IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received January 19, 2021, accepted March 22, 2021, date of publication April 2, 2021, date of current version April 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3070555

A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges

ALIA AL SADAWI[1], **MOHAMED S. HASSAN**[2], **AND MALICK NDIAYE**[1]

[1]Department of Engineering Systems Management, American University of Sharjah, Sharjah, United Arab Emirates
[2]Department of Electrical Engineering, American University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Mohamed S. Hassan (mshassan@aus.edu)

ABSTRACT Internet of things IoT is playing a remarkable role in the advancement of many fields such as healthcare, smart grids, supply chain management, etc. It also eases people's daily lives and enhances their interaction with each other as well as with their surroundings and the environment in a broader scope. IoT performs this role utilizing devices and sensors of different shapes and sizes ranging from small embedded sensors and wearable devices all the way to automated systems. However, IoT networks are growing in size, complexity, and number of connected devices. As a result, many challenges and problems arise such as security, authenticity, reliability, and scalability. Based on that and taking into account the anticipated evolution of the IoT, it is extremely vital not only to maintain but to increase confidence in and reliance on IoT systems by tackling the aforementioned issues. The emergence of blockchain opened the door to solve some challenges related to IoT networks. Blockchain characteristics such as security, transparency, reliability, and traceability make it the perfect candidate to improve IoT systems, solve their problems, and support their future expansion. This paper demonstrates the major challenges facing IoT systems and blockchain's proposed role in solving them. It also evaluates the position of current researches in the field of merging blockchain with IoT networks and the latest implementation stages. Additionally, it discusses the issues related to the IoT-blockchain integration itself. Finally, this research proposes an architectural design to integrate IoT with blockchain in two layers using dew and cloudlet computing. Our aim is to benefit from blockchain features and services to guarantee a decentralized data storage and processing and address security and anonymity challenges and achieve transparency and efficient authentication service.

INDEX TERMS Blockchain, IoT, smart contract, trust, IoT challenges, IoT security, decentralized IoT, cloudlet computing, dew computing, cloudlet-dew architecture.

I. INTRODUCTION

In today's digital world, advances and transformation in electronics, wireless communications, and networking technologies are not only rapid but also remarkable. While this led to a distinguishable hype in the performance of wireless devices and sensors, leading to the emergence of the Internet of things (IoT), it resulted in a significant increase in the complexity of cloud services and structures, as well. IoT was facilitated by the capabilities of Wireless Sensors Networks (WSN), Radio Frequency Identification (RFID), in addition to advances in other devices to sense, communicate and actuate through existing network infrastructure [1]. IoT allows for a digitally connected real world, whereby connected devices can exchange collected data, interact with each other, and remotely control objects across the Internet, possibly without human intervention. Basically, IoT is where the Internet meets the physical world [2] such that societies and industries can benefit from IoT to achieve a quantum shift towards a smart digitally controlled world. Therefore, the ways with which people interact with one another and with their surroundings as well as with the environment have been improved and reshaped due to the implementation of the IoT technologies. Consequently, one can say that people have reached a better understanding of the world while the IoT enables more efficient interaction with it.

Moreover, the IoT does not only enable a huge range of applications but covers a wide span of societies and industrial needs, as well. Specifically, IoT is expected to play a major role in transforming ordinary cities into smart ones,

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandra De Benedictis.

houses into smart homes, electrical grids into smart grids, and so on. Additionally, IoT has diverse applications including healthcare, sports, entertainment, as well as environmental applications and many more. On another front, IoT can be thought of as the backbone of digitizing the industrial sector by enabling optimized production and manufacturing processes in addition to cost reduction. Additionally, IoT has the ability to connect a huge number of devices to the extent that the number of connected IoT devices and sensors was estimated to reach 20 to 50 billion by 2020 [3]. It is also expected that IoT could be more complex in the future leading to a Network of Plentiful Things (NPT) [4].

Relevantly, due to the successful implementation of IoT in different fields, the number of newly established IoT networks is increasing around the world. As a result, IoT is becoming increasingly popular for consumers, industries, and organizations of different natures. Therefore, the need to develop and elevate the domain becomes essential bearing in mind the number of challenges posed by such an exponential evolution.

The significant proliferation of IoT applications in various sectors places some serious challenges that could limit the successful deployment of IoT, on one hand, and could possibly degrade the performance of existing systems, on the other hand. Unfortunately, these challenges could strongly be interrelated, therefore, a comprehensive system study is essential to understand these challenges and overcome them. It is also important to note that IoT is not a stand-alone technology but rather an integration of multiple technologies including communication and information technologies, electronic sensors and actuators in addition to computing and data analytic, all collaborating towards achieving the desired smartness [5], [6]. Unfortunately, the integration of those technologies increases the complexity of IoT systems, especially when implemented on large scales. Therefore, to address any arising issues when integrating scattered patterns of IoT devices using networks' interconnection, a central server structure was proposed in which all connected devices use for authentication. Such a structure can clearly call for unreliable interconnection of the integrated devices permitting sharing data with falsified authentication, which in turn can result in an insecure data flow [7]. Thus, centralized architectures of IoT networks could suffer from the difficulty of fulfilling the trust factor. In a related context, information trustworthiness is vital for the efficient operation of IoT networks [8] since connected devices would interact and operate based on this information. The challenge here is how far the data in IoT systems can be trusted. Usually, people trust the information provided by governments and financial institutions, but the question now is how to make sure that this information is not falsified or tampered with? The same applies to companies providing IoT services. Clearly, information fed by certain entities to IoT servers could be modified according to their interests, therefore, when this falsified information is communicated through the network to act upon, the performance of the whole network gets disturbed accordingly [9]. This is just another reason the centralized model of most IoT platforms could raise an issue of impracticality. Therefore, in many cases, devices need to perform data exchange directly and autonomously. Thus, many efforts have been made towards deploying decentralized IoT platforms [10]. Moreover, it is well known that a distinct attribute of IoT is generating an enormous amount of data [7] that requires energy and connectivity to communicate, process, and possibly store over long periods of time [8]. This problem could be inflated if the underlying IoT employs a centralized structure in which data communication is entirely done through a central storage hub. The situation is aggravated if data processing is also carried out at central servers, which requires increasing the processing capabilities for the existing infrastructure especially for large-scale IoT generating an enormous amount of data [11].

Also, the ability of IoT to connect devices of different natures ranging from small wearable gadgets to massive industrial systems has opened the door for a diversity of IoT-based applications. Such applications use different frameworks in which the ecosystem characteristics, mainly security mechanisms, determine the success of their deployment [2]. Clearly, the wider the range of IoT applications, the higher the expectation to reveal more related challenges to network security and privacy. Therefore, security issues should be investigated and tackled because threats, ranging from simple manipulation of data to the more serious problem of unauthorized control of IoT nodes and actuators [2] can jeopardize the reliability of the IoT network.

It is important to note that the privacy and security of exchanged data and its computations are equally important [12]. Privacy and security issues become more crucial with regards to the current trend of Internet-of-Everything (IoE), which comprises application-specific IoTs such as the Internet of Vehicles (IoV), Internet of Medical Things (IoMT), Internet of Battlefield Things (IoBT), and so on. Some of these IoT networks such as IoMT and IoBT are data-sensitive, therefore, it is essential to ensure security at the data, systems, and devices' levels. It is worth noting that threats could also be a result of a blunder of security measures, especially for application-specific IoT systems. For instance, it is known that IT team members have full control over IoT devices, endpoints, and the overall network in general, however, they are not necessarily fully acquainted with the specificity and detailed functionalities of every single device. This could cause chaotic situations resulting in security breaches simply due to performing what seemingly looks as routine operations [12].

Last but not least, a broader view of IoT systems characterizes a growing extensive adoption of cloud computing. While cloud-based centralized IoT platforms provide upgraded and powerful analytical capabilities, they augment the security and privacy challenges and heighten the difficulty of building a trusted functioning environment compared to constrained IoT devices, which might have some form of imperfect security solutions. Based on the above, security and trust issues constitute a serious problem for the reliability of IoT systems. As a result, this brings up the need to verify data to ensure that it has never been altered [9]. Here comes the role of ''blockchain'', which was proposed as a solution to those challenges. Therefore, it is necessary to explore and understand blockchain in order to derive value from it that would be an addition to IoT systems.

Recently, it was argued that integrating the novel ''blockchain'' technology with IoT can alleviate some of the challenges facing the deployment of IoT applications. However, surveying related work in the literature, it was clear that integration of blockchain with IoT is a relatively new topic where most of the conducted studies were dated only a few years back highlighting the fact that blockchain as an emerging technology is yet to be further explored. Also, from analyzing existing researches that cover the integration of blockchain with IoT, it was evident that those works only discussed some of the challenges facing IoT and presented blockchain as a solution without proposing any practical architectures, schemes, frameworks, nor analysis to help in integrating blockchain with IoT. Not only that, such works did not address all major challenges posed by IoT applications. Therefore, this survey intends to bridge such a gap and provides a comprehensive study that covers the important aspects of the topic. Thus, the main contributions of this work can be summarized as follows:

- Demonstrate the different challenges facing IoT especially with the growing complexity and size in contrast to other reviews in the literature, which focused only on challenges mostly related to security.
- Introduce blockchain concepts and shed light on its important architecture as a promising technology with a vital role in enhancing the performance of IoT-based applications by taking care of the major challenges facing them.
- Then, summarize and compare existing work in the literature, which suggested integrating blockchain in IoT deployments. Specifically, this study provides a screening survey of the main proposed architectural designs, schemes, and frameworks in the literature with the focus of integrating blockchain with IoT. In this survey, how far the integration process has gone and what are the successful steps taken in existing related research are also addressed.
- Highlight the challenges and limitations of IoT and blockchain integration process, which provides guidance for new integration designs.
- Provide the most suitable and comprehensive IoT–blockchain integrated architecture that addresses the challenges facing IoT systems and overcomes the challenges facing the integration process as well as IoT devices constraints, and smart contract implementation.

The rest of this paper is organized as follows. Section II introduces blockchain and its classification while Section III demonstrates blockchain structure and Section VI highlights the major characteristics of blockchains. Section IV provides a briefing about smart contracts and their potential for IoT-blockchain integration. Blockchian main characteristics are explained in section V while section VI discusses blockchain for IoT. The research survey is presented in section VII and the issues facing the integration of IoT and blockchain are explained in Section VIII. A literature survey conclusion is provided in Section IX. Section X explains the design requirements and Section XI proposes a decentralized architecture of the integration of IoT and blockchain. Finally, the article is concluded in Section XII.

II. BLOCKCHAIN

The revolutionary blockchain technology is a distributed peer to peer network. Blockchain facilitates exchanging transactions and information between non-trusting entities without intermediary or centralized third party. It consists of time-stamped, append-only records of data stored immutably, securely, nevertheless privately [13]. Blockchain is defined as ''a ledger of transactions, or blocks, that form to make a systematic, linear chain of all transactions ever made. While the blocks themselves are highly encrypted and anonymized, the transaction headers are made public and not owned or mediated by any specific person or entity.'' [14].

