

THE POSSIBILITY OF USING DISTRIBUTED LEDGER TECHNOLOGIES AS PAYMENT INFRASTRUCTURE



UDC 004.738.5

Zorana Kostić¹, Nenad Tomić²

¹University of Niš, Faculty of Mechanical Engineering, Niš, Serbia

²University of Kragujevac, Faculty of Economics, Kragujevac, Serbia

ORCID iD: Zorana Kostić
Nenad Tomić

 <https://orcid.org/0000-0001-8974-3916>
 <https://orcid.org/0000-0003-1565-3197>

Abstract. *The Internet of Things represents a communication network that enables people to interact with things, machines and objects in the business and living environment. Adding the ability to perform transactions to the information component leads to the creation of the so-called Internet of Value. Modern payment processing mechanisms do not meet the needs of the Internet of Value. In order to achieve a fast and economical financial flow, it is necessary to overcome the fragmentation of traditional payment systems and adopt the organizational structure of the Internet. The subject of the paper is the characteristics of three distributed ledger technologies. The aim of this paper is to determine the possibility of their use in order to build a payment infrastructure for the realization of the Internet of Value concept. Although the issue of security of the new payment infrastructure is equally important, the paper will focus on three key performances of the observed distributed ledger technologies: costs, throughput and scalability. The qualitative analysis shows that none of the analyzed technologies in practice has adequate performance in terms of throughput and scalability. Most operational solutions, even in experimental conditions, achieve poorer results than theoretically predicted ones.*

Key words: *Internet of Value, Blockchain, Hashgraph, Tangle, distributed ledger technologies, Internet of Things, Financial-technological integration*

JEL Classification: L17, O33

Received July 02, 2021 / Revised November 13, 2021 / Accepted November 22, 2021

Corresponding author: Zorana Kostić

University of Niš, Faculty of Mechanical Engineering, Aleksandra Medvedeva 14, 18000 Niš, Serbia

| E-mail: zorana.kostic@masfak.ni.ac.rs

INTRODUCTION

The beginning of the 21st century was marked by the race of manufacturers to raise the clock speed of computer processors and graphics cards and increase the Internet throughput. With the achievement of values that enabled the transfer of large amounts of data and its timely processing in application programs, the research focused on networking as many devices and learning given behaviors (Tomić, 2020, p. 363). The new information revolution relies on three processes: the Internet of Things, the processing of large amounts of data, and machine learning. The Internet of Things means a communication network that enables people to interact with things, machines and objects in the business and living environment (Tomić & Todorović, 2017, p. 97). In order to be involved in communication, devices must be equipped with appropriate sensors and microprocessors for receiving and processing basic information, actuators used to take certain actions, a modem for connecting to the Internet and software, which should enable data processing and, if possible, behavioral learning (Gupta & Gupta, 2020, p. 9). In this way, the Internet of Things represents the starting point of the information revolution, which provides inputs for processing large amounts of data and increases the need for machine learning.

A large number of established connections and communications do not have to refer only to the distribution of information, but can also imply the execution of payment transactions. The Internet of Things would thus become the basis for decentralized initiation and execution of transactions. Adding a financial component to the information would lead to the creation of the so-called Internet of Value (Floros, 2019). The biggest obstacle to the operationalization of this concept is the rigidity of traditional payment operations.

In order to fully use the potentials of the Internet of Things, it is necessary to build an adequate payment system. It should be borne in mind that the payment system would have to allow relatively fast finality of a large number of transactions, which would often belong to the category of micropayments. That is why the security and efficiency of the system are two key issues when designing a payment infrastructure for the Internet of Things. The subject of the paper will be the functional characteristics of three distributed ledger technologies (DLTs). The aim of this paper is to determine the possibility of their use in order to build a payment infrastructure for the realization of the concept of the Internet of Value.

The paper consists of three parts. The first part will explain the concept of the Internet of Value, identify its potentials for changing the way of doing business and life and determine the conditions for its implementation. In the second part of the paper, the technical characteristics of all three technologies will be analyzed individually: Blockchain, Tangle and Hashgraph. A qualitative analysis against three criteria: costs, throughput and scalability, will be in the focus of the third part. A conclusion regarding the possibilities of using DLTs for the construction of a new payment infrastructure will be made upon comparing their performances against desired values of these criteria.

1. FINANCIAL-TECHNOLOGICAL INTEGRATION WITH THE AIM OF CREATING THE INTERNET OF VALUE

The Internet of Things represents a paradigm of information integration, in which devices and objects, which are passive in nature, become intelligent stakeholders, capable of collecting and distributing information (Tiwary et al., 2018, p. 23). Information sharing is

not focused only on the people involved in certain processes, but the communication takes place on a m2m (man-to-machine or machine-to-machine) route. Intelligent objects not only process information, but also have the ability to take certain action, in terms of giving answers or sending requests. Given their ability to receive, process and transmit information, devices connected to the Internet of Things create a “smart work environment” or “smart home”. The end result of integrating devices into the Internet of Things should be the automation of routine activities in which the key source of error is the human factor. DeNisco (2017) lists manufacturing, transportation, medicine, power management, and consumer electronics as the five primary areas of application of the Internet of Things.

