r b e

ISSN 0034-7140
DOI 10.5935/0034-7140.20150001
Revista Brasileira de Economia, **69**(1), 3–16

Understanding Bitcoins: Facts and Questions

Bruno Saboia de Albuquerque*, Marcelo de Castro Callado†

Contents: **1. Introduction; 2. Digital Currencies; 3. Criptocurrencies; 4. Proof-of-Work; 5. Double-Spending; 6. Bitcoins; 7. Conclusion; A. Appendix.**

Keywords: **Bitcoins, Digital Currency, Criptocurrency.**

JEL Code: **O33, L86, E40.**

The objective of this work is to do a research challenge about the digital currency named Bitcoins, as well as exploit the general concept behind digital currencies and cryptocurrencies, and enumerate some of its current criticism and problems. Such currencies usage and public knowledge is increasing hastily on the last few months, and many questions arise with its popularity.

O objetivo deste trabalho é promover um desafio de investigação sobre a moeda digital chamada Bitcoins, bem como explorar o conceito geral das moedas digitais e moedas criptográficas, e enumerar alguns dos seus problemas e críticas. O interesse público sobre este tipo de moeda, bem como seu uso, vêm crescendo de maneira acelerada, e diversas questões surgem com o aumento da sua popularidade.

1. INTRODUCTION

The need for exchange is an ancient human characteristic. Since prehistoric times, trading of goods for another goods, services for goods or services for services was present in human endeavor. However, with the increase on the commerce and the exchange needs, the barter become less efficient.

It is known, because of Homer, that silver weights made the exchange easier on the Hellenic civilization, circa IX B.C. According to Passos and Nogami (2003), "the metals were the goods which attributes are closer than those expected for the monetary instruments". Nevertheless, even that system became obsolete after sometime—it was necessary to weight a lot of times to get the value of the ingots, creating difficulties to the official payments, to levy and to commerce itself. Under those circumstances, it was created a "precious metal disk, with a certain specific draw and weight".[1]

Since then, several evolutions has been incorporated to the currencies. The banknotes, for instance, were created, according to Kann (1963), on China, in a gradual process between the Tang dynasty (618–907) and Song dynasty (960–1279). Its creation was because it was a lot easier to create and transport banknotes than heavy cooper coins. If there was a large debt, a great amount of coins was necessary in order to execute the transaction. This difficulty lead to the creation of promissory notes,[2] which then lead to the creation of the state-issued banknotes.

*Bacharelando em Ciências Econômicas, Universidade Federal do Ceará (UFC), Brazil. E-mail: brunosaboia@alu.ufc.br

†Professor Associado, Universidade Federal do Ceará (UFC), Brazil. E-mail: marcelocallado@ufc.br

[1] http://www.angelinicoins.com/#!artigos (our translation)

[2] http://wsulawreview.org/DWhaley.pdf

Marco Polo was impressed on the banknote concept when he visited China. He wrote:

> The method of issue is very formal, as if the substance were pure gold or silver. On each sheet, which is to become a note, specially appointed officials write their name and affix their seal. When this work has been done in accordance with the rules, the chief impregnates his seal with pigment and affixes his vermilion mark at the top of the sheet. That makes the note authentic. This paper currency is circulated in every part of the Great Khan's dominions, nor dares any person, at the peril of his life, refuse to accept it in payment. (Boeykens, 2007)

The beginning of the state-issued banknotes bring some easiness to create inflation. According to Friedman (1970), "inflation is always and everywhere a monetary phenomenon". Therefore, the expansion of money in any form should, in a broad sense, generate a raise in the price level.[3] According to Rogoff and Reinhart (2010, p. 180) "there is no doubt that the invention of printed money has put inflation to a level of relevance without precedents."

When the metal coins were used as a exchange medium, there was a harder situation regarding the creation of currency. Spain suffered from a very high inflation rate, around 300% per annum according to Hamilton (1936) on the Age of Discovery, due to the fact that the crown used a good amount of the silver and gold extracted from the so-called "New World" to the process of coining. But in another locations, and even in Spain itself on a period prior to that, the price level was somewhat constant, and even fell a little bit, according to Adams (1985), due to the fact that the creation of money was never in a sudden and dramatic fashion, making the Iberian country an exception on the period.

The monopoly of bills and coins issuing made the governments able to use inflation as a mechanism to exert their policies and impose their agendas. According to Reinhart and Sbrancia (2011, p.2), the Bretton Woods system allowed a sharp decrease of the public debt/GDP ratio on the period between 1940 to 1970. Also, she points that a combination of a constant inflation dose, not in a very high rate or in a sudden and surprising way to the economic agents, allied to financial repression, is one of the most efficient ways of liquidating one government's debt, and was used by virtually every developed country after the World War II.[4] It is also interesting to note that this policy is only possible if the government has the monopoly of issuing money, and that the currency is a legal tender.[5]

On the gold standard system that, according to Lipsey (1979), begun because there was a broad acceptance of gold as a exchange medium, the governments had an obvious barrier to issue currency, the same mentioned before, and that states face at the medieval times: the extraction of the metal. The gold standard determines that the currency can be exchanged by an equivalent amount of gold, on a preset and fixed ratio. Therefore, the currency has a financial backing: gold. With that, the unrestricted issuing of currency could lead to a exchange of gold, draining the gold reserves of the government adopting those policies. This limits drastically the ability of a government to use inflation to liquidate its own debt, maybe one of the reasons that brought extinction to the gold standard.

