IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 27, 2020, accepted May 28, 2020, date of publication June 1, 2020, date of current version June 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2999213

A Survey on Blockchain-Fog Integration Approaches

HAMZA BANIATA AND ATTILA KERTESZ
Department of Software Engineering, University of Szeged, 6720 Szeged, Hungary
Corresponding author: Hamza Baniata (baniatah@inf.u-szeged.hu)

This work was supported in part by the Hungarian Scientific Research Fund under Grant OTKA FK 131793, and in part by the University of Szeged Open Access Fund under Grant 4713.

ABSTRACT Fog computing (FC) is the extension of Cloud Computing (CC), from the core of the internet architecture to the edge of the network, with the aim to perform processes closer to end-users. This extension is proven to enhance security, and to reduce latency and energy consumption. Blockchain (BC), on the other hand, is the base technology behind crypto-currencies, yet is implemented in wide range of different applications. The security and reliability, along with the distributed trust management criteria proposed in BC, excited the research community to integrate it with FC, in a step towards reaching a distributed and trusted, Data, Payment, Reputation, and Identity management systems. In this survey we present the up-to-date state-of-the-art of FC-BC integration with a detailed literature review and classification. We discuss and categorize the related papers according to the year of publication, domain, used algorithms, BC roles, and the placement of the BC in the FC architecture. Our research presents detailed observations, analysis, and open challenges for the BC-FC integration. We believe such conclusions may clarify the vision of the BC-FC integration, and calibrate the compass towards open issues and future research directions.

INDEX TERMS Blockchain, fog computing, Internet of Things.

I. INTRODUCTION

Fog Computing (FC) as proposed in [1] in 2012, and introduced later by Cisco in 2013 [2], is an extension of the cloud services into the edge of the network. Services provided by FC are similar to those provided by Cloud Computing (CC) paradigms, which may include Storage, Computation, and Communications. Although more than 95% of end-users do not really know how, why, or what data is being processed in the cloud [3], FC is actually characterized as a distributed cloud computing infrastructure that includes a set of physical machines with high-performance capabilities that are linked to one another [4]. The extension of CC into FC shall allow the cloud to provide faster, more reliable, and more distributed services that are able to cope up with the scalability, security, and performance requirements to deal with the expected heterogeneity during the development of the next generation of smart computing. Figure 1 represents how the cloud services can conceptually be provided at the edge of the network using FC.

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

FC as a whole solution of the high latency and network congestion [5] is thought of as a middle layer between the cloud and Things forming the Internet of Things (IoT). IoT applications researched and applied in the past decade by thousands of researchers and industry specialists, mainly depend on high rates of network response time, and reliability. Meanwhile, such applications require extended storage and computation abilities. This encouraged many to deploy FC for achieving the goals of their proposed IoT systems. In fact, FC is believed to have the major purpose of serving IoT applications at the edge of the network [6]. However, the integration of FC and IoT includes various challenges, such as the security and efficiency of communications. The development of a successful IoT system is usually challenged by Security and Privacy issues, the need of efficient data management schemes, the limitations of device resources (i.e. Memory, Processing power, etc.), Energy consumption, and connectivity into long distances and periods of time [7]. IoT-Cloud integration solved some of these challenges like providing processing power and unlimited storage, leading to have more than five billion devices connected nowadays to the internet on account of IoT [8]. FC, as the extension of

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

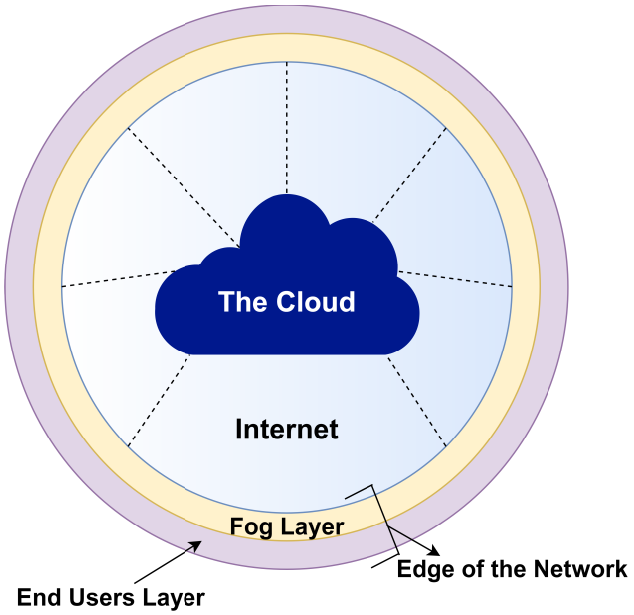

FIGURE 1. Cloud computing services extended to be performed at the edge of the network using Fog Computing.

CC is expected to solve more issues such as some privacy issues, energy consumption, real-time applications, and connectivity.

Nevertheless, major challenges remained open even when FC is integrated with IoT, such as the need of efficient data management schemes and Security issues. Also, IoT paradigm itself had branched new similar paradigms serving different purposes. A famous example of that is the Internet of Vehicles (IoV) paradigm, which is only similar to IoT in the general concept, yet different because it serves for different components, goals, standards, and technical solutions. All of the mentioned challenges excited the integration of FC systems with Blockchain technology, which is the core foundation technology of Bitcoin.[1]

Blockchain (BC), as proposed by [9] in 2008, deploys revolutionary concepts in the fields of Distributed Trust, Decentralized Economy, Security, and Reliability. Such deployment provided easier ways to perform tasks, that had to pass through a centralized Trusted Third Party (TTP) in the past, in a Peer-to-Peer manner. BC technology is capable to provide trusted, immutable, and fully decentralized data management and reliable payment methodologies. These criteria may solve the remaining major challenges for the FC-IoT integration, if correctly deployed. Generally, BC can provide four services to IoT-FC systems: Data Storage, Identity Management, Trading and payment method, and Rating/Reputation systems [10].

In this survey, we aim to provide an assessment of BC deployment in FC environments. In contrast, we aim to highlight the roles the BC played in such systems, and present how the research community visualizes the future

[1]https://bitcoin.org/

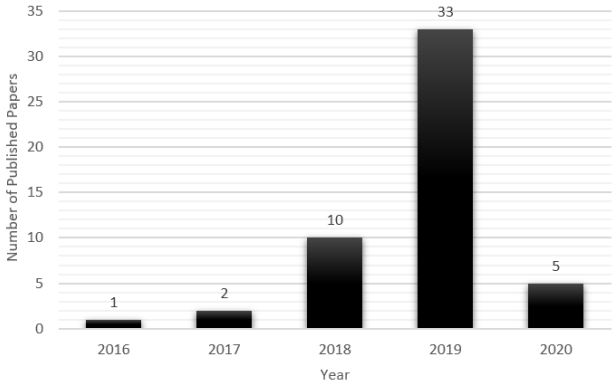

FIGURE 2. Distribution of published papers according to the year of publication.

