Blockchains
Overview & Applications

Roger Wattenhofer

ETH Zurich – Distributed Computing Group

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.

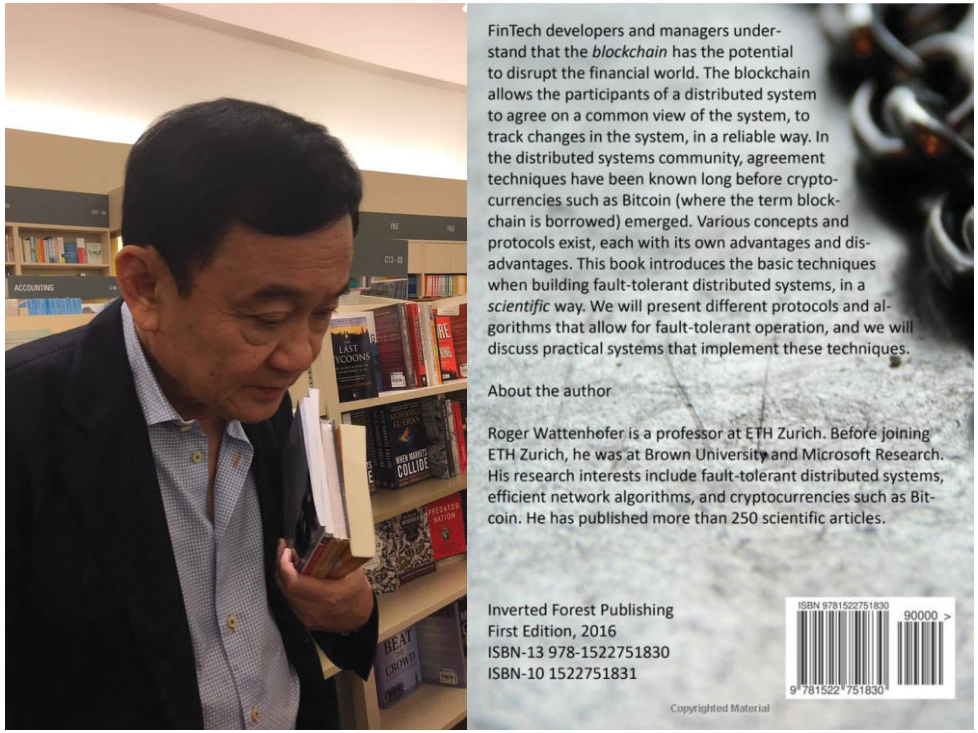
Page 1 of 1

MANUAL JOURNAL VOUCHER

PREPARED BY	DATE
W.L.R	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 JY3-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

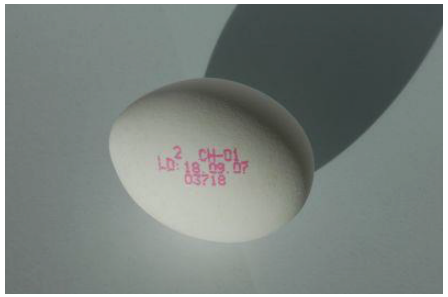


Blockchain Basics

Transaction

Transaction

Transaction

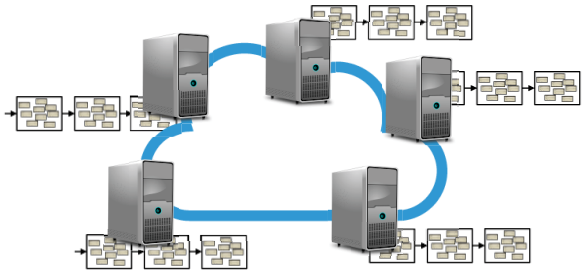


Transaction

Block

Blockchain

Blockchain is Replicated



Blockchain

Distributed Systems & Cryptography
(1982) (1976)

Blockchain

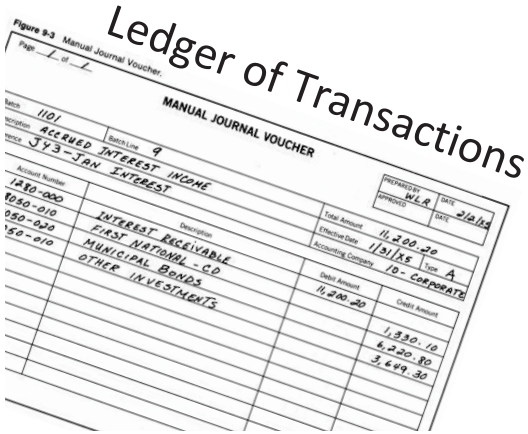
Distributed Systems & Cryptography
Fault-Tolerance & Digital Signatures

Rule of Thumb

Blockchains* may disrupt your business if you use signatures.

*or blockchain-like tech

Blockchain Variants

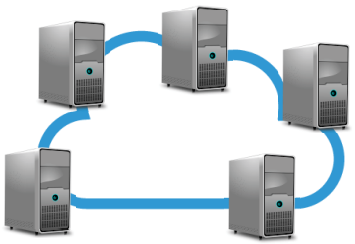


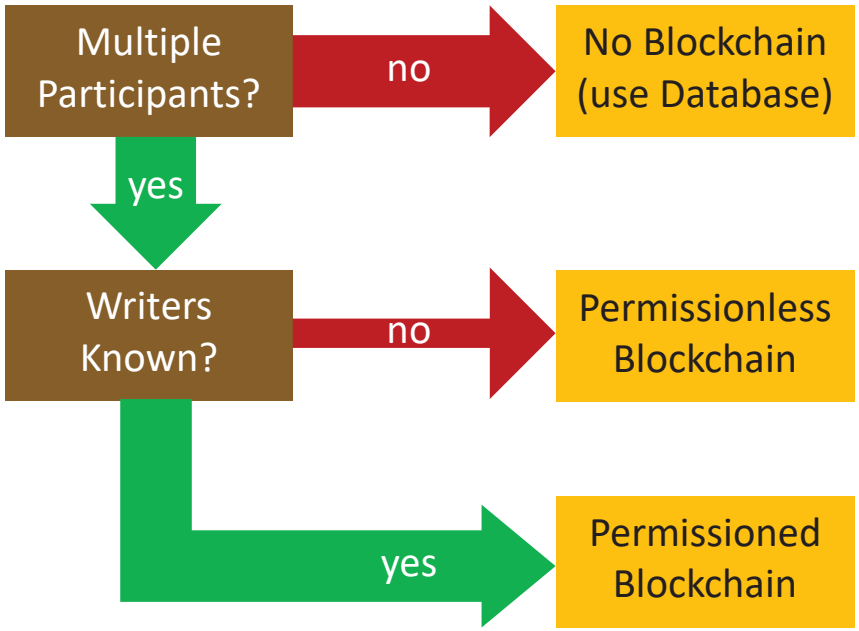
Ledger of Transactions

Bitcoin

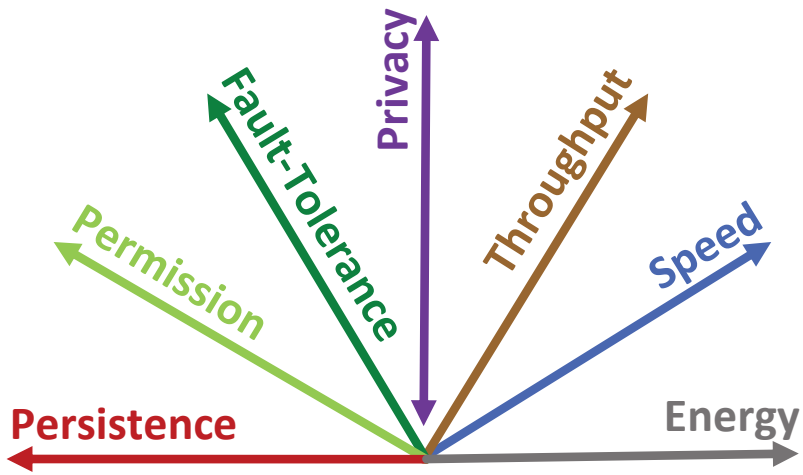
Permissionless / Open

Permissioned / Closed





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

sonntagszeitung.ch | 17. Dezember 2017 Wissen 55

«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

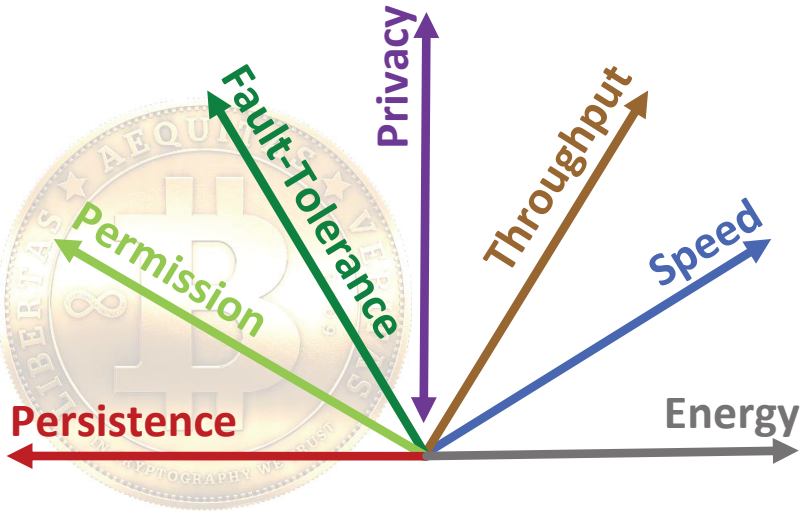
$1M/h $0.08/kWh

Proof of Work

Hashrate · Energy/Hash ≈ 1.3 GW

$13 \cdot 10^9$ GH/s 0.1 J/GH

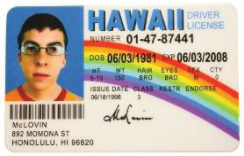
The Seven Blockchain Dimensions



What About Privacy?

It's Complicated.

Privacy



Anonymity/Public ⟷ Identity/Private

Applications

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

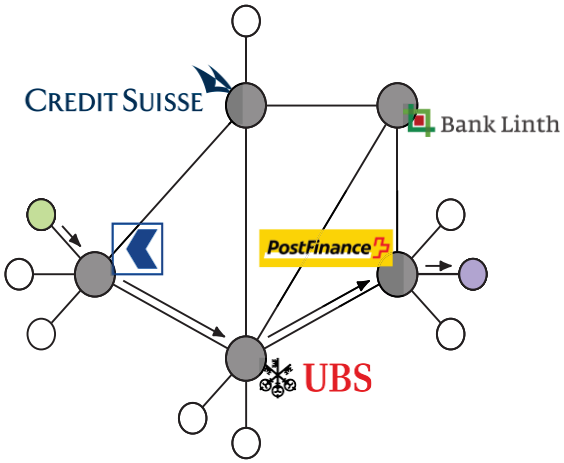
Permissioned Blockchain

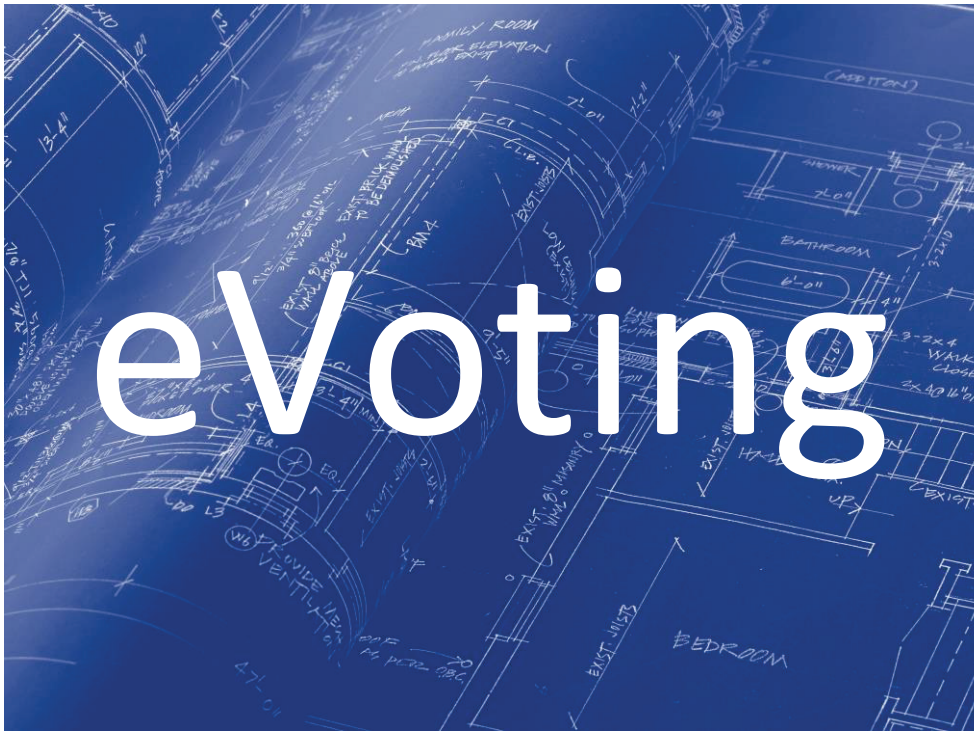
&

Payment Network

Permissioned Blockchain

Payment Network





What's Wrong with Paper?

