Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6672482, 25 pages
https://doi.org/10.1155/2021/6672482

Review Article

On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives

Clement Nartey,[1] **Eric Tutu Tchao**,[1] **James Dzisi Gadze**,[2] **Eliel Keelson**,[1] **Griffith Selorm Klogo**,[1] **Benjamin Kommey**,[1] **and Kwasi Diawuo**[3]

[1]*Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana*
[2]*Department of Telecommunications Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana*
[3]*Department of Computer Engineering, University of Energy and Natural Resources, Sunyani, Ghana*

Correspondence should be addressed to Eric Tutu Tchao; ettchao.coe@knust.edu.gh

Received 29 December 2020; Revised 4 March 2021; Accepted 13 April 2021; Published 29 April 2021

Academic Editor: Maria Fazio

Digitization and automation have engulfed every scope and sphere of life. Internet of Things (IoT) has been the main enabler of the revolution. There still exist challenges in IoT that need to be addressed such as the limited address space for the increasing number of devices when using IPv4 and IPv6 as well as key security issues such as vulnerable access control mechanisms. Blockchain is a distributed ledger technology that has immense benefits such as enhanced security and traceability. Thus, blockchain can serve as a good foundation for applications based on transaction and interactions. IoT implementations and applications are by definition distributed. This means blockchain can help to solve most of the security vulnerabilities and traceability concerns of IoTs by using blockchain as a ledger that can keep track of how devices interact, in which state they are and how they transact with other IoT devices. IoT applications have been mainly implemented with technologies such as cloud and fog computing, and AI to help address some of its key challenges. The key implementation challenges and technical choices to consider in making a successful blockchain IoT (BIoT) project are clearly outlined in this paper. The security and privacy aspect of BIoT applications are also analyzed, and several relevant solutions to improve the scalability and throughput of such applications are proposed. The paper also reviews integration schemes and monitoring frameworks for BIoT applications. A hybrid blockchain IoT integration architecture that makes use of containerization is proposed.

1. Introduction

Blockchain has been tagged as one of the most disruptive technologies of all time. There have been many applications in different sectors and industries such as finance [1], healthcare [2, 3], utilities [4], agriculture [5], real estate [6], and supply chain management [7, 8]. This is because trusted intermediaries that serve as gatekeepers for certain applications in these industries can be eliminated and those same applications can be run in a decentralized manner without any centralized authority. This is done efficiently without any compromise on efficiency and security which was not possible in times past.

The concept and implementation of blockchain have enabled the establishment of trustless peer-to-peer networks that enable participants on the network to transact and share data without having to trust each other. Third-party trusted intermediaries have been notoriously known to cause a delay in transaction times in most industries. An absence of such intermediaries would mean that there would be faster reconciliation between transacting parties and participants. Blockchains operate with a heavy reliance on cryptographic schemes and hashing functions which tend to bring a high sense of security and authoritativeness to all interactions and transactions in the network. Blockchains in past times were just seen as distributed ledgers or databases, but they have been empowered by smart contracts. Smart contracts are independent self-executing scripts that reside on blockchains that give it a high level of autonomy that combines all the aforementioned features to provide a truly distributed platform. This has earned the interest of many developers and industry giants in the Internet of Things (IoT) domain.

Internet of Things (IoT) has also had many implementations in different areas such as smart healthcare solutions [3], smart and connected agriculture [9, 10], smart homes [11, 12], wearables [13, 14], augmented reality [15, 16], and transportation [17], among others. IoT transforms traditional objects and devices into intelligent objects by exploiting technologies such as internet protocols and sensor networks.

Blockchains and IoT on their own have proven to bring immense advancement and advantages to the areas and sectors that they have been applied. The goal of this paper is to provide a comprehensive description of how blockchains and smart contracts work, their origins (i.e., Distributed Ledger Technologies (DLTs)), and the pros and cons of the technology. We would also seek to give some insight into IoT devices and networks and highlight the key considerations that are needed to use the two technologies together. This will enable readers to identify possible use cases in industries that do not already have such implementation. This would also empower anyone willing to implement a blockchain IoT (BIoT) project to know the right things to do and to make informed decisions when integrating blockchains into their project. Even if it means the project is to be started from scratch, the works analyzed in this paper would provide a sound basis to make the right technical choices.

