

References:

1. Makarov Y. Dy`yavol iz g`adzheta // Ukrayins`ky`j ty`zhden`. 2019. № 19 (599). Access mode: <https://tyzhden.ua/Columns/50/229963>.
2. Mary`novy`ch M. Demokraty`chny`j «mayatny`k» ta Ukrayina // Zbruch. 30.4.2019. Access mode: <https://zbruc.eu/node/88946>.
3. Genning` Fepel`. Vakuum pravyl ta insty`tucij // Ukrayins`ky`j ty`zhden`. № 7. 15-21.02. 2019. 271 p.
4. Charles P. Kindleberger: Debt Situation of the Developing Countries in Historical Perspective (1800–1945), in: Außenwirtschaft, Vol. 36 (1981), No. IV, pp. 372–380.

ZAHORODNII V. E.

National University «Odesa Law Academy»,
Rector, PhD in Law, Associate Professor

TISHCHENKO V. V.

National University «Odesa Law Academy»,
Head of the Department of Forensic Science, Corresponding Member of the
National Academy of Legal Sciences of Ukraine, Doctor of Law, Professor

DYNTU V. A.

National University «Odesa Law Academy»,
Associate Professor at the Department of Forensic Science, PhD in Law

THE ESTABLISHMENT OF CRYPTOCURRENCY

Key words: *Cryptocurrency, virtual currency, digital economy, Bitcoin.*

The process of establishing cryptocurrency as a mean of payment for current digital economy is described in the article. Moreover, the distinction between virtual currency and electronic money is scrutinized.

Currently because of «The Forth Industrial Revolution» [1, p. 35] and «rapid development of IT technologies the framework of economy was changed and caused the emergence of new phenomena – digital economy, which can be considered, as a series of economic, social and cultural activities that are performed online and are related to the use of information and communication technology» [2]. Thus, the digitalization of the economy has set up the boundless environment with renewed trading rules. Furthermore, it triggers the creation of the virtualization of the world bank system – a transformation of banking on the base of informational technology implementation into bank sector; according to the form it is a transition of bank sector into electronic flatness of utilization which can be seen in

following forms: electronic banking, electronic payment systems (domestic and international) [3].

Consequently, the high-speed rise of digital trade market and virtualization of the world bank system demanded the creation of the certain financial tool which can be used via the Internet and ensured the high speed of transactions. Such kind of instrument has become virtual currency [4].

Virtual currency is different than electronic money which is a digital means of fiat currency and is utilized for electronic transfer of reflecting fiat currency cost and is considered as a legal means of payment [5]. Furthermore, the distinction between virtual currency and other means of payment is the method of the emission of payment units and the organization of their storage and transfers system.

In addition, «unlike gold or silver virtual currencies have no non-monetary use or value – they are just bits of data» [6]. Furthermore, the value of virtual currencies is based on the convention among system's users which are working via the Internet [7].

According to the European Central Bank position which was expressed in «Virtual currency schemes – a further analysis» «virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money» [8]. Moreover, in report of the Financial Action Task Force virtual currency is considered as a «digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction and fulfills the above functions only by agreement within the community of users of the virtual currency» [9].

Very often the creation of cryptocurrency correlates with the replication to the social demand for a currency independent from banking and governmental institutions, after economic crises in 2008 when they lost their reliability.

However, the idea of private money is not new, it was articulated in the book of Austrian economist Friedrich August von Hayek «The Denationalization of money». His main idea was that government should be deprived of the money's emission monopoly with a target to prevent the inflation process [10]. Furthermore, Milton Friedman in 1999 during the interview admitted, that «...the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A, the way I can take a USD 20 bill and hand it over to you and then there is no record of where it came from» [6]. His prediction was precision because progressive instruments and systems are establishing neoteric paradigms for transactions and new channels of capital [11].

It should be noticed, that the roots of cryptocurrency go to the end of previous century, in particular 1983 David Chaum offered the idea of

combining transparency and anonymity of transaction for all users by utilizing «Blind signature» [12].

Then in 1990th was formed the movement of cryptoanarchists – cypherpunk whose idea was the usage of cryptography and other similar tools for changing social order. In 1993 one of the founder of the cypherpunk Eric Hughes announced the confidentiality of transactions by using multi-step encryption and published.

