

[DOI: 10.20472/EFC.2017.008.005](https://doi.org/10.20472/EFC.2017.008.005)

ANNA IWONA PIOTROWSKA

WSB University in Toruń, Poland

DARIUSZ PIOTROWSKI

Nicolaus Copernicus University in Toruń, Poland

BARRIERS TO THE FUNCTIONING OF THE BITCOIN SYSTEM - USER ASSESSMENT

Abstract:

Bitcoin is a system created to service micro-payments in e-commerce, as well as the digital unit of value functioning in the system's environment. When analysed, the behaviour of market participants indicates that the introduction of investment applications of the cryptocurrency, in parallel with its original payment application, had a tremendous impact on the larger-scale functioning of the system. This was aided by the functioning of many trading platforms allowing for exchange into traditional currencies and a high volatility of quotations.

Without doubt, bitcoin may be branded a ground-breaking financial innovation or a work of genius. However, the growing, and even global use of bitcoin has brought some of the system's imperfections to light. As the system developed, bitcoin users started to have a better view of the threats to the correct functioning of the system arising from its construction.

The paper aims to indicate the main barriers limiting the functioning of the bitcoin system, and its use in payments in particular. The work has adopted the following research hypothesis: In the early stages of bitcoin functioning, users had little awareness of the technological flaws of the system. The study analyses the literature on the subject and the results of a survey carried out among Polish bitcoin users. The analysis confirms of the research hypothesis, as it shows that in the system's first several years, users identified the following threats to the system's functioning: the speculative nature of bitcoin, the lack of adequate awareness in society which would allow for a widespread use of the innovation, potential too strict regulation of the cryptocurrencies market or its banning. The authors also present threats to the functioning of the system which in their opinion are of greatest importance at the moment. These relate to the existence of intermediaries, the lack of systemic incentives addressed to bitcoin merchants, growing costs and payment processing time. The authors intend to indicate those aspects of bitcoin's functioning in order to make the use of cryptocurrencies more conscious and contribute to limiting financial risk of system users.

Keywords:

Cryptocurrency, bitcoin, financial innovation, operational risk

JEL Classification: F65, G20, O31

Introduction

Bitcoin is in an innovative payment system and the unit of value functioning therein. Technological solutions applied in the bitcoin system were intended for carrying out micro-payments in e-commerce which are marked by high security levels, low costs and extensive anonymity. At the initial stage, when the system users were a small group of people fascinated with the idea of bitcoin, importance was ascribed to the original application of the cryptocurrency, i.e. for payment purposes. However, the development of the bitcoin system expressed in high volumes of transactions concluded is more related to the proliferation of the cryptocurrency's use in investments. System participants started seeing bitcoin is a type of alternative investment, rather than an instrument for making payments. This is also reflected in papers in the field of finance referring to the issue of bitcoin as they often analyse the behaviour of the cryptocurrency's quotations (Kristoufek, 2015; Brandvold, Molnar, Vagstad, Valstad, 2015; Baek, M. Elbeck, 2015; Cheung, Roca, Su, 2015; Ciaian, Rajcaniova, Kancs 2016). The study of available literature on the subject has shown that relatively little attention has been devoted to the use of bitcoin in payments (Polasik, Piotrowska, Wiśniewski, Kotkowski, Lightfoot, 2015; Leung, Dickinger, 2017; Schuh, Shy, 2015) and that the adopted systemic solutions were not perceived as a particularly significant limitation on the basic function of bitcoin.

The several years during which the world could observe the functioning of the system have undoubtedly proven its creator's genius. Nevertheless, the bitcoin system is not a perfect product. The development of bitcoin, and in particular the ever wider and more active use of the cryptocurrency, has shed light on certain imperfections which may threaten the effective functioning of the system in line with its underlying idea.

The paper aims to indicate the main barriers limiting the functioning of the bitcoin system, and its use in payments in particular. We have adopted the following research hypothesis: In the early stages of bitcoin functioning, users had little awareness of the technological flaws of the system.

