Cryptocurrency: A Cryptic How to

Uncovering the underpinnings of Bitcoin, the cryptocurrency that changed the world.

by

Fejiro Odibo

CCM702

Professor Bob Cooper

The internet is the cornerstone of change; the past few years have been dominated by innovations in social media where Facebook and Twitter have revolutionized the way we interact with our peers. The buzz surrounding so-called "cryptocurrencies," a new mode of exchange, has caused many to speculate its role within the next big revolution.

A cryptocurrency is a monetary system that relies on "cryptography," a process that secures financial information using mathematics, used by individuals in a distributed network, across the internet, rather than centralized banking in order to facilitate transactions (Meiklejohn et al., 2013). Cyrptocurencies were made public as the result of a self-published paper written by an anonymous author under the pseudonym of 'Satoshi Nakamoto' (Nakamoto, 2008).

Cryptocurrencies do not rely on any centralized government or authority -- yet still can be trusted as a store of value. There are many cryptocurrencies in the market each containing a different value; however, all cryptocurrencies begin with no intrinsic value and depend on the market for value through speculation and use. Today, the Bitcoin software is the most widely used cryptocurrency (Nakamoto et al., 2015) with a market value worth billions of dollars (Johnsson et al., 2014).

In 2013, the price of one Bitcoin soared passed the value of $1000 US dollars (Zhou, 2013), which commanded the attention of the financial and technological worlds. Currently the value of Bitcoin rests at $300 US dollars after a crash as a result of hacking incidents (Jubljana, 2015), negative press, and market correction of speculative pricing (Mourdoukoutas, 2013). Bitcoin's current price has definitely come a long way from it's past lack of value.

I sat down for coffee with Jonathan Gillett, a software engineering graduate researching finance and cryptography. I wanted to gain insight on the technology behind Bitcoin and how it could change things. Tall and bespectacled, Jonathan is a frequenter of Bitcoin meet ups and conferences. He is also a regular at the Decentral headquarters, an organization dedicated to furthering the adoption and integration of decentralized digital currency technologies. As I interviewed Jon, I was immediately taken by his passion and enthusiasm for the subject; although he had dedicated years delving through the complexity of Bitcoin, he gladly accepted the challenge of elucidating its inner workings in a short amount of time.

Feji: It seems that most people heard of Bitcoin when the price of 1 Bitcoin peaked at thousand dollars as well as its subsequent crash, what is your take on these events?

Jonathan: That's a very good question. Funnily enough, I knew about Bitcoin when the price was at 0.01 cents each. So you can image with such a dramatic increase in the value why there has been such speculation and hype surrounding Bitcoin. Much of the increase in price was driven by

speculation in addition to the fact that there is a limited supply, at present, approximately 14 million. When it crashed the price of one Bitcoin dropped to being approximately one third the value at its peak; this is largely in part to market correction and various security incidents in the news. These events were a warning to investors that Bitcoin is the wild west of technology; it's so new that people cannot accurately predict its future.

Feji: Cryptocurrency is quite the elusive concept, how does one begin to explain it to those who are unfamiliar with the technology?

Jonathan: Unlike traditional banking, with Bitcoin people undertake the role of a bank by validating transactions. Anyone can process payments using the Bitcoin software on their computer, and in doing so, are rewarded.The challenge is that in order to prevent abuse, the computers must solve a very challenging mathematical problem, this is a process called "mining" whereby, the first computer to solve the problem receives a reward which comes in the form of Bitcoin. Mining is a very difficult and time consuming process that requires large amounts of computing power that can cost thousands of dollars. The process is made difficult to deter "bad actors" or people with malicious intent. It is important to note that the only way more Bitcoin can be added to the supply in the economy is through these rewards provided to miners. Unlike traditional monetary systems, governments cannot decide how much to create, as it is a system strictly governed by mathematics.

A Bitcoin mining operation

Feji: How does one attain some Bitcoin without having to mine?

