Bitcoin: A Current Look at the World's Most Popular, Enigmatic and Controversial Digital Cryptocurrency

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

ILLINOIS INSTITUTE OF TECHNOLOGY

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

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY

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

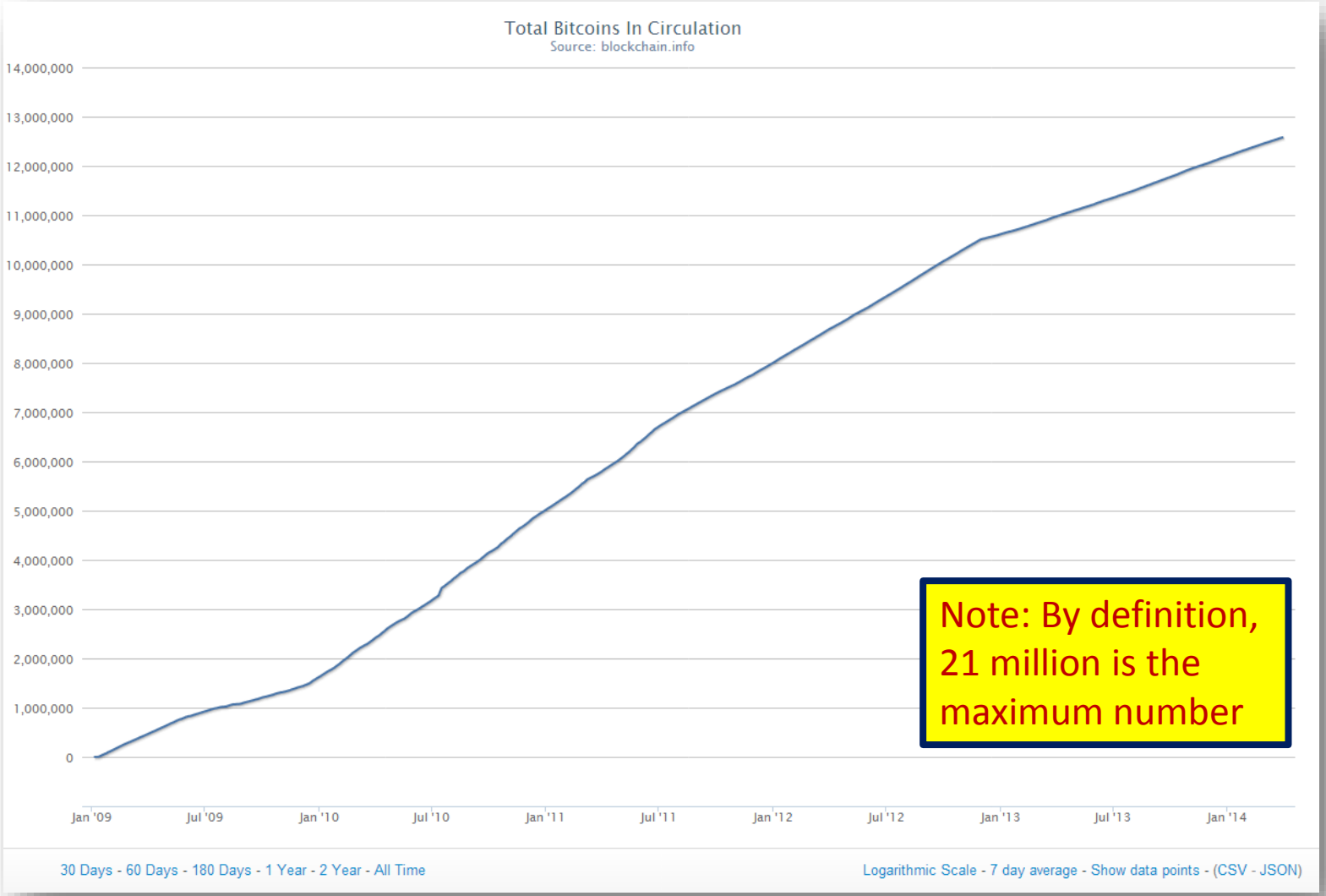
ILLINOIS INSTITUTE OF TECHNOLOGY

Bicoin Characteristics

- **Supported by the Bitcoin Foundation**
- **Bitcoin (BTC)**
- http://bitcoin.org/ or http://www.bitcoin.com
- 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

ILLINOIS INSTITUTE OF TECHNOLOGY

Total Bitcoins in Circulation



Note: By definition, 21 million is the maximum number

Source: https://blockchain.info/charts/total-bitcoins

ILLINOIS INSTITUTE OF TECHNOLOGY

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"

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJLJybLCWrfDpN.

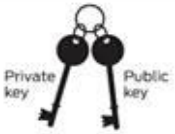
CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When 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 by 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.

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.

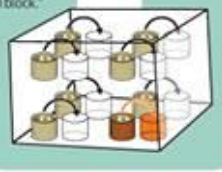
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

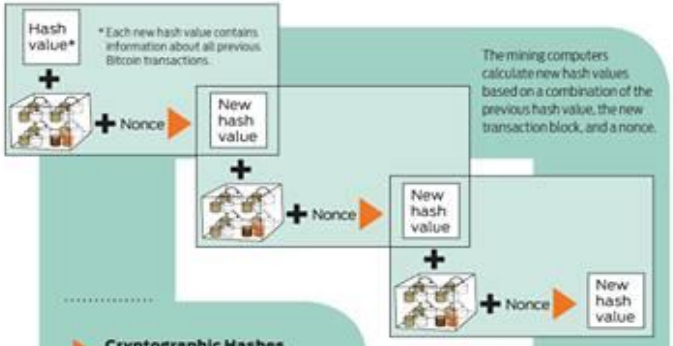
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all evil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

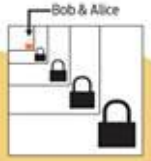
The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

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

Term	Explanation
AES SHA-256	The 256-bit encryption algorithm that is AES standard used for Bitcoin keys.
Bitcoin Network	The Internet-connected network comprised of the software and data that supports Bitcoin transactioms
Block Chain	The Bitcoin ledger of past transactions.
Difficulty	The measure of how difficult it is to find a new block compared to the easiest it can ever be
Exchange	A place that sells can buys Bitcoins, like a stock exchange.
Hash	It is a standard algorithmic function for the generation and verification of currency
Mining	Bitcoin mining serves 2 purposes, it creates the general ledger of Bitcoin transactions and it provides security.
Private Key	The secret cryptopgraphic key that is used to protect your Bitcoin account
Proof of Work	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.
Public Key	The public (shared) cryptopgraphic key that is used to protect your Bitcoin account
Transaction	Use of the Bitcoin to purchase good or services, or the purchase of sale of a Bitcoin, or fractional part of Bitcoin
Wallet	A service that will safely store your Bitcoin account for you.

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY

Brief Bitcoin History

- **2008** - White Paper - Bitcoin: A Peer-to-Peer Electronic Currency System by Satoshi Nakamoto
- **2008** - Bitcoin software goes Open Source
- **January 3, 2009** - Bitcoin Network is Launch 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 25, 2014 –** The IRS declares issues Virtual Currency Guidance stating that Bitcoin and other virtual currencies are "property" and retroactively now subject to taxes http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance and http://www.irs.gov/pub/irs-drop/n-14-21.pdf
- **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