The paper presents selected results of a pioneer study of Polish bitcoin users carried out by one of us between February and July 2014. The study employs a questionnaire survey distributed through online channels and in person during conferences regarding the matter. This contributed to a very broad outreach of the study. To the best of our knowledge, survey invitations containing a link to an anonymous online questionnaire were placed on all Polish websites visited by people interested in bitcoin that were operational during the study period, such as: forums, blogs, news services and social media¹. The survey received answers from 628 respondents², with the number of bitcoin users in Poland at that time estimated at 10–20 thousand at maximum.

¹ Services covered by the study: bitcoin.pl, bitcoin4u.pl, forum.bitcoin.pl, satoshi.pl, facebook.com.

² The survey was addressed to people interested in the cryptocurrency. The vast majority of respondents (86%) were already holding bitcoin.

Idea and basic assumptions of the bitcoin system

In our opinion, bitcoin is the first cryptocurrency verified in practice, used for payment and investment purposes, based on an open source system using cryptographic technologies in a distributed network of users to issue the cryptocurrency, register transactions and verify their correctness. Understanding the nature of bitcoin requires understanding its underpinning technological and ideological factors. This specific combination has had an impact on how the system is formed, and it largely justifies the literature's use of the notion of financial innovation with regard to bitcoin (Grinberg, 2012; Brito, Castillo, 2016; Kelly, 2015). From the technological viewpoint, the on-line emergence of the paper *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008), followed by the cryptocurrency itself, was the culmination of many years of attempts to create fully functional digital money. The solution proposed by S. Nakamoto is based to a large extent on the previously presented concepts regarding the issue of user anonymity and system decentralisation (Barber, Boyen, Shi, Uzun, 2012; Moore, 2013; Franco, 2015). Those two features of a payment system were particularly important for liberal cryptographers from the cypherpunk movement (May 1992; Hughes 1993). The developer of the bitcoin system knew this group and shared some of their ideas.

When put to analysis, the manifesto *Bitcoin: A Peer-to-Peer Electronic Cash System* indicates that S. Nakamoto was aiming at reducing costs of transactions carried out using electronic channels. This was to be attained by departing from the principle of trust and founding the payment system on cryptography, as well as introducing irreversible transactions. S. Nakamoto remarked that a third party authenticating transactions in electronic commerce and the option to reverse an electronic payment decrease the system's cost effectiveness.

When constructing the system, S. Nakamoto used a model of communication between Internet users based on a peer-to-peer network (Feld, Schönfeld, Werner, 2014). A network of equal participants has no hierarchical structure, no central unit, and different functions may be performed by any participant. This solution has contributed to creating a distributed system structure which granted considerable protection against destruction.

The issuance of cryptocurrency units in the bitcoin system is limited in time and automatic, and results from solving certain mathematical puzzles. New bitcoin units are a form of rewarding miners who by creating the correct block also verify the correctness of transactions submitted to the system. The reward was 50 bitcoins when the system launched in 2009, and was to be halved every four years in line with system assumptions. The amount of cryptocurrency issued is also controlled by adjusting, in two-week cycles, the difficulty of the mathematical problem to be solved by miners to the size of the computing power employed. This way, the correct block should be found at a fixed frequency of every 10 minutes (Badev, Chen, 2014).

