|  |
| --- |
| WRIT 340 |
| Aurum ex Machina: an Introduction to Bitcoins |
| For ILLUMIN Magazine |

|  |
| --- |
| Chuan (Jeffrey) Huang  3-28-2014  jeffrey810816@gmail.com |

## Abstract

Bitcoin is the pioneering cryptocurrency driven by the principles of cryptography and peer-to-peer networks, created as an alternative to fiat money, which is controlled by a central power,. It allows for pseudo-anonymous and almost instantaneous transfer of money for very little cost across the internet. The brand new Bitcoin community is facing many challenges and has many disadvantages, such as high volatility of the currency, association with crime, and lack of oversight. However, cryptocurrency is an exciting new concept that may leave a lasting legacy.

The rise of Bitcoin and the concept of cryptocurrency has taken the world by storm. Reactions have ranged from excitement to ridicule to suspicion. This article will attempt to demystify the fascinating new technology, clarify various myths and confusions surrounding cryptocurrencies, and examine recent developments and the future of the Bitcoin community.

## So What *Exactly* is Bitcoin?

Essentially, all the complex technical concepts boils down to this: Bitcoin is a special set of numbers that can be used as money, centred on a very long ledger of every transaction done with it. The system is lightweight, fast, and allows transactions between two individuals pseudo-anonymously to and from anywhere in the world with internet access. Its algorithm is designed to be neutral and not controlled by any one entity, and hence it is not easily manipulated by centralised powers, especially from countries with strict capital control. As Bitcoin is an open source project, which allows the protocol and concept to be freely viewed, altered, and used, this framework has quickly developed a unique economy and a very enthusiastic community around it.

## A More Technical Exmplanation

Regular currencies are essentially a standardised version of an IOU: the holder of this piece of paper or this rounded piece of metal is entitled to a certain value of goods and services when presenting it. Like all IOUs, currencies require some sort of guarantor to back up its value. In the case of the US dollar in the past, this guarantor was a promise for a certain quantity of gold from the government; in modern times, the gold standard has been replaced by fiat money, where the currency is not tied to a physical object, but rather has a value defined by the issuing agency, usually a central bank. The disadvantage of fiat money is that it is easily manipulated by a small and selected group of powerful individuals through monetary policies. In addition, its use and transfer, especially according national borders, is controlled by the state.

Enter cryptocurrencies: a system of exchange backed not by a physical object or an agency, but by principles of encryption. Instead of a having a bank to print money and issue unique serial numbers to each banknote, cryptocurrencies are issued and maintained by one long transaction ledger, known as the *block chain[[1]](#footnote-1)[1]*, which is stored on each Bitcoin user’s computer and constantly synced with one another using software known as *digital wallets*, which are analogous to their more traditional counterparts. When, say, Alice, identified with a unique *Bitcoin address* that is essentially a public key, wants to send, say, 0.25 bitcoins (0.25 BTC) to Bob, she petitions to add this transaction to the block chain. However, a system must be in place so that the transaction is verified by other people connected to the block chain, and so that Alice cannot verify her own transactions in order to abuse the system and double spend her bitcoins.

To do this, Bitcoin uses an idea known as *proof-of-work*: in order to verify the transaction, the verifier must solve a complex math problem involving the hash function; a way of encrypting data that is, by design, only solvable by brute-forcing the question. This process requires a significant amount of computational power, and therefore real world resources of time and electricity. To incentivise people to do this verifying process, the system rewards the first verifiers with a certain quantity of bitcoins, which allows new bitcoins to be seeded into the economy without a distributing agency. This verification process is known as *mining[[2]](#footnote-2)[1]*, as it is analogous to mining for precious minerals to mint into coins in traditional currency systems.

