IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 October 2022, accepted 20 November 2022, date of publication 23 November 2022,
date of current version 30 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3224222

SURVEY

A Systematic Literature Review of Lightweight Blockchain for IoT

DENIS STEFANESCU[1,2], LETICIA MONTALVILLO[1], PATXI GALÁN-GARCÍA[3], JUANJO UNZILLA[2], AND AITOR URBIETA[1]

[1]Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA), 20500 Arrasate (Mondragón), Spain
[2]Department of Communication Engineering, University of the Basque Country (UPV/EHU), 48013 Bilbao, Spain
[3]Entrii, 46024 Valencia, Spain

Corresponding author: Denis Stefanescu (distefanescu@ikerlan.es)

This work was supported in part by the European Commission through Horizon Europe Program under the RENAISSANCE Project under Agreement 101021911, in part by the Ayudas Cervera para Centros Tecnológicos Grant of the Spanish Centre for the Development of Industrial Technology (CDTI) under the Project EGIDA under Grant CER-20191012, and in part by the Basque Country Government under the ELKARTEK Program, project REMEDY–REal tiME control and embedded security under Grant KK-2021/00091.

ABSTRACT The Internet of Things (IoT) has become an essential part of our society. IoT devices are used in our houses, hospitals, cars, industry, etc., making our lives easier. Nonetheless, there are a number of serious concerns about security, privacy and performance issues in IoT. It has been proven that the aforementioned issues are strictly related to the high degree of centralisation of current IoT architecture. Thus, there is an increasing interest in adopting blockchain in IoT. However, blockchain adoption is not straightforward due to the power, storage and computational limitations of IoT. Consequently, the concept of lightweight blockchain is getting more and more attention from researchers and engineers. In this paper, we conduct a systematic literature review on the lightweight blockchain concept for IoT following the PRISMA methodology. We systematically analyse ''lightweight blockchain for IoT'' proposals in order to better understand the limitations of blockchain for IoT, the characteristics of the current work on this topic and further research opportunities. Specifically, we analyse the definition of lightweight blockchain that other authors give, the characteristics of the reviewed proposals, their ''lightweight'' aspects and their evaluation. Finally, we discuss the results of the review along with further research opportunities. Consequently, this work is mostly focused on understanding the technical and performance-related aspects of blockchain for IoT as a prelude to more specific analysis such as security (i.e., attacks, vulnerabilities, etc.).

INDEX TERMS Systematic literature review, blockchain, Internet of Things, lightweight blockchain, lightweight distributed ledger.

I. INTRODUCTION

The Internet of Things (IoT) consists of interconnected devices that are provided with unique identifiers and can communicate in order to achieve common goals in several areas and applications [1]. There is a great variety of common IoT applications, including smart homes, smart cities, smart grids, healthcare, connected vehicles, Industry 4.0, etc. The number of active IoT devices is predicted to reach 25 billion in 2030 [2]. The main difference between IoT and the classic Internet is the lack of human interaction. IoT devices can create information, analyse it and take action autonomously. Furthermore, IoT devices are typically characterised by low power, small memory and limited processing capability.

However, IoT comes with several challenges to security, privacy and efficiency, mainly due to the excessively centralised frameworks that are currently available. The aforementioned challenges and issues include vulnerability to denial-of-service (DoS) attacks, privacy concerns, and low scalability and storage [3].

Due to the issues outlined above, there has been increasing interest in adopting blockchain, the technology behind cryptocurrencies such as Bitcoin or Ethereum, in IoT. Blockchain includes several compelling characteristics, such

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

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

as decentralisation, trust, persistency and auditability. A distributed blockchain network would remove centralised points of failure and consequently improve IoT security, privacy and scalability [4]. As shown in Fig. 1, IoT networks are migrating from a past centralised database paradigm to a more contemporary cloud-oriented paradigm, aiming towards a decentralised model-based on the Web3 [5] concept driven by blockchain.

FIGURE 1. IoT paradigm evolution.

Nevertheless, applying blockchain in resource-constrained environments is not as simple as it may seem since early blockchain consensus algorithms have limited throughput, high resource consumption, lack of efficiency and a relatively high delay in storing transactions [6]. Furthermore, designing efficient blockchain solutions for IoT is not a straightforward process since every case scenario has different requirements and needs [7]. Consequently, there is a great deal of scientific effort in creating lightweight blockchain architectures that can be compatible with the limitations of IoT devices. Thus, we identified a clear need for a comprehensive and systematic analysis of the current work on this topic in order to understand the current 2022 state-of-the-art and how blockchain architectures can be further optimised in the next years. Specifically, our main contributions can be summarised as follows:

- Analysis of the concept of **lightweight** blockchain according to the current work. This is the first systematic literature review that is exclusively focused on the performance and efficiency aspects of blockchain for IoT. We comprehensively analyse over 98 ''blockchain for IoT'' proposals.
- A review and comparison of the characteristics and lightweight aspects of each proposal. We analyse several relevant blockchain characteristics such as the chain structure, the consensus and the storage approach.
- Analysis of the evaluation method of each solution. We study the implementation technology and the evaluated metrics.
- Our own definition of the concept of ''lightweight blockchain'', based on the gathered knowledge from the analysed proposals.
- A discussion regarding the results of our analysis and future research opportunities and trends in blockchain development for resource-constrained environments.

Consequently, this work is mainly focused on understanding the technical and performance-related aspects of blockchain for IoT as a prelude to more specific analysis, such as a security analysis of the current architectures (i.e., attacks, vulnerabilities, etc.).

The remainder of the paper is organised as follows. Section II provides an overview of the concepts that are addressed in this paper. Section III discusses other reviews and surveys on blockchain and IoT and also points out the differences between our review and the existing works, along with our contributions. Section IV presents the review methodology and the data collection process. In Section V we present and discuss the study's results. In Section VI we discuss the results of the review in order to answer the research questions. We also discuss several research opportunities in this field. Finally, Section VII includes the paper's conclusions.

II. BACKGROUND

This section provides an in-depth overview of the concepts that are addressed in this paper: (i) blockchain and (ii) blockchain for IoT.

A. BLOCKCHAIN

A blockchain is a type of Distributed Ledger Technology (DLT) [8], in which all the transactions are stored in a chain of blocks that are linked via cryptography, as shown in Fig. 2. The chain continuously grows when new blocks are appended to it. Blockchain provides a distributed software architecture that allows agents (i.e., humans and systems) to interact with each other without a central authority. In the absence of a central authority, a blockchain network works collaboratively. Each node of the network executes a consensus protocol that defines a set of rules and verification mechanisms to ensure the security, reliability and veracity of the transactions and maximise resilience to failures and cyber-attacks. Specifically, blockchain allows the resolution of conflicts and eliminates information asymmetries by providing a transparent and verifiable record of all transactions, which cannot be altered.

There are two main types of blockchain [9]:

- **Permissionless.** In this type of blockchain, all devices can access the network and participate without any permission.
- **Permissioned.** In this type of blockchain, the participation must be authorised, and the actions that can be performed are controlled.

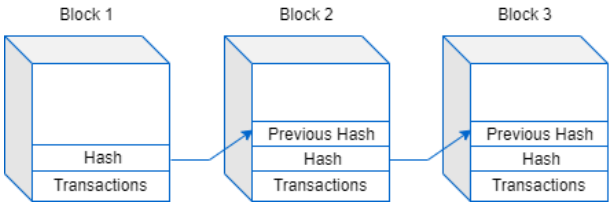

FIGURE 2. Blockchain representation.

Each user that performs transactions on a blockchain possesses a pair of public and private keys. The public key is used to provide a unique blockchain address for identification. The private key is used to sign the transactions. When adding a new transaction to the blockchain, the following procedure is followed:

1) The user signs the transaction with their private key.
2) The user broadcasts the transaction to the other nodes of the network.
3) Each peer that receives the signed transaction carries out its validation. If the validation is successful, the transaction is added to each local block that is under construction.
4) When the new block has been completed by reaching the maximum number of transactions that are allowed, or the maximum time established by the blockchain protocol for a new block proposal, the peers acting as miners (i.e., ''validators'') execute the established consensus protocol.
5) When a miner finishes executing the consensus algorithm, they add the new block at the end of their local blockchain copy.
6) The miner then broadcasts the new block to the network so that the rest of the nodes can verify it. If the validation is successful, then all the nodes of the network add the new block to their own copy of the blockchain so that it remains permanently registered. On the other hand, if the validation is not successful, then the block is discarded.

The consensus algorithm is a key element in blockchain [10]. It establishes the conditions that must be met to reach an agreement between the participating nodes on the validity of new blocks. Ideally, the consensus algorithm should give validators the same vote weight and then make decisions according to the majority of the votes. This scheme may be possible in permissioned networks. However, in public blockchains, this mechanism would lead to Sybil attacks, where a single user with multiple identities (i.e., controlling several nodes) would be able to take over and control the network. In decentralised networks, a user must be selected to add each block. This selection should be done randomly in order to avoid Sybil attacks. The solution proposed by the original PoW-based blockchain (i.e., Bitcoin) [11] avoids such attacks, as it requires miners to perform computationally expensive tasks in order to be elected as validators. Thus, a malicious node would be required to have more amount of computational power than all of the honest nodes. The ''work'' that is required in PoW-based consensus consists of performing heavy mathematical operations (i.e., mining). Specifically, this process consists of finding a random number (i.e., the nonce) that should cause the hash of the block header to have a certain number of zeros at the beginning. The required number of zeroes is established by a parameter called ''difficulty'' which establishes how many zeroes are required to be found. The more zeroes, the harder it is to find the right nonce. Despite being very computationally intensive, verifying the results of the mining process is a simple task for the rest of the nodes. However, even though this consensus approach provides great security benefits, it makes blockchain inefficient in terms of performance, scalability, and energy consumption [12]. Due to the issues mentioned above, several alternative consensus algorithms have been proposed. Furthermore, the lightweight blockchain concept started gaining popularity among researchers and enterprises. Table 1 includes a summary of the most used consensus algorithms and their limitations. We list the following algorithms: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Capacity (PoC), Proof of Authority (PoA), Proof of Elapsed Time (PoET), Proof of Activity (PoAc), RAFT and Proof of Burn (PoB).

Finally, another key blockchain feature that is worth mentioning is the ability to create smart contracts. Smart contracts were introduced to blockchain by the Ethereum platform. However, the concept of smart contract was first defined in 1996 by Szabo [13] as *''a computerised transaction protocol that executes the terms of a contract''*. Smart contracts are decentralised scripts with sufficient autonomy to be self-executed when certain conditions are met. Smart contracts are included in the blockchain and allow the execution of distributed and highly automated work.

B. BLOCKCHAIN AND IoT

The IoT can be defined as the interconnection of everyday objects that are connected to the internet. One of the core features of IoT is linking the physical world and digital world together. Sensors play a very important role in IoT [14]. Sensors collect data from the environment, which generates a great amount of useful information. According to [15], the development of IoT includes three phases: embedded intelligence, connectivity and interaction. Embedded intelligence means that devices can perform actions automatically. Connectivity in IoT is mostly given by wireless connections such as ZigBee, WiFi, 3G, etc. Finally, IoT devices must also be capable of interacting with each other autonomously. Thus, with IoT, the current human-to-human interaction will turn into machine-to-machine interaction. The identification of IoT devices is made mostly by the use of radio-frequency identification (RFID). RFID technology is an extension of the optical tags that are found in everyday objects. These tags include embedded intelligence so the identity of an object can be decoded remotely [16].

The IoT generates large volumes of data and requires connectivity and power for long periods of time [17]. This, together with the limitations of the network, computational capacity and limited power supply lead to a high number of challenges. Furthermore, heterogeneity in IoT networks is currently too high due to the lack of standard protocols in this field [18]. Other crucial challenges of IoT are privacy and security. In the current centralised IoT architectures, we cannot be sure if the data has not been tampered with, altered or falsified. Also, nowadays, in many areas, the traceability of assets during their life cycle is required, thus making the immutability of the data a key challenge.

Blockchain is considered by many researchers as the most appropriate solution to the challenges that are present in IoT due to its key features such as security, immutability, trust and decentralisation [19]. Blockchain could protect IoT networks against data tampering. Furthermore, the possibility of creating automatised software that is shared over a decentralised and cryptographically secure blockchain

TABLE 1. Consensus algorithms summary.

