WSIiZ Working Paper Series

WP 23 **October 2017**

DIGITAL MONEY: DANGERS AND OPPORTUNITIES

Łukasz Cywiński

Abstract

Despite a relatively short period that elapsed since the development of blockchain or Distributed Ledger technology (DLT), it has been put to multiple uses by Multinational Corporations, Central Banks, governments and individuals. It has been responsible for the emergence of digital money and revolutionary changes in a wide array of financial services. The paper examines opportunities and threats associated with the use of DLT, with a special emphasis on the first experimental digital money, applying a heuristic SWOT analysis. It includes the analysis of properties of BitCoin in comparison to traditional money together with detailed examination of protocols that created it in terms of associated dangers.

Keywords: Digital money; BitCoin, Distributed Ledger Technology, Blockchain technology; SWOT (Strengths, Weaknesses, Opportunities and Threats); financial services

JEL Codes: O33

Note: Expanded version of this a paper "Will Digital Money croud out National Currencies?" was submitted for publication in "Bezpieczny Bank" ISSN 1429-2939 in July 25, 2017.

University of Information Technology and Management in Rzeszow, Poland
Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie
ul. mjr H. Sucharskiego 2, 35-225 Rzeszów, Polska
Kontakt: Natalia Białek (natalijka@gmail.com) and Lukasz Cywinski (lukaszcywinski@outlook.com)

Digital Money: Dangers and Opportunities

By

Łukasz Cywiński[×/]

Table of contents

[×] Łukasz Cywiński, University of Information Technology and Management in Rzeszów, ul. Sucharskiego 2, 35-225 Rzeszów, Poland, e-mail: lukaszcywinski@outlook.com

Introduction

Distributed Ledger technologies (DLT), or more generally blockchain technologies, allow for fast transfer of detailed records within the global digital nexus in a virtually instantaneous manner. DLT can be configured to create social media, cloud computing, cost-free global communication networks and distributed financial crypto-networks i.e., BitCoin. In 2016 the World Economic Forum marveled over the potential of DLT to shape the future of innovation-driven economies worldwide. In spite of the fact that there is still a lack of clarity as to what DLT can do, its report envisages that by 2025 around ten percent of GDP will be stored on blockchains or blockchain related technology.

The configuration of networks based on the concept of blockchain cryptosystem designed by Nakamoto (2008) has been subject to scrutiny. One of its weaknesses is that the system that is both censorship resistant and entirely anonymous might be also murky and dangerous. For example, BitCoin is enabling the so called dark web, i.e., market for trade in illegal goods and services. It is feared that the DLT may turn out to be a Trojan horse designed to undermine the trust bestowed in democratic institutions in a long-run. It remains to be seen whether this happens.

Our discussion will focus mainly on the assessment of the extent to which DLT may lead to the creation of money that might become a full-fledged alternative to national currencies. The candidate for money has to fulfill simultaneously the following functions: it has to be able to serve as a medium of exchange, unit of account, store of value, and a standard of deferred payment. Since DLT has already allowed for the emergence of digital money as represented by BitCoin, the issue is not a purely academic one. We will seek to address such questions as: What is the relationship between digital money represented by BitCoin and traditional money? Which properties make digital money attractive? What are the possible pitfalls of its use?

The remainder of this paper is organized as follows. The first part concentrates on multiple applications of digital money. The next part shows protocols responsible for its inner mechanics and configuration – based on the model drafted by Nakamoto (2008). The paper provides also a brief discussion of functions and dangers related to digital money. It assesses dangers inherent in the technology that created digital money and BitCoin in particular. BitCoins' popularity in relation to other digital money systems motivated its choice; however since other protocols are merely clones of BitCoins, our analysis also applies to them. Since digital money is a relatively recent phenomenon in economics and there is no accepted methodology to assess and organize the known information about it, the analysis of digital money properties applies a universal heuristic approach by analyzing Strengths, Weaknesses, Opportunities and Threats (SWOT) of BitCoin as a base-model for the global digital currency.

