4(69) 2017

ISSN 1429-2939

BEZPIECZNY BANK

BFG

BANK GUARANTEE FUND

SAFE BANK is a journal published by the Bank Guarantee Fund since 1997. It is devoted to issues of financial stability, with a particular emphasis on the banking system.

All articles published in “SAFE BANK” are reviewed.

PUBLISHER:
Bank Guarantee Fund
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SECRETARY:
Ewa Teleżyńska, Małgorzata Polak
Telephone: 22 583 08 78, 22 583 05 74
e-mail: ewa.telezynska@bfg.pl; malgorzata.polak@bfg.pl

www.bfg.pl

DOM WYDAWNICZY ELIPSA

Typesetting and printing by:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel./fax 22 635 03 01, 22 635 17 85
e-mail: elipsa@elipsa.pl, www.elipsa.pl

DOI: 10.26354/bb.6.4.69.2017

Łukasz Cywiński*

WILL DIGITAL MONEY CROWD OUT NATIONAL CURRENCIES?

INTRODUCTION

The paper provides a contemporary discussion of functions and dangers related to digital money. And it assesses dangers inherent in the technology based on Bitcoin. The choice is motivated by Bitcoins' popularity in relation to other experimental digital money systems; since other protocols are merely clones of Bitcoins, this 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 DLT applies a universal heuristic approach by analyzing Strengths, Weaknesses, Opportunities and Threats (SWOT) with Bitcoin as a base-model for the global digital currency.

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 hitherto 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. Keeping that in mind

* Łukasz Cywiński works at the University of Information Technology and Management in Rzeszów.

this article concentrates on two scenarios: a) existing prototype digital money i.e. Bitcoin replacing national currencies in order to create a global virtual currency or b) adaptation of DLT by central banks.

DLT allows the elimination of a 'middle man' in a variety of transactions, which might help dramatically reduce red tape and transaction costs. DLT can do it by changing or by taking over three important roles; recording transactions, establishing identity and establishing contracts, which are traditionally carried out by the financial services' sector[1]. DLT allows for transferring and keeping track of all records in the nexus shared by many authorized users. For instance, DLT may help with creating an instant and lightweight global medical database.

The configuration of networks based on the concept of blockchain cryptosystem designed by Nakamoto[2] has been subject to scrutiny. One of its weaknesses is that the system that is both censorship resistant and entirely anonymous also in time becomes murky and dangerous. For example, Bitcoin enables the so called dark web, i.e., the market of 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 the long-run. It remains to be seen whether this would happen. Yet, Bitcoin (the most popular digital money), have been getting traction with its use becoming more widespread. So what makes the system deprived of authority self-sustainable? Digital money is based on trust achieved by the so called "consensus". This consensus is driven by anonymity ensured by cryptographic protocols and self-interest of the so called "nodes" –a creation of a software analyst and probably a hacker *alias* Nakamoto – who experimented with cryptographic protocol called proof-of-work. According to experts, the same could be done by applying other methods, i.e. proof-of-stake or practical Byzantine Fault Tolerance[3]. Bitcoin is a modified version of a protocol created to prevent rejection of service attacks or service abuses such as spam on a system by requiring some work from the service requester, usually by measuring the processing of computation.

Creating money from a system to sort spam is very unusual, therefore this paper assesses 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. What is the relationship between digital money as represented by Bitcoin

---

1 B. Marr, *How Blockchain Technology Could Change the World*, 2016, Forbes, http://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#72e19dcb49e0 [accessed: 12.01.2016].

2 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, Retrieved from https://bitcoin.org/bitcoin.pdf [accessed 11.08.2016].

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

and national currencies? Which properties make digital money attractive? Are there any potential benefits and threats associated with adopting DLT by central banks?

The remainder of this paper is organized as follows. The first part concentrates on the technology underpinning crypto-currencies and assesses its potential. The second part discusses main properties of bitcoins. The discussion of digital money as a possible substitute for national currencies is in part 3. The last part concludes.

DISTRIBUTED LEDGER TECHNOLOGY: ITS POTENTIAL

The Bitcoin blockchain technology's first application allows an instantaneous transfer of value through the Internet via decentralized online platform[4]. 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 a 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.

The Blockchain network represents the essence of the Schumpeterian creative destruction to the ways of storing, processing and organizing financial data. It takes advantage of the decentralized network, but at the same time it applies symmetry of information by creating multiple copies of the ledger. The Bitcoin network was the first large-scale experimental application of the Distributed Ledger Technology. And equally to the World Wide Web – that evolved beyond the email and the webpage – the Distributed Ledger Technology, based on various types of blockchains, bears the potential to evolve beyond Bitcoin or currently available digital money.

