BITCOIN, CURRENCY OF THE FREE MARKET

Dragoș-Iulian UDREA[1]

Abstract: *The purpose of this article is to present Bitcoin as a possible solution to many of the issues caused by having money administered by a monopoly. The introducing chapters of this article focus on demonstrating why monopolistic control over money will always limit freedom. Specifically, in regards to how the government has control over individual freedom through money. History has shown that people have sought ways to curb this kind of intervention on markets and in their lives - with Bitcoin being a result of their efforts. In the later chapters we aim to demonstrate why Bitcoin is such a significant step towards achieving a higher degree of individual freedom and we will support these claims through a series of technical, economical and philosophical arguments.*

Keywords: *bitcoin, cryptocurrency, free market, freedom.*

Introduction

It can be seen throughout history that the government has sought to exert control over markets, each time having a negative effect on their course and, by extension, on people's lives. People are put in an unpleasant situation, in which they must accept the rules of the game between the market and the government, because the main unit of action within it, money, aims to be liberalized[2] on one hand, and monopolized on the other. For the longest time and up to our present day, people are subject to the government's decision involving money[3]. Any consequences that arise from these decisions are the people's responsibility. The government's involvement in the markets and in our lives has been questioned time and time again. However, in the last few decades, significant improvements have been seen to what could potentially lead to completely excluding the government from all matters involving our money.

---

[1] M.A in Philosophy, University of Craiova.

[2] John Locke, *Second Treatise of Government*, C. B. Macpherson (edit.), Hackett Publishing Company, Inc. Indianapolis, Cambridge, 1980.

[3] Murray Rothbard, *What Has Government Done To Our Money?*, Ludwig von Mises Institute, Alabama,1991, p. 1.

A possible solution comes in the form of bitcoin[4], the popular and highly mediatized cryptocurrency that has been making waves on the internet for the last few years. There is more to bitcoin than slogans and headlines, and this article will bring into discussion the more technical, liberty-driven side of it. Ever since their conception, cryptocurrencies have always found a home among those communities that are skeptical of authority. Political activists, hackers, all those that were proponents of personal freedom, were enthusiastic about the potential of cryptocurrencies. However, back then, it was far from being realized, due to technological limitations and societal reasons. This would not last for long, as less than a decade later, cryptocurrencies would break into the mainstream and gain international attention through bitcoin. Most people may have heard about the substantial amount of dollars that a bitcoin is valued at. However, bitcoin's most important asset is that it has managed to jumpstart an idea in people's mind - that money can truly be free.

It is worth analyzing this side of bitcoin and to discover how computer science, economy and politics are merged into one framework that might potentially solve one of society's troubling issues. To better understand bitcoin, we must first understand the problems that it tries to address, specifically those related to money, right down to individual transactions made in physical and digital currency.

Against Fiat Money

Physical currency is exchanged from hand to hand, with people having control over the money they hold and the purpose it's meant to serve. While we own the specific amount of money, we are never in control of its actual value[5]. Instead, this is determined or highly influenced by the actions of a third party - be it a bank or, by extension, a government. Digital currencies function in a similar way and naturally share the same shortcomings as fiat. However, instead of existing in people's hands and wallets, digital currencies exist in data servers and terminals. This brings a new issue into question, that digital money is always kept by a third party. And as the world steers more and more towards using digital currencies, this problem only seems to become more prevalent. No matter how much

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org, 2009, pp. 1-9.

[5] Murray Rothbard, op. cit., p. 33.

we like to think that we are in control of our wealth, it is not a complete form of self-determination. There will always be a governing entity that will have the last word in matters involving money[6] - making it seem that money is under a dictatorship rather than a democracy. Many of society's woes can be attributed to this overreaching control of our wealth. Economic crises, inflation, corruption and general unrest have been by and large a byproduct of this kind of mishandling[7] - which for a long time has exceeded its intended purpose. People have been aware of this entrapment for the longest time and are constantly looking for ways to get out of it - to protect their wealth from the arm of the government.

Cryptocurrencies might be the solution that they are looking for - with bitcoin being the symbolic key to the free market, as it aims to give self-determination back to the people, allowing them to manage their wealth as they see fit. It was made as a reaction to the centralized nature of money and the entire baggage of flaws that come with it. It was also designed as a means to liberate day to day transactions from the watchful and intrusive presence of an intermediary party. It manages to do all of this by virtue of how it was conceived - with the intent to democratize transactions and eliminate the need of a middleman. In the following chapters we will explore how bitcoin came to be and how it succeeds to provide financial freedom. It is by no means a perfect instrument, as it has its fair share of valid critiques. However, at its core lies an idea that is definitely worth taking in consideration.

