Bitcoin: Concepts, Practice, and Research Directions

Ittay Eyal, Emin Gün Sirer

Computer Science, Cornell University

DISC Bitcoin Tutorial, October 2014
2008: The Bitcoin white paper
2009: Reference implementation
[Satoshi Nakamoto]
• Decentralized control
• Decentralized minting
• Easy to transfer
• Novel tech, new applications
Banks: criminals, who print money and lend it as debt.

Gold

Fiat

Bitcoin or oligarchy?

Separate church and state? Separate bank and state!

taxation is a crime!
Great Success!

Mt. Gox USD/BTC

[http://bitcoincharts.com/]

Copyright © 2014 Ittay Eyal, Emin Gün Sirer
Great Success!

Mt. Gox USD/BTC

Mt. Gox (USD)
Feb 11, 2014 − Daily
[Closing Price: 583.9]

[http://bitcoincharts.com/]

Copyright © 2014 Ittay Eyal, Emin Gün Sirer
Mostly Great Success

USD/BTC (Bitstamp)

[http://bitcoincharts.com/]
Acceptance
Acceptance

airBaltic
CheapAir.com
overstock.com
newegg.com
Dell
coinbase
CIRCLE
bitpay
Acceptance

Silk Road
anonymous marketplace

Shop by category:
- Cannabis(203)
- Ecstasy(35)
- Psychedelics(127)
- Opioids(39)
- Stimulants(68)
- Dissociatives(9)
- Other(197)
- Benzos(43)

recent feedback:

<table>
<thead>
<tr>
<th>seller</th>
<th>rating</th>
<th>feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1UP of Canada(97)</td>
<td>4 of 5</td>
<td>amazing weed, the order was flattened, which I like.</td>
</tr>
<tr>
<td>CaliforniaSunrise</td>
<td>5 of 5</td>
<td>Fast shipping. Nice stuff.</td>
</tr>
<tr>
<td>Rook</td>
<td>5 of 5</td>
<td>all good! thanks so much</td>
</tr>
<tr>
<td>illy</td>
<td>5 of 5</td>
<td>Very friendly. Fast</td>
</tr>
<tr>
<td>somatik</td>
<td>5 of 5</td>
<td>Order arrived quickly</td>
</tr>
<tr>
<td>gamey54</td>
<td>5 of 5</td>
<td>No issue at all, I own it.</td>
</tr>
<tr>
<td>mellowyellow</td>
<td>5 of 5</td>
<td>Item arrived quickly</td>
</tr>
<tr>
<td>dirtysof(100)</td>
<td>5 of 5</td>
<td>looks good</td>
</tr>
</tbody>
</table>

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney’s Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York
Many Players

• Farmers
• Payment services
• Investors
• Start-ups
• Venture Capital
• Miners
• Developers
• Researchers
Roadmap

• Protocol
• Security
• Research
• Non-technical
Bitcoin: Concepts, Practice, and Research Directions

Part I Protocol

Ittay Eyal, Emin Gün Sirer

Computer Science, Cornell University

DISC Bitcoin Tutorial, October 2014
Part 1 – Protocol

• Overview
• The Blockchain
• Block propagation
• Mining
• Transactions
Protocol Overview
Key Issues

1. Stealing
2. Double-spending ➔ Not a local solution
Global Ledger

M → A
A → B
B → C
Global Ledger

A → B

M → A

A → C

Copyright © 2014 Ittay Eyal, Emin Gün Sirer
Addresses and Transactions

\[ \text{txn}_{AB}, PK(C), sgn_{SK(B)} \]
## Addresses and Transactions

Transaction structure (roughly):

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>input 1</td>
<td>output 1, amount 1</td>
</tr>
<tr>
<td>input 2</td>
<td>output 2, amount 2</td>
</tr>
<tr>
<td>input 3</td>
<td>output 3, amount 3</td>
</tr>
<tr>
<td>input 4</td>
<td></td>
</tr>
</tbody>
</table>

Inputs are fully spent.
Goal

1. No stealing
2. No double-spending
The Blockchain
Global Ledger

Global Ledger of all transactions

Requirements

1. No central control
2. High availability, security
3. Impossible to manipulate
4. Distributed minting
Global Ledger of all transactions

Requirements
1. No central control
2. High availability, security
3. Impossible to manipulate
4. Distributed minting

Sounds like my bank!

