

Is Bitcoin Stable, Secure and Scalable?



Roger Wattenhofer

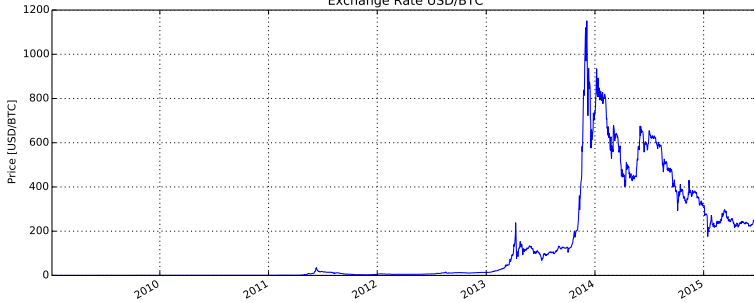
Hacker stahlen ETH- Doktoranden Bitcoin für 9 Millionen

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



Exchange Rate USD/BTC



Mt. Gox Seeks Bankruptcy After \$480 Million Bitcoin Loss

By Carter Dougherty and Grace Huang | Feb 28, 2014 8:59 PM GMT+0100 | [95 Comments](#) [Email](#) [Print](#)

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

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

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



Mark Karpeles, CEO of Mt. Gox, the world's largest bitcoin exchange, bows for an... [Read More](#)

What is Bitcoin?