The structure of this paper is as follows. In Section 2, we examine the root technology of blockchains (Distributed Ledger Technologies (DLTs)) and explain how blocks and chains are formed in blockchains. We also look into how smart contracts work. The section ends with a taxonomy of some common blockchains. The functioning of IoT devices and networks is also explained. In Section 3, some past BIoT implementations are considered and discussed in detail. In this section, the key technical choices that have to be considered for any BIoT implementation are outlined. The best cryptographic and consensus algorithms needed to integrate blockchains into IoT devices and networks are also discussed. Section 4 talks about the challenges that have been faced so far by current BIoT implementations as well as the issues that IoT developers and researchers would need to keep in mind when deploying a blockchain-based IoT solution. Section 5 explores more deeply the current challenges that have plagued and challenged other BIoT applications by considering the challenges faced in the aspects of privacy, security, scalability, throughput, and latency as well as some solutions that have been provided in literature to compact and solve them. Section 6 considers some future directions and recommendations that should be taken into account when BIoT solutions are being implemented. Section 7 summarizes all the contributions that we have made in the paper. Our conclusions are presented in Section 8.

2. Methodology

This paper reviewed a number of application scenarios where the adoption of BIoT applications has been proposed and even in some cases implemented.

2.1. Data Sources. This review used literature from 4 electronic databases as follows:

(i) Google Scholar

(ii) IEEE Xplore

(iii) Elsevier ScienceDirect

(iv) Springer SpringerLink

The search in all the databases returned 10900 results. Google Scholar and SpringerLink returned a number of unrelated results; thus, just the first 100 relevant and fitting results were considered for our review.

Our search through these databases was done based on the keywords that have been outlined in this paper. Search strings were formed from these keywords. The following search string was used:

(blockchain OR "block chain") AND
(IoT OR "Internet of Things" OR Internet of Things) AND
applications AND
(Security OR "Security") AND
(Privacy OR "Privacy")

The search was conducted in May 2020. The search took into consideration the application areas where BIoT had been used. We do note that the list of application scenarios mentioned in this review is not exhaustive but they provide a good overview of things that are possible with BIoTs. The procedure that was used is summarized in Figure 1. We chose some of the most promising application areas being studied by researchers now as well as some application areas that have not yet been studied by other existent detailed surveys. For example, [7] looked at methods of integrating blockchains with IoT, [18] reviewed IoT security, and [19] reviewed machine learning techniques for ensuring IoT security. None of these reviews analyzed in depth the integration of blockchain and IoT, its security and privacy aspects altogether. In addition, we have added some deep learning techniques for ensuring BIoT security and we have also provided some further research directions in the area of machine learning that still need to be applied to BIoTs. A hybrid blockchain IoT integration architecture that makes use of containerization is also proposed.

2.2. Selection Methods for Reviewed Literature

(i) *Temporal Selection*. The literature that we considered from our search was selected based on a three-year temporal criterion. The studies that were included were from the years 2017 to 2020. For example, the "Since 2020" filter on Google Scholar was used for this. The studies in 2020 that were considered were just those that were available at the time of conducting this research. The reason for choosing the three-year criterion was so that we may have access to the newest, most relevant, and exciting studies that are shaping future research

(ii) *Relevant Information Gathering and Selection*. The final list of considered studies for this review was based on a full-text reading of those studies which were within our temporal range. The papers used

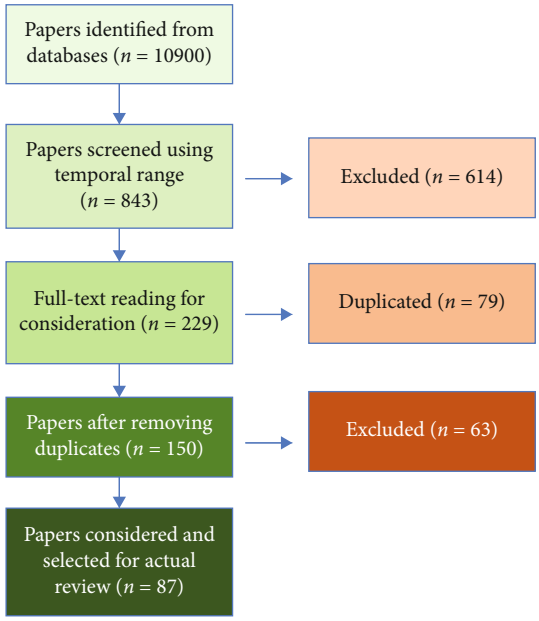

Figure 1: Research flow for paper and literature selection.

for the state-of-the-art section of this paper were those that provided a very good understanding of the underlying technologies that constitute blockchains and IoTs. In the rest of the review, we considered literature that provided novel solutions, frameworks, and architectures to BIoT implementations. Studies that were not closely related to the defined research topic were not considered and thus excluded from this review. Some of the literature appeared as duplicates in 4 different databases; thus, there were 229 publications considered but after eliminating the duplicates, 150 publications remained. The last selection phase was based on full-text reading, and 63 of these publications were excluded. This was due to the fact that some of the information discussed was quite general and others did not have full implementation or design details

3. State-of-the-Art

This section provides a review of the key concepts and provides adequate background knowledge about Distributed Ledger Technologies (DLTs), blockchain technology and its types, IoT, and BIoT (blockchain with IoT).

