
William Favre Slater, III, M.S. MBA, PMP, CISSP, CISA
Adjunct Professor, IIT School of Applied Technology

A Presentation for Forensecure 2014
Illinois Institute of Technology
Rice Campus, Wheaton, IL
April 2014
Agenda

• Introduction
• What is the Bitcoin?
• Bitcoin Terms
• Bitcoin History
• How does a Bitcoin Purchase Work?
• How does a Bitcoin Trade Work?
• How does a Bitcoin Mining Work?
• Comparing Bitcoin to Paypal
• Why is Bitcoin Popular?
• Bitcoins Strengths and Weaknesses
• Bitcoin Hype vs. Reality
• Bitcoin Dangers
• Latest Bitcoin News
• Bitcoin and the future of the Global Economy
• Other Cryptocurrencies
• Conclusion
• References
• Questions
Introduction

• Since the emergence of Bitcoin as the world’s leading “cryptocurrency” it has been met internationally with extreme reactions ranging from skepticism to fanaticism. It has also gotten the attention of governments and law enforcement agencies, as people have used Bitcoin’s attributes to undermine legal controls. This presentation will explain the Bitcoin, how it works, its strengths and weaknesses, the latest news about Bitcoin, and what it means for the future of the global economy.
What is the Bitcoin?

• Digital Currency
• A Decentralized, Peer-to-Peer Payment Network
• Requires the Internet to operate
• Anonymous, untraceable financial transactions
• A standardized “cryptocurrency” that uses a public key and a private key
Bicoin Characteristics

- Supported by the Bitcoin Foundation
- Bitcoin (BTC)
- blocks every 10 min
- coin supply 21 million coins will be available
- difficulty adjustment **1015 blocks, after 6 days**
- hashing algorithm **SHA256d**
- Initial Reward **50** coins per block
- Market Cap: $8 Billion (March 25, 2014)
- 80,000 Transactions / day
- Launch Date: January 3, 2009
Total Bitcoins in Circulation

Note: By definition, 21 million is the maximum number

Source: https://blockchain.info/charts/total-bitcoins
Why Does Bitcoin Have Value?

- You can buy good and services with it
- Investors speculate in it
- Scarcity
- People believe in it
- Good reputation, mostly
- Technophiles love it
- It’s “cool”
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

1. **Creating a New Address**
   - Bob creates a new Bitcoin address for Alice to send her payment to.
   - Bob and Alice both have Bitcoin "wallets" on their computers.
   - Wallets are files that provide access to multiple Bitcoin addresses.
   - Each address has its own balance of bitcoins.

2. **Verifying the Transaction**
   - It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

3. **Submitting a Payment**
   - Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.
   - Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

4. **Transaction Verified**
   - As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.
## Some Bitcoin Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES SHA-256</td>
<td>The 256-bit encryption algorithm that is AES standard used for Bitcoin keys.</td>
</tr>
<tr>
<td>Bitcoin Network</td>
<td>The Internet-connected network comprised of the software and data that supports Bitcoin transactions</td>
</tr>
<tr>
<td>Block Chain</td>
<td>The Bitcoin ledger of past transactions.</td>
</tr>
<tr>
<td>Difficulty</td>
<td>The measure of how difficult it is to find a new block compared to the easiest it can ever be</td>
</tr>
<tr>
<td>Exchange</td>
<td>A place that sells or buys Bitcoins, like a stock exchange.</td>
</tr>
<tr>
<td>Hash</td>
<td>It is a standard algorithmic function for the generation and verification of currency</td>
</tr>
<tr>
<td>Mining</td>
<td>Bitcoin mining serves 2 purposes, it creates the general ledger of Bitcoin transactions and it provides security.</td>
</tr>
<tr>
<td>Private Key</td>
<td>The secret cryptographic key that is used to protect your Bitcoin account.</td>
</tr>
<tr>
<td>Proof of Work</td>
<td>An economic time-stamped measure to deter service abuses on a network by requiring some work from the service requester, usually meaning processing time by a computer.</td>
</tr>
<tr>
<td>Public Key</td>
<td>The public (shared) cryptographic key that is used to protect your Bitcoin account</td>
</tr>
<tr>
<td>Transaction</td>
<td>Use of the Bitcoin to purchase good or services, or the purchase of sale of a Bitcoin, or fractional part of Bitcoin</td>
</tr>
<tr>
<td>Wallet</td>
<td>A service that will safely store your Bitcoin account for you.</td>
</tr>
</tbody>
</table>
What is **Bitcoind**?

