OPTIMAL PAYMENT INFRASTRUCTURE FOR THE INTERNET OF THINGS

Matić Jelena*

External Business Consultant at Clearstream Banking Frankfurt (Deutsche Börse AD), Frankfurt, Germany

Abstract:

The term Internet of Things (IoT) implies the highest level of integration of people with devices and machines that are used in business processes and everyday life. This refers to a network of devices, machines, vehicles and objects, connected by communication networks such as the internet, NFC and RFID, equipped with microprocessors, sensors and appropriate software, which enables data collection, their processing and timely distribution. To utilize the full potential of this concept, a special payment infrastructure needs to be built, and its sole purpose would be to transfer funds in the context of the new information revolution. The subject of the research is the need for the creation of new payment infrastructure for the realization of all advantages of the concept of the IoT. By comparing key performances of the blockchain and tangle as technologies for distributed database management, the goal of the paper is to point to their potential for their application in payments in the ecosystem of the IoT. Based on the comparative analysis of bitcoin and IOTA, i.e. blockchain and tangle technology, that it is necessary to strive for a solution that will not burden the system and that will be a means for achieving security at a high level at the same time.

Keywords:

Internet of Things, cryptocurrencies, blockchain, tangle, bitcoin, IOTA.

INTRODUCTION

The development of information and communications technologies (ICT) in the second half of the 20th century has changed the way of doing business for most industry branches. In addition to the informatization of traditional manufacturing activities, conditions were created to develop new service activities. Computers and computer systems, seen as the highest form of ICT application in business and life, have enabled the collection, processing and distribution of a huge amount of data, which would practically be impossible with manual labor. Communications services and the financial sector have improved at great speed under the influence of technical progress, while the industry of consumer electronics would practically be unimaginable without these achievements. The end of the 20th and the beginning of the 21st century were characterized by

Correspondence:

Matić Jelena

e-mail:

jelenamatic.srb@gmail.com

DOI: 10.15308/Sinteza-2021-170-176

a race of manufacturers to increase the clock rate of computer processors and graphic cards and bandwidth speed. In the last couple of years, however, the focus has shifted to connecting as many devices as possible and to their interaction when collecting, processing and distributing data. One of the key pillars of the new technological revolution is the Internet of Things (IoT), as the highest level of integration of people with devices and machines in their environment.

To utilize the full potential of this concept, integration of payment solutions is required. The inclusion of value transfer into the concept of the IoT leads to the Internet of Value (IoV), a global network which enables the flow of funds in addition to the flow of information. The problem with the realization of this idea is the fact that there is no adequate payment infrastructure.

The subject of the research is the need for the creation of new payment infrastructure for the realization of all advantages of the concept of the IoT. By comparing key performances of the blockchain and tangle as technologies for distributed database management, the goal of the paper is to point to their potential for application in payments in the IoT ecosystem.

The first part of the paper will explain the significance of the concept of the IoT for the revolution in business processes. The second part will focus on the characteristics of current and potential payment systems and their potential to contribute to the creation of the IoV. In the third part, the core functioning principles of blockchain and tangle technology will be compared, with the objective to identify the key advantages and disadvantages.

2. THE CONCEPT OF THE INTERNET OF THINGS

The creation and evolution of the internet have changed the outlines of the old society in many aspects. Namely, the application of new communications channels in all spheres of human life has considerably changed the character of how society functions and develops, whereas the development of the information-communications component was popularized during the last two decades. The implementation of new solutions has contributed to a noticeable change in conducting numerous activities to make them more efficient, i.e. easier and faster. That is why changes in the information-communications sphere can be seen as key drivers of development not only in the previous, but also in the upcoming period.

Among other things, the new information revolution is based on the concept of the IoT, whose founder is Kevin Ashton. The basic idea was to place an intelligent RFID bar code on a specific company product to know how many products have been sold at any time and when shelves should be restocked. In the early stage, it was noticed that this principle could be applied to numerous areas in everyday life.

The concept of the IoT comprises of all the devices which can be connected to the network and which can collect, send and function with the data they collect from the environment by using built-in sensors, processors and communications hardware [1]. That way, machines can communicate with other connected devices in a process called M2M communication (Machine-to-Machine). Users can adjust these devices, give them instructions or access data, which would represent a communication model called M2P (Machine-to-Person), although their operation is overall independent. This kind of technology enables access to everyday information in addition to other numerous activities, and it offers unprecedented possibilities thanks to the level of development and quality of equipment and components upon which it is based, but also thanks to the users' constant online presence in all spheres of business and life.

