UDC 004.75, 004.77 https://doi.org/10.20535/2786-8729.4.2024.311745

INTEGRATION OF BLOCKCHAIN TECHNOLOGY INTO THE INTERNET OF THINGS (OVERVIEW)

Roman Serebriakov
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0009-0002-1159-4708

Valentyna Tkachenko
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-1080-5932

Iryna Klymenko
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-5345-8806

The article presents an analytical overview of the issues of integrating blockchain technology into Internet of Things (IoT). The results of the analytical review make it possible to substantiate the purpose and advantages of integrating blockchain technology into the Internet of Things, as well as to summarize the main issues and substantiate a number of tasks for relevant and progressive scientific research in the field of modern information systems.

***Key words**:* blockchain, IoT, data security, consensus algorithm, smart contracts.

1. Introduction

Traditionally, blockchain is a technology that became a foundation of a large number of digital currencies, including Bitcoin [1], Ethereum [2] and others, and is a powerful tool for creating secure and reliable computer systems. Blockchain technology is a chain of blocks that are interconnected by hash functions in such a way that the formation of a new block is based on the hash of the previous ones. Thus, each node of a computer system connected to the blockchain network stores all information about transactions that have been performed previously. To verify transactions and create new blocks, the blockchain uses a consensus algorithm, a key mechanism that ensures data consistency in a distributed system. Its main goal is to ensure that all participants agree on the correctness of a particular operation or transaction, even in the case of possible failures or attacks. In this way, the main advantages of blockchain technology are achieved: decentralization, security, fault tolerance, and data immutability. Transparency can also be added to these advantages, as all transactions in the blockchain are open and accessible from the very first block created in 2009. At the same time, the network participants themselves remain anonymous thanks to cryptography and the use of wallet addresses.

As the Internet of Things [3] has largely integrated all technologies of distributed computer systems into its architecture and adapted them to its unified IoT ecosystem, the integration of blockchain technology into IoT systems is becoming an urgent challenge. This opens up new perspectives for systems based on IoT technology. The integration of blockchain technology and IoT infrastructure by implementing key blockchain mechanisms in the IoT network is intended to provide additional levels of security, reliability and protection during the interaction of numerous IoT devices, which makes it possible to create autonomous and secure computer systems in various fields that are somehow based on the IoT concept.

The IoT architecture is a multi-layered one that combines layers of many different data collection devices, network infrastructure for data exchange, distributed systems for data storage and processing, and user tools. Technologies such as edge computing or fog computing are designed to move some of the data processing and analysis functionality from the upper layers of IoT to the lower layers, as close to the source of the data as possible. Edge computing has a significant advantage not only in terms of reducing traffic and relieving communication channels, but also in terms of increasing data security due to its localization.

At the same time, the use of blockchain technology at the level of endpoint storage and data processing servers is natural, but given that modern IoT concepts consider distributed storage and data processing as an integral functionality, both on IoT devices and on the IoT edge, it should be assumed that blockchain technology should be integrated at the lower layers, closer to IoT devices, to data generation sources. This causes significant problems, which are primarily related to the limited resources of IoT devices, such as memory, computing power, energy consumption; bandwidth and speed of data transmission channels; high requirements of some consensus algorithms for the computing power of IoT devices. The attractiveness of integrating blockchain into IoT systems and the need to develop new methods and tools to improve the efficiency of such integration make this analytical review relevant, focusing on such issues as the limited scalability and speed of blockchain technology, which is critical for IoT, as well as the limited resources and energy efficiency of IoT devices, which is critical for blockchain technology.

2. Problem statement

The main goal of integrating blockchain into the IoT is to ensure security, transparency, and reliability during data exchange and storage. Users need to be sure that the data has not been altered or tampered during exchange and storage. Blockchain ensures that the data remains unchanged because, thanks to the consensus mechanism that confirms each transaction, any attempts to change the data in the chain require the approval of all other network participants. This ensures high protection against cheating and falsification, since hacking the network requires owning most of the blockchain nodes in the network.

A typical example of the use of blockchain and IoT technology is described in [4], where the authors describe the widespread use of blockchain in Europe for tracking products, including meat. The authors emphasize that this approach allows obtaining reliable information about the origin of animals, raw materials for their feeding and treatment, as well as data about their movement to ensure safe meat consumption and reduce the number of poisonings.

The food supply chain is implemented through smart contracts. Food packaging is equipped with sensors that can measure environmental conditions and access the blockchain. When the measurements exceed predefined limits, the transport company as well as producers and customers are automatically informed via smart contract functions. If the sensors do not record any deviations above or below the norm, it means that the shipment was made in optimal conditions.

Along with the benefits of integrating blockchain technology into IoT systems, there are challenges, the most obvious of which are the problems of insufficient energy efficiency and limited hardware resources of IoT devices. IoT devices usually have small memory capacity, small batteries, and weak computing resources. At the same time, blockchain requires significant computing resources and memory to implement its mechanisms. Thus, the question arises about how to use blockchain technology in the IoT system in the best way. Among the possible use cases are the following [4]:

1. Using blockchain in cloud storage for storing data. This approach allows to store data securely, but rejects the idea of using blockchain to securely exchange data between IoT devices themselves.

2. Deploying a full-fledged blockchain node on each IoT device. An extremely resource-intensive approach that greatly increases the cost of IoT devices, as it requires significant hardware resources for data storing and processing.

3. Finding a compromise. Placing a full-fledged blockchain node as close as possible to IoT devices. This approach also involves pre-processing data before sending it to the blockchain network.

This approach can be implemented with the help of light clients, proxy nodes, and fog computing technology.

Light clients and proxy nodes are used to ensure efficiency and reduce the load on IoT devices. A lightweight client [5], which can be a browser or separate software, allows you to interact with the blockchain network without downloading the full chain of blocks and saving device resources. But in this case, it needs quick access to the node that stores the full chain of blocks. Proxy nodes are used as intermediate nodes between IoT devices and the blockchain network. They can contain both a full and partial chain of blocks and can be connected to several IoT devices at once and completely offload them.

The key task to ensure the efficiency and security of a blockchain network is to choose the optimal consensus algorithm. Many of them require a lot of computing power, which leads to significant energy consumption and the need to provide significant hardware resources for devices. The emergence and development of alternative consensus algorithms helps to adapt the system to perform specific tasks without requiring a huge number of computational resources.