Jonathan: The easiest way to get Bitcoins is through an exchange either in person with someone through a service such as localBitcoins, which allows individuals to meet in person and exchange Bitcoins for cash. The second way would be to use an exchange, such as QuadrigaCX, these allow

one to transfer money from their bank account to purchase Bitcoin in exchange for Canadian dollars.

Feji: How can an individuals use Bitcoin?

Jonathan: An individual can use Bitcoin much the same as they could think of using any other payment system, the difference being that Bitcoin operates similar to a debit card in that one can only spend that which you have. However, unlike most systems, you are your own bank. You store your Bitcoin on your device similar to how you store cash in your wallet. There are many merchants accepting Bitcoin everyday including large companies such as expedia, and in most cases, for users to pay with Bitcoin, it's as simple as tapping the point of sale with their phone or scanning a QR code.

Feji: A part from being a potentially risky investment, what other risks are involved?

Jonathan: Let me start by saying that the actual mathematics that govern Bitcoin are very secure based upon the same security that banks and government rely on, if not even more secure. The greatest risk with Bitcoin is that if you are hacked or your device is stolen, if measures are not previously taken, it can be very easy for someone to steal your Bitcoins, this is due to the digital nature of Bitcoins. Unlike stealing cash or gold bars from a bank, there is no overhead to transferring Bitcoins, it is nearly instant.

Feji: How can one protect themselves against risks?

Jonathan: The easier way for one to protect themselves from thefts or other risks involved in Bitcoin is to ensure that you have numerous backups of your Bitcoin wallet, which is the software used to store your Bitcoins on your device. Any new Bitcoin software you use on your device nowadays will prompt you to configure regular back ups, it is pertinent that you do so. The second and equally important way is to password protect your Bitcoin wallet; this prevents anyone from spending your Bitcoins without knowing the password.

Feji: Are there any privacy concerns with Bitcoin?

Jonathan: Yes there are and this is one the poorly understood facts about Bitcoin. Remember earlier how i was discussing mining; in order for everyone participating to validate transactions the transactions must all be made public on the network. This means that it is possible to for someone who knows your Bitcoin address [the unique identifier that you send and receive Bitcoins from], they could possibly track all of your transactions. The best way to protect your privacy is to not reveal publicly what your Bitcoin address is, this way it is impossible to distinguish you from everyone else.

At the conclusion of the interview, it was very clear that Bitcoin had changed the world. Though many of us are not aware, Bitcoin has essentially democratized our financial system; its use making

banks and government redundant by transferring value and power into the hands of the people. With issues of privacy and security, the technology many require some fine-tuning along with a mode of education for new users. It seems that whether or not bitcoin is here to stay, it's applications could go beyond anything we've ever imagined.

References

Johnsson S., Levin J., Goldstein Z., Sarrar N., & Lopp J. (2014, January). Coinometrics combines economics, statistics, and mathematics to illustrate the cryptocurrency economy. Retrieved March 23, 2015, from http://www.coinometrics.com/Bitcoin

Jubljana, L. (2015, January 6). Bitcoin exchange Bitstamp suspends service after security breach. Retrieved March 26, 2015, from http://www.reuters.com/article/2015/01/06/us-bitstamp-cybersecurity-idUSKBN0KF0UH20150106

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of Bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.

Mourdoukoutas, P. (2013, December 6). Bitcoin Market In Sharp Correction, What Is Next? Retrieved March 26, 2015, from http://www.forbes.com/sites/panosmourdoukoutas/2013/12/06/Bitcoin-market-in-sharp-correction-what-is-next/

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012), 28.

Nakamoto, S., Andresen, G., Van der Laan, W., & et al. (2015). Bitcoin core integration/staging tree. Retrieved March 21, 2015, from https://github.com/Bitcoin

Zhou, W. (2013, November 27). Bitcoin price zooms through $1,000 as enthusiasm grows. Retrieved March 22, 2015, from http://www.reuters.com/article/2013/11/27/us-Bitcoin-trade-idUSBRE9AQ0YR20131127