+



+



=



Bitcoin Basics

The Bank of Bitcoin

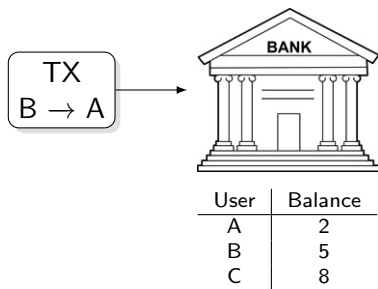


The Bank of Bitcoin

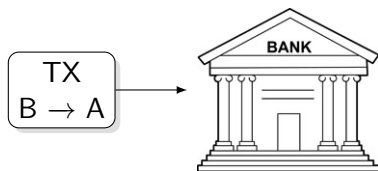


User	Balance
A	2
B	5
C	8

The Bank of Bitcoin



The Bank of Bitcoin



User	Balance
A	24
B	53
C	8

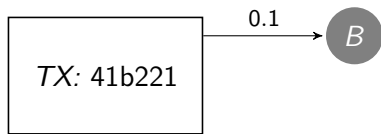
Opening an Account in Bitcoin



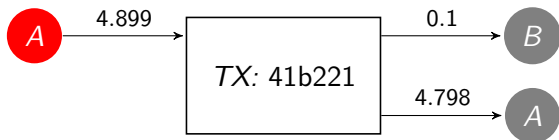
Transferring Bitcoins

TX: 41b221

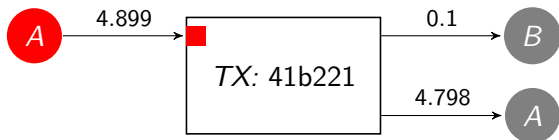
Transferring Bitcoins



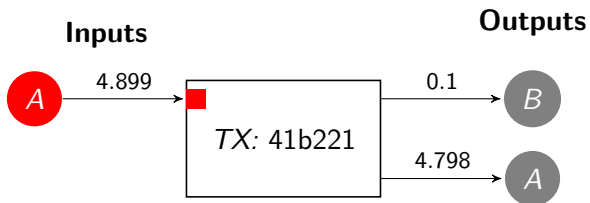
Transferring Bitcoins



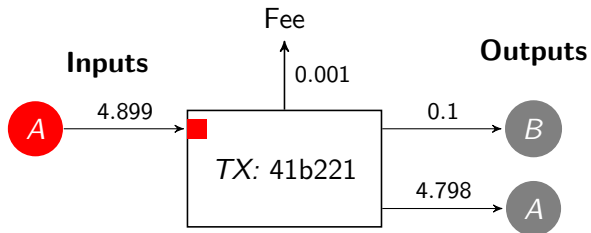
Transferring Bitcoins



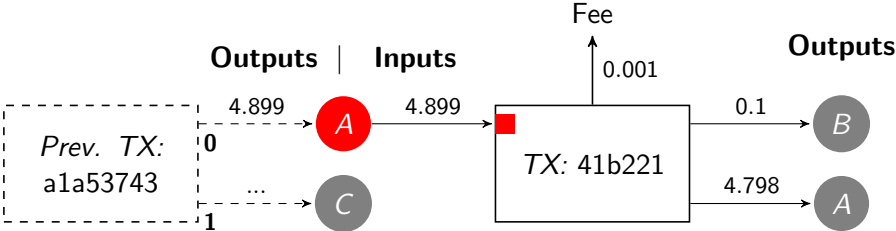
Transferring Bitcoins



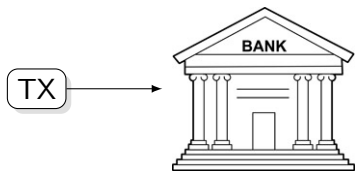
Transferring Bitcoins



Transferring Bitcoins

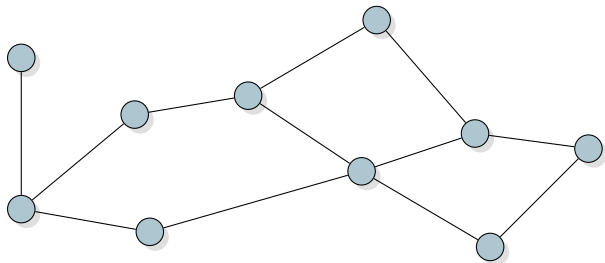


Distributing the Bank

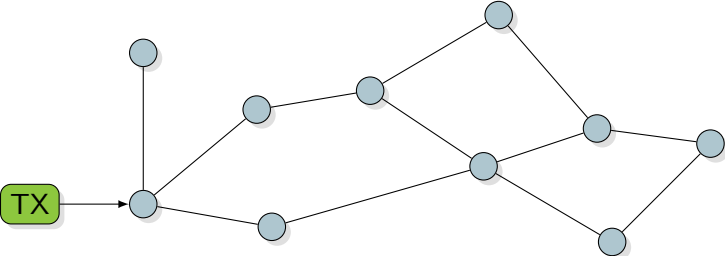


User	Balance
A	2
B	5
C	8

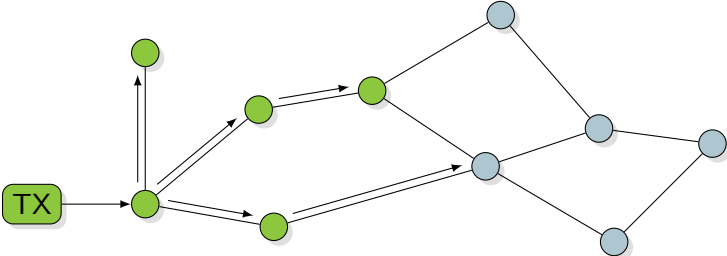
Distributing the Bank



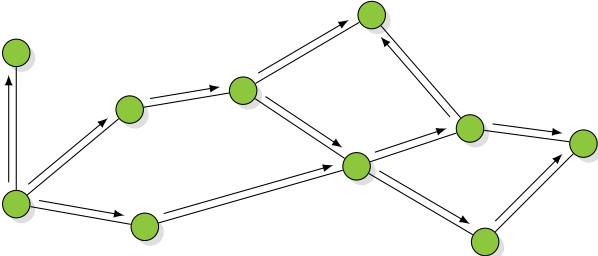
Distributing the Bank



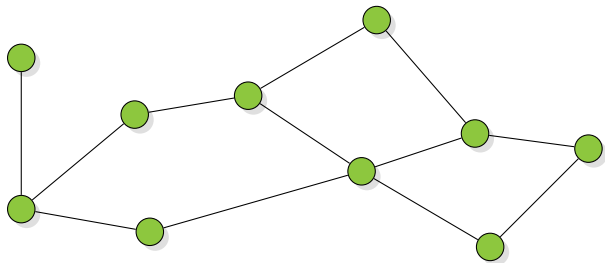
Distributing the Bank



Distributing the Bank



Distributing the Bank

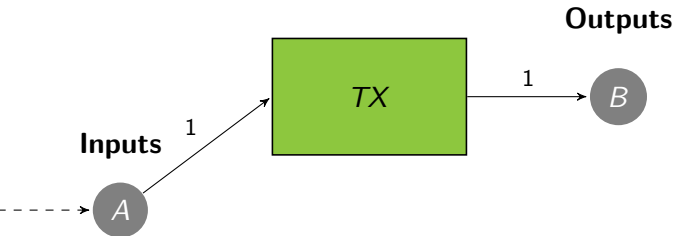


Let's Buy a Snack

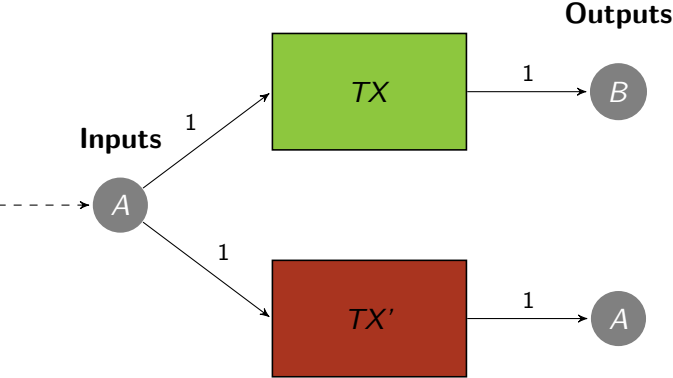
[Bamert, Decker, Elsen, W, Welten, 2013]



