Bitcoin has many different parts!
Part I: Bitcoin in 6 easy steps
Double spending: why ecash is hard

Alice

Bob

Charlie

BANK

Sign_A(Transfer X to B)

Sign_A(Transfer X to C)

Sign_Z(Transfer X to A)

Redeem X?
Step 1: Make the bank a global log

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

- Signature\textsubscript{A} Signature\textsubscript{B} Signature\textsubscript{C} ...
- Signature\textsubscript{A} Signature\textsubscript{B} Signature\textsubscript{C} ...
- Signature\textsubscript{A} Signature\textsubscript{B} Signature\textsubscript{D} ...

\textbf{Step 2: Participants vote on blocks}
Step 3: A random user picks

N-2

N-1

N

Signature_A

Signature_B

Signature_C
Step 4: Resolve conflicts by *forking*

Sign$_A$(Transfer X to B)

Signature$_A$

Sign$_A$(Transfer X to C)

Signature$_C$

Signature$_B$

Signature$_D$

Signature$_E$
Step 5: Incentivise correct blocks

Mint(X, A)  Signature$_A$

Mint(X, B)  Signature$_B$

Mint(X, C)  Signature$_C$

Mint(X, D)  Signature$_D$

Mint(X, E)  Signature$_E$
Step 6: Choose by hash power!

\[
\text{Mint}(X, A)
\]

\[
\text{SHA-256}(\text{Block}_{N-1}, n) = 0x0000000000000003f89\
\]

\[
\text{Mint}(X, B)
\]

\[
\text{SHA-256}(\text{Block}_{N-1}, n) = 0x0000000000000008c71\
\]

\[
\text{Mint}(X, C)
\]

**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.

<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>1Bhv6XjXBraivcATHwwLMscZ5xJm9FsPn</td>
<td>2014-02-13 21:21:57</td>
<td>Unconfirmed Transaction</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:15</td>
<td></td>
</tr>
<tr>
<td>1Enjoy1C4bYBr3tN4sMKxvvJDqG8NkdR4Z</td>
<td>2014-02-13 10:00</td>
<td>Unconfirmed Transaction</td>
</tr>
<tr>
<td>1SochiWwFFySPjQo2biVftXn8NRPCSQC</td>
<td>2014-02-13 10:00</td>
<td>Unconfirmed Transaction</td>
</tr>
</tbody>
</table>
Real time bitcoin

http://www.blockchain.info
Bitcoin is *transaction-based*
Bitcoin transactions specify *scripts*

scriptPubKey: \texttt{OP\_DUP OP\_HASH160 <pubKeyHash> OP\_EQUALVERIFY OP\_CHECKSIG}

\begin{center}
\begin{tikzpicture}
  \node (in) at (0,0) {IN: \>
    \begin{itemize}
      \item scriptSig ...
      \item scriptSig ...
    \end{itemize}
  };

  \node (out) at (2,-2) {OUT: \>
    \begin{itemize}
      \item scriptPub A, 5.9
    \end{itemize}
  };

  \node (in2) at (4,-4) {IN: \>
    \begin{itemize}
      \item scriptSig A
    \end{itemize}
  };

  \node (out2) at (6,-6) {OUT: \>
    \begin{itemize}
      \item scriptPubB, 5.0
      \item scriptPubA, 0.9
    \end{itemize}
  };

  \draw (in) -- (out);
  \draw (in2) -- (out2);
\end{tikzpicture}
\end{center}

Redemption script:

\texttt{<sig> <pubKey> OP\_DUP OP\_HASH160 <pubKeyHash> OP\_EQUALVERIFY OP\_CHECKSIG}
Bitcoin transactions specify scripts

```
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```
Bitcoin script features

- multiple signatures
- escrow
- time locking
- commitment opening

...
Part II: Mining & Consensus
51% attacks

Goldfinger Attack?
Checkpointing

How decentralized is Bitcoin?
Selfish mining

Observation: for $0.33 < x < 0.5$, a fraction $x$ of selfish miners can earn greater than a fraction $x$ of rewards.

Majority is not enough: Bitcoin mining is vulnerable
Ittay Eyal and Emin Gün Sirer. Financial Crypto 2014
Mining difficulty

Bitcoin Hash Rate vs Difficulty (2 Months)

- Hash Rate (504)
- Hash Rate (1000)
- Hash Rate (2016)
- Difficulty

Feb
Mar
Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty

- Block Generation Time (2009)
- Block Generation Time (2016)
- Estimated Next Difficulty
- 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

21.0M

25 BTC/ block

50 BTC/ block

12.5

6.25

3.125

1.5625

0.78125

Courtesy: Brian Warner
Total network capacity

- $2^{64}$ hashes per block (every 10 minutes!)
- $2^{75}$ hashes in 2013
  - In exchange for ~US$250M
- Consuming > 100 MW
Bitcoin mining hardware

**TerraMiner™ IV – 2TH/s Networking 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.
Should I mine bitcoins?

Chilkoot pass,
Klondike 1898
Mining pools

Mint(25, K_{\text{POOL}})

0x00000000000000003f89...
0x000000000000490c6b00...
0x000000000000a877902e...
0x000000000001e8709ce...
0x00000000000007313f89...
0x00000000000045a1611f...
0x000000000000000045a1611f..
Mining pools
Part III: Bitcoin as a currency
Why does Bitcoin have value?

Consensus

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

The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries
Joshua Kroll, Ian Davey, Ed Felten. WEIS 2013
Price during 2013
Price during 2013-2015

Market Price (USD)
Source: blockchain.info
Black Markets

Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace
Nicolas Christin, WWW 2013
Capital controls

As Inflation Rages In Iran, Bitcoin Software Not Available

Central Bank Of Cyprus Does Not Like Bitcoin

12:41 pm  Feb 7, 2014  EUROPE

ARTICLE  COMMENTS (9)

BITCOIN  CYPRUS  VIRTUAL CURRENCIES

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

Posted Dec 20, 2013 by John Biggs (@johnbiggs)
E-commerce

Payment Information

Credit/Debit card

Visa, Mastercard, American Express, Discover

Card Number *

Expiration Date *

01 Jan  ▼  2014  ▼
Beware the middleman: Empirical analysis of Bitcoin-exchange risk
Tyler Moore and Nicolas Christin, Financial Crypto 2013
Bitcoin ATMs
Bitcoin meetups
Bitcoin meetups

Buy and sell bitcoins near you


Trade bitcoins in 5616 cities and 233 countries including United States.

Sign up free
Part IV: Neat applications
Green Addresses  (speeding up payments)

IN: scriptSig ...
OUT: scriptPub A, 10.0

IN: scriptSig A
OUT: scriptPub O, 1.0
scriptPub A, 9.0
Green Addresses (speeding up payments)

IN: scriptSig ...
OUT: scriptPub G,
10.0

IN: scriptSig A
OUT: scriptPub O,
1.0
scriptPub A, 9.0

I promise to never double-spend!
Sequential micropayments

I promise to never double-spend!
Secure commitments (timestamping)

CommitCoin: carbon dating commitments with Bitcoin
Jeremy Clark, Aleksander Essex. Financial Crypto 2012
Randomness Beacon
Part V: Anonymity
Tracing Bitcoin transactions

Joint control

Change addresses
Building the transaction graph

