sciendo

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **23**, No 1
Sofia • 2023 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2023-0001

Blockchain-Fog Computing Integration Applications: A Systematic Review

Yehia Ibrahim Alzoubi[1], *Ali Aljaafreh*[2]

[1]*Department of Management Information Systems, American University of the Middle East, Kuwait*
[2]*Department of Management Information Systems, Mutah University, Jordan*
E-mails: yehia.alzoubi@aum.edu.kw Ali.jaafreh@mutah.edu.jo

Abstract**:** *The Fog computing concept has been introduced to aid in the data processing of Internet of things applications using Cloud computing. Due to the profitable benefits of this combination, several papers have lately been published proposing the deployment of Blockchain alongside Fog computing in a variety of fields. A comprehensive evaluation and synthesis of the literature on Blockchain-Fog computing integration applications that have emerged in recent years is required. Although there have been several articles on the integration of Blockchain with Fog computing, the applications connected with this combination are still fragmented and require further exploration. Hence, in this paper, the applications of Blockchain-Fog computing integration are identified using a systematic literature review technique and tailored search criteria generated from the study objectives. This article found and evaluated 144 relevant papers. The findings of this article can be used as a resource for future Fog computing research and designs.*

Keywords**:** *Blockchain, Fog, applications, classification, solution.*

1. Introduction

Cisco has introduced Fog Computing (FC) in 2012 to improve network architecture and fulfill the demands of huge amounts of data to be processed on the Cloud [1]. To put it another way, FC was created to help solve and overcome problems associated with Cloud computing, like the Internet of Things (IoT) applications with location awareness, Cloud-to-IoT device connectivity, and low response time [2]. FC is a Cloud-near-ground architecture that enables storage, administration, and communication with IoT devices. As a result, FC serves as a communication intermediary between IoT devices and the Cloud; nevertheless, it does not replace the Cloud [3]. Moreover, FC empowers and offers IoT devices with on-demand apps and services [4]. Furthermore, FC nodes enable IoT devices to do analysis and processing that requires more power and resources, reducing reaction time and meeting the delay-sensitive requirements of particular IoT applications [5].

Because the FC is a Cloud computing extension, it inherits some of the Cloud's issues. Due to FC's resource-constrained capabilities, the most noticeable limitations

are security and privacy concerns [6]. As a result, FC should give excellent solutions and approaches to safeguard IoT devices that work with it [7]. Due to a lack of resources and storage, as well as unique characteristics like decentralized structure, mobility, and several Fog node providers, the most effective Cloud computing solutions will not be applicable in FC [8]. Due to these constraints, a new set of challenges regarding FC's scalability capability has arisen [9]. Accordingly, new novel alternatives have been presented, with BlockChain (BC) being the most promising way to overcome FC restrictions [10, 11].

The BC technology, a distributed Peer-to-Peer (P2P) connected construction, may be utilized to avoid double-spending by addressing the issue of transaction order [12]. Bitcoin organizes transactions into a constrained-size structure called blocks that comprise timestamps [13]. The nodes (miners) in the network are responsible for connecting the blocks in chronological sequence, where every block contains the previous block hash to construct a BC [14]. As a result, the BC structure can maintain a reliable and auditable record of all transactions [15]. Since BC operates in a decentralized and untrustworthy manner, traditional enterprises that depend on centralized authority have been seriously impacted [16]. Security, robustness, transparency, and auditability are all intrinsic aspects of BC. Companies investing in BC are enabled to decentralize their infrastructures and lower transaction costs by enhancing transparency and strengthening security [11]. Several governments have included BC in their future informatization plans (e.g., China, USA, India, and South Korea), advocated for BC development in their public sectors, and have begun developing BC pilot projects in key industries. In China, BC has just begun to emerge as an essential framework for COVID-19 control. Chinese hospitals employ BC technology in various areas, including electronic health records, insurance claims, supply chain tracking, and detecting fake drugs [17]. BC may be used to support COVID-19 vaccination studies and analyze disease outbreak patterns, among other things. As a result, BC technology is regarded as the fourth network computing milestone [18].

Many studies consider BC one of the most effective ways of dealing with FC problems. However, there is a wide range of publications in this field. Although some studies review past research (e.g., [16, 19, 20]), they do not conduct a critical evaluation or classify the results using well-defined criteria. Furthermore, most of the survey articles are focused on a single application (e.g., eHealth, IoT, vehicles, and so on). While there have been several studies of BC technology, the state-of-the-art of BC-FC (BCFC)-enabled applications have gotten little attention. The lack of a clear and thorough review of existing BCFC-enabled applications is the key motivation for this study. Recent research published in the public domain (at least at the time this study has been undertaken) that systematically reviews the available literature regarding the applications of BCFC integrating are limited, to the best of the authors' knowledge. Therefore, this paper aims to address this in particular by answering three questions: (1) What is the evolution of BCFC-based apps over time? (2) What are the obstacles to BCFC integration and what are the future directions?

This research leads to a better understanding of BC characteristics and gives a glimpse of existing BCFC-enabled applications from various industries. This paper

emphasizes the increased academic attention and outlines the following contributions using a content analysis technique. First, this article provides a categorization of wide variations of BCFC applications in a variety of industries. This study is based on a thorough examination of each of the papers that have been selected using well-defined and justified criteria. The literature on BCFC integration is quite diverse; collecting the pertinent information systematically is not an easy undertaking [21]. The BCFC has eight primary domains that have been discovered; IoT, transportation, eHealth, computational resource providers, energy, video streaming, financial, and global collaboration. Second, this paper lays forth a road map of potential research topics, issues, and opportunities for which more research is needed to assist researchers. This was accomplished by addressing the limits of peer-reviewed articles and identifying some unresolved concerns in infrastructure, platform, and technological restrictions of BC design that have an impact on processes in specific fields. This paper is far from complete since BC technology continues to improve at a dizzying pace.

The remainder of this paper is organized as follows. The background of BC is presented in Section 2. The study design is discussed in Section 3. The descriptive findings are discussed in Section 4. The BCFC integration applications are discussed in Section 5. The outstanding questions and study limitations are discussed in Section 6. This paper comes to a close with Section 7.

2. Research background

2.1. Fog computing background

According to K h a n et al. [22], edge computing includes three aspects: FC, Cloudlets, and Mobile edge computing. Edge computing is a self-contained computing paradigm that consists of a large number of dispersed heterogeneous gadgets that interface with the network and execute computational functions such as data processing and storage. These duties can also aid in the provision of lease-based solutions, in which a user leases a gadget and receives incentives in exchange. FC, according to Cisco, is an extension of Cloud computing that extends Cloud services and resources to the edge network (i.e., IoT devices). FC specifically relies on Cisco-designed gear that has computing capability in addition to standard device functions such as switches and routers. Mobile edge computing and Cloudlet are intended to deliver services solely to mobile users who have the option of using resources available locally. The definitions of edge computing and FC demonstrate that both technologies are conceptually similar, and as a result, the literature uses FC and edge computing interchangeably. Accordingly, this research investigates studies that have reported either FC or edge applications with BC. Furthermore, Cloudlet and Mobile edge are both parts of edge computing, therefore to extend or search, both FC and edge-related research have been considered.

2.2. Blockchain background

In concept, a BC should be considered a decentralized append-only time-stamped data construction [16]. BC enables the creation of dispersed untrustworthy P2P

networks, where individuals may connect in a verified way with no need for an authenticator [16]. Immutable ledger, transparent and public ledger, and anonymity of BC users are three requirements for BC construction. The body and the header of the block, which include the transactions list, are both included in the BC [19]. The block header contains several data, including the block size, a date, the number of transactions, and the version number. The Merkle root field represents the hash value of the current block. The previous block hash and all transactions are normally included in the BC, allowing for a cross-border distributed trust environment [23]. While trusted persons or centralized authorities can be corrupted, interrupted, or hacked, transactions in BC's public ledger are certified by a majority consensus of miner nodes participating in the validation process. The transaction data is recorded in a ledger that cannot be deleted or modified after it has been validated by a consensus (data are immutable) [24]. The BC communications are handled by Fog nodes, which are decentralized and scattered across the network. Each block in the BC is connected to the chain in a certain order. All nodes in the BC environment are connected to the network and maintain a local copy of the transaction data [23]. Before a miner node adds the confirmed transaction into a timestamped block, all parties involved mutually authenticate the transaction to reach a consensus decision. Then it transmits it to the rest of the network. For consistency, these data are updated regularly across all nodes [17]. This allows a large number of nodes that do not trust each other to reach authentication choices based on previous transactions. A public ledger maintains the verified transactions in a P2P network in the BC environment [16].

BC has several advantages including protection against single points of failure, a decentralized and trustless P2P system, salable and high speed and capacity technology, a secure and auditable approach, and the use of lightweight protocols that help IoT devices with limited resources and storage because it does not require third-party verification [16, 17, 19, 23, 25]. Even without centralized management or data storage, BC can thwart many threats. Accordingly, many applications presently rely on this technology rather than cryptocurrencies, such as FC-based apps, which are the subject of this study.

A consensus mechanism or algorithm is the technique by which a BC network obtains consensus. Because there is no central authority, the public BC (i.e., decentralized) is built as a distributed system, with dispersed nodes utilizing a consensus algorithm to agree on the legitimacy of transactions [18]. To put it another way, BC relies on distributed consensus to validate transactions, ensuring their consistency and integrity. Varied consensus processes have different effects on the BC system. The best (idealistic) consensus method advocates giving all miners the same weight in the validation process and then deciding by majority vote. The Proof-of-Work (PoW) is the most well-known consensus mechanism. To provide authenticity and verifiability, PoW requires performing a complex computational method, such as finding hashes with specific patterns [26]. Proof-of-Stake (PoS) algorithms divide stake blocks as per the miners' current wealth [23]. Other well-known consensus mechanisms include Byzantine Fault Tolerance (BFT) and its variations [25].

2.3. Blockchain types

There are several sorts of BCs based on the data that is handled, the availability of that data, and the activities made. As a result, public, private, and consortium BCs can be recognized [17]. Anyone on the Internet may see the ledgers of the BC, and anyone can contribute or confirm a block of transactions to the BC [27]. A public BC is a typical BC in which any participant may participate in the consensus process, retain a copy of the ledger, and freely query the ledger's transaction data. It is not feasible to utilize public BC in a business network since it is unable to secure secrets and has poor performance [28]. Only particular employees inside the business may verify and add transaction blocks to private BCs, but these transactions can be accessed online by them. A private BC is nearly entirely controlled by a single company, resembling a centralized design. It has weak scalability and the contents of the log may be modified by this company, despite providing strong access security and performance [11]. Only a small set of organizations (such as banks) may check and add transactions in consortium BC, although the ledger can be restricted or opened to a certain group. For the data exchange situation, the consortium BC is the ideal option. Members require authorization to use the BC, and they use a stable consensus mechanism that outperforms the public chain to provide justice in a mutually untrustworthy setting. Identical account information is given to each member [16].

Public BC implementations include Ethereum, Bitcoin, Litecoin, and, in general, most cryptocurrencies. The lack of infrastructure investments as well as the low administrative expenses are two of their most important advantages [13]. Private BC is often used in database management and auditing. Multichain is an open-source framework for creating and deploying private blockchains. Finally, in manufacturing and industrial organizations, such as the Hyperledger project, consortium BC is widely employed. Because BC technology is still in its infancy, efforts are continually being made to establish and improve BC platforms, such as Ethereum, which has just published tools for creating federated BCs [17].

2.4. Blockchain platforms

Many BC platforms have been discussed in the literature. The focus of this section will be on the distributed ledger BC that can meet the requirements of FC with distributed nature. In the following paragraphs, the well-known distributed ledger BC platforms are discussed [29-32].

- Bitcoin, which is the first and most frequently utilized dispersed cryptocurrency, maintaining a P2P network with no centralized authority and has exposed to the world to the BC innovation and platform. The BC network manages transactions and issues currency collectively. Because of Bitcoin's breakthrough, numerous additional alternative cryptocurrencies have been suggested and built. MultiChain, which is a private BC that may be used within or between businesses. MultiChain is an expanded open-source derivative of Bitcoin with substantial flexibility, access control, high reliability, and native commodities and bitstreams. Dash (or Digital Cash) is another extension of Bitcoin that prioritizes anonymity and allows for quick transactions. Peercoin, another extension of Bitcoin, has been

created to lower the amount of energy needed for currency mining owing to the use of the Proof-of-Work (PoW) consensus algorithm. To overcome this issue, Peercoin uses Proof-of-Stake (PoS), which may be a viable option on a public network.

- Ethereum is a platform that allows anybody to create and use BC-based smart-contract decentralized apps. Ethereum offers smart contracts to make the design of asset management easier than Bitcoin-based applications. Hydrachain is an Ethereum platform plugin for creating private ledgers. OriginTrail is yet another Ethereum extension that is used to communicate supply chain data. Streamr is another Ethereum extension that is used to exchange data in real-time. Streamr provides a worldwide data marketplace for users to purchase and sell data. Atonomi is another Ethereum extension that aims to develop secure IoT systems by providing an identification process. Grid+ is another Ethereum extension that has been created for use in the electricity industry, allowing intelligent power operators to pay power bills in real-time. HydraChain is an open-source Ethereum extension that also allows for the creation of permissioned distributed ledgers. HydraChain allows various components of the system to be readily changed based on client requirements. It provides a variety of tools that allow for faster development while also enhancing troubleshooting abilities. Quorum is an Ethereum-based BC platform that has been designed to make the creation of Ethereum's BC apps easier. Quorum is a great alternative for situations where transaction throughput and time are critical.
- Zcash is an open-source decentralized cryptocurrency that provides more transaction confidentiality than Bitcoin.
- Litecoin is a worldwide payment system that is decentralized. The main difference between Litecoin and Bitcoin is that Litecoin transaction time is 4 times faster than Bitcoin.
- Ripple processes transactions quicker than Bitcoin, which atomically resolves and records transactions. Ripple uses the Ripple consensus mechanism instead of Bitcoin's sluggish PoW algorithm, and blocks are only certified by a small number of validators miners to enable low-latency transactions.
- Monero is a permissioned, anonymous cryptocurrency by obfuscating the generators, routes, and quantities of transactions through the use of "Ring Confidential Transactions" (an algorithm that creates a collective signature to make real signatory unrecognizable) and "Stealth Address" (a one-time location for each transaction) technologies.
- Hyperledger is an open-source collaborative project designed to promote permissioned BC. Hyperledger offers an environment that includes a variety of modules and frameworks, each of which supports a particular form of consensus mechanism.
- Lisk is an open-source BC platform that facilitates the development of decentralized apps. Lisk allows users to create personal BCs, known as sidechains that store all data created by a decentralized application.
- Libra BC is a decentralized open-source platform that is programmable to provide a robust environment to meet financial needs. It makes it easier to create smart contracts by utilizing Move, a new programming language.