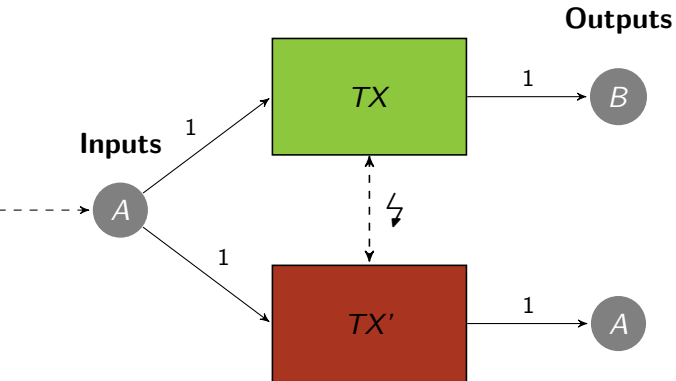
Doublespending



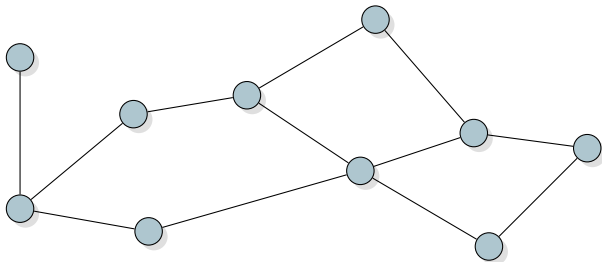
Doublespending



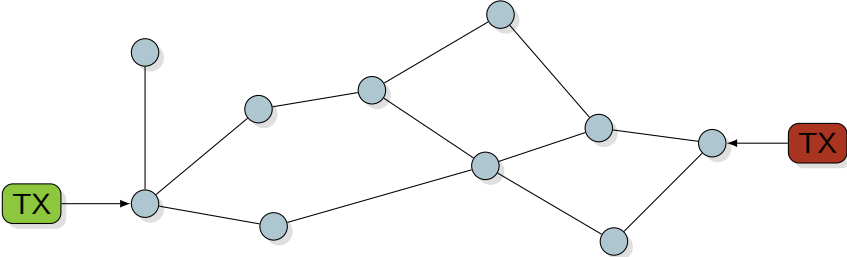
Doublespending



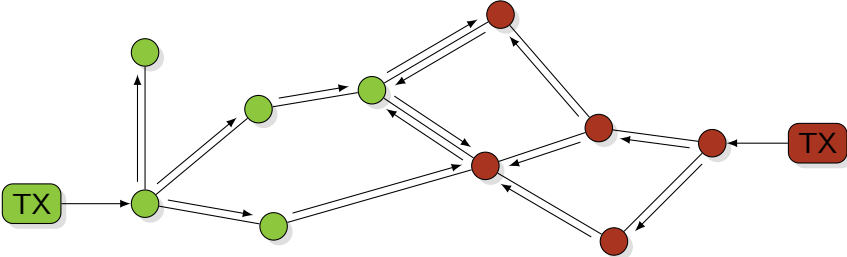
Transaction Conflicts



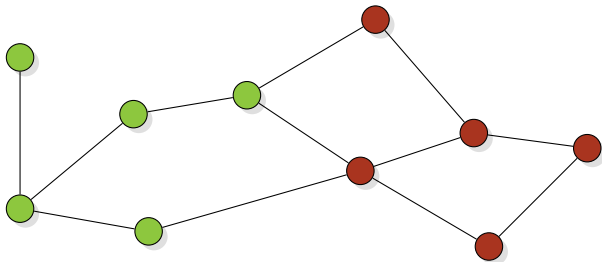
Transaction Conflicts



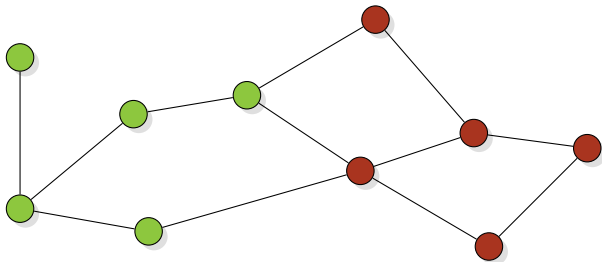
Transaction Conflicts



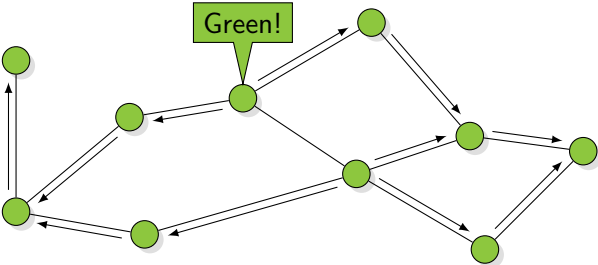
Transaction Conflicts



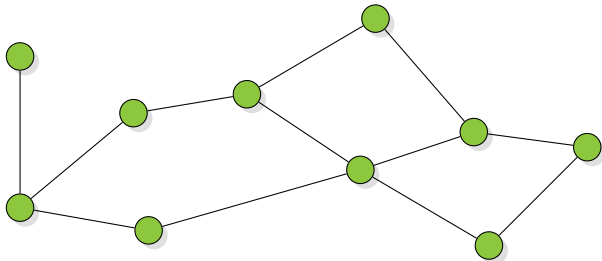
Resolving Conflicts



Resolving Conflicts



Resolving Conflicts



How to Choose a Leader?



Proof-of-Work



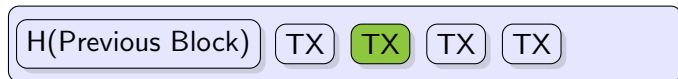
Proof-of-Work

Block

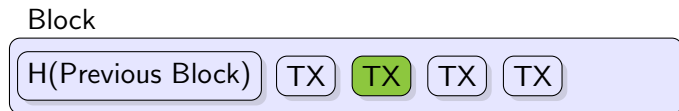


Proof-of-Work

Block

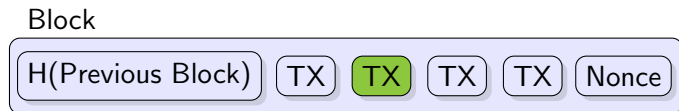


Proof-of-Work



- ▶ $H(\text{Block}) \rightarrow \text{fd2e2055f117bfa261b5a6c7e11df367}\dots$

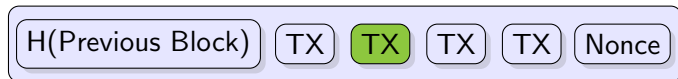
Proof-of-Work



- ▶ $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\dots$

Proof-of-Work

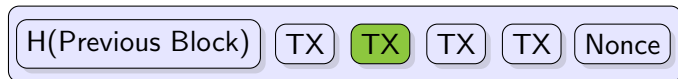
Block



- ▶ $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\dots$
- ▶ $H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\dots$

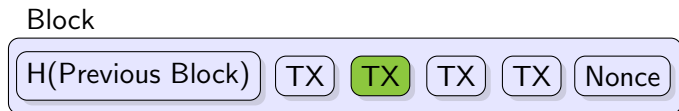
Proof-of-Work

Block



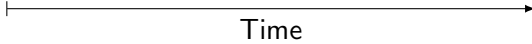
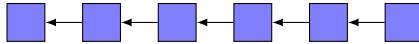
- ▶ $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\dots$
- ▶ $H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\dots$
- ▶ $H(\text{Block}|2) \rightarrow aec87c0ca2e5eb3f23111092f1089ada\dots$

Proof-of-Work

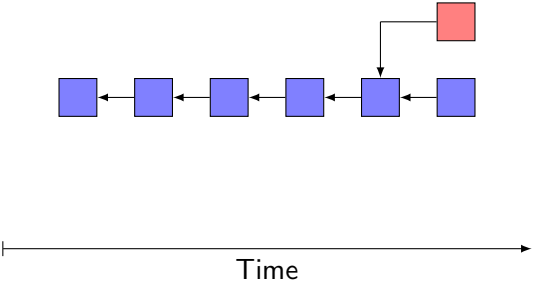


- ▶ $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\dots$
- ▶ $H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\dots$
- ▶ $H(\text{Block}|2) \rightarrow aec87c0ca2e5eb3f23111092f1089ada\dots$
- ▶ $H(\text{Block}|3) \rightarrow 777f75b2a8ecfdc8026c236fc1d2ffa0\dots$
- ▶ \vdots
- ▶ $H(\text{Block}|961127) \rightarrow 0000014823419622d4c133672a7d657e\dots$

The Blockchain

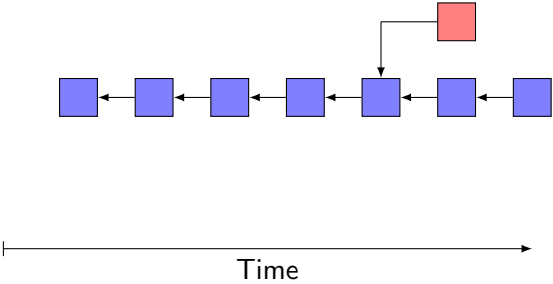


The Blockchain

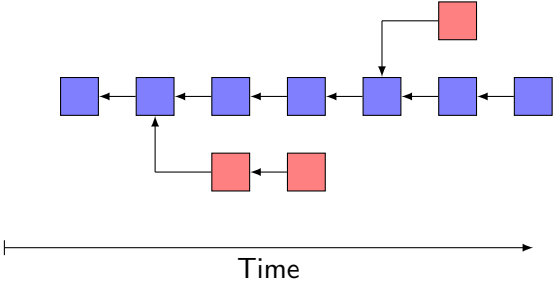


Is Bitcoin stable?