Algorithm	Summary	Limitations
PoW	The validators have to perform heavy computational work in order to prove their commitment to the network.	High energy consumption, low throughput, low scalability, 51% of power controls the network.
PoS	Validation capabilities are proportionally tied to the amount of owned cryptocurrency.	Less security than Pow, centralisation of power, poor scalability.
PBFT	A leader is selected to validate a block. Validation must be approved by 2/3 of the network.	Poor scalability, not suited for permissionless networks.
PoC	Validators use their free hard disk space to validate blocks.	Poor adoption, malware interference risk.
PoA	A set of trusted nodes perform the validation of the blocks.	The network relies on a few trusted nodes. If the trusted nodes are compromised, the whole network is compromised.
PoET	Block validation relies on a fair lottery system that is secured by specific hardware.	This algorithm relies on specialised hardware.
PoAc	A block is firstly mined using PoW, then a validator is elected using PoS.	It combines the drawbacks of PoW and PoS: high power consumption and centralisation of power.
RAFT	A network leader is elected within an arbitrary period of time. The leader manages the node requests and the replication of the data.	Low throughput.
PoB	Validators must prove their commitment to the network by destroying part of their assets.	Slower than PoW, and only suitable for cryptocurrency blockchains.

network would increase the autonomy of IoT. In addition, the lack of a central authority would make IoT able to operate more quickly. Furthermore, decentralisation would eliminate single-point failures, thus improving the security and reliability of IoT. The immutability of blockchain is also ideal for the traceability of the data.

It is clear that blockchain is a suitable solution to some of the most important challenges of IoT. However, the original blockchain proposal suffers from limited throughput, high resource consumption, lack of efficiency and delay in storing transactions. These limitations of blockchain contrast with the fact that IoT devices generate huge amounts of data and have serious computational and power limitations. Therefore, the original blockchain technology proposed in 2009 by Satoshi Nakamoto for financial purposes cannot be directly applied to IoT. Although **analysing the security of blockchain is out of the scope of this paper**, it is worth mentioning that blockchain also has some concerning security issues. The most common attack in blockchain is the 51% attack, where the number of malicious nodes is higher than the number of honest nodes, thus compromising the security of the network. DoS, man-in-the-middle or Sybil attacks can also affect blockchains. However, most P2P protocols and IoT infrastructures are already vulnerable to these kinds of attacks [20]. In conclusion, blockchain represents the missing piece of the puzzle to solve the security, privacy and reliability problems of IoT [21].

C. SECTION SUMMARY

In this section, we have explained the concept of blockchain, its functioning mechanisms and the different consensus algorithms that govern most of the current blockchain networks. In addition, we have explained the relation between blockchain and IoT, along with the present challenges and opportunities that the intersection of these two technologies brings.

III. RELATED WORK

We identified 24 related reviews of blockchain for IoT. We conducted a Google Scholar search using the following string:

(*"Blockchain"* AND *"Internet of Things"* OR *"IoT"* AND *"survey"* OR *"review"* OR *"state of the art"*)

Below we summarise the main contributions of each related survey. In Table 2, we provide a detailed classification and comparison of the related work, where we also highlight the focus and contributions of this paper.

Fernández-Caramés and Fraga-Lamas [9] presented a thorough review on how to adapt blockchain to the specific needs of IoT in order to develop blockchain-based IoT (BIoT) applications. Wu et al. [22], Ali et al. [23], Noby and Khattab [24], Abadi et al. [25] and Mezquita et al. [26] conducted comprehensive surveys on the applications of blockchain in IoT. Dai et al. [27] provided an overview of blockchain and its convergence with IoT by presenting a proposal of Blockchain of Things (BCoT). Memon et al. [28] provided a taxonomy of the challenges in the current IoT infrastructure and a literature survey with a taxonomy of the issues to expect in the future of IoT after adopting blockchain. Conoscenti et al. [29] tried to understand whether the blockchain and P2P approaches can be employed to foster a decentralised and private-by-design IoT. Lo et al. [30] focused on analysing the solutions proposed in academia and the methodologies used to integrate blockchain with IoT. Wang et al. [31] and Alladi et al. [32] discussed the integration of blockchain and IoT but only for one specific application: the Industrial Internet of Things (IIoT). Lao et al. [33] analysed popular blockchain-IoT architectures

TABLE 2. Related work comparison.

Ref.	Systematic literature review	"Lightweight" BC concept	Applications	BCIoT Evaluation	Technical aspects	Future directions
[3]						✓
[9]			✓		✓	✓
[22]					✓	✓
[23]			✓		✓	✓
[24]			✓			
[25]	✓		✓			
[26]					✓	
[27]			✓		✓	✓
[28]			✓			✓
[29]	✓		✓	✓		
[30]	✓		✓	✓		✓
[31]			✓			
[32]			✓			
[33]			✓		✓	
[34]			✓		✓	
[35]			✓		✓	
[36]			✓			
[37]			✓			✓
[38]					✓	✓
[39]			✓			✓
[40]				✓	✓	
[41]					✓	✓
[42]						✓
[43]		✓		✓		
This	✓	✓	✓	✓	✓	✓

but only discussed their consensus algorithms. Finally, Farahani [34] presented challenges, opportunities, applications and solutions of blockchain for e-health. Wang et al. [35] and Karthikeyyan et al. [36] surveyed the current limitations and security issues of IoT. Sengupta et al. [37] surveyed the attacks and security issues of blockchain when applied to IIoT. Khan and Salah [3] and Alamri et al. [38] discussed how blockchain could be a key enabler in solving many IoT security problems. Ferrag et al. [39] provided a classification of threat models considered by blockchain protocols in IoT networks and a taxonomy and a side-by-side comparison of the state-of-the-art methods towards secure and privacy-preserving blockchain. Madumidha [40] and Lin et al. [41] focused on the applicability of blockchain for IoT in order to tackle security issues. Alizadeh et al. [42] surveyed the most common attacks that affect blockchain networks and the solutions to mitigate them, intending to assess how malicious these attacks are in IoT.

Unlike the works that we previously mentioned, we systematically analyse the technical characteristics of a significant number of peer-reviewed blockchain architecture proposals for IoT that are categorised as ''lightweight''. We focus on studying the concept of **lightweight** blockchain starting from a general perspective (i.e., definitions) to a more specific overview (i.e., consensus, storage, cryptography, evaluation) of each proposal. The main goal of this study is to emphasise the specific technical aspects, needs, challenges and trends in blockchain development for fields of applications that require lightweight and efficient solutions. As far as we know, there is no systematic review that is completely focused on technical aspects of existing ''lightweight'' blockchain architectures for resource-constrained environments. There is only a short review paper [43] that provides a brief summary of eight solutions labelled as ''lightweight blockchain''. However, the aforementioned review lacks a proper analysis of the few summarised works.

IV. METHOD

In this section, we state the method that was used to conduct the systematic literature review. The method includes the search methodology and the used sources, the research questions, the eligibility criteria and the data collection process.

A. RESEARCH QUESTIONS

The main goal of this paper is to understand the concept of lightweight blockchain and gather relevant information based on the current work in order to help and promote further research in this field. The research questions that this study will address are as follows:

- **RQ1.** How do other authors define the concept of lightweight blockchain?
- **RQ2.** What characteristics do the lightweight blockchain proposals have?
- **RQ3.** In what aspects are the reviewed proposals lightweight?

- **RQ4.** How is lightweight blockchain evaluated?
- **RQ5.** How could we define the concept of lightweight blockchain?

RQ1 aims to gather different definitions of the concept of ''lightweight blockchain'' as it is a relatively new concept that does not have a standard and universal definition yet.

RQ2 pretends to study the main characteristics of the studied proposals in order to perform a comprehensive comparison. The characteristics that will be gathered are as follows:

- The type of the blockchain
- The structure of the framework
- The consensus protocol
- The type of storage

RQ3 is pointed on studying the parts of the reviewed proposals that are considered as lightweight in order to see which aspect are getting the most and the least attention from the researchers. The possible lightweight aspects will be classified as follows:

- Consensus
- Storage
- Architecture
- Cryptography

RQ4 intends to study the evaluation of each proposal in order to gather information about the existing platforms and methods of testing / evaluation as well as insights into how to properly build and test lightweight blockchain.

RQ5 aims to provide a definition of ''lightweight blockchain'' based on the gathered information in order to have a better comprehension of this concept.

B. PAPER INCLUSION CRITERIA

The selected papers on the topic of lightweight blockchain must achieve all of the four inclusion criteria in order to be eligible for this review. These criteria were defined in order to provide the most adequate papers that would help us provide an answer to all our research questions and achieve the objectives of this study. The criteria and the corresponding explanation is shown in Table 3.

C. THE SEARCH AND THE PAPER SOURCES

This study was conducted by manually searching through six of the most relevant scientific search engines:

- dblp (`https://dblp.org/`)
- Google Scholar (`https://scholar.google.es/`)
- Web Of Science (`http://wos.fecyt.es/`)
- Scopus (`https://www.scopus.com/search/form.uri`)
- IEEE Xplore (`https://ieeexplore.ieee.org/`)
- ACM (`https://dl.acm.org/`)

The search string for searching involved two main concepts: lightweight AND blockchain. The complete search terms are as follows:

(*lightweight AND "Blockchain"* OR *"Distributed ledger"* OR *"DLT"*)

The last search was carried out in October 2022.

Finally, the reference lists of the retrieved studies were manually searched in order to identify any additional relevant studies to could be included in this review.

D. STUDY PROTOCOL AND PROCESS

This study was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [44], which diagram is shown in Fig. 3. We decided to use the PRISMA protocol because it offers several key benefits:

- It demonstrates a quality review.
- It allows readers to assess strengths and weaknesses.
- It permits the replication of the reviewing process.
- Its structure is compatible with the standard guidelines for systematic literature reviews in computer science proposed in [45].

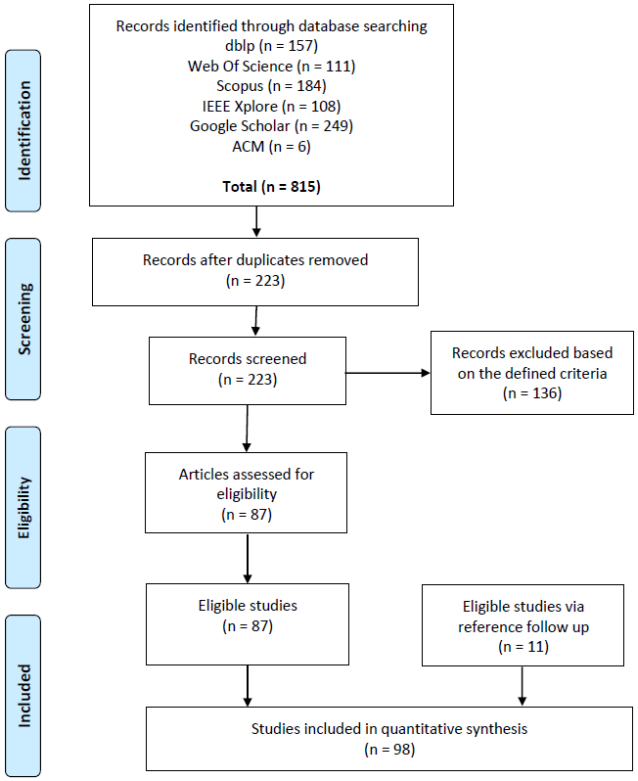

FIGURE 3. PRISMA flow diagram.

After retrieving the available articles following the defined research terms from the databases and removing the duplicates, each article's title and abstract were screened independently for eligibility using the criteria defined in Table 3. From a total of 223 papers, 87 were positively evaluated. Furthermore, 11 more papers were included in the study based on a reference follow-up of the papers that were initially elected, making for a total of 98 included papers.

One hundred thirty-five papers were excluded due to the following reasons:

- The paper is not focused on lightweight blockchain or other DLT: 94 papers

TABLE 3. Paper inclusion criteria.

No	Criteria	Explanation
1	The study must be an original research paper that introduces a novel lightweight blockchain framework or improves an inefficient aspect of blockchain.	The purpose of this study is to review the existing lightweight blockchain proposals for IoT in the existing literature. Survey and review papers will be excluded since they do not always include many details about their proposed solution.
2	The proposal must be aimed to improve at least one of the following aspects: consensus, storage, architecture, cryptography.	This study is completely focused on the performance of blockchain applied to IoT, hence, one of these four aspects has to be improved in order to be considered for this review.
3	The proposed solution must be evaluated.	This review is focused on studying the concept of lightweight blockchain in a practical manner rather than just theoretically. Hence, each proposal has to be evaluated.
4	The reviewed paper must be written in English.	English is the standard-universal language for scientific papers.

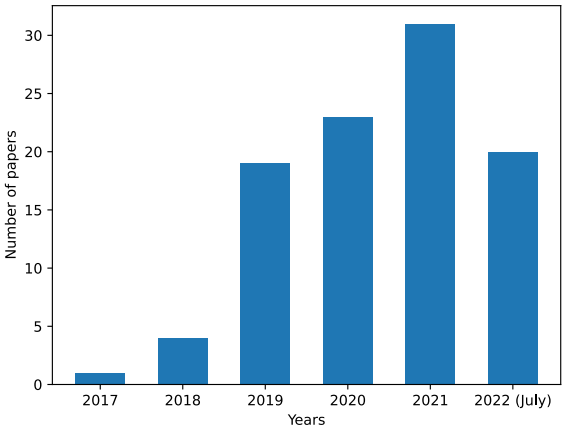

FIGURE 4. Number of eligible papers published each year.