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Value History in USD

12-months
April 2013 – March 2014

ILLINOIS INSTITUTE OF TECHNOLOGY

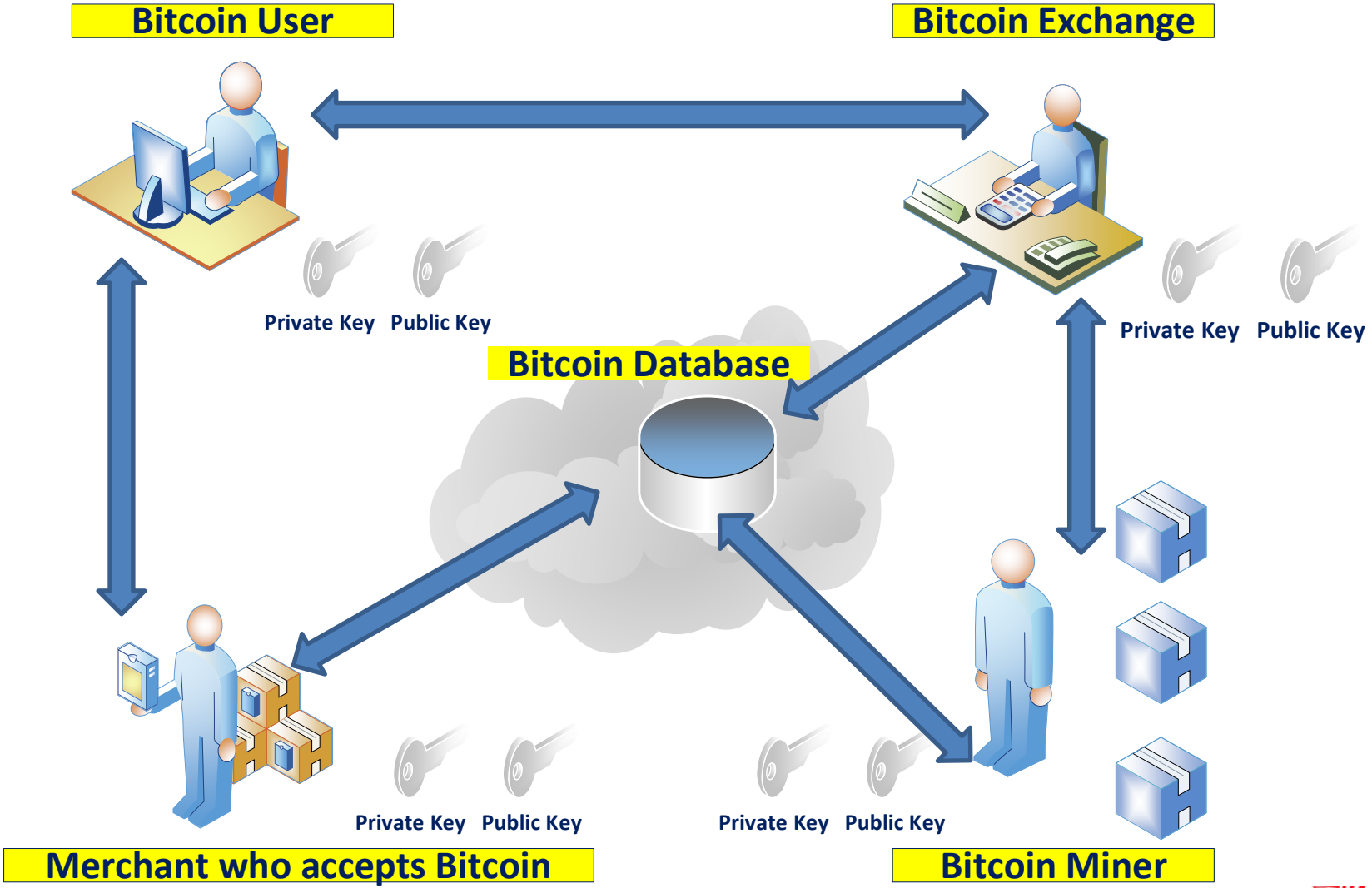
How Does the Bitcoin Network Operate?

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

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Actors



ILLINOIS INSTITUTE OF TECHNOLOGY

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.**

ILLINOIS INSTITUTE OF TECHNOLOGY

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

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY

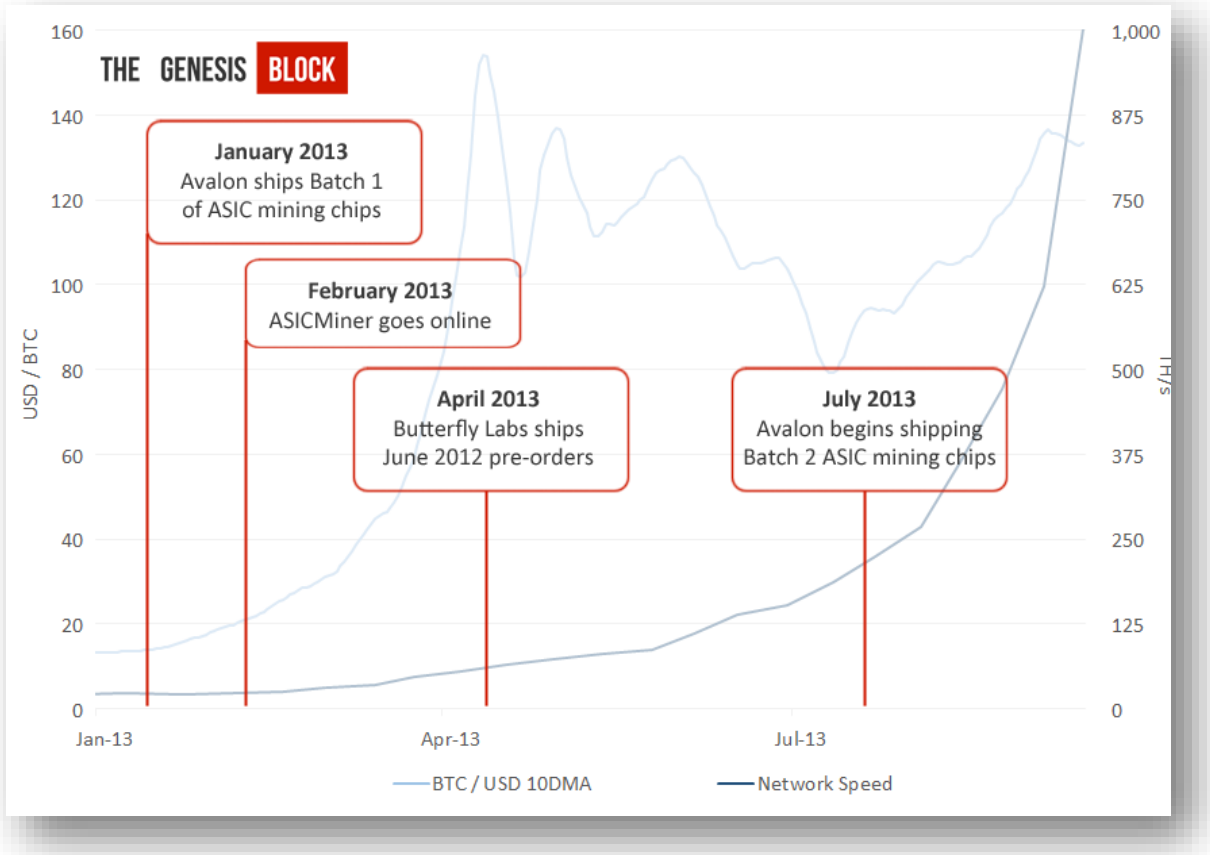
Bitcoin Mining

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.

Source: http://tradeblock.com/research/bitcoin-network-reaches-1-petahash-per-second/

ILLINOIS INSTITUTE OF TECHNOLOGY

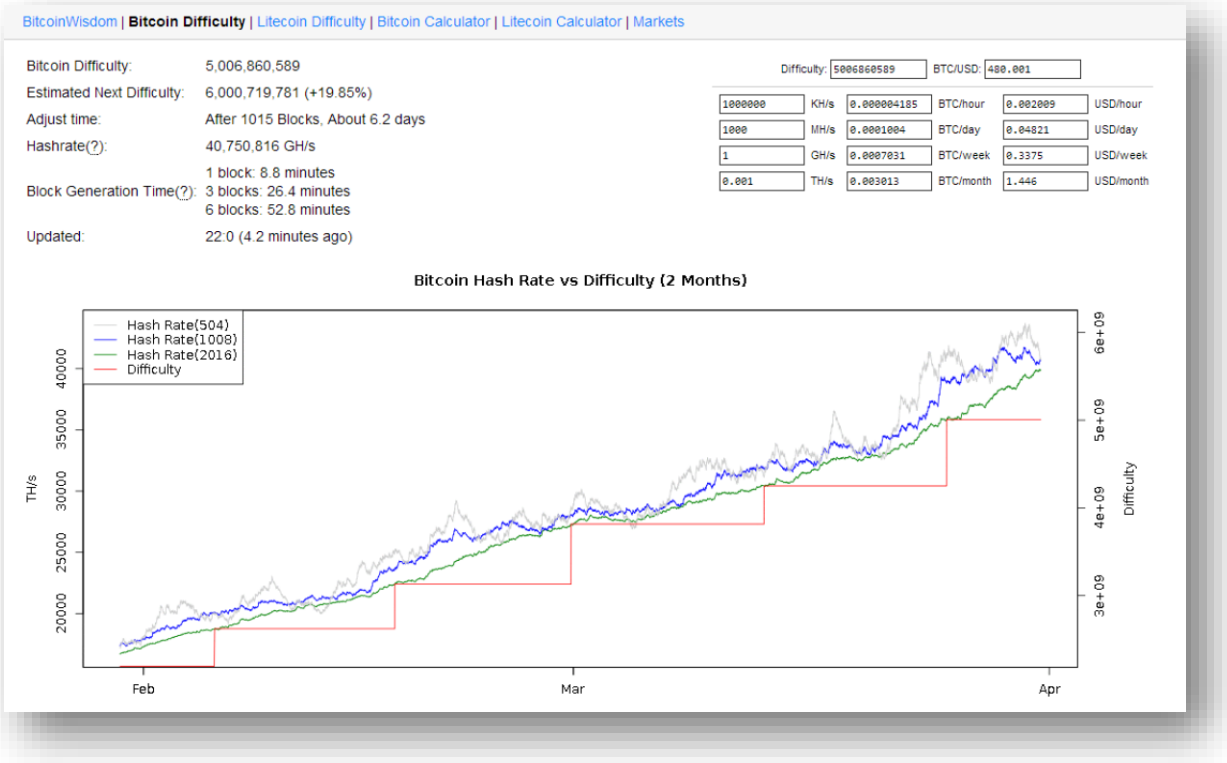
The Increase in Bitcoin Mining and Bitcoin Network Capability Positively Affects Bitcoin's Value