- The Internet Of Things Application (IOTA) is a decentralized cryptocurrency focused mainly on IoT; unlike Ethereum and Bitcoin, IOTA's data model is an acyclic-directed graph instead of a BC. Rather than utilizing miners to record transactions in blocks, every IOTA node works as a miner, and new transactions must approve two prior unconfirmed transactions before they may be approved. This indicates that network performance scales linearly according to the number of transactions sent. Since IOTA does not have throughput constraints or transaction fees, it is a suitable choice for IoT applications. IoT Chain and Hyundai Digital Asset Currency (HDAC) are other platforms designed to provide a lightweight system for satisfying the security and scalability requirements of IoT devices. Another platform built for IoT applications is Hedera Hashgraph, which uses directed acyclic networks with an asynchronous Byzantine Fault Tolerance (BFT) consensus mechanism to safeguard the system against intrusions.

Many platforms have been established for various objectives, as seen in the brief overview. Ethereum, Multichain, and Hyperledger are at the top of the list of platforms that are expected to continue to be used for FC applications since they integrate the most significant characteristics at the time.

3. Research methodology

A Systematic Literature Review (SLR) technique is used based on the principles set to find the applications of installing BC in FC. SLR is used to find, select, and synthesize relevant material to address a research topic [33]. The SLR methodology is critical for guiding the review process and providing a framework for comprehending BCFC-based applications [34]. To validate the categorization procedure of this publication, a review protocol has been devised. There are three stages: (1) locating studies, (2) selecting and evaluating studies, and (3) data extraction and synthesis.

3.1. Locating studies

The following seven well-known electronic databases have been used in this review. These databases are expected to provide enough literature coverage for this paper. IEEE Xplore, Elsevier ScienceDirect, Wiley Online Library, SpringerLink, Google Scholar, MDPI Online, SAGE Publication, ACM Digital Library, and Emerald Insight. Using the Boolean "AND" and "OR" operators, all potential combinations of BC, FC, and edge computing have been searched in the first step (i.e., FC OR edge computing AND BC). Because several writers refer to FC as edge computing, edge computing has been included in the search criteria. Peer-reviewed journal articles and conference proceedings are among the papers chosen. The steps of the review process, as well as the number of publications discovered at each stage, are depicted in Fig. 1. Any paper that explores BC as a method utilized in FC or edge computing has been included in this review for the reasons discussed in Section 2.1. This evaluation includes papers up to August 2021, including qualitative, quantitative, and mixed-methods investigations, as well as overview and review studies. Prefaces, poster sessions, editorial debates, news, article summaries, and reader's letters are not included in the search.

3.2. Study selection and evaluation

To save the selected studies, EndNote is utilized as a citation manager tool. In addition, in the first step, the backward snowball sampling strategy has been employed to find additional studies by searching the reference lists of the selected articles. There are 557 hits as a consequence of the first stage. The applied exclusion criteria include [34]:

1. The study must be written in English.
2. The research should not be repeated.
3. If the title does not explicitly describe BCFC integration.
4. If there is no mention of BCFC integration in the abstract.
5. If the full-text screening does not include a discussion of BCFC integration or a specific application of BCFC integration.

Separately, the 557 papers have been imported into EndNote and an Excel file. In the first step, the number has been reduced to 521 after removing non-English written and duplicated studies. The titles of the selected papers have been examined in the second step. Papers that were unrelated to BCFC integration have been omitted. Some titles, however, have been unable to be properly recognized and have been thus included in the next review round. Because of the study's title, 73 studies have been eliminated. Furthermore, another 147 studies have been eliminated after evaluating the abstracts of the selected papers. At this point, 301 studies have been recognized as being related to the study's objectives. In the third step, all potential studies have been subjected to a full-text review. 157 articles have been eliminated at this stage because they do not report on the BCFC integration or do not investigate any applications, leaving 144 papers for the final level of inclusion.

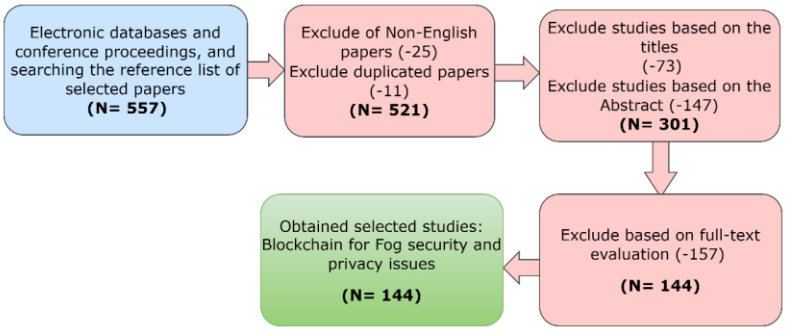


Fig. 1. Study selection process

3.3. Data extraction

All papers that matched the requirements for inclusion have been uploaded to MAXQDA11, a qualitative analysis program, and the data have been evaluated for emergent themes. Thirteen categories have been identified in this stage. All 144 articles included in the thematic analysis, as well as one set of categories and subcategories, have been agreed upon by all writers. The 144 selected studies (30-173) as indicated in Table 1, are addressed in the following sections. The thematic analysis of 144 papers have resulted in the identification of eight areas of BCFC-based applications. A large portion (i.e., 70 papers) discusses IoT applications followed by transportation

and eHealth applications. Monitoring and management, as well as energy applications, have gotten a lot of attention from scientists in recent years. Furthermore, four miscellaneous applications (applications that do not fit into any of the aforementioned categories) have been identified that emphasize BCFC technology's multidisciplinary potential.

Table 1. Selected study channel

Domain (144)	Study	
IoT (71)	[35-105]	
Transportation (28)	[106-133]	
eHealth (15)	[134-148]	
Energy (6)	[149-154]	
Computational resource providers (8)	[155-162]	
Video streaming (2)	[163,164]	
Financial (2)	[165,166]	
Global collaboration (6)	[167-172]	
Other (6)	Multimedia IoT	[173]
	Education	[174]
	Social Network	[175]
	Agricultural supply chain	[176]
	Robots	[177]
	Smart Applications	[178]

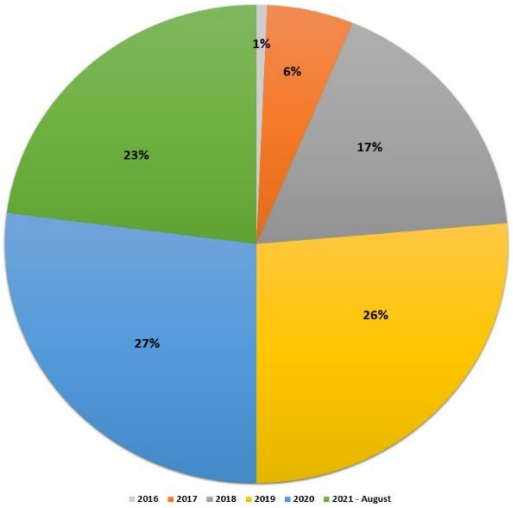


Fig. 2. Publication year-distribution

4. Descriptive analysis

The study looks at 144 academic publications that have been published between 2016 and August 2021. The descriptive analysis serves several purposes such as it gives intriguing insights into existing BC technology trends and how it is used; identifies gaps in the literature; facilitates the presentation of many research approaches that have been developed in the academic literature to date, and reinforces the categorization structure described in Section 5. Two criteria are used in the

descriptive analysis to classify the available literature: time and subject area distribution of publications, and the number of publications across time.

The IEEE Xplore database have provided the bulk of the studies (87), followed by Elsevier ScienceDirect (17 studies). The smallest number of studies (i.e., two) have been obtained from SAGE Publication. With 19 research, the Internet of Things Journal (IEEE Xplore) has the most BCFC integration papers. The majority of the research included are journal articles (104), with 38 conference pieces and only two book section articles following. The number of BCFC publications over time is seen in Fig. 2. While only one research has been released in 2016, the number of studies published each year is steadily increasing. This shows that BCFC is a new field that is just getting started. It also shows that interest in such new technology is growing these days.

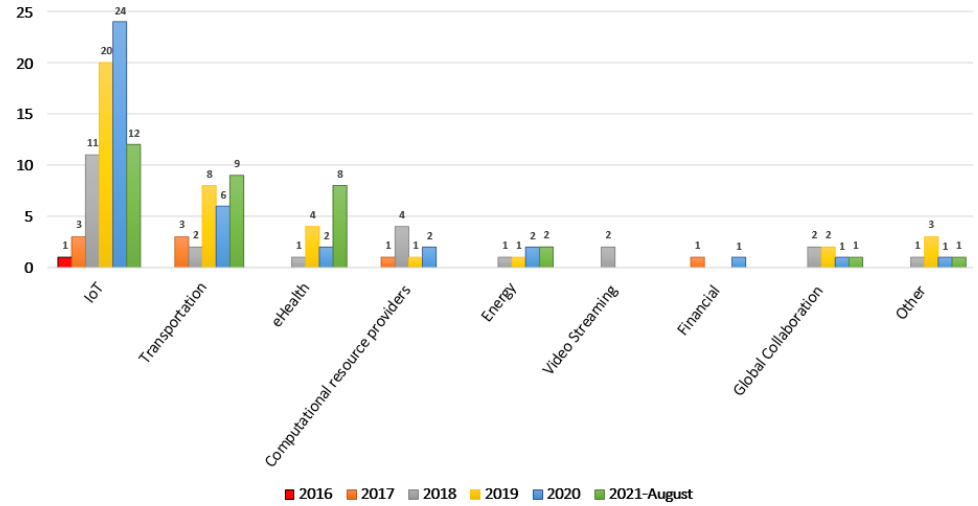


Fig. 3. Year-wise analysis of the selected studies domains

Fig. 3 shows a year-by-year examination of the papers that have been chosen. It's worth mentioning that the research focus is on IoT and transportation applications up until 2020. In 2021, however, the focus is on other applications such as eHealth, in addition to IoT and transportation. Furthermore, just one study addressing the possibility of BCFC integration in IoT has been released in 2016. As a result, during the last few years, research in the area of BCFC uses has slowly but steadily increased. This increased trend emphasizes the new and developing character of BC technology in FC, as well as the expanding academic interest in the province. Even though BC technology has been established with Bitcoin as its primary underlying concept, it has taken the research community many years to fully comprehend BC's capabilities and capitalize on its future uses. Unsurprisingly, BC has been thought of as a synonym for Bitcoin throughout its early years, and rather than adopting cutting-edge technology, researchers have concentrated on creating a foundation for applications [13]. Accordingly, publication material about BC-enabled apps has been extensively released since 2016.

5. RQ1: BC-Fog computing applications

Several apps, recently, have begun to use BC technology. BC has begun with Bitcoin (BC 1.0), then has moved on to BC 2.0, which includes smart contracts, and eventually has progressed into efficiency and coordination applications (BC 3.0) [179]. An application-oriented categorization approach is used in this paper since the focus is to identify BCFC's applications. The method used in this paper varies from other comparable studies as it employs, based on the literature, a robust scientific technique, making it more relevant to present BC advancements and illustrating future BC trends with great fidelity. As a result, a more thorough classification of BCFC-based applications is proposed, which is visually depicted in Fig. 4.

5.1. IoT devices

By enhancing, streamlining, and automating business processes, BCFC can become a significant source of innovative management and business concepts [99]. BCFC applications appear to provide significant performance and commercialization prospects while saving time and money [101]. BCFC integration involves, currently, a range of purposes for IoT devices. The BCFC capabilities are driving the increased interest and investment in creating decentralized IoT systems [180]. The primary aim of BCFC-based applications in the IoT environment is to enable secure and auditable data interchange in a heterogeneous context-aware situation with a great number of networked smart gadgets. To secure data interchanges in the IoT era, several authors have proposed BCFC architectures [38, 44, 62, 81, 97, 98, 100, 104, 181].

C e c h, G r o ß m a n n and K r i e g e r [62] utilize BCFC architecture to handle the problem of safely archiving and sharing sensing data. The MultiChain BC architecture has been utilized by the authors to link it to the virtual flexible FC gateway. As a result, this approach allows non-sensitive content to be readily accessible whilst limiting access to sensitive data. S i n g h et al. [81] have presented a secure BCFC architecture in which authentication, encryption, and BC are all employed to safeguard sensitive data. BC technology has been utilized to reduce energy and latency usage while simultaneously boosting security. L a l l a s, X e n a k i s and S t a m o u l i s [98] employ BCFC for real-time defect prediction and machinery supervision, in which computationally heavy tasks are distributed across fog nodes and data fusion constraints are defined and controlled by the cloud. J a n g et al. [97] introduce a BCFC architecture for IIoT that eliminates data fabrication by converting existing centralized database approaches to decentralized forms based on BC. Users are moved to the cloud to ensure their stability and integrity. To reduce network latency, the authors suggest employing a fog node to perform transaction verification and smart contracts. K u m a r et al. [100] utilize two AI techniques, random forest, and XGBoost, to provide total freedom in decision-making capabilities to the suggested security model. The authors introduce a distributed system based on BCFC to detect DDoS attacks. R e n et al. [181] have devised a method for increasing the security and reliability of stored data by merging BCFC with regeneration coding. A global BC is then formed in the cloud, while for IoT terminals, the local BC is generated to enable second validation. After the data is

stored in the cloud, it can be inspected and checked against the data in the local BC, for further increasing data protection.