Based on the above, we can generally conclude that the Internet of Things is a powerful ecosystem that covers many aspects of our lives, from smart homes and cities to industrial processes and the medical field. The integration of blockchain into IoT-based systems creates new opportunities for the development of next-generation systems characterized not only by fast real-time data collection, but also by a high level of security during data exchange and storage, and high reliability and fault tolerance. This allows to achieve a high level of transparency, security and automation, which is critical for many modern applications and business processes. However, building such systems requires the development of new and improvement of existing solutions to adapt blockchain mechanisms in IoT systems, taking into account the limitations of IoT devices and infrastructure.

Thus, the purpose of the study is to provide an analytical review of technologies and methods of integrating blockchain into the infrastructure of IoT systems, to substantiate the problems that affect the effectiveness of such integration in terms of improving security during data exchange and storage and increasing the reliability and resilience of IoT-based systems. The analytical review also aims to identify promising areas for the application of blockchain and IoT, as well as the reasons that impede the widespread adoption of these technologies. The analytical review addresses the following topical issues in detail:

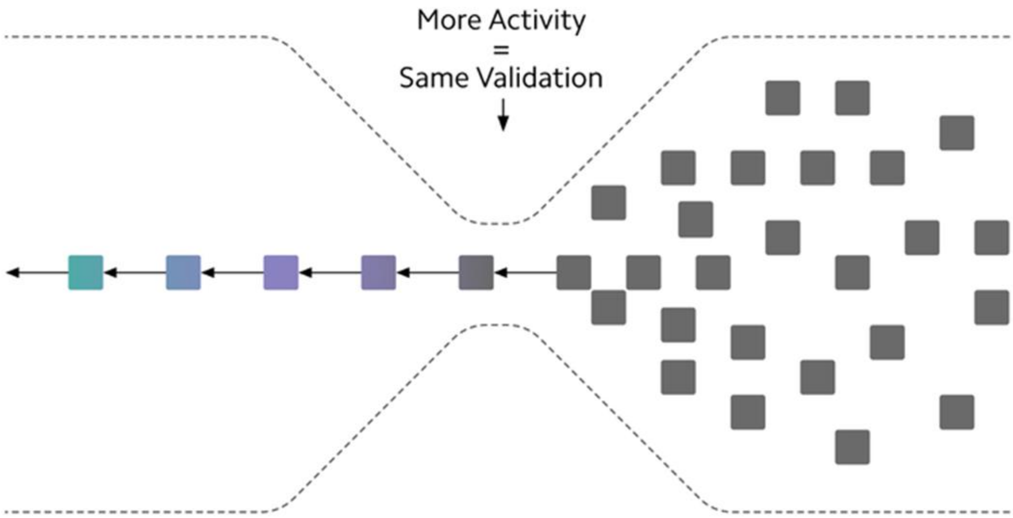
1. The problem of implementing blockchain technology in the IoT infrastructure that is caused by the specifics of these technologies.
2. The problem of using the Proof-of-Work (PoW) consensus algorithm in IoT and consideration of alternative algorithms.
3. The problem of using a full-fledged blockchain node in IoT infrastructure.
4. Overview of blockchain and IoT application areas and reasons for the lack of widespread implementation of this technology combination.

3. Literature review of the sources on identified issues

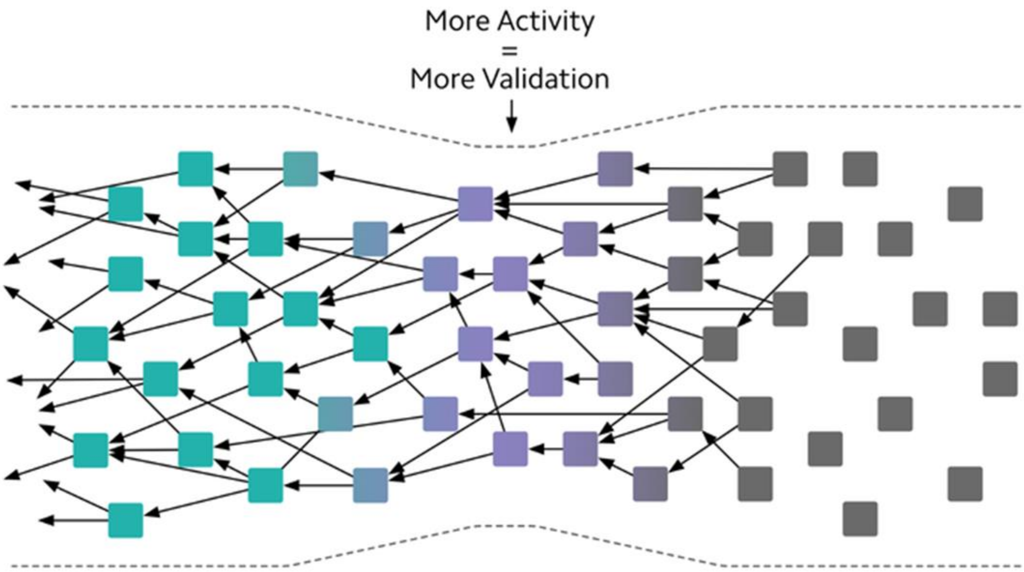
3.1. The problem of using blockchain technology in IoT infrastructure

In the introduction, it was noted that the use of blockchain in IoT carries challenges associated with low energy efficiency and limited hardware resources of IoT devices, as IoT devices usually have small computing resources, memory and battery capacity. Scalability is also an issue, as a large number of IoT devices generate a large amount of data, which is not well matched to the usually low bandwidth of the blockchain network. To solve these problems, you can use protocols that are suitable for working with IoT devices or even specially designed for them.

One of the most promising technologies that has all chances to solve the above problems is the IOTA cryptocurrency platform [6]. This platform is designed and developed specifically for the Internet of Things. The main principle that distinguishes IOTA from other platforms is the use of a technology called "Tangle" – a directed acyclic graph (DAG). Unlike the traditional blockchain, where transaction confirmation is based on the entire chain, when using Tangle, each new transaction is confirmed only by the two previous ones, forming a continuous graph (Fig. 1). Thus, the network is easily scalable, as an increase in the number of nodes leads to an increase in the number of transactions, and an increase in the number of transactions leads to faster processing and confirmation. Fig. 2 shows a comparison of the number of transactions per second that IOTA and some other popular blockchains can process. This figure shows that the Bitcoin network is currently capable of processing about 7 transactions per second (TPS), while IOTA is able to process more than 1000. Moreover, since the Pollen version 0.2.2 update on July 27, 2020, it has reached a maximum of more than 10 thousand TPS at a time.



a



b

Fig. 1 – How Tangle technology works [7]: *a* - the blockchain bottleneck;
b – the IOTA tangle scales.

