ASA

Risk Consultants

Research Note

The Future of Bitcoin

By: Divya Yadav

Applicable Sectors: Information Technology, Finance

Keywords: Digital Currency, Security, Economy, Regulations, Ethics

Abstract: Bitcoin is a form of digital currency that has gained popularity since its inception. While Bitcoin seems to be facing tough times with the shutdown of the Mt. Gox exchange, this research note discusses its history and its future. It is the third research note that ASA has devoted to the issues raised by virtual currency.

ASA

Risk Consultants

Introduction

Bitcoin has been in the news lately, having gained momentum over the last few years. Bitcoin is a peer-to-peer payment system and digital currency introduced as open source software in 2009 by developer Satoshi Nakamoto.[1] A bitcoin in itself is an encrypted string of data, or a hash, encoded to signify one unit of currency.[2] Bitcoin has value just like gold or silver but it is mined from code.[3]Bitcoin is alsoan online financial network that is similar to conventional payment networks like Visa or Paypal, except that it is a decentralized payment system..[4] Its peer to peer structure has with hundreds of computers all over the Internet working together to process Bitcoin transactions.[5]

What makes Bitcoin so appealing? To create a new financial service one needs to partner with a financial institution but Bitcoin has no such restrictions. At the present time,people don't need s permission to create a Bitcoin Financial Service[6]. This low barrier to entry may allow the creation of a new generation of innovative financial services, in much the same way that the Internet's open architecture led to innovative new online services.[7] Bitcoin appeals to people who believe it represents the spirit of libertarianism-- free, unfettered, and uncontrolled.[8] But this uncontrolled and free from government regulations also offers a safe haven for criminal activities to flourish.

Transactions with Bitcoins

Nakamoto wanted people to be able to exchange money electronically and securely without the need for a third party, such as a bank or a company like PayPal. He based Bitcoin on cryptographic techniques that allow one to be sure the money received is genuine, even if you don't trust the sender.[9] Bitcoin client software needs to be installed by users in order to make transactions with Bitcoins. Once the software is downloaded, it connects over the Internet to the decentralized network of all Bitcoin users and also generates a pair of unique, mathematically linked keys, which a user will need to exchange Bitcoins with any other client.[10] One key is private and the other is public and a version of it (dubbed a Bitcoin address) is given to other people so they can send you bitcoins.[11] Crucially, it is practically impossible—even with the most powerful supercomputer—to work out someone's private key from their public key, which in theory (and until recently) prevents anyone from impersonating the users.[12] When users perform a transaction, their Bitcoin software performs a mathematical operation to combine the other party's public key and their own private key with the amount of Bitcoins that the user wants to transfer.[13] The result of that operation is then sent out across the distributed Bitcoin network so the transaction can be verified by Bitcoin software clients not involved in the transfer.[14] This process ensures at least theoretically the safety of the users and validates that the transaction is happening between two real users.

The nature of the mathematics ensures that it is computationally easy to verify a transaction but practically impossible to generate fake transactions and spend Bitcoins that users don't own.[15] Since there is a public log for each transaction, it also serves as a deterrent for money laundering[16] and provides an additional layer of security to Bitcoin transaction system.

How to Secure Bitcoins

Bitcoins can be bought and exchanged in different currencies from exchange servers like Mt. Gox. To store this digital currency all users need is an account for Bitcoin wallet which essentially is just a website or a program and stores the digital codes for Bitcoins and provides an easy interface to monitor the transactions.

This all seems fast and easy, but the bottom line is all the money is being saved online and this makes it vulnerable to hackers who can go at great lengths to secure these codes and a user be virtually without any money in a matter of seconds. This poses a huge security risk for Bitcoin and will prevent users from relying on a model such as this. If a user wants to deal with Bitcoin he or she needs to be computer savvy themselves. It is at this point highly risky for computer novices. One of the ways to secure Bitcoins on a personal computer is to add a layer of encryption and not only by just means of a strong password because hackers can still track the keystrokes.[17] A good idea would be to store all the information offline with the help what is called cold storage wallets.