- The paper does not include an evaluation section: 16 papers
- It is not a research paper, or it is a review paper: 14 papers
- The paper is not written in English: 6 papers
- The paper is not available on the internet: 6 papers

Fig. 4 shows the number of eligible papers for each year since 2017, which is the year when the oldest paper of the included studies was published. We have noticed a considerable increment of published papers on lightweight blockchain in the last few years. By middle 2022 the number of lightweight blockchain papers is already more than half of the total number of papers related to this topic in 2021. This shows that the topic of lightweight blockchain is getting more and more attention, thus it is becoming increasingly relevant each year.

The data extraction methodology from the included papers was defined following the research questions of this study and other possible relevant information. The extracted data are as follows:

- The author(s) name, the title, the publication year, the language the reference and the type of the paper.
- The definition of "lightweight blockchain" given by the author(s).
- The main characteristics of the proposal: blockchain type, structure, consensus and storage.
- The lightweight aspects of the proposal: architecture, storage, consensus and cryptography.
- The evaluation process of each proposal: implementation method and evaluated metrics.
- Possible research opportunities for the future.

V. RESULTS

In this section, we present the results of the collected data addressing the research questions that have been defined in Section IV. Please note that we only report what is found in the papers that have been reviewed.

A. RQ1: HOW DO OTHER AUTHORS DEFINE THE CONCEPT OF LIGHTWEIGHT BLOCKCHAIN?

In this subsection, we study how the authors of the reviewed papers define the concept of lightweight blockchain. We identified several characteristics that a blockchain system should have in order to be considered lightweight, according to the authors of the reviewed papers.

Most authors (n = 58) mention a low computational burden when referring to lightweight blockchain. Low network delay and overhead are mentioned by 38 authors. Low storage requirements are mentioned by 34 authors. Throughput capacity is mentioned by 30 authors. Finally, only 22 authors mention energy consumption when referring to lightweight blockchain. Fig. 5 shows the gathered results.

B. RQ2: WHAT CHARACTERISTICS DO THE LIGHTWEIGHT BLOCKCHAIN PROPOSALS HAVE?

In this subsection, a classification and comparison of the main characteristics of the reviewed proposals are presented. The complete classification and comparison of the characteristics of the reviewed solutions can be found in Table 4. The first column of the table provides the references of the reviewed papers. The rest of the columns correspond to the characteristics of the reviewed solutions. The characteristics that we gathered from the reviewed papers are as follows:

- The type of the blockchain in terms of access control.

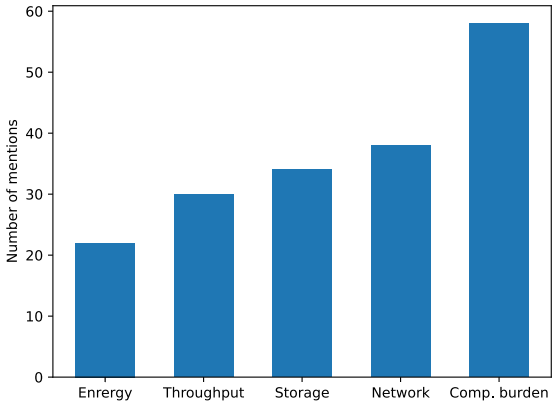

FIGURE 5. Aspects mentioned when referring to lightweight blockchain.

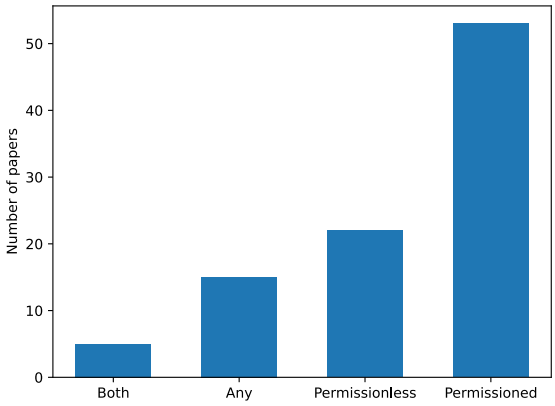

FIGURE 6. Most used blockchain types.

- The structure of the blockchain architecture.
- The consensus protocol.
- The storage approach of the proposed architecture.

Below we provide a summary of the characteristics that were reviewed for each of the included papers and an assessment of the gathered information.

1) BLOCKCHAIN TYPE

As stated in Section II, there are two main types of blockchain: permissioned and permissionless. Out of 98 proposals, 78 were specifically designed as permissioned (n = 56) or permissionless (n = 22) blockchains, whereas five use both types in the same framework. In addition, 15 proposals were not designed for a specific type of blockchain; thus they could be used in both permissioned and permissionless environments (i.e., "any" type). Fig. 6 shows the distribution of this characteristic among all of the studied proposals.

2) STRUCTURE

Originally, all the nodes in a blockchain network could take the role of miners/validators while storing the entire chain. This type of blockchain structure can be defined as the "classic" structure. In resource-constrained environments, this type of structure is not usually possible [87]. Therefore, 49 authors divide the network into different layers of devices that have different capabilities and roles. In addition, the clustering method, where clusters of nodes are maintained by a cluster head, is also common, as it is used in 20 proposals. Both approaches (layering and clustering) can also be combined, as can be seen in 10 works. Another approach is the Directed Acyclic Graph (DAG), which is a structure used in a different type of DLT and was firstly introduced by IOTA [142]. The DAG architecture was used in only seven works. Finally, 28 authors maintain the "classic" one-layered blockchain structure in their proposals. Fig. 7 shows the distribution of the blockchain structure found in the reviewed papers.

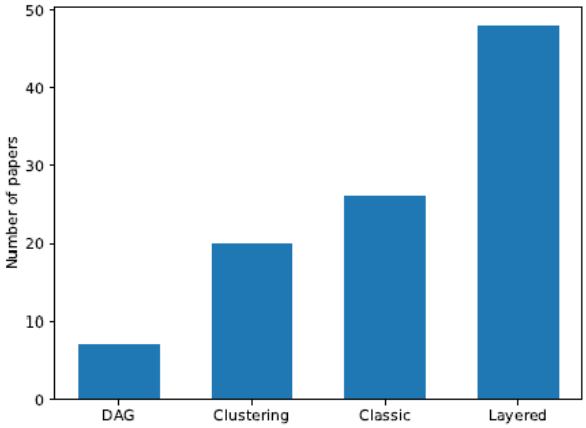

FIGURE 7. Most used blockchain structures.

Note that, in Table 4, some proposals where the structure could not be determined due to the lack of information or the incompatibility of the type of proposal with this categorization. Thus, in five proposals, the structure parameter was marked with a "not applicable" abbreviation (N/A).

3) CONSENSUS

Within the results of our analysis, we can divide the consensus algorithms in two groups:

1) **Custom-made consensus algorithms.** We define a custom consensus algorithm as an algorithm that was specifically developed for the proposed lightweight blockchain framework and was not used in any other framework or system. In 25 papers, we can find different custom algorithms that are randomness, vote, time, trust or location-based.
2) **Generic consensus algorithms.** We define a generic consensus algorithm as an algorithm that was not specifically developed for a specific lightweight blockchain framework research study, or is applied in multiple frameworks or systems. In 43 papers, we can find generic lightweight consensus algorithms such as Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), Raft, Proof of Authority (PoA) and Proof of Capacity (PoC).

The original consensus algorithm of blockchain is the PoW [11]. However, this algorithm is well known for its low efficiency and high resource requirements [143], which makes it unfeasible for resource-constrained devices.

TABLE 4. Main characteristics of the reviewed proposals.

Ref.	Blockchain Type	Structure	Consensus	Storage
[6]	Any	Classic	Randomness-based	On-BC
[46]	Both	Layered	PoW & PoS	Cloud
[47]	Both	Layered & Clustering	Trust-based	Cloud
[48]	Both	Layered & Clustering	Time-based	Cloud
[49]	Permissioned	Layered	Vote-based	On-BC
[50]	Permissioned	Layered	Round-robin	On-BC
[51]	Permissioned	Classic	Round-robin	On-BC
[52]	Permissioned	Layered & Clustering	PoS	Cloud BC
[53]	Both	Layered	PBFT	On-BC
[54]	Permissionless	Classic	Traffic-based	On-BC
[55]	Permissioned	Classic	Reputation-based	On-BC
[56]	Permissioned	Layered & Clustering	PBFT	On-BC
[57]	Permissioned	Layered & Clustering	Trust-based	Cloud
[58]	Permissioned	N/A	PBFT	Temporary
[59]	Permissionless	Classic	Enhanced PoW	On-BC
[60]	Permissionless	Layered	Enhanced PoW	On-BC
[61]	Permissioned	Layered	Vote-based	Off-chain
[62]	Permissioned	Layered	PBFT	On-BC
[63]	Permissioned	Clustering	N/A	On-BC
[64]	Permissioned	Classic	PoET or RAFT	On-BC
[65]	Permissioned	Layered	RAFT	On-BC
[66]	Any	Clustering	Trust-based	N/A
[67]	Any	Layered	Trust-based	Cloud
[68]	Permissionless	Layered	Enhanced PoW	Off-chain
[69]	Permissionless	Clustering	LDC	On-BC
[70]	Permissioned	N/A	PoC	N/A
[71]	Permissioned	Layered	PoA	On-BC
[72]	Permissionless	Classic	EPBC	On-BC
[73]	Permissionless	Clustering	PoW	On-BC
[74]	Permissioned	Clustering	PBFT	On-BC
[75]	Any	Classic	N/A	On-BC
[76]	Permissioned	N/A	N/A	N/A
[77]	Permissionless	Classic	PoW	On-BC
[78]	Permissioned	Layered	PBFT	On-BC
[79]	Permissionless	Classic	DPoR	Off-chain
[80]	Permissionless	Classic	Trust-based	On-BC
[81]	Permissioned	N/A	PoBT	On-BC
[82]	Permissioned	Clustering	PoS	Temporary
[83]	Permissionless	Layered	Enhanced PoW	On-BC
[84]	Both	Layered & Clustering	Trust-based	Cloud
[85]	Any	Layered	Enhanced PoW	On-BC
[86]	Permissioned	Layered	N/A	On-BC
[87]	Any	Layered & Clustering	PoW	Cloud
[88]	Permissionless	DAG & Clustering	PoW	Temporary
[89]	Permissionless	Clustering	Enhanced PoW	N/A
[90]	Permissioned	Classic	Trust-based	Temporary
[91]	Permissioned	Classic	PBFT	On-BC
[92]	Permissioned	Classic	N/A	Cloud
[93]	Permissioned	Layered	Apache Kafka	Off-chain
[94]	Any	Layered	Enhanced PoW	Cloud
[95]	Any	DAG	N/A	Temporary
[96]	Permissioned	Clustering	Enhanced PoW	On-BC
[97]	Permissioned	Classic	PBFT	Off-chain
[98]	Permissioned	Classic	N/A	On-BC
[99]	Permissioned	Layered	Vote-based	On-BC
[100]	Permissioned	N/A	PBFT	On-BC
[101]	Permissioned	Layered	Apache Kafka	On-BC
[102]	Permissioned	Layered	PBFT	On-BC
[103]	Any	DAG	Custom MCMC	On-BC
[104]	Permissionless	DAG	PoW	On-BC
[105]	Permissionless	DAG	Custom	On-BC

TABLE 4. *(Continued.)* **Main characteristics of the reviewed proposals.**

[106]	Permissioned	Classic	PBFT	On-BC
[107]	Permissioned	Layered	N/A	Cloud
[108]	Permissioned	Layered	PBFT	On-BC
[109]	Permissioned	Classic	PBFT	On-BC
[110]	Permissioned	Classic	PBFT	Cloud
[111]	Permissioned	Classic	Custom	On-BC
[112]	Permissioned	Classic	PoS & PBFT	On-BC
[113]	Permissioned	Layered	PoS	On-BC
[114]	Permissioned	Classic	PBFT	Off-chain
[115]	Any	Layered	PoW	On-BC
[116]	Permissioned	Classic	Enhanced PoW	On-BC
[117]	Any	DAG	PoA	On-BC
[118]	Permissioned	Classic	PBFT	On-BC
[119]	Permissionless	Layered & Clustering	PoW	Temporary
[120]	Permissionless	Layered	Enhanced PoW	On-BC
[121]	Permissioned	Classic	PoA	On-BC
[122]	Permissioned	Layered	PoA	On-BC
[123]	Permissionless	Layered	Enhanced PoW	On-BC
[124]	Permissioned	Layered	Enhanced PoW	On-BC
[125]	Permissioned	Clustering	Custom	On-BC
[126]	Permissioned	Layered	Reputation-based	On-BC
[127]	Permissioned	Layered	PBFT	On-BC
[128]	Permissionless	Layered	N/A	Off-chain
[129]	Permissioned	Layered & Clustering	PBFT	On-BC
[130]	Permissioned	Layered	PBFT	Temporary
[131]	Permissionless	Classic	Custom	On-BC
[132]	Permissioned	Layered	Custom	Cloud
[133]	Permissionless	Layered	Enhanced PoW	Cloud
[134]	Any	Layered	Reputation-based	Off-chain
[135]	Any	Layered	N/A	On-BC
[100]	Permissioned	Classic	PBFT	On-BC
[136]	Any	Layered	Custom	On-BC
[137]	Permissioned	Classic	Custom	Off-chain
[138]	Permissionless	Layered	PoA	Cloud
[139]	Permissioned	Clustering	PBFT	Cloud
[140]	Any	DAG	Reputation-based	On-BC
[141]	Permissioned	Classic	PBFT	On-BC

Therefore, most authors employed more efficient consensus algorithms when building lightweight blockchain solutions. These algorithms are as follows: PoS, PBFT, PoET, PoA, PoC, PoR, Raft and other custom-made consensus. All of the alternative consensus algorithms that were used in the reviewed papers were designed to overcome the drawbacks of the PoW algorithm in resource-constrained environments. 13 authors presented an enhanced version of the PoW algorithm rather than implementing a novel algorithm. Fig. 8 shows the distribution of the discussed types of consensus in the reviewed papers.