Today billions of devices form an integral part of this platform, where they use built-in hardware and software to send and receive messages through various communications protocol. Mobile phones could be used to access the internet, and they could also be connected to another part of hardware which would be located in the house or in the workplace. Based on that, it can be said that one of the end products of the concept of the IoT is the creation of a smart work environment and smart homes in which every device would function automatically to create a more quality and more innovative life for people [2]. In other words, the ultimate goal of the concept of the IoT can be interpreted as the creation of an automated life and work for people and the creation of a smart environment in which it would be easier for individuals to control all situations and in which conditions would be created that would make work and routine operations much faster.

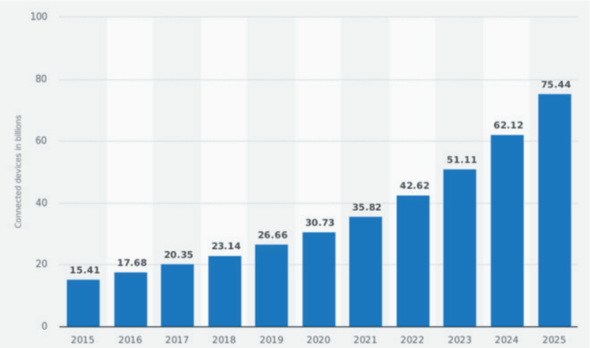

Figure 1: An estimate of how many devices would be connected by 2025, shown in percentages

Figure 1 shows the concept of the IoT, where the increase in percentages from 2015 to 2021 was 20.41%, while it is estimated that the increase will even reach 75.44% by 2025.

By observing the evolution of the internet, it can be concluded that the concept of the IoT represents the third stage in communication via the internet [3]. In the first stage, the content was not interactive, so the users could clearly be divided into those who created the content and those who used the content. In this stage, the content on the web could be watched, listened to or read, but users could not participate in its creation. The next stage in the development of the internet offered considerably broader opportunities because the boundary between those who created the content and those who used it disappeared, because in this stage anyone could not only create, but also use specific content at the same time. All that is the result of the fact that most web locations also contain a social component which offers the possibility of participation by adding photos, videos, comments and similar content. Finally, it is precisely the concept of the IoT that is developed in the third stage of the development of communication via the internet. In this stage communication does not only exist between individuals, but also between specific devices, which means that things that are inherently passive now also have an active role, since communication can also be realized between them. This is a stage in which things will be transformed into "smart workers" that could exchange information about them and their environment.

3. APPLICATION OF THE EXISTING PAYMENT INFRASTRUCTURE IN THE INTERNET OF THINGS ECOSYSTEM

One might ask what kind of payment architecture would be suitable to the development of the concept of the IoT. In other words, the question is whether and to what extent the existing mechanisms of payment match the key characteristics of the new information revolution, and if not, which models of payment would be most suited to the given concept. Considering the given question, experts agree that the existing payment architecture would not be suitable to the new concept of the IoT for several reasons. First, they believe that payments in cash would not be by the desired level of automation on which the concept of the IoT is based, whereas traditional cashless forms of payment are unsuitable because they are slow and because their transaction costs are high [4]. Additionally, since it is believed that micropayments will play a key role in the new information revolution and smart environment, instruments of payment should accordingly be suitable to make payments of small amounts. Since debit cards are suitable for payments of large amounts due to processing costs, it is believed that these payment mediums would not be suitable to the planned environment.

From today's perspective, POS terminals represent a dominant channel, considering executing cashless transactions, but they would not represent a good solution as a payment channel in the concept of the IoT because they are stationary, i.e., they are tied to a physical location [5]. In that sense, the new information revolution will inevitably cause changes not only in the way the society functions, but also in the way payments are made in terms of channels and instruments. The creation of a special payment infrastructure, intended solely for the transfer of funds in the context of the new information revolution, would lead to the realization of the concept of the IoV. To achieve that, it is necessary to abandon the existing payment mechanisms and to base the future payment architecture on the organizational structure of the internet. In other words, to enable the transition to the concept of the IoV, it is necessary to unify the network of all payment systems, which would imply the integration of national and commercial banks, payment systems and electronic money systems.

According to the previously stated, when designing an optimal payment system for the concept of the IoT, two key prerequisites must be met: to create a digital identity of the device or to perform its integration through the owner's identity and to make sure that transactions are economical, especially considering micropayments. Since it is to be expected that many devices will be used to make payments in the future, then these transactions should be institutionalized in some way. It is proposed that each device should get its own digital identity so that it would be recognized when executing future transactions. An alternative to this approach would be to create a centralized system with a digital identity, which is based on a unique device to which all other devices would be connected. From the current perspective, these devices are still in the development stage, although certain conceptual solutions already exist, which can be seen in the example of Amazon Echo.