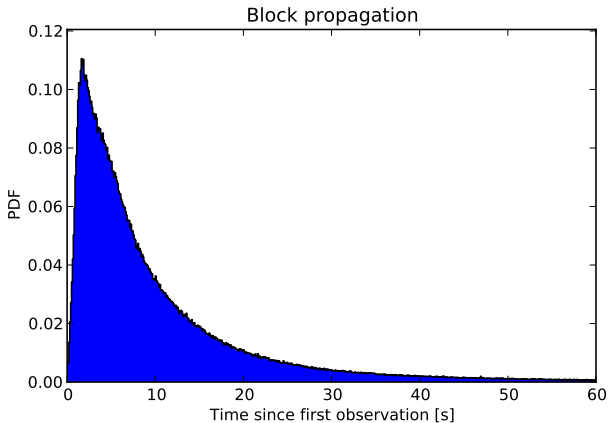
The Blockchain



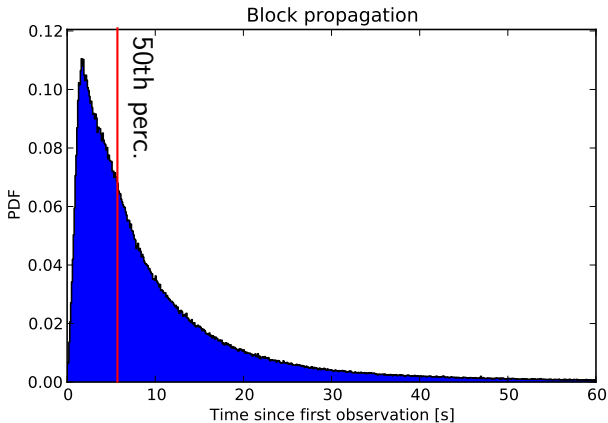
The Blockchain



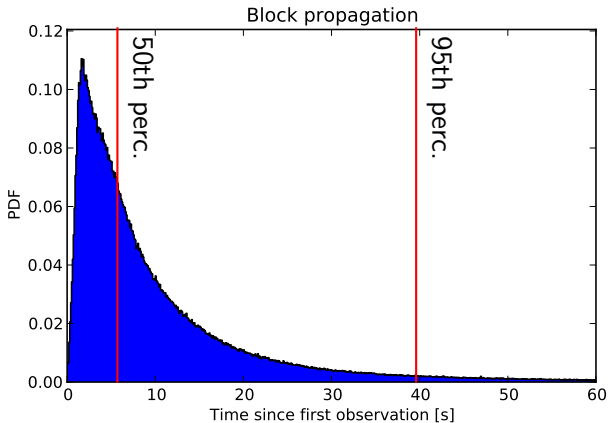
Propagation Speed



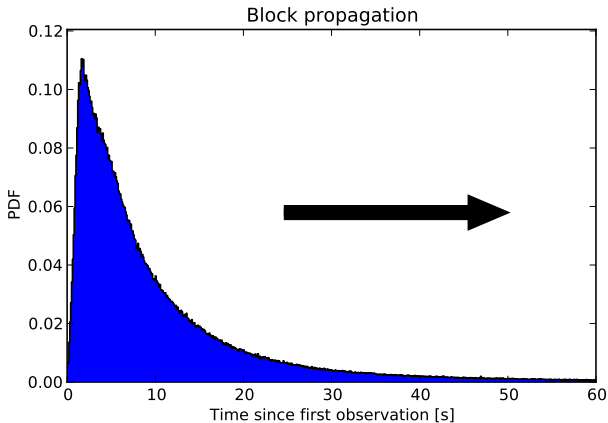
Propagation Speed



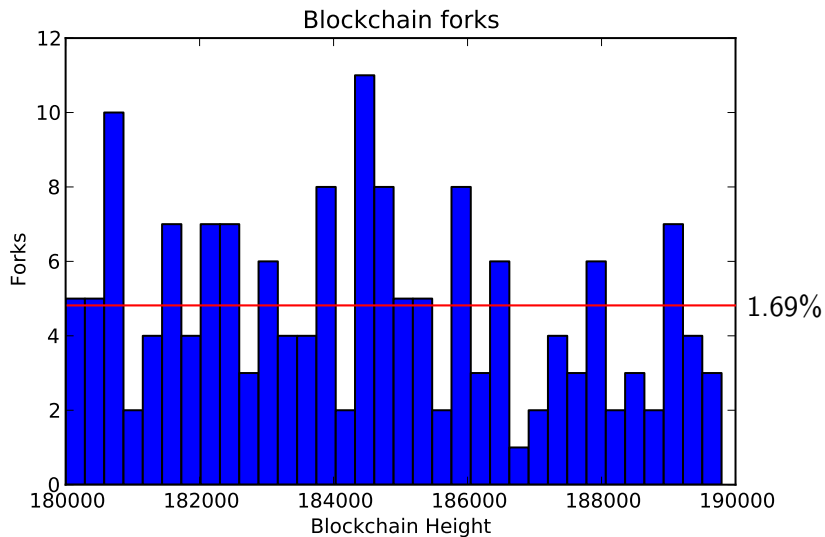
Propagation Speed



Propagation Speed

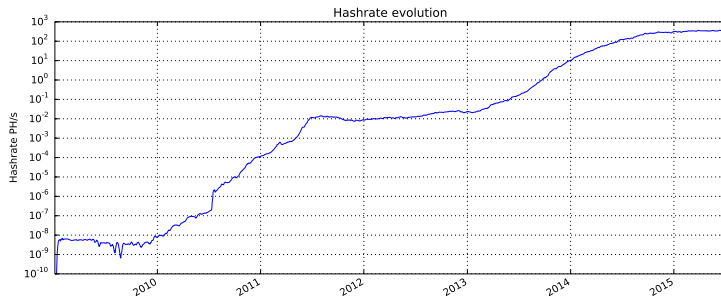


Blockchain Forks

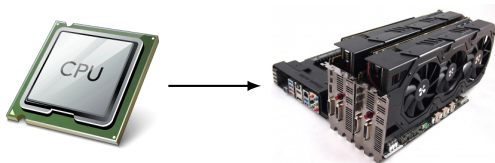
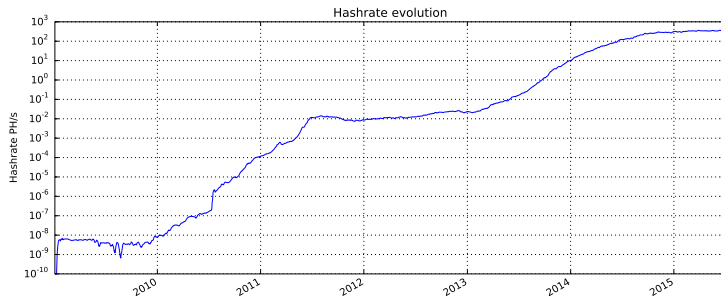


[Decker, W, 2013]

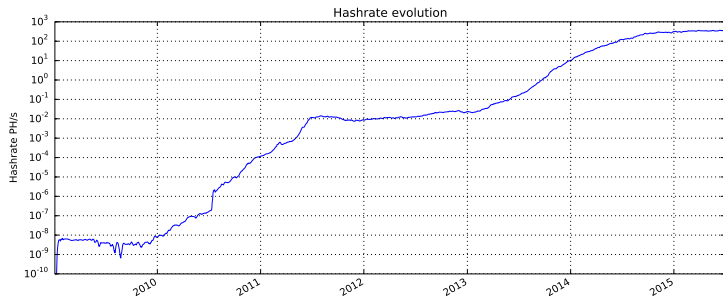
Aside: Mining Evolution



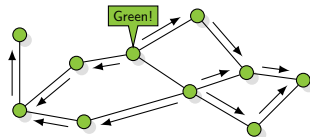
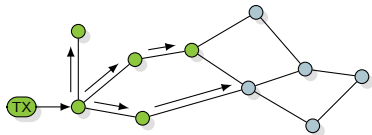
Aside: Mining Evolution



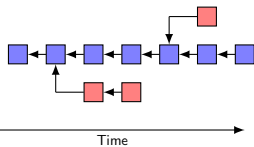
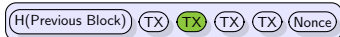
Aside: Mining Evolution



Summary



Block



How to Lose \$500M



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

The MtGox Incident

- ▶ July 2010: First trade on MtGox
- ▶ May 2011: Transaction malleability identified as low priority issue
- ▶ February 7, 2014: MtGox halts withdrawals
- ▶ February 10, 2014: MtGox announces loss of 850,000 bitcoins (620 millio USD) and cites transaction malleability as root cause
- ▶ February 28, 2014: MtGox files for bankruptcy
- ▶ March 7 2014: MtGox finds 200,000 bitcoins
- ▶ August 2015: MtGox CEO is arrested

