

Cryptocurrency and Internet of Things: Problems of Implementation and Realization

Lyubomyr Sopilnyk¹, Andriy Shevchuk², Vasyl Kopytko³, Rostyslav Sopilnyk¹,
Larysa Yankovska¹

¹ *Lviv University of Business and Law*

99 Kulparkivska Street, Lviv, 79021, Ukraine

² *Cherkasy State Technological University*

460 Shevchenko Boulevard, Cherkasy, 18006, Ukraine

³ *Lviv Branch of Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan*

12a I. Blazhkevych Street, Lviv, 79052, Ukraine

DOI: [10.22178/pos.38-1](https://doi.org/10.22178/pos.38-1)

JEL Classification: G00

Received 01.08.2018


Accepted 15.09.2018

Published online 20.09.2018

Corresponding Author:

Lyubomyr Sopilnyk

sopilnyk01@gmail.com

© 2018 The Authors. This article is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) 

Abstract. IoT (Internet of Things) requires the implementation of digital encryption of information, transaction support and recording of all events for security. It can provide cryptocurrencies protocols with adding an additional possibility of payments. This opportunity is not so much demanded at the hardware level as in the software implementation. We have discovered that IoT devices are widely used for illegal purposes for trusts or network consolidated attacks, and virtually no legal and useful ways of using their hardware-distributed capabilities. Standardization and compatibility in IOT network should become the main tools for the possibility of introducing new solutions, testing their utility, performance and safety. The standardization of a new approach to interactive protocols in the IOT network and the Internet with a finance approach is now inevitable. We need new IEEE standards for cryptocurrencies and IoT functioning. They must include standards for protocol functioning, transaction validation and saving, privacy and security support. Cryptocurrencies and IoT interaction diagram was proposed. The IoT network devices technology will be in future instance of the smart class of digital physical systems, which also encompasses technologies such as smart homes, intelligent transportation systems, smart cities etc. The financial aspect for purchasing software, services, solutions and sales of the resulting benefits will complement this network with additional capabilities. The development of standards for the financial level of functioning is also necessary.

Keywords: Internet of Things; cryptocurency; blockchain; technologies implementation and realization.

INTRODUCTION

The global financial system entered in a new phase of development with the creation of cryptocurrency with using of IT. The first concept of crypto coins was introduced in 2009 with the creation of an anonymous author of the Bitcoin. The main technologies for the distribution and operation of such a system at the same time were developed: decentralized functioning without the ability of control by governments or financial centers; the possibility of fast transfers and pay-

ments through digital networks; the anonymity of participants in the exchange process and direct payments; logging of transactions in the form of technologies blockchain. The capitalization of Bitcoin's has reached \$ 186 billion, with 10 major cryptocurrencies of \$ 200 billion in 2017, indicating their rapid popularity, high demand and credibility [1]. The IoT network also growth with its market rapidly. The overall number of online capable devices increased by 30 % within the year and have reached 8.4 billion in

2017. The number of IoT supported devices will be about 30 billion objects in 2020 by predictions. The IoT market size now is near 561 billion US \$ it is also estimated will reach \$7.1 trillion by 2020 [2]. The process of cheapening devices has led to a large number of attempts to use them with the benefit of real life. So, these two new innovative tools are very closely interconnected, which determines their mutual use in the future. They both use similar data transfer protocols and their combination can enhance their application and practical significance.

Researchers such as P. Vigna, M. Casey [3], J. Fry, E. Cheah [4], A. Narayanan, J. Bonneau, E. Felten, A. Miller [5], and others were engaged in research of cryptocurrencies. The IoT was investigated by M. Gigli, S. Koo [6], A. Castellani, N. Bui, P. Casari, M. Zach, M. Zorzi [7] and others. The study of the combination of these two technologies is now beginning. The purpose of the publication is to determine problems of implementation and realization cryptocurrency using with IoT network.

