BitCoins

By

Charles Ogles

ICTN 4040

April 1st, 2014

Abstract

The Bitcoin is one of the most widely known forms of virtual currency. It was designed to keep the market from being inflated by slowly releasing coins into the system. Some companies have begun accepting Bitcoins, even though the currency's actual worth varies based on opinion. The network is used by consumers to farm and maintain currency by breaking down algorithms. Some users have even custom built machines solely for the purpose of mining bitcoins. Unfortunately, some people will try to mislead others and steal currency from their virtual wallets. Hackers will at times hold companies hostage with Denial of Server attacks. Company networks are then returned after they have been leveraged in order to procure Bitcoins as payment. The currency is gone forever once it is lost. This makes it hard to recovery lost or stolen currency, or trace what it is being used for and who is spending it. The FEDs have locked down sites and confiscated millions of dollars' worth of virtual currency used for illegal transactions over the internet.

What is a Bitcoin? It is the first decentralized digital currency devised by a mysterious figure known as Satoshi Nakomoto in 2009. It has been currently gaining popularity in online communities. It's used as an untraceable fund to purchase items online from other people without having to deal with 3rd party companies such as banks or creditors.

Spending Bitcoins has become increasingly easy due to the rising number of online retailers beginning to accept the currency. Furthermore, smart phones make using Bitcoins as easy purchasing via cash transactions. You can actually use current forms of currency to purchase Bitcoins, which in return raises the value of the coins. Having a virtual wallet gives you the ability to print or save your information for safekeeping. Bitcoins use public-key cryptography. This requires a public and private key in order for you to have a wallet in which you are able to make transactions with bitcoins. Cryptography is a mathematical ID that provides protection for the spender, which is useful because it keeps the same bitcoins from being re-spent. If a person were trying to take advantage of the system by spending bitcoins in two different locations at the same time, the servers doing the mining and the block chain would see it. They would report the bitcoins as being used twice, which would nullify the transaction. This eliminates the need for banks and fees that you are currently faced with when dealing with the American dollar. Bitcoins are also untraceable which increases the ability to hide purchases and sales, meaning that taxing these transactions is more difficult.

New bitcoins are produced at a high rate through a process known as mining. There are a total of 21 million Bitcoins to be mined through a mathematical encryption process that a machine can solve; based on that outcome a block is generated. The hash rate is the processing of a Bitcoin’s mathematical operations, and the further along the calculations go the longer they take. You can set your computer up to be a solo miner or you can join a pool of others who are working to break mass amounts of mathematical data. Usually there are 25 bitcoins to a block if you’re lucky enough to find one. This isn’t easy because you are trying to match hashes and checking each individually would be very time consuming. Computers or devices like Raspberry Pi (computer running linux) and usb keys are used to help mine Bitcoins. It is highly unlikely that you will ever earn a Bitcoin by yourself due to the hash rate which causes calculations to take progressively longer to complete. You have the option of joining peer to peer pools This is where other users are putting their computer power together as a collective, in hopes of un-mining more bitcoins. The profits in this scenario are smaller because any blocks with coins are split amongst all participants, which obviously deters some from joining

What makes Bitcoins so attractive to malicious hackers is the fact that the transactions only take place between two users. This means that if they are traded fast they become basically untraceable. So the system doesn't only attracts consumers who don't want to leave a paper trail, but criminals as well; from your common day drug dealer to the obscured hacker. The website Silk Road lost $28 million dollars' worth of Bitcoins, which is roughly 29,655 Bitcoins. The site's virtual wallet was seized by the feds because the Bitcoins were used to facilitate the trade of drugs and to bankroll other illegal activities. The personal computer of Ross Ulbricht, the alleged mastermind of silk road, had 144,336 Bitcoins on it when it was seized. He was charged with computer hacking, narcotics distribution, and money laundering; actions which had allegedly procured him the equivalent of 130 million dollars.

Unlike credit cards or other forms of currency that leaves a paper trail, Bitcoins cannot be recovered. If you were to lose your bitcoins due to a machine crash or paid for something and didn't receive the item, then those Bitcoins are gone forever. You do, however, have the ability to print out your bitcoins rather than digitally storing them. When a hacker is able to get a hold of your virtual wallet and transfer your Bitcoins, there is no way to get them back. The best way to store your Bitcoins is through a separate device such as a thumb drive. Even this has its weaknesses though; thumb drives can be lost and there is also an inherent failure rate on the part of the manufacturers when producing them. Once your virtual wallet has been compromised you are either losing time or money because bitcoins can be purchased from real brokers.

Are bitcoins worth the hassle? Networking among the Bitcoin community is essential to its growth and security. Whereas when each coin is represented by cryptography, it's also accounted for over the network so that the same coins do not get reproduced during the mining phase. This helps keep the currency from flooding the market, while at the same time keeping a certain amount released to the public so that the currency is actually useable. The amount of computers needed to have the necessary computing power to make mining Bitcoins worth it, outweighs the actual profit gained. Not only that, working in pools has its own security risk due to the individual machine configuration of each computer in the pool. Since the file has your wallet encryption saved, it makes it easy for malicious hackers to get ahold of your UN or PW and taking your bitcoins. Therefore, normal malware or Trojans on your other machines would make you an easy target for profit loss.