To sum up everything that has been stated, the following question can be asked: could cryptocurrencies be an instrument of payment on which the functioning of a smart society would be based? It is overall undeniable that in the concept of the IoT, only electronic money could contribute to the development of its full potential. Among numerous variants of commercial electronic money, state forms of electronic money could emerge as one of the rational solutions soon. When it comes to cryptocurrencies, from the aspect of their basic characteristics, they would certainly be a suitable solution, having in mind that they are suitable for small payments and that they do not require large transaction costs. However, when it comes to using cryptocurrencies as one of the main payment methods in the smart society era, there is a considerable polarization of opinions. For one, it is pointed out how the chances of the current systems being in wider use are quite slim in future circumstances even though cryptocurrencies have their advantages, and that is mostly because of their high volatility, having in mind that their prices fluctuate considerably in short periods. In the case of bitcoin, a problem might also be seen in poor scalability because in the upcoming period, when everything will be automated to achieve greater speed and efficiency, it would be necessary to secure a satisfactory speed of carrying out transactions as well.

4. A COMPARATIVE ANALYSIS OF FUNCTIONAL CHARACTERISTICS OF BLOCKCHAIN AND TANGLE

The blockchain represents the first operational form of DLT. It is designed to function in an environment in which there is no central institution that can confirm the authenticity of data and in which the participants do not trust each other [6]. Blockchain consists of a series of blocks, in which the previously performed transactions are stored. The content of each subsequent block must be following the state to which the previously installed blocks have led. This means that entity X could not spend the funds in transaction q if it had already spent the funds in a previously accepted transaction p. If this entity X tries to do that, transaction q will be discarded and it can not become part of a new block. The mechanism by which the authenticity of new transactions is verified and by which new transactions are packed into blocks is called a consensus protocol [7].

The block has two parts: a header and a body. In the block header, the ordinal number is entered, then the timestamp, to determine the chronological order of the assembled blocks, then the previous block hash, afterward the Merkle tree root, which means that new transactions must be linked to all that was previously entered and with the hash record of the new block. The block body contains the transactions which the miner wants to confirm [8].

The blockchain is characterized by the division of roles among the participants. Nodes are the participants that have permission to perform transactions, i.e. to appear as payers and recipients of funds. Miners are the participants who pack transactions into blocks, confirm them and add new blocks to the chain. The validation process itself involves reaching consensus among miners and can be more or less compute-intensive [9]. The choice of the consensus-building protocol depends on the type of blockchain system which was used.

Overall, each cryptocurrency has its own blockchain and the largest number of cryptocurrencies (starting from bitcoin onwards) has a public blockchain, which can be accessed by anyone and all the transactions that have taken place in the chain of blocks can be seen.

Moreover, in this system, anyone can be a miner - anyone can perform transactions and participate in the creation of blocks. The mining process itself shall be further elaborated in the subsequent part of this paper. One of the key features of a public blockchain is the fact that the protocol that manages the system is in the form of an open-source code, and each of the participants can review it and suggest possible improvements in terms of code completion. On the other hand, numerous cryptocurrencies use private blockchain, which ensued as a result of the fact that some users of blockchain technology did not like the transparency in the public blockchain system along with the fact that this system is available to everyone. Following that, private blockchains have been designed in which the code is not visible to everyone, but only to those entities that have a license issued by the creator or owner of the blockchain. However, private blockchain systems are rarely used for cryptocurrencies and are mostly used for other business applications.

Based on the information mentioned above, key differences between these two forms of blockchain technology can be observed. On the one hand, public blockchains are open and they provide more freedom to participants both in conducting transactions and in the process of decision-making and improvement of protocols. It is precisely this transparency of public blockchains that represents their most significant advantages, primarily when it comes to stronger resistance of blockchains to potential attacks. Hence, it is very difficult to have such many nodes to jeopardize the normal flow of information through the network. Another advantage of public blockchains is reflected in the stability of the database due to the fact that the entire database is located on thousands of computers spread all over the world. Apart from that, a group of miners with a very large cumulative processing power maintain the blockchain network. Even if somebody wanted to perform a change of base, most participants would have to agree with that change, although it is very unlikely that most participants would agree to change something that could jeopardize the integrity and security of the network.

However, apart from all the advantages mentioned above, public blockchains also have certain disadvantages. Thus, the main disadvantage related to the concept of public blockchains is the slow system of managing and deciding, because it is necessary to establish consensus. Another disadvantage of public blockchain technology is reflected in a very limited capacity of blockchains, not only in the number of transactions which can be processed, but in the amount of data which can be stored in the chain of blocks as well. However, the stated facts depend on the protocol which was chosen for establishing consensus, but it is a general problem of all the key systems of crypto currencies.

