

Stroukal, Dominik

Article

Can Bitcoin become money? : Its money functions and the regression theorem

International journal of business & management

Provided in Cooperation with:

International Institute of Social and Economic Sciences, Prague

Reference: Stroukal, Dominik (2018). Can Bitcoin become money? : Its money functions and the regression theorem. In: International journal of business & management 6 (1), S. 36 - 53.
doi:10.20472/BM.2018.6.1.004.

This Version is available at:
<http://hdl.handle.net/11159/1967>

Kontakt/Contact

ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics
Düsternbrooker Weg 120
24105 Kiel (Germany)
E-Mail: [rights\[at\]zbw.eu](mailto:rights[at]zbw.eu)
<https://www.zbw.eu/econis-archiv/>

Standard-Nutzungsbedingungen:

Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte.
<https://zbw.eu/econis-archiv/termsfuse>

Terms of use:

This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence.

CAN BITCOIN BECOME MONEY? ITS MONEY FUNCTIONS AND THE REGRESSION THEOREM

DOMINIK STROUKAL

Abstract:

Bitcoin as a payment system indisputably offers an advantage over the government currencies in transaction time and costs. On the other hand the moneyness of Bitcoin itself is questioned. This paper analyzes Bitcoin from the Austrian perspective and compares the qualities of Bitcoin with qualities of good money in order to find out whether Bitcoin could serve as money. The examined properties are portability, storability, divisibility, recognizability, homogeneity and scarcity. Moreover it examines the consistency of Bitcoin emergence as a medium of exchange with Mises' regression theorem and identifies the non-monetary value of Bitcoin. The result of this theoretical analysis shows that Bitcoin's properties can facilitate the functions of money.

Keywords:

Bitcoin; cryptocurrency; regression theory; money; money functions

JEL Classification: E42, E44, E52

Authors:

DOMINIK STROUKAL, University of Economics, Prague, Czech Republic, Email: dominikstroukal@gmail.com

Citation:

DOMINIK STROUKAL (2018). CAN BITCOIN BECOME MONEY? ITS MONEY FUNCTIONS AND THE REGRESSION THEOREM. International Journal of Business and Management, Vol. VI(1), pp. 36-53.

INTRODUCTION

“An economic good that is defined entirely in terms of bits and bytes is unlikely ever be produced spontaneously on a free market,” wrote Guido Hülsmann in 2008 (Hülsmann 2008:33). One year later, in early 2009, Satoshi Nakamoto announced Bitcoin. While most people have only heard about Bitcoin in relation to its volatility or the selling of drugs and child porn on Silk Road, there are already studies which have turned the debate to the academic field, trying to explain Bitcoin from an economic point of view.

There are several studies which demonstrate either the technical (Grinberg 2011) or the economical (Dwyer 2014) nature of Bitcoin.¹ Aim of this paper is to theoretically find out whether Bitcoin can serve as money and whether it violates the regression theorem. Šurda (2012) who also examines Bitcoin from a market point of view and Graf (2013) who devotes himself to the regression theorem will serve as a starting point. Both papers are strictly academic, although neither of them is published.

In order to address this problem, we will assess the properties of Bitcoin and investigate whether it meets the requirements of good money according to Jevons (1898), Menger ([1871] 2007) and Hülsmann (2008). We will discuss the differences arising from the Bitcoin's electronic nature and illustrate the new possibilities. In the section dealing with regression theorem, we will present different approaches to the Bitcoin's non-monetary value and consider the importance of imagination in the case of digital goods.

In the first part there are defined terms as used in the work and the qualities we are looking for. The second part examines selected Bitcoin qualities: portability, divisibility, homogeneity, recognizability, storability and scarcity. The third part identifies whether Bitcoin is consistent with Mises' regression theorem.

1. WHAT IS MONEY

Money is *“a stock of assets that can be readily used to make transactions”* (Mankiw 2010:80). This definition, from a macroeconomic textbook, is correct, but a more comprehensive definition (corresponding to popular belief) can be made in term of its functions, which also reflects the broader social impact of money. Indeed, Mishkin (2004:45) states that money has to be defined by its function and not by its form. In this regard, money has three purposes – it serves as a store of value, as a unit of account and as a medium of exchange.

The Austrian point of view is represented by Ludwig von Mises who notes that *“the function of money is to facilitate the business of the market by acting as a common medium of exchange.”* (Mises 1953:29), and thus he defines money as *“the thing which serves as the generally accepted and commonly used medium of exchange.”* (Mises [1949] 1998:398). Notice that, according to Mises, money serves as a medium of exchange and that its other functions are

¹ Other studies are emerging, for example Selgin (2013), Yermack (2014) or Luther and White (2014).

derived from this function: *"This is its only function. All the other functions which people ascribe to money are merely particular aspects of its primary and sole function, that of a medium of exchange."* (Mises [1949] 1998:398). Its "secondary functions" come with higher liquidity with the passing of time, as originally presented by Peter Šurda (2012), who also points out that more recent Austrian economists, such as Salerno (2010) and White (1984), consider the superiority of the medium in terms of its exchange function and accentuate the importance of liquidity.

