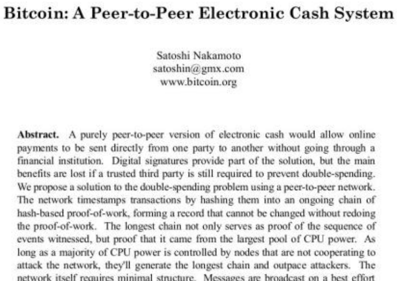
# *Blockchains*
# Overview & Applications

*Roger Wattenhofer*

*ETH Zurich – Distributed Computing Group*

CURRENCY OF THE FUTURE?

# 2008



**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

# Blockchain

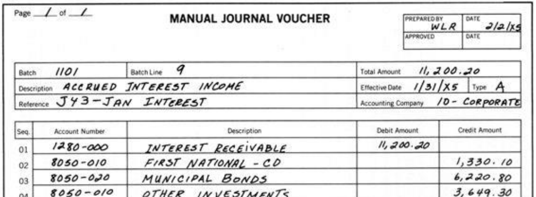


**Figure 9-3** Manual Journal Voucher.

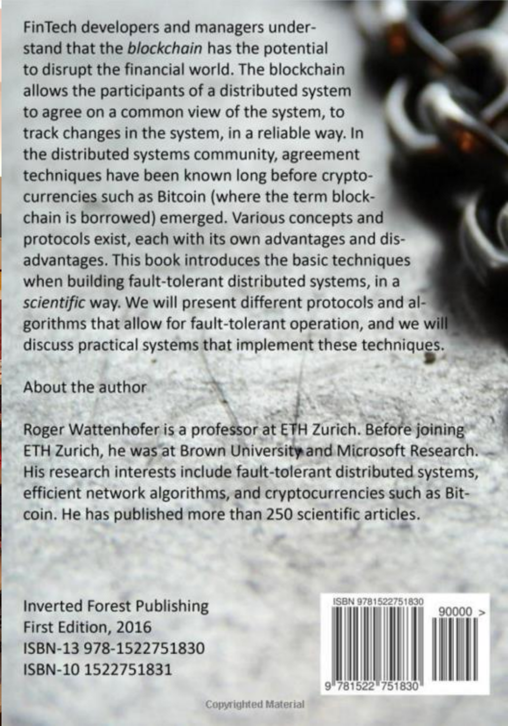
Page 1 of 1

MANUAL JOURNAL VOUCHER

| | |
|---|---|
| PREPARED BY WLR | DATE 2/2/X5 |
| APPROVED | DATE |

| | | | |
|---|---|---|---|
| Batch 1101 | Batch Line 9 | Total Amount 11,200.20 | |
| Description ACCRUED INTEREST INCOME | | Effective Date 1/31/X5 | Type A |
| Reference J43-JAN INTEREST | | Accounting Company 10- CORPORATE | |

| Seq. | Account Number | Description | Debit Amount | Credit Amount |
|---|---|---|---|---|
| 01 | 1280-000 | INTEREST RECEIVABLE | 11,200.20 | |
| 02 | 8050-010 | FIRST NATIONAL - CD | | 1,330.10 |
| 03 | 8050-020 | MUNICIPAL BONDS | | 6,220.80 |
| 04 | 8050-010 | OTHER INVESTMENTS | | 3,649.30 |



FinTech developers and managers understand that the *blockchain* has the potential to disrupt the financial world. The blockchain allows the participants of a distributed system to agree on a common view of the system, to track changes in the system, in a reliable way. In the distributed systems community, agreement techniques have been known long before cryptocurrencies such as Bitcoin (where the term blockchain is borrowed) emerged. Various concepts and protocols exist, each with its own advantages and disadvantages. This book introduces the basic techniques when building fault-tolerant distributed systems, in a *scientific* way. We will present different protocols and algorithms that allow for fault-tolerant operation, and we will discuss practical systems that implement these techniques.

About the author

Roger Wattenhofer is a professor at ETH Zurich. Before joining ETH Zurich, he was at Brown University and Microsoft Research. His research interests include fault-tolerant distributed systems, efficient network algorithms, and cryptocurrencies such as Bitcoin. He has published more than 250 scientific articles.

Inverted Forest Publishing
First Edition, 2016
ISBN-13 978-1522751830
ISBN-10 1522751831

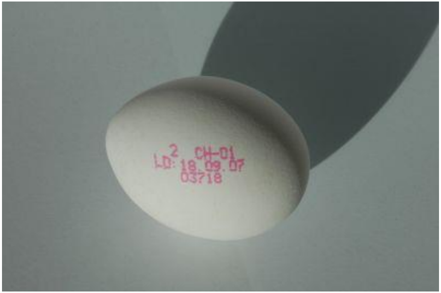
ISBN 9781522751830
90000 >
9 781522 751830

# Blockchain Basics

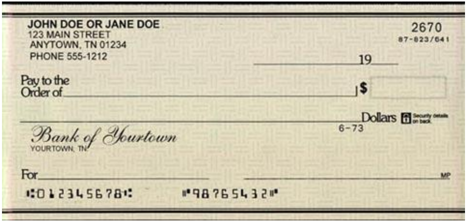
# Transaction

# Transaction

# Transaction



# Transaction



JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars 🔒 Security details on back

6-73

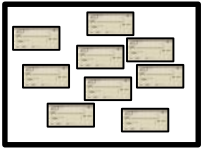
Bank of Yourtown
YOURTOWN, TN

For

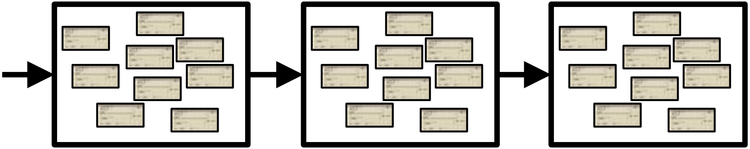
MP

⑆012345678⑆ ⑈987654321⑈

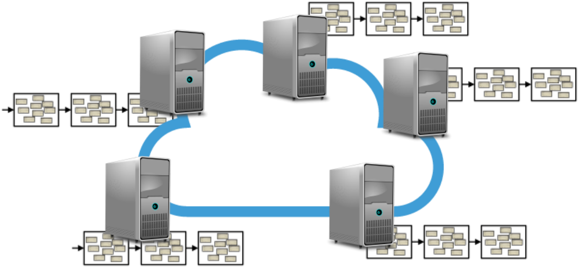
# Block



# Blockchain



# Blockchain is Replicated



# Blockchain

| Distributed Systems | & | Cryptography |
|---|---|---|
| (1982) | | (1976) |

# Blockchain

Distributed Systems & Cryptography

Fault-Tolerance & Digital Signatures

# Rule of Thumb

Blockchains* may disrupt your business if you use signatures.

*or blockchain-like tech

# Blockchain Variants

# Ledger of Transactions

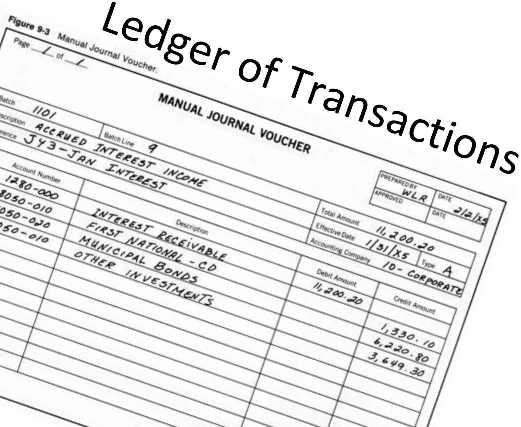


**Figure 9-3** Manual Journal Voucher.

Page 1 of 1

**MANUAL JOURNAL VOUCHER**

Batch 1101

escription ACCRUED INTEREST INCOME

Batch Line 9

erence J43-JAN INTEREST

PREPARED BY WLR DATE 2/2/X5

APPROVED DATE

Total Amount 11,200.20

Effective Date 1/31/X5

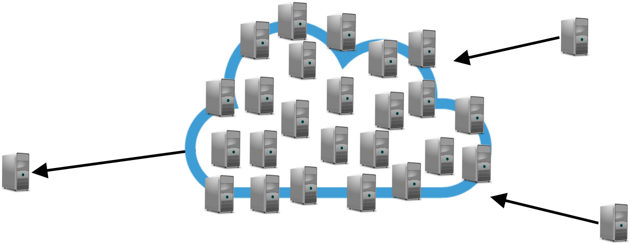
Accounting Company 10- CORPORATE

Type A

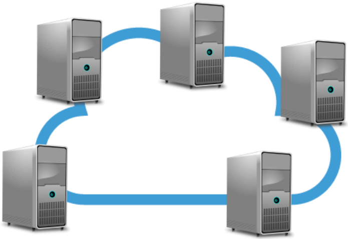
| Account Number | Description | Debit Amount | Credit Amount |
|---|---|---|---|
| 1280-000 | INTEREST RECEIVABLE | 11,200.20 | |
| 8050-010 | FIRST NATIONAL - CD | | 1,330.10 |
| 050-020 | MUNICIPAL BONDS | | 6,220.80 |
| 050-010 | OTHER INVESTMENTS | | 3,649.30 |

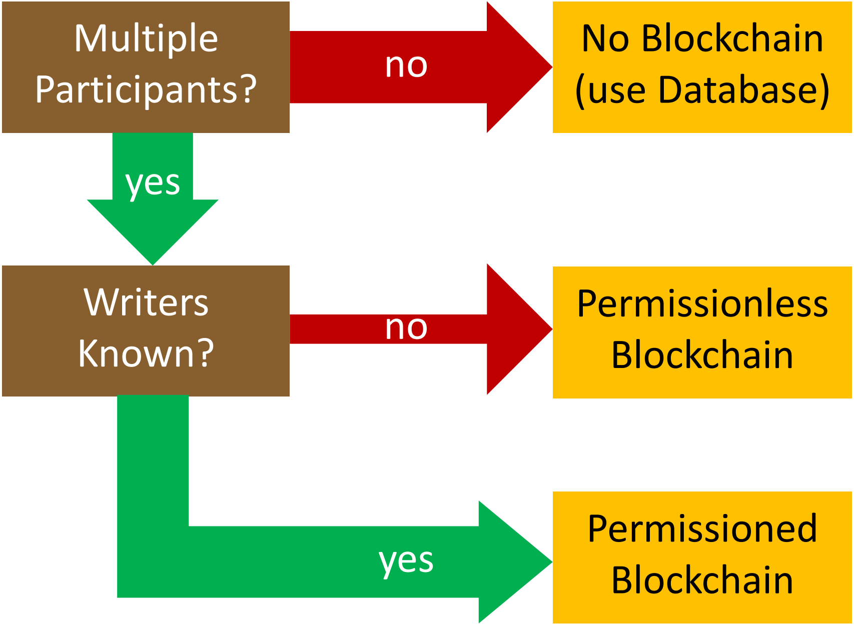
Bitcoin

# Permissionless / Open



# Permissioned / Closed





Multiple Participants?

no

No Blockchain (use Database)

yes

Writers Known?

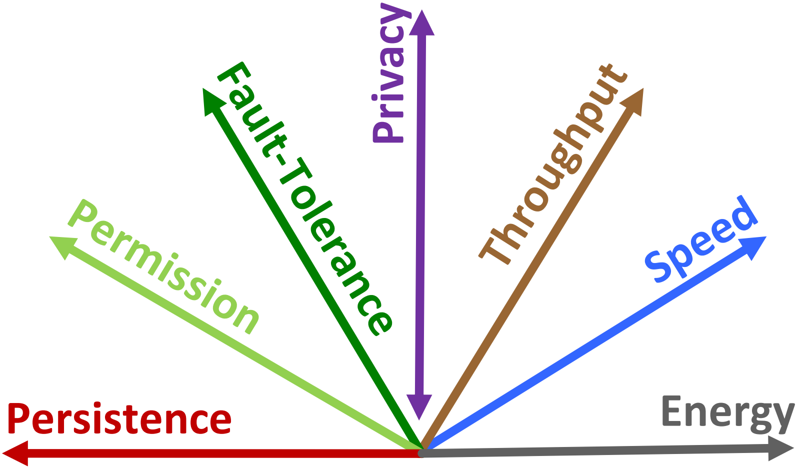
no

Permissionless Blockchain

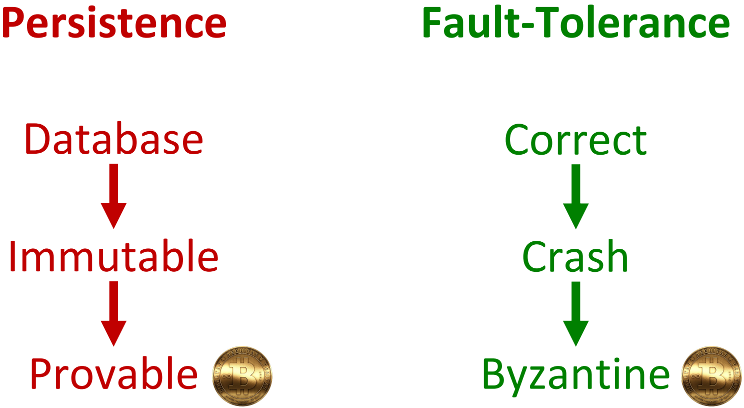
yes

Permissioned Blockchain

# The Seven Blockchain Dimensions



# Blockchain



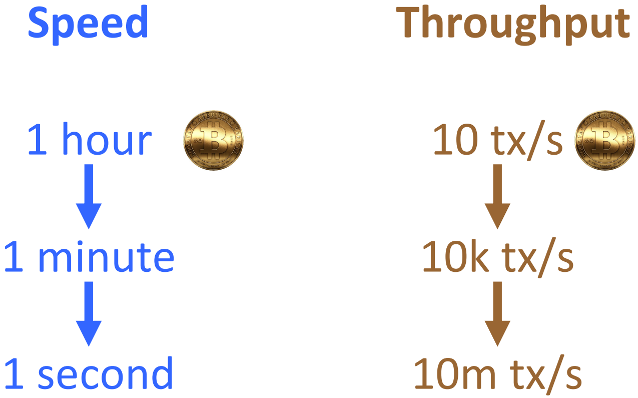
**Persistence**

Database ↓ Immutable ↓ Provable ₿

**Fault-Tolerance**

Correct ↓ Crash ↓ Byzantine ₿

# Blockchain



**Speed**

1 hour

1 minute

1 second

**Throughput**

10 tx/s

10k tx/s

10m tx/s

# Blockchain

**Scalability**

10 nodes

↓

100 nodes

↓

1000 nodes

# Energy Consumption

# «Ich wäre nicht überrascht, wenn Bitcoin verboten würde»

ETH-Informationstechnologe Roger Wattenhofer über den Energiebedarf der Kryptowährung und bessere Alternativen

Prof. Dr. Roger Wattenhofer vom Departement Informationstechnologie und Elektrotechnik der ETH Zürich

# Economic Incentives

Market / Energy Value ≈ 12 GW

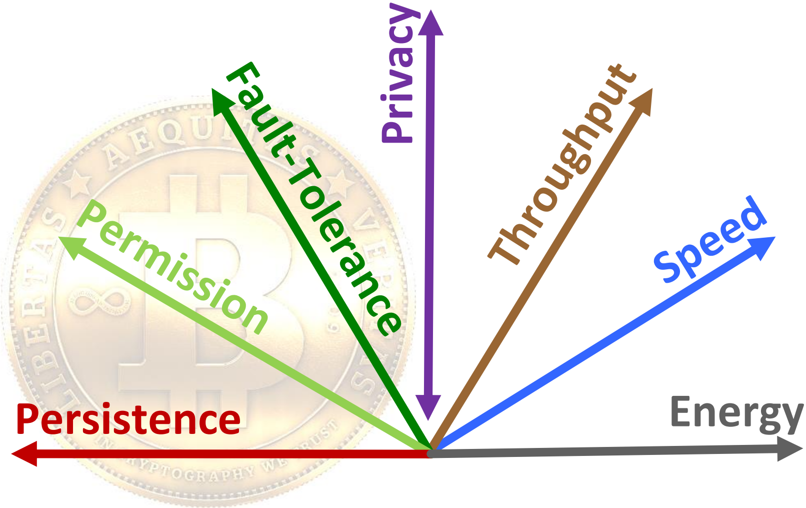
$1M/h

$0.08/kWh

# Proof of Work

$$\underset{13 \cdot 10^9 \text{ GH/s}}{\text{Hashrate}} \quad \cdot \quad \underset{0.1 \text{ J/GH}}{\text{Energy/Hash}} \quad \approx \quad 1.3 \text{ GW}$$

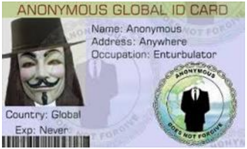
# The Seven Blockchain Dimensions



# What About Privacy?

# It’s Complicated.

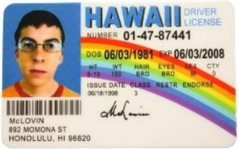
# Privacy


ANONYMOUS GLOBAL ID CARD

Name: Anonymous
Address: Anywhere
Occupation: Enturbulator

Country: Global
Exp: Never

ANONYMOUS
DOES NOT FORGIVE


HAWAII DRIVER LICENSE

NUMBER 01-47-87441
DOB 06/03/1981 EXP 06/03/2008

| HT | WT | HAIR | EYES | SEX | CTY |
|---|---|---|---|---|---|
| 5-10 | 150 | BRO | BRO | M | 0 |

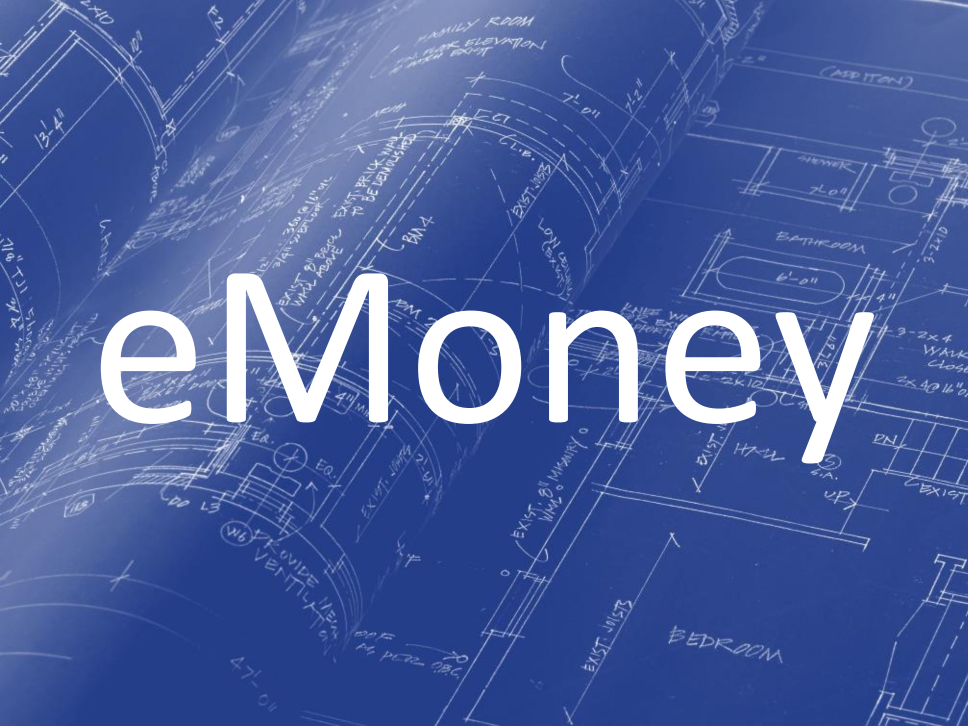
| ISSUE DATE | CLASS | RESTR | ENDORSE |
|---|---|---|---|
| 06/18/1998 | 3 | | |

McLOVIN
892 MOMONA ST
HONOLULU, HI 96820

Anonymity/Public ↔ Identity/Private

# Applications

# eMoney


FAMILY ROOM
(ADDITION)
SHOWER
BATHROOM
EXIST. BRICK WALL TO BE DEMOLISHED
EXIST. 8" BRICK WALL ABOVE
EXIST. JOISTS
HALL
DN
UP
PROVIDE VENTILATION
BEDROOM
EXIST. 8" MASONRY WALL

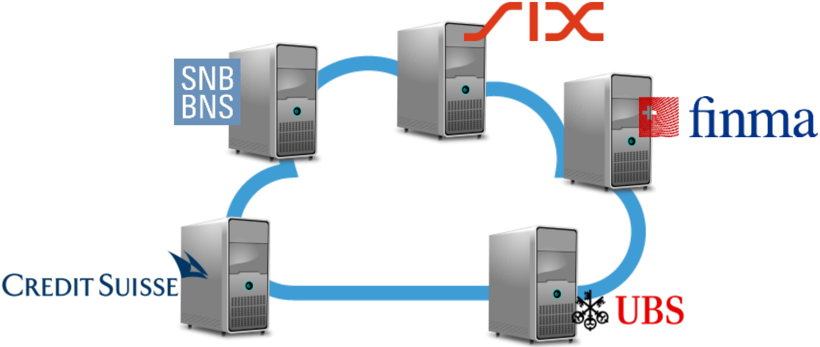
| Bitcoin | eMoney |
|---|---|
| Anonymity | Accountability |
| Open/Anarchic | Closed/Private |
| Blockchain | Paxos, PBFT, … |
| Eventual Consistency | Strong Consistency |
| Proof-of-Work | Central Banks |

# Permissioned Blockchain

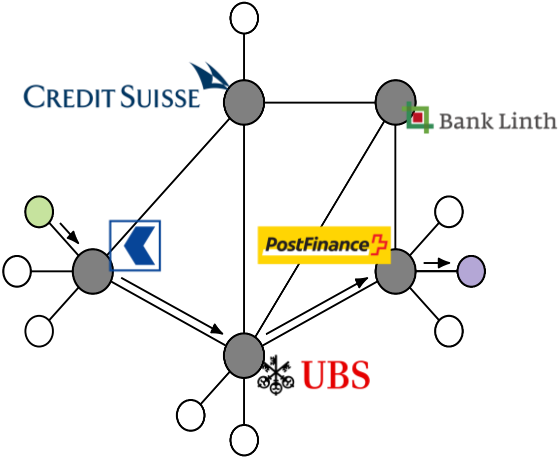
# &

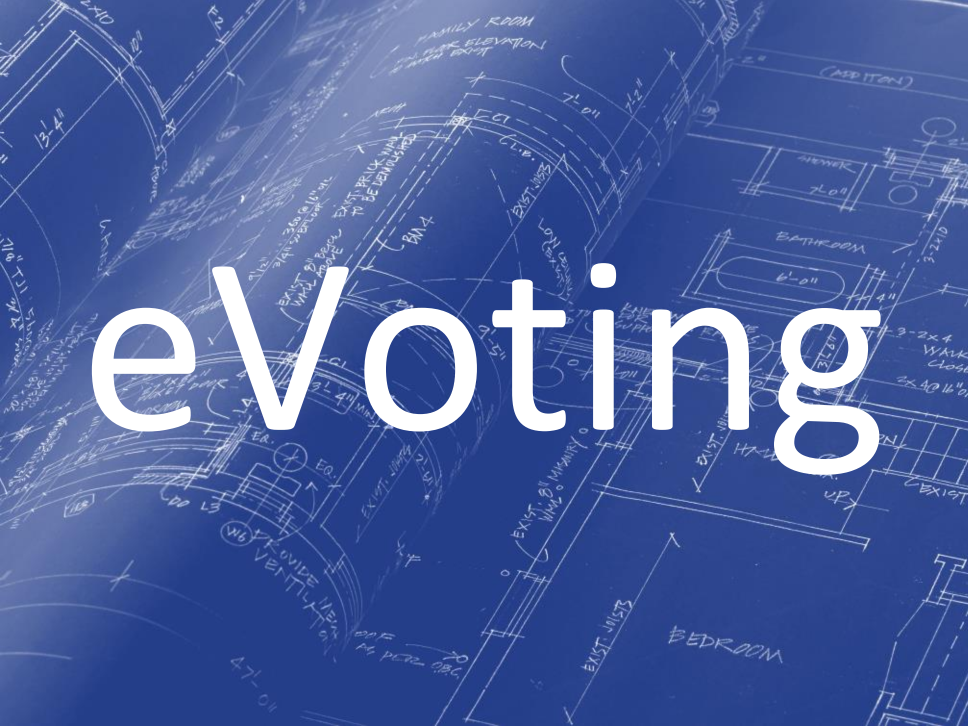
# Payment Network

# Permissioned Blockchain



# Payment Network



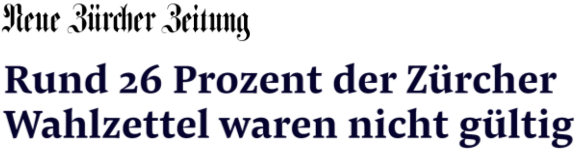

FAMILY ROOM
(ADDITION)
SHOWER
BATHROOM
EXIST. JOISTS
PROVIDE VENTILATION
BEDROOM

# eVoting

# What’s Wrong with Paper?

# Cost

# Verifiability



Neue Zürcher Zeitung

Rund 26 Prozent der Zürcher Wahlzettel waren nicht gültig

# Anonymity

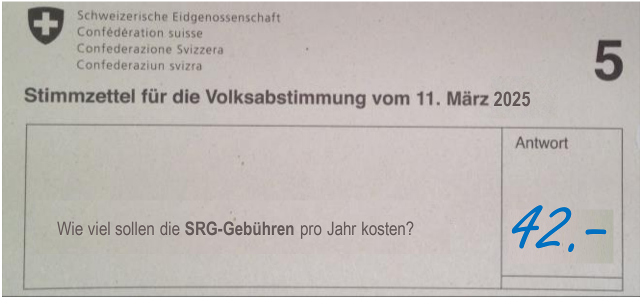
Identity Swapper

Identity Mixer

…

# Election Help

# Democracy Beyond Yes or No



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

5

**Stimmzettel für die Volksabstimmung vom 11. März 2025**

| | Antwort |
|---|---|
| Wie viel sollen die **SRG-Gebühren** pro Jahr kosten? | 42,- |

# Don’t bring a Blockchain to a Gunfight

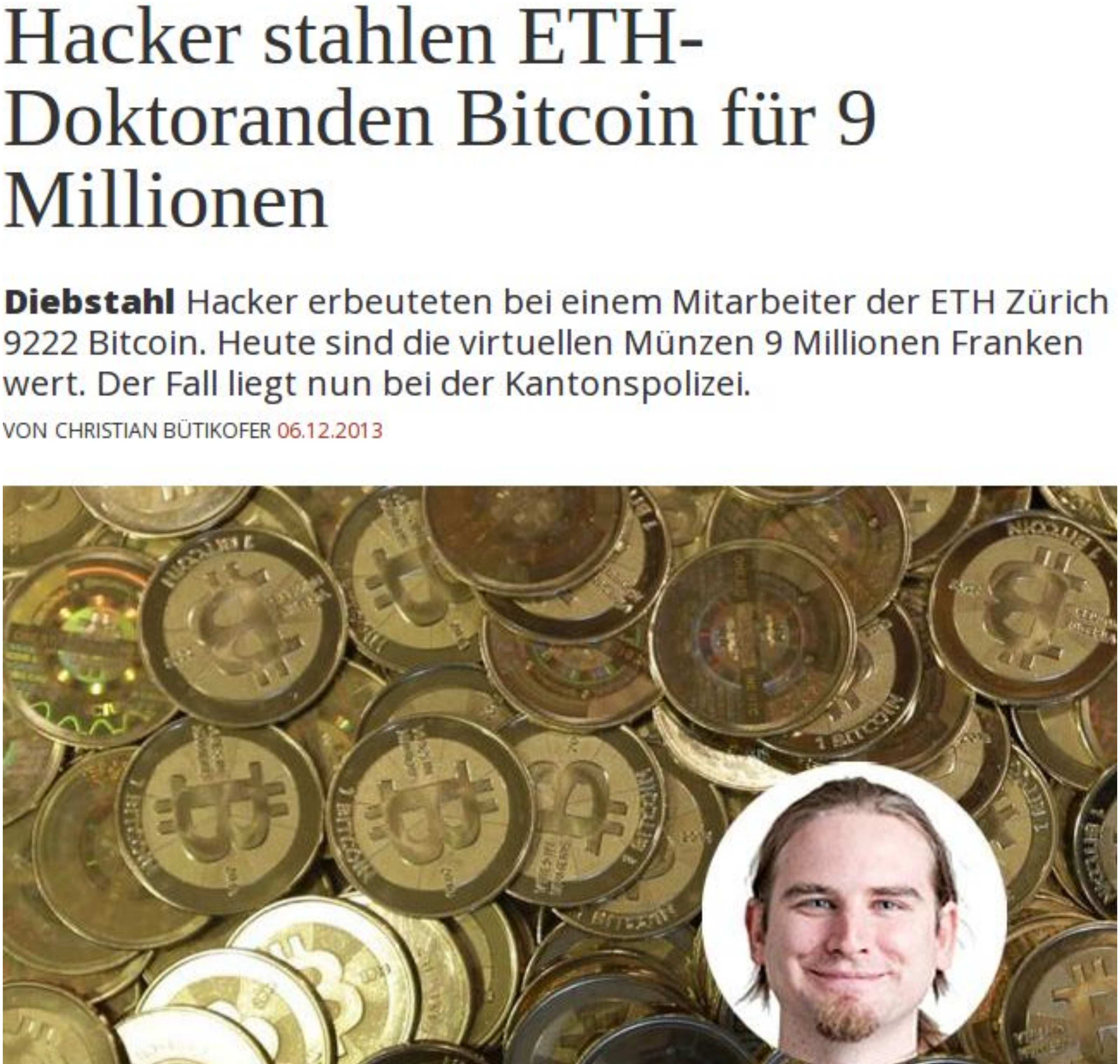
# Thank You!