Currently, most of the developed and under development countries print currencies without financial backing and in a centralized manner, meaning that only their respective central banks has the power to emit currency, which concentrates a great amount of power to make monetary policies to the government decision makers.

[3] There were a few cases, however, that monetary expansion did not bring out-of-control levels of inflation. The recent US case is an example of it. That generally occurs because there is a strong demand for that currency, even with the expansion. On a general sense, however, it seems that printing bills lead to inflation. Nevertheless, there are some who argue that the models are wrong and inflation is not a monetary phenomenon (see http://pragcap.com/inflation-does-not-appear-to-be-monetary-base-driven and http://www.bis.org/publ/bppdf/bispap77e.pdf).

[4] https://www.imf.org/external/np/seminars/eng/2011/res2/pdf/crbs.pdf, p.6, Box 1.

[5] http://www.merriam-webster.com/dictionary/legal%20tender

2. DIGITAL CURRENCIES

Digital currencies are a relatively modern concept in contrast to the evolutions previously discussed. There is a crucial difference between digital currencies and the currently circulating government issued currencies. First, it is necessary to make a distinction between *digital money* and *digital currency*.

Grignon (2009) asserts that "Digital money is simply the idea that, thanks to technology, money can now be a digital object, a unique serial number that can be directly exchanged anonymously and without accounting, just as one person would hand a dollar bill to another person. You had it. Now they have it. Very simple."

The digital money is already in widespread usage. For instance, when someone does a deposit on a bank account, the system identifies the owner and creates a credit according to the value of the deposit. This money can now be considered digital money, and can be exchanged by real money on an ATM machine, being eliminated on the process, or transfered to another person who can trade it for goods or services through a credit card, or withdraw in as banknotes as said previously.

This is different from the concept of digital currencies. A digital currency is like a real currency, but they are not issued by central banks nor necessarily financially backed in the national currency, as the digital money. Therefore, the issuing is decentralized, and is not decided by politicians, but by technical aspects, usually well-defined. For instance, the bitcoins uses an cryptographic algorithm to generate[6]the currency, which is made by the network users and not by a centralized government body.[7] According to (Melik, 2012), "there are people who like the idea of a currency which bypasses the men in grey suits who have controlled everything until now".

Despite those facts, there are many questions regarding the absence of regulation, and its implications. There are some fear that the digital currencies would make crimes as money laundering or drug dealing more easy.[8] To open a conventional bank account, one needs several documents, such as a valid ID and proof of residence, whereas to register to a digital currency it is only necessary a valid IP address.[9] However, there are several techniques to hide the real IP address, such as using proxies, which make the tracing of bad users more difficult. Regarding that, Melik (2012) says: "That leaves the system open to abuse".

There is also the possibility of electronic fraud affect the bitcoins user. For instance, there is an attack known as "phising",[10] which consist into trick the user to think that he is on a legit website, but actually malicious users are the owners of the website, which then stole data such as passwords. According to (Patil, 2013), "in May 2013, we found a phishing site that spoofed a popular digital currency company". Attacks such as this one make clear that users need training and education in order to not be fooled, and turn the digital currencies world into a fraud paradise.

Recently, Thailand has become the first country to officially ban bitcoins activities, making them illegal in its territory.[11] According to (Trotman, 2013), "the ruling means it is illegal to buy and sell bitcoins, buy or sell any goods or services in exchange for bitcoins, send any bitcoins to anyone outside of Thailand, or receive bitcoins from anyone outside the country".

3. CRIPTOCURRENCIES

Criptocurrencies are a subset of digital currencies. They are also on the set of alternative currencies because they are different from the traditional fiat money, currently in use in most of the countries.

[6]The bitcoin community usually refers to the process of creating new coins as "mining".

[7]https://www.weusecoins.com/en/mining-guide

[8]http://www.bbc.co.uk/news/business-19785935

[9]http://www.ietf.org/rfc/rfc791.txt

[10]http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

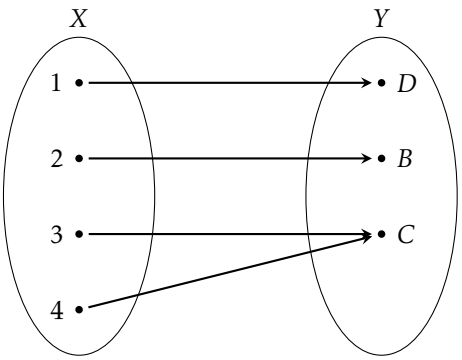
[11]http://www.telegraph.co.uk/finance/currency/10210022/Bitcoins-banned-in-Thailand.html

The term criptocurrency was coined by Wei Dai, in 1998,[12] in an article published on an internet group known as cypherpunks.[13] In a broad sense, the big difference between criptocurrencies and the regular digital currencies is the fact that the creation is decentralized an controlled by a cryptographic mechanism known as *hash function*.

A hash function is, basically, a mathematical function that maps data from variable size to fixed size. On this sense, it is a surjective function, since that the domain will eventually be "depleted", so the mapping will connect a previously connected element on the counter-domain. Formally speaking, let $f: X \to Y$, then f is surjective if

$$\forall y \in Y, \exists x \in X, f(x) = y. \tag{1}$$

Figure 1. Surjection visually demonstrated. Note that element C on the counter-domain is mapped to two elements on the domain, 3 and 4. Since hash functions maps an infinite set into a finite one, surjection will happen.