Basically, the Internet of Things does not require the implementation of payment solutions. The messages sent by the mentioned stakeholders do not have to be only of an informative nature, but they can initiate an action that involves making payment. This would give the devices, with the prior authorization of the owner, the opportunity to make purchases of the necessary products and services. Internet of Values is the key to permanent supply chains, whether they are households or industrial systems. Smart home appliances would be able to order new stocks of consumer goods on time, the condition of which they can monitor. Smart industrial systems would provide an additional tool for managing just-in-time supply chains, removing the human factor as the cause of temporary downtime in the production cycle. In a broader context, the Internet of Value refers not only to enabling devices to perform a transaction, but to networking all stakeholders into a global value exchange network. Money transfer would be only one aspect of the exchange, because the same infrastructure could be used to exchange financial instruments and for smart contracts (Finance monthly, 2018). In addition to the unique infrastructure, the key advantage of the Internet of Value should be the elimination of middleman and the reduction of exchange costs to a level close to zero (Ripple, 2017).

Modern payment organization does not meet the needs of the Internet of Value. Due to its manual nature, cash payments are not considered. Non-cash payment system shows good throughput characteristics, which means that it is able to support the growing volume of transactions. However, the key drawback in this case is the cost of transactions and the issue of creating a digital identity of devices as payment initiators. Due to the large number of middlemen (which, depending on the situation, may involve two to four institutions), non-cash payment transactions produce certain costs, which are charged in the form of a commission. That is why such a way of organizing is inadequate for micropayments. In order to achieve a fast and economical financial flow, it is necessary to overcome the fragmentation of traditional payment systems and adopt the organizational structure of the Internet. In other words, a payment system that would support the creation of the Internet of Value must enable the integration of traditional payment transactions, electronic payment systems such as digital wallets, electronic money and cryptocurrencies, through the construction of a completely new infrastructure (Cheng, 2015). Existing payment instruments could be replaced by completely new ones within this new infrastructure. The construction of a new payment infrastructure would redefine the number and role of middlemen in transactions, which would enable not only faster payment, but also lower costs.

There is an immanent security problem for all electronic payment systems. Therefore, ensuring the security of the new payment infrastructure would be one of the key issues. In addition, the new infrastructure must have satisfactory operational characteristics. In order to achieve the aim of the paper, the authors have formed a research question: do existing distributed ledger technologies have satisfactory operational characteristics? The

analysis will include in particular cost, throughput and scalability. In the third part of the paper, a qualitative analysis will be performed in order to obtain the answer. A positive answer would mean that some or all of them can be used as the technological basis of the payment system for the Internet of Value. In case of a negative answer, the authors will explain their key operational shortcomings.

2. DISTRIBUTED LEDGER TECHNOLOGIES

Distributed ledger technologies are considered to be one of the foundations of the fourth industrial revolution. The concept became known to the general public with the advent of Bitcoin, the first cryptocurrency (Nakamoto, 2008). Although Blockchain, as the best-known form of this technology, is often equated with cryptocurrency systems themselves, DLTs are widely used in supply chain management, transportation, healthcare, and other industries. The basis of this technology is the general ledger, which records transactions between two parties, so that once entered ledgers cannot be subsequently changed (Iansiti & Lakhani, 2017). Transactions are any instruction that lead to a change in the state of the system and do not have to refer only to payments. DLTs are digitally stored data with consensus-based accuracy, mutually synchronized and shared independently of national borders, platforms used for its reading and writing, or institutions and organizations using it (Walport, 2015, p. 5). There is no single system administrator or central database in which data is entered first (Scardovi, 2016, p. 36).

In addition to Blockchain, Tangle and Hashgraph have been developed as alternative operational solutions to DLT. In the following parts, the key functional characteristics of all three technologies will be presented.

2.1. Blockchain

Blockchain is the first operational form of DLT. It is designed to operate in an environment where there is no central institution to validate data and where participants do not trust each other (Bamakan, Motavali & Bondarti, 2020). It consists of a series of blocks, in which the executed transactions are stored. The content of each subsequent block must be in accordance with the state to which the previously installed blocks have led. This means that entity X would not be able to spend in transaction q the funds it has already spent in previously accepted transaction p. If it tried, transaction q would be discarded and could not become part of the new block. The mechanism by which the authenticity of new transactions is verified and packed into blocks is called a consensus protocol (Schneider, 1990).

Figure 1 shows a general way of connecting blocks of information. The block has two parts: a header and a body. In the block header, enter the ordinal number, then the timestamp, to determine the chronological order of the assembled blocks, hash of the previous block, the Merkle tree root, which means that new transactions must be related to all previously entered, and hash of the new block. In the part that is marked as the body of the block, there are transactions that the miner wants to confirm.

