Virtual Currencies and their Relevance to Digital Forensics

PRESTON MILLER

Presentation Overview

- Virtual Currency
  - Cryptocurrency
- Bitcoin
  - Basics: Obtaining, Usage, and History
- Digital Forensics Relevance

Virtual Currency

HTTP://WWW.MYBIGAPPLENY.COM/WP-CONTENT/UPLOADS/2014/01/VIRTUAL-CURRENCY-620X320.JPG

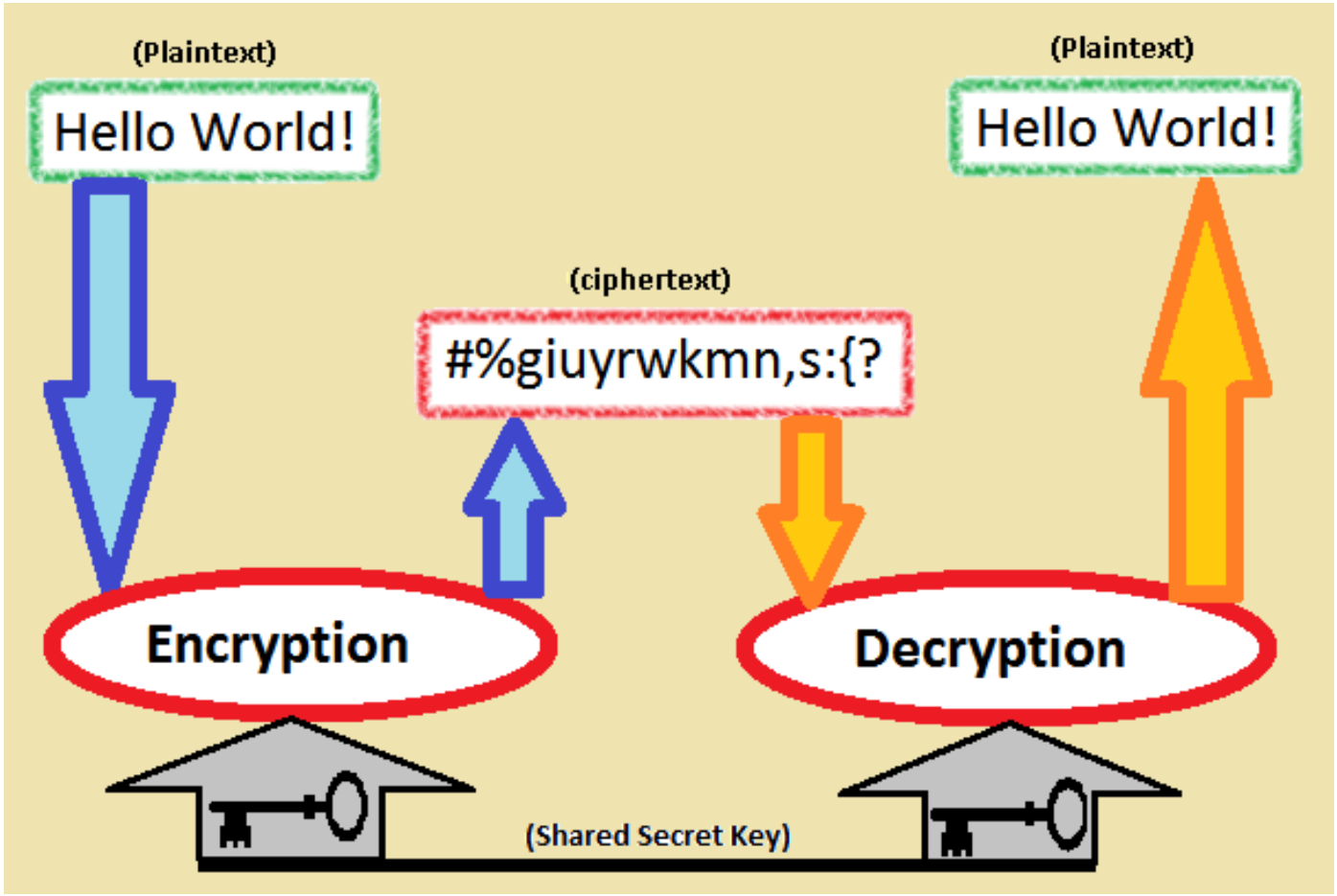
What is Virtual Currency

- In 2013, the US Department of Treasury designated virtual currency as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency”.
- Code of Federal Regulations:
  1. Act as legal tender.
  2. Circulate customarily.