In 2008, an unknown person or group by the pseudonym Satoshi Nakamoto presented the blockchain technology as the backbone of the cryptocurrency Bitcoin. However, since then, blockchain has established a reliable and efficient performance and found its way to many other applications such as supply chain management, digital identity, voting, healthcare services, insurance, digital assets management, IoT, artificial intelligence, big data [13] and many other applications where trust needs to be established between entities, whether human or machine, who do not fully trust each other and operate in a decentralized environment [15]. There are three types of blockchain identified as per the mechanism regulating nodes access privileges , which are public, hybrid, and private blockchain [16].

1) Public blockchain: used in cryptocurrencies network. It is a permissionless blockchain where transactions are visible by all participants in the network, however, the identity of nodes initiating those transactions are kept anonymous [16]. It is entirely decentralized, peer to peer network and is not owned by a single entity. [17].
2) Private blockchain: is a permissioned blockchain, which specifies a list of permissioned participants with particular characteristics to operate within the network [13], [16]. This type's ownership belongs to a single entity that controls the block creation [18]. A private blockchain is usually used by organizations to record transactions or assets transfer data on a limited user base [18].
3) Federated or consortium or hybrid blockchain: This is a semi-private blockchain, which is a combination of a public and a private blockchain [17]. It could be

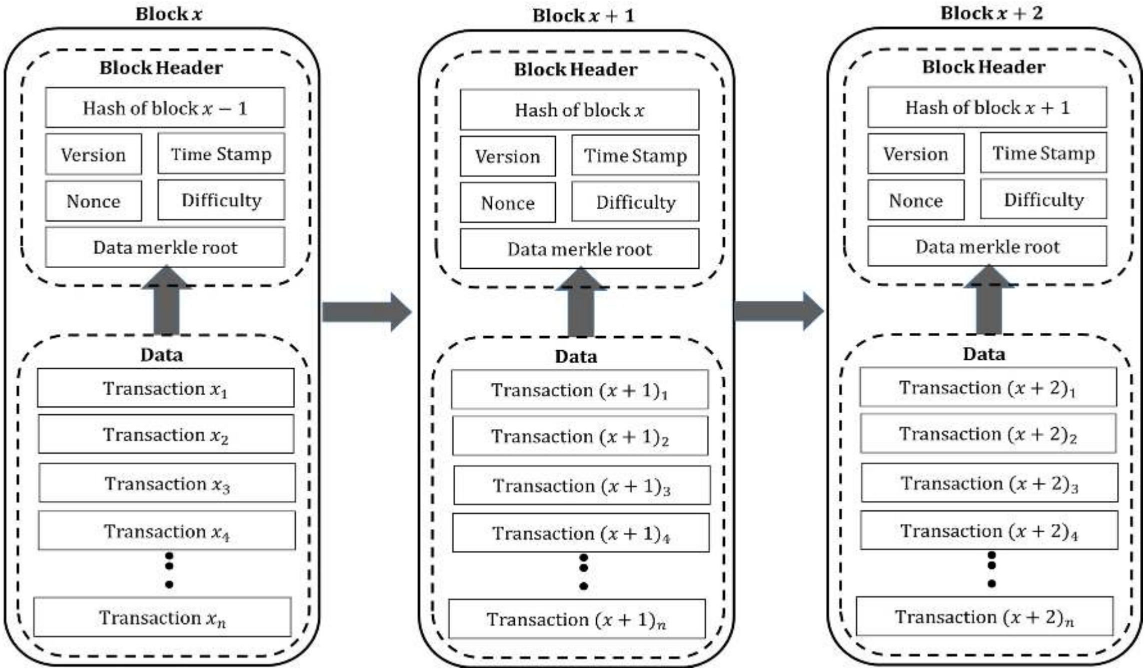

FIGURE 1. Blockchain structure.

considered a scaled-down public blockchain available to a specific privileged group of nodes.

As per the characteristics of IoT networks and based on the above classification of blockchain, it is foreseen that private and federated blockchains are the most suitable types to be integrated with IoT and add value to it. As per public blockchain, which has been so far used in cryptocurrency since it is the only network where all people might have the interest to join to trade bitcoins. However, IoT networks are designed for special purpose applications where certain groups or parties are interested in joining rather than the whole public.

III. BLOCKCHAIN STRUCTURE

Blockchain is a distributed public database of all executed digital events shared among participants. Public events records are verified by a mechanism that requires consensus of the majority of participants in the network [10]. This is called a consensus algorithm and it takes many forms such as Proof of Work (POW), Proof of Stake (POS), and others [19]. Blockchain can utilize any of them based on the requirements of the design. Figure 1 demonstrates the structure of blockchain. Basically, when information is contained in a block, it needs to be authenticated before being added to the chain. This is the role of specified nodes in the network called miners, which have to solve a mathematical puzzle of certain difficulty in order to verify the block and get rewarded for their effort. When a block is verified and chronically added to the blockchain, the contained data become immutable and can never be altered or erased. Accordingly, the identical database copies possessed by each participant get updated [20]. It is vital to know that the emergence of blockchain facilitated smart contracts implementation and made them one of the most popular technologies that add high levels of customization to traditional transactions [15]. In essence, a smart contract is an application that resides on blockchain and provides the service of linking entities that do not fully trust each other to achieve a pre-set goal or perform a prespecified function in case certain conditions occur. Many proposed IoT-Blockchain integrated architectures utilized smart contracts in the integration process in a way that serves the goal of the integration itself or resolve more challenges facing IoT. To understand smart contracts' role in the evolved IoT-Blockchain integrated design, the structure and characteristic of a smart contract should be explored first. This is demonstrated in the following section.

IV. SMART CONTRACT AND ITS POTENTIAL FOR IOT-BLOCKCHAIN INTEGRATION

In [21] smart contracts are referred to as "self-executing codes that enable the system to enforce the clauses of a contract through certain trigger events" while smart contract utility is viewed by [22] as a computerized process performed on a blockchain that is automatically triggered when a pre-set agreed on data gets recorded as a transaction in a block. In this context, and as per [10], one of the important characteristics of operating in a digital environment is the ability to create programs and algorithms that could be executed to perform a specific action without human intervention in case a certain pre-set term(s) agreed to by all involved parties occur. Smart contracts are programs or coded scripts that have unique addresses and are embedded in the blockchain network. An IoT device representing a node can operate a smart contract by just sending a transaction to its address. Every smart contract automatically and independently gets executed on every node in the blockchain. Therefore, every node will run as a virtual machine (VM), and the blockchain network will act as a distributed VM [21] while the system, as a whole, operates as a single ''world computer'' [23]. The execution of the contract is enforced by the blockchain consensus protocol.

When a smart contract is executed, each node updates its state based on the outcomes obtained after running the smart contract. Such a replication process provides great potential for decentralized network control [24]. Consequently, tasks and actions usually managed or performed by a central third party authority are transferred to the blockchain [19].

Smart contracts are supported by many blockchains, however, Ethereum is the first blockchain that adopted smart contracts. It is a public, distributed, blockchain-based computing platform and operating system, and the second-largest cryptocurrency after bitcoin [25]. Ethereum was launched in the year 2015 as the world's programmable blockchain, which means that it could be used by developers to build brand new types of decentralized applications or ''dapps''. Ethereum decentralized applications are predictable, reliable, and combine the benefits of blockchain technology and cryptocurrency. Ethereum's digital money is called Ether or ETH and can be used in many Ethereum-based applications. It is worth mentioning that no company or centralized organization controls Ethereum. It is maintained by diverse global contributors who work on the core protocol and consumer applications.

Once Smart contracts are uploaded to Ethereum, they will automatically run as programmed every time they get triggered [23]. The node that initiated the smart contract pays an execution fee called ''Gas'' to perform the function of the program. Gas is the incentive for nodes to perform the contract and ensure that it is obliged by the blockchain network. It is scaled according to the amount of computational power needed to perform the contract functions [26]. Smart contracts have associated code and data storage. The code is written in a high-level language called ''Solidity'', which is explicitly used to write smart contracts and supports their execution in the Ethereum world computer decentralized environment. However, the code should comply with a low-level bytecode in order to run in the EVM. EVM stands for a virtual machine that is similar to a computer's CPU, which runs machine code such as $x86 - 64$ [23].

Smart contracts run only when called by a transaction. However, a contract can call another one, which in turn may call another contract and so on. It is important to note that smart contracts cannot run in the background or by themselves. Also, they cannot be executed in parallel, therefore, Ethereum world computer is considered a single-threaded machine [23]. Smart contracts are turning into complete systems [26], meaning that they can solve any computation problem. This is an extremely important feature added to blockchain especially that it allows most of existing verifiable programs to transfer to and operate in blockchain [26]. Moreover, smart contracts have many advantages that add automation and therefore strengthens blockchain. One of which is that they are superior to traditional agreements due to the security they provide since they are stored and executed in blockchain. Also, the self-executed events and actions are easily traceable in blockchain and are irreversible. Furthermore, those contracts are updated in real-time and are capable of executing actions and trades. Lastly, the above features of smart contracts do not only reduce significantly the network-performance' costs [21] but lower anticipated risks [13], errors, and disruptions, as well.

Smart contracts were proposed as a cornerstone in comprehensive systems combining IoTs and blockchains. The result is an autonomous system aiming to pay for consumed and provided IoT resources [27]. Also, smart contracts manage and record all IoT interactions while providing a reliable and secured processing tool resulting in trusted actions. Therefore, smart contracts can securely model the logic supporting IoT applications [28].

Since a smart contract consists of functional codes and data with a specific address on a blockchain, then any device can call the functional code. Consequently, functions can trigger events resulting in applications, which can listen to events and react to them [28]. An outstanding example is a system adopted by Kouvola Innovation in Finland in which pallets were equipped with RFIDs and provided with shipping tasks and willing carriers. RFIDs communicate pallets' needs to potential carriers using a blockchain. When an offer is provided by a carrier, the blockchain aligns it with pre-set conditions, price, and service. If the offer matches the pre-specified conditions, the smart contract gets executed automatically on blockchain, and pallets are moved as per the contract. Every move is visible and traceable on blockchain thanks to RFIDs and sensors [29]. It is worth mentioning that the majority of IoT applications either use Ethereum or at least are compatible with it. Basically, smart contracts define the application logic and the IoT devices connected to it send their measurements and data whenever a transaction calls for that particular smart contract [30]–[32].

V. BLOCKCHAIN CHARACTERISTICS

As demonstrated, blockchain is characterized by a robust structure that grants it many valuable features. The following are the main distinguishing features, which add value to any sector implementing blockchain technology [13], [16], [33]:

1) Decentralization: network participants have access to data records without the control of a central authority.
2) Distribution: each node poses a copy of the data records, which are continuously updated
3) Security: blockchian structure of linking blocks using hash algorithm ensures that generated blocks cannot be erased or modified.
4) Transparency: data encapsulated in blocks are visible to all participants in the blockchain.

5) Automation: fulfilled by the concept of smart contract in which certain action could be automatically triggered by a specific smart contract program whenever a set of prespecified conditions are met.
6) Traceability: blockchain holds a historical record of all data from the date it was established. Such a record can be traced back to the original action.
7) Privacy: although blockchain is transparent, participants' information is kept anonymous using private/public key.
8) Reliability: blockchains have been successfully implemented by various organizations due to its features and robust structure.