The Blockchain is characterized by the division of roles among the participants. Nodes are participants that have permission to execute transactions, i.e. to appear as payers and recipients of funds. Miners are participants who pack transactions into blocks, validate them and add new blocks to the chain. The validation process itself involves

reaching consensus among miners and can be more or less computer-intensive (Ismail & Materwala, 2019). The choice of consensus protocol depends on the type of Blockchain system used.

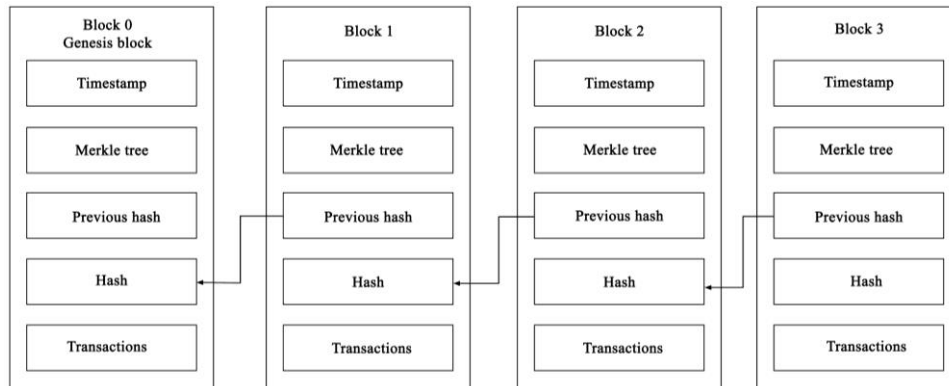


Fig. 1 Basic layout of connected blocks in a Blockchain

Source: Zhu, Zheng & Liv (2018)

The basic classification of Blockchain systems is into public and private. With public Blockchains, there is no strict division of roles, so one participant can only be a node or a miner if able to meet the criteria that are most often technical (Lin & Liao, 2017). With private Blockchains, there is a clear division of roles. A small number of pre-identified participants, who often form a consortium related to a business process regulated by a Blockchain, may play the role of a miner (Wang et al., 2019). Depending on the design of the system, the role of nodes can either be publicly available, or obtained under certain criteria. Private Blockchain systems are intended for business applications with a finite number of participants, which are often known in advance. To create a payment infrastructure, it is necessary that the role of nodes be publicly available to all interested participants, while the role of miners can be reserved for known participants.

Blockchain is already used in the construction of the payment infrastructure of a large number of cryptocurrencies. It has long been believed that cryptocurrencies will become not only decentralized electronic money, free of political influence, but also a means of micropayments, inherent in the Internet of Things. However, the reality is that cryptocurrencies are currently applicable as instruments of speculative investment. One of the reasons is the frequent and sudden change in the price of leading cryptocurrencies. Another reason is the performance of the consensus protocol.

All protocols intended for public Blockchain systems have problems with scalability, although there are marked differences in this group (Tomić, Todorović & Jakšić, 2021). Furthermore, miners in all protocols of this group must bear relatively high financial investments (with significant differences in terms of the amount of investment). As a result, all protocols imply the existence of some form of financial reward for assembling the block, which makes the system expensive and unsuitable for micropayments. The problem of protocols intended for private Blockchain systems is insufficient application in the field of cryptocurrencies. Theoretically, this group of protocols shows higher scalability and lower cost of the system itself (Tomić, 2021). Examples on which that can

be determined are not representative, due to the very low use of cryptocurrencies based on them. In practice, the most widely used protocol is known as proof-of-work (PoW). It is at the same time the most unfavorable protocol in terms of performance, due to high initial investments, high energy load of the system and poor scalability.

2.2. Tangle

The first noticeable difference between Tangle and Blockchain is that transactions are not packed in blocks, but are entered independently in the public ledger. Although both Blockchain and Tangle rely on the mathematical concept of directed acyclic graph (DAG), Blockchain has only one path (from the previous to the next block), while Tangle represents a more complex network, in which transactions are not linearly related to each other, but involve branching. When entering each new transaction, the two previously entered ones must be validated so the initiator guarantees that they do not lead to double spending (Makhdoom et al. 2019, p. 259). In this way, Tangle technology brings the validation of transactions closer. All participants in the network are equal, without division of roles into initiators and miners (Safraz et al. 2019, p. 361). The appearance of a hypothetical Tangle network can be seen in Figure 2.

