IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 6, 2021, accepted September 4, 2021, date of publication September 13, 2021, date of current version September 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3112228

Demystifying Blockchain Technology for Resource-Constrained IoT Devices: Parameters, Challenges and Future Perspective

INNA ROMASHKOVA[1], MIKHAIL KOMAROV[2], (Senior Member, IEEE), AND ALEKSANDR OMETOV[3], (Member, IEEE)

[1]Technology Consulting, PricewaterhouseCoopers Ltd., 125047 Moscow, Russia
[2]Graduate School of Business, National Research University Higher School of Economics, 119049 Moscow, Russia
[3]Electrical Engineering Unit, Tampere University, 33720 Tampere, Finland

Corresponding author: Aleksandr Ometov (aleksandr.ometov@tuni.fi)

This work was supported by the Graduate School of Business National Research University Higher School of Economics.

ABSTRACT One of the most promising enablers for the secure distributed operation of the Internet of Things (IoT) systems could be based on a mathematical construct widely known as blockchain that aims to neglect the system's centralization and scalability properties. This paper aims to map the requirements and features of both systems, highlight the main co-existence challenges and technological candidates for smoother integration of IoT and blockchain, as well as provide the standartization outlook. Moreover, an architectural approach to an integrated solution is identified based on classic literature review methodology aiming to consider the IoT versus blockchain characteristics mapping and outlining related challenges. Critical solutions to address the integration bottlenecks include moving from Proof-of-Work (PoW) to Distributed Proof-of-Stake (DPoS) consensus, adding a Fog overlay to the architecture model, and leveraging the synergies combining the benefits of blockchain and IoT technology are highlighted.

INDEX TERMS Distributed information systems, Internet of Things, decentralized control, computer security.

I. INTRODUCTION

The emerging paradigm of the Internet of Things (IoT) and various related concepts are more and more coupling together towards a shared goal of enabling the smart objects to communicate in proximity and over the Internet to collect comprehensive data providing personalized automation services with minimal deliberate human interaction [1]. In this regard, modern platforms are still being built on a model that implies a centralized server, which provides services such as data processing, device coordination, and authorization [2]. Essentially, it has several challenges mainly related to privacy, single point of failure, and other concerns [3].

As one of the enabling solutions, the Distributed Ledger Technology (DLT) is expected to become an enabler to resolve the present issue of centralized paradigms [4]. In DLT, each device is expected to have equal access rights and a copy of the entire (or essential part) ledger being powered by the blockchain mathematical construct known for its immutability features [5]. Simultaneously and with the IoT ecosystem growth supporting billions of devices in mind, a distributed approach is becoming a more promising solution for handling a heavy number of transactions generated by those.

Today, DLT is already being recognized by the industry and research community as a disruptive technology poised to play an essential role in the management, control, and security of IoT devices [6]. It can monitor a vast number of connected nodes and provide transaction processing and coordination between those, which will assist in creating a resilient ecosystem for future devices [7]. Overall, DLT is foreseen as a promising solution due to its intrinsic properties suitable for IoT environments. The integration of these technologies is a new opportunity for the business industry. This paper provides a closer outlook at one of the underlying concepts of distributed ledger, particularly on the blockchain mathematical construct with immutability features from an IoT perspective [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

Storing the IoT data in the cloud has both advantages and disadvantages [9]. When it comes to data manipulation, it should be borne in mind that the cloud provider must be a trusted instance as it controls the data in the cloud and the services associated with it. In contrast, the blockchain is organized so that all nodes in the network maintain the same copy (or share) of the blockchain state, and trust is distributed among all nodes in the network. Therefore, if the data on one device is modified, the system will reject this procedure, and the state of the blockchain will remain unchanged.

The second difference is based on the fact that cloud servers may be influenced by various aspects, including but not limited to cyberattacks, power, cooling, and other issues being, essentially, as a single point of failure [10]. Whereas in blockchain, data are replicated across many computers or nodes, and multi-node problems do not disrupt the operation.

Indeed, the utilization of blockchain-based systems would bring potential bandwidth overuse [11]. Furthermore, as the blockchain's size grows, storage, throughput, and processing power demands increase. Consequently, it may not be possible for all nodes to process a block at some point. Overall, through the Peer-to-Peer (P2P) distributed network architecture, it is believed that blockchain can enhance data security and availability as an alternative to centralized cloud storage and computing. Nevertheless, the problem of blockchain scalability associated with the ever-increasing size is worth considering [12]. In a traditional cloud-IoT system, this situation can be resolved by adding more servers, using load balancing techniques, or increasing the bandwidth to handle the added transactions, while distributed systems require additional research.

The main goals of this work are:

- To analyze the possibility of integrating blockchain and IoT segments;
- To identify potential challenges of the integration process;
- To determine the critical parameters of blockchain and their relation to IoT for more efficient integration.

The rest of the paper is organized as follows. Section II provides general motivation and opportunities of IoT/blockchain integration. Next, both systems' main requirements are identified and summarized in Section III, followed by the integration challenges in Section IV. The most promising opportunities for developing IoT-blockchain suitable architecture are further provided in Section V. Next, Section VI outlines the most suitable solutions for the previously identified challenges, thus, forming a direction for future research. The last section summarises the discussion.

II. OPPORTUNITIES INTEGRATION IoT AND BLOCKCHAIN

In this section, we determine how the blockchain use can affect the IoT [13]. Notably, the characteristics of both should be identified and considered when integrating these technologies. The following should be taken into careful consideration:

1) Computing and service delivery can be deployed in geographically dispersed locations;
2) The IoT devices may range from small embedded sensors with limited resources to high-performance servers;
3) There is a constant increase in the amount of data and number of devices;
4) IoT systems are heterogeneous: systems can consist of several types of devices with different hardware and software that comply with different standards and protocols;
5) IoT environment is dynamic: devices can be activated, terminated, connected, or disconnected from the network at any time;
6) Some IoT devices have a high degree of mobility: devices can be indifferent administration areas throughout their entire life cycle.

Having identified the possibilities of integrating IoT technology and blockchain, it is worth noting the potential benefits of developing a decentralized IoT infrastructure based on the blockchain. We have identified the following IoT characteristics that can be improved by blockchain or problems that can be solved during integration as well as the capabilities of distributed approach for a specific characteristic or problem, respectively [1], [2], [6], [14]–[16]. The analysis results are presented in Table 1. The main identified groups are related to performance, security and privacy, flexibility, and practicality.

Summarising the above study of blockchain capabilities within the IoT, three main problems can be solved through the integration of these technologies, namely:

1) A distributed and decentralized approach can eliminate a single point of failure;
2) A smart contract can be used to collect dynamic data accurately, automatically, and promptly;
3) The function of protection against unauthorized access allows one to ensure the safe and orderly placement of data in the registry.

Meanwhile, it is worth highlighting the concepts related to security: confidentiality, integrity, and availability. Confidentiality ensures that data will not be transferred to unauthorized parties, integrity, data are protected from unauthorized (or unintentional) modification or deletion, and availability is the likelihood that a blockchain is working correctly at any given time.

Despite conflicting opinions about blockchain security, it should be noted that many experts in the field argue that blockchain is an effective solution to security problems in the IoT environment. As a result of the integration, it is possible to, e.g., track the state of billions of connected devices, transaction processing, and coordination between devices, which ultimately leads to eliminating a single point of failure and, in general, allows for a more resilient IoT ecosystem. At the same time, cryptographic algorithms guarantee the safety of data.

TABLE 1. Main IoT and Blockchain integration benefits.

