Cryptocurrencies
bitcoin, blockchain & beyond

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
Cryptocurrencies
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Available Supply</th>
<th>Volume (24h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$8,981,243,870</td>
<td>$574.31</td>
<td>15,638,375 BTC</td>
<td>$71,004,500</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$1,172,919,101</td>
<td>$14.51</td>
<td>80,853,613 ETH</td>
<td>$9,933,140</td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$216,171,881</td>
<td>$4.68</td>
<td>46,149,551 LTC</td>
<td>$5,031,230</td>
</tr>
<tr>
<td>4</td>
<td>Ripple</td>
<td>$201,593,968</td>
<td>$0.00578</td>
<td>34,868,679,462 XRP *</td>
<td>$552,597</td>
</tr>
<tr>
<td>5</td>
<td>The DAO</td>
<td>$162,984,082</td>
<td>$0.138973</td>
<td>1,172,775,159 DAO *</td>
<td>$1,502,090</td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$51,232,986</td>
<td>$7.87</td>
<td>6,510,786 DASH</td>
<td>$248,316</td>
</tr>
<tr>
<td>7</td>
<td>Lisk</td>
<td>$46,560,900</td>
<td>$0.465609</td>
<td>100,000,000 LSK *</td>
<td>$2,472,480</td>
</tr>
<tr>
<td>8</td>
<td>Dogecoin</td>
<td>$27,584,159</td>
<td>$0.000263</td>
<td>104,686,099,387 DOGE</td>
<td>$506,232</td>
</tr>
<tr>
<td>9</td>
<td>MaidSafeCoin</td>
<td>$25,406,247</td>
<td>$0.056140</td>
<td>452,552,412 MAID *</td>
<td>$421,888</td>
</tr>
<tr>
<td>10</td>
<td>DigixDAO</td>
<td>$20,670,600</td>
<td>$10.34</td>
<td>2,000,000 DGD *</td>
<td>$65,517</td>
</tr>
</tbody>
</table>
What is Bitcoin?

+ + =
Technology
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

Prev. TX: a1a53743

Inputs

Outputs

Fee 0.001

0.1

B
Transferring Bitcoins

TX: 41b221

Inputs

Outputs

Fee 0.001

Prev. TX: a1a53743 4.899 4.798 0.1
Transferring Bitcoins

TX: 41b221

Outputs

Fee 0.001

Prev. TX: a1a53743

4.899 → 0.1 → 4.798

A → TX: 41b221 → B

A → TX: 41b221 → A
Transferring Bitcoins

TX: 41b221

Inputs

A  4.899

Outputs

TX: 41b221

B  0.1

A  4.798
Transferring Bitcoins

Inputs

TX: 41b221

Outputs

Fee

0.001

0.1

4.798

A

B

A

Transferring Bitcoins

TX: 41b221

Inputs

Outputs

Fee

0.001

0.1

4.798

A

B

A
Transferring Bitcoins

Prev. TX: a1a53743

Outputs

Inputs

Fee 0.001

Prev. TX: a1a53743

Outputs

TX: 41b221

A

B

C

A

0.1

4.798
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
Doublespending

\[
\begin{align*}
\text{Inputs} & \quad 1 \\
& \quad 1 \\
& \quad 1 \\
\text{TX} & \quad 1 \\
\text{TX'} & \quad 1
\end{align*}
\]
Doublespending

\[ \text{Inputs} \rightarrow \text{A} \rightarrow \text{TX} \rightarrow \text{TX}' \]
Transaction Conflicts
Transaction Conflicts
Transaction Conflicts
Resolving Conflicts
Resolving Conflicts
Resolving Conflicts
How to Choose a Leader?
Proof-of-Work
Proof-of-Work
Proof-of-Work

Block

\[ H(\text{Previous Block}) \quad \text{TX} \quad \text{TX} \quad \text{TX} \quad \text{TX} \]
Proof-of-Work

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

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

- $H(\text{Block} | 1) \rightarrow \text{f2496854af8bf989171587a9259f634f}...$

- $H(\text{Block} | 2) \rightarrow \text{aec87c0ca2e5eb3f2311092f1089ada}...$

- $H(\text{Block} | 3) \rightarrow \text{777f75b2a8ecfdc8026c236fc1d2a0}...$

- $H(\text{Block} | 961127) \rightarrow \text{0000014823419622d4c133672a7d657e}...$
Proof-of-Work

Block

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

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

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

Block

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

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

- \( H(\text{Block}|0) \rightarrow 094d66aa7c844a9dbb516a41259b5877\ldots \)
- \( H(\text{Block}|1) \rightarrow f2496854af8bf989171587a9259f634f\ldots \)
- \( H(\text{Block}|2) \rightarrow aec87c0ca2e5eb3f23111092f1089ada\ldots \)
- \( H(\text{Block}|3) \rightarrow 777f75b2a8ecfdec8026c236fc1d2ffa0\ldots \)
- \( \vdots \)
- \( H(\text{Block}|961127) \rightarrow 0000014823419622d4c133672a7d657e\ldots \)
The Blockchain

Time
The Blockchain

Time
Is Bitcoin stable?
The Blockchain
The Blockchain
Propogation Speed

Block propagation

Time since first observation [s]

PDF

http://bitcoinstats.com

[Decker, W, 2013]
Propagation Speed

http://bitcoinstats.com

[Decker, W, 2013]
Blockchain Forks

[Decker, W, 2013]
Aside: Mining Evolution
Aside: Mining Evolution

[Graph showing hashrate evolution from 2010 to 2015.]
Aside: Mining Evolution

Hashrate evolution

[Graph showing the increase in Hashrate from 2010 to 2015]

[Images of a CPU, a graphics card, and a mining rig]
500 MW
Summary

Block

\( H(\text{Previous Block}) \)  TX  TX  TX  TX  Nonce

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

- July 2010: First trade on MtGox
- May 2011: Transaction malleability identified as low priority issue
- February 7, 2014: MtGox halts withdrawals
- February 10, 2014: MtGox announces loss of 850,000 bitcoins (620 million 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

Red!

TX?

MT.Gox
Transaction Malleability Attack
Incident Timeline

 Cumulative malleable doublespends

[Decker, W, 2014]
Incident Timeline

[Decker, W, 2014]
Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss

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

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.
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
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels
Micropayment Channels
Duplex Micropayment Channels

\[ T = 100 \]
\[ T = 100 \]
\[ T = 100 \]
\[ T = 99 \]
\[ T = 100 \]
\[ T = 100 \]
\[ T = 99 \]
\[ T = 100 \]
\[ T = 99 \]
Summary
Economy
BTC in USD
Inflation
Fungibility

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

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

- saver
- miner
- relay
- payer
- payee
What is Money?

- Medium of Exchange
- Unit of Account
- Store of Value
What is Money?
Summary
Thank You!
Questions & Comments?

Thanks to my co-author
Christian Decker