Private digital money is possibly the most obvious application of DLT. Therefore, it provides the best example for understanding the principles behind the core mechanics of the network. 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

[4] B. Marr, *How Blockchain Technology Could Change the World*, 2016, Forbes, http://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#72e19dcb49e0 [accessed: 12.01.2016].

successful. And in the case of digital money that two parties made a transaction. Quintessentially, this is analogical to sending an important letter or a coded note. That note includes a public stamp – recognized by everyone and a secret seal used to decrypt the massage. Both the stamp and a secret seal are coded by a powerful cryptographic protocol.

The fundamental property of the abovementioned 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 announcement is not only a declaration that the transaction took place. But over time it also becomes – after it has been processed with other similar transactions – a much desired bit of a "golden nugget". This happens because 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 sorted and converted, the same way we recycle paper leaflets or notes, but faster – and they are chained with other transactions the same way we blend a papier-mâché. The Blockchain is an anonymous block of linked notes or banknotes.

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 the case of digital money that the note is real.

But, where does the nodes' incentive come from? Nodes perform a process similar to paper recycling factories that add fiber to the papier-mâché. Computer program is designed to do the same thing. And allows nodes to collect the extra part, extra Bitcoin and sometimes even a small commission. The authenticity of digital money is ensured by the existing blockchains of previous transactions. "The first Bitcoins were transacted in January 2009 and by June 2011 there were 6,5 million Bitcoins in circulation among 10,000 users."[5] Since then, nodes and users, proved that establishing trust on cognitive module based on self-interest and anonymous secrecy is possible.

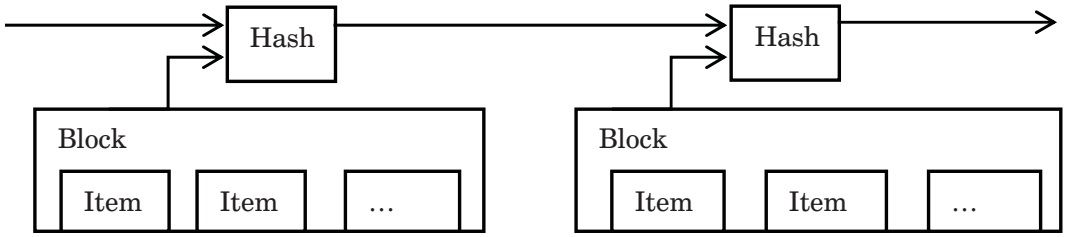
The symmetry of information, the balanced ledger or the public consensus in the case of prototype digital money is maintained automatically without any involvement of third parties. This is possible because the more users make transitions with i.e. Bitcoin the more trustworthy the currency becomes. The

---

[5] F. Reid, M. Harrigan *An Analysis of Anonymity in the Bitcoin System*, 2011, International Conference of Privacy, Security, Risk and Trust and IEEE on Social Computing DOI: 98-0-7695-4578-3/11.

cryptographic algorithm accepts only very specific strings of data – only *hash* values recognized by all nodes in the system holding copies of previous public ledgers. To achieve that recognition – or 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. $H_{23} = H(y_2 \mid y_3)$ that are needed for verification are continued to be processed as long as the single value is obtained – the so called: round root value[6], hereinafter RH_i, and for previous transaction RH_{i-1}. The timestamp for a completed block of transactions is than $yn = \{(y_{n-1}), (H_{n-1}), (H_n), (RH_{i-1})\}$. Figure 1 demonstrates chaining blocks of transactions with hash.

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



Source: S. Nakamoto, *Bitcoin…*, *op. cit.*.

The 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[7]. The hashcash scans H_n back until it receives a zero-bit value hash. It was precisely this function that was originally created to assess the value of the spam that "throttle systematic abuse of un-metered internet resources such as e-mail"[8]. It is a CPU-cost function that computes a special token used as a proof-of-work. In the 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 consists 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

6 See: D. Bayer, S. Haber, W.S. Stornetta, *Improving the efficiency and reliability of digital time-stamping Sequences II: Methods in Communication* 1993 Security and Computer Science, pp. 329–334 and H. Massias, X.S. Avila, J.-J. Quisquater, *Design of a secure timestamping service with minimal trust requirements,* 1999, 20th Symposium on Information Theory in the Benelux, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.6228 [accessed: 11.08.2016].

7 A. Back, *Hashcash – a denial of service counter-measure*, 2002, http://www.hashcash.org/papers/hashcash.pdf [accessed: 11.08.2016].

8 A. Back, *Hashcash – a denial of service counter-measure*, 2002, http://www.hashcash.org/papers/hashcash.pdf [accessed: 11.08.2016], p. 1.

of the semiconductor-based computers. *Chal*() function becomes the public announcement, because it contains $H(\cdot)$ with defined size of bits l. The procedure takes the following form:

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

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"[9]. According to Nakamoto[10] if a hacker assembles more CPU power than all honest nodes combined, he or she would find it more profitable to use this power to generate new coins rather than to destroy the system. In the 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.