A cryptographic hash function is similar to a regular hash function, but it should have some elements that make it useful in the cryptography context. One of them is the fact that whatever changes are made on the original data, even a very slight one, generates a very different output. The result yielded by a cryptographic hash function is known as digest. Acording to (Friedl, 2005), "a 'hash' (also called a 'digest', and informally a 'checksum') is a kind of 'signature' for a stream of data that represents the contents. The closest real-life analog we can think is 'a tamper-evident seal on a software package': if you open the box (change the file), it's detected".

Indeed, one of differences between hash functions and other cryptographic functions is the fact that, due to the surjective nature of the hash, it is not possible to determine the generating message from the generated message. On ordinary cryptography, the goal is to scramble one message, and then unscramble it on some other point. In other words, the generating function should be bijective in order to make it work.[14] The bijective functions therefore have an inverse function.[15]

The hash algorithms make it impossible to know the original message from the digest, but they render another kind of attack possible, namely "hash collision".[16] This is due to a mathematical idea called

[12] http://bitcoin.org/en/faq#what-is-bitcoin

[13] http://www.weidai.com/bmoney.txt

[14] For instance, both asymmetric and symmetric encryption techniques supposes that one encrypted message can be decrypted later. See http://support.microsoft.com/kb/246071/en-us.

[15] http://www.mathsisfun.com/sets/function-inverse.html

[16] http://permabit.wordpress.com/2008/07/18/what-do-hash-collisions-really-mean/

the "pigeonhole principle", or "Dirichlet box principle".[17] Despite this being outside of this article's scope, it is important to know the cryptographic principles in order to understand criptocurrencies.

4. PROOF-OF-WORK

According to Nakamoto (2011), the criptocurrencies should use the idea of using hash algorithms to create the so-called "proof-of-work", which means a manner to confirm that there was some kind of computational work involved to create a given quantity of money. On bitcoins, this validation is not made on a centralized way, but instead peer-to-peer (P2P) technology. Therefore, if some change are made to the bitcoin generation protocol, the community should follow it broadly, otherwise it is not considered valid. This concept is analog to what happens on the file sharing network known as "bittorrent": if someones conects to it with a different protocol version, it would not be able to transfer files, unless that there exists more people using that same protocol. Ultimately, what this means is that the rules behind the generation of bitcoins is community-driven.

The proof-of-work is where the generation of bitcoins lies. According to Dai (1998), "anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual".

Proof-of-work is a key concept to bitcoins and cryptographic currencies in a broad sense, since it prevents undiscriminated issuing of the currency, which would turn it into an impractical idea.

5. DOUBLE-SPENDING

Only the proof-of-work is not enough to enforce the correct transaction flow on crytpocurrencies. On the conventional ones, this flow occurs in a trivial way. Let A and B be two imaginary persons. Whenever a payment is made, person A gives the money to person B and should receive the expected goods or services for that amount. It is now impossible to person A to spend the same banknote with a distinct operation, since the physical bill is not in possession of him anymore.

However, the conventional bills can be counterfeited. With physical bills, the solution by the issuing body is to make counterfeiting hard, since they have the printing monopoly. Obviously, digital coins have the same issue. Generally, it is used a centralized model, where a central authority validates the transaction, or grants the right to another institution to do it. This occurs, for instance, with banks. They have the authorization of some monetary institution, like the central bank, to make those transactions, which are accepted by the system, in an operation known as clearing.[18]

The double-spending is the analog concept to counterfeiting on physical money, but for digital currencies. For criptocurrencies, it is necessary to verify, whenever you receive an unit of money, if that same unity, represented by a hash, was used by the same person on a different transaction.[19] Namely, even if someone knows a valid hash, is necessary to verify the real owner of the hash.

Cryptocurrencies can solve this problem with two approaches: centralized or decentralized. Each currency implements its own solution to the problem. According to Nakamoto (2011), bitcoins uses a decentralized methodology. Each transaction is recorded, and it is propagated by the P2P network. This avoids that some specific node has significant importance on the process of exchanging bitcoins.

[17] http://www.math.ucsd.edu/ jverstra/dirichletbox.pdf

[18] https://www.ecb.europa.eu/pub/pdf/other/glossaryrelatedtopaymentclearingandsettlementsystemsen.pdf

[19] This of course does not imply that one user cannot use the same hash twice. If he spends the money, and then receive the same money in the future, he can receive it. What he cannot do is to spend the same hash twice at the same time.

6. BITCOINS

6.1. Overview

Bitcoin is a criptocurrency.[20] It is the first real implementation of the initial idea from Wei Dai, that he firstly called B-Money. One of the key concepts to bitcoins is the decentralization. As mentioned before, this is possible by using the P2P protocol, that creates an autonomous transaction and proof-of-work verification network. It is also the most widespread used currently.[21]

Next the previously enumerated concepts will be analyzed, but in a specific fashion in relation to its implementation on the bitcoin protocol, and also another aspects related to the currency.