Although anything can serve as commodity money, over time we have discovered that certain intrinsic properties are characteristic of many types of money, since they make them more comfortable to use and more marketable. The beginning of the theory of the quality of money can be found in ancient Greece. According to Aristotle there are four defining characteristics of money: durability, portability, divisibility and having intrinsic value. There were successful attempts to identify the characteristics even before Adam Smith. Jevons (1898) writes: *"Many recent writers, such as Huskisson, MacCulloch, James Mill, Garnier, Chevalier, and Walras, have satisfactorily described the qualities which should be possessed by the material of money. Earlier writers seem, however, to have understood the subject almost as well. Harris explained these qualities with remarkable clearness in his 'Essay upon Money and Coins', published in 1757, a work which appeared before the 'Wealth of Nations', yet gave an exposition of the principles of money which can hardly be improved at the present day."* Harris's conclusion, which was mentioned, is that precious metals are suitable commodity for money for *"being durable, portable, divisible, without loss and equal goodness everywhere"* (Harris 1757:37). Adam Smith ([1776] 2005) noted the importance of the homogeneity of money which can lower transaction costs and he pointed out that there was no need to put value on identical coins. Jevons (1898:31) summarized the necessary qualities of money which, according to him, are: utility and value, portability, indestructibility, homogeneity, divisibility, stability of value and recognizability.

As mentioned, money can be defined in terms of its functions. Krugman writes: *"Money, the classical economists argued, serves three functions: it is a medium of exchange, a unit of account, and a store of value"* (Krugman 1984:262), Kiyotaki and Wright argue that: *"Which goods are used as money depends on intrinsic properties (storability, recognizability...etc) and extrinsic belief"* (Kiyotaki and Wright 1989). According to these assumptions, we should define the intrinsic properties of those commodities which serve the above mentioned functions in order to find out whether or not Bitcoin is a good candidate to become money.

Based on definitions above and works of Menger ([1871] 2007), Jevons (1898) and Hülsmann (2008) we can assign selected properties to the functions of money, which they facilitate.

Table 1 presents them.

Medium of Exchange	Unit of Account	Store of Value
Portability	Divisibility	Storability/Durability
Divisibility		Stability of Value
Homogeneity		Scarcity
Recognizability		

Table 1: The properties of good money and the functions they facilitate

2 THE QUALITY OF BITCOIN

2.1 Portability

If we define money as the most common medium of exchange, we need it to be usable in exchange without any obstacles. Good money should be easily carried and easily transferable from one place to another. Because of hard portability some commodities which were used as a medium of exchange mostly in the past faded into the background, being replaced with precious metals and, later, with fiat money.

We can see that portability has two dimensions important for good money in today's world. As Mises writes: "*The modern organization of the clearing system and the institution of fiduciary media have made commerce independent of the volume and weight of the monetary material*" (Mises 1953:100) We can either pay with the medium of exchange itself or we can use a money substitute and third party services to facilitate the process of payment. In each case we need to determine the transaction cost of the particular trade and compare fiat money (e.g., a wire transfer or payment with money itself) with Bitcoin.

The portability of Bitcoin is said not to be an issue, at least in more developed countries. Here, we can identify a contradiction in terms since we consider money to be the generally accepted medium of exchange, while in the case of missing technology, Bitcoin can hardly be considered widely accepted. Thus we might assume that it cannot become money because of a lack of this. According to Gertchev (2014) Bitcoin has to generate sufficiently large demand initially, in order to generalize its usage, and he argues that Bitcoin might fail because it has two disadvantages – non-uniform level of technological development and vulnerability of an economy based on one specific technology. In addition, he implies that Bitcoin can be more of a complicating factor than a facilitator of economic relations.

Although from today's perspective the technology might seem inadequate, tomorrow we can see market innovations capable of making Bitcoin payments accessible to everyone. Ignoring any revolutionary technology or device supporting the transfers of Bitcoins, we can say without any doubt that in three years the number of potential Bitcoin users will grow as the number of smartphones among people will.

Besides rapidly spreading technology, there is another solution which is applicable even now, which makes Bitcoin as a medium of exchange more available, and which is ignored by Gertchev. The transfer does not require internet access. In the case of payment offline, a trusted third party can provide assistance as in the example of physical coins given by Cacascius. Thus, there is a recognizable coin which contains a Bitcoin. It would be short sighted to say Bitcoin cannot become money based on current solvable obstacles.

Still, there are two properties which should be determined in order to evaluate the effectiveness of Bitcoin in terms of portability: the speed of transactions and their cost. In using Bitcoin, there is no centralized trusted third party as in the case of a credible bank, PayPal or Western Union. The security and operating of the Bitcoin network is ensured by independent data processors, which have access to the entire transaction database – ‘blockchain’. In Bitcoin terminology these are called ‘miners’ and their data processing is called ‘mining’. The miners try to add a new part (block), which includes all recent Bitcoin transactions, to the blockchain. The blockchain is basically an account book, a sequence of records of transactions. There is competition among processors as to who will solve the block and thus be rewarded for its solution. On the other hand everyone can watch over the other miners because whereas finding the solution is highly unlikely, checking the solution is trivial.

In other words, we need to find out how quickly the data processors are able to confirm the transaction and what the price for this confirmation is in order to decide how effectively the Bitcoin network works.

We can observe that the execution of a transaction might be faster in some cases compared to other money transfer services. Bitcoin can be sent anywhere in the world within a few minutes – the average transaction confirmation time takes around 10 minutes. After a transaction is sent to the network, it may be included in a new block – confirmed. In order to preclude double-spending,² we should not consider the transaction to be final until a certain number of blocks verify the transaction. We can consider a transaction to be confirmed when it occurs in at least six blocks.³ The six blocks, then, only represent a ‘low enough’ probability for someone with a ‘high enough’ hashrate to spend his Bitcoins twice. It does not constrain us in any way – we can still accept instant payments, just with a higher risk.

As mentioned, to link a new block to the blockchain, a difficult mathematical problem has to be solved. The number of miners, who attempt a solution, has no influence on the speed of finding a solution – the difficulty of the problem is automatically adjusted in order to have an average of 6 solutions per hour. The result of such adjusting has one significant effect - the transaction confirmation time will not be reduced as the network size increases. The following table compares the speed of Bitcoin transfers, international and domestic wire transfers, SEPA payment, PayPal payments and Western Union payments. As can be seen, the transaction speed of Bitcoin is superior to the transaction speed of money substitutes of fiat money. Outside

² Double-spending is a successful spending of money more than once. This problem is prevented by confirmations.