Cost

Verifiability

Neue Zürcher Zeitung

Rund 26 Prozent der Zürcher Wahlzettel waren nicht gültig

Anonymity

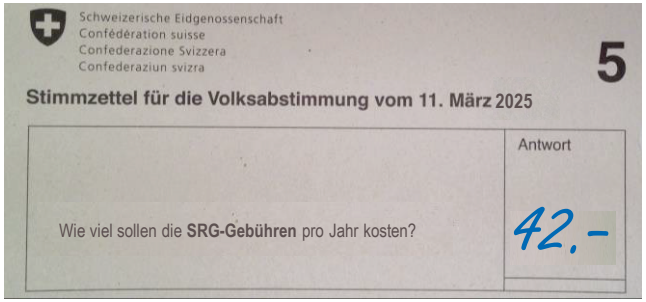
Identity Swapper

Identity Mixer

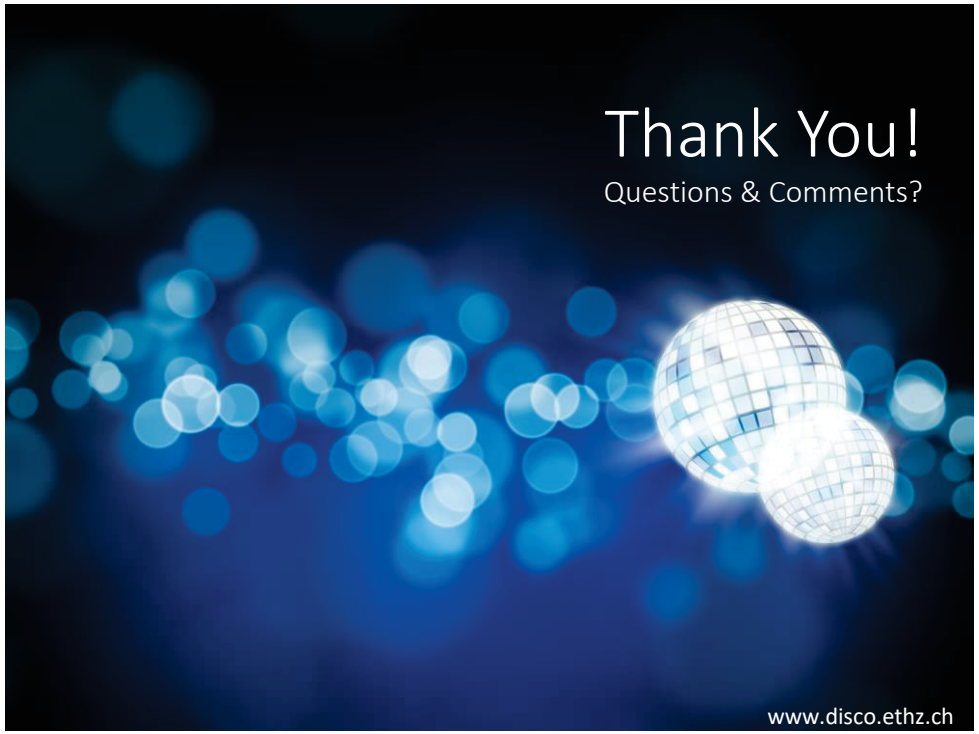
…

Election Help

Democracy Beyond Yes or No



Don’t bring a Blockchain
to a Gunfight



Scaling Bitcoin

Micropayment Channel Networks

Roger Wattenhofer

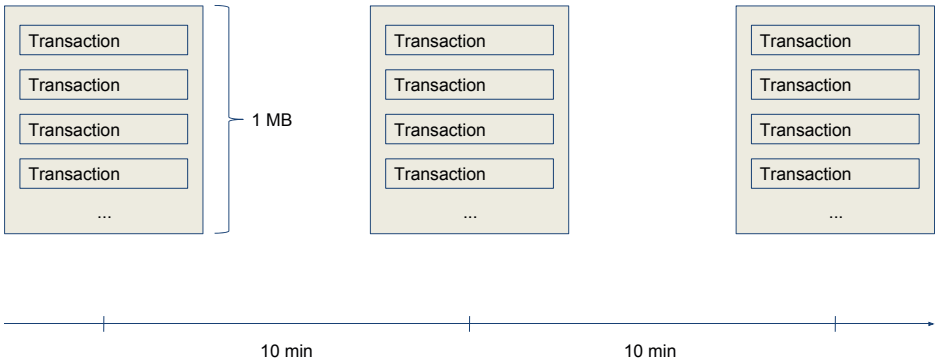
Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

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

The Blockchain

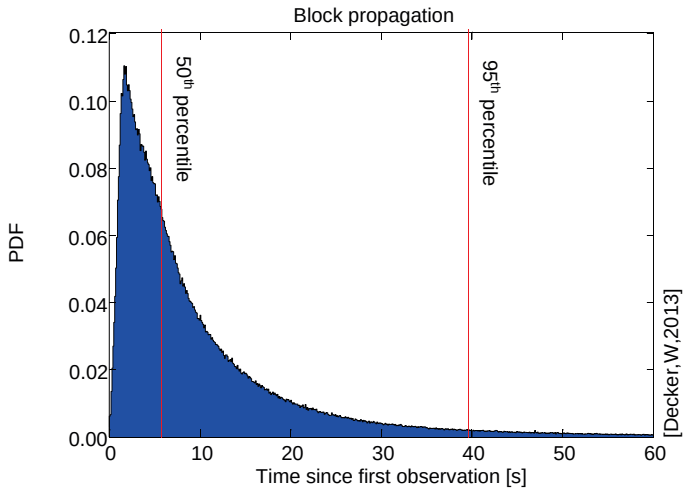
Can Bitcoin be a Real Currency?



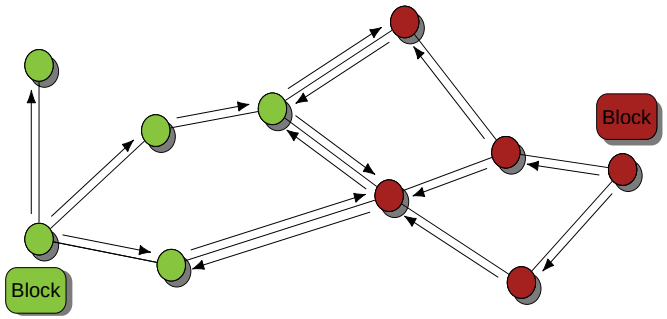
Avg Tx Fee in Dec 2017: > $50!

Just Change Parameters?

Propagation Speed



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

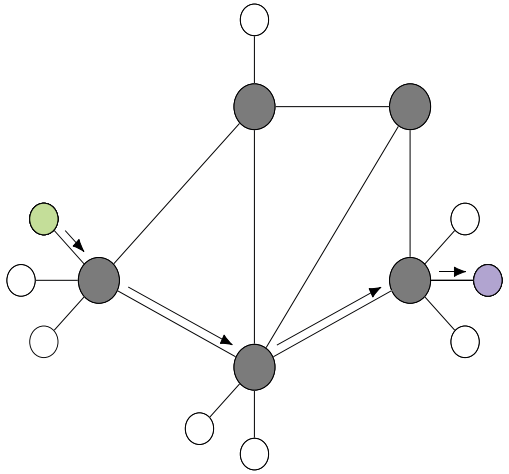
Micropayments?

Fundamental Scalability Problem:
Every Node Sees Every Single Transaction

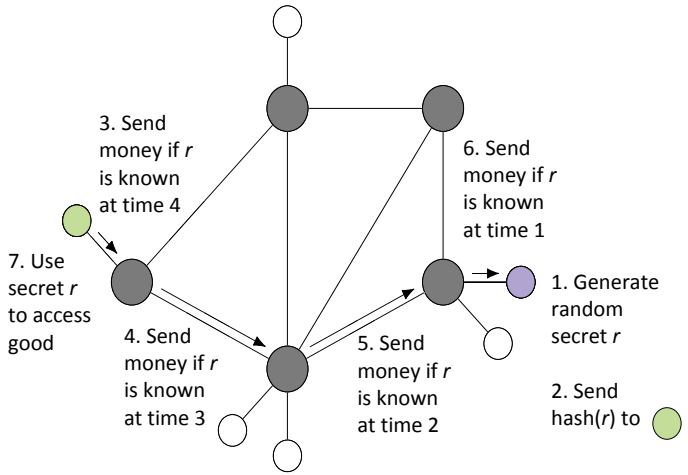
Payment Networks

Hashed Timelocked Contract (HTLC)

Payment Network



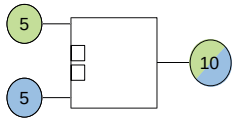
HTLC Example (sells to)



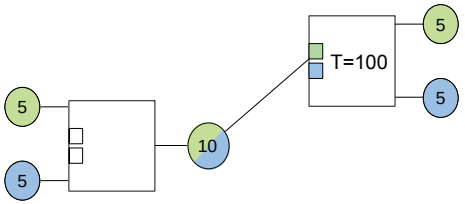
Single Hop in Network

Duplex Micropayment Channels (Example for Smart Contract)

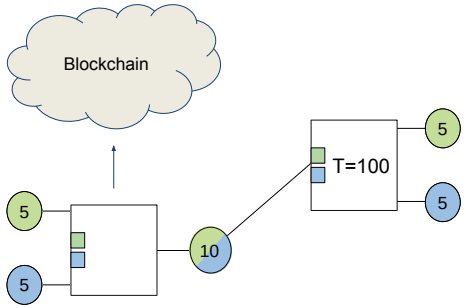
Duplex Micropayment Channel



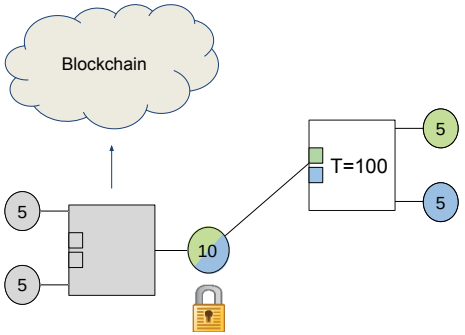
Duplex Micropayment Channel



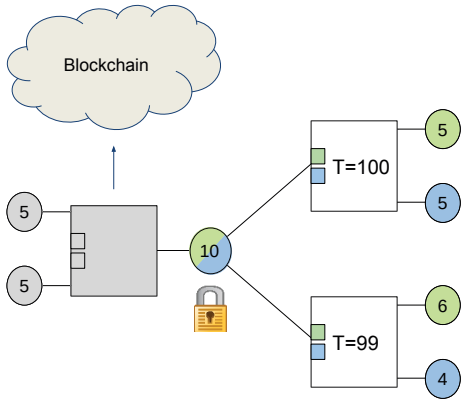
Duplex Micropayment Channel



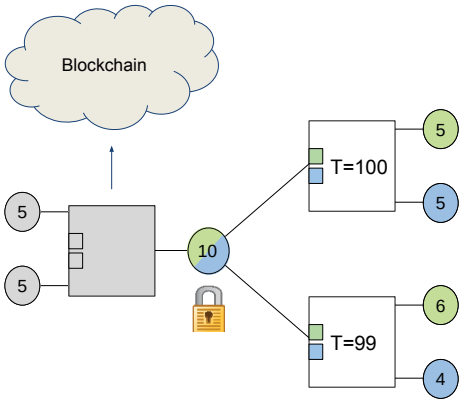
Duplex Micropayment Channel



Duplex Micropayment Channel



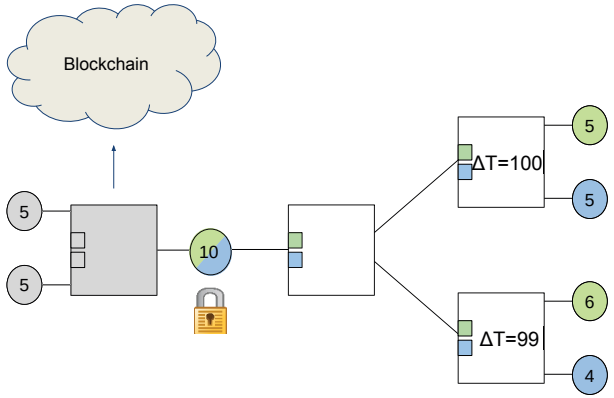
Duplex Micropayment Channel



Channel must be renewed often?

[Decker,W,2015]

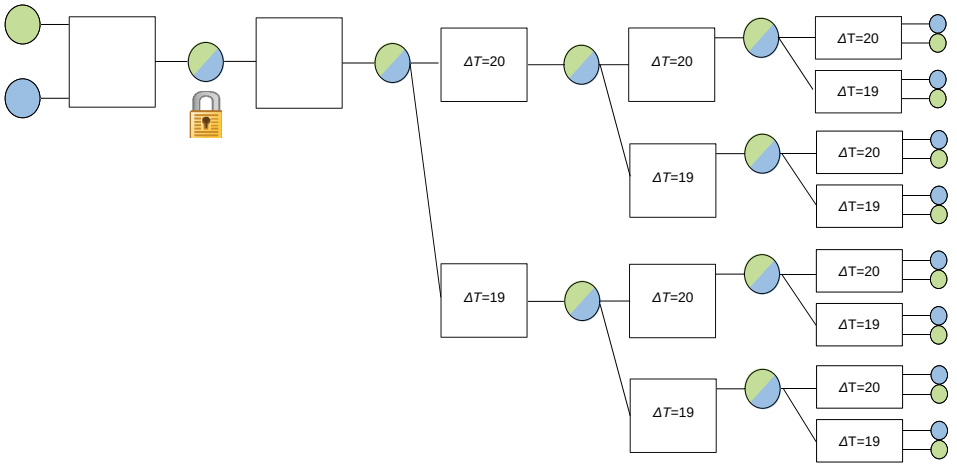
Duplex Micropayment Channel



Relative timelocks to keep channel alive forever!

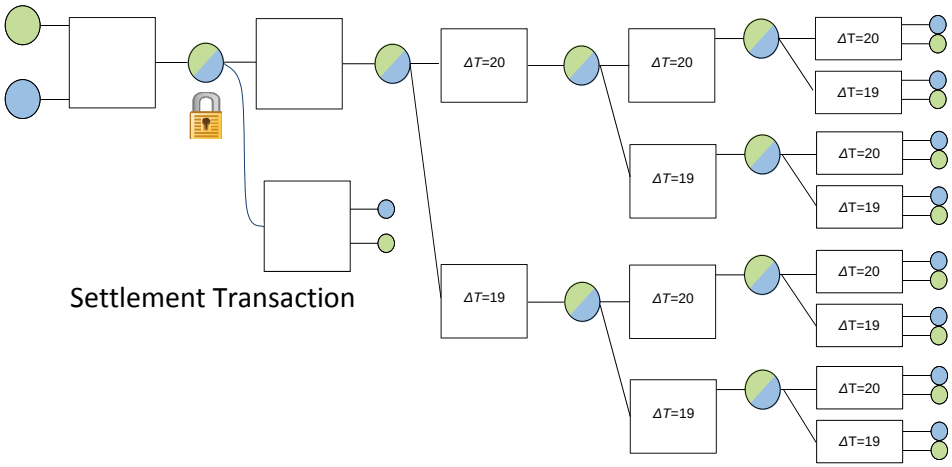
But only 99 transactions?