	Benefit	Description & References
Performance	Fault tolerance	Network governance mechanisms for IoT require high availability. Blockchain provides fault-tolerant record storage mechanisms that enable fault detection through distributed consensus protocols. [2], [9]
	Audit capability	In an IoT environment, it is possible to track sensor data and prevent malicious data duplication. IoT devices can be uniquely identified in a distributed device, and the history of connected devices can help in troubleshooting. Record immutability improves control over data storage and sharing. [9], [15], [17]
	Implementation of transactions	IoT applications can utilize smart contracts to transport the sensor data across different infrastructures owned by multiple stakeholders. [1], [14]
Security	Deployment and maintenance efficiency	The distributed approach allows data duplication on a considerable number of devices, on the one hand, creating data redundancy, on the other hand, reducing data transmission latency and management overhead. [15]
	Resilience	Blockchain technology stores redundant replicas of records on nodes, which allows to maintain the data integrity and can ensure the resilience of IoT platforms. [2], [17]
	Trust	The problem of trust in the blockchain is solved through consensus mechanisms. Trust between the parties to the transaction is ensured due to the absence of intermediaries. [1], [2], [15]
	Reliability	There is no single point of failure in the blockchain model. As a result, devices can communicate with each other even in the event of a failure in any part of the system. [1], [14], [15]
	Confidentiality/ anonymity	Transactions on the blockchain use a digital identity created using Public Key Infrastructure (PKI) cryptography and a hashing algorithm. IoT applications with sensitive information can use this mechanism to hide the real identity of the network. Data privacy can be ensured through smart contracts that establish access rules, conditions, and times to allow a specific person or group of users to own, control, or access data. [1], [14], [16], [17]
	Record transactions for the account and audit	Blockchain allows data to be written to a decentralized ledger. It enhances confidence when moving assets across infrastructure owned by a large number of different stakeholders. [14]
	Authentication and data integrity	The blockchain ensures that the actual sender verifies data through cryptographic mechanisms. The technology also provides reliable traceability since all transactions are recorded in a distributed ledger. [1], [18]
	Secure communication	The blockchain excludes key management and distribution. Each IoT device has its unique Globally Unique Identifier (GUID) and asymmetric key pair installed and connected to the blockchain network. [6], [16]
Flexibility	M2M communication	A blockchain can form the basis on which devices can perform transactions autonomously. [1], [17]
	Adaptability	Blockchain runs on heterogeneous hardware platforms. The blockchain-based IoT framework can adapt to different environments and use cases to meet IoT users' growing needs and demands. [2]
Practicality	Decreasing hardware costs	Dedicated server maintenance costs are reduced through integration since there is no need for additional dedicated servers and the use of computing and member storage capabilities. Main expenses would be related to the genesis period of the system operation. [1], [2], [15], [19]
	Cost of intermediaries	The technology allows parties to trade assets and services directly with each other. [15], [20]

III. REQUIREMENTS DEFINITION

Further investigation of the integrated IoT/blockchain system is based on studying both systems' critical parameters. It is essential to understand that it is rather difficult to formulate specific requirements for implementing these technologies' interoperation and practical implementation experience. It is also worth noting that many factors affect the integration effectiveness, including the scope, IoT platform, blockchain type, and many more.

When examining the parameters of IoT and blockchain, it is worth considering the architectural layers. It was evident that the parameters' values and even the parameters themselves can differ significantly on different model layers. In this paper, the IoT parameters are studied in connection to the architecture's application level.

The study of the possibility of integrating IoT and blockchain allowed us to identify the main parameters of user devices operating in blockchain systems and associate them with the blockchain parameters themselves. As a result, Table 2 was formed, covering the source of information, the properties of the blockchain and its characteristics, and the IoT parameters corresponding to a particular characteristic in a quantitative and/or qualitative way.

One of the main parameters is related to the actual network – bandwidth. The IoT concept involves Machine-to-Machine (M2M) communication with the devices exchanging data and performing transactions instead of conventional humans. As the number of systems continues to grow, bandwidth requirements also increase. For example, for smart grid and M2M, the value may range from 1 to 100 kilobytes per second per node [14], [15], [21]–[24].

Realistically, the second main parameter is scalability. The high requirement is because the integration of IoT and blockchain needs to be supported by too many devices under the umbrella of massive Machine-Type Communications (mMTC). The increase in functionality and size should not degrade the performance of the original system [21], [25].

The next significant IoT parameter is resource consumption. The requirements for read-only memory and random access memory are classified according to the type of software implementation. For an ultra-light implementation, up to 4 KB of ROM and 256 bytes of RAM are required,

TABLE 2. Main IoT and Blockchain parameters relation.

	Blockchain Parameter	IoT Parameter	Significance	Quantitative Assessment	Additional Notes & References
Performance	Bandwidth	Bandwidth	High	1-100 Kbps	[14], [15], [21]–[24]
	Scalability	Scalability	High	–	[21], [25]
	Resource Consumption	Memory utilization	Very High	Implementation-specific	ROM: 4KB (ultralight/low cost); 32 KB (lightweight); RAM: 256 bytes (ultralight); 8KB (low cost); 8KB (Lite); CPU: Frequency = 48 MHz (TI Launchpad); Frequency = 1200 MHz (Raspberry Pi 3B); Frequency = 3400 MHz (Dell Optiplex); Signature time: 7716 ms (TI Launchpad); 372 ms (Raspberry Pi 3B); 3.5ms (Dell Optiplex); Hashing: 82.9 seconds (Raspberry Pi 3B); 4.1 seconds (Dell Optiplex); Latency: 4.0-12.0 ms (control); <50.0 ms (process monitoring) [14], [22], [26]–[32]
		RAM	Low	Implementation-specific	
		Processor	–	Implementation-specific	
		Time to sign a transaction	Very High	Implementation-specific	
		Time for hash calculation	Low	Implementation-specific	
	Latency	Network Latency	Low	Environment-specific	[9], [21], [23], [24], [33], [34]
Security	Privacy	Privacy	High	N/A	Requires protection against unauthorized access to the network and user data. [9], [25], [32], [35]–[37]
		Authentication	High	N/A	[38], [39]
		Identity control	High	N/A	Identity management framework must be built into systems. [40]
	Integrity	Integrity	High	–	Sent data should be delivered to the target without any changes. [9], [25], [41]
	Control	Control Speed	High	ms-level	Solutions should be provided. [42], [43]
	Predictability	Predictability	High	–	Time should be predictable. [15], [44]
	Protocol	Security Protocol Selection	Very High	N/A	Using the "Device-Of-Blockchain" protocol / using DTLS and / or TLS [6], [9], [45]
Flexibility	Compatibility	Interoperability	Very High	N/A	No need to keep a copy of the complete blockchain and do mining. IoT devices in the Blockchain network structure); Nodes of IoT devices do not need a direct connection to the blockchain network, the proxy server can act as a traffic regulator. [18], [19], [25], [40], [46]–[50]
	Ease of Use	Interface	Low	N/A	Using GUI, front-end components. [25], [28], [40], [51]–[53]

an inexpensive implementation requires up to 4 KB of ROM and 8 KB of RAM, a lightweight implementation requires up to 32 KB of ROM and 8 KB of RAM [14], [22], [26]–[31], [54], [32].

Example parameters, e.g., processor and time to execute blockchain consensus algorithms, are presented for three kinds of hardware platforms, namely TI Launchpad, Raspberry Pi 3B, and Dell Optiplex in, e.g., [14], [22], [26]–[32], [54]. The CPU for the first platform is CC2650, Cortex-M3, and 1 core. For the second – BCM2837, Cortex-A53, and 4 cores. For the third – Intel Core i7-6700, 8 cores with the approximate processor frequency is 48 MHz, 1200 MHz, and 3400 MHz, respectively. Those already allow for the excitability of blockchain primitives on the devices.

From the delay perspective, the required time to sign a transaction when choosing the TI Launchpad platform is 7716 ms, with the second – 372 ms, with the third – 3.5 ms. Simultaneously, the time to calculate a basic Proof-of-Work (PoW) for one transaction for the Raspberry Pi is 82.9 seconds, and for the Intel Core i7-6700 – 4.1 seconds [14], [22], [26]–[32], [54].

By analogy with the ''bandwidth'' parameter, a specific numerical value for ''network latency'' is provided for the example of a smart city and M2M communication, and varies within $4.0 - 12.0$ ms for mobile control and less than 50.0 ms for process monitoring. In general, many researchers point out that latency should be low, while bandwidth, on the contrary, should be high [9], [21], [23], [24], [33], [34].

Confidentiality in blockchain parameters includes not only conventional ''confidentiality,'' but also ''authentication,'' and ''identification'' (in contrast to IoT). In general, during operation, only approved clients can access the system, and one of the solutions may require multi-factor authentication to ensure 100% identity. Also, the requirement for the identification process itself is high since all potential attacks must be detected as soon as possible, the network must be maximally protected from any types of attacks [9], [25], [32], [35]–[40].

