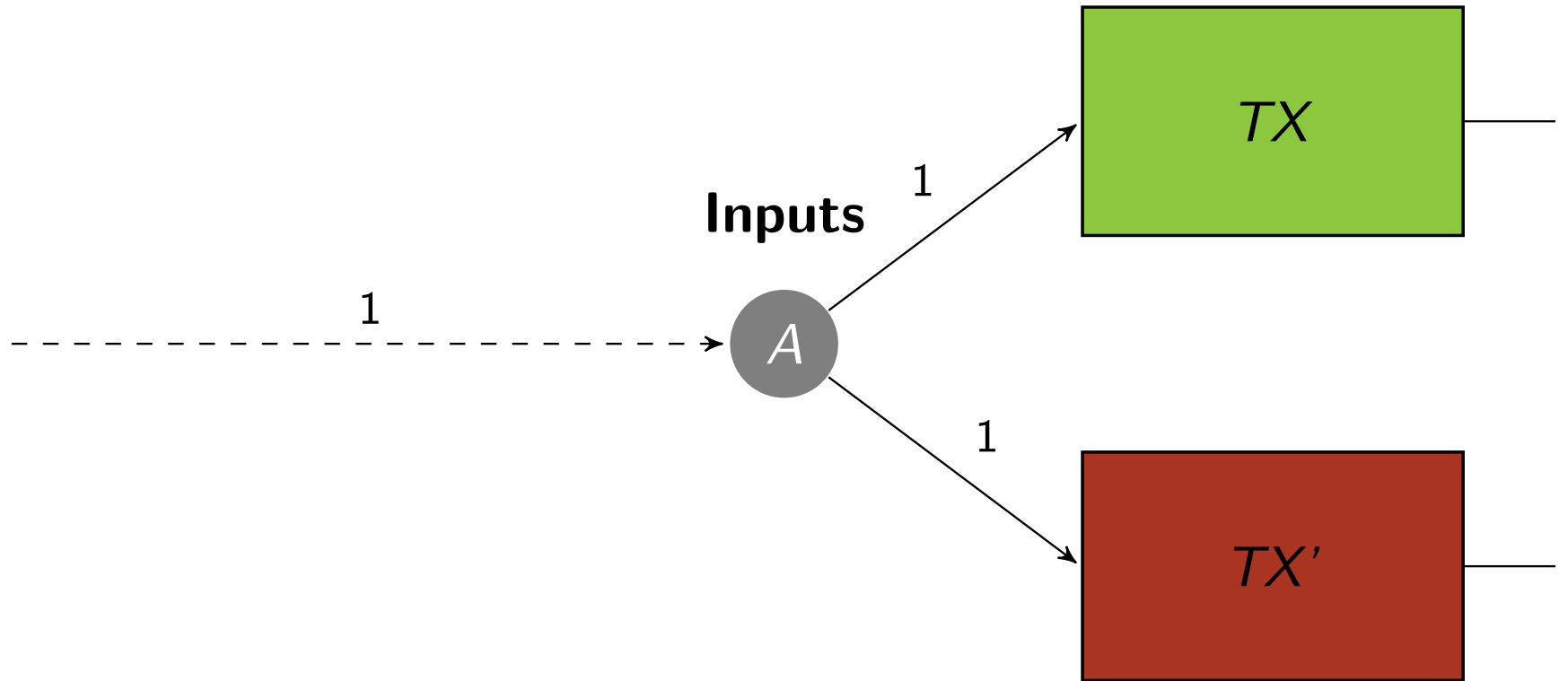# Distributing the Bank

Distributing the Bank

Let's Buy a Snack
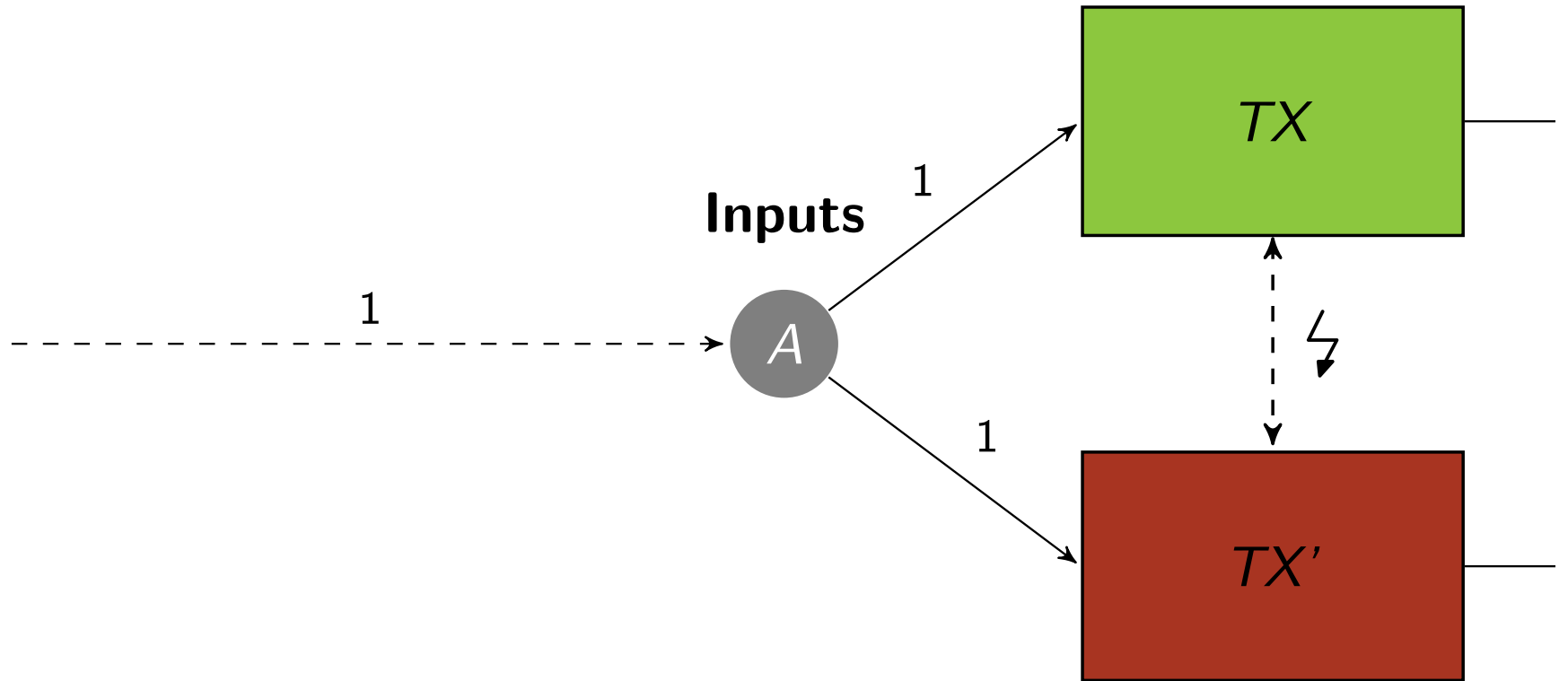
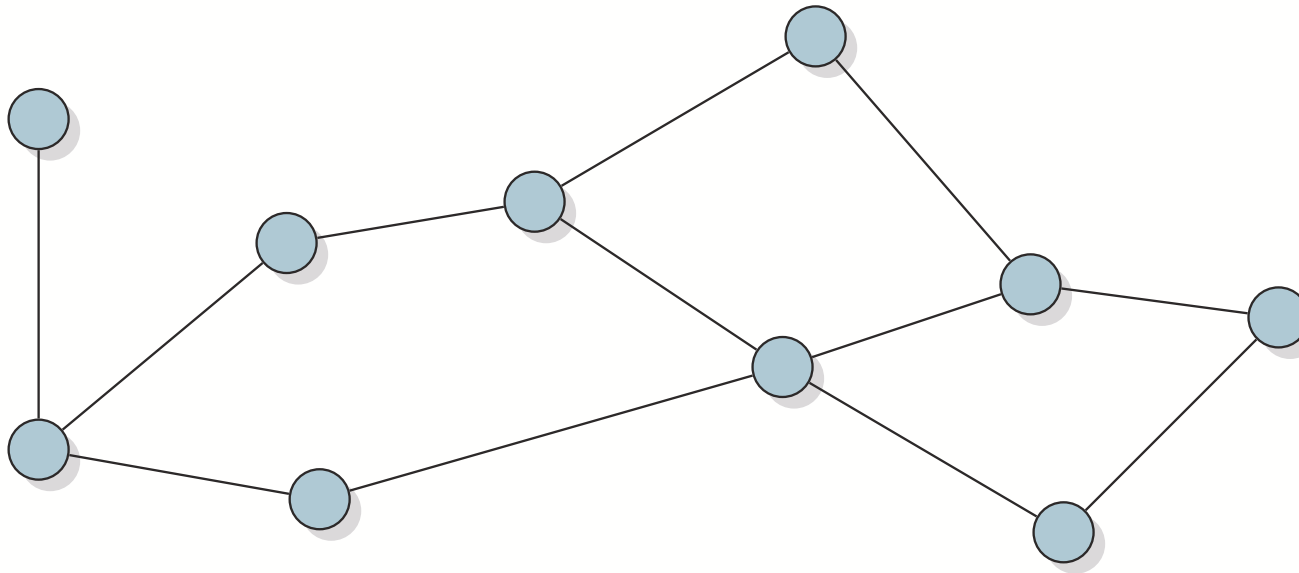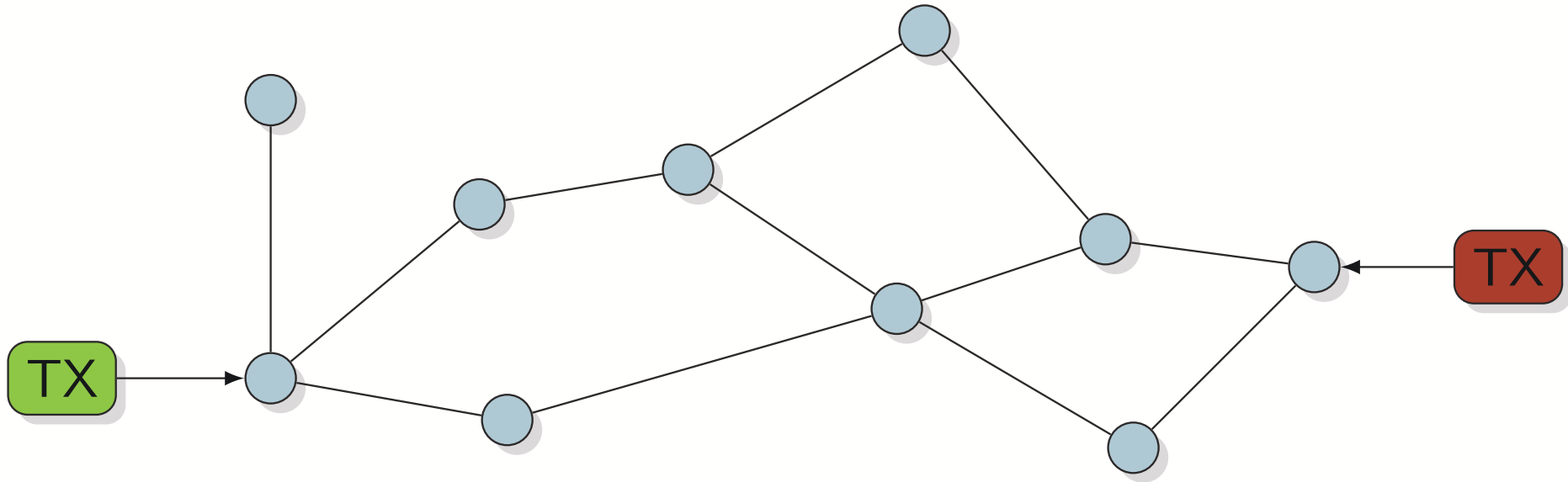[Bamert, Decker, Elsen, W, Welten, 2013]
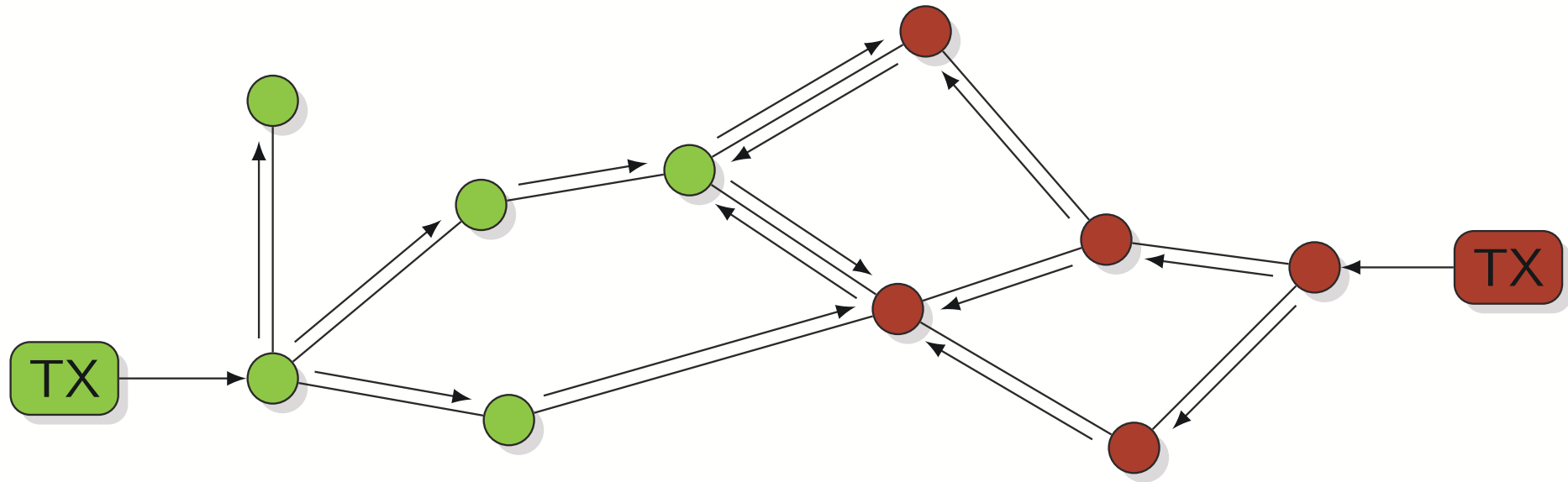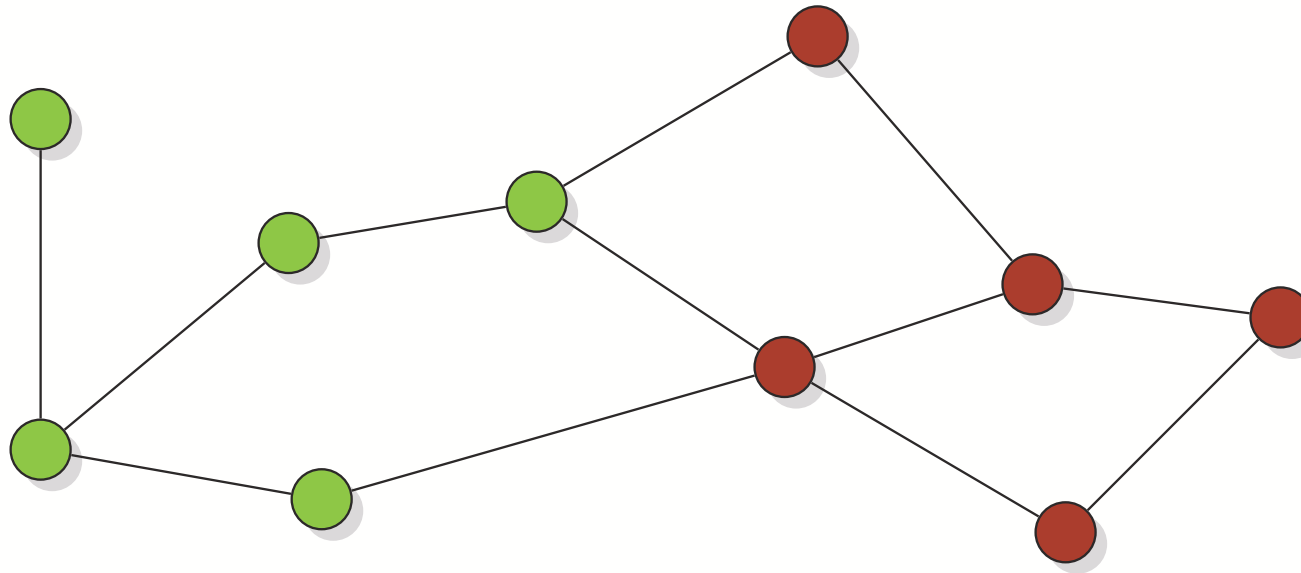
Doublespending