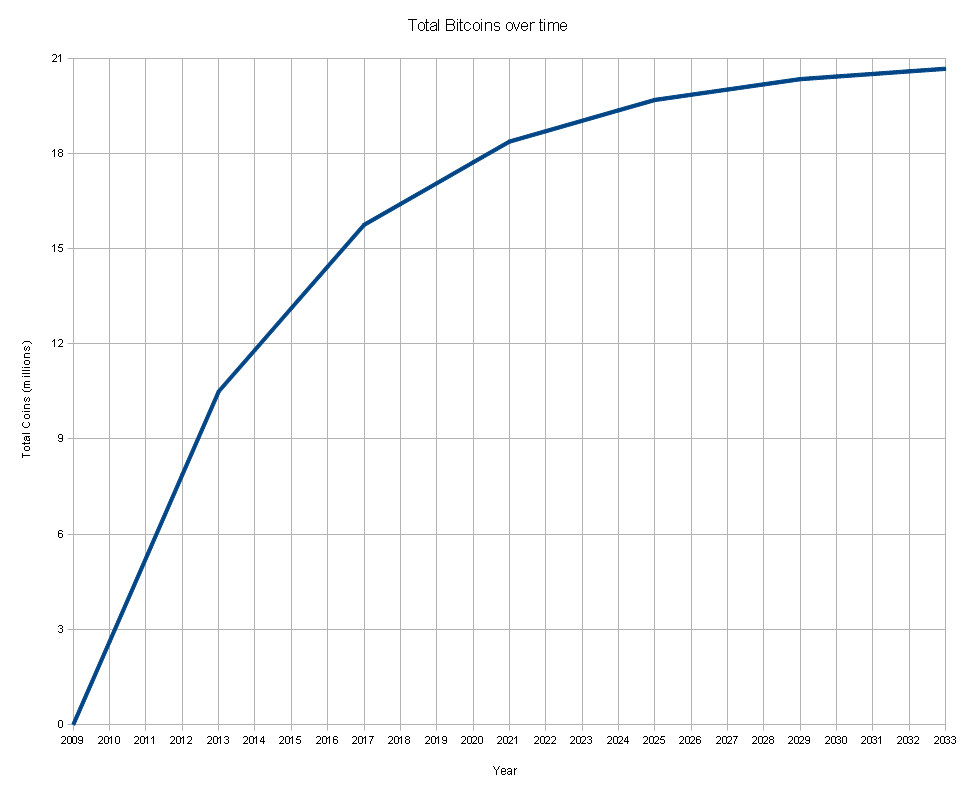
The benefit of this system is twofold: as hash functions are unique numbers integral to the mining process, we can simply use the hashes to identify the coins themselves, eliminating the need for the issuing agency[[3]](#footnote-3)[2]. In addition, the creation of new bitcoins is fixed and hard-coded into the Bitcoin protocol, and therefore no single party can restrict or increase the supply of currency to affect its price. The rate of Bitcoin mining is set to decrease logarithmically, by increasing the difficulty and halving the reward of mining after a set number of transactions. There is a hard limit of twenty-one million bitcoins, after which mining does not yield bitcoins from the system, but users may still award miners with transaction fees, which has increased over the years. As bitcoins are divisible into units up to 10-8 BTC[[4]](#footnote-4)[3], known as one Satoshi, it should not limit the expansion of the currency. The last bitcoin is estimated to be mined in year 2140[[5]](#footnote-5)[3].

Figure 1: Graph showing the total number of bitcoins in circulation as a function of time. As the rate of mining decreases, the total number of bitcoins will plateau.

Found at <http://readwrite.com/2013/11/20/bitcoin-bubble-investment#awesm=~ozKvLpOqCvXimT>

As the return to mining decreases, Bitcoin miners began forming *mining pools*, where each individual miner dedicates a part of their computational power to a collective, and when one person within the pool gets a reward, it is divided among the pool in proportion with one’s computational power contribution, much like a company mining for precious metals may hire multiple workers to work a mine and pay each miner according to their work done. This ensures that miners with very basic hardware who have too small a probability of obtaining the reward are able to make bitcoins from mining.

## But Why *Not* Bitcoin?

The first Bitcoin transaction, known as the *genesis block*, was created only recently in 2009 by a hacker who goes by the pseudonym of Satoshi Nakamoto. As such, the community as well as the system is still in its infancy and therefore suffers from several teething issues.

Firstly, Bitcoin is volatile. It is estimated to be at least seven times as volatile as gold and eight times as volatile as the S&P 500[[6]](#footnote-6)[4]. This trait has made owning bitcoins more like a roller coaster ride than having cash in your pocket, thereby making it difficult to use as a medium of exchange. This writer began approaching in March of 2013, when the price of bitcoins was around 1 BTC to $30 USD. In the year since then, the price of 1 bitcoin has risen up to as high as $1200 USD, dropped back down twice to $100 USD, recovered, and then finally stabilising at the current price of around $440 USD, as of May 7th, 2014. This volatility has led many Bitcoin owners to treat it as a very high risk investment rather than a currency.