Questions & Comments?

www.disco.ethz.ch

# *Scaling Bitcoin*
# Micropayment Channel Networks

*Roger Wattenhofer*



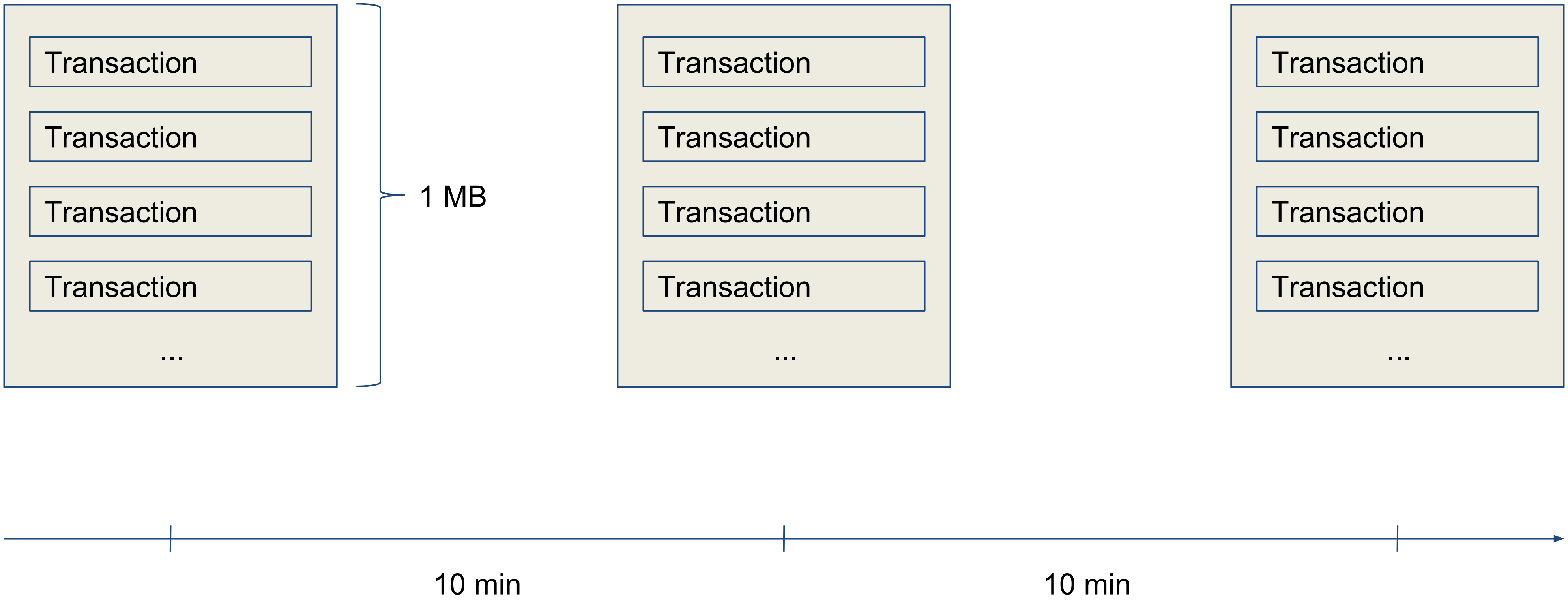
# Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

**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

# Can Bitcoin be a Real Currency?

# The Blockchain



Transaction
Transaction
Transaction
Transaction
...

1 MB

Transaction
Transaction
Transaction
Transaction
...

Transaction
Transaction
Transaction
Transaction
...

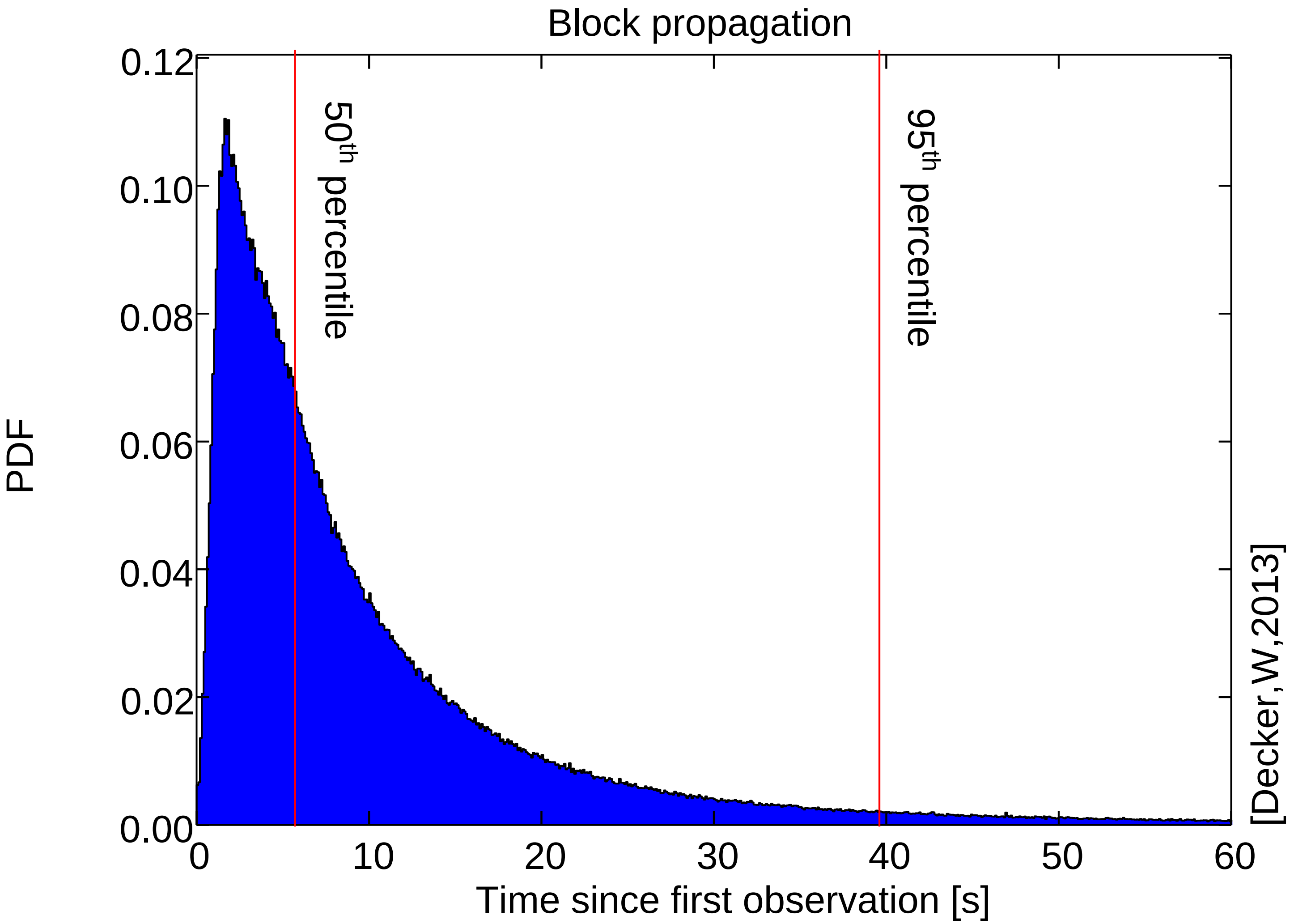
10 min

10 min

Avg Tx Fee in Dec 2017: > $50!

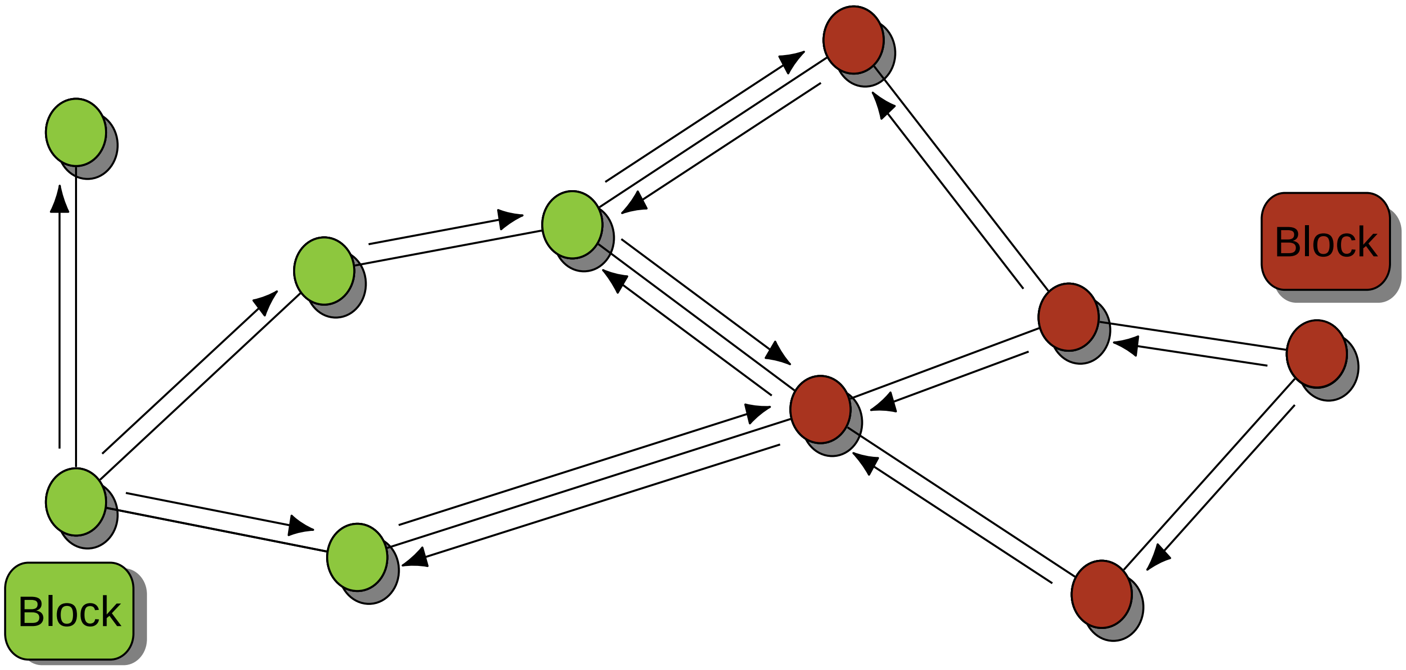
# Just Change Parameters?

# Propagation Speed



[Decker,W,2013]

# Blockchain Forks



# Increasing Propagation Speed?

Small network diameter

Just verify block headers before passing on

Reuse transactions already known

# Does it Help?

# Not Really

Still less than (roughly) 100 tx/s

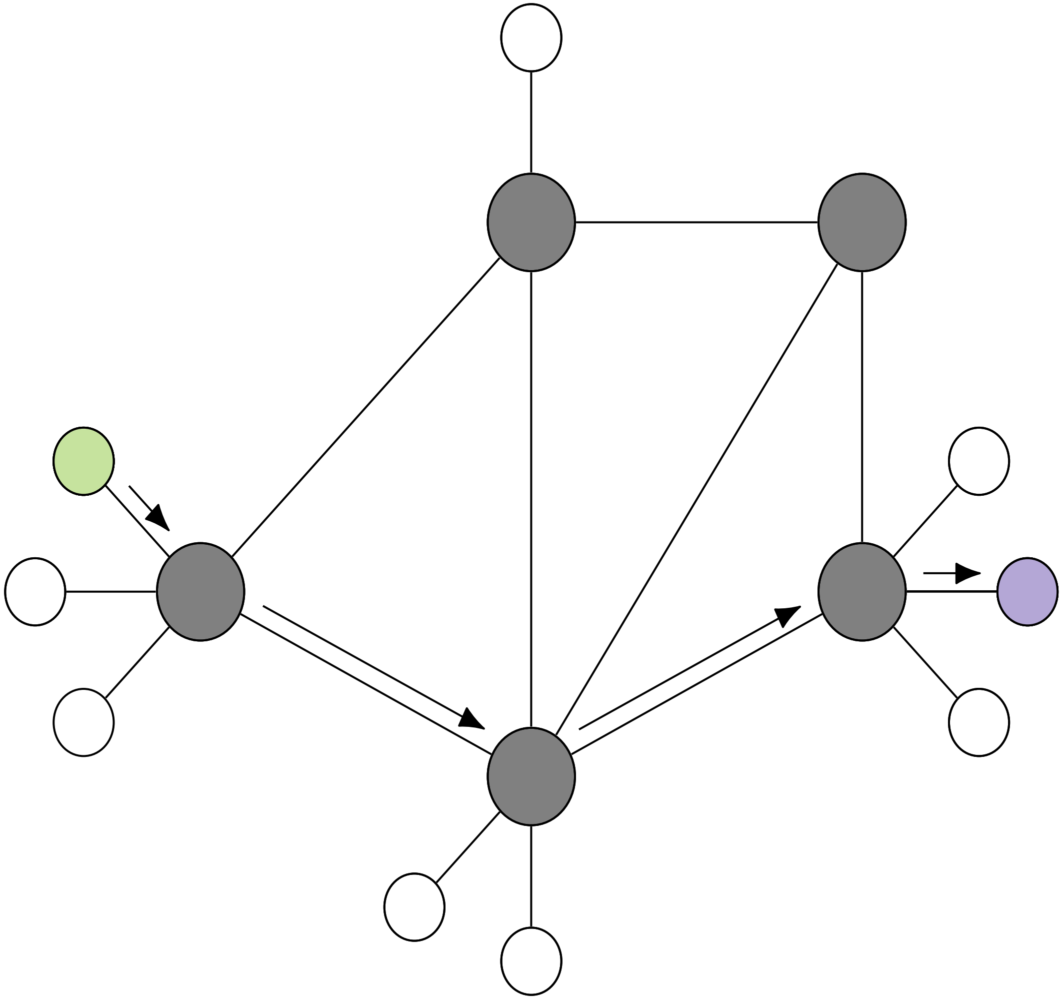
Visa: 56 000 tx/s

Micropayments?

# Fundamental Scalability Problem:
# Every Node Sees Every Single Transaction

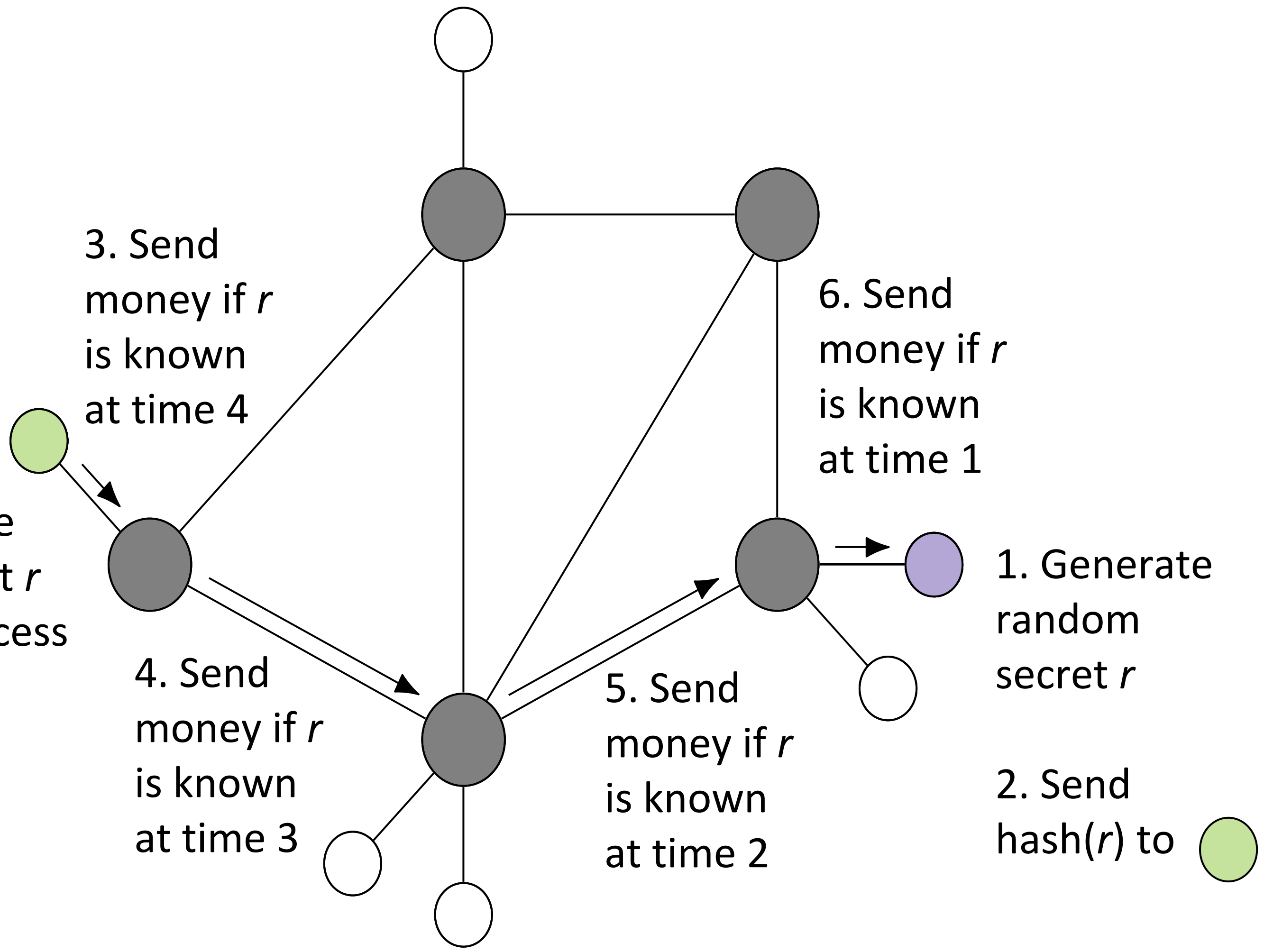
# Payment Networks

# Payment Network



# Hashed Timelocked Contract (HTLC)

# HTLC Example ( 🟣 sells to 🟢 )



1. Generate random secret *r*

2. Send hash(*r*) to 🟢

3. Send money if *r* is known at time 4

4. Send money if *r* is known at time 3

5. Send money if *r* is known at time 2

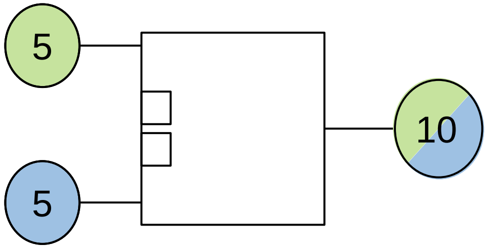
6. Send money if *r* is known at time 1

7. Use secret *r* to access good

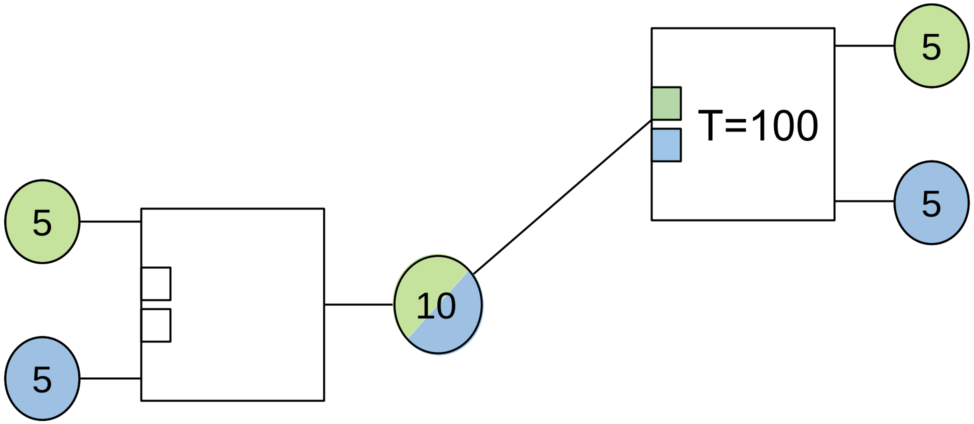
# Single Hop in Network

# Duplex Micropayment Channels (Example for Smart Contract)

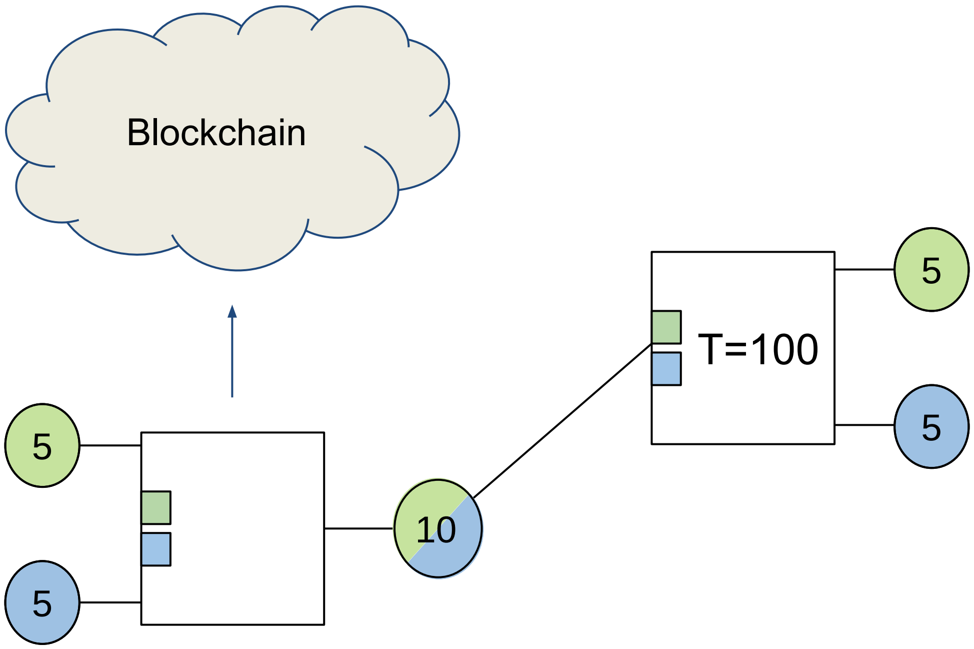
# Duplex Micropayment Channel



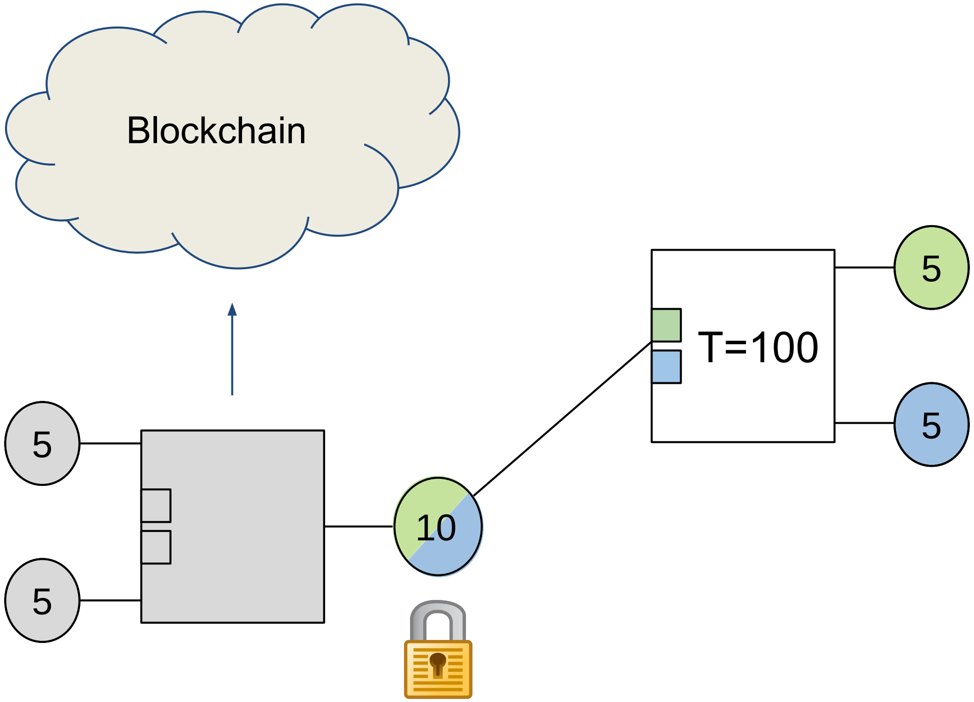
# Duplex Micropayment Channel



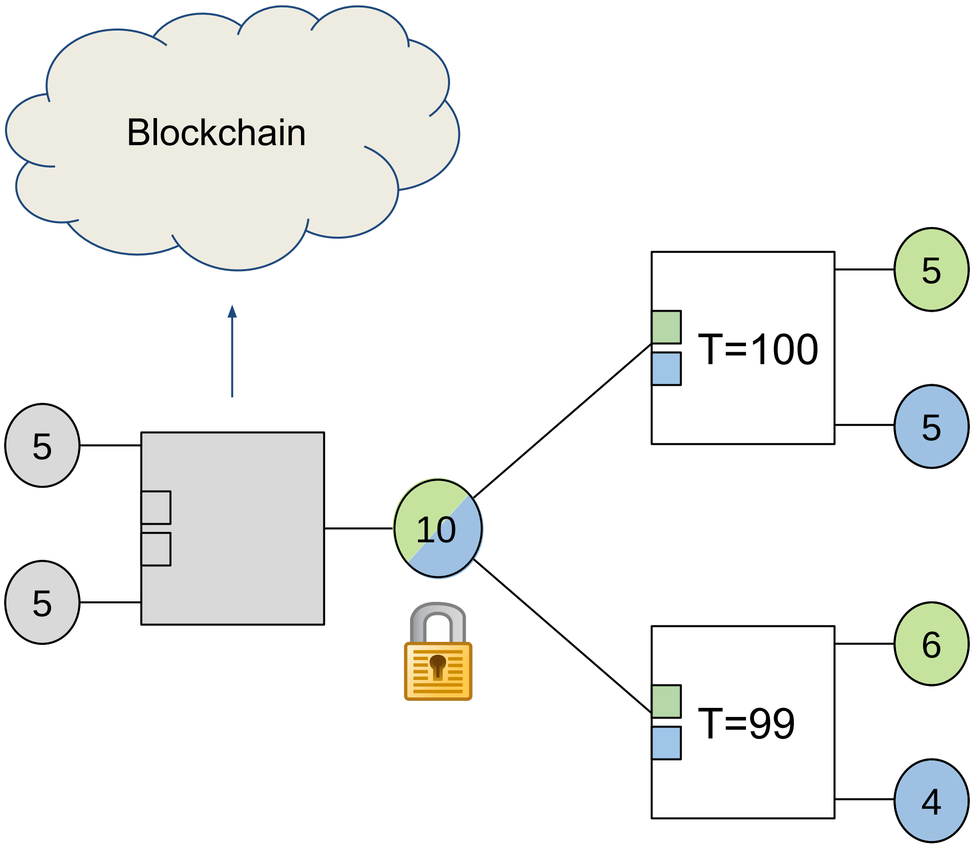
# Duplex Micropayment Channel



# Duplex Micropayment Channel

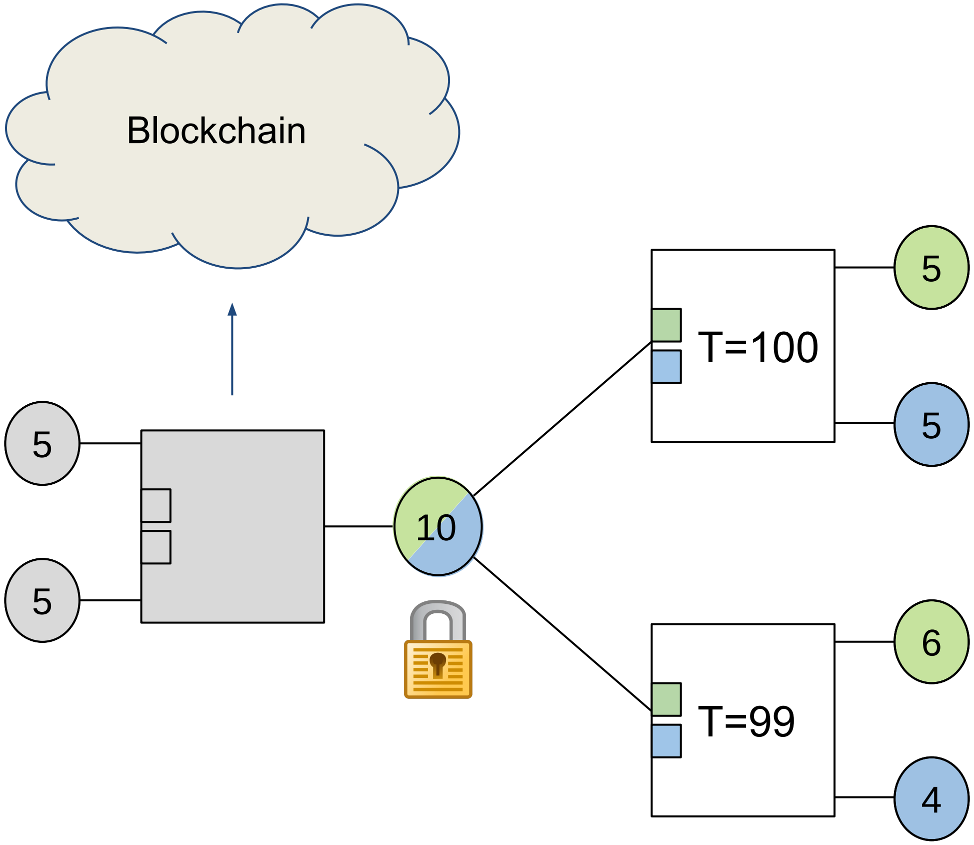


# Duplex Micropayment Channel



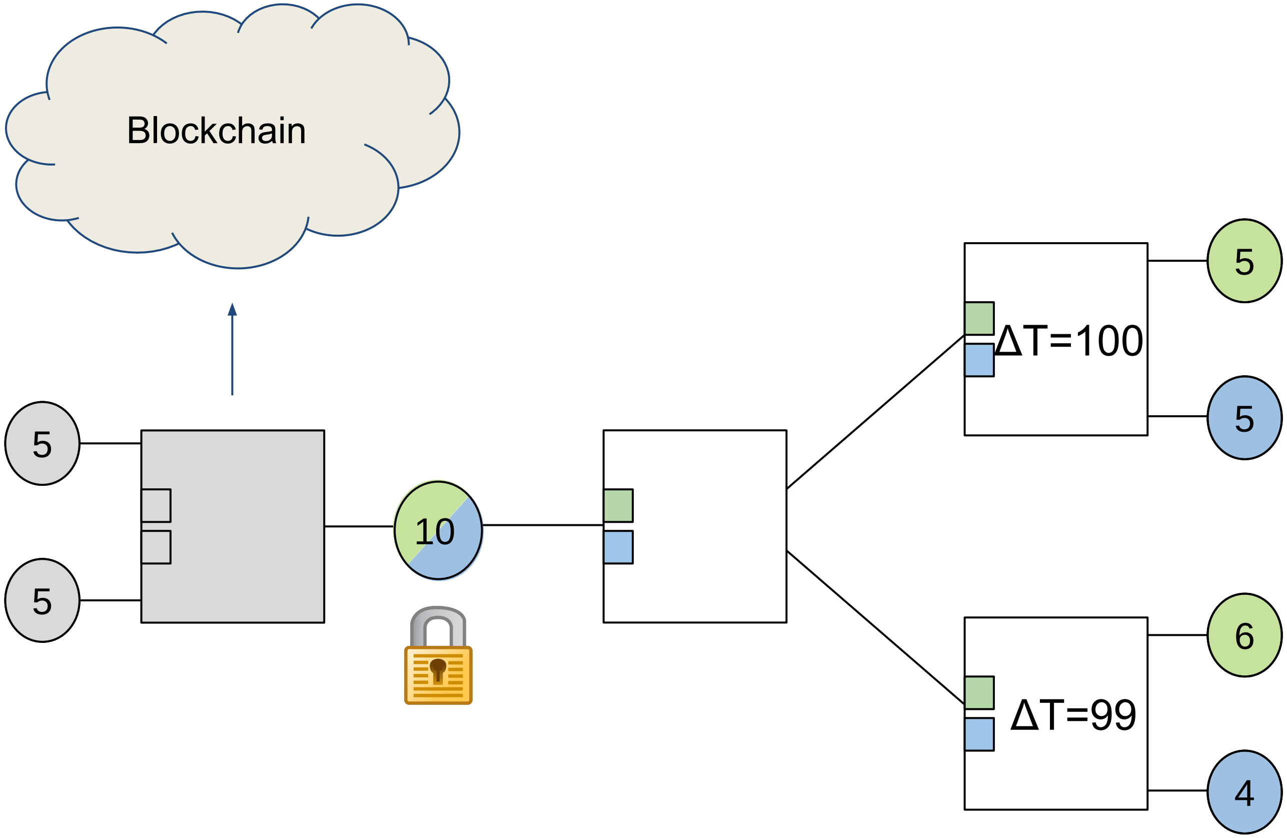
[Decker,W,2015]

# Duplex Micropayment Channel



Channel must be renewed often?