Bitcoin or other digital money is just one of many applications of the blockchain technology analogically to paper that can be used either to print money or news articles or leaflets. It is discussed that augmented blockchains can be used to hold medical data or store complex information about cross-border value-added transactions. In principle, this would allow for the low-cost, constant flux of information exchanged between multiple clients, multiple institutions or multiple enterprises. In other words, in contrary to the paper note, the main property of distributed digital ledger is constant change and instant self-recyclability. Despite its unquestionable utilities, the blockchain technology might also have yet undiscovered limitations.

THE MAIN PROPERTIES OF BITCOIN

The technology behind Bitcoin – the first experimental application of a distributed ledger based on the blockchain – spawned many replicas, all pulling from the same open source code. Thus, it does not come as a surprise that nowadays the Internet is overcrowded with other versions of private digital money, such as Ethereum or Ripple – all competing to become the global currency. The Bitcoin,

[9] S. Nakamoto, *Bitcoin…*, *op. cit.*
[10] *Ibidem.*

however, is the most popular application of DLT so far, and the first that was called 'the money ofthe future'.

The Bitcoin has attracted transactions worth billions of US dollars. However, does it fulfill the three most important functions 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 purchasers give to suppliers when they want to acquire commodities or services. To be a unit of account, it needs to be a standard people are willing to use to post prices and record debts. Finally, to be a store of value it needs to be a thing that people can use to transfer purchasing power from the present to the future.

According to Krugman[11] "the Bitcoin is evil", and he is not convinced that it can serve as a good store of value. He compares the 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 compares this to the value of gold limited by the mining technology. This is not a well-founded analogy as the Bitcoin is (a) limited by the semiconductor technology, with yet undiscovered nor fully understood limitations; and (b) the decision to limit its supply was made arbitrarily by a team of programmers and not by the technology's limitations.

The technology was designed to render impossible for third parties to manipulate the price. There are, however, organizations striving to take control over the supply of Bitcoins and set new rules on the minting process. Theoretically, minting rules could be amended while still maintaining all blockchain processes. From 2009 to 2011 the Bitcoin development was managed by Nakamoto (according to The Economist's 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 the Bitcoin Foundation that manages further software development of the Bitcoin network and that foundation has the necessary resources to control the supply rules.

According to Egorova's and Torzhevskiy's[12] (2016) the supply rules for Bitcoin can be represented by the function: $Q = A[1 - \exp^{-S_i t}]$, where, Q – is a theoretical quantity of the Bitcoin, A – the limit of 21 million bitcoins (imposed by its founders), i denotes the number of nodes in the system, t denotes time, and S is a function parameter which defines growth acceleration or deceleration depending on the so called halving rule. The *modus operandi* of the halving rule creates a discrete reward to the amount of compensation. In the case of Bitcoin this could be represented by:

---

[11] P. Krugman, *Bitcoin is Evil*, 2013, Retrieved from https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/.

[12] N.E. Egorova, K.A. Torzhevskiy, *Bitcoin: Main Trends and Perspectives*, 2016, British Journal of Economics, Management & Trade, 12(1) pp. 1–11.

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

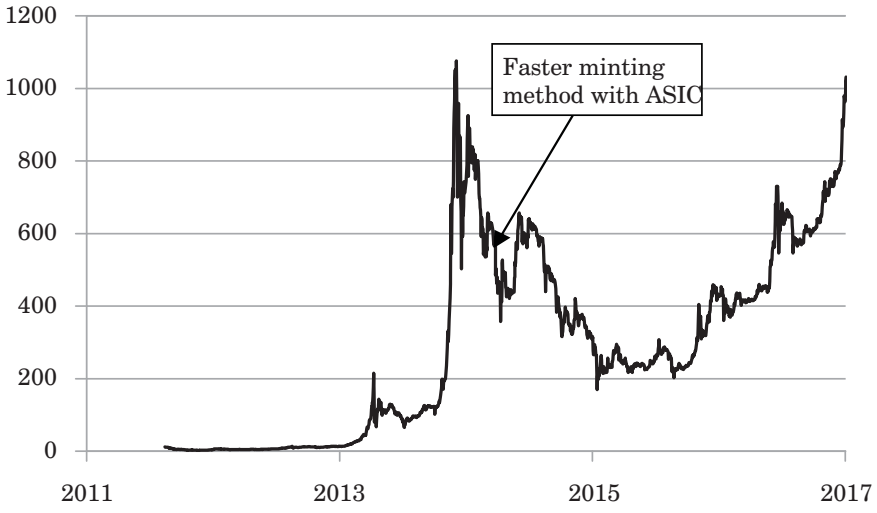
where $q = 0.5$ – correction coefficient, j – in this case represents a correction number for emission reward and S_0 is a first time reward (50 bitcoins); $t \in [0,T]$. Conditional, yet programmable supply rules combined with unspecified supervision is the reason that makes Bitcoin unable to serve as a tool for the economic policy.