³ “There is nothing special about the default, often-cited figure of 6 confirmations. It was chosen based on the assumption that an attacker is unlikely to amass more than 10% of the hashrate, and that a negligible risk of less than 0.1% is acceptable. Both these figures are arbitrary, however; 6 confirmations are overkill for casual attackers, and at the same time powerless against more dedicated attackers with much more than 10% hashrate.” (Rosenfeld 2011)

of the wired world, fiat or commodity money is superior if we consider virtually instant face-to-face transfers.

Method	Average transfer of funds time
Bitcoin	Based on the number of confirmations 0-60 min
International wire transfer	Up to 15 days
Domestic wire transfer	1-2 days
SEPA	Up to 3 days
PayPal	Instantly, funds withdraw in 3-4 days
Western Union	Instantly (paid in cash/ withdrawn in cash)

Table 2: Average transfer time for funds. Retrieved 21. 5. 2016 from official documents of the largest Czech commercial bank (Komerční banka), Paypal and Western Union webpages.

The analysis of the transaction cost is more complicated. Transaction fees are generally charged by payment processors to facilitate a transaction, and it can vary based on many variables. In the case of Bitcoin, the data processing performed by miners has to be paid for – not even free lunch is for free, and although we can say that the direct transaction costs are low, there are also certain hidden costs. We can identify three ways in which the user pays for the transaction: direct transaction fees, bounties paid to miners, and increased risk.

First, there are direct transaction fees. Basically we can categorize transactions according to two subgroups: namely transactions which do not require any fee in order to be executed immediately and transactions which do. There is no mandatory fee to be paid using Bitcoin, however, there is no guarantee the transaction will occur immediately. In other words, the transaction does not have to be included in the next block. The confirmation time for transactions which do not include fees, although they qualified for it, might be even more than 24 hours.

In the current version the transaction can be sent without fees, whenever the sent data is smaller than 1000 bytes and all transaction outputs are larger than 0.01 BTC. Otherwise, there is a fee 0.0001 BTC for every 1000 bytes of data sent. This abstract information is illustrated in the diagram at Blockchain.info (2016). Here, we can observe that the average cost of a transaction is around 0,0002 BTC, which is roughly 15 US cents.⁴

⁴ The ratio of USD/BTC is due to high volatility and easier further conversion set to \$750 for one Bitcoin unit.

Figure 1: Average cost per transaction (BTC) – Data source:

The following table compares the transaction fees of Bitcoin transfers, international and domestic wire Transfer, SEPA payments, PayPal Payments and Western Union transfers. The direct fees are considerably lower when paying with Bitcoin. The difference in transaction costs increases with distance – the greater the distance, the more considerable the difference is. Again, outside of the digital world we can consider some of face-to-face transfers of fiat or commodity money free of charge.

Method	Fees
Bitcoin	0.0002 BTC = \$0,15
International wire transfer	0.9% (min \$11,25)
Domestic wire transfer	\$0.75
SEPA	\$9.75 \$75 (payment over \$67750)
PayPal	To receive money: 1.9%-3.4% + \$0.5
Western Union	Quick pay pricing: 1.8% -9% (according to the amount sent)

Table 3: Average prices for funds transfers. Retrieved 21. 5. 2016 from official documents of the largest Czech commercial bank (Komerční banka), Paypal and Western Union webpages.

Secondly, there is a bounty for the miner, who successfully solved the mathematical problem. This bounty is added to the fees paid for the transactions involved. So the reward for a mined block has two parts – the block bounty and the cumulative fees paid for the transactions contained in the mined block. This reward goes directly to the miners in order to incentivize them to keep mining (data processing). As long as the block reward makes the mining profitable, we do not have to expect higher transaction fees. The size of the block reward decreases with the quantity of blocks mined, as shown in the Table 4.

Block	Reward Era	BTC/block	Year	Start BTC	BTC Increase	End Limit	BTC % of
0	1	50	2009	0		50.00000006%	
210000	2	25	2013	10500000	50.00000000%	75.00000008%	
420000	3	12,5	2017	15750000	16.66666667%	87.50000010%	
630000	4	6,25	2021	18375000	7.14285714%	93.75000010%	
840000	5	3,125	2025	19687500	3.33333333%	96.87500011%	
1050000	6	1,5625	2029	20343750	1.61290323%	98.43750011%	
1260000	7	0,78125	2033	20671875	0.79365079%	99.21875011%	

1470000	8	0,390625	2037	20835938	0.39370079%	99.60937511%
1680000	9	0,1953125	2040,9	20917969	0.19607843%	99.80468761%
1890000	10	0,09765625	2044,9	20958984	0.09784736%	99.90234386%
2940000	15	0,00305175	2064,9	20998718	0.00305194%	99.99694833%
3990000	20	0,00009536	2084,9	20999960	0.00009536%	99.99990468%
5040000	25	0,00000298	2104,8	20999999	0.00000298%	99.99999706%
6090000	30	0,00000009	2124,8	21000000	0.00000009%	99.99999993%
6720000	33	0,00000001	2136,8	21000000	0.00000001%	100.00000000%
6930000	34	0	2141	21000000	0.00000000%	100.00000000%

Table 4: The reward for a mined block – Data source: Blockchain.info (2015)

Halving the reward for a mined block every four years will reduce the profits of miners. Therefore, in the long run as the size of block reward diminishes, it is expected that bounties will be replaced with transaction fees in order to motivate miners to continue confirming transactions.