VI. BLOCKCHAIN FOR IOT

Today's large-scale IoT systems consist of a considerably huge number of interacting devices using central servers to store, authenticate, and analyze data. Unfortunately, such architecture is not an effective one, as discussed in Section I. In addition, there are other challenges that arise with the IoT centralized structure or at least inflate as a result of it. Blockchain, as an emerging technology, would provide an essential solution to the problems facing IoT, especially when utilizing smart contracts, which shall play an important role in managing and securing IoT devices. Blockchain solves IoT issues as explained in what follows.

Elimination of central authority: Blockchain as a decentralized network eliminates the concept of central servers, which does not only remove central points of failures and bottlenecks [34] but improves fault tolerance and scalability, as well. In blockchain, data is stored in a decentralized manner where each network participant would have a copy of all transactions. Consequently, identical copies of data that is continuously updated will be stored in network nodes rather than being stored in central servers. Therefore, when blockchain is integrated with any layer of the IoT paradigm such as cloud or edge servers, it builds a distributed data storage. This shall provide redundancy and make disruption extremely difficult [35]. Also, the data authentication process will be carried on by blockchain's consensus mechanism without the need for central servers. Blockchain provides trusted, unique, and distributed authentication of IoT devices where participants can identify every single device. As per data analysis, it could be executed with the aid of the smart contract facility provided by blockchain. Those advantages are extremely important, especially for large scale IoT systems.

Peer to peer accelerated direct messaging: The peer to peer structure of blockchain does not only make direct messaging between them possible but also makes peer messaging faster compared to the present centralized IoT structure. Additionally, IoT applications can take advantage of this feature by providing device-agnostic and decoupled-applications [30]. This is possible thanks to the distributed ledger characteristics of blockchains, which not only eliminates the need for a central authority but enables to coordinate the processing of transmitted data between devices [4] and stores devices interaction, state, and exchanged data immutably in blockchain's ledger. Also, data flow in the centralized IoT system differs from that in the decentralized IoT-blockchain integrated system, especially that the integration takes different forms and designs.

Automation and resource utilization: Blockchain enables direct and automated interaction between IoT devices using smart contracts. Also, blockchain's smart contract facilitates resource usage by running an on-demand code or smart algorithm to manage resource utilization and automate payments when the requested service is completed. This process shall be performed automatically and without human intervention [35]. Additionally, blockchain empowers next-generation applications and enables the development of smart autonomous assets services. Furthermore, smart contracts can automate IoT software and hardware update and upgrade rights in addition to resetting IoT devices, initiating their repair request, and changing their ownership. Finally, smart contracts can support decentralized IoT devices authentication using specific rules embedded in their logic.

Secure code deployment: Since blockchain provides immutable and secured transaction storage, codes could also be pushed into the IoT devices in a secure manner [36]. Also, IoT devices' status could be checked and updates could be performed safely [30].

Built-in trust: Blockchain peer to peer structure based on consensus mechanism grant higher trust to IoT data since all participants are in posses of a tamper-proof copy of all transactions. If all nodes have the data and the means to verify that it has not been altered or tampered with then trustworthiness could be achieved [37], [38].

Security: Blockchain cryptographic structure is based on hashing each block and including it in the successive block. This process of block hashing forms the virtual chain that connects them and grants blockchain its name. There is no way to modify/change data in any block unless the hashes of that block along with all successive blocks were recalculated, which is almost an impossible task. Besides, hypothetically speaking, even if all the previously mentioned hashes were recalculated, the structure of a blockchain as a distributed data record does not allow any falsified data authentications because the consensus of the majority of nodes is required before updating data records [18]. Therefore, it is claimed that security and immutability are always guaranteed. This structure enhances the security of IoT systems since blockchain can store exchanged massages of the IoT devices' as transactions and validate them with the aid of smart contracts. Therefore, IoT communications and generated data will be securely stored as an encrypted and digitally-signed blockchain transactions [9], [28]. Also, integrating IoT systems with blockchain can utilize smart contracts to automatically update devices' firmwares that deal with vulnerable breaches and consequently enhance the total security of the underlying IoT system [28]. Furthermore, implementing blockchain can optimize current IoT secure standard protocols [9]. For instance, the Internet Protocol version 6 (IPv6) has a 128-bit address space while blockchain has a 160-bit address space [39]. Blockchain uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to generate a 160-bit hash of public key address [40] for around 1.46×10^{48} IoT devices, which drastically reduces the address collision probability and hence is secure enough to provide a Global Unique Identifier (GUID). Also, assigning an address to an IoT device using blockchain does not require any registration or uniqueness verification [9]. In addition to enhancing security, blockchain eliminates the need for a central authority, therefore, it will eliminate the need for the Internet Assigned Numbers Authority (IANA) in charge of global allocation of IPv6 and IPv4 addresses. Lastly, blockchain enhances scalability in securing IoT devices since it provides 4.3 billion addresses more than IPv6 which is a more scalable solution for IoT compared to IPv6 [9].

Data privacy: The other part of the cryptographic structure of blockchain is based on private/public key pair, which ensures that only the specified recipient or the node that owns and manages the private key is able to access data. Therefore, privacy is achieved where no entity other than the one having the private key can access or control the data. Also, data privacy could be achieved and maintained using smart contracts where a set of access rules are specified in the logic of the code to allow certain users or entities to access, control, or own the data whether it was in transient or at rest.

Historical action records: Data records of all transactions are stored immutably in blocks and can be traced back by any node to the very first transaction. To clarify the importance of this characteristic, we refer the readers to the work in [41] where the authors presented a blockchain-based traceability system. This system provides traceability services to suppliers and retails by inspecting and verifying the provenance of products and confirm their quality. As per IoT devices, all transactions made to or by IoT are stored in blockchain and can be traced back by any network participant [9]. The traceability feature provided by blockchain enhances the quality of service for IoT devices since it enables tracing resources and verify the service level agreement established between clients and IoT service providers [35].

Cost reduction in developing huge internet infrastructure: Large scale IoT requires upgrading the underlying network infrastructure to increase its capability to provide IoT connectivity, whereas, the decentralized blockchain eliminates this need and saves upon its cost.

Transparency: The latest developments in technology have led to cloud computing concepts, which increased the IoT ability to analyze and process data and consequently take real-time actions. Therefore, it is without any doubt that cloud computing contributed to the development of IoT systems [42]. However, it acts as a black box when coming to data transparency. Participants usually do not have any clear vision of where and how the data they provide is going to be used [30].

Enhance IoT systems interoperability: which is the ability of IoT systems to interact with physical systems and exchange the generated data between IoT systems themselves. Blockchain is capable of enhancing the interoperability of IoT systems by transforming and storing IoT data into blocks. This process converts, compresses, and stores heterogeneous IoT data into an integrated blockchain where it provides uniform access to different IoT systems connected as peers in it [43].

Governance of access and identities: Identity and access management (IAM) of IoT devices is facing multiple challenges such as the change of ownership during the lifetime of IoT devices from manufacturer to supplier then to retailer, until they end up in the hands of their consumers [44], [45]. Also, consumer ownership may change in case the IoT device is compromised, decommissioned, or resold. Another issue facing IAM is managing the attributes of the IoT devices such as serial number, manufacturer, make type, location, deployment GPS coordinates. Another challenge related to IoT identity and access management is the IoT relationships, which may take the form of device-to-device, device-to-human, or device-to-service. Also, the types of IoT' relationships could vary from deployed by to use by or sold by, shipped by, upgraded by, repaired by, and so on [9]. Blockchain is capable of addressing the above challenges securely and effectively since it has been utilized to provide authorized and trusted identity registration and management, ownership tracking, and assets monitoring. Blockchain can register and provide identities to IoT devices with different attributes that are connected in a complex relationship and store all this information securely and immutably in a distributed manner. Therefore, blockchain supports a trusted and decentralized IoT identity governance and tracking throughout the life-cycle of the device [9].

Reliability and robustness: Blockchain eliminates central servers which increases privacy and security in IoT paradigm,therefore, the integration of blockchain with IoT systems would result in a reliable robust system. It is well known that IoT can facilitate information digitization, however, the reliability of such information is

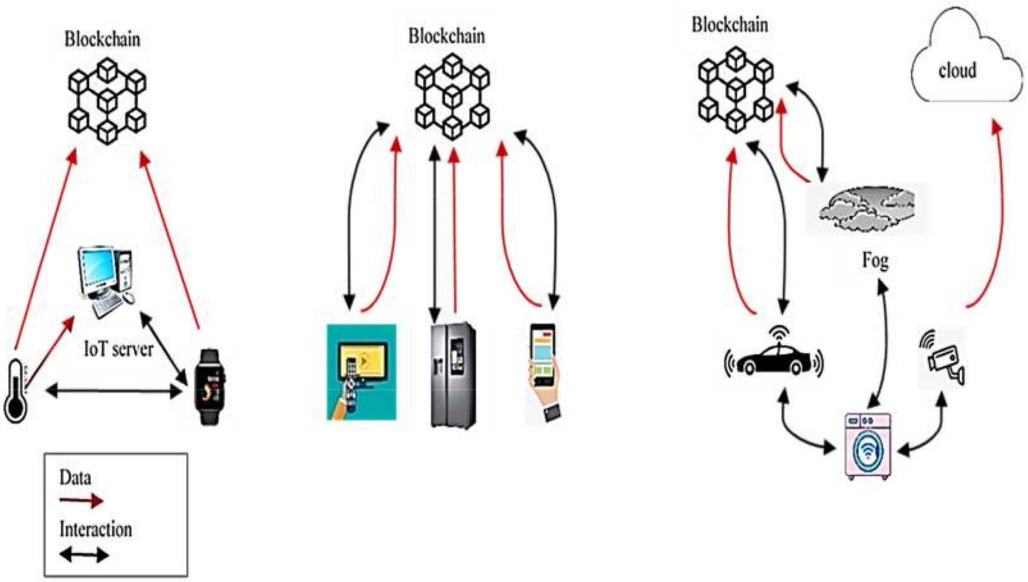

FIGURE 2. Types of blockchain –IoT integration.

still a challenge [30]. Blockchain solved this issue by increasing the reliability of a proposed integrated system. Blockchain reliability along with the long history of its flawless implementation in many fields ensures high robustness [4].

From the above, it is clear that employing blockchain could complement IoT with secured and trusted information to solve the issues related to transparency, latency, and Internet infrastructure. Moreover, IoT was recently integrated with some computing infrastructures to overcome a few of its limitations related to storage and processing. One of which is cloud computing, which played a vital role in solving many issues. However, it established a centralized network architecture, which complicates reliable data sharing among other impracticalities [42]. Blockchain, in contrast, addresses IoT problems and maintains a decentralized structure to solve further issues and add more value. Similarly, fog computing was also integrated with IoT to enhance its performance by minimizing exiting limitations. Fog computing uses end devices to perform a substantial amount of computation, storage, and communication locally and route it over the Internet. Fog computing if follows the distributed structure of blockchain could utilize more powerful devices such as gateways and edge nodes, which could then be reused as blockchain components. Therefore, Fog computing, which restructured IoT by including a new layer between cloud computing and IoT devices is expected to facilitate the integration of IoT and blockchain [30].