Duplex Micropayment Channel



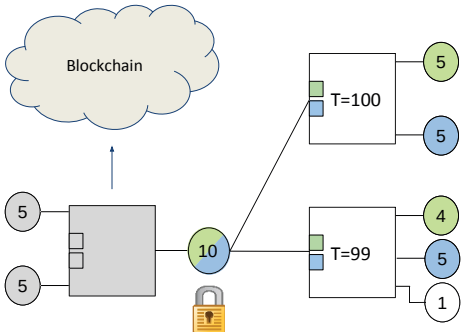
[Decker,W,2015]

Duplex Micropayment Channel

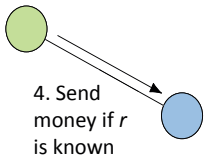


Settlement Transaction

HTLC Revisited

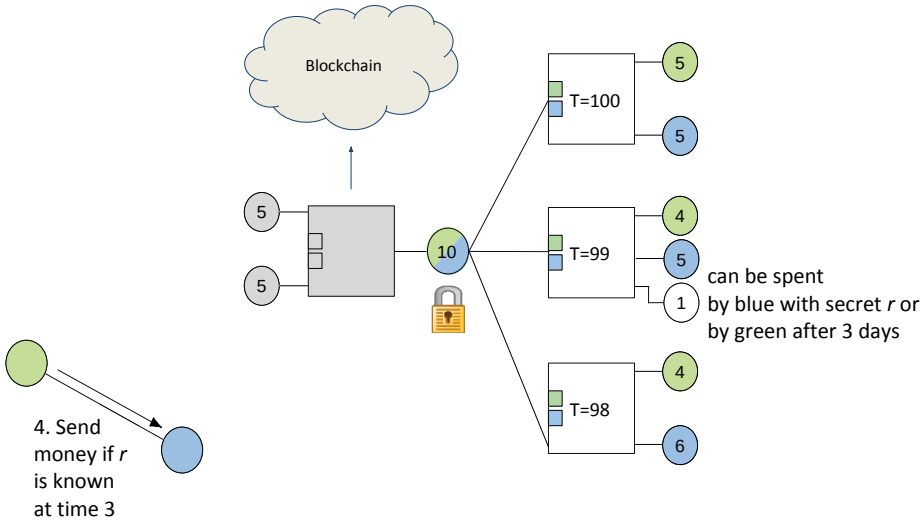


can be spent
by blue with secret *r* or
by green after 3 days



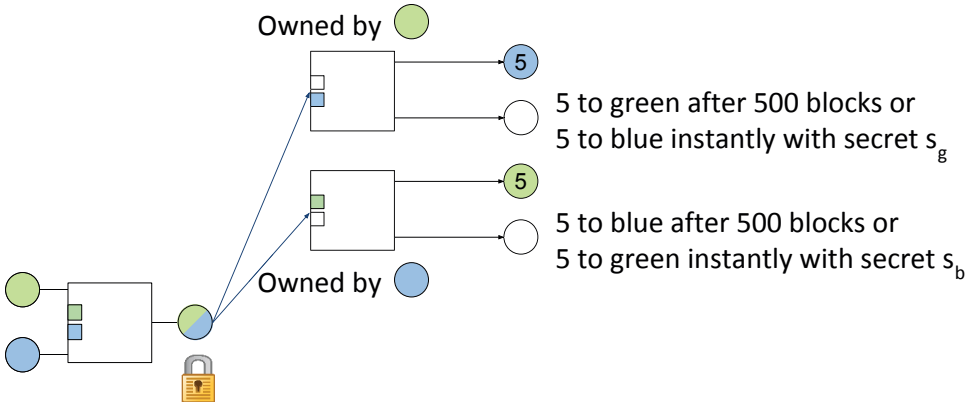
4. Send
money if *r*
is known
at time 3

HTLC Revisited



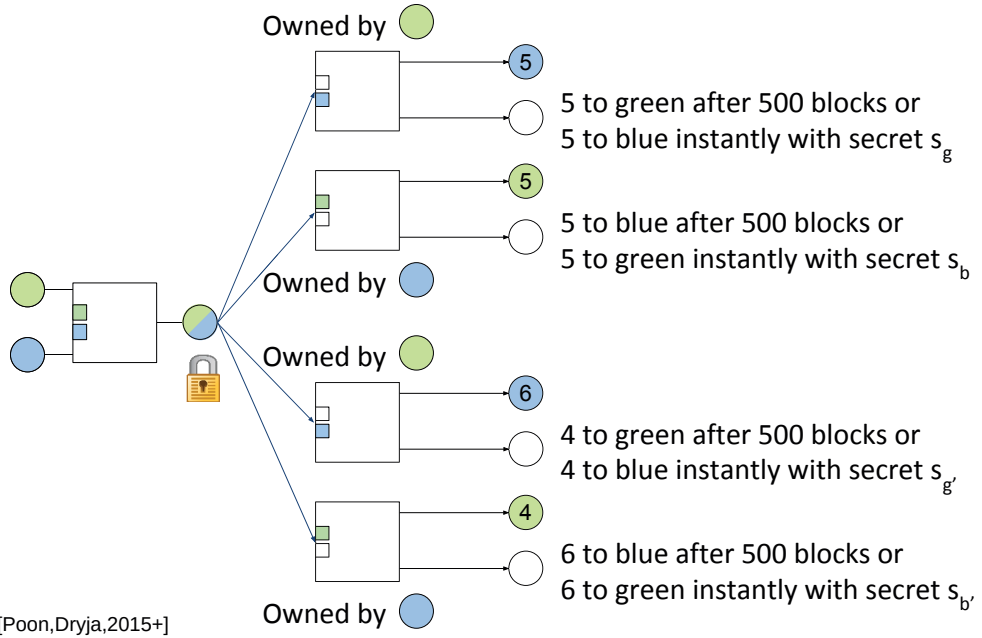
Lightning Network

Lightning Network Channel



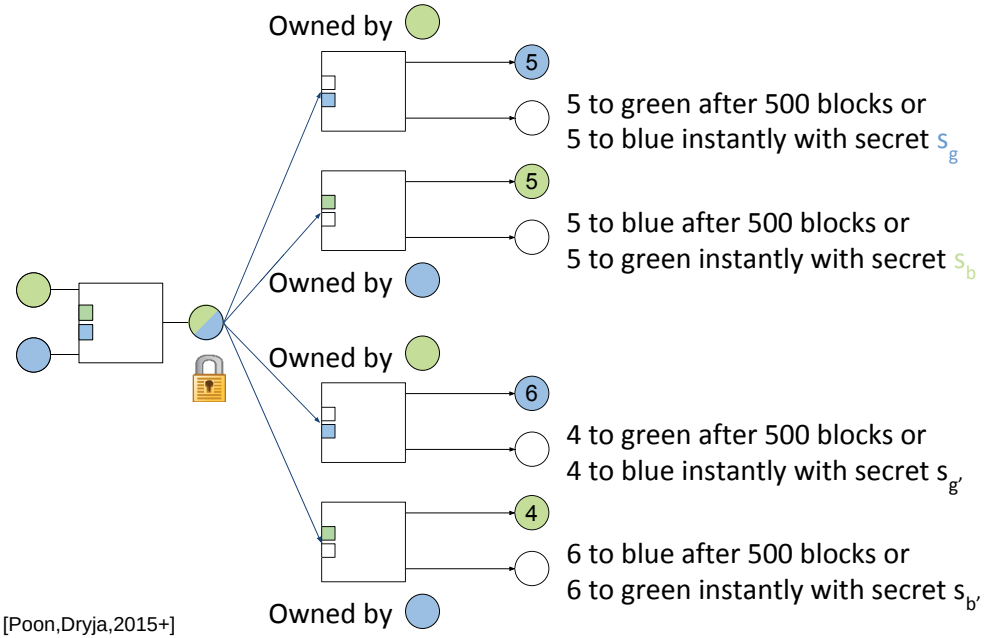
[Poon,Dryja,2015+]

Lightning Network Channel



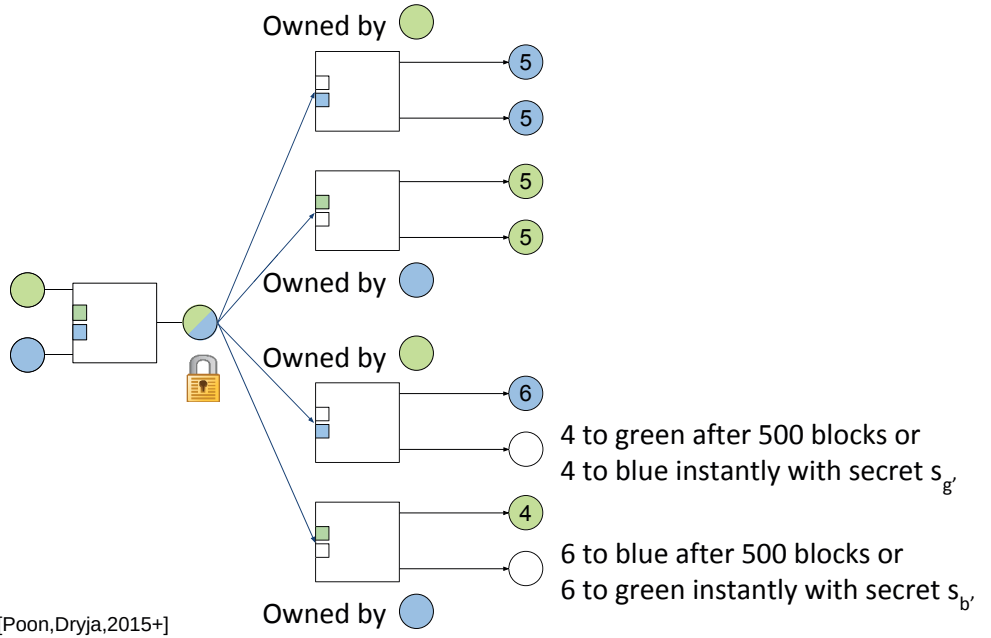
[Poon,Dryja,2015+]

Lightning Network Channel



[Poon,Dryja,2015+]

Lightning Network Channel



[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

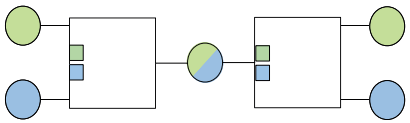
200-800M channels only

… has locked-in funds

all my bitcoins are locked-in… sad.

Blockchain Space

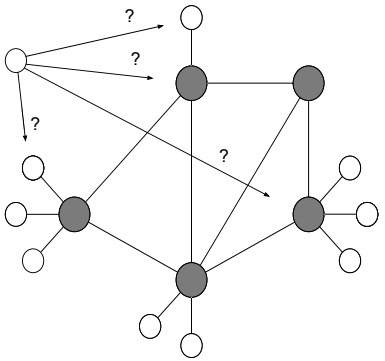
Blockchain space ≅ number of signatures



Funding Settlement

so far 4 signatures
for every channel

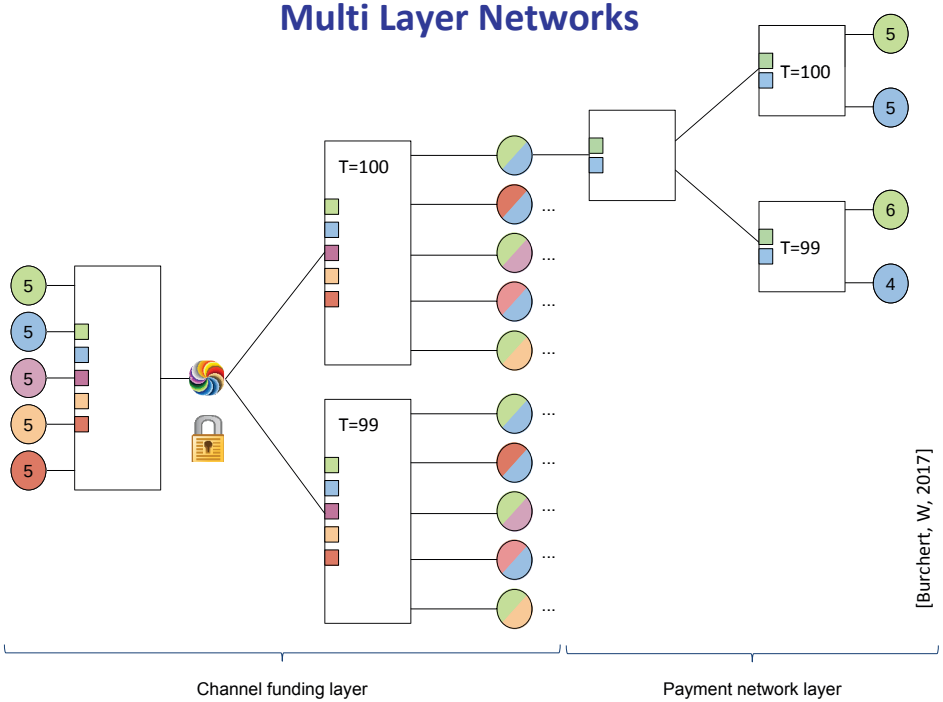
Locked Funds



A node wants to make connections…

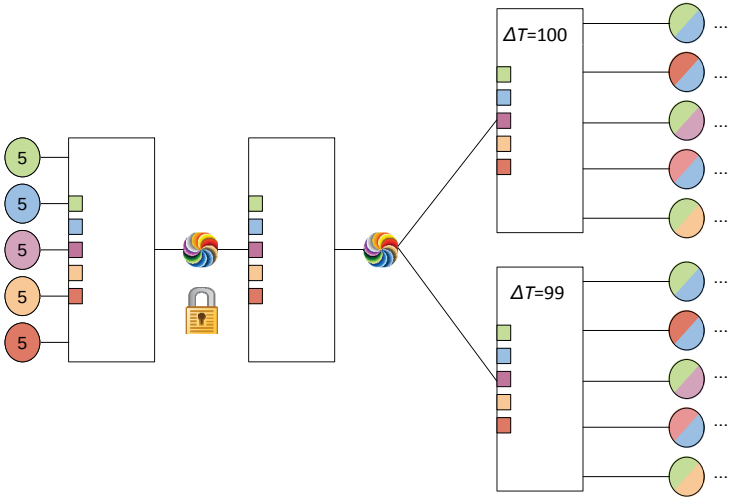
Where does it lock the funds?

Multi Layer Networks



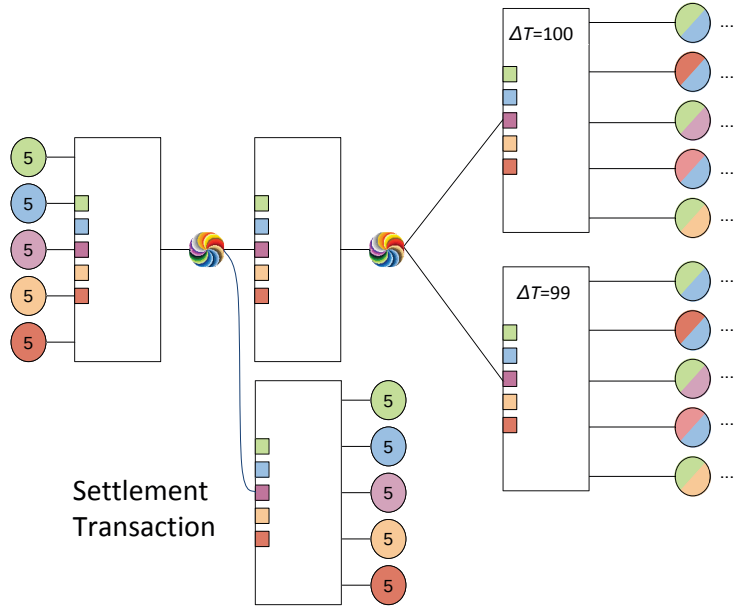
[Burchert, W, 2017]

Multi Layer Networks



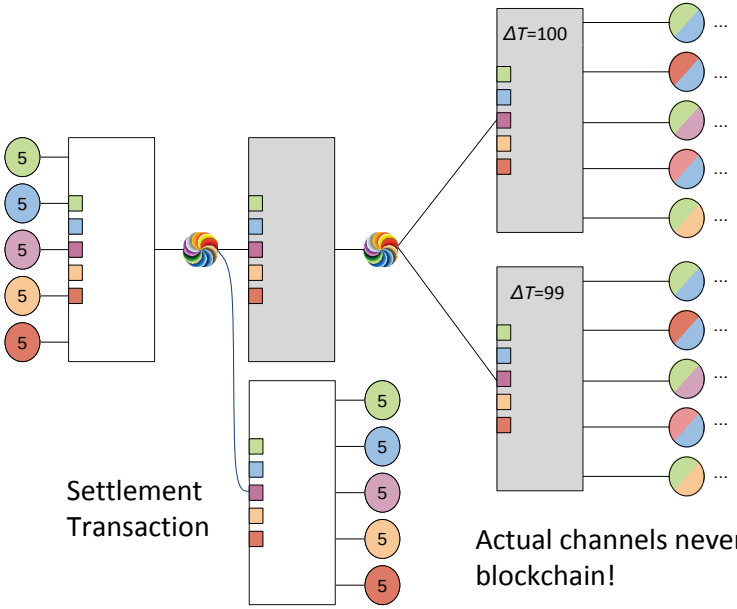
[Burchert, W, 2017]

Multi Layer Networks



[Burchert, W, 2017]

Multi Layer Networks

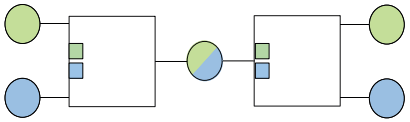


Actual channels never reach the blockchain!