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 – i.e. a conglomerate of anonymous nodes. The initial idea behind the Bitcoins was that as the limit is reached, the incentive for the nodes would change from the reward to a small commission. In the case of Bitcoin the commission for each node i is:

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

In the case of digital money the minting rules are the most important factor of the 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. Moreover, the efficiency of the 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 the Application Specific Integrated Circuit (ASIC) based systems (Figure 2).

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



Source: own elaboration based on 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 the period between 2013–2015 the total number of bitcoins increased from 10.6 million to13.7 million units). In the long run this might threaten the network integrity, therefore the minting was deliberately hardened in the halving process. The price of the Bitcoin again skyrocketed to more than USD 1000 per Bitcoin. More people became interested in new, peculiar money and wanted to acquire it. This created a business opportunity for nodes that stored previously minted bitcoins, they founded companies which offered so called BitWallets or Bitcoin Gambling Sites. Popular despite the fact that they offer limited security.

The ability to perform as a store of value and unit of account in the case of the Bitcoin is related to cybersecurity. In the present configuration the Bitcoin is based on the advanced crypto-technology and facilitates an irreversible transfer. It should not come as a surprise that this property of the 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[13]. 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 the stolen property. In the past, the main task of a bank was to provide safety from theft. The digital money market does not guarantee compensation for the 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[14].

The cybercrime is not the only argument against bitcoins as the currency. One of the main properties that distinguish the Bitcoin from traditional money is its volatility. The price of the 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[15] "Bitcoin volatility process seems more influenced by negative (bad news) than positive shocks. Not surprisingly, the Bitcoin market is highly driven by self-

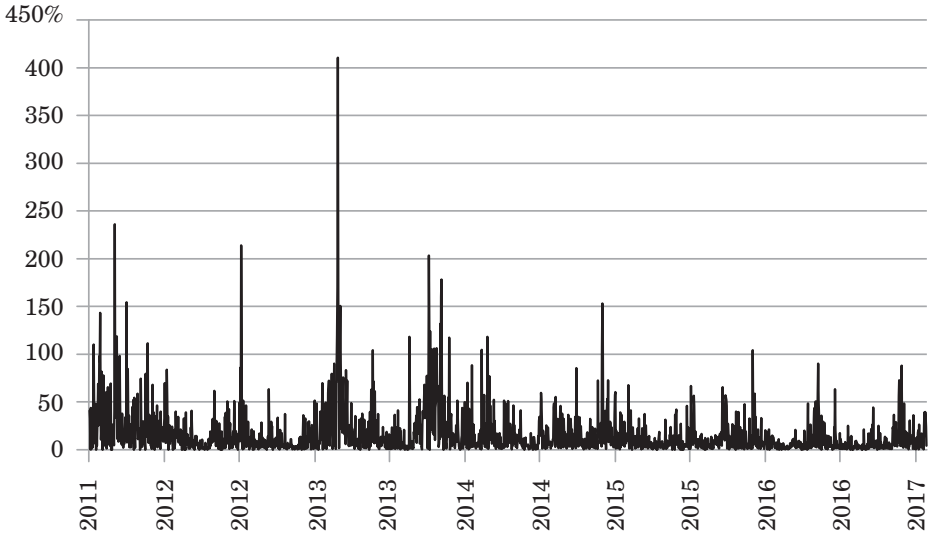
[13] P. Vigna, *People Love Talking About Bitcoin More Than Using It*, 2017, The Wall Street Journal, https://www.wsj.com/articles/people-love-talking-about-bitcoin-more-than-using-it-1491989403 [accessed: 16.04.2017].

[14] T. Moore, N. Christin *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, 2013, Financial Cryptography Data Security 7859.

[15] J. Bouoiyour, Selmi R., *Bitcoin Price: Is it really that New Round of Volatility can be on way*?, 2015. Retrieved from: http://mpra.ub.uni-muenchen.de/65580/, p. 10.

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.

Figure 3. Bitcoin's decreasing volatility in 2011–2017



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

The 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 the Bitcoin short-run volatility increase costs of doing 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 a particular good or service. In the case of the 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} so called Satoshi, and this could cause some problems for many people in terms of comprehending and comparing prices of goods and services.

Using Bitcoin requires an initial investment. This includes an intangible investment, such as getting acquainted with the general principles of the software, and tangible investments, such as setting up and installing equipment for the payment system. In some cases the specialized gear can be substituted with the commonly accessible mobile electronic devices. But then again, mobile phones are easily hacked. The level of general computer knowledge in the case of prototype digital money needs to be at least intermediate. And advanced users will be better equipped to deal with many dangers associated with the cybercrime. More

proficient users can even become "the bank", although the code of the Bitcoin is complex and requires both analytical skills and some background in economics.