According to Shahbazi and Byun [104], BC can transform manufacturing systems from cloud-centric to distributed FC design. The BC technology is used in their proposal to transmit data and perform manufacturing systems transactions, while the machine learning method provides for increased data analysis of a huge industrial dataset. Cinque, Esposito and Russo [57] have described how to employ BCFC to establish a federated trust management system in which fog nodes assist sensor nodes to provide trust provision and computation. Jayasinghe et al. [72] have introduced TrustChain, a privacy-preserving BC that combines the capabilities of BCs with trust principles to tackle concerns with existing BC designs. TrustChain is created in such a way that it only keeps data that clients have been permitted to save. Encryption and anonymization techniques are used to protect pertinent data. Misra et al. [36] suggest utilizing a private BC to deploy the SDN in the fog to thwart such real-time adversarial assaults on controllers. If the miners uncover improper flow rules, BC allows the SDN fog nodes to return to an earlier flow rule while reporting the offending controller. The authors also have suggested encrypting the material before putting it into the blocks to protect it from unwanted users. Similarly, Muthanna et al. [58] suggest a BCFC architecture that employs an SDN to provide high availability and security for delay-sensitive apps. BC has been utilized to ensure the safety of decentralization. Using game theory, Casado-Vara et al. [74] present an architecture that combines BC and FC to improve the quality of data collected by IoT devices. To do this, Casado-Vara et al. [74] have developed a distributed and self-organized cooperative algorithm, that analyzes the collected data. In addition, to increase data security, a BC-based architecture is proposed.

Moreover, the network's great resource management and scalability are enabled by functioning in an autonomous and decentralized manner. Wang et al. [60] look at techniques for sharing resources between the Cloud users and the Fog node. The suggested approach uses BC's incentive and punishment system to motivate Fog nodes to donate resources actively. Lei et al. [65] have introduced Groupchain (using PoW and PBFT consensus mechanisms), a novel scalable BCFC architecture using public BC with a two-chain structure that is appropriate for IoT services computing. Baouya et al. [67] propose a BCFC device control that is scalable and capable of delivering trust on-demand modifications with minimal impact on IoT resources. By opportunistically combining BC with Software Defined Networks (SDN) and container orchestration technologies, Ceccarelli et al. [103] have studied how to handle dispersed trust information and allow trusted configuration operations in the Industrial IoT (IIoT). Seitz et al. [96] have demonstrated the IIoT Bazaar, a distributed marketplace for commercial edge apps that employs BC to ensure transparency and app installation tracking for all parties. Núñez-Gómez, Caminero and Carrión [94] propose a novel architecture dubbed Heterogeneous, Interoperable, and DistRibuted Architecture (HIDRA) based on an Ethereum BC implementation aiming at resource orchestration in FC-IoT applications. Pan et al. [77] propose an EdgeChain framework (BIoT-based

architecture) that employs a credit-based resource management mechanism using smart contracts to control the behavior of IoT devices by enforcing regulations.

BC interoperability allows for autonomous and secure processes [46, 66, 79], which may be used to improve conventional transportation networks or e-commerce platforms, and key management in IoT [132]. BC interoperability refers to the capacity of multiple BC protocols to actively interact with one another. As a result, multiple chains may communicate and share data. This will enable resource sharing, which is a necessary element of BCFC compatibility [182]. Rahman et al. [68] recommend a BCFC infrastructure to provide secure and private smart contract services for the long-term economy that depends on IoT in smart cities. Kumar et al. [93] employ two Artificial Intelligence (AI) approaches, Random Forest (RF) and XGBoost, to offer the proposed security framework full autonomy in decision-making skills. Furthermore, a decentralized and secure P2P approach is employed to improve the security of wireless sensors and IoT networks allowing for greater management of these networks [70]. Kumar et al. [100] propose the BlockEdge, a BCFC-based framework to address some of the existing IIoT challenges. Ren et al. [181] have developed a technique combining BC and regeneration coding to increase the security and dependability of stored data. Shahbazi and Byun [104] have deployed BCFC to improve data integrity by approving key validation.

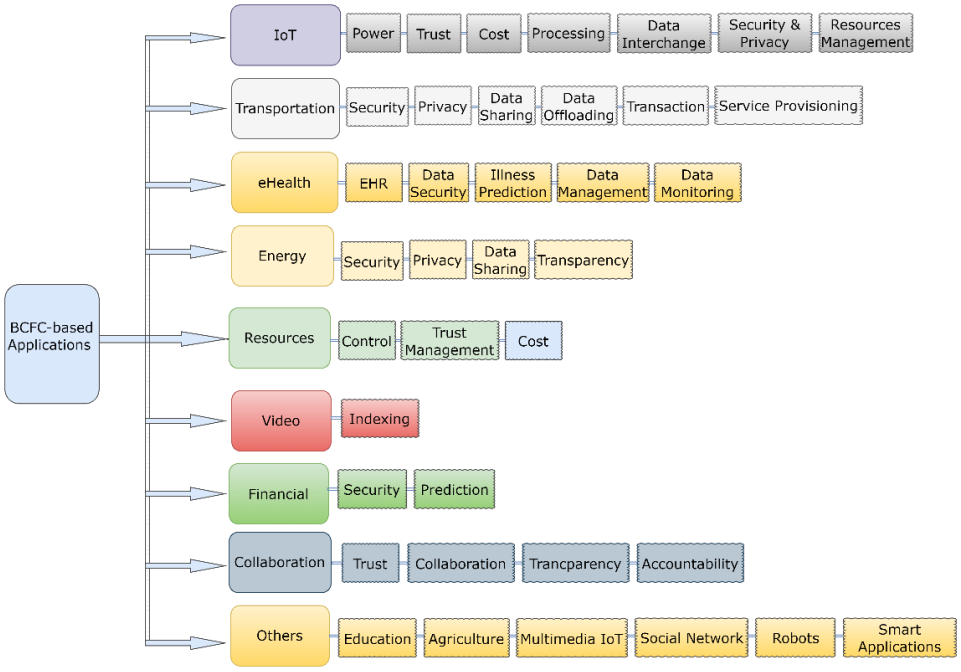


Fig. 4. BCFC-based applications taxonomy

Moreover, BCFC can enhance privacy-preserving [90] and privacy validation mechanisms [45]. Almadhoun et al. [63] has presented a user authentication scheme based on BCFC integration to authenticate users for access to IoT devices. Arun et al. [84] have created a method that permits authentication between edge

users and freshly added Fog servers. The technique instructs the Fog servers to keep one secret key per user, with the user performing hash-based encryptions and decryptions. Patwary et al. [76] suggest a distributed location-based Device to Device (D2D) mutual authentication system based on BCFC integration, without relying on any intermediary or trusted third party. Qu et al. [105] have presented a new BCFC-enabled federated learning approach that ensures data privacy and allows IoT devices to communicate local learning updates to a global learning BC-based model that can be validated by miners.

The use of BCFC-based IoT systems might address several concerns, including the high maintenance costs and power associated with centralized alternatives and a real-time payment service [91, 92]. Yang, Lu, J. Wu [41] propose a smart-toy-edge-computing-oriented data-sharing prototype using HLF v1.0 to save time and money, and ensure that disputes are resolved fairly. Furthermore, trust can be enhanced in IoT applications by deploying a BCFC-based approach to preserve the reputation of publicly available Fog nodes [56, 57, 72]. Wu et al. [80] have presented the BlockEdge, a BCFC-based framework that allows edge-centric networks to trust collaborative services. Holste et al. [61] demonstrate VarOps, a BCFC-based framework that allows application developers to focus on features that can be reused across various frameworks. Other BCFC-based IoT applications have been revealed also in the literature. Tuli et al. [53] propose the FogBus framework, which can connect various IoT-enabled equipment to Fog and Cloud infrastructures. The framework makes it easier to deploy IoT applications, monitor resources, and manage them.

Some constraints, like the low storage and processing power of IoT devices, impede BC development [64, 95]. Accordingly, some authors have proposed a different approach to building a public ledger that overcomes these concerns while also boosting IoT services [47, 91, 95]. Zhang, Zhu and Xu [91] have presented BPAF, a BCFC protocol that enables private and secure authentication of IoT devices. Dorri et al. [117] and Xu et al. [82] offer a secure lightweight BCFC architecture for IoT. By isolating the Broadcast Domain, Saputro, and Sari [55] have proposed Lightweight Multi-Fog (LMF) BC, which incorporates FogBus algorithms, and the Lightweight Scalable BC (LSB) which uses Distributed Time-based Consensus Algorithm (DTC Algorithm).

Another limitation that may restrict BC adoption is the long processing time [89]. Several works have been published to address this issue. Guo et al. [75] offer a lightweight encryption system with outsourced decryption to minimize latency and enhance availability and integrity. Yang et al. [47] have developed a distributed matching mechanism within the context of matching theory to optimize the social well-being of resource-restricted Fog nodes. A SoftEdgeNet model has been developed by Sharma et al. [78] using Software-Defined Network (SDN) as a means of simplifying the administration of dynamic network properties and devices [36, 58, 69]. To improve the routine and practicality of FC, Jung et al. [51] suggest a user-friendly BCFC architecture. Ziegler, Großmann and Krieger [52] have proposed a BCFC architecture using the Plasma framework to address the performance drawbacks. Memon et al. [54] project a DualFog-IoT architecture that

divides the computational resources of the Fog layer into two parts: the Fog Mining Cluster (FMC) and the Fog Cloud Cluster (FCC). Singh et al. [81] have demonstrated a BCFC Architecture Network (BFAN) in smart cities to minimize latency and energy consumption of IoT devices while also improving security.

5.2. Transportation

Due to their capacity to provide road safety and preventive measures for drivers and passengers, vehicular networks are regarded as among the most relevant intelligent transportation systems research issues and anchoring for future smart city environments [109, 128, 130]. One of the major focuses of BCFC-based applications in the transportation field is to enhance transaction security [107, 111]. Eddine et al. [129] have proposed EASBF, a BCFC-based authentication system to enable security in the Internet of vehicles. Nadeem et al. [116] have presented a BCFC-based architecture to safeguard drivers' privacy. Several solutions have been provided such as Bidding-Price-based Transaction (BPT) [109] and BC-based Event-Driven Message (EDM) 5G-enabled automotive edge computing interface [125].

Unmanned Aerial Vehicles (UAV) or Drones are now widely utilized in a variety of applications, including natural disaster monitoring, soil and agricultural analysis, road and traffic surveillance, and consumer product delivery, in addition to defence and military uses. Other drones can receive some information, such as drone identification and flying modes. This data may be sent between drones using radio frequency transmissions and 5G networks [133]. Few studies have been recently proposed using deep neural networks on radio frequency signals to identify drones and recognize their flight modes [132]. However, the transmission of radio frequency signals between drones and 5G nodes must be safe and decentralized, and the accuracy of identification and detection must be improved. Accordingly, Gumaei et al. [131] have proposed a system combining a deep recurrent neural network, a BC, and edge computing. In this system, radio frequency signals, from various drones in various flight modes, are remotely detected and gathered on a Cloud server in order to train a deep recurrent neural network model, which is subsequently distributed to edge devices for identifying drones and their flight modes. The BC, in this system, ensures data integrity and data transmission security [133].

Task offloading is another purpose of BCFC-based applications in the transportation field. Without a tamper-proof audit, centralized compute offloading poses a security risk. It is unable to protect against false reporting, free-riding, spoofing, and repudiation attacks [121]. As a result, Huang et al. [121] have proposed a decentralized Parked Vehicle aided FC (PVFC), in which smart contract executions arrange and validate request posting, workload completion, task appraisal, and reward assignment automatically. Liao et al. [120] suggest a QUeuing-delay aware, handover cost aware, and Trustfulness Aware-Upper Confidence Bound (QUOTA-UCB) algorithm to fix issues such as reducing task offloading delay, queuing delay, and handover expense of missing data. Iqbal et al. [122] have proposed a safe FC paradigm in which RoadSide Units (RSUs), based on reputation rankings held on a distributed BC ledger, shift responsibilities to neighboring Fog vehicles. Lakhan et al. [127] suggest a Mobility Aware BC-Enabled offloading

scheme (MABOS) to enable the protection of mobile vehicles. The study's goal is to minimize application connectivity and computation costs while also addressing the security and mobility of the vehicle. In their work, C h a n g et al. [132] suggest using the BC in the network establishment of a drone system, in which Drones are used as BC miners for service provisioning, collecting computing resources from edge computer nodes or each other as required.

In vehicular FC, there are still several issues with the secure and reliable transmission of sensory data [118]. To address these concerns, K o n g, S u and M a [124] propose an efficient, verifiable sensory data collecting and sharing method in vehicular FC using a permissioned BC. K o n g et al. [130] and K o n g et al. [123] have developed a resource management system based on BCFC integration to increase the security and fairness of resource transactions. For accurately managing vehicle reputation, a three-weight subjective logic model is used [123]. K o n g et al. [130] have provided a verified sensory data collection and sharing method in vehicular FC employing a permissioned BC. The suggested method allows accurate and verified sensory data computation throughout the data collection phase by merging the homomorphic 2-disjunctive normal form cryptosystem with an identity-based signcryption method. S u n et al. [128] propose a BCFC-based reputation crowdsourcing framework where vehicle sensors and terminal computers that upload captured data to Fog nodes make up the consumer stratum.

Another focus of BCFC-based applications in transportation is transaction privacy. L i, Z h u and L i n [108] suggest CoRide, a Collaborative-Ride hailing service that preserves privacy using a BCFC-assisted vehicular network to track c-ride data and build smart contracts to connect passengers and drivers. L i, Z h u and L i n [110] have suggested a carpooling method using a BCFC-based approach that supports conditional privacy to verify users in a conditionally anonymous manner. Y a o et al. [114] suggest a Lightweight Anonymous Authentication (BLA) based on BCFC integration for distributed vehicles implement a flexible cross-data center authentication system and to establish anonymity. K a u r et al. [115] have developed a key exchange and a cross-data center authentication based on BCFC integration to keep track of network data.