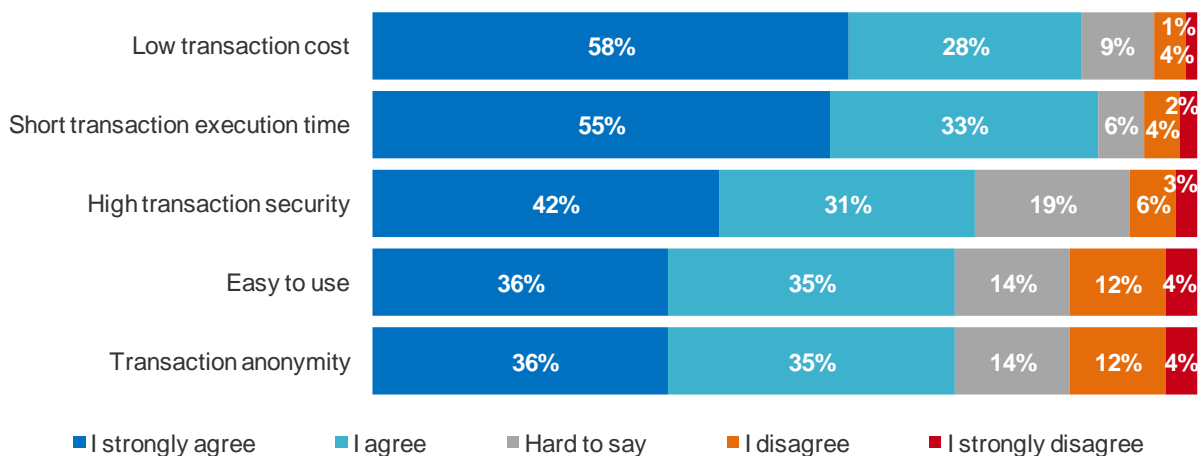
Adding a block to the blockchain means that the network, and more precisely miners, have confirmed that the bitcoins of a person making a transfer of funds have not been

previously spent. After receiving six confirmations, the risk that a completed transaction will be reversed nears zero. This method of verifying the correctness of transactions has drastically limited the chances of double spending (Nian, Chuen, 2015).

Results of the empirical study

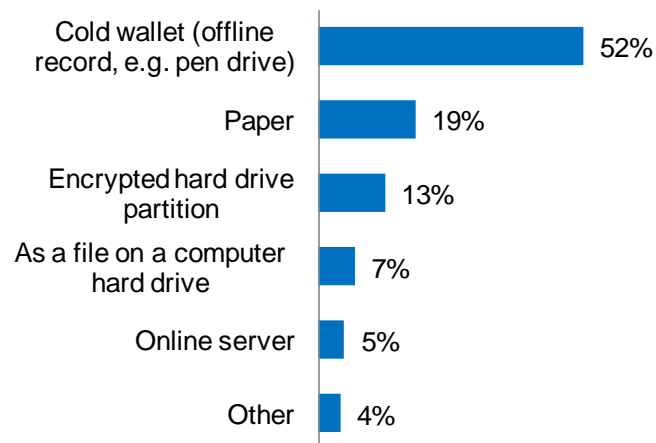
The responses obtained in the study (Figure 1) point to a high level of optimism of the respondents in terms of the selected features of the bitcoin system. The answers placed special emphasis on low transaction costs and high transaction speed. They may be attributed to the fact that at the time, miners applied small transaction fees and that bitcoin was probably mainly used for investment purposes because if bitcoin was frequently used in payments, a 10-minute wait for the first transaction confirmation would surely be reflected in a larger share of negative marks. Less optimistic answers to other questions should be associated with the existence of apparent anonymity, a phenomenon described by Möser et al. (2013) and Reid and Harrigan (2013), and user awareness of the complex nature of the system. These features translated into limited trust in the system's solutions in the domain of trade security, and storage of the cryptocurrency in particular.