6.2. Double-spending

On bitcoins, the double-spending is avoided by verifying the public ledger, which is a bookkeeping of the transactions made with bitcoins since its creation. This inquiry is also decentralized using the P2P network. Therefore, all the transactions with a given bitcoin can be traced back to the moment of its creation.[22]

Obviously, this implies on the problem of defrauding the block chain[23] itself. Some malicious agent can modify the block chain in its own benefit. Again, the solution to this problem is act decentralized, which is a central idea on the concept of bitcoins. According to King, Williams, and Yanofsky (2013), "the first thing that bitcoin does to secure the ledger is decentralize it. There is no huge spreadsheet being stored on a server somewhere. There is no master document at all".

Actually, the ledger is split in two parts. Each block contains the activity of transactions from until 10 minutes ago. King et al. (2013) says that "the ledger is broken up into blocks: discrete transaction logs that contain 10 minutes worth of bitcoin activity apiece. Every block includes a reference to the block that came before it, and you can follow the links backward from the most recent block to the very first block, when bitcoin creator Satoshi Nakamoto conjured the first bitcoins into existence".

Also, it is necessary to digitally sign the transactions, which means that there must be a hash algorithm validating the transaction, and then it is added to the block and distributed on the P2P network, and therefore the other miners[24] will know the existence and attest or not the validity of the transaction. If there is an attempt of inserting an invalid transaction on the block, it will be refused by the other network nodes. Hence, most of the nodes must adhere to a new protocol in order to be accepted as a valid change.[25] That shows how important is the concept of decentralizing on bitcoins concept.

6.3. Proof-of-work

The proof-of-work on bitcoins is given by creating a digest produced by an algorithm created by the NSA known as SHA-256C.[26] This is algorithm receive a string (objects that represent sequences of characters) with an arbitrary size, and returns a string with 64 characters. For instance, the string "`Bitcoins`" generates the following digest:[27]

```
aa0921d24d095df038a0c0a32eb0d644f1882e3a0a3d8814175c4e1cebbf84fb
```

[20] http://bitcoin.org/en/faq#what-is-bitcoin

[21] http://www.forbes.com/sites/reuvencohen/2013/11/27/the-top-30-crypto-currency-market-capitalizations-in-one-place/

[22] http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

[23] The public ledger containing all transactions. See https://blockchain.info/wallet/bitcoin-faq.

[24] Computer program that is designed to execute the algorithm to generate bitcoins.

[25] This concept is analogous to what happens on the popular file transfer network, bittorrent.

[26] http://tools.ietf.org/search/rfc4634
http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf

[27] http://www.cplusplus.com/reference/string/string/

While the string "cryptocurrencies" generates the following digest:

```
471a97f90b5df17b2f4a79d40f5d5d73fd6c46df96b34d2334c68aea90a8494b
```

The digests generated by this algorithm are on the hexadecimal format.[28]

On the bitcoins protocol, there is a rule that is necessary in order to generate a valid hash: it must possess a certain amount of leading zeros. The actual amount of zeros determines the difficulty level: the bigger the number of leading zeros needed, the harder is to find a valid result. This difficult is automatically adjusted by the network itself, according to the mining rate.[29] Therefore, none of the previous hashes are actual bitcoins: the first one starts with "aa0" and the second one starts with "471". If the difficulty is low, then a low number of leading zeros is needed to compose a valid bitcoin. For instance, the difficult can be to find only one leading zero, then any string on the format "0…" is valid, whereas if the protocol only authorizes two zeros, then a valid hash should follow the pattern "00...". Since the string size is fixed on 64 characters, each additional leading zero diminish the total number of possibilities, therefore making the mining process more difficult.

This is the general concept, but in practice it works slightly different. The input string is the previous transaction block, to which is added a random number with the intention of changing the resulting hash. This number is called *nonce*.[30] The idea behind the nonce is to generate a completely different hash. As we seen before, any minor change on the input string should result on a very different hash. For instance, let "Hello World!0" be our input string. Applying the SHA-256 algorithm to this string, the following hash will be yielded:

```
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
```

If there is a minor change on the end of the string, replacing the "0" for a "1", the new string will be "Hello World!1". This new string will result in the following hash:

```
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
```

None of those hashes is valid as bitcoins, because they do not start with zeros.

Let x be the ending number. If we keep incrementing x by one, we will eventually find a valid bitcoin. Suppose that the difficult is set to three leading zeros. Then we are looking for a hash such as

$$H = \text{SHA256}(\text{"Hello World!"} + x) \mid H = \text{"000…"}$$

Starting with $x = 1$, the following hashes will be yielded:[31]

$$\begin{aligned}
\texttt{Hello, World!1} &\Rightarrow \texttt{1312af…}\\
\texttt{Hello, World!2} &\Rightarrow \texttt{e9afc4…}\\
\texttt{Hello, World!3} &\Rightarrow \texttt{ae3734…}\\
\vdots \quad & \quad \vdots \quad \Rightarrow \quad \vdots\\
\texttt{Hello, World!4248} &\Rightarrow \texttt{6e110d…}\\
\texttt{Hello, World!4249} &\Rightarrow \texttt{c00419…}\\
\texttt{Hello, World!4250} &\Rightarrow \texttt{0000c3…}
\end{aligned}$$

[28] http://mathworld.wolfram.com/Hexadecimal.html

[29] This rate can be defined as how much bitcoins will be mined on a given period of time.