History of Bitcoin

The history of cryptocurrencies as we know them today can be traced back to the late 90's - in 1998. Back then, an anonymous programmer and crypto-anarchist[8] under the pseudonym Wei Dai, made the first attempts to merge cryptography and digital currencies into a unitary concept. This project came in the form of B-money[9], a rudimentary form of cryptocurrency that served as the precursor to bitcoin. The intention behind this development

[6] *Ibidem*, p. 2.

[7] Ludwig Mises, *The Theory of Money and Credit*, Yale University Press, London, 1953. p. 97.

[8] Timothy C. May, *The Crypto Anarchist Manifesto*, www.activism.net, 22 November 1992.

[9] Wei Dai, *B-money*, http://www.weidai.com/bmoney.txt, 1998.

was for it to be used as a monetary system inside an insular economy - which was mainly composed of programmers and economists that shared similar libertarian ideals.

At that time, the effort behind B-money, as well as the system itself was considered revolutionary and lauded, albeit in a hushed manner, by different communities around the still emerging internet. Users of B-money praised it for its core feature - the anonymity - that it provided. This was in stark contrast to other digital currencies at the time, which relied on third parties or centralized systems in order to facilitate transactions. However, B-money's lifespan would ultimately turn out to be very short as multiple problems arose after its implementation. The fact that it was not regulated by a centralized body also proved to be B-money's greatest shortcoming, as it was marred by poor functionality and numerous technical issues. For starters, for it to function, users required a hefty bit of computer know-how, which was something novel for the time. Besides that, completing a transaction was a laborious task, requiring a series of confirmations from both parties that were engaged in the trade. The lack of an administrative body meant that B-money was also 'left to the wind' in terms of security, proving itself to be easily exploitable. Such vulnerabilities tarnished the image of B-money as a potentially viable monetary system and ran it completely into the ground. It was ultimately discontinued, however, it proved itself to be ground-zero for the prospect of a decentralized monetary system.

Along the years, many programmers, economists and libertarian activists would try to perfect the cryptocurrency formula. The turning point for this would come on 31 of October, 2008 in a computer science forum. A user on the forum, who went by the name of Satoshi Nakamoto, published the white paper for the first version of bitcoin, titled *"bitcoin: A Peer-to-Peer Electronic Cash System"*.[10] Through this publication, Nakamoto would offer solutions to the problems that impeded cryptocurrencies for so long - which were the lack of security, functional tracking and the dilemma of double-spending. On top of that, Nakamoto would also publish the entire code that ran bitcoin, as open source - allowing for everyone to see the inner workings of the system. The groundwork was laid for cryptocurrencies and it was indisputable proof that they were indeed viable to be used as monetary systems. Time would be the best indicative

[10] Satoshi Nakamoto, op. cit., pp. 1-9.

of this, as shortly after, in 2009, bitcoin would gain rapid adoption within the crypto community. Along the years it would have a meteoric rise, gaining worldwide attention and becoming the poster child for the cause of libertarianism and the free market.

Technical aspects of Bitcoin

Bitcoin has managed to solve five fundamental issues that made people question the validity of cryptocurrencies - the *"double-spending"* problem, anonymity, maintenance of the system, accountability of transactions and volume. The obvious solution to these problems would be to have an administrator that keeps everything in check, yet the technology behind bitcoin has managed to completely replace the need for this with a more favorable alternative[11].

The double spending problem. It is achieved through a technology called blockchain, whose purpose is to decentralize how bitcoin operates. In computer science terms, it is a peer to peer system. This type of system functions through the collective effort of users who are *"equally privileged, equipotent participants in the application"*. This means that all the users engaged in the system maintain the same information. Once new information is added, it is updated for all users. Once this information is written-in, it cannot be altered since it is compared to all existing records of it. This prevents individual users from editing information in their favor. In broad terms, through this democratized implementation, bitcoin's blockchain technology has made it so that once a new entry has been recorded in the system - a transaction - it can no longer be duplicated - spent twice by the same user. It is technically impossible to alter the reality of the blockchain, unless the records from all users are altered. Through this method, bitcoin provides a solution to the problem of *"double-spending"*, preventing the same bitcoin to be used twice by the same user, as once it is used, it would be removed from one user and credited to the other.