Doublespending
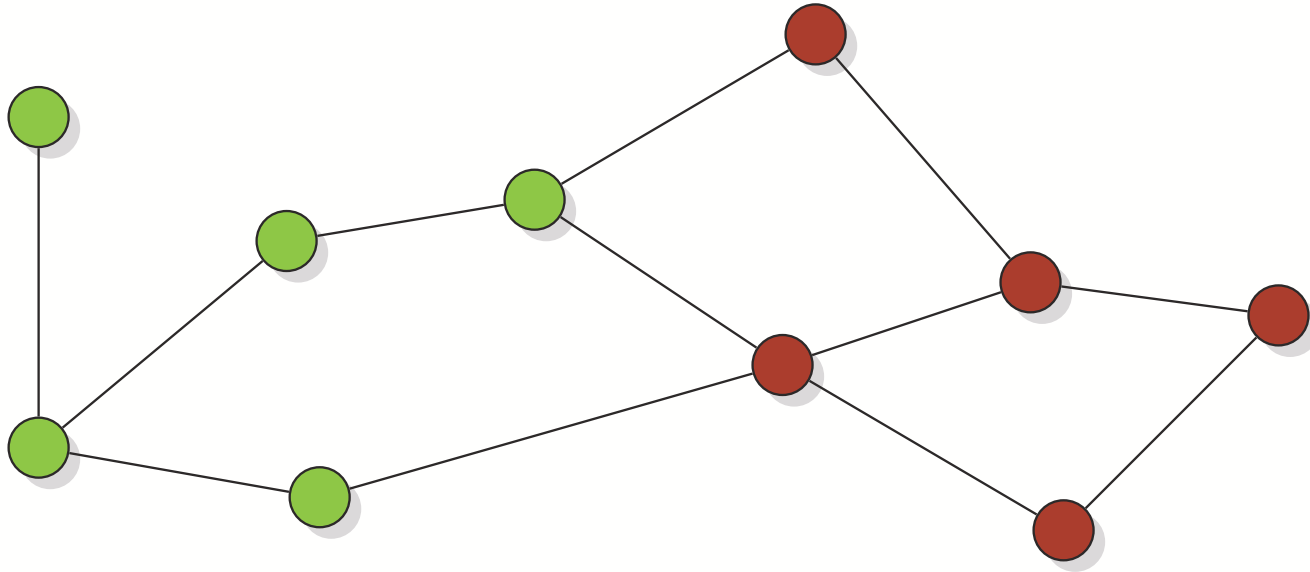
Doublespending

Transaction Conflicts

Transaction Conflicts
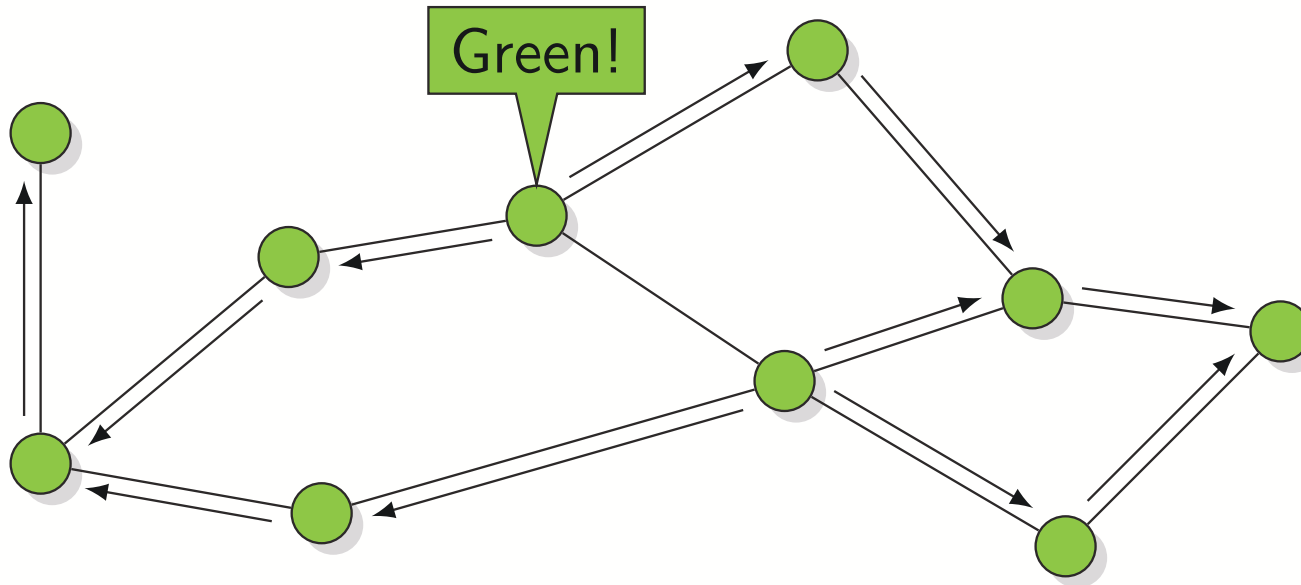
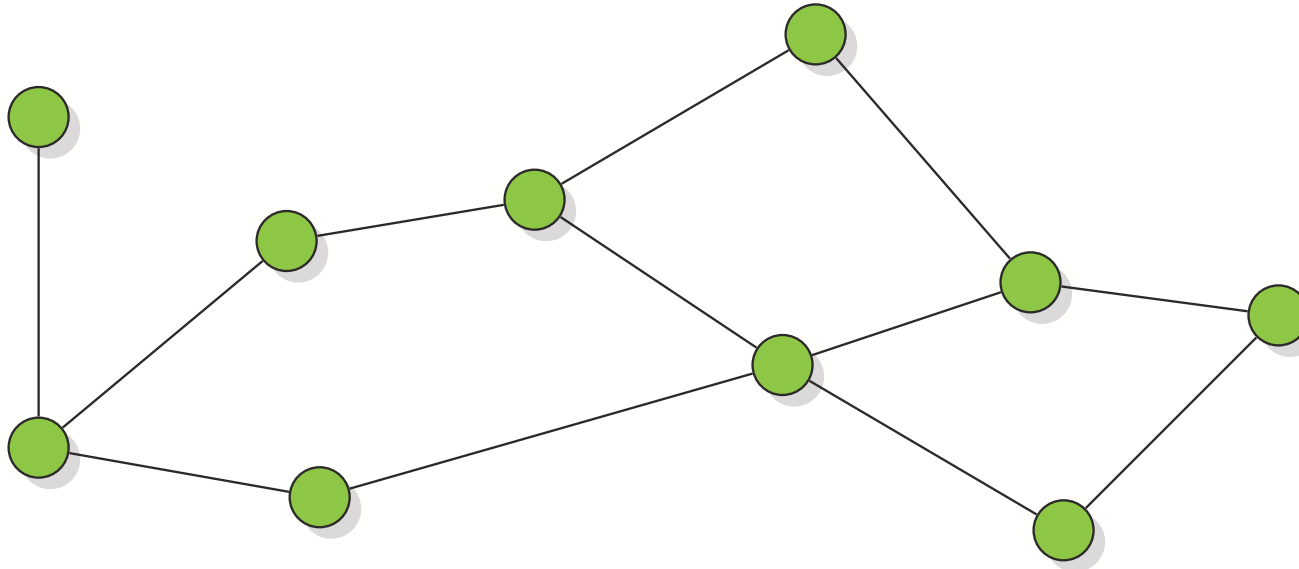# Transaction Conflicts

Transaction Conflicts

Resolving Conflicts

Resolving Conflicts

Resolving Conflicts

How to Choose a Leader?

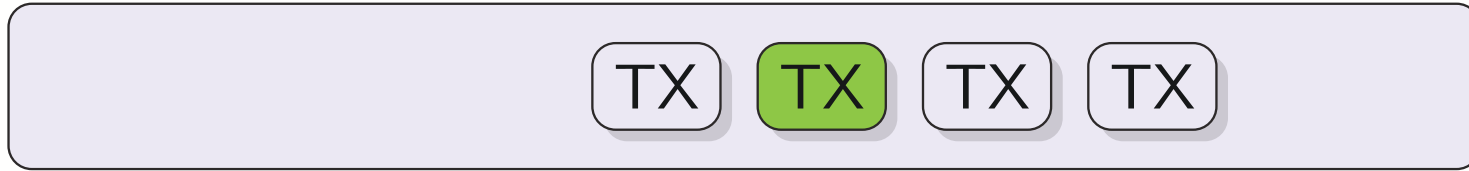# Proof-of-Work

Proof-of-Work
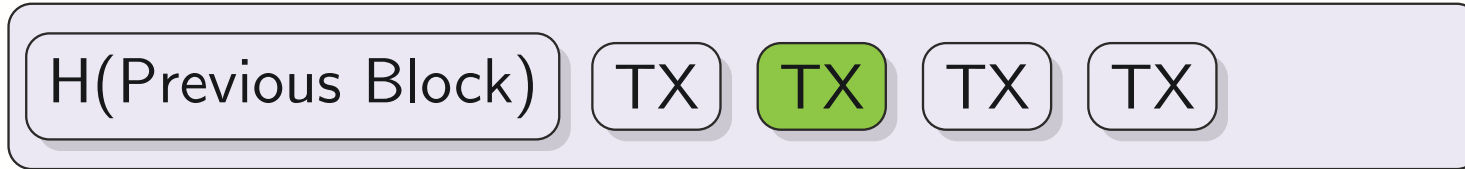
Block

TX TX TX TX

Proof-of-Work

Block

Proof-of-Work

Block
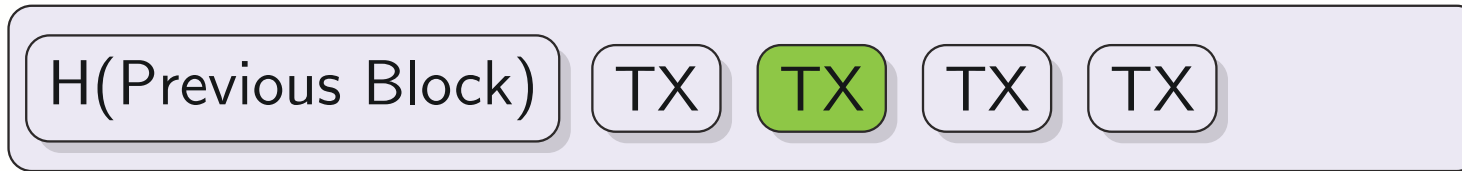
- H(Block) → fd2e2055f117bfa261b5a6c7e11df367...

Proof-of-Work

Block

H(Previous Block) TX TX TX TX Nonce
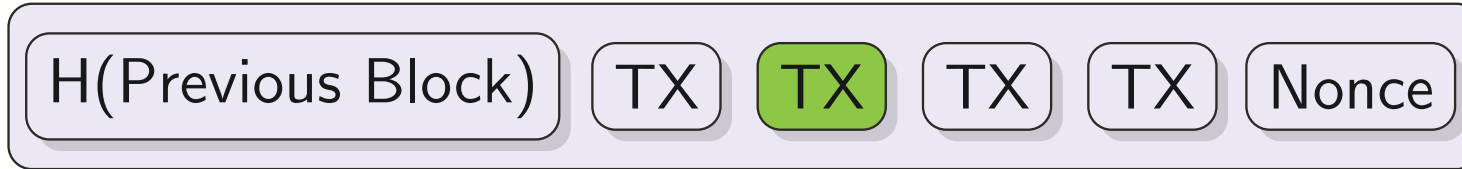
▶ H(Block|0) → 094d66aa7c844a9dbb516a41259b5877...

Proof-of-Work

Block
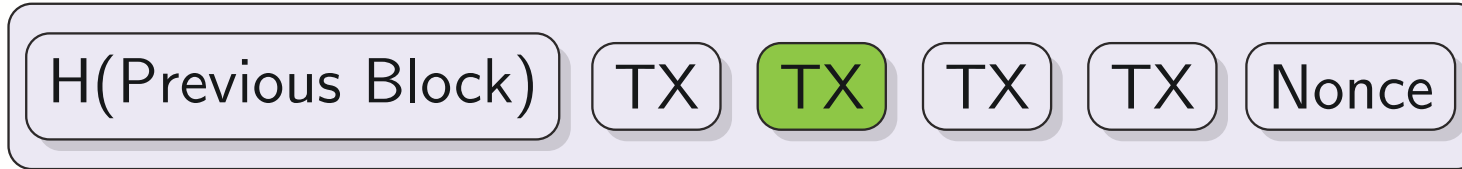
- ▶ H(Block|0) → 094d66aa7c844a9dbb516a41259b5877...
- ▶ H(Block|1) → f2496854af8bf989171587a9259f634f...

Proof-of-Work

Block

- H(Block|0) → 094d66aa7c844a9dbb516a41259b5877...
- H(Block|1) → f2496854af8bf989171587a9259f634f...
- H(Block|2) → aec87c0ca2e5eb3f23111092f1089ada...

Proof-of-Work

Block

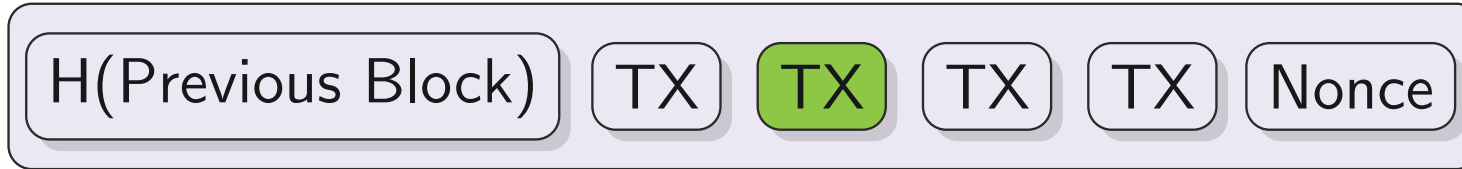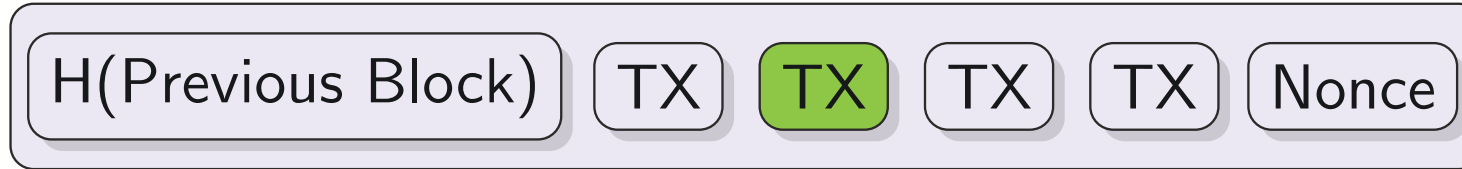| H(Previous Block) | TX | TX | TX | TX | Nonce |

- $H(\text{Block}|0) \rightarrow$ 094d66aa7c844a9dbb516a41259b5877...
- $H(\text{Block}|1) \rightarrow$ f2496854af8bf989171587a9259f634f...
- $H(\text{Block}|2) \rightarrow$ aec87c0ca2e5eb3f23111092f1089ada...
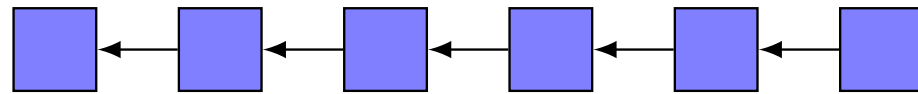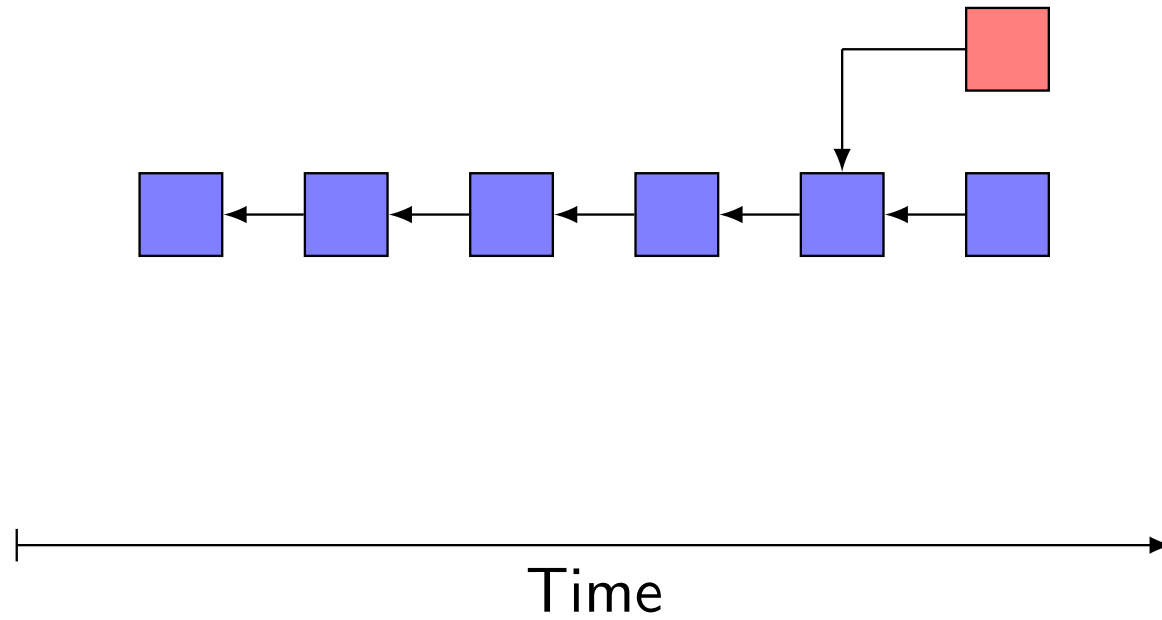- $H(\text{Block}|3) \rightarrow$ 777f75b2a8ecfdc8026c236fc1d2ffa0...