Many IoT systems require management tasks to be completed within a few milliseconds in terms of control speed, making this requirement more critical [42], [43]. The next parameter assumes time predictability. IoT devices interact with the environment in real-time, so the timing must be predictable. In a decentralized system, transaction confirmation is probabilistic, which confirms the difficulty of applying an integrated approach and the importance of in-depth analysis of potential problems [15], [44].

The communication and routing protocols used in IoT systems may not be secure enough. For the integrated solution's reliable operation, it is necessary to use Datagram Transport Layer Security (DTLS). The use of the Device-Of-Blockchain (DOB) protocol can help improve the transmitted data integrity [6], [9], [45].

The parameter ''interoperability'' implies IoT devices' requirements, depending on the approach to implementing an integrated solution. The first case assumes that IoT devices will be located in the blockchain network structure. They do not need to keep a copy of the complete blockchain and do mining in this case. This concept allows for maximum decentralization due to the lack of a single central node for managing or monitoring nodes. In the second case, IoT devices are outside the structure of the blockchain network. This approach observes the blockchain as a separate part. In this case, the central base station is located for direct interaction with the IoT devices' nodes and focuses on the processing and subsequent delivery of transaction blocks to the network. After confirming a transaction on the blockchain network, the IoT device receives a notification [18], [19], [25]. Interoperability is also a common requirement. The system must interact with a large number of different applications. Regardless of system types, interoperability ensures that data can be shared without any problem [40], [46]–[50].

The requirement for IoT endpoint device interfaces is rated as ''medium''. It is only siutable for systems with Graphical User Interfaces (GUIs) and applications that should provide an external interface [25], [28], [40], [51]–[53].

More than forty scientific works devoted to describing the interconnection of the IoT and blockchain were analyzed in this section. As a result, the blockchain's four fundamental properties have been identified: performance, usability, flexibility, and security. These metrics are considered the most important when integrating IoT and blockchain. Within the selected blocks framework, the IoT and blockchain technology parameters were determined and correlated, and their qualitative and/or quantitative assessments were also described. It is essential to understand that IoT parameters are more specific/detailed, but the parameters' names are the same because there is no need for detailing. This part of the analysis's primary purpose was to identify distributed ledgers' fundamental properties and parameters and determine the IoT's corresponding parameters.

IV. GENERAL INTEGRATION CHALLENGES

As already mentioned, IoT and blockchain integration allows solving several problems associated with particular bottlenecks in the IoT ecosystem. Even today, it can be concluded that IoT can benefit from the decentralized paradigms offered by blockchain. Nevertheless, it is worth considering the limited research and development in blockchain that leave many problems unresolved. Moreover, with such a variety of devices involved in the IoT, achieving absolute decentralization through blockchain remains challenging.

It is generally worth paying particular attention to the problematic aspects of communication during the integration phase as well as to understand the roles of network Edge devices for the IoT needs [55], e.g., participants in the blockchain network can act as full or light nodes. In the first case, we are talking about how the entire copy of the blockchain is placed. Light nodes can send transactions to the chain and post copies of block headers. It is a more straightforward entry point to the blockchain using limited computing resources.

Thus, the effectiveness of integration is influenced by many factors. Nevertheless, it is crucial to understand the main problem areas, and Table 3 presents the result of the analysis of the issues of the integrated approach.

The four most common blocks were identified during the analysis: performance, usability, safety, and flexibility. While there is a promising potential in integrating IoT and blockchain, the study has shown that there are several challenges that require more detailed consideration and resolution. It should be noted that the analysis of the revealed blockchain parameters showed that the PoW consensus mechanism is not suitable for IoT technology due to the limited computing resources of these devices. In this case, applying a DPoS approach can significantly simplify integration. The advantages of this algorithm include a democratic approach, scalability, and low energy consumption. The key disadvantages are possible centralization and possible DDoS attacks since the validators' identities are known. In general, the ability to designate nodes that will confirm transactions allows DPoS to be applied in an integrated solution.

Comparing Tables 1 and 3, it is evident that many problems have very similar behavior. The most significant device security case includes privacy, vulnerability, reliability, and other aspects. According to many authors, it is important to note that while blockchain aims to address security and privacy concerns in IoT transactions and tracking, the ledger-related corresponding aspects need to be maintained since they are not entirely secure at this time. Therefore, it is vital to correlate risks and opportunities for integration in security issues at this stage.

First, blockchain solves security issues in the IoT so that transactions are performed with addresses, not identifiers, and users can generate different addresses for different transactions. However, in this case, it should be borne in mind that each user can access every transaction on the network, and therefore there is a risk that the identity can be identified, for example, by analyzing address patterns.

Secondly, the decentralized approach allows IoT devices to communicate only through predefined protocols, increasing security. Nevertheless, because devices are in a permanent connection mode with this approach, they become potentially more vulnerable to various attacks.

Thirdly, the blockchain allows solving the problem of secure exchange between heterogeneous IoT devices, ensuring the transmitted data's reliability by guaranteeing their immutability. However, one of the vital security flaws is the so-called 51% attack, in which attackers seize more than 50% of the power, which allows them to control transaction confirmation and block generation.

Thus, the analysis made it possible to identify several problem areas of interaction between blockchain and IoT.

TABLE 3. Main IoT and Blockchain integration challenges.

	Problem	Description & References
Performance	Limited scalability	The blockchain tends to increase in size, energy, storage, which directly affects performance and throughput. The solution may replace the applied PoW algorithm with alternative options, in particular, PoS. [1], [15], [18], [27], [28], [35], [46]
	Transaction throughput	Millions of connected devices on IoT networks exchange data and perform transactions simultaneously. It requires high throughput. The blockchain has limitations on the block size and the time interval used to generate a new block. [15], [18], [46]
	Network throughput	IoT devices that run at the endpoint have severe throughput limitations. Edge devices and servers may have sufficient throughput, but blockchain throughput requirements may exceed the application's bandwidth requirements. [14], [15], [18], [28], [48]
	Transaction latency	The blockchain is not suitable for time sensitive IoT applications as it requires fully confirmed transactions. [14], [15], [18], [19]
	Single points of failure	IoT technology with heterogeneous networks, architectures, and protocols become more vulnerable to single points of failure. Effective integration requires mechanisms and standards to provide redundancy with a trade-off between cost and reliability throughout the infrastructure. [6], [54]
	Resource limitation / energy consumption	Consensus in a centralized architecture is provided by a trusted (third) party. The blockchain mechanism requires solving complex mathematical problems to validate, process transactions, and secure the network. It leads to increased energy requirements. [1], [6], [14], [15], [18], [21], [27], [28], [35], [46], [54]
	Data processing	Validation and processing time should be kept to a minimum to ensure timely storage and analysis of data. [1], [15], [27]
Security	Hardware vulnerability	The use of inexpensive and low-power devices can affect the vulnerability of the equipment. [6]
	Predictability	IoT devices operate in real-time. Devices require predictable timing, and communication latency between devices is limited. The consensus in the blockchain is achieved uncertainly, and the completion of a transaction is probabilistic. [15]
	Blockchain vulnerability	The consensus mechanism can be compromised. Private keys can be used to eavesdrop accounts. [6], [27]
	Data storage	The database in the registry must be replicated in the network. It is necessary to validate the transaction and ensure data integrity with a huge cost in a decentralized network. End nodes in an IoT system are made up of devices with limited memory. The size of the registry usually increases with the number of transactions. Since the registry is multiplying, there is a problem with storage. [1], [15], [27], [46]
	Confidentiality	In the blockchain, each participant can access every transaction on the network since all data are public. In this connection, the identity of the user can be identified by analysing address patterns. [1], [15], [21], [27], [28], [35], [48]
Flexibility	Working with periodically connected devices	IoT devices include, for example, periodically connected mobile phones. The startup cost for these types of devices to write data on the network can outweigh the benefits of bandwidth, compute, and storage costs. New blockchain protocols and frameworks are needed to reduce infrastructure costs when using blockchain to record IoT transactions. [14]
	Interaction real systems/ blockchain	Blockchains purely exist in the cyber world, while the IoT devices operate in the physical world. This raises the problem of the gap between the physical and cyber worlds. [28]
Practicality	Costs and expenses	Deployment of blockchain-based applications is currently expensive due to the fact that organizations need to invest heavily in technology and service providers, equipment, qualified resources, etc. Also, registry replication increases the cost of running IoT servers as they constantly store and check for registry updates. [1], [19], [27], [28]
	Transaction fee	Most open blockchain technologies charge transaction fees. IoT devices cannot store all data on such a blockchain, as storing data requires transaction fees. [14]
	Lack of governance	Decentralized blockchain has no central authority or decision-making organization. This technology has no legal regulations. [27]
	Lack of suppliers	The tools currently available for the blockchain ecosystem have quantitative, qualitative and functional limitations. [27]
	Awareness & understanding	Due to the limited information on the practical application of blockchain, there is widespread misunderstanding of the need for its implementation. [27]
	Socio-cultural factors	Blockchain implies a radical shift from the traditional approach to decentralization, which for many means a loss of control. [27]
	Lack of experience	There is a significant shortage of qualified personnel, knowledge, skills and abilities. This is necessary to implement the integration solution. [1], [27]

The issues of security, practicality, and performance when using these technologies together are controversial. On the one hand, it is clear that blockchain solves the most critical problems in the IoT. On the other hand, the security of the blockchain is actively discussed and has not been proven at the moment.