Anonymity. Users engaged in bitcoin's system are completely anonymous, as the main system does not require any personal information from its users. Instead, it identifies users and stores their bitcoins through their wallet and public key. Together, these two come to create a user's

[11] Kevin Dowd, *New Private Monies – A Bit Part Player*, Hobbs the Printers, Institute of Economic Affairs, London, 2014, pp. 40-41.

bitcoin account that facilitates transactions. The wallet is the medium through which bitcoins in possession are stored. This wallet carries a numeric key that is known as a public key which allows the user to identify, initiate and link to other users' accounts, precisely in order to start a transaction. The public key system works like an e-mail system, in which information is sent from one address to another. This means that when two users want to participate in a transaction, they would share the public key between each other. The public key itself is displayed as a series of characters and by its tangled nature, it is difficult to remember or to associate with a person. People in day to day transactions don't identify each other by their credit card number. To add to this layer of anonymity, bitcoin also employs the use of a private key, which unlike the public key, is meant to be kept hidden and only known by the owner of a wallet. The private key system works like an electronic password system, where the owner must remember a password that grants access to a system - in this case, it is used to access the wallet and validate a transaction. It is necessary for a private key to not be lost, because due to the anonymization of the system and the lack of a central administrator, it can no longer be recovered.

Maintenance. As the public ledger accrues more information about transactions, it becomes more difficult to maintain, requiring more computational power. Those that lend computational power are awarded a sum of bitcoin. This maintenance process requires that the system be kept active, permanently turned on, and updated. The maintenance of the system must be done in such a way as to provide space for each user who wishes to participate in it. Then, another maintenance objective is to verify and update the transactions made, in order to determine if they are valid. Therefore, users who choose to maintain the system, invest their electricity and processing power for the smooth running of the entire system, and for this, they are automatically awarded a sum of bitcoin. By virtue of this design, bitcoin does not need a centralized network to run on.

The accountability or transparency of transactions. Bitcoin employs the use of a system known as the public ledger, which allows users to verify transactions that have been made. Through this system bitcoin ensures fairness, by giving everyone a clear picture of how the currency circulates. Its role is to store information about all bitcoin transactions, in order to establish the current number of coins in circulation and to allow users to cross-check that the listed transactions are indeed true to what everyone

else sees. The ledger itself also serves as a visual representation that there are no instances of double-spending, allowing users to scrutinize the logs to see if there have been any erroneous transactions.

Volume. A common critique of currency is that its value fluctuates wildly, being prone to inflation or outright made obsolete by a governing body. Out of fear of losing their personal savings, people have turned to commodities as stores of value[12]. To address this issue headon, Bitcoin was also modelled with the intention to serve as a store of value. It follows the example of gold, with the aim to have a finite amount of bitcoin in existence. The way the system does this is by making the process of obtaining more bitcoin less and less lucrative. Also, future units of bitcoin will become increasingly more difficult to obtain. This entire ecosystem is set as a means to prevent over inflation and market saturation. This process of diminishing makes the number of available bitcoins halve every 4 years. Therefore, to discourage a monopoly over the means of obtaining bitcoin and to maintain its price stable, the system has a set limit in place. Currently, judging by the constant rate at which bitcoin has been mined, it has been established that their final number will be 21 million units[13].

Common critique of Bitcoin

Although it is praised and appreciated for its potential, bitcoin draws its fair share of critiques. These are mostly due to the attention it attracts, often from disreputable parties. Due to their anonymous nature, cryptocurrencies are of great interest to individuals who engage in criminal activities, precisely to be used as means to transact in unlawful environments. It is true, the implications of cryptocurrencies are profound and must be taken into account, because anyone who wants to join the bitcoin community will realize that not only the advantages of the currency, but also the continued liberalization of the market, bring great responsibilities. Of course, many critics would argue that a fully liberalized market would lead to chaos, where economic laws would not be respected and fraud and abuse would be the order of the day. This implies that we would need the government to prevent these kinds of woes and an alternative to the status quo would be much worse. On the contrary, what

[12] Garrick Hileman, Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, Cambridge University, 2017.