$\vdots$

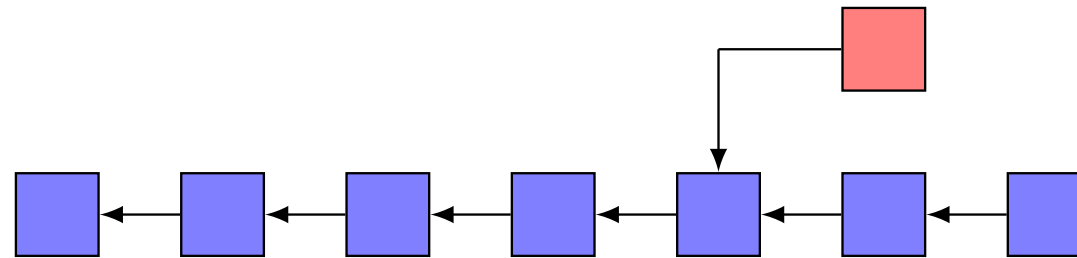- $H(\text{Block}|961127) \rightarrow$ 0000014823419622d4c133672a7d657e...
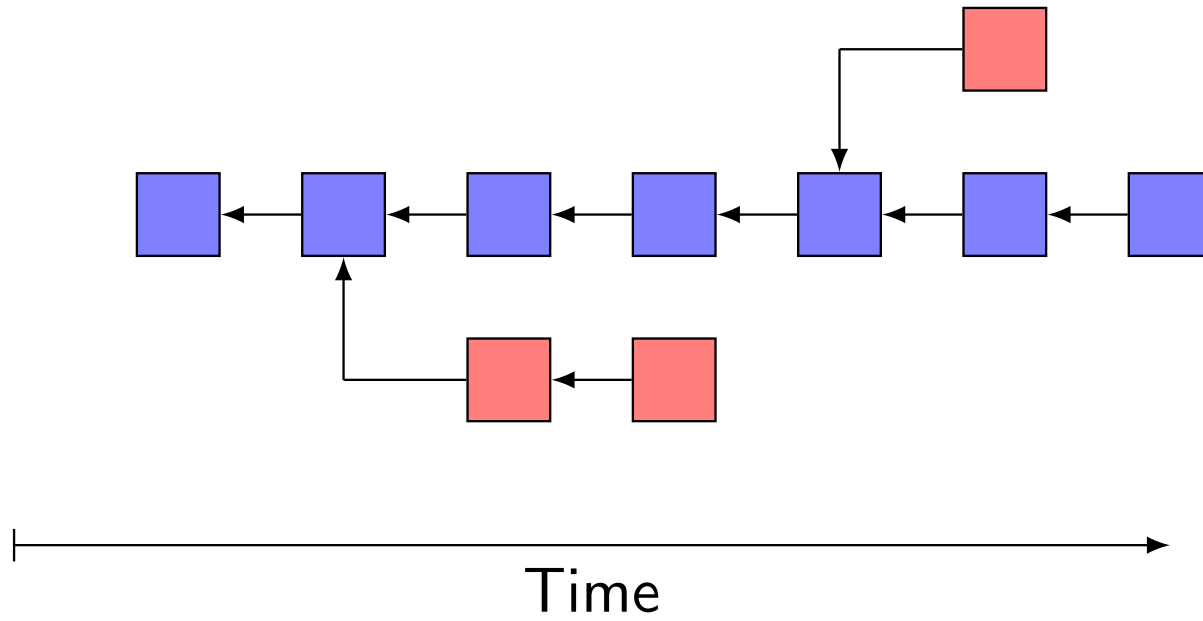
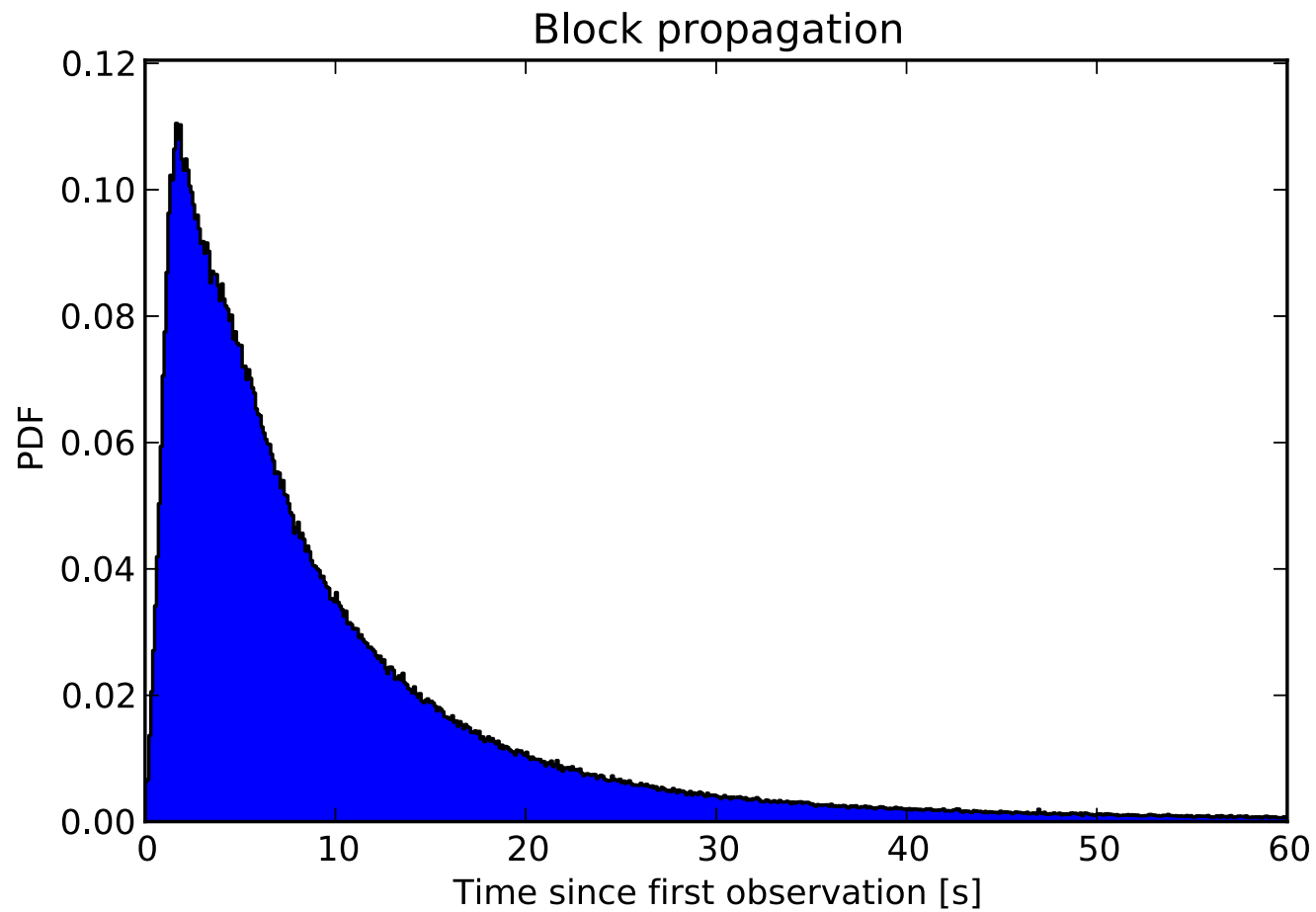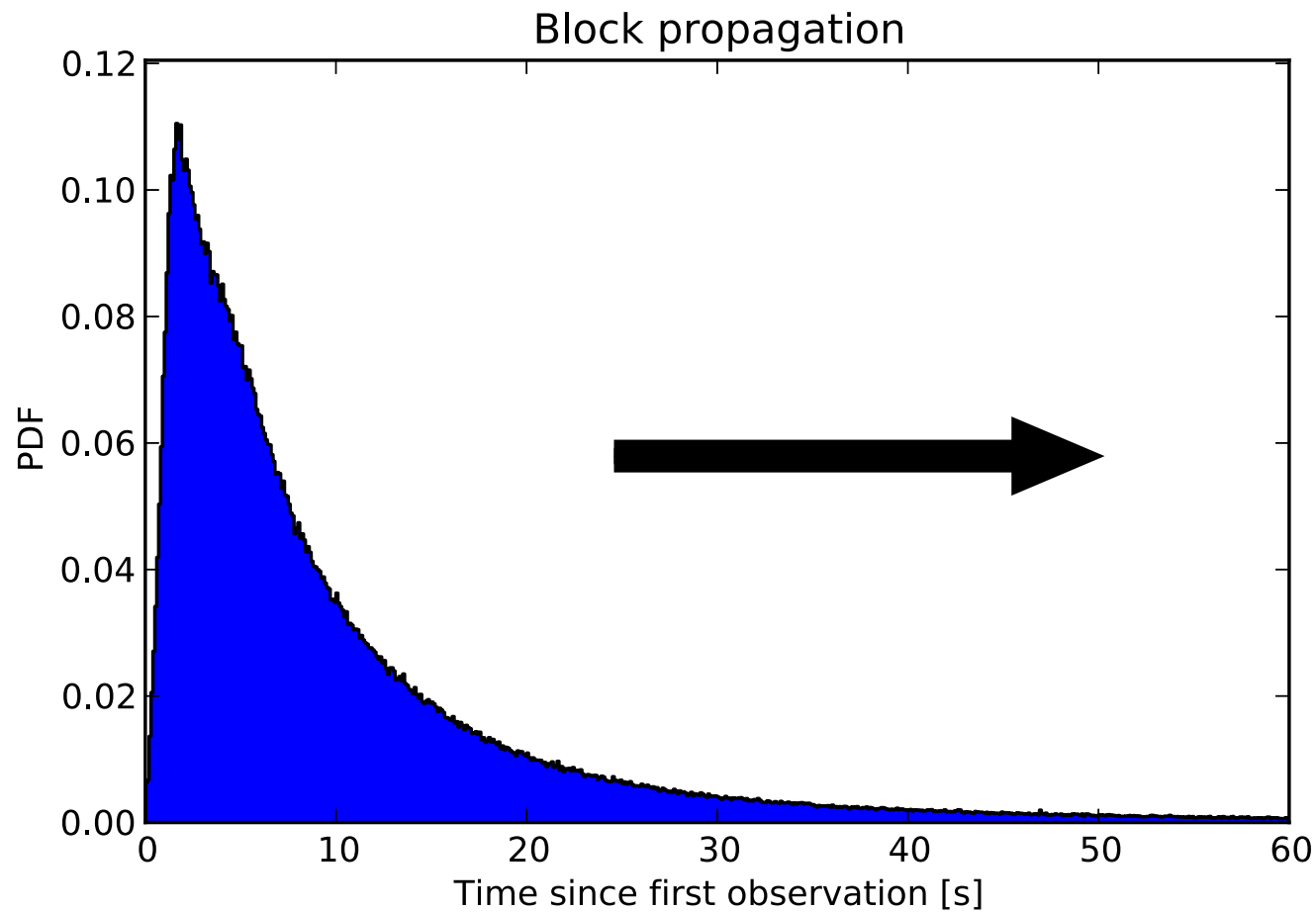# The Blockchain

The Blockchain

Time

Is Bitcoin stable?

The Blockchain

Time

The Blockchain

Time

Propagation Speed

Block propagation
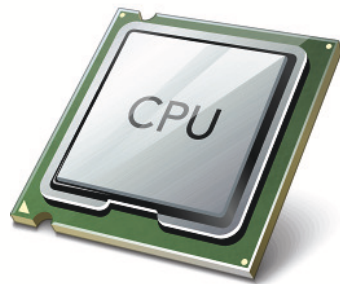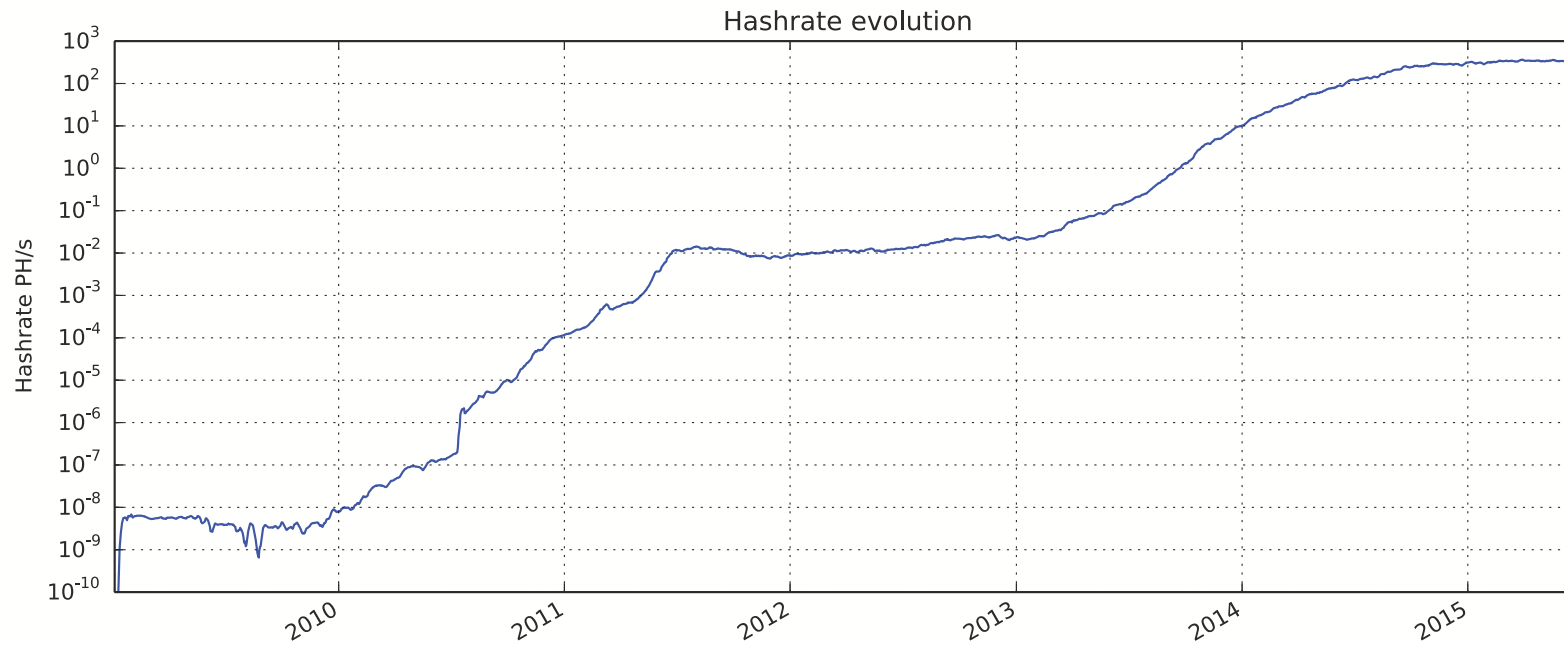
[Decker, W, 2013]