Cold storage wallets store private Bitcoin keys offline, so that they can't be stolen by someone else on the Internet.[18]

Impact on Economy

We have discussed how Bitcoin works and the mechanism to make the transaction and store that money. But we still need to know if Bitcoin or virtual currency in general is here to stay and, if it is, how it will impact our economy. Interestingly enough Bitcoin is not the first digital currency to have come out in the market but is definitely the first one to survive because it is "the first cryptocurrency with the deep structure, wide adoption, and trading momentum to achieve escape velocity".[19]

Timothy Carmody suggests that "Bitcoin is backed by no government, and its value isn't rooted in precious metals. Instead, it's distributed across the entire network of users, its roots in complex digital mathematics. Bitcoin supporters say that this makes the currency immune to manipulation by politicians or oligarchs seeking to move its value up or down for politics or profit".[20] Some researchers and investors note that Bitcoin could be a permanent solution to a fluctuating economy. Carmody suggests further that, with governments' financial and credit troubles causing major problems for their currencies, global investors are looking for something firmer than the promise of a central bank.[21] He suggests that, like gold or other precious metals used as specie, Bitcoins are scarce. But their scarcity is algorithmic, as opposed to

natural or accidental.[22] Additionally, according to Carmody, "Bitcoin mining guarantees a fixed rate of inflation (relative to itself)".[23]

Bitcoin can be especially helpful in countries that still do not deal in credit and debit cards. It will provide a way for people to make transfers without having to worry about fraud. Carmody again: "Money has become data, especially when you view money as a transactional unit that needs to be transferred and delivered from one platform to another. Digital currency offers that and with much more security especially the world we live in today where ever transaction happens online. Though it will never replace financial institutions' current systems, Carmody believes that Bitcoin has the capability to set up an "international payment system".[24] He suggests that

"If Bitcoin becomes widespread, respected, and legitimate, that pressures everyone—all the central banks and banking companies—to bring down those costs in order to stay competitive".[25]

Regulation

Regulation on Bitcoin differs in each country. While it's completely legal to complete transactions in Bitcoins in the U.S. and Germany, Russia on the other hand has branded it illegal because it views a substitute for money.[26]

Government has no centralized control over Bitcoins like they do have at traditional financial services which makes it especially harder to regulate Bitcoin. But in the wake of recent failures of Mt. Gox and the breakup of Silk Road, the U.S. is planning to impose some regulation. “Benjamin Lawsky, New York's financial services superintendent, said he will issue "BitLicenses" to companies dealing with Bitcoins. That would mark the most significant step thus far in the United States to regulate the digital currency”.[27] These “Bitcoin exchanges should have to warn their customers virtual transactions are irreversible, Bitcoin values are volatile and they should carefully guard their digital wallet keys”.[28] Bitcoin exchanges might also be forced to adopt the same "know-your-customer" requirements, which currently force financial institutions to keep an eye on customer behavior and report suspicious activity to law enforcement.[29]

Regulation will only add credibility to the digital currency and provide a trusted and safe platform for customers to make transactions.

Ethical Considerations and Recent Cases

While the idea of Bitcoin and digital currency seems appealing and very scientific, there are still many ethical considerations. Criminal activity involving Bitcoin has largely centered around theft of the currency, money laundering, the use of botnets for mining, and the use of bitcoins in exchange for illegal items or services.[30]

Bitcoin's decentralized network is being put to test in wake of recent incidents that test the lack of regulations. The most fundamental threat was a bug in some basic software that determines how Bitcoins are moved between digital accounts. That forced several of the largest Bitcoin exchanges to shut down for most of last week and raised questions about the sturdiness of the programming underlying the currency.[31] But the biggest shock came from the shutdown of Mt. Gox, a Bitcoin exchange that handled almost 70%[32] of Bitcoin transactions. "It announced that around 850,000 Bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time".[33] This incident seriously challenges the credibility and future of Bitcoin. While people may view regulations a a way for government to interfere, a lack of regulation has a way of attracting criminals and a ground to conduct illegal activities.

Silk Road was a marketplace that dealt in drug related transactions made through Bitcoin. In October, the U.S. Federal Bureau of Investigation shut the marketplace down.Shortly thereafter, however, tech savvy outlaws started Silk Road 2.[34] It is primarily used to buy and sell drugs. Bitcoins are the only kind of currency accepted on the site, because they are traded electronically and are difficult to trace to individuals. But Bitcoin accounts also lack protections that most bank accounts have, including government-backed insurance.[35]That means the Bitcoins stolen from the Silk Road users are gone forever. The hackers took advantage of the same the glitch that impacted Mt. Gox and stole

worth $2.7 million from customers.[36] This incident serves as a reminder that regulations and laws are necessary to keep harmful entities at bay and in order fora novel concept like Bitcoin to boom.