Note that, in 10 proposals, the consensus algorithm is not mentioned. Therefore, the consensus parameter was marked in Table 4 with a "not available" abbreviation N/A.

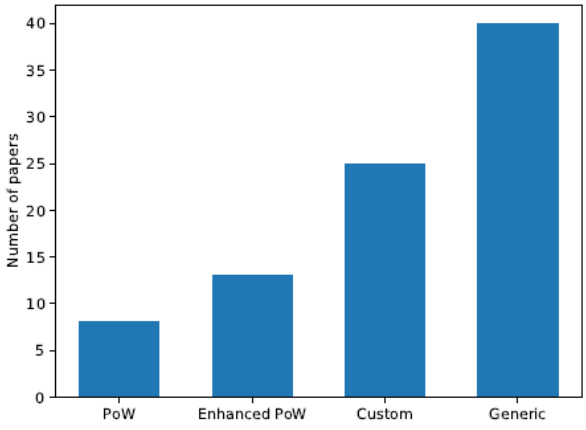

FIGURE 8. Most used types of consensus protocols.

4) STORAGE

Besides the consensus algorithm, storage is also a major issue in the blockchain-based IoT environments [58]. This issue can be easily tackled in some fields where historical data are not important and therefore are stored temporarily, as can be seen in four of the reviewed papers. However, most of the time, this is not the case. Therefore, according to the results of our analysis, data storage can be addressed as follows:

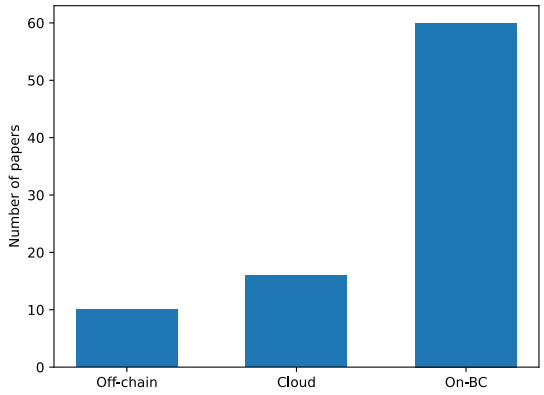

FIGURE 9. How data is stored in lightweight blockchain.

- **On the blockchain (On-BC).** In 63 proposals, the data are kept inside the ledger. However, usually, lightweight IoT devices do not have sufficient storage space to keep the whole ledger. Therefore, 21 authors propose layered architectures where the data are stored in specifically designed storage nodes or layers within the blockchain.
- **Cloud.** Sixteen authors combined Cloud Computing with blockchain in order to tackle the storage issue. In the framework that is presented in [47], the authors assume that a smart home user already has a Cloud account such as Dropbox, OneDrive, etc. Uddin et al. [52] are the only authors that propose a cloud-based blockchain rather than just Cloud storage. They claim that this type of blockchain is the most optimal choice for the high processing and storage requirements of IoT.
- **Off-chain.** Ten authors proposed architectures where the data are stored off-chain (e.g., in a local server or database). In this approach, the only data that has to be stored on the shared ledger are its hashes in order to assure its integrity. However, storing data off-chain does not assure its availability.

Fig. 9 shows the distribution of the type of data storage in the reviewed papers.

Note that, in Table 4, there are three proposals where the storage approach could not be determined due to the lack of information or the incompatibility of the type of proposal with the categorization of this characteristic. Thus, the storage parameter was marked with a ''not applicable'' abbreviation (N/A).

C. RQ3: IN WHICH ASPECTS ARE THE REVIEWED PROPOSALS "LIGHTWEIGHT"?

In this subsection, a study on the lightweight aspects of the reviewed proposals is presented.

Table 5 contains the reference number of each proposal, a brief description and the aspects that were taken into account in order to deliver a lightweight solution. The studied aspects are as follows:

- The consensus algorithm
- The storage approach
- The architecture
- The cryptography

We established an evaluation criterion for each one of the considered aspects: consensus, storage, architecture and cryptography, as shown below.

1) CONSENSUS

In permissioned networks, resource-intensive consensus such as PoW is not necessary [144]. Thus, we will consider that a proposal is lightweight in terms of consensus if it is a permissioned framework that uses:

- A custom vote, time, trust or location based algorithm.
- A generic consensus algorithm that was designed as an efficient alternative to PoW such as: Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), Raft, Proof of Authority (PoA), Proof of Capacity (PoC) and Proof of Reputation (PoR).

Furthermore, an enhanced version of the PoW algorithm could also be considered as lightweight if the authors provide enough evidence on its suitability for resource-constrained devices.

2) STORAGE

As we mentioned in Section V-B, one of the main features of blockchain is the fact that the ledger is replicated in all devices involved in the network. Thus, if attackers want to forge the data, they must hack the majority of devices [58]. However, a resource-constrained device cannot maintain the blockchain continuously because of its low capabilities. Therefore, we consider a solution to be lightweight in terms of storage if:

- The data are stored temporarily on the blockchain.
- The data are stored outside the blockchain (e.g., on the Cloud or in an external database or server).
- There is enough evidence that the size of the data or blocks is reduced so that the storage of the blockchain is feasible on resource-constrained devices.
- The data are only stored in a specific storage layer or storage nodes within the blockchain.

3) ARCHITECTURE

Resource-constrained devices are unable to participate and maintain a blockchain network [83]. Therefore, a lightweight architecture must divide the network in various layers and/or clusters that give the involved devices different tasks according to their capabilities.

4) CRYPTOGRAPHY

Blockchain technology is strongly based on cryptography [145]. However, cryptography processing in resource-constrained devices is not straightforward. Therefore, we will consider a solution as cryptographically lightweight if there is strong evidence of a significant performance improvement related to the cryptographic part of blockchain for resource-constrained environments.

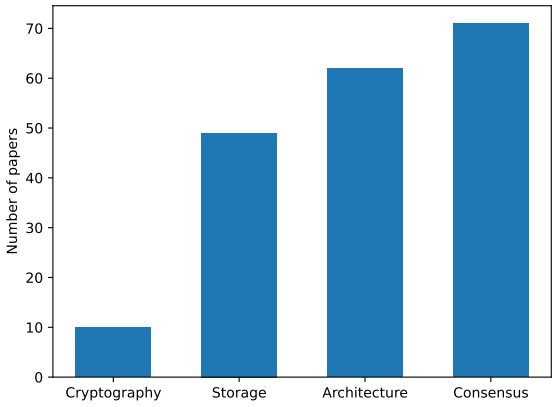

FIGURE 10. Lightweight aspects of the lightweight blockchain proposals.

As it can be seen in Fig. 10 and Table 5, based on our criteria, 74 proposals include a lightweight consensus, 63 a lightweight architecture, 49 a lightweight storage and 11 a lightweight cryptography. Only four proposals are lightweight in all aspects: consensus, storage, architecture and cryptography.

D. RQ4: HOW IS LIGHTWEIGHT BLOCKCHAIN EVALUATED?

In this subsection, we study the evaluation of the reviewed papers. We review the method of implementation of each paper and the evaluated metrics. Apart from the reference and a brief description of each proposed solution, Table 6 includes information about the implementation method (column II) and the metrics that have been evaluated in each case (column III).

1) IMPLEMENTATION METHOD

Twenty-four authors used a high level programming language for the implementation such as Python (n = 13), Java (n = 6), C/C++ (n = 3), JavaScript (n = 1) and iOS Swift (n = 1). Thus, Python, Java and C/C++ are the most commonly used programming languages for lightweight blockchain development. Twenty-three authors implemented their proposals in specific blockchain development platforms such as Hyperledger (n = 11), Ethereum (n = 10) or Multichain (n=2). Platforms such as Hyperledger Ethereum or Multichain offer great possibilities for implementing lightweight blockchains as they are suited for permissioned networks that include lightweight consensus. Twenty-two authors used generic simulators such as the NS-3 network simulator (n = 10), Cooja (n = 4), Matlab (n = 4), Colored Petri Net (n=1) or custom made simulators such as "ZeroCaloSimu" (n=1) or "BlockLite" (n = 2). Finally, 29 authors did not provide information on how their solution was developed. Hence, in that case, the implementation parameter was marked with a "not available" abbreviation (N/A). Fig. 11 shows the distribution of the implementation methods that were used in the reviewed papers.

TABLE 5. Lightweight aspects of the reviewed proposals.

Ref.	Lightweight Aspects			
	Consensus	Storage	Architecture	Cryptography
[6]	✓			
[46]	✓	✓	✓	
[47]	✓	✓	✓	
[48]	✓	✓	✓	✓
[49]	✓	✓	✓	
[50]	✓		✓	
[51]	✓			
[52]	✓	✓	✓	
[53]	✓	✓	✓	
[54]	✓			
[55]	✓		✓	
[56]	✓		✓	
[57]	✓	✓	✓	
[58]	✓	✓		
[59]	✓			
[60]		✓	✓	✓
[61]	✓		✓	
[62]	✓	✓	✓	✓
[63]	✓	✓	✓	
[64]	✓			
[65]	✓	✓	✓	
[66]	✓		✓	
[67]	✓	✓	✓	
[68]		✓	✓	
[69]			✓	
[70]	✓			
[71]	✓	✓	✓	
[72]		✓		
[73]		✓	✓	
[74]	✓	✓	✓	
[75]			✓	
[76]				✓
[77]		✓		
[78]	✓	✓	✓	
[79]	✓	✓		
[80]	✓			
[81]	✓	✓		
[82]	✓	✓	✓	
[83]		✓	✓	
[84]	✓	✓	✓	✓
[85]		✓	✓	✓
[86]	✓	✓	✓	
[87]		✓	✓	
[88]		✓	✓	
[89]	✓			
[90]	✓	✓		
[91]	✓			
[92]		✓		
[93]	✓	✓	✓	
[94]		✓	✓	
[95]		✓	✓	
[96]			✓	✓
[97]	✓	✓		
[98]	✓			
[99]	✓		✓	
[100]	✓	✓		
[101]	✓	✓	✓	
[102]	✓	✓	✓	
[103]	✓			
[104]			✓	
[105]	✓			
[106]	✓			
[107]		✓	✓	
[108]	✓		✓	
[109]	✓			
[110]	✓	✓		
[111]	✓			

TABLE 5. *(Continued.)* **Lightweight aspects of the reviewed proposals.**

[112]	✓			
[113]	✓		✓	
[114]	✓	✓		
[115]			✓	
[116]	✓			
[117]	✓		✓	
[118]	✓			
[119]		✓	✓	
[120]	✓		✓	
[121]	✓			
[122]	✓		✓	
[123]	✓		✓	
[124]	✓		✓	✓
[125]	✓		✓	
[126]	✓		✓	
[127]	✓		✓	
[128]		✓	✓	
[129]	✓		✓	
[130]	✓	✓	✓	
[131]	✓			
[132]	✓	✓	✓	✓
[133]		✓	✓	✓
[134]	✓	✓	✓	
[135]			✓	
[100]	✓			
[136]	✓		✓	
[137]	✓		✓	
[138]	✓	✓	✓	
[139]	✓	✓	✓	
[140]	✓		✓	
[141]	✓			✓

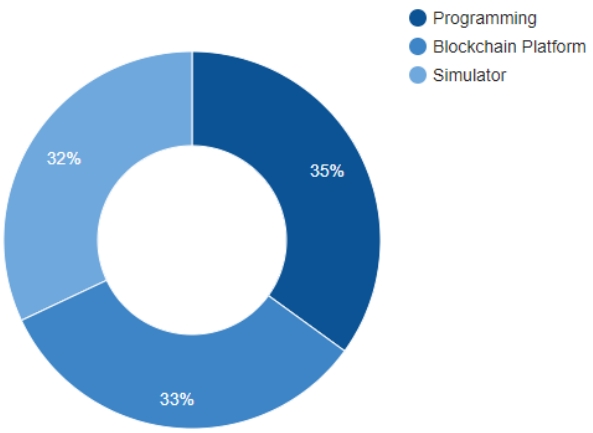

FIGURE 11. Implementation methods of lightweight blockchain.