Propagation Speed

Block propagation
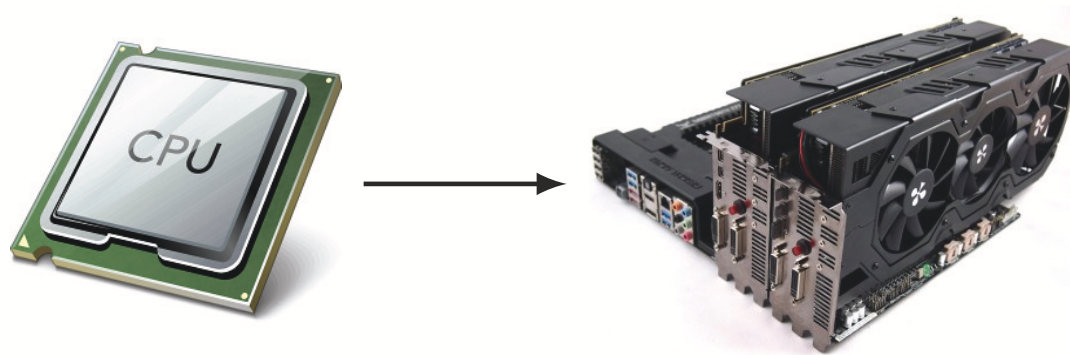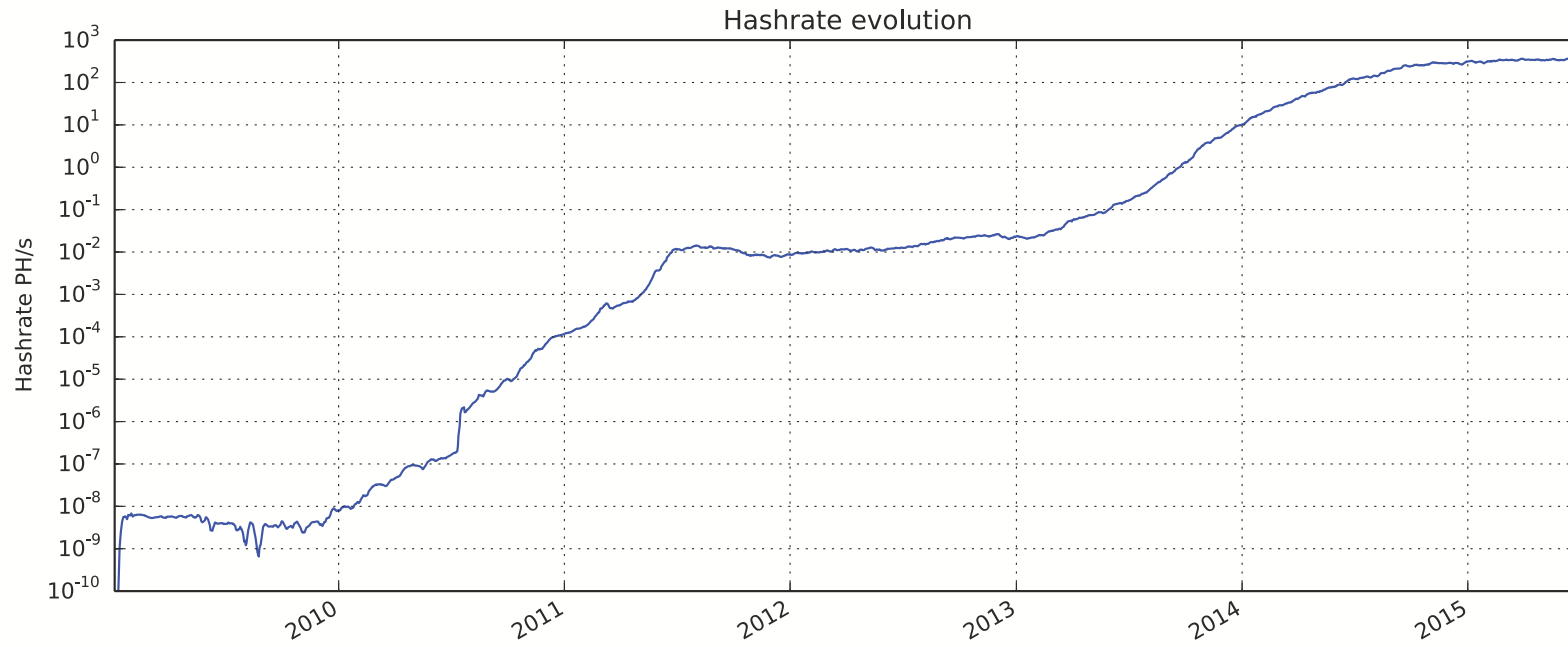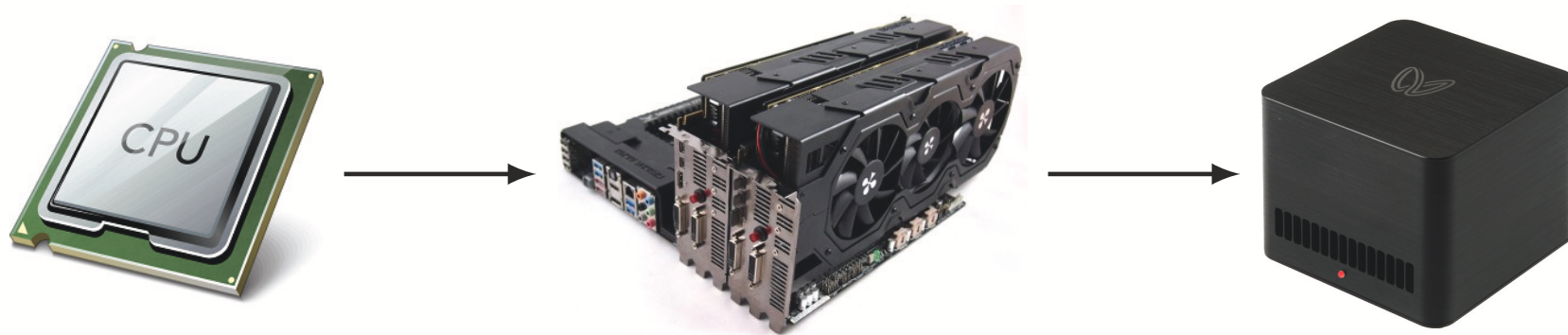
[Decker, W, 2013]

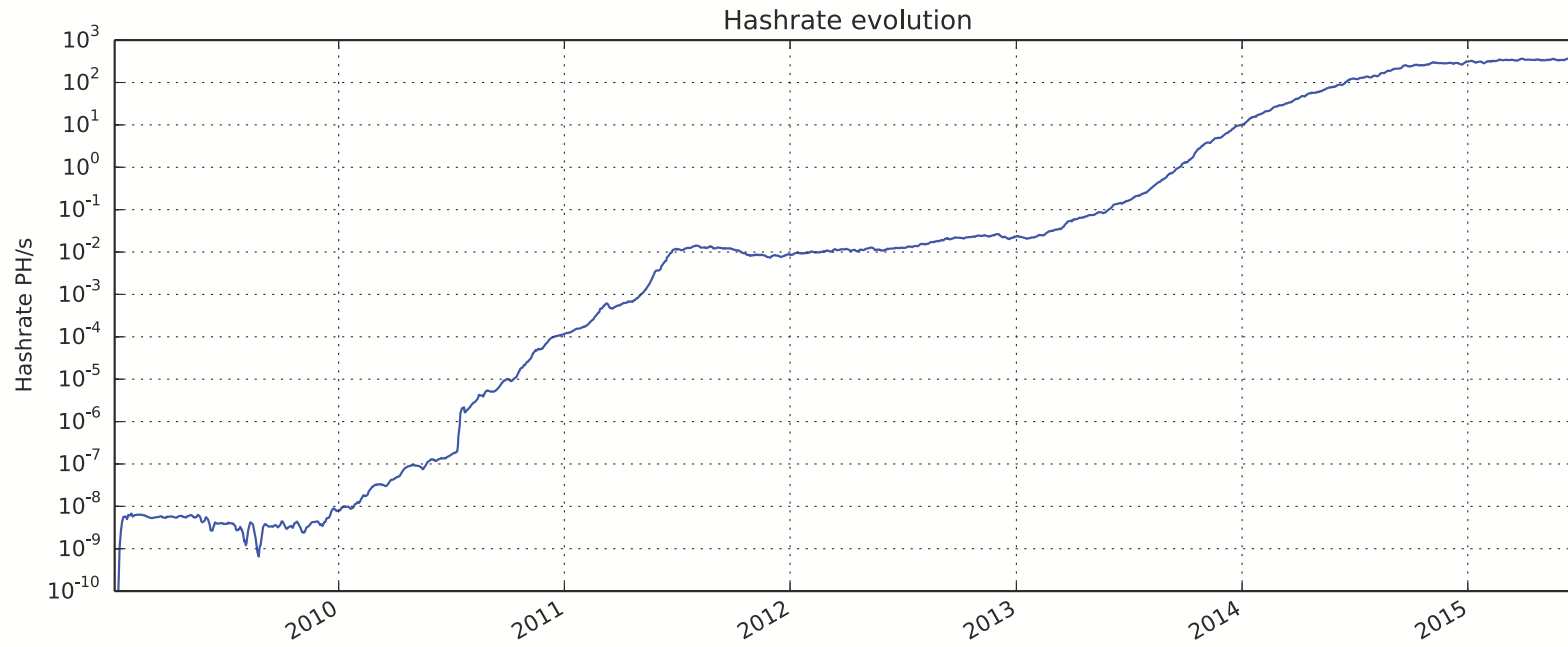# Blockchain Forks
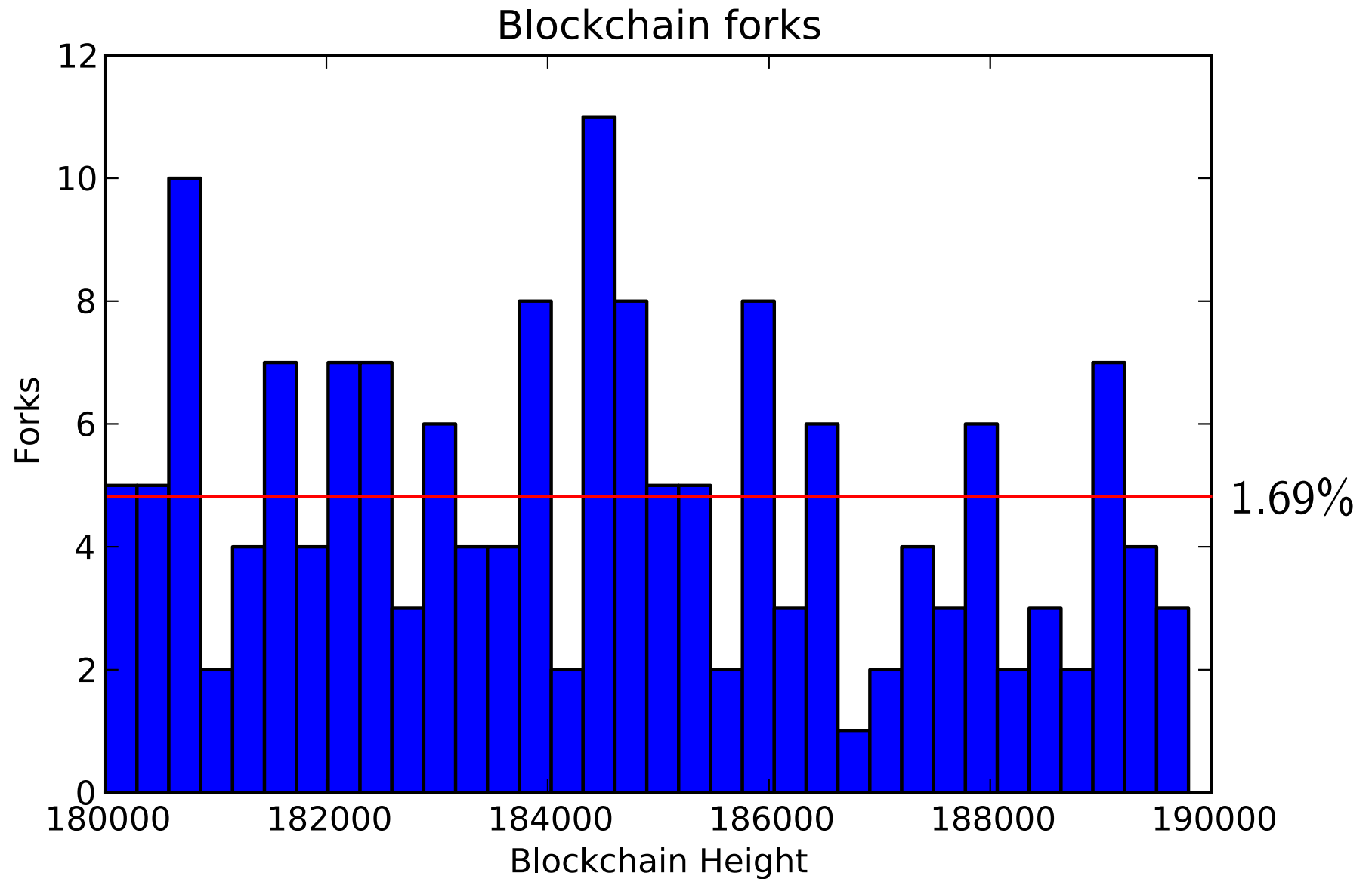
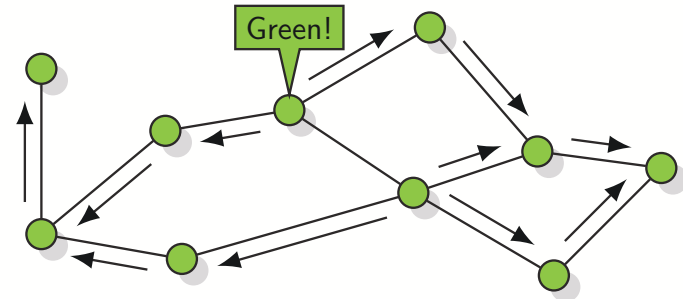[Decker, W, 2013]

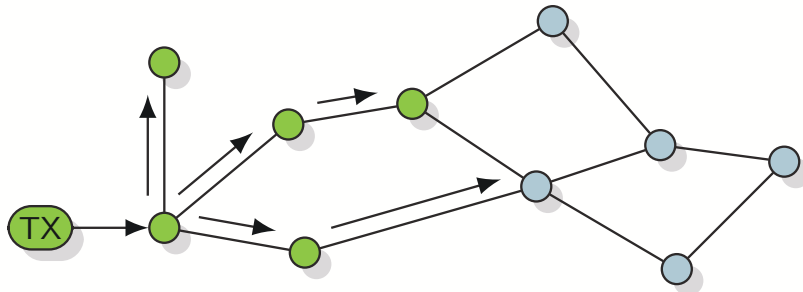# Aside: Mining Evolution

Aside: Mining Evolution

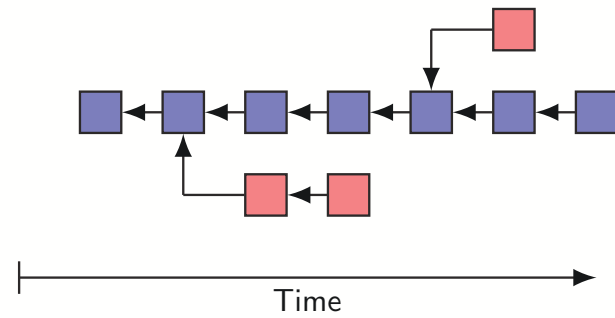# Aside: Mining Evolution

Hashrate evolution

500 MW

Summary
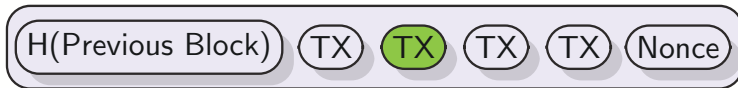
Stories

How to Lose $500M

Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks.

The MtGox Incident

▶ July 2010: First trade on MtGox

▶ May 2011: Transaction malleability identified as low priority issue

▶ February 7, 2014: MtGox halts withdrawals

▶ February 10, 2014: MtGox announces loss of 850,000 bitcoins (620 millio USD) and cites transaction malleability as root cause

▶ February 28, 2014: MtGox files for bankruptcy

▶ March 7 2014: MtGox finds 200,000 bitcoins

▶ August 2015: MtGox CEO is arrested

Signatures

61 af bb 4d e9 f8 b8 74 86 1e

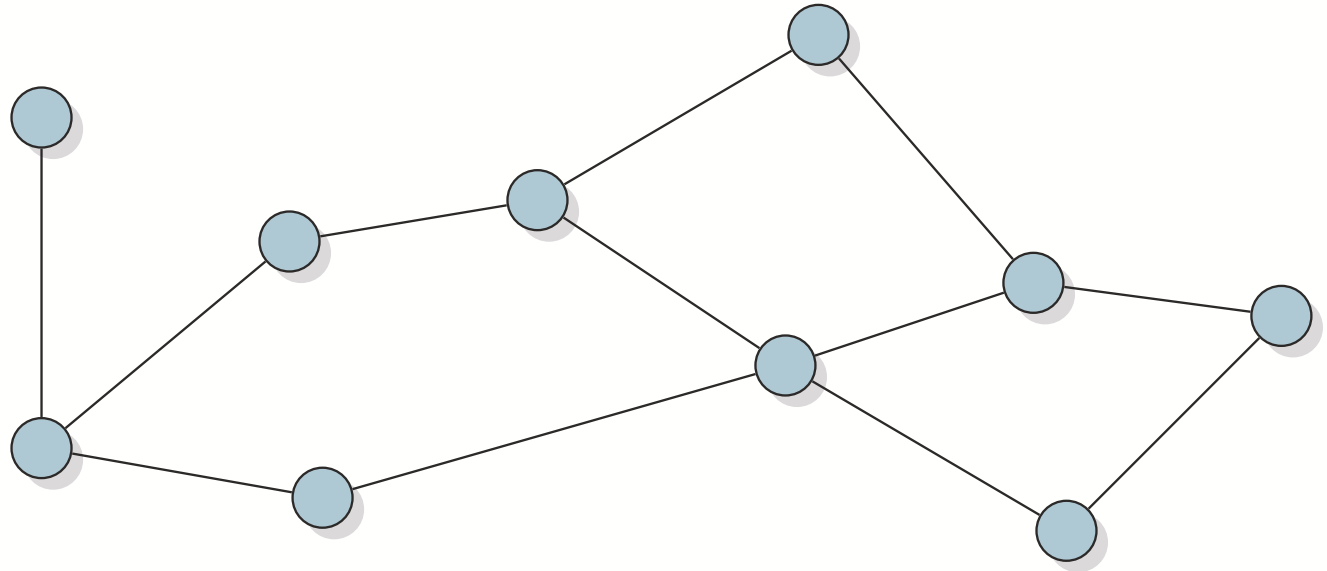# Signatures

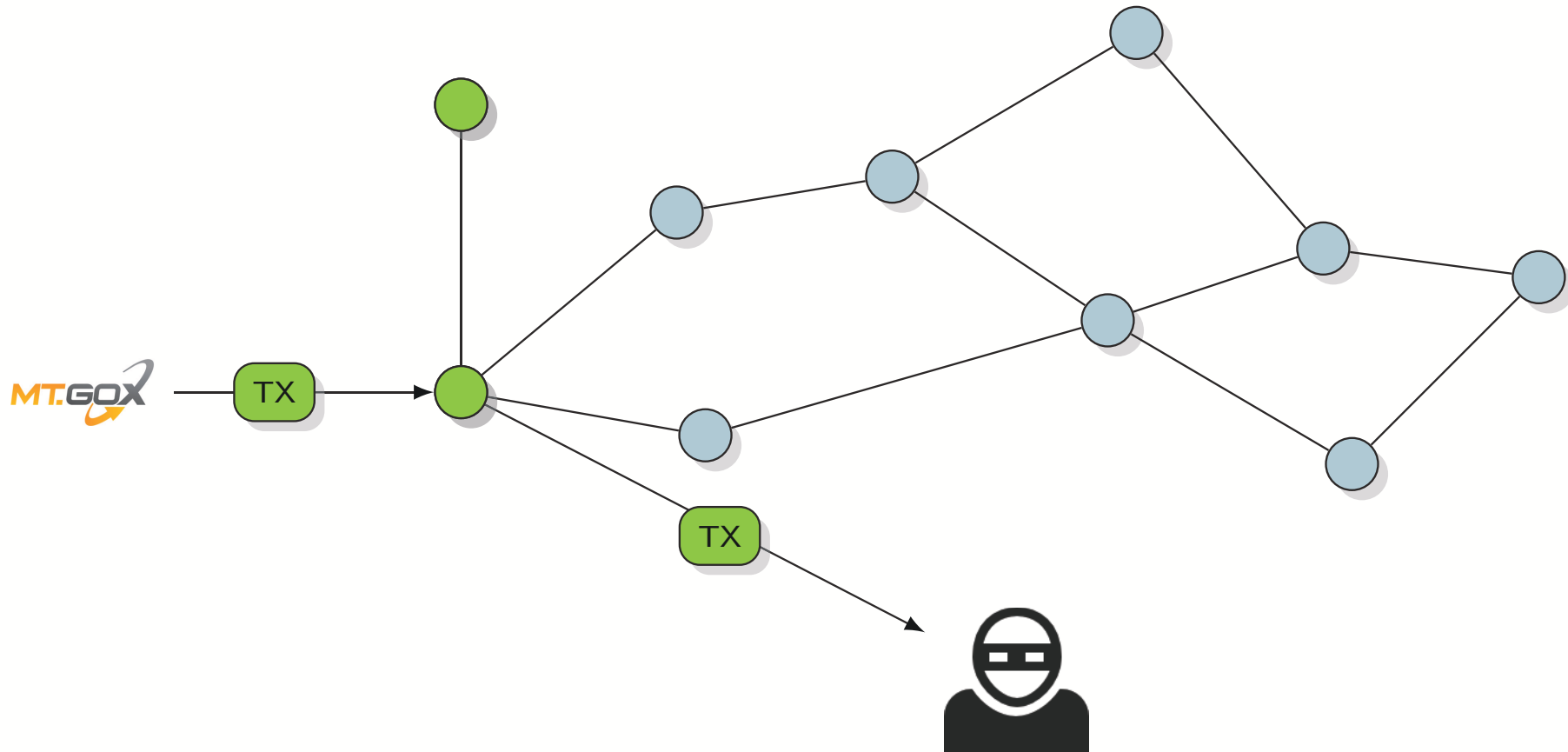**00 00 61 af bb 4d e9 f8 b8 74 86 1e**

There are multiple ways to serialize a signature:

- Multiple push operations (1 byte, 2 byte, 4 byte)
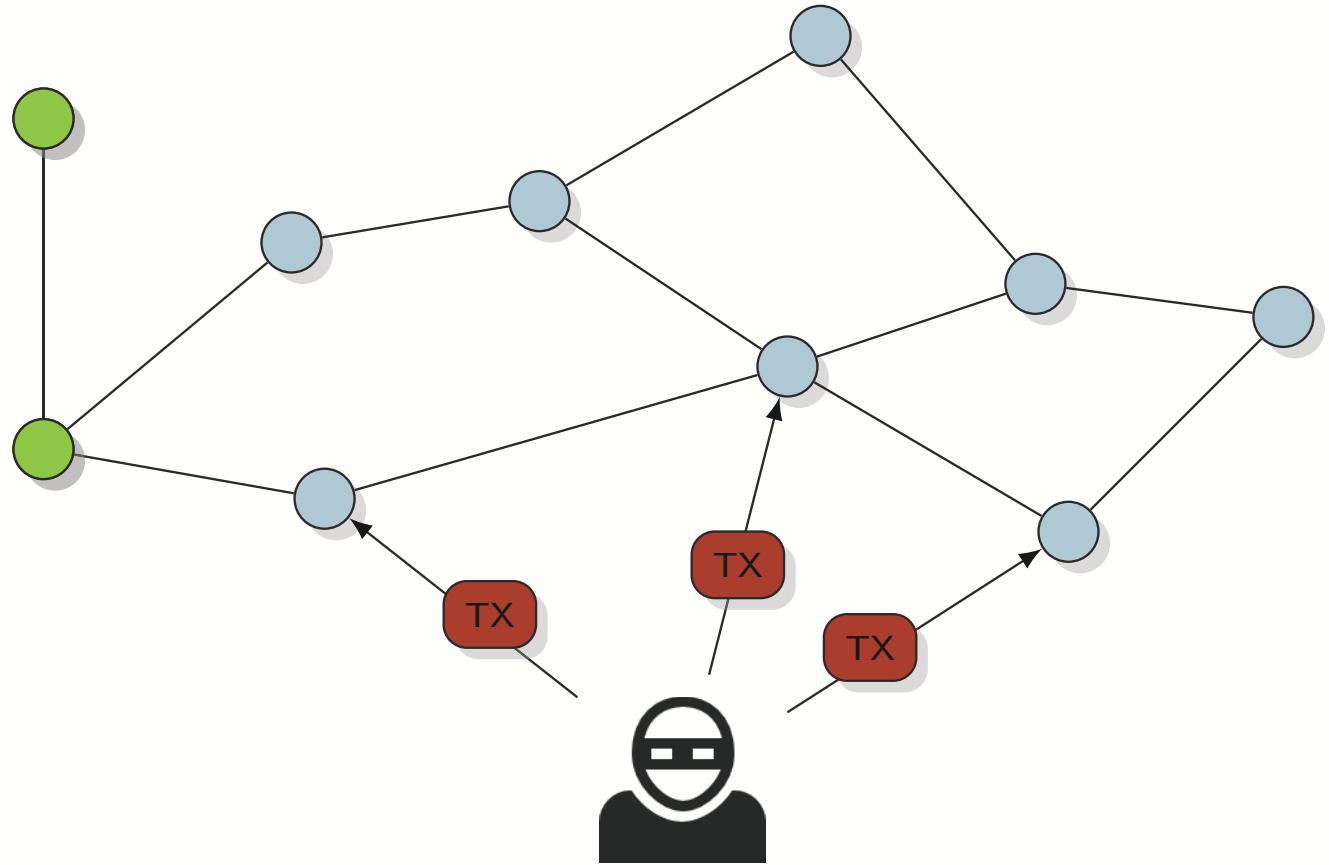- Non-canonical DER encodings
- Padding
- ...

Transaction Malleability Attack

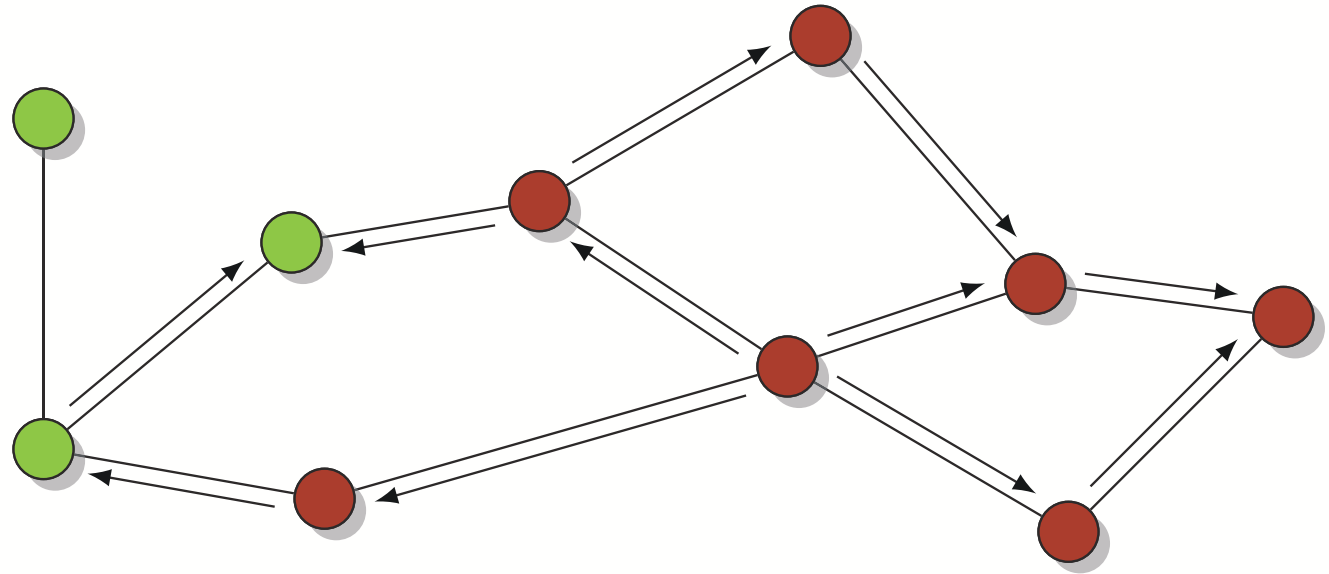# Transaction Malleability Attack

Transaction Malleability Attack

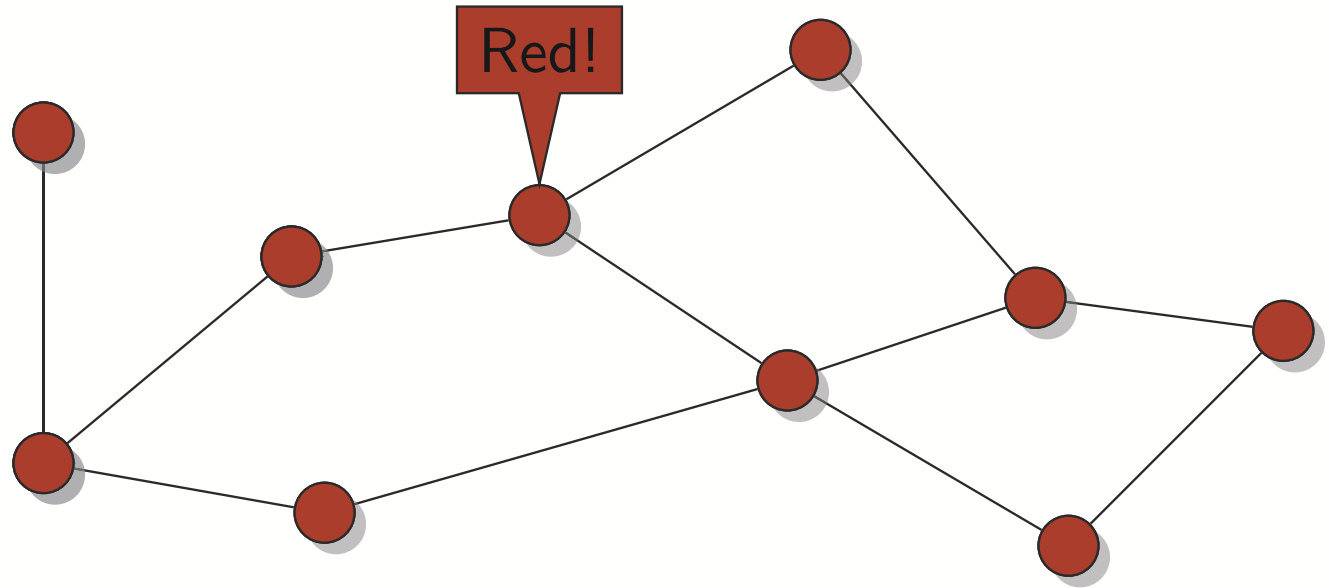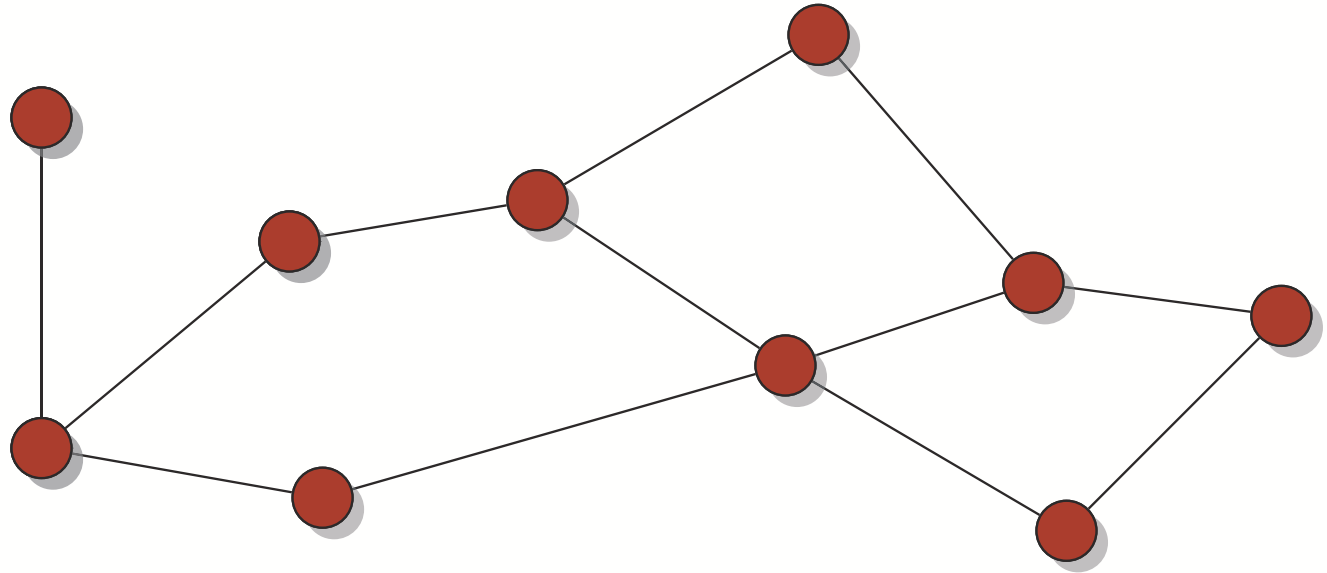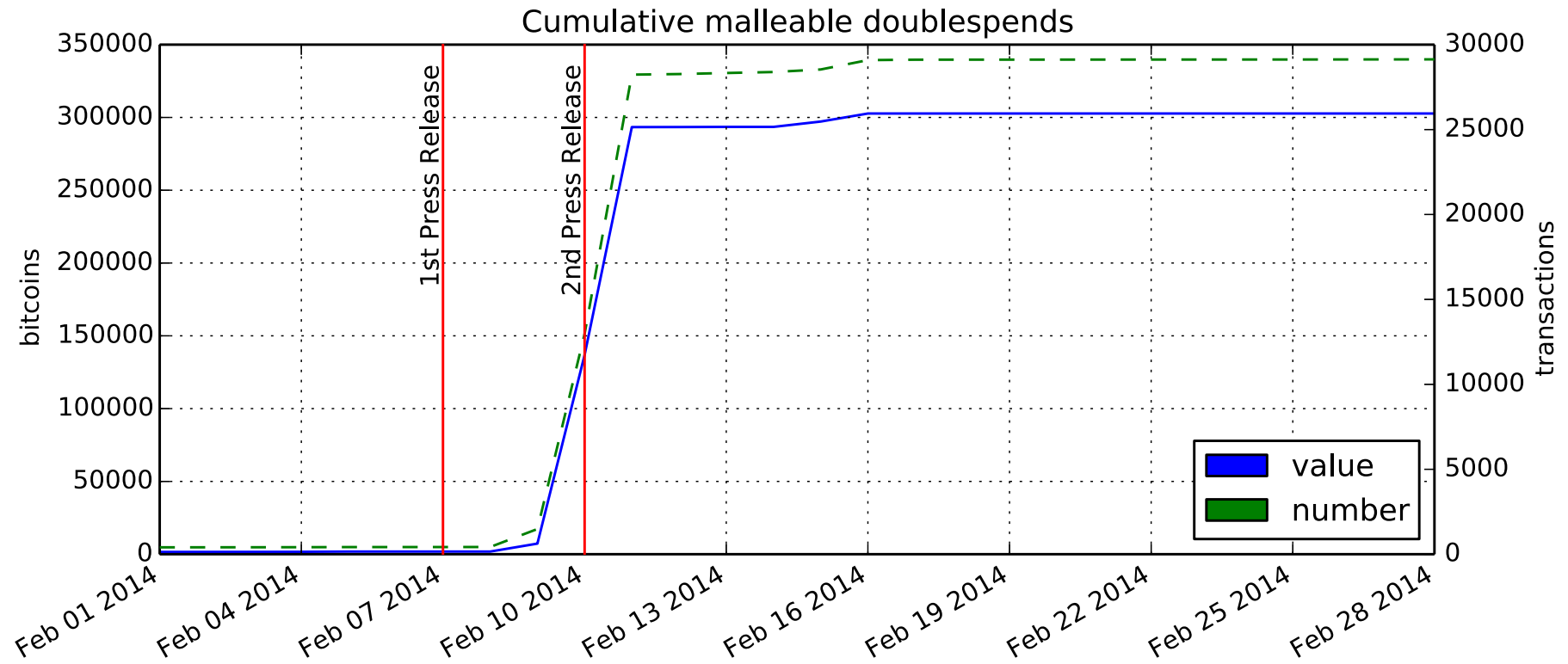# Transaction Malleability Attack

Transaction Malleability Attack

Transaction Malleability Attack

Incident Timeline

Cumulative malleable doublespends

[Decker, W, 2014]