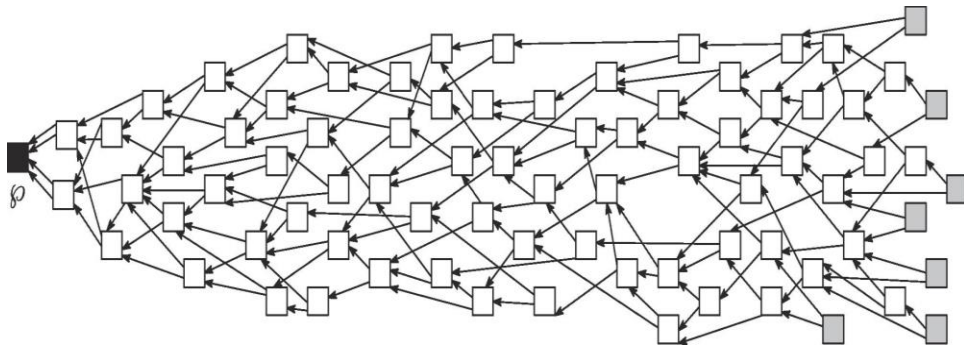


Fig. 2 Hypothetical appearance of a Tangle transaction network

Source: Popov, Saa & Finardi (2019, p. 162)

At the left end of the picture is the initial transaction, while the light squares mark all subsequent transactions that have been validated (in terminology they are marked as vertices). The directional arrows indicate which two transactions each new transaction selected as a reference when entering. Gray squares indicate new transactions that have been entered but have not yet been validated (in terminology, they are referred to as tips). The best outcome for the whole system would be that each initiator when entering a new transaction chooses tips for reference. However, in practice, the initiator does not know whether the transaction they take for reference has already been validated by other initiators. Therefore, Figure 2 shows that certain transactions are references for only the next one, while other references are for as many as the next four. In practice, Markov Chain Monte Carlo (MCMC) simulation is used to select reference transactions. After the selection, the initiator must check that the transactions do not represent a double spending of funds. They then perform an abbreviated form of the PoW algorithm, which is simpler

than that applied to Bitcoin and other cryptocurrencies. It is necessary to find the appropriate nonce, whose hash fits with certain data in reference transactions (Popov, 2015, p. 3). Because it is simpler, PoW consumes less energy and lasts shorter than cryptocurrencies. After all this, the new transaction becomes part of the network, but remains a tip.

In order for a transaction to become a vertice, its “weight” needs to exceed the previously determined limit. The weight is proportional to the work invested in validating it. The total weight is the sum of the weight of the transaction itself and the weight of all transactions that directly or indirectly validate it (Silvano & Marcelino, 2020, p. 309). Thanks to MCMC simulation, those branches of the network that have a higher total weight are more likely to be selected to add new transactions, while the rest of the network is abandoned. In this way, the system is protected from the possibility of hiding certain transactions in a cut-off part of the network, which would enable double spending.

Tangle technology was designed as an infrastructure for IOTA cryptocurrency in 2015. As the name of the cryptocurrency itself suggests, its primary goal is to be used in the Internet of Things ecosystem. The absence of specialized miners allows the IOTA system to function without commissions, which makes it cheaper compared to competing cryptocurrency systems. The absence of commissions makes IOTA a good choice for micropayments, which will account for a significant share of total payments in the Internet of Things ecosystem (Jiang et al. 2019, p. 2). The biggest potential disadvantage of Tangle is considered to be the lack of implementation of smart contracts.

2.3. Hashgraph

Hashgraph is a variant of DAG, developed in 2016 by Swirld (Baird, 2016). The basic idea was to bring technology closer to the way people communicate and transmit information to each other. Nodes in Hashgraph often communicate, choosing a partner at random. During communication, they share information about new transactions initiated by them, but also about transactions initiated by other nodes. In that way, each node can check whether it is up to date with the latest events on the network, i.e. whether there is data on the last performed transactions. If it turns out that the node already knows everything it learns when communicating with the partner, it means that its information is equal to or better than the information of the partner. If it turns out that during the communication it received information about new transactions that it did not know, the node adjusts its database to new knowledge. The goal is for all nodes to be as well informed as possible thanks to frequent mutual communications (Sharma et al. 2020, str. 342-343).

The principle of information exchange is based on the same principle on which gossip is transmitted between people. During communication, the node tells the partner what it has done since the previous communication, but also what it has learned about other nodes during communication with them. That is why the way of determining the order and validity of transactions with a Hashgraph is called “gossip about gossip”. A hypothetical network of Hashgraphs can be seen in Figure 3. Nodes are marked with A-E, while vertices denote events, which represent the process of information exchange. For example, Bob contacts Ed, where everyone exchanges information about known transactions. Dave and Carol do it at the same time. After that, Ed contacts Carol, conveys the information he had and the information he learned from Bob in the previous event. Carol contacts Bob at about the same time, passing on the information she had and the information she learned from Dave in the previous event. If there are no new transactions in the meantime, all four nodes – Bob, Carol, Dave and Ed –

have exactly the same information. In the next step, Bob contacts Alice, so she also gets all the information that Bob previously possessed.