BC-Fog integration. To get close to our goals, we searched for published papers and surveys whose main topic is Blockchain and Fog Computing.[2] We found 8 surveys and 43 articles. Hence, the a total number of papers concerned with our topic is 51 papers.

We study those papers in the following two sections as Section II presents the surveys, while Section III presents and discusses the articles. In the two sections, we present the papers according to their year of publication. Figure 2 presents the distribution of papers according to the year of publication. As can be observed in the figure, the first research work discussing the integration of BC and FC was published in 2016. Section IV presents our observations and analysis, and discusses the open challenges, while Section V concludes our work.

II. RELATED WORK

In this section, we briefly present the surveys we found in the literature discussing BC and FC. Table 1 concludes these surveys in a step to present how our work differs from previous research efforts. As can be noticed in the table, most of the previous review works surveyed specific topics or projects in the FC-BC domain. The novelty of our survey, on the other hand, is the discussion of all papers that survey/propose FC-BC integration. Such discussion may provide wider vision of the domain, and hence, deeper understanding, and more generalized observations.

In 2017, a brief conceptual research surveying the criteria needed to develop a cryptocurrency system that integrates neuron technologies, artificial intelligence, blockchain, and fog computing was presented in [11]. The research mainly focused on the economical aspects rather than technical details, in a step towards understanding the threats, challenges, benefits, and expectations of replacing national currencies with cryptocurrencies. A comparison of the cost of computation and storage when using Ethereum

[2]papers whose titles include the words "Blockchain" AND "Fog", at: scholar.google.com; last accessed: February-15-2020, and ScienceDirect.com; last accessed: February-16-2020.

TABLE 1. Surveys discussing FC-BC integration, including our work.

Ref.	Domain	Year	Aim
[11]	Economy & Politics	2017	Compare Cryptocurrency to national currencies
[12]	FC-BC	2018	Compare Golem, iExec and SONM projects
[13]	Smart environments	2019	Assessment and Analysis of Smart IoT-BC
[14]	IoT-FC	2019	Security and Privacy
[15]	IoT-FC-BC	2019	Cryptography assisment
[16]	SIoV	2019	Trust factors, challenges, models, and vision
[17]	eHealth-BC	2020	State-of-the-art Identity management systems
[18]	IoT-FC-BC	2020	General concepts (Book Chapter)
Our Survey	FC-BC	2020	State-of-the-art Integration Assessment

blockchain vs. when using Amazon SWF was conducted in [19]. Accordingly, it was found that the average cost of executing the same process instance on Ethereum is two orders of magnitude higher than on Amazon SWF, i.e. 0.000925US$/instance on SWF vs. 0.36US$/instance on Ethereum.

Authors of [12] surveyed three ongoing Fog-Based BC projects; Golem, iExec and SONM, from a technical point of view. The survey concluded that, even for those three most mature Fog-Based BC solutions, they still lack standardization since they are mainly based on ad-hoc communications. The three solutions use Ethereum[3] platform with different properties. SONM focuses on IaaS and plans to later support PaaS. Golem provides only SaaS, where users assign tasks to be performed by Providers whose probability of payment equals to v/T; v being the amount of money the provider deserves, and T being the total money paid for the provided service. For IExec, the Proof-of-Contribution (PoCOT) [20] algorithm is used, while a security deposit is made by providers, just like in the Proof-of-Stack (PoS) [21]. Providers have the choice to offer their services in an Application Store, while consumers of the service are able to choose the provider according to the reputation and the prices offered.

In 2019, authors of [13] provided a comprehensive study on approaches of smart campuses and universities. The study highlighted main features, communications architectures, BC potential applications, examples, and challenges of smart IoT-Fog-Cloud campus deployment. It was indicated that using traditional database systems provides more efficient latency and energy consumption than using BC, hence, BC deployment is not always the best choice. However, according to this study, only one out of 13 studied smart campus deployments supported FC, while none of them supported BC. Authors of [14] surveyed potential security and privacy challenges in fog-enabled IoT systems, while they shallowly discussed how BC may enhance such systems.

Authors of [15] investigated light weight cryptographic solutions that might be suitable for IoT-FC-BC systems. As transactions must be signed in order to be validated, the faster the signing, the faster the system. Accordingly, an experimental comparison evinced that hashing and encoding using ChaCha with EdDSA, instead of SHA-256 with elliptic curve cryptography (ECC), respectively, enhances a fog-based BC system in terms of CPU utilization and number of network transmitted packets. In [16], trust management models for the Social Internet of Vehicles (SIoV), were surveyed and discussed. In contrast, they analyzed the trust factors in such systems, such as the reputation, the environment, system expectations and goals, etc. then they analyzed the challenges faced by a trust management system in SIoV systems, such as the privacy, the heterogeneity, mobility, and Quality of Service (QoS). After that they reviewed existing Trust models, and trending solutions to solve the challenges faced by such models, such as BC and FC, and how blockchain and fog computing can boost the development of trusted SIoV model. Accordingly, they presented and discussed the envisioned future SIoV network when enhanced by BC and FC.

Lately in 2020, authors of [17] surveyed decentralized Blockchain-based identity management systems, and the possible scenarios of adopting such systems to enhance health-care applications. While authors of [18] presented the basic concepts of IoT, FC, BC, the FC-BC general deployment framework, opportunities, and challenges. They clarified how the decentralization property of BC can be applied at the device level, the fog level, or the cloud level, and briefly discussed some of the famous consensus algorithms.

All presented surveys came to an agreement on advantages of the BC-Fog integration, which include enhanced security, integrity, reliability, fault-tolerance, and credibility, thanks to the distribution of processing units of IoT and FC, and the decentralization and trust management mechanisms deployed within the BC algorithms. On the other hand, such combination of different technologies suggested agreed on challenges as well, such as Privacy issues, Latency, Legal issues, and Standardization issues.

