Bitcoin: System Architecture, Opportunities and Challenges

Sascha Boehme
saschafb@gmail.com

March 9, 2015
“The only way to confirm the absence of a transaction is to be aware of all transactions.”

Content

What is Bitcoin?

System Architecture

Opportunities

Challenges

Closing

Q&A
WHAT IS BITCOIN?

SYSTEM ARCHITECTURE

OPPORTUNITIES

CHALLENGES

CLOSING

Q&A
What is Bitcoin?

Bitcoin is a Cryptocurrency

Source: Royal Canadian Mint

© Sascha Boehme

saschafb@gmail.com
What is Bitcoin?

Bitcoin is a Cryptocurrency

Bitcoin is money and a peer-to-peer payment network

Sources: Royal Canadian Mint, bitcoin.org

© Sascha Boehme saschafb@gmail.com
Money is a ...

- **medium of exchange**
  something that people can use to buy and sell from one another;

- **unit of account**
  providing a common basis for prices;

- **store of value**
  which means people can save it and use it later.

What is Bitcoin?
A cryptocurrency is based on digital cryptography

Derives trust from
• NOT from legal tender statutes
• NOT from chemical/physical properties
• mathematical properties
• based on established, trusted, cryptographic principles
  – cryptographic hashing
  – digital signatures
  – public key infrastructure
What is Bitcoin?

**Bitcoin as a peer-to-peer network is ...**

- decentralized
- distributed
- democratic
- without the existence of a central authority
# How does Bitcoin work?

<table>
<thead>
<tr>
<th>What is Bitcoin?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bitcoin</strong></td>
</tr>
<tr>
<td><strong>bitcoins</strong></td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
</tr>
</tbody>
</table>
| **Public/Private key** | The receiver’s public key is his Bitcoin address  
                          The sender’s private key is used to digitally sign the transaction |
| **Block**        | Validated collection of transactions over 10 minutes, created through mining |
| **Mining**       | Generates a block and validates transactions through proof-of-work, creating new bitcoins in the process |
| **Blockchain**   | Timestamped sequence of linked blocks  
                          The public ledger |
What is Bitcoin?

What does a bitcoin look like?

Paper Wallet

Login Link: https://blockchain.info/wallet/5d413aeb-332e-4e1e-9b8a-e6b14e3c39d3
Mnemonic: bowl belly engine hockey database dramas fathering evil cooks

Scan to Load & Verify

Scan To Redeem

1MdCjxRVzWHSzjxGjQw1YKT5wLPHq4xVT
KoA5q3JMnUAixWpJ3h999LoEuayE3eoUHxw4kgcENg17ErikXB

© Sascha Boehme
What is Bitcoin?

Properties of Bitcoin

• Decentralized
• Distributed
• Democratic
• Anonymous
• Fast, cheap, and irreversible
• Secure
• No double spending
What is Bitcoin?

System Architecture

Opportunities

Challenges

Closing

Q&A
"Good architecture meets the goals of the system"

Source: Prof. Ed Crawley, ESD.34, MIT
System Architecture

A new electronic cash system for online payments

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.

The current payment system consists of three stakeholder groups

- **Primary Beneficiaries**
  - Payers
  - Payees

- **Beneficial Stakeholders**
  - Banks
  - Credit Card Companies
  - Money Transmitters
  - EPI Providers
  - Clearing Houses
  - Payment Processors

- **High Leverage Stakeholders**
  - Policymakers
  - Regulators
  - Central Banks

- **Needs & Goals**
  - Secure
  - Irreversible
  - Fast
  - Cheap
  - Easy to use
  - Direct
  - Anonymous

The needs and goals of the primary beneficiaries and high leverage stakeholders should drive the architecture.
System Architecture

Based on the needs and goals we can formulate a system problem statement to synthesize the system

System Problem Statement (SPS): “To provide willing parties a means:
• to transact directly with each other without the need for a trusted third party,
• by transferring a unique piece of digital property,
• using an electronic payment system based on cryptographic proof instead of trust.”

While also (descriptive goals):
• Being secure (no theft, fraud or double spending)
• Ensuring transactions are valid and irreversible
• Being fast, cheap and easy to use
• Providing anonymity to the parties involved
• Complying with pertinent regulation
• Allowing monetary policy

The SPS gives us a means to measure the quality of the architecture.
# System Architecture

## How does Bitcoin compare to the current payment system?

<table>
<thead>
<tr>
<th>Goals</th>
<th>Bitcoin</th>
<th>Current system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>✓</td>
<td>✖</td>
</tr>
<tr>
<td>Anonymity</td>
<td>✓</td>
<td>✖</td>
</tr>
<tr>
<td>Fast, cheap, and irreversible</td>
<td>✓</td>
<td>✖</td>
</tr>
<tr>
<td>Security</td>
<td>✓</td>
<td>(√)</td>
</tr>
<tr>
<td>No double spending</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Easy to use</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Compliance</td>
<td>✖</td>
<td>✓</td>
</tr>
<tr>
<td>Monetary Policy</td>
<td>✖</td>
<td>✓</td>
</tr>
</tbody>
</table>

Bitcoin currently fulfills many of the needs of the primary beneficiaries in the payment system. However, it does not fulfill the needs of the high leverage stakeholders.
System Architecture

Bitcoin was designed with two stakeholder groups in mind.