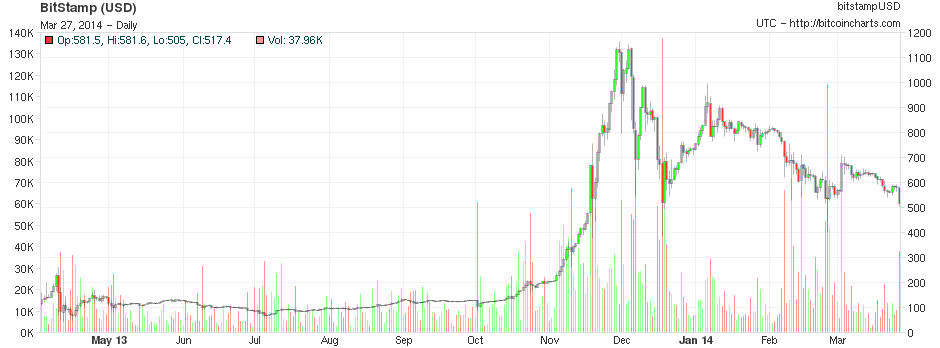
However, some have contended that this volatility is due to the difficulty of liquidating the currency and will be alleviated as the list of merchants accepting Bitcoin rapidly expands[[7]](#footnote-7)[5].

Figure 2: Price of Bitcoin on exchange site Bitstamp over a one-year period.

Found at: <http://bitcoincharts.com/charts/bitstampUSD#rg360ztgSzm1g10zm2g25zv>

Bitcoin also had a notorious history of being associated with illegal activity. Before its shutdown in October of 2013, one of the largest sources of Bitcoin transactions was Silk Road, the largest black market auction website in an encrypted network known as Tor hidden service, where people would take advantage of Bitcoin’s anonymity to trade illegal goods; mostly narcotics, followed by money laundering, hacking, murder-for-hire and weapons. This association helped demonise the technology as a criminal tool and damaged its reputation[[8]](#footnote-8)[4].

Since the demise of Silk Road, black-marketeers have realised that the nature of the block chain, as a permanent record of every transaction, allows investigators to persecute them by tracing the flow of bitcoins from Silk Road’s account[[9]](#footnote-9)[6]. The link between criminal activity and cryptocurrency has therefore been reduced, despite the later rebirth of Silk Road 2.0, but the juxtaposition remains.

While one of the main draws of Bitcoin is its disassociation from any government or organisation, it also suffers from it. Without the oversight of legal entity to compensate for potential losses, Bitcoin is especially vulnerable to bankruptcy, hackers, and scams. Although the currency itself is based on an encryption that is nigh undefeatable, the surrounding software for digital wallets and money exchange sites are not. The most prominent instance of this is the bankruptcy of Japan-based Mt. Gox, which was the largest Bitcoin exchange, handling 70% of all transactions[[10]](#footnote-10)[7]. The company suddenly filed for bankruptcy protection in March of 2014 after shutting down withdrawals the month before, taking 650,000 BTC, worth around $120 million USD, with it[[11]](#footnote-11)[8][[12]](#footnote-12)[9]. Japan’s existing legal system was neither prepared nor designed to handle the case.

There are, however, those who see the failure of Mt. Gox to be a good development for the currency. The death of one exchange paves the way for newer and better ones to take its place, allowing the free market to improve the currency system in a form of Darwinism. In addition, the event acted as a stress test for cryptocurrency: despite undergoing a catastrophic meltdown, Bitcoin survived and maintained a relatively stable price after the initial shock[[13]](#footnote-13)[7].

## Bitcoin Jr.: It’s Many Derivatives

As Bitcoin is an open source project, there have been many derivatives and alternative cryptocurrencies that have been developed since its inception, most of which were intended to be improvements to the Bitcoin protocol. A notable exception is Dogecoin, a satirical parody based on the internet meme Doge that gained its own following despite its facetious origins, inadvertently assisting the spread of cryptocurrencies[[14]](#footnote-14)[10].

Currently, all of these alternate cryptocurrencies pale in comparison to Bitcoin in volume. The largest, Ripple, has a market capitalisation of $1.2 billion, 1/7th of Bitcoin’s $6.97 billion; the second largest, Litecoin, is 1/20th of Bitcoin’s size at $400 million[[15]](#footnote-15)[11].

Some have predicted that Bitcoin will not survive in the long run, but rather, its legacy will continue in the form of an improved digital currency, or one backed by a more established organisation rather than a group of anonymous hackers[[16]](#footnote-16)[12].

## Conclusion: Future Imperfect

Bitcoin, as a concept and as a technology, is definitely in its infancy; the software is still being improved against hacks and exploits, the infrastructure of exchanges, merchants and consumers is still being established, and the currency’s reputation with the general public is still poor. The future of cryptocurrency may be as unpredictable as its market price, but it is undeniably a revolutionary concept that has the exciting potential to change the world.