2) EVALUATED METRICS

In this sub-subsection, we study the metrics that were evaluated in the reviewed papers. This review is focused on the performance of blockchain; hence, we omit security evaluations. As it can be seen in Fig. 12, the authors of the reviewed papers have evaluated a wide range of performance metrics. Each author evaluated different metrics based on different criteria. The authors mostly focus on evaluating metrics that are related to their proposal's strengths and aimed improvements. We can frame the gathered evaluated metrics in the following categories:

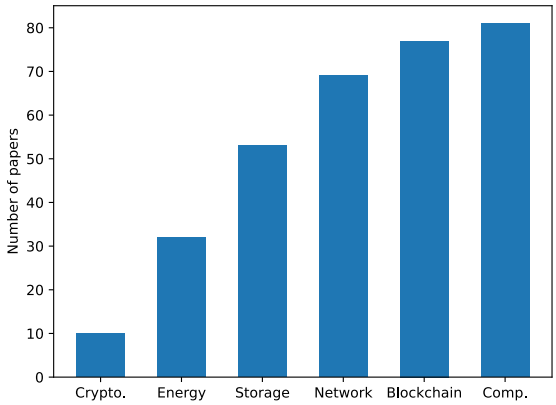

FIGURE 12. Evaluated metrics.

- **Computational. (n = 82)** The metrics that are related to the computational resources such as the CPU, the memory, etc.
- **Blockchain. (n = 78)** The metrics that are related to the blockchain transactions, blocks and consensus.
- **Network. (n = 69)** The metrics that are related to the network communication, such as bandwidth, latency, etc.
- **Storage. (n = 53)** The metrics that are related to the data storage.
- **Energy. (n = 33)** The metrics that are related to the energy or power consumption.
- **Cryptography. (n = 11)** The metrics that are related to the cryptographic functions.

E. RQ5: HOW COULD WE DEFINE THE CONCEPT OF LIGHTWEIGHT BLOCKCHAIN?

According to the information that was gathered in order to answer to the previous five research questions, we can define the concept of lightweight blockchain as:

A framework that has proved its viability in resource-constrained environments and includes the following five characteristics:

- *Low computational burden*
- *Low network overhead*
- *Low storage requirements*
- *High throughput*
- *High energy efficiency*

VI. DISCUSSION AND FUTURE DIRECTIONS

In this section, we analyse the results of our study and give our own insights. We also discuss several research opportunities that we have identified during the review process. This section is divided in three subsections:

- Section VI-A is related to the technical aspects of lightweight blockchain. Specifically, it addresses RQs 1, 2, 3 and 5.
- Section VI-B is related to the evaluation of lightweight blockchain. Specifically, it addresses RQ4.
- In Section VI-C we provide a summary of the open research gaps and future directions in lightweight

TABLE 6. Lightweight blockchain evaluation summary.

Ref.	Implementation	Evaluated metrics
[6]	Java	Processing time
[46]	NS-3	Authentication time, block size
[47]	Cooja, NS-3	Consensus processing time, time overhead, energy consumption, packet overhead
[48]	Cooja & NS-3	Processing time, energy consumption, packet overhead
[49]	N/A	Computational time, communication cost
[50]	Multichain	Authentication service execution time, block transmission rate, block validation delay
[51]	Multichain	Authentication requests execution time
[52]	Java	Block generation time, energy consumption
[53]	C/C++	Time per transaction, private keys distribution time, network supervision time
[54]	Matlab	Routing latency, traffic of swarm of UAS networking
[55]	NS-3	Processing time, data transferred
[56]	N/A	Processing time, transactions per second, package overhead
[57]	Hyperledger	Throughput, transaction latency, communication time, block generation time
[58]	Python	Consensus delay, blockchain size
[59]	ZeroCaloSimu	Bandwidth consumption, transactions per second
[60]	BlockLite	Block generation time, mining time per block, blocks per second
[61]	iOS Swift	The system functioning on resource-constrained devices
[62]	Hyperledger	Transactions per second, network response time, digital signatures overhead
[63]	C++	Transactions per millisecond, performance of read operations data lookup
[64]	Hyperledger	Transactions per second, computational overhead
[65]	N/A	Computational overhead, communication overhead
[66]	N/A	Network traffic overhead, processing overhead, energy saving
[67]	N/A	Resource consumption, latency
[68]	N/A	Mining speed & power consumption, signature performance, transactions per second, storage
[69]	N/A	Space occupancy, network delay, network energy consumption
[70]	Python	Network latency, transactions per second, transaction verification, block mining, block verification, vote verification
[71]	Ethereum	Transaction packaging time, transactions per second
[72]	N/A	Proof generation, proof verification
[73]	Ethereum	Resource usage
[74]	N/A	Computational and communication overhead
[75]	Ethereum	Network throughput & latency
[76]	N/A	Storage requirement, communication overhead, computational overhead
[77]	Java	Transaction verification rate, storage, data reliability, data availability
[78]	N/A	Transaction overhead
[79]	N/A	Block generation time, data accuracy, truth value accuracy, task cost
[80]	NS-3	Network overhead, block generation latency
[81]	Hyperledger	Computational time, memory requirement, bandwidth requirement
[82]	N/A	Storage cost
[83]	Python	CPU usage, block generation speed, computational cost, consensus stability, network usage, storage
[84]	Python	Transaction processing time, block validation processing time, hash rate, hash quality, storage
[85]	NS-3	Consensus processing time, implementation cost (hardware implementation area), power consumption
[86]	N/A	Storage cost
[87]	Python & NS-3	Storage cost, block propagation time, number of calculations
[88]	N/A	Storage cost
[89]	Cooja	Number of transactions mined, latency, consensus time, energy consumption
[90]	C	The increment of the Flash and RAM memory occupation and the average network latency
[91]	Hyperledger	Storage efficiency, computational cost, communication cost
[92]	Ethereum	Computational complexity, communication overhead
[93]	N/A	CPU usage, memory usage, transactions performance
[94]	Matlab	Consensus algorithm complexity, consensus efficiency
[95]	N/A	Transaction throughput, memory usage, CPU utilization, bandwidth consumption
[96]	N/A	Resource utilization, consensus delay
[97]	Ethereum	Blockchain size, CPU and memory overhead, storage latency, PKI latency
[98]	Ethereum	Storage cost, computational cost
[99]	N/A	Computational cost, communication overhead
[100]	Hyperledger	Transactions per second, consensus delay, communication times
[101]	Hyperledger	Transactions per second, scalability, storage cost, block weight

TABLE 6. *(Continued.)* **Lightweight blockchain evaluation summary.**

[104]	N/A	Transactions per second
[102]	Hyperledger	Scalability, storage cost, transactions delay, processing time
[103]	N/A	DAG consensus: cumulative weights, number of tips, simulation time
[105]	Python	Transaction confirmation overhead, validation overhead
[106]	Matlab	Operating capability under the symmetric and asymmetric information environments
[107]	Python	Authentication delay, application delay, network usage and energy consumption
[108]	Ethereum	Gas cost, response time
[109]	Python	Storage overhead, consensus latency
[110]	Hyperledger	Transfer speed, migration time
[111]	Ethereum	Disk usage, memory allocation, CPU usage, throughput, power consumption
[112]	NS3	Cryptography computational cost
[113]	N/A	Power consumption, CPU usage, block transmission cost, message transmission overhead
[113]	Java	Computational cost, storage, communication overhead, consensus delay
[115]	Javascript	Execution time, throughput, concurrent requests overhead ratio
[116]	Python	Block generation time
[117]	N/A	Performance, power consumption, resource usage
[118]	NS3	Communication and computational overheads, average delay, energy consumption
[119]	Java, Python	Computation and communication costs
[120]	Python	Energy consumption, consensus time, latency
[121]	Cooja	Cryptography performance, energy consumption, communications cost
[122]	Java	Mining time
[123]	N/A	CPU and RAM usage
[124]	Hyperledger	Transaction latency, throughput
[125]	N/A	Data overhead
[126]	N/A	Reputation fluctuation
[127]	N/A	Communication overhead, storage bandwidth, consensus time
[128]	Ethereum	Storage size, upload response time, query response time
[129]	Python	Throughput, block mining and reading times, memory overhead
[130]	N/A	Authentication latency, communication overhead, consensus latency, storage cost
[131]	N/A	Communication overhead
[132]	N/A	Block mining computation cost, throughput, transaction confirmation latency
[133]	BlockLite	Mining delay, block generation time, throughput
[134]	N/A	Lottery-based consensus selection time
[135]	N/A	Average latency, transferred data
[100]	Hyperledger	Throughput, delay, communication time
[136]	N/A	CPU and RAM usage, energy consumption
[137]	N/A	Consensus latency, download and upload delay
[138]	Ethereum	Delays, computational performance
[139]	NS3	Computational and communication overhead
[140]	ColoredPetriNet	Difficulty impact on mining times
[141]	Matlab	Encryption time

blockchain for IoT that we mentioned in the previous subsections.

A. LIGHTWEIGHT BLOCKCHAIN TECHNICAL ASPECTS

We identified very few solutions that are lightweight in all of the studied aspects: consensus, architecture, storage and cryptography. Thus, there is a clear need to design complete lightweight blockchain frameworks.

When it comes to lightweight blockchain, the majority of researchers think about the computational burden of blockchain in the first place. Blockchain offers major security and privacy features to networks that are composed of untrusted devices. However, these advantages come at a huge cost in terms of computational burden. According to most of the authors, the part of blockchain that mostly causes its computational burden is the consensus algorithm. In consequence, many alternatives to the original PoW consensus algorithm of blockchain have been proposed. According to the results of the study, vote-based consensus algorithms are highly efficient and secure, whilst the PoW algorithm is the least efficient. It is worth mentioning that improving the PoW algorithm is also a studied option. However, we found out that enhancing the performance of the consensus algorithm could have a serious impact on the security of blockchain. That is why most authors design permissioned blockchain architectures for IoT. In a trusted environment, the security features of the consensus algorithm can be reduced in order to lower its computational burden. Another effective method of reducing the computational burden of blockchain is to design layered and/or clustered architectures. Dividing an architecture into various layers or clusters prevents resource-constrained devices from performing heavy

computational tasks such as mining. However, this approach also has a negative impact on some benefits of blockchain. Ideally, all devices should participate in the blockchain network in order to assure maximum security and trust. Thus, our conclusion on the computational burden issue is that further research is required. There is a considerable need to develop more lightweight consensus algorithms without sacrificing security. We also believe that currently, designing layered architectures where IoT devices do not have to perform heavy tasks is an optimal approach.

The second concern of the researchers that work on lightweight blockchain solutions is the network overhead. In blockchain, all the transactions that occur in the network must be replicated in all nodes. In addition, lightweight consensus that is based on voting also carries an enormous communication burden. For example, the PBFT consensus needs to constantly exchange information regarding blocks validation between all the nodes of the network. That is why the performance of PBFT dramatically decreases when the number of nodes is high (i.e., more than 20) [144]. One of the most effective ways to reduce the network burden in blockchain is presented in [83]. The authors observed that during blocks verification, the information broadcast by peer nodes overlapped. Hence, they designed a lighter block structure named LightBlock. This approach reduces the necessity of sending the entire data to the other nodes more than one time. This approach reduced the network overload by over 90%. However, reducing the network burden in distributed systems while maintaining the full availability and integrity of the data is still a major issue that needs further research. One of the greatest drawbacks of blockchain is its low throughput. Bitcoin can only process seven transactions per second [11], whereas conventional payment systems like VISA or PayPal can process thousands. The low throughput of blockchain is not only a major issue in financial applications. IoT generates thousands of exabytes annually [146], and all that data has to be processed rapidly. The throughput is another aspect of blockchain that is strictly tied to the consensus algorithm. The heavy consensus process of blockchains greatly reduces their throughput. The most remarkable mechanism that has been proposed in order to improve the throughput of blockchain is the reputation-based consensus. One of the most effective reputation consensus is proposed in [47]. In this type of consensus, the nodes that have a good reputation are able to generate transactions at a much faster rate. This is because when trust is created, the verification process decreases for the nodes that have proved to be trustworthy. However, one of the major drawbacks of reputation-based consensus is that a trusted (i.e., permissioned) environment is required. Therefore, improving throughput in permissionless blockchains is still a major issue that needs further research.