- Primary Beneficiaries
  - Payers
  - Payees

- Beneficiary Stakeholders
  - Bitcoin

- High Leverage Stakeholders

Bitcoin ignores all of the high leverage stakeholders and replaces the beneficiary stakeholders with new ones.
The Bitcoin Startup Ecosystem: Six Different Bitcoin Company Categories

Source: State of Bitcoin 2015, Coindesk

© Sascha Boehme
saschafb@gmail.com
System Architecture

**Bitcoin has the potential to revolutionize the payment industry**

<table>
<thead>
<tr>
<th>Goals</th>
<th>Bitcoin today</th>
<th>Current system</th>
<th>Bitcoin tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Anonymity</td>
<td>✓</td>
<td>✗</td>
<td>(✓)</td>
</tr>
<tr>
<td>Fast, cheap, and irreversible</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Security</td>
<td>✓</td>
<td>(✓)</td>
<td>✓</td>
</tr>
<tr>
<td>No double spending</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Easy to use</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compliance</td>
<td>✗</td>
<td>✓</td>
<td>(✓)</td>
</tr>
<tr>
<td>Monetary Policy</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

If Bitcoin evolves to fulfill the needs of the high leverage stakeholders, it could replace the current payment system. However, there will be trade-offs between goals.
WHAT IS BITCOIN?
SYSTEM ARCHITECTURE
OPPORTUNITIES
CHALLENGES
CLOSING
Q&A
Money transfer and online payments

“There is no reason, in principle, why final settlements could not be carried out by the private sector without the need to be cleared through the central bank.”

— Mervyn King, Governor of the Bank of England, 1999

Payments are cheaper, faster, and more secure with Bitcoin than with traditional payment systems, benefiting both sides of the transaction.
Potential to combat poverty and oppression

• There are about 2.5 billion unbanked people in the world
• Access to basic financial services is a promising antipoverty technique
• M-Pesa is a mobile payment system using phones, not banks, in countries such as Kenya and Tanzania
• Kipochi allows M-Pesa users to exchange bitcoins

Bitcoin can provide people in developing countries with inexpensive access to financial services on a global scale.
Micropayments

“The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions.”

- Pay per article instead of a subscription fee without pop-up ads
- Pay for Wi-Fi by the second on the go
- Pay milli-bitcoins per Email to avoid spam

Opportunities

Bitcoin allows the emergence of business models that were previously uneconomical

 What is Bitcoin?

System Architecture

Opportunities

Challenges

Closing

Q&A
Challenges

• Adoption
• Regulation
• Criminal Use
• Price Volatility
Regulatory frameworks around the world vary widely
Challenges

Regulation in the U.S.

Private currency

Money transmission laws
• Consumer protection: NYDFS BitLicense

AML and Terrorism Financing
• FinCEN

CFTC
• Commodity and currency derivatives

Regulation is both, a risk for the diffusion of Bitcoin if too heavy handed, and a boon if done right.
Challenges

The Silk Road case

Silk Road had an estimated $200 million in sales. 95% of which for drugs.

In October 2013 Silk Road was shut down

Silk Road was illegal, but so is dealing drugs in the physical world for dollars.
Mt. Gox was the worst scandal in Bitcoin history and precipitated the burst of the bubble in early 2014. An estimated $500 million in bitcoins were lost.
Price History – 2 Years

Source: blockchain.info (March 4, 2015)

© Sascha Boehme

saschafb@gmail.com
Challenges

The price of a bitcoin has fluctuated wildly in the past

- Extreme volatility deters the mainstream from holding bitcoins as a store of value
- And makes it unsuitable as a unit of account
- Merchants instantly exchange bitcoins for fiat
- But volatility will subside as
  - speculators leave the system
  - market capitalization rises
  - shorts become available
  - concentration decreases and liquidity increases
WHAT IS BITCOIN?

SYSTEM ARCHITECTURE

OPPORTUNITIES

CHALLENGES

CLOSING

Q&A
"The digital currency known as Bitcoin is only six years old ... It is, quite simply, one of the most powerful innovations in finance in 500 years."

P. Vigna, M. Casey: The Age of Cryptocurrency, 2015

© Sascha Boehme

saschafb@gmail.com
Bitcoin resources

- http://bitcoin.org
- http://blockchain.info
- http://www.coindesk.com
- http://two-bit-idiot.tumblr.com
- http://www.reddit.com/r/Bitcoin/
- Video “How Bitcoin works under the hood”: https://www.youtube.com/watch?v=Lx9zgZCMqXE
- P. Vigna, M. Casey: The Age of Cryptocurrency, 2015
- http://mitbitcoinexpo.org

© Sascha Boehme
saschafb@gmail.com
Contact details

Sascha Boehme

saschafb@gmail.com

www.linkedin.com/in/saschab Boehme

17nVzYtumxAyd6ycUv9Xu46GySxUTHwzp