III. BC-FC PROPOSED INTEGRATION SOLUTIONS

In this section, we present and discuss the remaining 43 articles that propose systems to benefit from the advantages of BC-FC integration, or proposing solutions for different challenges faced by the FC-BC integration. Having analyzed these papers, we found that most of the papers discuss solutions for IoT-FC-BC integration. Maybe this is caused by the fact that FC was initially introduced

[3]https://ethereum.org/

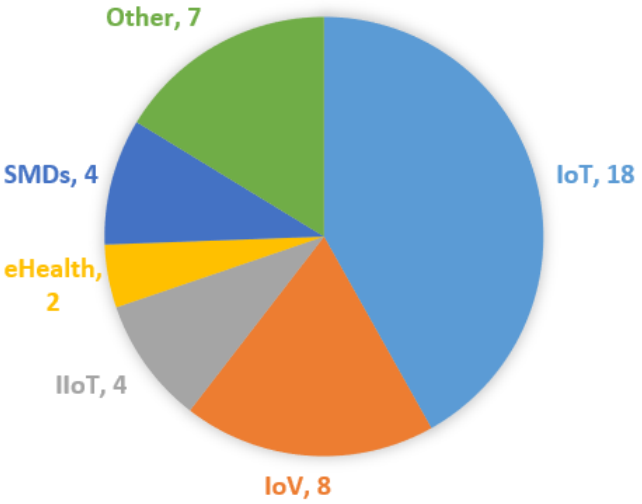

FIGURE 3. A categorization of the studied articles according to their research domain.

to specifically rise and enhance IoT applications. However, we found that other papers discuss FC-BC integration when deployed in different environments, such as Smart Mobile Devices (SMDs), Internet of Vehicles (IoV), Industrial Internet of Things (IIoT), and eHealth. Figure 3 presents our categorization of the 43 articles according to their domain, while Table 2 concludes those articles regarding their domain, the role that the deployed BC played, the used consensus algorithms, the layer of FC where BC is deployed (as FC architecture's default definition clarifies it has three main layers [22]), and the properties/challenges that the corresponding article had enhanced. In Table 2: D, I, T, R, E, F, C, and O notations stand for: Data Storage Management, Identity/Authentication Management, Trading/Payment Management, Rating/Reputation Management, End-User layer, Fog Layer, Cloud Layer, and Other purpose/layer, respectively. In the following sub-sections, we discuss the articles according to the domain categorization presented in Figure 3.

A. INTERNET OF THINGS APPLICATIONS (IoT)

Similarly to the SaaS and PaaS paradigms provided by the cloud, authors of [23] proposed Blockchain-as-a-Service in FC-IoT systems, for which finding the hosting environment was declared as the biggest challenge. That is, the Things are, by definition, resource and energy limited. On the other hand, hosting the BC in the cloud increases the latency, which was an original drawback of Cloud Computing that FC was proposed to solve. Hence, the authors were only left with the option of hosting the BC in the fog layer, which was experimentally proven to be the best choice.

In 2017, authors of [4] proposed a distributed cloud architecture based on BC technology with Proof-of-Service (PoSER) consensus, in order to speed up the processing of large amounts of IoT data. In this architecture, the fog nodes provides the computation capabilities while the cloud layer plays the controlling and monitoring role. Computations and storage tasks are handled by the fog nodes as long as they are able to, otherwise they are offloaded to the cloud which, apparently, may increase the latency and resource consumption. The BC is deployed in the cloud layer to allow the user to choose/award the service provider, and to enhance the transparency of the cloud reputation regarding the provided service. Contributions, such as the performance of a computation, the transfer/storage of a file, are registered into the BC, hence providing a proof of the service provided. Authors of [24] proposed mapping the identity of the Things to the IP address of the gateway they are connected to, and save these information in a BC. Accordingly, no sybil or spoofing attacks occurs, nor does a single point of failure, which are issues that may occur when using a classic database.

In 2018, authors of [25] investigated deploying cloud/fog resources as computing power of the Proof-of-Work (PoW) [9] based BC miners. That is, exhaustive puzzle solving computations being offloaded to the cloud instead of being locally solved, if the profit was maximized. Authors of [26] proposed a TTP-free BC-Fog authentication scheme using Ethereum platform, aiming to control the remote access to Things in IoT systems. Fog nodes in this scheme are responsible for the storage, computing, and access management tasks on behalf of a group of IoT resource-poor devices. Further, keccak256 hashing algorithm was deployed, while the primary role of the chain is to hold a list of users and their authorized access to IoT devices. The access authority granted for users is configured by system administrators at the initialization phase of the system, and can be updated through time. Authors of [27] presented their BC-based IoT-Cloud supply chain system, whose main purpose is evaluating quality metrics for agriculture and food production. BC was deployed as a trusted, reliable, immutable, database to collect and save sensed data. The results of the proposed system is provided in [64].

In 2019, authors of [28] proposed CrowdChain, a Fog-assisted Blockchain-based crowd sensing framework, where BC is deployed for performing the payments/rewards, and record the identities in a chain located in the fog. Proof-of-Concept (PoC) [65] was used by [29] in the MultiChain[4] platform, where Blockchain-based Function-as-a-Service was proposed to have immutable, local storage of protected streamed real-time sensor data. Another approach for integrating FC and BC proposed in [30], where the concept of Plasma BCs was deployed. The Plasma BCs concept suggests that various BCs be dedicated for different purposes in the same system, where each is a parent or a child of other chain. Clearly, such concept fits perfectly, if well implemented, in a FC architecture, where fog nodes manage edge devices, and are managed by fog servers. The proposed integration enhances the security and privacy as parents and children are only aware of the least information about each other.

[4]https://www.multichain.com/

TABLE 2. Blockchain deployment in FC-BC integration.

Domain	Ref.	Blockchain Role	Algorithm	FC Layer	Enhanced Property/Solved Challenge
IoT:	[23]	D, I, T, & R	N/A	F	Latency & Standardization
	[4]	R	PoSer	C	Latency & Optimization
	[24]	I	N/A	F	Privacy & Security
	[25]	T	PoW	C	Energy Consumption
	[26]	I	PoW, keccak256	C	Privacy
	[27]	D	N/A	C	Security
	[28]	T & I	PoW	F & C	Privacy & Security
	[29]	D	PoC	C	Security & Standardization
	[30]	D, I, T, & R	PoC	F & C	Privacy & Security
	[31]	D	PoW	F & C	Standardization
	[8]	D	PoW	F	Security & Standardization for DTB apps
	[32]	D	N/A	C	N/A
	[33]	D	N/A	C	N/A
	[34]	O	N/A	F	Security
	[35]	D & R	N/A	C	Reliability & Credibility
	[36]	D	PoW	C	High efficiency using dockerized components
	[37]	R	PoW	F & C	Security, Privacy, & credibility
	[38]	R & I	PoA	F	Trust
SMDs:	[39]	D & I	PoC	F	Mobility
	[40]	D & T	PoW	E & C	Offloading Computations to the Fog
	[41]	T	PoW	C	Resource efficiency
	[42]	D	BFT	C	Standardization & access control
IoV:	[43]	D	PoS	F	Privacy
	[44]	D	PoS	C	Heterogeneity & Privacy
	[45]	D	PoET	F & C	Latency
	[46]	D, I & R	PoW & PBFT	F & C	Inter-operation & Mobility of VANETs
	[47]	D	PoW	C	Security
	[48]	D & T	zk-SNARKs, DAP	C	Decentralization and Anonymity
	[49]	D & I	PBFT	F & C	Privacy & Security
	[50]	D & I	PBFT	F & C	Security & Network Overhead
eHealth:	[51]	D	N/A	F	Security
	[52]	T	PoW & PoA	C	Latency & Security
IIoT:	[53]	D, T & I	PoW & PoA	C	Trust & Optimization
	[54]	D	HLF	F & C	Security
	[55]	D	PoW OR PoS, OR PoA	C	Heterogeneity & Resource efficiency
	[56]	T	PoC	C	Trust
Other:	[57]	I	PoC	F	Security
	[58]	I	PoS	O	Privacy & Security
	[59]	I	PoAh	C	Privacy
	[60]	O	PoW	O	Energy & Memory Consumption
	[61]	T	PoC	C	Flexible Heterogeneous deployment
	[62]	D & I	PBFT	C	Security
	[63]	T	PoW	F & C	QoS & Security

The authors implemented and validated their proposed system using PoC algorithm and Ethereum platform.