3.1. Distributed Ledger Technology (DLT). Distributed Ledger Technology (DLT) is not a single technology. DLT uses a combination of technologies that have a considerable history in mathematics, computer science, and commercial applications. These technologies include the private/public-key cryptography, cryptographic hash functions, distributed databases, consensus algorithms, and decentralized/distributed processing.

It is required that in order to create and use a DLT, a peer-to-peer (P2P) network must be established among all participants of the DLT. All these technologies come together to create a distributed database that is shared and possessed by each member in the network [20]. Thus, a set of protocols are designed to replicate this database which is represented in a timestamped and an ordered manner which is called a ledger [21]. The data in the ledger that is possessed by each party in a DLT network is kept consistent by means of hash chaining. Any DLT must have these features: decentralized architecture, be trustless, must have collective maintenance and a reliable database, and maintain the anonymity of nodes [9]. These facts can be expounded upon as follows:

(i) *Decentralized*. There is no centralization in the whole system, and thus, if one node in the system crashes or goes off the network, the system should still be up. This goes to speak of the robustness of DLTs

(ii) *Trustless*. Nodes on blockchain networks are capable of trusting one another since the system is running with full transparency

(iii) *Collective Maintenance*. The nodes and the blocks on the system are maintained by no one and everyone since blockchains have consensus algorithms that help to prove the authenticity of blocks

(iv) *Reliable Database*. Every node receives a copy of the current ledger as it is. The reliability of the blockchain ledger has been shown to scale with an increase in the number of nodes available on the blockchain network. Thus, in theory, any traditional blockchain system has a tolerance of 51% [9, 22], which means for an attacker to gain control of the network, that person would have to take control of 51% of the nodes

(v) *Anonymity*. Since there is no need for trust in the network, nodes can remain anonymous and there is no need to reveal the identity of a node

There are two main classes of DLTs. These are blockchains and Directed Acyclic Graph (DAG). Blockchains are DLTs that have their origins in cryptocurrencies. Blockchains are talked about in much detail in Section 3.2.1. Directed Acyclic Graphs (DAGs), on the other hand, works with a graph structure that is directed with no cycles connecting to any other edges. This allows a DAG to keep the trustless properties of DLTs because, since the edges of the graph are directed and go only in one direction, it makes it impossible to revert the entire graph structure. The graph being directed in one direction also allows the DAG to have the feature of traceability. This is because whenever you start at any one edge, you can follow through the graph structure all the way to where it ends. Some popular examples of DAGs are Hedera Hashgraph and IOTA.

3.2. Understanding Blockchains. In this section, we discuss the building blocks that make up blockchain technology. This is to help understand the rest of the paper.

3.2.1. Blockchain. The blockchain technology is a part of a set of technologies called Distributed Ledger Technologies.

These technologies are capable of tracking, coordinating, carrying out transactions, and storing information from different devices in different locations thus eliminating the need of a centralized cloud system. Blockchain technology has been growing at an ever-increasing rate over the past few years. A report by Statista shows that the startup investment capital into blockchain rose to about 550 million U.S. dollars in 2016 and forecasted that by 2021, investments that would have been made into the technology will be well over 2.3 billion U.S. dollars [23, 24].

The rise of cryptocurrencies has led to the rapid popularity of the blockchain technology. Bitcoin [21] was the first of the bunch to surface and has been seen by people as the king of cryptocurrencies. Others have also grown in popularity over the years, and these include the likes of Ethereum [25], Ripple [26], and Dogecoin [27]. The building blocks of blockchains inherited from DLTs are shown in Figure 2.

The use of cryptocurrencies was said to revolutionize the way payments were going to be made in the future when they started to go mainstream due to their advantages over traditional hard currencies [23]. This was due to the fact that middlemen were going to be eliminated, money transfer merchant fees were going to be reduced to probably below 1%, and there was going to be a reduction in the amount of time it takes to transfer and receive funds. This has not really taken effect yet due to the many misconceptions and misinformation about these blockchain-based currencies. It is still being referred to as an immature technology even though it has come very far since its inception. The associated challenges may take a few years to solve.

The concept of a blockchain was originally proposed to be used as a tool for cryptocurrency, but that is not all you can do with blockchains. Many researchers have proposed and presented surveys and studies on the application of blockchain in different fields. These range from proposed architectures of blockchains and smart contracts in the deployment of BIoT solutions [28] to blockchain for big data and industrial applications [29, 30]. These research works have led to the development of many applications on blockchain systems called Distributed Applications (DApps) [31]. In [32], platforms which facilitate the development of DApps for IoT devices such as IOTIFY, iExec, and Xage were discussed.