Other BCFC-based transportation applications are also revealed in this paper. O u, D e n g and L u o [106] introduce a BCFC-based method that allows autonomous machine learning without the need for a centralized authority, B o n a d i o et al. [112] offer an architecture, based on BCFC integration, to establish complete context awareness for the vehicular Ad hoc, G a o et al. [113] have investigated how BCFC and SDN can work together to make VANET systems run well on a 5G network.

5.3. eHealth

Based on existing BCFC integration, academic and corporate researchers have begun to study applications aimed at enhancing the data security and privacy of healthcare systems. Smart contracts, fraud detection, and identity verification are examples of technological solutions implemented in healthcare applications [140]. In clinical studies, BCFC technology might alleviate difficulties of scientific credibility including data degrading, missing data, selective publishing, and endpoint switching,

as well as concerns about patients' informed permission [134]. Many users have expressed worries about the privacy of patient information or the ability to modify data that is only visible to doctors. Shukla et al. [147] introduced a solution, based on BCFC integration, for IoT devices' identification and patient data authentication. Rahman et al. [141] have demonstrated a safe therapeutic model, in which patients can own and manage their personal information even without the involvement of a trusted third party, such as a therapy facility. Uddin et al. [139] suggest a decentralized eHealth architecture based on BC technology. To guarantee patient privacy while outsourcing duties, a patient agent program employs a BC-boosted task-offloading technique and a lightweight BC consensus mechanism Gao et al. [145] have provided a new framework called SGX in the IoT-Cloud medical health (IoMT) using BCFC to maintain a trusted environment and data confidentiality.

BCFC can play a key role in public healthcare applications such as Electronic Health Records (EHR), an online medical data system for patients that allows for patient access and health claims [13]. A BCFC-based EHR may be thought of as a protocol that allows users to access and preserve their health data while maintaining confidentiality and privacy [135]. The advantages of a BCFC-based EHRs system are numerous: records are distributed; hackers cannot alter the data since there is no centralized owner or hub. Data is always accessible, updated, and gathered from many sources into a single, unified data repository [135]. Abdellatif et al. [144] have introduced a Medical-Edge-BC (MEdge-Chain) approach for dealing with vast volumes of medical records.

BC technology can address present health information system interoperability issues and establish a technological standard that enables safe electronic health data exchange across patients, healthcare providers, medical care facilities, and medical experts [136]. Ismail et al. [143] propose a framework to enhance data sharing by employing BC methods and data operations to prevent data from altering. The digital cryptocurrency GlucoCoin has been used to build an incentive system to encourage users to contribute fresh data to the system [138]. Simpson and Quist-Aphetsi [142] suggest a framework that makes it simple to ensure that a patient's medical information is accessible across multiple healthcare institutions.

Another promising BCFC-based eHealth application is illness prediction [138]. Gul et al. [146] have proposed a BCFC-based business model for healthcare where certain data can be analyzed for prediction, which enables health centers to plan before disaster strikes. Gul et al. [146] suggest a smart healthcare business model that is capable of predicting customer status and awarding incentives based on the business rules established by participating businesses. BCFC-based monitoring frameworks for illness prediction are proposed by [137] and [148]. Islam et al. [137] propose a BCFC-integrated management system centered on the development of clustered-based retrieved characteristics for human activity identification. Speed-Up Robust Features (SURF) have been used to choose relevant points for human activities in films. The validity of the proposed system has been increased by employing the Error-Correction-Output-Codes (ECOC) technique, which enables the classification of multi-class activities. Shynu et al. [148] suggest a BCFC-integrated healthcare service for sickness forecasting. Cardiovascular problems are

taken into account while making forecasts. Initially, the patient's health data is collected through fog Nodes and saved on a BC. When compared to current neural network approaches, the proposed method has a prediction accuracy of more than 81%.

5.4. Energy applications

The growth of network technology is contributing to the rising trend of smart grid adoption, as the linked environment provides a variety of options for electrical data collecting. The potential uses of BCFC in the energy sector are many, and they might have a vast influence on both platforms and processes [151, 152]. BC has the potential to save prices while also enabling new marketplaces and business models [150], can enhance the privacy and security of the data [153, 154] and can enhance energy systems' trust and transparency [154]. To deal with energy security and privacy issues G a i et al. [151] suggest a permissioned BC-Edge System for Smart Grid Networks (PBEM-SGN), G u a n et al. [153] have introduced a Smart Grid approach, Privacy-preserving Multi-party computing (BPM4SG), based on dual-side BC, and W a n g et al. [154] suggest a key agreement and authentication system based on BC. By employing it, the protocol is capable of providing effective key management and conditional privacy without the usage of additional complex cryptosystems [154].

To deliver intelligent controls/governance in the smart grid, it is necessary to have a variety of data-sharing methods [149, 151]. G a i et al. [151] have designed a permissioned BC-edge architecture for smart grid systems in order to address two major worries: privacy and security. The authors have used covert channel authorization techniques and group signatures to assure user validity. BC's smart contracts have been employed to construct an optimum security-aware strategy. G u a n et al. [153] have developed a smart grid system for privacy-preserving multi-party computing. The data segmentation technique is used to ensure the security of multi-party computation in edge nodes (e.g., summing). The consortium BC and smart contract are utilized to increase system security and reduce dependency on trustworthy third parties. Utility providers' interactions with their consumers over power usage have improved since the advent of smart grid technologies [151]. However, because taking reads are done through the Internet, a risk that the data will be compromised if it falls into the wrong hands exists. Deploying BCFC, G a o et al. [150] use the sovereign BC technology to offer transparency and provenance in data sharing, C h e n et al. [149] have created a three-tier architecture-based data aggregation system that provides significant support for accomplishing efficient and safe data gathering in smart grids, and B a i et al. [152] have proposed a multi-edgechain structure that accommodates thousands of edge data and enhances on-chain data efficiency to accomplish cross-chain edge data sharing.

5.5. Computational resource providers

BCFC-based applications are expected to enhance monitoring management and control [156, 158], trust management [156], and security of management [155, 159]. D e b e et al. [156] propose a system for monetizing BCFC-based services. The proposed solution is dependable, decentralized, and automated, which improves QoS

and client satisfaction. Using the Ethereum BC and its intrinsic smart contract features, the proposed solution regulates communications between FC and IoT gadgets [156]. Jeong, Kim and Jang [155] have suggested a secure FC system based on BC. This approach can avoid single-point failure, Sybil attacks, and IP spoofing. The digital signature is used in this system to protect the legitimacy and non-repudiation. Stanciu [158] presents a BCFC-based process management approach based on the IEC 61499 standard that uses BC technology as a foundation for distributed and hierarchical control systems. Using a game-theoretic approach, Xiong et al. [157] have investigated the interaction between providers of Fog/Cloud and miners' resource management. They recommend a lightweight architecture based on PoW-BC where the consensus process is offloaded to the Cloud/Fog [157]. Similarly, Xiong et al. [160] propose a cost-effective way to manage mobile BCFC resources. Huang et al. [159] propose a BCFC-based scheme for computation outsourcing based on Bitcoin BC. The scheme is built based on smart contracts and lightning networks. The proposed scheme may be integrated with current scheduling software to increase the security of exchange among charging piles and electrical cars. BC has been employed to ensure that, regardless of how a malevolent entity acts, an honest entity will be rewarded [159]. Bhattacharya et al. [161] have developed a mobile framework based on BC to make the mining process easier by optimizing the IoT resources acquired from the FC. Tang et al. [162] have deployed BCFC integration to validate the identity of each Fog server and establish a secure offloading environment. To minimize query time and enhance offload security for possible fog servers, a BC-based offloading technique has been created. However, since each server, should store a copy of the transaction, there will be a significant communication overhead if several queries are to be handled by one fog server at once [162].

5.6. Video streaming

Surveillance data created by ubiquitously distributed video sensors are now generating an enormous volume of data. Identifying items of interest from hundreds of video frames is quite difficult [163]. To address this issue, it is necessary to make huge data indexable. Instead of relying on batch processing at Cloud centers, it is perfect to construct pattern indexes in real-time. FC enables the execution of time-sensitive operations at the network’s edge. The FC devices on-site capture information in the form of frames and extract important attributes [164]. Exchanging index information among devices in various tiers, on the other hand, creates security problems, since adversaries may capture or alter with characteristics to deceive the surveillance system. Accordingly, an encrypted secure route between the Fog nodes is suggested by Nikouei et al. [164] to safeguard the index data using a BC-enabled technique. Liu et al. [163] suggest a unique BC-based video streaming architecture with variable block sizes. The authors also have designed an incentive scheme to foster collaboration among video transcoders, content suppliers, and users. The authors have employed a multipliers-based algorithm with a low-complexity alternating direction technique [163].

5.7. Financial applications

BC is expected to play a key role in the long-term viability of the world economy, helping the current financial systems, consumers, and society overall [13]. The world financial system is investigating how BCFC-based applications for financial assets like derivatives, fiat money, and securities might be utilized [165]. For example, BC technology can revolutionize capital markets by providing a more efficient means to conduct activities such as securities and derivatives trades, financial audits, loan management schemes, digital payments, general banking services, and cryptocurrency payment and exchange. Prediction marketplace systems, which operate as oracles or information sources, are another fascinating area that has the potential to affect companies and cryptocurrencies [165]. Furthermore, the financial industry adoption of BC will result in cost reductions in areas such as central finance reporting, compliance, centralized operations, and business operations [166]. In their work, G u et al. [165] propose a BC-based crowdsensing framework to deal with security risks. The proposed framework aids in the validation of given sensor data and avoids record manipulation [165]. P o k r o v s k a i a [166] reports that the capacity to offer a high degree of information security through systems like Ethereum enables the development of trustworthy and transparent taxation and regulating system for all interactions.

5.8. Global collaboration

An overview of modern manufacturing companies reveals that successful global manufacturing enterprises have strong collaboration between designers, manufacturers, and customers, resulting in shorter production cycles and more customer satisfaction. Several previous initiatives have recently been completed to allow the collaborative platform to create successful collaboration with the manufacturing, design, and consumer perspectives [167, 168]. However, establishing trust and effectively utilizing consumer perspectives remains a difficulty. Accordingly, B a r e n j i et al. [168] suggest a BCFC-based collaborative design and manufacturing platform to enable triple communication and cooperation spanning manufacturing, client sections, and design in a secure environment. R i v e r a, R e f a e y and H o s s a i n. [167] propose using a BCFC-based framework to offer a trusted cooperation mechanism between edge servers. A permissioned BC technique has been utilized to create a trustworthy design that also offers cooperation benefits. Machine learning is utilized to group and classify customer views, and BCFC integration is suggested to improve security and reliability [168].

On the other hand, the BCFC is anticipated to enhance supply chain accountability and transparency [169, 171]. BC may be used in logistics, detecting counterfeit items, reducing paper load processing, facilitating provenance tracing [172], and allowing buyers and sellers to trade directly without the need for middlemen [171]. Furthermore, it has been shown that the deployment of applications based on BCFC will improve the security of supply chain networks [170], leading to more strong contract management processes between third and fourth-party logistics in order to ensure traceability, improving tracking methods, and combating information asymmetry [171], improves data management throughout the

e-commerce supply chain [170], and finally, it can help to develop smart transportation networks and provide novel decentralized industrial architectures [169].

5.9. Other applications

This section covers research on BCFC-based applications that aren't part of the above-mentioned categories. Multimedia IoT applications, for example, are proposed in [173], education applications are proposed in [174], social networks are proposed in [175], and agriculture applications [176].

Education. BCFC integration can address privacy and security problems in ubiquitous learning settings, and it can be used to store educational data linked to reputational incentives [174]. Fernández-Caramés and Fraga-Lamas [174] discuss the current state of play in terms of using the newest critical technologies (such as IoT, FC, and BC) to construct smart campuses and institutions. In smart campuses, IoT nodes and gateways must be linked, and designs must be installed that allow for not only a broad range of communications via the latest wireless and cable technologies, but also lower energy consumption to increase the battery life of IoT nodes.

Multimedia IoT. BCFC integration can enhance security, privacy, and trust in multimedia IoT applications. Liang et al. [173] have introduced secure service discovery, which is tamper-proof and eavesdropping-resistant, to enable service discovery in multimodal IoT situations. To overcome the challenge of securely propagating encrypted location information and trust evidence across many apps, a scalable cross-BC structure is presented [173].

Social network. In the social media era, another intriguing use may be identified for BCFC integration. End-users, through user-centric BCFC applications, may be able to track, control, and claim sovereignty over every piece of content they share. Zhu and Badr [175] propose a BCFC architecture to assure security. Users may easily manage smart devices by establishing tamper-proof digital identities and building a new authentication class and authorization methods for IoT devices [175].

Agriculture. The trustworthiness of information about organic agri-products has long been a barrier to small and medium-sized farms participating in high-value-added agriculture [176]. However, non-transparency due to intrinsic features such as centralization, monopoly, and asymmetry are still major consumer trust issues. BC may overcome cost and efficiency flaws, especially for geographically scattered small and medium-sized farms in distant locations. Hu et al. [176] propose a BCFC-based trust architecture that has a significantly superior cost-to-efficiency ratio.

Robots. Podsevalov et al. [177] have used the BCFC integration architecture in vacuum cleaning robot's systems taking advantage of all transactions on multiple servers that should be recorded to the BC database to enhance data sharing security.

Smart applications. In their work, Kochovski et al. [178] have deployed a BCFC-based trust model to handle extremely dynamic and complicated distributed smart application scenarios, although the study had been originally motivated by the growth of smart applications in the construction industry.