[Burchert, W, 2017]

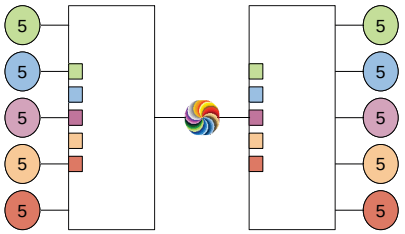
Blockchain Transactions

old



4 signatures per channel

new

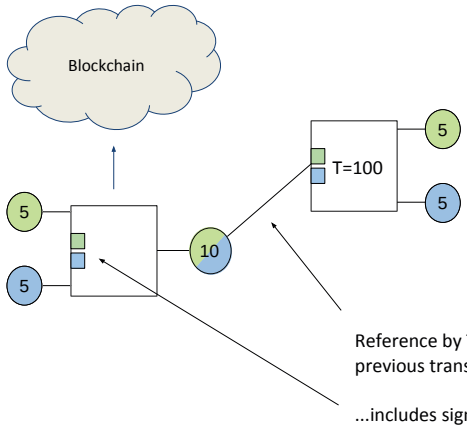


2 signatures per user

independent of channels

What Else is Needed?

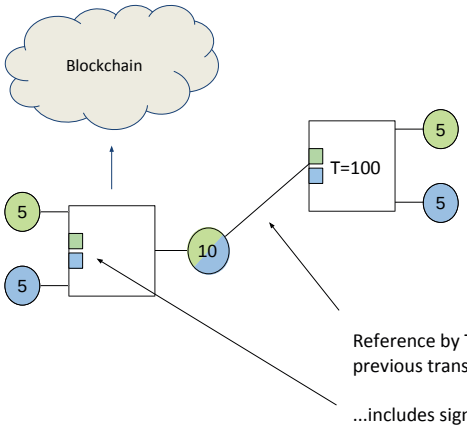
Spending from Unsigned Transactions



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.

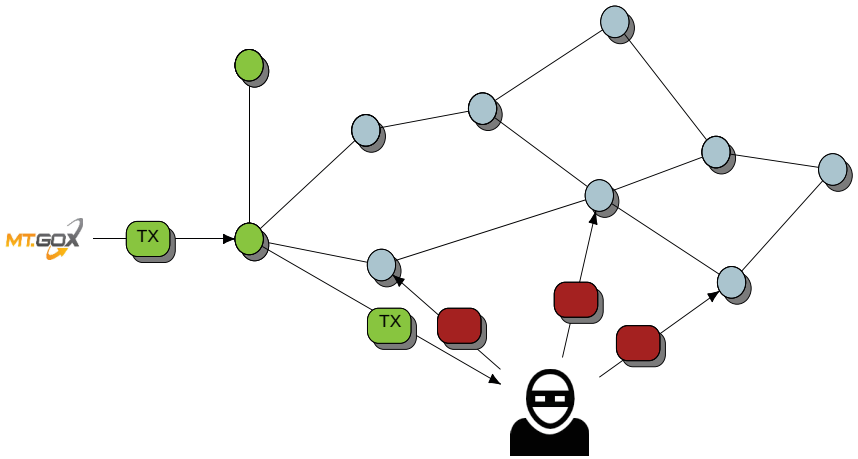
Signatures

0000 61afbb4de9f8b874861e

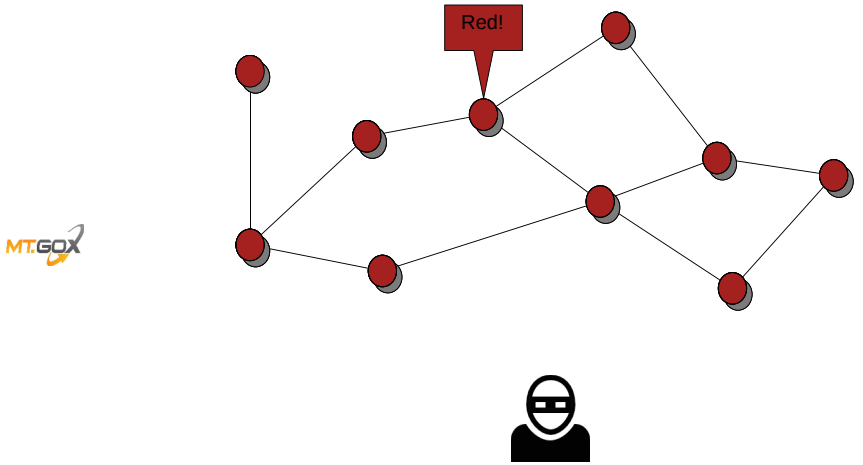
There are multiple ways to serialize a signature:

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

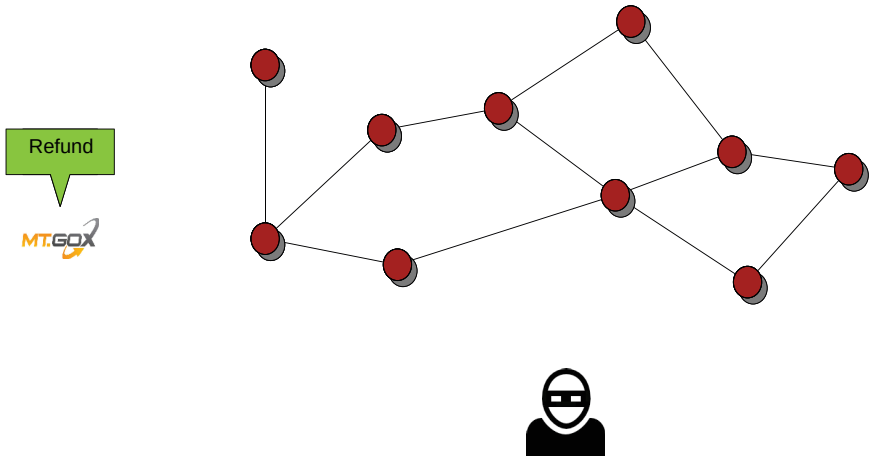
Transaction Malleability Attack



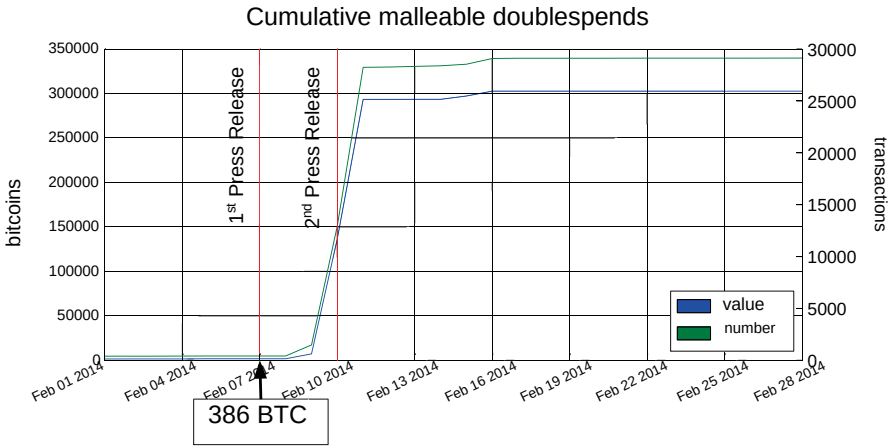
Transaction Malleability Attack



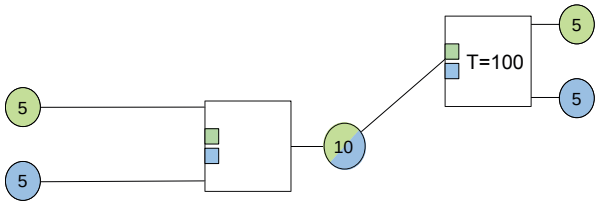
Transaction Malleability Attack



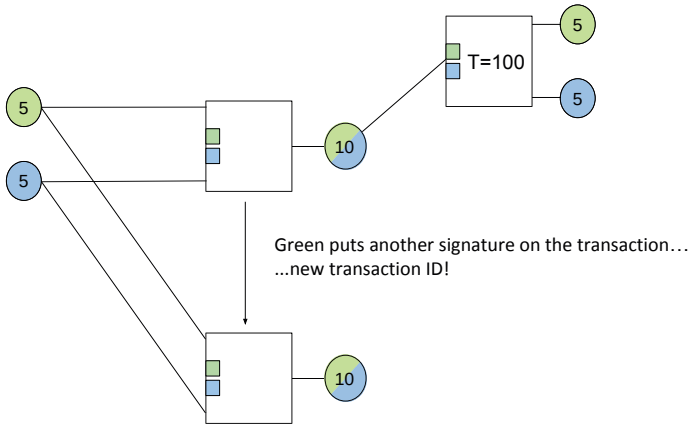
Incident Timeline



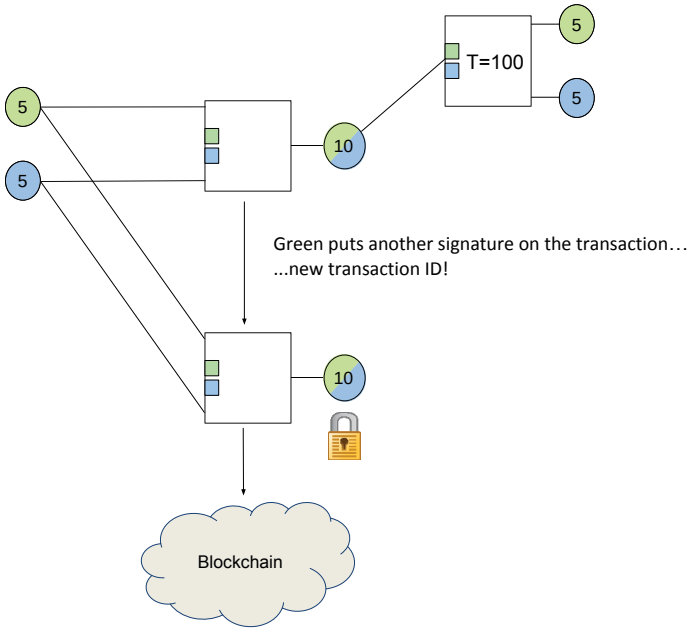
Malleability



Malleability



Malleability



How is this fixed?

Segregated Witness

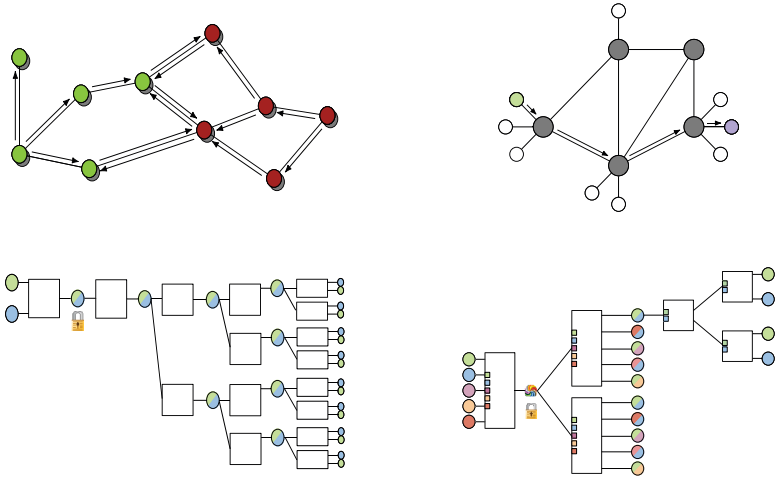
Introduce a new type of transaction

Signatures are separated from the rest

Softfork compatible

Became active as BIP 141 in August 2017

Summary



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

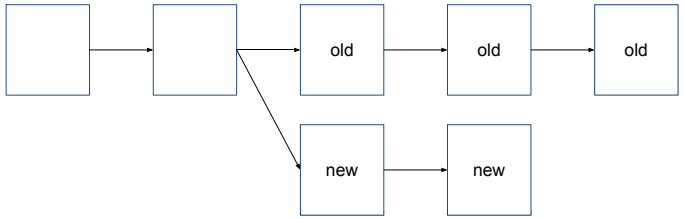
- New miners reject old blocks
- Old miners reject new blocks

-> Two blockchains exist

Softforks

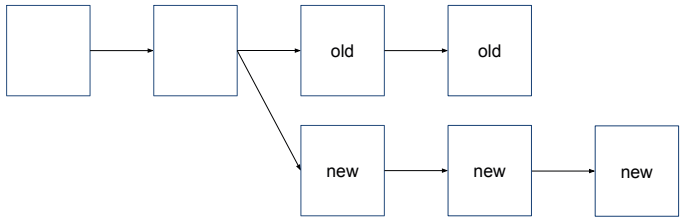
Old miners accept blocks of the new miners