What is Cryptocurrency?

- A virtual currency that employs cryptography as a security mechanism.

Well, What's Cryptography?



HTTP://UPLOAD.WIKIMEDIA.ORG/WIKIPEDIA/COMMONS/F/F8/CRYPTO.PNG

Types of CryptoCurrencies

Bitcoin

Litecoin

Dogecoin

Coinye

Bitcoin

HTTP://WWW.SIKHARCHIVES.COM/WP-CONTENT/UPLOADS/2011/08/VIRTUAL_CURRENCY_2011.08.20.JPG

What is Bitcoin?

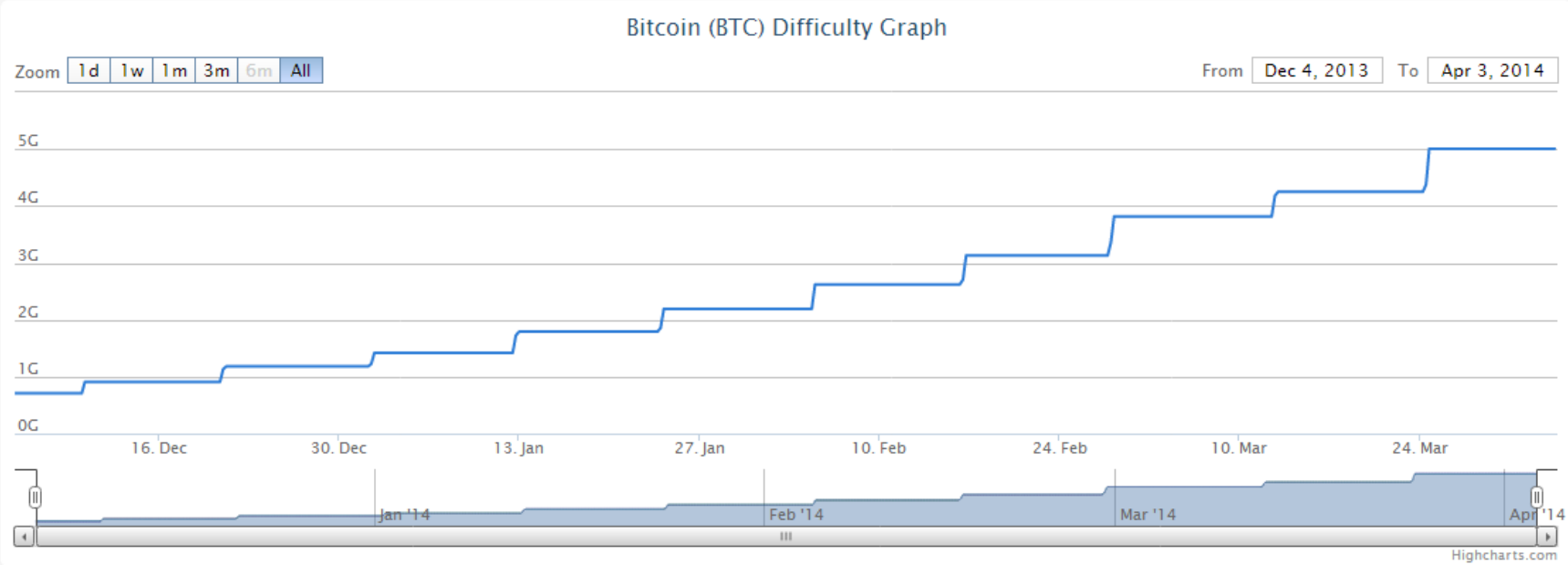
- A decentralized, peer-to-peer cryptocurrency whose creation is attributed to Satoshi Nakamoto. Commonly denoted as BTC.
- Satoshi Nakamoto's true identity is unknown. Is it a single person or a group?
- Bitcoin stimulates scarcity to raise its value in two ways:
  1. There are a finite number of Bitcoins that can be created (21 million).
  2. Bitcoins become progressively harder to "mine" as more enter circulation.

