A REVIEW ON CRYPTOCURRENCY: THE VOLATILITY OF BITCOINS

[1] Vikash Gupta, [2]Shrey Rungta, [3]Vishnu Soni

[1,2,3]Institute of Engineering & Management

Salt Lake Electronics Complex, Kolkata-700091. India

Email: 21vikashgupta@gmail.com

Abstract

This study seeks to analyze conceptual, innovative, marketing and quantitative aspects of Bitcoin (BTC) and how these are reflected in the volatility of its return. After describing basic concepts of digital currencies and BTC, an electronic currency created in 2009, we contextualize BTC as a financial innovation. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution .We propose a solution to the double-spending problem using a peer-to-peer network. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone In my contribution I want to analyses this currency-system from a sociocy bernetic point of view .After presenting the basic mechanisms of Bitcoin money creation, the value regulation etc. We want to focus the basic processes of self-organization in this high-complex social system.

Keywords*: Bitcoin, Innovation*.

INTRODUCTION

Developed by Satoshi Nakamoto (2008), possibly a pseudonym used by programmers, BTC was deployed on January 3, 2009 and is the most popular encrypted digital currency in the world. According to Nakamoto (2008), use of the P2P4 network enables operations without the strict need for third parties, transactions are recorded chronologically and information remains available. P2P networks allow data transmission without the need for a central server and have the capacity to be self-organizing and fault-tolerant. Each BTC user has two "keys": one public and one private. The public key identifies the user on the network and uses a digital signature algorithm called ECDSA. Each user can have as many public keys as desired. For every transaction, the users involved must provide their respective public keys, which can be checked by any network user. BTC issuance is limited to 21 million and the issue rate is decreasing over time.

Taylor (2013) indicates that 58.8% of the total were issued by 2013 and by 2032, that percentage will be 99%, the prices of BTC are very variable ,earlier rises in the prices can be viewed with the help of demonstrated curve.

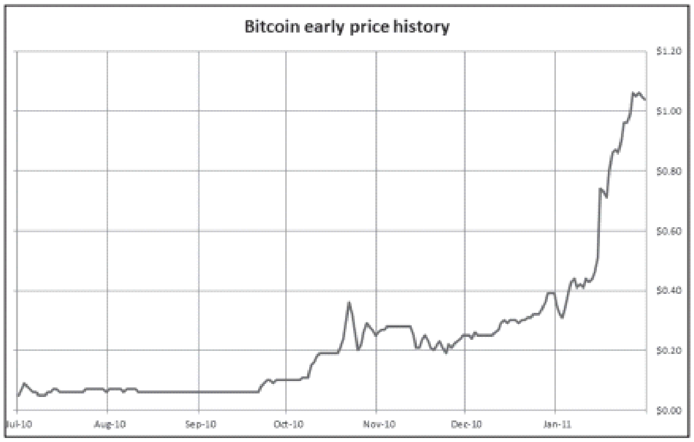

FIGURE 1 - EARLY CHART OF BITCOIN PRICED IN USD

BITCOIN’S BLOCK CHAIN- PUBLIC BOOKKEEPING:

Miners, the nodes responsible for operating the Bitcoin network, verify that transactions are valid and update the block chain with new blocks consisting of the latest transactions on a regular basis. The Bitcoin software run by miners on their individual computers incorporates the Bitcoin protocol with its set of rules and agreements. Overall, the Bitcoin network requires that the block chain (public book ledger) be continually updated with the addition of new blocks. Cryptographic hash is a complex algorithm that performs a very basic task–transforming text of arbitrary length (an entire book, a document, a sentence, or even a single word) into a fixed length string of numbers that appears random. The following Figure 3 provides some examples. The output of a hash function, or simply hash, is usually called the message digest and can be considered the document’s "fingerprint". A Bitcoin user has no control over what the output will look like. Also, given a specific digest output, finding an input that would generate it is nearly impossible. Thus, generating a digest is easy, but deriving the original text from the digest is impossible. Miners looking for the solution must usually calculate the hash millions of times to find the right pattern, but only a single hash calculation by other miners is necessary to validate it once it is found .Bitcoin’s hash algorithm, which creates the contents of the digest from the input text, makes the system described above possible. Thus, an ideal cryptographic hash function has four main properties:

1. Computing the hash value corresponding to any given message is simple.

2. Generating a message that has a given hash is impossible.

3. Modifying a message without changing the hash is impossible.

4. Finding two different messages having the same hash is impossible.

HOW BITCOIN WORKS:

To transact in bitcoin, one broadcasts to the bitcoin network the public key of the payee and the amount of bitcoin one intends to transfer. Every bitcoin address has an associated private key that acts as a password to ensure that all transfers are authorized. The private key is to transact in bitcoin, one broadcasts to the bitcoin network the public key of the payee and the amount of bitcoin one intends to transfer. Every bitcoin address has an associated private key that acts as a password to ensure that all transfers are authorized. The private key is:

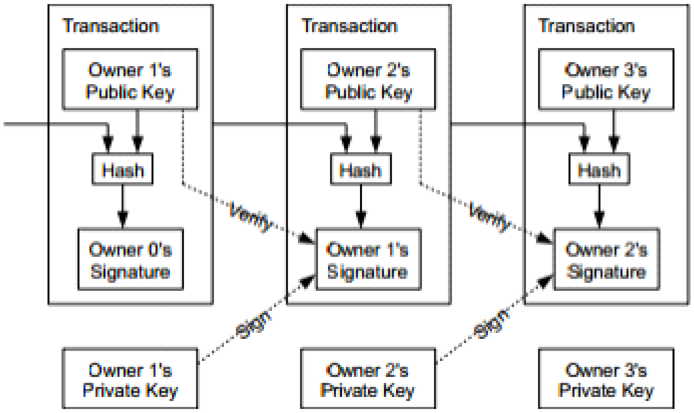

Figure 2: Algorithm for creation of private key to be used in every Bitcoin transfer

The primary concern of the payee is that the amount of bitcoin being transferred has already been spent, and therefore does not belong to the payer. Another concern is the rate of creation, since a high degree of inflation could reduce the value of one’s holdings. What allows bitcoin to be functional is that it overcomes these two major obstacles facing any digital currency: avoiding double spending and controlling creation (Velde 2013). Both of these problems are solved in the process of mining.

BITCOIN AS A STORE OF VALUE:

In the current state of Bitcoin, I believe that the only substantial use case that it has is a store of value, similar to gold. It is a speculative asset because it has no practical value outside of the fact that there is a promise of future value. As a store of value, Bitcoin has several favorable properties. First of all, it can be owned and easily stored. Unlike gold, Bitcoin can be stored on a USB stick, regardless of the amount you own. Gold takes up physical space, and holding large amounts of it can become noticeable. Bitcoin also has a fixed amount. In total, there will be no more than 21 million Bitcoin available to the world. Gold, while rare, continues to be mined, and the supply continues to increase. Bitcoin is also hard to imitate. It cannot be counterfeited, although scammers can sell to ignorant buyers.

IS BITCOIN SAFE? YES:

1. Bitcoin is encrypted and secure:
And not just normal, run-of-the-mill encrypted. Bitcoin is encrypted and backed with a special system called blockchain. Blockchain uses volunteers — a whole lot of them — to work together to encrypt the transactions that happen on the Bitcoin system. And in doing so, they make sure that all personal information is kept hidden away from any spying eyes, and that even if hackers do manage to get into the system, there’s nothing of value to steal.

2. Bitcoin is public:
   “Wait, that doesn’t sound safer” you might be thinking, but by “public”, we mean all the transactions are transparent and available to the public even if the people involved are anonymous. That means no one can cheat, scam, or otherwise fraud the system. They’re also irreversible, so once you get your Bitcoins, or sell them, no one can go and demand their money back. With Bitcoin, it’s like having thousands of people watching your wallet to make sure no one tries to steal anything.

3. Bitcoin is decentralized:
   Bitcoin has servers all over the world, and over ten thousand nodes keeping track of all the transactions happening on the system. And that’s important, because it means if something was to happen to one of the servers or nodes, the others can pick up the slack. It also means trying to hack into one of the servers is pointless: there’s nothing there you could steal that the other nodes and servers couldn’t prevent, unless you happen to control 51% of the nodes.