Doesn’t sound like my bank.
Global Ledger

- Distributed system
- Open
- Consensus (not exactly)
- Byzantine model
The Blockchain

Ledger

Blockchain

block
The Blockchain

Ledger

Blockchain

block
The Blockchain

Ledger

Blockchain

block
• Clients issue unforgeable transactions.
• Miners collate transactions and ...
• add them to blockchain by solving cryptopuzzles, for which they receive a reward (minted coins).
Transaction and Block Propagation

- Nodes propagate legal transactions and blocks.
- Blocks are difficult to create
Auto-adjusting difficulty cryptopuzzle:

\[
\text{SHA256(SHA256(block-header))} < \text{target}
\]
Forks

- Longest chain of blocks
  - Tiebreaker: earliest

A weak form of consensus
Fork Resolution

- Requirement: compute majority is honest
- Hardest chain of blocks (aggregate difficulty)
  - Or the one you heard of first.
Fork Resolution

- Requirement: **compute majority is honest**
- **Hardest** chain of blocks (aggregate difficulty)
  - Or the one you heard of first.

Dishonest majority controls blockchain

(More on that later)
Block Propagation
For blocks larger than $20kB$: $1kB \Rightarrow +80msec$
Block Propagation

Large miners connected directly with low latency.

For blocks larger than 20kB:
1kB $\Rightarrow +80\text{msec}$

[Decker and Wattenhofer ‘13]
Block Propagation

For blocks larger than 20kB:
1kB $\Rightarrow$ +80msec

Header before block?

[Decker and Wattenhofer ‘13]
Mining
Motivation?

- Prize:
  - **Mining**: Newly minted coins (today 25฿, total 21 million at 2140)
  - Transaction fees (up to $10^{-4}$ ฿/1KB).

How?

- **Coinbase** transaction
- Transactions **fees**
Mining

Difficulty rise:

Total Network Hash Rate

Hash Rate [TH/sec]

(More on that later)

[Blockchain.info]
Difficulty rise:

Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!

I admit, like a lot of others, I've found myself with a bit of a bitcoin obsession lately. I find the vast amount of effort it takes to create something that doesn't actually exist, completely fascinating. So I decided to find out how much computing power is exerted in the effort to mine and run the global bitcoin network.

Back in May, the bitcoin network hashrate estimate on bitcoinwatch.com passed 1 exaFLOPS (1,000 petaFLOPS) -- over 8 times the combined speed of the top 500 supercomputers. Today the aggregate bitcoin FLOPS measurement stands at 64 exaFLOPS (64,000 petaFLOPS). To contrast that number, this month the top 500 supercomputers combined clocked in at 0.250 exaFLOPS (250...
Mining Pools

Example: (700 USD/BTC)

- **Avg revenue:** $6.71 / day
- **HW break even:** ~1.5 years (w/ free power)
- **Time to block:** over 7 years

**Butterfly Labs 50 GH/s**
$2,500
300W
Mining Pools

- Pool with power $\alpha$ gets $\alpha$ of blocks
- Each miner makes the average ($-$ pool fee)
Mining Pools
Mining Pools

How can they tell?
Mining Pools

\[ \text{hash(\cdot)} < \text{target} \]

\[ \text{hash(\cdot)} < \text{pool-target} \]

Bitcoin Network
Mining Pools

(More on that later)

[Blockchain.info, February 2014]
Transactions
Transactions

Ledger

Blockchain

block
Transactions
Transactions

- Input 1
- Input 2
- Input 3

- Output 1, amount 1
- Output 2, amount 2
Pay-to-PubkeyHash

output: scriptPubKey

Input: scriptSig

Copyright © 2014 Ittay Eyal, Emin GünenSirer
Pay-to-PubkeyHash

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

scriptSig: \texttt{<sig> \ <pubKey>}

\begin{itemize}
  \item \textbf{output}: scriptPubKey
  \item \textbf{Input}: scriptSig
\end{itemize}

Address is the \textbf{public key hash}.