How Do you Get Bitcoins?

- Bitcoins are contained in mathematical equations that must be solved by computers to unlock the coins, this is referred to as “mining”.
- When an equation is solved, a “block” of Bitcoins are released. The number of Bitcoins in that block depends on the amount of coins in circulation. Less coins are released as the total number of Bitcoins in circulation increases. There are currently around 12 million Bitcoins in circulation.
- As more coins are in circulation, the equations become progressively more difficult.

Bitcoin Equation Difficulty

Bitcoin Difficulty Graph and Bitcoin Difficulty Chart History



Now What?

- Bitcoins obtained from mining or purchasing can be stored in an “e-wallet” in one of two ways:
  1. Locally on your computer
  2. Online
- Pick your poison. If your hard drive gets destroyed you will lose all of your coins (unless you have a backup). If the provider of the online wallet gets hacked you could lose all of your coins.
- E-wallets use private and public keys (cryptography) to secure and transfer your coins.

And, Then?

- Continue to buy, sell, or use your Bitcoins to purchase actual real life commodities from vendors that accept Bitcoins.
- Bitcoins are traded by sending from your wallet to the “address” of the recipient’s wallet. Or by scanning a QR code that corresponds to the recipient’s wallet.
- Currently, the user adoption rate for Bitcoins has far outpaced vendor adoption rate.
- Overstock.com currently accepts Bitcoins as a form of payment.

Idea for Bitcoin Conceived
October 2008

Bitcoin Project Started
November 2008

Software for Trading Created
January 2009

"laszlo" Makes First Real-Word Transaction
February 2010

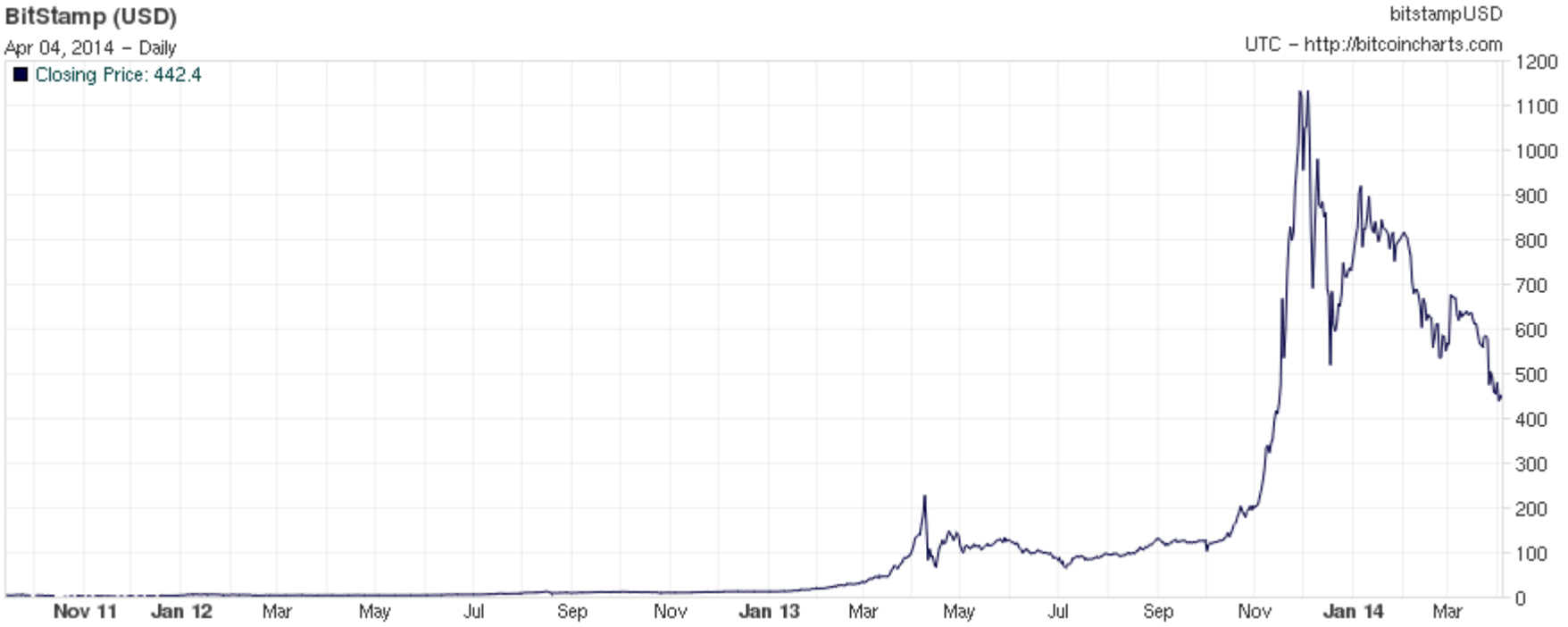
US Senate Hearing on Virtual Currencies
November 2013