- **Bitcoind** is a program that implements the Bitcoin protocol for command line and remote procedure call (RPC) use. It is also the first Bitcoin client in the network’s history. It is available under the MIT License in 32-bit and 64-bit versions for Windows, GNU/Linux-based Oses, and Mac OS X.
Brief Bitcoin History

- **2008** - Bitcoin software goes Open Source
- **January 3, 2009** - Bitcoin Network is Launched to support Bitcoin Purchases and Financial Transactions
- **July 31, 2010** - Bitcoin Network Speed reaches 1 Gigahash / second
- **May 31, 2011** - Bitcoin Network Speed reaches 1 Terrahash / second
- **September 15, 2013** – Bitcoin Network Speed reaches 1 Petahash / second
- **October 2, 2013** – The FBI shut down the Silk Road website that accepted Bitcoins for the sale of drugs
- **November 29, 2013**, Bitcoin value hits highest ever at $1129.74
- **January 24, 2014** – BitInstant CEO Charlie Shrem and Robert Faiella arrested and charged with money laundering $1 million through the Silk Road online business using BTC
- **February 26, 2014** - Mt. Gox Bitcoin Exchange files for bankruptcy, claiming over $500 million in lost Bitcoins from hacker attack
- **February 26, 2014** – First Meta CEO Autumn Radtke found dead of suspected suicide
- **February 27, 2014** – Satoshi Nakamoto is found hiding in plain sight in California
- **March 20, 2014** – Mt. Gox CEO announces that $200 million of missing money was found in an old BTC Wallet after a Federal Judge in Chicago had ordered a probe of transactions
- **March 27, 2014** – People’s Bank of China orders the close of all Chinese Bitcoin Exchanges by April 15, 2014
- **March 28, 2013** – Bitcoin Network Speed reaches 45 Petahash / second
- **April 8, 2014** – Bitcoin’s Lead Developer, Gavin Andresen steps down
- **April 8, 2014** – Bitcoin 2.0 Conference in New York City kicks off
Bitcoin Value History in USD

12-months
April 2013 – March 2014
How Does the Bitcoin Network Operate?

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block, using the accepted block as the previous hash.

Source: Bitcoin: A Peer-t-Peer Electronic Cash System by Satoshi Nakamoto
https://bitcoin.org/bitcoin.pdf

by William Favre Slater, III

Bitcoin Actors

- **Bitcoin User**
- **Bitcoin Exchange**
- **Merchant who accepts Bitcoin**
- **Bitcoin Miner**

**Bitcoin Database**

Private Key
Public Key

Private Key
Public Key

Private Key
Public Key

Private Key
Public Key
How does a Bitcoin Purchase Work?

• Assume: the new Bitcoin user has a means to purchase Bitcoin
• Contact a Bitcoin exchange via the Web and make the purchase at the current value of a Bitcoin
• Send a check or a money order with your ID to the Bitcoin exchange.
• The Bitcoin exchange will credit your Bitcoin account ensure your Bitcoin account is added to the network

• Note: The Bitcoin value can increase, decrease, or stay the same. I bought Bitcoin on Feb. 20, 2014 at $632. On March 30, 2014, my Bitcoin was worth $478.
How does a Bitcoin Trade Work?

• Assume: the Bitcoin user has a legitimate Bitcoin account and knows their balance
• The Bitcoin user finds a business that accepts payments in Bitcoins.
• The Bitcoin user submits their public Bitcoin ID information
• The Bitcoin authorized merchant processes the payment
• The Bitcoin user receives the goods or services
How does a Bitcoin Mining Work?