Figure 1. Respondents' assessment of bitcoin features



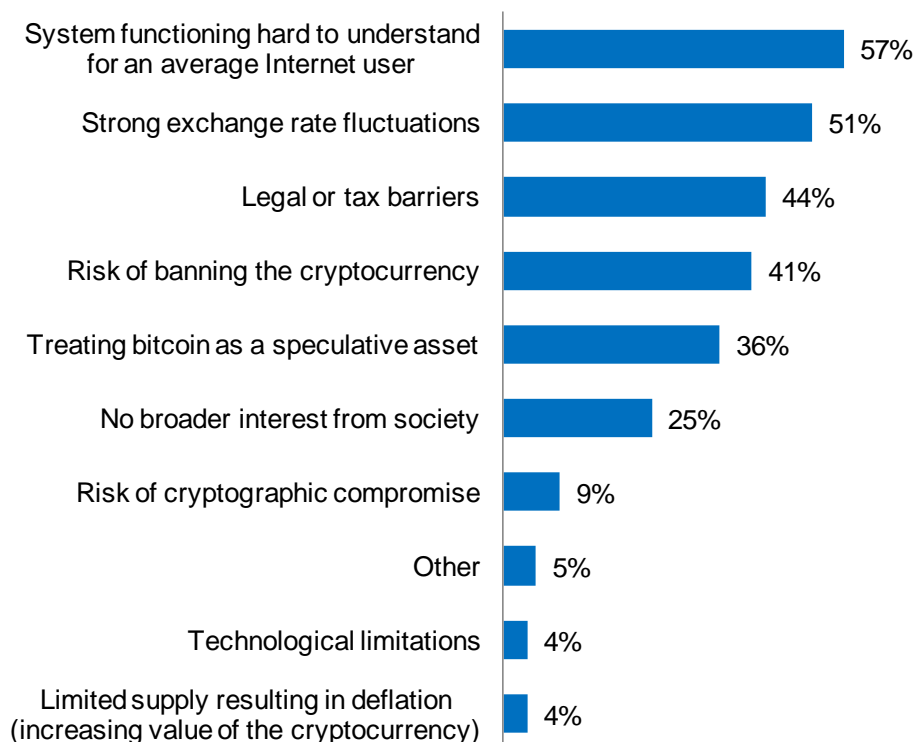
Source: questionnaire survey of bitcoin users, N=588-590.

The respondents perceived the digital nature of bitcoin as the main threat to the system's functioning. Users were aware that they could lose bitcoins as a result of a hacker attack, so they took preventive measures. Answers presented in Figure 2 regarding a safe place for storing bitcoin indicate that 71% of the respondents preferred carriers not connected to the Internet. Of that number, 52% said that the safest method was saving private keys offline, e.g. on a pen drive, and 19% chose recording them on paper. The data regarding the preferred forms of storing cryptocurrency units seem to defy the intended use of bitcoin for payments.

Figure 2. The safest place for storing bitcoins

Source: questionnaire survey of bitcoin users, N=570.

An analysis of Figure 3 provides ample information on areas which threaten the development of the bitcoin system from the respondents' point of view. In general, the remarks emphasise external threats for the bitcoin system. Strong exchange rate fluctuations, legal and tax barriers, or risk of a ban indicate that threats were sought in factors independent of the system's construction. The same may be said about the most frequent answer, focusing on the lack of knowledge in society regarding the system's functioning, which combines the impact of technological and sociological factors.

Figure 3. Barriers to the development of bitcoin

Source: questionnaire survey of bitcoin users, N=607, respondents could choose up to 3 answers.

In 2014, i.e. after the bitcoin system had been functioning for five years, Polish users noticed threats to development in factors directly related with the bitcoin system's construction only to a minor extent. Only 4% of the answers pointed to technological limitations, presented in more detail further in the paper.

Technical and technological threats to the functioning of the bitcoin system

The development of bitcoin has disclosed certain processes or phenomena which have a negative impact on the efficient and intended functioning of the system. These include, in our opinion: the system being dependent on financial intermediaries, including banking sector institutions, lack of systemic incentives addressed to bitcoin merchants, rising transaction costs and low transaction capacity of the bitcoin system.

One of the cornerstones of the bitcoin payment system, i.e. the elimination of the financial intermediary in the process of carrying out a transaction, has never been achieved in practice. The bitcoin system could truly be considered fully independent if it comprised only direct transactions between cryptocurrency holders. At the very early stage, virtually any interested person could mine cryptocurrency units after installing the dedicated software. Whereas as the system developed, the need to have expensive and highly specialised mining hardware became a serious barrier to acquiring the cryptocurrency this way. Therefore, it turned out that in order for the system to develop and be used on a broader scale, it would be necessary to have certain groups of specialised financial intermediaries. However, their introduction brought about new types of threats for bitcoin users.