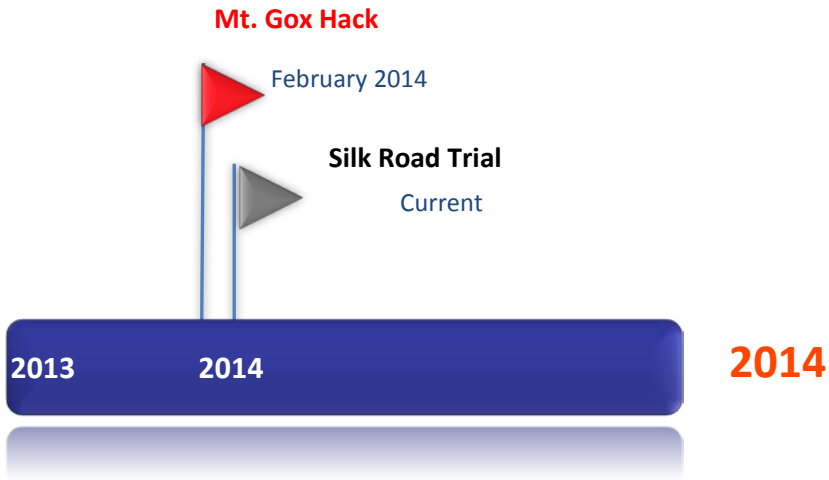
Mt. Gox Hack
February 2014

Silk Road Trial
Current

2008 2009 2010 2011 2012 2013 2014

2014




Mt. Gox Hack
February 2014
Silk Road Trial
Current
2013
2014
2014

Mt. Gox Hack

- In April 2014, The oldest and largest Bitcoin exchange based in Tokyo was hacked and lost 850,000 Bitcoins, valued at 477 million USD.
- Mt. Gox immediately declared bankruptcy. Many believed this event signaled the end of Bitcoin.