[30] https://en.bitcoin.it/wiki/Proof_of_work

[31] The results were truncated to the first 6 characters. The complete hashes, with 64 characters, can be calculated at http://www.xorbin.com/tools/sha256-hash-calculator.

So, the nonce 4250 outputs a valid bitcoin. An interesting fact about this is that the previous nonce, 4249, generates what one can perceive as an "almost" valid bitcoin, because its leading pattern is "`c00`". This does not means that this number is actually "closer" to a valid bitcoin than any other non-valid nonce. Each additional attempt of mining a valid bitcoin does not leaves one "closer" to get a valid hash. This is analog to rolling a 6 faced dice $n-1$ times without getting a 3, and expect to have a greater chance of rolling a 3 in the nth throw. This is a fallacy, known as "Gambler's Fallacy".[32]

This is a very simplified explanation of how the proof-of-work is operated on bitcoins. In reality, the protocol is more complex than that, and the blocks have a predefined format, which is part of bitcoins protocol.[33]

6.4. Privacy

On the bitcoins protocol, there is the possibility of encrypting the transactions, making more difficult or practically impossible to determine the source or the destination of the transaction. This is done throughout the concept of private and public keys. Despite this fact, this is not an intrinsic characteristic of the protocol, and is up to the parties involved in the transaction to determine whether it will be encrypted, since all transactions are publicly available on the chain block, as mentioned before.

Regular banks protect this kind of information using their own software. On the bitcoins protocol, this is up to the users. Despite that, there is a strong correlation between bitcoins and anonymity. According to Reid and Harrigan (2011), "anonymity is not a prominent design goal of Bitcoin. However, Bitcoin is often referred to as being anonymous. We have performed a passive analysis of anonymity in the Bitcoin system using publicly available data and tools from network analysis. The results show that the actions of many users are far from anonymous".

Obviously, anonymity concerns the governments, because it makes difficult to trace criminal action such as drug dealing, and make easy to avoid taxes. The Silk Road website allowed users to buy drugs in some sort of auction.[34] A lot of criticism was made to bitcoins because it diminishes the risk and facilitates access to the so-called black markets.[35]

6.5. Regulation

Despite the fact of association with bitcoins and its illegal usage, the regulation upon it is relatively weak. Recently, the Singapore government became the first one to give instructions on how bitcoins will be taxed, which was a pioneering act, since most of the governments are not clear regarding this issue.[36]

As mentioned before, Thailand was the first country to ban bitcoins activities, but other countries seems permissive in regarding to the use of the currency. In Brazil, for instance, some stores accept bitcoins.[37] Those questions are not completely clear, but the discussion caused by bitcoins will probably bring the governmental attention to the matter.

[32] http://www.nizkor.org/features/fallacies/gamblers-fallacy.html

[33] https://en.bitcoin.it/wiki/FAQ#How_does_the_proof-of-work_system_help_secure_Bitcoin.3F

[34] http://www.theatlantic.com/technology/archive/2011/06/libertarian-dream-a-site-where-you-buy-drugs-with-digital-dollars/239776/

[35] http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

[36] http://venturebeat.com/2014/01/10/singapore-clarifies-tax-on-bitcoin-exchanges-and-sales/

[37] http://lojabitcoin.blogspot.com.br/

6.6. Supply cap

Since the maximum number of hashes that are valid as bitcoins will diminish with the ongoing mining, there will be a moment that all mined out, and therefore creation of new coins will be impossible. This event will occur in some date circa 2140, and then it will be 21 millions of bitcoins in the economy.[38]

As the proof-of-work is the only effective way of generating bitcoins, and since there is a maximum amount of bitcoins, an inflationary outbreak seems unlikely. Unlikely the conventional fiat money, which makes possible for the government to take arbitrary decisions that create inflation, the bitcoins are generated according to a mathematical model that allows precise predictions regarding the amount of the supply on a given period time.

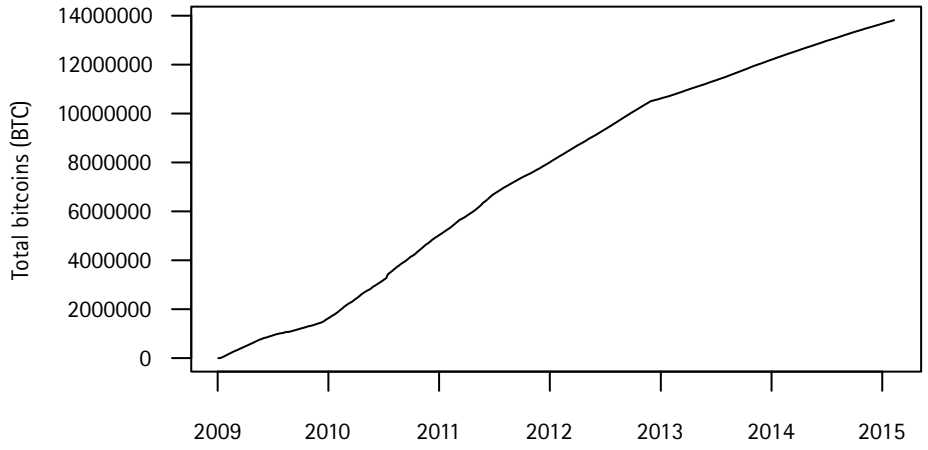
6.7. Deflationary spiral

Deflationary spiral is a situation "where falling prices, defaults, bankruptcies, and falling wages reinforce each other in a continuous cycle".[39] Hypothetically, this could lead to the complete failure of an entire economic system.[40]

Since bitcoins have a limited amount, there were concerns that a deflationary spiral would be inevitable, because the holders of the money would hold it, since the deflation means that the money will have a greater value in a future time. However, according to Roberts (2011, as cited in Simonite (2011)), "(deflation) is considered very destructive in today's economies, mostly because when it occurs, it is unexpected (but) in a Bitcoin world, everyone would anticipate that, and they know what they got paid would buy more then than it would now".