There are no international laws regulating DLT, and certainly no global agenda nor any agreement that would tackle it from the legal point of view. That is why in reality, the price of the Bitcoin depends on many issues probed and exploited by governments. In November 2013 the Chinese Central Bank (CCB) barred other banks from managing Bitcoin transactions. As a result, the global demand for bitcoins decreased significantly, but it did not stop the trade over the "Chinese Internet". Officially the CCB's decision was motivated by the fact that Bitcoin is not backed-up nor represented by any country, and therefore could not have the same legal status as the yuan. And this argument has a strong merit. Over the last few years the Bitcoin became very popular in China. In 2016 more than 95% of the Bitcoin trade took place in that country alone[16].

The Chinese use of Bitcoin differs from most "shocks" presented later in this paper because demand for Bitcoin in China is propelled primarily by demand created by the institutional regime itself. Investors from China use Bitcoin to buy other currencies discreetly outside the attention of the government. Trading fees in China are high due to the national bank's policy to keep the yuan's exchange rate under the 2 percent daily change. The Bitcoin allows to bypass the fees and maintain the anonymity at the same time. Does the Chinese government see Bitcoin as a Trojan horse designed to leak the capital out of the country? Perhaps it does, because in January 2017 the Bank of China tried to prevent the outflow by devaluing the yuan and requiring Bitcoin exchanges to suspend withdrawals until they updated compliance systems. In theory, this could "kill" the Bitcoin with one swift blow, but investors quickly realized what was happening and the drop in the price was noticeable, but not devastating. The Chinese Internet, despite the general belief, is not entirely censored by the government, its users conduct essential business or surf the web via Virtual Private Networks.

For many people the Bitcoin is 'the alternative money'. Before April 2013 (see the figure 2) the value of Bitcoin was increasing only moderately. That changed when "investors started to pay attention to the crypto-currency; the enthusiasm for Bitcoins even propelled prices to briefly trade higher than gold"[17]. In 2013 the price of the Bitcoin was increasing partially because of the Cypriot banking crisis and the abovementioned Chinese demand. In the case of the former, one of the conditions of the EU and IMF bailout – after the Cyprus' government decided to nationalize its Popular Bank in response to Greek deposits' withdrawal in

---

16 L. Shin, *Bitcoin's Price Was Volatile Last Week, But Not Last Year*, 2017, Forbes, https://www.forbes.com/sites/laurashin/2017/01/09/bitcoins-price-was-volatile-last-week-but-not-last-year/#784fa1e8126f [accessed: 15.03.2017].

17 See: Kitco News *2013: Year of the Bitcoin*, 2013, Forbes. https://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/#1633fd66303c [accessed: 15.03.2017].

2009–2011 – was to levy a tax on deposits. When Cypriots learned about the deal, they rushed to banks to withdraw the money. The Bitcoin's price surged shortly thereafter because people from Spain and Greece anticipated similar problems and started to reallocate money outside the banking system. The Bitcoin was therefore used to 'hide' the money prior to an anticipated crisis.

Shifting money outside the banking system anonymously and safely requires advanced knowledge. Most of the registered blockchain transactions are not entirely anonymous. The secrecy is only an option reserved for users that are able to set up their own storage and secure network, which is equally hard. The majority of other users make Bitcoin transactions and store Bitcoins on private exchange markets. To set up a fully functional account, these third parties usually require a passport, an ID card, a driving license, a proof of residency, a bank statement or a tax return in order to verify the account.

So what makes prototype digital money so popular if anonymity is only a myth? Most likely, low transaction costs in comparison to traditional money. Not surprisingly, multinational corporations, soon after the Bitcoin became popular, started to accept it as a method of payment. For instance, Microsoft accepts bitcoins 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.

There is another reason why it is not safe to make the Bitcoin a national currency at least in its current stage of development. At the end of 2016, the Chinese government decided to devaluate the yuan which shortly thereafter increased the price of the Bitcoin – the stress on the Chinese financial market shifted investors' attention mainly towards private digital money. The Chinese government wanted to stop its citizens moving money out of the country, and at the beginning of January 2017, set new anti-money laundering rules. Chinese Bitcoin trading sites had been temporarily shut down until they proved to meet the necessary legal requirements. This caused the price of the Bitcoin to plunge over 31% in less than two weeks from US$ 1129.87 to US$ 775.89. Let it be assumed that more countries adopted the Bitcoin currency as their own, for instance on the similar terms as Kosovo and Montenegro adopted the Euro as the national currency. Consequences of the China's anti-money laundering policy – otherwise a good policy – could have catastrophic impact on trade of these hypothetical adopters, and perhaps on others, as well. If the Bitcoin became a global currency adopted by many countries would it become a Trojan horse designed to undermine the trust bestowed in democratic institutions? The Table 1 summarizes the present analysis of the blockchain-based digital money as a model of the global currency.

The Bitcoin is an experimental application of digital money. Is it not safe to treat it as a candidate to become a global currency in its current configuration?