We can conceive of the revenue for a miner from a successfully mined block in terms of the following relationship:

$$\text{Revenue \$} = \text{Revenue (BTC)} \times \text{nominal exchange rate (\$/BTC)}$$

$$\text{Revenue (BTC)} = \text{bounty (BTC)} + \text{transaction fees collected (BTC)}$$

The conclusion is simple – once the bounty drops, in order for a miner to stay in the business (assuming that we prefer the Bitcoin network to have various miners and that we are working with the marginal miner) there has to be an increase in the nominal exchange rate or the transaction fees collected. The transaction fees constitute 1/250 of the miner's reward,⁵ thus, in order to the revenue in BTC to stay the same there has to be 125 times higher transaction fee or the number of transactions in year 2017, when the bounty drops to 12,5 BTC.

The last thing we need to consider regarding the costs of Bitcoin transactions is the probability of fraud. The service provided by banks is not only about transferring money, but also about safety. The risk of fraud is thus passed on to the consumer, which makes transactions more expensive. A study presented by Moore and Christin (2013) has shown that 45 percent of Bitcoin exchanges have shut down.

Services like Coinbase (which can secure the transaction) or Trezor (hardware wallet) might become more mainstream and solve this problem. Anyway, the possibility of choice if and how to secure a wallet is advantageous – it gives us a chance to renegotiate the terms, namely the current tradeoff between payment and safety among our current payment systems.

⁵ Counting with 0,1BTC/ block.

2.2 Divisibility

Money should be effortlessly divisible into smaller units without losing value in order to allow for the purchase of cheaper goods, although there is the possibility of using multiple mediums of exchange in order to facilitate trade as Davies shows: *“Until well into the present century horses were the main monetary unit of the Kirghiz of the Russian steppes, and formed their main store of value, though sheep were used as subsidiaries, with lambskins being used as small change.”* (Davies 2002:43). In particular, and considering the matter from Jevon’s perspective, some commodities are not suitable since: *“The hardest gems can be broken, and steel can be cut by harder steel. But the material of money should be not merely capable of division, but the aggregate value of the mass after division should be almost exactly the same as before division.”* (Jevons 1898:36). This problem is not observed in case of precious metals where smaller portions of metal can be melted together whenever needed. Nevertheless we know from history that gold coins were generally used for larger payments while silver coins were used for smaller payments (Mises 1953) .

In every centralized economy, there is the possibility of directly increasing the supply of banknotes of any value – whether through a central bank or some other government agency – which makes the divisibility of fiat money indisputable. Moreover, as Mises notes: *“The modern organization of the clearing system and the institution of fiduciary media have made commerce independent of the volume and weight of the monetary material.”* (Mises 1953:100)

On the other hand, there are a limited number of Bitcoins – around 13 million today. This number is growing, such that up to 21 million should be reached in 2141 (more accurate numbers, showing the exact growth in Bitcoin supply, can be found in Table 4). Afterwards, the number of Bitcoins in circulation will stop increasing and no more Bitcoins will be ever generated.

It is important to understand, that the exact amount of money – Bitcoins in this case – is not relevant, so long as Bitcoin is effectively and infinitely divisible. The reason as to why the number is just 21 million is not known, but since there are more similarities with gold and since Bitcoin is often compared to it, the amount chosen by Satoshi Nakamoto might well be a symbolic – the total amount of gold mined in history can be imagined as a cube with a 21 meter long edges. Currently one Bitcoin is divisible down to 8 decimal places, calling the smallest unit Satoshi. There is no need to have smaller units, but although there is no need for additional decimals now, they can be added later if necessary. The protocol can be modified to handle even smaller amounts, but it would have to meet certain requirement because any change has to be implemented by convincing every user to download new software.

We need to imagine the scope for the growth of the value of Bitcoin in order to evaluate the usefulness of smaller denomination than one Satoshi. Rick Falkvinge estimates the target value of Bitcoin as from \$100,000 to \$1,000,000 based on following calculation. He assumes that: *“Bitcoin is a transactional currency. As such, it is competing for market share on the transactional currency market”* (Falkvinge 2013), and estimates the possible market share of Bitcoins. According to his calculations, based on the amount of money in circulation worldwide, the total size of the transactional currency market is around \$60 trillion. Once Bitcoin captures

just a one percent share of this market, the price of a single coin should be around \$100,000. If ever Bitcoin hits this rate, then one Satoshi will equal \$0.001.

2.3 Storability

A good money material should be storable at low cost and it should not depreciate with time. *“It must not evaporate like alcohol, nor putrefy like animal substances, nor decay like wood, nor rust like iron. Destructible articles, such as eggs, dried codfish, cattle, or oil, have certainly been used as currency; but what is treated as money one day must soon afterwards be eaten up. Thus a large stock of such perishable commodities cannot be kept on hand, and their value must be very variable”* (Jevons 1898:35). The chosen good should not be perishable over time, which can negatively affect its marketability. But, as Menger writes, nor should there be any loss in value caused by the number of previous users of the commodity: *“Gold nuggets can pass through any number of hands without any decrease whatsoever in marketability. But articles of clothing, bedding, prepared foods, etc. would be suspect and almost unsaleable, or at any rate of greatly depreciated value, in the hands of the gypsy, even if they had not been used by him and even if he had, from the beginning, acquired them only with the intention of passing them on in exchange.”* (Menger [1871] 2007:254)

There is no depreciation in the case of Bitcoin – it does not change in any way with an increasing amount of transfers. The storage of Bitcoin is relatively simple since Bitcoin is an electronic currency. The keypair – which allows us to control the balance of an account – can be stored on any device, which is capable of storing 64 bytes of data. It does not even have to be an electronic device, since we can write the keypair down on paper or even memorize it. Since the keypair is basically two numbers we can copy them as many times as desirable in order to store them safely, wherever we prefer. The only cost is our responsibility for this sensitive data.