MATHEMATICAL FORMULATION OF THE PROBLEM

A potential bitcoin miner would seek to maximize potential economic profit. Each miner chooses his or her individual hashrate h to satisfy this objective. The rewards of mining are a function of a known quantity q awarded for a successfully mined block multiplied by a price p that is determined by market forces by bitcoin users and over which miners have no control. As such, p is a considered a stochastic variable. Given the winner-take-all nature of mining rewards, a miner receives those awards with a probability σ, which depends on the hashrate of the individual miner h versus the hashrate of the overall network H.

METHOD OF SOLUTION

As such, mining revenue r can be specified as:

$r = \sigma p$ where, $\sigma = h/H$

There are certain costs associated with supplying a hashrate h. The associated variable costs can be specified as a function of h multiplied by some cost factor c. There will also be some fixed costs fc associated with entering the mining market. Total costs tc of entrance can thus be modeled as:

$tc= ch +fc$

Expected profit Π is then a function of revenue less total costs. Expected profit is:

$\Pi = r - tc$

$\Pi = (h/H)\, pq - ch -fc$

Each miner is unaware of the behavior of other miners. Therefore, the overall hashrate supplied can be thought of as a function of the individual contribution h and the amount of effort k contributed by each other miner. The market will consist of n active miners, and so H can be specified as follows.

$H = h + (n-1)k$

$\Pi = [\ hpq/h + (n-1)\ k] - ch - fc$ -----(i)

Three conditions will hold in equilibrium. First, each individual miner will be profit maximizing, and therefore the first order condition foc of profit with respect to h will equal 0. This sets marginal revenue, which in this case is the increase in probability of being the successful miner from increasing h, equal to marginal cost, which in this case is the cost of supplying the increase in h. Second, in equilibrium it will be assumed that each miner has access to the same technology, and so each miner will make produce put forth the same amount of effort, so h will equal k. Free entry will also be assumed, so potential miners will produce as long as there is a profit incentive to do so. Therefore, in equilibrium, economic profit will be zero.

$foc = pq/[h+(n-1)k] - hpq/ [h+(n-1)k]^2 - c = 0$ ------(ii)

$k = h$ -----(iii)

$\Pi = 0$ ------(iv)

NUMERICAL RESULTS AND DISCUSSION:

To maximize the profit of a potential miner, we need to solve for n and h simultaneously given the above conditions as in (i), (ii), (iii), (iv) results in the following equilibrium values for n and h, denoted as h* and n*, respectively.

$$h^* = \frac{\sqrt{fcpq} - fc}{c}$$

$$n^* = \frac{\sqrt{fcpq}}{fc}$$

BITCOIN IN INDIA:

India tops in usage of smart phones, social media, etc., and financial institutions are digitalizing the transactions very fast. From 2015 India was trading Bitcoin, but it gets a real entry only in November 2016 when government demonetized 86% of paper currency overnight. This was due to people having bulk paper currency of untaxed and black money, were in search of innovative ways for laundering money to avoid government interference and to avoid paying tax. This paved way to buy Bitcoins to conceal their money so that these transactions would not be under security by the government However, India has not had a positive stance towards Bitcoins and other cryptocurrencies. A high-level government panel on virtual cryptocurrencies has recommended a ban on all virtual cryptocurrencies in India. The committee had submitted its report on 23 July 2019, along with a proposed draft bill, Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019.Bitcoin in India is mainly bought from digital currency exchanges like

ZebPay, CoinDelta, CoinSecure, etc., through a credit card. Zebpay even had an Android and iPhone app which allowed individuals to link their bank accounts for quick transfers. There was a KYC requirement and buyers needed to verify their ID by simply clicking a photo of their PAN card.

INVESTMENT OPPORTUNITIES:

The first advocates of Bitcoin did not intend for it to be used as an asset, but with the mushrooming of exchanges where it could be easily purchased and sold, the currency became one. While not with the same approach, traditional investment experts also don't see merit in Bitcoin as an investment. "Certainly for any investment to find a way in to a portfolio, there needs to be a very sound regulation around it, which does not currently exist in the Indian perspective. That's one of the reasons we would not recommend people to put it in to their portfolios. Secondly, for any investment instrument, it's very important that the true value of that instrument can be assessed on the basis of some fundamental factor. What happens today, is when the price of the Bitcoin doubles in three months, for example, there is no fundamental reason that can be associated as to why it doubled.