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 costs. ❖ The technology can be adapted to cut the intermediary costs to many ledgers operating simultaneously. ❖ The blockchain technology is very counterfeit resistant and censorship resistant. In case of a fraud the nodes would register that the number of units does not match the total number of units produced. ❖ Trust based on the consensus significantly cuts the number of the red tape. ❖ High 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 the cyber security. These factors make it easier for cyber criminals to avoid consequences of a theft. ❖ Experimental digital money is not a legal tender, and thus it is not linked with the economy of any country. Businesses and individuals accept it voluntarily, which 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 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 which makes it possible to be used i (after modifications) as a tool for the economic policy. ❖ The system is constructed in such a way that producing counterfeit units it is not impossible, but highly impractical; anyone who possesses 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 databases or legal actions embedded in the financial system etc.	❖ The prototype digital money was designed to create inflation-free currency by applying artificial limit to the number of total units produced by nodes. If the cost of the electricity and maintenance costs exceed the profits from the commission, the nodes can lose the incentive to carry on the work. ❖ Creating digital money that allows for a 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 the trust bestowed in democratic institutions. It might serve as a Trojan horse.

Source: own elaboration.

For instance, storing digital money today is too risky. 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. All you need is to know what you are looking for, and match identities with the *hash*. However, the Bitcoin is just one application of the Distributed Ledger Technology. Can an improved version of digital money based on the blockchain principle become one day a national currency? Exploring this question leads to a deeper discourse about the nature of digital money – its defined strengths and weaknesses, opportunities and associated threats.

DIGITAL MONEY AS A NATIONAL CURRENCY

At the current – experimental stage of development, digital money can create tangible threats to national economies. The Bitcoin for instance, represents the idea of the crypto-anarchy imbedded in the financial system. It introduced a system where "the government is not temporarily destroyed but permanently forbidden and permanently unnecessary"[18]. Perhaps, this is why when adapted on the global scale, it would become a Trojan horse destined to undermine trust bestowed in governmental institutions.

Despite obvious dangers, as a medium of exchange even the experimental or prototype digital money enables transactions that are quicker and less expensive than any former form of a bank transfer. Therefore, a fully developed blockchain network – that applies concepts of the distributed ledger combined with secure and experienced institutions would create abundance of very useful financial applications. For instance, international transactions as easy, and as quick as sending an SMS.

The prototype digital money already functions as a good medium of exchange. In fact, it has a comparative advantage over traditional money in terms of the speed and commission costs. The Bitcoin i.e. provides exchange similar to a credit card payment or a bank transfer for a very little transaction cost. Those costs in the case of standard national currencies are much higher because institutions that provide financial services must cover more intermediary costs. Moreover, in the case of international transfers, traditional money needs to compensate for additional procedures in the clearing system and additional authentication. The average cost of a Bitcoin transfer is less than 1 percent, whereas a traditional online payment charges the fees that are between 2–5%[19]. Notwithstanding that

[18] W. Dai, *b-money*, 1998 , http://www.weidai.com/bmoney.txt [accessed: 11.08.2016].

[19] P. Cianian, M. Rajcaniova, d'A. Kancs, *The digital agenda of virtual currencies: Can BitCoin become a global currency?*, 2016, Inf Sys E-Bus Manage 14:883-919.

Bitcoin offers almost instantaneous execution of the transfer and in the case of traditional money, the transfer in some cases can take up to several working days.

What costs could be reduced? The shared distributed ledger is decreases the processing costs of operations and hence decreases transaction costs. 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 itis costly to verify and record each step. That is why the average closing takes roughly 50 days. The Blockchain offers a solution: a trusted, immutable digital ledger, visible to all participants, that shows every element of the transaction."[20]

A popular difference between prototype digital money and traditional money is that the former uses one integrated protocol that replaces a clearing system formerly managed by hundreds of commercial banks. In this regard, the Bitcoin system serves as a good example – it can instantaneously process thousands of transactions without anyone's supervision. However, it needs to be noted that as the network becomes more entangled it would require faster calculators. So far, digital revolution is able to keep up with growing demand for computing power, but would it be the same if more people used blockchains?

The growing hunger for processing power increases electricity consumption. The nexus of nodes designed to process transitions on the country-level scale would consume monstrous amounts of electricity. The great deal of the value of the Bitcoin is determined precisely by the technology behind the speed of mainframes and the price of electricity. The semiconductor technology plays two roles in the price mechanism of digital money. In the short run, when the computational power increases the value of digital money would fall, but in the long run, faster calculators would increase the efficiency of the network.

In the case of prototype digital money i.e. the Bitcoin, the price of electricity is linked with the nodes' incentive to maintain the network. This might create a serious problem for the Bitcoin in the future. A small commission might not be enough to sustain the network after deducting electricity costs. Will the Bitcoin blockchain collapse before it reaches 21 million Bitcoins? Or perhaps this will be the time when blockchain-based national currencies will take over the space that it is currently occupied by the Bitcoin and alike.