The consequence of this is the lower efficiency of the network, which can be seen best in the example of the bitcoin network which can process only a few transactions per second.

Comparative analysis of blockchain and tangle raises the question of whether tangle is the technology of the future for storing and verifying the information. The first differences observed are the difference in the structure between blockchain and tangle, both of which continue to build an independent and self-governing network of transactions. Tangle is just one of the operational solutions of the DAG (Directed Acyclic Graph) system. It is based on a mathematical model and on the architecture used to organize, record, store and verify the information [10]. More precisely, tangle represents the system of records of individual transactions which were not collected into blocks and which were not linearly organized, as it is the case with blockchains.

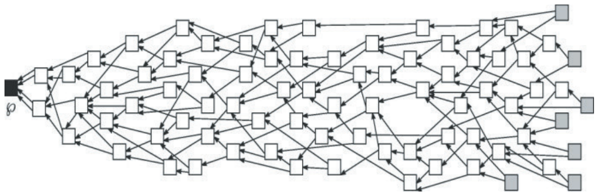

Figure 2: The structure of message validation in the network tangle [11]

Figure 2 shows the message validation structure in the network tangle. From this figure, one can see the validation of messages in the tangle network, which can be with a large and small load. Highlighted areas represent recent transactions. The direction of the arrows shows which other two transactions are confirmed when they occur. With more transactions, the process becomes more complex, which can lead to some transactions waiting longer until they are approved for the first time.

Prior to the execution of transactions via tangle, the previous two transactions have to be verified. At the same time, the word "acyclic" indicates that past transactions can neither verify future transactions nor present ones. The whole system comes down to the fact that the machines can communicate with each other M2M and they all together make one huge network.

On the other hand, one of the basic problems of blocking has been overcome by tangle. Hence, the devices can be connected to the network and perform their functions smoothly, even if M2M transactions are small. Another critical part of most blockchain systems is scalability, as the ledger becomes larger, a delay in functioning occurs - as a cause and effect relationship. Tangle technology is based on a different principle. The more devices are connected, the more the network develops, and thus creates a good basis for building an overall self-linking microeconomy, where machines can cooperate with each other and contribute to the acceleration of flow.

When it comes to cryptocurrencies, in addition to the investment aspect, one should also take into consideration their role in the future innovative and automated society, indicating that they could be an adequate payment instrument in the post-information revolution. A real example of this is the IOTA, for which many experts point out that it is designed for the concept of the IoT.

To be useful as a payment network, IOTA must provide a method by which the transaction will be considered securely validated, that is, when the transaction is accepted for public consensus. There are two approaches to creating consensus in the loop, and these are the currently implemented coordinator approach and the distributed approach. A coordinator is an entity that controls IOTA, where a zero-value transaction is entered every two minutes, by the values called a milestone. By using a coordinator, the definition of consensus is simple; consensus represents each transaction to which the confirmed milestone refers, while the others have not been confirmed. A consensus is defined by the coordinator and this consensus represents each transaction that already has a verified milestone. Also by using a milestone, this digital currency is safe against attacks, as it validates transactions that have been done in the last two minutes.

IOTA also has a transaction of origin, which is directly or indirectly confirmed by all other transactions [12]. If there is no direct confirmation path of the transaction between them, and if there are at least two paths in relation to the other transactions that connect them to the transactions, then those two transactions are indirectly confirmed. What is characteristic of IOTA cryptocurrency is that unlike Bitcoin and most other cryptocurrencies it is not based on blockchain technology but on tangle technology which means that transaction costs are insignificant [13]. Having in mind the information given above, as well as features which set IOTA apart from other digital currencies (no transaction costs, no scalability problems), it can certainly be expected that this cryptocurrency will be far more significant in the future.

As it can be observed, tangle and blockchain have a lot in common. These are two technologies which are based on cryptography, with different systems of functioning. In the case of blockchains, each previous record with information on all executed transactions that are distributed among the special users who maintain the system (miners) in the chain of blocks must be verified for each subsequent record.

Each node in the blockchain must have a valid updated version of the public ledger. The updating of each public ledger leads to a burden, and thus causes a slowdown, as stated in the previous paragraph. So, it is concluded that the size of the block is limited, as well as the number of blocks that can be "built" during each hour. As the ledger becomes heavier, the task of mining becomes more and more complicated, the system becomes slower, and the mining process itself becomes more expensive. All of the above leads us to ask the question of whether new cryptocurrencies tend to overcome existing problems.