RESULTS AND DISCUSSION

Cryptocurrency and IoT

The concept of cryptocurrency was introduced in 2009 with the creation of an anonymous author of the first such currency Bitcoin [1]. At the same time, the main technologies for the distribution and operation of such a system were developed: decentralized functioning without the ability of control by governments or financial centers; the possibility of fast transfers and payments through digital networks (Internet); the anonymity of participants in the exchange process; the input and output of fiat money and the logging of transactions in the form of technology blockchain. IoT is defined by scientists as open and comprehensive network of intelligent devices and objects with electronics, software, sensors that have the capacity to auto-organize, share and send information, data and resources, reacting and acting in face of situations and changes in the environment [6, 7]. The IoT network allows objects to be controlled remotely across existing network infrastructure (or Internet) with integration process of the physical world objects and devices into network and computer based systems with improved management, efficiency, accuracy and economic benefit in addition to reduced human intervention [6, 7]. The network may consist of such things as such as media and

network devices, sensors, heart monitoring implants, biochip transponders on farm animals, cameras streaming, auto or drones with built-in sensors, DNA analysis devices for environmental/food/pathogen, field operation devices that assist firefighters in search and rescue operations and many others. The vision of the IoT has evolved due to a convergence of multiple technologies, including smart devices, wire and wireless communication, smart home, real-time analytics, machine learning, artificial intelligence, neural networks, smart agents, commodity sensors, and embedded systems [8, 9]. Cryptocurrencies and IoT interaction diagram we can see on Figure 1.

The IoT network devices technology will be in future instance of the smart class of digital physical systems, which also encompasses technologies such as smart homes, intelligent transportation systems, smart cities etc. The financial aspect for purchasing software, services, solutions and sales of the resulting benefits will complement this network with additional capabilities. The development of standards for the financial level of functioning is also necessary. While security is a concern there are many things being done to protect devices. IoT devices data is following cryptographic standards and encryption is being used in end-to-end scenarios of relationships between them. Certificates x.509 are also being used to verify device identity. We need new IEEE standards for cryptocurrencies and IoT functioning. They must include standards for protocol functioning, transaction validation and saving, privacy and security support. Now there is IEEE P2413 draft Standard for an Architectural Framework for the Internet of Things Working Group. This draft standard defines an architectural framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. A new financial perspective standards development will be required after the adoption of the final version of P2413. New standards are required for cryptography methods and certificates for using cryptocurrencies and transaction logging databases as blockchain or tangle, payments validation and may be mining procedures. Also important is a quick response to new developments in this area. New concepts are constantly appearing in the field of cryptocurrency: smart contracts, digital tokens, mining methods etc. Creating a hardware and software sandbox like platform for testing and possible implementation would be expedient.

