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

Price [USD/BTC]
Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss

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.
What is Bitcoin?
Bitcoin Basics
The Bank of Bitcoin
The Bank of Bitcoin

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
The Bank of Bitcoin

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>

TX
B → A
The Bank of Bitcoin

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2 4</td>
</tr>
<tr>
<td>B</td>
<td>5 3</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
Opening an Account in Bitcoin

Private Key → Public Key → Address
Transferring Bitcoins

TX: 41b221
Transferring Bitcoins

TX: 41b221

Inputs

Outputs

Fee 0.001

Prev. TX: a1a53743

0.1

B
Transferring Bitcoins

A → TX: 41b221 → B

TX: 41b221

A → TX: 41b221 → B

B → A

Fee: 0.001

Prev. TX: a1a53743

4.899 → 4.798

0.1
Transferring Bitcoins

TX: 41b221

Inputs

Outputs

Fee 0.001

Prev. TX: a1a53743 4.899

<table>
<thead>
<tr>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
</tr>
<tr>
<td>4.798</td>
</tr>
</tbody>
</table>

A → TX: 41b221 → B

B → A
Transferring Bitcoins

Inputs

A → 4.899

Outputs

TX: 41b221

B → 0.1

A → 4.798
Transferring Bitcoins

Inputs

A → 4.899

TX: 41b221

Fee

0.001

Outputs

A → 4.798

B → 0.1
Transferring Bitcoins

Prev. TX: a1a53743

Outputs  |  Inputs

A

4.899  |  4.899

C

Outputs

TX: 41b221

Fee

0.001

0.1

4.798

B

A
Distributing the Bank

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
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

Inputs $\rightarrow$ $TX$ $\rightarrow$ Outputs

$A$ $\rightarrow$ $TX$ $\rightarrow$ $B$
Doublespending

Inputs

Outputs

TX

TX'

A

B

1

1
Doublespending

```
Inputs: A

TX

Outputs: B

TX'

A
```
Transaction Conflicts
Transaction Conflicts
Transaction Conflicts
Transaction Conflicts
Resolving Conflicts
Resolving Conflicts

Green!
Resolving Conflicts
How to Choose a Leader?
Proof-of-Work

TX  TX  TX  TX

...
Proof-of-Work

Block

TX  TX  TX  TX
Proof-of-Work

Block

H(Previous Block)  TX  TX  TX  TX
Proof-of-Work

H(Previous Block) → fd2e2055f117bfa261b5a6c7e11df367...
Proof-of-Work

- $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\ldots$
Proof-of-Work

Block

\[ H(\text{Previous Block}) \quad \text{TX} \quad \text{TX} \quad \text{TX} \quad \text{TX} \quad \text{Nonce} \]

- \[ H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\ldots \]
- \[ H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\ldots \]
Proof-of-Work

Block

\[
\begin{array}{c}
\text{H(Previous Block)} \quad \text{TX} \quad \text{TX} \quad \text{TX} \quad \text{TX} \quad \text{Nonce}
\end{array}
\]

- \( \text{H(\text{Block}|0)} \rightarrow 094d66aa7c844a9dbb516a41259b5877\ldots \)
- \( \text{H(\text{Block}|1)} \rightarrow f2496854af8bf989171587a9259f634f\ldots \)
- \( \text{H(\text{Block}|2)} \rightarrow \text{aec87c0ca2e5eb3f23111092f1089ada}\ldots \)
Proof-of-Work

- $H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\ldots$
- $H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\ldots$
- $H(\text{Block}|2) \rightarrow \text{aec87c0ca2e5eb3f23111092f1089ada}\ldots$
- $H(\text{Block}|3) \rightarrow 777f75b2a8ecf6c8026c236fc1d2ffa0\ldots$
  
  
- $\vdots$
- $H(\text{Block}|961127) \rightarrow 0000014823419622d4c133672a7d657e\ldots$
The Blockchain
The Blockchain
Is Bitcoin stable?
The Blockchain
The Blockchain
Propogation Speed

http://bitcoinstats.com

[Decker, W, 2013]
Propagation Speed

![Block propagation graph](http://bitcoinstats.com)

[Decker, W, 2013]
Propagación de Velocidad

PDF de propagación de bloque

50th perc. 95th perc.

http://bitcoinstats.com

[Decker, W, 2013]
Propagation Speed

Blockchain Forks

[Decker, W, 2013]
Aside: Mining Evolution

Hashrate evolution
Aside: Mining Evolution

Hashrate evolution

Hashrate PH/s

2010 2011 2012 2013 2014 2015

10^-10
10^-9
10^-8
10^-7
10^-6
10^-5
10^-4
10^-3
10^-2
10^-1
10^0
10^1
10^2
10^3

CPU

GPU
Aside: Mining Evolution

Hashrate evolution

![Hashrate evolution graph](image-url)
Summary

Block

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

Green!

Time
How to Lose $500M
Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks.
The MtGox Incident

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

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

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

There are multiple ways to serialize a signature:

- Multiple push operations (1 byte, 2 byte, 4 byte)
- Non-canonical DER encodings
- Padding
- . . .
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Transaction Malleability Attack
Incident Timeline

[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

Today:
- Bitcoin: 1 transaction per second
- Credit Cards: > 10,000 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
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels

\[ T = 100 \]
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

T=100

T=99
Bidirectional Transfers
Bidirectional Transfers
Bidirectional Transfers
Duplex Micropayment Channels
Duplex Micropayment Channels
Duplex Micropayment Channels
Duplex Micropayment Channels

\[ T = 100 \]

\[ T = 99 \]

\[ T = 100 \]

\[ T = 99 \]
Duplex Micropayment Channels

\[ T = 100 \]

\[ T = 99 \]

\[ T = 100 \]

\[ T = 99 \]

\[ T = 100 \]

\[ T = 99 \]

\[ T = 100 \]

\[ T = 99 \]
Summary

Refund
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

\[
\text{confidence}(TX) = \square
\]
Transaction Confidence

\[ \text{confidence}(TX) = \text{bar graph} \]
Transaction Confidence

\[\text{confidence}(TX) = \text{[Diagram]}\]
Transaction Confidence

\[ \text{confidence}(TX) = \text{green bar} \]
Doublespend Detection

[Bamert, Decker, Elsen, W, Welten, 2013]
Time to Detection

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

[Probabilty of successful double spend]

- Node sample size:
  - 0.00
  - 0.05
  - 0.10
  - 0.15
  - 0.20
  - 0.25
  - 0.30
  - 0.35
  - 0.40
  - 0.45

- Probability:
  - 0.00
  - 0.05
  - 0.10
  - 0.15
  - 0.20
  - 0.25
  - 0.30
  - 0.35
  - 0.40
  - 0.45

[References:
Bamert, Decker, Elsen, W, Welten, 2013]
Successful Doublespend

Probability of successful double spend

Node sample size

[0.00, 0.05, 0.10, 0.15, 0.20, 0.25, 0.30, 0.35, 0.40, 0.45]

Probability

Bamert, Decker, Elsen, W, Welten, 2013