Signatures

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

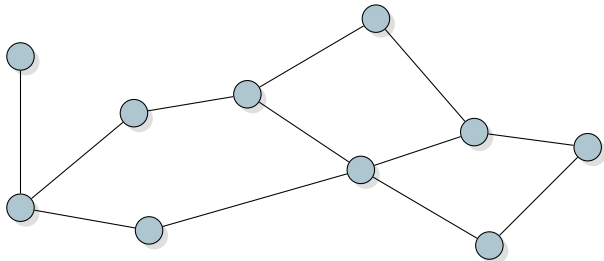
Signatures

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

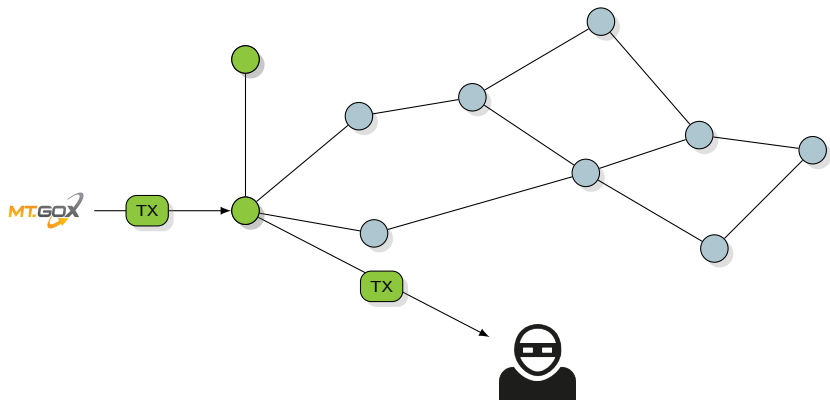
There are multiple ways to serialize a signature:

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

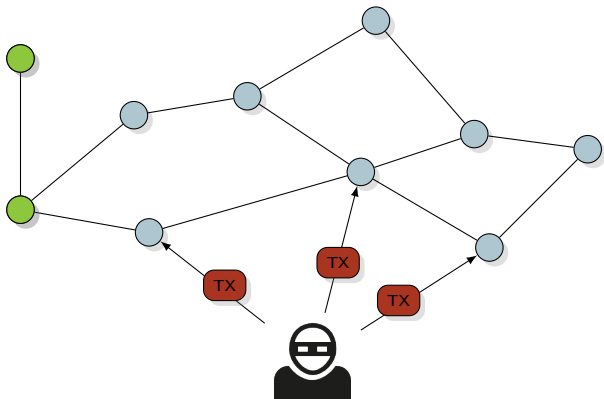
Transaction Malleability Attack



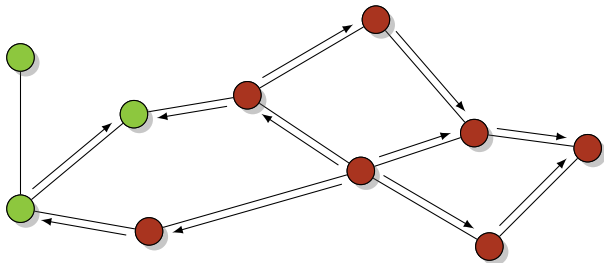
Transaction Malleability Attack



Transaction Malleability Attack



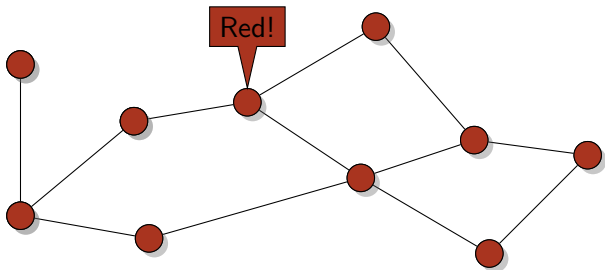
Transaction Malleability Attack



Transaction Malleability Attack

TX?

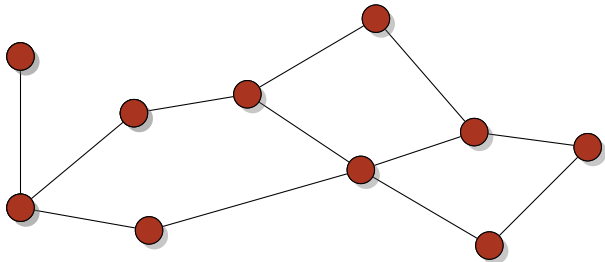
MT.GOX



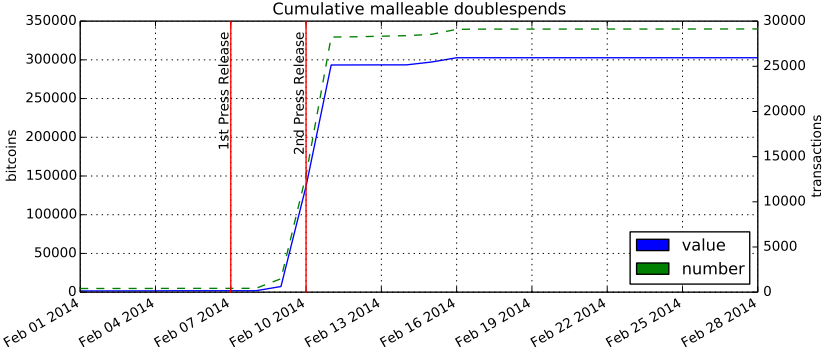
Transaction Malleability Attack

Refund

MT.GOX

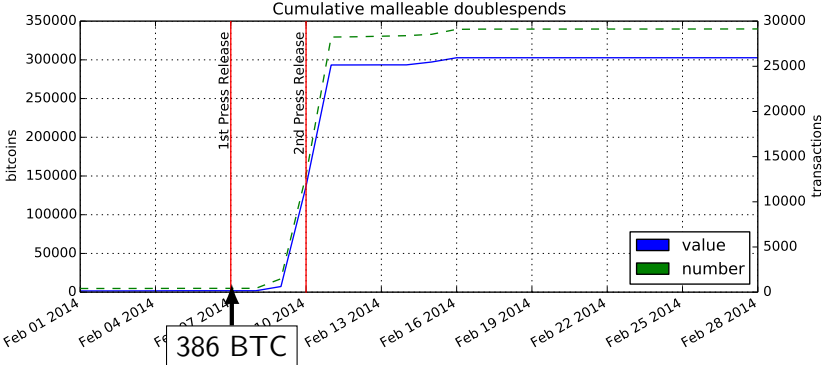


Incident Timeline



[Decker, W, 2014]

Incident Timeline



[Decker, W, 2014]

Is Bitcoin Secure?