Another advantage of IOTA is the absence of transaction fees due to a different approach to the concept of payment systems compared to traditional cryptocurrencies, which greatly facilitates micropayments. The IOTA network uses the Proof-of-Work (PoW) concept, in which a node that wants to add a transaction must process two other transactions in the network. In other words, this node pays for its transaction with its computing power. This approach encourages users to use the

IOTA network to build their applications and platforms where they can handle a large number of transactions without spending on processing fees.

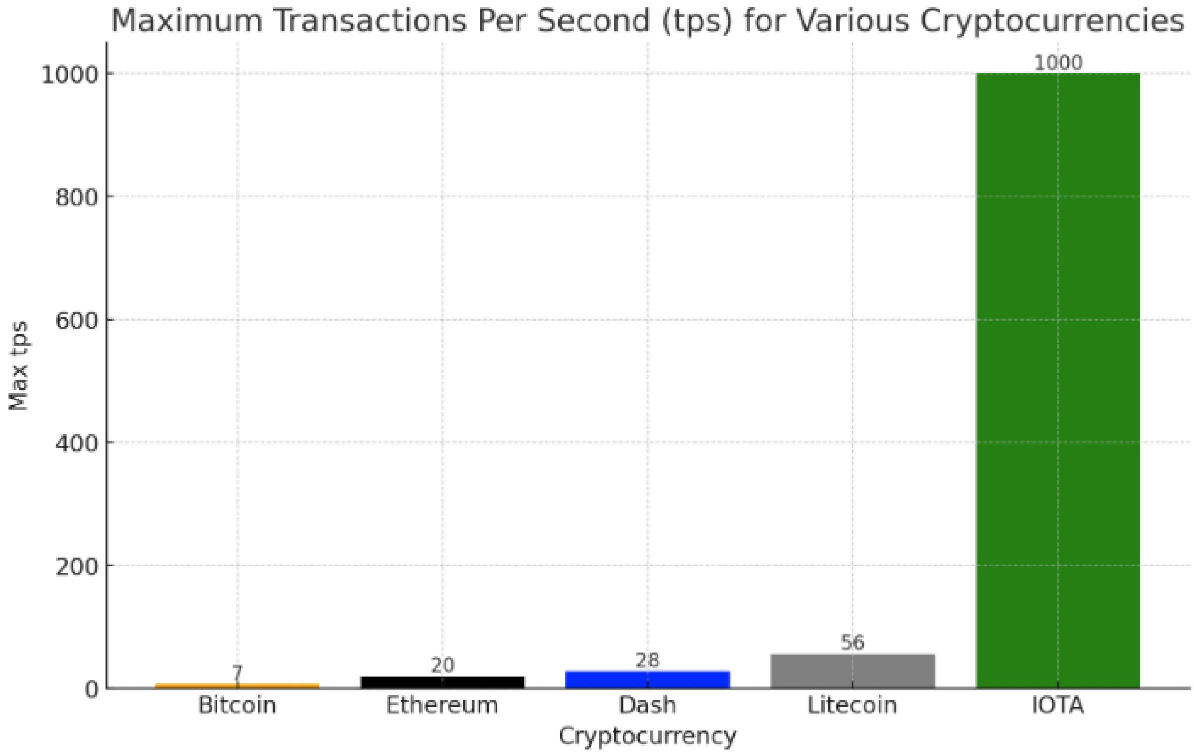


Fig. 2 – Number of transactions per second (TPS) in different blockchains

But is it advisable to use PoW for IoT? There are several nuances here. First, the computational task that a node has to perform is much smaller than in traditional blockchains, which makes it more suitable for use in the Internet of Things (IoT). And it is needed to avoid double-spending and ensure network support by paying for the execution of its transaction by processing others. Secondly, nodes in the IOTA network are usually deployed not on IoT devices themselves, but on specialized servers or hosts. That is, the principle of a light client or proxy node is used.

In 2023, smart contracts were also integrated into IOTA. This feature provided developers with new tools to create decentralized applications (DApps) on the platform. Since there are no fees for deploying and using smart contracts on IOTA, this approach makes the platform cost-effective for developers and users. In addition, thanks to Tangle's technology, smart contracts on IOTA can be processed much faster than on other platforms such as Ethereum. However, despite the recent emergence and early stage of smart contract development on IOTA, the variety of tools for creating, testing, and debugging smart contracts is relatively smaller and still suitable for creating smaller and simpler contracts.

But of course, IOTA is not a perfect platform and has its drawbacks. One of the main sources of criticism against IOTA is the coordinator, a centralized node managed by the company itself. Its main task is to confirm the legitimacy of a transaction. The emergence of such a node was necessary because in the early stages of the IOTA network development, when the number of participants and transactions was low, there was a risk of double-spending attacks. To prevent this, a sufficient number of trustworthy participants was needed to ensure the security of the network. But since mining, i.e. receiving a commission for participating in confirming the authenticity of a transaction, is not available in IOTA, it was difficult to guarantee this. Therefore, the coordinator temporarily took on this role.

Criticism has been directed against the implementation of such a mechanism. The presence of a coordinator contradicts the idea of decentralization, which is the basis of most blockchains. Its existence creates a single point of failure, making the network vulnerable to attacks or regulatory interference. It was the vulnerability of the coordinator that led to the Trinity incident [8], when IOTA was forced to shut it down to prevent theft. This case further emphasized the network's dependence on a centralized component.

The developers are aware of the existing problems and are actively working to solve them. Coordicide is currently under development, an update that will completely eliminate the coordinator and make IOTA a fully decentralized network. But while Coordicide is still in the early stages of development, other alternative platform options that can work with IoT infrastructure should be considered. So, in general, IOTA is a promising technology with a unique approach to transaction execution. It is designed specifically for the IoT and has a number of advantages over its competitors, but security issues are still discouraging users from using this technology.