What can be expected on currencies with well-defined supply limits differs slightly from what happens with traditional fiat money. According to Simonite (2011), "the consequence will likely be slow and steady deflation, as the growth in circulating bitcoins declines and their value rises".

Figure 2. Bitcoins growth rate is almost linear: total bitcoins in circulation. (Source data: blockchain.info)

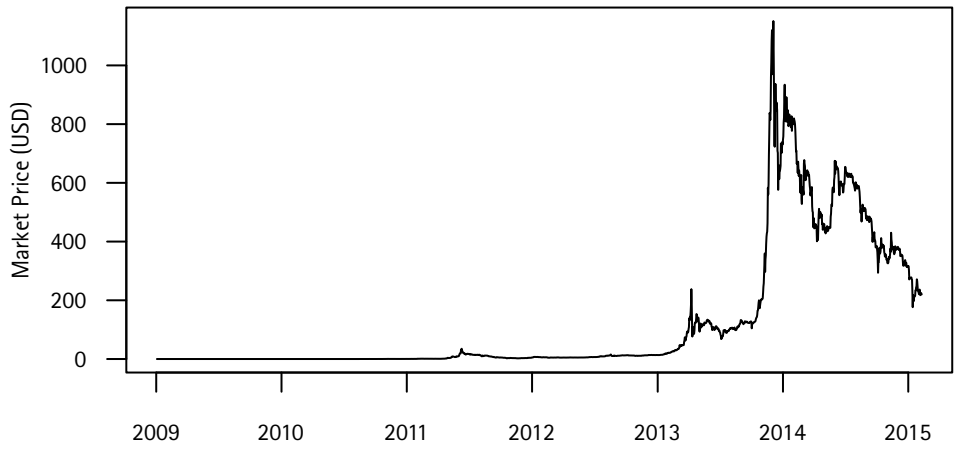


[38] https://en.bitcoin.it/wiki/Bitcoin

[39] http://snbchf.com/economic-theory/deflationary-spiral/

[40] http://web.mit.edu/krugman/www/spiral.html

Figure 3. Bitcoins had a strong appreciation against the US dollar: Market Price (USD). (Source data: blockchain.info)



6.8. Criticism

Some experts were harsh on criticizing bitcoins. Nevertheless, there is a lot of misunderstanding involving the bitcoins concepts. The president of the north-american company PayPal, David Marcus, said that bitcoins is not a currency.[41] However, even amongst those who do consider bitcoins as a currency, there is some criticism.

One of the points is that the bitcoins generates a huge waste of computational resources. The estimated processing power of the bitcoins network is 130 petaflops.[42] The computational power of the FoldingHome project, which simulates the folding of proteins for medical research, is around 12 petaflops.[43] In Iceland, there is a giant data center which only goal is to mine bitcoins.[44] Therefore, the central argument lies in the assumption that such power could be used with other intentions. Indeed, some criptocurrencies do use part of the processing power for other ends. For instance, Gridcoins transfer part of the miner's processors to scientific calculations,[45] through the BOINC network.[46]

Another source of criticism regards the transaction costs with bitcoins. According to the critics, there is lack of knowledge regarding the mechanics of that costs, which leads many uses to believe that transactions are free. Actually, according to Levine (2014), "as of today miners took home about 3.5 percent of the value of transactions that they processed. Which is more than credit card companies".

As mentioned before, there is also those who says that bitcoins enhance the black market and outlaw activities such as money laundry, and also that the criptocurrency is more useful to criminal then to ordinary people. Furthermore, they say that bitcoins create a kind of "criminal paradise".[47] Also, they say that bitcoins is not immune to stealing. Recently, a website which intent was to sell drugs had

[41] http://venturebeat.com/2013/12/10/paypal-president-on-bitcoin-i-dont-think-it-is-a-currency/

[42] A petaflop is a measure of processing power, and is defined as one thousand trillion operations with floating points per second. See http://petaflop.info/.