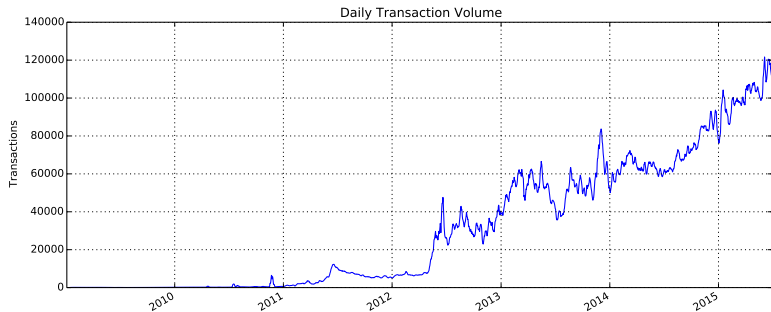
Securing Your Bitcoins



[Bamert, Decker, W, 2013]

Does Bitcoin Scale?

The Bitcoin Ecosystem is Growing



Scalability Limits

- ▶ Disk space: < 500 transactions per second

Scalability Limits

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

Scalability Limits

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

Scalability Limits

- ▶ Disk space: < 500 transactions per second
- ▶ Processing power: < 200 transactions per second
- ▶ Network bandwidth: < 100 transactions per second
- ▶ Artificial 1MB limit: < 3 transactions per second

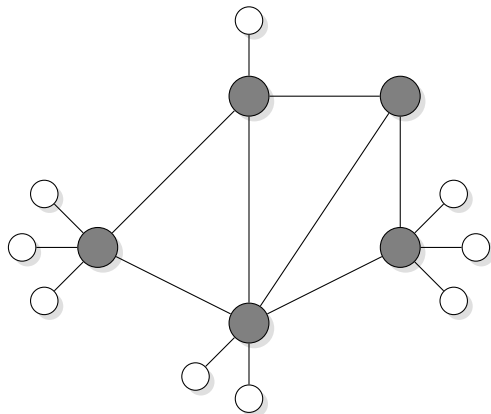
Scalability Limits

- ▶ Disk space: < 500 transactions per second
- ▶ Processing power: < 200 transactions per second
- ▶ Network bandwidth: < 100 transactions per second
- ▶ Artificial 1MB limit: < 3 transactions per second

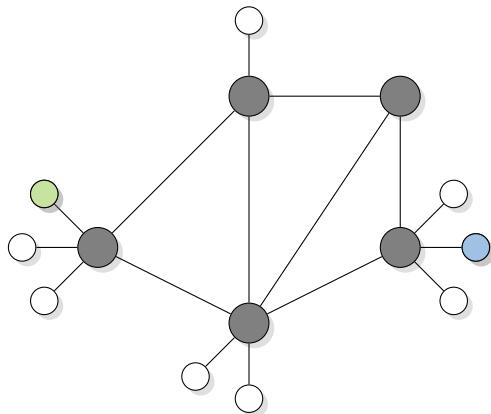
Today:

- ▶ Bitcoin: 1 transaction per second
- ▶ Credit Cards: $> 10,000$ transactions per second

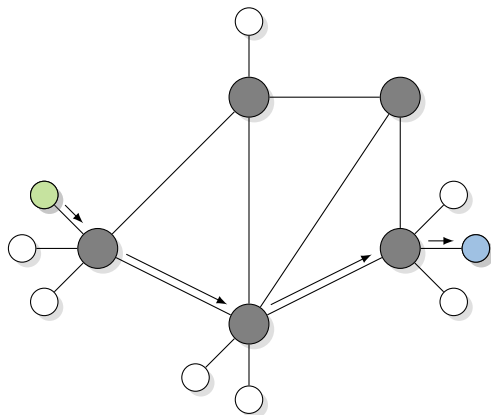
Payment Network



Payment Network



Payment Network



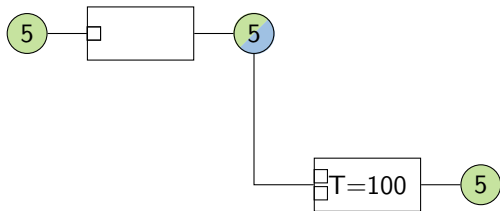
Micropayment Channels

5

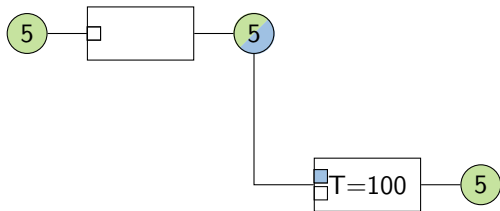
Micropayment Channels



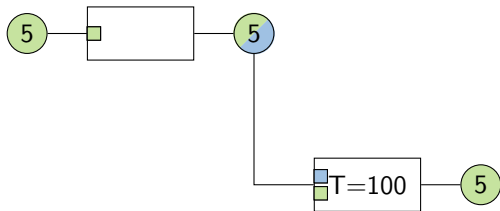
Micropayment Channels



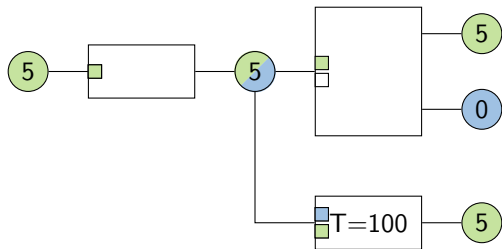
Micropayment Channels



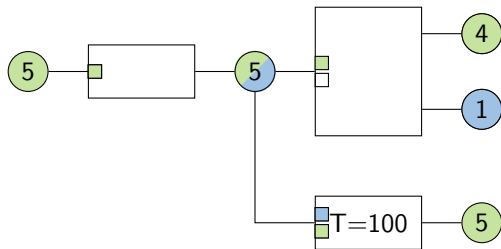
Micropayment Channels



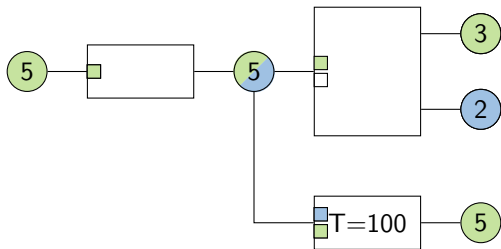
Micropayment Channels



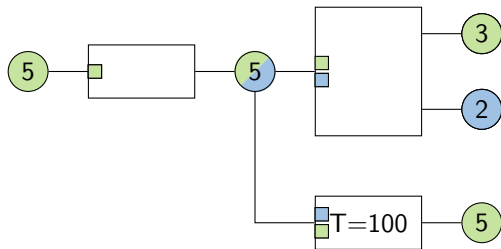
Micropayment Channels



Micropayment Channels



Micropayment Channels



Atomic Multiparty Opt-In



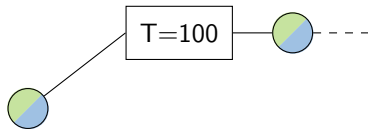
Atomic Multiparty Opt-In



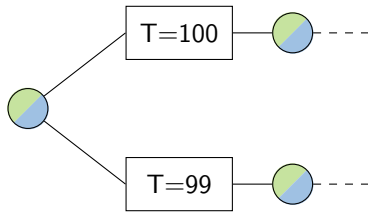
Atomic Multiparty Opt-In



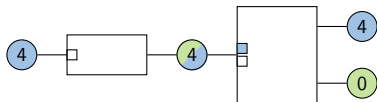
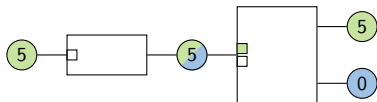
Invalidating Transactions