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
Sarah Meiklejohn et al, IMC 2013
Bitcoins carry a transaction history

- identification
- censorship
- recovery from theft
- economic analysis

Towards Risk Scoring of Bitcoin Transactions
Möser, Malte, Rainer Böhme, and Dominic Breuker, BITCOIN 2013
Mixes
Mixes today

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.

-The Bitcoin Wiki

An inquiry into money laundering tools in the Bitcoin ecosystem Möser, Malte, Rainer Böhme, and Dominic Breuker, ECRIME 2013
Better mixes with warranties

If $v \xrightarrow{k_{esc}}$ by $t_{in}$
Will you send $v$ to my address $k_{out}$ by time $t_{out}$?

Sure! Just send your coins $k_{esc}$
Sign($v, t_{in}, t_{out}, k_{out}, k_{esc}$)

If $v \xrightarrow{k_{esc}}$ by $t_{in}$, but not $v \xrightarrow{k_{out}}$ by $t_{out}$
The client publishes

Anyone can verify cheating (Ideally) no one trusts anymore

Mixcoin: Anonymity for Bitcoin with accountable mixes
Coin Join

IN:
- scriptSig P
- scriptSig M
- scriptSig S

OUT:
- scriptPub P', 1.0
- scriptPub M', 1.0
- scriptPub S', 1.0
Zerocoin:
Anonymous distributed e-cash from bitcoin
Ian Miers, Christina Garman, Matthew Green, Avi Rubin. IEEE Oakland 2013
Zerocash

“Cryptocurrencies are just a gateway drug to SNARKS”

Zerocash: Decentralized Anonymous Payments from Bitcoin
E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza IEEE Oakland 2014
Part VI: Extensions & Altcoins
Types of changes to Bitcoin

- overlay
- soft fork
- hard fork
- alternate chain
- alternate systems
Overlays
Soft fork changes

- Pay-to-script-hash
- Pay-to-SNARK (CoinWitness)
- ECDSA-P256 replacements
- Zerocoin
Hard fork changes

- Change block size
- Change block frequency
- Various bug fixes
- Restructuring the chain
<table>
<thead>
<tr>
<th>Rank</th>
<th>Altcoin</th>
<th>Market Cap</th>
<th>Price</th>
<th>Circulating Supply</th>
<th>Market Value</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$7,097,242,840</td>
<td>$564.76</td>
<td>12,566,750 BTC</td>
<td>$2,268,1,849</td>
<td>-1.30 %</td>
</tr>
<tr>
<td>2</td>
<td>Ripple</td>
<td>$1,218,679,623</td>
<td>$0.012</td>
<td>99,999,996,204 XRP*</td>
<td>$187,080</td>
<td>-3.18 %</td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$418,684,497</td>
<td>$15.55</td>
<td>26,929,454 LTC</td>
<td>$12,818,307</td>
<td>-3.74 %</td>
</tr>
<tr>
<td>4</td>
<td>Auroracoin</td>
<td>$77,601,206</td>
<td>$7.30</td>
<td>10,634,451 AUR**</td>
<td>$628,741</td>
<td>+7.93 %</td>
</tr>
<tr>
<td>5</td>
<td>Peercoin</td>
<td>$55,510,590</td>
<td>$2.61</td>
<td>21,261,439 PPC</td>
<td>$180,299</td>
<td>-3.19 %</td>
</tr>
<tr>
<td>6</td>
<td>Dogecoin</td>
<td>$38,281,608</td>
<td>$0.0006</td>
<td>64,273,042,487 DOGE</td>
<td>$1,146,122</td>
<td>-6.67 %</td>
</tr>
<tr>
<td>7</td>
<td>Nxt</td>
<td>$33,546,132</td>
<td>$0.034</td>
<td>999,997,096 NXT*</td>
<td>$127,871</td>
<td>-5.60 %</td>
</tr>
<tr>
<td>8</td>
<td>Namecoin</td>
<td>$22,326,015</td>
<td>$2.67</td>
<td>8,356,432 NMC</td>
<td>$128,414</td>
<td>-3.29 %</td>
</tr>
<tr>
<td>9</td>
<td>Silicon Valley Coin</td>
<td>$21,053,209</td>
<td>$1.20</td>
<td>17,536,750 XSV**</td>
<td>$15,150</td>
<td>?</td>
</tr>
</tbody>
</table>
Other altcoins

- Ethereum
- Ripple
Bitcoin limitations

● ~7 transactions per second
  ○ Visa: ~10k tps (peak)
● $2^{48}$ currency units
  ○ ~32k per person on earth
● 0.0001 BTC transaction fees typical
  ○ ~$0.40 US
● ~60 minutes confirmation delay

A reserve currency?
Questions