VII. RESEARCH SURVEY

Recently, integrating blockchain with IoT was addressed in the literature offering a diversity of contributions. Some work proposed an overview of challenges facing IoT and blockchain's integration by conducting a systematic literature review [2], [46], [47], while others investigated certain challenges in the IoT paradigm and demonstrated a framework to face those challenges or at least a few of them [12], [48]. Other studies created evolved IoT system architecture by integrating blockchain in various configurations and explained its reflected benefits on IoT's performance and the eliminated challenges [35], [49]. In relation to the last type of researches, it is important to know that different works proposed different IoT–blockchain paradigm. Specifically, when integrating blockchain with IoT, the communication between systems' layers was clarified and accounted for. Therefore, devices and IoT infrastructure interactions were taking different forms, whether to be inside the IoT, through blockchain, or by creating a hybrid design that involves both [30]. Different integration schemes will typically result in various levels of acquired benefits. Figure 2 demonstrates the types of blockchain–IoT integration. Many review papers were found in literature such as [2], [4], [12], [30], [46] in which authors demonstrated the benefits and challenges of integrating IoT with blockchain. However, none of them reviewed the available blockchain - IoT integration frameworks and architectures as we did in this research.

In [50], the authors introduced a new IoT architecture called ''EdgeABC''. This model consists of three layers: An IoT smart device layer, a distributed agent controller architecture based on blockchain, and a hierarchical edge computing servers. The architecture in [50] utilized blockchain in the middle layer to ensure resource transaction data integrity. The study implemented a developed task offloading and resource allocation algorithm on blockchain in the form of a smart contract. The proposed model could be implemented in any typical application such as smart healthcare, home, building or factory. Another security model and protocol was proposed by [51] to provide decentralized cryptographic keys and trust information storage for Wireless Sensor Networks using blockchain technology. The aim of the blockchain authentication and trust module (BATM) in [51] was to allow each network component to authenticate information about every node within their networks.

The authors in [35] proposed a distributed blockchain-based cloud architecture model, fog computing, and software-defined networking SDN. The model aimed to efficiently manage raw IoT data streams at the edge of the network and the distributed cloud. The model consists of three layers: IoT devices, SDN controller network based on blockchain for fog nodes, and distributed cloud based on blockchain.

The authors in [52] proposed architecture for Blockchain of Things (BCoT), where a blockchain-composite layer forms a middleware between IoT and industrial applications to hide the heterogeneity of the lower layers while providing blockchain-based services to facilitate different industrial applications. Also, researchers discussed blockchain potentials for 5G-beyond networks.

Blockchain was integrated into more than one layer in the architectural model presented by [53]. A hierarchical authentication architecture comprising of a physical network layer, blockchain edge layer, and blockchain network layer was demonstrated to improve authentication efficiency and data sharing among various IoT platforms. The study evaluated the authentication mechanism using MATLAB and Hyperledger Fabric. In a related context, the problem of a single point failure at gateway nodes was tackled by [54]. This study proposed a decentralized blockchain-based IoT management system to solve the gateway node censorship problem that utilizes a gossip-based diffusion protocol. The designed protocol aimed to deliver all messages from sensors to all full nodes and improve blockchain-based IoT management systems security. Another P2P network architecture was designed by [55], which integrated blockchain and edge computing for IoT applications to achieve secured data storage and high system performance. The architecture design consisted of three layers: a cloud layer, an edge layer, and a device layer. The resources in the cloud could be configured as nodes on the blockchain, which is separated from the application layer. Also, a Proof-of-Space solution based on smart contracts was adopted to authenticate information. Another flexible blockchain architecture in edge computing was demonstrated by [49]. This study proposed a blockchain-based data management scheme (BlockTDM), which supports matrix-based multichannel data isolation to protect sensitive information by utilizing smart contracts. Internet of Drones (IoD) could also benefit from blockchain's specific features to face its challenges as well. This was implied by [48] in their design of a blockchain-based access control scheme for an IoD environment. Their scheme was used to support access control between any two neighbor drones and between a drone and its associated ground station server (GSS). Testing and simulation proved that the proposed scheme could help to resist various attacks and increase communications security.

The integration of IoT and blockchain is applied in power systems as well. The work in [56] proposed structural applications incorporating IoT and blockchain in distributed generation systems, smart buildings, energy hubs, and management of residential electric vehicles. The study aimed to benefit from blockchain features in solving issues related to the huge amount of generated information that needs to be securely transferred, stored, and analyzed to enhance grids' performance and reliability. Also, an article by [57] demonstrated the integration of blockchain with IoT ecosystems trading platforms and provided practical scenarios and a case study to establish end-to-end trust for trading IoT devices and corresponding data. Trust and authentication also were the core issues tackled in [58]. The authors in [58] designed a secondary authentication scheme for IoT devices to access a Wi-Fi network using three smart contracts. The scheme aimed to identify IoT devices located within a legal range. The cost of IoT-blockchain integration was discussed in [59] which analyzed the cost of storing data from several IoT sensors on Ethereum blockchain via smart contracts under two options: Appending new data or overwriting on existing data. The conducted cost analysis aimed at enabling practical applications of blockchain and smart contracts in IoT applications.

In related research, [60] designed, developed, and tested a blockchain tokenizer device that connects any industrial machine to blockchain platforms. The study aimed to build an enabling technology to diffuse blockchain in industrial applications and act as a bridge between Industrial IoT, and blockchain world by tokenizing industrial assets. Devices were tested at the hardware and software levels on two industrial supply chain use cases. Researchers used Ethereum programming language to develop a smart contract that can be used to enable the creation of a digital twin (building a virtual model of a product to simulate systems) by producing a blockchain token. Also, research by [61] explored how integrating IoT and blockchain would benefit shared economy applications focusing on security and decentralization features. The researchers proposed shared economy application scenarios enabled by integrating IoT and blockchain. The integration of blockchain with industrial IoT was the focus of another research conducted by [62]. The study introduced a blockchain-enabled IoT framework where components interactions, data processing, and storing were done through a smart contract. Further research in the same context was carried on where a decentralized self-organized trading platform for IoT devices using blockchain was designed by [63]. The authors of this work modeled the resource management and pricing problem between the cloud provider and blockchain miners using game theory. Nash equilibrium of the proposed Stackelberg game was achieved by introducing a multiagent reinforcement learning algorithm. Furthermore, some conducted researches aimed at improving and optimizing IoT-blockchain integration architecture such as [64]. This research addressed blockchain consensuses dynamic management needed to deal with the high dynamics of IoT applications. Researchers designed application-aware consensus management for software-defined intelligent blockchain and an intelligent scheme to analyze packets at the IoT application-layer. Also, [65] aimed at quantifying the performance of constrained IoT devices in terms of reducing transaction delay and cost. These researchers proposed models based on inter-ledger mechanisms and smart contracts to provide decentralized authorization for IoT devices. Another study by [66] presented an optimization policy for IoT sensors sampling rate using blockchain and Tangle technologies. The proposed model aimed to minimize the age of information (AoI) experienced by end-users taking into consideration resource networking and processing constraints. Table 1 summarizes the demonstrated researches pointing at their contribution, application area, and the challenges they addressed.

It is noticed from the surveyed research works that blockchain has many forms in which it could be integrated with IoT networks based on the required outcome performance and the addressed challenges. In addition, researches agreed on the conclusion that integrated IoT-blockchain systems demonstrate better performance compared to standard benchmark IoT systems prior to blockchain integration.

VIII. ISSUES FACING THE INTEGRATION OF IOT AND BLOCKCHAIN

The integration of IoT with blockchain came as a rescue for the IoT paradigm where it provides valuable opportunities and resolves many of the challenges facing IoT. However, limitations do exist due to the challenges facing the integration itself in the form of newly created obstacles, which clearly opens doors for contemporary research ideas. Currently, the literature mainly focuses on the features offered by blockchain that would elevate IoT architecture and widen its application in a much effective manner [52], [67], [68]. Issues such as security, traceability, transparency, efficiency, and trust will be enhanced in the presence of blockchain in IoT systems. However, researchers need to tackle the issues that appeared due to the integration and eliminate them before the potentials of the integration could be fully revealed. Remember that blockchain technology was designed for powerful computers in an Internet paradigm in the first place and this is not the exact case for IoT as will be explained later. In this section, several major challenges incorporating IoT-blockchain integration are identified and discussed as follows.

A. IOT RESOURCES CONSTRAINTS

Many IoT devices such as sensors, RFID tags, and smart meters are resource-constrained. Usually, these devices suffer from inferior computing capabilities, poor network connection capability, limited storage space, and low battery power [9]. On the other hand, blockchains have their own special requirements. Firstly, the consensus algorithm needs extensive computing power, which consumes energy, therefore, not practical for low-power IoT devices [9]. Secondly, the size of blockchain data is bulky so it is infeasible to store the whole blockchain in each IoT device, especially with the fact that IoT generates massive data in real-time, which makes the situation even worse [46]. Thirdly, blockchain is designed assuming stable network connections [69], which may not be feasible for IoT that can normally suffers poor network IoT devices connection or unstable network due to the failure of nodes (e.g. battery depletion) [70]. In most cases, the situation of the IoT devices cannot be detected until it is tested, while in many other cases the devices work perfectly fine for a period of time then the situation changes for many reasons such as disconnection, short circuit, and program obsolescence [30].

B. SECURITY SUSCEPTIBILITY

Many industries growingly deploy wireless networks for their applications due to their scalability and feasibility. However, the wireless medium suffers from many security breaches such as passive eavesdropping, jamming, denial of service, and others [71]. Furthermore, due to IoT devices' resource constraints, it is difficult to manage the public/private keys encryption algorithms [46], especially in a distributed environment. Besides, many IoT systems contain different types of devices that vary in computational capabilities meaning that not all devices can carry out, for example, the encryption algorithm at the same speed [72]. Meanwhile, blockchain has its vulnerabilities such as malicious nodes hijacking blockchain's messages with the purpose of delaying block broadcasting.

C. POSSIBLE PRIVACY BREACHING

Blockchain utilizes private/public key pairs as a mechanism to preserve data privacy. However, this encryption method might not be robust enough in some cases. It was found that user identity could be revealed using learning and inferring multiple transactions performed by one common user [73]. Furthermore, storing all data on a blockchain could be more serious in case of any privacy leakage [74].

D. INCENTIVE MECHANISM CHOICE

Blockchain networks have different incentive mechanisms that are used to mine blocks. Some use Proof of Work (POW) while others use Proof of Stake (POS). However, there are many more algorithms. In general. there are two types of incentive mechanisms in blockchains:

1) The reward for mining a block and
2) The compensation for processing a contract

Choosing the proper incentive for the blockchain application is a sensitive issue that affects the continuous effort provided by nodes in general and miners in particular [32]. To illustrate the issue, for Bitcoin blockchain, the first miner that solves the POW puzzle will be rewarded a certain amount of bitcoins. However, rewards are halved every 210,000 blocks. This decrement incentive structure will discourage miners and make them shift to another blockchain especially knowing that POW consumes a huge amount of energy. This is an

TABLE 1. Researches addressing IoT-blockchain integration.