Distributed Ledger Technology: its potential

BitCoin the blockchain technology's first application allows an instantaneous transfer of value through the Internet via decentralized online platform (Marr, 2016). The technology is meticulously designed to provide fast exchange of data. BitCoin does this very efficiently using the network that has no central server. Generally the information on the Internet is distributed asymmetrically and most of it is stored in the so called "deep web" inaccessible from the position of standard search engine i.e. Google or Bing. The open-access architecture of the Internet allowed programmers to create private protocols that in number of occasions created new ingenious ways of organizing data by sending and receiving specific types of coded information. Blockchain network, represents this essence of creative destruction in the ways of storing, processing and organizing data into information and knowledge. It takes advantage of decentralized network but at the same time it applies symmetry of information by creating multiple copies of the ledger. BitCoin network was the first large-scale experimental application of the Distributed Ledger Technology. And equally to the World Wide Web – that evolved beyond email and webpage – Distributed Ledger Technology, based

on various types of blockchains, bears the potential to evolve beyond BitCoin or private digital money.

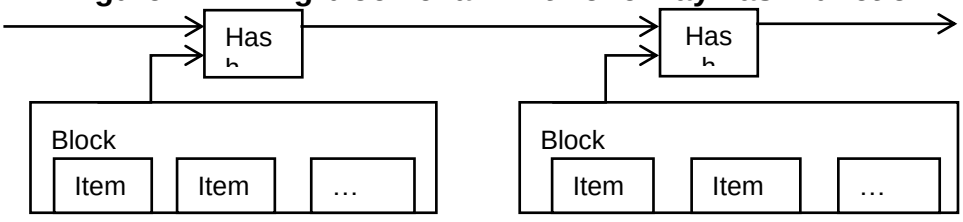
The fundamental property of digital money's blockchain network is anonymity – users are identified through the so called *hash values* (strings of symbols) that replace identities. To process information without central server and to maintain the ledger without error, every user of the blockchain keeps two sets of keys – a public key and a private signature key. The public information is in the essence an announcement that the connection took place and it was successful – and in the case of digital money that two parties made a transaction.

The fundamental property of cryptographic protocol is to maintain trust and confidentiality. Announcing to the public, that *the note* exists and that it was sent over the Internet is a crucial element of blockchain network infrastructure. The next owner of the note adds up to the public hash that links with first owner's secret public key. In the case of the abovementioned two parties, communication lasts only as long as they send the note to one another. In the environment created by the Internet network this takes only milliseconds. The BitCoins are converted, the same way we recycle the used paper, but faster – and they are chained with other transactions. They create anonymous block of linked notes called a blockchain.

The abovementioned 'recycling' process is done by volunteering nodes – their task is to process public announcements and provide the so called "solution" – a string of information that represents new efficient block recognized by everyone in the network. This means that whoever makes a new transaction, acknowledges the authenticity of the previous transactions – or in case of digital money that the note is real. But, where does the nodes' incentive come from? In case of digital money network, when information is processed new coins are minted the same way paper recycling factories add fiber to the papier-mâché. The nodes simply collect the extra part plus a small commission. The authenticity of digital money is ensured by the existing blockchains of previous transactions. Nodes and the users, thus create a new kind of trust established on the cognitive module based on self-interest and anonymous secrecy propelled by the bandwagon effect.

The above does not explain why the network is stable. Because initially it was not, though it becomes stable over time. The symmetry of information, the balanced ledger or the public consensus in case of digital money is maintained automatically without any involvement of the third parties. The cryptographic algorithm accepts only very specific strings of data – only the hash values recognized by all nodes in the system holding copies of previous public ledgers. To achieve that recognition – in other words the abovementioned public consensus, all transactions are time-stamped by the procedure based on the binary tree structure that works by rounds with fixed duration. Registered hash values i.e. $H_{23} = \mathrm{H}(y_2 \mid y_3)$ that are needed for verification are continued as long as the single value is obtained – so called: round root value (see: Bayer, Haber and Stornetta, 1993; Massias, Avila and Quisquater, 1999), that becomes RH_i for previous transaction RH_{i-1} (see: figure 1). Moreover, the information about the users is anonymous. Therefore the timestamp for a completed block of transactions $y_n = \{(y_{n-1}),(H_{n-1}),(H_n),(RH_{i-1})\}$ is counterfeit-resistant assuring network's stability.