Source: http://tradeblock.com/research/bitcoin-network-reaches-1-petahash-per-second/

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Mining: Block Generation Time vs. Difficulty



Source: https://bitcoinwisdom.com/bitcoin/difficulty

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Mining: Block Generation Time vs. Difficulty

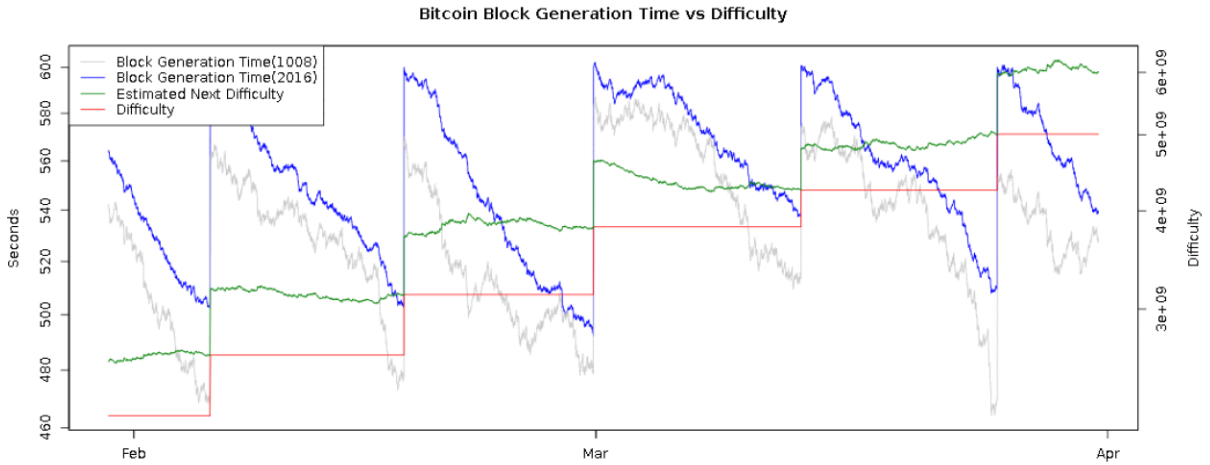


Chart Explained

Red line
The difficulty.

Green line
The estimated next difficulty.

Blue line
Average block generation time of **2016** blocks. Block generation time is also known as **confirmation time**.

Grey line
Average block generation time of **1008** blocks.

If grey line less than blue line, The generation time is **decreasing**.

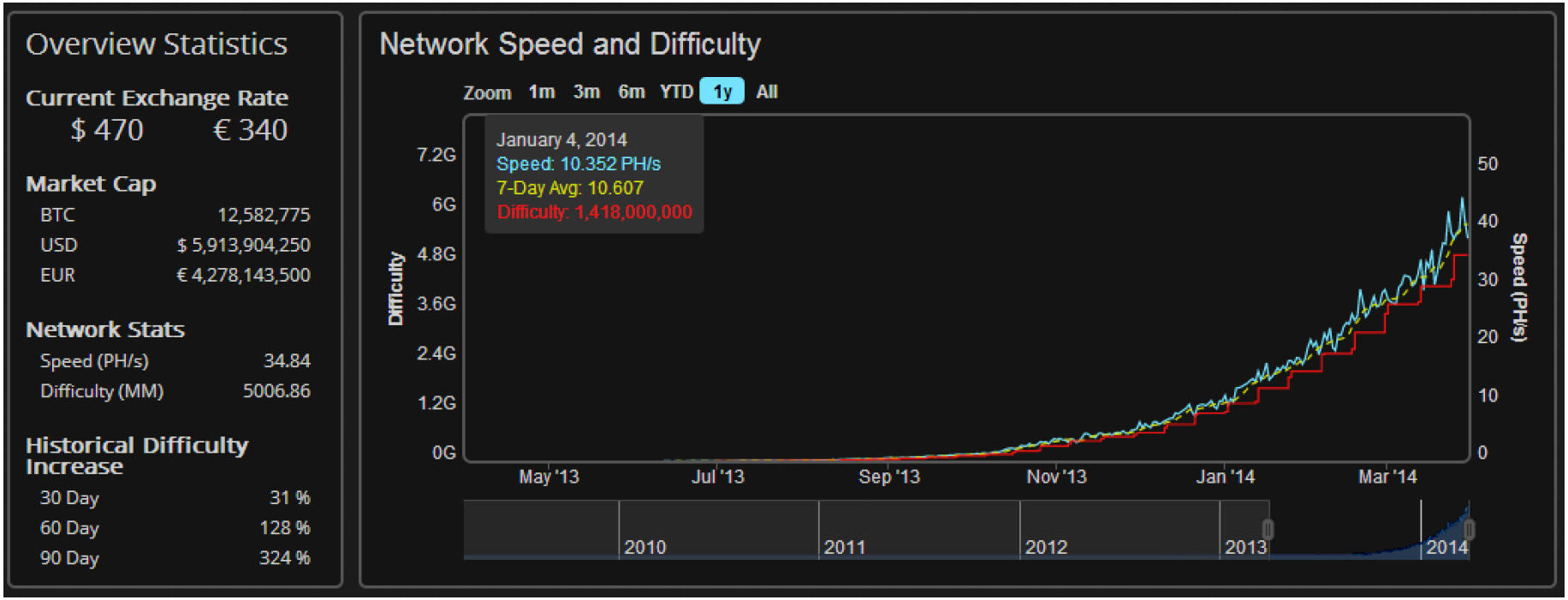
The more grey line is lower than blue line, the faster generation time is decreasing.

After **2016** blocks generated, Bitcoin will adjust difficulty to estimated difficulty in order to keep the block generation time at **600** seconds.

Source: https://bitcoinwisdom.com/bitcoin/difficulty

ILLINOIS INSTITUTE OF TECHNOLOGY

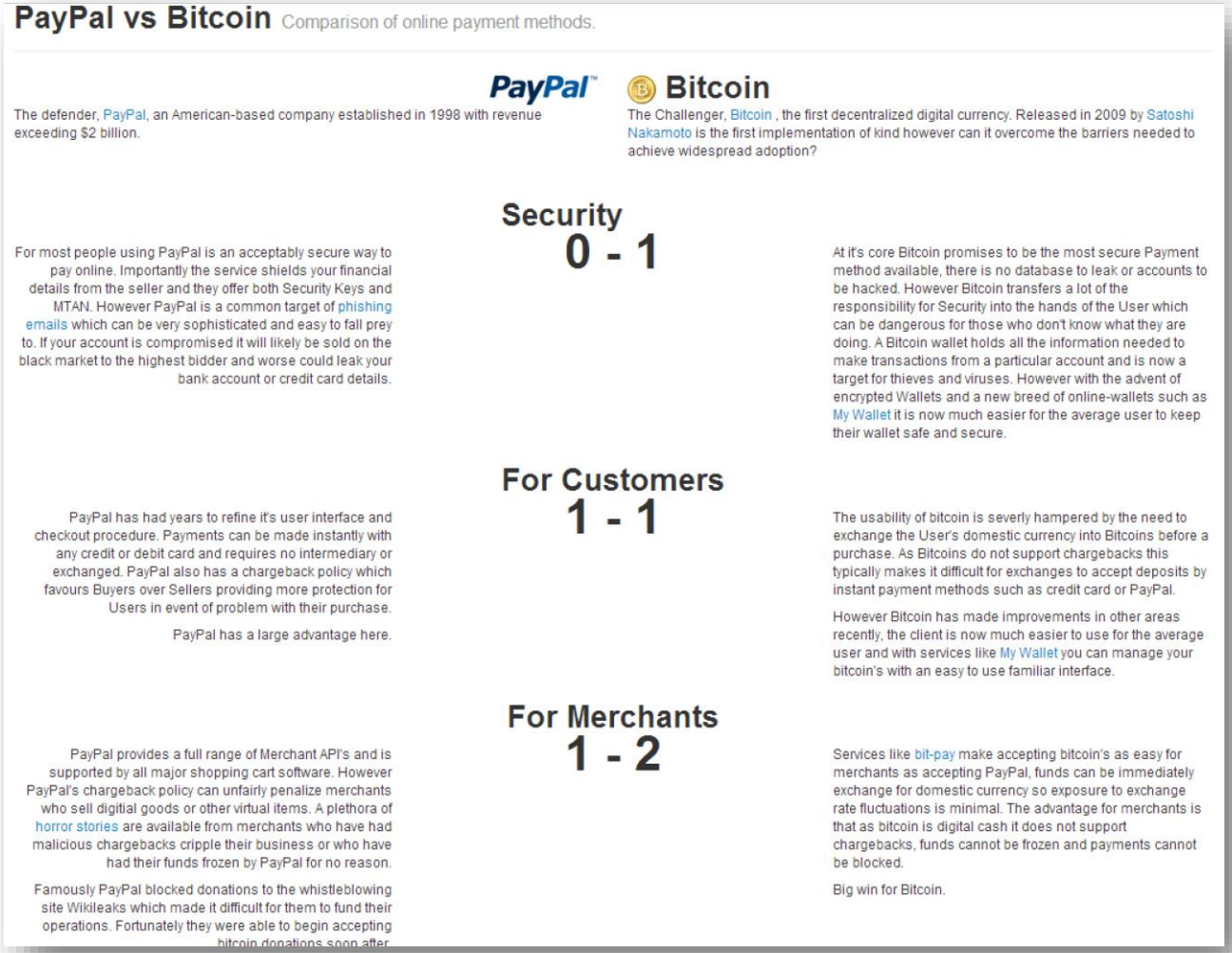
Bitcoin Mining: Block Generation Time vs. Difficulty