6. RQ2: Open issues and future research directions

Several insights on the limits of BCFC-based applications may be gleaned from this SLR. As discussed in Section 5, BCFC is currently being used in a variety of scientific fields and commercial sectors, throwing up a world of research possibilities. Because BC and FC are new technologies, such integration may likely require several years and a tremendous deal of effort to achieve. Some of the limits of the BCFC integration are explained below, as well as many opportunities for future research. While the majority of these limitations may be attributed to the nature and properties of the BC, some can be attributed to the combination with FC.

- **Suitability of BC.** While many professionals see BC being used in practically any project, many are unaware of the idea behind that, mainly in managing the data. For example, BC will offer no value to existing technical solutions if there is no need to be saved at any time. Moreover, BC is appropriate when untrustworthy sources or a lasting record is required [134]. So, when numerous jointly distrusting objects are required to cooperate, BC might be a suitable option. Hence, it is important to check the suitability of BC in BCFC-based applications before implementation [13].
- **Resources and scalability.** The majority of cryptocurrencies have a rather modest transaction rate. Without any doubt, the widespread adoption of cryptocurrencies will have to fix the response rate challenge. As a result, BC designs suffer substantial latency difficulties, which may get more critical as time goes on. One of the most significant disadvantages of BC technology, particularly as it applies to public BCs, is the excess of mining system resources due to energy consumption and computational power [65]. The efforts are focused on using other consensus algorithms that can reduce power usages such as PoS and DPoS [95, 123]. Another solution is by using lightweight BC such as the work of [75, 83, 115].
- **Privacy and security.** Although BCs have many advantages in terms of privacy and security, it still has several limits and flaws. Since data are recorded publicly, privacy is still an issue for public BCs [183]. Furthermore, precautions like pseudonym techniques are insufficient to ensure the privacy of these transactions. In addition, sensitive data can be disclosed in transactions based on Bitcoin [153, 184]. Despite the number of solutions provided in literature to address this issue, these solutions do not apply to all applications, for example applying these solutions requires more resources in resource-constrained IoT devices [124]. On the other hand, while BC increases the security and flexibility of FC data, it may influence functions such as data integrity and dependability [167]. Furthermore, data corruption is caused by a variety of circumstances, including device failure and the surrounding atmosphere and device failure, in addition to usual attacks [88]. Different platforms are vulnerable to different percentages of attacks, such as 51% for Ethereum and Bitcoin and 33% for HLF and Multichain [167].
- **Big data, artificial intelligence & quantum computing.** The structure of BC, which is secure, may be utilized to make huge data administration easier, however, data analyses utilizing the BC entail much overhead. Auditing, currently, has been facilitated by the introduction of AI in conjunction with faster processors

and greater storage areas [131]. Machine learning algorithms, on the other hand, are at the heart of AI and are characterized by their opacity, which originates from the vast number of potential features contained in a classifier that limits human's understanding of AI decisions [104]. The utilization of AI and big data allows for a plethora of intriguing and novel applications based on BC. However, BCFC-based AI approaches require Fog nodes to have BC interface and AI capabilities as well as control and management facilities. In addition, the execution of smart contracts is entirely predictable. This can be a significant difficulty for AI because AI execution outcomes are typically unpredictable, random, or approximate. This necessitates a unique approach to approximation computing and the development of consensus procedures that guarantee the agreement of mining nodes on outputs with a specific level of accuracy and confidence [185]. On the other hand, Future research must devise new consensus mechanisms that take into account evidence based on the quality (e.g., data, algorithms, and learning models) [167].

Huge computations may be processed using quantum computing. BC and quantum computing (e.g., Quantum Dot systems) can be utilized to increase the security and speed of computation [186]. However, Quantum computing, on the other hand, has the potential to destroy all present security and privacy countermeasures [135]. Quantum computing, in other words, will make it simpler and faster for adversaries to break security and privacy protocols [187]. This calls for the development of new privacy and security safeguards to deal with quantum computing's capabilities. As a result, this is yet another unsolved problem and potential research direction [13].

- **Storage.** Although BC may enhance storage capacity, it creates additional issues in terms of FC nodes. Every node must keep a growing number of transactions [15]. As a result, scaling a traditional BC is intrinsically problematic. Moreover, for directly sending transactions to the BC, the FC node necessitates computational burden (i.e., large computational resources are demanded). The key three strategies proposed in the literature to address this issue are data compression, filtering, and off-chain storage [30]. Data compression shortens the time required for processing, transporting, and storing produced data. Another idea is to combine the BC with current P2P storage, which allows for massive volumes of data to be stored off the chain, to solve the storage problem [188].
- **Mobility.** Clients in some applications, such as transportation and eHealth, require highly adaptable mobility rules due to their constant movement. While FC can address this issue, the BCFC combination will raise another issue. A break-off occurs when clients leave one FC node and goes to another. Few articles have attempted to improve mobility issues (e.g., [119, 167]); however, this had a negative impact on other parameters including privacy and latency [127].
- **Standardization.** The number of BCFC-based applications number is rapidly increasing, resulting in a large number of disparate solutions [16]. The large range of implementations and functionalities leads to difficult interoperability challenges, which obstruct standardization. Many firms are working together to address this issue. Because regional laws are a concern, the present Cloud centralized regulatory framework is incompatible with the BCFC distributed architecture,

especially for public BC networks [189, 190]. Moreover, not all organizations are adopting BC because of the absence of standards and laws [191]. The availability of diverse FC node device developers, as well as different BC consensus mechanisms, transaction procedures, and smart contract features, is a significant hurdle to BCFC. That is, there are no universal standards and regulations [15, 192]. The unregulated expansion of cryptocurrencies, on the other hand, allows for the formation of scenarios in which hypothetical attacks or malevolent currency interactions might trigger a catastrophe [185]. Because data would be accessible from the publicly stored data in BC, interoperability and standardization will boost AI and forecasting systems. This opens the door to more precise answers in a variety of scenarios [13].

Since BC technology lacks centralized management, global standards must be defined. Several organizations have taken steps to standardize the use of BC [23]. Since 2016, the International Organization for Standardization (ISO) has started and developed many BC initiatives. Furthermore, the European Union Parliament earlier adopted a BC resolution titled "Distributed ledger technologies and BC: fostering trust via disintermediation." In addition, the International Association for Trusted Blockchain Applications (IATBA) was established, bringing together BC manufacturers and consumers from all over the world, as well as officials from regulatory and standard-setting authorities.

7. Conclusions

BC is seen as a potential technology that can address the rising problems of FC. This article systematically reviews the recent studies that have been published, with a particular focus on BCFC-based applications. This paper answers RQ1 by identifying and discussing eight major BCFC-based applications including and IoT, transportation, eHealth, computational resource providers, energy, video streaming, financial, global collaboration. Other applications are also identified and discussed including education, multimedia IoT, social networks, agriculture, robots, and smart applications. Although many diverse applications of BCFC integration have been explored and discussed in this article, many areas may benefit from this integration. The most advantageous BC means would be a widely well-acknowledged tool that makes it easier to use BC. Different businesses may adopt BCFC integration without the need for centralized Cloud computing.

In addition, the study addresses RQ2 by exploring and evaluating the potential limitations of BCFC-based applications. These limitations relate to the BCFC application itself, the scalability limitations of BC and FC, BC standardizing, security and privacy, and emerging technologies such as AI and quantum computing. These drawbacks should be taken into account in future BCFC-based apps. This paper is among the first efforts that systematically discover BCFC-based applications. Therefore, more research will be required in such an evolving environment. As a consequence, the business and research community may find this study beneficial in evaluating future directions for the adoption of BC in FC applications.

References

1. Bellavista, P., J. Berrocal, A. Corradi, S. K. Das, L. Foschini, A. Zanni. A Survey on Fog Computing for the Internet of Things. – Pervasive and Mobile Computing, Vol. **52**, 2019, pp. 71-99.
2. Cao, H., S. Liu, L.Wu, Z. Guan, X. Du. Achieving Differential Privacy against Non-Intrusive Load Monitoring in Smart Grid: A Fog Computing Approach. – Concurrency and Computation: Practice and Experience, Vol. **31**, 2019, e4528.
3. Zhang, G., T. Wang, G. Wang, A. Liu, W. Jia. Detection of Hidden Data Attacks Combined Fog Computing and Trust Evaluation Method in Sensor-Cloud System. – Concurrency and Computation: Practice and Experience, Vol. **33**, 2021, pp. 1-1.
4. Elazhary, H. Internet of Things (IoT), Mobile Cloud, Cloudlet, Mobile IoT, IoT Cloud, Fog, Mobile Edge, and Edge Emerging Computing Paradigms: Disambiguation and Research Directions. – Journal of Network and Computer Applications, Vol. **128**, 2019, pp. 105-140.
5. Alzoubi, Y. I., V. H. Osmanaj, A. Jaradat, A. Al-Ahmad. Fog Computing Security and Privacy for the Internet of Thing Applications: State-of-the-Art. – Security and Privacy, Vol. **4**, 2021, e145.
6. Khalid, T., M. A. K. Abbasi, M. Zuraiz, A. N. Khan, M. Ali, R. W. Ahmad, J. J. Rodrigues, M. Aslam. A Survey on Privacy and Access Control Schemes in Fog Computing. – International Journal of Communication Systems, Vol. **34**, 2021, e4181.
7. Pereira, J., L. Ricardo, M. Luís, C. Senna, S. Sargento. Assessing the Reliability of Fog Computing for Smart Mobility Applications in VANETs. – Future Generation Computer Systems, Vol. **94**, 2019, pp. 317-332.
8. Adams, C. A Privacy-Preserving Blockchain with Fine-Grained Access Control. – Security and Privacy, Vol. **3**, 2020, e97.
9. Jamil, B., M. Shojafar, I. Ahmed, A. Ullah, K. Munir, H. Ijaz. A Job Scheduling Algorithm for Delay and Performance Optimization in Fog Computing. – Concurrency and Computation: Practice and Experience, Vol. **32**, 2020, e5581.
10. Alzoubi, Y. I., A. Al-Ahmad, A. Jaradat. Fog Computing Security and Privacy Issues, Open Challenges, and Blockchain Solution: An Overview. – International Journal of Electrical & Computer Engineering, Vol. **11**, 2021, pp. 5081-5088.
11. Kwon, J. H., Y. K. Kim, A. Temir, K. Artykbayev, M. F. Demirci, M. H. Kim. Blockchain-Based Multi-Fogcloud Authentication System. – In: Advances in Computer Science and Ubiquitous Computing, J. J. Park, S. J. Fong, Y. Pan, Y. Sung, Eds. Cham, Springer, 2021, pp. 521-528.
12. Khan, M. A., K. Salah. IoT Security: Review, Blockchain Solutions, and Open Challenges. – Future Generation Computer Systems, Vol. **82**, 2018, pp. 395-411.
13. Casino, F., T. K. Dasaklis, C. Patsakis. A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. – Telematics and Informatics, Vol. **36**, 2019, pp. 55-81.
14. Sengupta, J., S. Ruj, S. D. Bit. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. – Journal of Network and Computer Applications, Vol. **149**, 2020, 102481.
15. Alzoubi, Y. I., A. Alahmad, H. Kahtan. Blockchain Technology as a Fog Computing Security and Privacy Solution: An Overview. – Computer Communications, Vol. **182**, 2022, pp. 129-152.
16. Yang, R., F. R. Yu, P. Si, Z. Yang, Y. Zhang. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. IEEE – Communications Surveys & Tutorials, Vol. **21**, 2019, 1508-1532.
17. Ma, Y., Y. Sun, Y. Lei, N. Qin, J. Lu. A Survey of Blockchain Technology on Security, Privacy, and Trust in Crowdsourcing Services. – World Wide Web, Vol. **23**, 2020, pp. 393-419.
18. Mohanta, B. K., D. Jena, S. S. Panda, S. Sobhanayak. Blockchain Technology: A Survey on Applications and Security Privacy Challenges. – Internet of Things, Vol. **8**, 2019, 100107.