Old miners are majority



Everyone switches here

New miners are majority



Everyone switches here

Economy and Other Problems

Roger Wattenhofer

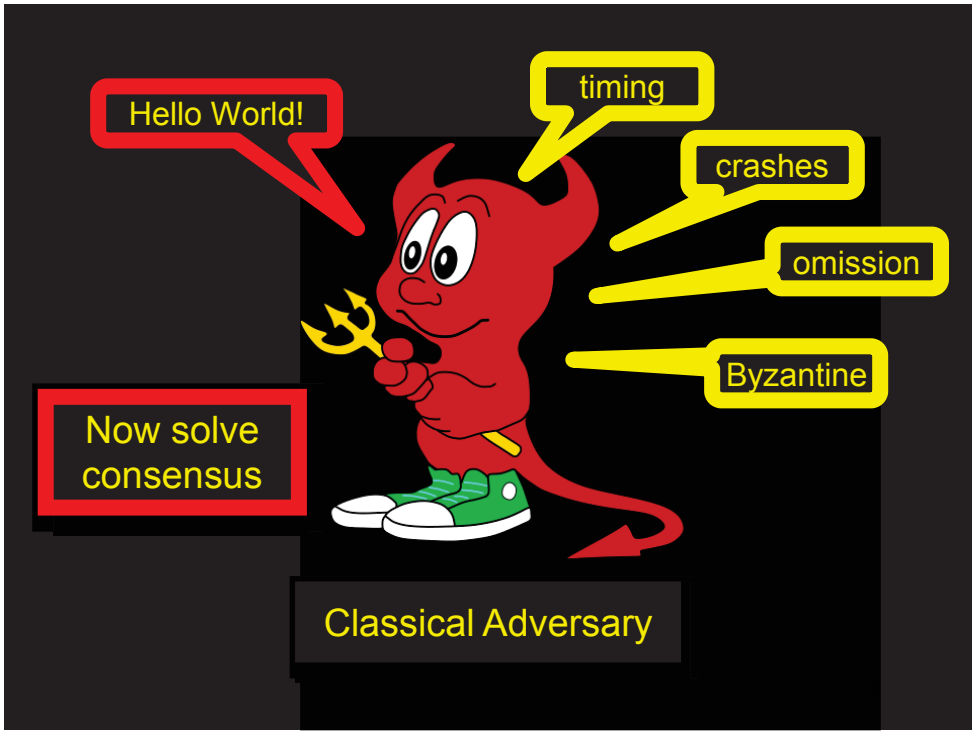
(Thanks to Maurice Herlihy for some colorful slides)

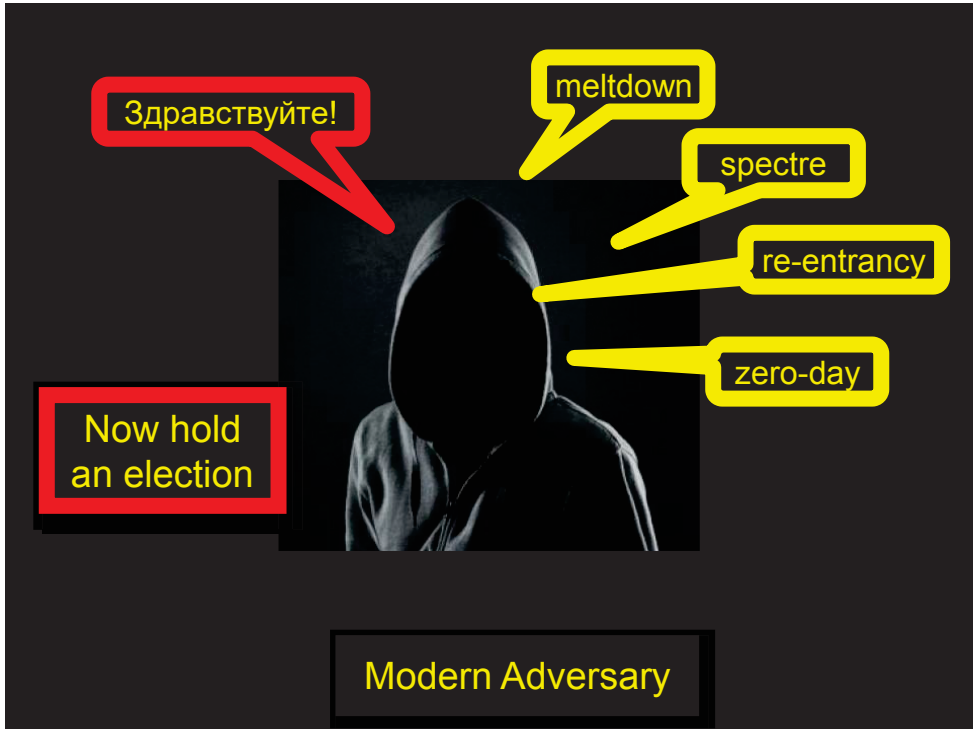
ETH Zurich – Distributed Computing Group

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





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"

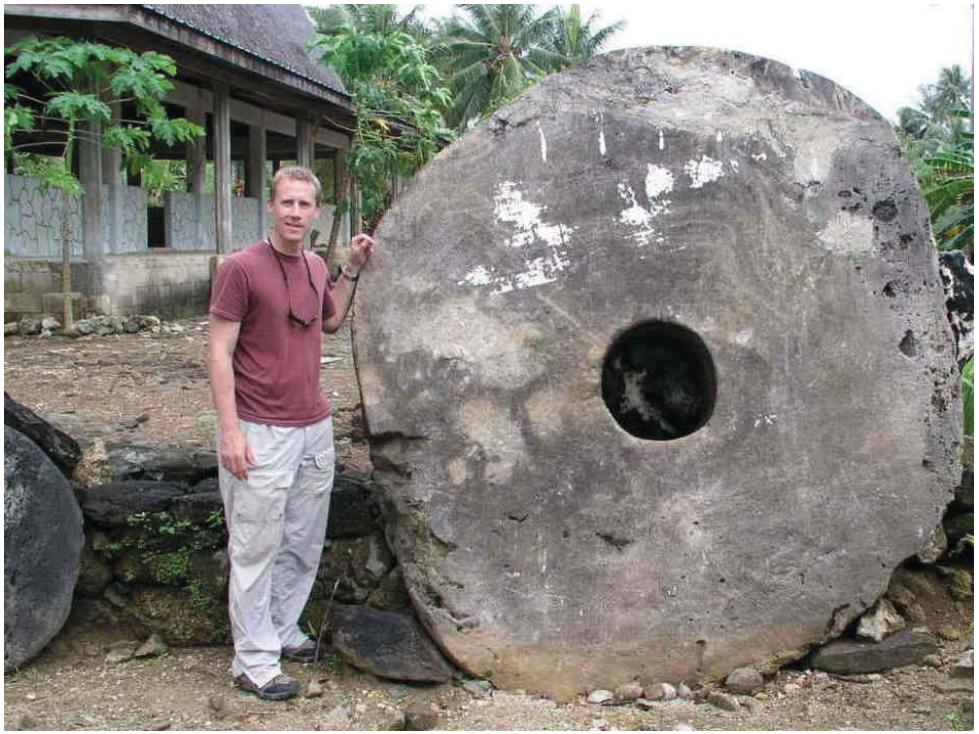
"Unlikely to impact the finance sector"

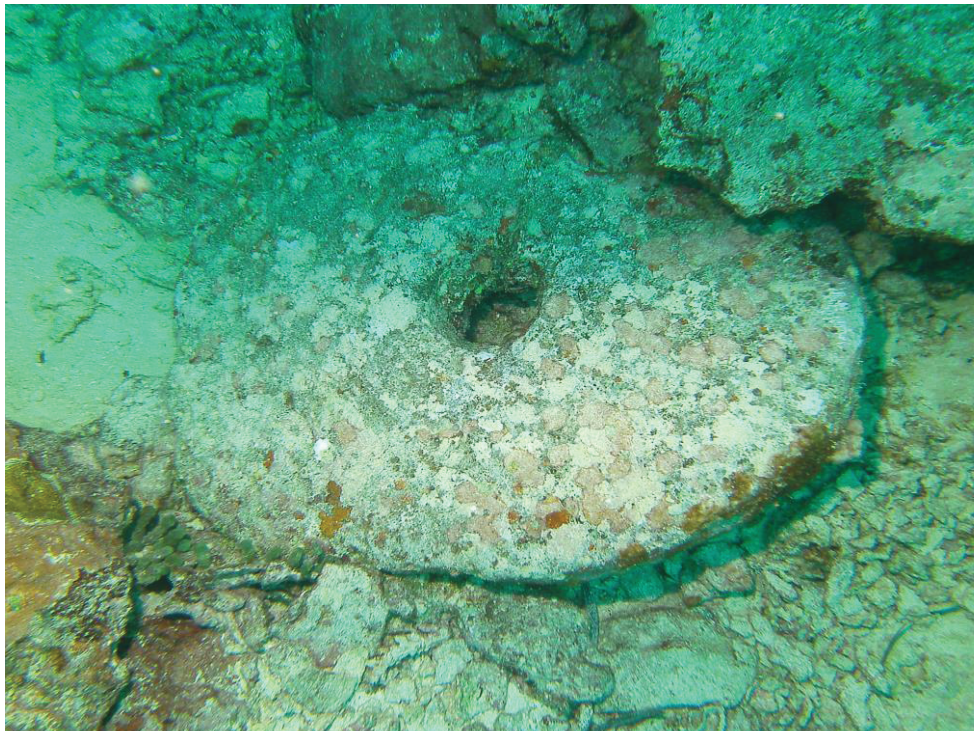
What is Money?

BTC in USD

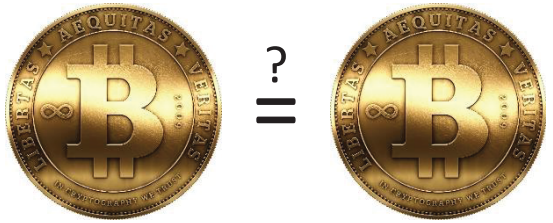

10,000
1,000
100
10
1.0000
USD


Kantonalbank
500 g
Fine Gold
999.9
2115
21152
250g
Fine Gold
999.9
18722
999.9
005719
FEINGOLD





Fungibility

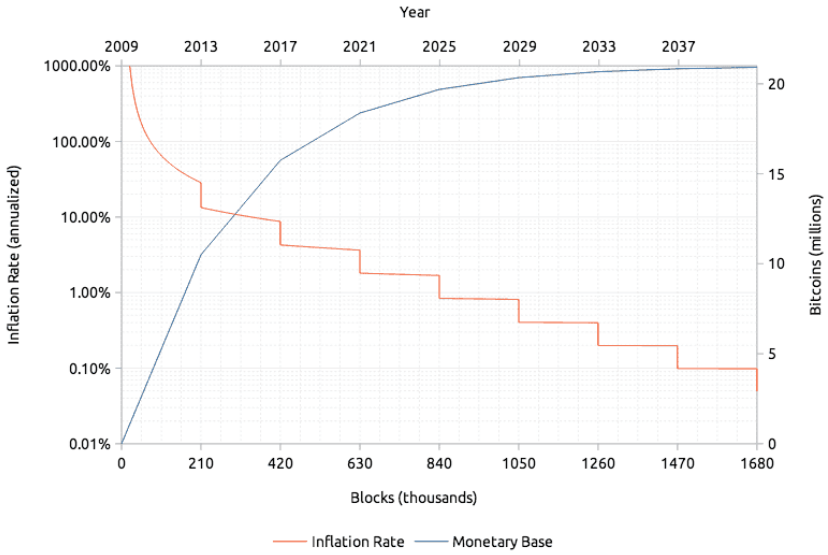


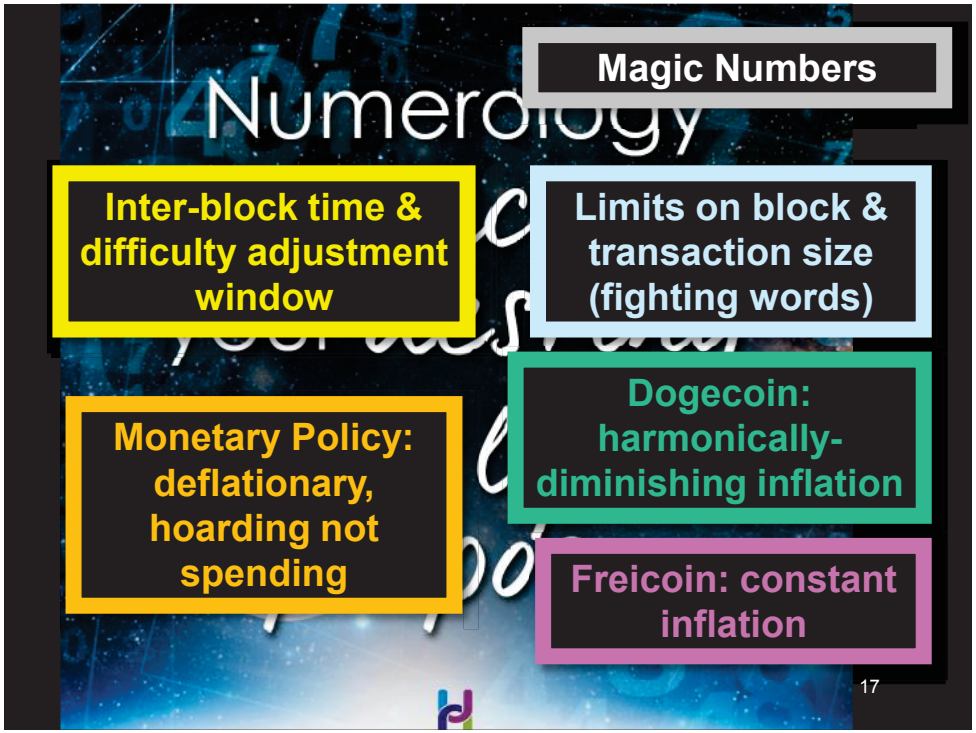
18

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

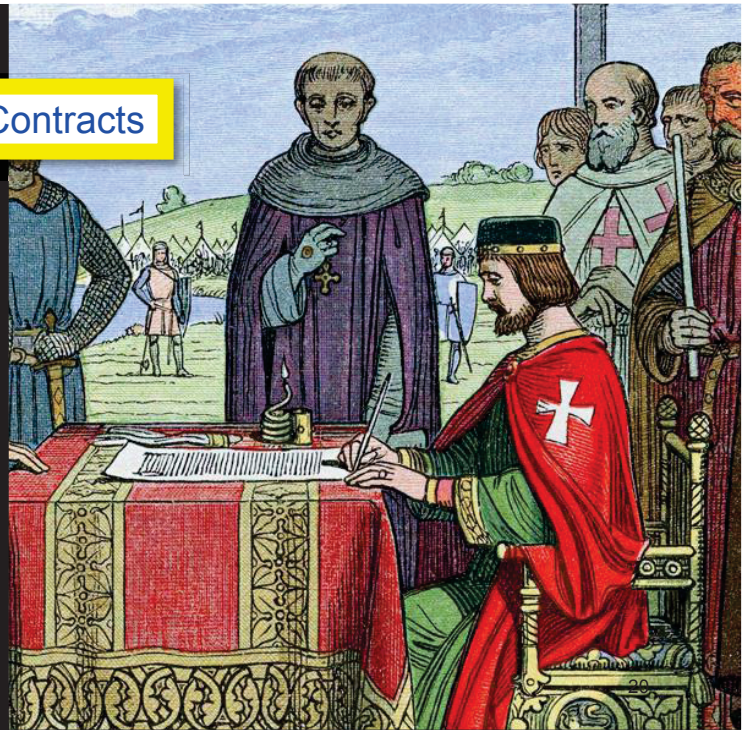




What is Money?

What is Money?

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.