Source: https://tradeblock.com/mining/

ILLINOIS INSTITUTE OF TECHNOLOGY

Comparing Bitcoin to Paypal



PayPal vs Bitcoin

Comparison of online payment methods.

	PayPal	Bitcoin
	The defender, PayPal, an American-based company established in 1998 with revenue exceeding $2 billion.	The Challenger, Bitcoin , the first decentralized digital currency. Released in 2009 by Satoshi Nakamoto is the first implementation of kind however can it overcome the barriers needed to achieve widespread adoption?
Security **0 - 1**	For most people using PayPal is an acceptably secure way to pay online. Importantly the service shields your financial details from the seller and they offer both Security Keys and MTAN. However PayPal is a common target of phishing emails which can be very sophisticated and easy to fall prey to. If your account is compromised it will likely be sold on the black market to the highest bidder and worse could leak your bank account or credit card details.	At it's core Bitcoin promises to be the most secure Payment method available, there is no database to leak or accounts to be hacked. However Bitcoin transfers a lot of the responsibility for Security into the hands of the User which can be dangerous for those who don't know what they are doing. A Bitcoin wallet holds all the information needed to make transactions from a particular account and is now a target for thieves and viruses. However with the advent of encrypted Wallets and a new breed of online-wallets such as My Wallet it is now much easier for the average user to keep their wallet safe and secure.
For Customers **1 - 1**	PayPal has had years to refine it's user interface and checkout procedure. Payments can be made instantly with any credit or debit card and requires no intermediary or exchanged. PayPal also has a chargeback policy which favours Buyers over Sellers providing more protection for Users in event of problem with their purchase. PayPal has a large advantage here.	The usability of bitcoin is severly hampered by the need to exchange the User's domestic currency into Bitcoins before a purchase. As Bitcoins do not support chargebacks this typically makes it difficult for exchanges to accept deposits by instant payment methods such as credit card or PayPal. However Bitcoin has made improvements in other areas recently, the client is now much easier to use for the average user and with services like My Wallet you can manage your bitcoin's with an easy to use familiar interface.
For Merchants **1 - 2**	PayPal provides a full range of Merchant API's and is supported by all major shopping cart software. However PayPal's chargeback policy can unfairly penalize merchants who sell digitial goods or other virtual items. A plethora of horror stories are available from merchants who have had malicious chargebacks cripple their business or who have had their funds frozen by PayPal for no reason. Famously PayPal blocked donations to the whistleblowing site Wikileaks which made it difficult for them to fund their operations. Fortunately they were able to begin accepting bitcoin donations soon after.	Services like bit-pay make accepting bitcoin's as easy for merchants as accepting PayPal, funds can be immediately exchange 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.

Source: https://blockchain.info/wallet/paypal-vs-bitcoin

ILLINOIS INSTITUTE OF TECHNOLOGY

Comparing Bitcoin to Paypal

For Merchants
1 - 2

PayPal provides a full range of Merchant API's and is supported by all major shopping cart software. However PayPal's chargeback policy can unfairly penalize merchants who sell digitial goods or other virtual items. A plethora of horror stories are available from merchants who have had malicious chargebacks cripple their business or who have had their funds frozen by PayPal for no reason.

Famously PayPal blocked donations to the whistleblowing site Wikileaks which made it difficult for them to fund their operations. Fortunately they were able to begin accepting bitcoin donations soon after.

Services like bit-pay make accepting bitcoin's as easy for merchants as accepting PayPal, funds can be immediately exchange 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

PayPal accounts are tied directly to your bank account or credit card and PayPal is a regulated financial institution in many countries. PayPal payments are not in any way anonymous and it is not recommended you make purchase using PayPal that you would not be confortable with the authorities knowing about.

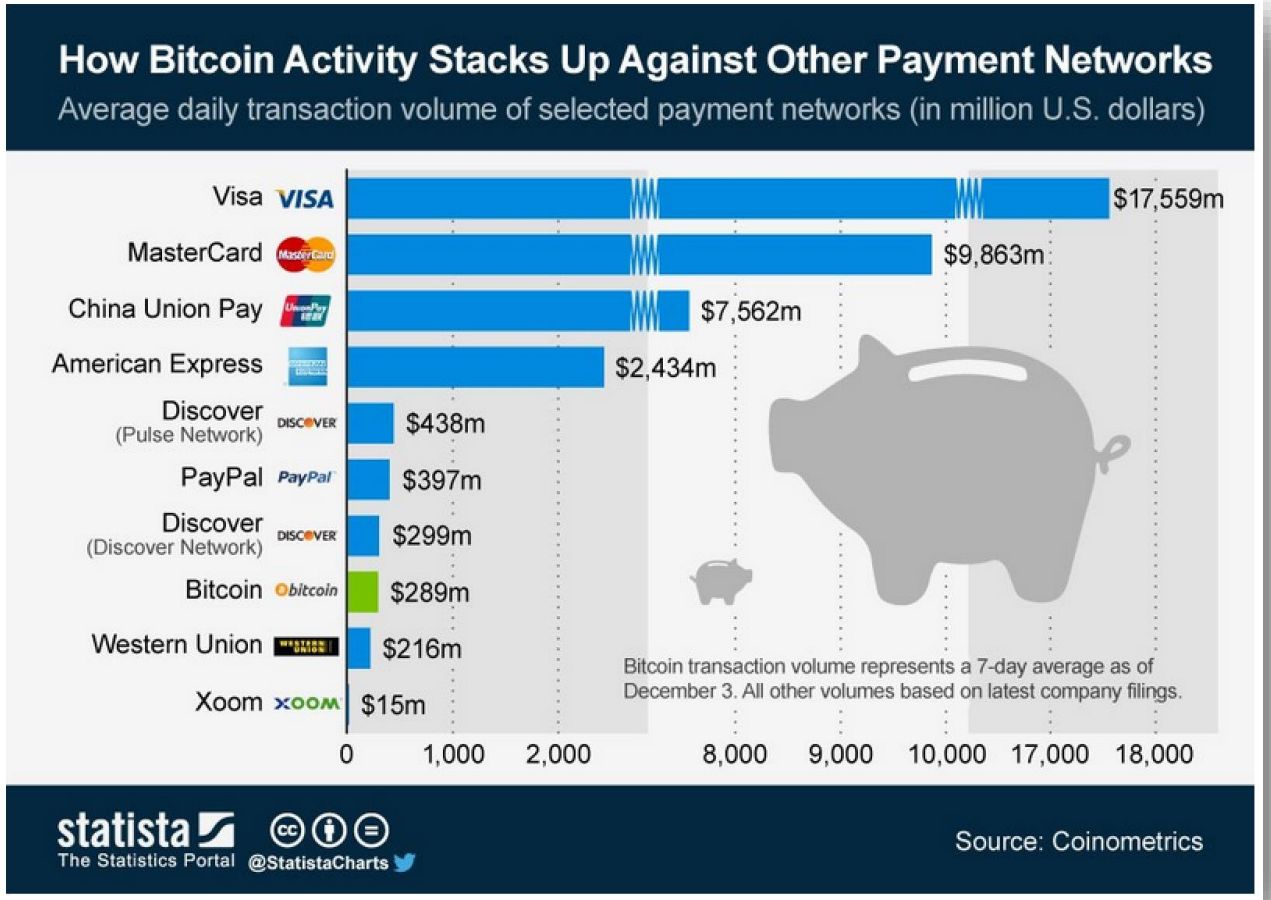
A history of every bitcoin transaction ever made is available right here on this site. However transactions do not need to be tied to a bank account or individual and they are essentally anonymous if some basic precautions are taken. My Wallet can hold up to 1000 unique bitcoin addresses and it is recommended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