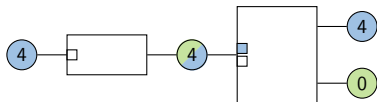
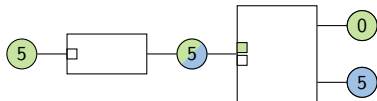
Invalidating Transactions



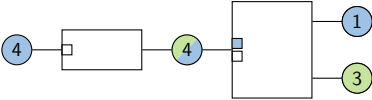
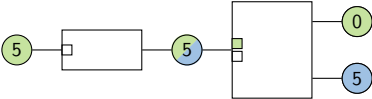
Bidirectional Transfers



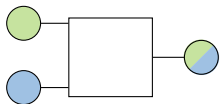
Bidirectional Transfers



Bidirectional Transfers



Duplex Micropayment Channels

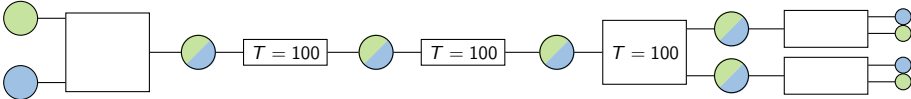


Setup

Invalidation Tree

Micropayment Channels

Duplex Micropayment Channels

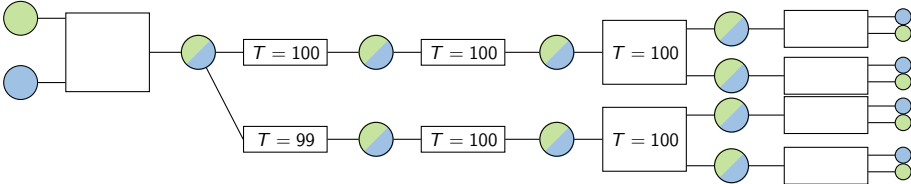


Setup

Invalidation Tree

Micropayment Channels

Duplex Micropayment Channels

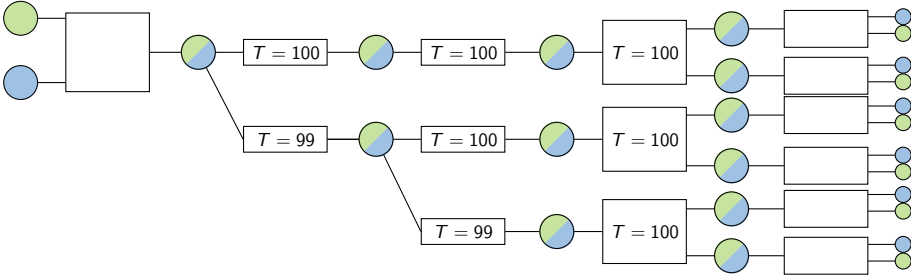


Setup

Invalidation Tree

Micropayment Channels

Duplex Micropayment Channels

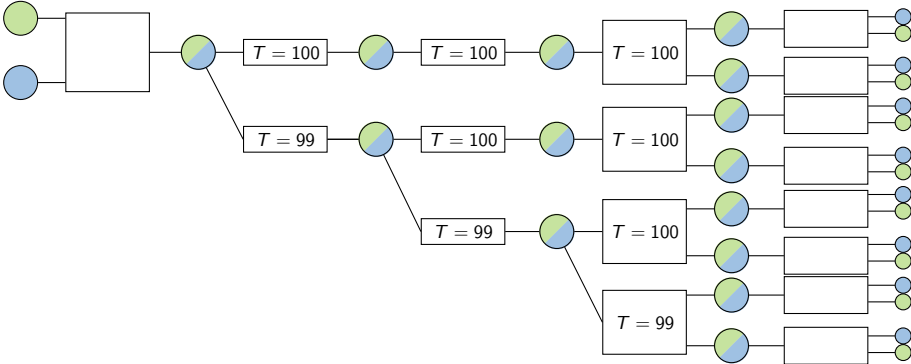


Setup

Invalidation Tree

Micropayment Channels

Duplex Micropayment Channels

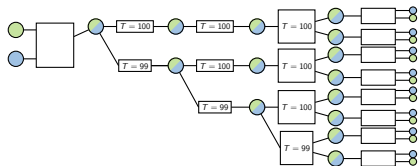
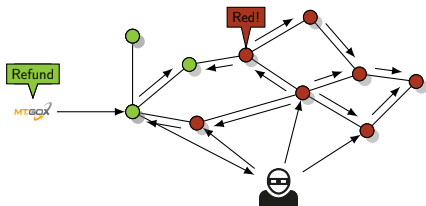


Setup

Invalidation Tree

Micropayment Channels

Summary



Thank you, questions?



Thanks to Christian Decker

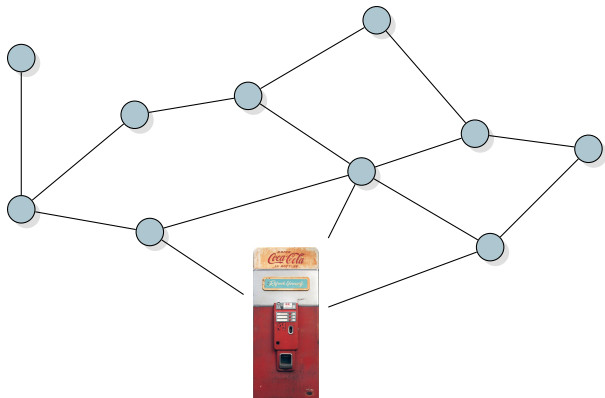
Securing Fast Payments

Let's Buy a Snack

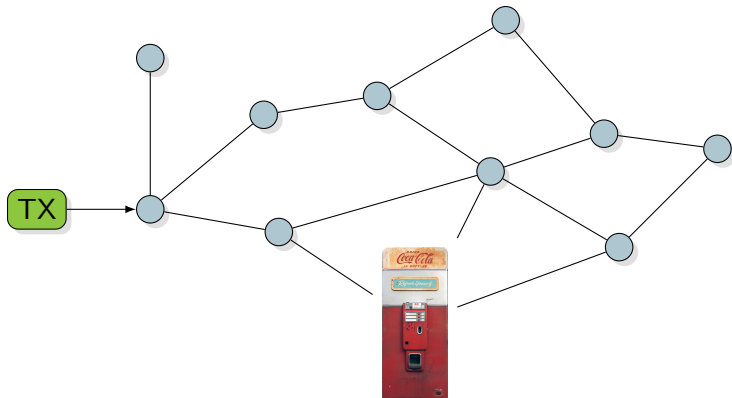
[Bamert, Decker, Elsen, W, Welten, 2013]