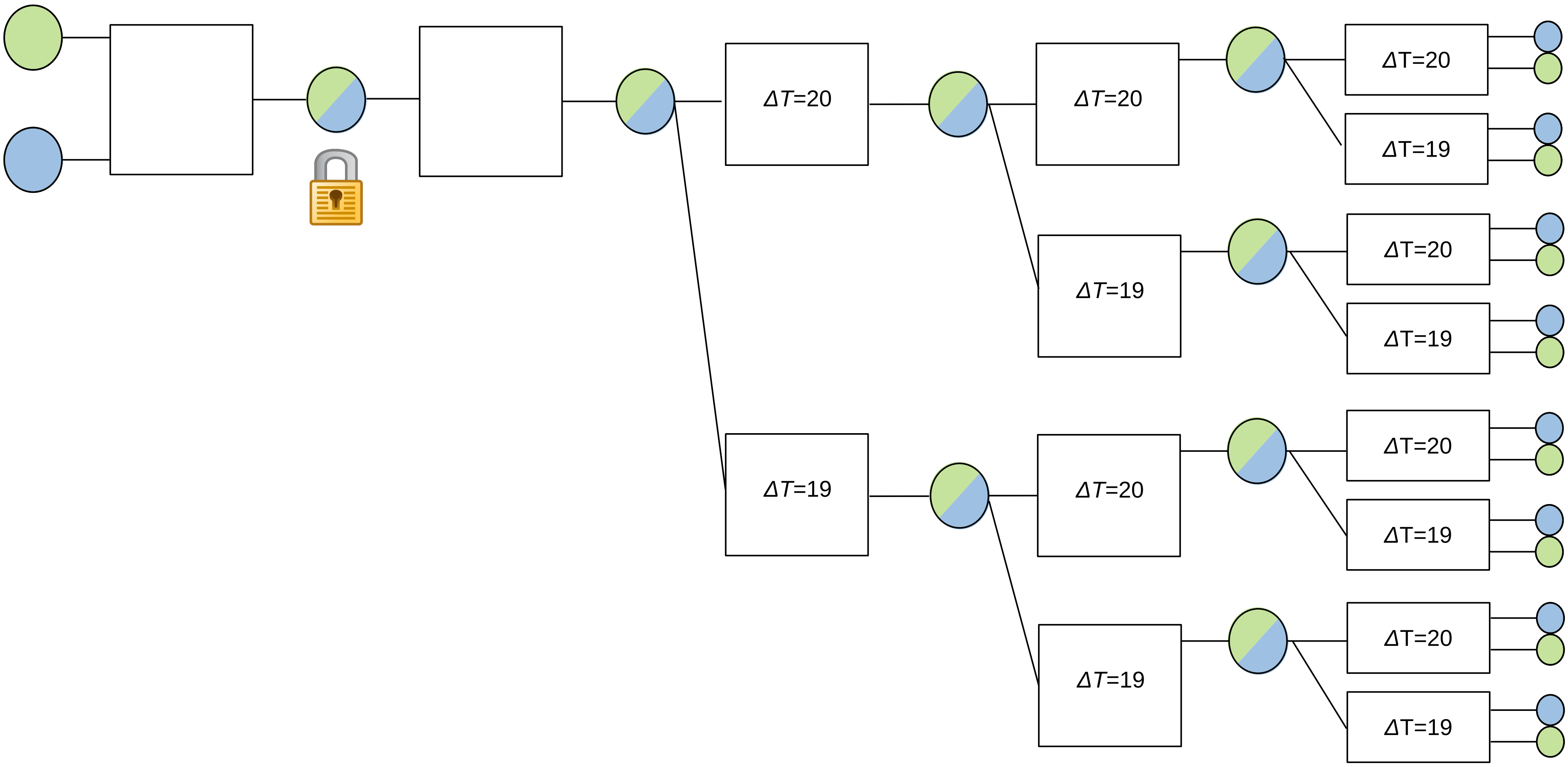
# Duplex Micropayment Channel



Relative timelocks to keep channel alive forever!

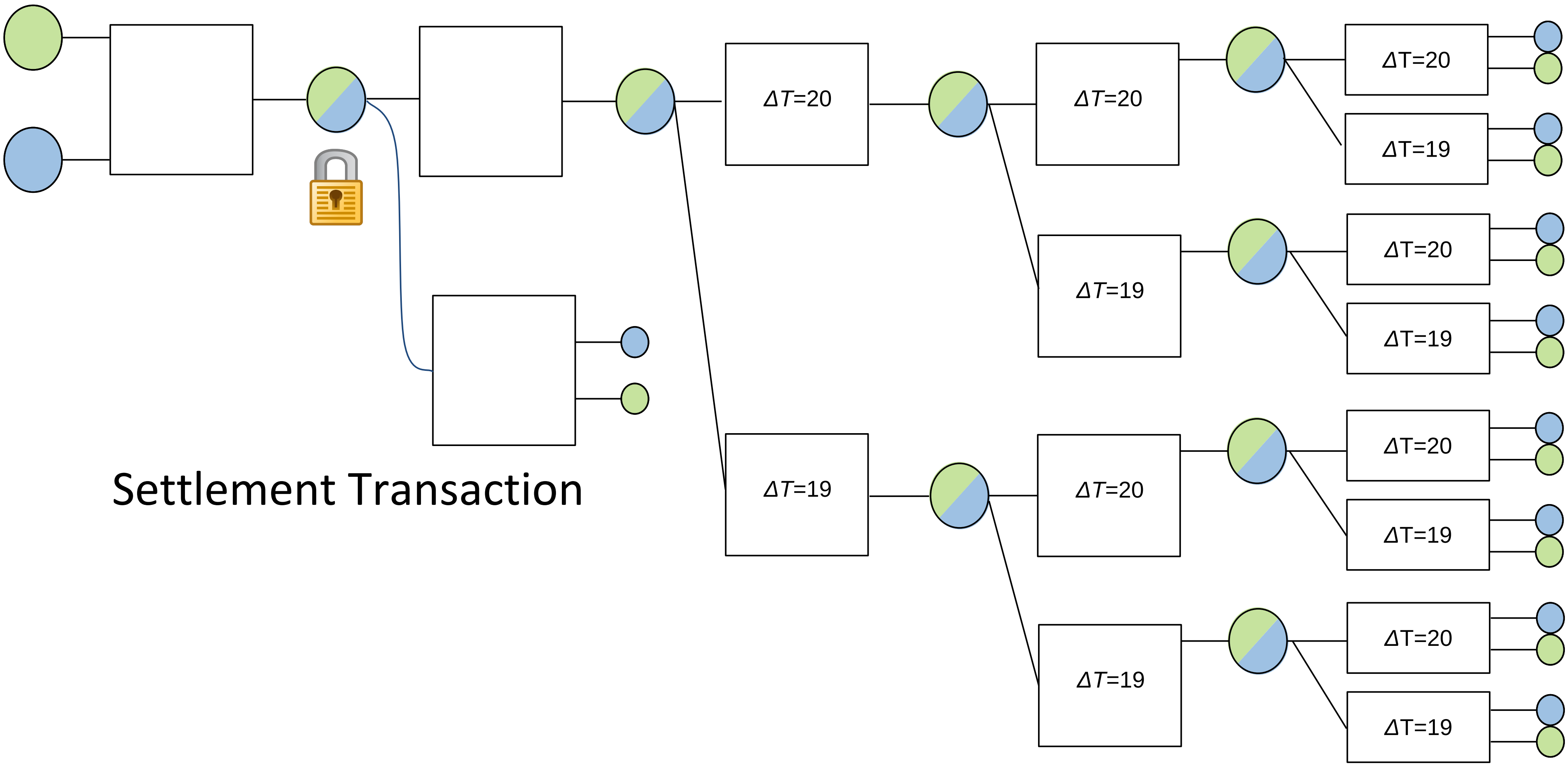
But only 99 transactions?

# Duplex Micropayment Channel



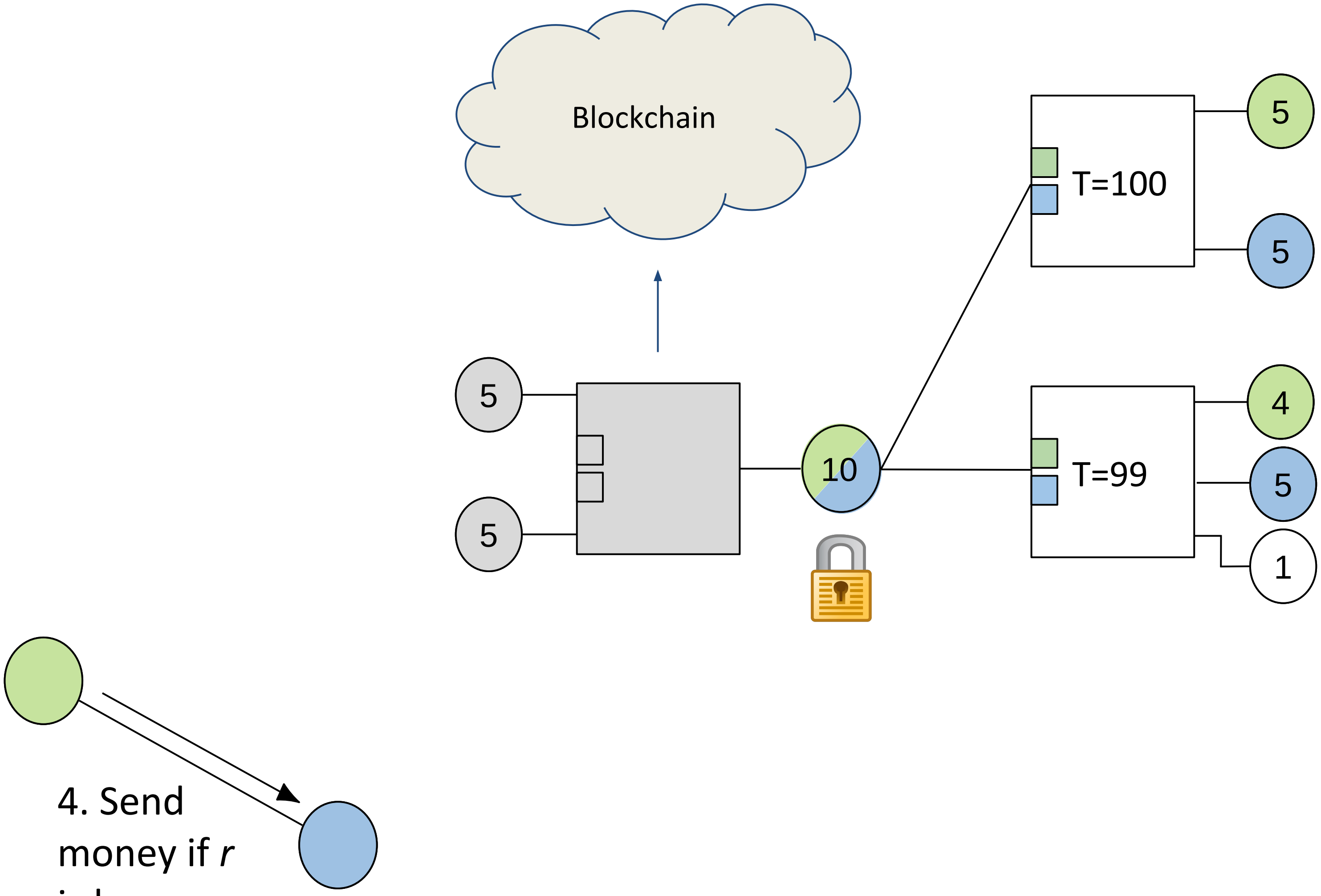
[Decker,W,2015]

# Duplex Micropayment Channel



Settlement Transaction

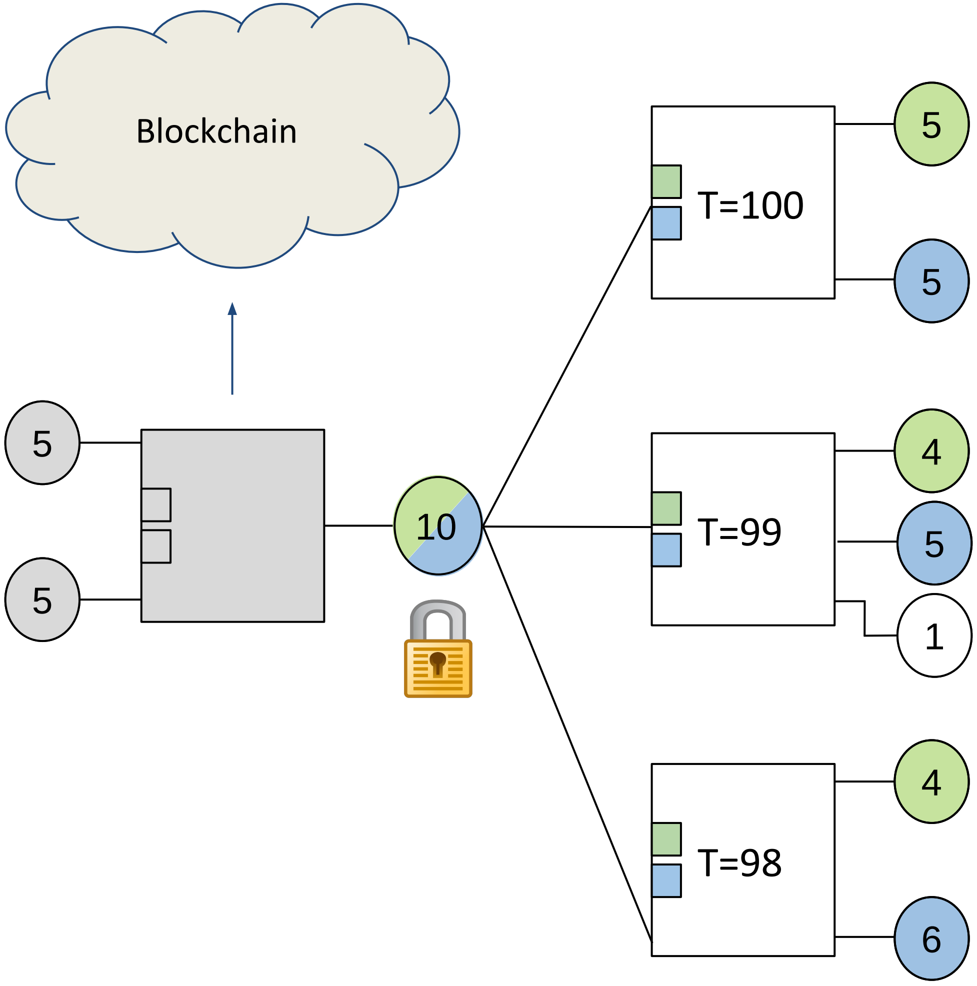
# HTLC Revisited



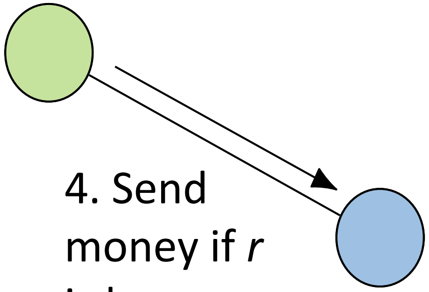
can be spent
by blue with secret *r* or
by green after 3 days

4. Send
money if *r*
is known
at time 3

# HTLC Revisited



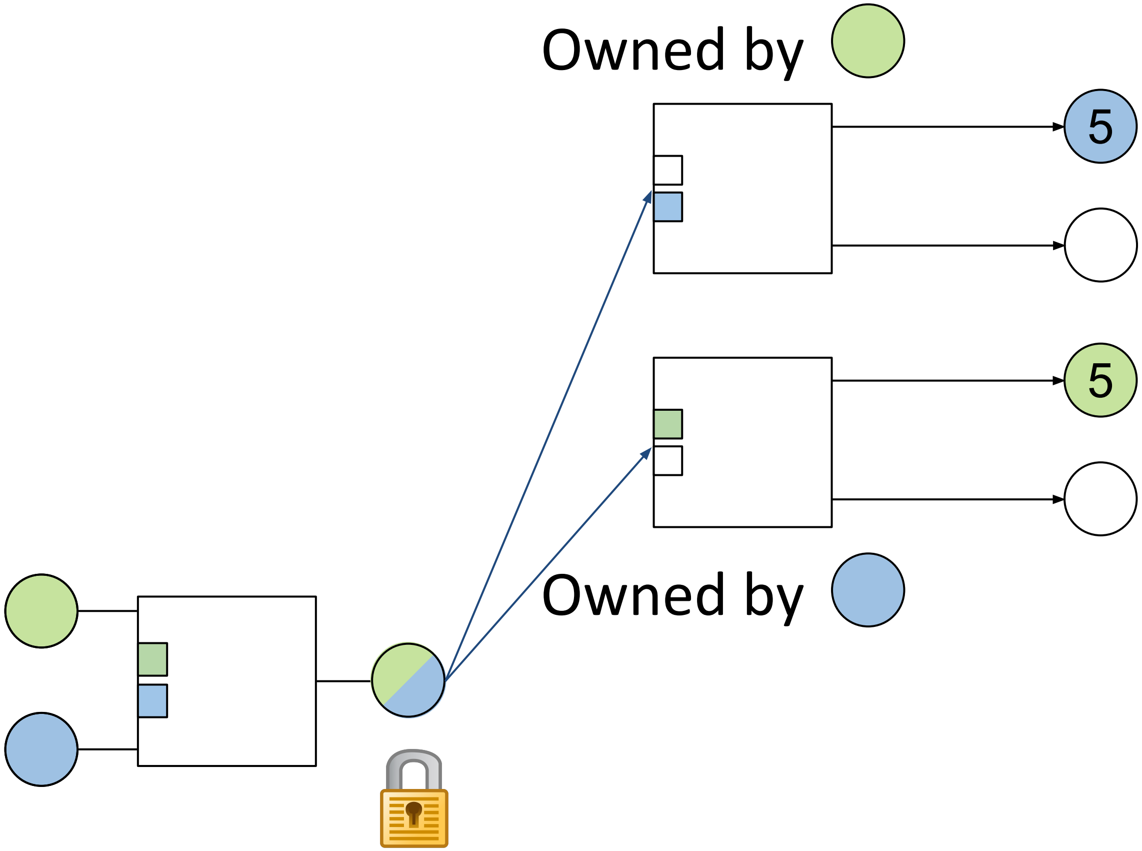
can be spent
by blue with secret *r* or
by green after 3 days



4. Send
money if *r*
is known
at time 3

# Lightning Network

# Lightning Network Channel



Owned by

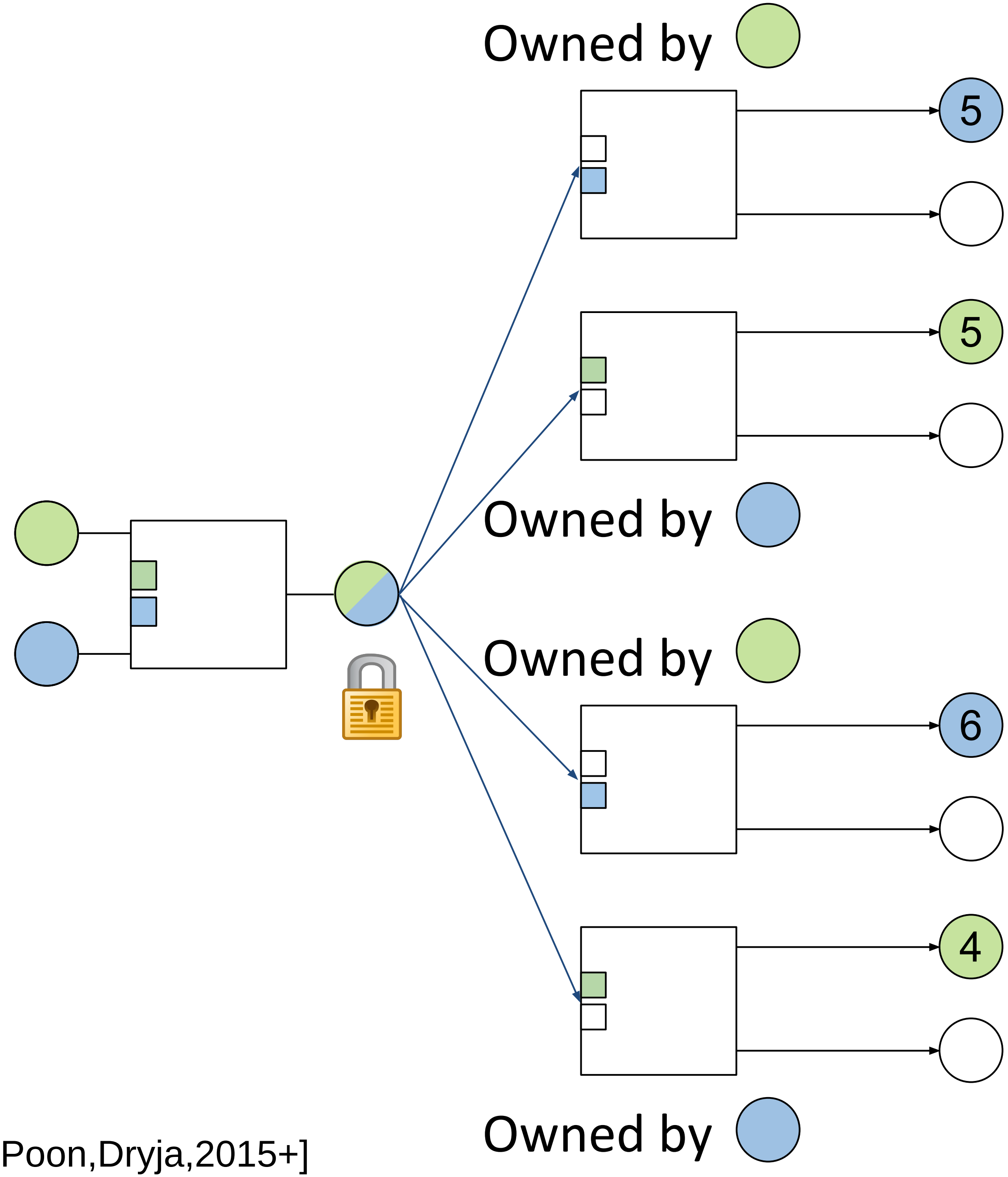
5 to green after 500 blocks or
5 to blue instantly with secret $s_g$

5 to blue after 500 blocks or
5 to green instantly with secret $s_b$

Owned by

[Poon,Dryja,2015+]

# Lightning Network Channel



Owned by 🟢

5 to green after 500 blocks or
5 to blue instantly with secret $s_g$

5 to blue after 500 blocks or
5 to green instantly with secret $s_b$

Owned by 🔵

Owned by 🟢

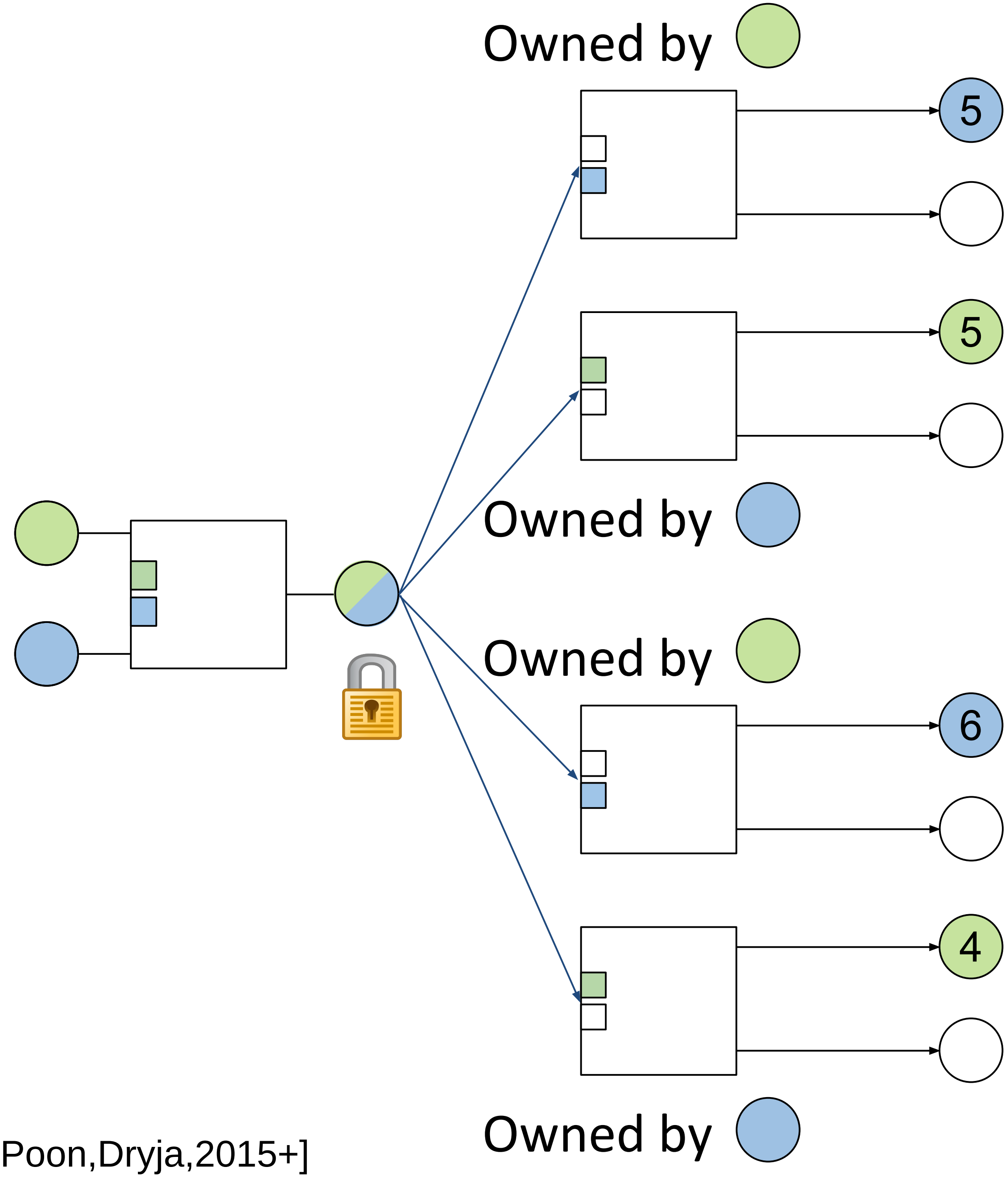
4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