Mt. Gox Hack
February 2014
Silk Road Trial
Current
2013
2014
2014

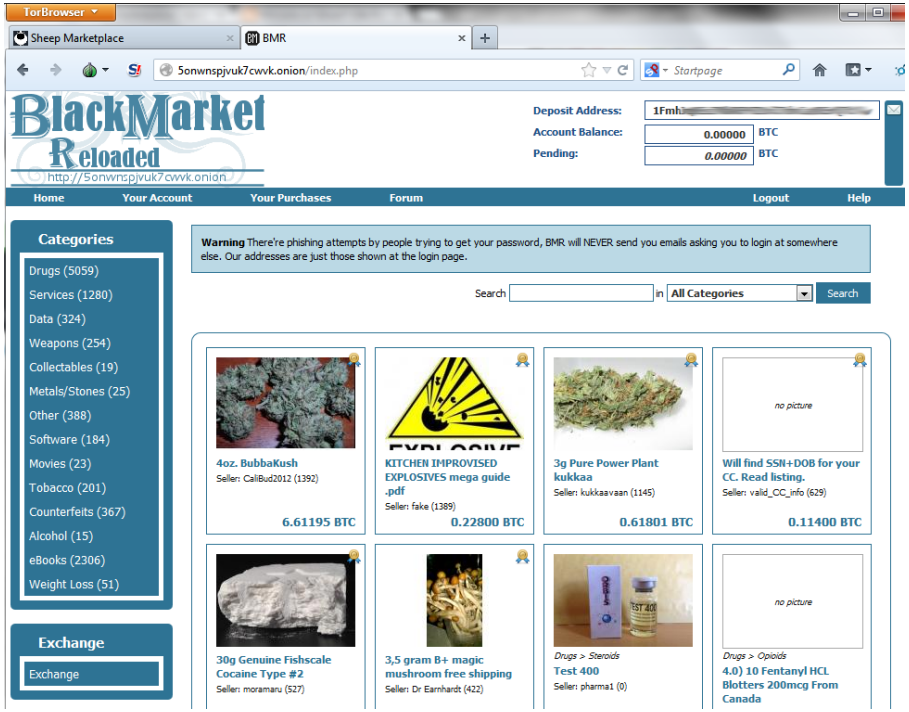
What's Silk Road

- Essentially, the black market Amazon. You can purchase drugs, weapons, child pornography, hire hackers, hire assassins, and more. Purchases are made with Bitcoins.
- Silk Road is normally accessed with a special anonymous browser, known as the Tor browser or the Onion Router.
- Tor, in simplest terms, could be thought of as a web browser (like IE, Chrome, Firefox, etc), but with the added feature of near complete anonymity.

Silk Road Trial

- Ongoing trial against the creator of the Silk Road website, Ross Ulbricht ("The Dread Pirate Roberts"), will determine how Bitcoins are handled going forward.
- Ulbricht is charged with money laundering, conspiracy to traffic narcotics, conspiracy to commit computer hacking, and running a "continuing criminal enterprise".
- IRS recently decided that Bitcoins are property and not currency.
- Ulbricht's lawyer claims charges should be dropped. Why? Because Bitcoins aren't currency.