Currently, the incentive to use digital money, such as Bitcoin is related to the number of existing users in the network. If only few businesses accepted Bitcoins as a method of payment, the encouragement to acquire costly equipment or

[20] G. Rometty, *How Blockchain Will Change Your Life The technology's potential goes way beyond finance*, The Wall Street Journal 2016, http://www.wsj.com/articles/how-blockchain-will-change-your-life-1478564751 [accessed: 29.11.2017].

investment of time to learn the technology would be rather moderate. One of the man challenges in becoming a global currency would be to convince users to conduct daily business using bitcoins[21]. So far, the number of the Bitcoin's users has been increasing, although not as fast as many enthusiasts claim[22].

It is doubtful that current prototypes of digital money can soon replace national currencies as many fervently convince. It is more likely that the national currencies learn to assimilate the DLT. The potential of the blockchain technology can be summarized by the fact that despite no government guarantees and the high volatility, and despite the market being far from mature, in 2016 there were 34 thousand businesses accepting various kinds of experimental digital money payments in 51 countries. Among them there are 16 multinational corporations, 180 financial institutions and 732 operators providing Automated Teller Machines (ATM) that accept and exchange digital money. Bitcoins are accepted by charities, such as Wikipedia, Red Cross and Amnesty International. From takeaways to knowledge-intensive services. In the hands of central banks this technology can be further improved and refined to produce a counterfeit-free and cheap financial system.

According to the European Central Bank[23], digital money or virtual money is a "digital representation of value that is neither issued by the central bank or public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored and traded electronically". However, this definition is precise in the light of further applications of the DLT or perhaps it describes only the private digital money? At the end of 2015, the Danish government proposed to switch entirely to cashless transitions[24] and in Sweden in 2016, more than 50% of bank branches no longer keep cash on hand nor take cash deposits[25]. If the Danish or Swedish central bank decided to switch to blockchain-based systems, would that not make it digital or virtual money?

The Blockchain technology seems to accelerate innovation in the global financial data management, and that is why many governments and central banks are interested in assimilating and perhaps improving this technology in the near

---

21 P. Cianian, M. Rajcaniova, d'A. Kancs *The digital agenda…*, *op. cit.*

22 See: J. Cobham, *Bitcoin and the Future of Money*, Harvard Political Review 2016, http://harvardpolitics.com/united-states/bitcoin-future-money/ [accessed: 04.04.2017].

23 European Central Bank *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*, 2016, Directive 2009/101/EC. Retrieved from https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf, p. 3.

24 V. Harrison, *This could be the first country to go cashless*, 2015, http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/ [accessed: 11.05.2017].

25 J. Henley, *Sweden leads the race to become cashless society*, 2016, https://www.theguardian com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe [accessed: 11.05.2017].

future. The Blockchain is the multipurpose technology, and that is why various institutions and companies think about different applications for it.

In December 2015 the British Government was advised to support the following companies: Digital Catapult, Future Cities Catapult, and Open Data Institute. The UK government also created the Alan Turing Institute – specializing in the data science that will help to create "cryptocurrencies for British institutions". According to Grigg[26] there are several kinds of institutional and business points of interests for the blockchain technology: the cryptography (as a science), software engineering, property rights control, accounting, governance, and finance. Showing a trend, distributed ledgers will be used in the future.

The Bitcoin creates the environment where nodes have enough incentive to willingly give up their processing power, time and electricity consumption to manage working stations constantly calculating extremely difficult mathematical problems by adding transactions to the next blockchain – bit after bit. Perhaps Central Banks can create similar systems of incentives that will honor nodes minting digital money? According to Sir Mark Walport[27] – the UK Government Scientific Adviser – Governmental Institutions need to adapt to the DLT and assimilate this technology into their structures. So far, in 2016 and 2017 only a small number of governments experimented with the DLT treating it seriously – with the British and Estonian governments leading the way in Europe. In the future, adopting blockchains might be not just efficient, but necessary because (despite crypto-anarchic assumptions) increasing difficulty and decreasing profitability of minting will make nodes lose the interest in sustaining the network. At that point, it will be up to the governments to take over.

Can the blockchain become a national currency and replace cash? Probably yes. But only if governments have the control over the code that creates the blockchain and can limit the influence of other governments over the work of nodes. Otherwise, digital money cannot serve as a tool for the economic policy.

The Blockchain technology is expected to transform the banking industry. According to Guo and Liang[28] , the DLT might become a new source of growth that will reverse its current downward trend in innovations. They call the blockchain technology "the greatest disruption of the Internet finance for the traditional banking industry".

---

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

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

28 Y. Guo, C. Liang *Blockchain application and outlook in the banking industry*, 2016, Financial Innovation 2:24 DOI: 10.1186/s40854-016-0034-9.