Authors of [31] proposed an integration framework for IoT-Fog-Cloud infrastructures, namely FogBus, wherein a Java implemented PoW-based BC is supported for applications requiring high data integrity. Introducing a real-world case study, different criteria of FogBus were measured resulting higher latency, network usage, and energy consumption when Blockchian is used instead of regular database, which agrees with the results in [13], and explains the results in [19].

Authors of [8] proposed virtual segregation of the fog layer into two clusters. One of them behaves similarly as a middle layer between the Things and the cloud. The other cluster is dedicated to BC-related tasks, namely Fog Mining Cluster (FMC). Here, the latency effect, caused by the addition of a PoW-based BC, was deeply discussed. They concluded that out of the three main categories of IoT-FC applications (i.e. Real-Time applications, such as traffic collision avoidance systems, Non-Real-Time applications, such as weather updates systems, and Delay-Tolerant Blockchain applications (DTB), such as smart parking lot systems, and smart home systems, only DTB applications are advised to deploy BC. Nevertheless, in their proposed model, a PoW-based BC was deployed in the FMC cluster, which contains the mining fog nodes, to mine the blocks containing data obtained from Things.

Authors of [32] proposed a framework for IoT-FC systems controlled and managed by an SDN network. BC was added to this framework only as a structural component; hence, BC was not integrated nor simulated with the proposed framework. Similarly, authors of [33] presented a SDN-based architecture in which the Things connect with, and use, cloud

resources through fog nodes and gateways. BC was suggested to be deployed in the cloud to save the analyzed data, and the set of transactions executed in the system. However, the usage of BC, as data management approach, in this architecture was not analyzed nor shown to be more efficient than other approaches. Authors of [34] proposed a multi-fog BC model to increase the availability in the LSB model proposed in [66]. The proposed model uses the property of broadcast domains that appears with the deployment of FC, hence, distributes the tasks to different domains in order to decrease the probability of security attacks.

Authors of [35] proposed a model in which BC is deployed in IoT-Fog-Cloud environment, to hold information about the contributed resources by fog nodes. The resulting BC in this system provides reliable and credible evaluation index for fog nodes. In this model, the BC presents a log of satisfaction of system components by fog nodes; i.e. the more completed tasks and contributed resources fog nodes provide, the higher the satisfaction degree, and hence the more profit for the fog nodes. Authors of [36] presented an intuitive bench framework aiming to enable easy design of software, namely VarOps. The proposed framework considers the variability property, which makes it possible to re-use docker components, and hence, increase the efficiency of new proposed solutions. The proposed framework deploys BC as a data management controller, Smart Contracts for validating requests, Trustful and Trust-less Smart Oracles for controlling the components of the docker technology, and presents some example use cases.

Authors of [37] proposed a creative reputation system for fog nodes, that are delivering services to the IoT devices, using BC Ethereum smart contracts. The system suggests that IoT devices rate fog nodes according to specific criteria, and fog nodes obtain, accordingly, trustworthiness value that would indicate how reliable they are. Meanwhile, IoT devices' credibility is also computed, according to specific contributions, for the more credible the IoT device, the more effective its evaluation is on the final score of evaluated fog nodes. On the same topic, yet on the contrary, authors of [38] proposed a BC-Based Trust Management model in which the ''run by the fog'' chains store the trustworthiness values of network entities according to given criteria, and store entities' real identifiers. When an entity's trust value is requested by some IoT devices, the fog responds with the requested value obtained from the locally-saved chain. However, this trust management model requires the IoT device to be connected to at least three fog nodes in order to forbid faulty responses from a probable malicious fog node, which might be considered a drawback.

B. SMART MOBILE DEVICES APPLICATIONS (SMDs)

In 2018, authors of [39] proposed a BC-based Distributed Mobility Management handover scheme in fog environments. Their solution focused on the resolution of hierarchical security issues without affecting the network layout. The proposed scheme deployed three different BCs; one in the fog server recording the failed handover attempts, the second controls the mobility anchors and access routers, while the third embraces the mobile entities' information. Authors of [40] presented an approach to enable mobile end-users to offload their computations to fog nodes while moving. The proposed approach used a Spacial-Temporal Database with R-Tree data structure, a PoW-based BC, and suggested FogCoin tokens, all deployed for rewarding system entities for their computation power. However, it also suggests that each mobile device saves and updates the whole chain locally, which we believe is a drawback, because of the high energy and storage consumption expected to be tolerated by the resource-limited end mobile devices.

In 2019, authors of [41] proposed an auction mechanism for offloading computations, such as puzzle solving tasks in PoW, from resource-poor BC miners, such as mobile devices, to the fog or the cloud. This allocation of computing resources to miners was shown to be computationally efficient. Authors of [42] proposed Blockchain-as-a-Platform for FC applications using the Corda distributed ledger platform.[5] Groups of vacuum cleaners, representing Things, were connected to Raspberry Pi nodes, representing fog nodes, to which the maps of the cleaned areas were transmitted. The maps then were transmitted to the Corda platform, representing the cloud, in which data are processed and saved on the BC. Finally, the user monitors and controls the system through a web-server software.

C. INTERNET OF VEHICLES APPLICATIONS (IoV)

In 2018, authors of [43] proposed a privacy-preserving BC-assisted Fog-Cloud carpooling scheme, where BC is deployed for data management. The deployed private BC in this scheme uses the PoS algorithm for clients selection, and only stores the hash values of encrypted carpooling data, while the actual data are saved on the cloud. Fog nodes on the other hand are deployed for collecting real-time carpooling queries, and for matching passengers with drivers.