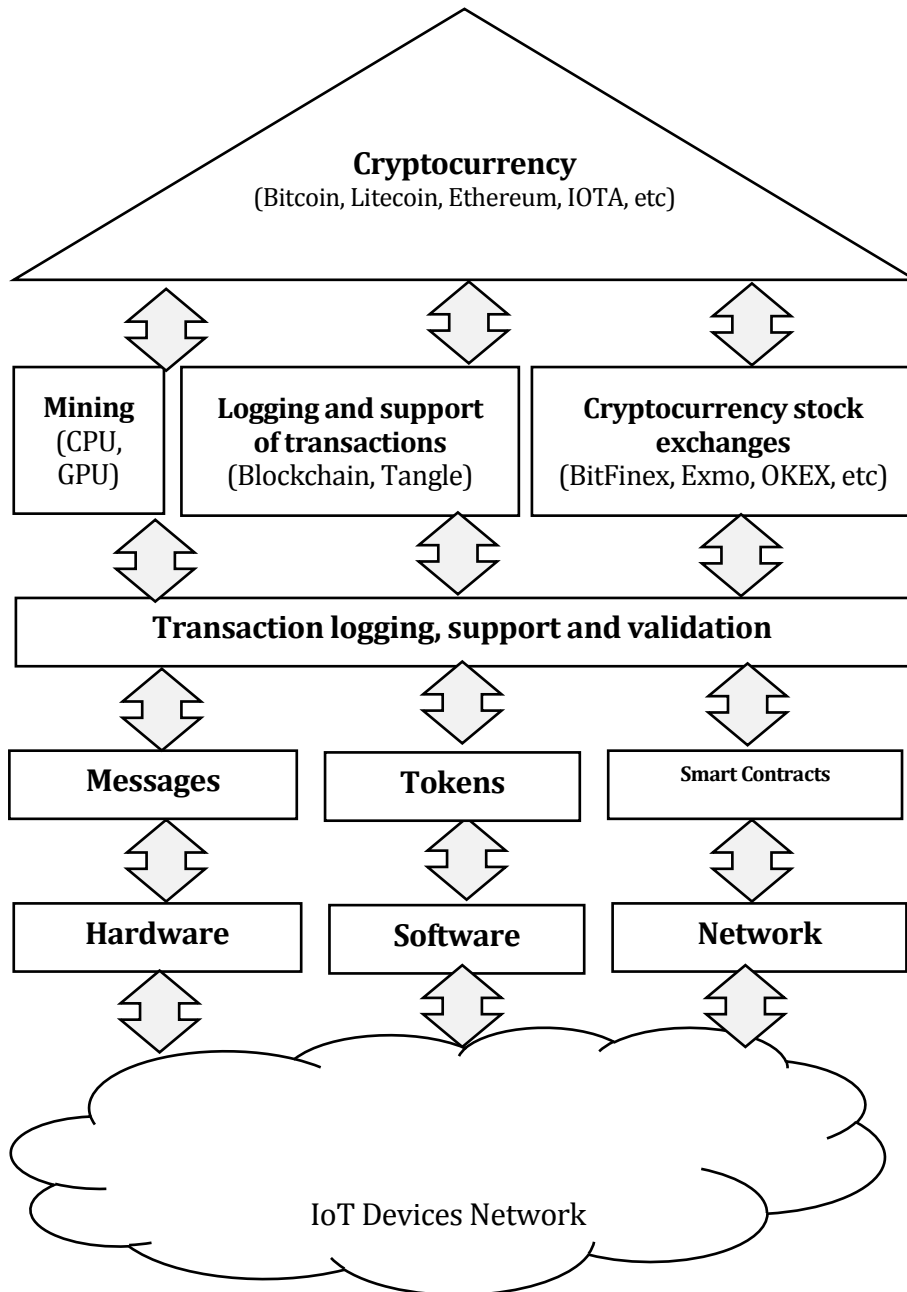


Figure 1 – Cryptocurrencies and IoT interaction diagram

The development of a rigorous model with the necessary standards should allow better development of insights and facilitate the creation of new projects of cryptocurrency and IoT. It is necessary to take into account all the peculiarities of implementation, ranging from the hardware platform and programming languages to the financial aspects, due to the large number of future transactions in the network of devices all over the Internet.

IoT and IoTA

Some example of the transformation of the financial system with the help of cryptocurrency can be determined by the growth of the rate and

capitalization of IOTA coins at the end of 2017 year. IOTA was developed in October 2015. The appearance of various cripples after the creation of Bitcoin has defined certain requirements for digital money and investors have begun to look for the best options that can be applied in real life. Earlier on the market appeared cryptocurrency IOTA, intended for payments in the IoT, which was developed taking into account the existing shortcomings of such systems in the transactions. Among the benefits of its development, a new transaction verification system was identified - Tangle, faster than comparators time required for a transaction, free transaction without interest and a convenient method of calculation without large comma values - the currency is

immediately distributed in millions of units (MI IOTA). The sender must confirm the two previous transactions of arbitrary senders using a simple PoW algorithm in order to send the transaction to the IOTA network. PoW calculations take from a few seconds to several minutes, depending on the GPU, the PoW algorithm in IOTA is optimized for the GPU and some luck. Sender data is broadcast to the network and awaits confirmation from the following transactions once the PoW solution is received. It is considered to be confirmed once the transaction receives sufficient confirmation from other senders. The Raiblocks architecture in IOTA is defined as a lattice of blocks. This is not a one-dimensional block, like that of Bitcoin or the Ethereum; rather, it is a database in which each address gets its own block. The user sends funds, creating two blocks: the sender unit on its own block; and the recipient's block on the recipient's block. To get tokens, the user does not have to be on the network. The address purse automatically pockets all received funds. Once the user opens access to their funds. This procedure actually means signing the recipient's block with its private key, which finally adds it to the personal block of the recipient. Transactions in IOTA are added to the Tangle structure, which is a directed acyclic DAG graph. A complex name in practice means a data structure that guarantees the absence of a loop, that is, starting from one node, it is impossible to return to it again. As more transactions are added to the Tangle, the weight of the parent transactions grows. When the transaction is gaining sufficient weight, it acquires the status of confirmed. Facilities with new cryptocurrency transactions did not go unnoticed and at the end of 2017 year, Microsoft announced an alliance with its founders and intentions of future use for its projects and applications, after which the IOTA course grew more than 10 times and capitalization increased from 8 up to \$ 15 billion in a few days. This process demonstrates companies and investor's search for new tools to create a platform for financial transactions and settlements in various areas of human activity, taking into account past shortcomings and shortcomings and continued progress in this field. But in the case of the IOTA cryptocurrency for IoT the possible drawback is that this currency is pre-mined while devices in the network could use surplus resources to generate coins. But the best way in the future is to use excess of computing power and energy for more needed calculations and for