One of the main features of blockchain is the fact that the ledger is replicated in all devices involved in the network. Thus, if attackers want to forge the data, they must hack most of the devices in the network. However, a resource-constrained device cannot maintain the blockchain continuously because of its low capabilities. Specifically, due to insufficient storage capacity, these types of devices cannot assure blockchain's property of immutability [58]. According to the results of our study, there are three main approaches for lightweight blockchain storage:

- Storing the data in the blockchain, but not on all devices. This approach is very typical in layered architectures, where the data are stored in nodes that have sufficient storage. However, this approach separates the lightweight devices from the blockchain network itself. As we mentioned before, ideally, all devices should fully participate in the blockchain network.
- Storing the data off-chain is a simple yet effective method of reducing the storage burden in blockchain. In this approach, the only data that has to be stored in the blockchain are its hashes in order to assure its integrity. However, storing data off-chain does not assure its availability, which is a major issue. Therefore, we recommend using this approach in environments where data loss is not a major concern.
- Cloud computing is another effective method of reducing the storage burden in blockchain. This method is very similar to the previous one. However, cloud storage is maintained by a third party. Thus, we recommend using this approach only if the privacy and the availability of the data are not critical.

In conclusion, we identified a clear need to further research the integration of Cloud computing with blockchain in order to deliver safe, lightweight storage for resource-constrained environments. Furthermore, assuring the availability of the data in an off-chain storage approach is also a great challenge that requires further research. Nonetheless, novel approaches that would reduce the storage burden of on-chain data would be the most appropriate method of improving this aspect.

Energy consumption is the least aspect that authors mention when working on lightweight blockchain. However, this aspect has a huge impact on our world. Thus, it is not less important. According to [147], Bitcoin mining consumes the same amount of energy as the entire country of Denmark. Nevertheless, the huge energy consumption of blockchain not only involves environmental issues. Millions of IoT devices run on batteries [148], making blockchain unfeasible for a great part of lightweight devices. Energy consumption is mostly tied to the consensus algorithm. Therefore, improving the consensus algorithm also has a positive impact on energy consumption. For example, the authors in [83] propose a ''green'' consensus algorithm that reduces mining, with the specific purpose of reducing the energy consumption of blockchain in industrial environments. Many authors completely removed the mining process of the consensus in order to reduce energy consumption. However, as we mentioned before, removing mining could drastically reduce the security of the blockchain. This is why the most efficient consensus algorithms are available only in permissioned networks. Therefore, we recommend further research on efficient consensus for permissionless blockchain.

Very few authors focused on cryptographic improvements. Cryptography is a core feature of blockchain [149]. However,

cryptography incurs a major burden, especially in lightweight IoT devices. Therefore, some of the reviewed papers aimed at reducing the burden that cryptography causes in IoT. In [85], the authors address the performance and energy consumption of the hash function in the mining process. They propose a novel mechanism that can change the hash algorithm used for mining by adjusting to the network traffic. The works [150] and [151] address similar a problematic regarding the performance of crpyptographic functions in blockchain. The work in [150] propose a blockchain-based vehicle-to-vehicle communication scheme with a low $\mathcal{O}(1)$ time complexity whilst the work in [151] goes one step further and analyzes the implementation of Federated Learning (FL) algorithms in blockchain for IoT schemes. FL algorithms improve blockchain-based IoT architectures by adding privacy and by further reducing overhead. Similarly, the authors in work [84] improve the used algorithms from the proposal presented in [47] achieving better security and performance results. However, we believe that the cryptography enhancement has received too little attention from the researchers and that there is room for more improvements. Novel lightweight cryptographic functions for blockchain need to be developed. Furthermore, it is also important to take into account quantum computing, which can pose a major threat to the security of blockchain [152].

Another approach for lightweight blockchain that is worth mentioning is the DAG structure. IOTA introduced this type of DLT aiming at IoT environments. However, this framework is not completely decentralised yet, since it has a centralised coordinator. The coordinator is run by IOTA Foundation in order to assure the security of the network. Currently, DAG-based blockchain can be completely decentralised and secure only when there is a high volume of transactions. One highly relevant lightweight blockchain architecture based on DAG structure is presented in [88]. In this paper, the authors try to tackle the storage issue of blockchain by proposing a DAG network for vehicular social networks. In the proposed architecture, only recent data that is useful for the drivers is maintained in the ledger. Furthermore, the main ledger is divided into various topic groups, which also greatly reduces the storage requirements. One particular DAG approach is presented in [104], where the authors design a DAG architecture that is very similar to blockchain, thus maintaining its greatest drawbacks such as huge energy consumption due to PoW mining. However, this particular DAG structure offers much more throughput capacity than regular blockchains. In conclusion, DAG is a promising solution. However, this technology still has some important limitations and challenges, such as centralisation and security issues [142]. Furthermore, DAGs still require real-world validation in several IoT areas. Apart from DAG DLTs, there are several efficient blockchain solutions that are suitable for IoT; the Hyperledger ecosystem, with Fabric and Sawtooth as the most used blockchains, and other platforms such as R3 Corda or Ethereum 2.0 with the novel PoS scheme that was recently released. Hashgraph is also an emerging solution that offers great efficiency. However, this technology has not yet been consolidated.

Finally, according to the previous discussion, we conclude that the most justifiable aspects that make a blockchain ''lightweight'' are as follows: efficient consensus algorithm, external storage and efficient cryptographic implementations. Consequently, the aforementioned characteristics guarantee low energy consumption, low network overhead, low computational and storage burdens, and overall high throughput capacity.

B. LIGHTWEIGHT BLOCKCHAIN EVALUATION

This paper is focused on the performance aspects of blockchain for IoT. Thus, we analysed the evaluation of the reviewed papers. Specifically, we analysed the implementation methods and the evaluated metrics of the lightweight blockchain proposals.

1) IMPLEMENTATION METHODS

Our analysis shows that there is a wide range of implementation methods for deploying blockchain networks. We identified a clear lack of a simple, universal and standardised testing and evaluation platform for lightweight blockchain. Furthermore, the conducted experiments could not accurately reproduce the system behavior in a real-world environment due to the following reasons:

- Developing a blockchain framework proof of concept from scratch using a high-level programming language is not a simple task, and there is no guarantee that it will provide reliable results.
- Available test environment might use different mechanisms from the real world implementation.
- Normally, only a small number of IoT devices are used.
- Simulations might not provide accurate results for all case scenarios.

2) EVALUATED METRICS

Each author focused on different metrics in order to validate their lightweight blockchain proposal. There are two main reasons for this; First, the authors focus on different problematic aspects of blockchain and DLTs. For example, in [104] the authors claim that improving blockchain's throughput makes this technology sufficiently suitable for IIoT, and therefore, only measure the transactions per second of their solution. On the other hand, the authors in [83] take more aspects into account and therefore include more metrics in their evaluation. Second, the fact that authors use many distinct platforms to perform their experiments also impacts the measured metrics. For example, Hyperledger comes by default with several tools that can be used for performance evaluation purposes, such as Hyperledger Caliper, whereas other platforms such as Ethereum only include metrics related to the blockchain blocks and transactions. Moreover, the existence of multiple evaluation environments developed from scratch provides infinite possibilities when defining evaluation metrics.

The results of this study have proven that lightweight blockchain must possess several key characteristics in order to be applied to IoT: low computational burden, low network overhead, low storage requirements, high throughput and high energy efficiency. Therefore, a standardised metrics scheme for evaluating blockchain or other DLT solutions for IoT should be developed. Also, there is not clear what performance values are acceptable for a blockchain to be considered ''lightweight''. For example, how many transactions per second are enough or can be acceptable for a blockchain architecture for IoT? Establishing a consensus in this regard is an important challenge that needs to be addressed if standardised methodologies for lightweight blockchain are to be developed.

In conclusion, the high variability of the evaluated metrics in lightweight blockchain shows that it is necessary to develop a systematic and standard methodology in order to evaluate lightweight blockchain solutions. This would accelerate and facilitate the development and adoption of blockchain in IoT.

C. FUTURE DIRECTIONS SUMMARY

In the analysis of the results, we identified the following research opportunities and challenges for the further development of lightweight blockchain solutions:

1) Design complete blockchain solutions for IoT that are lightweight in all aspects: consensus, architecture structure, storage and cryptography.
2) Develop lightweight consensus algorithms that are suitable for permissionless blockchain networks.
3) Reduce the network overhead in distributed systems while maintaining the full availability and integrity of the data.
4) Improve throughput and reduce the network overhead in permissionless networks without reducing the security of the consensus algorithm.
5) Advance on the integration of Cloud computing with blockchain while guaranteeing the availability of the data.
6) Reduce the energy consumption of the consensus algorithms in permissionless networks.
7) Develop novel lightweight cryptographic algorithms for blockchain while taking into account quantum computing.
8) Eliminate centralization in DAG DLTs and solve its security issues.
9) Develop DLT solutions for specific IoT fields, such as Industry 4.0, smart homes, healthcare, etc., while tackling the specific issues and needs of each field.
10) Develop blockchain interoperability solutions in order to enable secure and efficient communication between heterogeneous blockchains.
11) Advance in the establishment of a standardised testing platform and metrics for blockchains and other DLTs (IOTA, Hashgraph, etc.).

VII. CONCLUSION

In this work, we systematically reviewed 98 ''lightweight blockchain for IoT'' proposals that have been published since 2017. This is the first systematic literature review that provides a comprehensive analysis of specific technical aspects that can be found in the current blockchain for IoT architecture proposals. We analysed and categorised several characteristics of the blockchains, their lightweight aspects and their evaluations. Finally, we outlined the existing shortcomings and identified future research opportunities.

Our review proves that the concept of lightweight blockchain is constantly increasing its popularity each year. The analysed papers cover a wide variety of applications, and they are generally focused on a few specific problematic aspects of blockchain when it comes to its application in resource-constrained environments. Despite the relatively high number of proposed solutions in this field, there is still much research to be done, as the balance between security and efficiency in the blockchain is delicate. If the security properties of blockchain are reduced, then this technology becomes pointless when compared to other options. Thus, further research must be done in order to further improve blockchain-based IoT architectures. Furthermore, most of the proposed solutions are developed on many different platforms. Thus, they cannot be fairly compared, and most proofs-of-concept are typically in a too early stage of development. Finally, the increasing number of different blockchain solutions highlights the need to devise interoperable solutions.

According to the results of our study, the most promising yet unexplored DLT type is the DAG. This structure requires much less energy consumption, has zero fees and offers high throughput. However, ''classic'' blockchains are not yet outdated, since vote-based or round robin consensus algorithms along with layered Edge architectures are also efficient and could be used in many IoT applications. Other promising solutions regarding the storage burden of blockchain seems to be the use of decentralized databases such as IPFS to store the actual data. Finally, research regarding post-quantum cryptography for blockchain is also promising, since quantum computing poses a significant threat to the current blockchain architectures.

REFERENCES

[1] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, ''Internet of Things (IoT) security: Current status, challenges and prospective measures,'' in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, vol. 5, no. 4, Dec. 2015, pp. 336–341.

[2] B. Jovanovic, ''Internet of Things statistics for 2021-taking things apart,'' *DataProt*, vol. 21, Mar. 2021.

[3] 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.

[4] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, ''Blockchain technology innovations,'' in *Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON)*, Jun. 2017, pp. 137–141.

[5] J. Potts and E. Rennie, ''Web3 and the creative industries: How blockchains are reshaping business models,'' in *A Research Agenda for Creative Industries*. Cheltenham, U.K.: Edward Elgar Publishing, 2019, pp. 93–111.

[6] A. Dorri and R. Jurdak, ''Tree-chain: A fast lightweight consensus algorithm for IoT applications,'' in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 369–372.