The cost relating the storability of Bitcoin is extremely low and not dependent on third party services. Unlike Fiat money we can store Bitcoin on any device capable of storing 64 bytes.

2.4 Recognizability and Homogeneity

To recognize the medium of exchange, the commodity and its value on first sight makes the trade much smoother and faster. Jevons (1898:38) argues that *“As a medium of exchange, money has to be continually handed about, and it will occasion great trouble if every person receiving currency has to scrutinize, weigh, and test it”* He adds an example: *“Precious stones, even if in other respects good as money, could not be so used, because only a skilled lapidary can surely distinguish between true and imitation gems.”* (Jevons 1898:39)

Bitcoin is reasonably homogenous; on the one hand we can distinguish them and on the other hand they are all the same. It is similar to current banknotes with unique serial numbers. Moreover, the blockchain provides us with the information about every transaction that a particular Bitcoin has realized in the past, and therefore we cannot only see on which address they currently are, but we can also see where they were before. We can check the balance of our counterparty and thus know if they can pay from their Bitcoin wallet. No lapidaries are needed because the test itself is in the code.

2.5 Scarcity and Stability of Value

In seeking why tangible goods are the subject of property rights, Kinsella concludes: *“A little reflection will show that it is these goods’ scarcity – the fact that there can be conflict over these goods by multiple human actors. The very possibility of conflict over a resource renders it scarce...”* (Kinsella 2008:29). The scarcity in case of intangible goods should be defined in the same way – there should be the possibility of conflict over Bitcoins in order to be able to say that Bitcoin is scarce. Whether there is such conflict can be illustrated by prices *“When the price of a good is zero, demand exceeds supply. Only if the supply of free goods exceeds the demand for free goods do we say those goods are not scarce.”* (Marcus 2004)

Bitcoin is a digital good and, regarding digital goods, we need to distinguish between Bitcoins and standard digital goods: *“An example of a necessarily nonscarce good is a thing in demand that can be replicated without limit, so that I can have one, you can have one, and we can all have one”* (Tucker and Kinsella 2010).

Bitcoin is a different kind of a digital good – there is no possibility of multiple actors using the same coin simultaneously without mutual interference. As Graf (2014b:17) argues: *“Bitcoin has brought authentic rival scarcity into the realm of digital goods. This is not the artificially imposed, legally constructed scarcity of intellectual property legislation. The Bitcoin protocol has set up a type of scarcity that is inherent to and inseparable from the nature of the digital good itself”*. And as is explained above, there is a constrained number of Bitcoin units in the network. Thus we can consider Bitcoin to be scarce; there is demand for a limited number of Bitcoins, which cannot be copied and which act as a rival good.

The scarcity of fiat money is a problem – a state can issue as much paper money as desired. As Mises writes: *“It was this idea that led Adam Smith and Ricardo to the opinion that it was very beneficial to reduce the cost of producing money by resorting to the use of paper printed currency. However, things appear in a different light to the students of monetary history. If one looks at the catastrophic consequences of the great paper money inflations, one must admit that the expensiveness of gold production is the minor evil”* (Mises [1949] 1998:418). The number of Bitcoins is a given, and thus there is no possibility of high inflation. Bitcoin ‘production’ is based on a rigid mathematical calculation. As Hülsmann (2008, p. 80) notes, commodity money is superior to fiat money: *“In this crucial respect they are far superior to paper money notes, which can be multiplied ad libitum and which, as universal experience shows, have been multiplied.”*

The fact that Bitcoin is by its definition scarce is closely related to one of its current issues, namely the problem with volatility of its price. As Mises ([1949] 1998:416) puts it, changes in value can stem from the demand for money and its supply or in the demand for other goods and their supply. Because the supply of Bitcoin is given and we can expect the demand for other goods and their supply to be stable in short run, we can conclude that the volatility of Bitcoin is on its demand side. With expected rise in demand we can expect higher liquidity and thus lower volatility. Indeed, Šurda (2012:69) found that there is a negative correlation between Bitcoin volatility (measured in terms of daily, weekly or monthly USD price change) and liquidity

(measured in terms of daily, weekly or monthly slope of the cumulative bids and asks on Mt.Gox). It does make sense that with more people demanding Bitcoin one, even large, transaction cannot change the price much. So it follows from our expectation that Bitcoin network will grow that its value will be more stable over time.

2.6 Summary

The analysis shows how Bitcoin can facilitate the market by acting as money and how it can potentially compete with other mediums of exchange to become money. Its intrinsic properties fulfill Menger's, Hülsmann's and Jevon's requirements for a good to become more liquid, and thus to have a chance to become money under Mises definition – as the most common medium of exchange. Bitcoin is portable, divisible, storable with respect to depreciation, homogenous, easily recognizable, and unlike fiat money always scarce. Whether Bitcoin will or will not become money one day is not a matter of the analysis of its properties – which are appropriate – but rather a matter of the free market and time. Bitcoin behaves as a medium of exchange today, having advantages of portability and storability over fiat money.

3 BITCOIN AND THE REGRESSION THEOREM

3.1 The Regression Theorem

The economic function of money is directly connected with its objective exchange-value – if there were no objective exchange-value, there would not be any demand for money. There is circularity: *“Whoever spends money to buy any good or service ranks the marginal utility which keeping the money has for him against the marginal utility of acquiring the good. These value scales of the various buyers and sellers determine the individual supply-demand schedules and hence all money prices; yet, in order to rank money and goods on his value scale, money must already have a marginal utility for each person, and this marginal utility must be based on the fact of pre-existing money prices of the various goods”* (Rothbard 2009:269).