Owned by 🔵

[Poon,Dryja,2015+]

# Lightning Network Channel



Owned by 🟢

5 to green after 500 blocks or
5 to blue instantly with secret $s_g$

5 to blue after 500 blocks or
5 to green instantly with secret $s_b$

Owned by 🔵

Owned by 🟢

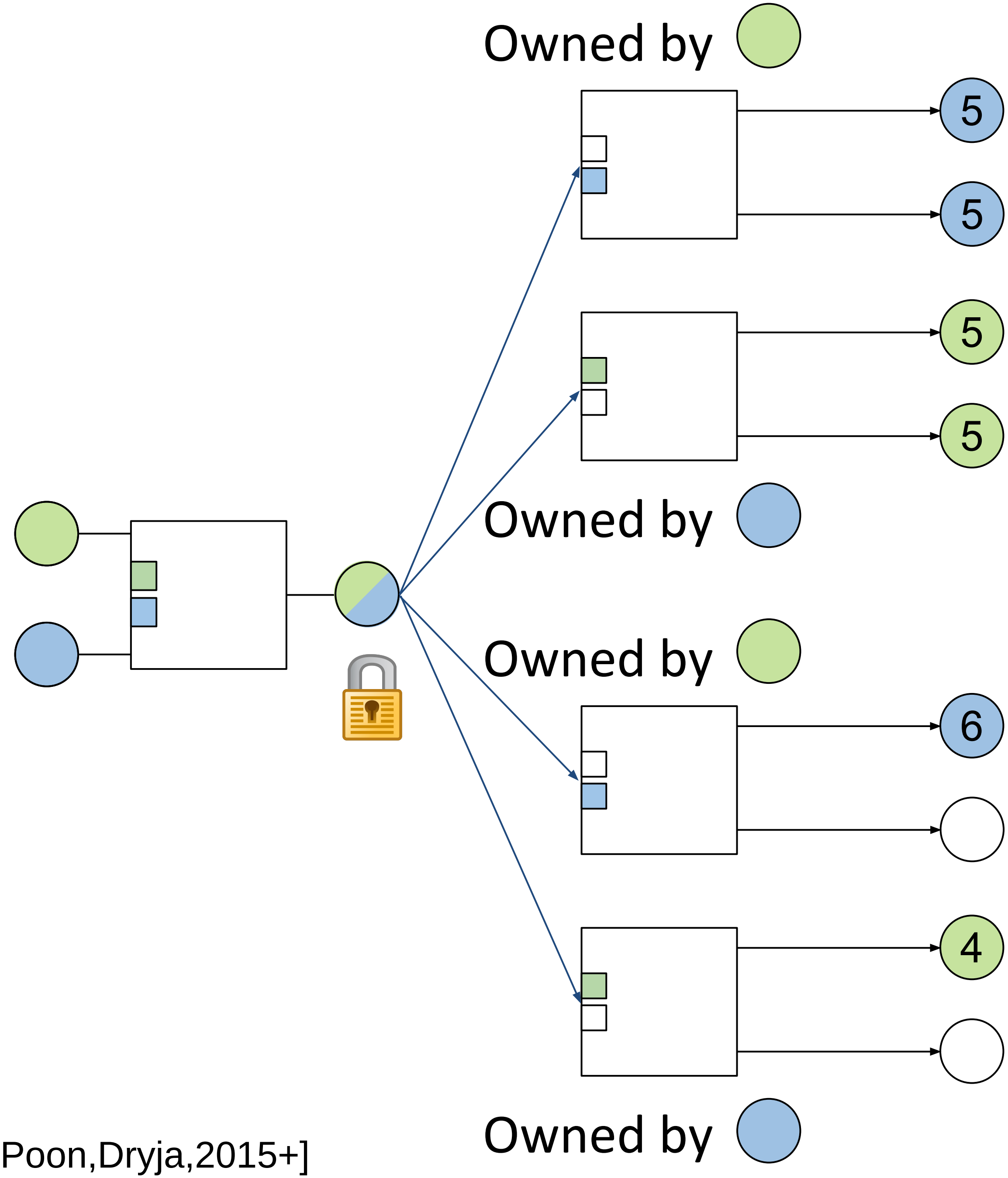
4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

Owned by 🔵

[Poon,Dryja,2015+]

# Lightning Network Channel



Owned by

Owned by

Owned by

Owned by

4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

[Poon,Dryja,2015+]

# Solved?

# Still Too Many Channels!?

# Each and Every Channel

… needs two transactions on blockchain

… has locked-in funds by both parties

# Each and Every Channel

… needs two transactions on blockchain

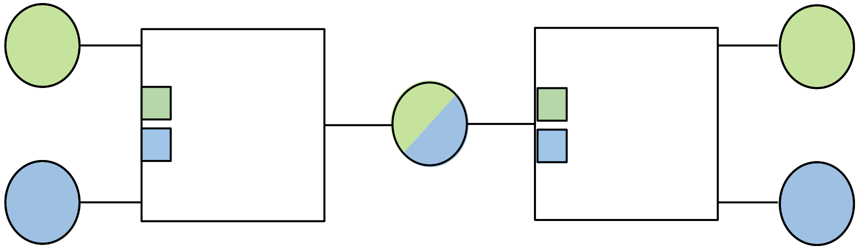
200-800M channels only

… has locked-in funds

all my bitcoins are locked-in… sad.

# Blockchain Space

Blockchain space ≅ number of signatures

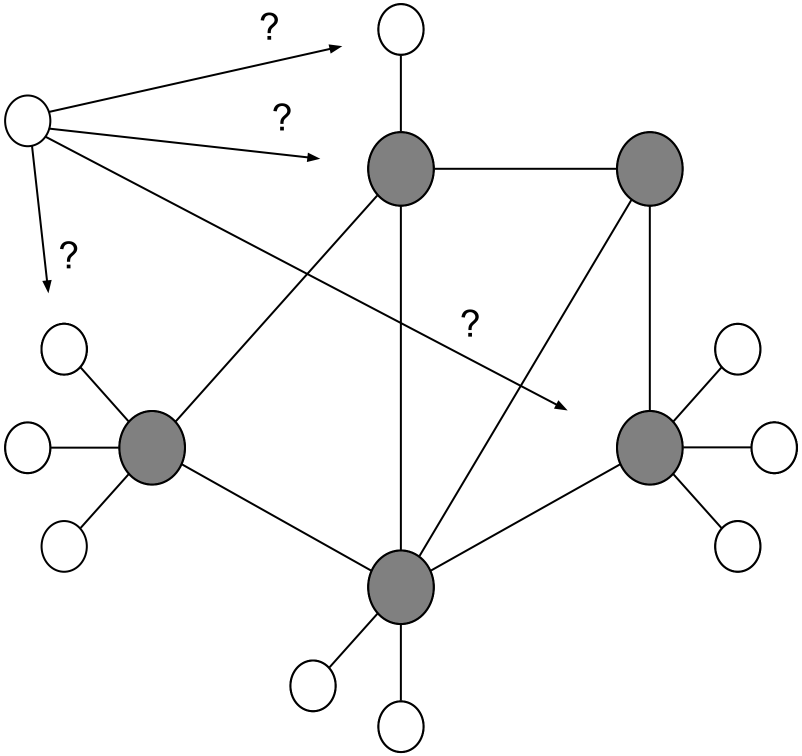


Funding

Settlement

so far 4 signatures
for every channel

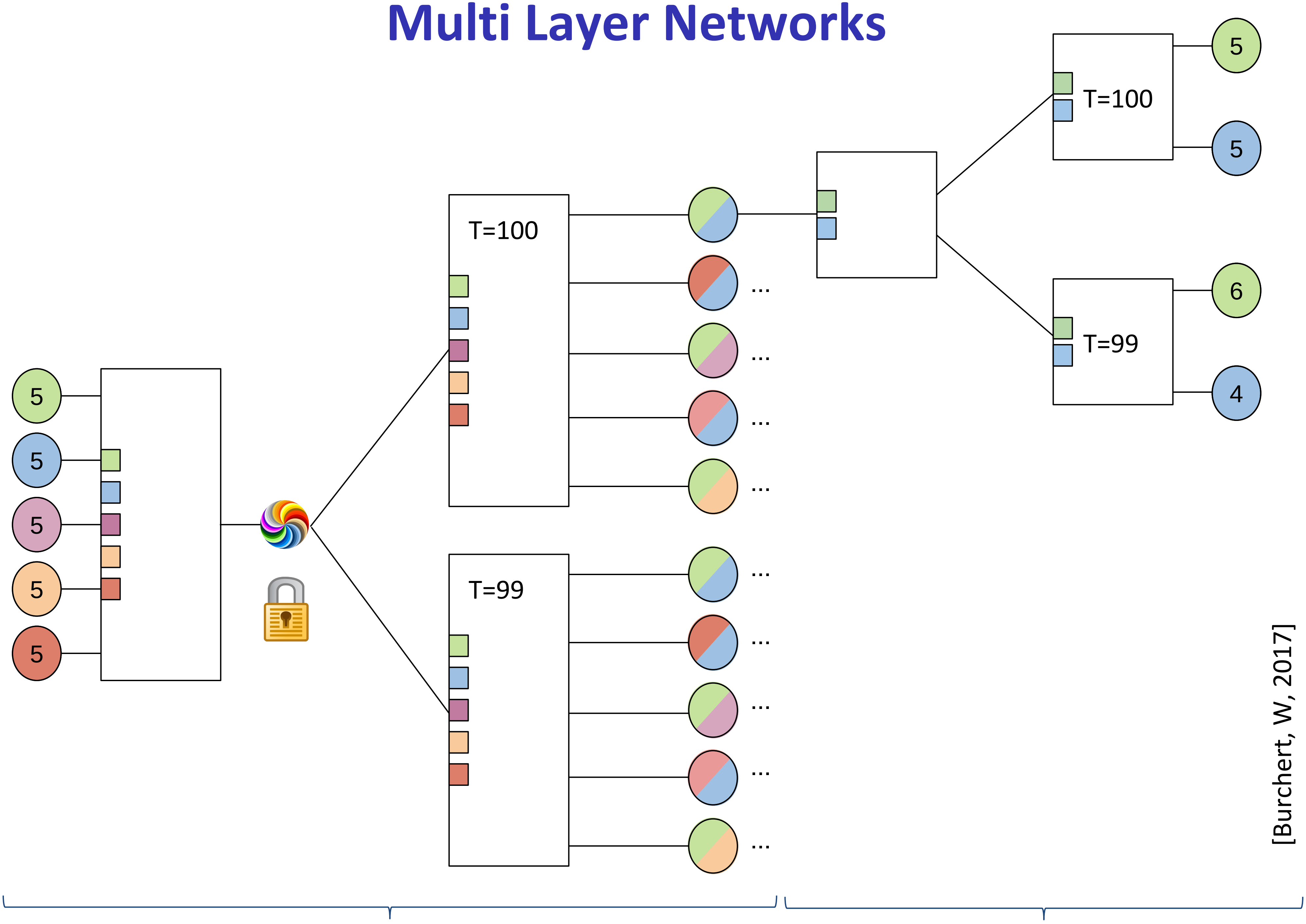
# Locked Funds



A node wants to make connections…

Where does it lock the funds?

# Multi Layer Networks

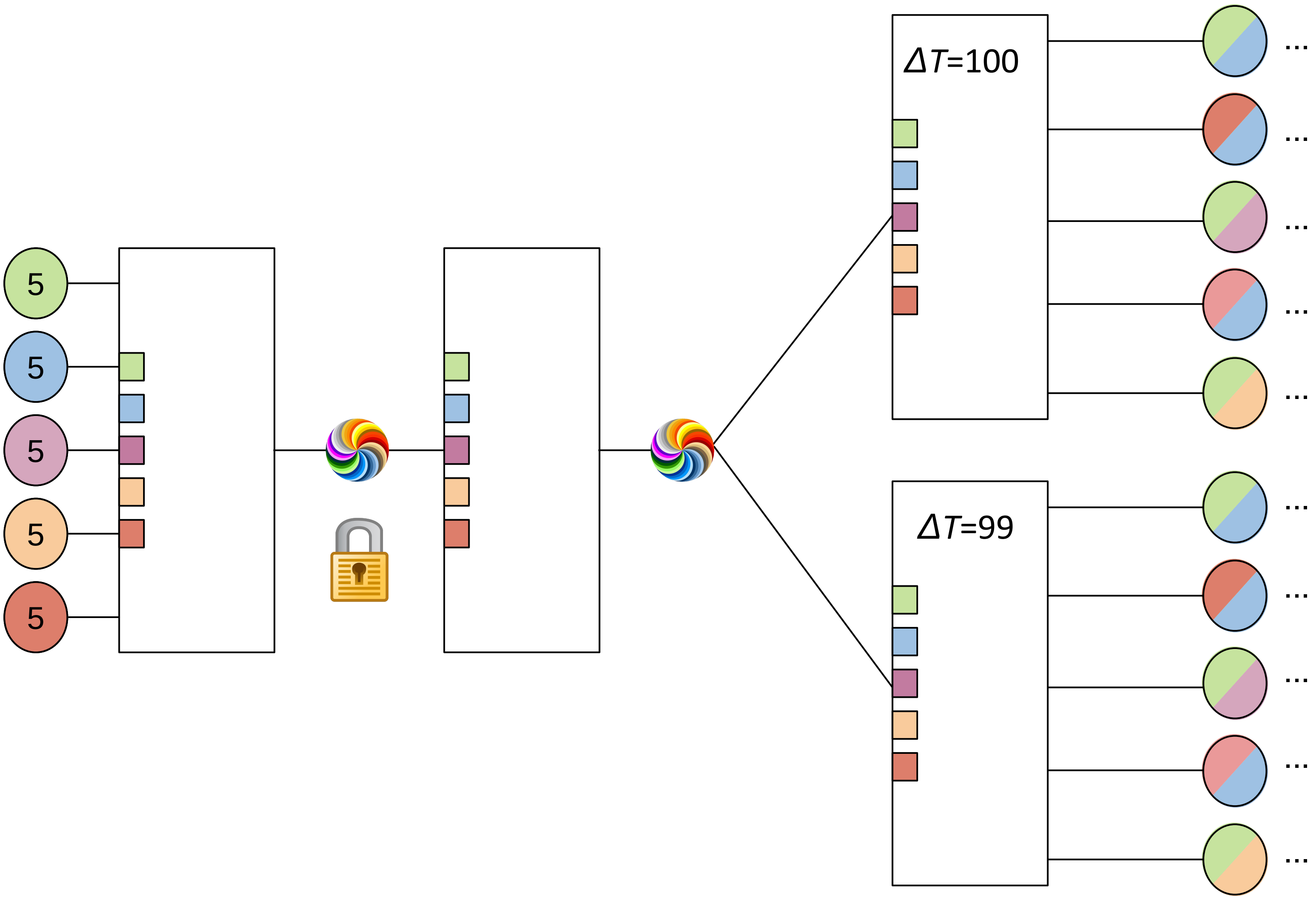


[Burchert, W, 2017]

Channel funding layer

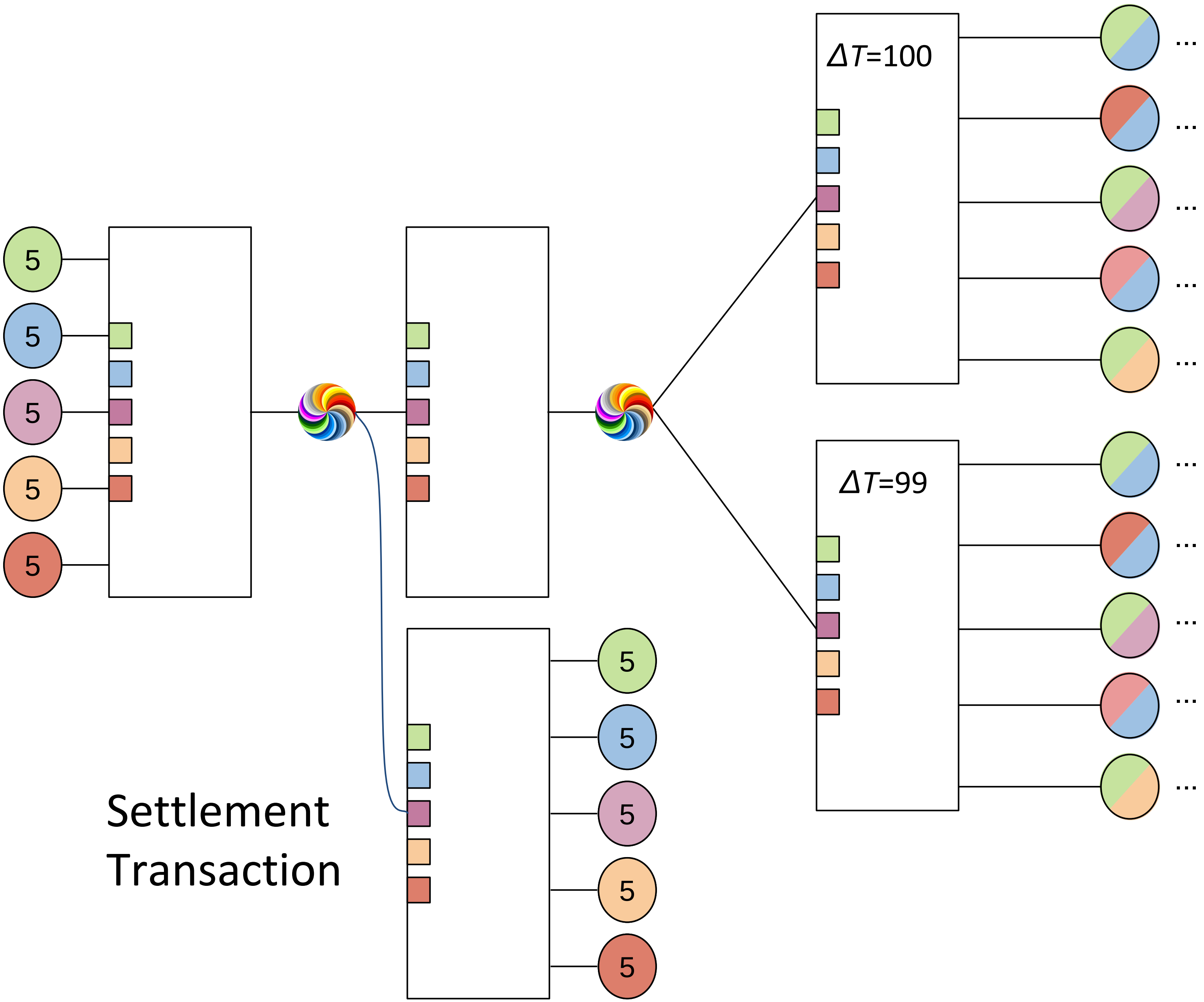
Payment network layer

# Multi Layer Networks



[Burchert, W, 2017]

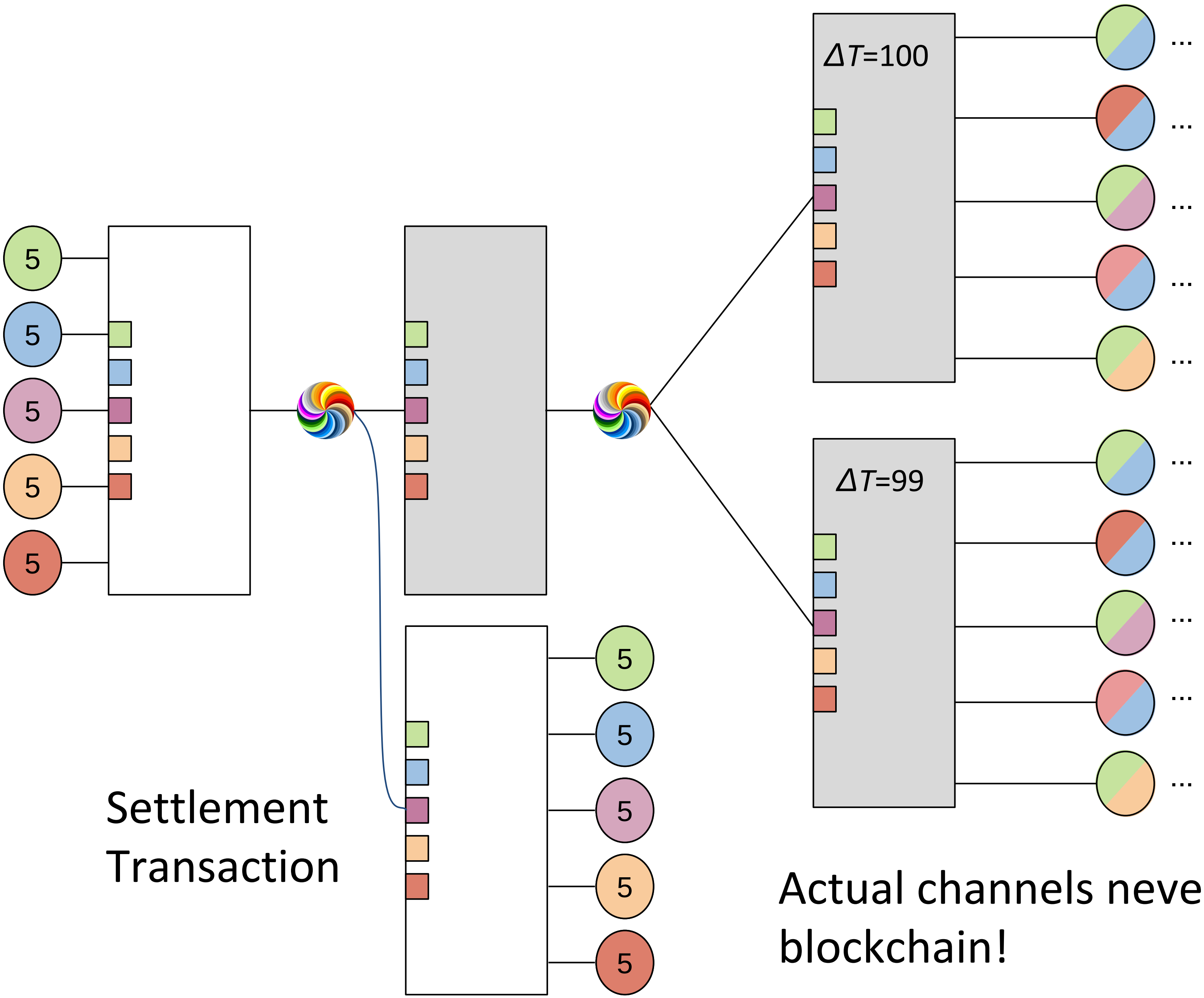
# Multi Layer Networks



Settlement
Transaction

[Burchert, W, 2017]

# Multi Layer Networks



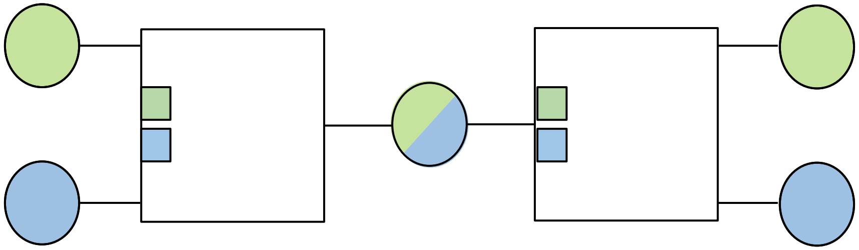
Settlement Transaction

Actual channels never reach the blockchain!

[Burchert, W, 2017]

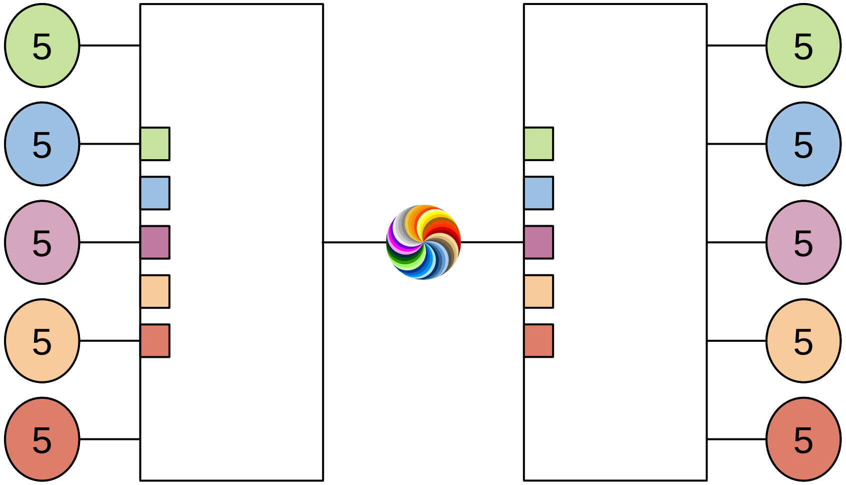
# Blockchain Transactions

old



4 signatures per channel

new

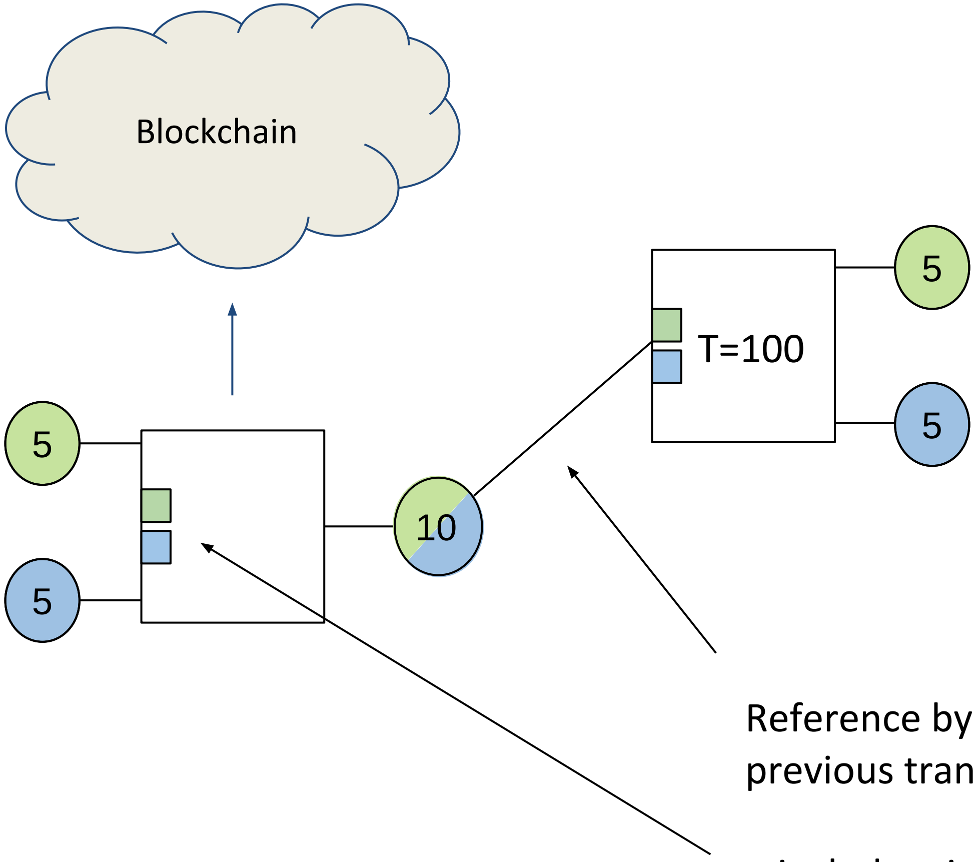


2 signatures per user

independent of channels

# What Else is Needed?

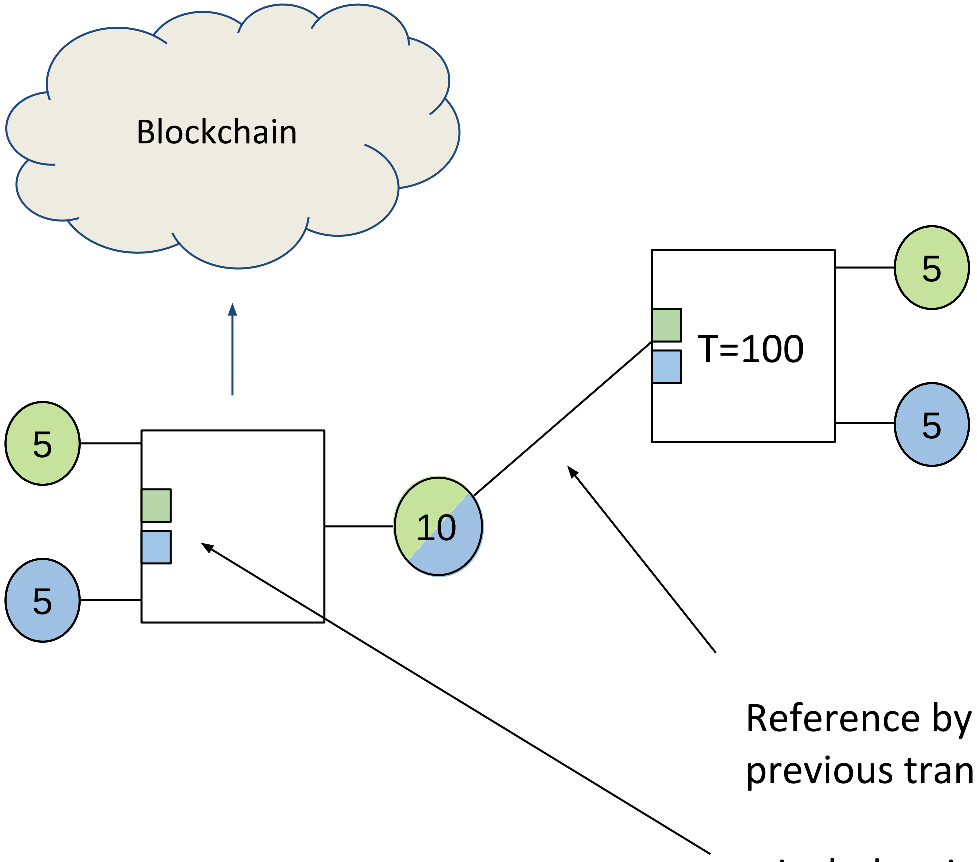
# Spending from Unsigned Transactions



Reference by Transaction ID: Hash of previous transaction…

...includes signatures!