[13] Kevin Dowd, op. cit., p. 41.

we can observe is that the government's multiple failures are an indicative that it does not have the ability to control the market. And even if the government were to be able to steer the market, it would do so in an inadequate way, oblivious of the needs and wants of people. In cases like this, where the government is unable to provide people with means to obtain what they desire, it facilitates the formation of black markets. The government's draconic and oftentimes irrational bans on various markets leads to an increase in demand for numerous goods. Just as an example, when bitcoin was on the rise, its decentralizing power has found a use in the trade of illegal substances. However, is this not the manifestation of a free market? Of a market that finds a solution when the government proves itself unreliable? In its early years, bitcoin became known for being used as the only accepted payment method on Silk Road[14] - an online market that specialized in the trade of drugs and various substances with a psychoactive effect. This undoubtedly tarnished bitcoin's reputation, however, it is not the instrument's fault in this matter. And people can't be blamed for seeking out ways to protect their transactions. In fact, most of the blame should be directed at the government, by working against the interests of its people and by setting up the conditions for a market such as Silk Road to function.

Another critique of bitcoin is that its decentralized nature does not guarantee to protect people's wealth, that it is too unstable to be used reliably. There is indeed truth to these sentiments, yet the same argument can be used against fiat currencies. As time and time throughout history there have been instances of currencies being completely devalued and people losing their savings. In the case of bitcoin, an event took place in its early years. One that could have completely destabilized the system and as a result of which bitcoin would not have been able to take off. It took place in 2010, when the system faced an instability in terms of the public ledger's ability to sort transactions. It was becoming unresponsive to duplicate transactions, thus allowing infinite transactions with the same bitcoin currency, leading to an inflation scenario as severe as one caused by governments. However, the vulnerability has been addressed, and duplicate bitcoins have been removed from exchanges[15]. It is true that if this were to occur in a time and place where bitcoin were the norm, it would

[14] *Ibidem,* p. 46.

[15] *Ibidem,* pp. 45-50.

cause a lot of suffering. Regrettably, there are no perfect solutions to mitigate these kinds of situations, since they are not necessarily concerned with bitcoin, but more with the reality of large economies and how sturdy they can be made against instabilities. On the other hand, it can be noted that in bitcoin's case, the issue was addressed in a timely manner and the system was able to get back up on its feet. If an individual were to cause this, people would be able to hold him accountable. Whereas a government could crash an economy through no fault of the citizens and no one would be able to hold it accountable. There are many other examples that can be given, yet all of them lead to the same conclusion - each time the government meddles with the people's money, it destabilizes the market, it makes people poorer without them having no recourse or a way to protect their wealth. A government's ban on a good creates a situation where demand increases. This enables the conditions for obscure, secondary markets to appear, which operate outside of the law. This situation pushes people to pursue less reputable ways to obtain the respective goods[16]. Ultimately, should people go down this route, they are the ones to be punished and demonized. In this case, is there any wonder why bitcoin is the preferred alternative?

Conclusion

The basis of this article was to draw attention to the danger of government's unrestrained control over people's wealth. On several occasions, we have signaled that overreaching control on economic activities will invariably lead to people forfeiting a great deal of their personal freedoms. It is known that there have been many attempts throughout history to elude the government's grasp, yet most of them fell short or did little to achieve significant results. The invention of bitcoin and the blockchain technology gave people the possibility to escape the prying eyes of their rulers and allowed them to freely commit transactions without ever fearing repercussions. With this idea in mind, we wanted to demystify the intricacies of how bitcoin works in hopes of showing that it has real liberating potential and that it is much more than a tool for financial speculation and fraud - it is a way to financial and personal freedom unlike we ever had before.

[16] *Ibidem*, p. 71.

Bibliography

DAI, Wei, *B-money*, http://www.weidai.com/bmoney.txt, 1998.

DOWD, Kevin, *New Private Monies – A Bit Part Player*, Hobbs the Printers, Institute of Economic Affairs, London, 2014.

HILEMAN, Garrick; Rauchs, Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge University, 2017.

LOCKE, John, *Second Treatise of Government*, C. B. Macpherson (edit.), Hackett Publishing Company, Inc. Indianapolis, Cambridge, 1980.

MISES, Ludwig, *The Theory of Money and Credit*, Yale University Press, London, 1953.

MAY, Timothy C., *The Crypto Anarchist Manifesto*, www.activism.net, 22 November 1992.

NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org, 2009.

ROTHBARD, Murray, *What Has Government Done To Our Money?*, Ludwig von Mises Institute, Alabama, 1991.