A standalone group of challenges is related to the lack of standards. The organizations involved in their development include ISO, IEEE, ITU-T focus group, and W3C. Currently, the organizations represented are creating the standards necessary for a reliable and secure implementation of a blockchain / integrated solution (only a small part has already been published).

The preparation of standards in the field of DLT was carried out by the ITU-T focus group, which partially allows understanding the activities happening in this domain [56]. The ISO committee is only planning to publish similar standards and documents. The reports will present the blockchain

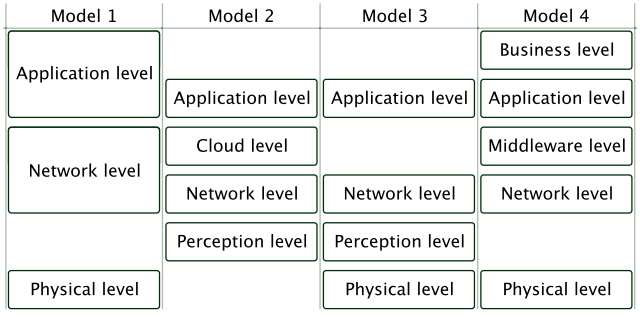

FIGURE 1. Differences in the IoT architectural layers interpretation.

and DLT reference architecture, guidelines for managing these technologies, and practical application. A series of such standards will allow fixing the basis to become possible to work with the technology faster and more efficiently [57].

The international non-profit association of IEEE has already published a number of related general requirements for cryptocurrency exchange [58], a standard for blockchain-based IoT data management framework [59], and a draft IEEE-approved standard data format for blockchain systems [60]. IEEE activities are also underway to create a standard for functional requirements and assessment in blockchain-based IoT data management [61], [62]. A series of IEEE Blockchain Initiative standards are also being developed aiming to describe various parameters and structures of distributed ledgers/blockchain technologies in multiple sectors of the economy, including their relation to IoT [63].

It is worth mentioning that there are other project groups and associations, but, as a rule, active development at the moment is mainly focused on DLT and blockchain separately from IoT. In this connection, the lack of standardization leads to limitations for the full-scale application of IoT solutions with a decentralized approach.

V. IoT OPERATION OVER BLOCKCHAIN-BASED ARCHITECTURE

The scale of an ecosystem that supports the concept of data-intensive decentralization running on billions of devices requires solving interoperability issues between systems. Otherwise, the desired synergies will not be achieved when integrating IoT and blockchain. Furthermore, it should be noted that interoperability requires trust between interacting platforms.

It is worth considering potentially related architectures to move on to the integration of blockchain technology with IoT. Due to the lack of standardization of IoT products, researchers have not found a unified reference model suitable for any IoT scenario. Layered architectures and their objectives/functions or goals are discussed in various literature and have slight variations. In this regard, Figure 1 presents a generalized literature study result to identify various IoT architecture models [9], [14], [18], [64], [65].

In general, three- to five-tier are distinguished from the pool of proposed architectures, see first three models in Figure 1. However, analysis has shown that the models have both similarities and fundamental differences. Thus, the first approach presents a three-tier model. The physical layer comprises many IoT devices, including but not limited to sensors (such as wireless for environmental monitoring), Radio Frequency Identification (RFID) tags, and mobile phones [9], [14], [66]. This layer is responsible for connecting various devices, exchanging messages, and collecting information at the top level. Based on the collected data, IoT devices can make context-sensitive and autonomous decisions using actuators.

Typically, the following characteristics of a conventional IoT deployment are noted at this level:

- A level consists of dissimilar devices, software, and hardware;
- Devices are deployed in distributed locations;
- Devices may be limited in resources;
- A large number of devices leads to the creation of a large amount of data;
- Devices can be stationary, or they can have a high degree of mobility.

The network layer focuses on transferring information that has already been collected or processed by IoT devices. Data are transmitted using various communication technologies such as 4G, 5G, WiFi, LPWaN, or Bluetooth [46], [67], [68]. Finally, the application layer comprises various IoT applications using vast amounts of data collected and processed in the previous layers. The applications may create digital services in healthcare, smart parking, smart home, smart city, and more.

Since IoT technology is evolving rapidly, a simple three-tier model cannot provide a sufficiently accurate abstraction. The next model under consideration is four-tier [64]. The apparent difference from the previous architecture is the Cloud Computing layer. Some authors note that cloud servers with more processing power, better data analysis features, and improved storage capacity can process vast amounts of data more efficiently and respond quickly to it.

The third approach is distinguished by the presence of a physical layer and a level of perception [65]. The physical layer is more about the underlying hardware and acts as a unifying platform for smart objects. The perception layer performs the ordinary task of collecting data from sensors.

The fourth architecture is a significantly more detailed extension of the first model [9], [18]. The network layer has been split into network and middleware layers. The new network layer still handles transferring data, while the middle layer handles user requests, performs immediate message delivery, integrates, and formats data. In general, a new level lies between IoT devices and IoT applications and aims to solve their interoperability problem. Moreover, the authors distinguish a business layer designed to represent a higher IoT ecosystem-level abstraction in this approach. It is responsible for managing the entire system. The level builds business

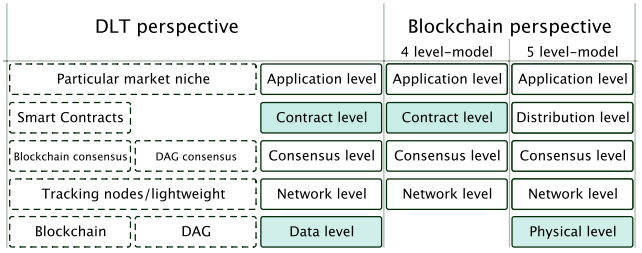

FIGURE 2. Differences in the IoT architectural layers interpretation.

models and graphs and performs data analysis, depending on future development recommendations. Since this paper considers DLT as an overlay on top of the blockchain, it is worth analyzing the similarities and differences in the layers of technology data architectures [18], [67]. The left side in Figure 2 depicts a five-layer distributed ledger model.

The data layer, or baseline, describes how data are stored in the registry. Since DLT is a broader term, at this level, there are two main types of distributed ledgers, namely blockchain and Directed Acyclic Graph (DAG). It is defined as the interconnected nodes at the network level. Here, the authors also highlight the tracking node, which requires more computing power, and lightweight nodes, which allow users to check the inclusion of transactions in a block without downloading the entire block's data. The third level determines which consensus algorithm is used, e.g., PoW, Proof-of-Stake (PoS), Proof-of-Activity (PoA), etc. One of the most widely known examples of a DAG consensus algorithm is Tangle [18], [67]. The next layer is called the smart contract layer, which corresponds to a program on the blockchain that performs specific actions when certain conditions occur, e.g., payment of a fee to a contractor when providing a service. Finally, the application layer is the topmost layer that acts as a user interface and allows third-party software developers to create distributed or decentralized platforms for various IoT use cases, e.g., smart home, smart city, smart transport, etc.