… no such specification for The DAO. There is no …cification for what The DAO is *supposed to* … are hardly any comments in The DAO … developers may have been thinking …

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

… It was its …

THE LATEST HEADLINES

Page Discussion

ERC20 Token Standard

See also Ethereum Based Tokens and ERC20 Wallet Support

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

Standard for tradeable tokens

Widely used for ICOs

Market cap about $40 Billion

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

```
function totalSupply);
function balanceOf(address _to, … returns (uint balance);
function transfer(address _from, … returns (bool success);
function transferFrom(address _spender, uint _value) returns (bool success);
function approve(address _owner, address _spender) returns (uint _value);
function allowance(address indexed _from, address indexed _to, uint _value);
event Transfer(address indexed _owner, address indexed _spender, uint _value);
event Approval
```

I am willing to allow this party …

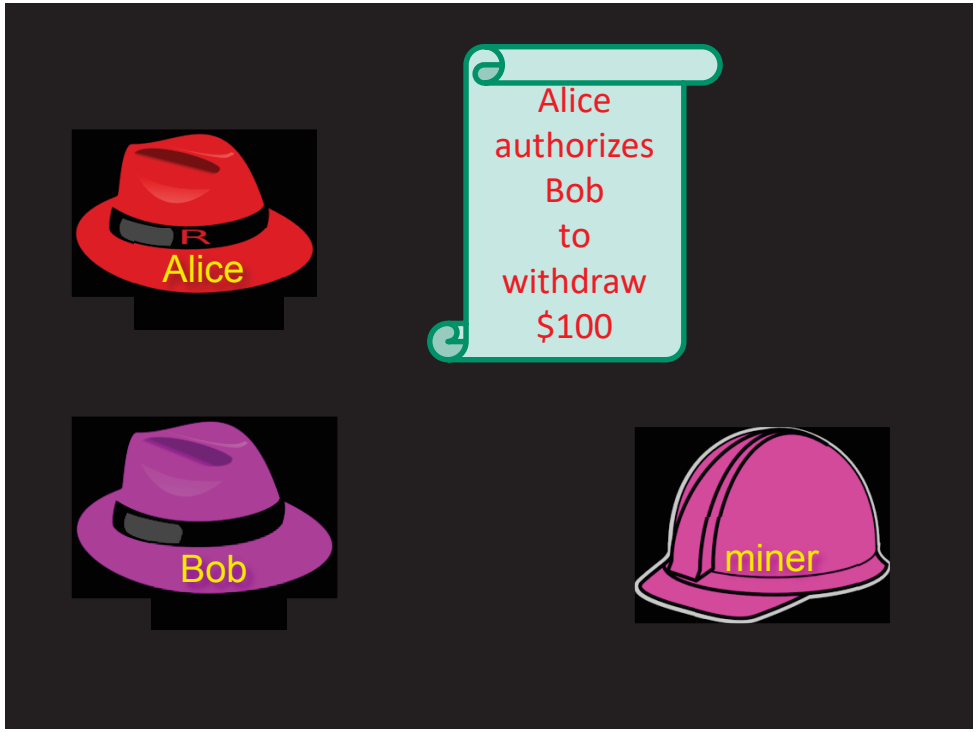
… to withdraw this amount …

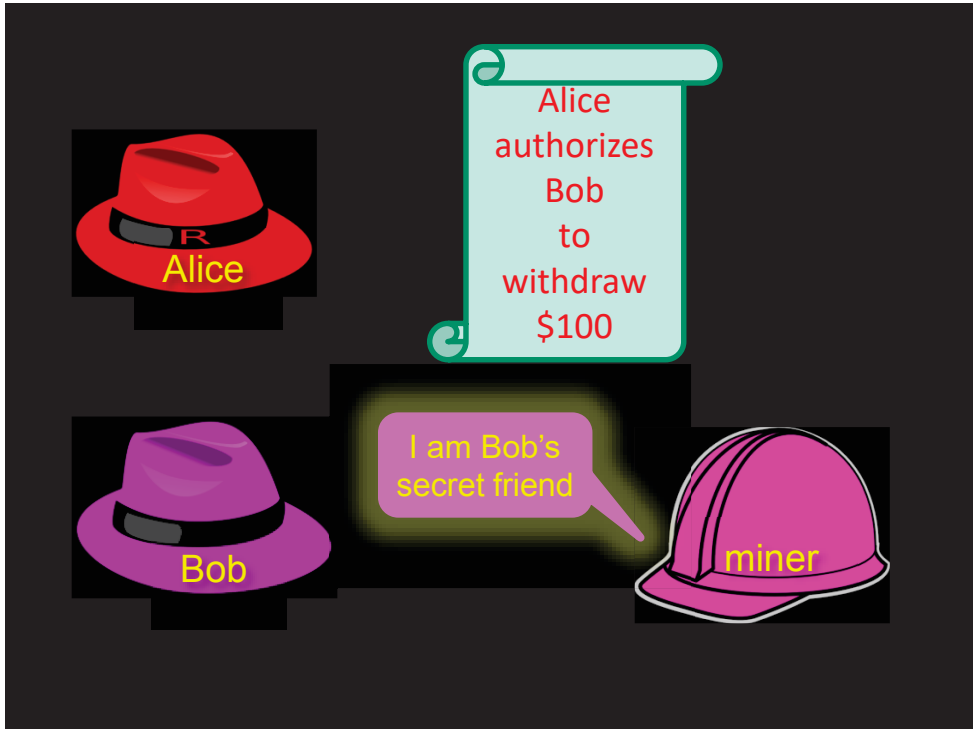
```
}

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

function allowance(address …ner, address _spender) constant returns (uint2
```

… from my account.

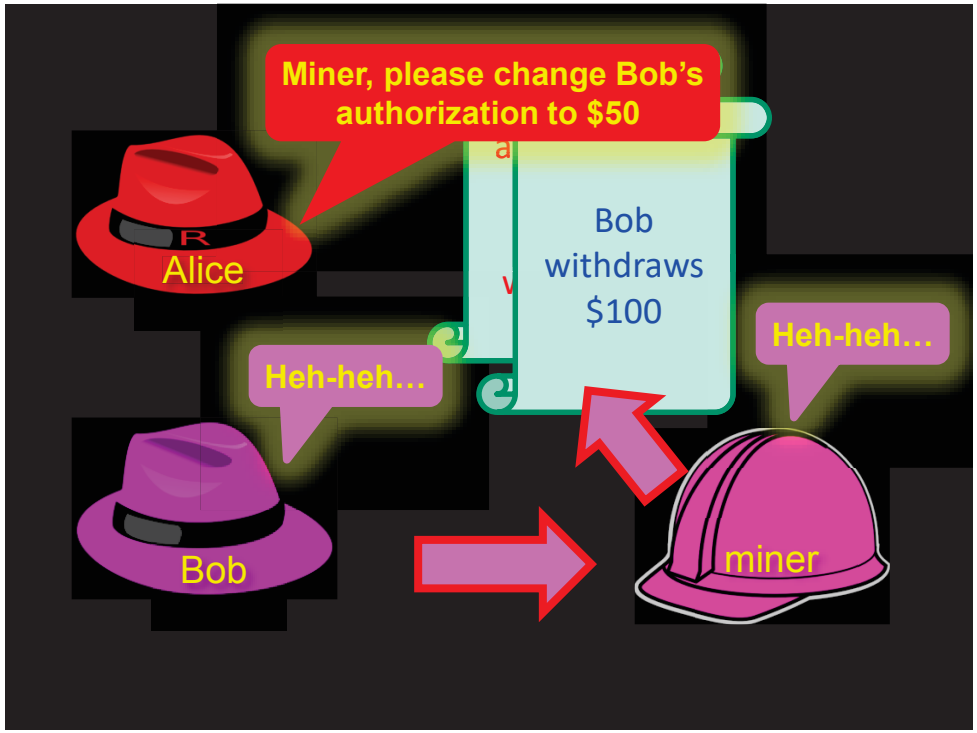

Alice
authorizes
Bob
to
withdraw
$100
Alice
Bob
miner

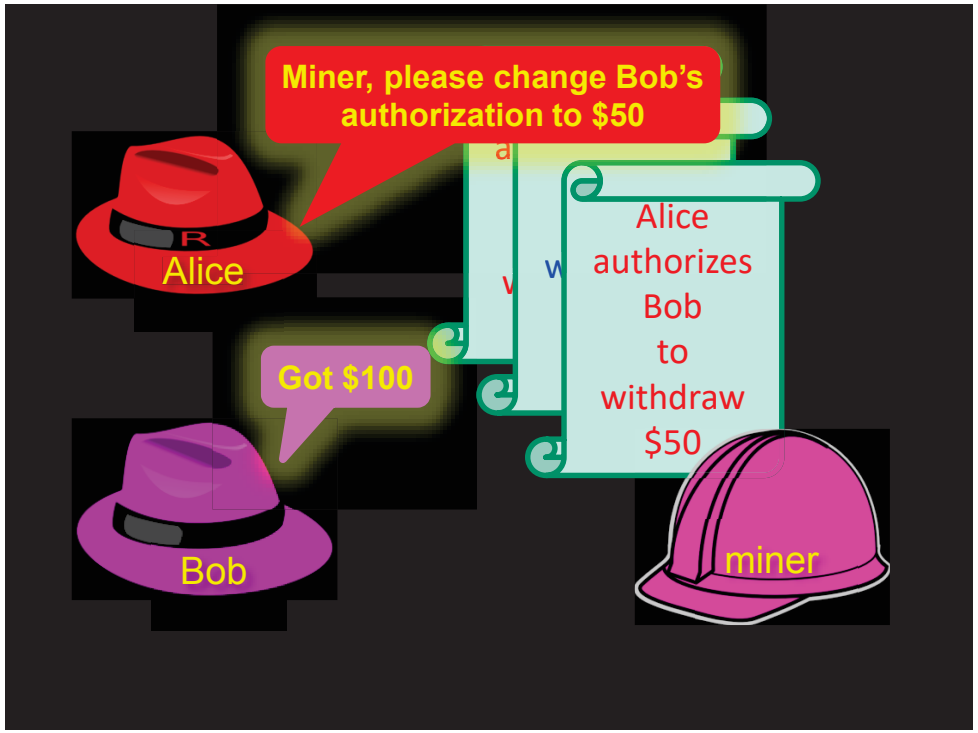

Alice
authorizes
Bob
to
withdraw
$100
I am Bob's
secret friend
Alice
Bob
miner

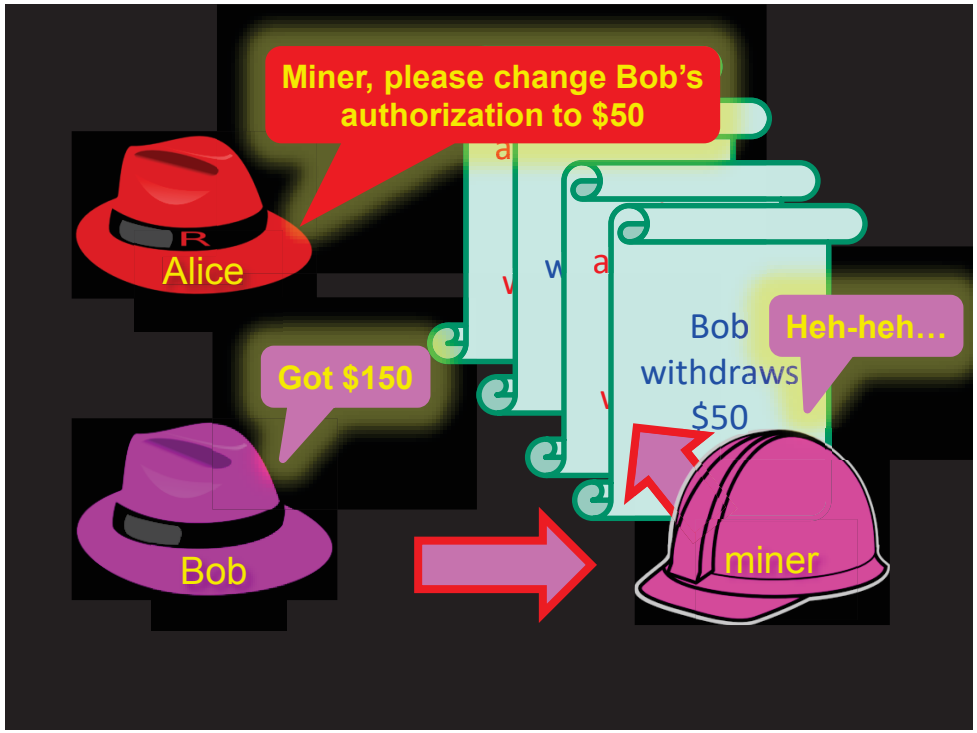

Miner, please change Bob's
authorization to $50
authorizes
Bob
to
withdraw
$100
Alice
!!!
!!!
Bob
miner


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

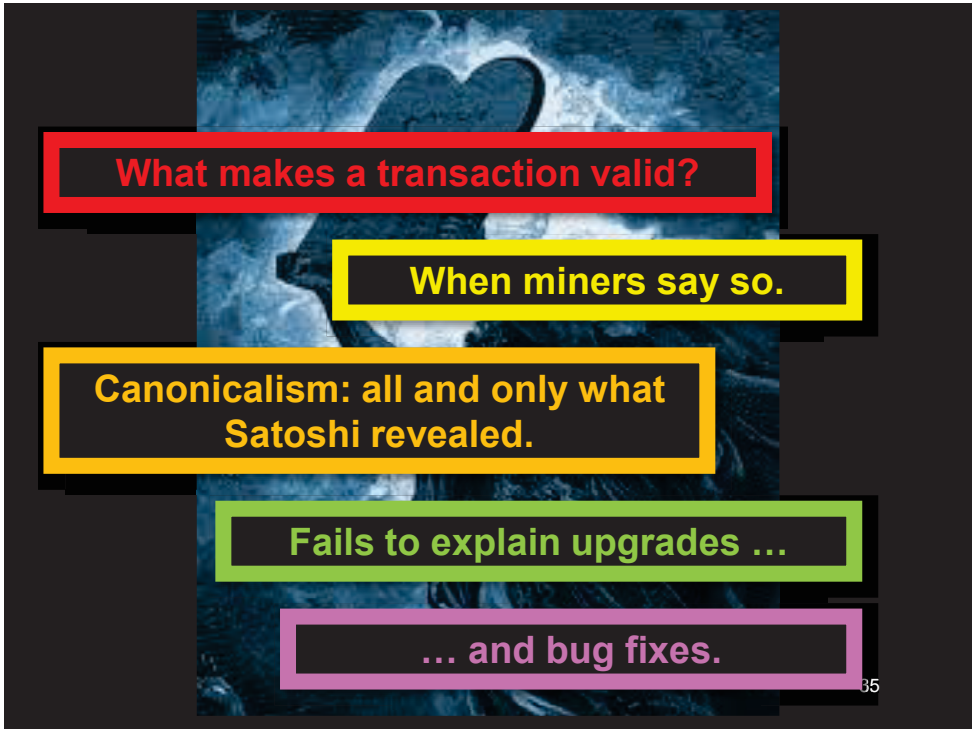

Miner, please change Bob's authorization to $50
Alice
Bob
withdraws
$100
Bob
miner