19. B a n i a t a, H., A. K e r t e s z. A Survey on Blockchain-Fog Integration Approaches. – IEEE Access, Vol. **8**, 2020, pp. 102657-102668.
20. U r i a r t e, R. B., R. D e N i c o l a. Blockchain-Based Decentralized Cloud/Fog Solutions: Challenges, Opportunities, and Standards. – IEEE Communications Standards Magazine, Vol. **2**, 2018, pp. 22-28.
21. P e t e r s e n, K., S. V a k k a l a n k a, L. K u z n i a r z. Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. – Information and Software Technology, Vol. **64**, 2015, pp. 1-18.
22. K h a n, W. Z., E. A h m e d, S. H a k a k, I. Y a q o o b, A. A h m e d. Edge Computing: A Survey. – Future Generation Computer Systems, Vol. **97**, 2019, pp. 219-235.
23. L u, Y. Blockchain and the Related Issues: A Review of Current Research Topics. – Journal of Management Analytics, Vol. **5**, 2018, pp. 231-255.
24. G a o, Y., W. W u, P. S i, Z. Y a n g, F. R. Y u. B-ReST: Blockchain-Enabled Resource Sharing and Transactions in Fog Computing. – IEEE Wireless Communications, Vol. **28**, 2021, pp. 172-180.
25. A l s h e h r i, M., B. P a n d a. A Blockchain-Encryption-Based Approach to Protect Fog Federations from Rogue Nodes. – In: Proc. of 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, pp. 6-13.
26. W a n g, Y. A Blockchain System with Lightweight Full Node Based on Dew Computing. – Internet of Things, Vol. **11**, 2020, 100184.
27. K u m a r, G., R. S a h a, M. K. R a i, R. T h o m a s, T.-H. K i m. Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics. – IEEE Internet of Things Journal, Vol. **6**, 2019, pp. 6835-6842.
28. K i w e l e k a r, A. W., P. P a t i l, L. D. N e t a k, S. U. W a i k a r. Blockchain-Based Security Services for Fog Computing. – In: Fog/Edge Computing for Security, Privacy, and Applications. Vol. **83**. W. Chang, J. Wu, Eds. Cham, Springer, 2021, pp. 271-290.
29. D a b b a g h, M., K.-K. R. C h o o, A. B e h e s h t i, M. T a h i r, N. S. S a f a. A Survey of Empirical Performance Evaluation of Permissioned Blockchain Platforms: Challenges and Opportunities. – Computers & Security, Vol. **100**, 2021, 102078.
30. F a r a h a n i, B., F. F i r o u z i, M. L u e c k i n g. The Convergence of IoT and Distributed Ledger Technologies (DLT): Opportunities, Challenges, and Solutions. – Journal of Network and Computer Applications, Vol. **177**, 2021, 102936.
31. K u o, T.-T., H. Z a v a l e t a R o j a s, L. O h n o-M a c h a d o. Comparison of Blockchain Platforms: A Systematic Review and Healthcare Examples. – Journal of the American Medical Informatics Association, Vol. **26**, 2019, pp. 462-478.
32. V a n H i j f t e, S. Blockchain Platforms: A Look at the Underbelly of Distributed Platforms. – Synthesis Lectures on Information Concepts, Retrieval, and Services, Vol. **8**, 2020, i-239.
33. K i t c h e n h a m, B., S. C h a r t e r s. Guidelines for Performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report, EBSE-2007-01, 2007.
34. A l z o u b i, Y. I., A. Q. G i l l, A. A l-A n i. Empirical Studies of Geographically Distributed Agile Development Communication Challenges: A Systematic Review. – Information & Management, Vol. **53**, 2016, pp. 22-37.
35. L u o n g, N. C., Y. J i a o, P. W a n g, D. N i y a t o, D. I. K i m, Z. H a n. A Machine-Learning-Based Auction for Resource Trading in Fog Computing. – IEEE Communications Magazine, Vol. **58**, 2020, pp. 82-88.
36. M i s r a, S., P. K. D e b, N. P a t h a k, A. M u k h e r j e e. Blockchain-Enabled SDN for Securing Fog-Based Resource-Constrained IOT. – In: Proc. of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'20), Toronto, Canada, 2020, pp. 490-495.
37. T a r i q, N., M. A s i m, F. A l-O b e i d a t, M. Z u b a i r F a r o o q i, T. B a k e r, M. H a m m o u d e h, I. G h a f i r. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. – Sensors, Vol. **19**, 2019, 1788.
38. W h a i d u z z a m a n, M., M. J. N. M a h i, A. B a r r o s, M. I. K h a l i l, C. F i d g e, R. B u y y a. BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture. – IEEE Access, Vol. **9**, 2021, pp. 106655-106674.

39. D u, Y., Z. W a n g, V. L e u n g. Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issues. – Future Internet, Vol. **13**, 2021, 48.
40. Y a n g, H.-K., H.-J. C h a, Y.-J. S o n g. Secure Identifier Management Based on Blockchain Technology in NDN Environment. – IEEE Access, Vol. **7**, 2018, pp. 6262-6268.
41. Y a n g, J., Z. L u, J. W u. Smart-Toy-Edge-Computing-Oriented Data Exchange Based on Blockchain. – Journal of Systems Architecture, Vol. **87**, 2018, pp. 36-48.
42. Y e o w, K., A. G a n i, R. W. A h m a d, J. J. R o d r i g u e s, K. K o. Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. – IEEE Access, Vol. **6**, 2017, pp. 1513-1524.
43. S h a r m a, V., I. Y o u, F. P a l m i e r i, D. N. K. J a y a k o d y, J. L i. Secure and Energy-Efficient Handover in Fog Networks Using Blockchain-Based DMM. – IEEE Communications Magazine, Vol. **56**, 2018, pp. 22-31.
44. F a r h a d i, M., D. M i o r a n d i, G. P i e r r e. Blockchain Enabled Fog Structure to Provide Data Security in IoT Applications. – In: Proc. of Middleware'18, Rennes, France, 2018, pp. 1-2.
45. B a n i a t a, H., A. K e r t é s z. PF-BVM: A Privacy-Aware Fog-Enhanced Blockchain Validation Mechanism. – In: Proc. of 10th International Conference on Cloud Computing and Services Science (CLOSER'20), Online Streaming, 2020, pp. 430-439.
46. W u, D., N. A n s a r i. A Cooperative Computing Strategy for Blockchain-Secured Fog Computing. – IEEE Internet of Things Journal, Vol. **7**, 2020, pp. 6603-6609.
47. Y a n g, L., M. L i, H. Z h a n g, H. J i, M. X i a o, X. L i. Distributed Resource Management for Blockchain in Fog-Enabled IoT Networks. – IEEE Internet of Things Journal, Vol. **8**, 2020, pp. 2330-2341.
48. L i u, X. Towards Blockchain-Based Resource Allocation Models for Cloud-Edge Computing in IoT Applications. – Wireless Personal Communications, 2021, pp. 1-19. DOI: https://doi.org/10.1007/s11277-021-08213-9.
49. F e r r a g, M. A., L. S h u, X. Y a n g, A. D e r h a b, L. M a g l a r a s. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. – IEEE Access, Vol. **8**, 2020, pp. 32031-32053.
50. S a m a n i e g o, M., U. J a m s r a n d o r j, R. D e t e r s. Blockchain as a Service for IoT. – In: Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 2016, pp. 433-436.
51. J u n g, M. Y., W.-S. K i m, S.-H. C h u n g, J. W. J a n g. A Blockchain-Based ID/IP Mapping and User-Friendly Fog Computing for Hyper-Connected IoT Architecture. – Journal of Information Communication Technology and Digital Convergence, Vol. **2**, 2017, pp. 12-19.
52. Z i e g l e r, M. H., M. G r o β m a n n, U. R. K r i e g e r. Integration of Fog Computing and Blockchain Technology Using the Plasma Framework. – In: Proc. of IEEE International Conference on Blockchain and Cryptocurrency (ICBC'19), Seoul, South Korea, 2019, pp. 120-123.
53. T u l i, S., R. M a h m u d, S. T u l i, R. B u y y a. Fogbus: A Blockchain-Based Lightweight Framework for Edge and Fog Computing. – Journal of Systems and Software, Vol. **154**, 2019, pp. 22-36.
54. M e m o n, R. A., J. P. L i, M. I. N a z e e r, A. N. K h a n, J. A h m e d. DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things. – IEEE Access, Vol. **7**, 2019, pp. 169073-169093.
55. S a p u t r o, M. Y. A., R. F. S a r i. Securing IoT Network Using Lightweight Multi-Fog (LMF) Blockchain Model. – In: Proc. of 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Bandung, Indonesia, pp. 183-188.
56. D e b e, M., K. S a l a h, M. H. U. R e h m a n, D. S v e t i n o v i c. IoT Public Fog Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain. – IEEE Access, Vol. **7**, 2019, pp. 178082-178093.
57. C i n q u e, M., C. E s p o s i t o, S. R u s s o. Trust Management in Fog/Edge Computing by Means of Blockchain Technologies. – In: Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1433-1439.

58. Muthanna, A., A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, A. Koucheryavy. Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. – Journal of Sensor and Actuator Networks, Vol. **8**, 2019, 15.
59. El Kafhali, S., C. Chahir, M. Hanini, K. Salah. Architecture to Manage Internet of Things Data Using Blockchain and Fog Computing. – In: Proc. of 4th International Conference on Big Data and Internet of Things, Rabat, Morocco, pp. 1-8.
60. Wang, H., L. Wang, Z. Zhou, X. Tao, G. Pau, F. Arena. Blockchain-Based Resource Allocation Model in Fog Computing. – Applied Sciences, Vol. **9**, 2019, 5538.
61. Holste, B., V. Stankovski, P. Kochovski, A. Puliafito, P. Massonet. Blockchain Based Variability Management Solutions for Fog Native Open Source Software. – In: Proc. of 27th International Conference on Information, Communication and Automation Technologies (ICAT'19), Sarajevo, Bosnia and Herzegovina, 2019, pp. 1-6.
62. Cech, H. L., M. Großmann, U. R. Krieger. A Fog Computing Architecture to Share Sensor Data by Means of Blockchain Functionality. – In: Proc. of IEEE International Conference on Fog Computing (ICFC'19), Prague, Czech Republic, 2019, pp. 31-40.
63. Almadhoun, R., M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah. A User Authentication Scheme of IoT Devices Using Blockchain-Enabled Fog Nodes. – In: Proc. of 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 2008, pp. 1-8.
64. Sharma, P. K., M.-Y. Chen, J. H. Park. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. – IEEE Access, Vol. **6**, 2017, pp. 115-124.
65. Lei, K., M. Du, J. Huang, T. Jin. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing. – IEEE Transactions on Services Computing, Vol. **13**, 2020, pp. 252-262.
66. Ashik, M. H., M. M. S. Maswood, A. G. Alharbi. Designing a Fog-Cloud Architecture Using Blockchain and Analyzing Security Improvements. – In: Proc. of 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, pp. 1-6.
67. Baouya, A., S. Chehida, S. Bensalem, M. Bozga. Fog Computing and Blockchain for Massive IoT Deployment. – In: Proc. of 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2020, pp. 1-4.
68. Rahman, M. A., M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, M. Guizani. Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. – IEEE Access, Vol. **7**, 2019, pp. 18611-18621.
69. Rathore, S., B. W. Kwon, J. H. Park. BlockSecIoTNet: Blockchain-Based Decentralized Security Architecture for IoT Network. – Journal of Network and Computer Applications, Vol. **143**, 2019, pp. 167-177.
70. Alam, T. Design a Blockchain-Based Middleware Layer in the Internet of Things Architecture. – JOIV: International Journal on Informatics Visualization, Vol. **4**, 2020, pp. 28-31.
71. Alam, T. IoT-Fog: A Communication Framework Using Blockchain in the Internet of Things. – International Journal of Recent Technology and Engineering, Vol. **7**, 2019, pp. 1-5.
72. Jayasinghe, U., G. M. Lee, Á. MacDermott, W. S. Rhee. Trustchain: A Privacy Preserving Blockchain with Edge Computing. – Wireless Communications and Mobile Computing, Vol. **2019**, 2019, Article ID 2014697. DOI: https://doi.org/10.1155/2019/2014697.
73. Pahl, C., N. El Ioini, S. Helmer. A Decision Framework for Blockchain Platforms for IoT and Edge Computing. – In: Proc. of 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS), Crete, Greece, 2018, pp. 105-113.
74. Casado-Vara, R., F. de la Prieta, J. Prieto, J. M. Corchado. Blockchain Framework for IoT Data Quality via Edge Computing. – In: Proc. of 1st Workshop on Blockchain-Enabled Networked Sensor Systems (BlockSys'18), ACM, Shenzhen, China, 2018, pp. 19-24.
75. Guo, R., C. Zhuang, H. Shi, Y. Zhang, D. Zheng. A Lightweight Verifiable Outsourced Decryption of Attribute-Based Encryption Scheme for Blockchain-Enabled Wireless Body Area Network in Fog Computing. – International Journal of Distributed Sensor Networks, Vol. **16**, 2020, 1550147720906796.

76. P a t w a r y, A. A.-N., A. F u, S. K. B a t t u l a, R. K. N a h a, S. G a r g, A. M a h a n t i. FogAuthChain: A Secure Location-Based Authentication Scheme in Fog Computing Environments Using Blockchain. – Computer Communications, Vol. **162**, 2020, pp. 212-224.
77. P a n, J., J. W a n g, A. H e s t e r, I. A l q e r m, Y. L i u, Y. Z h a o. EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts. – IEEE Internet of Things Journal, Vol. **6**, 2018, pp. 4719-4732.
78. S h a r m a, P. K., S. R a t h o r e, Y.-S. J e o n g , J. H. P a r k. SoftEdgeNet: SDN Based Energy-Efficient Distributed Network Architecture for Edge Computing. – IEEE Communications Magazine, Vol. **56**, 2018, pp. 104-111.
79. C h e n, Z., H. C u i, E. W u, Y. L i, Y. X i. Secure Distributed Data Management for Fog Computing in Large-Scale IoT Application: A Blockchain-Based Solution. – In: Proc. of IEEE International Conference on Communications Workshops (ICC Workshops'20), Dublin, Ireland, 2020, pp. 1-6.
80. W u, B., K. X u, Q. L i, S. R e n, Z. L i u, Z. Z h a n g. Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks. – IEEE Network, Vol. **34**, 2020, pp. 30-36.
81. S i n g h, P., A. N a y y a r, A. K a u r, U. G h o s h. Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities. – Future Internet, Vol. **12**, 2020, 61.
82. X u, Y., G. W a n g, J. Y a n g, J. R e n, Y. Z h a n g, C. Z h a n g. Towards Secure Network Computing Services for Lightweight Clients Using Blockchain. – Wireless Communications and Mobile Computing, Vol. **2018**, 2018, Article ID 2051693.
83. A l k h a z a a l i, A. H., A. O ğ u z. Lightweight Fog Based Solution for Privacy-Preserving in IoT Using Blockchain. – In: Proc. of International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA'20), Ankara, Turkey, 2020, pp. 1-10.
84. A r u n, M., S. B a l a m u r a l i, B. S. R a w a l, Q. D u a n, R. L. K u m a r, B. B a l a m u r u g a n. Mutual Authentication and Authorized Data Access between Fog and User Based on Blockchain Technology. – In: Proc. of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'20), Toronto, Canada, 2020, pp. 37-42.
85. L a u t e r t, F., D. F. P i g a t t o, L. G o m e s. A Fog Architecture for Privacy-Preserving Data Provenance Using Blockchains. – In: Proc. of IEEE Symposium on Computers and Communications (ISCC'20), Rennes, France, 2020, pp. 1-6.
86. M o u n n a n, O., A. E l M o u a t a s i m, O. M a n a d, T. H i d a r, A. A b o u E l K a l a m, N. I d b o u f k e r. Privacy-Aware and Authentication Based on Blockchain with Fault Tolerance for IoT Enabled Fog Computing. – In: Proc. of 5th International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, pp. 347-352.
87. C h e n, T., L. Z h a n g, K.-K. R. C h o o, R. Z h a n g, X. M e n g. Blockchain Based Key Management Scheme in Fog-Enabled IoT Systems. – IEEE Internet of Things Journal, Vol. **8**, 2021, pp. 10766-10778.
88. F a n, Y., G. Z h a o, X. L e i, W. L i a n g , K.-C. L i, K.-K. R. C h o o, C. Z h u. SBBS: A Secure Blockchain-Based Scheme for IoT Data Credibility in Fog Environment. – IEEE Internet of Things Journal, Vol. **8**, 2021, pp. 9268-9277.
89. G h a r b i, C., L. H s a i r i, E. Z a g r o u b a. A Secure Integrated Fog Cloud-IoT Architecture Based on Multi-Agents System and Blockchain. – In: Proc. of 13th International Conference on Agents and Artificial Intelligence (ICAART'21), Online Streaming, 2021, pp. 1184-1191.
90. P a v i t h r a n, D., J. N. A l-K a r a k i, K. S h a a l a n. Edge-Based Blockchain Architecture for Event-Driven IoT Using Hierarchical Identity Based Encryption. – Information Processing & Management, Vol. **58**, 2021, 102528.
91. Z h a n g, C., L. Z h u, C. X u. BPAF: Blockchain-Enabled Reliable and Privacy-Preserving Authentication for Fog-Based IoT Devices. – IEEE Consumer Electronics Magazine, Vol. **11**, 2021, pp. 88-96. DOI: https://doi.org/10.1109/MCE.2021.3061808.
92. B a n i a t a, H., A. K e r t e s z. FoBSim: An Extensible Open-Source Simulation Tool for Integrated Fog-Blockchain Systems. – PeerJ Computer Science, Vol. **7**, 2021, e431. DOI: https://doi.org/10.7717/peerj-cs.431.