The right side of Figure 2 shows two different models utilized for blockchain technology [18], [67]. The main difference between the five-layer and four-layer models is the presence of a physical layer and replacing the contract level with a propagation layer, which consists of communication protocols that can define the rules for propagating a message or block in the network. It should be noted that the architectures proposed by the authors are based on integration with the IoT, which is considered as an applied level of the ecosystem.

The integration of the IoT and blockchain has an opportunity to overcome a centralized IoT architecture's problems and apply the benefits of blockchain technology in practice. The analysis of the sources made it possible to determine a five-level general integrated model that combines the functions of traditional IoT systems and blockchain systems. Typically, authors add blockchain as a separate layer between the network and application layers, as shown in Figure 3.

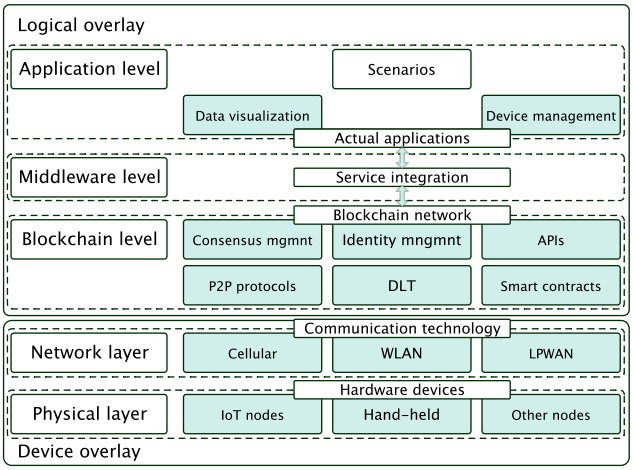

FIGURE 3. Integrated architecture.

The first level is usually either the level of perception or the physical level. The same physical layer of the IoT includes the IoT devices associated with the blockchain application [1], [18], [64], [69]. The baseline goal in both cases is to accurately perceive the environment and collect relevant data through various IoT objects.

Network and security devices perform network management and routing at the network level, allowing all IoT entities to communicate and exchange data over the global Internet. In general, this layer is similar to the network layer of the traditional blockchain layer.

The most critical layer in this architecture is the blockchain layer. The main modules required to implement the function of blockchain technology in the IoT ecosystem include:

1) P2P communication protocols: required for decentralized communication between various IoT entities;
2) The distributed ledger: required for decentralized data storage;
3) Smart contracts: required to carry out transactions without the intervention of third parties;
4) Big Data analytics module: required to provide electronic storage, processing, and analysis of data in real-time;
5) Consensus management module: required to maintain trust between interacting nodes in the network;
6) An identity management module: required to control and identify various nodes in the IoT network);
7) Application Programming Interface (API): allows IoT applications to access blockchain services.

When integrating the IoT and the blockchain, an important point is choosing a consensus mechanism for which the described consensus management module is responsible. Studies have shown that it is more efficient to build registries using PoS or DPoS. Researchers are also considering an integrated solution as both a mass service system and a system with Markov chains, described in detail ins [3], [8]. In general, this leads to the need to include the Fog level in an integrated solution. Fog computing, in this case, acts as

a liaison, aimed at distributing and approximating computations to end devices per a distributed approach [70], [71].

The technology also allows recording digital interactions to perform them safely, controlled, transparent, efficient, and interruption-resistant. When one attempts to add a transaction to the chain, all network participants check it using an algorithm, and, next, the approved transactions are combined into a block and distributed among each node in the network.

The middleware layer is different from that of the IoT. The layer focuses on managing the blockchain, integrating its services, and providing additional security services as well as support for ease of integration with the application level [72]. The top layer includes various IoT applications and provides data visualization tasks. It is similar to the IoT system and traditional blockchain architectures.

To summarize, when analyzing the IoT architectures, blockchain systems, and the integrated model, a particular pattern was identified, that is, the levels, as a rule, have a similar functional load. The authors highlight various multi-level frameworks, which are based on the possibility of combining technologies in order to improve their work. The main task of the integrated approach, as a rule, includes solving the issues of secure storage of large amounts of data generated by IoT devices. For this purpose, all modules necessary to implement blockchain technology in the IoT ecosystem were described.

Overall, IoT devices are responsible for generating data in the architectures, as mentioned earlier. Blockchain can serve as a secure distributed database responsible for secure storage and avoidance of malicious changes. Once a block is confirmed and added as part of the blockchain, the transactions contained in the block and transactions in all previous blocks are protected from unauthorized access. Different research papers highlight the need for an additional data storage layer, focusing on blockchain-based storage since IoT sensor devices do not have much space to record all generated and monitored data. As a rule, this level includes security functions: immutability, availability, integrity, minimum block creation time, scalability, and verified access. After considering the architecture of IoT, DLT, blockchain, and the integrated model, the most common approaches for the interaction of the selected technologies were identified [2] and highlighted in Figure 4.

Figure 4 (A) depicts a scenario when all the interactions between nodes are recorded/replicated via the IoT gateways act as endpoints for the network. In this case, end-nodes register with the gateway device, and the gateway forwards the data to the blockchain (in a somewhat similar manner yet simplified way as PoS). This approach allows tracking all communications associated with a specific gateway and each end-device's service. However, not all transmitted data needs to be stored in the blockchain. The blockchain itself can be used as a governance mechanism. In this case, it should be borne in mind that the degree of decentralization is not as detailed as when devices send transactions directly to the blockchain. It would provide the best battery life

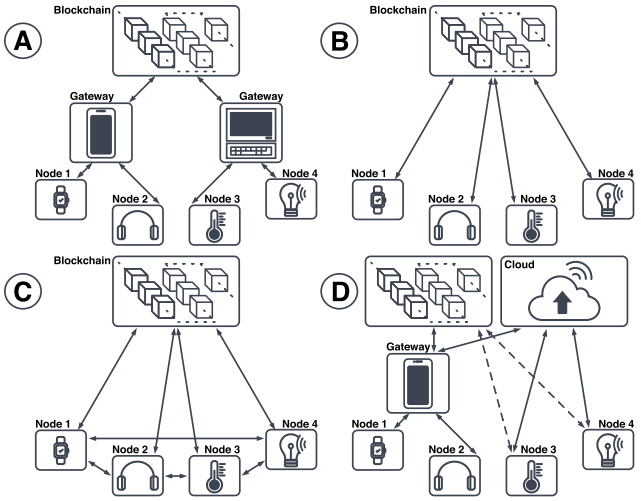

FIGURE 4. Integrated architecture.

for end-devices in trade-offs involving an intermediate and, preferably, power-independent node.

The main difference between the integration depicted in Figure 4 (B) is the lack of a gateway. It is assumed that IoT devices do not contain a copy of the blockchain but simply push the transactions [73]. With this approach, IoT devices need to be equipped with strong cryptographic functions, which will tremendously affect the device's price and computational expenses. The trade-off here is a higher degree of autonomy for IoT devices and applications versus the increased computational complexity of the hardware.

In Figure 4 (C), the IoT devices also push transactions directly to the blockchain but can still communicate with each other directly. This integration introduces the need for routing and discovery protocols, whereby this approach provides low latency between IoT devices and the ability to register specific interactions on the blockchain. This approach is more effective for scenarios with frequent interactions with appropriate requirements for high throughput, low latency, and adequate data reliability.

The last approach focuses on converging the cloud services and blockchain integration. Figure 4 (D) shows that IoT devices can interact with the blockchain both through a gateway (as in (A)) and without the gateway involvement (as in (B)), while it is possible to interact with the cloud in the same way either directly or through a gateway. This type of integration implies taking advantage of decentralized IoT accounting and communication in real-time.

To summarize the discussion on the architectures, it is worth considering the requirements of IoT devices while choosing integration schemes. With a small enough number of interactions and the need for consistent recordkeeping, the first and second approaches will be most effective. For higher performance, a hybrid approach may perform better.

VI. FUTURE PERSPECTIVE

After identifying the critical problems of integrating IoT and blockchain technology, it is essential to highlight the

future research directions and approaches to overcome those challenges. As the analysis has shown, there are still a lot of unresolved issues. It is crucial that, at the moment, it is difficult to define and describe the solution to a specific problem. However, the analysis made it possible to identify three main trends to eliminate the previously identified issues [1], [48].