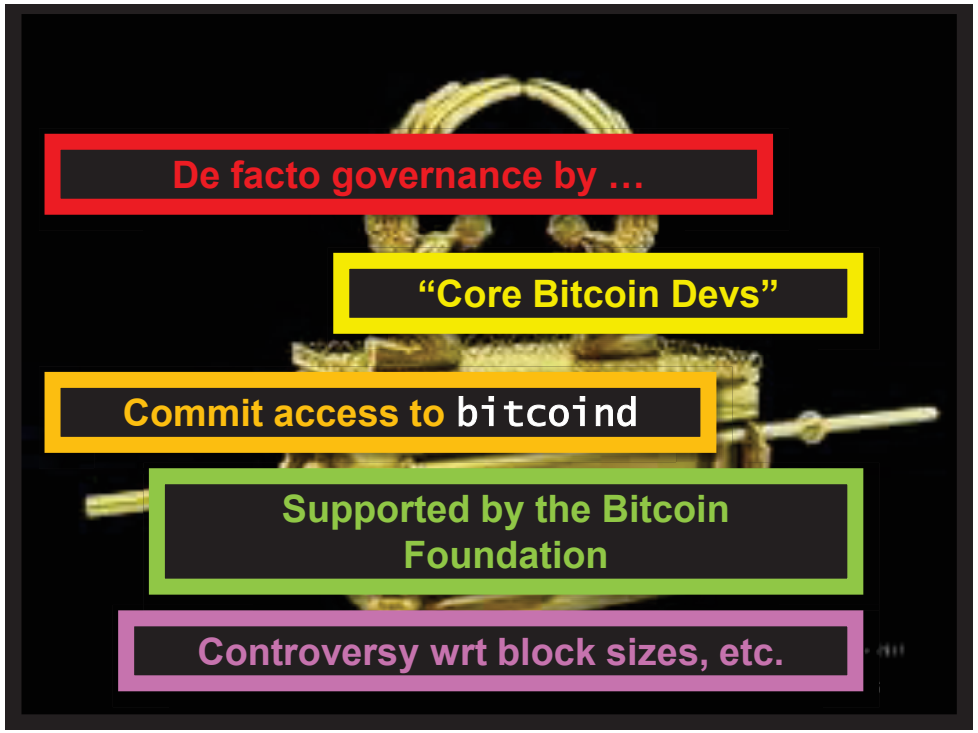

Miner, please change Bob's authorization to $50
Alice
Bob
withdraws
$100
Heh-heh…
Heh-heh…
Bob
miner

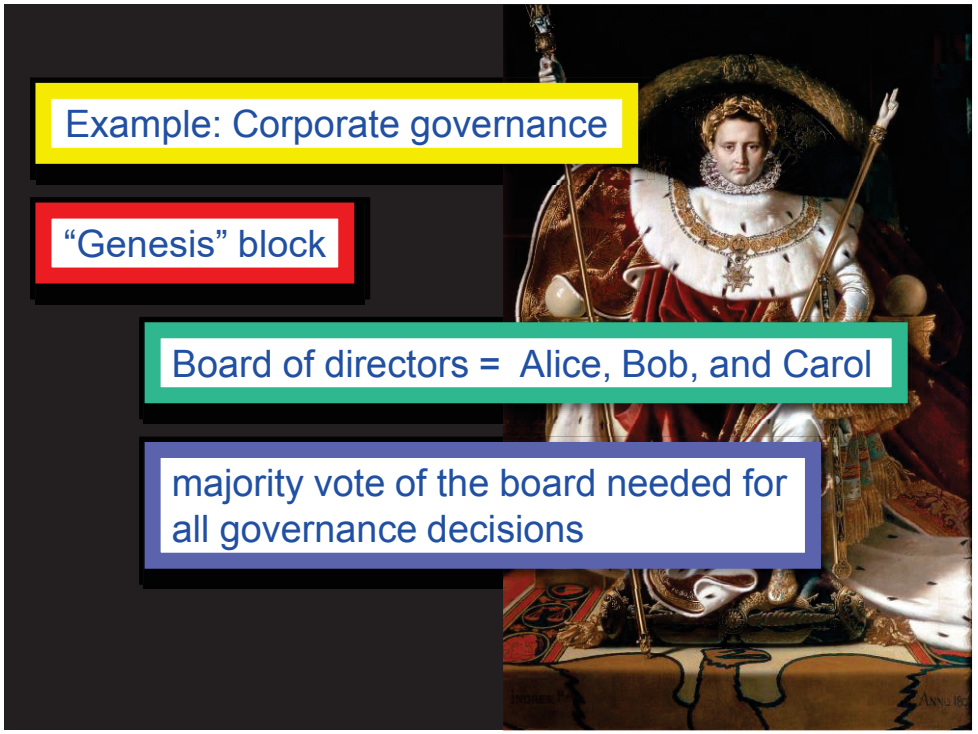

Miner, please change Bob's authorization to $50
Alice
Alice
authorizes
Bob
to
withdraw
$50
Got $100
Bob
miner


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

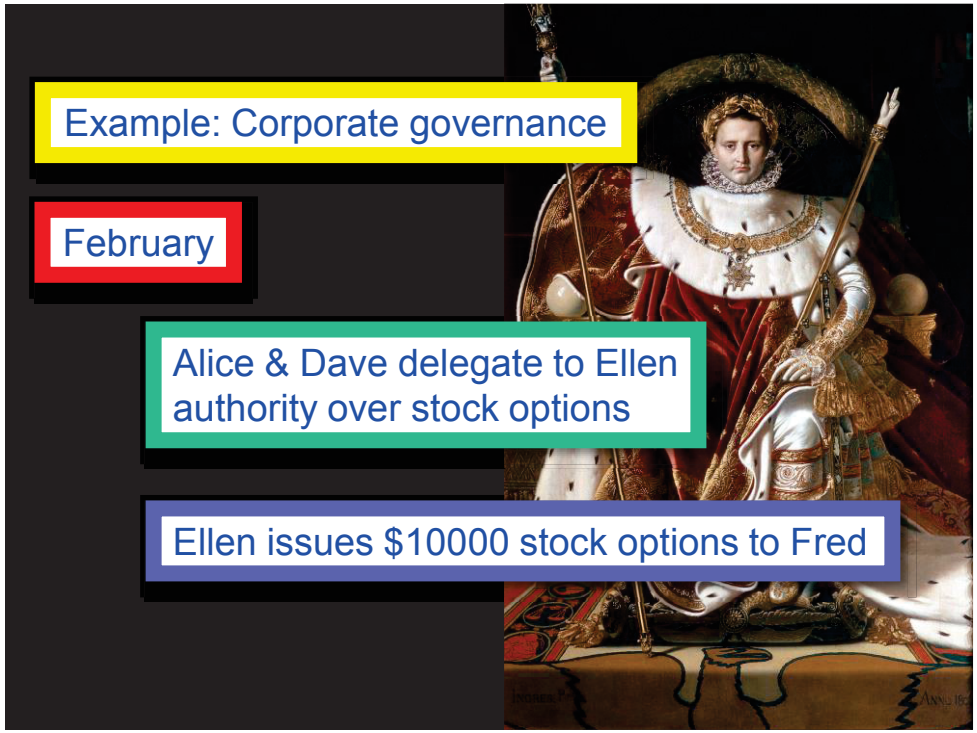

user
miner
relay
developer
hodler

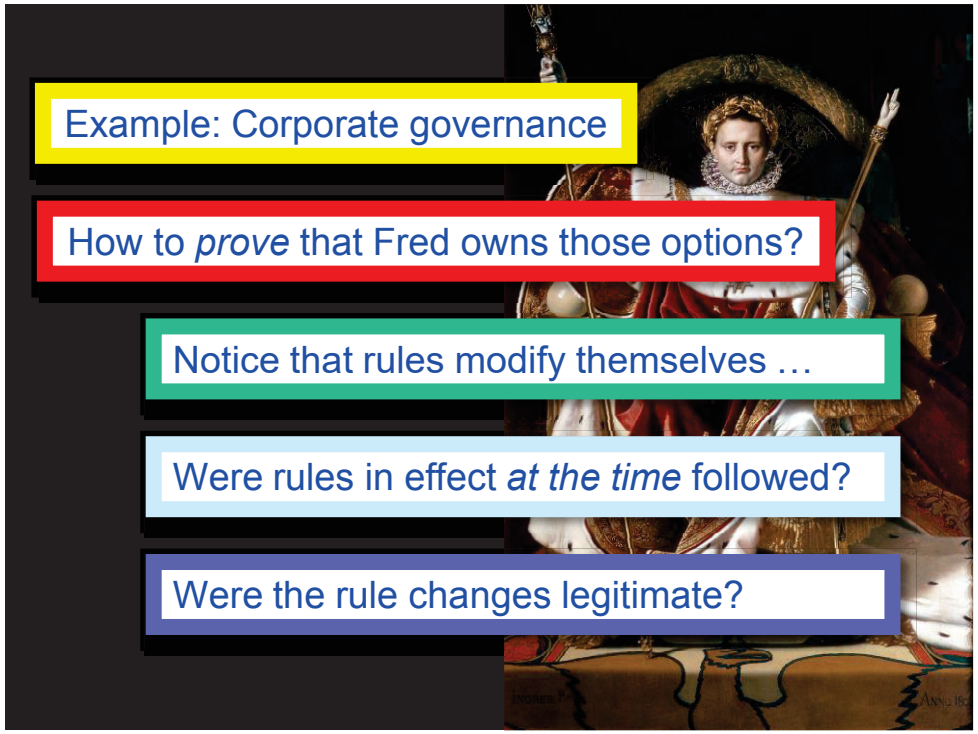

What makes a transaction valid?
When miners say so.
Canonicalism: all and only what Satoshi revealed.
Fails to explain upgrades …
… and bug fixes.
35

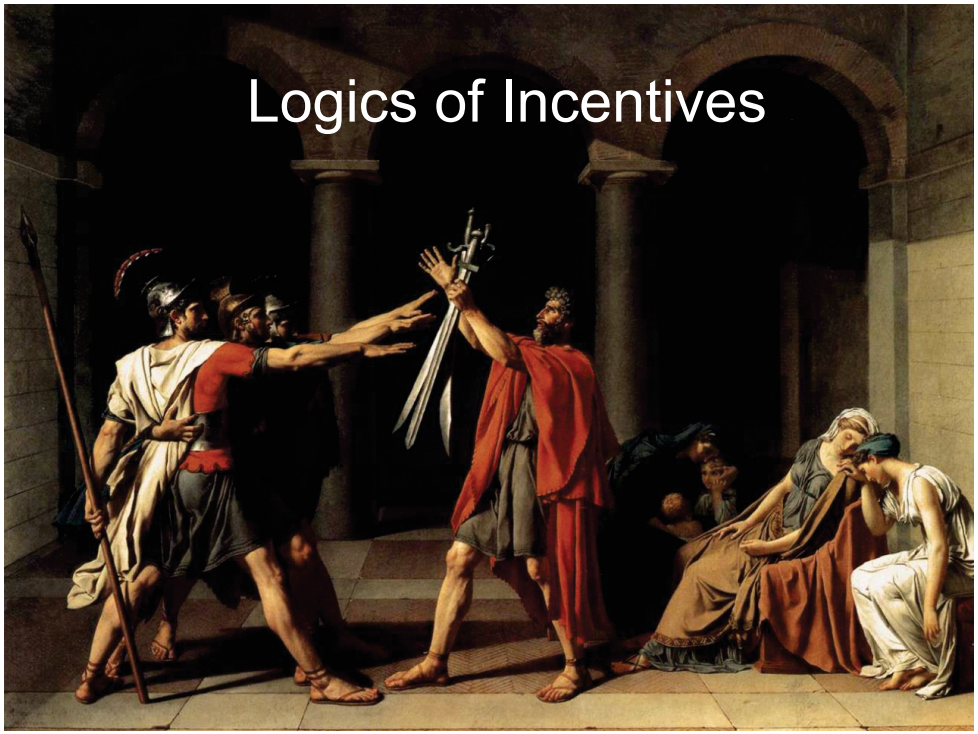

De facto governance by …
“Core Bitcoin Devs”
Commit access to bitcoind
Supported by the Bitcoin Foundation
Controversy wrt block sizes, etc.

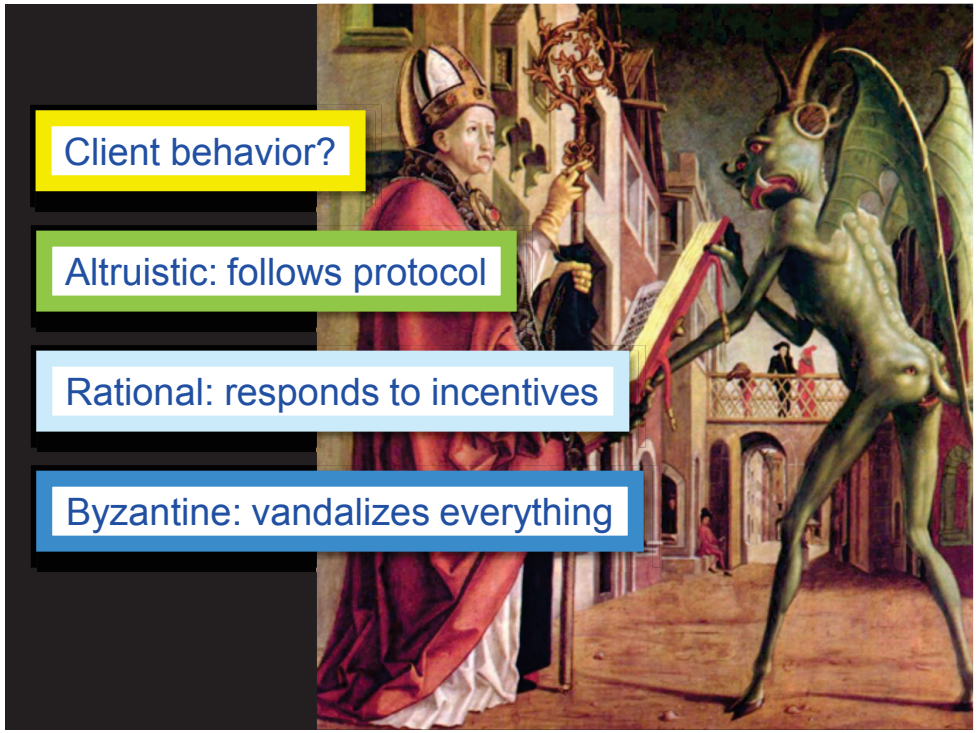

Example: Corporate governance
“Genesis” block
Board of directors = Alice, Bob, and Carol
majority vote of the board needed for all governance decisions


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
Eventual 51% attack!


Small-Game Fallacy:
If you assume motive is short-term profit maximization …
You will miss this attack!