Research /year	Contribution	Application	Addressed challenges/area of improvement					
			Security	*Privacy*	*Centralization*	*Trust*	*Speed*	*Reliability*
[[50]]	Architecture model	Smart healthcare /home/building /factory	*		*		*	*
[[51]]	Security model and protocol	General	*	*		*		*
[[35]]	Architecture model	General	*		*			*
[[52]]	BCoT Architecture model	Industrial applications	*	*	*			
[[53]]	Hierarchical architecture model	General	*	*	*	*		
[[54]]	Architecture model, protocol	General	*	*	*			*
[[55]]	Architecture model	General	*	*				
[[49]	Architecture model, scheme	General	*					
[[48]	Control scheme, modeling	IoD	*	*				*
[[56]]	Scenarios, framework	Smart grid						*
[[57]	Case study, scenarios	IoT ecosystem				*		*
[[58]]	authentication scheme	General	*					
[[59]]	Cost analysis	General	*					*
[[60]]	Design, implement and test a device tool	Industrial IoT in Supply-chain				*		*
[[61]]	Scenarios	Shared economy applications	*		*			
[[62]]	Framework	Industrial IoT					*	
[[63]]	Platform design, modeling, algorithm	Industrial IoT						*
[[64]]	Architecture model, scheme	General	*					*
[[65]]	Modeling	General						*
[[66]]	Modeling	Time-sensitive (healthcare)						*

important point that should be considered when designing a consensus algorithm for the integrated network.

E. PERFORMING BIG DATA ANALYTICS

There is a growing trend for analysis of IoT real-time generated data. This type of data is of a massive volume and usually heterogeneous, however, it has high business value [75]. Big data analysis of IoT generated data could reveal hidden valuable and meaningful information that aids in making intelligent decisions. However, applying conventional big data analysis for the integrated IoT-blockchain system is challenging due to the following:

1) IoT devices suffer from resource limitations and inferior computing capabilities. These issues prevent deploying complicated big data analytics methods directly at IoT devices. Uploading the data to clouds for computation and performing big data analysis is a proposed solution, however, it could lead to long latency and privacy concerns [42].
2) Blockchain technology protects privacy via public/private key digital signature. On one hand, performing big data analysis of anonymous data is difficult, while on the other hand decrypting data is a time-consuming process that results in inefficient data analytics [76].

F. SCALABILITY OF THE INTEGRATED SYSTEM

Blockchain scalability is measured by the throughput of transactions per second against the number of IoT nodes and the number of concurrent workloads [43]. The scalability of current blockchains limits their implementation in large scale IoT applications [46]. Specifically, IoT devices generate gigabytes real-time data while blockchain is not designed to store that huge amount of data [30]. For example, Bitcoin blockchains may not be suitable for IoT due to their poor scalability. Some blockchains can process only a few transactions per second. This clearly is a bottleneck for the IoT systems [30]. Such a situation is solved by implementing consortium or private blockchain. There are many platforms for consortium blockchain such as Hyperledger [77].

G. IOT DEVICES MOBILITY AND NAMING

Blockchain network structure differs from that of IoT in the sense that nodes were not meant to find each other in the network. For illustration, looking at Bitcoin blockchain, the IP address for senders is included in the transaction and is used to build the network topology by other nodes. This topology is not practical for IoT networks because many IoT devices are mobile all the time [78].

H. SMART CONTRACT IMPLEMENTATION

Any instability of IoT devices could compromise the validation of smart contracts. Furthermore, smart contracts could be overloaded in cases that require accessing multiple data sources. It is known that smart contracts, being one of blockchain's features, are decentralized and distributed, however, they do not share resources or distribute performing functions in order to run a huge amount of computational tasks. In other words, each smart contract is simultaneously executed over multiple nodes where the distribution is only for contracts' validation and not for performing functions and codes [30].

I. BLOCKCHAIN STANDARDIZATION

IoT developers consider standardization of blockchain as a vital issue that shall decide the future of the integration between them because it is expected to provide the required guidance for developers and customers as well [79]. It is worth mentioning that setting blockchain standards should take into account the relevant industry standards that are currently being followed, especially the ones related to IoT. Therefore, many European countries established standards for blockchain' financial transactions to increase confidence in the market [80]. Also, the ISO approved the new standard for blockchain and distributed ledger technology (ISO/TC 307) [81]. Besides, legislation related to cybersecurity should be considered in the integrated IoT-blockchain systems such as the EU Network and Information Security (NIS) directive, which was adopted by the European Commission in 2016 to enhance cybersecurity across the EU [82] and the general data protection regulation (GDPR) proposed by EU on 2018 to harmonize data protection and privacy laws for individuals [83]. The integrated system has to consider the above laws in addition to some other rules and notifications regarding personal data breach in cases of applications that grant access to or edit personal and enterprise data. Furthermore, blockchain is structured around connecting people from different countries were so far no global legal compliance code exists, and that represents an issue for manufacturers and service providers [46].

IX. LITERATURE SURVEY CONCLUSION

From reviewing related work in literature, it was concluded that integrating blockchain with IoT could take various forms and designs depending on the required outcome, application, and addressed challenges as demonstrated in Section VIII. Besides, it is argued in the literature that integrated systems demonstrated better performance compared to standard benchmark IoT systems with no blockchain integration [7].

Additionally, the surveyed studies did not only agree on the feasibility of the integration but proposed a variety of designs to achieve it, as well. While some have focused on the general architectural prospectives required for the integration; others concentrated on mitigating specific issues by introducing the blockchain. Moreover, some other researchers have utilized the integration as a platform to deploy certain applications. However, many issues and challenges have not been tackled by researchers such as constraints of IoT devices, analysis of big data in addition to others previously demonstrated challenges regarding the integration of IoT –blockchain. This research is based on integrating blockchain in two out of the three layers; namely, the dew and cloudlet layers, forming the final architectural design. Our aim is to benefit from features and services provided by blockchain to guarantee a decentralized data storage while addressing security anonymity challenges and achieve transparency and efficient authentication service.

Despite the continuous effort to design suitable IoT–blockchain integrated architecture, many issues limit proper implementation as well as the applications' range of the integrated system in order to guarantee its optimal usage. Therefore, there is an increase in the demand for an efficient design that takes into consideration the challenges facing the integration process, mainly, IoT devices constraints, big data analytic, security, and privacy. Also, the appropriate method should be investigated to facilitate proper smart contract implementation.

X. DESIGN REQUIREMENT

To design a high-performance distributed and scalable IoT network architecture with the goal of successfully integrating blockchain with dew and cloudlet computing to meet current and future challenges while offering support for new service requirements, the following design principles must be fulfilled:

- Efficiency: The integrated system should operate at optimal performance even though its nodes consist of heterogeneous devices.
- Resilience: In case any node fails, computational tasks should not be affected and the system should continue to work through the rest of the operational nodes.
- Decentralized data storage: The integrated architecture should extend the storage capacities of IoT devices by employing the storage capacities of blockchain technology.
- Scalability: This is a vital principle in designing an IoT network with the ability to manage future growth in terms of the number of devices and amount of information they generate.
- Ease of deployment: All nodes even the ones located at the edge of the Internet should be allowed to join the network without complicated configurations.
- Data integrity: The integrated system must have a reliable built-in data verification mechanisms to ensure the accuracy and consistency of data in the decentralized environment.
- Security: Securing the IoT network is one of the main objectives of introducing a new design architecture. Therefore, to ensure a holistic design of the integrated system, data confidentiality and security must be adequately addressed.
- Data authenticity: Data transactions should be authenticated and validated in a heterogeneous and decentralized dew computing environment.
- Privacy: Users' data privacy should be guaranteed by blockchain. This will ensure network participants that their transferred information is not being tracked or altered.
- Offloaded computation: The processing tasks outsourced to other servers, such as dew servers in our proposed design, by IoT end devices should be verified in order to produce accurate results.
- Low latency: The integrated system design should consider delays incurred during computation processes as well as data transmission from one node to another. To ensure low latency, it is important to identify what computation tasks are involved, as for our architecture, decide whether they should be performed at the end devices, dew servers, or at the cloudlet layer.
- Access control: It is fundamental to enforce access policies in the network to regulate the viewing and sharing of users' data.
- Adaptability: The architecture must be flexible enough to adapt to the changing environments, expanded customer pools along with their demands, and increased complexities in possible future applications while maintaining acceptable levels of system throughput, delays, and security.

XI. PROPOSED DECENTRALIZED ARCHITECTURE FOR INTEGRATION IOT AND BLOCKCHAIN

The proposed blockchain-based architecture is built to mitigate the multiple challenges facing the integration of IoT and blockchain. This proposed architecture consists of three layers; a device layer, a dew-blockchain layer, and a cloudlet-blockchain layer. Integrating blockchain with dew and cloudlet computing is intended to provide authentication efficiency, processing, and data storage services. Dew computing is a contemporary computing model that emerged after the wide success of cloud computing. However, cloud computing uses centralized servers to provide its services, while Dew computing uses on-premises computers to provide cloud-friendly, and collaborative micro services to end-users [84]. As a matter of fact, Dew computing goes beyond the concept of a network-storage and network-service, to a distributed sub-platform computing hierarchy [85]. Some researchers suggested an extension to the Open Systems Interconnection (OSI) model by adding a new (i.e. eighth) layer called the context layer on top of the application layer. As defined in [86], Dew computing is "an on-premises computer software-hardware organization paradigm in the cloud computing environment where the on-premises computer provides functionality that is independent of cloud services and is also collaborative with cloud services. The goal of dew computing is to fully realize the potentials of on-premises computers and cloud services". From this definition, the main features of dew computing are independence and collaboration. Dew computers provide substantial functionalities independently from the cloud layer, however, they collaborate with it. Dew computing is the closest layer in the network hierarchy to the IoT devices as demonstrated in Figure 3. Also, it is not only applicable in cases of powerful local