Figure 1 Linking block-chain with one-way hash function.



Source: Nakamoto (2008)

Described process requires a lot of computing power and very little storage. The value assigned to the public hash is assessed based on the proof-of-work cost-function called Hashcash (Back, 2002). The hashcash scans H_n back until it receives a zero-bit value hash. This function was originally created to assess the value of the spam that "throttle systematic abuse of un-metered internet resources such as e-mail" (Back, 2002 p.1). It is a Central Processing Unit or for short a CPU-cost function that computes a special token used as a proof-of-work. In case of digital money usually a public announcement is issuing a challenge: C to the nodes using a $chal(s,w)$ function to compute token: τ using a: $mint(C)$ function. When the challenge is completed the server applies the evaluation function: $value(\tau)$ to evaluate the token. The challenge consist of bit-string $s = \{0,1\}^*$, and w that denotes a parameterized amount of work – used to compensate for the Moore's observation about increasing efficiency of the semiconductor-based computers. $Chal()$ Function becomes the public announcement, it contains $H(\cdot)$ with defined size of bits l. The procedure takes the following form:

$$\begin{cases} C \leftarrow chal(s(H\{0,1\}^l),w) \\ \tau \leftarrow mint(C) \\ v \leftarrow value(\tau) \end{cases}, \qquad (1)$$

The computing power of the CPU is therefore a "mining effort" to obtain the hash value for the block of transactions – previously referred to as "the solution". Because parameter w is designed to compensate for the "increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour" (Nakamoto, 2008). According to Nakamoto (2008) if a hacker assembles more CPU power than all honest nodes combined, he would find it more profitable to use this power to generate new coins rather than to destroy the system. In case of BitCoin the level of minting difficulty increased dramatically since the early stage. This happened because the nodes learned new cost effective methods of computation using specially designed circuits.

The Main Properties of BitCoin

BitCoin is able to attract transactions worth billions of US dollars. However, does it fulfill the three most important function of money: Can it function as a medium of exchange? Can it function as a unit of account? And as a store of value? To be a medium of exchange it needs to be an "item that buyers give to sellers when they want to buy goods and services" (Mankiw 2009 p. 339). To be a unit of account, it needs to be a "yardstick people use to post prices and record debts" (Mankiw 2009 p. 339). Finally to be a store of value it needs to be "an item that people can use to transfer purchasing power from present to the future" (Mankiw, 2009 p. 339).

Krugman (2013) in his blog wrote that "BitCoin is evil" and that he is not convinced if it can be a good store of value. He compares BitCoin to gold and concludes that "placing a ceiling on the value of BitCoins is computer technology and the form of the hash function (…) until the limit of 21 million BitCoins is reached. Placing a floor on the value of BitCoins is… what, exactly?" He relates to the value of gold limited by mining technology. BitCoin is related to semiconductor technology, with yet undiscovered nor fully understood limitations. Decision to limit its supply was made by a team of programmers and not by technology's limitations. If BitCoin in its essence is not entirely institution-free nor it is pluralistic, why so many sources claim that the third parties do not play any role in the creation of its value? As mentioned above there are no third parties registering transactions on the

ledger but there are other organizations striving to take control over the supply of BitCoins. For example, individuals that set the rules on minting process. Theoretically it is possible that these rules could be amended maintaining blockchain compatibility. Until 2011 BitCoin development was managed by anonymous hacker Satoshi Nakamoto (according to The Economist article from May 2nd 2016 this pseudonym belongs to Craig Steven Wright); after Nakamoto's disappearance the key development work has been done by Gavin Andresen and his team. In 2014 Anderson created a BitCoin Foundation that manages further software development of BitCoin network and that foundation has the necessary resources to control the supply rules.