Recently ads on Yahoo, infected with Malware, caused a large scale botnet used to help set up a Bitcoin mining collective from normal users. Mining Bitcoins requires a mass amount of computer processing power, but utilizing the background computing power of multiple computers could be a good alternative. This would be a great way to mine coins that in no way would harm you other than via your power bill or the money spent to purchase such machines. If you consider that the ads on Yahoo reach millions of people each day would make it a very high security risk for the average user. So not only can the information off your PC be stolen but it also could be used in a large scale minning operation to turn a profit for someone else if you don't have up-to-date antivirus software or malware protection. The fact that virtual currencies are starting to get more popular is a reason why many security analysts feel things will only get worse as this type of currency is made more accessible to the everyday consumer. Distributed Denial of Service attacks are also causing people with Bitcoin wallets grief as they are left to at the mercy of the attacker. BTC-China had an attacker use up to 100G/Bits per second bandwidth to hold them hostage for Bitcoins. European payment processor BIPS said it had been hit with a DDoS attack and then hacked to the total of 1,300 Bitcoins equaling 1 million dollars. Hackers know that since the currency can be exchanged very fast it will be impossible for the coins to be returned to the original owner.

With Bitcoins it’s a hit or miss, big risk. You could potentially make a lot of money with trading them and using them. At the same time, there is a costly risk involved. The future seems to tend towards virtual currency, considering more and more people are purchasing things online. It will be up to new technology to determine how safe it can be. Personally, I can’t say that the risk is worth the chance of what you could lose. If you don’t know understand how Bitcoins work, it is probably best to steer clear of virtual currency. If it was free of meddling then it would be a great idea but I don’t feel this is a good idea to give up our current money for it. In some sense there is always an arms race for better currency: As hackers becomes more sophisticated in their attacks, so does the encryption method; and as the encryption methods become better, there are always hackers trying to crack it which leaves the user at the complete mercy of the end user and their safe computer use.

References

Startbitcoin. "Beginners Guide to Mining Bitcoins." *Beginners Guide to Mining Bitcoins*. Startbitcoin, n.d. Web. 14 Apr. 2014. <http://startbitcoin.com/>.**http://www.economist.com/node/21563752**

Raszl, Ivan. "Blog of Ivan Raszl." *Blog of Ivan Raszl*. N.p., n.d. Web. 14 Apr. 2014. <http://raszl.com/blog/bitcoin-benefits-and-risks>.

Munson, Lee. "Feds Seize Silk Road's $28 Million Bitcoin Wallet." *Naked Security*. N.p., 20 Jan. 2014. Web. 14 Apr. 2014. <http://nakedsecurity.sophos.com/2014/01/20/feds-seize-silk-roads-28-million-bitcoin-wallet/>.

Whitney, Lance. "Yahoo Malware Turned PCs into Bitcoin Miners - CNET." *CNET News*. CBS Interactive, 9 Jan. 2014. Web. 14 Apr. 2014. <http://news.cnet.com/8301-1009_3-57616958-83/yahoo-malware-turned-pcs-into-bitcoin-miners/>.

Nargren. "UbuntuHak: Bitcoin Basics and Ubuntu 12.04." *UbuntuHak: Bitcoin Basics and Ubuntu 12.04*. N.p., 26 Nov. 2012. Web. 14 Apr. 2014. <http://ubuntuhak.blogspot.com/2012/11/bitcoin-basics-and-ubuntu-1204.html>.

Mcmillan, Robert. "Want Cheaper Bitcoins? Hit Someone With a DDoS Attack | Enterprise | WIRED." *Wired.com*. Conde Nast Digital, 24 Nov. 0013. Web. 14 Apr. 2014. <http://www.wired.com/2013/11/ddos_bitcoin/>.

*Bradbury, Danny. "Serials Solutions Article Linker." *Serials Solutions Article Linker*. Elsevier, Nov. 2013. Web. 14 Apr. 2014. <http://jw3mh2cm6n.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info:sid/summon.serialssolutions.com&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.atitle=The+problem+with+Bitcoin&rft.jtitle=Computer+Fraud+%26+Security&rft.au=Bradbury%2C+Danny&rft.date=2013-11-01&rft.pub=Elsevier+B.V&rft.issn=1361-3723&rft.eissn=1873-7056&rft.volume=2013&rft.issue=11&rft.spage=5&rft_id=info:doi/10.1016%2FS1361-3723%2813%2970101-5&rft.externalDBID=n%2Fa&rft.externalDocID=350097537¶mdict=en-US>.

*Leah, M. G. (2014, Mar 14). The face behind bitcoin. *Newsweek, 162* Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1504810381?accountid=10639