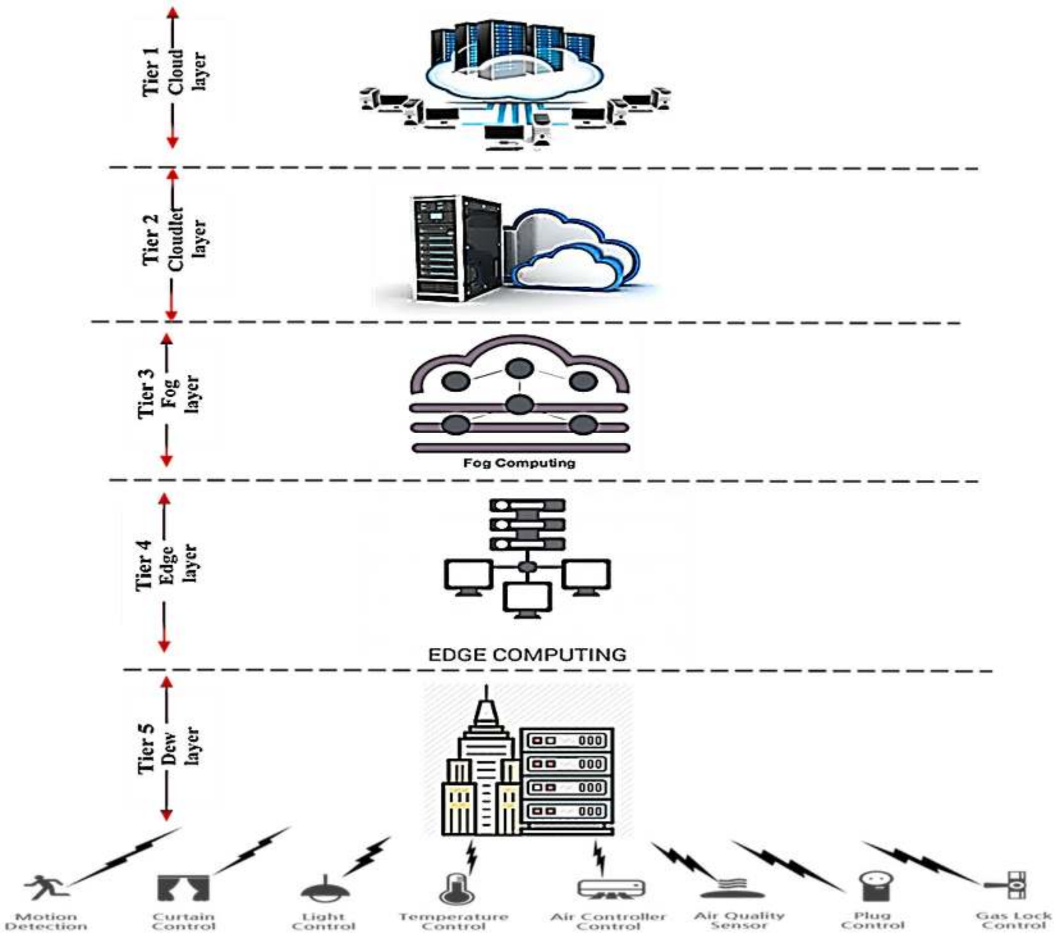

FIGURE 3. 5 Tier network layer hierarchical structure.

computers and applications, simple applications maybe not rich enough but still considered a dew computing application [86]. As previously mentioned, one of the major issues facing the integration process is IoT resource constraints in terms of computational capabilities, storage space, and power supply. This was solved by introducing a Dew layer in the design. Dew on-premises computers could contain a duplicated fraction of the World Wide Web or serve as files storage that automatically synchronizes with its cloud copy (such as Dropbox). Additionally, dew computing hosts on-premises database synchronized in real-time with cloud database and serve as a backup to each other. This facilitates big data analysis, which represented a challenge for integrating blockchain with IoT. Furthermore, dew computers may host software or serve as a platform supporting development applications [86]. Our proposed dew-cloudlet architecture can be considered as an extension to the client-server architecture, in which two servers are located at both ends of a communication link [87]. Although fog and edge computing are still viewed as useful technologies, however, they heavily rely on connectivity. Dew servers, on the other hand, grant users more flexibility and control over their data even at the absence of an Internet connection. Primarily, the dew server stores a local copy of the data and synchronizes it with a master copy upon restoring the Internet connection [87]. This feature is not the only valuable characteristic that distinguishes dew computing from other technologies, which made it a strong candidate and most suitable to be integrated with blockchain technology, dew computing has the significant advantages of self-healing, autonomic self-augmentation, self-adaptive, user-programmability, extreme scalability, and capability of performing tasks in a highly heterogeneous IoT device environment [87]. Clearly, and after reviewing the issues facing the integration of IoT and blockchain, dew computing features appear to be tailored made to address the integration process challenges.

This is not the first time dew servers are integrated with blockchain. Research by [88] introduced dew computing as a blockchain client forming a new kind of blockchain called Dewblock. This system solved the issue of clients having to keep a huge amount of blockchain data in order to act as a full node in a blockchain. The proposed system brings in a new approach in which the data size of a client is reduced while the features of a full node are still maintained.

This enables clients to enjoy the features of full nodes in blockchain without needing to store the growing blockchain data. The study approach was inspired by dew computing principles to develop Dewblock based on cloud-dew architecture. In the system, a dew client operates independently to perform blockchain activities while it collaborates with the cloud server to maintain the integrity of the blockchain network. Therefore, every blockchain user has to deploy a cloud server. This system clearly demonstrated the two main features of dew computing which are independence and collaboration.

The other layer in the integration architecture is the cloudlet layer, which is a resource-rich, trusted, small-scale cloud data center located at the edge of the Internet [84]. The proposed design is providing solutions to many challenges and upgraded performance for the IoT paradigm.

A. AN OVERVIEW OF THE PROPOSED ARCHITECTURE

A three-layer architecture is proposed in this study to solve the problems of devices' constraints, big data analysis, data privacy, and security in IoT systems as well as other challenges facing the IoT paradigm. Additionally, our design shall increase authentication efficiency and enhance data storage and processing capabilities. The architectural design consists of perception or sensing layer, dew layer, and cloudlet layer as shown in Figure 4. Blockchain is integrated into two of those layers, precisely the dew layer, and the cloudlet layer. In general, blockchain usage comes in three types: as a decentralized storage database, as a distributed ledger, or as a supporting distributed services provided by smart contracts. Blockchain is integrated with dew and cloudlet computing to provide fundamental requirements of IoT, which are: computation offloading, outsourced data storage, and management of network traffic. In what follows, we introduce these three layers.

1) The device layer: Located at the edge of the network, the device layer consists of IoT sensing devices and actuators used to monitor and control various smart applications and send the locally generated data to the dew layer to utilize its resources in performing requested services and other tasks. The participation of IoT devices in the blockchain network is facilitated by capable servers in the upper dew and cloudlet layers. Thus, heavier operations are performed by those servers while end devices carry out lighter tasks such as accepting firmware updates
2) The dew Layer: The IoT device layer transmits the generated raw data to the dew layer, which consists of higher-performance controllers connected in a distributed manner using the blockchain technology. Each dew controller represents a node in a consortium blockchain and covers a small associated device community. The dew layer is responsible for timely service delivery, data analysis, data processing and reporting of results to the cloudlet and device layers whenever needed. Specifically, the dew layer provides localization, while the cloudlet layer provides wide-area monitoring and controlling. Dew computing is characterized by its high scalability, which is ''the ability of a computer system, network or application to handle a growing amount of work, both in terms of processing power as well as storage resources or its potential to be easily enlarged in order to accommodate that growth'' [85]. Also, dew computing equipments are capable of performing complex tasks and running a large variety of applications effectively. To provide such functionality, devices at this layer are self-adaptive and ad hoc programmable. Thus, by integrating them with consortium blockchain, they become more capable to run applications in a distributed manner without a central communication point or central device. This powerful characteristic of the dew layer enables it to support a large number of heterogeneous devices connected in a peer-to-peer environment meanwhile avoid the risk of a single point failure. Additionally, the dew layer peer-to-peer servers provide decentralized and distributed storage facilities used for additional data storage, real-time data analytics, different data communication handling. Furthermore, the dew layer brings services closer to end devices which shall improve overall performance and lower latency.

Moreover, dew servers can transfer messages between themselves, which shall assist in coordinating data processing, save cost, and time. This became possible due to the deployment of blockchain that serves as a distributed platform supporting secured data transmission across the network. Besides, the ability to convey peer to peer messages in the network, dew nodes perform light processing and analysis for their data as well as for peer nodes. This facilitates self-organization in a dynamic environment where dew nodes could be added and removed at any time. Equally important, dew servers forward real-time data analytics either to the distributed cloudlet layer for long term storage or further processing and analysis or back to end devices depending on the network requirements.

From the above, it is clear that this layer's distributed blockchain architecture creates a pool of mobilized resources that provide extra data storage and speed computations and data analysis. In case of substantial or intensified computational requirements that dew layer can not handle, servers request services form the cloudlet layer and offload the workload to it. Not only blockchain provides decentralized services of storing, processing, and analyzing terminal information but also supports creating smart contracts that further lower latency and increase throughput for dew servers and distributed resources on the cloudlet layer. Smart contracts are utilized to define the authentication mechanism and integrate different protocols of heterogeneous

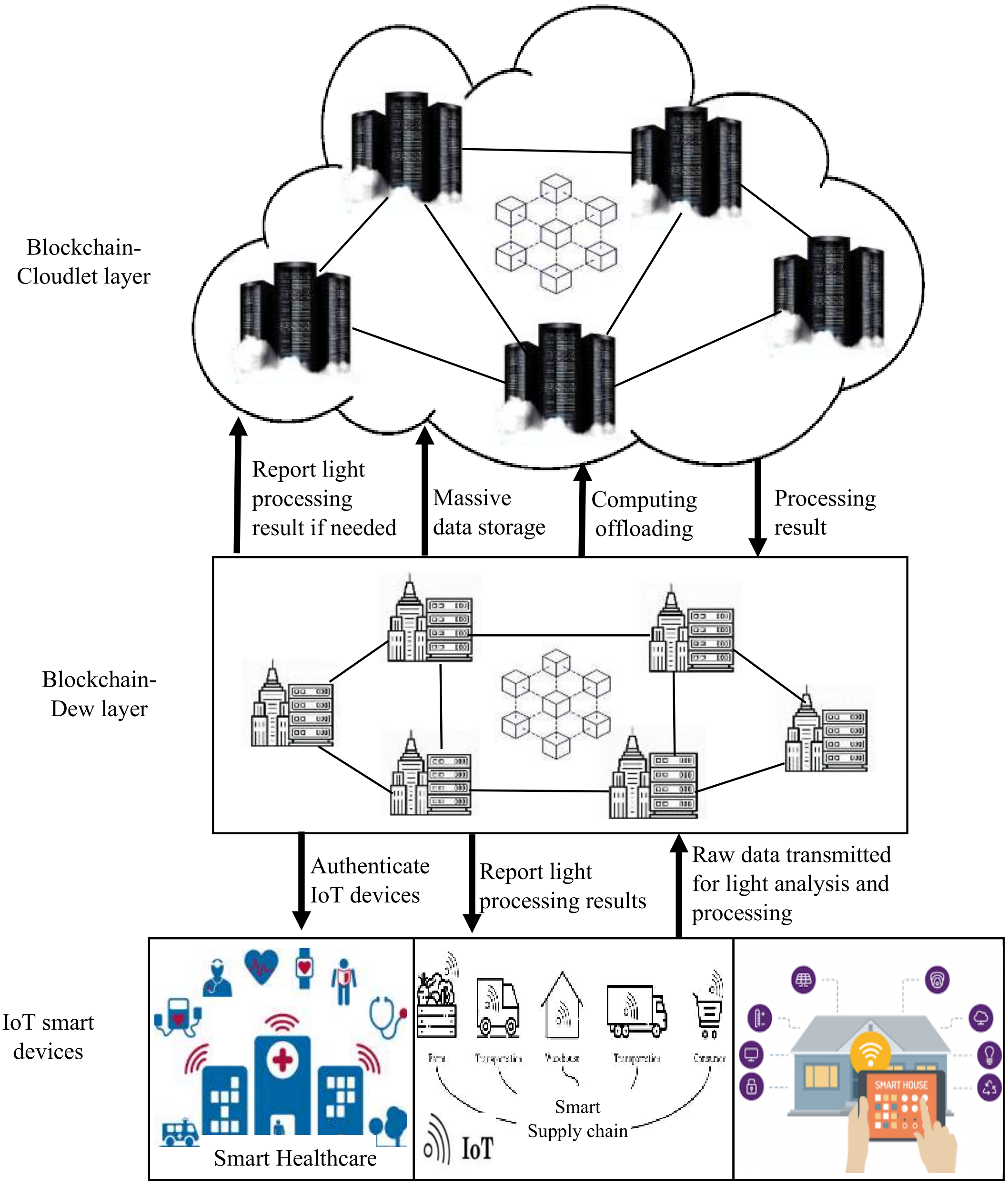

FIGURE 4. The proposed IoT-blockchain integrated architecture.