Transaction Confidence

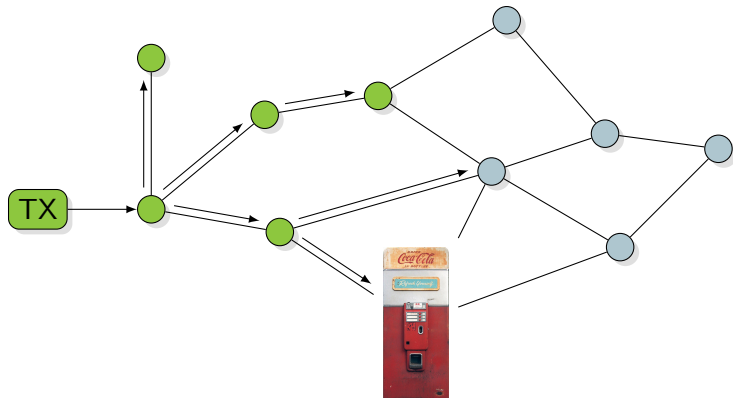



Transaction Confidence



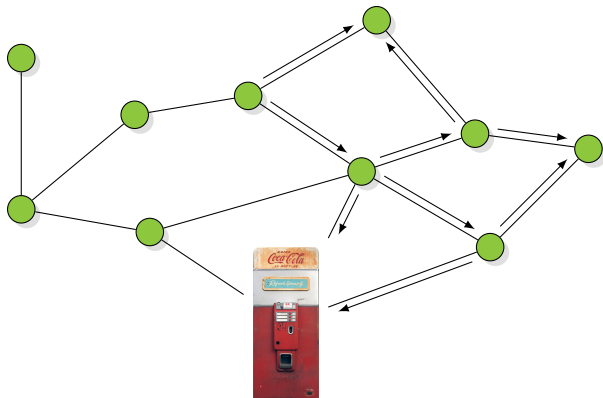
$$\text{confidence}(TX) = \boxed{}$$

Transaction Confidence



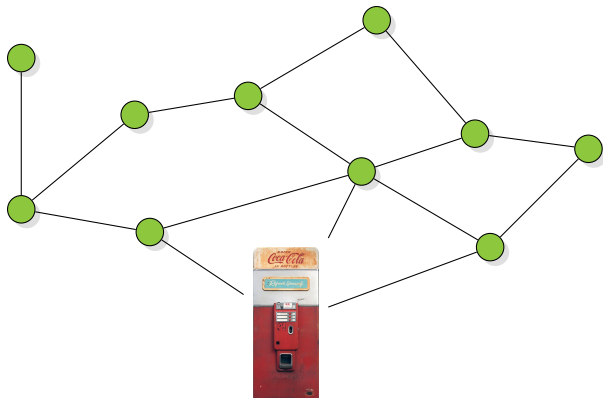
$confidence(TX) =$ 

Transaction Confidence



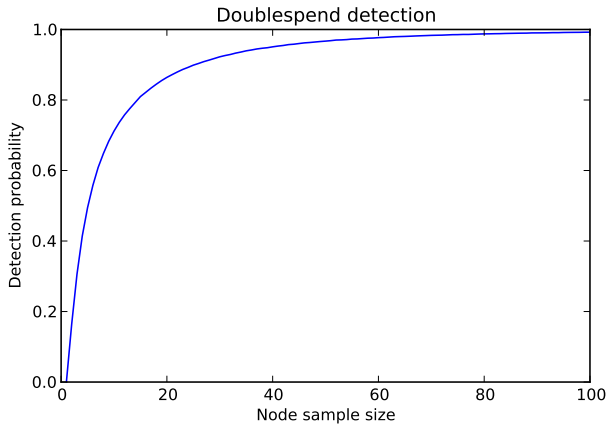
$$\text{confidence}(TX) = \text{[Progress Bar]}$$

Transaction Confidence



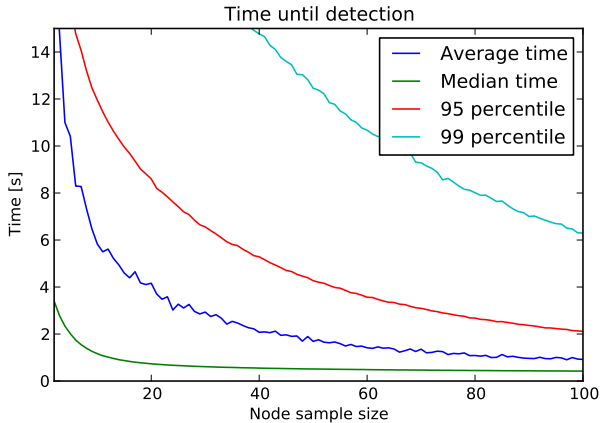
$$\text{confidence}(TX) = \text{█}$$

Doublespend Detection



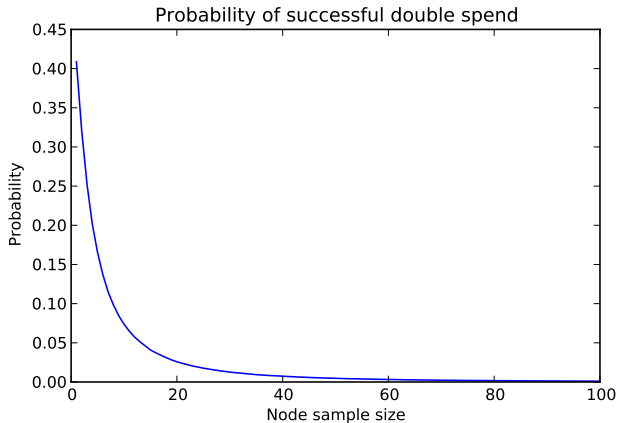
[Bamert, Decker, Elsen, W, Welten, 2013]

Time to Detection



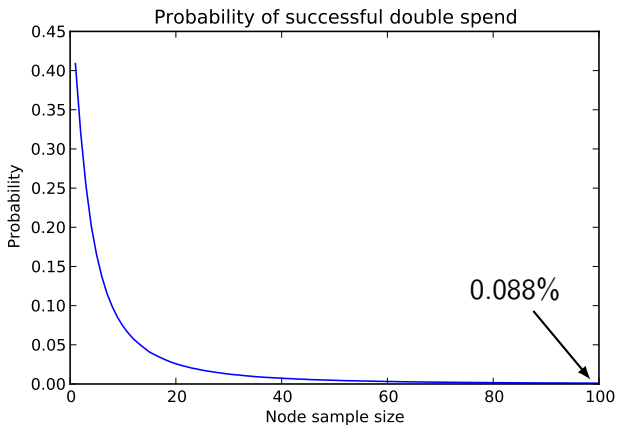
[Bamert, Decker, Elsen, W, Welten, 2013]

Successful Doublespend



[Bamert, Decker, Elsen, W, Welten, 2013]

Successful Doublespend



[Bamert, Decker, Elsen, W, Welten, 2013]