Owner \textbf{signs} with matching \textbf{private key}.
Pay-to-PubkeyHash

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

scriptSig: \texttt{<sig> <pubKey>}

Verification script

\begin{verbatim}
<sig>
<pubKey>
OP\_DUP
OP\_HASH160
<pubKeyHash>
OP\_EQUALVERIFY
OP\_CHECKSIG
\end{verbatim}
## Pay-to-PubkeyHash

**scriptPubKey:**
```
OP_DUP OP HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

**scriptSig:**
```
<sig> <pubKey>
```

### Stack

```
<sig>
```

### Verification script

```
<pubKey>
```
```
OP_DUP
```
```
OP_HASH160
```
```
<pubKeyHash>
```
```
OP_EQUALVERIFY
```
```
OP_CHECKSIG
```
Pay-to-PubkeyHash

scriptPubKey: \texttt{OP\_DUP\ OP\_HASH160 \textless pubKeyHash\textgreater\ OP\_EQUALVERIFY\ OP\_CHECKSIG}

scriptSig: \texttt{\textless sig\textgreater\ \textless pubKey\textgreater}

\begin{tabular}{|c|c|}
\hline
\texttt{<pubKey>} & \texttt{<sig>} \\
\hline
\end{tabular}
Pay-to-PubkeyHash

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

scriptSig: \texttt{<sig>\ <pubKey>}

\begin{center}
\begin{tabular}{|c|}
\hline
\texttt{<pubKey>} \\
\hline
\texttt{<pubKey>} \\
\hline
\texttt{<sig>} \\
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{|c|}
\hline
\texttt{OP\_HASH160} \\
\hline
\texttt{<pubKeyHash>} \\
\hline
\texttt{OP\_EQUALVERIFY} \\
\hline
\texttt{OP\_CHECKSIG} \\
\hline
\end{tabular}
\end{center}
Pay-to-PubkeyHash

scriptPubKey: **OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG**

scriptSig: **<sig> <pubKey>**

---

**Stack**

```
<table>
<thead>
<tr>
<th>hash160(&lt;pubKey&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;pubKey&gt;</td>
</tr>
<tr>
<td>&lt;sig&gt;</td>
</tr>
</tbody>
</table>
```

**Verification script**

```
<table>
<thead>
<tr>
<th>&lt;pubKeyHash&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP_EQUALVERIFY</td>
</tr>
<tr>
<td>OP_CHECKSIG</td>
</tr>
</tbody>
</table>
```
Pay-to-PubkeyHash

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

scriptSig: \text{<sig>\ <pubKey>}

<table>
<thead>
<tr>
<th>Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{&lt;pubKeyHash&gt;}</td>
</tr>
<tr>
<td>hash160(\text{&lt;pubKey&gt;})</td>
</tr>
<tr>
<td>\text{&lt;pubKey&gt;}</td>
</tr>
<tr>
<td>\text{&lt;sig&gt;}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verification script</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{OP_EQUALVERIFY}</td>
</tr>
<tr>
<td>\text{OP_CHECKSIG}</td>
</tr>
</tbody>
</table>
Pay-to-PubkeyHash

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

scriptSig: \hspace{1cm} <\texttt{sig}> \hspace{1cm} <\texttt{pubKey}>

\begin{center}
\begin{tabular}{c}
\hline
\texttt{Stack} \hline
\hline
\texttt{<pubKey>}
\hline
\texttt{<sig>}
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{c}
\hline
\texttt{Verification} \hspace{1cm} \texttt{script} \hline
\hline
\texttt{OP\_CHECKSIG}
\hline
\end{tabular}
\end{center}
Pay-to-PubkeyHash

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`

scriptSig: `<sig> <pubKey>`

Stack

Verification script

Return true.
Other Transaction Types

- **Coinbase**
  No input

- **Pay to Script Hash (P2SH)**
  Script in signature (receiver side)

- **Multisig**
  Require k/n signatures