Game Theory

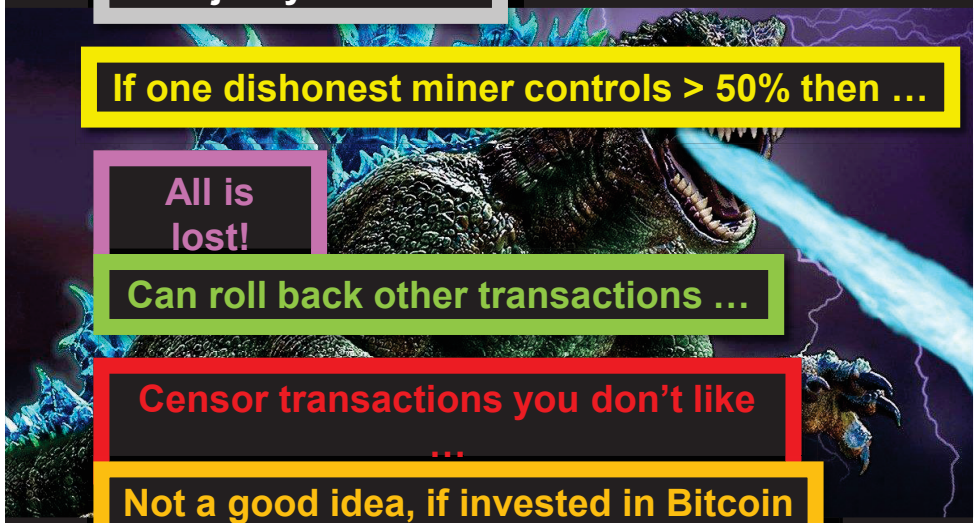
Nakamoto claims: Bitcoin is stable as long as miners follow own self-interest.

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?

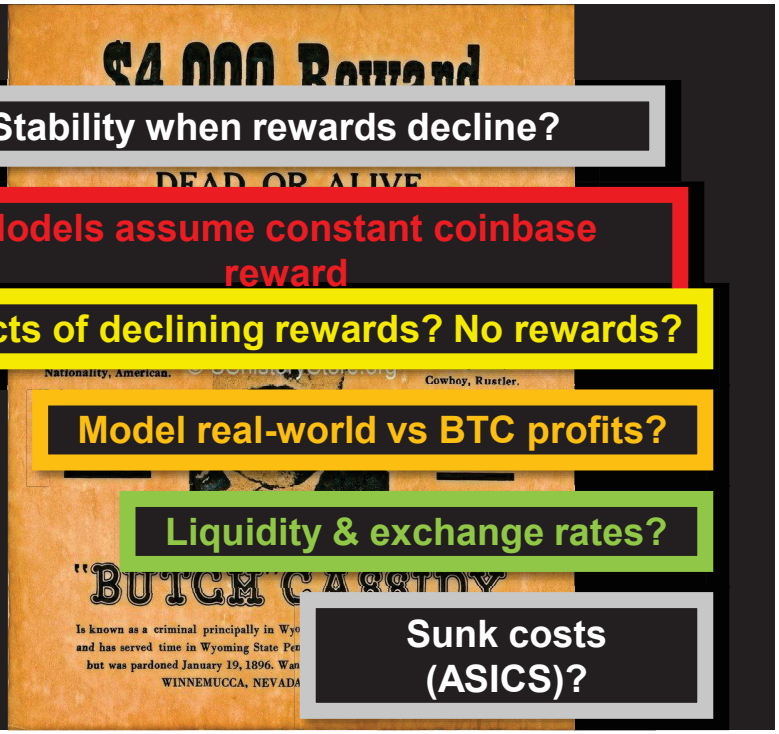
Miners could form cartel …

… to simulate evil majority miner?

Stable? Would members defect?

Real issue: mining pools are a thing

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

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

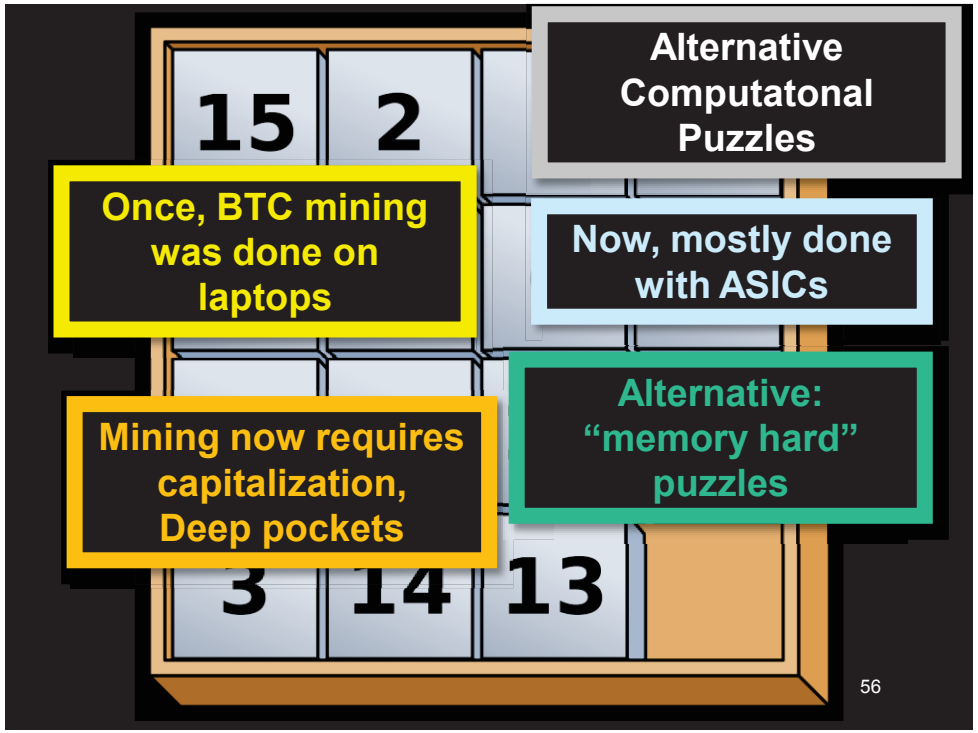
Peer-to-Peer stability

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



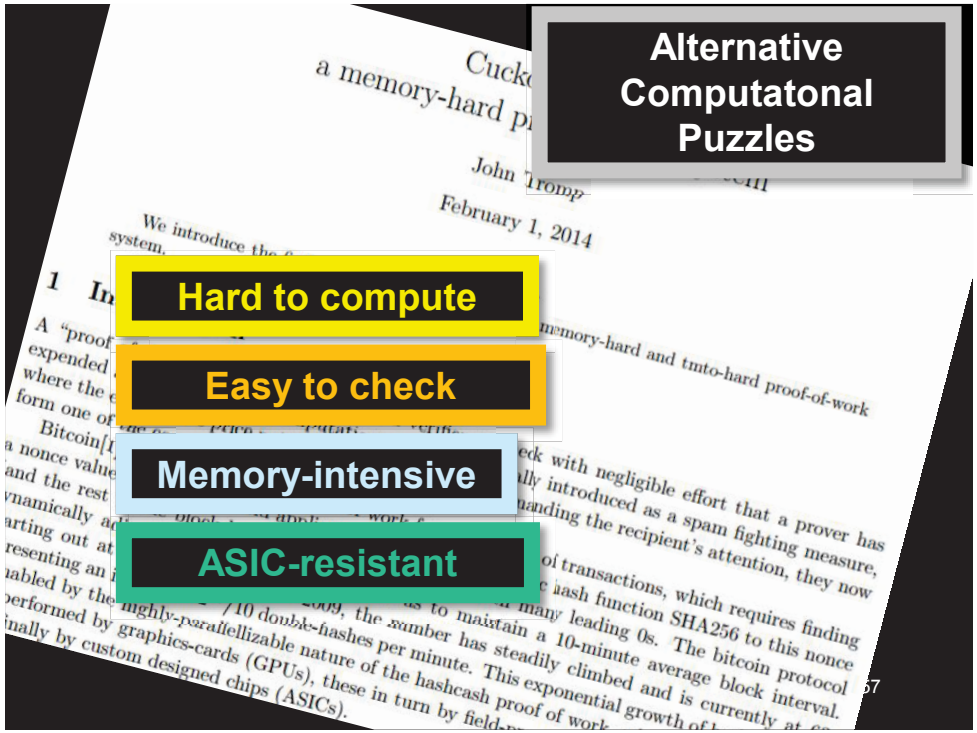
Once, BTC mining was done on laptops

Now, mostly done with ASICs

Alternative: "memory hard" puzzles

Mining now requires capitalization, Deep pockets

Alternative Computatonal Puzzles



Hard to compute

Easy to check

Memory-intensive

ASIC-resistant

Alternative Computatonal Puzzles

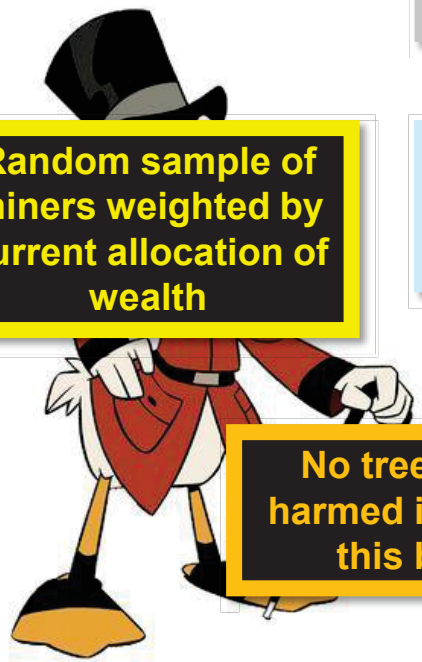
Not-outsourcable puzzles …

… 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

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM

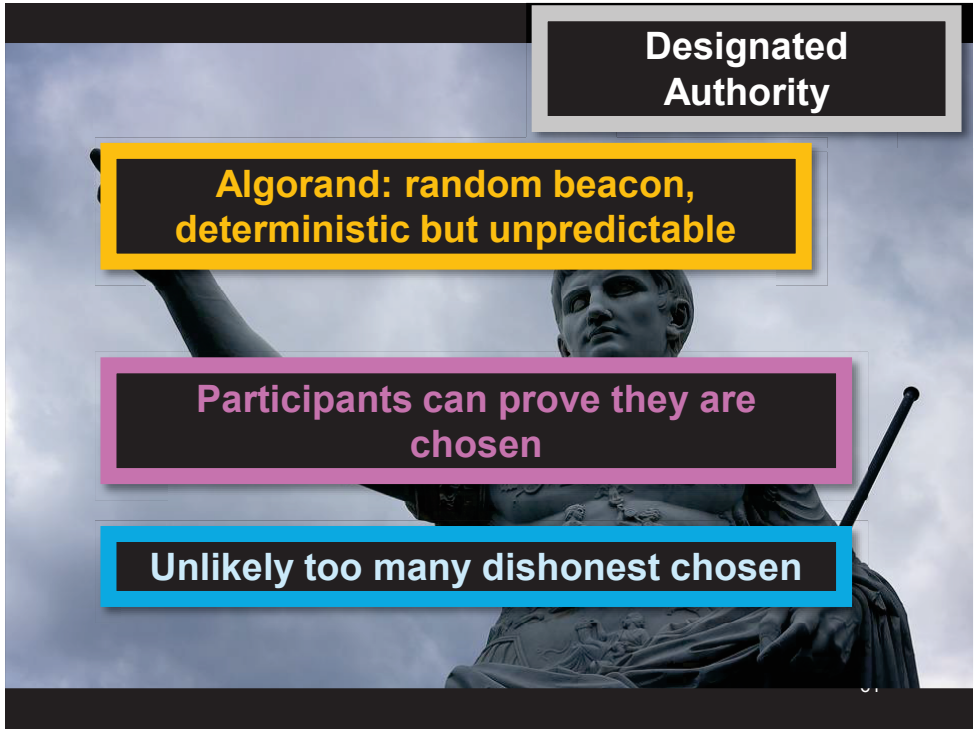
I've got an idea, and I'm wondering

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 Payments among

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.	
[illegible]	[illegible]		●		●	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 [119]	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

Frequent, recurring transactions

Done off-chain, post summary transactions infrequently

The Bitcoin Off-Chain Instant

Thaddeus Dryja

Better latency, throughput, privacy, etc.

January 14, 2016
DRAFT Version 0.5.9.2

Abstract

Cross-chain swaps

Re: Alt chains and atomic tr
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' explanation page to develop and clarify the solution as needed

I suggest we use the wiki

Alice has alt-coin, wants bitcoin

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

that can only be spent if you have the

Step 2

Bob has bitcoin, wants alt-coin

x to B.

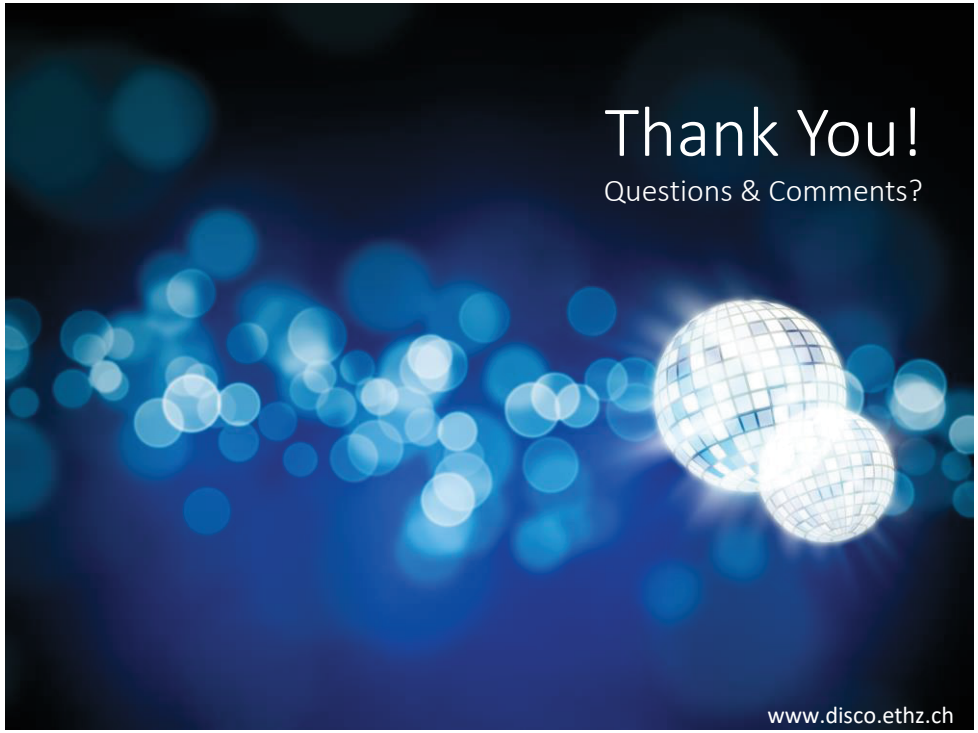
for H(x)

The can now both spend the

Multiphase protocol guarantees atomic swap

as to provide x to the

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


Thank You!
Questions & Comments?
www.disco.ethz.ch