[7] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.
[8] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey Shaoan Xie Hong-Ning Dai Huaimin Wang," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 1–24, 2017.
[9] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[10] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.
[11] S. Squarepants, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, Oct. 2008.
[12] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, "Proof of contribution: A modification of proof of work to increase mining efficiency," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 636–644.
[13] N. Szabo, "Smart contracts: Building blocks for digital markets," *EXTROPY, J. Transhumanist Thought*, vol. 18, no. 2, p. 28, 1996.
[14] M. Conner, "Sensors empower the 'Internet of Things,'" *Elect. Des. News*, vol. 55, no. 10, p. 32, 2010.
[15] L. Tan and N. Wang, "Future internet: The Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. 376–380.
[16] H. Kopetz, "Internet of Things, real-time systems," *Int. J. Innov. Advancement Comput. Sci.*, vol. 3, no. 8, pp. 1–20, 2011.
[17] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 375–376.
[18] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in *Proc. Future Technol. Conf. (FTC)*, Dec. 2016, pp. 731–738.
[19] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain, Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100006.
[20] 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.
[21] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.
[22] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.
[23] 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.
[24] D. A. Noby and A. Khattab, "A survey of blockchain applications in IoT systems," in *Proc. 14th Int. Conf. Comput. Eng. Syst. (ICCES)*, Dec. 2019, Art. no. 201914.
[25] F. A. Abadi, J. Ellul, and G. Azzopardi, "The blockchain of things, beyond Bitcoin: A systematic review," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1349–1354.
[26] Y. Mezquita, R. Casado, A. Gonzalez-Briones, J. Prieto, and J. M. Corchado, "Blockchain technology in IoT systems: Review of the challenges," *Ann. Emerg. Technol. Comput.*, vol. 3, no. 5, pp. 17–24, Dec. 2019.
[27] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[28] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based IoT: A comparative survey and way forward," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 4, pp. 563–586, Apr. 2020.
[29] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.
[30] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019.
[31] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, vol. 10, Jun. 2020, Art. no. 100081.
[32] T. Alladi, V. Chamola, R. M. Parizi, and K.-K.-R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.
[33] 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. Surveys*, vol. 53, no. 1, pp. 1–32, Jan. 2021.
[34] 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.
[35] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.
[36] P. Karthikeyyan, S. Velliangiri, and M. I. T. Joseph. S, "Review of blockchain based IoT application and its security issues," in *Proc. 2nd Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT)*, Jul. 2019, pp. 6–11.
[37] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.
[38] M. Alamri, N. Z. Jhanjhi, and M. Humayun, "Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 5, pp. 244–258, 2019.
[39] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[40] M. S. Madumidha, "Blockchain Security for Internet of Things: A literature survey the Internet of Things (IoT) is experiencing a tremendous growth in areas of research and industry; however, still suffers from security issues. Conventional security mechanisms haven," *Int. J. Pure Appl. Math.*, vol. 119, no. 16, pp. 3677–3686, 2018.
[41] H. Hui, X. An, H. Wang, W. Ju, H. Yang, H. Gao, and F. Lin, "Survey on blockchain for Internet of Things," *J. Internet Services Inf. Secur.*, vol. 9, no. 2, pp. 1–30, May 2019.
[42] M. Alizadeh, K. Andersson, and O. Schelén, "A survey of secure Internet of Things in relation to blockchain," *J. Internet Services Inf. Secur.*, vol. 10, no. 3, pp. 47–75, 2020.
[43] D. Hanggoro and R. F. Sari, "A review of lightweight blockchain technology implementation to the Internet of Things," in *Proc. IEEE Region 10 Humanitarian Technol. Conf. (R10-HTC)*, Nov. 2019, pp. 275–280.
[44] D. Moher et al., "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Med.*, vol. 151, no. 4, p. 264, Aug. 2009.
[45] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," School Comput. Sci. Math., Keele Univ., Tech. Rep. 5, 2007.
[46] D. M. Sheeba and S. Jayalakshmi, "Lightweight blockchain to improve security and privacy in smarthome," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 6, pp. 5021–5027, Mar. 2020.
[47] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.
[48] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020.
[49] M. Singh, G. S. Aujla, and R. S. Bali, "ODOB: One drone one block-based lightweight blockchain architecture for Internet of Drones," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 249–254.
[50] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using Internet of Drone Things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 166–173, Aug. 2021.
[51] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 972–976, May 2022.
[52] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, "A lightweight blockchain based framework for underwater IoT," *Electronics*, vol. 8, no. 12, p. 1552, Dec. 2019.

[53] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.

[54] J. Wang, Y. Liu, S. Niu, and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Comput. Commun.*, vol. 165, pp. 131–140, Jan. 2021.

[55] J. Xi, S. Zou, G. Xu, and Y. Lu, "CrowdLBM: A lightweight blockchain-based model for mobile crowdsensing in the Internet of Things," *Pervas. Mobile Comput.*, vol. 84, Aug. 2022, Art. no. 101623.

[56] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.

[57] X. Xu, Z. Zeng, S. Yang, and H. Shao, "A novel blockchain framework for industrial IoT edge computing," *Sensors*, vol. 20, no. 7, pp. 1–16, 2020.

[58] T. Kim, J. Noh, and S. Cho, "SCC: Storage compression consensus for blockchain in lightweight IoT network," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.

[59] C.-W. Huang and Y.-C. Chen, "ZeroCalo: A lightweight blockchain based on DHT network," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 38–42.

[60] F. H. Pohrmen and G. Saha, *LightBC: A Lightweight Hash-Based Blockchain for Secured Internet Things*, vol. 1165. Singapore: Springer, 2021.

[61] Y. Yu, S. Zhang, C. Chen, and X. Zhong, "LVChain: A lightweight and vote-based blockchain for access control in the IoT," in *Proc. IEEE 4th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2018, pp. 870–874.

[62] M. S. Siddiqui, T. Ali, A. Nadeem, W. Nawaz, and S. S. Albouq, "BlockTrack-L: A lightweight blockchain-based provenance message tracking in IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 463–470, 2020.

[63] A. C. Connelly, S. A. R. Zaidi, M. Z. Shakir, and H. Ahmadi, "A lightweight permission-based blockchain for IoT environments," in *Proc. Int. Conf. U.K.-China Emerg. Technol. (UCET)*, Aug. 2020, pp. 1–4.

[64] S. Lee, J. Lee, S. Hong, and J.-H. Kim, "Lightweight end-to-end blockchain for IoT applications," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 8, pp. 3224–3242, 2020.

[65] A. H. Alkhazaali and O. Ata, "Lightweight fog based solution for privacy-preserving in IoT using blockchain," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2020, pp. 1–10.

[66] A. Prabhakar and T. Anjali, "TCON—A lightweight trust-dependent consensus framework for blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 1–6.

[67] M. Y. Ary Saputro and R. F. Sari, "Securing IoT network using lightweight multi-fog (LMF) blockchain model," in *Proc. 6th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2019, pp. 183–188.

[68] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang, "PCBChain: Lightweight reconfigurable blockchain primitives for secure IoT applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 10, pp. 2196–2209, Oct. 2020.

[69] W. Zhang, Z. Wu, G. Han, Y. Feng, and L. Shu, "LDC: A lightweight dada consensus algorithm based on the blockchain for the industrial Internet of Things for smart city applications," *Future Gener. Comput. Syst.*, vol. 108, pp. 574–582, Jul. 2020.

[70] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Microchain: A hybrid consensus mechanism for lightweight distributed ledger for IoT," 2019, *arXiv:1909.10948*.

[71] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–12, Nov. 2018.

[72] L. Xu, L. Chen, Z. Gao, S. Xu, and W. Shi, "EPBC: Efficient public blockchain client for lightweight users," in *Proc. 1st Workshop Scalable Resilient Infrastructures Distrib. Ledgers, Colocated ACM/IFIP/USENIX Middleware Conf.*, 2017, pp. 1–7.

[73] R. Doku, D. B. Rawat, M. Garuba, and L. Njilla, "LightChain: On the lightweight blockchain for the Internet-of-Things," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2019, pp. 444–448.

[74] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. H. Ahmed, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 20–24.

[75] 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.

[76] A. Albakri, L. Harn, and M. Maddumala, "Polynomial-based lightweight key management in a permissioned blockchain," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–9.

[77] Z. Yulong, N. Baoning, L. Peng, and F. Xing, *A Novel Enhanced Lightweight Node for Blockchain* (Communications in Computer and Information Science), vol. 1156. Singapore: Springer, 2020.

[78] R. A. Michelin, N. Ahmed, S. S. Kanhere, A. Seneviratne, and S. Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 3–5.

[79] J. An, J. Cheng, X. Gui, W. Zhang, D. Liang, R. Gui, L. Jiang, and D. Liao, "A lightweight blockchain-based model for data quality assessment in crowdsensing," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 1, pp. 84–97, Feb. 2020.

[80] M. T. Lwin, J. Yim, and Y. B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks," *Sensors*, vol. 20, no. 3, pp. 1–19, 2020.

[81] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, Mar. 2020.

[82] A. R. Shahid, N. Pissinou, C. Staier, and R. Kwan, "Sensor-chain: A lightweight scalable blockchain framework for Internet of Things," in *Proc. IEEE Int. Congr. Cybermatics, 12th IEEE Int. Conf. Internet Things, 15th IEEE Int. Conf. Green Comput. Commun., 12th IEEE Int. Conf. Cyber, Phys.*, Jul. 2019, pp. 1154–1161.

[83] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019.

[84] J. Guruprakash and S. Koppu, "EC-ElGamal and genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain," *IEEE Access*, vol. 8, pp. 141269–141281, 2020.

[85] B. Seok, J. Park, and J. H. Park, "A lightweight hash-based blockchain architecture for industrial IoT," *Appl. Sci.*, vol. 9, no. 18, p. 3740, Sep. 2019.

[86] N. H. Kim, S. M. Kang, and C. S. Hong, "Mobile charger billing system using lightweight blockchain," in *Proc. 19th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Sep. 2017, pp. 374–377.

[87] Y. Yu, S. Liu, P. L. Yeoh, B. Vucetic, and Y. Li, "LayerChain: A hierarchical edge-cloud blockchain for large-scale low-delay IIoT applications," *IEEE Trans. Ind. Informat.*, vol. 3203, no. 7, pp. 5077–5086, Jul. 2021.

[88] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A lightweight DAG-based blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5749–5759, Jun. 2020.

[89] N. V. S. R. Andola and V. Shekhar, "PoEWAL: A lightweight consensus mechanism for blockchain in IoT," *Pervasive Mobile Comput.*, vol. 69, Nov. 2020, Art. no. 101291.

[90] W. Tiberti, A. Carmenini, L. Pomante, and D. Cassioli, "A lightweight blockchain-based technique for anti-tampering in wireless sensor networks," in *Proc. 23rd Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2020, pp. 577–582.

[91] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, pp. 36868–36878, 2021.

[92] K. Li, Y. Yang, S. Wang, R. Shi, and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102189.

[93] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Tikiri—Towards a lightweight blockchain for IoT," *Future Gener. Comput. Syst.*, vol. 119, pp. 154–165, Jun. 2021.

[94] O. A. S. Ekanayake and M. N. Halgamuge, "Lightweight blockchain framework using enhanced master-slave blockchain paradigm: Fair rewarding mechanism using reward accuracy model," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102523.

[95] S. R. Cherupally, S. Boga, P. Podili, and K. Kataoka, "Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity," in *Proc. Int. Conf. Inf. Netw.*, 2021, pp. 267–272.