## Works Cited

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]*,* Available: <https://bitcoin.org/bitcoin.pdf>

[2] Ghassan O. Karame et al. Two Bitcoins at the Price of One? Double-Spending Attacks on

Fast Payments in Bitcoin [Online], Available: <http://eprint.iacr.org/2012/248.pdf>

[3] Bitcoin Wiki. *FAQ* [Online], Available: <https://en.bitcoin.it/wiki/FAQ>

[4] Mark T. Williams. (2013, December 5). *Beware of Bitcoin* [Online]*,* Available: <http://cognoscenti.wbur.org/2013/12/05/bitcoin-currency-mark-t-williams>

[5] Tommy Wilkes. (2013, April 11). *Backer Defends Virtual Currency Bitcoin after Big Fall* [Online], Available: <http://www.reuters.com/article/2013/04/11/us-bitcoin-currency-idUSBRE93A0P020130411>

[6] Zachary Schneider. (2014, February 17). *Bitcoin: Why is it Prone to Criminal Activity?* [Online], Available: <http://lawstreetmedia.com/news/headlines/bitcoin-why-is-it-prone-to-criminal-activity/>

[7] Paul Vigna. (2014, February 25). *5 Things about Mt. Gox’s Crisis* [Online], Available: <http://blogs.wsj.com/five-things/2014/02/25/5-things-about-mt-goxs-crisis/>

[8] Carter Dougherty and Grace Huang. (2014, February 28). *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin* Loss [Online], Available: <http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html>

[9] Steven Musil. (2014, March 20). *Mt. Gox Finds 200,000 Missing Bitcoins in Unused wallet* [Online], Available: <http://www.cnet.com/news/mt-gox-finds-200000-missing-bitcoins-in-unused-wallet/>

[10] David Gilbert. (2013, December 20). *What is Dogecoin? The Meme that Became the Hot New Virtual Currency* [Online], Available: <http://www.ibtimes.co.uk/what-dogecoin-meme-that-became-hot-new-virtual-currency-1429847>

[11] *Crypto-Currency Market Capitalisations* [Online], Available: <http://coinmarketcap.com/>

[12] Maureen Farrell. (2013, May 14). *Strategist Predicts End of Bitcoin* [Online], Available: <http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/>

1. [1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]*,* Available: <https://bitcoin.org/bitcoin.pdf> [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. [2] Ghassan O. Karame *et al.* *Two Bitcoins at the Price of One? Double-Spending Attacks on*

   *Fast Payments in Bitcoin* [Online]*,* Available: <http://eprint.iacr.org/2012/248.pdf> [↑](#footnote-ref-3)
4. [3] Bitcoin Wiki. *FAQ* [Online], Available: <https://en.bitcoin.it/wiki/FAQ> [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)
6. [4] Mark T. Williams. (2013, December 5). *Beware of Bitcoin* [Online]*,* Available: <http://cognoscenti.wbur.org/2013/12/05/bitcoin-currency-mark-t-williams> [↑](#footnote-ref-6)
7. [5] Tommy Wilkes. (2013, April 11). *Backer Defends Virtual Currency Bitcoin after Big Fall* [Online], Available: <http://www.reuters.com/article/2013/04/11/us-bitcoin-currency-idUSBRE93A0P020130411> [↑](#footnote-ref-7)
8. [↑](#footnote-ref-8)
9. [6] Zachary Schneider. (2014, February 17). *Bitcoin: Why is it Prone to Criminal Activity?* [Online], Available: <http://lawstreetmedia.com/news/headlines/bitcoin-why-is-it-prone-to-criminal-activity/> [↑](#footnote-ref-9)
10. [7] Paul Vigna. (2014, February 25). *5 Things about Mt. Gox’s Crisis* [Online], Available: <http://blogs.wsj.com/five-things/2014/02/25/5-things-about-mt-goxs-crisis/> [↑](#footnote-ref-10)
11. [8] Carter Dougherty and Grace Huang. (2014, February 28). *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin* Loss [Online], Available: <http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html> [↑](#footnote-ref-11)
12. [9] Steven Musil. (2014, March 20). *Mt. Gox Finds 200,000 Missing Bitcoins in Unused wallet* [Online], Available: <http://www.cnet.com/news/mt-gox-finds-200000-missing-bitcoins-in-unused-wallet/> [↑](#footnote-ref-12)
13. [↑](#footnote-ref-13)
14. [10] David Gilbert. (2013, December 20). *What is Dogecoin? The Meme that Became the Hot New Virtual Currency* [Online], Available: <http://www.ibtimes.co.uk/what-dogecoin-meme-that-became-hot-new-virtual-currency-1429847> [↑](#footnote-ref-14)
15. [11] *Crypto-Currency Market Capitalisations* [Online], Available: <http://coinmarketcap.com/> [↑](#footnote-ref-15)
16. [12] Maureen Farrell. (2013, May 14). *Strategist Predicts End of Bitcoin* [Online], Available: <http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/> [↑](#footnote-ref-16)