In 2019, authors of [44] proposed the integration of the IoV with FC and BC in a system where drivers from different service providers can be paired with riders. Such proposal makes it possible to combine clients of different companies, to provide more consumption of the service, and hence more revenues. Meanwhile, the privacy of users is preserved by anonymous authentication scheme, and BC is deployed for recording rides and creating smart contracts to pair riders with drivers. Authors of [45] deployed an alternative of the PoW algorithm, similar to the recently proposed Proof-of-Elapsed-Time (PoET) consensus algorithm [67], in their proposed BC inspired IoV framework. To do so, they investigated classical epidemic flooding based, network coding inspired and chord protocols, while they designed a BC-based distributed consensus sensing application. The system has been tested by resorting to the OMNeT++ framework to achieve the needed results of reacting on traffic anomalous conditions. BC in

[5]https://www.corda.net/

this framework was deployed as a log of past transactions related to a specific important incident that needs to be kept unchanged, such as the occurrence of an accident.

Authors of [46] analyzed the BC-SDN integration for effective operation of Vehicular Ad-hoc Networks (VANETs) in 5G and fog computing paradigms. BC was deployed here for several purposes; authentication, access control, data management, reputation management (through a proposed trust model), and policy enforcement (using smart contracts). FC on the other hand, was deployed to enhance the handover problems in such high mobility environment. Authors of [47] suggested a distributed PoW-based BC architecture for securing VANETs, where BC keeps a record of services, provided by different cloud providers. Meanwhile, FC is deployed for connecting the vehicles directly to the BC.

Authors of [48] proposed a BC-based IoV data transaction scheme, where BC is deployed for payment purposes. The proposed scheme allows data consumers to anonymously get/pay the data they need/the service, using asymmetric encryption and smart contracts. The full anonymity in this scheme was guaranteed by using a Decentralized Anonymous Bitcoin Payment (DAP) scheme, which is a part of the Zero-Cash proposal in 2014 [68].

Authors of [49] proposed a BC-assisted authentication for distributed Vehicular Fog Services (VFS). A consortium, permissioned, semi-decentralized BC model, in which selected group of nodes are responsible for block validation, and Practical Byzantine Fault Tolerance (PBFT) [69] consensus algorithm, were adopted. Pseudonyms were used in this mechanism to guarantee the anonymity, as with each authentication a new pseudonym is generated by the client vehicle itself. However, BC is not deployed for keeping authentication keys, but for storing authentication results, while the keys are generated in a corporation with a fully trusted authority. On the same topic, authors of [50] deployed ECC in a BC-based IoV authentication and key-exchange scheme, where PBFT-based BC was also deployed for maintaining the network information, and ECC was deployed for the actual authentication. The proposed scheme was compared with [49], and was found more efficient in terms of computational and communications overhead, and was validated in terms of security and safety using the AVISPA tool [70].

D. E-HEALTH APPLICATIONS

In 2019, authors of [51] proposed a BC-based human activity monitoring framework for eHealth applications without declaring the properties, or deployment methodologies of the used Blockchain. Authors of [52] proposed a BC-IoT system that monitors Glucose levels for Diabetes patients. Their proposed system takes advantage of the low latency of computations offered by FC for mobile sensors, which is highly beneficial in emergency situations, while BC is deployed to incentivize patients for sharing their private health information, and to allow them to securely and privately buy medical equipment. In this solution, BC is built using a metacoin called GlucoCoin, and the system was evaluated by having it run on two different Ethereum testnets; Rinkeby (Proof-of-Authority (PoA) [71]) and Ropsten (PoW).

E. INDUSTRIAL INTERNET OF THINGS APPLICATIONS (IIoT)

In 2018, authors of [53] proposed a Blockchain-based Industrial Internet of Things (IIoT) Bazaar, using Ethereum and PoA. The main goal of this Bazaar idea is to provide a marketplace for IIoT applications based on the technologies of FC, BC, and Augmented Reality. BC was deployed for performing trusted payment transactions, trusted authentication for consumers and providers, and application data storage.

In 2019, authors of [54] studied how to integrate BC and fog technologies in a smart factory environment. Accordingly, they proposed an IoT-Fog-Cloud system architecture where the cloud and fog nodes act as BC nodes. The main usage of the BC was to record and register the transactions performed between the three layers of the system.

In [55] the deployment of BC in supply chain MCM networks was proposed for originated systems in the 4.0 Industry era. The BC in this proposed framework replaced the regular database to save data generated by the Things and fog nodes, and the decisions made by the cloud. This replacement was theoretically shown to be beneficial for connecting highly-heterogeneous resources within the network. In [56] a Trust Management architecture for a CCTV system, using PoC algorithm in FC platforms, was proposed. In this architecture, BC was basically deployed for collecting payments using a proposed smart AI protocol.

F. OTHER FC-BC APPLICATIONS

In 2018, authors of [57] proposed a BC-enhanced FC security architecture, namely FOCUS, where the BC is deployed as an identity management ledger by recording users and organizations identities.

In 2019, authors of [58] surveyed the smart contract protocols and proposed three-party TTP-Free BC-based smart contract signing protocol in Fog environments. The BC role was to guarantee that all signing parties will reveal their signature or they will lose their deposit as a penalty. Authors of [59] proposed a BC-based authentication mechanism to mainly forbid cloud insider attacks that may actively manipulate, or passively disclose, private clients' data. Using this system, data is saved regularly at the cloud, but can only be disclosed by authenticated users. credentials are saved on BC while any entry to the data shall be preceded by a proof of authentication (PoAh) [72]. The proposed mechanism was proven mathematically and experimentally optimal against insider data manipulation. Authors of [60] proposed a statistical method to solve the puzzle in the PoW algorithm using the expectation maximization algorithm and polynomial matrix factorization. The proposed method achieves the puzzle solution with less iterations, leading to less required time, energy, and memory consumption.

Lately in 2020, authors of [61] presented their initial work results on the DECENTER project.[6] The showcase deployed Ethereum BC for payment orders, while using a PoC algorithm. The project aims to help users extend their infrastructures, and easily get access to private computational resources using FC through simple GUI. Authors of [62] suggested adding the BC to their previously-proposed approach in [73], for protecting fog-enabled systems from malicious nodes. BC was deployed in this approach for delivering two services: data management and data access control. Also, a Cryptographic Materials Issuer, which can be somehow considered a TTP, and PBFT algorithm were both deployed in the approach. The approach was not tested nor simulated as the authors considered it as their future research direction.

Authors of [63] proposed a BC cryptocurrency-based payment system for the provided public fog services. In this approach, fog nodes provide computation and storage services for end-users, while end-users pay for the provided services, depending on the QoS and satisfaction level using Ethereum platform. FC service providers, and end-users, are evaluated by the reputation system presented in [37]. Evaluation criteria may differ in different scenarios, but for the validation criteria of the experiments held in this research, the QoS and satisfaction for fog nodes, and commitment to payment for end-users, were evaluated.