Among the alternative blockchain protocols, we can also mention Litecoin [9] and Ethereum Light Client [10]. Litecoin is a cryptocurrency that was created in 2011 by Charlie Lee as one of the first alternatives to Bitcoin. Litecoin is a separate branch in the development of the Bitcoin platform and has a similar principle of operation, but with some differences. The main goal of Litecoin was to overcome some of the limitations of Bitcoin. For example, Litecoin has a higher block creation frequency, so it is able to process transactions faster, making it attractive for use in the Internet of Things (IoT). In addition, the use of the Scrypt hashing algorithm reduces computing requirements, making Litecoin mining more accessible to devices with limited computing capabilities, which are common in IoT devices. Litecoin remains a popular choice in the cryptocurrency world as an alternative to Bitcoin and is used on cryptocurrency exchanges and in payment systems. Its fast transaction processing and low fees make Litecoin attractive for micropayments, which in turn is a very important feature for the Internet of Things.

The Ethereum Light Client is a simplified version of the Ethereum client that allows you to interact with the Ethereum network without fully downloading the blockchain. It is designed for devices with limited resources, such as mobile phones or IoT devices. The Light Client receives information about the state of the network from full-fledged nodes through special protocols that allow it to check the status of contracts and transactions without having to store the entire blockchain. The Ethereum Light Client is an important tool for extending the capabilities of Ethereum in the world of IoT and mobile applications, where limited computing resources make it too difficult to deploy a full Ethereum node.

3.2. Problems in using PoW in IoT.

The consensus algorithm is a key mechanism of the blockchain network that ensures the unity of data in a distributed system. Its main goal is to ensure that all participants agree about the correctness of a particular operation or transaction, even in the event of possible failures or attacks [11]. Thus, it determines whether a new block can be added to the general chain.

Let's now take a closer look at the problems of the Proof-of-Work (PoW) consensus algorithm, in particular in the context of the Internet of Things (IoT). To solve a complex computational task to confirm the legitimacy of adding a new block to the blockchain network, PoW requires a large amount of computing power and significant energy costs [12]. For IoT devices, such costs are critical and can greatly complicate or even stop their functioning.

1. Energy efficiency: Many IoT devices run on batteries or other limited power sources, such as rechargeable batteries, so high energy consumption can seriously reduce their operating time.

2. Limited computing resources and memory: IoT devices usually have limited memory and computing capabilities. Using PoW on such devices can be overwhelming, as they may not have enough power to quickly solve complex math problems.

3. Scalability problem: IoT infrastructure can include a large number of devices that generate a large amount of data. PoW can become very impractical for processing the large number of transactions that will be generated by IoT devices.

Therefore, to use blockchain technology in IoT infrastructure, it is necessary to choose alternative consensus algorithms that do not require a large amount of energy and computing resources. Such algorithms as Proof of Stake (PoS), Delegated Proof of Stake (DPoS) [13], as well as algorithms based on fault tolerance and efficient use of resources, such as Proof of Authority (PoA) or Directed Acyclic Graph (DAG), will become more optimal for use in IoT infrastructure.

3.3. The problem of using a full blockchain node in IoT

At the moment, a full Ethereum node weighs about 450 GB, while Bitcoin weighs about 400 GB. This is a very significant amount of data for IoT devices, which usually have limited memory, processing power, and bandwidth. Launching a full node can lead to a critical overload of these resources, as a result of which the device may stop responding to any requests at all. Therefore, to implement blockchain technology in the IoT infrastructure, alternative methods are used, such as lightweight clients or proxy servers, which ensure the availability and efficiency of data exchange between IoT devices and the blockchain network.

In these scenarios, all computations and transaction validation are performed on full-fledged blockchain nodes, which are servers or powerful computers. Such nodes should be located as close as possible to IoT devices to ensure low latency and efficient communication. This approach is called edge computing, and the nodes that perform the computation are called edge nodes. This architecture allows IoT devices to interact with the blockchain network without delays when performing large computing tasks, which contributes to the efficient use of limited resources inherent in these devices. Examples of such use include Electrum for Bitcoin and Infura for Ethereum.

Cloud-based BaaS (Blockchain-as-a-Service) platforms are also becoming widely used, providing IoT developers with access to blockchain infrastructure without the need to set it up and maintain it. Study [14] states that these services are already provided by giant companies, including Microsoft and Amazon.

But are there cases where deploying a full blockchain node on an IoT device is really necessary? Yes, but there are very few cases where such a use case is truly justified. Such cases may include autonomous vehicles or medical devices that require a high level of security and reliability. Deploying full blockchain nodes on such devices will allow them to independently verify all transactions without relying on external devices, as security is vital in the operation of such devices.

Also, the use of a full node may be justified if the blockchain network is launched within a single organization, i.e. a private blockchain. And if such a network does not receive a large number of transactions, then full blockchain nodes can be deployed on IoT devices, as the network will be relatively small and will not need to store a large number of completed transactions.

But if, on the contrary, the blockchain network starts to grow rapidly, then you need to look for ways to slow down this process. The first thing to do when using blockchain technology in IoT infrastructure is to limit the amount of data that IoT devices send to the blockchain network, since not all data generated by an IoT device is important. Let's consider an example of tracking air temperature using an IoT device located at a weather station that broadcasts the temperature in real time. The IoT device itself can measure the air temperature every 10–20 seconds, or even a few minutes. But the air temperature may not change in such a short period of time, so constantly sending data to the network that the temperature is still 20°C is just a waste of resources.

So the data can be simply filtered or processed before being sent to the blockchain network. The concept of fog computing is very well suited for these actions (Fig. 3). It involves processing data as close to the source as possible, i.e. from IoT devices, before it is transferred to the blockchain network, which will reduce the load on the network itself [15].

