What You Need to Know About Bitcoin & Crypto

Benjamin Jun, HVF Labs
Is this the Future of Money?

BTC market cap = 10% US M0 Money Supply

Coinbase Users > Charles Schwab Users

“Summer of Crypto” 2X market cap
Today’s Agenda

1/ FUNDAMENTALS
• Bitcoin, Blockchain, and Smart Contracts
• Ethereum, Tokens, and ICOs

2/ APPLICATIONS
• Blockchain for the Enterprise
• Case: Identity and Federations
• Legal – Smart Contracts, Blockchain, and ICOs

3/ ATTACKS
• Cryptocurrency Attacks and Security Challenges
• Bad Actors in ICOs, Ransomware
Bitcoin: A Peer-to-Peer
Electronic Cash System (2008)

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction
Units of Value

Token value based on supply & demand
SHA-256 Hash Function (adopted 2002)

1. Repeat SHA-256 until result = “rare”
2. Credit the finder

Hashes

<table>
<thead>
<tr>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000000000000000000000023279ea4059b36d44a354b1d283560c0db0860c508f620d</td>
</tr>
</tbody>
</table>
Modern Mining Tools

**GEFORCE® GTX 1080 Ti**
Founders Edition
LEARN MORE

$699.99
OUT OF STOCK

Free Shipping
Limit 2 per customer

---

**GEFORCE® GTX 1080**
Founders Edition
LEARN MORE

$549.99
OUT OF STOCK

Free Shipping
Limit 2 per customer

---

**GEFORCE® GTX 1070 Ti**
Founders Edition
LEARN MORE

$479.99
NOTIFY ME

Free Shipping

---

**GEFORCE® GTX 1070**
Founders Edition
LEARN MORE

$399.99
OUT OF STOCK

Free Shipping
Limit 2 per customer

---

**GEFORCE® GTX 1060**
Founders Edition
LEARN MORE

$299.99
OUT OF STOCK

Free Shipping
Limit 2 per customer
Contracts

Bitcoin
Signed Transfers

Alice’s Car
Transfer to Bob

Bob’s Car
Transfer to Cheryl

Alice Signs
Bob Signs
Digital Signatures

Alice —> Bob
Bob —> Cheryl
Cheryl —> Dan
Dan —> Eve

Merkle - Diffie - Hellman
Luca Pacioli  ~1500

Medici Family
Debtors & Creditors (1605-1633)
When Contracts Aren’t Centralized...

FORGED DATA

DOUBLE SPEND
Public Ledger
Satoshi’s Blockchain
Order From Crowds
A Closer Look
Bitcoin Statistics (April 2018)

Supply = ~17M bitcoins (BTC)
Demand = exchange rate: $8000 USD per BTC

- **$137B** in circulation (3.6% of US M0 money supply)
- Daily on-chain transactions: **$5B** (3.5%)
- Daily mining: **144 “winners”, 1800 BTC, $14.4M**
Bitcoin Blockchain (Ledger!)

Size: 164GB
(April 2018)

1500-2000 transactions

New block every ~10 min
# Block #132749: Header Data

## Block Depth & Time

<table>
<thead>
<tr>
<th>Height</th>
<th>132749 (Main Chain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>2011-06-23 06:50:15</td>
</tr>
</tbody>
</table>

## Hashes

<table>
<thead>
<tr>
<th>Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
</tr>
<tr>
<td>Previous Block</td>
</tr>
</tbody>
</table>

Lots of leading zeros...
Block #132749: Transactions

Transactions

Mining “winner” gets 50 BTC

Transfer of 424 BTC
Identity ("Wallet") Management

Bitcoin Address

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
</tr>
<tr>
<td><strong>Hash 160</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No. Transactions</strong></td>
</tr>
<tr>
<td><strong>Total Received</strong></td>
</tr>
<tr>
<td><strong>Final Balance</strong></td>
</tr>
</tbody>
</table>
Wallet Operations

Key Management
- Create Private Keys
- Derive Public Keys
- Distribute Public Keys
- Monitor For Outputs

Sign Outbound Transactions
- Create Unsigned Txes
- Sign Txes
- Broadcast Txes

Monitor Blockchain For Incoming BTC
Place Outbound Transactions to Blockchain
Decentralized, Trustless, Transparent

Bitcoin is coordinated under policies set in motion by Satoshi in 2008. It has no central administrator and no governing body*.

* These folks may want to talk to you:
  - Securities and Exchange Commission
  - Commodity Futures Trading Commission
  - Internal Revenue Service
  - US States
  - Department of Treasury
Post-Satoshi World
“Trust” and Enforcement

1. Fiat

2. Guarantor

3. Consensus, Transparency
Internet-Scale Routing, Membership

ARPANET, 1980
Contract Virtualization
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction
HVF Labs

ben@hvflabs.com
## Transaction

<table>
<thead>
<tr>
<th>Standard TxIn</th>
<th>Spend Coinbase TxOut</th>
<th>Coinbase/Generation</th>
<th>Standard TxOut Script</th>
<th>Coinbase TxOut Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 VI 32 4 VI SigScript</td>
<td>4 32 4 VI SigScript</td>
<td>4 32 4 VI SigScript</td>
<td>4 VI 8 VI PkScript</td>
<td>8 VI PkScript</td>
</tr>
</tbody>
</table>

**Version**: #TxIn

**TxIn 0**: TxIn 1

**TxIn 1**: TxIn 2

**TxOut 0**: TxOut 1

**TxOut 1**: LockTime

**Sig&PubKey (script)**

**Signature (script)**

**Arbitrary Data**

---

Scripts and DER encoding both use big-endian values, all other serializations use little-endian.