In 1994 Timothy C. May published the work «The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666» where he described safe untraceable encrypted transactions, which would use the P2P system which does not need verification by third parties and would cause the independent from the government [13].

In 1998 Wei Dai offered cryptocurrency «b-money». He wrote «I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word «anarchy», in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations» [14].

In 2005 Nick Szabo was created «Bitgold». As a libertarian wing of cypherpunk inspired by the novel of Ayn Rand «Atlas Shrugged» he wanted to create «Galt's Gorge» in the cyberspace – free trade zone. Firstly he came to idea of creation smart-contracts which was based on blockchain system in 1990th, and later on invented cryptocurrency.

Currently, the most popular cryptocurrency which is used by bidirectional flow is Bitcoin. Bitcoin is decentralized P2P (Person to Person) payment network, which serves its users without central bodies and agents. From the users' point of view, Bitcoin is analog of cash but only for the Internet (In Bitcoin information site). The maximum amount of Bitcoin in the world is restricted and cannot be more than 21 million.

The creation of Bitcoin is correlated with the name of Satoshi Nakamoto, who on September 3, 2009, via the Internet published an article «Bitcoin: A Peer-to-Peer Electronic Cash System» [15], in which he described the main principals of new cryptocurrency. The main characteristics which distinguish Bitcoin from traditional electronic money and cashless settlements that Bitcoin is not debt obligations of the issuer.

References:

1. Schwab, K. (2016). The Forth Industrial Revolution. Geneva, World Economic Forum, 172 p.
2. Zupan, G. (2016). E-skills and Digital Economy. Statistical Office of the Republic of Slovenia. Retrieved from: http://www.stat.si/StatWeb/File/DocSysFile/8970/e-skills_and_digital_economy.pdf (accessed 13 May 2019).
3. Pelo, A. (2015). Virtualization of the global banking system in the context of globalization. [Visnyk ONU im. I.I. Mechnikova]. Retrieved from: http://visnyk-onu.od.ua/journal/2015_20_2_1/05.pdf. (in Ukrainian). (accessed 13 May 2019).

4. Dyntu V. Dykyi O. (2018). Cryptocurrency in the system of money laundering. [Baltic Journal of Economic Studies]. Vol. 4. No. 5. Retrieved from: <http://www.baltijapublishing.lv/index.php/issue/article/view/539>
5. Karcheva H. and Nikitchuk S. (2015). Virtualnyi innovatsiini valiuty yak valiuty maibutnoho. [Finansovi prostr], 2 (18). Retrieved from: <http://fp.cibs.ubs.edu.ua/files/1502/15kgtviv.pdf>. (in Ukrainian). (accessed 13 May 2019).
6. World Savings and Retail Banking Institute. (2014). Virtual currencies: passion, prospects and challenges. Retrieved from: https://www.wsbi-esbg.org/SiteCollectionDocuments/Virtual%20currencies_passion,%20prospects%20and%20challenges.pdf (accessed 13 May 2019).
7. Dziuba J. and Orzeszko T. (2015). Finance and Accounting for Sustainable Development – Responsibility, Ethic, Financial Stability. [Publishing House of Wrocław University of Economics]. Retrieved from: http://www.dbc.wroc.pl/Content/30185/Lukasiewicz-Kaminska_Digital_Currencies_And_Their_Impact_2015.pdf (accessed 13 May 2019).
8. European Central Bank. (2015). «Virtual currency schemes – a further analysis». Retrieved from: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (accessed 13 May 2019).
9. Financial Action Task Force. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. Retrieved from: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (accessed 13 May 2019).
10. Hayek F. (1976). The Denationalization of money. [The institute of economic affairs]. London, 108p.
11. Hileman G. and Rauchs M. (2017). Global cryptocurrency benchmarking study [Cambridge Centre for Alternative Finance]. Cambridge. Retrieved from: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf (accessed 13 May 2019).
12. Chaum, D. (1982). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto 82* (3), p. 199–203.
13. May, T. (1992). The CryptoAnarchist Manifesto. Retrieved from: <https://www.activism.net/cypherpunk/crypto-anarchy.html>. (accessed 13 May 2019).
14. Dai, W. (1998). Retrieved from: <http://www.weidai.com/bmoney.txt> (accessed 30 October 2018).
15. Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: <https://bitcoin.org/bitcoin.pdf> (accessed 13 May 2019).