artificial intelligence. The existing model of interaction between devices with hardware, network and application levels should be supplemented by a level of distributed calculations, which will include the ability of local calculations and work on global tasks. Cryptocurrency better than all other with options for calculations, accumulation and first protocol realization on the market will appear, which will become an absolute leader and replace all the others. Hardware background for this crypto coins will be in IoT network in any case from the point of view of the need for places and methods for conducting monetary payments. But already in early 2018 we saw the problem of the spread of cryptocurrencies, among which there were sharp changes in the exchange rate and the lack of practical implementation, including into the Internet of things. IoT requires the implementation of digital encryption of information, transaction support and recording of all events for security. It can provide cryptocurrencies protocols with adding an additional possibility of payments. This opportunity is not so much demanded at the hardware level as in the software implementation. We have discovered that IoT devices are widely used for illegal purposes for trusts or network consolidated attacks, and virtually no legal and useful ways of using their hardware-distributed capabilities. Standardization and compatibility in IOT network should become the main tools for the possibility of introducing new solutions, testing their utility, performance and safety. A clear position of the government at this stage is extremely important in the issue of supporting the innovative component of cryptocurrency and developing a strategy to prevent the possible negative impact from their active use and implementation. The growth of capitalization of major cryptocurrencies, the worldwide spread of technologies such as mining, blockchain and ICO has forced most developed countries to apply different regulatory methods to a new process, which will now undoubtedly change the global financial system. The top priority for countries governments is to create the necessary legislation and conditions for the development of new projects and products using cryptocurrency. Leading financiers around the world are now raising questions about whether cryptocurrencies are a financial pyramid and a bubble that can be devaluated at any time and lead depositors to bankruptcy. Obviously, the new financial system is undergoing repeated transformations and corrections, but in

our opinion, impairment is impossible to zero. This is due to the fact that the crypto coins unambiguously found their scope of application in the form of rapid and safe transfer of funds from one point of the world to another, anonymous and documented transactions. A bankruptcy of some crypto project will lead to the fact that it will inevitably be redeemed for further use, and thus the complete collapse of the new system is very unlikely. The process of including in the IoT financial component will better organize a distributed system and solve the problems of payback and practical use.

Problems of cryptocurrency usage

The global financial system entered a new phase of innovation with the development of cryptocurrency with using of IT, protocols and networks. Around the new digital decentralized crypto system for 9 years of existence was created new infrastructure in the form of mining and support of transactions, funds, bidding and exchanges, placement and creation of new projects. The growth of capitalization of Bicoins and other major cryptocurrencies already has a significant impact on the world economy and global development. Most countries began with the growth of Bitcoin imposed to ban the further development of cryptocurrency - restrictive laws adopted in China, Korea, USA. They are trying to detain the owners of electronic exchanges, prohibit the use of ICO (cryptocurrencies IPO) and enter operating taxes. Some governments have been thinking about using cryptocurrencies and even announcing the creation of their own. The top financiers in the world are now raising questions about whether cryptocurrency and Bitcoin, in particular, are a financial pyramid and a bubble that can devaluate at any time and lead depositors to bankruptcy. Obviously, the new financial system is undergoing repeated transformations and corrections, but in our opinion, impairment is impossible to zero. This is due to the fact that the cryptocurrency unambiguously found their scope of application in the form of a fast and safe transfer of funds from one point of the world to another, anonymous and documented transactions. With the bankruptcy of a particular cryptocurrency project it will inevitably be redeemed for further use, and thus the complete collapse of the new system is very unlikely. The new financial instrument with the use of new digital currency and blockchain tech-