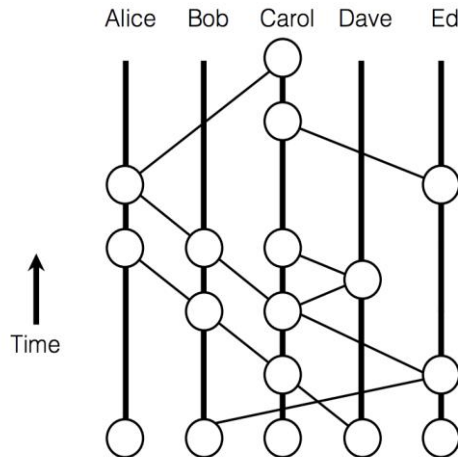


Fig. 3 Hypothetical appearance of a network of events in a Hashgraph
Source: Baird (2016)

The event consists of four components: a timestamp, which serves to establish a chronological order, transaction lists, hash of parents of the event, and transaction lists (Hassija, Saxena & Chamola, 2020, p. 54). The time of occurrence of the event is not the timestamp indicated by the initiator of the transaction, but the medial timestamp, which is determined based on the moment of receipt at all involved nodes. This prevents the initiator from falsifying the origin of the transaction and moving it chronologically earlier. Another consequence of this feature is that of the two transactions that occurred at the same time, the one about which gossip was distributed faster will be positioned chronologically earlier. Hash values represent the records of the last event for each of the included nodes.

Achieving consensus, i.e. validation of transactions, is done by the so-called virtual voting. Since all nodes have a copy of the same record of transactions, it can be assumed that each of them would declare to vote. Therefore, it is not necessary for the nodes to really vote, because based on the same information and the same sequence of events, they will always adopt the same list of transactions (Kaur & Gandhi, 2020, p. 393). Since the votes are not really sent, there is no burden on the network by sending messages, nor waiting for all nodes to declare themselves, so the decision is made immediately. The Hashgraph provides network security in accordance with the principle of asynchronous federated Byzantine agreement (aFBA), which leads to a positive outcome in the case when less than $N/3$ nodes are malicious, where N is the total number of nodes (Graczyk, 2018). Even in the event that malicious nodes virtually vote for the list of fraudulent transactions, in the following events, a fair majority will convince them that there is another list of true transactions.

3. COMPARATIVE ANALYSIS OF DISTRIBUTED LEDGER TECHNOLOGIES

The key operational performances of the payment systems are costs, throughput and scalability. In other words, the payment system must have an acceptable price of functioning, because the costs are passed on to the users of the system in the form of commissions. An ideal payment system would allow financial flow with costs close to zero. Then, the payment system must allow the flow of a large number of transactions per unit of time, thus demonstrating its applicability in global payments. Finally, the system must be scalable, i.e. its key characteristics (including throughput and cost) must not change drastically with the increase in the number of participants (Laudon & Traver, 2008). Systems that do not show good results according to the stated criteria can lead to a slowdown in the economic activity they need to service.

Blockchain is a pioneering endeavor in the field of DLT. Its qualities come to the fore when creating closed decentralized platforms, because it enables distributed input of new data and immutability of already entered ones (Schueffel, 2017). It is the dominant technical basis for creating cryptocurrencies. Despite that, Blockchain does not show good characteristics as a payment infrastructure. The main problems of PoW as the most common algorithm for reaching consensus are low throughput and low scalability. Low throughput leads to the accumulation of outstanding transactions, so payers have to offer more commissions for new transactions, in order to be built into the block across the line. Poor scalability is observed during a sharp increase in the number of miners who are actively working on assembling blocks. As the algorithm adapts to the total computing power, this means that as the number of miners increases, it will be relatively more difficult to find an appropriate solution to the cryptographic puzzle. Since the number of assembled blocks does not change, the reward that miners receive will not change either. This means that the entire system will operate at a loss, because the same reward will be shared with a larger number of miners, who consume more energy and invest more computing power. Both negative characteristics affect the increase in the price of an individual transaction.

The final conclusion is that Blockchain systems are as expensive as the technical infrastructure for the payment system of the future. Such a conclusion may seem contradictory at first glance, with the conclusion that almost all cryptocurrencies are based on them. It should be borne in mind that the most popular cryptocurrencies function as investment instruments and not as electronic money. Their value fluctuates too often with pronounced amplitudes, making them unsuitable for measuring the value of other goods (Ammous, 2018). Consequently, cryptocurrencies actually record many times fewer transactions than they would realize if actually used for payments. Despite this, most cryptocurrencies are already facing a backlog of transactions. The exception is Ripple, the cryptocurrency that uses the FBA protocol to reach consensus, which is intended for closed Blockchain systems. This protocol enables the execution of many times more transactions per second compared to the protocols for public Blockchain systems (Tomić, 2021). The company that issued Ripple is currently aiming to build a single payment system, which would enable the interoperability of the various payment systems that exist today. When it comes to the cryptocurrency itself, theoretically its throughput is up to 10,000 transactions per second, although the experiment yielded two and a half times lower value (McCaleb, 2017). The problem is that these values are not achieved in practice over a long period of time, as well as the high volatility of values.