According to Egorova's and Torzhevskiy's (2016) the supply rules for BitCoin can be represented by the function: $Q = A\left[1 - \exp^{-S_i t}\right]$, where, Q – is a theoretical quantity of BitCoin, A – the limit of 21 million BitCoins (imposed by its founders), i denotes number of nodes in the system, t denotes time, and S is a function parameter which defines growth acceleration or deacceleration depending on the so called halving rule. The modus operandi of the halving rule creates a discrete reward to the amount of compensation. In case of BitCoin:

$$S_i = \begin{cases} S_0, & t_0 \le j < t_0 + 1 \\ S_i(j-1)q, & t_0 + j - 1 \le j \le t_0 + 1 \end{cases}, \qquad (2)$$

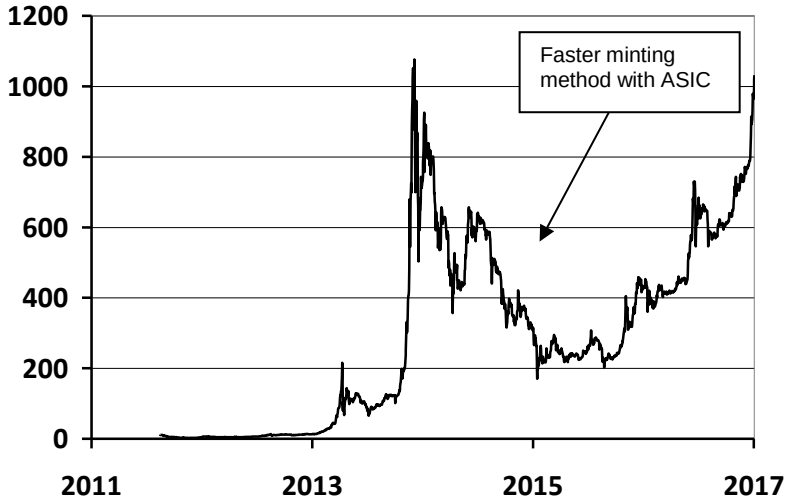
where $q = 0.5$ – correction coefficient, j – in this case represents a correction number for emission reward and S_0 is a first time reward (50 BitCoins); $t \in [0, T]$.

Although the supply of BitCoins is limited to 21 million BitCoins, the limit of emission embodied in the automated protocol can be amended by anyone who controls the parameter. The initial idea behind the BitCoins was that after the limit is reached the incentive for the nodes would change from the reward to a small commission. In case of BitCoin the commission for each node i is:

$$K_i = \begin{cases} 0, & if \quad S_i > 4BTC \\ 0.0005\ BTC & if \quad S_i \le 4BTC \end{cases}.$$

Abovementioned rules are created specifically for the BitCoin, other for instance public digital money might emceed different rules that would hand in the control over to Central Bank. In case of digital money the minting rules are the most important factor of success. One of the dangers imbedded in the BitCoin structure is that the rules behind the emission might not create enough incentive for nodes to carry on the work after they reach the limit of 21 million units. The efficiency of blockchain technology, and thus its supply is inseparably linked with computational speed of volunteering nodes. In 2014 the value of BitCoin was falling because of the introduction of new methods of solving the $chal(s, w)$ function with Application Specific Integrated Circuit (ASIC) based systems (Figure 2).

Figure 2 BitCoin to USD exchange rate in 2011 – 2017.

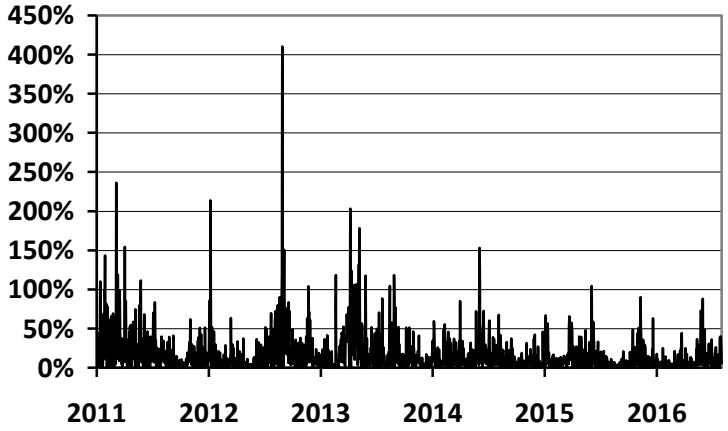


Source: data retrieved from investing.com

New methods of calculating complex brute force algorithms shortened the time needed for achieving the total number of BitCoins and in consequence lowered its price (in 2013-2015 the total number of BitCoins increased from 10.6 million to 13.7 million units). In the long run this might threaten the network integrity, therefore the minting was hardened in the halving process. The price of BitCoin again skyrocket to more than USD 1000 per BitCoin. More people became interested in new strange money and wanted to acquire it. This created a business opportunity for nodes that stored minted BitCoins, they founded companies which offered so called BitWallets or BitCoin Gambling Sites. However, abovementioned firms rarely offered secure storage.