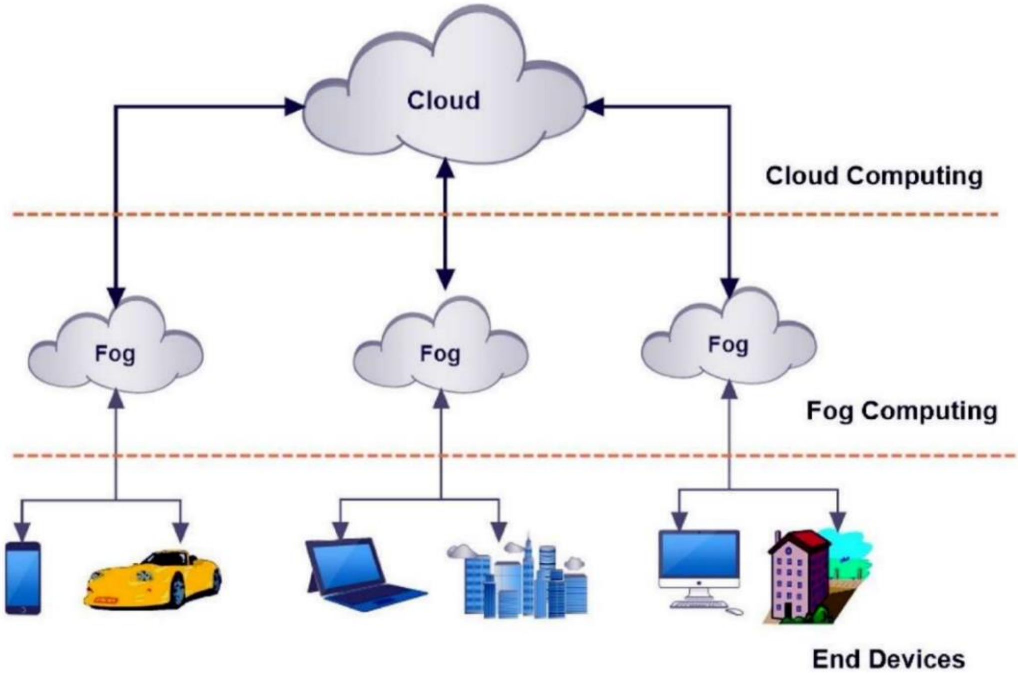


Fig. 3 – Fog computing concept workflow [16]

Fog computing can include on-site data pre-processing, filtering, aggregation, or validation, performed directly on the IoT device if the device's resources are sufficient for such manipulations, or on the edge node if the edge computing approach is used. And of course, before sending a large amount of data, you can compress it using an archiver or hashing function.

3.4. The problem of the insufficient implementation of blockchain technology.

The combination of blockchain technology and IoT can be useful in many areas of our lives: financial, legal, logistics, healthcare, etc. IoT is already used in almost all spheres of human life, but blockchain technology has not yet become widespread. This problem can be characterized as "the problem of not using the full potential of blockchain technology in various spheres of our lives." Therefore, I consider it necessary to review the sources that offer different approaches to such an application and to understand why the problem described above exists.

1. *Financial sector*

Blockchain technology was created as part of a decentralized payment system, so its use in the financial sector is a top priority to ensure resilience in banking systems and financial institutions. The implementation of secure microtransactions can open up new business opportunities by allowing customers to pay for goods and services quickly and conveniently using cryptocurrency and IoT devices. Also, money transfers abroad have become more convenient, as this procedure is much simpler and cheaper.

For example, the payment network developed by Ripple [16], which is based on the XRP cryptocurrency, uses an innovative approach to the system of transactions and records in the blockchain aimed at ensuring compliance with the requirements of regulatory authorities governing money transfers. Unlike the Bitcoin protocol, where anyone can contribute their computing resources to verify transactions and maintain the network, the XRP network provides this opportunity only to approved participants.

But what about the blockchain technology itself, is there much interest in it in the financial sector? To answer this question, we can consider the paper [17], where the authors analyze various sources and determine by the number of publications how popular blockchain has been in the field of FinTech, a combination of technology and financial services. Thus, the authors of the article identified several iterations of blockchain development, starting from 2008 and the emergence of cryptocurrencies, continuing with the period of creating smart contracts and decentralized applications, and ending with the use of blockchain as a distributed storage in digital infrastructure.

After briefly reviewing the main characteristics of blockchain and how it works, the authors moved on to the main objective of this paper: to highlight how blockchain architecture can help the financial sector gain a competitive advantage. For this purpose, a systematic literature review was conducted, analyzing the content of the 50 most relevant articles from 26 different business, finance, and information systems journals published between 2008 and 2022. After analyzing these papers, it became clear that interest in blockchain in the financial sector grew after the emergence of smart contracts, namely after 2015.

So why, despite all the advantages, is the development of blockchain in the financial sector still at an early stage? Undoubtedly, there are a number of challenges that prevent the widespread adoption of this technology. Among these challenges are technical and organizational problems, as well as challenges related directly to the users themselves, i.e. social and regulatory. Many users, no matter how trite it may sound in the 21st century, still do not trust new technologies, and banks and financial institutions are not in a hurry to implement new technologies and radically change the system that already works.

Given the low throughput of the main blockchains, the authors concluded that blockchain is a promising technology, but its potential is still not fully understood. Perhaps in the future, when all the drawbacks of this technology are eliminated, it will indeed become the basis of the global financial system. However, the authors of the article are sure, that now is the perfect time for scientists, researchers, banks and other financial institutions to further study and research blockchain technology and its development within the financial sector.

We should also highlight the scalability problem, which is based on low bandwidth, long delays in transaction execution, and high energy consumption, which reduces efficiency. This problem is described in [18], and its solution is currently a priority. Reviewing the previous source, we have found that one of the main factors that discourages banks and financial institutions from using blockchain is its low throughput, i.e. the number of transactions it can process per unit of time. At least the main types of blockchains that banks could trust, such as Bitcoin and Ethereum, have this problem. So solving it is a priority. Based on 110 reviewed sources, the authors of the article have considered various proposed solutions, such as second-level scaling, sharding, and the use of special consensus mechanisms. As a result, this article suggests areas for future research to address the scalability problem through distributed computing and parallel data processing. Such an approach may be optimal in the context of developing efficient and high-performance blockchain systems capable of fulfilling the needs of financial institutions and banks by performing a large number of transactions per unit of time.

2. *Logistics sector*

Blockchain can be used to create a supply tracking system. It can be used to track the location and condition of goods throughout the supply chain, which will certainly ensure transparency, as well as eliminate problems with falsification, theft, and improve the efficiency of the entire system.

One of the most popular companies using this technology is IBM with its IBM Food Trust project [19], a collaborative network of producers, processors, wholesalers, distributors, manufacturers, retailers and other participants that provides transparency and accountability throughout the food supply chain. Built on the IBM Blockchain, this system connects participants through an immutable and shared record of food origin, transaction data, and order processing details. Their slogan is as follows: “Data is the world's most essential ingredient”. And indeed, every year it becomes harder to argue with this statement as data becomes the most valuable resource in our time.