The approach used in tangle is based on the general ledger being distributed among all users, not just among miners, which actually means that each network participant must perform the function of a miner. With transactions performed via tangle, the system becomes more powerful, which means that each new record in the book contains the same amount of information as the previous one. The verification process itself is reduced to just two transactions, without the need to maintain the entire network.

Based on previously facts, it can be concluded that:

- Tangle has better power throughput and is more scalable, and over time it becomes faster and more powerful. However, the situation with bitcoin is different; the general ledger becomes more loaded with information, which leads to a slowdown and lower productivity.
- Tangle transactions do not produce high transaction costs as is the case with most blockchain-based cryptocurrencies.
- On the other hand, bitcoin, as a representative example of a cryptocurrency based on blockchain, shows that it is more secure and more resistant to hacking ventures than IOTA thanks to a complex verification algorithm.

5. CONCLUSION

The overall conclusion is that blockchain systems are expensive as the technical infrastructure for the payment system of the future. Such a conclusion may seem contradictory at first glance, since almost all cryptocurrencies are based on them. Tangle currently represents the technical basis of a smaller number of cryptocurrencies, of which IOTA and nano should be singled out. The advantage of tangle is the reduction of transaction costs by eliminating the division of participants into nodes and miners. The advantage that these cryptocurrencies have is that transactions are not packed in blocks, so the waiting time for confirmation of the transaction is shorter.

While most systems experience the problem of scalability with the growth of the number of participants and executed processes, the situation is different with tangle - the greater danger is posed by the absence of participants and by a small number of transactions because it increases the time required to execute an individual transaction.

The main problem is that neither IOTA nor nano are in the group of major cryptocurrencies. This does not mean that they have not yet been tested at the level of workload that they would suffer with the number of users who have ether or bitcoin. At the beginning of March 2021, bitcoin had a market capitalization of over 620 billion US dollars, IOTA around 3 billion, and nano only 0.93 billion of US dollars. Low capitalization was accompanied by lower trading volume. We can conclude two things: firstly, IOTA and nano did not have the opportunity to show real limitations in throughput and scalability, and secondly, since they are less attractive in trade, they were partially spared by the attacks suffered by systems of more popular cryptocurrencies.

REFERENCES

[1] G. Russo, B. Marsigalia, F. Evangelista, M. Palmaccio and M. Maggioni, “Exploring regulations and scope of the Internet of Things in contemporary companies: a first literature analysis,” *Journal of Innovation and Entrepreneurship*, vol. 4, no. 1, 2015.

[2] T. M. Fernandez-Carames and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32797-33001, 2018.

[3] N. Tomić and V. Todorović, “The future of payments in the Internet of things,” in *Sinteza 2017 - International Scientific Conference on Information Technology and Data Related Research*, Belgrade, 2017.

[4] C. Skinner, “Payments hold the key to the Internet of Things,” 1 June 2016. [Online]. Available: https://www.thebanker.com/Transactions-Technology/Payments-hold-the-key-to-the-Internet-of-Things?ct=true. [Accessed 1 June 2021].

[5] N. Tomić, Organizacija savremenog platnog prometa, Kragujevac: Ekonomski fakultet Univerziteta u Kragujevcu, 2020.

[6] S. M. H. Bamakan, A. Motavali and A. B. Bondarti, “A survey of blockchain consensus algorithms performance evaluation criteria,” *Expert Systems with Applications*, vol. 154, 2020.

[7] F. B. Schenider, “Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial,” vol. 22, no. 4, pp. 299-319, 1990.

[8] Y. Zhu, Z. Zheng and C. Lv, “Anonymous Voting Scheme for Boardroom with Blockchain,” *International Journal of Performability Engineering*, vol. 14, no. 10, pp. 2414-2422, 2018.

[9] L. Ismail and H. Materwala, “A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions,” *Symmetry 2019*, vol. 11, no. 10, 2019.

[10] S. Popov, O. Saa and P. Finardi, “Equilibria in the tangle,” *Computers & Industrial Engineering*, vol. 136, pp. 160-172, 2019.

[11] S. Popov, “The tangle, version 1.4.3,” 30 April 2018. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf . [Accessed 2 June 2021].

[12] W. F. Silvano and R. Marcelino, “Iota Tangle: A cryptocurrency to communicate Internet-of-Things data,” *Future Generation Computer Systems*, vol. 112, pp. 307-319, 2020.

[13] Y. Jiang, C. Wang, Y. Wang and G. Lang, “A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management,” *Sensors*, vol. 19, no. 9, 2019.