• Mining programs work to perform processing to insert a Bitcoin securely into a valid block chain.
• Processing is very computationally intensive, and uses a lot of CPU time, and a lot of electrical power.
• Rewards:
  – When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 25 bitcoins; this value will halve every 210,000 blocks.
  – Additionally, the miner is awarded the fees paid by users sending transactions. The fee is an incentive for the miner to include the transaction in their block. In the future, as the number of new Bitcoins miners are allowed to create in each block dwindles, the fees will make up a much more important percentage of mining income.
# How does a Bitcoin Mining Work?

## The Bitcoin Mining Ecosystem

### CPU Mining

Early Bitcoin client versions allowed users to use their CPUs to mine. As the network hashrate grew with more power efficient GPU miners the amount of Bitcoin's produced by CPU mining became lower than the cost of power to operate the CPUs. The option still exists in the reference Bitcoin client, but it is disabled by default.

### GPU Mining

GPU Mining is drastically faster and more efficient than CPU mining. See the main article: Why a GPU mines faster than a CPU. A variety of popular mining rigs have been documented.

### FPGA Mining

FPGA mining is a very efficient and fast way to mine, comparable to GPU mining and drastically outperforming CPU mining. FPGAs typically consume very small amounts of power with relatively high hash ratings, making them more viable and efficient than GPU mining.

### ASIC Mining

An application-specific integrated circuit, or ASIC, is a microchip designed and manufactured for a very specific purpose. ASICs designed for Bitcoin mining were first released in 2013. For the amount of power they consume, they are vastly faster than all previous technologies and already has made GPU mining financially unwise in some countries and setups.

### Mining Services

Mining contractors provide mining services with performance specified by contract. They may, for example, rent out a specific level of mining capacity for a set price for a specific duration. Mining shares provide Mining as a Service (MaaS). These break large-scale datacenter mining down to easily manageable pieces that are available in the form of shares of equipment. Hosted mining services create some systemic risk for the Bitcoin system because they undermine the security assumption that the control of mining power is well distributed. If too much mining becomes consolidated in large hosting providers and an attacker is able to compromise some of these providers they could potentially disrupt the Bitcoin system or rip off people they transact with reversals.
The first FPGAs were initially announced on the bitcointalk forums and offered 100-400 MH/s. At the time FPGAs were first introduced, the cost/benefit was questionable with top-end GPUs able to run at 700 MH/s, but they did offer additional benefits. Notably, a single computer could run stacks of FPGA miners, compared with just a few GPUs under normal conditions.

The Increase in Bitcoin Mining and Bitcoin Network Capability Positively Affects Bitcoin’s Value

Bitcoin Mining: Block Generation
Time vs. Difficulty

Source: https://bitcoinwisdom.com/bitcoin/difficulty
Bitcoin Mining: Block Generation Time vs. Difficulty

Source: https://bitcoinwisdom.com/bitcoin/difficulty
Bitcoin Mining: Block Generation

Time vs. Difficulty

Overview Statistics

Current Exchange Rate
- $470
- €340

Market Cap
- BTC: 12,582,775
- USD: $5,913,904,250
- EUR: €4,278,143,500

Network Stats
- Speed (PH/s): 34.84
- Difficulty (MM): 5006.86

Historical Difficulty Increase
- 30 Day: 31%
- 60 Day: 128%
- 90 Day: 324%

Source: https://tradeblock.com/mining/
Comparing Bitcoin to Paypal

Source: https://blockchain.info/wallet/paypal-vs-bitcoin
Comparing Bitcoin to Paypal

For Merchants

1 - 2

Services like bit-pay make accepting bitcoin's as easy for merchants as accepting PayPal, funds can be immediately exchanged for domestic currency so exposure to exchange rate fluctuations is minimal. The advantage for merchants is that as bitcoin is digital cash it does not support chargebacks, funds cannot be frozen and payments cannot be blocked.

Big win for Bitcoin.

Anonymity

1 - 3

A history of every bitcoin transaction ever made is available right here on this site. However transactions do not need to be tied to a bank account or individual and they are essentially anonymous if some basic precautions are taken. My Wallet can hold up to 1000 unique bitcoin addresses and it is recommended you change addresses regularly to avoid leaving a trail.