IoT platforms. Dew nodes can access any smart contract by sending a transaction to its address and therefore invoke its function. Meanwhile, terminal identity anonymity and communication security are maintained by the cryptography algorithm and public/private key pair.

3) The cloudlet layer: The cloudlet layer consists of more powerful resources to provide long-term data processing, analytics and storage, in addition to a higher level reporting and communication. Such cloudlet resources are configured as blockchain nodes capable of participating in the mining process to ensure data privacy and integrity. We propose a distributed cloudlet layer based on blockchain technique to provides secure, scalable, reliable, low-cost, high-availability services, and on-demand access to computing infrastructures. Cloudlet layer hosts massive storage and computational facilities that when used with blockchain, a complete replication of all records being shared among them is maintained

The flowchart in Figure 5 further explains the message flow between layers in the proposed architecture.

B. CONSENSUS MECHANISM

The consensus mechanism in blockchains is crucial for both the dew and cloudlet layers to provide secure and timely access, consequently, offering quality computing services.

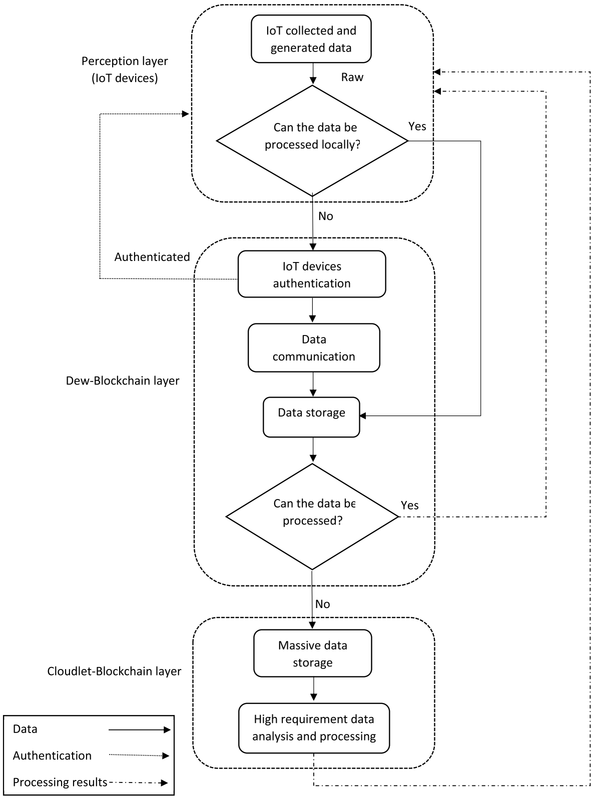
Perception layer
(IoT devices)
IoT collected and generated data
Raw
Can the data be processed locally?
Yes
No
Authenticated
IoT devices authentication
Data communication
Dew-Blockchain layer
Data storage
Can the data be processed?
Yes
No
Cloudlet-Blockchain layer
Massive data storage
High requirement data analysis and processing
Data
Authentication
Processing results

FIGURE 5. The message flow between layers in the proposed IoT-blockchain integrated architecture.

The adopted mechanism in both layers is Practical Byzantine Fault Tolerance (PBFT). Byzantine Fault Tolerance enables distributed computer networks to reach sufficient and valid consensus even though malicious nodes might exist in the network performing malicious acts such as failing to send information or sending incorrect ones. Here, the role of BFT is to protect the system from catastrophic failure by decreasing the effect of those malicious nodes [89].

BFT stemmed from the Byzantine Generals' Problem. It is a computer science term describing the situation that involves multiple parties who should agree on a single strategy to prevent network failure bearing in mind that some nodes might be unreliable or malicious [89]. BFT has been utilized in nuclear power plants, airplane engine systems, and almost in any system that depends on many sensors to take a decision or action. Moreover, it is used in blockchain networks where trust needs to be established between nodes who do not fully trust each other [90]. In 1999, a published research introduced the Practical Byzantine Fault Tolerance (pBFT) algorithm [89]. The reason behind choosing pBFT in our architecture is its distinguished high-performance Byzantine state machine replication and its capability of processing thousands of requests per second with sub-millisecond increased latency. Also, pBFT is effective in providing high-throughput transactions [90]. In order to further increase the throughput of the network, we suggest using a consensus round every specific number of mined blocks and perform blockchain sharding. Here, miners are split into smaller groups called shards capable of processing transactions simultaneously resulting in higher throughput [90].

C. STRENGTHS OF PBFT

Practical Byzantine Fault Tolerance (pBFT) algorithm has many strong points that support our choice of adopting it in our architecture, the following are the main strengths

1) Transaction quick finalization: the structure of pBFT imply that transactions could be validated and finalized without the need for multiple confirmations. Also, there is no waiting period after including the block in the chain to ensure that a transaction is secured [91].
2) Energy efficiency: pBFT does not require intensive energy consumption such as POW as described in section VIII. Even if the system adopts POW almost every 100 mined blocks to prevent Sybil attack, the increase in energy consumption is not significant [91].
3) Low reward variation: miners incentive is one of the issues facing the integration of IoT with blockchain, which was discussed previously in section VIII. pBFT solves this issue because it requires collective decision through voting on records by signing messages, unlike POW in which miners only add the next block and get rewarded. In the pBFT network, every node can be incentivized. Therefore, there is no fear of nodes or miners leaving the network due to unacceptable rewards [91].

D. THE WEAKNESS OF PBFT

Although (pBFT) proved to be reliable and strong, the following explains its main weakness.

1) Sybil attacks: pBFT consensus could be affected by Sybil attacks, where a single party controls or manipulates a large number of nodes which enables them to control and modify the blockchain and thus comprises security. This threat is lowered in large size networks. However, considering the scalability problem of pBFT, the solution is to use sharding or combine another type of consensus algorithm as suggested above [91].

E. INTEGRATION CHALLENGES AND FULFILLMENT OF DESIGN REQUIREMENTS IN THE PROPOSED IOT-BLOCKCHIAN ARCHITECTURE

In this section, the satisfaction of previously specified design principles, as well as solutions to many integration challenges, are discussed.

- Information created by clients smart devices and sensors such as videos and photos, GPS data, health data by wearable devices, and smart home statuses detected by the sensors usually contains gigantic amounts of valuable data that when analyzed will benefit individuals and societies as a whole. Big data analysis was one of the discussed issues facing blockchain. We propose dew

computing as a solution to this problem. Dew servers shall be able to store and participate in big data analysis, which could not be performed on IoT devices due to their constrained resources nor in blockchain alone due to encryption dilemma.
- Computation offloading service was included in our architecture to relieve intensive and heavy computation tasks from the less capable IoT devices to more powerful dew servers. This solves the problem of computational and power demanding POW consensus algorithm. This means that the consensus mechanism will be deployed in the dew-blockchain layer. The same problem was further tackled by adopting pBFT algorithm which consumes less power.
- Also, resource-constrained mobile devices that communicate their data using wireless links represent a security vulnerability -as discussed earlier in Section VIII- shall benefit from the deployed computation offloading service. With dew servers deployed at the edge of the network, closer to end devices, dew-blockchain layer resources can take the processing load from the devices. Those tasks involve hash computations, encryption and decryption, as well as consensus mechanism, are offloaded from the devices and outsourced to dew servers for execution. Blockchain safeguards the security aspects of this module in case a computation operation requires assignment to multiple dew nodes. Being relieved of such operations, end devices' battery lifetime gets increased and execution of tasks speeds up with increased efficiency and security.
- Outsourcing decentralized data storage, which outweighs the centralized storage in conventional cloud computing. The decentralized data storage provided by the integration of dew computing and blockchain exploits the benefits of both technologies to increase storage sizes, heighten the security of stored data, and keep data closer to the end devices layer. Storing data on dew servers close to consumers shall decrease the communication latency and elevate the system availability and performance. The large storage capacity offered by dew computing complements the validated security in blockchain to ensure a decentralized storage management in a peer to peer environment without entrusting the data to a centralized authority. The same applies to the cloudlet-blockchain layer which although not close to consumers but shares with the dew-blockchain layer the capability to provide access decentralized and secured data storage facilities.

XII. CONCLUSION

IoT network is growing tremendously in terms of types of applications and number of devices. This created many challenges that need urgent solutions to enable exploiting the full potential of IoT in the future. On the other hand blockchain technology appeared as a distributed immutable transparent decentralized and secured technology that has a promising role in many sectors. The characteristics and structure of blockchain make it a strong candidate to solve IoT system issues through integration. The integration process captured the attention of many researchers who came up with different IoT -Blockchain integrated architectures and designs. However, none of the proposed studies was capable of solving most of the challenges nor exploring the full potential of blockchain to benefit from it in the IoT paradigm. This research proposes a new architecture based on three layers system consisting of; devices layer, dew-blockchain layer, and cloudlet-blockchain layer. It is the only architecture that utilizes dew computing in the integration process between IoT and blockchain. The novelty of including dew and cloudlet computing serves the final design by bringing computing resources as close as possible to the IoT devices so that traffic in the core network can be secured and with the minimum end-to-end delay between the IoT devices and computing resources. In addition to adopting cloudlet computing as a means to bringing servers closer to IoT devices, the proposed architecture reduces the end-to-end delay by utilizing private and consortium blockchains, which requires a transaction verification time in the order of milliseconds opposite to public blockchain, which needs a transaction approval time in the order of minutes [13]. In addition, it is the only design that does not include a cloud layer and instead depends on distributed cloudlets for higher-level computational tasks and ultimate decentralization in addition to reducing the end-to-end message delay. Our architectural design solved many problems facing IoT systems such as constraints of IoT devices, big data analysis, data privacy, and security in IoT systems, data storage, intensive computational and analytical requirements as well as core network traffic.

REFERENCES

[1] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.

[2] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[3] J. Rivera and R. van der Meulen, "Forecast alert: Internet of Things—Endpoints and associated services, worldwide," Tech. Rep., 2016.

[4] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, 2018.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[7] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[8] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the Internet of Things: Challenges and opportunities," *IEEE Netw.*, vol. 30, no. 2, pp. 92–100, Mar. 2016.

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

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[11] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May 2016.

[12] M. Banerjee, J. Lee, and K.-K.-R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[13] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.

[14] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms," *Bus. Horizons*, vol. 62, no. 3, pp. 273–281, May 2019.

[15] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018.

[16] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?" *Int. J. Prod. Econ.*, vol. 211, pp. 221–236, May 2019.

[17] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ, USA: Wiley, 2016.

[18] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, 2015.