# Spending from Unsigned Transactions



Reference by Transaction ID: Hash of previous transaction…

...includes signatures!

We need to move the signatures out of the transaction ID!

# Are We Finally Done?!?

*“Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks. This confirmed the presence of transactions which need to be examined more closely*

# The MtGox Incident

- July 2010: First trade on MtGox
- 2011: Transaction malleability identified as low priority issue
- February 7, 2014: MtGox halts withdrawals
- February 10, 2014: MtGox cites transaction malleability as root cause
- February 28, 2014: MtGox files for bankruptcy

MtGox claims that 850,000 bitcoins (620 million USD) were lost due to transaction malleability.

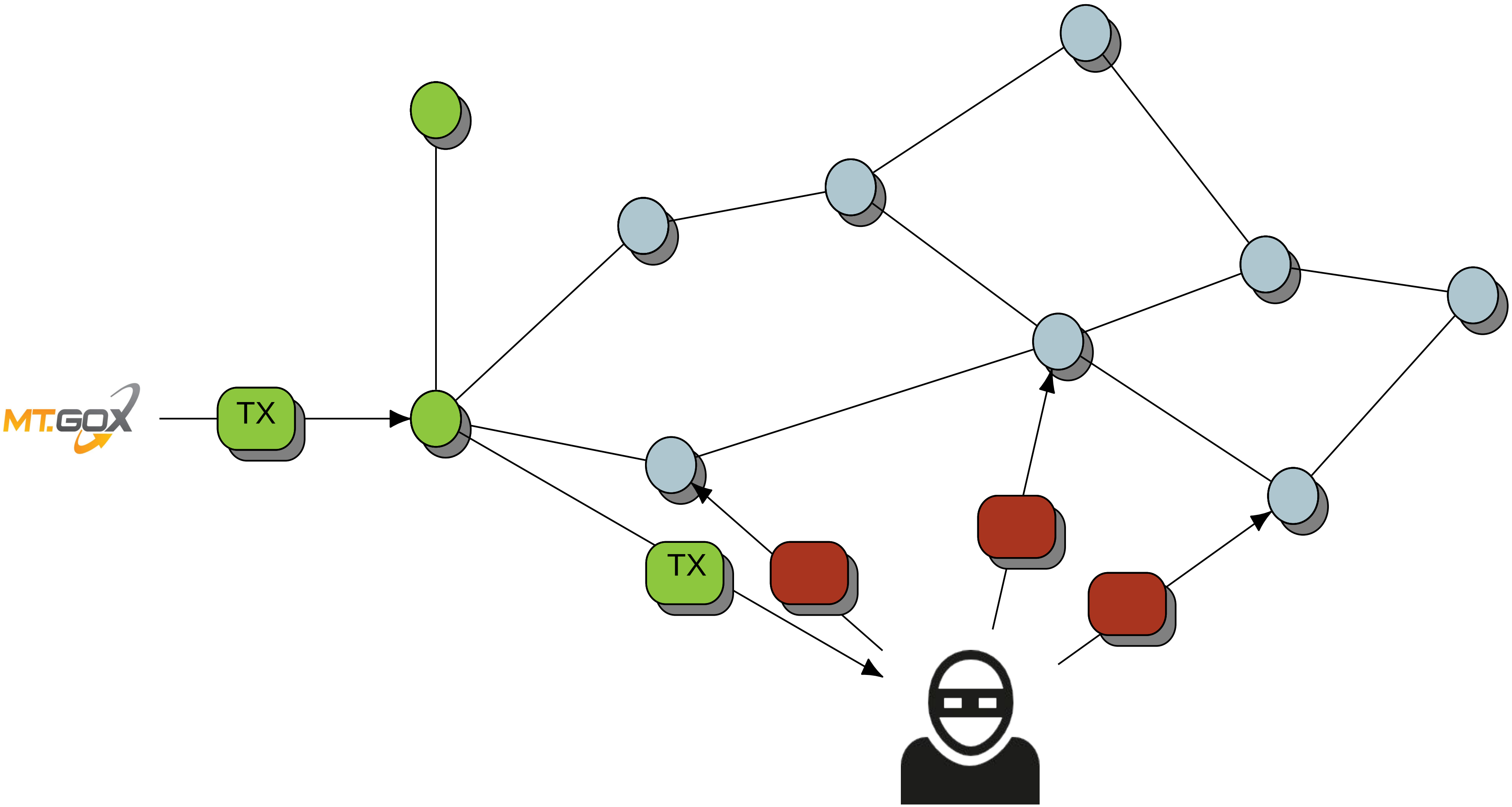
# Signatures

**0000 61afbb4de9f8b874861e**

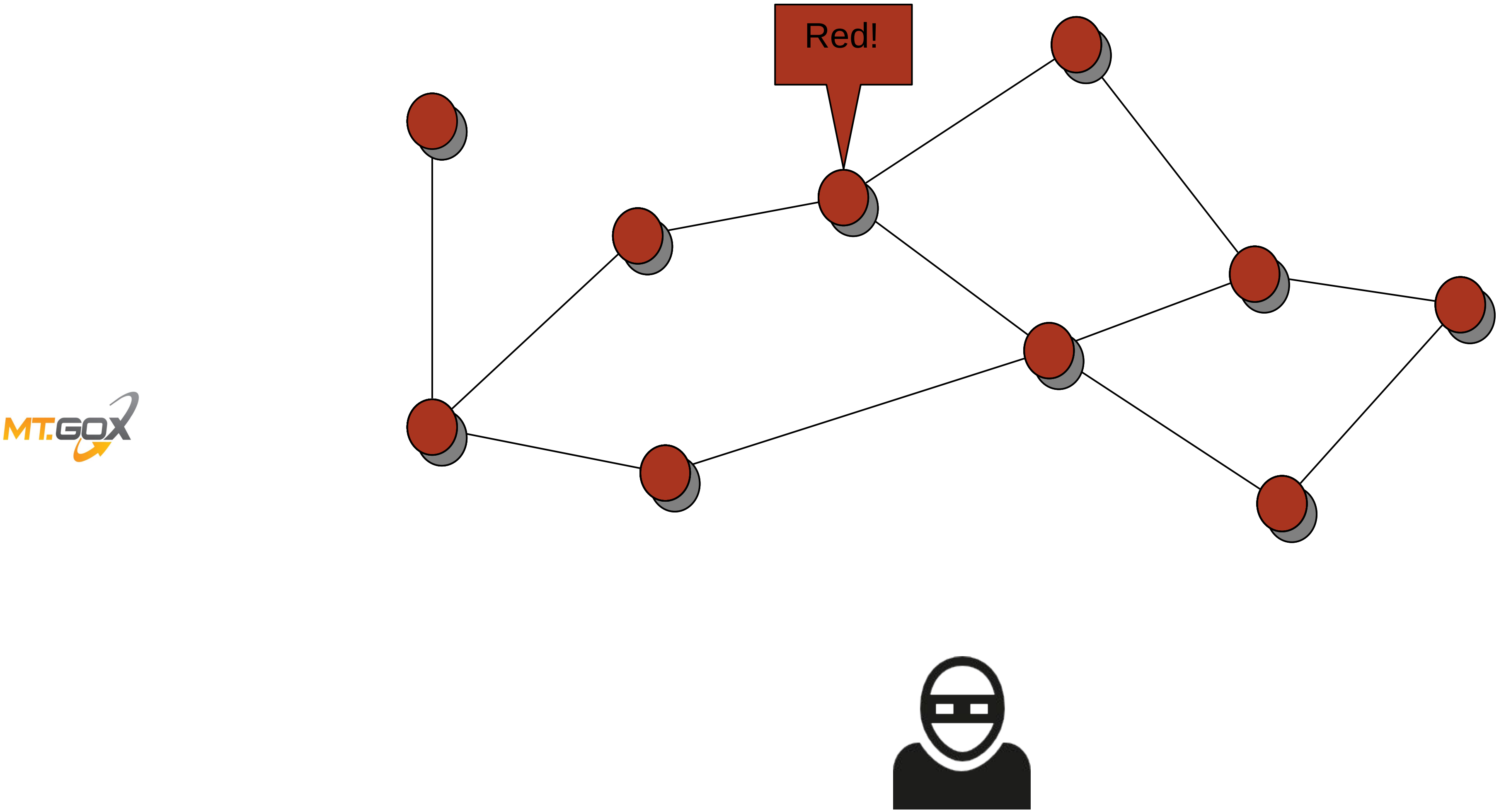
There are multiple ways to serialize a signature:

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

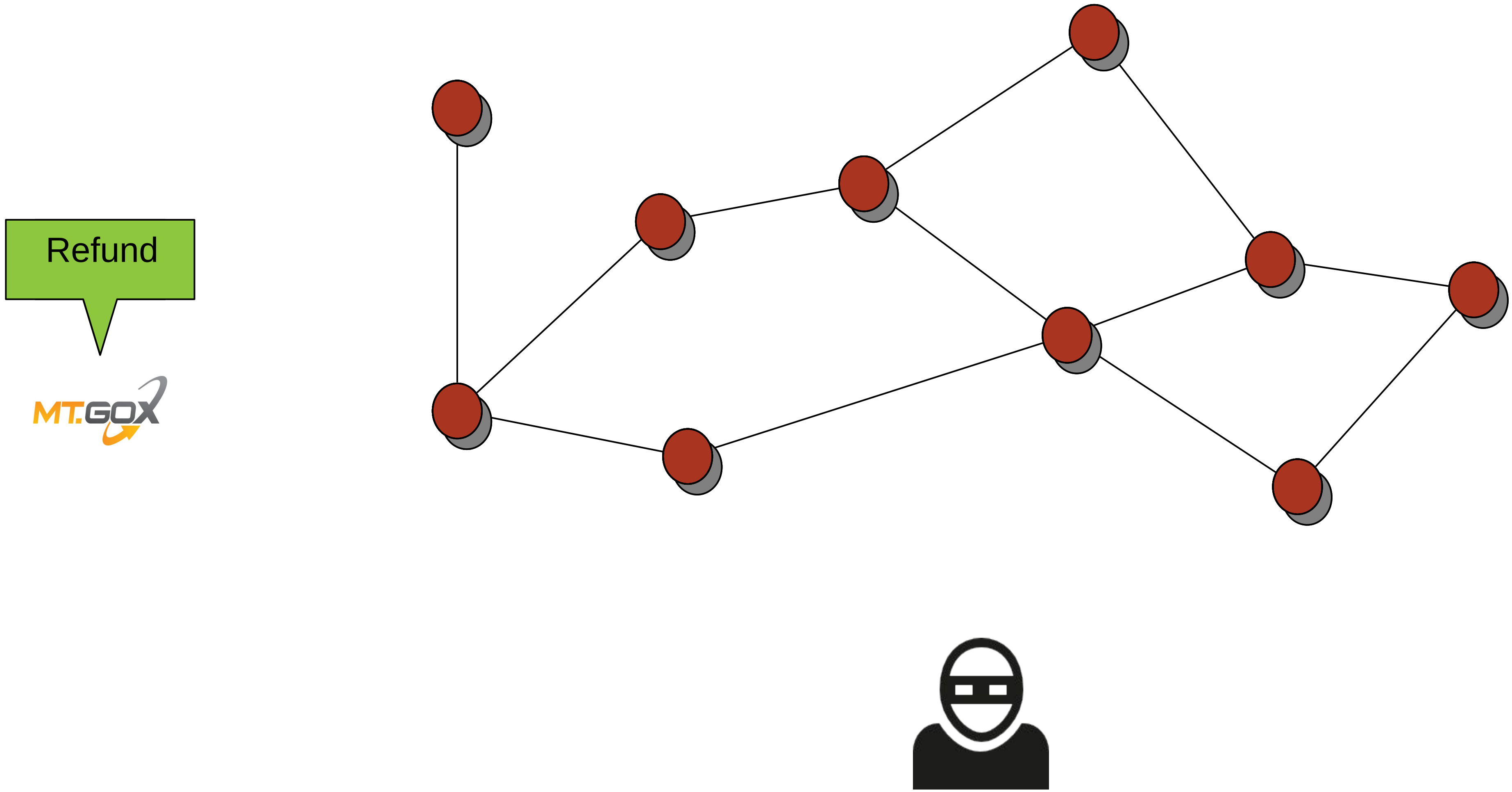
# Transaction Malleability Attack



# Transaction Malleability Attack

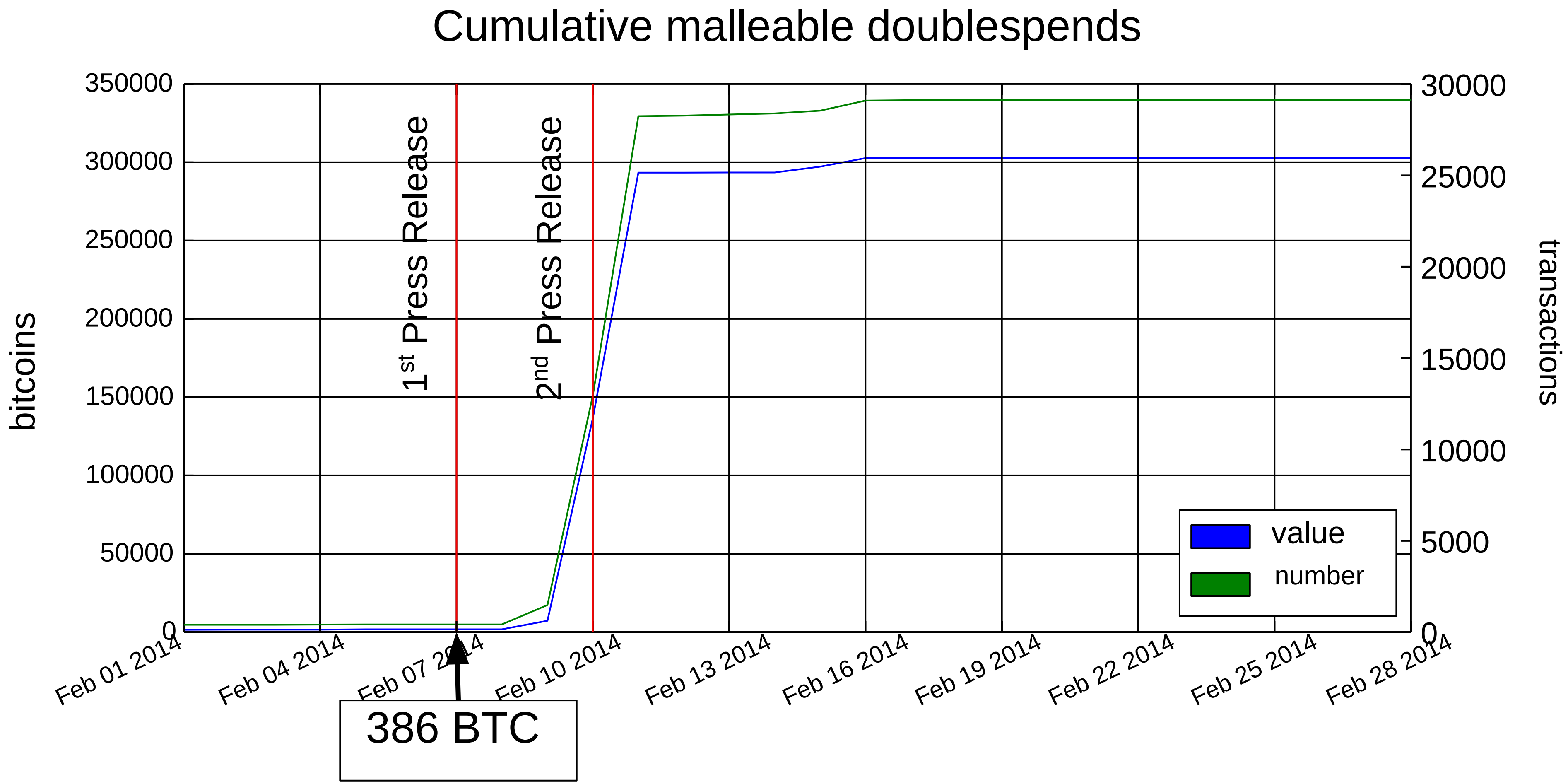


# Transaction Malleability Attack

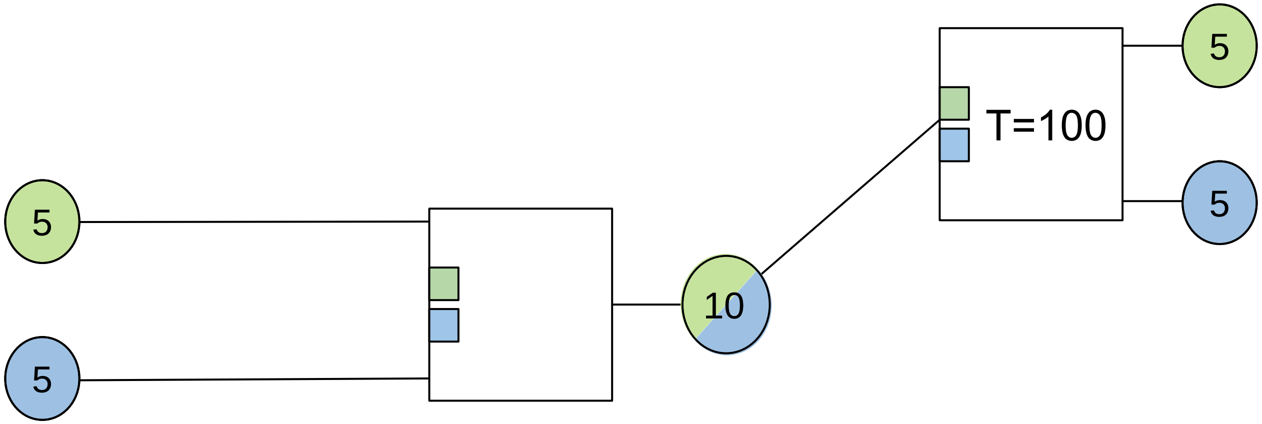


Refund

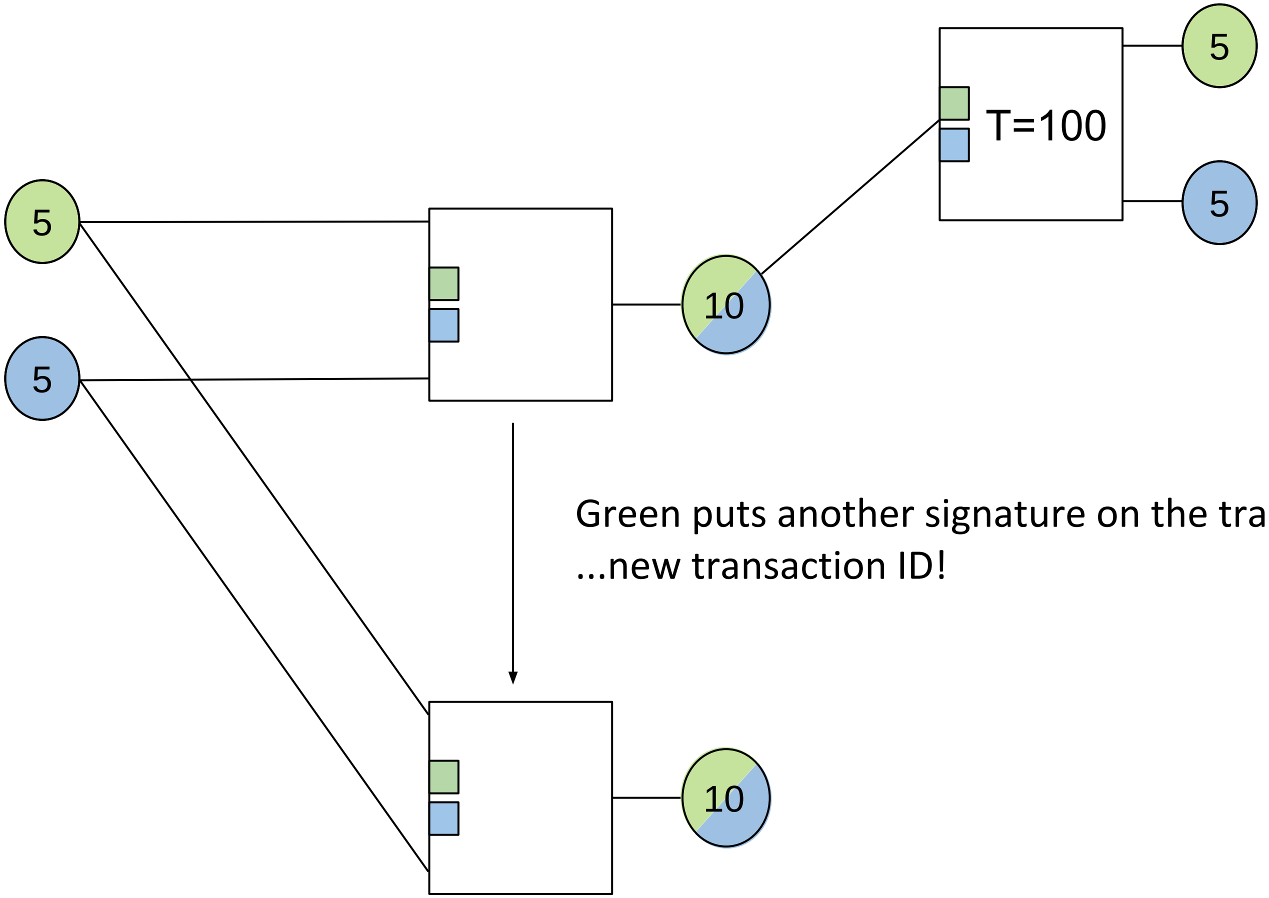
# Incident Timeline



# Malleability

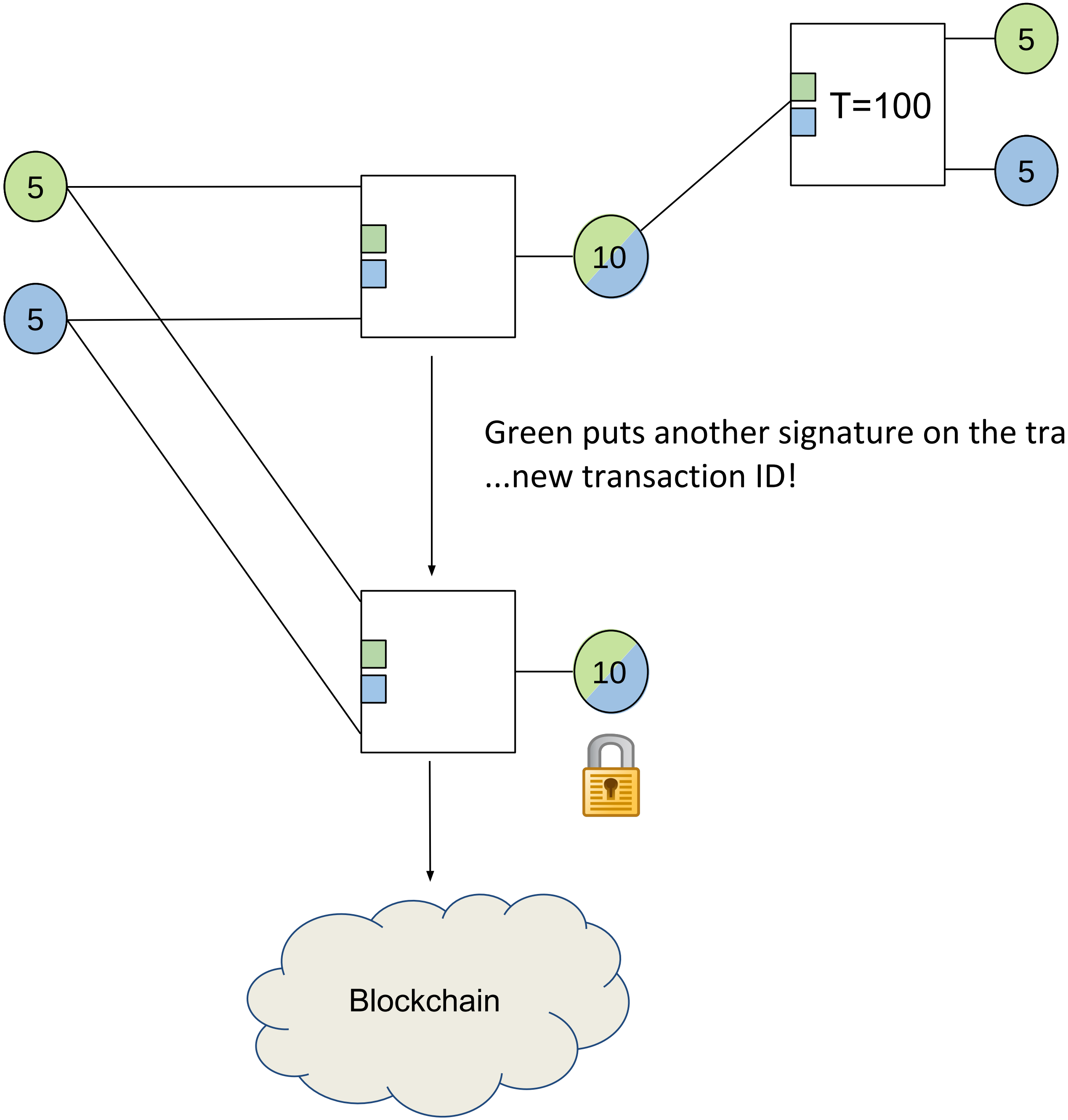


# Malleability



Green puts another signature on the transaction…
...new transaction ID!

# Malleability



Green puts another signature on the transaction…
...new transaction ID!