And the winner is, Bitcoin! A new technology which is just beginning to come into it's own. Sure there are some hurdles to jump but the ability to truly take control of your own finances is worth some minor inconvenience. If you value liberty, then you should value bitcoin.

Source: https://blockchain.info/wallet/paypal-vs-bitcoin
Comparing Bitcoin to Paypal

![Graph showing Bitcoin transaction volume compared to other payment networks.](http://www.businessinsider.com/bitcoin-versus-paypal-comparison-2013-12)
Why is Bitcoin Popular?

• New
• It’s easily available via the Internet
• International appeal
• It’s “cool”
• It’s supported by many “cool” businesses
• Exciting because it’s in the news
• Anonymous, and uses strong encryption, so it creates a sense of Privacy
• People understand electronic payments because easy to use services like PayPal have been around since 2000
Bitcoin in Daily Transactions

Daily Transaction Volume

$48,454,142

Linear Chart

Daily Transaction Quantity

66,328

Source: http://www.coinometrics.com/bitcoin/btix
Bitcoin in Daily Transactions

Logarithmic Chart

$48,454,142  66,234

Source: http://www.coinometrics.com/bitcoin/btix
Bitcoin in Daily Transactions

Volume and Quantity (Log scale) Chart

Daily Transaction Volume
$48,454,142

Daily Transaction Quantity
66,041

Bitcoin in Daily Transactions

Quantity (Log scale) Chart

$48,454,142

65,894

Source: http://www.coinometrics.com/bitcoin/btix
Bitcoin Legality by Country

Legend

- Yes
- Restricted
- No
- Not Established - yet

Bitcoin Strengths and Weaknesses

• **Strengths**
  – Convenient
  – Anonymous
  – Popular
  – Increasingly accepted in Business Transactions for goods and services
  – Open Source
  – Supported on all computing platforms and most smart phones
  – Uses the Internet
  – Not regulated by a central authority like the Federal Reserve
  – International Support

• **Weaknesses**
  – Misunderstood
  – It’s volatile in value
  – Restricted in some places, forbidden in Iceland
  – The image has been tarnished by bad news (drug dealers, kiddie porn, Mt. Gox bankruptcy, etc.)
  – The IRS is now very interested – Retroactively!
  – Not regulated by a central authority like the Federal Reserve
  – Losses are not insured
  – Hacker vulnerabilities (small, but they do exist)
  – The NSA is currently developing cryptoanalysis software and compute capabilities to defeat Bitcoins cryptographic scheme

April 10, 2014
# Bitcoin Hype vs. Reality

<table>
<thead>
<tr>
<th>Hype</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin is safe</td>
<td>It can be hacked</td>
</tr>
<tr>
<td>Bitcoin is anonymous and offers privacy</td>
<td>With entities like the NSA, nothing is or does</td>
</tr>
<tr>
<td>Bitcoin is a great investment</td>
<td>No. You can lose money. I have lost 25% since Feb. 20, 2014</td>
</tr>
<tr>
<td>Bitcoin mining is lucrative</td>
<td>The IRS is making Retroactive Rulings about Bitcoin as “property”. Talk to your lawyer AND your Accountant.</td>
</tr>
<tr>
<td>Bitcoin is simple to use and understand</td>
<td>Do your homework</td>
</tr>
<tr>
<td>Bitcoin will become more widely used and accepted</td>
<td>Maybe, but after more than five years, it hasn’t happened yet</td>
</tr>
<tr>
<td>Bitcoin still has a good name and is widely recognized.</td>
<td>Maybe yes. But events like the Silk Road shutdown, Mt. Gox bankruptcy and Autumn Radtke’s death don’t help Bitcoin’s image</td>
</tr>
</tbody>
</table>
Bitcoin Dangers

- It is still a volatile “investment”
- Vulnerability to Hackers
- Anonymous cryptocurrency transactions can and will arouse suspicion
- No central authority to regulate it
- Not insured
- Some experts have developed an extensive case AGAINST investing in Bitcoin
- The PBOC is working to ban Bitcoin inside China – March 27, 2014
- The IRS is regulating it retroactively – Virtual Currency Guidance – March 25, 2014