IV. OBSERVATIONS, ANALYSIS, AND CHALLENGES

According to our detailed study of BC-FC integration solutions, provided in Sections II and III, and concluded in Tables 1 and 2, we found that the following key observations can be made:

1) BC can highly enhance FC systems in terms of Security, Reliability, and Decentralization. On the other hand, deploying BC in FC systems is costly in terms of Money, Energy, and Latency. Hence, systems that require lower costs, round-trip-time or energy consumption, should not use the BC technology.
2) As clarified in Figure 3, most of BC-FC integration solutions were proposed for IoT and related applications, such as IoV, IIoT, and eHealth applications.
3) As clarified in Figure 4, most BC-FC integration solutions deployed BC for Data Management purposes, as a more reliable alternative of a classical Database.
4) The vast majority of BC-FC integration approaches used Proof-based algorithms. To be more precise, most of the solutions deployed a variation of PoW-based consensus algorithm, Despite the fact that PoW-based BCs are the highest energy consuming compared to other algorithms. These observations are clarified in Figure 5.
5) Unless the article clearly proposes and defines another approach, we assumed that BC is deployed in the cloud layer when it is used for Payment/Trading purposes. Following this assumption, most BC-FC integration solutions deployed the BC in the cloud layer. This is clarified in Figure 6.
6) So far, BC has not yet been implemented in SMDs, IIoT, OR eHealth applications for Reputation management purposes. Also, BC has not yet been implemented in eHealth applications for Identity management purposes.

[6]https://www.decenter-project.eu/

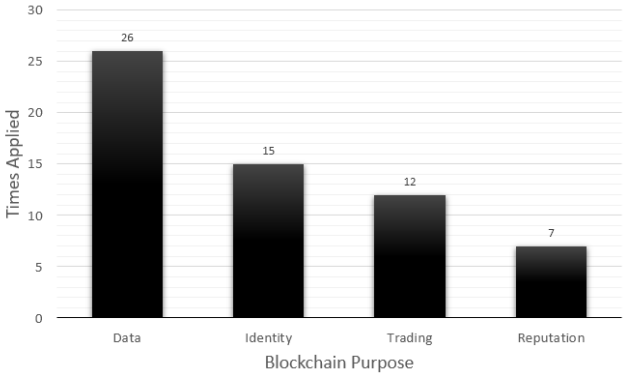

FIGURE 4. Usage of BC in FC environments.

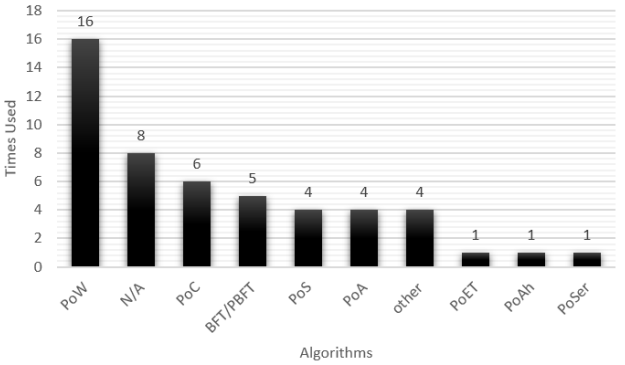

FIGURE 5. Usage of different consensus algorithms in FC environments.

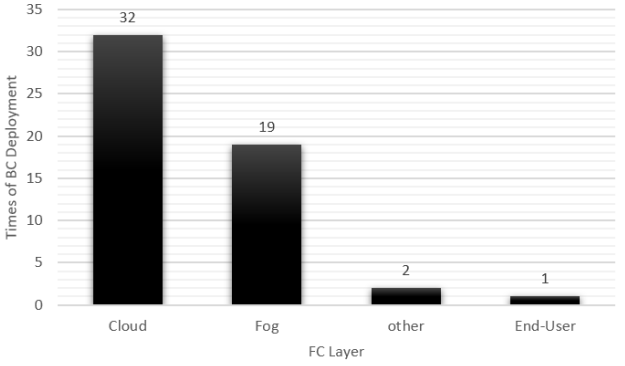

FIGURE 6. Placement of BC in the proposed BC-FC solutions.

We tried to find a correlations between the role of the deployed BC and the used algorithm, or between the role of the deployed BC and the layer where the BC is deployed, but unfortunately we could not. However, we next conclude the enhanced properties by BC-FC integration, and challenges:

A. ENHANCED PROPERTIES

1) Optimization: Several solutions proposed models or protocols that enhance the output of the system. The reached optimization solutions are mostly local, yet outperforms other solutions.
2) Security: Several articles enhanced the security using the BC instead of regular databases. The deployment of BC is highly recommended in systems that rely on the integrity and accountability.
3) Reliability & Credibility: Deploying the BC in the cloud makes the proposed system highly reliable, and almost impossible for its database to be altered by any party, especially when using the PoW algorithm. This criterion motivated many researchers to deploy the BC in the cloud.
4) Resource efficiency: The best placement of the BC in a FC architecture is the fog layer. This is because of decreasing the usage of the virtual resources in the cloud, hence decreasing the cost and latency, and increasing the QoS. However, deploying the BC increases the latency in most scenarios, hence, the balance of BC latency, DB latency, Cloud latency, shall be individually studied for each case.
5) Access control: Deploying the BC for controlling the authentication in a system was proposed in several articles. This deployment makes it nearly impossible to access information without the correct permission.
6) Decentralization: This property was shown to be highly beneficial in many applications. The BC fulfils the needed criteria to cope up with the decentralized fog/cloud, hence the successful deployment of BC in FC was shown to be beneficial, applicable, and practical.
7) Anonymity: As this is an important success factor for applications that require high levels of privacy, several articles deployed BC for obtaining anonymity of clients while using public systems. This is achieved in BC by the deployment of asymmetric encryption, and decentralized consensus without using TTPs.