The ability to perform as a store of value and unit of account in case of BitCoin is related to cybersecurity. In the present configuration BitCoin is based on the advanced crypto-technology and facilitates irreversible transfer. It should not come as a surprise that this property of BitCoin was exploited by cybercriminals. For instance, in August 2016 Bitfinex – one of the most popular crypto-market in the Internet – was hacked by a Black Hat Hacker. The main aim of a "black hat" is to gain administrative power over the system. In the case of Bitfinex the hacker stole 120 thousand BitCoins worth at that time US$65 million (Vigna, 2016). Bitfinex specialized in Exchange Trading, Margin Trading and Funding, Deposits and Bit-Wallets management. And since the transfer is irreversible and censorship-free, it is impossible to recover stolen property. In the past the main task of the bank was to provide safety from theft. Digital money market does not guarantee compensation from cybercrime. The network itself is secure the hacking takes place mostly in the ecosystem of third-party intermediaries supporting currency conversion that build up around BitCoin (Moore & Christian, 2013).

Figure 3 BitCoin's decreasing volatility in 2011-2017



Source: own calculation based on data retrieved from investing.com;
Volatility was calculated for trading period that equals 365 days.

Cybercrime is not the only argument against using BitCoins. One of the main properties that distinguish BitCoin from traditional money is its volatility. The price of BitCoin can skyrocket or crash by more than 25 percent in a matter of hours. And this makes it highly questionable in terms of day-to-day purchases. Although, the volatility of BitCoin, as measured by the ratio of standard deviation of daily transactions and square root of a trading period, has been falling since 2011 (see figure 3), it remains very high. According to Bouoiyour and Selmi (2015 p. 10) "Bitcoin volatility process seems more influenced by negative (bad news) than positive shocks. Not surprisingly, the BitCoin market is highly driven by self-fulfilling expectations." The first BitCoin users consisted of technology enthusiasts and criminals, though slowly the attention to use it shifted towards traders and speculators. And strangely BitCoin nowadays reminds more of the speculative investment than money.

BitCoin's current high volatility affects also its ability to serve as a unit of account because it makes it hard to measure the value of goods and services. Risky changes in BitCoin short-run volatility increase costs of business in several ways. Businesses need to frequently adjust prices to avoid cuts in returns. This might confuse customers who are unable to spot the true relative price of particular good or service. A niche thus created is filled by third-parties that present elegant solutions to diminish volatility. Yet the same third parties are usually the weakest link in the digital money network, because they are vulnerable to hacking. In case of BitCoin the ability to serve as a unit of account is also jeopardized by its extremely high divisibility. One BitCoin is divisible to 10^{-8} Satoshi, and this could cause some problems for many people in terms of comprehending and comparing prices of goods and services.

Despite recognized imperfections, the prototype digital money functions as a medium of exchange. In fact it has a comparative advantage over traditional money in terms of speed and commission costs. BitCoin provides exchange similar to credit card payment or bank transfer for very little transaction cost. In fact it is just the cost of maintaining the system. Although transaction cost can increase if the user does not have the necessary skills to create own storage. If he or she uses a BitWallet service provided by the intermediating firm it might moderately increase the fee depending on the additional security measures or contract arrangements. Despite that, transaction costs in case of standard national currencies are much higher because institutions that provide financial services must cover more intermediary costs. Moreover in case of international transfers traditional money needs to compensate for additional procedures in the clearing system and additional authentication. The average cost of BitCoin transfer is less than 1 percent whereas traditional online payment charges the fees that are between 2-5 percent (Cianian, Rajcaniova and Kancs, 2016).