Digital Forensics Relevance



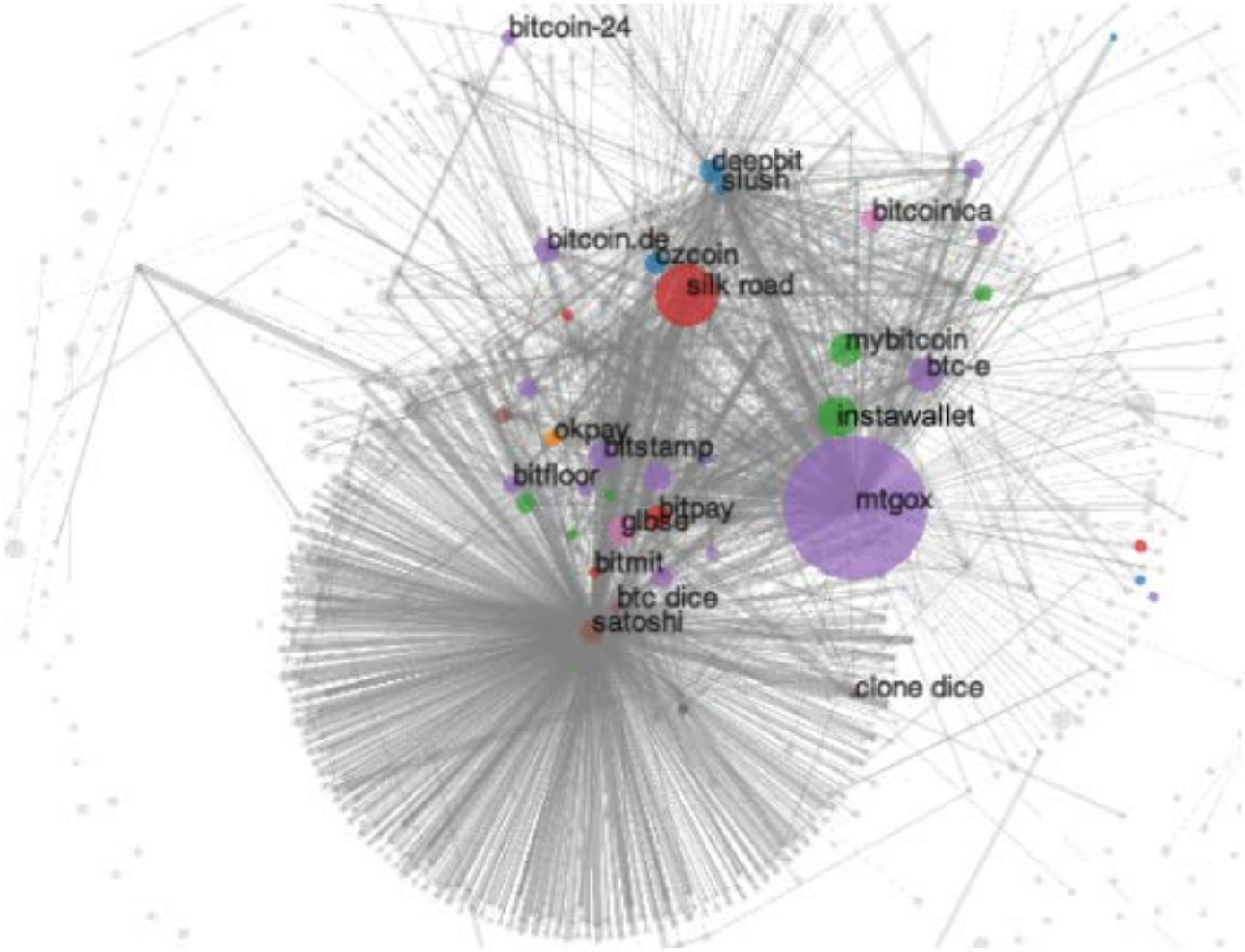
HTTP://WWW.MAGNETFORENSICS.COM/WP-CONTENT/UPLOADS/FILES/BITCOIN/BMR1.PNG

Why are we Interested in Bitcoin?

- Bitcoin is often thought to be an anonymous means of acquiring nefarious goods online.
- Is it anonymous? Yes and no.
- While names are not associated with transactions, metadata (data about data) of transactions are recorded and publically accessible to anyone, including Law Enforcement without the need of a subpoena or probable cause.
- Address of both wallets, amount transferred, and more are recorded for each transaction in this “block chain”.

Not so Anonymous

- Recent studies have demonstrated that about 40% of Bitcoin users are able to be identified through these public transaction logs.
- This is due, in part, to Bitcoin's increased reliance on a few large accounts.


bitcoin-24
deepbit
slush
bitcoinica
bitcoin.de
ozcoin
silk road
mybitcoin
btc-e
instawallet
okpay
bitstamp
bitfloor
mtgox
bitpay
bitmit
btc dice
satoshi
clone dice

References

1. Nicholas A. Plassaras. Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law.* **377(14):** (2014).
2. Paul Hunton. Data attack of the cybercriminal: Investigating the digital currency of cybercrime*. Computer Law & Security Review*. **28(2):** 201-207 (2012).
3. Susan A. Some basic rules for using 'bitcoin. *ABA Journal*. **99(7):** (2013).
4. Danton Bryans. Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal.* **441(89):** (2014).
5. Michael Betancourt. Bitcoin. *Theory Beyond the Codes.* (2013).
6. Gordon Griffin. Virtual Currencies in the Crosshairs*. Criminal Justice*. **62(28):** (2013).
7. Olga Kharif. Virtual Currencies Gain in Popularity. *Businessweek Online.* **5:** (2009).
8. 8. Tim Harford. Bitcoin; A year in a word*. USA*. **1:** (2013).
9. Andy Greenberg. Bitcoin's Price Plummets As Mt. Gox Goes Dark With Massive Hack Rumored. *Forbes Online*. http://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/. (2014).
10. http://en.wikipedia.org/wiki/Bitcoin
11. http://en.wikipedia.org/wiki/Virtual_currency
12. http://en.wikipedia.org/wiki/Cryptocurrency