Mises solves this problem with his regression theorem, by adding a time-component to this relationship. As Rothbard explains *“the price of a good on day X is determined by the marginal utility of the good on day X and the marginal utility of money on day X, which last in turn depends on the prices of goods on day X – 1.”* (Rothbard 2009:270) This regress backwards is not infinite – we can arrive to the point where the good begins to be used as a medium of exchange, whereby the previous day's prices are fully determined by the price established through barter. The first person, who buys the good as a medium of exchange, buys it from a person who treats it as a good, rather than as a medium of exchange. At this point, there is no monetary demand – only its subjective use-value.

In order to evaluate Bitcoin in light of the regression theorem, we need to determine what the theorem means for us and what condition has to be fulfilled so that the theorem is applicable. Mises is very specific about how money achieves prices: *“This always happens when the conditions appear; whenever a good, which has not been demanded previously for the employment as a medium of exchange, begins to be demanded for this employment, the same*

effects must appear again; no good can be employed for the function of a medium of exchange which at the very beginning of its use for this purpose did not have exchange value on account of other employments. And all these statements implied in the regression theorem are enounced apodictically as implied in the apriorism of praxeology. It must happen this way Nobody can ever succeed in constructing a hypothetical case in which things were to occur in a different way." (Mises [1949] 1998:407). An important point is made here. In order for a commodity to achieve monetary value, it has to be this way, the value of the money has to emerge this way or else the regression theorem is wrong (1); the economic good must possess exchange value based on a non-monetary function – there has to be demand for its direct use (2).

Currently the most controversial thing about Bitcoin is the non-monetary value which divides the Austrian economists based on their opinion. Many, such as Kramer (2011) and Shostak (2014), argue that there is no such a non-monetary value in the case of Bitcoin: *"Observe that a bitcoin is not a thing; it is a unit of a non-material virtual currency. A bitcoin has no material shape; hence from this perspective the notion that it could somehow replace fiat money is not defensible"* (Shostak 2014). Terrell (2001) even doubts, that digital currency is viable. Others, such as Suede (2011), seek to challenge the Mises' regression theorem, arguing that the emergence of Bitcoin was possible based on existing prices of goods even without any direct-use value. Meanwhile, Graf (2013) and Šurda (2012) are convinced that Bitcoin does not violate the regression theorem.

3.2 Non-monetary Value

The doubts about the non-monetary value of Bitcoin have their root in the Satoshi's original paper (Nakamoto 2009). He refers to Bitcoin as a "peer to peer version of electronic cash" or "electronic coins" which might lead to the hasty conclusion that there cannot be any non-monetary value – thus it cannot satisfy the regression theorem.

We need to find the direct-use value to reject the expanded notion that Bitcoins are just a digital abstraction. On this topic, Mises argues: *"Ultimate ends are ultimately given, they are purely subjective, they differ with various people and with the same people at various moments in their lives"* (Mises [1949] 1998:95). The fact that he cannot see the direct-use value can be explained with lack of imagination. Graf provides a nice example of where the direct-use value might arise: *"Consider, for example, the geek value hackers find in creating and attempting to crack encryption codes of any kind: 'Dude, look at this code; I bet you can't crack it' may indeed be more highly valued to some people in some context than 'real' economic objects or specific quantities of money."* (Graf 2014a) Although some might consider Bitcoin to be utterly useless except in terms of its monetary value, someone else does not have to. Speaking about human action, Mises writes: *"The notions of abnormality and perversity therefore have no place in economics. It does not say that a man is perverse because he prefers the disagreeable, the detrimental, and the painful to the agreeable, the beneficial, and the pleasant. It says only that he is different from other people; that he likes what others detest; that he considers useful what others want to avoid."* (Mises [1949] 1998:95) Thus we would be to better focus on the search for the non-monetary use and value of Bitcoin rather than judge what can satisfy human needs.

We already have a terminology for such a thing which satisfies human needs and therefore which is valued. We call it an economic good and as Mises writes, the medium of exchange has to be an economic good in order to serve its function: *“Media of exchange are economic goods. They are scarce; there is a demand for them. There are people on the market who desire to acquire them and are ready to exchange goods and services against them.”* (Mises [1949] 1998:398) Thus, we should determine whether Bitcoin can be treated as an economic good. As Mises explains: *“Economic goods which in themselves are fitted to satisfy human wants directly and whose serviceableness does not depend on the cooperation of other economic goods are called consumers' goods or goods of the first order. Means which can satisfy wants only indirectly when complemented by cooperation of other goods are called producers' goods or factors of production or goods of a remoter or higher order.”* (Mises [1949] 1998:93) Thus we should consider either find how Bitcoin can be used directly to satisfy human needs, or how we can employ it in order to produce a good which satisfies human needs, as Menger clears: *“These requirements are the quantities of goods of higher order that are necessary, in the existing state of technology of the relevant branches of production, for supplying our full requirements for goods of first order.”* (Menger [1871] 2007:84)

At the point where we accept that human needs can be different, another problem occurs. This problem seems to be found already at the beginning. Bitcoin is intangible, which is acceptable: *“An economic good does not necessarily have to be embodied in a tangible thing.”* (Mises [1949] 1998:94), but moreover, we are not able to capture it in any way. We cannot save it to our hard drive, we are only able to use it in the network, change the place of the Bitcoin unit in the network, which makes hard to understand, it can be called an economic good. The explanation as to why we might consider Bitcoin to be digital good offers Graf (2014a) and it is summed up above. There are similar cases to that of the Bitcoin, whereby an economic good which satisfies a human need is only part of a network. In the popular game World of Warcraft people play different characters and, once they stop, they often sell them on to other players. Equally, there are people who are willing to pay more than \$200 for them, therefore, the items within a game must have some direct-use value to them – it has to satisfy them in some way. The most attractive thing about this example is that they are only selling and buying the passwords to their accounts. There is no data, which they might store in a flash drive; they are buying a character, which only exists within the world of the game. If we do not question whether these characters from a game are economic goods we should not question Bitcoin.