Incident Timeline

Cumulative malleable doublespends
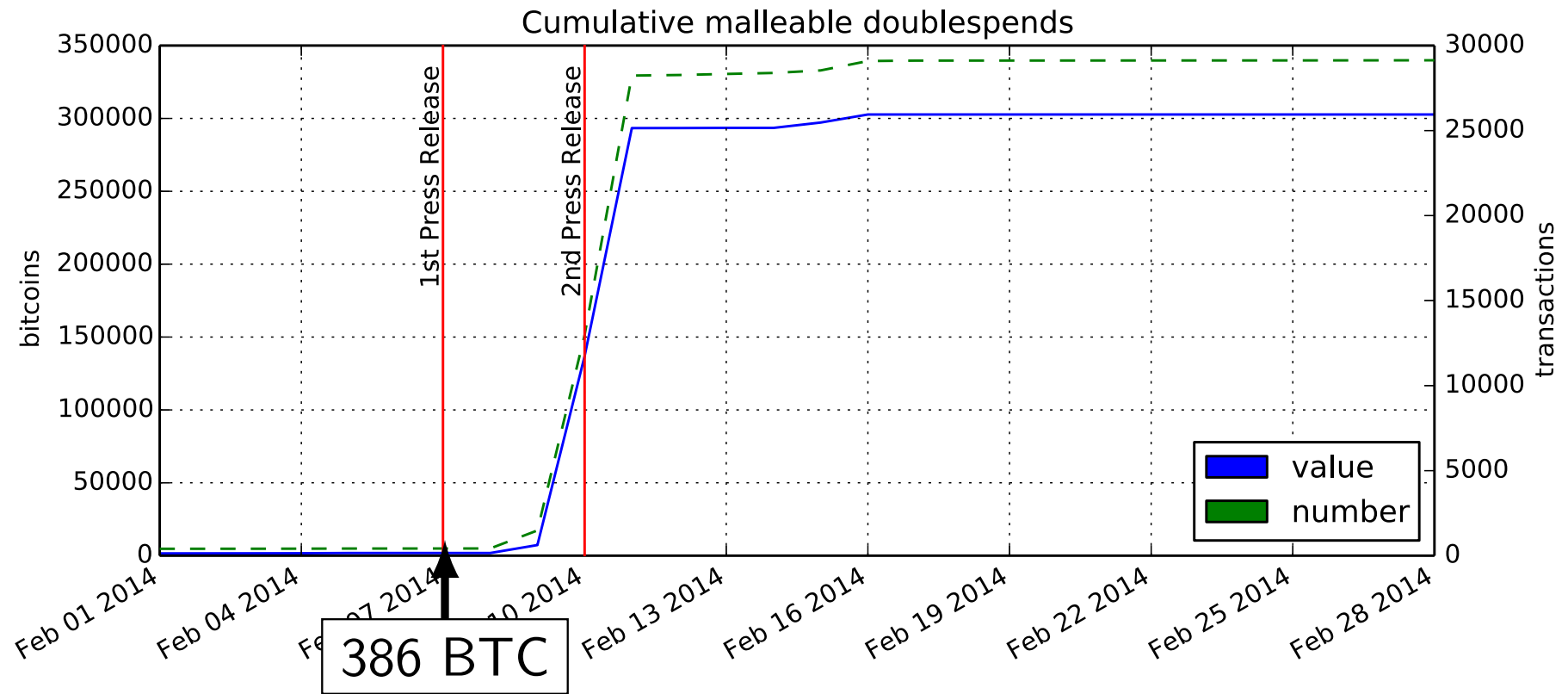
[Decker, W, 2014]

Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss

By Carter Dougherty and Grace Huang | Feb 28, 2014 8:59 PM GMT+0100 | **95 Comments** ✉ **Email** 🖶 **Print**

Mt. Gox, once the world's largest Bitcoin exchange, filed for bankruptcy in **Japan** saying about $480 million in Bitcoins belonging to its customers and the firm were missing.

"The company believes there is a high possibility that the Bitcoins were stolen," Mt. Gox said in a statement.

The filing follows three weeks of speculation about the fate of the Tokyo-based exchange, which suspended withdrawals on Feb. 7. Since Bitcoins exist as bits of software, they can be stolen if a hacker gains access to the computers and servers used to run online exchanges, where the virtual currency can be traded

for dollars, euros and other currencies

Mark Karpeles, CEO of Mt. Gox, the world's largest bitcoin exchange, bows for an... **Read More**
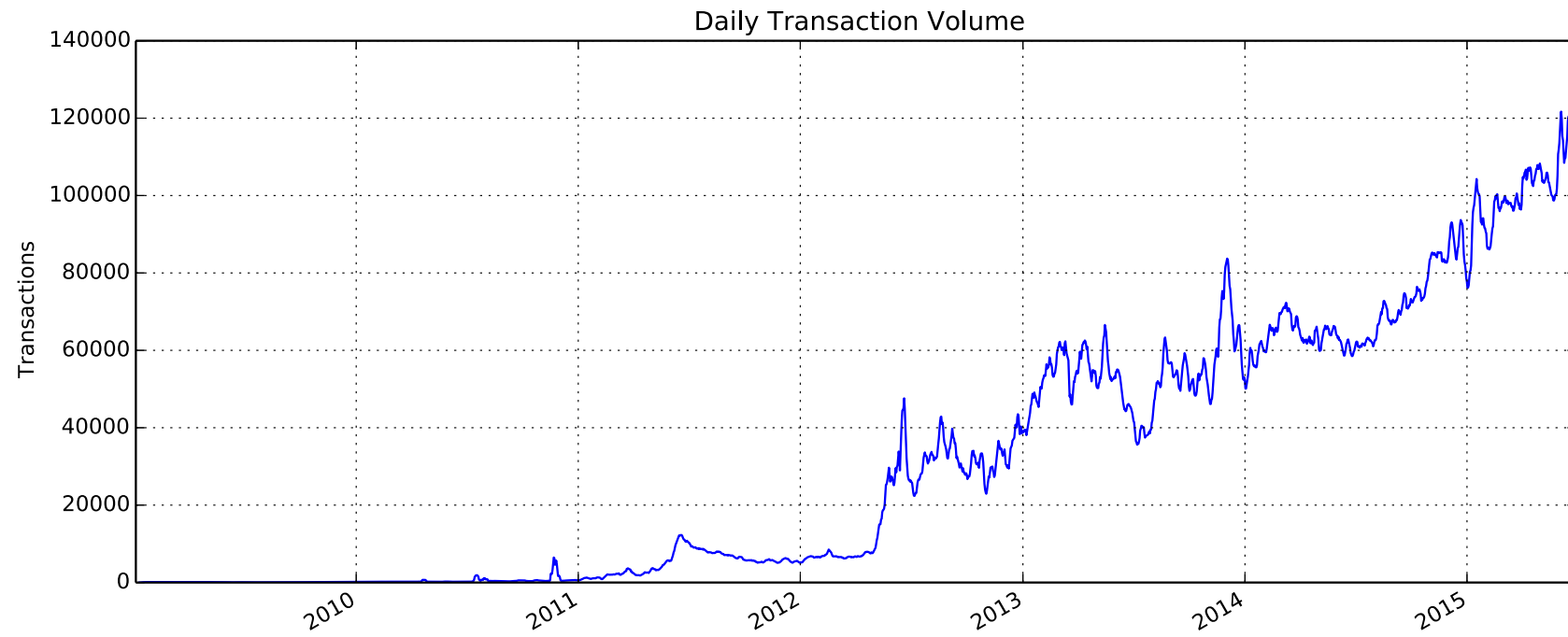
Is Bitcoin Secure?

Securing Your Bitcoins

[Bamert, Decker, W, 2013]

Does Bitcoin Scale?

The Bitcoin Ecosystem is Growing

Daily Transaction Volume

Scalability Limits

- Disk space: < 500 transactions per second

Scalability Limits

- Disk space: < 500 transactions per second
- Processing power: < 200 transactions per second

Scalability Limits

- Disk space: < 500 transactions per second
- Processing power: < 200 transactions per second
- Network bandwidth: < 100 transactions per second

Scalability Limits

- Disk space: < 500 transactions per second

- Processing power: < 200 transactions per second

- Network bandwidth: < 100 transactions per second

- Artificial 1MB limit: < 3 transactions per second

Scalability Limits

- Disk space: < 500 transactions per second

- Processing power: < 200 transactions per second

- Network bandwidth: < 100 transactions per second

- Artificial 1MB limit: < 3 transactions per second

Today:

