Intro to Bitcoin Research

or

“Why Bitcoin is a full employment act for security engineers”

Joseph Bonneau
CITP, Princeton

Thanks to Andrew Miller, Arvind Narayanan, Jeremy Clark, Joshua Kroll, Ed Felten
Part I: Bitcoin in 6 easy steps
Double spending: why ecash is hard

Alice
- $\text{Sign}_A (\text{Transfer X to B})$
- $\text{Sign}_A (\text{Transfer X to C})$

Bob
- Redeem X?

Charlie
- Redeem X?

BANK
- Redeem X?

Sign$_Z (\text{Transfer X to A})$
Step 1: Make the bank a global log

(the block chain)
Step 2: Participants vote on blocks

Signature_A  Signature_B  Signature_C
...
Signature_A  Signature_B  Signature_C
...
Signature_A  Signature_B  Signature_D
...
Step 3: A random user picks

- N-2
  - \( \text{Signature}_A \)

- N-1
  - \( \text{Signature}_B \)

- N
  - \( \text{Signature}_C \)
Step 4: Resolve conflicts by *forking*

Sign\textsubscript{A} (Transfer X to B)

Sign\textsubscript{A} (Transfer X to C)

Sign\textsubscript{B}

Sign\textsubscript{C}

Sign\textsubscript{D}

Sign\textsubscript{E}
Step 5: Incentivise correct blocks

Mint(X, A) \[\text{Signature}_A\]
Mint(X, B) \[\text{Signature}_B\]
Mint(X, C) \[\text{Signature}_C\]
Mint(X, D) \[\text{Signature}_D\]
Mint(X, E) \[\text{Signature}_E\]
Step 6: Choose by hash power!

Mint(X, A)

SHA-256(Block_{N-1}, n) = 0x00000000000000003f89...

Mint(X, B)

SHA-256(Block_{N-1}, n) = 0x00000000000000008c71...

Mint(X, C)

Mining difficulty
Preventing double spending

\[ \text{Sign}_A(\text{Transfer X to B}) \]

\[ \text{Sign}_A(\text{Transfer X to C}) \]

Longest chain wins
## Transaction confirmation (~6 blocks)

### My Wallet: Be Your Own Bank.

**Transactions** Summary of your recent transactions

<table>
<thead>
<tr>
<th>To / From</th>
<th>Date</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Today 10:27:48</td>
<td>26 Confirmations</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:57:</td>
<td></td>
</tr>
<tr>
<td>1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn</td>
<td>2014-02-13 21:21:57</td>
<td>Unconfirmed Transaction 0.00000001 BTC</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:24:57</td>
<td></td>
</tr>
<tr>
<td>1Enjoi1C4bYBr3tN4sMKxvvJDqG8NkdR4Z</td>
<td>2014-02-13 10:21:57</td>
<td>Unconfirmed Transaction 0.00000001 BTC</td>
</tr>
<tr>
<td>1ScoiWwFFySPjQo2biVfxn8NRPCSQC</td>
<td>2014-02-13 10:21:57</td>
<td>Unconfirmed Transaction 0.00000001 BTC</td>
</tr>
</tbody>
</table>
Bitcoin is *transaction-based*
Part II: Mining & Consensus
51% attacks

Goldfinger Attack?
Checkpointing

Bitcoin is *not* fully decentralized.
Selfish mining

Observation: for $0.33 < x < 0.5$, a fraction $x$ of selfish miners can earn greater than a fraction $x$ of rewards [Eyal, Sirer 2013]
Mining difficulty

Bitcoin Hash Rate vs Difficulty (2 Months)
Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty

10 minutes

2 weeks
Mining rewards

Total BTC In Existence

blocks: 0, 210k, 420k, 630k, 840k, 1.05M, 1.26M

Time: 2009, +4 years, +8, +12, +16, +20, +24

25 BTC/block
50 BTC/block
12.5
6.25
3.125
1.5625
0.78125

Brian Warner
Total network capacity

- $2^{64}$ hashes per block (every 10 minutes!)
- $2^{75}$ hashes in 2013
  - In exchange for ~US$250M
Bitcoin mining hardware

TerraMiner™ IV – 2TH/s
Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card
The Monarch BPU 300 C
$1,497.00

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.
Why would anybody mine bitcoins?

Chilkoot pass, Klondike 1898
Mining pools

BTC Guild: 15%
Part III: Bitcoin as a currency
Why does Bitcoin have value?

Consensus

• Consensus in state (blockchain)
• Consensus in payment
• Consensus in rules

[Kroll, Felten 2013]
Price during 2013

Mt. Gox (USD)
Dec 03, 2013 – Daily

Op:1100, Hi:1106, Lo:1065, Cl:1089
Vol: 2.824K

UTC – http://bitcoincharts.com
Black Markets

Silk Road: US$14M in Revenue in 2012 [Christin 2012]
Capital controls

As Inflation Rages In Iran, Bitcoin Software Not Available

Central Bank Of Cyprus Does Not Like Bitcoin

BTC China CEO Attempts To Calm The Bitcoin Market After RMB Deposit Shutdown
E-commerce

Payment Information

Credit/Debit card

- Visa
- Mastercard
- American Express
- Discover

Card Number *

Expiration Date *

01 Jan ▼ 2014 ▼

PayPal

The safer, easier way to pay.

Learn More

Bitcoin

Accepts here

Learn More

RewardsPay

Discover Choice Privileges

What's this?

V.me by Visa

Learn More

I want to use a promo code

Why Can't I Use a Gift Card?
Bitcoin exchanges

Around half of all exchanges have collapsed [Moore, Christin 2012]
### Geographic distribution of nodes (as of Dec 2013)

<table>
<thead>
<tr>
<th>Country</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>50484</td>
</tr>
<tr>
<td>China</td>
<td>48863</td>
</tr>
<tr>
<td>Germany</td>
<td>17232</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>15334</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>13721</td>
</tr>
<tr>
<td>Canada</td>
<td>9416</td>
</tr>
<tr>
<td>Netherlands</td>
<td>7077</td>
</tr>
<tr>
<td>Australia</td>
<td>5469</td>
</tr>
<tr>
<td>France</td>
<td>5024</td>
</tr>
<tr>
<td>Poland</td>
<td>4706</td>
</tr>
</tbody>
</table>
Questions