# How is this fixed?

# Segregated Witness

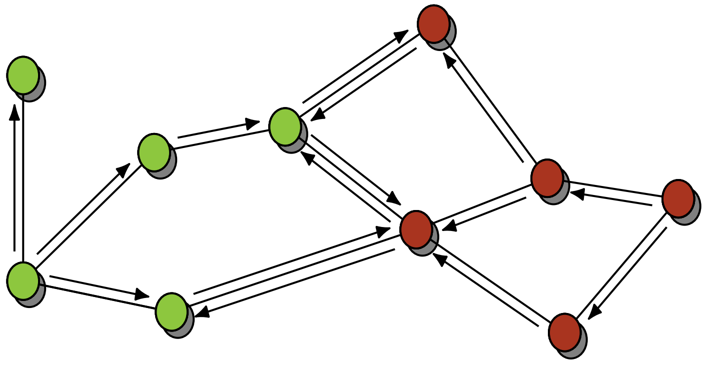
Introduce a new type of transaction

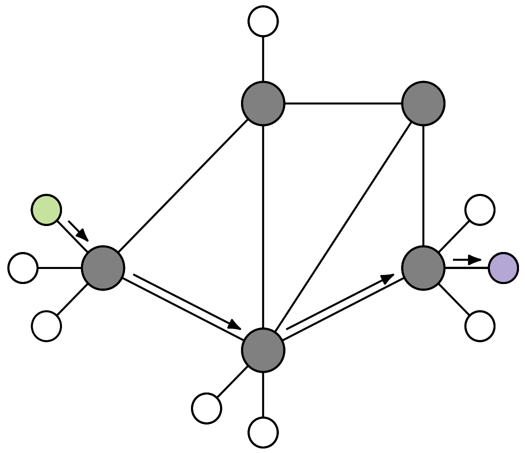
Signatures are separated from the rest

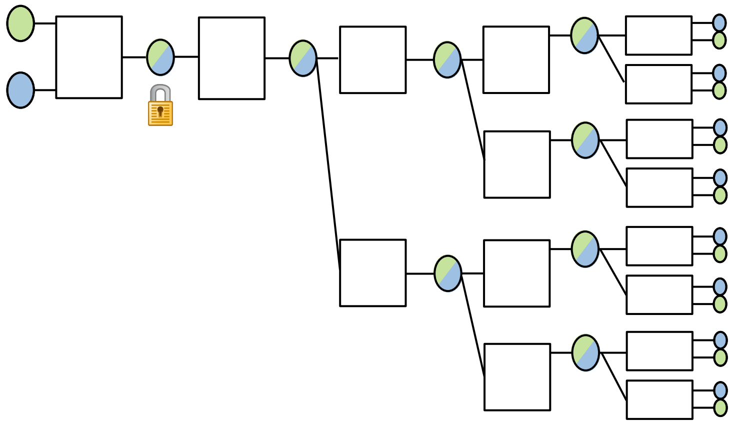
Softfork compatible

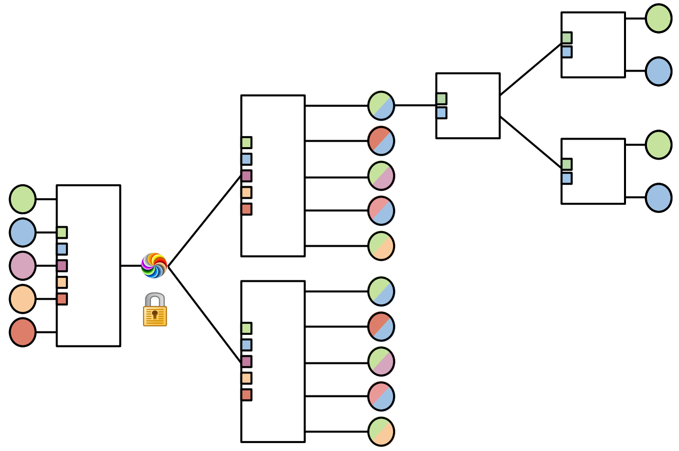
Became active as BIP 141 in August 2017

# Summary









*Thank you!*

# Questions?

Thanks to
Christian Decker
Conrad Burchert

# Softforks vs Hardforks

## Softfork

- Old miners accept blocks of the new miners
- New miners reject some blocks

-> If new miners are majority, everyone mines on the same chain

## Hardfork

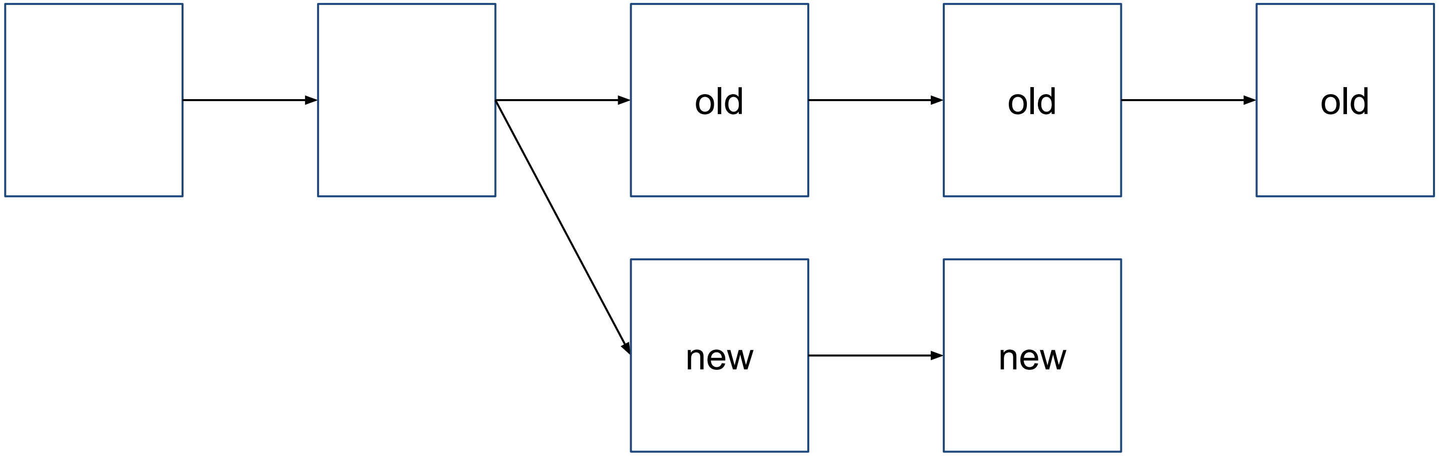
- New miners reject old blocks
- Old miners reject new blocks

-> Two blockchains exist

# Softforks

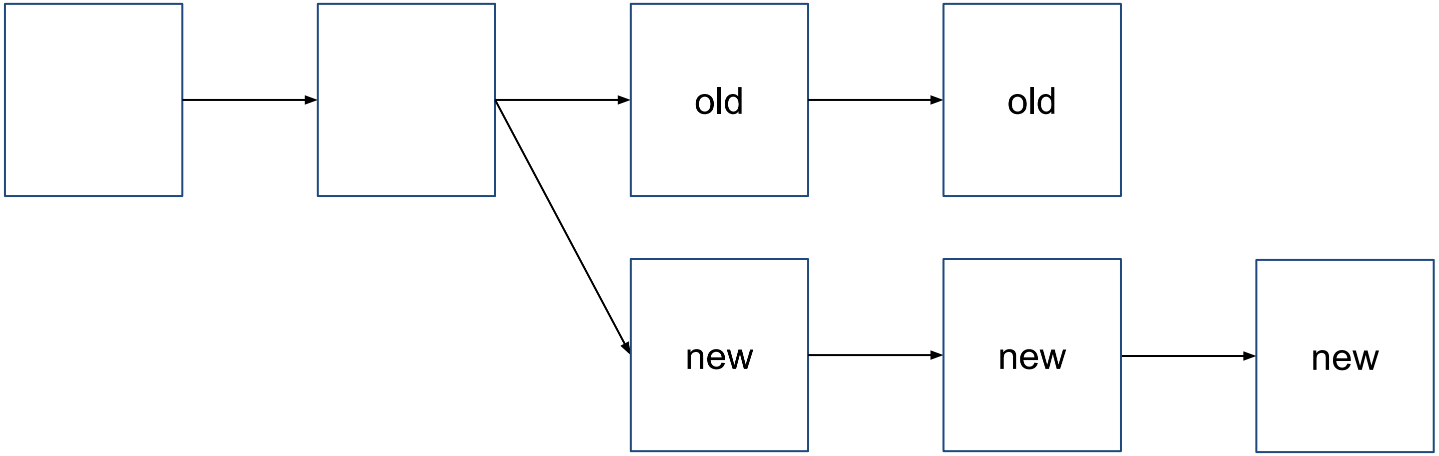
Old miners accept blocks of the new miners

Old miners are majority



Everyone switches here

New miners are majority

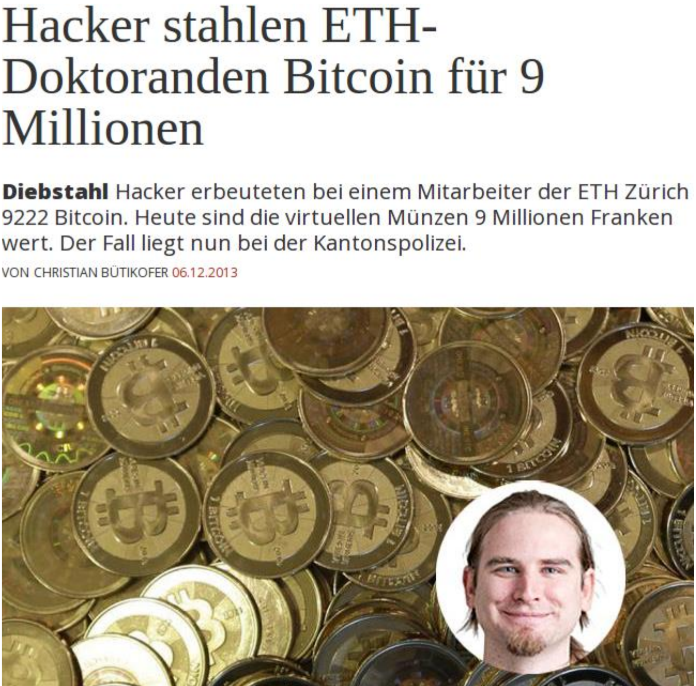


Everyone switches here

# *Economy and Other Problems*

*Roger Wattenhofer*

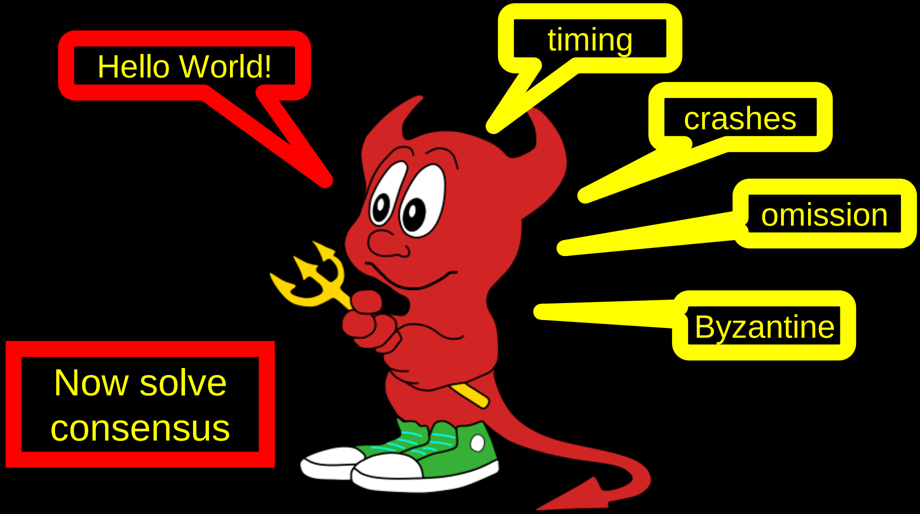
(Thanks to Maurice Herlihy for some colorful slides)



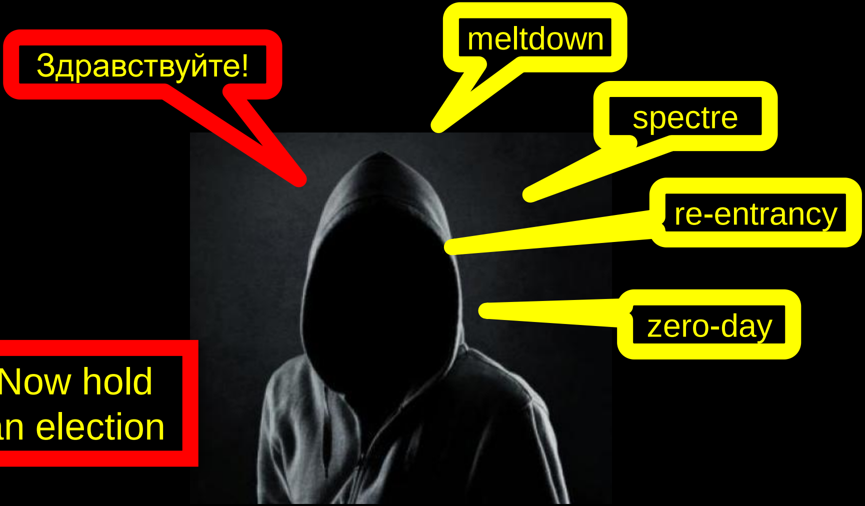
# Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

**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



Classical Adversary



Now hold
an election

Modern Adversary

# The Market

- Cryptocurrencies are a new asset class, worth >$100B
  - Hundreds of currencies
- $1.4B invested in startups, as of Jan 2017
- Billions of value in ICOs
- Black Hats Meet White Hats
  - Dark net market operators & Bank of England at the same conferences
- Social movement
  - Hodlgang!

# Hype

“First practical solution to a longstanding problem in computer science, Byzantine Generals.”

“Satoshi solved a problem that academic computer scientists thought was impossible”

“Bitcoin is digital gold, it will put us back onto a sound monetary policy”

“Bitcoin will end wars”

# … and Criticism

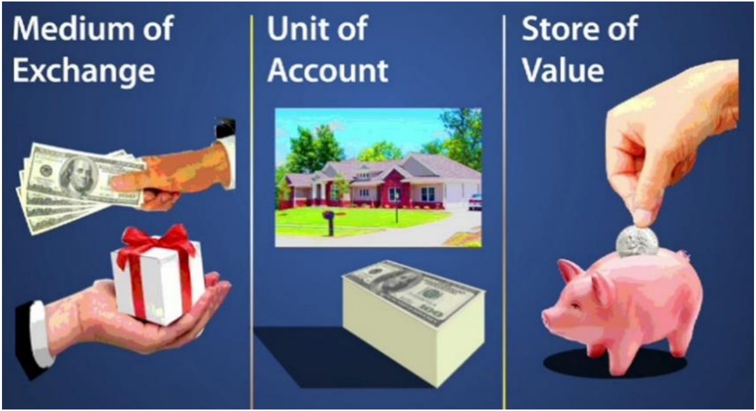
“A non-deliberate Ponzi scheme”

“It’s yet another eventually consistent database”

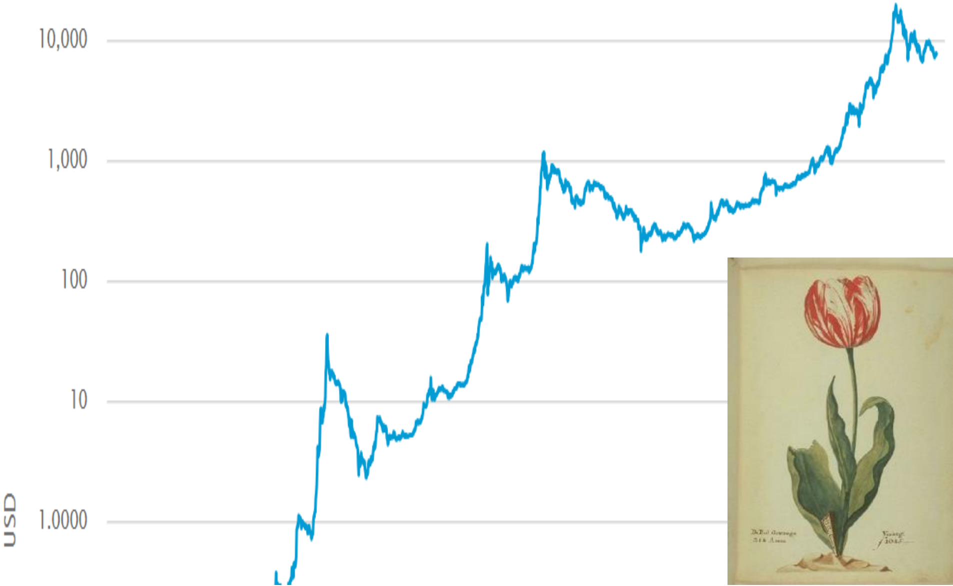
“Flawed technology, inherently limited in scale and performance”

“Unlikely to impact the finance sector”

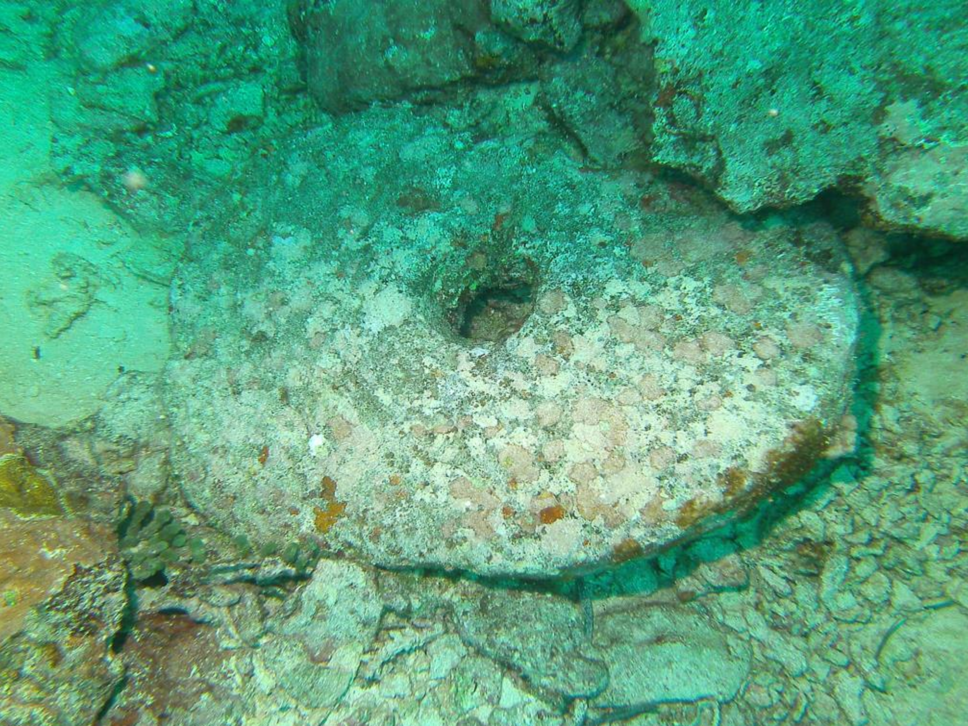
# What is Money?



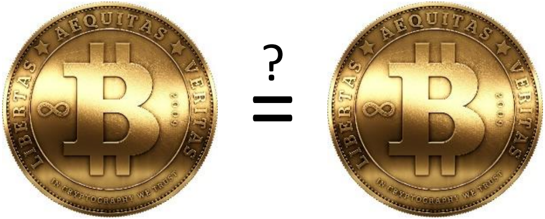
# BTC in USD

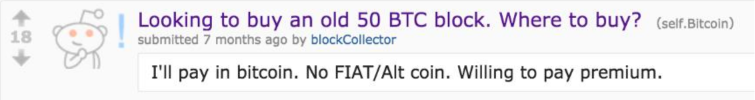


Kantonalbank
Banque Cantonale
500 g
Fine Gold
999,9
21152
DEGUSSA
FEINGOLD
999,9
1000 g
G 820
250g
Fine Gold
999,9
18722
ESSAYEUR FONDEUR
005719
999,9



# Fungibility



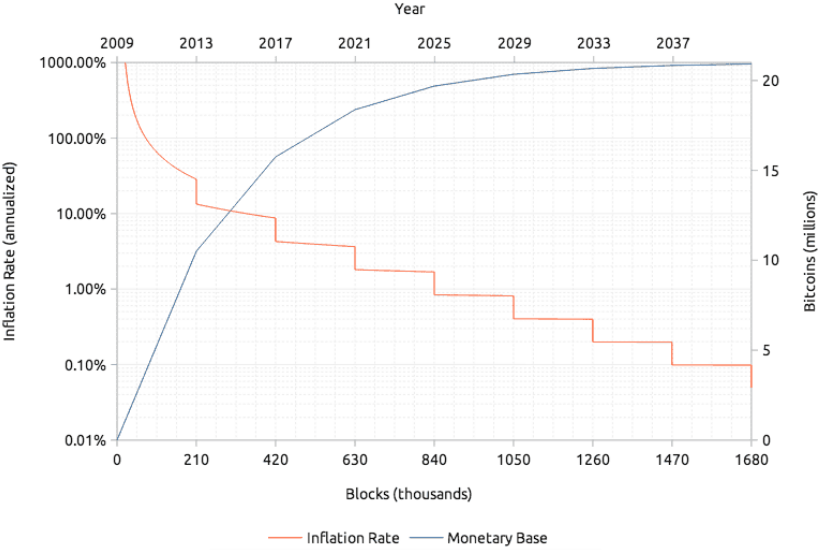

18

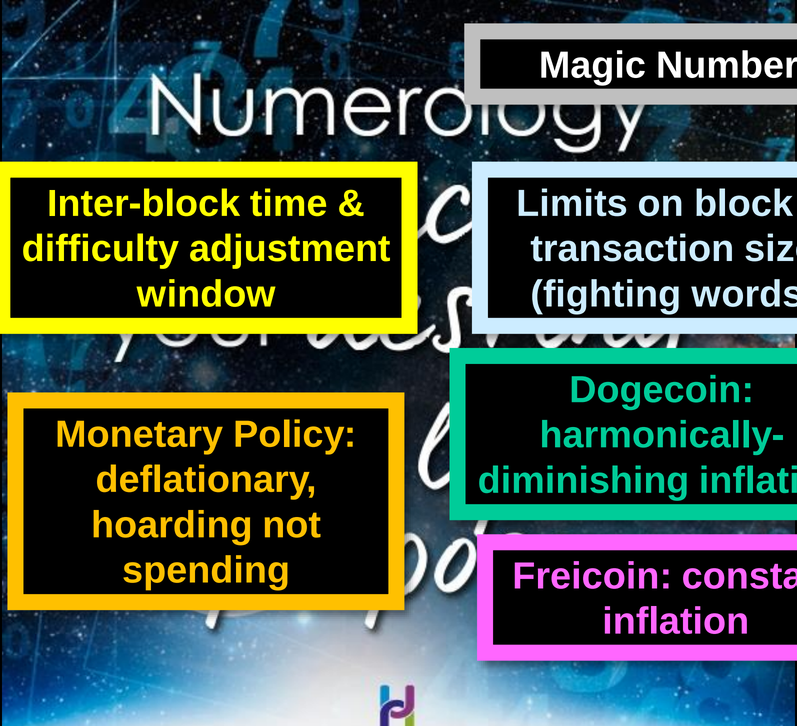
Looking to buy an old 50 BTC block. Where to buy? (self.Bitcoin)

submitted 7 months ago by blockCollector

I'll pay in bitcoin. No FIAT/Alt coin. Willing to pay premium.

# Inflation


Year
2009
2013
2017
2021
2025
2029
2033
2037
1000.00%
100.00%
10.00%
1.00%
0.10%
0.01%
Inflation Rate (annualized)
20
15
10
5
0
Bitcoins (millions)
0
210
420
630
840
1050
1260
1470
1680
Blocks (thousands)
Inflation Rate
Monetary Base



# Magic Numbers

Inter-block time & difficulty adjustment window

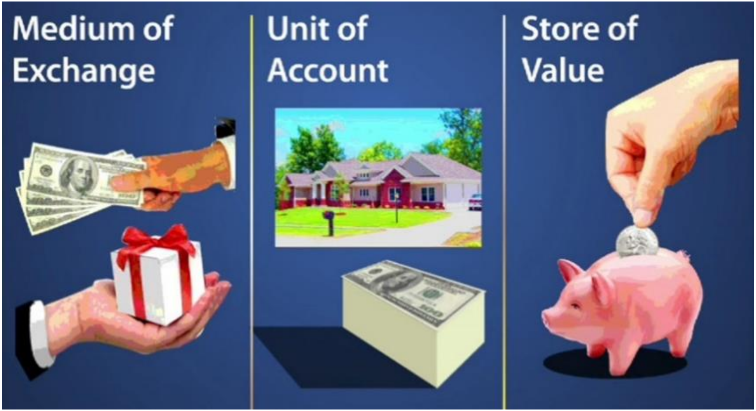
Limits on block & transaction size (fighting words)

Monetary Policy: deflationary, hoarding not spending

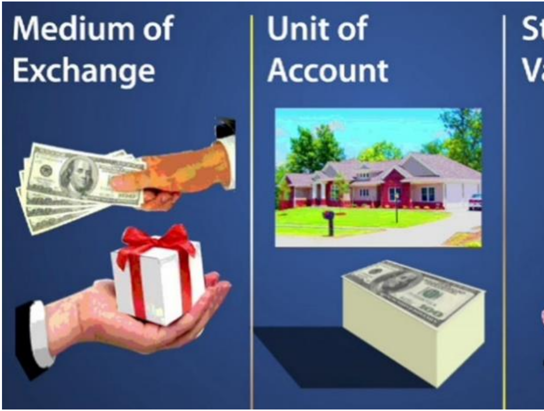
Dogecoin: harmonically-diminishing inflation

Freicoin: constant inflation

# What is Money?



# What is Money?



DEBT

THE FIRST 5,000 YEARS

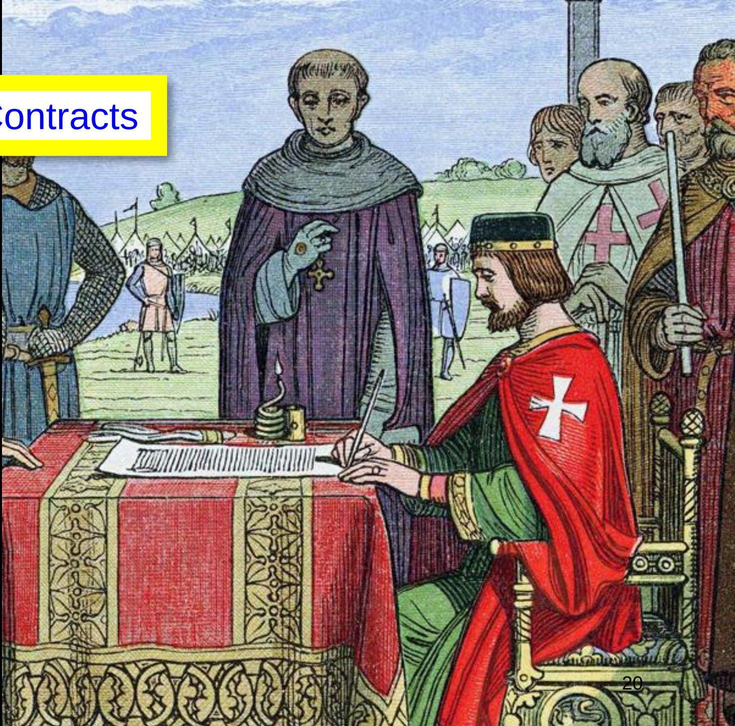
DAVID GRAEBER

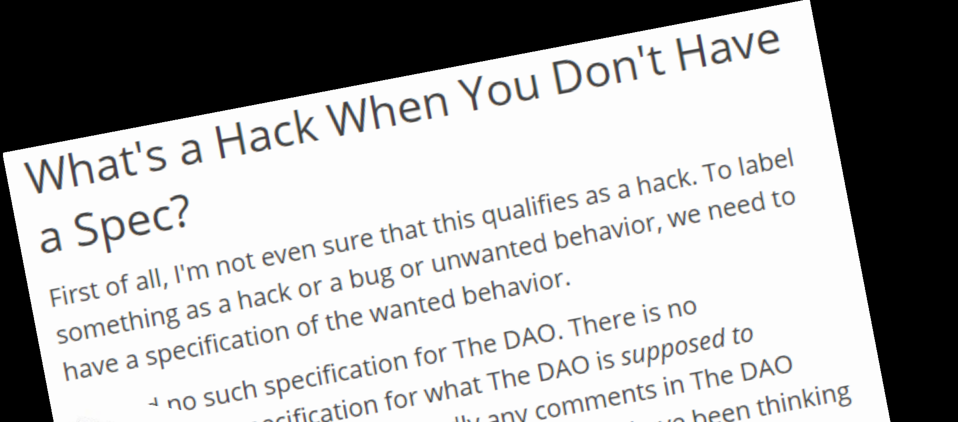
"A BRILLIANT, DEEPLY ORIGINAL POLITICAL THINKER."
REBECCA SOLNIT, AUTHOR
A PARADISE BUILT IN HELL

THANK YOU! COME AGAIN!

MELVILLE HOUSE PUBLISHING

# Smart Contracts



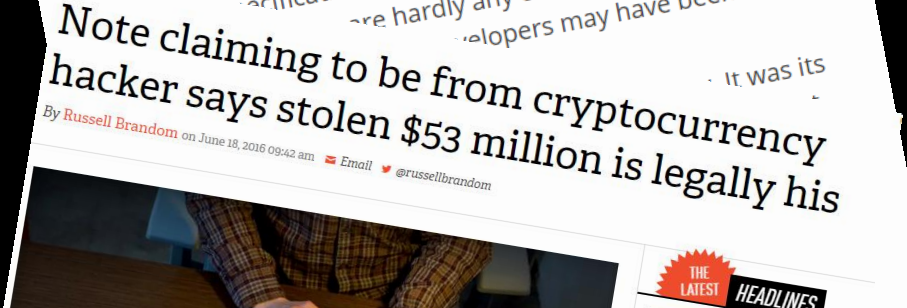


# What's a Hack When You Don't Have a Spec?

First of all, I'm not even sure that this qualifies as a hack. To label something as a hack or a bug or unwanted behavior, we need to have a specification of the wanted behavior.