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

Source: https://blockchain.info/wallet/paypal-vs-bitcoin

ILLINOIS INSTITUTE OF TECHNOLOGY

Comparing Bitcoin to Paypal



Source: http://www.businessinsider.com/bitcoin-versus-paypal-comparison-2013-12

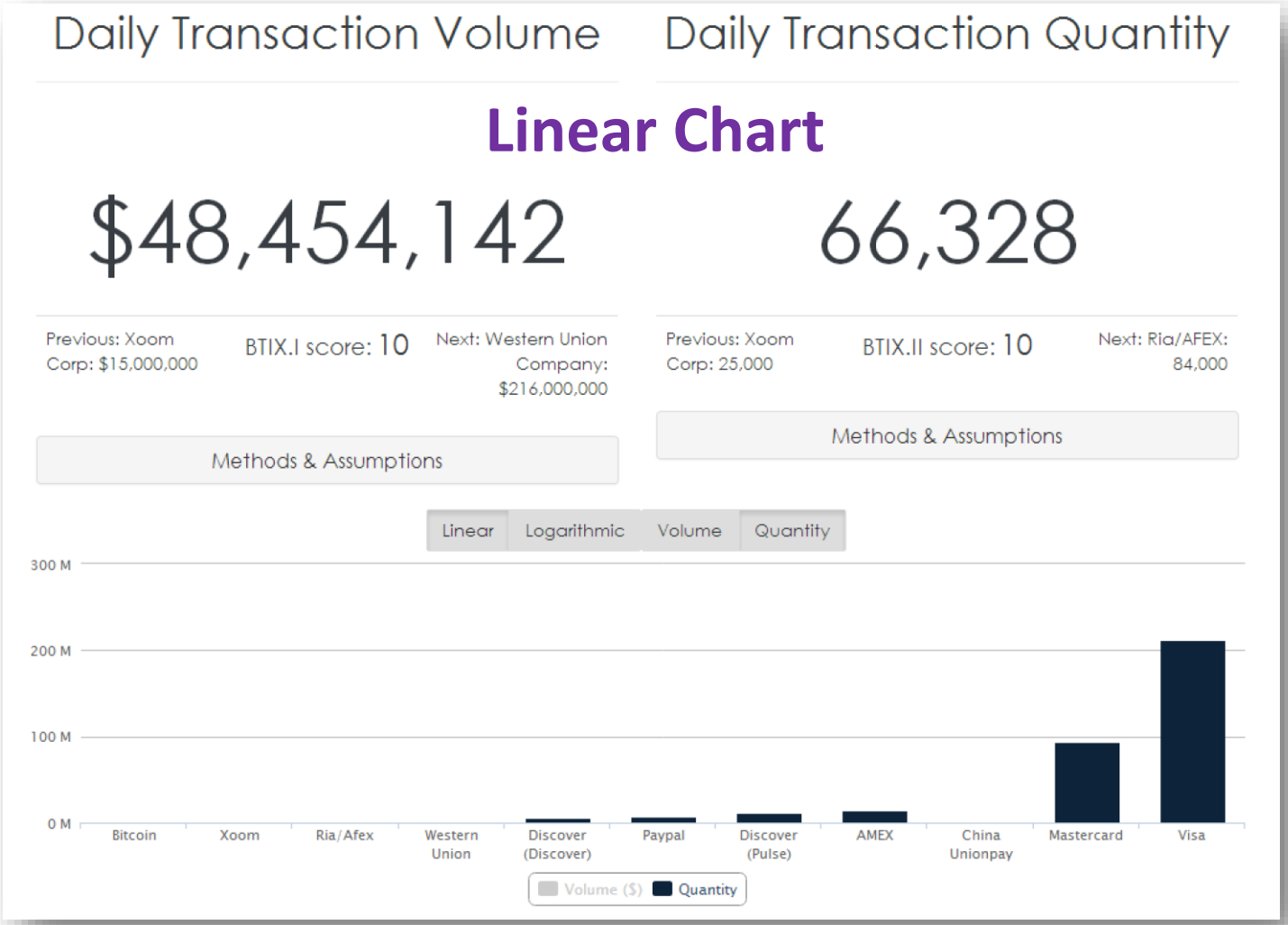
ILLINOIS INSTITUTE OF TECHNOLOGY

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

ILLINOIS INSTITUTE OF TECHNOLOGY

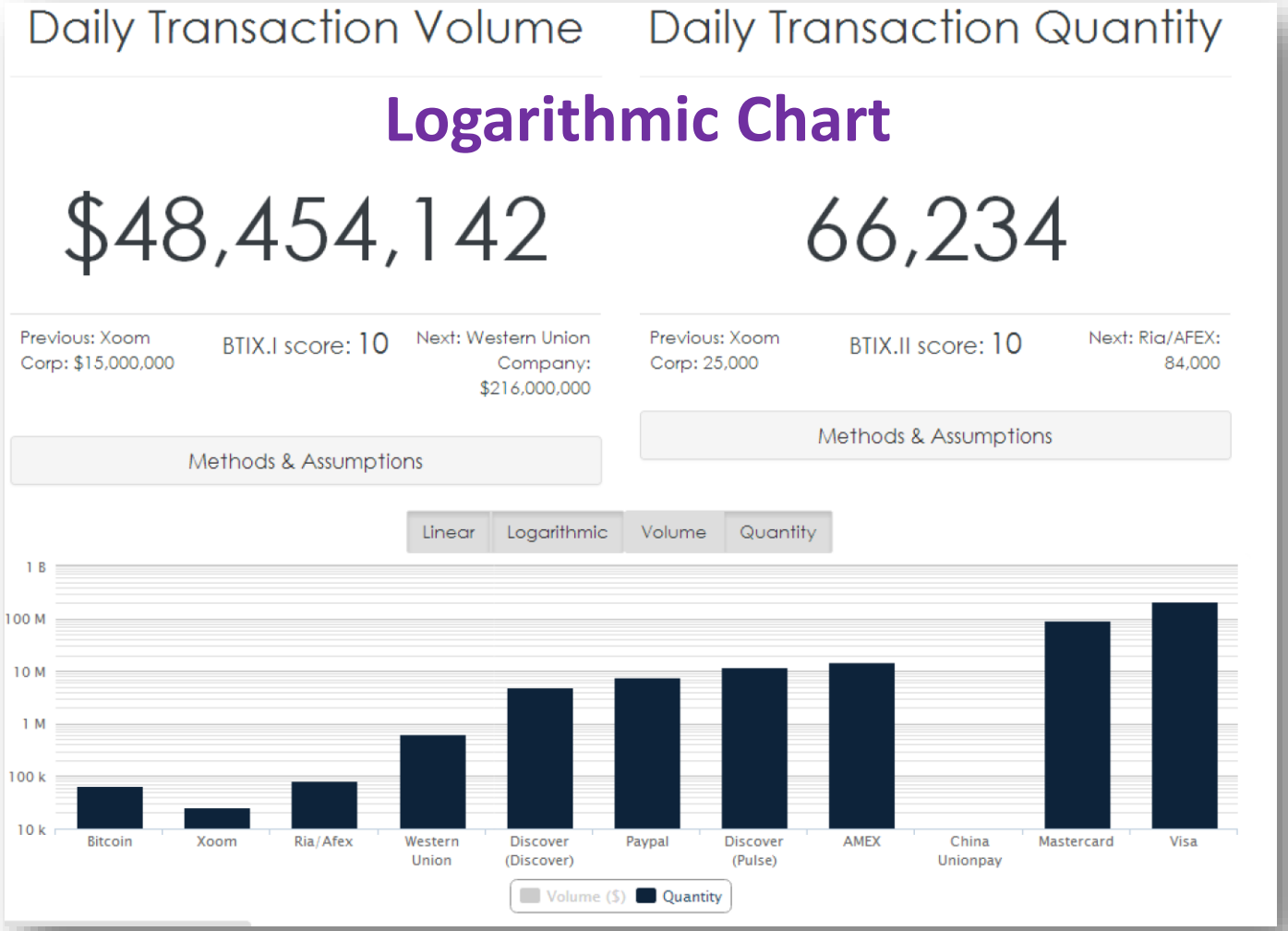
Bitcoin in Daily Transactions



Source: http://www.coinometrics.com/bitcoin/btix

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin in Daily Transactions



Source: http://www.coinometrics.com/bitcoin/btix

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin in Daily Transactions

Daily Transaction Volume | Daily Transaction Quantity

Volume and Quantity (Log scale) Chart

$48,454,142

Previous: Xoom Corp: $15,000,000

BTIX.I score: 10

Next: Western Union Company: $216,000,000

Methods & Assumptions

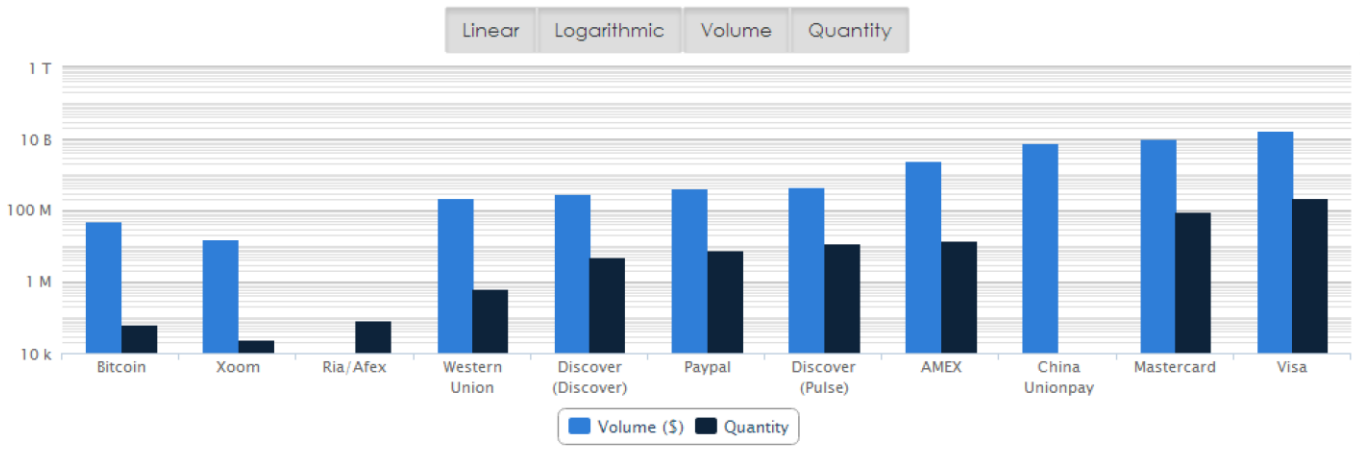
66,041

Previous: Xoom Corp: 25,000

BTIX.II score: 10

Next: Ria/AFEX: 84,000

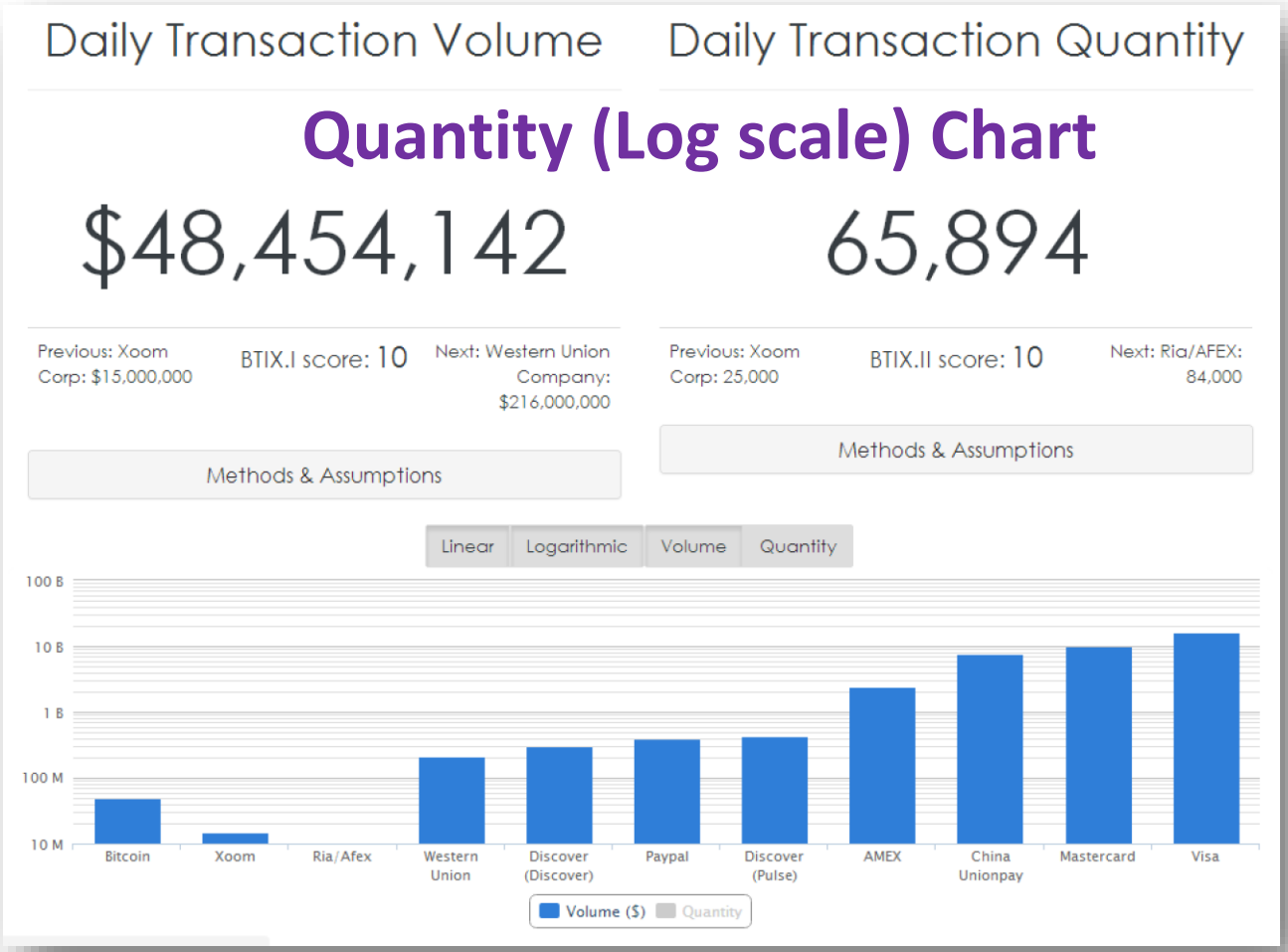
Methods & Assumptions



Source: http://www.coinometrics.com/bitcoin/btix