Notwithstanding that BitCoin offers almost instantaneous execution of the transfer and in case of traditional money the transfer in some cases can take up to several working days.
So what makes a prototype digital money popular if anonymity is only a myth? Most likely low transaction costs in comparison to traditional money. Not surprisingly Multinational Corporations soon after BitCoin begun to be popular started to accept it as a method of payment. For instance Microsoft accepts digital money for Xbox games, phone apps and software. Spendabit, Overstock, DuoSearch and BazaarBay specialize in the retail shopping and they all accept other digital money as well. Most of the prices are recalculated to USD for convenience, however DuoSearch shows them primarily in BitCoin.
A popular difference between prototype digital money and traditional money is that the former uses one integrated protocol that replace clearing system formerly managed by hundreds of commercial banks. BitCoin system is very efficient it can instantaneously process thousands of transactions without anyone's supervision. In time the network becomes more entangled and the mathematical problems require faster calculations. But so far digital revolution is able to keep up with its growing demand for computing power. The nexus of nodes consumes monstrous amounts of electricity. The great deal of the value of BitCoin is determined by the technology behind the speed of mainframes and the price of electricity. Semiconductor technology plays two roles in the price mechanism of digital money. In the short run when the computational power increases the value of BitCoin falls, but in the long run faster calculators are able to process more transactions and the efficiency of the network increases. Moreover, the price of electricity is linked with the nodes' incentive to maintain the network. Would a small commission be enough to sustain the network after deducting electricity costs? If not the network will collapse before it will reach 21 million BitCoins.
Before BitCoin reach 21 million units we can learn a great deal about possibilities created by trust based on consensus for instance that it allows transnational financial transactions that are as fast as SMS. Thanks to the speed of Internet bandwidth we are able to test new ideas and create new technologies that reduce the number of intermediaries or even create new markets and new business environments. BitCoin is one application of Distributed Ledger Technology. Can a digital money based on the blockchain become one day a national currency? Exploring this question leads to a deeper discourse about the nature of digital money – its strengths and weaknesses, opportunities and associated threats. Table 1 summarizes my analysis of the blockchain based digital money as a model for global currency.

Table 1 Strengths, Weaknesses, Opportunities and Threats associated with Digital Money

Strengths	Weaknesses
• Digital money has a comparative advantage as a medium of exchange over traditional money. The technology provides exchange similar to credit card payments, but it is very fast and significantly cuts transaction cost. • The technology can be adapted to cut the intermediary costs to many ledgers operating simultaneously. • Blockchain technology is very counterfeit resistant and censorship resistant. In case of fraud the nodes would register that the number of units do not match the total number of units produced. • Trust based on consensus significantly cuts the number of red tape. • Very fast transaction speed (especially international transactions). • Multiple copies of the ledger increase stability and safety.	• Consumes more computing power than it actually requires – its hashcash function overcompensates for the Moore's law. • Scarce number of units, irreversible transfer and anonymity links its value to cyber security. The last makes easier for cyber criminals to avoid the consequences of theft. • Experimental digital money is not a legal tender, and thus it is not linked with the economy of any country. Business and individuals accept it voluntarily what makes its adoption relatively slow. • High volatility might confuse users because they would be unable to spot its true relative price. • In the current stage of development digital money reminds more of a speculative investments than money. • Lack of control over murky or illegal transactions.
Opportunities	**Threats**
• Hashcash function has a build in parameter to compensate for increasing computing speed. The same parameter allows to edit minting speed according to needs of the economy what makes possible to use it (after modifications) as a tool for economic policy. • The system is constructed in such a way that producing counterfeit units it is not impossible, but highly impractical; anyone who possess a computing power of enough magnitude would find it more profitable to become an honest node. • Other applications: i.e.: for global supply chains, global medical database or legal actions embedded in financial system etc.	• The prototype digital money was designed to create inflation-free currency by applying artificial limit to number of total units produced by nodes. If cost of electricity and maintenance costs exceed the profits from the commission, the nodes can lose incentive to carry on the work. • Creating digital money that allows for reversible transfer is challenging because once nodes are in consensus any amendment would increase the entropy of the system and at some point the system could crash. • The system was designed to undermine trust bestowed in democratic institutions. It might serve as a Trojan horse.