The energy consumption problem in the blockchain is one of the key ones and is closely related to the applied consensus algorithm. PoW requirements are known to go far beyond the capabilities of IoT devices. Moving to PoS and then DPoS will facilitate integrating the two technologies [14].

Significantly, for the previous discussion, most conventional systems and, mainly, networks still lack appropriate support for IoT-grade scalability. Many researchers work in this direction proposing a wide variety of modern solutions for both a high number of devices and generated load support, and there are comprehensive surveys and discussion papers on this topic available [74], [75].

For example, some researchers propose to offload the computation to more powerful nodes, i.e., to utilize so-called Lightweight nodes (partial nodes) that are dependent on the full nodes to function in a somewhat similar to PoS manner [76]. Although the whole blockchain does not need to be stored, the increased number of lightweight nodes may significantly affect the workload on blockchain servers.

Another opportunity to reduce the network load is to manipulate the number of transactions [77]. Its high number may negatively impact the speed of the network based on the data load in case of a need for a big number of full/validator nodes [78]. Therefore, a long duration is required to reach a consensus, which results in the degradation of overall performance. Another case to be considered is the possibility for the capability rate of data synchronization in the system to be lower than the rate of transactions required to record in the blockchain system [79]. Overall, the duration of response towards the request increases as the number of computing devices increases [80]. These methods, known as the Layer-2 scaling, attempt to minimize the interaction with the blockchain to reduce the latency from the users' perspective but do not improve the throughput of blockchains [81].

Moreover, the IoT clouds could be used to store the data more efficiently. Fog computing aims to expand the capabilities of cloud storage as well as provide a functionality of transparent and collective interactions [82]. This combination offers the most efficient way to distribute the load on servers and devices, which will affect the efficiency of the integrated system [14], [48].

Nonetheless, one of the critical integration issues is IoT devices' limitations, which contrasts sharply with blockchain requirements in computation, storage, and network bandwidth. Solutions to this problem include using a hybrid architecture, in which computing bottlenecks are transferred to more powerful devices (for example, gateways), or the use of several local / multi-tier blockchain systems. Nevertheless, this can increase the risk of unfair transaction processing through collusion. The possibility of implementing

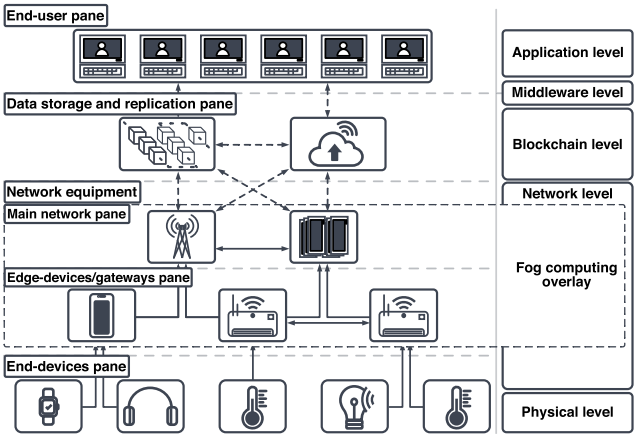

FIGURE 5. Integrated architecture.

computationally cheaper consensus mechanisms and hashing algorithms to reduce energy costs for mining is also being considered. Furthermore, the third option aims to create mini-chains in which old transactions are deleted to reduce the computational load of full nodes, while the blockchain headers are preserved to maintain the ability to verify the longest blockchain [17]. Given that the end devices of the IoT cannot fully support blockchain processes, and the server layer is an effective solution for blockchain technologies, we can talk about an approach aimed at connecting a centralized IoT deployment with a decentralized network [14].

Thus, the third trend is to combine the benefits of IoT technology and distributed ledger, in other words, to build a hybrid model. This approach will reduce the load on IoT devices by supporting a hybrid distributed architecture of centralized networks.

From the architectural perspective, one of the most promising approaches that could be applied is the integration of IoT, blockchain, and Fog computing paradigms [83]. The analysis of DLT and IoT architectures, the capabilities of these technologies, and the bottlenecks of the described approach carried out in this work made it possible to determine the key factors that should be considered when developing a model [16], [84]–[87]. The requirements identified in the literature and further systematized include:

- The model should take into account the resource constraints of the end devices;
- The model should provide for a solution to the problem of data confidentiality;
- The model should support the offloading of data and information storage;
- The model should support interactions not only between IoT devices and blockchain technologies but also direct interactions between IoT mechanisms.

Based on the above requirements, the Fog computing empowered model (see Figure 5) appears to be a promising enabler for the following set of reasons. Interactions are made using Fog nodes that may be dynamically selected depending on device constraints and situational awareness by

grouping the connected end devices into several levels based on, e.g., available computational power and/or battery. As a result, the physical layer of the architecture of the integrated approach will be divided into two levels. The zero level includes various resource-constrained devices with the data collection as the main function. Due to the fact that devices of this level have minimal processing power, the security mechanisms are generally very low on this level, thus the nodes are not expected to not interact with each other directly but through semi-trusted Fog nodes, i.e., in case the sensor needs access to the resources of another zero-level device, the request is sent through a higher-level node Fog. The validity of the request is decided by all nodes at a higher level through a distributed consensus according to the blockchain mechanism, e.g., PoS or PoA. Evidently, level 1 may include nodes responsible for processing and analyzing data received from the zero level. Due to the fact that devices of this level have more powerful resources from any perspective, they have the ability to interact with each other and, accordingly, support the verification mechanism.

Furthermore, the issue of scalability is quite common when integrating IoT and blockchain. In this regard, it becomes important to determine an effective approach for data offloading in terms of storage and processing. The proposed platform allows storing hashes of transactions in the registry, while the actual payload is stored either on a more powerful Fog node or in remote cloud storage.

The model should also take into consideration the fact that not all transmitted data needs to be stored on the blockchain, as this increases the requirements for storage and bandwidth. The blockchain in the hybrid model acts as a governance mechanism. Thus, this concept allows for the integration of decentralized recordkeeping through blockchain and real-time IoT communications. The main challenge here is the correct choice of interactions for the two possible options.

Thus, the integrated approach model builds on the previously described integrated approach architecture Figure 5 shows the three key layers of the integrated model proposed in this paper. Here, the physical layer and two proposed layers are followed by the application layer responsible for the interaction capabilities of the IoT and blockchain user devices.

For a more detailed understanding of the operation of the proposed model, it is necessary to describe a test scenario. To represent the situation, the healthcare sector was chosen, that is, the use of the IoT and blockchain for collecting, protecting, and exchanging data about extremely sensitive human health-related data. The biometric data (body temperature, pressure, pulse, etc.) are collected using wearable sensors at the lowest end-devices pane. At the higher network pane, the load is distributed and analyzed. To satisfy confidentiality, personal/confidential data are stored in a (de)-centralized (hospital-level) cloud database. Meanwhile, the hash of each entry is stored on the blockchain (both cloud and blockchain are, thus, operating on data storage and replication pane). In addition, blockchain also acts as a cloud access control interface, which ensures accountability and traceability of data access.

Ultimately, a valid user obtains access to already processed data through a mobile phone, tablet, laptop, or another device in the end-user pane. For example, a physician may request the patient data stored in a distributed registry or cloud storage, but access is only granted to a portion of the data that becomes visible to the requester on intermediate devices. The model presented in Figure 5 also supports smart contacts: the processes of providing medical services are recorded using a smart contract, the data which cannot be modified or added later on. All actions with medical data are recorded in a distributed ledger, and healthcare providers can participate in the same contract together. Thus, the described example shows how the secure exchange of medical information between stakeholders ensures the confidentiality and integrity of medical records between stakeholders. The model also allows to reduce the cost of transactions in the healthcare sector, and restricting access to medical records increases the efficiency of work through the blockchain.

In summary, it is worth noting that the model recommended in this section is one of the architectural solutions of the integrated approach. This model covers the imposed requirements and allows solving integration problems, data are processed, and security and medical system requirements associated with the consumption of a large amount of computing resources, storage of confidential data, and scalability.