93. K u m a r, P., R. K u m a r, G. P. G u p t a, R. T r i p a t h i. A Distributed Framework for Detecting DDoS Attacks in Smart Contract-Based Blockchain-IoT Systems by Leveraging Fog Computing. – Transactions on Emerging Telecommunications Technologies, Vol. **32**, 2021, e4112.
94. N ú ñ e z-G ó m e z, C., B. C a m i n e r o, C. C a r r i ó n. HIDRA: A Distributed Blockchain-Based Architecture for Fog/Edge Computing Environments. – IEEE Access, Vol. **9**, 2021, pp. 75231-75251.
95. H e, Y., Y. W a n g, C. Q i u, Q. L i n, J. L i, Z. M i n g. Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. – IEEE Internet of Things Journal, Vol. **8**, 2020, pp. 2226-2237.
96. S e i t z, A., D. H e n z e, D. M i e h l e, B. B r u e g g e, J. N i c k l e s, M. S a u e r. Fog Computing as Enabler for Blockchain-Based IIoT App Marketplaces – A Case Study. – In: Proc. of 5th International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 2018, pp. 182-188.
97. J a n g, S.-H., J. G u e j o n g, J. J e o n g, B. S a n g m i n. Fog Computing Architecture Based Blockchain for Industrial IoT. – In: Proc. of International Conference on Computational Science, Cham, 2019, pp. 593-606.
98. L a l l a s, E. N., A. X e n a k i s, G. S t a m o u l i s. A Generic Framework for a Peer to Peer Blockchain Based Fog Architecture in Industrial Automation. – In: Proc. of 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 2019, pp. 1-5.
99. H u a n g, J., L. K o n g, G. C h e n, M.-Y. W u, X. L i u, P. Z e n g. Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism. – IEEE Transactions on Industrial Informatics, Vol. **15**, 2019, pp. 3680-3689.
100. K u m a r, T., E. H a r j u l a, M. E j a z, A. M a n z o o r, P. P o r a m b a g e, I. A h m a d, M. L i y a n a g e, A. B r a e k e n, M. Y l i a n t t i l a. BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks. – IEEE Access, Vol. **8**, 2020, pp. 154166-154185.
101. B o u a c h i r, O., M. A l o q a i l y, L. T s e n g, A. B o u k e r c h e. Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry. – Computer, Vol. **53**, 2020, pp. 36-45.
102. R e n, Y., F. Z h u, J. Q i, J. W a n g, A. K. S a n g a i a h. Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. – Applied Sciences, Vol. **9**, 2019, 2058.
103. C e c c a r e l l i, A., M. C i n q u e, C. E s p o s i t o, L. F o s c h i n i, C. G i a n n e l l i, P. L o l l i n i. FUSION – Fog Computing and Blockchain for Trusted Industrial Internet of Things. – IEEE Transactions on Engineering Management, 2020. DOI: https://doi.org/10.1109/TEM.2020.3024105**.**
104. S h a h b a z i, Z., Y.-C. B y u n. Improving Transactional Data System Based on an Edge Computing-Blockchain-Machine Learning Integrated Framework. – Processes, Vol. **9**, 2021, 92.
105. Q u, Y., L. G a o, T. H. L u a n, Y. X i a n g, S. Y u, B. L i, G. Z h e n g. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. – IEEE Internet of Things Journal, Vol. **7**, 2020, pp. 5171-5183.
106. O u, W., M. D e n g, E. L u o. A Decentralized and Anonymous Data Transaction Scheme Based on Blockchain and Zero-Knowledge Proof in Vehicle Networking (Workshop Paper). – In: Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. X. Wang, H. Gao, M. Iqbal, G. Min, Eds. Cham, Springer, 2019, pp. 712-726.
107. L e i, A., H. C r u i c k s h a n k, Y. C a o, P. A s u q u o, C. P. A. O g a h, Z. S u n. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. – IEEE Internet of Things Journal, Vol. **4**, 2017, pp. 1832-1843.

108. L i, M., L. Z h u, X. L i n. CoRide: A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing. – In: Security and Privacy in Communication Networks. SecureComm 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. S. Chen, K. Choo, X. Fu, W. Lou, A. Mohaisen, Eds. Cham, Springer, Vol. **305**, 2019, pp. 408-422.
109. D e w a n t a, F., M. M a m b o. BPT Scheme: Establishing Trusted Vehicular Fog Computing Service for Rural Area Based on Blockchain Approach. – IEEE Transactions on Vehicular Technology, Vol. **70**, 2021, pp. 1752-1769.
110. L i, M., L. Z h u, X. L i n. Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing. – IEEE Internet of Things Journal, Vol. **6**, 2019, pp. 4573-4584.
111. M i k a v i c a, B., A. K o s t i ć-L j u b i s a v l j e v i ć. Blockchain-Based Solutions for Security, Privacy, and Trust Management in Vehicular Networks: A Survey. – The Journal of Supercomputing, Vol. **77**, 2021, pp. 1-56. DOI: https://doi.org/10.1007/s11227-021-03659-x.
112. B o n a d i o, A., F. C h i t i, R. F a n t a c c i, V. V e s p r i. An Integrated Framework for Blockchain Inspired Fog Communications and Computing in Internet of Vehicles. – Journal of Ambient Intelligence and Humanized Computing, Vol. **11**, 2020, pp. 755-762.
113. G a o, J., K. O.-B. O. A g y e k u m, E. B. S i f a h, K. N. A c h e a m p o n g, Q. X i a, X. D u, M. G u i z a n i, H. X i a. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. – IEEE Internet of Things Journal, Vol. **7**, 2019, pp. 4278-4291.
114. Y a o, Y., X. C h a n g, J. M i š i ć, V. B. M i š i ć, L. L i. BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. – IEEE Internet of Things Journal, Vol. **6**, 2019, pp. 3775-3784.
115. K a u r, K., S. G a r g, G. K a d d o u m, F. G a g n o n, S. H. A h m e d. Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure. – In: Proc. of IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6.
116. N a d e e m, S., M. R i z w a n, F. A h m a d, J. M a n z o o r. Securing Cognitive Radio Vehicular ad hoc Network with Fog Node Based Distributed Blockchain Cloud Architecture. – International Journal of Advanced Computer Science and Applications, Vol. **10**, 2019, pp. 288-295.
117. D o r r i, A., M. S t e g e r, S. S. K a n h e r e, R. J u r d a k. Blockchain: A Distributed Solution to Automotive Security and Privacy. – IEEE Communications Magazine, Vol. **55**, 2017, pp. 119-125.
118. K a n g, J., R. Y u, X. H u a n g, Y. Z h a n g. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles. – IEEE Transactions on Intelligent Transportation Systems, Vol. **19**, 2017, pp. 2627-2637.
119. L i, H., D. H a n, M. T a n g. A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing. – IEEE Systems Journal, Vol. **15**, 2020, pp. 3189-3200. DOI: https://doi.org/10.1109/JSYST.2020.3009447.
120. L i a o, H., Y. M u, Z. Z h o u, M. S u n, Z. W a n g, C. P a n. Blockchain and Learning-Based Secure and Intelligent Task Offloading for Vehicular Fog Computing. – IEEE Transactions on Intelligent Transportation Systems, Vol. **22**, 2020, pp. 4051-4063.
121. H u a n g, X., D. Y e, R. Y u, L. S h u. Securing Parked Vehicle Assisted Fog Computing with Blockchain and Optimal Smart Contract Design. – IEEE/CAA Journal of Automatica Sinica, Vol. **7**, 2020, pp. 426-441.
122. I q b a l, S., A. W. M a l i k, A. U. R a h m a n, R. M. N o o r. Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network. – IEEE Access, Vol. **8**, 2020, pp. 52968-52980.
123. K a n g, J., R. Y u, X. H u a n g, M. W u, S. M a h a r j a n, S. X i e, Y. Z h a n g. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. – IEEE Internet of Things Journal, Vol. **6**, 2018, pp. 4660-4670.
124. K o n g, Q., L. S u, M. M a. Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog with Blockchain. – IEEE Transactions on Intelligent Transportation Systems, Vol. **22**, 2020, pp. 4889-4898. DOI: https://doi.org/10.1109/TITS.2020.2983466.

125. N k e n y e r e y e, L., B. A d h i T a m a, M. K. S h a h z a d, Y.-H. C h o i. Secure and Blockchain-Based Emergency Driven Message Protocol for 5G Enabled Vehicular Edge Computing. – Sensors, Vol. **20**, 2020, 154.
126. L i u, H., Y. Z h a n g, T. Y a n g. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. – IEEE Network, Vol. **32**, 2018, pp. 78-83.
127. L a k h a n, A., M. A h m a d, M. B i l a l, A. J o l f a e i, R. M. M e h m o o d. Mobility Aware Blockchain Enabled Offloading and Scheduling in Vehicular Fog Cloud Computing. – IEEE Transactions on Intelligent Transportation Systems, Vol. **22**, 2021, pp. 4212-4223.
128. S u n, L., Q. Y a n g, X. C h e n, Z. C h e n. RC-Chain: Reputation-Based Crowdsourcing Blockchain for Vehicular Networks. – Journal of Network and Computer Applications, Vol. **176**, 2021, 102956.
129. E d d i n e, M. S., M. A. F e r r a g, O. F r i h a, L. M a g l a r a s. EASBF: An Efficient Authentication Scheme over Blockchain for Fog Computing-Enabled Internet of Vehicles. – Journal of Information Security and Applications, Vol. **59**, 2021, 102802.
130. K o n g, M., J. Z h a o, X. S u n, Y. N i e. Secure and Efficient Computing Resource Management in Blockchain-Based Vehicular Fog Computing. – China Communications, Vol. **18**, 2021, pp. 115-125.
131. G u m a e i, A., M. A l-R a k h a m i, M. M. H a s s a n, P. P a c e, G. A l a i, K. L i n, G. F o r t i n o. Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. – IEEE Network, Vol. **35**, 2021, pp. 94-100.
132. C h a n g, Z., W. G u o, X. G u o, T. C h e n, G. M i n, K. M. A b u a l n a j a, S. M u m t a z. Blockchain-Empowered Drone Networks: Architecture, Features, and Future. – IEEE Network, Vol. **35**, 2021, pp. 86-93.
133. A l o q a i l y, M., O. B o u a c h i r, A. B o u k e r c h e, I. A l R i d h a w i. Design Guidelines for Blockchain-Assisted 5G-UAV Networks. – IEEE Network, Vol. **35**, 2021, pp. 64-71.
134. Y a q o o b, I., K. S a l a h, R. J a y a r a m a n, Y. A l-H a m m a d i. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. – Neural Computing and Applications, Vol. **34**, 2021, pp. 1-16. DOI: https://doi.org/10.1007/s00521-020-05519-w.
135. B h a v i n, M., S. T a n w a r, N. S h a r m a, S. T y a g i, N. K u m a r. Blockchain and Quantum Blind Signature-Based Hybrid Scheme for Healthcare 5.0 Applications. – Journal of Information Security and Applications, Vol. **56**, 2021, 102673.
136. A r u l, R., Y. D. A l-O t a i b i, W. S. A l n u m a y, U. T a r i q, U. S h o a i b, M. J. P i r a n. Multi-Modal Secure Healthcare Data Dissemination Framework Using Blockchain in IoMT. – Personal and Ubiquitous Computing, 2021, pp. 1-13.
DOI: https://doi.org/10.1007/s00779-021-01527-2.
137. I s l a m, N., Y. F a h e e m, I. U. D i n, M. T a l h a, M. G u i z a n i, M. K h a l i l. A Blockchain-Based Fog Computing Framework for Activity Recognition as an Application to e-Healthcare Services. – Future Generation Computer Systems, Vol. **100**, 2019, pp. 569-578.
138. F e r n á n d e z-C a r a m é s, T. M., P. F r a g a-L a m a s. Design of a Fog Computing, Blockchain and IoT-Based Continuous Glucose Monitoring System for Crowdsourcing mHealth. – Proceedings, Vol. **4**, 2019, 37.
139. U d d i n, M. A., A. S t r a n i e r i, I. G o n d a l, V. B a l a s u b r a m a n i a n. Blockchain Leveraged Decentralized IoT eHealth Framework. – Internet of Things, Vol. **9**, 2020, 100159.
140. M c G h i n, T., K.-K. R. C h o o, C. Z. L i u, D. H e. Blockchain in Healthcare Applications: Research Challenges and Opportunities. – Journal of Network and Computer Applications, Vol. **135**, 2019, pp. 62-75.
141. R a h m a n, M. A., M. S. H o s s a i n, G. L o u k a s, E. H a s s a n a i n, S. S. R a h m a n, M. F. A l h a m i d, M. G u i z a n i. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. – IEEE Access, Vol. **6**, 2018, pp. 72469-72478.
142. S i m p s o n, G., K. Q u i s t-A p h e t s i. A Centralized Data Validation Approach for Distributed Healthcare Systems in Dew-Fog Computing Environment Using Blockchain. – In: Proc. of International Conference on Cyber Security and Internet of Things (ICSIoT'19), Accra, Ghana, 2019, pp. 1-4.