B. CHALLENGES

1) Standardization: Despite the several attempts to standardize BC-FC integration, as presented in previous sections, such integration is still new. Many possibilities, and wide range of applications are encouraged to deploy BC in FC systems. Such observations imply that current standardization attempts are only the first step towards a successful standard integration.
2) Privacy: Using BC in Fog-enabled environments indeed enhances the security and anonymity of users and applications. These advantages were taken into consideration for BC deployment. Yet the full decentralization proposed by FC and BC, which leads to high levels of security, decreases the privacy levels of clients. Data and identity privacy are taken care of using BC, yet usage and location privacy are often exposed. Moreover, the privacy in FC is poorly discussed in the literature, and deploying BC in such system increases the privacy concerns.
3) Latency: The deployment of BC is proven to be beneficial for different properties. It was also proven, however, that it increases the latency and jitter in most scenarios. For this, and other reasons, such as the energy consumption of the BC systems, BC is not recommended for real-time or time-sensitive applications.
4) Energy consumption: Deploying BC is a critical factor for energy consumption levels in systems. As most of the proposed applications deployed a PoW-based BC, the energy consumption remains as a challenge despite the several attempts to use different algorithms. This challenge is generally related to any BC-based system whether, or not, it was deployed in FC environments. Other algorithms have some drawbacks that are not tolerable by some applications, this may encourage the research society to find other alternatives to the PoW algorithms, yet satisfy the high security and reliability provided by PoW.
5) Trust: As FC and BC technologies are new solutions, the first integration approach of the two was only four years ago. Today we can find less than fifty articles discussing such integration and its applications. These facts imply that such integration needs many years and a lot of efforts to become a reality. Otherwise, it will not be trusted despite many advantages it can provide.
6) Mobility: Some applications in the IoV and the eHealth domains require highly adaptive mobility controls, due to the continuous movement of clients. FC solves this, but when it is integrated with BC it becomes a challenge again. Some articles approached some enhancement of the mobility handling while deploying BC, yet this negatively affected other criteria, like latency and privacy.
7) Legalization issues: Blockchain technology is the base foundation of cryptocurrencies and digital economy. As cryptocurrency concepts are still not accepted nor legalized in many countries around the world, Blockchain technology is ignorantly illegal as well. We showed in this survey how BC can be deployed for different reasons than digital money, such knowledge needs to be globally provided that BC is not the same as digital money, yet it is the backbone of it. Having such technology being illegal leads to falling behind the global technological trends, hence, makes it a challenge for any BC-based solution.

V. CONCLUSIONS AND FUTURE WORK

As Blockchain (BC) technology was introduced in 2009, and Fog Computing (FC) was introduced in 2013, some efforts towards integrating those two technologies were made. In this survey we have discussed and analyzed published papers that integrate BC and FC technologies. We classified those papers with respect to their type, domain, year of

publication, BC role, consensus algorithm, and the layer in which the BC was deployed. Our discussion and analysis of the papers led us to several major observations, properties, and open challenges regarding the BC-FC integration. We will use and deploy those observations and analysis in our future research works whose main focus is the implementation of user-friendly Fog-enhanced Blockchain-based solutions and simulations.

REFERENCES

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, 2012, pp. 13–16.

[2] H.-J. Cha, H.-K. Yang, and Y.-J. Song, "A study on the design of fog computing architecture using sensor networks," *Sensors*, vol. 18, no. 11, p. 3633, Oct. 2018.

[3] N. Pokrovskaia, T. Khansuvarova, and R. Khansuvarov, "Network decentralized regulation with the fog-edge computing and blockchain for business development," in *Proc. Eur. Conf. Manage., Leadership Governance*, 2018, pp. 205–212.

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

[5] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency Comput., Pract. Exper.*, vol. 28, no. 10, pp. 2991–3005, Jul. 2016.

[6] Cisco. (2019). *Cisco Fog Data Services*. Accessed: Jan. 15, 2020. [Online]. Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/fog-data-services/index.html?dtid=osscdc000283

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[8] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things," *IEEE Access*, vol. 7, pp. 169073–169093, 2019.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptogr. Mailing*, Mar. 2009. [Online]. Available: https://metzdowd.com

[10] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.

[11] N. N. Pokrovskaia, "Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation," in *Proc. 20th IEEE Int. Conf. Soft Comput. Meas. (SCM)*, May 2017, pp. 709–712.

[12] R. B. Uriarte and R. DeNicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 22–28, Sep. 2018.

[13] T. M. Fernández-Caramés and P. Fraga-Lamas, "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," *Appl. Sci.*, vol. 9, no. 21, p. 4479, Oct. 2019.

[14] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, Apr. 2019.

[15] G. George and S. Sankaranarayanan, "Light weight cryptographic solutions for fog based blockchain," in *Proc. Int. Conf. Smart Struct. Syst. (ICSSS)*, Mar. 2019, pp. 1–5.

[16] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, 2019, Art. no. 1550147719825820.

[17] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: State of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, Jan. 2020.

[18] A. A. Alli and M. Fahadi, "Chapter four blockchain and fog computing: Fog-blockchain concept, opportunities, and challenges," *Blockchain in Data Analytics*. Newcastle, U.K.: Cambridge Scholars Publishing, 2020, p. 75.

[19] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Apr. 2017, pp. 257–260.

[20] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, "Proof of contribution: A modification of proof of work to increase mining efficiency," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, Jul. 2018, pp. 636–644.

[21] A. Barhanpure, P. Belandor, and B. Das, "Proof of stack consensus for blockchain networks," in *Proc. Int. Symp. Secur. Comput. Commun.* Singapore: Springer, 2018, pp. 104–116.

[22] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *J. Syst. Archit.*, vol. 98, pp. 289–330, Sep. 2019.

[23] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436.

[24] M. Y. Jung, W.-S. Kim, S.-H. Chung, and J. W. Jang, "A blockchain-based ID/IP mapping and user-friendly fog computing for hyper-connected IoT architecture," *IJICTDC*, vol. 2, no. 2, pp. 12–19, 2017.

[25] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[26] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2018, pp. 1–8.

[27] A. Carbone, D. Davcev, K. Mitreski, L. Kocarev, and V. Stankovski, "Blockchain based distributed cloud fog platform for IoT supply chain management," in *Proc. 8th Int. Conf. Adv. Comput., Electron. Electr. Technol. (CEET)*, Feb. 2018, pp. 51–58.

[28] X. Gu, J. Peng, W. Yu, Y. Cheng, F. Jiang, X. Zhang, Z. Huang, and L. Cai, "Using blockchain to enhance the security of fog-assisted crowdsensing systems," in *Proc. IEEE 28th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2019, pp. 1859–1864.

[29] H. L. Cech, M. Grossmann, and U. R. Krieger, "A fog computing architecture to share sensor data by means of blockchain functionality," in *Proc. IEEE Int. Conf. Fog Comput. (ICFC)*, Jun. 2019, pp. 31–40.

[30] M. H. Ziegler, M. Grobmann, and U. R. Krieger, "Integration of fog computing and blockchain technology using the plasma framework," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 120–123.

[31] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing," *J. Syst. Softw.*, vol. 154, pp. 22–36, Aug. 2019.

[32] A. Muthanna, A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *J. Sensor Actuator Netw.*, vol. 8, no. 1, p. 15, Feb. 2019.

[33] S. El Kafhali, C. Chahir, M. Hanini, and K. Salah, "Architecture to manage Internet of Things data using blockchain and fog computing," in *Proc. 4th Int. Conf. Big Data Internet Things*, Oct. 2019, pp. 1–8.

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

[35] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, "Blockchain-based resource allocation model in fog computing," *Appl. Sci.*, vol. 9, no. 24, p. 5538, Dec. 2019.