Tangle currently represents the technical basis of a small 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. Also, it is possible to speed up the validation of executed transactions at the very moments when the system suffers the most pressure (Divya & Biradar, 2018). Therefore, the throughput of IOTA and Nano is higher than that of the most commonly used cryptocurrencies and can be compared to the values shown by Ripple. The advantage that these currencies have is that transactions are not packed in blocks, so the waiting time for validation of the transaction is shorter. While most systems suffer from the problem of scalability with the growth of the number of participants and executed processes, the situation is reversed with Tangle – the greater danger is the absence of participants and a small number of transactions, because it raises the time required to execute an individual transaction.

The main problem is that neither IOTA nor Nano are in the group of large cryptocurrencies. This does not mean that they have not yet been tested at the level of workload 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 930 billion US dollars, IOTA about 3.7 billion, and Nano only 0.7 billion US dollars (coinmarketcap.com). Low capitalization was accompanied by lower trading volume. Two conclusions can be drawn: first, IOTA and Nano did not have the opportunity to show real limitations in throughput and scalability, and second, as less attractive in trade, they were partially spared the attacks suffered by systems of more popular cryptocurrencies. Despite this fact, IOTA suffered a serious attack at the beginning of 2020, which stopped the operation of the system for several days (Osborne, 2020).

A major drawback in the case of the widespread use of Tangle-based cryptocurrencies may be the use of the PoW protocol when validating transactions. Regardless of the fact that the cryptographic puzzle is simpler than with the Blockchain, there is certainly a strain on the computer's processor and power consumption. Therefore, it can be concluded that transaction costs still exist, only they are expressed indirectly, through energy consumption, and not directly through commission (Fernandes, 2018).

Hashgraph in theory offers the highest throughput of the observed technologies (it is estimated that there could be hundreds of thousands of transactions per second). Another advantage is that the Hashgraph alone ensures that all transactions are viewed chronologically and executed in that order. Since the system is closed, Swirld's primary goal was not to create a new cryptocurrency, but to build dedicated business applications for customers. The Hedera Hashgraph is the first open platform based on that technology, which in 2019 issued the Hbar token. The market capitalization of one Hbar coin at the beginning of July 2021 was about 1.62 billion US dollars, with a price of about 0.18 dollars per coin. The small significance that the Hbar token has in the cryptocurrency ecosystem does not provide an opportunity to validate the theoretically predicted high throughput values in practice.

CONCLUSION

The use of DLT in the development of payment systems has two trends. The first shows that a dominant number of cryptocurrencies are being developed on the technological basis of Blockchain, with PoW as a consensus protocol. The vast majority of cryptocurrencies have a negligibly small application in payments, so the problems of low throughput and scalability do not interfere with their work. It can be said that all decentralized cryptocurrencies are used only as speculative investment instruments.

In contrast, there is a trend of gradual centralization in DLT-based payment systems. The first venture in this direction came from Ripple, which proposed the development of cryptocurrency, but also an inter-institutional payment system, in which cross-border payments would be made faster and cheaper with the use of cryptocurrency as a means of currency conversion. Technology giant Facebook announced in June 2019 the creation of a new centralized stablecoin, Libra, which should be supported by a large consortium of companies from various sectors. The COVID-19 pandemic slowed down the implementation of this system, but the project is still active. Hashgraph technology fits into this trend, and can be used to create a closed system in which payment institutions communicate with each other and harmonize transaction lists. However, due to the equalization of nodes and miners, the Tangle could not be the basis for the creation of a centralized system.

The paper provides sufficient evidence to answer the formulated research question. None of the analyzed technologies has shown in practice that it has adequate performance in terms of throughput and scalability. Most operational solutions have shown that even in experimental conditions they achieve poorer results than theoretically predicted ones. In addition, almost all operational solutions are burdened with high costs, whether they are expressed directly, through commissions, or burden users indirectly, through electricity costs. Most systems have suffered a number of serious attacks in the past that have resulted in financial losses for some participants. Although security was not the criterion of analysis, the fact that in order to achieve adequate security, the payment system of the Internet of Value should be centralized cannot be ignored.

Payment operations have always functioned on the principle of centralization. In this regard, the demand for complete repression of middlemen from the new payment infrastructure is not realistic. The paper can contribute by providing key guidelines for building new systems and modifying existing ones in order to transform payment transactions. The Internet-of-Value-based payment system may require high throughput and low costs, but it can by no means be fully open and decentralized. The paper shows that the elimination of middlemen does not necessarily lead to a reduction in transaction costs, but opens up greater opportunities for abuse.

The key limitation of the paper is the lack of security analysis of these technologies. Although it is stated that the systems based on them suffered attacks from third parties, there was no analysis of the built-in protection mechanisms. It should be borne in mind that it is not possible to ensure the security of a system that does not bring costs, but it is only a question of how the costs will be distributed. If decentralized systems are insisted upon, consensus protocols will create lower or higher costs for participants. If security is entrusted to a centralized institution, or a consortium of a smaller number of participants, other users will have to pay for that security through commissions.