CONCLUDING COMMENTS

To engage with remote financial transactions people need trust. The Bitcoin – a prototype digital money – provides trust based on the self-interest of the group of anonymous nodes. It does it despite being in the early stage of development. Notwithstanding that its presence created a global economic response of unprecedented power and quality. As the prototype, the Bitcoin provided instant global transactions without trusted third parties or formal political arrangements. It demonstrated that even at the current stage of development the prototype digital money has unique qualities i.e.: extreme resistance to counterfeit, to the point where it would be simply impractical to counterfeit because anyone who have the access to enough computing power, would find it more profitable to create legitimate units instead, and become the "Bank".

At the current stag,e experimental blockchain networks shift the creation of money from the government and banks to distributed nodes based virtually anywhere in the world. Despite the widespread beliefs, the Bitcoin is not free from the influence of third parties. The price of the Bitcoin is influenced by governments that impose taxes on the price of electricity, and the price of a selected basket of other currencies – notably the Chinese yuan. Moreover, the Bitcoin is not free from influence – it is controlled by a narrow group of individuals that can, in theory, manipulate the reward system for the node's minting effort.

Currently, the prototype digital money does not fulfill all criteria of the currency – mainly because of its immense volatility. Therefore, it cannot be used as a national currency, nor the global currency. The Bitcoin cannot serve as a tool for the economic policy. However, its other properties allow it to become very popular. Mainly the 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. The technology behind digital money is based on a very secure algorithm. It applies a secure and counterfeit resistant *hash* functions that replace users, identities and makes processing transactions very fast.

The Blockchain technology can create positive, as well as negative, externalities. The positive effects are associated with fast transaction speed, low fixed costs and reduction of intermediaries. The negative effects are associated with cryptographic anonymity that draws the attention from e.g. drug or human traffickers or money launderers. The current experience in digital money development shows also that the weakest link in the safety of the 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 is associated with the very limited ability to serve as a tool for the 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.

Acknowledgments

Acknowledgments should be given to Bartłomiej Kamiński for taking the time to provide very important comments and suggestions. Acknowledgments should also be given to the anonymous reviewer for helpful and constructive comments that greatly contributed to improving the final version of the paper. Needless to add, the author is solely responsible for expressed views.

The article is an effect of the project – „Financialization – New Trends and Directions of Development" – international conference, conducted by the University of Information Technology and Management in Rzeszów with the National Bank of Poland under the scope of an economic educational program.

Abstract

Despite a relatively short period that elapsed since the development of the 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 the DLT, with a special emphasis on the first experimental digital money, applying a heuristic SWOT analysis. It includes the analysis of properties of the Bitcoin in comparison to traditional money together with detailed examination of protocols that created it in terms of associated dangers.

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

References

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

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

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

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

Cianian P., Rajcaniova M., Kancs d'A., *The digital agenda of virtual currencies: Can BitCoin become a global currency?*, 2016, Information Systems E-Business Management 14:883-919 doi: 10.1007/s10257-016-0304-0.

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

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

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

Egorova N.E., Torzhevskiy K.A., *Bitcoin: Main Trends and Perspectives*, 2016, British Journal of Economics, Management & Trade, 12(1).

European Central Bank *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*, 2016, Directive 2009/101/EC. Retrieved from https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf.

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

Guo Y., Liang C. *Blockchain application and outlook in the banking industry*, 2016, Financial Innovation 2:24 DOI: 10.1186/s40854-016-0034-9.

Haber S., Stornetta W.S., *How to time-stamp a digital document*, Journal of Cryptology 1991, Vol. 3, No. 2.

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

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

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

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

Krugman P., *Bitcoin is Evil*, 2013, Retrieved from https://krugman.blogs.nytimes.com/2013/ 12/28/bitcoin-is-evil/.

Marr B., *How Blockchain Technology Could Change the World*, 2016. 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., *Makroekonomia*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2009.

Massias H., Avila X.S., Quisquater J.-J., *Design of a secure timestamping service with minimal trust requirements*, 1999, 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., *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, 2013, *Financial Cryptography Data Security* 7859, 25-33.

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

Palmeri T., *Looking for Liberland*, 2016, 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., *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, Chicago Journal of International Law 2013, Vol. 14, No. 1, Article 12. Retrieved from http://chicagounbound.uchicago.edu/cjil/vol14/iss1/12.

Reid F., Harrigan M., *An Analysis of Anonymity in the Bitcoin System*, 2011, International Conference of Privacy, Security, Risk and Trust and IEEE on Social Computing DOI: 98-0-7695-4578-3/11.

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

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

Vigna P., *People Love Talking About Bitcoin More Than Using It*, The Wall Street Journal 2017. Retrieved from https://www.wsj.com/articles/people-love-talking-about-bitcoin-more-than-using-it-1491989403.

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

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