One of the options for implementing a supply tracking system is to use smart contracts on the blockchain and the Internet of Things. The integration of these technologies in logistics is very useful as some goods require constant monitoring of storage conditions and location. IoT-based logistics focuses on warehousing, receiving and shipping goods, tracking their location and condition, and creating an up-to-date database of goods available in warehouses. Therefore, the application of blockchain, namely smart contracts, and IoT to the logistics sector improves the transparency and security of the entire process, increases trust between the logistics company and the insurance company, and significantly reduces the risk of fraud.

In order to integrate these technologies in the field of logistics, an abstract model based on blockchain and IoT should be created. In the overview part, the paper [20] presents the leading cryptocurrencies offering tokens for logistics, describes the traditional model of a cloud environment for logistics and transportation, and then introduces its own abstract model based on blockchain and IoT. This abstract model proposes a seven-layer blockchain structure: physical layer, data layer, network layer, consensus layer, stimulation layer, contract layer, and application layer. The top five layers represent the transactions conducted through blockchain technology, and the bottom two layers form the IoT blockchain layer, which provides communication channels between IoT sensors, the physical wireless network, and the blockchain network.

In addition to creating an abstract model, the successful implementation of blockchain technology in the logistics sector may depend on some factors, such as obtaining a real-time data stream or the ability to track goods. In [21], a special methodology is considered to identify and analyze thirteen key factors that affect the success of blockchain implementation in logistics. After that, this study classifies these factors to better understand which factors are more important. The authors of the article underline that by identifying the key factors that are necessary for your system, you can successfully implement blockchain and IoT technologies in the logistics sector.

Overall, the combination of blockchain and IoT is proving to be very useful in logistics, especially for end users and insurance companies. The latter should have the greatest interest in the development and implementation of these technologies.

3. *Healthcare sector*

In the healthcare sector, blockchain can be used to securely and reliably store patient medical records. This approach can guarantee the integrity and confidentiality of patient data when it is transferred between hospitals and medical institutions. In addition, tracking the delivery and intake of medications to patients will help to avoid fraud and ensure that patients receive proper medical care.

As an example, Guardtime [22] is an Estonian company that develops blockchain-based cybersecurity solutions. Their products and services are designed to protect data, ensure integrity, and prevent counterfeiting in various industries, including healthcare, supply chains, and finance. Guardtime uses its own KSI (Keyless Signature Infrastructure) technology, which allows data to be protected without the use of cryptographic keys, making the system more resistant to cyberattacks. And the data itself is stored in the blockchain for greater transparency and authenticity. Guardtime is widely used by the Estonian government to protect its e-voting systems, by NATO to protect sensitive data transfers, and by Maersk, one of the world's largest shipping companies, to track and verify container cargo.

Integration of blockchain with the Internet of Things can also be used to increase the security and efficiency of data exchange in electronic medical records and remote patient monitoring, as described by the authors of the article [23]. This work also focuses on solving security issues, including data integrity and authentication of IoT devices using blockchain features such as decentralization and data immutability.

In addition to the secure exchange of medical data, there is a wide range of applications of blockchain in healthcare, described in [24]. These include organizing patient consent for medical procedures, controlling the supply of medicines, and managing clinical research. The paper also discusses the challenges associated with blockchain's disadvantages, such as high energy consumption and scalability issues, and describes possible solutions to these problems. Many researchers from around the world are currently trying to explore how blockchain technology can be used to improve the healthcare sector, focusing on its benefits, challenges, and potential solutions for this industry.

4. *Legal and governmental sectors*

Blockchain has the potential to revolutionize many aspects of the legal and governmental spheres, offering increased security, transparency, and efficiency. Its use can be useful in electronic voting systems, providing transparency in elections. This way, every vote can be recorded in the blockchain, where it can be verified at any time, which will help to reduce the possibility of manipulation and fraud in elections.

In the legal sphere, we cannot ignore the importance of using blockchain to store data in the judicial system, including evidence and court case files, to prevent their further “disappearance” or falsification. The use of blockchain as an immutable database for storing evidence is described in article [25]. The authors emphasize that the immutability of the blockchain ensures that records cannot be changed after they have been saved, but they note that the blockchain itself cannot confirm the accuracy of the data at the time of its entry. Therefore, there is still a need to create a reliable and objective evidence base, after which the blockchain will ensure the safe storage of these materials. Blockchain technology is already being used in some places in the US judicial system, but the authors note that the implementation of this technology in the judicial system at the regional level has challenges both from the technical and legislative sides, as different states have different laws.

In the government sector, blockchain is irreplaceable in creating an electronic voting system and can also be useful for managing medical institutions and energy infrastructure, according to the authors of the article [26]. The use of blockchain can be useful in various government agencies, educational institutions, and critical infrastructure. The main idea of the authors is that replacing the human factor and a lot of bureaucracy with blockchain is a good idea, but implementing this technology and building a system based on this technology that will work correctly is a serious challenge that needs to be done.

It is important to note that some countries are already taking the first steps in using blockchain technology at the state level. For example, Estonia uses eEstonia [27], which is based on blockchain technology, to provide electronic services to its citizens. This system is used for secure and transparent electronic voting, access to public services and online identification, as well as for maintaining a register of land and real estate ownership. eEstonia is a prime example of how blockchain can be used to improve the efficiency and transparency of government services.

All of the above examples demonstrate the diversity and power of blockchain technology, especially when combined with the Internet of Things, to solve specific problems in various industries. Blockchain has the potential to change many aspects of these areas, providing greater security, transparency, and efficiency. Its main task is to eradicate corruption schemes from various areas, which will lead to a better life for the entire society.

5. *Smart cities*

A special attention should be paid to the use of blockchain to realize the smart city concept. With the help of IoT devices placed throughout the city, information can be collected to optimize infrastructure and increase the level of device autonomy. Data collected from air pollution and temperature sensors, transport and energy infrastructure monitoring systems can be used for smart city management, ensuring optimal use of resources and services [28]. Blockchain technology can be used to ensure security and transparency in the exchange of data between different devices and systems in the city. Blockchain can also help ensure transparency and security in various areas of life described in the previous paragraphs, as well as create a transparent and honest voting system that will help to solve key issues within the smart city [29].