For the two years following the inception of the Bitcoin network, we cannot speak about any monetary value associated with it. (Graf 2014b) Bitcoin was not used as a medium of exchange. We can observe two ideas, how Bitcoin can be used, which were further developed. Bitcoin can work as anti-spam security and as a form of agreement used in a distributed contractual scheme, the latter of which offers impressive options:

- (1) The application of smart property – property, where the owner is defined as the holder of a marked Bitcoin;
- (2) Transferable virtual property – Kinsella (2008) demonstrates the difference between digital goods and economic goods, whereby there is generally no conflict over digital goods, because

they can be copied without any limitations. Graf (2014b) argues that Bitcoin is a rival good, which does not behave in the same way as a normal digital good. According to this theory, we can create a digital good, which cannot be controlled by central authority and which can be exchanged between peers, but which can have only one owner.

These technical innovations need both – a Bitcoin network and Bitcoins, thus anyone who wanted to examine the possibilities needed them. The Bitcoin's direct-use value can originate there. The argument that these services were never functional is not valid, because an economic good of a higher order does not stop being an economic good just because the relevant economic good of the first order is not yet ready.

As a consumer good, Bitcoin can be seen as a toy – testing of Bitcoin features with other users – or as a badge of membership – possession of Bitcoins can be considered as sign of commitment (Graf 2013).

The second argument against this non-monetary function of Bitcoin is the strength of demand, or its width. First of all, as noted by Mises, there is no such requirement; and secondly, we might look more closely at the example of gold, where no one questions its non-monetary function. There is a nice argument as to why the limited initial demand for Bitcoins is sufficient. We need to study what gold was good for thousands of years ago. In particular, it was only used for ornamentation - there was no industrial use of gold. The demand for gold was neither wide nor strong. From this point of view, Bitcoin is much like gold. Gold jewelry created the direct usage of gold, and which is capable of making people happy just as Bitcoin makes some people happy. There are just different people who appreciate different things. This is what Graf (2013:27) describes: *"At some points and for some persons, Bitcoin units could have functioned as a toy-like set of digital objects that could be collected incidentally or even competitively in the course of the above processes of experimentation."* As attractive as glittering gold can be new technology for many people. The possession of Bitcoins can be satisfying for people who like technology because it shows that the holder is part of a community.

3.3 Summary

Bitcoin does not violate the regression theorem. The regression theorem does not say how wide or strong non-monetary demand should be, it only says that there should be non-monetary demand, which can be found. As has been shown, Bitcoin has been used as a toy and as a symbol of community during the first two years of its existence, without any monetary value. It was also used as producers' good, while people examined the new technology and tried to improve the current conception of smart property using coloured Bitcoins, or tried to upgrade their anti-spam security. In case of Bitcoin, its current nonmonetary usage is even more attractive than before, as the network has grown. As Mises argues, the non-monetary demand does not have to persist once the monetary occurs the regression theorem tries to explain the first emergence of monetary demand for a good *"This certainly does not involve explaining the specific monetary exchange value of a medium of exchange on the ground of its industrial exchange value."* (Mises [1949] 1998:406)

CONCLUSION

Based on the analysis we might consider Bitcoin a good candidate to become a generally used medium of exchange, according to Mises' definition – money. Bitcoin meets the requirements of the regression theorem and thus can acquire monetary value in the first step. We can consider Bitcoin an economic good based on the impossibility of copy, the possibility of conflict over it and the ability to satisfy human needs. In the beginning there was a demand based on unique properties which did not have roots in monetary usage, but in specific human needs and possible business models which need the network and Bitcoins. At this point, the monetary demand could start arising. Bitcoin has now become a medium of exchange, with many services known from the world of fiat money. The outcome of the second step of the money emergence – the competition among mediums of exchange cannot be predicted because of many unpredictable factors, but the good money requirements based on Menger ([1871] 2007), Jevons (1898) and Hülsmann (2008) are met. Bitcoin can be sent anywhere in the world within a few minutes and can be divided without any limits. Bitcoins are homogenous and it is inexpensive to recognize them and store them. The biggest challenge to the fiat money is the scarcity of Bitcoin. The impossibility to duplicate it is a good feature for creditors and the government will never be able to do any monetary policy with a cryptocurrency of this type.

Although the study has successfully demonstrated the moneyiness of Bitcoin, it has certain limitation in terms of used sources. Bitcoin is a new technology and thus there are not a sufficient number of peer-reviewed sources. Moreover, its electronic nature results in debates which develop and take place almost exclusively on the internet.

At this point we believe Bitcoin can compete with any other medium of exchange and the research should focus more on the future and possible scenarios. The transaction fees in the long run should be calculated, because the diminishing block reward can significantly affect the amount of fees. The second area we suggest to examine is the role of government and the following questions: how can Bitcoin or similar technology serve to the government and how it can be banned.

REFERENCES

- Blockchain.info. 2016. "Bitcoin Charts - Blockchain.info." Blockchain.info. Retrieved May 21, 2016 (<http://blockchain.info/charts>).
- Davies, G. 2002. *A History of Money: From Ancient Times to the Present Day*. Cardiff: University of Wales Press.
- Dwyer, G. 2014. "The Economics of Private Digital Currency." *Available at SSRN 2434628* 20. <https://doi.org/10.2139/ssrn.2434628>
- Falkvinge, R. 2013. "The Target Value For Bitcoin Is Not Some \$50 Or \$100. It Is \$100,000 To \$1,000,000. - Falkvinge on Infopolicy." falkvinge.net. Retrieved May 21, 2016

(<http://falkvinge.net/2013/03/06/the-target-value-for-bitcoin-is-not-some-50-or-100-it-is-100000-to-1000000/>).