143. I s m a i l , S., R. A l m a y o u f, S. C h e h a b, S. A l g h a m d i, A. A l m u t a i r i, B. A l a s m a r i, R. A l t h e r w y. Edge IoT-Cloud Framework Based on Blockchain. – In: Proc. of 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-7.
144. A b d e l l a t i f, A. A., L. S a m a r a, A. M o h a m e d, A. E r b a d, C. F. C h i a s s e r i n i, M. G u i z a n i, M. D. O'C o n n o r, J. L a u g h t o n. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. – IEEE Internet of Things Journal, Vol. **8**, 2021, pp. 15762-15775. DOI: https://doi.org/10.1109/JIOT.2021.3052910.
145. G a o, Y., H. L i n, Y. C h e n, Y. L i u. Blockchain and SGX-Enabled Edge Computing Empowered Secure IoMT Data Analysis. – IEEE Internet of Things Journal, Vol. **8**, 2021, pp. 15785-15795. DOI: https://doi.org/10.1109/JIOT.2021.3052604.
146. G u l, M. J., B. S u b r a m a n i a n, A. P a u l, J. K i m. Blockchain for Public Health Care in Smart Society. – Microprocessors and Microsystems, Vol. **80**, 2021, 103524.
147. S h u k l a, S., S. T h a k u r, S. H u s s a i n, J. G. B r e s l i n, S. M. J a m e e l. Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. – Internet of Things, Vol. **15**, 2021, 100422.
148. S h y n u, P., V. G. M e n o n, R. L. K u m a r, S. K a d r y, Y. N a m. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. – IEEE Access, Vol. **9**, 2021, pp. 45706-45720.
149. C h e n, S., L. Y a n g, C. Z h a o, V. V a r a d a r a j a n, K. W a n g. Double-Blockchain Assisted Secure and Anonymous Data Aggregation for Fog-Enabled Smart Grid. – Engineering, Vol. **8**, 2020, pp. 159-169. DOI: https://doi.org/10.1016/j.eng.2020.06.018.
150. G a o, J., K. O. A s a m o a h, E. B. S i f a h, A. S m a h i, Q. X i a, H. X i a, X. Z h a n g, G. D o n g. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. – IEEE Access, Vol. **6**, 2018, pp. 9917-9925.
151. G a i, K., Y. W u, L. Z h u, L. X u, Y. Z h a n g. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks. – IEEE Internet of Things Journal, Vol. **6**, 2019, pp. 7992-8004.
152. B a i, F., T. S h e n, Z. Y u, K. Z e n g, B. G o n g. Trustworthy Blockchain-Empowered Collaborative Edge Computing-as-a-Service Scheduling and Data Sharing in the IIoE. – IEEE Internet of Things Journal, Vol. **9**, 2021, pp. 14752-14766. DOI: https://doi.org/10.1109/JIOT.2021.3058125.
153. G u a n, Z., X. Z h o u, P. L i u, L. W u, W. Y a n g. A Blockchain Based Dual Side Privacy Preserving Multi Party Computation Scheme for Edge Enabled Smart Grid. – IEEE Internet of Things Journal, Vol. **9**, 2021, pp. 14287-14299. DOI: https://doi.org/10.1109/JIOT.2021.3061107.
154. W a n g, J., L. W u, K.-K. R. C h o o, D. H e. Blockchain-Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure. – IEEE Transactions on Industrial Informatics, Vol. **16**, 2020, pp. 1984-1992.
155. J e o n g, J. W., B. Y. K i m, J. W. J a n g. Security and Device Control Method for Fog Computer Using Blockchain. – In: Proc. of International Conference on Information Science and System, Jeju, Republic of Korea, 2018, pp. 234-238.
156. D e b e, M., K. S a l a h, M. H. U. R e h m a n, D. S v e t i n o v i c. Monetization of Services Provided by Public Fog Nodes Using Blockchain and Smart Contracts. – IEEE Access, Vol. **8**, 2020, pp. 20118-20128.
157. X i o n g, Z., S. F e n g, W. W a n g, D. N i y a t o, P. W a n g, Z. H a n. Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks. – IEEE Internet of Things Journal, Vol. **6**, 2018, pp. 4585-4600.
158. S t a n c i u, A. Blockchain Based Distributed Control System for Edge Computing. – In: Proc. of 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 2017, pp. 667-671.
159. H u a n g, X., C. X u, P. W a n g, H. L i u. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. – IEEE Access, Vol. **6**, 2018, pp. 13565-13574.
160. X i o n g, Z., Y. Z h a n g, D. N i y a t o, P. W a n g, Z. H a n. When Mobile Blockchain Meets Edge Computing. – IEEE Communications Magazine, Vol. **56**, 2018, pp. 33-39.

161. B h a t t a c h a r y a, P., S. T a n w a r, R. S h a h, A. L a d h a. Mobile Edge Computing-Enabled Blockchain Framework – A Survey. – In: Proc. of ICRIC 2019. P. Singh, A. Kar, Y. Singh, M. Kolekar, S. Tanwar, Eds. Springer, Cham, Vol. **597**, 2020, pp. 797-809.
162. T a n g, W., X. Z h a o, W. R a f i q u e, W. D o u. A Blockchain-Based Offloading Approach in Fog Computing Environment. – In: Proc. of IEEE Intl. Conf. on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, 2018, pp. 308-315.
163. L i u, M., F. R. Y u, Y. T e n g, V. C. L e u n g, M. S o n g. Distributed Resource Allocation in Blockchain-Based Video Streaming Systems with Mobile Edge Computing. – IEEE Transactions on Wireless Communications, Vol. **18**, 2018, pp. 695-708.
164. N i k o u e i, S. Y., R. X u, D. N a g o t h u, Y. C h e n, A. A v e d, E. B l a s c h. Real-Time Index Authentication for Event-Oriented Surveillance Video Query Using Blockchain. – In: Proc. of 4th IEEE International Smart Cities Conference (ISC2), Kansas City, USA, 2018, pp. 1-8.
165. G u, X., J. P e n g, W. Y u, Y. C h e n g, F. J i a n g, X. Z h a n g, Z. H u a n g, L. C a i. Using Blockchain to Enhance the Security of Fog-Assisted Crowdsensing Systems. – In: Proc. of 28th International Symposium on Industrial Electronics (ISIE), Vancouver, BC, Canada, 2019, pp. 1859-1864.
166. P o k r o v s k a i a, N. N. Tax, Financial and Social Regulatory Mechanisms within the Knowledge-Driven Economy. Blockchain Algorithms and Fog Computing for the Efficient Regulation. – In: Proc. of 20th IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, 2017, pp. 709-712.
167. R i v e r a, A. V., A. R e f a e y, E. H o s s a i n. A Blockchain Framework for Secure Task Sharing in Multi-Access Edge Computing. – IEEE Network, Vol. **35**, 2020, pp. 176-183.
168. B a r e n j i, A. V., H. G u o, Y. W a n g, Z. L i, Y. R o n g. Toward Blockchain and Fog Computing Collaborative Design and Manufacturing Platform: Support Customer View. – Robotics and Computer-Integrated Manufacturing, Vol. **67**, 2021, 102043.
169. D a v c e v, D., L. K o c a r e v, A. C a r b o n e, V. S t a n k o v s k i, K. M i t r e s k. Blockchain-Based Distributed Cloud/Fog Platform for IoT Supply Chain Management. – In: Proc. of 8th International Conference on Advances in Computing, Electronics and Electrical Technology (CEET), IEEE, Kuala Lumpur, Malaysia, 2018, pp. 51-58.
170. C a r o, M. P., M. S. A l i, M. V e c c h i o, R. G i a f f r e d a. Blockchain-Based Traceability in Agri-Food Supply Chain Management: A Practical Implementation. – In: Proc. of IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 2018, pp. 1-4.
171. M o n d a l, S., K. P. W i j e w a r d e n a, S. K a r u p p u s w a m i, N. K r i t i, D. K u m a r, P. C h a h a l. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. – IEEE Internet of Things Journal, Vol. **6**, 2019, pp. 5803-5813.
172. J a n g i r a l a, S., A. K. D a s, A. V. V a s i l a k o s. Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. – IEEE Transactions on Industrial Informatics, Vol. **16**, 2019, pp. 7081-7093.
173. L i a n g, H., J. W u, X. Z h e n g, M. Z h a n g, J. L i, A. J o l f a e i. Fog-Based Secure Service Discovery for Internet of Multimedia Things: A Cross-Blockchain Approach. – ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), Vol. **16**, 2020, pp. 1-23.
174. F e r n á n d e z-C a r a m é s, T. M., P. F r a g a-L a m a s. Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities. – Applied Sciences, Vol. **9**, 2019, 4479.
175. Z h u, X., Y. B a d r. Fog Computing Security Architecture for the Internet of Things Using Blockchain-Based Social Networks. – In: Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Canada, 2018, pp. 1361-1366.

176. H u, S., S. H u a n g, J. H u a n g, J. S u. Blockchain and Edge Computing Technology Enabling Organic Agricultural Supply Chain: A Framework Solution to Trust Crisis. – Computers & Industrial Engineering, Vol. **153**, 2021, 107079.
177. P o d s e v a l o v, I., O. I a k u s h k i n, R. K u r b a n g a l i e v, V. K o r k h o v. Blockchain as a Platform for Fog Computing. – In: Proc. of 19th International Conference on Computational Science and Its Applications, Saint Petersburg, Russia, 2019, pp. 596-605.
178. K o c h o v s k i, P., S. G e c, V. S t a n k o v s k i, M. B a j e c, P. D. D r o b i n t s e v. Trust Management in a Blockchain Based Fog Computing Platform with Trustless Smart Oracles. – Future Generation Computer Systems, Vol. **101**, 2019, pp. 747-759.
179. F e r n á n d e z-C a r a m é s, T. M., P. F r a g a-L a m a s. A Review on the Use of Blockchain for the Internet of Things. – IEEE Access, Vol. **6**, 2018, pp. 32979-33001.
180. A l z o u b i, Y. I., A. A l-A h m a d, A. J a r a d a t, V. O s m a n a j. Fog Computing Architecture, Benefits, Security, and Privacy, for the Internet of Thing Applications: An Overview. – Journal of Theoretical and Applied Information Technology, Vol. **99**, 2021, pp. 436-451.
181. R e n, Y., Y. L e n g, Y. C h e n g, J. W a n g. Secure Data Storage Based on Blockchain and Coding in Edge Computing. – Mathematical Biosciences and Engineering, Vol. **16**, 2019, pp. 1874-1892.
182. A l z o u b i, Y. I., A. A l-A h m a d, H. K a h t a n, A. J a r a d a t. Internet of Things and Blockchain Integration: Security, Privacy, Technical, and Design Challenges. – Future Internet, Vol. **14**, 2022, 216.
183. B a n i a t a, H., A. A n a q r e h, A. K e r t e s z. PF-BTS: A Privacy-Aware Fog-Enhanced Blockchain-Assisted Task Scheduling. – Information Processing & Management, Vol. **58**, 2021, 102393.
184. A l A h m a d, A. S., H. K a h t a n, Y. I. A l z o u b i, O. A l i, A. J a r a d a t. Mobile Cloud Computing Models Security Issues: A Systematic Review. – Journal of Network and Computer Applications, Vol. **190**, 2021, 103152.
185. S a l a h, K., M. H. U. R e h m a n, N. N i z a m u d d i n, A. A l-F u q a h a. Blockchain for AI: Review and Open Research Challenges. – IEEE Access, Vol. **7**, 2019, pp. 10127-10149.
186. G i l l, S. S. Quantum and Blockchain Based Serverless Edge Computing: A Vision, Model, New Trends and Future Directions. – Internet Technology Letters, 2021, pp. 1-6, e275. DOI: https://doi.org/10.1002/itl2.275.
187. K h a l i d, Z. M., S. A s k a r. Resistant Blockchain Cryptography to Quantum Computing Attacks. – International Journal of Science and Business, Vol. **5**, 2021, pp. 116-125.
188. H e w a, T. M., A. B r a e k e n, M. L i y a n a g e, M. Y l i a n t t i l a. Fog Computing and Blockchain Based Security Service Architecture for 5G Industrial IoT Enabled Cloud Manufacturing. – IEEE Transactions on Industrial Informatics, Vol. **18**, 2022, pp. 7174-7185. DOI:10.1109/TII.2022.3140792.
189. M i s h r a, A., Y. I. A l z o u b i, M. J. A n w a r, A. Q. G i l l. Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations. – Computers & Security, 2022, 102820.
190. M i s h r a, A., Y. I. A l z o u b i, A. Q. G i l l, M. J. A n w a r. Cybersecurity Enterprises Policies: A Comparative Study. – Sensors, Vol. **22**, 2022, 538.
191. A l z o u b i, Y. I., A. G i l l, A. M i s h r a. A Systematic Review of the Purposes of Blockchain and Fog Computing Integration: Classification and Open Issues. – Journal of Cloud Computing, Vol. **11**, 2022, pp. 1-36.
192. E l n e e l, D. A. H., H. K a h t a n, A. S. F a k h a r u d i n, M. A b d u l h a k, A. S. A l-A h m a d, Y. I. A l z o u b i. The Factors Influenced by Stakeholder Identification in e-Learning Systems: A Survey. – Journal of King Saud University-Science, 2023, 102566.

Received: 30.06.2022; Second Version: 02.02.2023; Accepted: 13.02.2023