VII. REVIEW SUMMARY

This article describes the potential of the integration of blockchain and the Internet of Things. Despite highlighting the main promising perspectives, this work presents an architectural approach to an integrated solution. The model consists of five layers, each of which is responsible for a specific function. Potential problems of the proposed integrated approach were identified and classified. Critical solutions to address the integration bottlenecks include moving from PoW to DPoS consensus, adding a Fog overlay to the architecture model, and leveraging the synergies from combining the benefits of blockchain and IoT technology. This paper postulates that building a hybrid model enabling cloud computing, fog computing, and distributed ledger capabilities would allow the integration of Blockchain and IoT in the most efficient way.

For researchers and integrators, it is essential to have a look at the blockchain/IoT integration aspect from a historical perspective. On the one hand, the IoT ecosystem's key component is wireless communications present on the network level and ''below'' in the integrated architecture model. The evolution of those systems undergoes a tremendous change over past years switching from conventional human-to-human communications towards machine-oriented ones. An enormous number of research and standardization activities took place during the past 20 years, completely revising the communication ecosystems.

In contrast, the blockchain is still at a very early development phase, and the first standardization activities took place only at the end of the last decade. Currently, IEEE, ISO, and ITU have provided their outlook/recommendations on how the actual integration between blockchain, networks, and applications are exported to happen. However, the number of related standards is still significantly low, i.e., at present, the integrators of blockchain systems do not have much influence on the protocol design at this point of blockchain evolution, thus, the operation would still take place over state-of-the-art networks with present protocols. However, we foresee that many technologies would face changes while adapting to the challenges highlighted in the paper, yet, it is still the standardization bodies to decide the directions.

LIST OF ACRONYMS

CPU	Central Processing Unit
IEEE	Institute of Electrical and Electronics Engineers
API	Application Programming Interface
DAG	Directed Acyclic Graph
DDoS	Denial-of-Service attack
DLT	Distributed Ledger Technology
DOB	Device-Of-Blockchain
DPoS	Distributed Proof-of-Stake
DPoS	Distributed Proof-of-Stake
DTLS	Datagram Transport Layer Security
GUID	Globally Unique Identifier
GUIs	Graphical User Interfaces
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LPWAN	Low-Power Wide-Area Network
M2M	Machine-to-Machine
mMTC	massive Machine-Type Communications
P2P	Peer-to-Peer
PoA	Proof-of-Activity
PoS	Proof-of-Stake
PoW	Proof-of-Work
PKI	Public Key Infrastructure
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read-only memory
TLS	Transport Layer Security
W3C	World Wide Web Consortium and International Telecommunication Union
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

REFERENCES

[1] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[3] S. Smetanin, A. Ometov, N. Kannengieser, B. Sturm, M. Komarov, and A. Sunyaev, "Modeling of distributed ledgers: Challenges and future perspectives," in *Proc. IEEE 22nd Conf. Bus. Informat. (CBI)*, vol. 1, Jun. 2020, pp. 162–171.

[4] A. Sunyaev, "Distributed ledger technology," in *Internet Computing*. Cham, Switzerland: Springer, 2020, pp. 265–299.

[5] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[6] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[7] S. B. Rane and Y. A. M. Narvel, "Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future industry 4.0," *Benchmarking: Int. J.*, vol. 28, no. 5, pp. 1883–1908, May 2021.

[8] S. Smetanin, A. Ometov, M. Komarov, P. Masek, and Y. Koucheryavy, "Blockchain evaluation approaches: State-of-the-art and future perspective," *Sensors*, vol. 20, no. 12, p. 3358, Jun. 2020.

[9] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.

[10] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustain. Comput. Inform. Syst.*, vol. 19, pp. 174–184, Sep. 2018.

[11] Y. Bardinova, K. Zhidanov, S. Bezzateev, M. Komarov, and A. Ometov, "Measurements of mobile blockchain execution impact on smartphone battery," *Data*, vol. 5, no. 3, p. 66, Jul. 2020.

[12] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[13] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, "Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2016, pp. 1–6.

[14] G. Sankar Ramachandran and B. Krishnamachari, "Blockchain for the IoT: Opportunities and challenges," 2018, *arXiv:1805.02818*. [Online]. Available: http://arxiv.org/abs/1805.02818

[15] Q. He, N. Guan, M. Lv, and W. Yi, "On the consensus mechanisms of blockchain/DLT for Internet of Things," in *Proc. IEEE 13th Int. Symp. Ind. Embedded Syst. (SIES)*, Jun. 2018, pp. 1–10.

[16] S. Paavolainen and P. Nikander, "Security and privacy challenges and potential solutions for DLT based IoT systems," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–6.

[17] P. Charalampidis and A. Fragkiadakis, "When distributed ledger technology meets Internet of Things–benefits and challenges," 2020, *arXiv:2008.12569*. [Online]. Available: http://arxiv.org/abs/2008.12569

[18] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, 2020.

[19] P. Danzi, A. E. Kalor, R. B. Sorensen, A. K. Hagelskjaer, L. D. Nguyen, C. Stefanovic, and P. Popovski, "Communication aspects of the integration of wireless IoT devices with distributed ledger technology," *IEEE Netw.*, vol. 34, no. 1, pp. 47–53, Jan. 2020.

[20] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the Internet of Things: A survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–34, 2019.

[21] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, "A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019.

[22] D. Letz, "Hardware requirements of blockchain clients," Diode IO, Taipei City, Taiwan, Tech. Rep., 2019.

[23] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Electr. Eng.*, vol. 72, pp. 266–273, Nov. 2018.

[24] M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikolie, "Design of a low-latency, high-reliability wireless communication system for control applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 3829–3835.