Combining blockchain and IoT technologies, it will be possible to create an effective city infrastructure in which data collected by IoT devices can be automatically recorded in the blockchain. This approach ensures trust in the transmitted information and eliminates the possibility of its falsification, which allows building highly efficient decentralized systems for managing electricity, water supply, transportation, and utilities.

In general, the concept of a smart city using blockchain and IoT opens the way to innovative and efficient city management, which contributes to improving the quality of life of its residents. There is hope that over time, we will see examples of how the use of blockchain in specific industries will merge to create smart cities as part of the digitalization of all possible areas of our life.

4. Discussion

Blockchain technology is extremely useful in many areas of human life, in particular, as an immutable and secure database for data storage. Smart contracts are demonstrating their effectiveness, especially in the financial sector, by automating and securing transactions. However, the combination of blockchain and IoT is especially relevant in the logistics sector, where the use of sensors and detectors to obtain data on goods and then store them in the blockchain helps to protect information from deletion and falsification. This approach allows better automation of the delivery process and provides end users with the highest quality goods, while insurance companies can make informed decisions based on reliable data.

In addition, the integration of blockchain and IoT has significant potential in the development of the smart city concept. The infrastructure built on the basis of these technologies can ensure efficient management of urban communications, connectivity, and service delivery systems. This approach will create a city management system based on reliable data collected from IoT devices and stored in a blockchain. This integration will help to increase the efficiency of city management and improve the overall quality of life of its residents.

Despite the great potential of blockchain, there are unresolved issues that require further research. This usually includes technical aspects such as the scalability problem and drawbacks of consensus algorithms. But the biggest problem is the lack of blockchain adoption in various spheres of our lives, despite the fact that this technology has a significant potential for development.

Based on the analytical review of the literature sources, several areas for further research can be identified:

1. Developing new or improving existing consensus algorithms for use in IoT. The literature analysis revealed that the Proof-of-Work (PoW) algorithm is not the best option for use in IoT due to its high energy consumption and computing resource requirements. At the same time, there are many other algorithms, a lot of them are under development and appear every year. And all of this is aimed to improve the efficiency of work in specific conditions, for specific cases. Therefore, among the possible studies, it makes sense to focus on creating a new or improving an existing consensus algorithm that will be focused specifically on working with IoT devices.

2. Developing or improving data processing methods at different levels of the IoT infrastructure to increase the efficiency of data storage in the blockchain. Processing data before sending it to the blockchain network is an important process that directly affects the efficiency of the system. This process helps to reduce the load on the blockchain network and prevent the need to create unnecessary transactions. One of the possible solutions to this problem may be the implementation of artificial intelligence. AI can perform the task of classifying or even clustering data, i.e. grouping it according to criteria determined by the artificial intelligence itself. In addition, AI can filter data and determine which data is important and which can be ignored and not stored in the blockchain at the pre-processing stage. This approach should significantly increase the efficiency of the system using the blockchain network and the Internet of Things.

3. Further development of blockchain technology for effective integration into the IoT paradigm. Although blockchain has the potential to be widely used in various industries, its implementation is still quite limited. Future research could focus on creating examples of such implementation. This does not have to be a large project; it can be a model or a basic project with basic functions that can become the foundation for a comprehensive system. The development of such projects will help to better understand the problems and challenges that may be encountered when implementing blockchain in real life. This also allows to implement fresh ideas and develop new functions. In addition to all above, it will certainly help to accelerate the development of these technologies in the scientific environment.

Conclusion

An analytical review of the problems of integrating blockchain technology into the Internet of Things (IoT) was made. The main advantages of blockchain technology, including decentralization, immutability, transparency and security, were considered, and the main challenges that arise when implementing this technology in IoT, including the problems of scalability, energy efficiency and limited resources of IoT devices, were described. The article also describes the disadvantages of using the PoW (Proof-of-Work) consensus algorithm in IoT, the inexpediency of deploying a full blockchain node on an IoT device, and the insufficient implementation of blockchain technology in various spheres of our life.

The article outlines areas for further research, including the development or improvement of consensus algorithms, the development of methods for processing data before sending it to the blockchain, and the further development of blockchain technology for effective integration with IoT technology. Therefore, further research will focus on both solving the technical problems of the technology itself, especially when interacting with IoT infrastructure, and creating examples of the implementation of these technologies in various spheres of our lives.

References

[1] Nakamoto S., Bitcoin: A peer-to-peer electronic cash system, 2008 [Online]. Accessed: Aug. 16, 2024. Available: https://bitcoin.org/bitcoin.pdf

[2] Buterin V., Ethereum white paper, 2014 [Online]. Accessed: Aug. 16, 2024. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2

[4] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190. https://doi.org/10.1016/j.future.2018.05.046

[5] Chatzigiannis, P., Baldimtsi, F., Chalkias, K. (2022). SoK: Blockchain Light Clients. In: Eyal, I., Garay, J. (eds) Financial Cryptography and Data Security. FC 2022. Lecture Notes in Computer Science, vol 13411. Springer, Cham. https://doi.org/10.1007/978-3-031-18283-9_31

[6] IOTA Documentation // IOTA Foundation WIKI [Online]. Accessed: Aug. 16, 2024. Available: https://wiki.iota.org/get-started/introduction/iota/introduction/.

[7] On the Tangle, White Papers, Proofs, Airplanes, and Local Modifiers // IOTA Foundation Blog [Online]. Accessed: Aug. 16, 2024. Available: https://blog.iota.org/on-the-tangle-white-papers-proofs-airplanes-and-local-modifiers-44683aff8fea/

[8] Trinity Attack Incident Part 1: Summary and next steps // IOTA Foundation Blog [Online]. Accessed: Aug. 16, 2024. Available: https://blog.iota.org/trinity-attack-incident-part-1-summary-and-next-steps-8c7ccc4d81e8/.

[9] Litecoin (LTC): What It Is, How It Works, vs. Bitcoin // Investopedia [Online]. Accessed: Aug. 16, 2024. Available: https://www.investopedia.com/articles/investing/040515/what-litecoin-and-how-does-it-work.asp

[10] Light clients // Ethereum Documentation [Online]. Accessed: Aug. 16, 2024. Available: https://ethereum.org/en/developers/docs/nodes-and-clients/light-clients/.