[19] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing blockchains: Characteristics & applications," 2018, *arXiv:1806.03693*. [Online]. Available: http://arxiv.org/abs/1806.03693

[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, White Paper, 2019. [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper/

[21] Q. Tang and L. M. Tang, "Toward a distributed carbon ledger for carbon emissions trading and accounting for corporate carbon management," *J. Emerg. Technol. Accounting*, vol. 16, no. 1, pp. 37–46, Mar. 2019.

[22] *Hotspot for Blockchain Innovation*, I. A. Deloitte, Israel, 2016.

[23] *Learn About Ethereum*, Ethereum, 2020. [Online]. Available: https://ethereum.org/en/about/

[24] B. Fu, Z. Shu, and X. Liu, "Blockchain enhanced emission trading framework in fashion apparel manufacturing industry," *Sustainability*, vol. 10, no. 4, p. 1105, Apr. 2018.

[25] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper 37, 2014, vol. 3.

[26] W. Shao, Z. Wang, X. Wang, K. Qiu, C. Jia, and C. Jiang, "LSC: Online auto-update smart contracts for fortifying blockchain-based log systems," *Inf. Sci.*, vol. 512, pp. 506–517, Feb. 2020.

[27] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54.

[28] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[29] A. Kawa and A. Maryniak, *SMART Supply Network*. Berlin, Germany: Springer, 2019.

[30] 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.

[31] H. Sun, S. Hua, E. Zhou, B. Pi, J. Sun, and K. Yamashita, "Using Ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling," in *Proc. Int. Conf. Blockchain*. Berlin, Germany: Springer, 2018, pp. 3–17.

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

[33] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC Trends Anal. Chem.*, vol. 107, pp. 222–232, Oct. 2018.

[34] P. Veena, S. Panikkar, S. Nair, and P. Brody, "Empowering the edge practical insights on a decentralized Internet of Things," IBM Inst. Bus. Value, 2015, vol. 17.

[35] 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.

[36] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Dec. 2016, pp. 116–119.

[37] D. Kundu, "Blockchain and trust in a smart city," *Environ. Urbanization ASIA*, vol. 10, no. 1, pp. 31–43, Mar. 2019.

[38] M. J. Casey and P. Vigna, "In blockchain we trust," *MIT Technol. Rev.*, vol. 121, no. 3, pp. 10–16, 2018.

[39] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Newton, MA, USA: O'Reilly Media, 2014.

[40] N. Taleb, "Prospective applications of blockchain and bitcoin cryptocurrency technology," *TEM J.*, vol. 8, no. 1, pp. 48–55, 2019.

[41] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov. 2017.

[42] P. Wang, R. X. Gao, and Z. Fan, "Cloud computing for cloud manufacturing: Benefits and limitations," *J. Manuf. Sci. Eng.*, vol. 137, no. 4, pp. 1–9, Aug. 2015.

[43] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[44] I. Friese, J. Heuer, and N. Kong, "Challenges from the identities of things: Introduction of the identities of things discussion group within kantara initiative," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 1–4.

[45] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the Internet of Things," *J. Cyber Secur. Mobility*, vol. 1, no. 4, pp. 309–348, 2013.

[46] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, Jun. 2018.

[47] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[48] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020.

[49] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2013–2021, Mar. 2020.

[50] K. Xiao, Z. Gao, W. Shi, X. Qiu, Y. Yang, and L. Rui, "EdgeABC: An architecture for task offloading and resource allocation in the Internet of Things," *Future Gener. Comput. Syst.*, vol. 107, pp. 498–508, Jun. 2020.

[51] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017, *arXiv:1706.01730*. [Online]. Available: http://arxiv.org/abs/1706.01730

[52] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[53] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5549–5561, May 2020.

[54] S. He, Q. Tang, C. Q. Wu, and X. Shen, "Decentralizing IoT management systems using blockchain for censorship resistance," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 715–727, Jan. 2020.

[55] Nyamtiga, Sicato, Rathore, Sung, and Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, Jul. 2019.

[56] H. Hosseinian, H. Shahinzadeh, G. B. Gharehpetian, Z. Azani, and M. Shaneh, "Blockchain outlook for deployment of IoT in distribution networks and smart homes," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 10, no. 3, p. 2787, Jun. 2020.

[57] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Jul. 2018.

[58] Y. Chen, X. Wang, Y. Yang, and H. Li, "Location-aware Wi-Fi authentication scheme using smart contract," *Sensors*, vol. 20, no. 4, p. 1062, Feb. 2020.

[59] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, "A cost analysis of Internet of Things sensor data storage on blockchain via smart contracts," *Electronics*, vol. 9, no. 2, p. 244, Feb. 2020.

[60] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, and L. Rizzello, "A blockchain tokenizer for industrial IOT trustless applications," *Future Gener. Comput. Syst.*, vol. 105, pp. 432–445, Apr. 2020.

[61] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications," *Procedia Comput. Sci.*, vol. 98, pp. 461–466, 2016.

[62] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial Internet of Things technology," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1442–1453, Dec. 2019.

[63] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, ''Resource trading in blockchain-based industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[64] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, ''Application-aware consensus management for software-defined intelligent blockchain in IoT,'' *IEEE Netw.*, vol. 34, no. 1, pp. 69–75, Jan. 2020.

[65] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, and G. C. Polyzos, ''Decentralized authorization in constrained IoT environments exploiting interledger mechanisms,'' *Comput. Commun.*, vol. 152, pp. 243–251, Feb. 2020.

[66] A. Rovira-Sugranes and A. Razi, ''Optimizing the age of information for blockchain technology with applications to IoT sensors,'' *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 183–187, Jan. 2020.

[67] S. Aich, S. Chakraborty, M. Sain, H.-I. Lee, and H.-C. Kim, ''A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study,'' in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 138–141.

[68] J. Lin, Z. Shen, A. Zhang, and Y. Chai, ''Blockchain and IoT based food traceability for smart agriculture,'' in *Proc. 3rd Int. Conf. Crowd Sci. Eng. (ICCSE)*, 2018, pp. 1–6.

[69] F. Knirsch, A. Unterweger, and D. Engel, ''Implementing a blockchain from scratch: Why, how, and what we learned,'' *EURASIP J. Inf. Secur.*, vol. 2019, no. 1, p. 2, Dec. 2019.

[70] F. Samie, V. Tsoutsouras, L. Bauer, S. Xydis, D. Soudris, and J. Henkel, ''Computation offloading and resource allocation for low-power IoT edge devices,'' in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 7–12.

[71] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ''A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,'' *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[72] A. Torkaman and M. A. Seyyedi, ''Analyzing IoT reference architecture models,'' *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 8, p. 154, 2016.

[73] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, ''A survey on security and privacy issues of bitcoin,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[74] A. Dorri, S. S. Kanhere, and R. Jurdak, ''MOF-BC: A memory optimized and flexible blockchain for large scale networks,'' *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.

[75] V. Grover, R. H. L. Chiang, T.-P. Liang, and D. Zhang, ''Creating strategic business value from big data analytics: A research framework,'' *J. Manage. Inf. Syst.*, vol. 35, no. 2, pp. 388–423, Apr. 2018.

[76] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, ''Big data analytics for manufacturing Internet of Things: Opportunities, challenges and enabling technologies,'' *Enterprise Inf. Syst.*, vol. 14, nos. 9–10, pp. 1279–1303, 2019.

[77] *Hyperledger*, T. L. Found., 2020.

[78] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini, ''CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[79] B. Carson, G. Romanelli, P. Walsh, and A. Zhumaev, ''Blockchain beyond the hype: What is the strategic business value,'' McKinsey Company, Tech. Rep., 2018, pp. 1–13.

[80] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, ''Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards,'' *Overview Rep. Brit. Standards Inst. (BSI)*, vol. 40, p. 40, May 2017.

[81] *Blockchain and Distributed Ledger Technologies*, ISO, Geneva, Switzerland, 2016.

[82] *E. U. A. for Cybersecurity*, Eur. Commission, 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[83] *The General Data Protection Regulation (GDPR)*, European Patent Office, Munich, Germany, 2020.

[84] Y. Pan, P. Thulasiraman, and Y. Wang, ''Overview of cloudlet, fog computing, edge computing, and dew computing,'' in *Proc. 3rd Int. Workshop Dew Comput.*, 2018, pp. 20–23.

[85] K. Skala, D. Davidovic, E. Afgan, I. Sovic, and Z. Sojat, ''Scalable distributed computing hierarchy: Cloud, fog and dew computing,'' *Open J. Cloud Comput.*, vol. 2, no. 1, pp. 16–24, 2015.

[86] Y. Wang, ''Definition and categorization of dew computing,'' *Open J. Cloud Comput.*, vol. 3, no. 1, pp. 1–7, 2016.

[87] P. P. Ray, ''An introduction to dew computing: Definition, concept and implications,'' *IEEE Access*, vol. 6, pp. 723–737, 2018.

[88] Y. Wang, ''A blockchain system with lightweight full node based on dew computing,'' *Internet Things*, vol. 11, Sep. 2020, Art. no. 100184.

[89] *What is Consensus Algorithm in Blockchain & Different Types of Consensus Models*, Medium, BangBit Technol., Bengaluru, India, 2018.

[90] M. Vukolić, ''The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,'' in *Proc. Int. Workshop Open Problems Netw. Secur.* Berlin, Germany: Springer, 2015, pp. 112–125.

[91] *What is Practical Byzantine Fault Tolerance (pBFT)*, Crush Crypto, Vancouver, BC, Canada, 2020.

ALIA AL SADAWI received the B.Sc. degree in electrical and electronics engineering, and the M.Sc. degree in engineering systems management from the American University of Sharjah, United Arab Emirates, in 2016, where she is currently pursuing the Ph.D. degree. She is also a Graduate Teaching Assistant working with the American University of Sharjah. She was involved in multiple projects related to decision making, sustainability in smart city and blockchain application in supply chain, logistics and carbon trading. Her research interests include blockchain integration with the IoT and their applications in the smart industrial sector.

MOHAMED S. HASSAN received the M.Sc. degree in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 2000, and the Ph.D. degree in electrical and computer engineering from the University of Arizona, USA, in 2005. He is currently a Full Professor of electrical engineering with the American University of Sharjah. He was involved in multiple projects related to free space optical communications, electromagnetic shielding, demand response and smart grids, anti-static flooring and fiber optic sensors for infrastructure health monitoring applications in addition to EV wireless charging systems. His research interests include multimedia communications and networking, wireless communications, cognitive radios, resource allocation and performance evaluation of wired networks, and next generation wireless systems.

MALICK NDIAYE received the M.S. degree in quantitative methods in economics, optimization and strategic analysis from the University of Paris 1 Sorbonne, France, and the Ph.D. degree in operations research from the University of Burgundy, France. He has worked with the University of Birmingham, U.K., and the King Fahd University of Petroleum and Minerals, Saudi Arabia, before joining the American University of Sharjah. His recent scholarly work focuses on developing last-mile delivery routing solutions, vehicle routing optimization in cold supply chain, and the use of emerging technology to improve logistics systems. His research interests include operations research, supply chain, and logistics systems management. He is a Certified Supply Chain Professional from the American Association for Operations Management (APICS).