Source: own elaboration

Digital money is reducing costs. The shared distributed ledger is decreasing the processing costs of operations and hence decreases transaction cost. Moreover the technology can be adapted to cut the intermediary costs to many ledgers at the same time. “Consider the process of buying a house, a complex transaction involving banks, attorneys, title companies, insurers, regulators, tax agencies and inspectors. They all maintain separate records, and it’s costly to verify and record each step. That’s why the average closing takes roughly 50 days. Blockchain offers a solution: a trusted, immutable digital ledger, visible to all participants, that shows every element of the transaction.” (Rometty, 2016)

Although the prototype digital money is not a good store of value. Some of the Individual Retirement Account (IRA) providers offer individual retirement accounts that provide direct ownership interests in BitCoin (Zweig 2017). The incentive comes from the prompt increase of the market value of BitCoin. In March 2012 one BitCoin was worth around 5 USD and six years later its price surpassed 1200 USD. However, BitCoins “unlikely to move up and down in sync with rest of (…) portfolio”, because BitCoin is wildly volatile (Zweig, 2017).

Blockchain technology is in the early stage of development. Is it safe in the current configuration? Storing digital money today can come with the risk. The network is based on the open source protocol that can be reviewed by anyone and accessed by everyone. The recent hacking incidents show that anyone with the sufficient knowledge can potentially gain access to third party storage databanks. The open-source nature of the code makes it also easier for the Black Hat Hackers to gain knowledge about the workings of the digital money storage systems. Would it not be safer if the code would be stored by central bank and the speed of mining process adapted to the needs of the economy? Perhaps it would.

Concluding comments

To engage with remote financial transactions people need trust. BitCoin a prototype digital money maintains a structural integrity with a new kind of trust based on the nexus established by the group of anonymous nodes. Despite being in the early stage of development the application of digital money created a global economic response of unprecedented power and quality. Digital money provides instant global transactions without trusted third parties or formal political arrangements. Moreover, even at current stage of development digital money have unique qualities that makes it increasingly popular i.e.: extreme resistance to counterfeit, to the point where it would be simply impractical because anyone who have the access to enough computing power, would find it more convenient and profitable to create legitimate units instead, and become the “Bank”. The network shifts the creation of money from government and banks to distributed nodes based anywhere in the world.

Despite widespread beliefs BitCoin is not free from the influence of the third parties. The price of BitCoin is influenced by governments that impose taxes on the price of electricity, the price of selected basket of other currencies – notably Chinese yuan and last but not least the narrow group of individuals that can in theory manipulate the reward for the node’s minting afford.

Currently the prototype digital money does not fulfill all criteria of the currency – mainly because of its immense volatility. However it allows instantaneous peer-to-peer transfer of value via Internet-based decentralized platform which many central banks consider a novelty worth exploring. The experimental digital money is still ‘evolving’ – its volatility over time decreases, therefore perhaps in the future it will progress beyond speculative investment. Technology behind digital money is based upon very efficient algorithm – it eliminates intermediaries, uses open-access architecture and creates trust based on cryptographic consensus. It applies a secure and counterfeit resistant one way hash functions that replace users identities and makes processing transactions very fast.

Creative destruction introduced by blockchain technology can create positive as well negative externalities. Positive spillover effects are associated with fast transaction speed, low fixed costs and reduction of intermediaries. Negative spillovers are associated with cryptographic anonymity that draws

the attention of i.e. drug or human traffickers or money launderers. Current experience in digital money development shows also that the weakest link in the safety of system is lined to third party organizations that try to take the role formerly reserved for banks – the so called cryptocurrency markets.

One of the main weaknesses of the prototype digital money can be associated with very limited ability to serve as a tool for economic policy. Though the inner algorithm is equipped with the parameter that can serve as an instrument changing minting difficulty and thus its supply. Because the prototype digital money is not a legal tender there is no institution that holds the reserve of digital money and hence there is no interest rate nor any Bank that lends digital money. Moreover adoption of BitCoin as a national currency would be dangerous, because the adopting economy would lose the ability to set up its monetary policy.