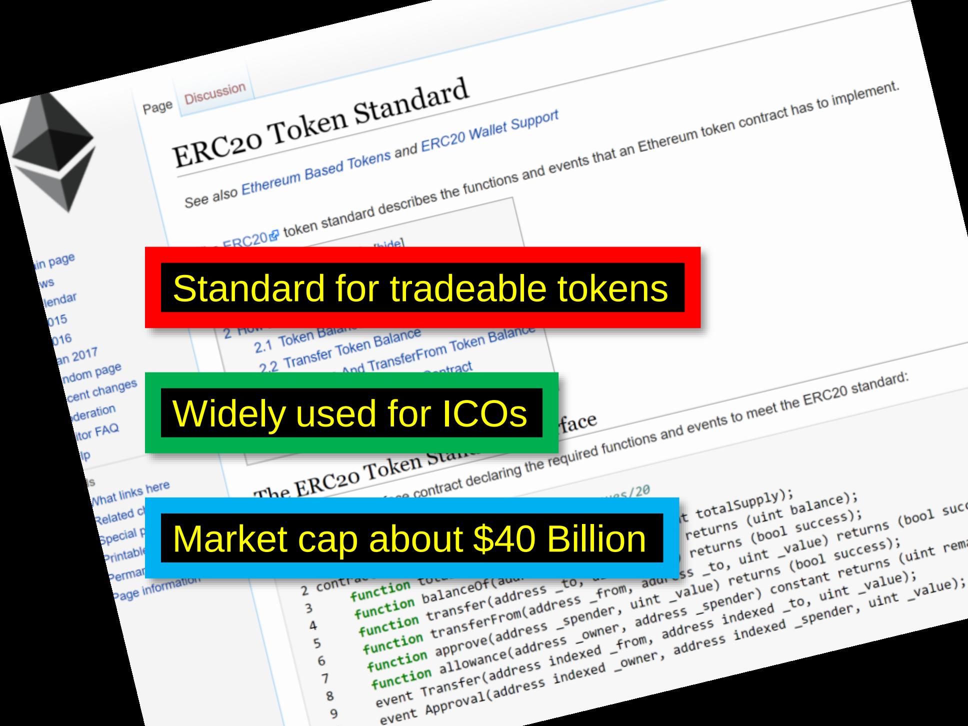
d no such specification for The DAO. There is no
ecification for what The DAO is *supposed to*
re hardly any comments in The DAO
velopers may have been thinking

It was its



# Note claiming to be from cryptocurrency hacker says stolen $53 million is legally his

By Russell Brandom on June 18, 2016 09:42 am Email @russellbrandom



# ERC20 Token Standard

See also Ethereum Based Tokens and ERC20 Wallet Support

The ERC20 token standard describes the functions and events that an Ethereum token contract has to implement.

[hide]

2 How

2.1 Token Bala

2.2 Transfer Token Balance

And TransferFrom Token Balance

Contract

## The ERC20 Token Stan … face

face contract declaring the required functions and events to meet the ERC20 standard:

ues/20

```
contrac
    function tota                                  t totalSupply);
    function balanceOf(add                         returns (uint balance);
    function transfer(address _to, u               returns (bool success);
    function transferFrom(address _from, address _to, uint _value) returns (bool suc
    function approve(address _spender, uint _value) returns (bool success);
    function allowance(address _owner, address _spender) constant returns (uint rema
    event Transfer(address indexed _from, address indexed _to, uint _value);
    event Approval(address indexed _owner, address indexed _spender, uint _value);
```

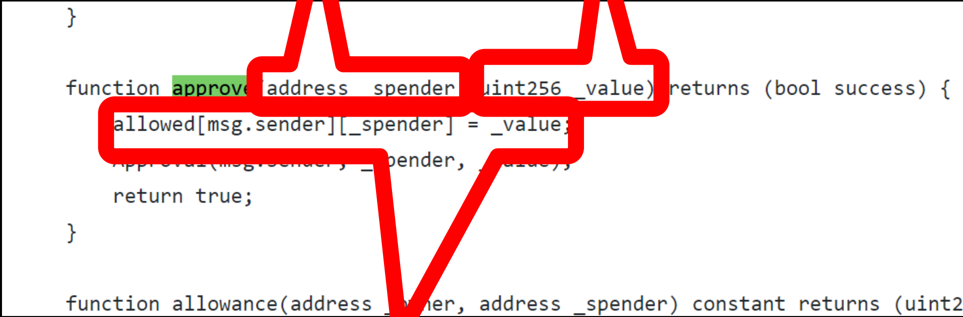
Standard for tradeable tokens

Widely used for ICOs

Market cap about $40 Billion

I am willing to allow this party …

… to withdraw this amount …



```
    }

    function approve(address _spender, uint256 _value) returns (bool success) {
        allowed[msg.sender][_spender] = _value;
        Approval(msg.sender, _spender, _value);
        return true;
    }

    function allowance(address _owner, address _spender) constant returns (uint2
```

… from my account.

Alice
authorizes
Bob
to
withdraw
$100

Alice
Bob
miner

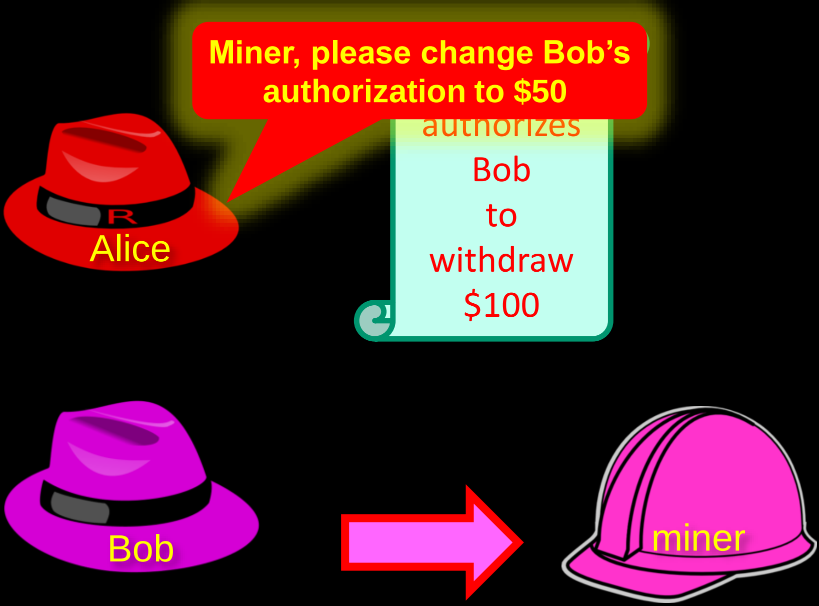
Alice
authorizes
Bob
to
withdraw
$100

I am Bob’s
secret friend

Miner, please change Bob’s authorization to $50

authorizes
Bob
to
withdraw
$100

Alice
!!!
Bob
!!!
miner



Miner, please change Bob’s authorization to $50

authorizes Bob to withdraw $100

Miner, please change Bob’s authorization to $50

Alice

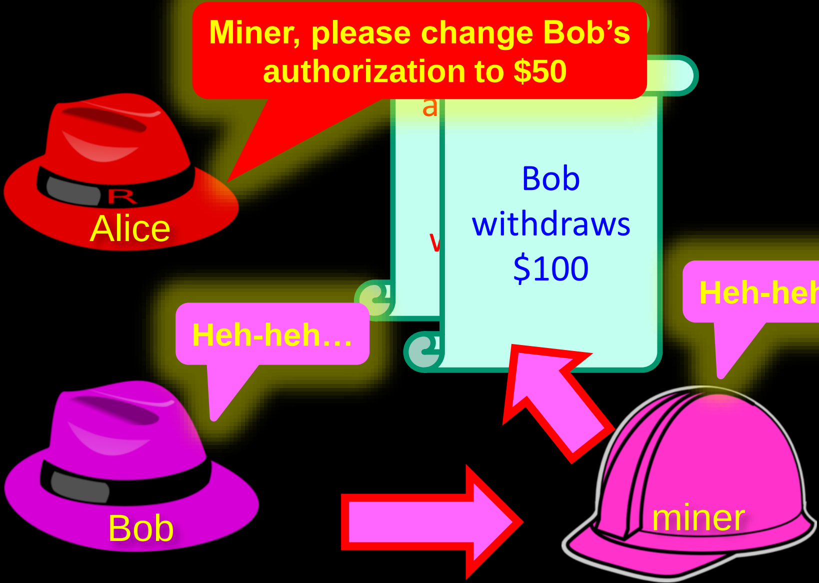
a

v

Bob withdraws $100

Bob

miner



Miner, please change Bob’s authorization to $50

Alice

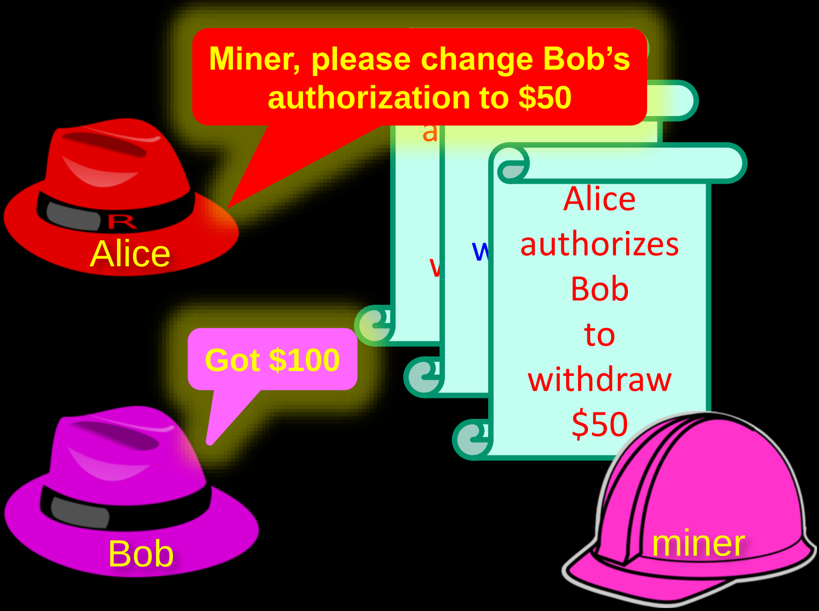
Bob withdraws $100

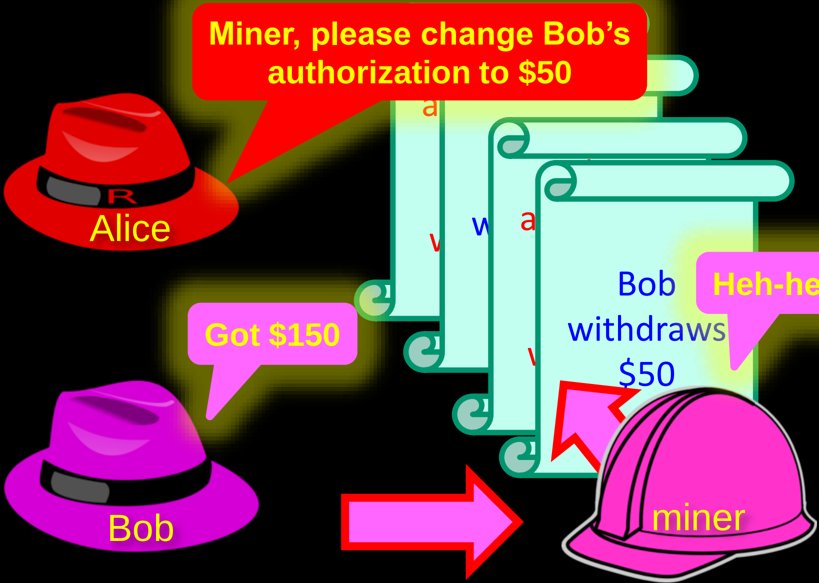
Heh-heh…

Heh-heh…

Bob

miner


Miner, please change Bob’s authorization to $50
Alice
Got $100
Bob
Alice authorizes Bob to withdraw $50
miner


Miner, please change Bob’s authorization to $50
Alice
Got $150
Bob
Bob withdraws $50
Heh-heh…
miner

user
miner
relay
developer
hodler

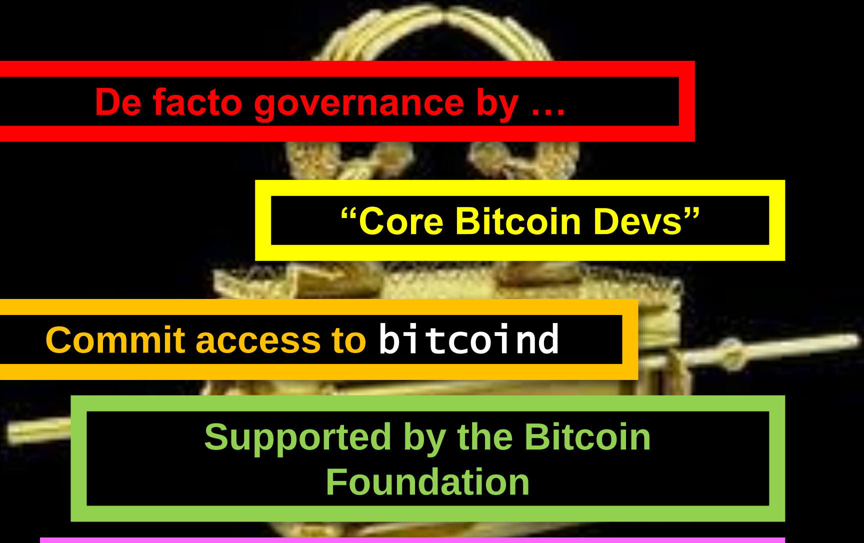
What makes a transaction valid?

When miners say so.

Canonicalism: all and only what Satoshi revealed.

Fails to explain upgrades …

… and bug fixes.



De facto governance by …

“Core Bitcoin Devs”

Commit access to `bitcoind`

Supported by the Bitcoin Foundation

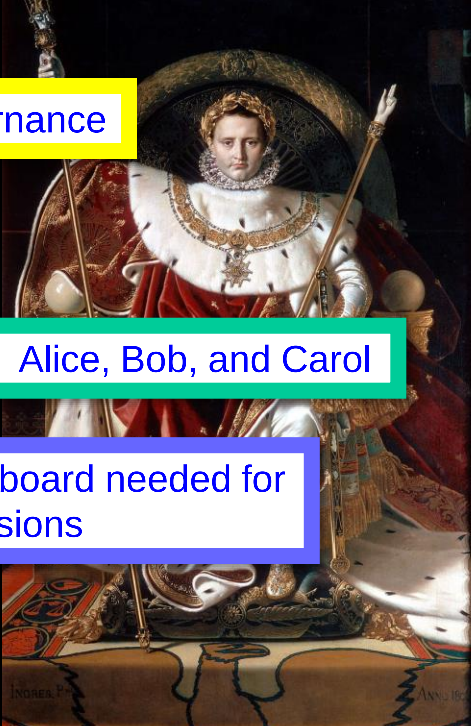
Controversy wrt block sizes, etc.

# Example: Corporate governance

“Genesis” block

Board of directors = Alice, Bob, and Carol

majority vote of the board needed for all governance decisions



## Example: Corporate governance

January

Carol resigns from board

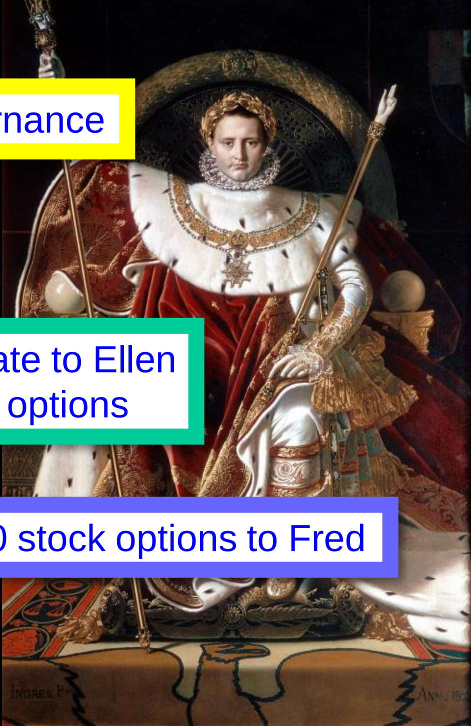
Alice & Bob vote to replace her with Dave

# Example: Corporate governance

February

Alice & Dave delegate to Ellen authority over stock options

Ellen issues $10000 stock options to Fred



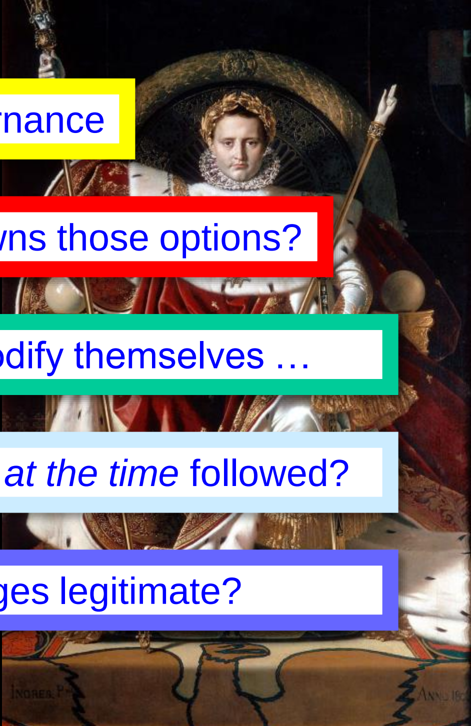
# Example: Corporate governance

How to *prove* that Fred owns those options?

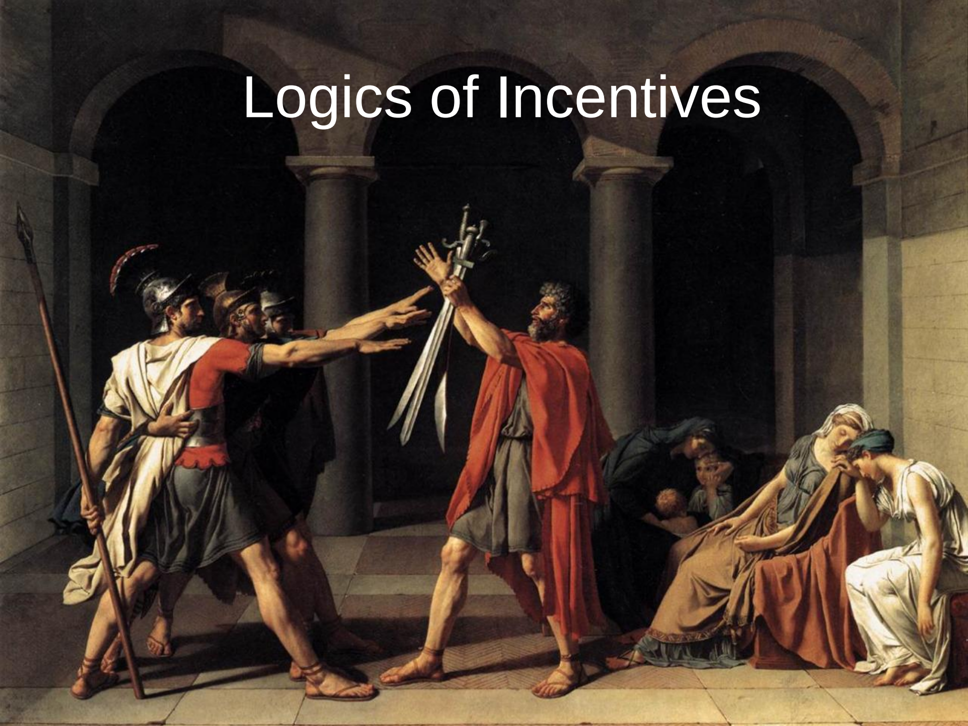
Notice that rules modify themselves …

Were rules in effect *at the time* followed?

Were the rule changes legitimate?



# Logics of Incentives



Client behavior?

Altruistic: follows protocol

Rational: responds to incentives

Byzantine: vandalizes everything

# Small Game Fallacy

The dangerous illusion that clients' objective functions known to system designers

# Example: Selfish Mining

Bitcoin miners that withhold newly-mined blocks …

Sometimes earn disproportionate profits

Reduce own earnings, but …

Reduce others more!

Mining cartel might bully others into i

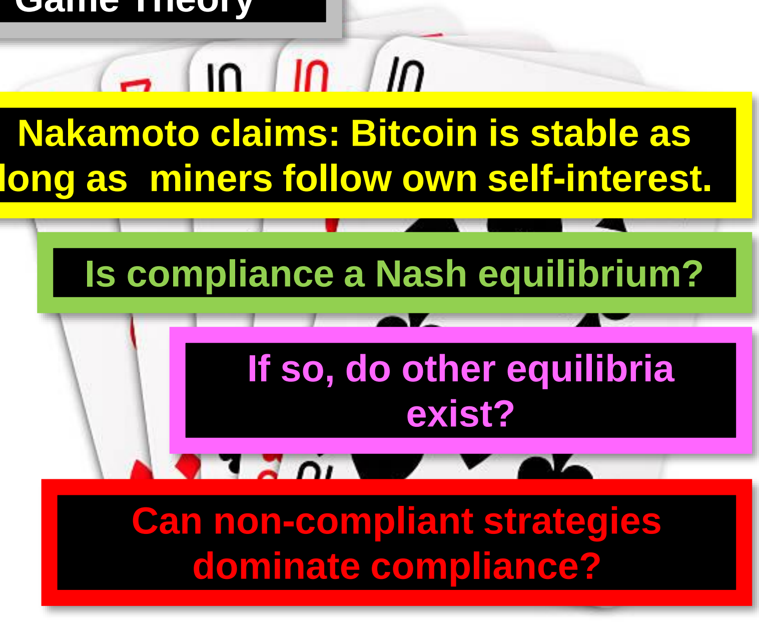
Eventual 51% attack!

# Small-Game Fallacy:

If you assume motive is short-term profit maximization …

You will miss this attack!

# Game Theory



Nakamoto claims: Bitcoin is stable as long as  miners follow own self-interest.

Is compliance a Nash equilibrium?

If so, do other equilibria exist?

Can non-compliant strategies dominate compliance?

# Majority miner?

If one dishonest miner controls > 50% then …

All is lost!

Can roll back other transactions …

Censor transactions you don’t like …

Not a good idea, if invested in Bitcoin stability, reputation

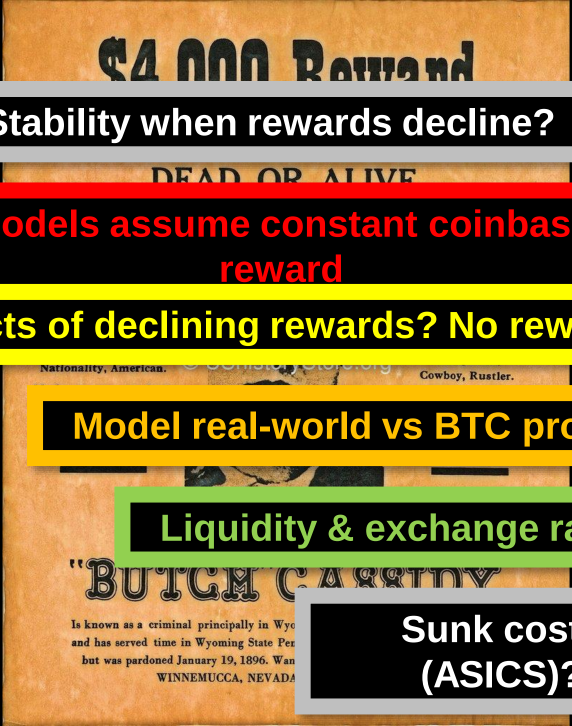
## What if miners collude?

Miners could form cartel …

… to simulate evil majority miner?

Stable? Would members defect?

Real issue: mining pools are a thing


$4,000 Reward
DEAD OR ALIVE
Nationality, American.
Cowboy, Rustler.
"BUTCH CASSIDY"
Is known as a criminal principally in Wyo
and has served time in Wyoming State Pen
but was pardoned January 19, 1896. Wan
WINNEMUCCA, NEVADA

Stability when rewards decline?

Models assume constant coinbase reward

Effects of declining rewards? No rewards?

Model real-world vs BTC profits?

Liquidity & exchange rates?

Sunk costs (ASICS)?

# Goldfinger Attacks

**Intent to bring down Bitcoin, not profit**

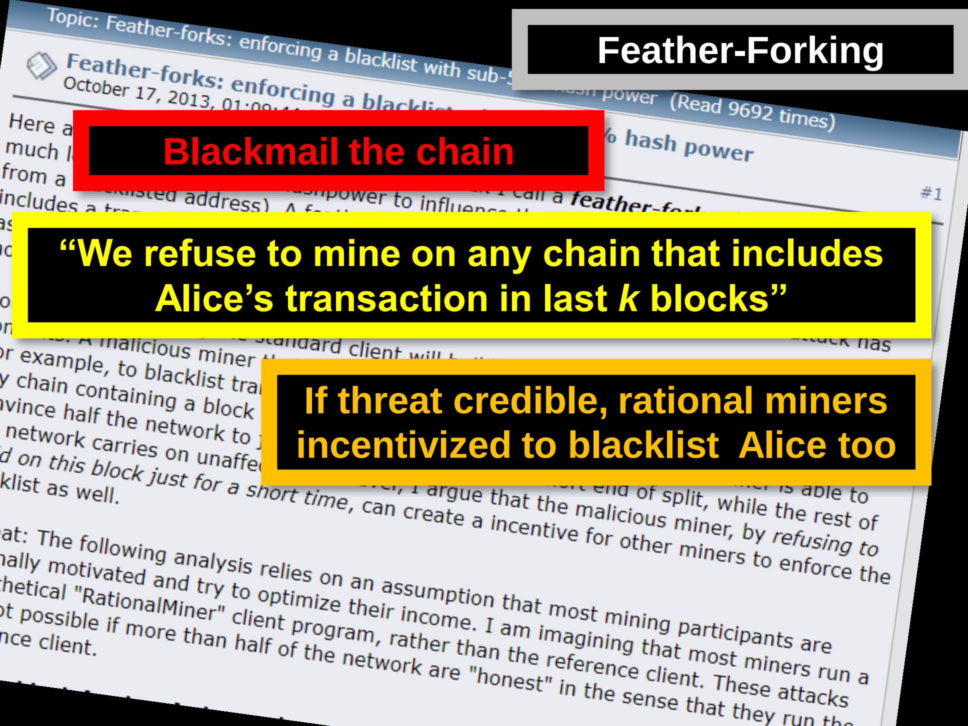
**Hostile state actor?**

**Protest?**

**Short position?**

**“alt-coin infanticide” actually happens**

# Feather-Forking



Topic: Feather-forks: enforcing a blacklist with sub-5 hash power (Read 9692 times)

Feather-forks: enforcing a blacklist % hash power

October 17, 2013, 01:09:4

#1

Here a
much l
from a
includes a tra klisted address). A feat ashpower to influence th k I call a *feather-fork*
as
no

o
on
s. A malicious miner the standard client will b attack has
or example, to blacklist tra
y chain containing a block
nvince half the network to j
network carries on unaffec ever, I argue that the short end of split, while the rest of miner is able to
*d on this block just for a short time*, can create a incentive for other miners to enforce the malicious miner, by *refusing to*
klist as well.

at: The following analysis relies on an assumption that most mining participants are
nally motivated and try to optimize their income. I am imagining that most miners run a
thetical "RationalMiner" client program, rather than the reference client. These attacks
ot possible if more than half of the network are "honest" in the sense that they run the
nce client.