ILLINOIS INSTITUTE OF TECHNOLOGY

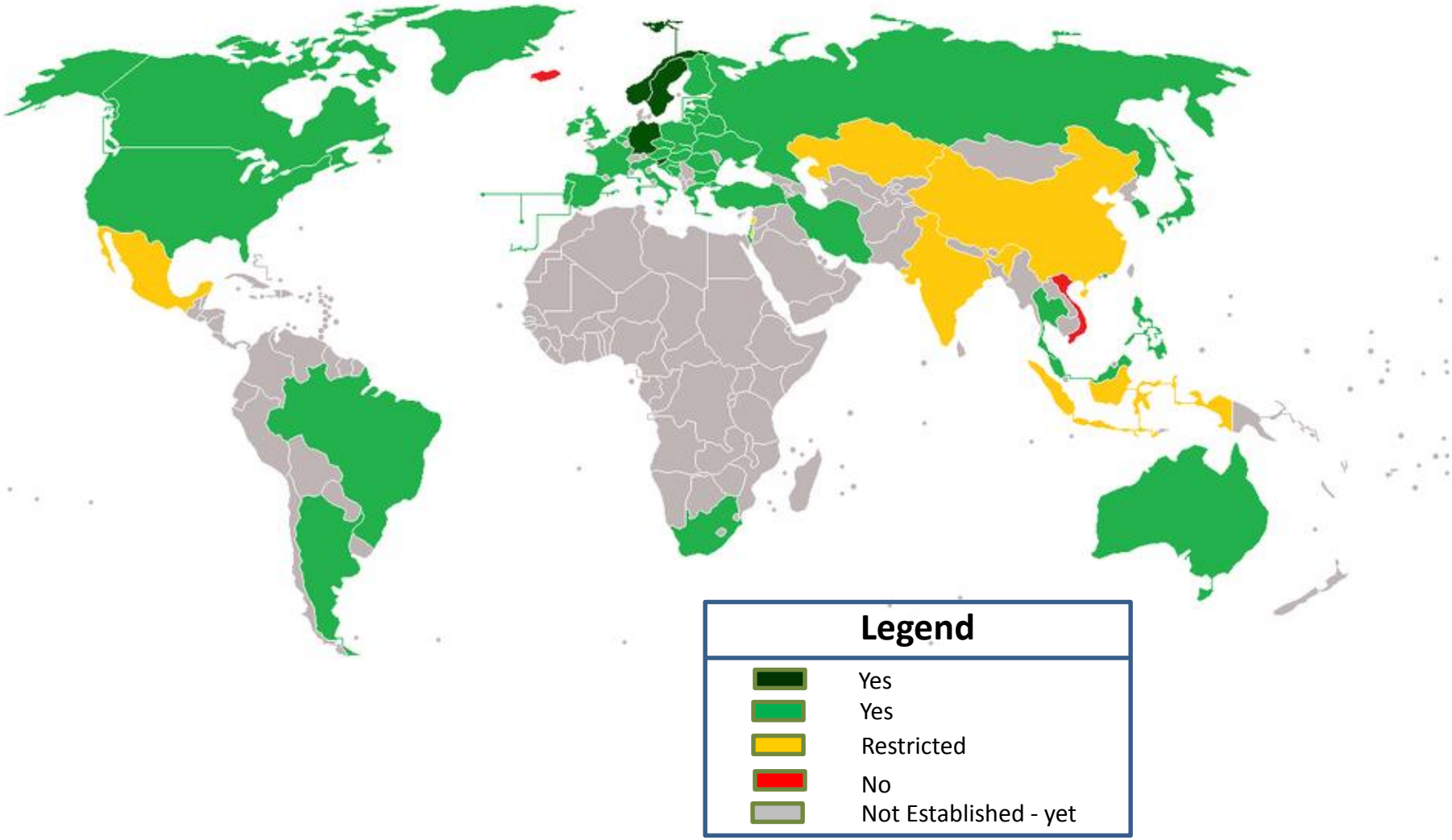
Bitcoin in Daily Transactions



Source: http://www.coinometrics.com/bitcoin/btix

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Legality by Country



Source: http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country

ILLINOIS INSTITUTE OF TECHNOLOGY

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 cyrptoanalysis software and compute capabilities to defeat Bitcoins cryptographic scheme

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Hype vs. Reality

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

ILLINOIS INSTITUTE OF TECHNOLOGY

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

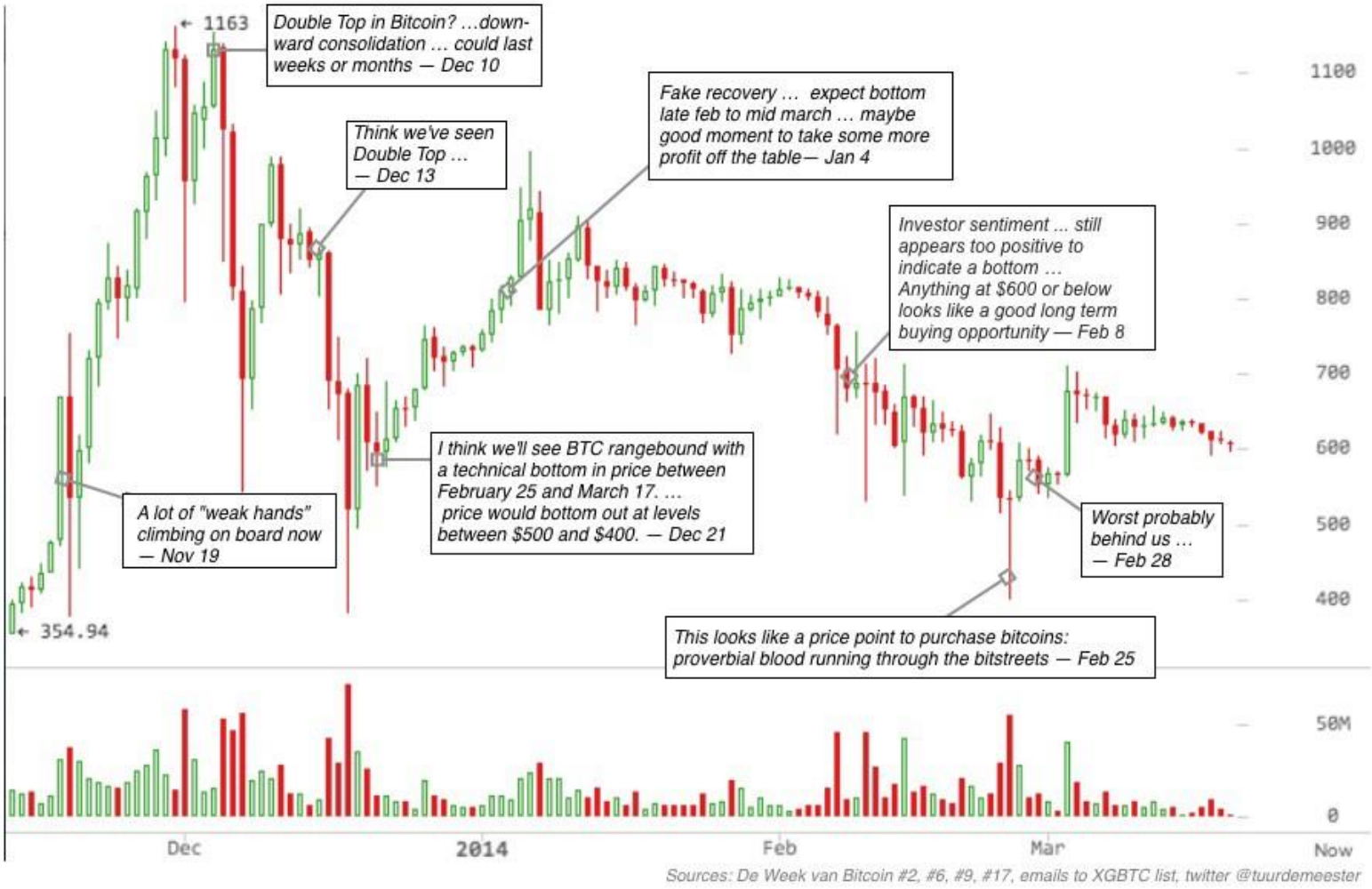
ILLINOIS INSTITUTE OF TECHNOLOGY

Latest Bitcoin News

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 http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance and http://www.irs.gov/pub/irs-drop/n-14-21.pdf

ILLINOIS INSTITUTE OF TECHNOLOGY

Latest Bitcoin News



Source: http://www.coindesk.com/whither-price-bitcoin/

ILLINOIS INSTITUTE OF TECHNOLOGY

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

Hyperinflation in Germany in 1923