[43] https://folding.stanford.edu/home/past-the-10-petaflop-scale/

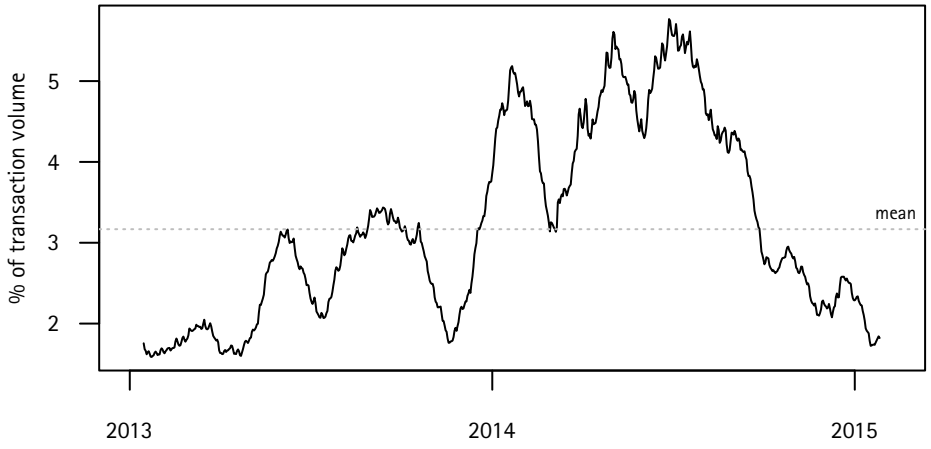
[44] http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?_r=0

[45] http://www.gridcoin.us
http://bitcoinmagazine.com/13187/putting-the-blockchain-to-work-for-science-gridcoin

[46] http://boinc.berkeley.edu

[47] http://www.businessinsider.com/bitcoin-libertarian-paradise-would-be-hell-on-earth-2013-12

Figure 4. Transaction costs in bitcoins as a percentage of transaction volume—30-day moving average. (Source data: blockchain.info)



more than 100 million US dollar worth of bitcoins stolen.[48] There was also an incident in China where 5 million US dollars worth of bitcoins vanished from a platform known as GBL (Global Bond Limited). The creators of the platform allegedly did it deliberately, effectively stealing their client's money.[49] Those are not isolated incidents, but one of the main causes of problems regarding security is the lack of proper actions by the user themselves. Similarly to other online operations, is necessary to handle bitcoins transaction with proper care.

In March 2014, Autumn Radtke, First Meta's CEO, allegedly committed suicide in her private domicile in Singapore. According to the English news website, *Daily Mail*, "The death of Radtke is the latest piece of bad news to hit the crisis-ridden bitcoin currency following the collapse of the Japanese-based Mt Gox exchange last week after $400m went missing and the closure of the Flexcoin bank yesterday in Canada after computer hackers robbed $600,000".[50]

Criptocurrencies in general were also criticized on money laundering grounds. According to Marian (2013), "as demonstrated by recent events, virtual currencies present regulators with significant challenges. On May 23, 2013, the U.S. federal government brought an indictment against the operators of Liberty Reserve, a popular virtual currency, charging the operators with money laundering and operating an unlicensed money-transmitting business". On the specific case of bitcoins, the question of whether it facilitates or not the evasion of taxes is open, but some even call the criptocurrency a "tax haven[51] or "the ultimate offshore bank account".[52]

According to those critics, bitcoins, unlike the traditional tax havens, are harder to uncover because they lack the necessity of having a bank, therefore they are anonymous and harder for a government to track.[53] In light of those facts, Marian (2013) says that he believes that "tax-evaders—under the threat of the new regime—may soon abandon traditional tax-haven jurisdictions in favor of cryptocurrencies".

[48] http://www.businessinsider.com/220-million-sheep-marketplace-bitcoin-theft-chase-2013-12

[49] http://rt.com/business/banshee-bitcoin-vanish-china-601/

[50] http://www.dailymail.co.uk/news/article-2573863/Bitcoin-exchange-CEO-dead-home-suspected-suicide-age-28.html#ixzz3C50UTYu6

[51] http://www.politico.com/story/2013/08/bitcoin-tax-haven-95420.html

[52] https://economicsandliberty.wordpress.com/2011/08/23/bitcoin-the-ultimate-offshore-bank-account/

[53] http://www.dailydot.com/business/bitcoin-offshore-tax-haven/

Nevertheless, this is not currently a problem for policymakers, but should become one in the future. As Marian (2013) exposes it, "given the small volume of the current Bitcoin market, it is hard to imagine that the tax evasion associated with it is of any real significance. Most commentators, however, expect the markets of Bitcoin and other cryptocurrencies to grow over the next few years". Since the professor's assumption that "cryptocurrencies offer, at least theoretically, a near-perfect alternative to tax-evaders who can no longer find a safe haven in tax-haven jurisdictions" (Marian, 2013), governments must prepare for the challenge of adapting their tax collection plan in a world in which criptocurrencies are a commonplace.

7. CONCLUSION

The concept of cryptocurrencies, despite being new, is a subject that has an increasing attention. There are many open questions regarding those currencies. The purpose of the present work is to mitigate, at least superficially, most of the common questions about this new format of money.

Despite not being the only cryptocurrency, bitcoins has been the most successful one in terms of generating public attention. Maybe one of the reasons for that is because it was the first one to be used in a considerable scale. Some stores already accept it, and even large companies, such as Dell, are beginning to accept bitcoins,[54] which clearly makes the cryptocurrency a predecessor. Many other currencies where created after bitcoins. Some of them suffer from the same problems, and others have advantages that bitcoins do not possess. It is hard to foresee which of those will succeed, but we can consider the bitcoin a relatively success in terms of its usage and the news volume that it generates.

It was also possible to determine that bitcoins will have a minor deflationary characteristic. Deflation is a subject that raise concerns upon many economists, since it had devastating consequences to the Japan's economy on the 1990 decade, for example. According to Ito and Mishkin (2004, p. 2), it was a lost decade for the Asian country. Nevertheless, as discussed, bitcoin's deflation should be small and predictable, and therefore it does not seems to be a structural problem within the currency.