[25] M. S. Ferdous, K. Biswas, M. J. M. Chowdhury, N. Chowdhury, and V. Muthukkumarasamy, "Integrated platforms for blockchain enablement," in *Advances in Computers*, vol. 115. Amsterdam, The Netherlands: Elsevier, 2019, pp. 41–72.
[26] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems—A comparative analysis," in *Data Privacy Management and Autonomous Spontaneous Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2013, pp. 333–349.
[27] K. Mironov, S. Trishin, A. Makhmutov, V. Kartak, and T. Sauter, "On application of distributed ledgers for Internet of Things in Russia," in *Proc. VIth Int. Workshop 'Crit. Infrastructures: Contingency Manage., Intell., Agent-Based, Cloud Comput. Cyber Secur.' (IWCI)*, 2019, pp. 240–244.
[28] J. Crumb, A. Fedak, and C. A. Wiklof, "System and method of authenticating conformity to specification using a distributed ledger," US Patent App. 16 684 522, Jun. 18, 2020.
[29] L. P. I. Ledwaba, G. P. Hancke, S. J. Isaac, and H. S. Venter, "Developing a secure, smart microgrid energy market using distributed ledger technologies," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, vol. 1, Jul. 2019, pp. 1725–1728.
[30] A. Torkaman and M. Seyyedi, "Analyzing IoT reference architecture models," *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 8, p. 154, Aug. 2016.
[31] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, May 2019.
[32] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing key management in LoRaWAN with permissioned blockchain," *Sensors*, vol. 20, no. 11, p. 3068, May 2020.
[33] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in IoT systems: End-to-end delay evaluation," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8332–8344, Oct. 2019.
[34] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.
[35] H. Kakavand, N. Kost De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," *Innov. Cyberlaw Policy*, pp. 1–27, 2017.
[36] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 1180–1184.
[37] E. P. Moro and A. K. Duke, "Distributed Ledger Technologies and the Internet of Things: A devices attestation system for smart cities," *J. Brit. Blockchain Assoc.*, vol. 3, p. 12500, Apr. 2020.
[38] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.
[39] A. Durand, P. Gremaud, and J. Pasquier, "Decentralized LPWAN infrastructure using blockchain and digital signatures," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 12, p. e5352, Jun. 2020.
[40] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.
[41] A. Wijesundara, L. Joong-Sun, T. Dara, S. Hiroyuki, and O. Takashi, "Development of a firmware authenticating and updating scheme for smart home IoT devices using distributed ledger technologies," in *Proc. Comput. Secur. Symp.*, 2019, pp. 817–823.
[42] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.
[43] C.-Y. Chen, M. Hasan, and S. Mohan, "Securing real-time Internet-of-Things," *Sensors*, vol. 18, no. 12, p. 4356, Dec. 2018.
[44] A. Dorri, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.
[45] A. Kuzmin, "Blockchain-based structures for a secure and operate IoT," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–7.
[46] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7.
[47] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.
[48] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019.
[49] K. R. Özyílmaz and A. Yurdakul, "Work-in-progress: Integrating low-power IoT devices to a blockchain-based infrastructure," in *Proc. Int. Conf. Embedded Softw. (EMSOFT)*, Oct. 2017, pp. 1–2.
[50] G. Dittmann and J. Jelitto, "A blockchain proxy for lightweight IoT devices," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2019, pp. 82–85.
[51] S. Singh, "A blockchain-based decentralized application for user-driven contribution to open government data," Dept. Inform., Technische Universität München, Munich, Germany, Tech. Rep., 2018.
[52] M. Pustišek and A. Kos, "Approaches to front-end IoT application development for the Ethereum blockchain," *Procedia Comput. Sci.*, vol. 129, pp. 410–419, 2018.
[53] M. Pustišek, N. Bremond, and A. Kos, "Electric switch with Ethereum blockchain support," *IPSI TIR*, vol. 14, no. 1, pp. 21–28, 2018.
[54] A. Elsts, E. Mitskas, and G. Oikonomou, "Distributed ledger technology and the Internet of Things: A feasibility study," in *Proc. 1st Workshop Blockchain-enabled Netw. Sensor Syst.*, 2018, pp. 7–12.
[55] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
[56] International Telecommunication Union. (2021). *Focus Group on Application of Distributed Ledger Technology*. [Online]. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
[57] *Blockchain and Distributed Ledger Technologies*. Standard ISO/TC 307, 2021. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
[58] *IEEE Standard for General Requirements for Cryptocurrency Exchanges*, Standard IEEE 2140.1-2020, 2020. [Online]. Available: https://standards.ieee.org/standard/2140_1-2020.html
[59] *IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management*, Standard IEEE 2144.1-2020, 2020. [Online]. Available: https://standards.ieee.org/standard/2144_1-2020.html
[60] *IEEE Standard for Data Format for Blockchain Systems [Approved Draft]*, Standard IEEE 2418.2-2020, 2020. [Online]. Available: https://standards.ieee.org/standard/2144_1-2020.html, 2020.
[61] *Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management*, Standard IEEE P2144.2, 2019. [Online]. Available: https://standards.ieee.org/standard/2144_1-2020.html
[62] *Standard for Assessment of Blockchain-Based Internet of Things (IoT) Data Management*, Standard IEEE P2144.3, 2019. [Online]. Available: https://standards.ieee.org/standard/2144_1-2020.html
[63] IEEE Blockchain Initiative. (2021). *IEEE Recognizes the Vital Role Standards Will Play in the Development and Adoption of Blockchain Technologies*, [Online]. Available: https://blockchain.ieee.org/standards
[64] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in Internet of Things and AI," *Big Data Cognit. Comput.*, vol. 4, no. 4, p. 28, Oct. 2020.
[65] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, vol. 15, pp. 21–28, Sep. 2019.
[66] A. Ometov, Y. Bardinova, A. Afanasyeva, P. Masek, K. Zhidanov, S. Vanurin, M. Sayfullin, V. Shubina, M. Komarov, and S. Bezzateev, "An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends," *IEEE Access*, vol. 8, pp. 103994–104015, 2020.
[67] S. S. Panda, B. K. Mohanta, M. R. Dey, U. Satapathy, and D. Jena, "Distributed ledger technology for securing IoT," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–6.
[68] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards secure IoT communication with smart contracts in a blockchain infrastructure," 2020, *arXiv:2001.01837*. [Online]. Available: http://arxiv.org/abs/2001.01837
[69] W. Villegas-Ch, X. Palacios-Pacheco, and M. Román-Cañizares, "Integration of IoT and blockchain to in the processes of a university campus," *Sustainability*, vol. 12, no. 12, p. 4970, Jun. 2020.
[70] S. Pešić, M. Tošić, O. Iković, M. Radovanović, M. Ivanović, and D. Bošković, "Conceptualizing a collaboration framework between blockchain technology and the Internet of Things," in *Proc. 20th Int. Conf. Comput. Syst. Technol.*, Jun. 2019, pp. 56–61.

[71] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based IIoT app Marketplaces–A case study," in *Proc. 5th Int. Conf. Internet Things: Syst., Manage. Secur.*, Oct. 2018, pp. 182–188.
[72] X. Li, P. Russell, C. Mladin, and C. Wang, "Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 86–95, Apr. 2021.
[73] R. Pirmagomedov, A. Ometov, D. Moltchanov, X. Lu, R. Kovalchukov, E. Olshannikova, S. Andreev, Y. Koucheryavy, and M. Dohler, "Applying blockchain technology for user incentivization in mmWave-based mesh networks," *IEEE Access*, vol. 8, pp. 50983–50994, 2020.
[74] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.
[75] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, and P. Saxena, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer, 2016, pp. 106–125.
[76] A. I. Sanka and R. C. C. Cheung, "Efficient high performance FPGA based NoSQL caching system for blockchain scalability and throughput improvement," in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Dec. 2018, pp. 1–8.
[77] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—A systematic review," *IEEE Access*, vol. 8, pp. 23663–23673, 2020.
[78] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," *Appl. Health Economics Health Policy*, vol. 16, no. 5, pp. 583–590, Jul. 2018.
[79] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.
[80] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367.
[81] M. Jourenko, K. Kurazumi, M. Larangeira, and K. Tanaka, "SoK: A taxonomy for layer-2 scalability related protocols for cryptocurrencies," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 352, Apr. 2019.
[82] N. Mäkitalo, T. Aaltonen, M. Raatikainen, A. Ometov, S. Andreev, Y. Koucheryavy, and T. Mikkonen, "Action-oriented programming model: Collective executions and interactions in the fog," *J. Syst. Softw.*, vol. 157, Nov. 2019, Art. no. 110391.
[83] K. Lei, M. Du, J. Huang, and T. Jin, "Groupchain: Towards a scalable public blockchain in fog computing of IoT services computing," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 252–262, Mar. 2020.
[84] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain–based multi–layered internet–of–Things network," *Procedia Comput. Sci.*, vol. 132, pp. 469–476, Jan. 2018.
[85] B. Farahani, F. Firouzi, and M. Luecking, "The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions," *J. Netw. Comput. Appl.*, vol. 177, Mar. 2021, Art. no. 102936.
[86] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
[87] K. Sok, J. N. Colin, and K. Po, "Blockchain and Internet of Things opportunities and challenges," in *Proc. 9th Int. Symp. Inf. Commun. Technol. (SoICT)*, 2018, pp. 150–154.

INNA ROMASHKOVA received the B.Sc. degree in business informatics from the Plekhanov Russian University of Economics, and the M.Sc. degree in e-business from the Graduate School of Business, National Research University Higher School of Economics, in 2021. She is currently an Employee of PwC consulting company. Her research interests include robotic process automation, the Internet of Things, and blockchain technology.

MIKHAIL KOMAROV (Senior Member, IEEE) received the bachelor's degree in IT, in 2008, the bachelor's degree in management, in 2009, the degree in IT, in 2010, the Ph.D. degree in Russia, in 2012, and the Ph.D. degree in Finland, in 2016. Since 2012, he has been an Invited Expert and a Speaker with the UN Internet Governance Forum. He is currently a Full Professor with the Department of Business Informatics, Graduate School of Business, National Research University Higher School of Economics. He has a membership of the Steering Committee of the IEEE Conference on Business Informatics; Academy of Management; Association of Information Systems; and Technical Committee on Business Informatics and Systems IEEE. He is a Founding Member of the Special Interest Group on Big Data Applications at the Association of Information Systems. His research interests include e-business, mobile commerce, distributed ledger technology, and new business models.

ALEKSANDR OMETOV (Member, IEEE) received the Specialist degree in information security from Saint Petersburg State University of Aerospace Instrumentation (SUAI), Russia, in 2013, and the M.Sc. degree in information technology and the D.Sc.(Tech.) degree in telecommunications from Tampere University of Technology (TUT), Finland, in 2016 and 2018, respectively. He is currently a Postdoctoral Research Fellow with Tampere University (TAU), Finland. He is also working on EU H2020 MCSA A-WEAR and APROPOS projects. His research interests include wireless communications, information security, computing paradigms, blockchain technology, and wearable applications.