[96] S. Khan, W. K. Lee, and S. O. Hwang, "AEchain: A lightweight blockchain for IoT applications," *IEEE Consum. Electron. Mag.*, vol. 2248, pp. 1–12, 2021.
[97] D. Na and S. Park, "Fusion chain: A decentralized lightweight blockchain for IoT security and privacy," *Electron.*, vol. 10, no. 4, pp. 1–18, 2021.
[98] O. Naseer, S. Ullah, and L. Anjum, "Blockchain-based decentralized lightweight control access scheme for smart grids," *Arabian J. Sci. Eng.*, vol. 46, no. 9, Sep. 2021, Art. no. 0123456789.
[99] W. Lu, Z. Ren, J. Xu, and S. Chen, "Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1246–1259, Jun. 2021.
[100] C. Li, J. Zhang, X. Yang, and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102602.
[101] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.
[102] S. Biswas, K. Sharif, F. Li, I. Alam, and S. Mohanty, "DAAC: Digital asset access control in a unified blockchain based E-health system," *IEEE Trans. Big Data*, vol. 8, no. 5, Oct. 2020, Art. no. 61772077.
[103] B. Son, J. Lee, and H. Jang, "A scalable IoT protocol via an efficient DAG-based distributed ledger consensus," *Sustainability*, vol. 12, no. 4, pp. 1–11, 2020.
[104] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4134–4145, Jun. 2020.
[105] S. Park and H. Kim, "DAG-based distributed ledger for low-latency smart grid network," *Energies*, vol. 12, no. 18, p. 3570, Sep. 2019.
[106] L. Guo, J. Chen, S. Li, Y. Li, and J. Lu, "A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 576–587, Aug. 2022.
[107] T. Baker, M. Asim, H. Samwini, N. Shamim, M. M. Alani, and R. Buyya, "A blockchain-based fog-oriented lightweight framework for smart public vehicular transportation systems," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108676.
[108] Q. Yao, T. Li, C. Yan, and Z. Deng, "Accident responsibility identification model for Internet of Vehicles based on lightweight blockchain," *Comput. Intell.*, vol. 2021, pp. 1–24, May 2022.
[109] Z. Wang, R. Xiong, J. Jin, and C. Liang, "AirBC: A lightweight reputation-based blockchain scheme for resource-constrained UANET," in *Proc. IEEE 25th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2022, pp. 1378–1383.
[110] J. Doyle, M. Golec, and S. S. Gill, "BlockchainBus: A lightweight framework for secure virtual machine migration in cloud federations using blockchain," *Secur. Privacy*, vol. 5, no. 2, pp. 1–11, Mar. 2022.
[111] J. A. Guerra, J. I. Guerrero, S. García, S. Domínguez-Cid, D. F. Larios, and C. León, "Design and evaluation of a heterogeneous lightweight blockchain-based marketplace," *Sensors*, vol. 22, no. 3, p. 1131, Feb. 2022.
[112] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May 2022.
[113] Y. Jiang, X. Xu, H. Gao, A. D. Rajab, F. Xiao, and X. Wang, "LBlockchainE: A lightweight blockchain for edge IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 16, 2022, doi: 10.1109/TITS.2022.3157447.
[114] L. Vishwakarma, A. Nahar, and D. Das, "LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 5983–5994, Jun. 2022.
[115] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N. M. F. Qureshi, and C. Su, "Lightweight blockchain based remote mutual authentication for AI-empowered IoT sustainable computing systems," *IEEE Internet Things J.*, early access, Feb. 18, 2022, doi: 10.1109/JIOT.2022.3152546.
[116] V. Mardiansyah and R. F. Sari, "Lightweight blockchain framework for medical record data integrity," *J. Appl. Sci. Eng.*, vol. 26, pp. 91–103, Apr. 2022.
[117] B. Wang and X. Hu, "Lightweight blockchain system for resource-constrained IoT devices," in *Proc. 2nd Int. Conf. Internet Things Smart City (IoTSC)*, vol. 12249, F. Falcone, H. Cui, and X. Ye, Eds. Bellingham, WA, USA: SPIE, 2022, pp. 1–8.
[118] K. E. Bilami and P. Lorenz, "Lightweight blockchain-based scheme to secure wireless M2M area networks," *Future Internet*, vol. 14, no. 5, p. 158, May 2022.
[119] M. Gupta, R. B. Patel, S. Jain, H. Garg, and B. Sharma, "Lightweight branched blockchain security framework for Internet of Vehicles," *Trans. Emerg. Telecommun. Technol.*, pp. 1–30, Apr. 2022.
[120] S. Wadhwa and Gagandeep, "Lightweight modified consensus approach in IoT blockchain," in *Proc. Int. Conf. Emerg. Smart Comput. Informat. (ESCI)*, Mar. 2022, pp. 1–5.
[121] Y. F. E. Djéné, M. S. El Idrissi, P.-M. Tardif, B. El Bhiri, Y. Fakhri, and Y. K. Bekali, "Lightweight-blockchain for secured wireless sensor networks: Energy consumption of MAC address-based proof-of-authentication," in *Advanced Technologies for Humanity*, R. Saidi, B. El Bhiri, Y. Maleh, A. Mosallam, and M. Essaaidi, eds. Cham, Switzerland: Springer, 2022, pp. 182–192.
[122] M. A. Abdullah, O. H. Alhazmi, and K. Aloufi, "Securing Internet of Things environment using lightweight blockchain approach," in *Proc. 4th Int. Conf. Appl. Autom. Ind. Diag. (ICAAID)*, Mar. 2022, pp. 1–7.
[123] D. Zakariae, "A lightweight blockchain framework for IoT integration in smart cities," *Turkish J. Comput. Math. Educ. (TURCOMAT)*, vol. 12, no. 5, pp. 889–894, Apr. 2021.
[124] X. Qin, Y. Huang, Z. Yang, and X. Li, "LBAC: A lightweight blockchain-based access control scheme for the Internet of Things," *Inf. Sci.*, vol. 554, pp. 222–235, Apr. 2021.
[125] J.-L. Lee, P. BusiReddyGari, and B. Thompson, "A lightweight smart meter framework using a scalable blockchain for smart cities," in *Proc. IEEE 7th World Forum Internet Things (WF-IoT)*, Jun. 2021, pp. 433–438.
[126] X. Xu and J. Peng, "A lightweight two-layer blockchain mechanism for reliable crossing-domain communication in smart cities," 2021, *arXiv:2110.14860*.
[127] W. Li, M. He, W. Zhu, and J. Zheng, "A study on lightweight and secure edge computing based blockchain," in *Proc. IEEE 12th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2021, pp. 256–261.
[128] Z. Wang, L. Wang, F. Xiao, Q. Chen, L. Lu, and J. Hong, "A traditional Chinese medicine traceability system based on lightweight blockchain," *J. Med. Internet Res.*, vol. 23, no. 6, Jun. 2021, Art. no. e25946.
[129] A. A. Mamun, F. Yan, and D. Zhao, "BAASH: Lightweight, efficient, and reliable blockchain-as-a-service for HPC systems," in *Proc. Int. Conf. High Perform. Comput., Netw., Storage Anal.*, New York, NY, USA, Nov. 2021, pp. 1–18.
[130] H. Chai, S. Leng, J. He, K. Zhang, and B. Cheng, "CyberChain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4620–4631, May 2022.
[131] R. Zhang, M. Song, T. Li, Z. Yu, Y. Dai, X. Liu, and G. Wang, "Democratic learning: Hardware/software co-design for lightweight blockchain-secured on-device machine learning," *J. Syst. Archit.*, vol. 118, Sep. 2021, Art. no. 102205.
[132] Q. Xie, F. Dong, and X. Feng, "ECLB: Edge-computing-based lightweight blockchain framework for mobile systems," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Apr. 2021.
[133] F. H. Pohrmen and G. Saha, "LightBC: A lightweight hash-based blockchain for the secured Internet of Things," in *Proc. Int. Conf. Innov. Comput. Commun.*, D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds. Singapore: Springer, 2021, pp. 811–819.
[134] J. Yuan and L. Njilla, "Lightweight and reliable decentralized reward system using blockchain," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.
[135] N. Ding and Y. Zhao, "Lightweight blockchain based on storage resource optimization for Internet of Vehicles," in *Proc. IEEE Int. Intell. Transp. Syst. Conf. (ITSC)*, Sep. 2021, pp. 1063–1068.
[136] J. P. Mehare and M. M. Bartere, "Lightweight blockchain secured framework for smart precise farming system," in *Proc. Int. Conf. Comput. Intell. Comput. Appl. (ICCICA)*, Nov. 2021, pp. 1–6.
[137] D. Na and S. Park, "Lightweight blockchain to solve forgery and privacy issues of vehicle image data," in *Proc. 22nd Asia–Pacific Netw. Operations Manage. Symp. (APNOMS)*, Sep. 2021, pp. 37–40.
[138] H. H. Saeed, A. B. Masood, and H. K. Qureshi, "LSM: A lightweight security mechanism for IoT based smart city management systems using blockchain," *Int. J. Innov. Sci. Technol.*, vol. 3, no. 5, pp. 1–14, Dec. 2021.

[139] H. Materwala and L. Ismail, "Secure and privacy-preserving lightweight blockchain for energy trading," in *Proc. 8th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2021, pp. 394–399.
[140] X. Zhang, R. Li, W. Hou, and H. Zhao, "V-Lattice: A lightweight blockchain architecture based on DAG-lattice structure for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 2021, pp. 1–17, May 2021.
[141] A. D. Dwivedi, R. Singh, S. Dhall, G. Srivastava, and S. K. Pal, "Tracing the source of fake news using a scalable blockchain distributed network," in *Proc. IEEE 17th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Dec. 2020, pp. 38–43.
[142] M. Divya and N. B. Biradar, "IOTA-next generation block chain," *Int. J. Eng. Comput. Sci.*, vol. 7, no. 4, pp. 23823–23826, Apr. 2018.
[143] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.
[144] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (Hyperledger Fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 253–255.
[145] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of used cryptography in blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.
[146] D. Mourtzis, E. Vlachou, and N. Milas, "Industrial big data as a result of IoT adoption in manufacturing," *Proc. CIRP*, vol. 55, pp. 290–295, Jan. 2016.
[147] J. Truby, "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy Res. Social Sci.*, vol. 44, pp. 399–410, Oct. 2018.
[148] X. Liu and N. Ansari, "Toward green IoT: Energy solutions and key challenges," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 104–110, Mar. 2019.
[149] C. Cachin, "Blockchain, cryptography, and consensus," *Electron. Proc. Theor. Comput. Sci.*, vol. 261, pp. 1–63, Nov. 2017.
[150] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021.
[151] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102355.
[152] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

DENIS STEFANESCU received the bachelor's degree in computer engineering from the University of the Basque Country (UPV/EHU), Spain, in 2019, and the master's degree in cybersecurity from the Open University of Catalonia, Spain, in 2020, with an excellent average grade (9.2 out of 10). He is currently pursuing the Ph.D. degree with the IKERLAN Technology Research Centre, Basque Research and Technology Alliance (BRTA), Arrasate-Mondragon, Spain.

His current research interests include cybersecurity, blockchain, the Internet of Things (IoT), industry 4.0, and edge/fog/cloud computing. He received the award for the best academic record.

LETICIA MONTALVILLO received the B.S. and M.S. degrees in computer science from the University of Mondragon (MU), and Polytechnic University of Catalonia BarcelonaTech (UPC), respectively, and the Ph.D. degree *(cum laude)* in computer science from the University of the Basque Country (UPV/EHU), in 2018, with international mention.

After a Pre-doctoral stay at Danfoss Drives, where she had the opportunity to get industrial insights and partially validate her research on Software Product Lines (SPLs). She has been working for IKERLAN, since 2018. She is a member of the Cybersecurity in Digital Platforms Team. Her research interests include software product lines (SPLs) and variability management, secure software development life cycle (S-SDLC), industry 4.0, cybersecurity in cloud/digital platforms, and blockchain applicability for industry 4.0 use cases. She participates in European funded projects, and she carries out technology transfer projects in aforementioned areas. She is the coauthor of peer-reviewed research articles, published in international conferences and JCR journals. She also serves the community as a reviewer in international conferences.

PATXI GALÁN-GARCÍA received the Ph.D. degree in computer science and telecommunications doctoral program from Deusto University *(cum laude unanimously)* with international mention, in 2016.

After a Pre-doctoral stay at the Department of Human Language Technology and Pattern Recognition, RWTH University of Aachen, Germany, directed by Prof. Hermann Ney. His research interests include NLP focused on cybersecurity, big data, bioengineering, machine learning, mobile platforms, the fog IoT, social network monitoring, semantic web, industry 4.0, data analysis and smart elements for people, mobile devices, and energy or cities. In the last four years, in private companies, he has carried out projects related to big data, blockchain, digital identity, supply chain traceability, natural language processing, industry 4.0, and smart network security. He has participated as the author in research articles, some of them Q1, published in national and international conferences and articles in JCR journals.

JUANJO UNZILLA received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in communications engineering from the UPV/EHU, in 1990 and 1999, respectively.

He was the Head of the Electronic and Telecommunications Department, from 2001 to 2004, and the Vice-Chancellor of UPV/EHU, from 2004 to 2013. He is currently a Professor with the Communications Engineering Department, UPV/EHU, where he teaches subjects related to telecommunication networks and services. He is a member of the I2T Research Laboratory, where he participates in several regional, national, and European Research and Development projects. His research interests include SDN and NFV in 5G networks, its applications to industrial communications, and cybersecurity in distributed systems. He is one of the co-founders of the spin-off Keynetic focused on cybersecurity services to SMEs, in 2017.

AITOR URBIETA received the Ph.D. degree *(cum laude unanimously)* in computer engineering from the University of Mondragon, in 2010, with international mention.

He has been with IKERLAN, since 2007, where he currently leads the Cybersecurity in Digital Platforms Research Team. His current research interests include cybersecurity in digital platforms, the Internet of Things (IoT), cybersecurity in communication protocols, blockchain, end-to-end security, vulnerability monitoring, threat detection, fog computing, edge computing, the IoT environment validation, and middleware. He has participated as the author or coauthor in more than 20 scientific publications in the previously mentioned areas, some of them Q1, published in national and international conferences and articles in JCR journals.