Application of blockchain technology will become increasingly important for governmental institutions, multinational corporations, international financial institutions and individuals. The technology in the public ledger mode is relatively easy to replicate but very hard to configure. Because of that the blockchain technology has many applications yet to be discovered in the near future. The technology behind digital money is still in the early stage of development, but it has already proven that it holds the potential to shape the future of global financialization.

References

Back, A. (2002) Hashcash – a denial of service counter-measure. Retrieved from http://www.hashcash.org/papers/hashcash.pdf

Bayer, D., Haber, S., Stornetta, W.S. (1993) Improving the efficiency and reliability of digital time-stamping Sequences II: Methods in Communication. Security and Computer Science, 329-334.

Bouoiyour, J., Selmi R. (2015) Bitcoin Price: Is it really that New Round of Volatility can be on way? Retrieved from http://mpra.ub.uni-muenchen.de/65580/

Castro, M., Liskov, B. (1999) Practical Byzantine Fault Tolerance Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA.

Cianian, P., Rajcaniova, M., Kancs d'A. (2016) The digital agenda of virtual currencies: Can BitCoin become a global currency? Inf Sys E-Bus Manage 14:883-919 doi: 10.1007/s10257-016-0304-0.

Cobham, J. (2016) Bitcoin and the Future of Money Harvard Political Review. Retrieved from http://harvardpolitics.com/united-states/bitcoin-future-money/

Dai, W. (1998) b-money. Retrieved from http://www.weidai.com/bmoney.txt

European Central Bank (2016) Opinion of the European Central Bank of 12 December 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. Retrieved from https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf

Economist, The (2016) Craig Steven Wright claims to be Satoshi Nakamoto. Is he? Retrieved from http://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin

Grigg, I. (2005) Triple Entry Accounting Retrieved from http://iang.org/papers/triple_entry.html

Haber, S. Stornetta, W.S. (1991) How to time-stamp a digital document. Journal of Cryptology, vol. 3, no 2, 99-111.

Haber, S., Stornetta W.S. (1997) Secure names for bit-strings. Proceedings of the 4th ACM Conference on Computer and Communications Security, 28-35.

Harrison, V. (2015) This could be the first country to go cashless. Retrieved from http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/

Henley, J. (2016) Sweden leads the race to become cashless society. Retrieved from https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe

Kitco News (2013) 2013: Year of the Bitcoin. Forbes. Retrieved from https://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/#1633fd66303c

Marr, B. (2016) How Blockchain Technology Could Change the World. Retrieved from http://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#72e19dcb49e0

Mankiw, G. N., Taylor P. M., (2009) Makroekonomia. Warszawa: Polskie Wydawnictwo Ekonomiczne.

Massias, H., Avila, X.S., Quisquater, J.-J. (1999) Design of a secure timestamping service with minimal trust requirements. In: 20th Symposium on Information Theory in the Benelux. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.6228

Moore. T., Christin N. (2013) Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. Financial Cryptogr Data Secur 7859, 25-33.

Nakamoto, S., (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Palmeri, T. (2016) Looking for Liberland. Politico. Retrieved from http://www.politico.eu/article/looking-for-liberland-serbia-croatia-vit-jedlicka-danube-swamp-anarchist-libertarian-utopia-taxation-flood-plain-swamp/

Plassaras, N. A. (2013) Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. Chicago Journal of International Law Vol. 14: No. 1, Article 12. Retrieved from http://chicagounbound.uchicago.edu/cjil/vol14/iss1/12

Rometty, G. (2016) How Blockchain Will Change Your Life The technology's potential goes way beyond finance. The Wall Street Journal. Retrieved from http://www.wsj.com/articles/how-blockchain-will-change-your-life-1478564751

Shin, L. (2017) Bitcoin's Price Was Volatile Last Week, But Not Last Year. Forbes. Retrieved from https://www.forbes.com/sites/laurashin/2017/01/09/bitcoins-price-was-volatile-last-week-but-not-last-year/#784fa1e8126f

Walport, M. (2015) Distributed Ledger Technology: beyond block chain. United Kingdom Government Office of Sciences. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Zweig, J.(2017) Should You Have Bitcoin in an IRA? The Wall Street Journal. Retrieved from https://www.wsj.com/articles/should-you-have-bitcoin-in-an-ira-1484341903