- Bitcoin: 1 transaction per second

- Credit Cards: $> 10,000$ transactions per second

Payment Network
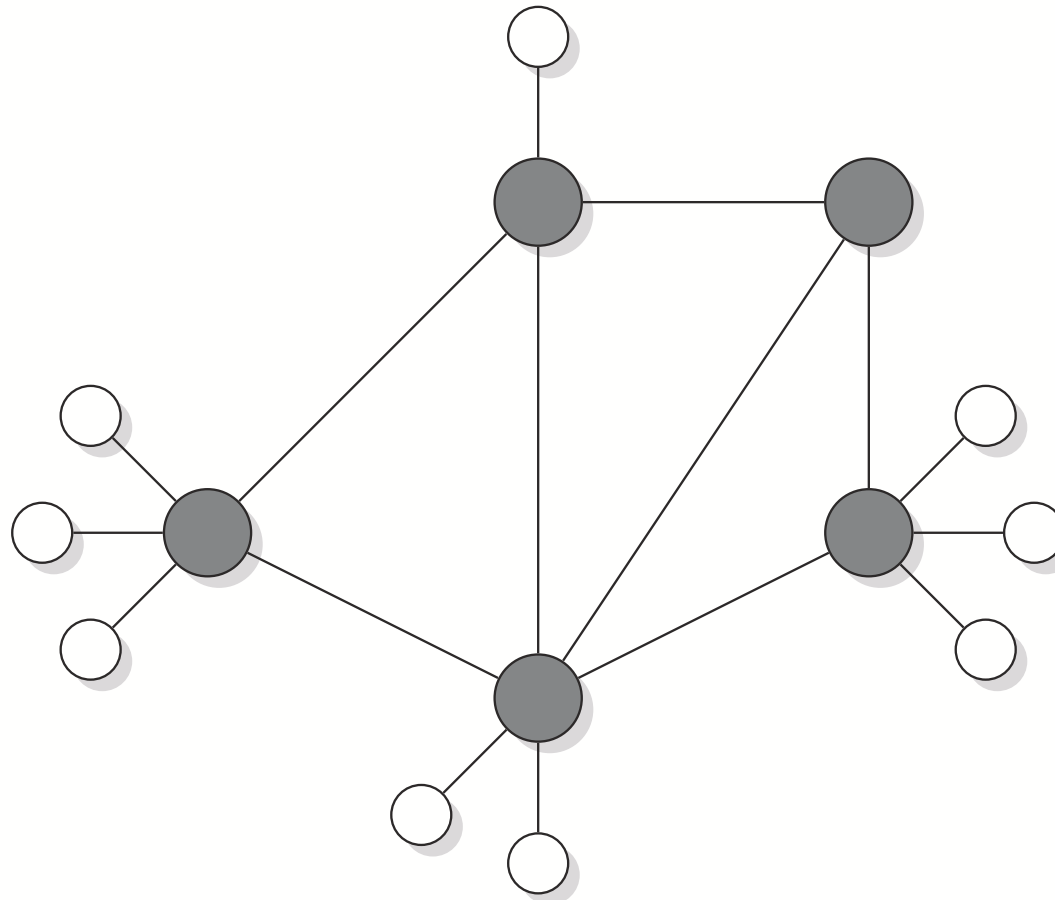
Payment Network
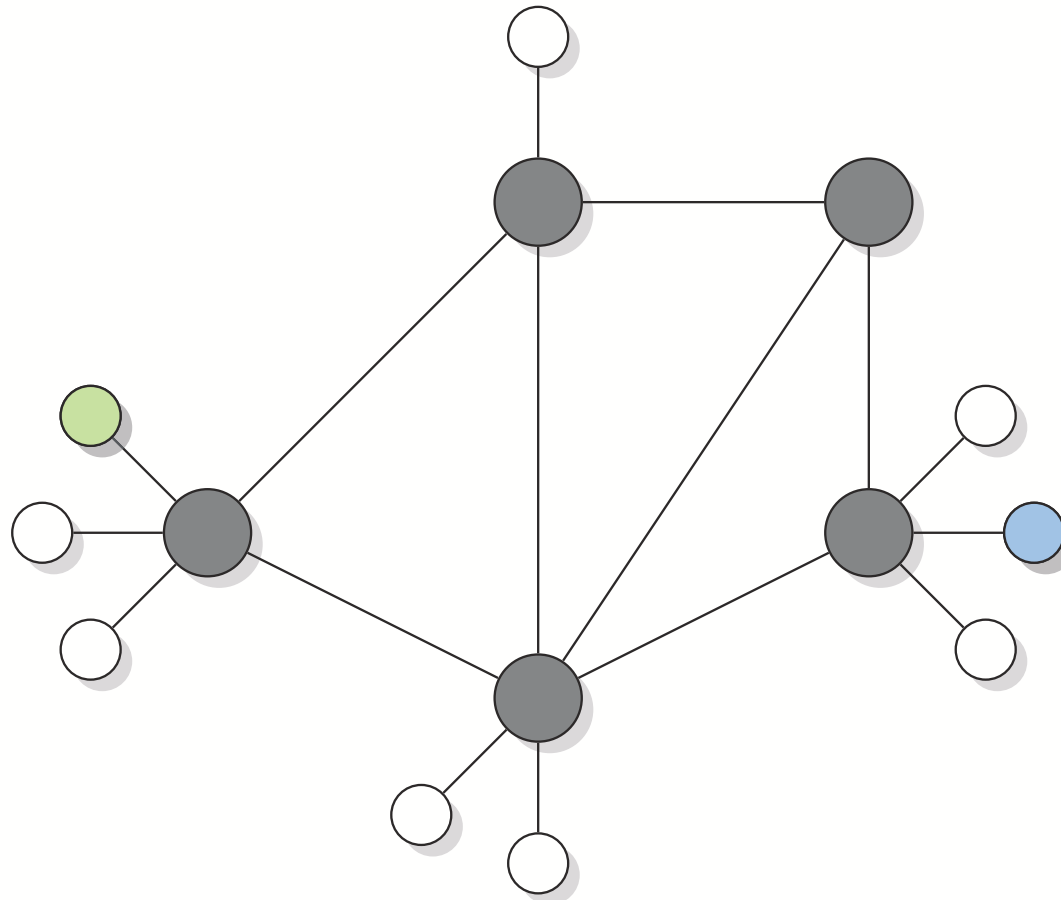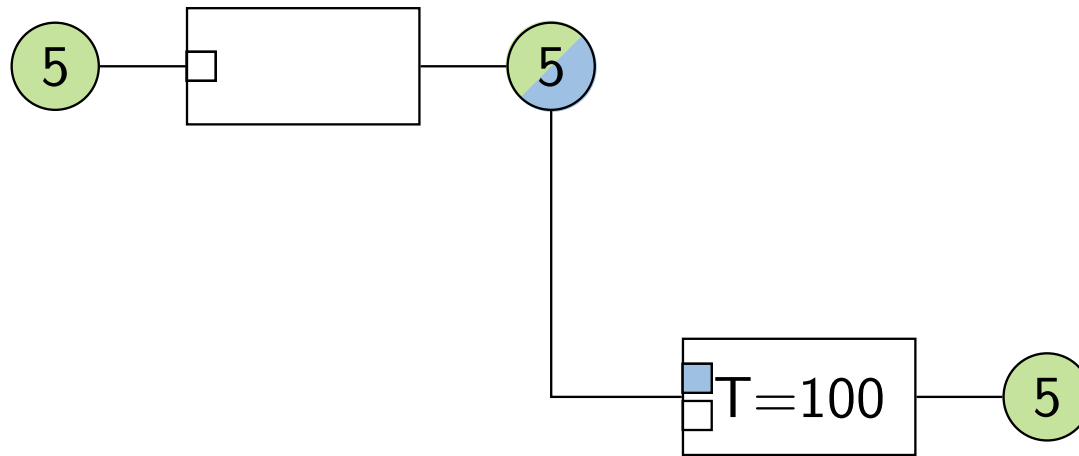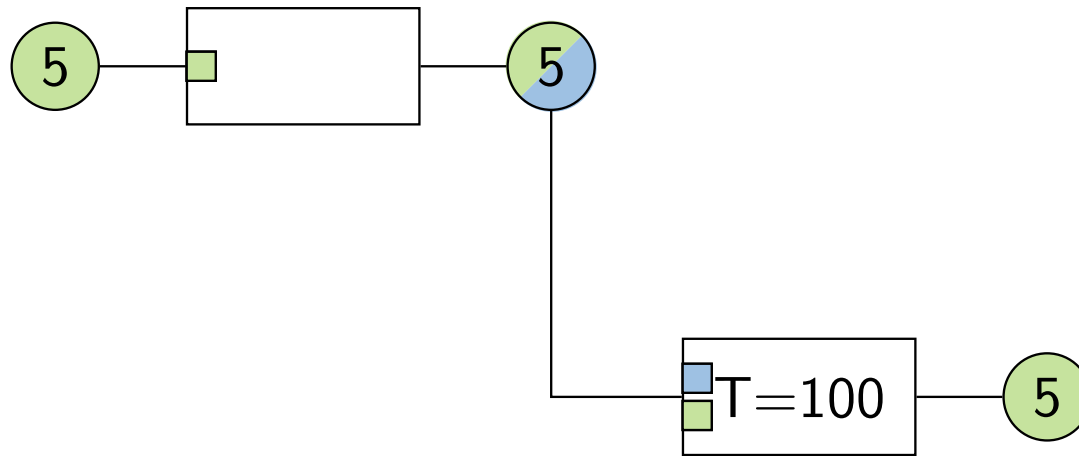
Payment Network
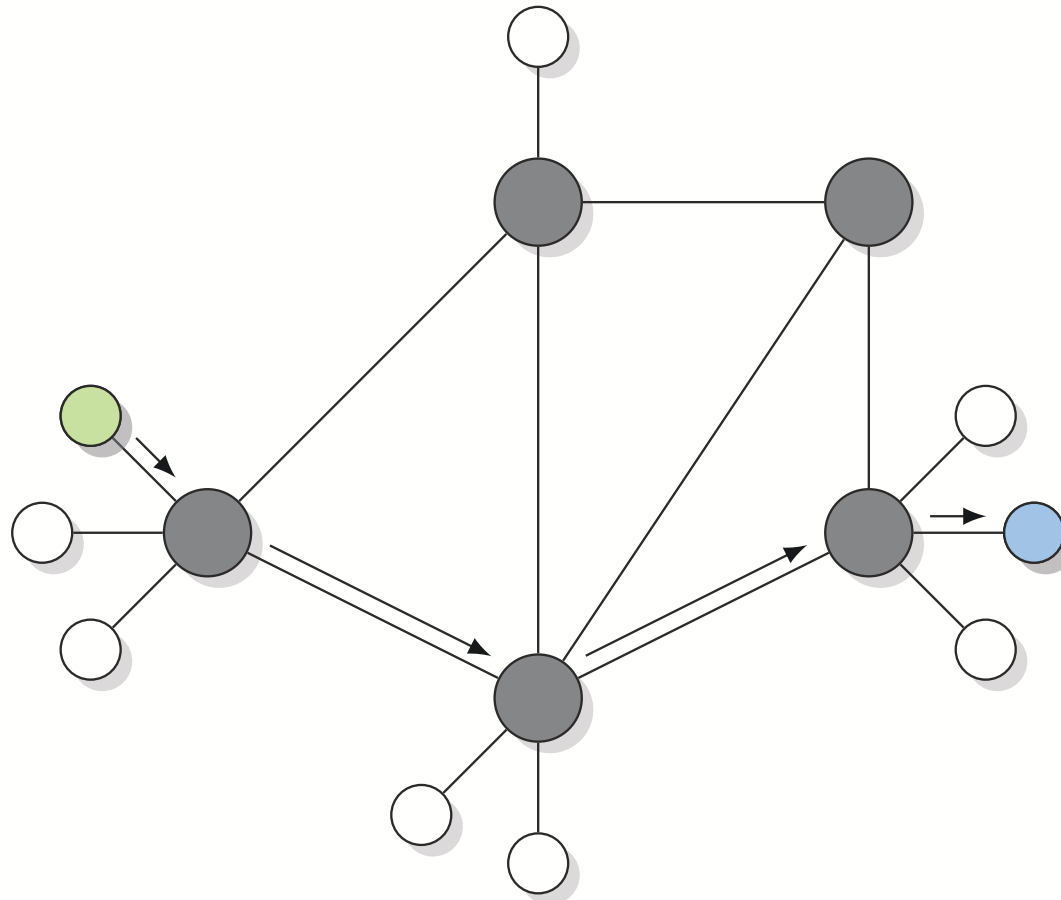
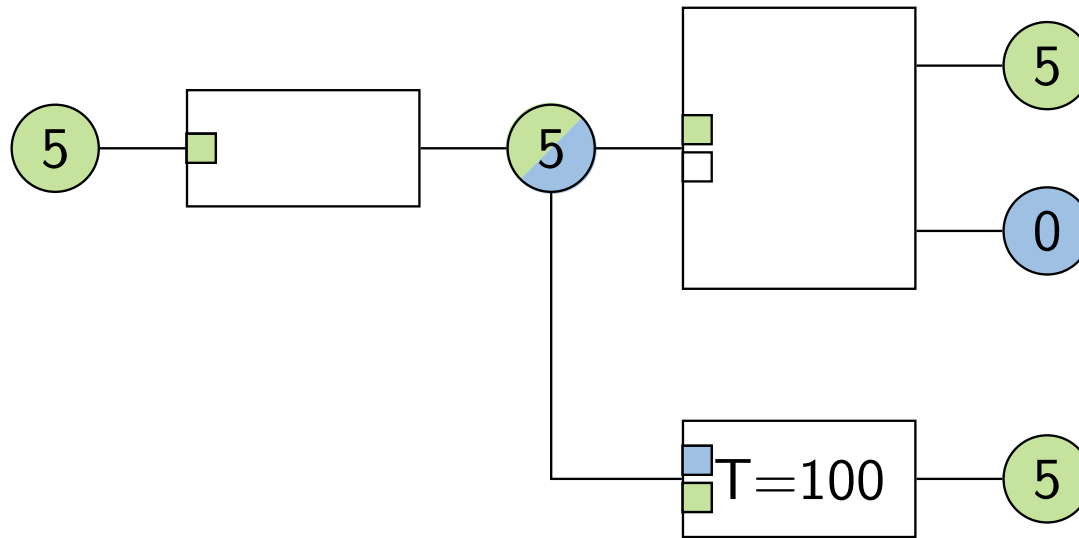# Micropayment Channels
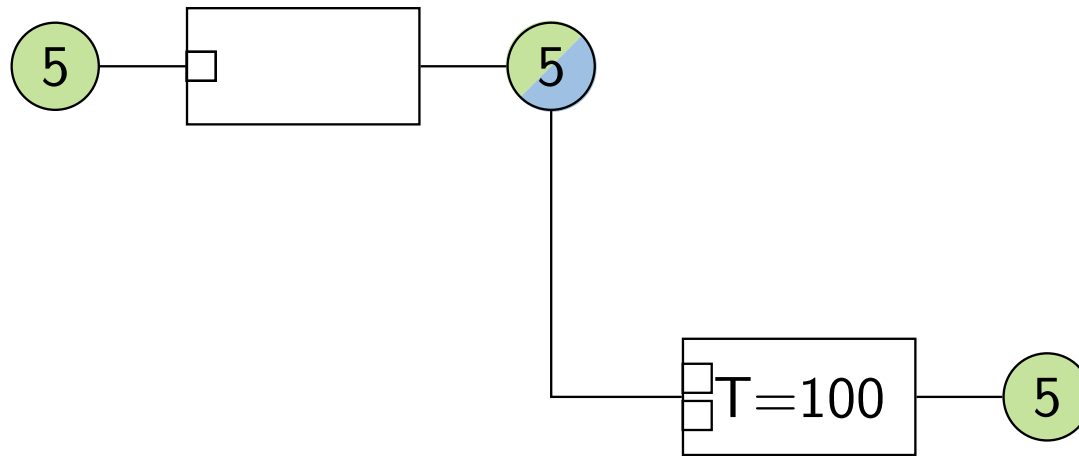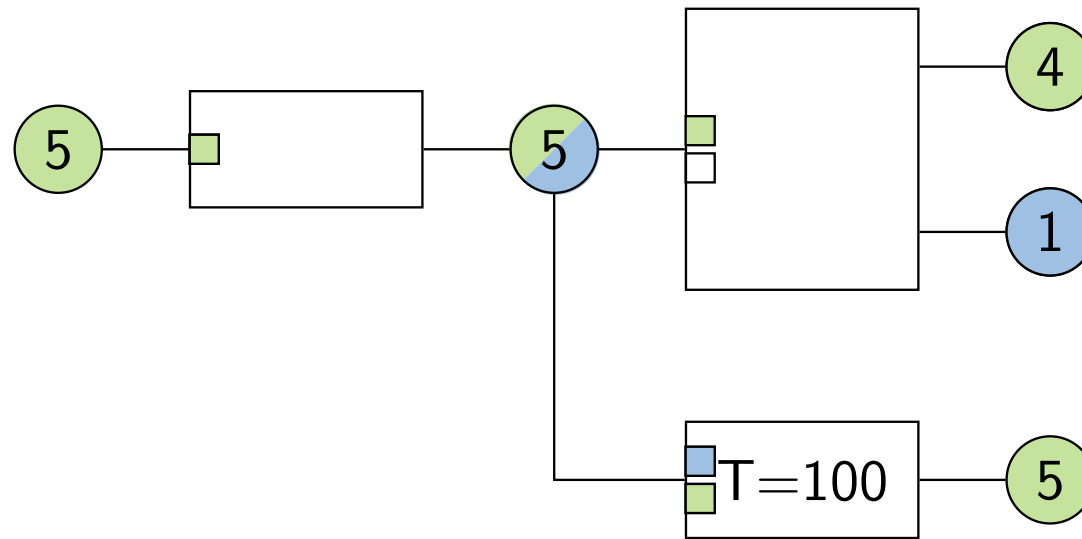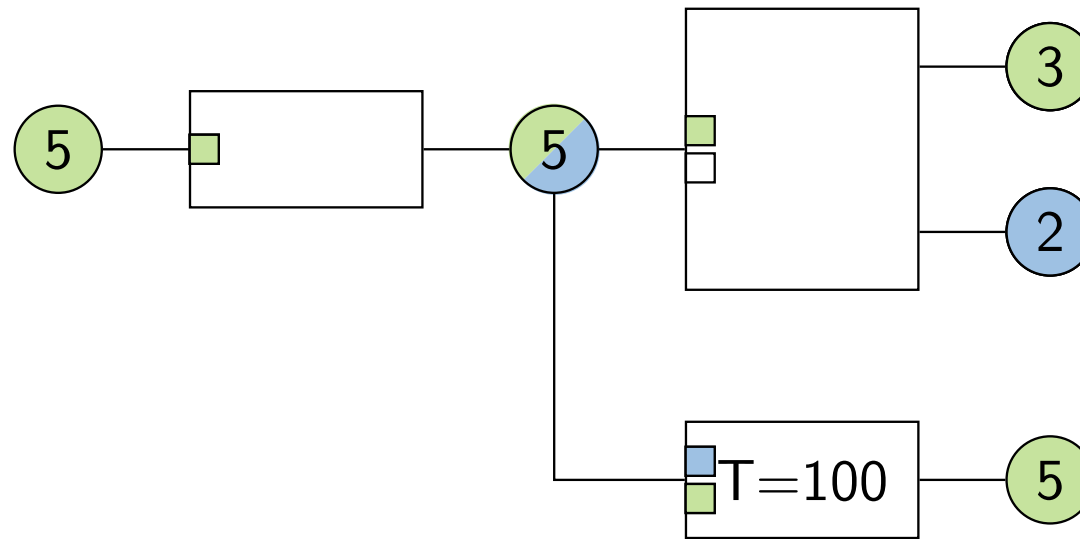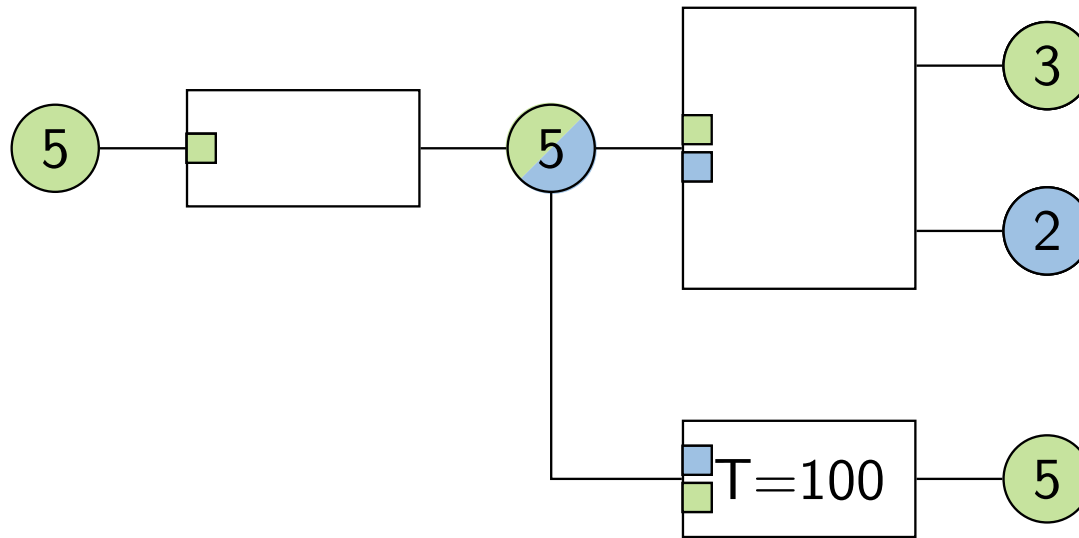
Micropayment Channels

Micropayment Channels

Micropayment Channels

Micropayment Channels

Micropayment Channels
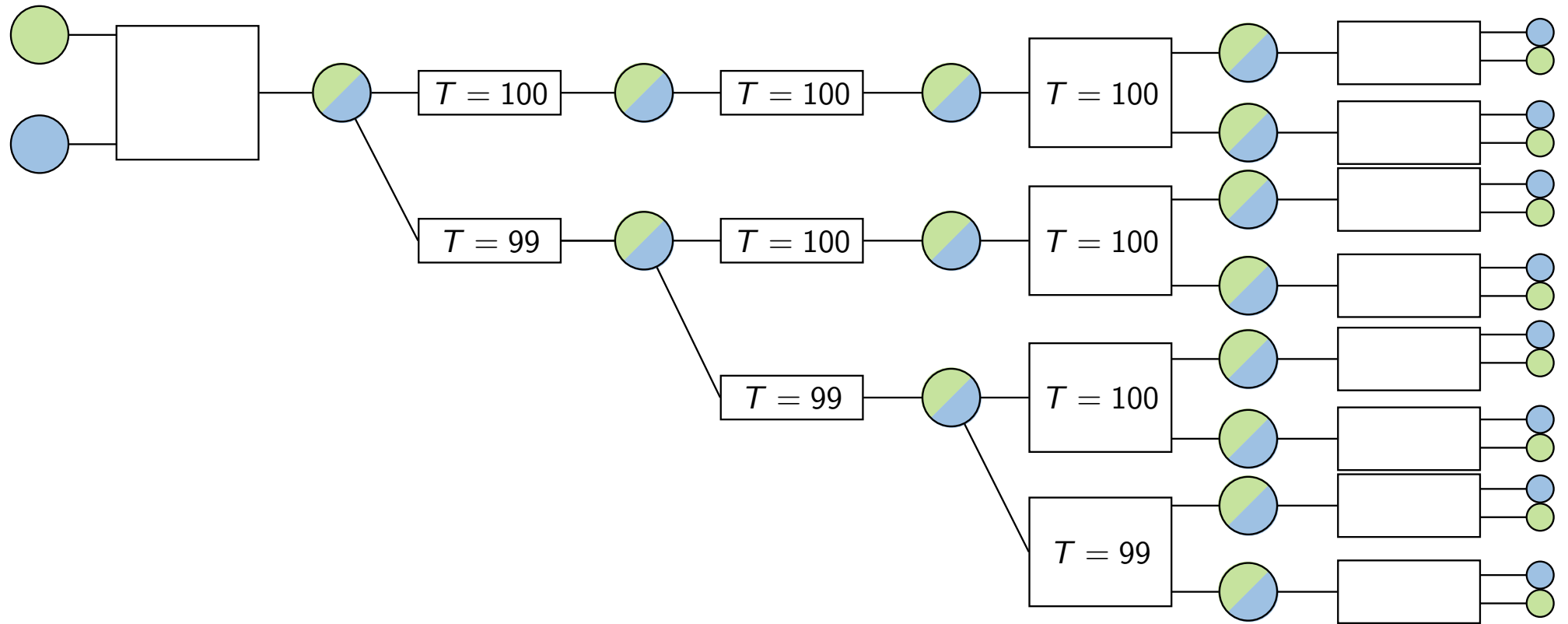
Micropayment Channels

Micropayment Channels

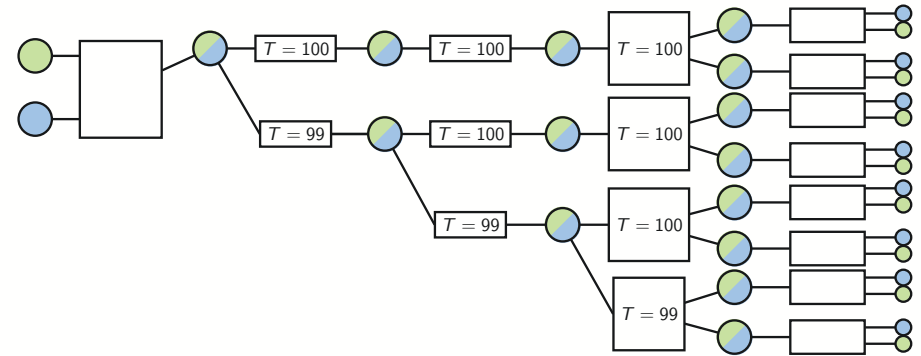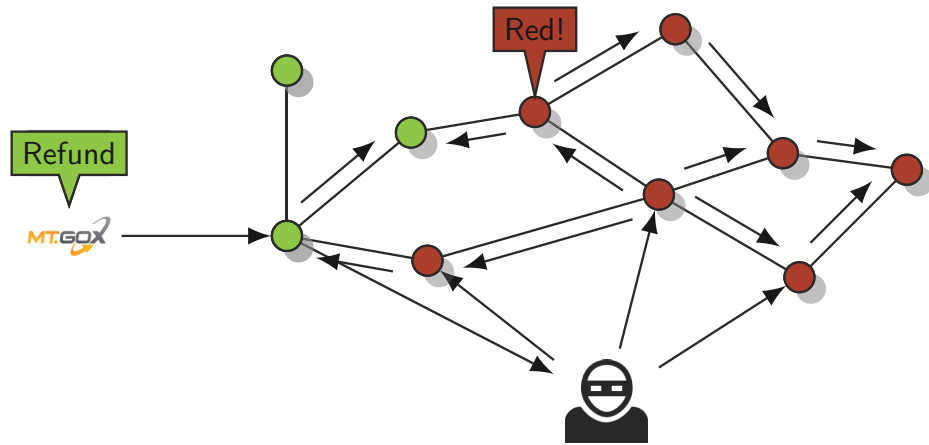# Micropayment Channels