Blackmail the chain

“We refuse to mine on any chain that includes Alice’s transaction in last *k* blocks”

If threat credible, rational miners incentivized to blacklist  Alice too

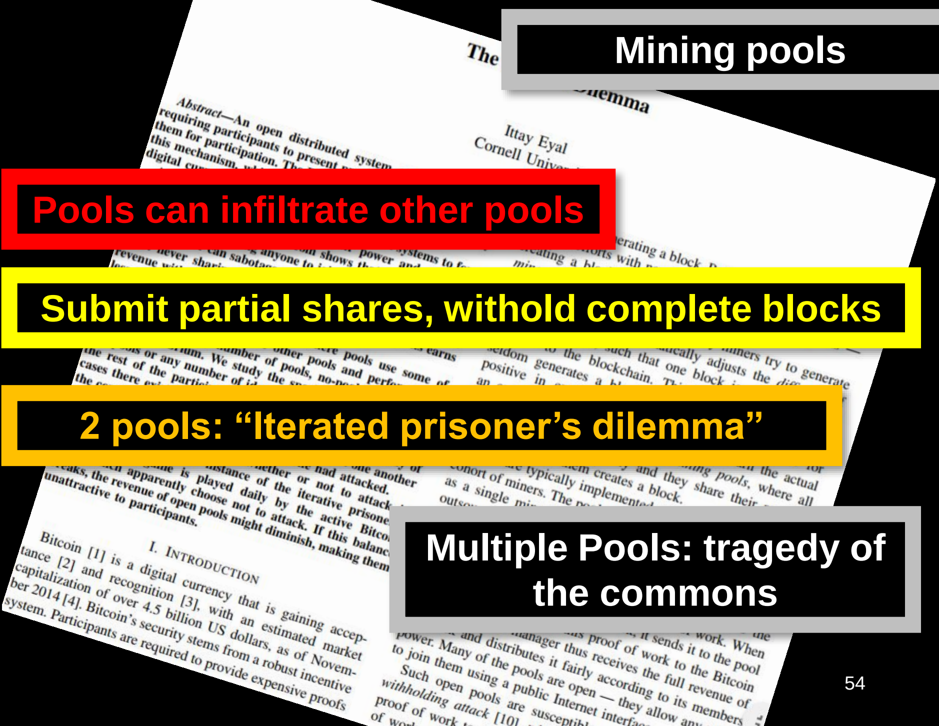
# Mining pools

Pools can infiltrate other pools

Submit partial shares, withold complete blocks

2 pools: “Iterated prisoner’s dilemma”

Multiple Pools: tragedy of the commons



The … Dilemma

Ittay Eyal
Cornell Univ…

*Abstract*—An open distributed system requiring participants to present … them for participation. … this mechanism, … digital cu…

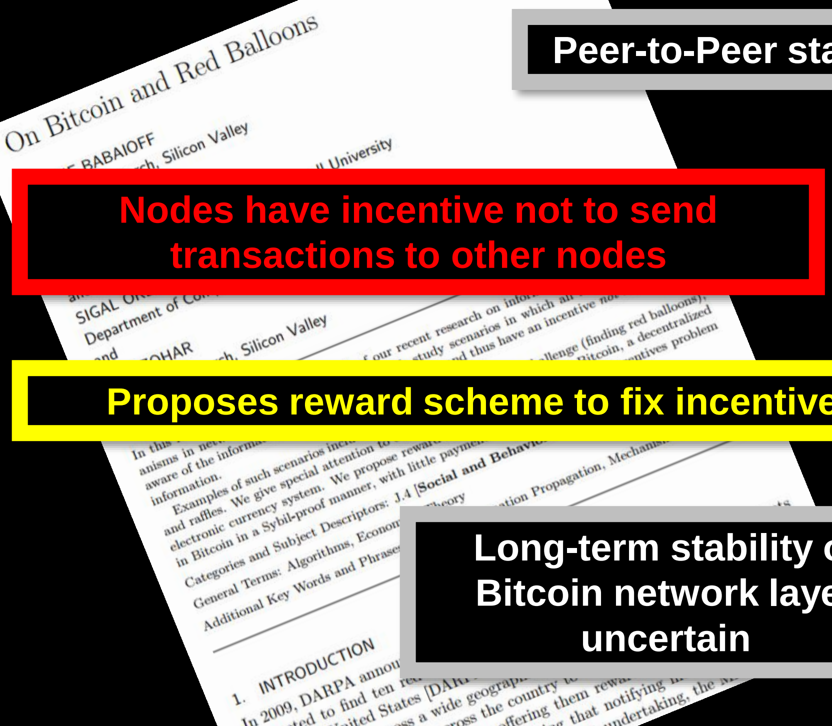
… apparently choose not to attack. If this balanc… eaks, the revenue of open pools might diminish, making them unattractive to participants.

I. INTRODUCTION

Bitcoin [1] is a digital currency that is gaining acceptance [2] and recognition [3], with an estimated market capitalization of over 4.5 billion US dollars, as of November 2014 [4]. Bitcoin’s security stems from a robust incentive system. Participants are required to provide expensive proofs

… work. When … it sends it to the pool … proof of work to the Bitcoin … manager thus receives the full revenue of … and distributes it fairly according to its members power. Many of the pools are open — they allow any… to join them using a public Internet interfa… Such open pools are susceptibl… *withholding attack* [10] … proof of work …

# Peer-to-Peer stability



On Bitcoin and Red Balloons

BABAIOFF

...rch, Silicon Valley

...l University

SIGAL OR...

Department of Co...

and

...ZOHAR

...ch, Silicon Valley

...f our recent research on info... study scenarios in which all... and thus have an incentive not... challenge (finding red balloons), ... Bitcoin, a decentralized ... incentives problem

In this ... anisms in net... aware of the informa... information.

Examples of such scenarios incl... and raffles. We give special attention to ... electronic currency system. We propose rewar... in Bitcoin in a Sybil-proof manner, with little paymen...

Categories and Subject Descriptors: J.4 [Social and Behavio...

General Terms: Algorithms, Econom... Theory

Additional Key Words and Phrase... ...ation Propagation, Mechanis...

1. INTRODUCTION

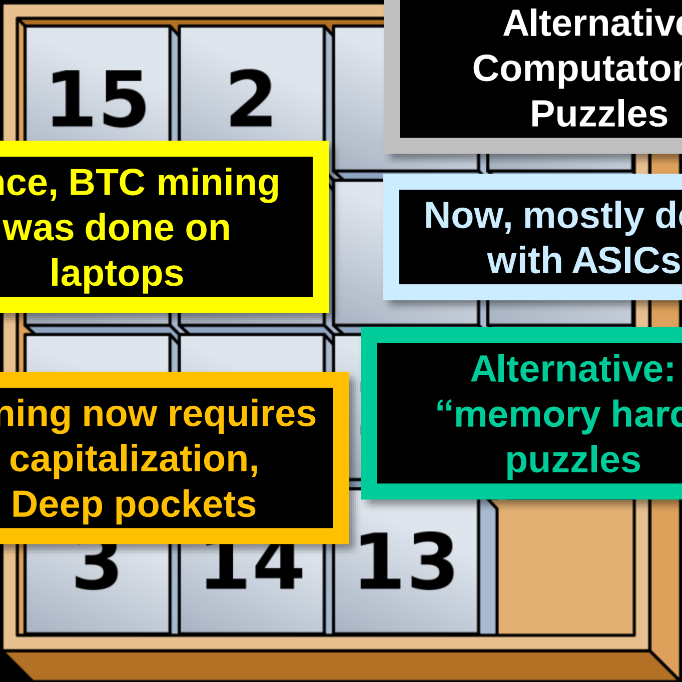
In 2009, DARPA annou... ...ted to find ten red ... ...nited States [DARP... ...ss a wide geograph... ...cross the country to ... offering them rewa... ...that notifying th... ...undertaking, the ...

**Nodes have incentive not to send transactions to other nodes**

**Proposes reward scheme to fix incentive**

**Long-term stability of Bitcoin network layer uncertain**

# Alternative Computatonal Puzzles



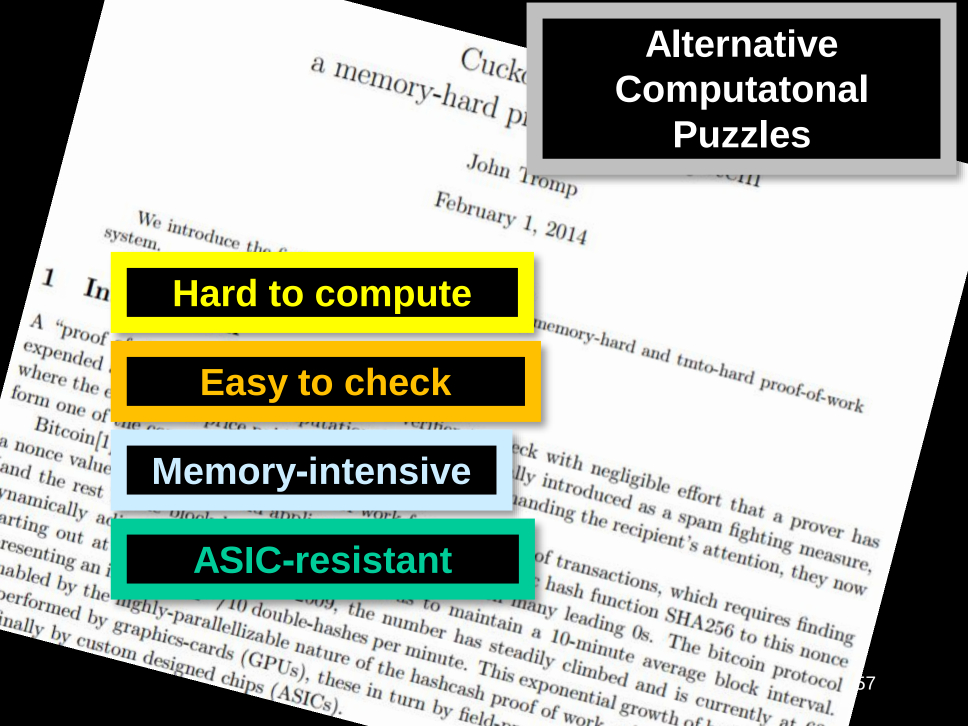
Once, BTC mining was done on laptops

Now, mostly done with ASICs

Mining now requires capitalization, Deep pockets

Alternative: “memory hard” puzzles

# Alternative Computatonal Puzzles



Cuck

a memory-hard p

John Tromp

February 1, 2014

We introduce the … memory-hard and tmto-hard proof-of-work
system.

1 In

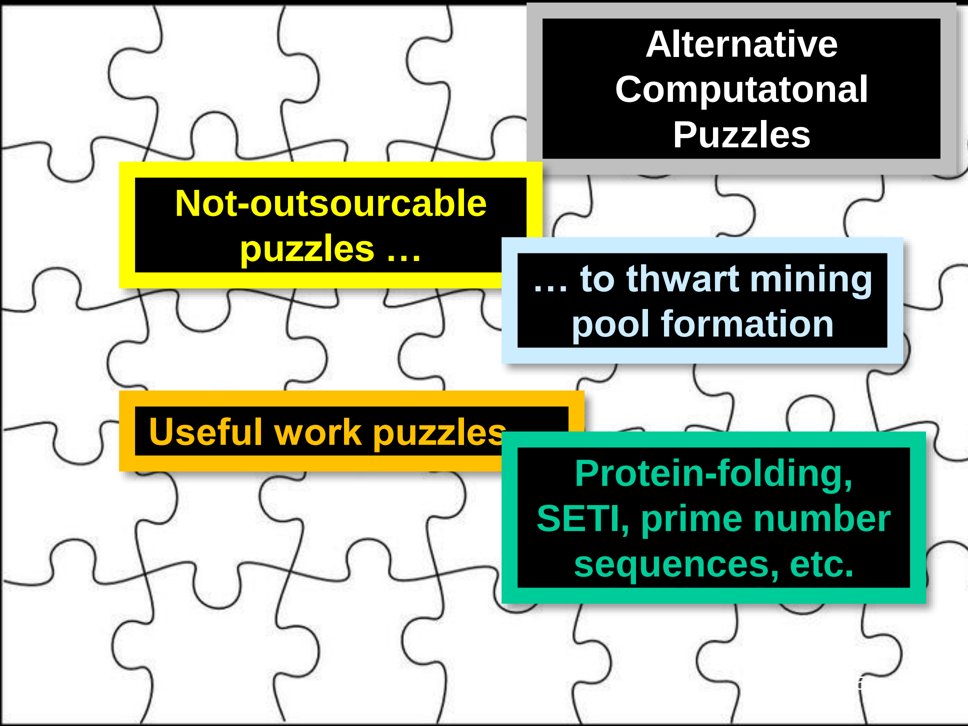
A "proof …
expended … eck with negligible effort that a prover has
where the e … lly introduced as a spam fighting measure,
form one of … nanding the recipient's attention, they now
Bitcoin[1 … of transactions, which requires finding
a nonce value … hash function SHA256 to this nonce
and the rest … many leading 0s. The bitcoin protocol
ynamically a … to maintain a 10-minute average block interval.
arting out at … 2009, the number has steadily climbed and is currently at
resenting an i … /10 double-hashes per minute. This exponential growth of
nabled by the highly-parallellizable nature of the hashcash proof of work
erformed by graphics-cards (GPUs), these in turn by field-
inally by custom designed chips (ASICs).

**Hard to compute**

**Easy to check**

**Memory-intensive**

**ASIC-resistant**



# Alternative Computatonal Puzzles

Not-outsourcable puzzles …

… to thwart mining pool formation

Useful work puzzles

Protein-folding, SETI, prime number sequences, etc.

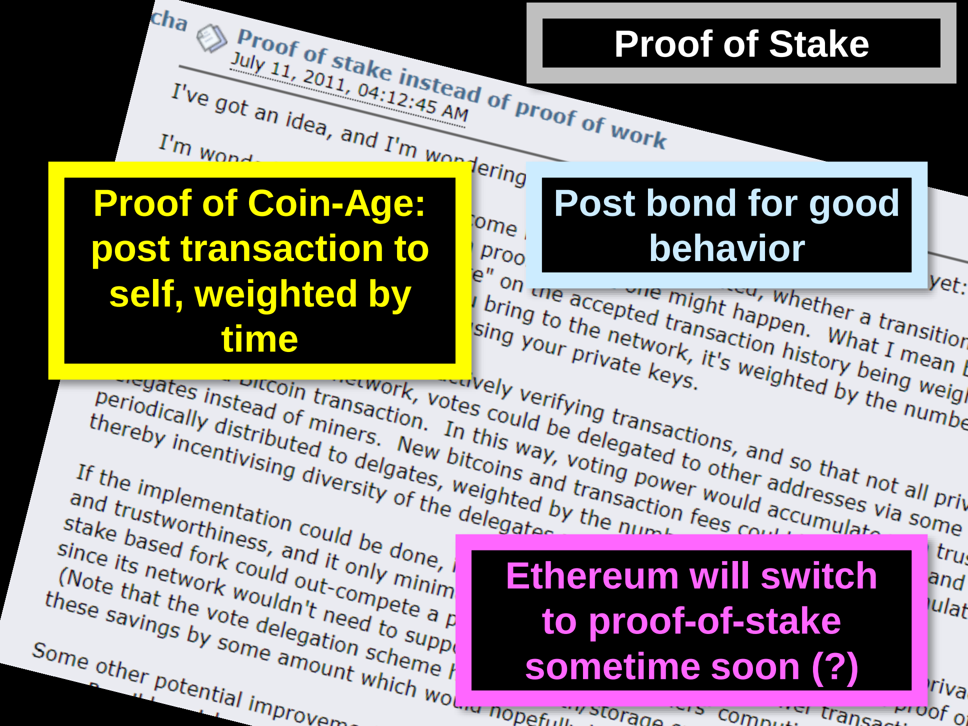
# Proof of Stake

Random sample of miners weighted by current allocation of wealth

Harder to acquire 51% wealth than 51% hashpower?

No trees were harmed in mining this block

# Proof of Stake



cha

Proof of stake instead of proof of work

July 11, 2011, 04:12:45 AM

I've got an idea, and I'm wondering

I'm wond

ome yet:

proo ed, whether a transition

one might happen. What I mean b

e" on the accepted transaction history being weig

bring to the network, it's weighted by the numbe

sing your private keys.

ctively verifying transactions, and so that not all priv

etwork, votes could be delegated to other addresses via some

Bitcoin transaction. In this way, voting power would accumulat

legates instead of miners. New bitcoins and transaction fees coul

periodically distributed to delgates, weighted by the num

thereby incentivising diversity of the delegates

trus

and

ulat

If the implementation could be done,

and trustworthiness, and it only minim

stake based fork could out-compete a p

since its network wouldn't need to supp

(Note that the vote delegation scheme h

these savings by some amount which wo hopefully /storage ers comput er transacti

riva

proof o

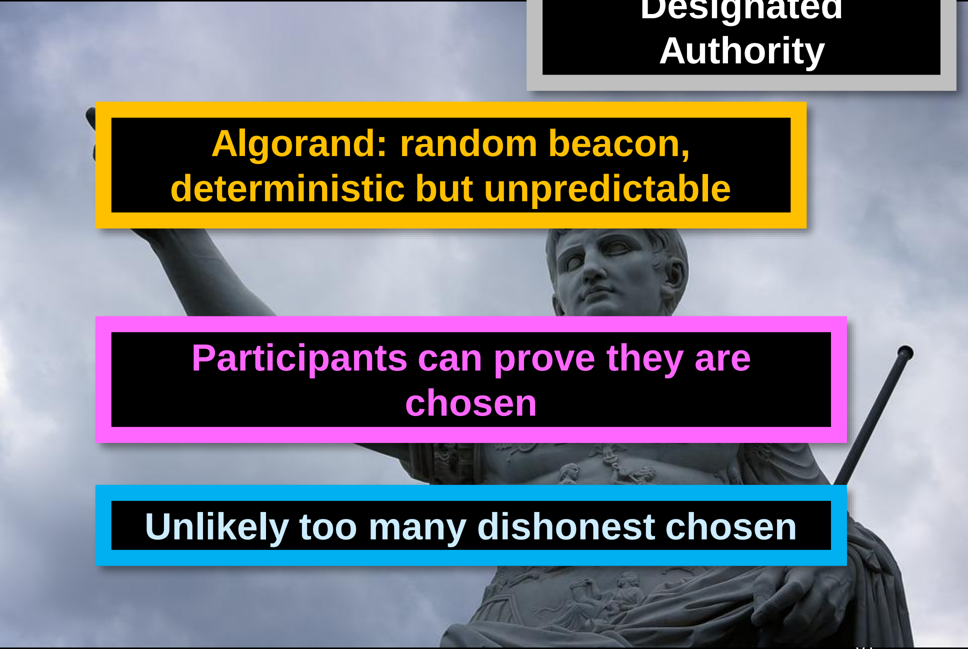
Some other potential improvem

Proof of Coin-Age: post transaction to self, weighted by time

Post bond for good behavior

Ethereum will switch to proof-of-stake sometime soon (?)

# Designated Authority

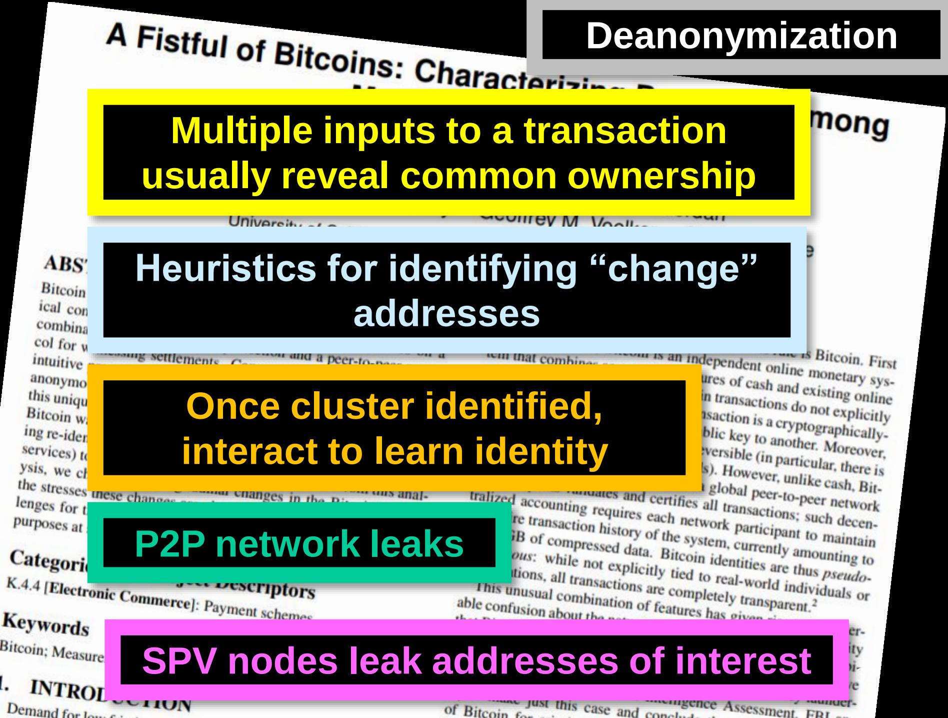


Algorand: random beacon, deterministic but unpredictable

Participants can prove they are chosen

Unlikely too many dishonest chosen

# Deanonymization



A Fistful of Bitcoins: Characterizing

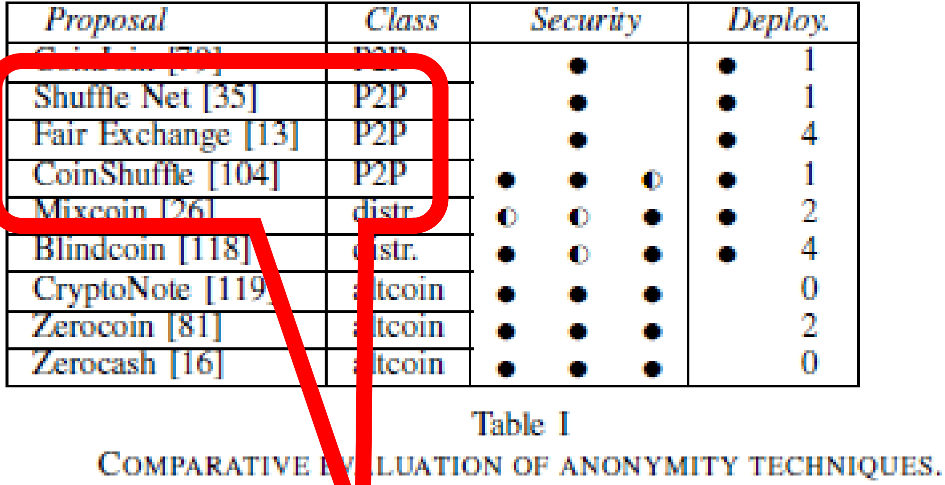
Multiple inputs to a transaction usually reveal common ownership

Heuristics for identifying "change" addresses

Once cluster identified, interact to learn identity

P2P network leaks

SPV nodes leak addresses of interest

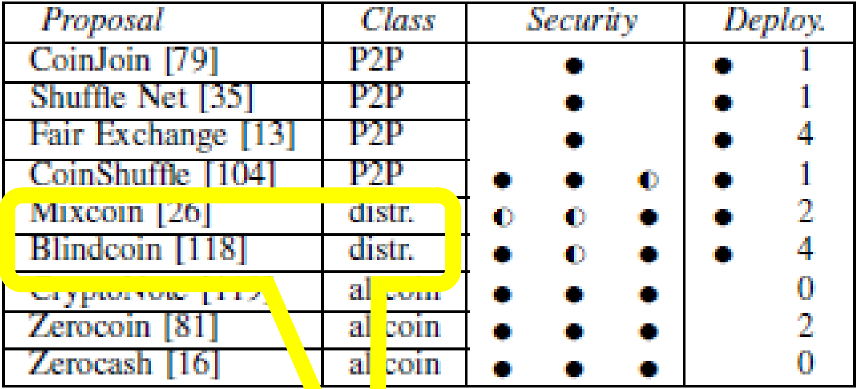


| *Proposal* | *Class* | *Security* | | | *Deploy.* | |
|---|---|---|---|---|---|---|
| CoinJoin [78] | P2P | | ● | | ● | 1 |
| Shuffle Net [35] | P2P | | ● | | ● | 1 |
| Fair Exchange [13] | P2P | | ● | | ● | 4 |
| CoinShuffle [104] | P2P | ● | ● | ◐ | ● | 1 |
| Mixcoin [26] | distr. | ◐ | ◐ | ● | ● | 2 |
| Blindcoin [118] | distr. | ● | ◐ | ● | ● | 4 |
| CryptoNote [119] | altcoin | ● | ● | ● | | 0 |
| Zerocoin [81] | altcoin | ● | ● | ● | | 2 |
| Zerocash [16] | altcoin | ● | ● | ● | | 0 |

Table I

COMPARATIVE EVALUATION OF ANONYMITY TECHNIQUES.

**Holders create series of transactions which (privately) permute ownership**

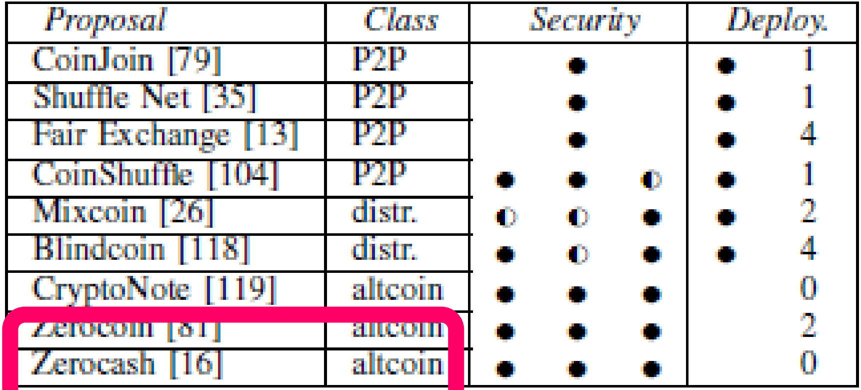


| Proposal | Class | Security | | | Deploy. | |
|---|---|---|---|---|---|---|
| CoinJoin [79] | P2P | | ● | | ● | 1 |
| Shuffle Net [35] | P2P | | ● | | ● | 1 |
| Fair Exchange [13] | P2P | | ● | | ● | 4 |
| CoinShuffle [104] | P2P | ● | ● | ◐ | ● | 1 |
| Mixcoin [26] | distr. | ◐ | ◐ | ● | ● | 2 |
| Blindcoin [118] | distr. | ● | ◐ | ● | ● | 4 |
| CryptoNote [117] | altcoin | ● | ● | ● | | 0 |
| Zerocoin [81] | altcoin | ● | ● | ● | | 2 |
| Zerocash [16] | altcoin | ● | ● | ● | | 0 |

Table I

COMPARATIVE EVALUATION OF ANONYMITY TECHNIQUES.

Holders send transactions to 3rd party mixer, receive transactions back

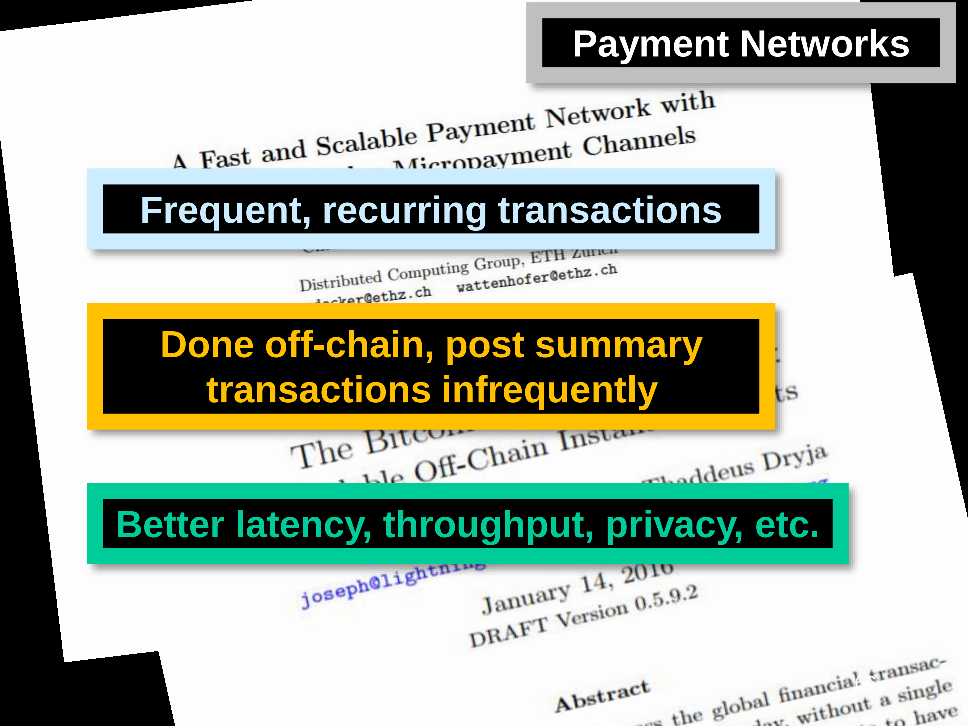


| *Proposal* | *Class* | *Security* | | | *Deploy.* | |
|---|---|---|---|---|---|---|
| CoinJoin [79] | P2P | | ● | | ● | 1 |
| Shuffle Net [35] | P2P | | ● | | ● | 1 |
| Fair Exchange [13] | P2P | | ● | | ● | 4 |
| CoinShuffle [104] | P2P | ● | ● | ◐ | ● | 1 |
| Mixcoin [26] | distr. | ◐ | ◐ | ● | ● | 2 |
| Blindcoin [118] | distr. | ● | ◐ | ● | ● | 4 |
| CryptoNote [119] | altcoin | ● | ● | ● | | 0 |
| Zerocoin [81] | altcoin | ● | ● | ● | | 2 |
| Zerocash [16] | altcoin | ● | ● | ● | | 0 |

Table I
COMPARATIVE EVALUATION OF ANONYMITY TECHNIQUES.

Altcoins that use zero-knowledge proofs for unlinkability

# Payment Networks



A Fast and Scalable Payment Network with
Micropayment Channels

Distributed Computing Group, ETH Zurich
decker@ethz.ch wattenhofer@ethz.ch

The Bitcoin
Off-Chain Instant
ts

Thaddeus Dryja

joseph@lightning

January 14, 2016
DRAFT Version 0.5.9.2

Abstract

the global financial transac-
without a single
to have

Frequent, recurring transactions

Done off-chain, post summary transactions infrequently

Better latency, throughput, privacy, etc.

# Cross-chain swaps

Activity: 1162

Re: Alt chains and atomic t

May 21, 2013, 01:31:21 PM

> Quote from: ripper234 on May 21, 2013, 08:25:59 AM
>
> I must admit I do not fully understand Mike Hearns' explanati
> page to develop and clarify the solution as neede
>
> I suggest we use the wiki

This basically

reci

H(x)

ng H(x).

hat can only be spent if you have the

A sends coins to <B's public key> and x for

Step 2

B knows th

s x to B.

x for H(x)

The can now both spend th

If A ref

as to provide x to the

se to unlock the coins he sent B, until he wants to spend

s potentially a problem

Alice has alt-coin, wants bitcoin

Bob has bitcoin, wants alt-coin

Multiphase protocol guarantees atomic swap

# Thank You!

Questions & Comments?