[36] B. Holste, V. Stankovski, P. Kochovski, A. Puliafito, and P. Massonet, "Blockchain based variability management solutions for fog native open source software," in *Proc. 27th Int. Conf. Inf., Commun. Autom. Technol. (ICAT)*, Oct. 2019, pp. 1–6.

[37] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using Ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019.

[38] M. Cinque, C. Esposito, and S. Russo, "Trust management in fog/edge computing by means of blockchain technologies," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1433–1439.

[39] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, May 2018.

[40] W. Tang, X. Zhao, W. Rafique, and W. Dou, "A blockchain-based offloading approach in fog computing environment," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Ubiquitous Comput. Commun., Big Data Cloud Comput., Social Comput. Netw., Sustain. Comput. Commun. (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, Dec. 2018, pp. 308–315.

[41] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 9, pp. 1975–1989, Sep. 2019.

[42] I. Podsevalov, O. Iakushkin, R. Kurbangaliev, and V. Korkhov, "Blockchain as a platform for fog computing," in *Proc. Int. Conf. Comput. Sci. Appl.* Cham, Switzerland: Springer, 2019, pp. 596–605.

[43] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.

[44] M. Li, L. Zhu, and X. Lin, "Coride: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Cham, Switzerland: Springer, 2019, pp. 408–422.

[45] A. Bonadio, F. Chiti, R. Fantacci, and V. Vespri, "An integrated framework for blockchain inspired fog communications and computing in Internet of vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 755–762, Sep. 2019.

[46] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4278–4291, May 2020.

[47] S. Nadeem, M. Rizwan, F. Ahmad, and J. Manzoor, "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 288–295, 2019.

[48] W. Ou, M. Deng, and E. Luo, "A decentralized and anonymous data transaction scheme based on blockchain and zero-knowledge proof in vehicle networking (workshop paper)," in *Proc. Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*. Cham, Switzerland: Springer, 2019, pp. 712–726.

[49] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[50] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. H. Ahmed, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[51] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services," *Future Gener. Comput. Syst.*, vol. 100, pp. 569–578, Nov. 2019.

[52] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the Internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care," *Sensors*, vol. 19, no. 15, p. 3319, Jul. 2019.

[53] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based IIoT app marketplaces—A case study," in *Proc. 5th Int. Conf. Internet Things, Syst., Manage. Secur.*, Oct. 2018, pp. 182–188.

[54] S.-H. Jang, J. Guejong, J. Jeong, and B. Sangmin, "Fog computing architecture based blockchain for industrial IoT," in *Proc. Int. Conf. Comput. Sci.* Cham, Switzerland: Springer, 2019, pp. 593–606.

[55] E. N. Lallas, A. Xenakis, and G. Stamoulis, "A generic framework for a peer to peer blockchain based fog architecture in industrial automation," in *Proc. 4th South-East Eur. Design Autom., Comput. Eng., Comput. Netw. Social Media Conf. (SEEDA-CECNSM)*, Sep. 2019, pp. 1–5.

[56] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Gener. Comput. Syst.*, vol. 101, pp. 747–759, Dec. 2019.

[57] X. Zhu and Y. Badr, "Fog computing security architecture for the Internet of Things using blockchain-based social networks," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1361–1366.

[58] H. Huang, K. Li, and X. Chen, "Blockchain-based fair three-party contract signing protocol for fog computing," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 22, p. e4469, Nov. 2019.

[59] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors*, vol. 19, no. 20, p. 4444, Oct. 2019.

[60] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[61] M. Savi, D. Santoro, K. Di Meo, D. Pizzolli, M. Pincheira, R. Giaffreda, S. Cretti, S.-W. Kum, and D. Siracusa, "A blockchain-based brokerage platform for fog computing resource federation," in *Proc. 23rd Conf. Innov. Clouds, Internet Netw. Workshops (ICIN)*, Feb. 2020, pp. 1–3.

[62] M. Alshehri and B. Panda, "A blockchain-encryption-based approach to protect fog federations from rogue nodes," 2020, *arXiv:2001.04490*. [Online]. Available: http://arxiv.org/abs/2001.04490

[63] M. Debe, K. Salah, M. H. Ur Rehman, and D. Svetinovic, "Monetization of services provided by public fog nodes using blockchain and smart contracts," *IEEE Access*, vol. 8, pp. 20118–20128, 2020.

[64] D. Davcev, K. Mitreski, S. Trajkovic, V. Nikolovski, and N. Koteli, "IoT agriculture system based on LoRaWAN," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–4.

[65] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[66] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and privacy," 2017, *arXiv:1712.02969*. [Online]. Available: http://arxiv.org/abs/1712.02969

[67] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* Cham, Switzerland: Springer, 2017, pp. 282–297.

[68] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474.

[69] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[70] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2005, pp. 281–285.

[71] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, "Managing smart home appliances with proof of authority and blockchain," in *Proc. Int. Conf. Innov. for Community Services*. Cham, Switzerland: Springer, 2019, pp. 221–232.

[72] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, Jan. 2019.

[73] M. Alshehri and B. Panda, "An encryption-based approach to protect fog federations from rogue nodes," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, 2019, pp. 225–243.

HAMZA BANIATA received the B.Sc. degree in computer and military sciences from Mutah University, Jordan, in 2010, and the M.Sc. degree in computer science from The University of Jordan, in 2018. He is currently pursuing the Ph.D. degree with the Doctoral School of Computer Science, SZTE, Hungary.

He is a member of the IoT Cloud Research Group, Department of Software Engineering. He is also a member of the OTKA-FK131793 Project financed by the Hungarian Scientific Research Fund. Prior to starting the Ph.D. degree in 2019, he had served in the Jordan Armed Forces for 12 years, where he was promoted to the rank of Captain, in 2017. His work experience includes different roles in the domains of ICT and security, inside, and outside the military. His current research interests include the domains of security, privacy and trust of cloud/fog computing, the Internet of Things, and blockchain systems.

ATTILA KERTESZ is currently an Associate Professor with the Software Engineering Department, University of Szeged, Hungary, leading the IoT Cloud Research Group of the Department. His research interests include the federative management of the Internet of Things (IoT), fog and cloud systems, and data management issues of distributed systems in general. He is also the Leader of the National Project OTKA FK 131793 financed by the Hungarian Scientific Research Fund and a work package Leader of the GINOP IoLT Project financed by the Hungarian Government and the European Regional Development Fund. He was a member of numerous program committees for European conferences and workshops. He has published over 100 scientific articles having more than 1000 independent citations.

Prof. Kertesz is also a Management Committee Member of the INDAIR-POLLNET and CERCIRAS COST actions. He has also participated in several successful European projects, including ENTICE EU H2020, COST IC1304, COST IC0805, SHIWA, S-Cube EU FP7, and the CoreGRID EU FP6 Network of Excellence projects.