First bitcoin trading platforms, frequently referred to as exchanges, emerged around a year after bitcoin started functioning online. They link the bitcoin system with the traditional financial system, and are currently the most common place for carrying out bitcoin sale and purchase transactions. It should be noted that using the platforms makes the functioning of the bitcoin system subject to the actions of banking sector institutions which in a sense are in competition with bitcoin. This is related to the need to hold a bank account containing funds in traditional currencies used to purchase the cryptocurrency or obtained from its sale. Banks may therefore track or block the actions of system users. This is not only theory: there have been instances where banks terminated agreements with customers transferring funds to the accounts of exchanges (Gawin, 2015) or closed bank accounts of trading platforms (BitMarket.pl, 2015).

Despite the undeniable advantages of exchanges within the bitcoin system in the form of valuing cryptocurrency units and facilitating bitcoin trade, they also bring many threats which are not thoroughly recognised by system participants. Firstly, starting an account on the platform requires that the user provide personal data. In fact, it is not exactly known who their operator is and for what purposes they may be used. This, coupled with the efforts needed to open an account, may in turn be a significant barrier to new users' entry into the system. Secondly, the common usage of the term

'exchange' when referring to the currency trading platforms is misleading because it may provide a false sense of security. It should be noted that the functioning of cryptocurrency trading platforms is generally not supervised by financial market regulators and funds collected in the accounts of platforms are not covered by any guarantee or compensation system. Thirdly, in the case of stock exchanges, bankruptcies happen to listed companies and not the trading markets themselves. In the relatively short history of cryptocurrencies, however, there have been several high-profile instances of unexpected closures of trading platforms. The best-known cases include Mt. Gox and Bitcurex, and they resulted in tremendous losses for cryptocurrency holders. When looking for reasons for bankruptcies of cryptocurrency trading markets, many name the lack of appropriate technical and IT security against hacker attacks or experience in running this kind of business. However, one more factor should also be considered: the potential conscious and purposeful criminal activity of platform operators. Gaining user trust and making a professional appearance may lead to mass theft of funds from the platform's clients, denominated both in cryptocurrencies and traditional currencies. The manner in which cryptocurrency exchanges function, different from that of stock exchanges, facilitates such criminal activities and is a source of risk for bitcoin users. While traditional stock exchanges are places where certain instruments are offered for sale and the investors continue to own them, it is completely different in the case of cryptocurrencies. Someone who wants to sell bitcoins must transfer them to the exchange's address and wait for the payment for their sale. Such functioning of the platforms is determined by the bitcoin's construction, namely the fact both the public and the private key have to be known in order to transfer the title to the cryptocurrency.

Another factor having effect on the bitcoin system's potential for development is the lack of systemic incentives addressed to bitcoin merchants. An innovative solution based on financial incentives and elements of competition addressed to people developing and maintaining the system contributed to a quick expansion of the bitcoin network users. However, in order to speak of success of the new payment solution, it is necessary to create a wide network of bitcoin merchants in parallel to the user network. Without it, the system will not have economic use and will cease to be attractive for its users. The bitcoin system has practically ignored the issue of its connection with real business because the manner in which the acceptance network could be developed was not provided for. Apart from the lack of chargeback, there were no incentives for merchants who bear many costs and risks related to their participation in the network. This issue was quickly noticed by market participants and was partially resolved by payment providers. These companies intermediate between bitcoin users and merchants, providing payment in a traditional currency. Additionally, they free merchants from the exchange rate risk, accounting problems, tax settlement of transactions, or the risk of an error during processing a bitcoin transaction. Despite numerous benefits, the small-scale operations of processors demand caution when discussing their favourable impact on bitcoin payments acceptance levels and risk reduction in high-value transactions.