ILLINOIS INSTITUTE OF TECHNOLOGY

Other Cryptocurrencies

- Major
  - Blackcoin (uses Proof-of-Stake)
  - Namecoin
  - Litecoin
  - Dogecoin
  - PPCoin
  - Mastercoin
- Others
  - See list at right

1 Currencies
- 1.1 Major
  - 1.1.1 Bitcoin (BTC)
  - 1.1.2 Namecoin (NMC)
  - 1.1.3 Litecoin (LTC)
  - 1.1.4 Dogecoin (Doge)
  - 1.1.5 PPCoin (PPC)
  - 1.1.6 Mastercoin (MSC)
- 1.2 New
  - 1.2.1 Hashcoin (HSC)
  - 1.2.2 Coino (CON)
  - 1.2.3 RonPaulCoin (RPC)
  - 1.2.4 Betacoin (BET)
  - 1.2.5 Nxt (NXT)
  - 1.2.6 Globe (GLB)
- 1.3 Minor
  - 1.3.1 Megacoin (MEC)
  - 1.3.2 AnonCoin (ANC)
  - 1.3.3 Franko (FRK)
  - 1.3.4 FeatherCoin (FTC)
  - 1.3.5 CraftCoin (CRC)
  - 1.3.6 Tonal Bitcoin (TBC)
  - 1.3.7 IxCoin (IXC)
  - 1.3.8 Devcoin (DEV)
  - 1.3.9 Freicoin (FRC)
  - 1.3.10 I0coin (I0C)
  - 1.3.11 Terracoin (TRC)
  - 1.3.12 Liquidcoin (LQC)
  - 1.3.13 BBQCoin (BQC)
  - 1.3.14 BitBar (BTB)
  - 1.3.15 Netcoin (NET)
  - 1.3.16 GoldCoin (GLD)
- 1.4 Dead / dying
  - 1.4.1 Qubic
  - 1.4.2 TimeKoin
  - 1.4.3 SC Solidcoin
  - 1.4.4 GG Geist Geld
  - 1.4.5 TBX Tenebrix
  - 1.4.6 FBX Fairbrix
  - 1.4.7 CLC Coiledcoin
  - 1.4.8 RUC Rucoin
  - 1.4.9 MMM MMMcoin
  - 1.4.10 Weeds
  - 1.4.11 Beertoken