Gertchev, N. 2014. "The Money-ness of Bitcoins." Mises.org. Retrieved May 21, 2016 (<http://mises.org/daily/6399>).

Graf, K. 2013. "The Origins of Bitcoin: Stages of Monetary Evolution." Konradsgraf.com. <http://konradsgraf.com/storage/On%20the%20Origins%20of%20Bitcoin%20Graf%2003.11.13.pdf>. Retrieved May 21, 2016 (<http://konradsgraf.com/storage/On%20the%20Origins%20of%20Bitcoin%20Graf%2003.11.13.pdf>).

Graf, K. 2014a. "Investigations and observations - Home - IN-DEPTH | Bitcoins, the regression theorem, and that curious but unthreatening empirical world." Konradsgraf.com. Retrieved May 21, 2016 (<http://konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html>).

Graf, K. 2014b. "Revisiting Conception of Commodity and Scarcity in Light of Bitcoin." Konradsgraf.com. Retrieved May 21, 2016 (<http://konradsgraf.com/storage/Commodity%20scarcity%20Bitcoin%20Graf%2017March2014.pdf>).

Grinberg, R. 2011. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal* 160-208.

Harris, J. 1757. *An Essay Upon Money and Coins*. London: G. Hawkings.

Hülsmann, JG. 2008. *The Ethics of Money Production*. Auburn: Ludwig von Mises Institute.

Jevons, WS. 1898. *Money and the mechanism of exchange*. New York: D. Appleton and Company.

Kinsella, S. 2008. *Against Intellectual Property*. Auburn: Ludwig von Mises Institute.

Kiyotaki, N and R Wright. 1989. "On Money as a Medium of Exchange." *Journal of Political Economy* 927-954. <https://doi.org/10.1086/261634>

Kramer, D. 2011. "Bitcoin: Just Another Bogus Medium of Exchange." lewrockwell.com. Retrieved May 21, 2016 (<http://www.lewrockwell.com/lrc-blog/bitcoin%E2%80%94just-another-bogus-medium-of-exchange/>).

Krugman, P 1984. "The International Role of the Dollar: Theory and Prospect." Pp. 261-278 in *Exchange Rate Theory and Practice*. Chicago: University of Chicago Press.

Luther, WJ and LH White. 2014. "Can Bitcoin Become a Major Currency?" *SSRN Working Paper*. Available at: <http://ssrn.com/abstract=2446604>.

Mankiw, G. 2010. *Macroeconomics*. New York: Worth Publishers.

Marcus, BK. 2004. *The Spectrum Should Be Private Property: The Economics, History, and Future of Wireless Technology*. Auburn: Ludwig von Mises Institut.

- Menger, C. [1871] 2007. *Principle of Economics*. Auburn: Ludwig von Mises Institut.
- Mises, L v. [1949] 1998. *Human action: A Treatise on Economics*. Auburn: Ludwig von Mises Institute.
- Mises, L v. 1953. *The Theory of Money and Credit*. New Haven: Yale University Press.
- Mishkin, FS. 2004. *The Economics of Money, Banking, and Financial Markets*. 7th ed. Boston: Pearson, Addison Wesley.
- Moore, T and N Christin. 2013. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk." *Springer* 25-33.
- Nakamoto, S. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System."
- Rosenfeld, M. 2011. "Analysis of hashrate-based double-spending." [bitcoil.co.il](https://bitcoil.co.il/Doublespend.pdf). Retrieved May 21, 2016 (<https://bitcoil.co.il/Doublespend.pdf>).
- Rothbard, MN. 2009. *Man, Economy, and State*. Auburn: Ludwig von Mises Institute.
- Salerno, J. 2010. *Money, Sound and Unsound*. Auburn: Ludwig von Mises Institute.
- Selgin, G. 2013. "Synthetic Commodity Money." *SSRN Working Paper*. Available at: <http://ssrn.com/abstract=2000118>.
- Shostak, F. 2014. "The Bitcoin Money Myth." *Mises.org*. Retrieved May 21, 2016 (<http://mises.org/daily/6411/The-Bitcoin-Money-Myth>).
- Smith, A. [1776] 2005. *An Inquiry into the Nature and Causes of the Wealth of Nations*. Penn State: The Pennsylvania State University.
- Suede, M. 2011. "The Economics of Bitcoin: Challenging Mises' Regression Theorem." *libertariannews.org*. Retrieved May 21, 2016 (<http://www.libertariannews.org/2011/07/07/the-economics-of-bitcoin-challenging-mises-regression-theorem/>).
- Šurda, P. 2012. "Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?" *economicsofbitcoin.com*. Vienna. Retrieved May 21, 2016 (<http://dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf>).
- Terrell, T. 2001. "Is Digital Currency Viable?" *mises.org*. Retrieved May 21, 2016 (<http://mises.org/daily/629>).
- Tucker, J and S Kinsella. 2010. "Goods, Scarce and Nonscarce." *mises.org*. Retrieved May 21, 2016 (<http://mises.org/daily/4630>).
- White, L. 1984. "Competitive payments systems and the unit of account." *American Economic Review* 699-712.
- Yermack, D. 2014. "Is Bitcoin a Real Currency? An Economic Appraisal." *SSRN Working Paper*. Available at: <http://ssrn.com/abstract=2361599>.