Costs related to the use of financial innovations are a significant factor determining the extent to which such innovations are applied (Schuh, Stavins 2013). There are generally two types of costs in bitcoin trading. The first one includes commissions charged by cryptocurrency trading platforms, and the other comprises single bitcoin transaction fees charged by miners (to the sender). The fee for transaction execution is expressed in bitcoin and does not depend on its value but rather on its size expressed in bytes³. Users can usually determine its value, and this translates into the transaction confirmation time. Recently, the costs of carrying out bitcoin payments have risen and we should be aware that this trend will continue. This results from the declining number of mined bitcoins which are a form of remuneration, but also from compensating for costs of electricity used up by miners. The rising fees are particularly noticeable in low-value transactions and may curb the use of the bitcoin system in that area. We believe that this phenomenon is contrary to the idea underlying the analysed payment system.

Literature regarding the subject matter indicates that the capacity of the bitcoin system is an important problem limiting the proliferation of the cryptocurrency on a global scale (Croman, Decker, Eyal, Gencer, Juels, Kosba, Miller, Saxena, Shi, Gün Sirer, Song, Wattenhofer, 2016; Herrera-Joancomarti, Pérez-Solà, 2016). The construction of the bitcoin system assumes that on average one new 1 MB block appears every 10 minutes. The small size of the block limits the number of authorised transactions to a maximum of 7 transactions per second, which means that one block may cover around 4000 transactions (Vukolić, 2016).

The low transaction capacity of the bitcoin system has been subject to wider discussion, taking place both in academic circles and in the cryptocurrencies community. Many Bitcoin Improvement Proposals appeared online, primarily suggesting that the size of blocks in the blockchain should be increased. One of the concepts states that this size could be raised to 2 MB (Garzik, 2015). Another proposal posits the reduction of information size of one transaction, which would result in including more transactions in one block (Lombrozo, Lau, Wuille, 2015). However, we should remember that increasing the block size or creating new blocks more frequently would result in making the bitcoin system several times more prone to attacks (Sompolinsky, Zohar, 2015).

The issue of the system's 'clogging' became particularly visible in 2016. Only slight adjustments have been introduced to the system to date because a consensus has not been reached by the vast majority of computing power contributors. This causes transaction queueing and higher fees, which is detrimental to user convenience. The lack of consent within the community may lead bitcoin to a hard fork, i.e. the forking of

³ On 26 April 2017, the Mycelium portfolio had a fee per transaction byte between 109 satoshis for low-priority transactions and 218 satoshis for priority transactions. If we assume that the average size of a single bitcoin transaction does not exceed 300 bytes, the fee should be in the range of 0.000327–0.000654 BTC. At the exchange rate of 1 BTC = 1300 USD, this means a fee between 0.43 USD and 0.85 USD. Franco (2015) reported that for version 0.9.1 of Bitcoin Core introduced in April 2014, the minimum fee was 0.00001 BTC per kB (almost 1 satoshi per byte). Having regard to the guarantee of transaction execution, the author suggested setting the fee at 0.0001 BTC per kB (almost 10 satoshis per byte). In practice, this would lead to a single transaction cost of 0.0001 BTC.

the transactions register into two chains. One of them would operate under rules similar to the existing ones, and the other under new rules allowing miners to set the block size (Hertig, 2017). However, the functioning of two chains and the emergence of two types of bitcoin in trade may generate problems with settling transactions.

Conclusion

At the early stages of bitcoin's functioning, users sought threats to the system's functioning in external factors. They were concerned with the potential introduction of excessively stringent regulations regarding the cryptocurrencies market or even a ban on the system. They also pointed to the instability of quotations and the speculative nature of the bitcoin cryptocurrency. However, apart from the system's complexity, no other flaws within the bitcoin system itself were noticed. We were led to this conclusion by analysing specialist literature in the field of finance and performing our own research. Therefore, it may be assumed that the hypothesis proposed in this paper has been confirmed. In retrospect, it seems that the threats indicated by bitcoin users proved to be largely apparent. They did not materialise because governments and financial market supervisors describes their view of bitcoin as moderately positive. Their decision was based on the fact that they saw the advantages of the bitcoin system and subdued their concerns over its negative impact on real economy due to the small size of the cryptocurrencies market.