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Associated Press. (2014). Mt. Gox finds 200,000 missing bitcoins. Retrieved from http://money.msn.com/business-news/article.aspx?feed=AP&date=20140321&id=17454291 on March 21, 2014.
- BBC. (2014). Troubled MtGox Bitcoin boss emerges after shut down Retrieved from http://www.bbc.com/news/technology-26352442 on February 26, 2014.
- Bitcoin Charts. (2014). Bitcoin Charts. Retrieved from http://bitcoincharts.com/ on March 1, 2014.
- Bitcoin. (2014). Bitcoin. Retrieved from https://bitcoin.com/ on April 10, 2014.
- Bitcoin.org. (2014). Bitcoin.org FAQs.. Retrieved from https://bitcoin.org/en/faq on April 10, 2014.
- Bitcoin Foundation. (2014). Bitcoin Foundation. Retrieved from https://bitcoinfoundation.org/ on April 10, 2014.
- Bitcoin Scammers. (2014). Bit Coin Scammers. Retrieved from http://bitcoinscammers.com/ on April 9, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Brown, E. Bitcoin bubble could burst as investors rush to withdraw cash. Retrieved from http://www.zdnet.com/bitcoin-bubble-could-burst-as-investors-rush-to-withdraw-cash-7000026410/ on February 17, 2014.
- Caughey, M. (2013). Bitcoin Step by Step, second edition. Amazon Digital Services.
- Caughey, M. (2013). Bitcoin Mining Step by Step. Amazon Digital Services.
- Chen, C. (2014). PBOC Orders All Chinese Banks And Third Party Payment Processors To Close Accounts Of Chinese Bitcoin Exchanges by 4/15. Retrieved from http://www.cryptocoinsnews.com/2014/03/27/pboc-orders-all-chinese-banks-third-party-payment-processors-shut-accounts-15-chinese-bitcoin-exchanges-april-15th/ on March 27, 2014.
- Demeester, T. (2014). Whither the Price of Bitcoin? Retreived from http://www.coindesk.com/whither-price-bitcoin/ on April 12, 2014.
- Hacking, J. (2014). Calif. man, Satoshi Nakamoto denies to be a Bitcoin founder. Retrieved from http://www.thewestsidestory.net/2014/03/07/calif-man-satoshi-nakmoto-denies-bitcoin-founder/ on March 7, 2014.
- Hornyak, T. (2014). 'Malleability' attacks not to blame for Mt. Gox's missing bitcoins, study says. Retrieved from http://www.pcworld.com/article/2114200/malleability-attacks-not-to-blame-for-mt-goxs-missing-bitcoins-study-says.html on March 27, 2014.
- Incencio, R. (2014). Ransomware and Bitcoin Theft Combine in BitCrypt. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/ on March 27, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Kadhim Shubber, K. 2014. Gavin Andresen Steps Down as Bitcoin's Lead Developer. Retrieved from http://www.coindesk.com/gavin-andresen-steps-bitcoins-lead-developer/ on April 8, 2014.
- Lee, T. B. (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/ on November 19, 2013.
- Markowitz, E. (2014). Cryptocurrencies Are the New Spam Frontier. Retrieved from http://www.vocativ.com/tech/bitcoin/cryptocurrencies-new-spam-frontier/ on March 28, 2014.
- NameCheap. (2014. NameCheap accepts Bitcoin for Domain Name Registration. Retrieved from https://www.namecheap.com/domains/registration.aspx?utm_source=facebook&utm_medium=ppc&utm_content=Namecheap%2Baccepts%2Bbitcoin%2Bpayments&utm_campaign=Bitcoin%2Bcampaign on March 25, 2014.
- Nakamoto. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on November 1, 2013.
- Petrovan, B. (2014) Researchers find Android apps that covertly mine Dogecoin, one of them with more than a million downloads. Retrieved from http://www.androidauthority.com/dogecoin-mining-android-apps-362142/ on March 27, 2014.
- Popper, N. (2013). Into the Bitcoin Mines, Retrieved from http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?hp&_r=0 on December 21, 2013.
- Preev. (2014). Current Value of Bitcoin. Retrieved from http://preev.com/ on March 20, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- SCGNEWS. (2014). Bitcoin Flash Crash - 80% Drop in Seconds - Down 20% After Stabilizing. Retrieved from http://scgnews.com/bitcoin-flash-crash-80-drop-in-seconds-down-20-after-stabilizing on February 10, 2014.
- SCGNEWS. (2014). The IRS Just Declared War on Bitcoin - Retroactively. Retrieved from http://scgnews.com/the-irs-just-declared-war-on-bitcoin-retroactively on March 27, 2014.
- Sharkey, T. (2014. Inside Bitcoins NYC Day 1: Bitcoin 2.0 Takes Center Stage.
- Retrieved from http://www.coindesk.com/inside-bitcoins-nyc-day-1-bitcoin-2-0-takes-center-stage/ on April 8, 2014.
- Wall Street Daily. (2014). Beware Bitcoin: An Insideous Ne Currency Scam - Free Investor's Report. Retrieved from http://signups.wallstreetdaily.com/X303Q1A8 on March 7, 2014.
- Wood, R. W. (2013). Sorry Bitcoin, IRS Gets Reports. Retrieved from http://www.forbes.com/sites/robertwood/2013/05/05/sorry-bitcoin-irs-gets-reports/ on March 15, 2014.
- Zetter, K. (2014). Digital Currency Founder: U.S. Indicted Me For Not Giving FBI My Source Code. Retrieved from http://www.wired.com/threatlevel/2014/01/liberty-reserve-source-code/ on January 30, 2014.
- Bitcoin Links: http://bit.ly/1eixu78 (over 38 million)

ILLINOIS INSTITUTE OF TECHNOLOGY

Questions?

ILLINOIS INSTITUTE OF TECHNOLOGY

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

Career Development Opportunities?

Illinois Institute of Technology

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

Information Technology and Management » Master of Cyber Forensics and Security »

Master of Cyber Forensics and Security

There is a critical need in both the government and private sectors for professionals equipped to prevent, counteract and investigate cybercrimes and information security breaches. According to Bloomberg the average cost of security breaches in the U.S. is 7.2 million dollars per incident. Gartner studies show that the average enterprise spends 5.6% of their it budget on information security, making this a nearly one trillion dollar a year industry. The need for educated professionals in this field is clearly spelled out in documents such as the U.S. Committee on National Security Systems Directive No. 500 Information Assurance (IA) Education, Training, and Awareness which mandates information assurance education for the professionals necessary to ensure the development and implementation of a comprehensive approach for the protection of U.S. Government national security systems and the information they store, process, or transmit.

The *Master of Cyber Forensics and Security* degree is designed to equip experienced information technology professionals with the necessary knowledge and tools to fill the need for educated cyber security and forensics practitioners, investigators and managers. Built around a strong core of courses originally developed for IIT's Information Technology and Management degrees, the program also draws on courses from the IIT Chicago-Kent College of Law curriculum to give cyber security and forensics practitioners the necessary thorough grounding in legal issues and compliance. Courses are taught by experts in the field who not only have academic knowledge but years of experience in the information security realm in both industry and government service.

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

ILLINOIS INSTITUTE OF TECHNOLOGY

Bellevue University

Bellevue, NE (land campus and online)

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

M.S. Cybersecurity

- 01 - CIS 608 Information Security Management
- 02 - CYBR 515 - Security Architecture and Design
- 03 - CYBR 510 Physical, Operations, and Personnel Security
- 04 - CIS 537 Introduction to Cyber Ethics
- 05 - CIS 607 Computer Forensics
- 06 - CYBR 520 Human Aspects of Cybersecurity
- 07 - CYBR 610 Risk Management Studies
- 08 - CYBR 525 Ethical Hacking and Response
- 09 - DET 630 Cyber Warfare & Deterrence
- 10 - CYBR 625 Business Continuity Planning and Recovery
- 11 - CYBR 615 Cybersecurity Governance and Compliance
- 12 - CYBR 650 Current Trends in Cybersecurity

http://www.bellevue.edu/degrees/graduate/cybersecurity-ms/

BELLEVUE UNIVERSITY

Presenter Bio: William F. Slater, III

- IT professional since July 1977
- Owner of Slater Technologies, Inc.
- Currently a Senior IT Consultant in IT Security, Information Security, IT Infrastructure Management, Data Center Operations & Development, IT Change Management, Application System Development, Technical Service Development, and Service Management
- An Adjunct Professor at the Illinois Institute of Technology – for six years
- Fiirst 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 & and 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

ILLINOIS INSTITUTE OF TECHNOLOGY

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.

ILLINOIS INSTITUTE OF TECHNOLOGY