BITCOIN'S ACCEPTANCE:

One of the biggest problems that cryptocurrencies face is acceptance. However, many businesses have started accepting Bitcoins. One of the largest PC companies in the US, Dell, started accepting Bitcoin in 2014. Travel website Expedia allows you to pay with Bitcoins. e-tailer Overstock.com has also partnered with Coinbase to allow customers to pay with bitcoins. Tech giant Microsoft also embraced bitcoins in December 2014.

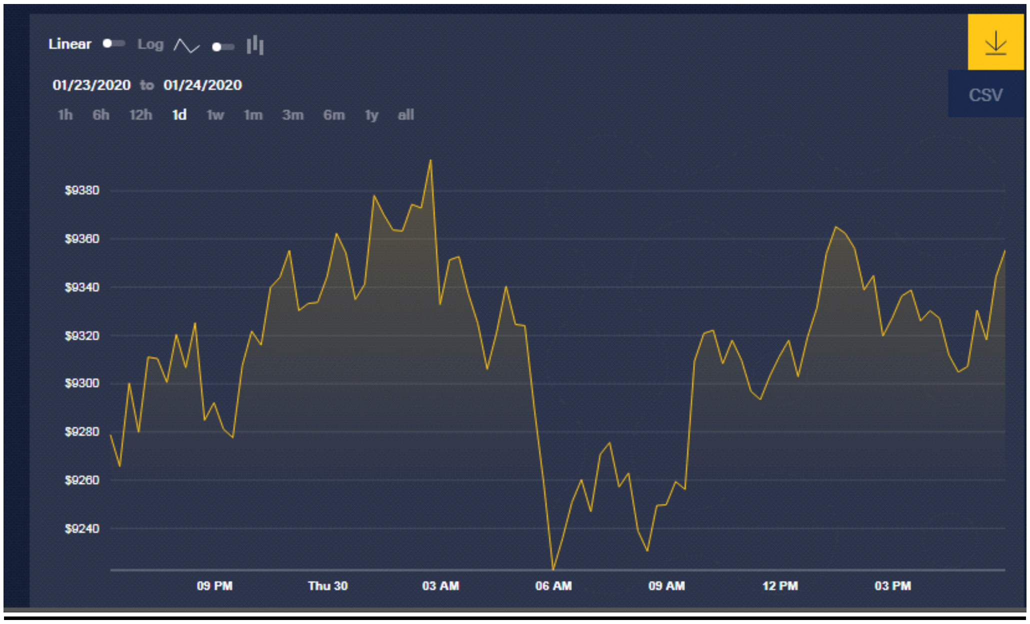

Figure 3: Graph showing the fluctuation in the rates of bitcoin in 24 hours

FUTURE OF BITCOIN:

Bitcoin is a digital currency that has many users. Bitcoins are not real objects, so some people call it an imaginary currency ("Bitcoin and the Future of Money"). Bitcoin transactions are made online and they are all saved in a file called "the Blockchain" (Sparkes, "Bitcoin to launch satellites as global backup").

CONCLUSION

This paper analyzed bitcoin from two perspectives: the user market and the mining market. To achieve the overall objective, the institutional and operational aspects of BTC were analyzed .The interesting result from the user market is a persistent deviation from absolute purchasing power parity despite a bitcoin not being qualitatively different regardless of where and how it is purchased. The second topic called into question the viability of bitcoin as a scalable currency. Bitcoin mining is a competitive market, and so the resources expended line up with the opportunities to earn revenues. We got into Bitcoin because we believe in the power of its technology, and we think it's deeply connected to the rest of computer science. While we've highlighted how seemingly amazing new technology can struggle to displace established institutions, we believe that in the long run, people will continue to find new commercially and socially useful things to do with Cryptocurrency technology.

REFERENCES:

1. Bitcoin and Cryptocurrency Technologies
2. Princeton Bitcoin
3. Crypto Revolution: bitcoin, Cryptocurrency and the Future of Money
4. The Book of Satoshi
5. Artigo64MicroeconomiaAplications
6. Programming Bitcoin
7. Alex Kroeger Essay on Bitcoin
8. www.coindesk.com
9. isaconf.confex.com
10. Towardsdatascience.
11. Cointelegraph.com
12. Bitcoinfuture.weebly.com