Conclusion

Public reception of Bitcoin has largely been mixed and most people are not even aware such a mode of money exists. People generally are very careful with money and would like to secure it with institutions that have credibility and is protected by government. Banks succeed because people have confidence in them, and because their deposits are insured. Bitcoin might not succeed but the idea of digital currency will live and flourish. Bitcoin has already made history and has provided an outlet in the times of a very fluctuating economy.

The ASA Institute of Risk and Innovation has been following this story for several years, and has already published two research notes that focus on digital currency: Justin Brecese's "Money from Nothing: The Socioeconomic Implications of "Cyber-currencies"" and Devin Luco's "Virtual Currency: The Next Generation Banking Model" to get a more holistic view on the world of digital currency.

ASA

Risk Consultants

References

[1] "Bitcoins". *Wikipedia*. Web. March 9, 2014. http://en.wikipedia.org/wiki/Bitcoin

[2] "Bitcoin 101- The Digital Currency Revolution". Web. March 9, 2014http://www.online-accounting-degrees.net/bitcoin/

[3] "Bitcoin 101" n. pag.

[4] Lee Timothy B. "12 questions about Bitcoin you were too embarrassed to ask". *The Washington Post*. November 19, 2013. Web. March 9, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/

[5] Lee Timothy B. n. pag.

[6] Lee Timothy B. n. pag.

[7] Lee Timothy B. n. pag.

[8] Krigsman Michael. "Is Bitcoin the future of money? Not a chance". *ZDNet*. October 11, 2013. Web. March 9, 2014. http://www.zdnet.com/is-bitcoin-the-future-of-money-not-a-chance-7000021814/

[9] Simonite Tom. "What Bitcoin Is, and Why It Matters". MIT Technology Review. March 25,

2011. Web. March 9, 2014 http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/
[10] Simonite Tom. n.pag.
[11] Simonite Tom. n.pag.
[12] Simonite Tom. n.pag.
[13] Simonite Tom. n.pag.
[14] Simonite Tom. n.pag.
[15] Simonite Tom. n.pag.
[16] Simonite Tom. n.pag.
[17] "How to store your bitcoins". February 20, 2014. Web. March 9, 2014. http://www.coindesk.com/information/how-to-store-your-bitcoins/
[18] "How to store your bitcoins". n.pag.
[19] Carmody Timothy. "Money 3.0: How Bitcoins May Change the Global Economy". *National Geographic*. October 14, 2013. Web. March 9, 2014. http://news.nationalgeographic.com/news/2013/10/131014-bitcoins-silk-road-virtual-currencies-internet-money/
[20] Carmody Timothy. n.pag.
[21] Carmody Timothy. n.pag.
[22] Carmody Timothy. n.pag.
[23] Carmody Timothy. n.pag.
[24] Carmody Timothy. n.pag.
[25] Carmody Timothy. n.pag.
[26] "Legality of Bitcoin by country". *Wikepedia.* Web. March 9, 2014. http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country
[27] Pagliery Jose. "Bitcoin regulation coming this year". *CNN Money*. February 12, 2014. Web. March 9, 2014. http://money.cnn.com/2014/02/12/technology/bitcoin-regulation/
[28] Pagliery Jose. n.pag.
[29] Pagliery Jose. n.pag.
[30] "Bitcoins". *Wikipedia*. Web. March 9, 2014. http://en.wikipedia.org/wiki/Bitcoin
[31] POPPER NATHANIEL. "Regulators and Hackers Put Bitcoin to the Test". *The New York Times.* February 17, 2014. Web. March 9, 2014. http://dealbook.nytimes.com/2014/02/17/regulators-and-hackers-put-bitcoin-to-the-test/?_php=true&_type=blogs&nl=todaysheadlines&emc=edit_th_20140218&_r=0
[32] "Mt. Gox". *Wikipedia.* Web. March 9, 2014. http://en.wikipedia.org/wiki/Mt._Gox
[33] "Mt. Gox". N.pag.

ASA

Risk Consultants

[34] Pagliery Jose. “Drug site Silk Road wiped out by Bitcoin”. *CNN Money.* February 14, 2014. Web. March 9, 2014. glitchhttp://money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin/

[35] Pagliery Jose. n.pag.

[36] Pagliery Jose. n.pag.