April 10, 2014

1. **February 26, 2014** - Mt. Gox Bitcoin Exchange files for bankruptcy, claiming over $500 million in lost Bitcoins from hacker attack (CEO Mark Karpeles pictured)

2. **February 26, 2014** – First Meta CEO Autumn Radtke found dead, and suicide is suspected

3. **February 27, 2014** – Satoshi Nakamoto is found hiding in plain sight in California

4. **March 25, 2014** – The IRS declares issues Virtual Currency Guidance stating that Bitcoin and other virtual currencies are “property” and retroactively now subject to taxes

Latest Bitcoin News

Bitcoin and the Future of the Global Economy

• The increasing visibility and acceptance of Bitcoin have given it positive international recognition

• Increasing concerns about the stability of U.S. Dollar and other fiat currencies (inflation, hyperinflation, debt, etc.), as well as geopolitical uncertainties have caused speculation in unusual investments like Bitcoin
Other Cryptocurrencies

• Major
  – Blackcoin (uses Proof-of-Stake)
  – Namecoin
  – Litecoin
  – Dogecoin
  – PPCoin
  – Mastercoin

• Others
  – See list at right
Conclusion

- **Bitcoin:**
  - A technical marvel made possible by software, hardware, strong cryptography, and the Internet
  - Has made significant progress in only 63 months
  - Has significant strengths and weaknesses
  - Has great potential because of popular support of talented nerds
  - Has attracted the interest of those who would like to control it (U.S. Government, especially the IRS)
  - Should be watched, studied, and understood carefully before making any big investments in Bitcoin accounts, mining, accepting transactions, etc.
References


References


References


References


• Bitcoin Links: http://bit.ly/1eixu78 (over 38 million)
Questions?
Career Opportunities?

• Yes – The U.S. Government is hiring Cybersecurity Professionals

• Private Industry will be picking up more and more Cybersecurity experts
Illinois Institute of Technology

- M.S. in Cyber Forensics and Security (land campus)

http://www.itm.iit.edu/cybersecurity/index.php

Bellevue University

Bellevue, NE  (land campus and online)

- M.S. in Cybersecurity
- B.S. in Cybersecurity

http://www.bellevue.edu/degrees/graduate/cybersecurity-ms/
Presenter Bio:
William F. Slater, III

- IT professional since July 1977
- Owner of Slater Technologies, Inc.
- An Adjunct Professor at the Illinois Institute of Technology – for six years
- First Data Center Manager of Microsoft’s Flagship Cloud Data Center, the Microsoft Chicago Data Center in 2008
- Managed Data Centers at BP from August 2001 – November 2006, was also a Change Management Manager and a System Administrator during that time.
- Have achieved 80 IT-related certifications, including PMP, CDCP, CISSP, SSCP, CISA, MCITP, MS Project, Visio, MCSE 2003 Security & Messaging, MCSD, MCAD, MCDST, and MCT
- Data Center Technology Program – Marist College & the Institute of Data Center Professionals, February 2008 – Received the Certified Data Center Professional Certification
- M.S. in Cybersecurity – Bellevue University, Bellevue, NE (completed on March 2, 2013)
- MBA, University of Phoenix, 2010
- MS in Computer Information Systems, University of Phoenix, 2004
- BS in Engineering Technology with a major in Computer Systems Technology, University of Memphis
- Published author & editor: Magazines, books, courseware
- Subject Matter Expert in Cybersecurity for Caveon Courseware and Testing
- Happily married (since December 2000) to Joanna K. Roguska, who is a professional web developer
- A former U.S. Air Force computer systems staff officer at Strategic Air Command Headquarters supporting the SAC Underground and SAC Battle Staff Command Control Communications Systems, July 1977 – October 1980
- Native of Memphis, Tennessee, born the same month and year as Bill Gates
- Resident of Chicago
- Active member of Chicago Police Judo Club and a Black belt in Kodokan Judo, since 1988
Presenter Bio:
William F. Slater, III

- **Current Position** – Project Manager / Sr. IT Consultant at Slater Technologies, Inc. Working on projects related to
  - Security reviews and auditing
  - ISO 27001 Project Implementations
  - Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor’s State University in UT
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.