The development of the bitcoin system helped its users detect threats to its functioning lying in the construction of the system itself. Technical and technological limitations may diminish the system's effectiveness and make its operation somewhat contrary to the idea for which bitcoin was created. The disadvantages presented in the paper have a negative impact particularly on the performance of the system's payment function.

Bitcoin system users are currently holding widespread discussions on the possibility of a 51% attack, the system's energy intensity, low transaction capacity, or the large size of the blockchain. We have also drawn attention to the rising costs of transaction execution and the fact that the cryptocurrency depends to a certain extent on the operation of intermediaries, including primarily banks and trading platforms. We have highlighted the importance of those phenomena for the system's functioning in both technological and ideological terms. We have also stressed the fact that besides the irreversibility of transactions, the bitcoin system does not have incentives addressed to merchants. The poorly-developed bitcoin payments acceptance network is largely detrimental to how the cryptocurrency may be used for payments in the economy, and as a consequence hampers the development of the bitcoin system.

Bitcoin users are able to scale down the negative effects of the technological barriers indicated in the paper by introducing system improvements. However, the functioning of a global system with a distributed user network has shown that there are problems with agreeing on improvement methods and their efficient implementation. The experiences of bitcoin users in that area are a guideline for the developers of other

cryptocurrency systems and indicate that substantial improvements should take place in the initial stages of a system's functioning, when it is easier to reach a consensus.

References

- Badev, A., Chen, M. (2014). Bitcoin: Technical Background and Data Analysis. *Finance and Economics Discussion Series*, Federal Reserve Board, pp. 1-38.
- Baek, C., Elbeck, M. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters*, Vol.22, Iss. 1, pp. 30-34. DOI: 10.1080/13504851.2014.916379.
- Barber, S., Boyen, X., Shi, E., Uzun, E. (2012). Bitter to Better – How to Make Bitcoin a Better Currency. *Lecture Notes in Computer Science*, Vol. 7397, s. 399-414. DOI: 10.1007/978-3-642-32946-3_29.
- BitMarket.pl, Wyłączenie wpłat na konta BitMarket.pl, 26.01.2015. Available at: <https://www.bitmarket.pl/docs.php?file=wylaczenie.html> (Accessed 4 March 2017).
- Brandvold, M., Molnar P., Vagstad, K., Valstad. O.C.A. (2015). Price Discovery on Bitcoin Exchanges. *International Financial Markets, Institutions & Money*, Vol. 36, pp. 18-35. DOI: <http://dx.doi.org/10.1016/j.intfin.2015.02.010>.
- Brito, J., Castillo, A. (2016). Bitcoin. A primer for policymakers. Mercatus Center at George Mason University.
- Cheung, A.W.K., Roca, E., Su, J.J (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, Vol. 47, Iss. 23. DOI: 10.1080/00036846.2015.1005827.
- Ciaian, P., Rajcaniova M., Kancs d'A. (2016). The economics of BitCoin price formation. *Applied Economics*, Vol. 48, No. 19, 1799-1815. DOI:10.1080/00036846.2015.1109038.
- Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G, Song, D., Wattenhofer, R. (2016). On Scaling Decentralized Blockchains. *Lecture Notes in Computer Science*, Vol. 9604, ss.106-125. DOI: 10.1007/978-3-662-53357-4_8.
- Feld, S., Schönfeld, M., Werner, M. (2014). Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. *Procedia Computer Science*, Vol. 32, pp. 1121-1126.
- Franco, P. (2015), *Understanding Bitcoin: Cryptography, Engineering and Economics*, Wiley.
- Garzik, J. (2015). BIP 102, Block size increase to 2MB. Available at: <https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki> (Accessed 29 January 2017).
- Gawin, M. (2015). Banki zamykają ROR-y za obrót bitcoinami, Bankier.pl. Available at: <http://www.bankier.pl/wiadomosc/Banki-zamykaja-ROR-y-za-obrot-bitcoinami-7233425.html> (Accessed 30 January 2017).
- Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Science and Technology Law Journal*, Vol. 4, No. 1, pp. 160-208.
- Herrera-Joancomarti, J., Pérez-Solà, C. (2016). Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. *Lecture Notes in Computer Science*, Vol. 9880, pp. DOI: 26-44. 10.1007/978-3-319-45656-0_3.
- Hertig, A. (2017). CoinDesk Explainer: The Bitcoin Unlimited Debate. Available at: <http://www.coindesk.com/coindesk-explainer-bitcoin-unlimited-debate/> (Accessed 25 April 2017).
- Hughes, E. (1993). A Cypherpunk's Manifesto. Available at <http://www.activism.net/cypherpunk/manifesto.html> (Accessed 24 August 2016).