Duplex Micropayment Channels
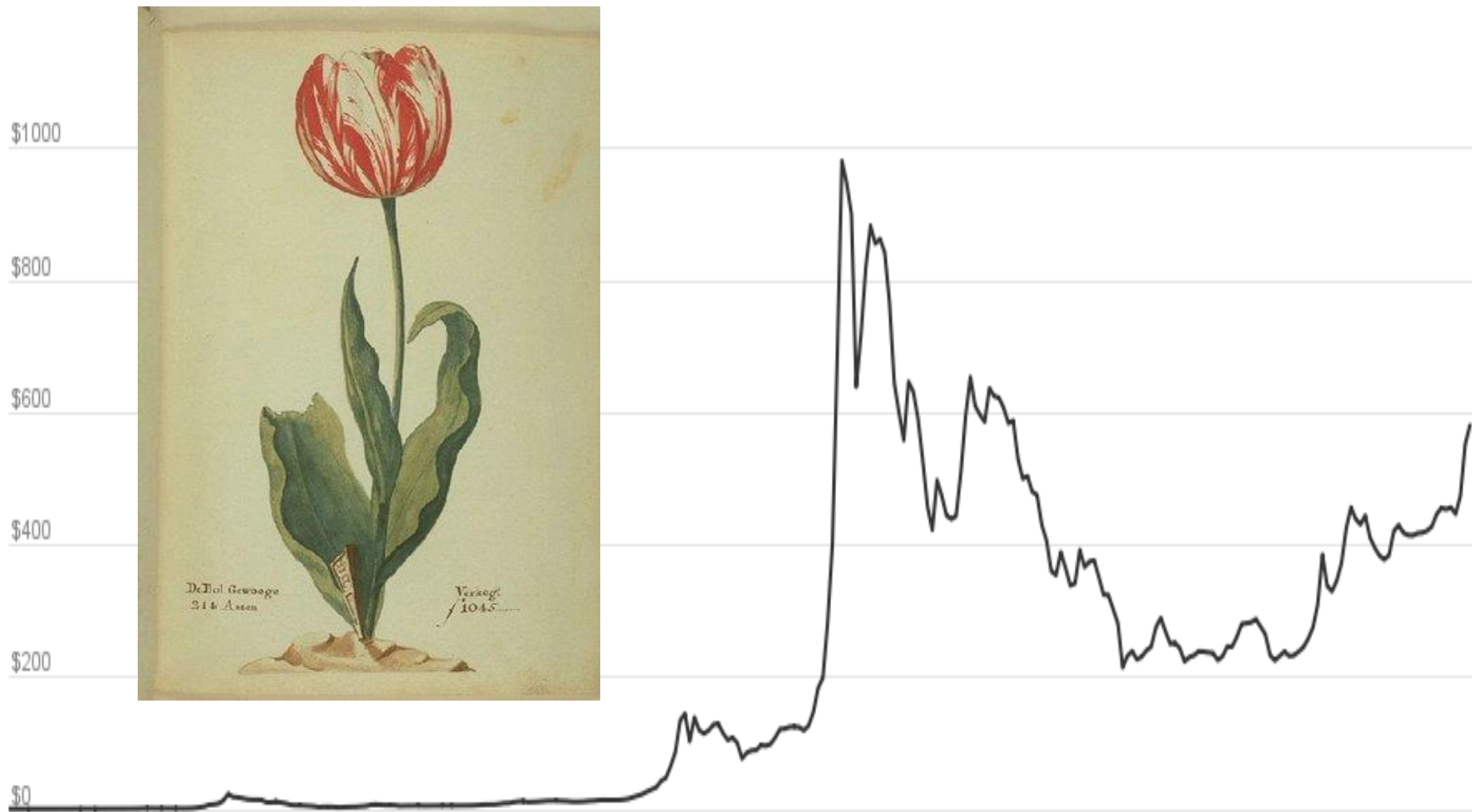

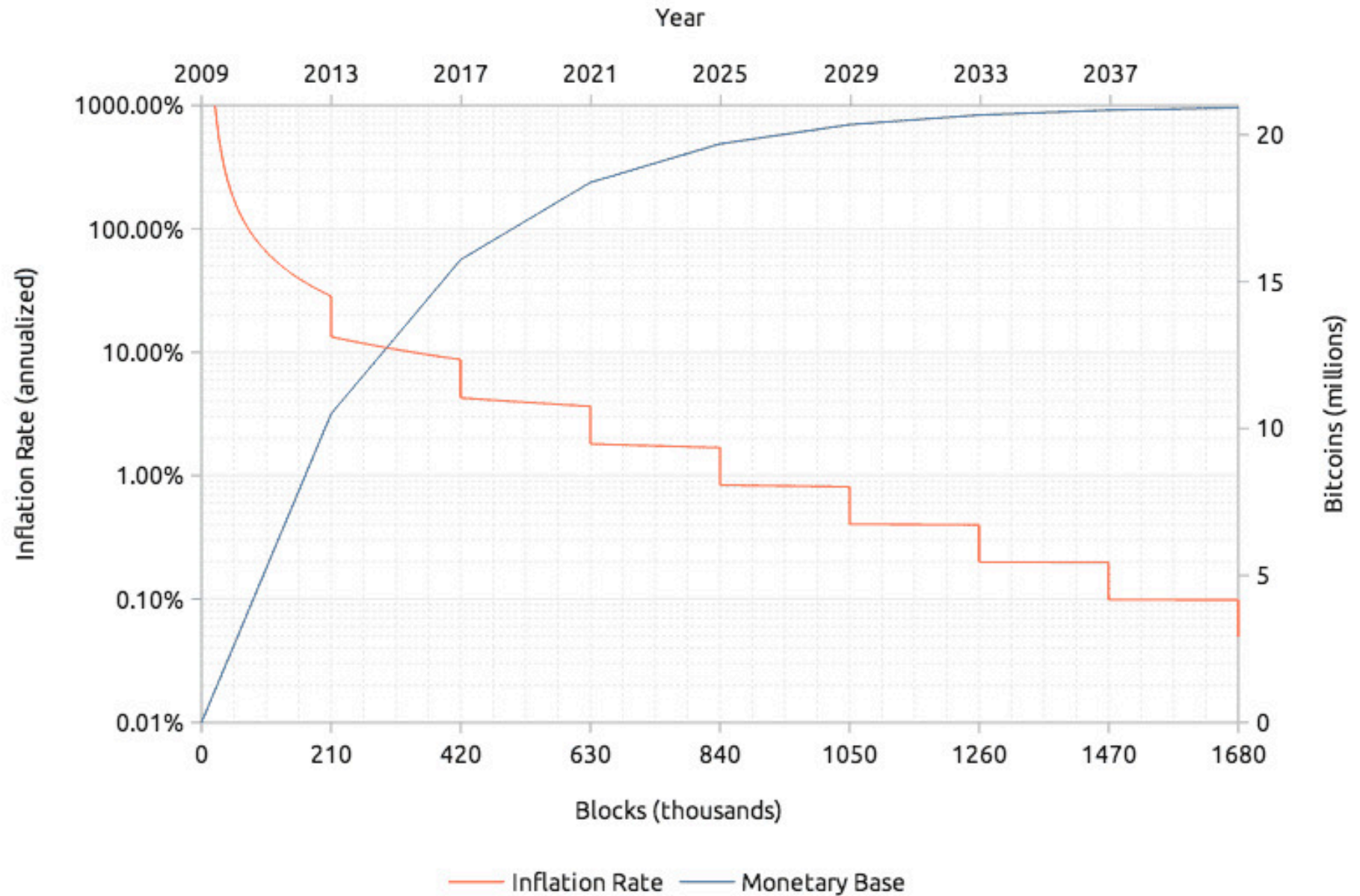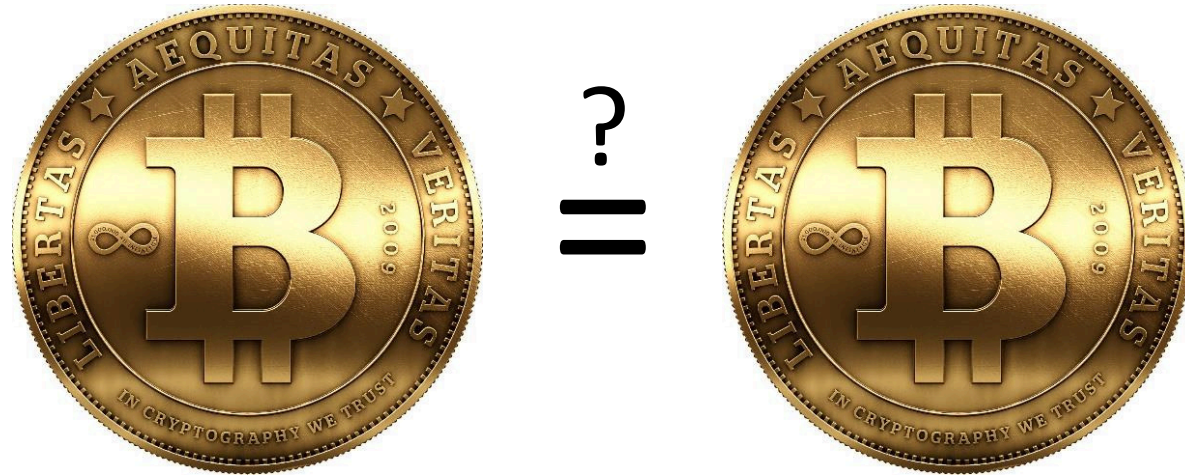Setup   Invalidation Tree   Micropayment Channels

Summary

Economy
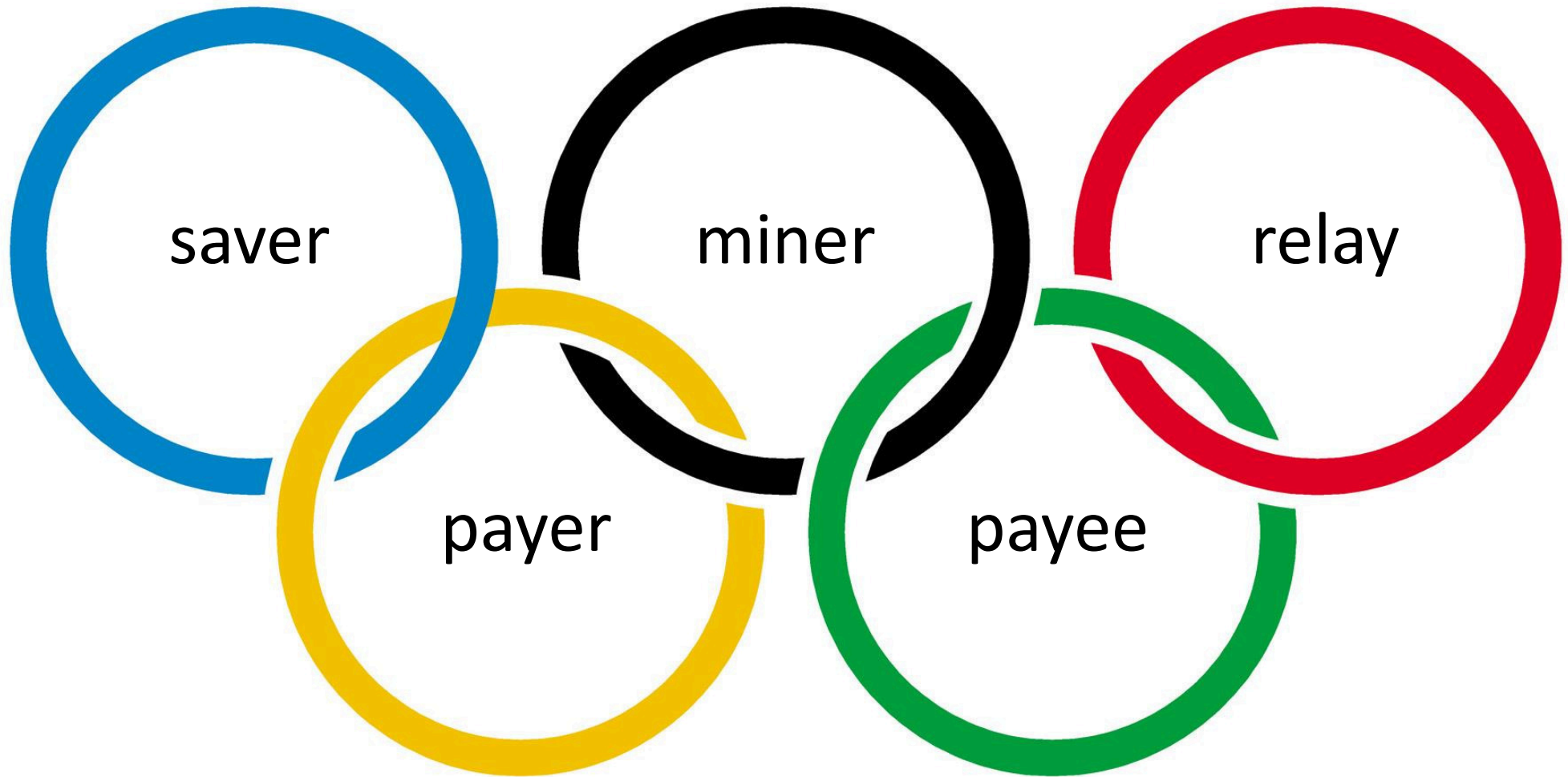
BTC in USD

Inflation

Fungibility

=?=

Looking to buy an old 50 BTC block. Where to buy? (self.Bitcoin)
submitted 7 months ago by blockCollector

18

I'll pay in bitcoin. No FIAT/Alt coin. Willing to pay premium.
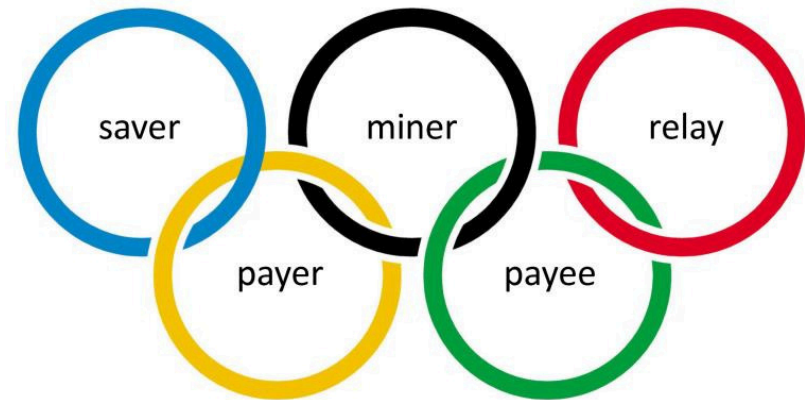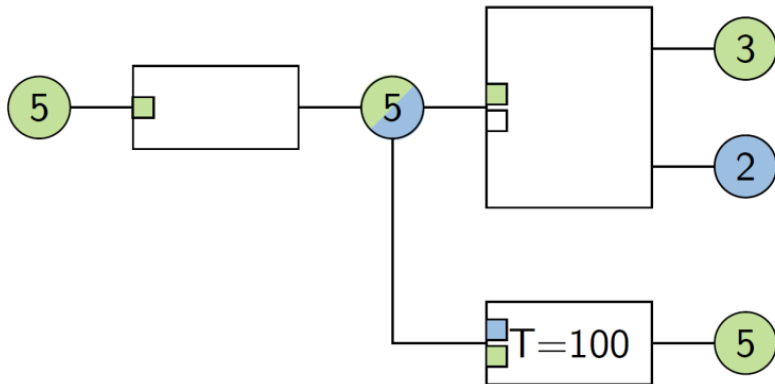
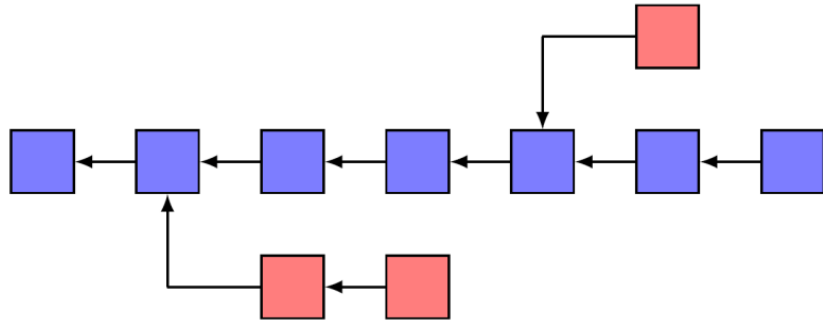# Improving Bitcoin?

What is Money?

What is Money?

Summary

Thank You!

Questions & Comments?

Thanks to my co-author
Christian Decker

www.disco.ethz.ch