[11] Hussein, Z., Salama, M.A. & El-Rahman, S.A. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. Cybersecurity 6, 30 (2023). https://doi.org/10.1186/s42400-023-00163-y

[12] Gans, J. (2023). Proof of Work Versus Proof of Stake. In: The Economics of Blockchain Consensus. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-33083-4_5

[13] Dong S, Abbas K, Li M, Kamruzzaman J. 2023. Blockchain technology and application: an overview. PeerJ Computer Science 9:e1705 https://doi.org/10.7717/peerj-cs.1705

[14] Alam T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. Computers. 2023; 12(1):6. https://doi.org/10.3390/computers12010006

[15] Atlam HF, Walters RJ, Wills GB. Fog Computing and the Internet of Things: A Review. Big Data and Cognitive Computing. 2018; 2(2):10. https://doi.org/10.3390/bdcc2020010

[16] Ripple Company // Ripple [Online]. Accessed: Aug. 16, 2024. Available: https://ripple.com/company/.

[17] Weerawarna, R., Miah, S.J. & Shao, X. Emerging advances of blockchain technology in finance: a content analysis. Pers Ubiquit Comput 27, 1495–1508 (2023). https://doi.org/10.1007/s00779-023-01712-5
[18] Rao, I.S., Kiah, M.L.M., Hameed, M.M. et al. Scalability of blockchain: a comprehensive review and future research direction. Cluster Comput (2024). https://doi.org/10.1007/s10586-023-04257-7
[19] IBM Food Trust // IBM [Online]. Accessed: Aug. 16, 2024. Available: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust.
[20] Aleksieva V, Valchanov H, Haka A, Dinev D. Logistics Model Based on Smart Contracts on Blockchain and IoT. Engineering Proceedings. 2023; 41(1):8. https://doi.org/10.3390/engproc2023041008
[21] Samad, T.A., Sharma, R., Ganguly, K.K. et al. Enablers to the adoption of blockchain technology in logistics supply chains: evidence from an emerging economy. Ann Oper Res 327, 251–291 (2023). https://doi.org/10.1007/s10479-022-04546-1
[22] Guardtime Technology [Online]. Accessed: Aug. 16, 2024. Available: https://guardtime.com/technology.
[23] Allam, A.H., Gomaa, I., Zayed, H.H. et al. IoT-based eHealth using blockchain technology: a survey. Cluster Comput (2024). https://doi.org/10.1007/s10586-024-04357-y
[24] Kasyapa MSB and Vanmathi C (2024) Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. Front. Digit. Health 6:1359858. doi: 10.3389/fdgth.2024.1359858
[25] Wang X, Wu YC and Ma Z (2024) Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. Front. Blockchain 7:1306058. doi: 10.3389/fbloc.2024.1306058
[26] James Clavin, Sisi Duan, Haibin Zhang, Vandana P. Janeja, Karuna P. Joshi, Yelena Yesha, Lucy C. Erickson, and Justin D. Li. 2020. Blockchains for Government: Use Cases and Challenges. Digit. Gov.: Res. Pract. 1, 3, Article 22 (July 2020), 21 pages. https://doi.org/10.1145/3427097
[27] Heller N. Estonia, the Digital Republic / Nathan Heller // The New Yorker. – 2017. [Online]. Accessed: Aug. 16, 2024. Available: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.
[28] Ullah, A., Anwar, S.M., Li, J. et al. Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex Intell. Syst. 10, 1607–1637 (2024). https://doi.org/10.1007/s40747-023-01175-4
[29] Alam, T. Blockchain and Big Data-based Access Control for Communication Among IoT Devices in Smart Cities. Wireless Pers Commun 132, 433–456 (2023). https://doi.org/10.1007/s11277-023-10617-8

УДК 004.75, 004.77 https://doi.org/10.20535/2786-8729.4.2024.311745

ІНТЕГРАЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В ІНТЕРНЕТ РЕЧЕЙ (ОГЛЯД)

Роман Серебряков
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: https://orcid.org/0009-0002-1159-4708

Валентина Ткаченко
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: https://orcid.org/0000-0002-1080-5932

Ірина Клименко
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: http://orcid.org/0000-0001-5345-8806

Одним з сучасних напрямків розвитку інформаційно-комунікаційних технологій, які еволюціонували в парадигму Інтернет речей (IoT), є прогресивна ідея використання технології блокчейн в IoT. Цей напрямок описаний в великій кількості сучасних літературних джерел, які зазначають значні переваги використання блокчейну, в першу чергу пов'язані з децентралізацією, незмінністю, прозорістю та безпекою. Це дозволяє зробити висновок про високу актуальність впровадження технології блокчейн в інформаційно-комунікаційні системи IoT. Однак авторами багатьох досліджень описуються значні проблеми, серед яких як проблема масштабованості самого блокчейну, так і проблеми енергоефективності та обмеженості ресурсів в пристроях IoT. Через ці проблеми впровадження технології блокчейн в Інтернет речей стає певним викликом та обумовлює актуальність і доцільність дослідження заданої тематики та пошуку ефективних рішень, які пов'язані з інтеграцією двох дуже потужних технологій в сучасних інформаційно-комунікаційних системах.

В статті представлений аналітичний огляд проблематики інтеграції технології блокчейн в IoT, зокрема питання використання в IoT алгоритму консенсусу Proof-of-Work (PoW) та застосування альтернативних протоколів блокчейну, серед яких IOTA, Ethereum Light Client та Litecoin, які дозволяють підвищити ефективність виконання поставлених задач у IoT-інфраструктурі з урахуванням обмеженості ресурсів пристроїв; існуючі проблеми та способи імплементації, такі як використання легких клієнтів та проксі серверів. Також розглядається доцільність використання повного вузла блокчейну на IoT-пристроях та способи збільшення ефективності системи за допомогою попередньої обробки даних перед їх відправленням до блокчейн мережі. В статті також висвітлюється проблема недостатнього впровадження технології блокчейн у різні сфери життя людини, а також пошук причин що зумовлюють дану проблему.

Результати аналітичного огляду в цілому дозволяють обґрунтувати мету та переваги інтеграції технології блокчейн в Інтернет речей, а також узагальнити основну проблематику і обґрунтувати ряд задач для актуальних і прогресивних наукових досліджень в області сучасних інформаційно-комунікаційних систем.

Ключові слова: блокчейн, IoT, безпека даних, алгоритм консенсусу, розумні контракти.