Subsequent research on this topic should be conducted periodically, in line with the progress of technological advances. Only Blockchain has been more than a decade old at the time of writing, while the other two technologies are still so new that they have not been adequately tested in practice. Within a few years, modifications may occur, which would bring some of the observed technologies closer to the possibility of being the technological basis of the payment infrastructure of the Internet of Value. At the same time, the number of networked devices in the Internet of Things will increase, which may change the perspective of looking at the problem of integration with the payment system.

Acknowledgement: *This research was financially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia (Contracts No. 451-03-9/2021-14/200109 and 451-03-9/2021-14)*

REFERENCES

- Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money?. *The Quarterly Review of Economics and Finance*, 70, 38-51.
- Baird, L. (2016). The Swirlds hashgraph consensus algorithm: fast, fair, byzantine fault tolerance, *Swirlds tech report TR-2016-01*, Retrieved from: <https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf> Accessed on: 14 May 2021.
- Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154, 113385. <https://doi.org/10.1016/j.eswa.2020.113385>
- Cheng, J. (2015) Towards the Internet of Value: The Internet of Things and the Future of Payment Systems, *Ripple*.
- DeNisco, A. (2017). The five industries leading the IoT revolution, *ZDNet*, February 1.
- Divya, M., & Biradar, N. (2018). IOTA – next generation block chain, *International Journal of Engineering and Computer Science*, 7(4), 23823-23826. <https://doi.org/10.18535/ijecs/v7i4.05>
- Fernandes, A. (2018). *What's wrong with IOTA*, Retrieved from: <https://aakilfernandes.github.io/whats-wrong-with-iota> Accessed on: 14 May 2021.
- Finance monthly (2018). *What is the Internet of Value and How will it Impact Finance?*, March 28, Retrieved from: <https://www.finance-monthly.com/2018/03/what-is-the-internet-of-value-and-how-will-it-impact-finance/> Accessed on: 16 April 2021.
- Floros, E. J. (2019). Web 3.0 – The Internet of Value, in: Chishti, S., Craddock, T. & Courtneidge, R. (eds.): *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*, Chichester, UK: John Wiley and Sons.
- Graczyk, M. (2018). Hashgraph: A Whitepaper Review, *Medium*, February 1, Retrieved from: <https://medium.com/opentoken/hashgraph-a-whitepaper-review-f7dfe2b24647#:~:text=Each%20node%20manages%20a%20directed,node%20that%20created%20an%20event> Accessed on: 14 April 2021.
- Gupta, Z. & Gupta, H. (2020). Foundation of IoT: an overview, in: Alam, M., Shakil, K.A. & Khan, S. (eds.) *Internet of things – concepts and applications*, Cham, Switzerland: Springer. 3-24
- Hassija, V., Saxena, V., & Chamola, V. (2020). Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory, *Computers Communications*, 149, 51-61. <https://doi.org/10.1016/j.comcom.2019.09.021>
- Iansiti, M., & Lakhani, K. R. (2017) The truth about blockchain, *Harvard Business Review*, 95(1), 118-127, Retrieved from: <https://hbr.org/2017/01/the-truth-about-blockchain> Accessed on: 14 April 2021.
- Ismail, L., & Materwala, H. (2019). A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry* 2019, 11, 1198. <https://doi:10.3390/sym11101198>
- Jiang, Y., Wang, C., Wang, Y., & Gao, L. (2019). A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. *Sensors* 2019, 19(9), 2042. <https://doi.org/10.3390/s19092042>
- Kaur, G., & Gandhi, C. (2020). Scalability in blockchain: challenges and solutions. In: Krishnan, S., Balas, V.E., Julie, E.G., Robinson, Y.H., Balaji, S. & Kumar, R. (eds.) *Handbook of research on blockchain technology*, London, UK: Academic Press. 373-406.
- Laudon, K. C., & Traver, C. G. (2008). *E-commerce: Business, Technology, Society* (4th edition). Pearson Education: London, UK.
- Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19(5), 653-659. [https://doi:10.6633/IJNS.201709.19\(5\).01](https://doi:10.6633/IJNS.201709.19(5).01)
- Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of network and computer application*, 125, 251-279. <https://doi.org/10.1016/j.jnca.2018.10.019>
- McCaleb, J., Crain, B. F., Couture, S., & Roy, M. (2017). *Soundcloud*. Retrieved from: <https://soundcloud.com/epicenterbitcoin/eb-128> Accessed on: 20 June 2021.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from: <https://bitcoin.org/bitcoin.pdf> Accessed on: 20 June 2021.
- Osborne, C. (2020). 2020's worst cryptocurrency breaches, thefts, and exit scams, *ZDNet*, December 7, Retrieved from: <https://www.zdnet.com/article/2020s-worst-cryptocurrency-breaches-thefts-and-exit-scams/> Accessed on: 20 June 2021.
- Popov, S. (2015). *The tangle*. Retrieved from:

- https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iotal_4_3.pdf Accessed on: 20 June 2021.
- Popov, S., Saa, O., & Finardi, P. (2019). Equilibria in the tangle. *Computers & Industrial engineering*, 136, 160-172. <https://doi.org/10.1016/j.cie.2019.07.025>
- Ripple (2017). *The Internet of Value: What It Means and How It Benefits Everyone*. Team Ripple, June 21, Retrieved from: <https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/> Accessed on: 26 June 2021.
- Safraz, U., Alam, M., Zeadally, S., & Khan, A. (2019). Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions. *Computers Network*, 148, 361-372. <https://doi.org/10.1016/j.comnet.2018.11.019>
- Scardovi, C. (2016). *Restructuring and innovation in banking*. London, UK: Springer.
- Schneider, F. (1990). Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial. *ACM Computing Surveys*, 22(4), 299-319. <https://doi.org/10.1145/98163.98167>
- Schueffel, P. (2017). Alternative distributed ledger technologies: Blockchain vs. Tangle vs. Hashgraph – A high-level overview and comparison. *SSRN electronic journal*. <http://dx.doi.org/10.2139/ssrn.3144241>
- Sharma, D. K., Pant, S., Sharma, M. & Brahmachari, S. (2020). Cryptocurrency mechanism for blockchains: models, characteristics, challenges and applications. In: Krishnan, S., Balas, V. E., Julie, E. G., Robinson, Y. H., Balaji, S., & Kumar, R. (eds.) *Handbook of research on blockchain technology*, London, UK: Academic Press. 323-346.
- Silvano, W. F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future generation computer systems*, 112, 307-319. <https://doi.org/10.1016/j.future.2020.05.047>
- Tiwary, A., Mahato, M., Chidar, A., Chandrol, M. K., Shrivastava, M., & Tripathi, M. (2018). Internet of Things (IoT): Research, Architectures and Applications. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4(3), 23-27.
- Tomić, N. (2020). *Organizacija savremenog platnog prometa [Organization of modern payment operations]*. Kragujevac: Ekonomski fakultet Univerziteta u Kragujevcu.
- Tomić, N. (2021). A review of consensus protocols in permissioned blockchains. *Journal of Computer Science Reserach*, 3(2), 32-39. <https://doi.org/10.30564/jcsr.v3i2.2921>
- Tomić, N., & Todorović, V. (2017). The future of payments in the internet of things. *International Scientific Conference on Information Technology and Data Related Research - Sinteza 2017*, Belgrade, 97-104. <https://doi.org/10.15308/Sintez2017-97-104>
- Tomić, N., Todorović, V., & Jakšić, M. (2021). A Survey on consensus protocols in permissionless blockchains. *Scientific conference on contemporary issues in economics, business and management – EBM 2020*, Kragujevac, 365-374.
- Walport, M. (2015). *Distributed ledger technology: beyond blockchain*. UK Government Office for Science, Retrieved from: <https://www.gov.uk/government/news/distributed-ledger-technology-beyondblock-chain> Accessed on: 26 June 2021.
- Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, 136, 10-29. <https://doi.org/10.1016/j.comcom.2019.01.006>
- Zhu, Y., Zheng, Z., & Liv, C. (2018). Anonymous Voting Scheme for Boardroom with Blockchain. *International journal of performability engineering*, 14(10), 2414-2422. <https://doi.org/10.23940/ijpe.18.10.p17.24142422>

MOGUĆNOST KORIŠĆENJA DISTRIBUTIVNIH LEDGER TEHNOLOGIJA KAO INFRASTRUKTURE PLAĆANJA

Internet stvari označava komunikacionu mrežu koja omogućava interakciju ljudi sa predmetima, mašinama i objektima iz poslovnog i životnog okruženja. Dodavanje mogućnosti izvođenja transakcija informacionoj komponenti, vodi stvaranju tzv. interneta vrednosti. Savremena organizacija platnog prometa nikako ne odgovara potrebama interneta vrednosti. Da bi se postigao brz i ekonomičan protok finansijskih sredstava, potrebno je prevazići fragmentiranost tradicionalnih platnih sistema i usvojiti organizacionu strukturu interneta. Predmet rada su karakteristike tri tehnologije za decentralizovano upravljanje bazama podataka. Cilj rada je da se utvrdi mogućnost njihove upotrebe u cilju izgradnje platne infrastrukture za realizaciju koncepta interneta vrednosti. Iako je pitanje sigurnosti nove platne infrastrukture podjednako značajno, rad će biti fokusiran samo na performanse posmatranih tehnologija za decentralizovano upravljanje bazama podataka. Analiza je pokazala da ni jedna od analiziranih

tehnologija u praksi ne poseduje adekvatne performanse u pogledu propusne moći i skalabilnosti. Većina operativnih rešenja čak i u eksperimentalnim uslovima postižu slabije rezultate od teorijski predviđenih vrednosti.

Ključne reči: internet vrednosti, blokčejn, hešgraf, tengl, distribuirano upravljanje bazama podataka, internet stvari, finansijsko-tehnološka integracija