We also observed a lot of criticism to the widespread usage of bitcoins. There is almost a dichotomy between those who thinks that bitcoins will solve a lot of current problems in the economic system created by fiat money, and those who thinks that cryptocurrencies like bitcoins have a highly destructive potential to society itself.

REFERENCES

Adams, C. (1985, Oct.). What happend to all the gold Spain got from the New World? *The Chicago Reader*. Retrieved from http://www.straightdope.com/columns/read/611/what-happened-to-all-the-gold-spain-got-from-the-new-world

Boeykens, C. (2007, Sept.). Paper money, a Chinese invention? *Museum of the National Bank of Belgium*. Retrieved from http://www.nbbmuseum.be/2007/09/chinese-invention.htm

Dai, W. (1998). b-money: A scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help. *weidai.com*. Retrieved from http://www.weidai.com/bmoney.txt

Friedl, S. (2005, May). *An illustrated guide to cryptographic hashes.* unixwiz.net: Steve Friedl UNIXWIZ.NET. Retrieved from http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Friedman, M. (1970). *The counter-revolution in monetary theory*. Transatlantic Arts.

Grignon, P. (2009, June 17). *Digital coin in brief.* Retrieved from https://archive.org/details/Digital_Coin_in_Brief_07-17-09

Hamilton, E. J. (1936, Dec.). Money, prices and wages in Valencia, Aragon and Navarre, 1351–1500. *Journal of the American Statistical Association*, *31*, 800–802.

[54] http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing

Ito, T., & Mishkin, F. S. (2004, Oct.). *Two decades of Japanese monetary policy and the deflation problem* (NBER Working Paper 10878). Cambridge, MA: National Bureau of Economic Research. Retrieved from http://www.nber.org/papers/w10878.pdf

Kann, E. (1963). *kann's history of Chinese paper money (ancient)* (Vol. I). International Banknote Society.

King, R. S., Williams, S., & Yanofsky, D. (2013, Dec. 17). *By reading this article, you're mining bitcoins.* Retrieved from http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins

Levine, M. (2014, Jan. 2). bitcoin is an expensive way to pay for stuff. *BloombergView*. Retrieved from http://www.bloombergview.com/articles/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff

Lipsey, R. G. (1979). *An introduction to positive economics* (5th ed.). Weidenfeld & Nicolson.

Marian, O. (2013, Oct. 1). Are cryptocurrencies super tax havens? *112 Michigan Law Review First Impressions*, *38*. Retrieved from http://ssrn.com/abstract=2305863

Melik, J. (2012, Oct. 2). Digital currency: Brave new world or criminal haven? *BBC: Business Daily*. Retrieved from http://www.bbc.co.uk/news/business-19785935

Nakamoto, S. (2011, Sept.). *Bitcoin: A peer-to-peer electronic cash system* (Tech. Rep.). www.bitcoin.org. Retrieved from http://bitcoin.org/bitcoin.pdf

Passos, C. R. M., & Nogami, O. (2003). *Princípios de economia*. Thomson.

Patil, A. (2013, June 25). Phishers claim to ensure security for digital currency users. *Symantec: Security Response Blog*. Retrieved from http://www.symantec.com/connect/blogs/phishers-claim-ensure-security-digital-currency-users

Reid, F., & Harrigan, M. (2011, Sept. 30). *bitcoin is not anonymous.* Fergal Reid's blog. Retrieved from http://anonymity-in-bitcoin.blogspot.com.br/2011/07/bitcoin-is-not-anonymous.html

Reinhart, C. M., & Sbrancia, M. B. (2011). *The liquidation of government debt* (NBER Working Paper No. 16893). Cambridge, MA: National Bureau of Economic Research. Retrieved from http://www.nber.org/papers/w16893

Roberts, R. (2011, Apr. 4). *Andresen on bitcoin and virtual currency* [interview (podcast)]. Retrieved from http://www.econtalk.org/archives/2011/04/andresen_on_bit.html

Rogoff, K. S., & Reinhart, C. M. (2010). *Oito séculos de delírios financeiros* [This time is different: Eight centuries of financial folly]. Rio de Janeiro: Campus Editora.

Simonite, T. (2011, May 25). What bitcoin is, and why it matters. *MIT Technology Review*. Retrieved from http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters

Trotman, A. (2013, July 29). Bitcoins banned in Thailand. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/finance/currency/10210022/Bitcoins-banned-in-Thailand.html

A. APPENDIX

A.1. Terminology

Since this paper deals with a relatively new concept, the naming of the involved terms is not completely accepted, established or well-defined. There were a significant effort to use the current naming from the community, but without a strict formal concert about the terms.

Some literatures bring the term virtual coins on the same meaning that the present paper uses for digital coins (or even digital currencies), on the terms of a non-physical variation of fiat money. Actually, for the community, the concept of virtual coins is associated with online gaming, like World of Warcraft, and therefore have completely distinct characteristics from those mentioned.

A.2. Sources

Most of the content regarding bitcoins are available on the internet. There are few academic research on the subject. Besides, since bitcoins brings a lot of new concepts to currencies, the subjects discussed on this paper suffer from constant update and change. This may lead to probable discrepancy between what is said here and what the sources actually said.