- Kelly, B. (2015). *The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World*, Wiley, Hoboken.
- Kristoufek, L. (2015). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. *PLoS ONE*, Vol. 10, Iss. 4, pp. 1-15. DOI: <https://doi.org/10.1371/journal.pone.0123923>.
- Leung, D., Dickinger, A. (2017). Use of Bitcoin in Online Travel Product Shopping: The European Perspective. In: *Information and Communication Technologies in Tourism*, Schegg R., Stangl B. (eds.), Springer. DOI: 10.1007/978-3-319-51168-9_53.
- Lombrozo, E., Lau, J., Wuille, P. (2015). BIP 141. Segregated Witness (Consensus layer), 21.12.2015. Available at: <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki> (Accessed 29 January 2017).
- May, T.C. (1992). *The Crypto Anarchist Manifesto*. Available at <http://www.activism.net/cypherpunk/crypto-anarchy.html>, (Accessed 22 August 2016).
- Moore, T. (2013). The promise and perils of digital currencies. *International Journal of Critical Infrastructure Protection*, Vol. 6, s. 147.
- Möser, M., Böhme, R., Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In: *eCrime Researchers Summit (eCRS 2013)*, IEEE, pp. 76-89. DOI: 10.1109/eCRS.2013.6805780.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: <https://bitcoin.org/bitcoin.pdf> (Accessed 6 May 2016).
- Nian, L.P., Chuen, D.L.K. (2015). Introduction to Bitcoin. In: *Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data*, D.L.K. Chuen (ed.), Elsevier, pp. 5-30.
- Polasik, M., Piotrowska, A.I., Wisniewski, T.P., Kotkowski, R., Lightfoot, G. (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. *International Journal of Electronic Commerce*, Vol. 20, No. 1, pp. 9-49. DOI:10.1080/10864415.2016.1061413.
- Reid, F., Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In: *Security and Privacy in Social Networks*, Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony, A.Pentland (ed.), Springer, pp. 197-223. DOI: 10.1007/978-1-4614-4139-7_10.
- Schuh, S., Shy, O. (2015). U.S. Consumers' Adoption and Use of Bitcoin and other Virtual Currencies. Available at: <http://www.bankofcanada.ca/wp-content/uploads/2015/12/us-consumers-adoption.pdf> (Accessed 25 April 2017).
- Schuh, S., Stavins, J. (2013). How Consumers Pay: Adoption and Use of Payments. *Accounting and Finance Research*, Vol. 2, No. 2, s. 1.
- Sompolinsky, Y., Zohar, A. (2015). Secure High-Rate Transaction Processing in Bitcoin, *Lecture Notes in Computer Science*, Vol. 8975, pp. 507-527. DOI: 10.1007/978-3-662-47854-7_32.
- Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Lecture Notes in Computer Science*, Vol. 9591, pp. 112-125. DOI: 10.1007/978-3-319-39028-4_9.