nology has actually been created. He is even backed up with hardware: computing power for mining and transaction support. But, the sphere of direct use of the most cryptocurrency and the products and services that can be purchased for them is not formed. A clear position of the government at this stage is extremely important in the issue of supporting the innovative component of cryptocurrency and developing a strategy to prevent the possible negative impact from their active use and implementation. There is also a need for taxation of this activity in the future by the state, with a definition of the time frame of the transitional process with zero tax to prevent the negative impact on the process of origin and development. Also global Internet for cryptocurrencies operation with IoT is needed. Russian possibility of the disconnecting from global Internet was appear in the news in 2014 and at the end of 2016. It is the first time country with large economy can change its connection type to the global Internet not at the beginning of its implementation as China, Iran or North Korea. Another country can do it in the future and not only on their own volition. And now are important and relevant the possible scenarios for disconnect some country from Internet. The main questions are how much costs this process and what will be after this with economy of the country. Global Internet is one of the important driver of development of the countries in our time. It is a financial network, news center, bank of exchange with new ideas, trends and goods. There are countries in the world that want to control traffic for its own population with propaganda reasons such as China, Iran, North Korea, Russia. There are three possible scenarios for absolute disconnection of the country or some other region from global Internet: country disconnect itself from global Internet; another countries disconnects some country from Internet; someone else disconnect country from Internet with hacker's attack. First choice can be realized in the country with centralized management of Internet Service Providers (ISP). Internet traffic can be controlled in the autonomous systems (AS) by tagging with Multiprotocol Label Switching (MPLS protocol) on controlled ISP's with routers and routing for non-tagged traffic with BGP disabled in this systems. So non-tagged traffic can be routed on high levels or trunked with no access to Internet clients and they will haven't access to other IP addresses than in its internal AS. Second scenario can be realized with the same schema

with source traffic detection on the Root DNS servers. Internet traffic from country with sanctions can be marked with MPLS with routing to all other AS disabled [10, 11]. There are some security fixes than with traffic delay from controlled country. It enables some protection from hacker's attack from this country like attacks of the Russian hacker's on USA election process at the end of 2016. Third scenario is some new from the out time.

CONCLUSIONS

IoT (Internet of Things) requires the implementation of digital encryption of information, transaction support and recording of all events for security. It can provide cryptocurrencies protocols

with adding an additional possibility of payments. This opportunity is not so much demanded at the hardware level as in the software implementation. We have discovered that IoT devices are widely used for illegal purposes for trusts or network consolidated attacks, and virtually no legal and useful ways of using their hardware-distributed capabilities. Standardization and compatibility in IOT network should become the main tools for the possibility of introducing new solutions, testing their utility, performance and safety. The standardization of a new approach to interactive protocols in the IOT network and the Internet with a finance approach is now inevitable.

REFERENCES

1. CoinMarketCap. (2018). Top 100 CryptoCurrencies by Market Capitalization. Retrieved July 1, 2018, from <https://coinmarketcap.com>
2. Statista. (2018). *Size of the global Internet of Things (IoT) market from 2009 to 2019 (in billion U.S. dollars)*. Retrieved July 1, 2018, from <https://www.statista.com/statistics/485136/global-internet-of-things-market-size/>
3. Vigna, P., & Casey, M. (2015). *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: St. Martin's Press.
4. Fry, J., & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, 47, 343–352. doi: [10.1016/j.irfa.2016.02.008](https://doi.org/10.1016/j.irfa.2016.02.008)
5. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Oxford: Princeton and Oxford Princeton University Press.
6. Gigli, M., & Koo, S. (2011). Internet of Things: Services and Applications Categorization. *Advances in Internet of Things*, 01(02), 27–31. doi: [10.4236/ait.2011.12004](https://doi.org/10.4236/ait.2011.12004)
7. Castellani, A. P., Bui, N., Casari, P., Rossi, M., Shelby, Z., & Zorzi, M. (2010). Architecture and protocols for the Internet of Things: A case study. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. doi: [10.1109/percomw.2010.5470520](https://doi.org/10.1109/percomw.2010.5470520)
8. Kurzweil, R. (2016). *The singularity is near: When humans transcend biology*. London: Duckworth.
9. Russell, S., & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd ed.). Upper Saddle River: Pearson.
10. Roberts, H., Laroche, D., Faris, R., & Palfrey, J. (2011). *Mapping Local Internet Control*. Retrieved August 1, 2018, from <https://pdfs.semanticscholar.org/bdd5/be2dd6706ca1c1659cf2c9bd26811b9c802d.pdf>
11. Murdoch, S., & Anderson, R. (2008). *Tools and Technology of Internet Filtering*. Retrieved August 1, 2018, from <http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-3.pdf>