The inner workings of blockchain systems show their heavy dependence on cryptographic algorithms. Based on the cryptographic principles of the blockchain, every node on the network would thus receive two keys: a public key (for encryption), which is used by other nodes to encrypt messages targeted at that node, and a private key (for decryption), which allows that node to read its messages. Thus, the public key works as the unique address or identifier of the node on the network while the private key is used by a node on the network to approve and sign transactions. This means that only a node which has the appropriate private and public key is capable of decrypting messages that are sent corresponding to a particular public key. This is what is termed as asymmetric cryptography [33, 34].

When a node makes a transaction, it uses its private key to sign that transaction thereby authenticating it. This is then passed on to the node's one-hop peer for broadcasting through the network. If there is an error or a problem in the transmission of the transaction data, it will not be decrypted. As the data is moved on by peer-to-peer broadcasting, each node verifies that the transaction is valid before retransmission occurs. Thus, the data is propagated through the network with integrity.

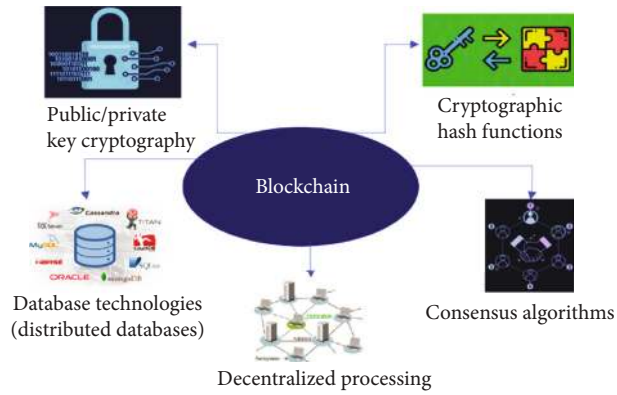

Figure 2: The five arms of blockchain technologies.

Transactions which are proven in this way are then organized into timestamped blocks by special nodes on the network called miners. The consensus algorithm that is run as part of the blockchain determines which miners are elected as well as the data that is included as new blocks on the chain. Each block in a blockchain (see Figure 3) contains an ordered set of records or transactions and a hash of the previous block in its header (starting from an initial block called the "genesis" block). This means its hash depends on the hash of its parent. Any change in the data of one block would affect all other blocks that follow. Such a change would require a new consensus process (for example, "proof-of-work" or "proof-of-stake").

As new blocks are propagated through the network, the nodes verify that previous transactions have not been tampered with and that a new block is referencing the previous block added on the chain by checking its hash. If both the transaction and its hash are verified, the block is added successfully unto the chain of blocks, thus updating the ledger [23].

3.2.2. Smart Contracts. A blockchain is a very robust technology that can be made up of any type of data, as well as code, in its records and ledger. Storing code is not the same as executing code; thus, having the ability to execute code on a blockchain gives it a new set of superpowers which brings us to the aspect of smart contracts [35]. Apart from cryptocurrencies and data storage, many other complex applications can be built on top of blockchain which are powered by these smart contracts. This has led to the development of concepts such as Decentralized Applications (Dapps), Decentralized Autonomous Organizations (DAOs), smart tokens, and property assets (being used to represent real-life assets). This used in conjunction with cryptocurrencies has caused a major disruption in financial services over the years [31].

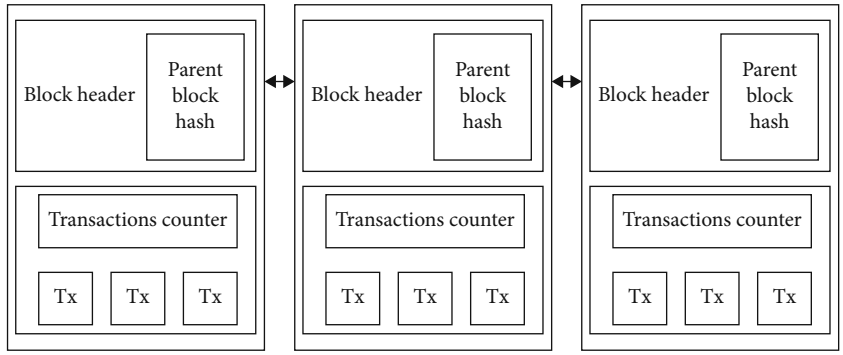

Figure 3: Blockchain sample containing blocks with hashes (adopted from [31]).

The term smart contract is usually misunderstood by many, but it is simply a piece of code that contains arbitrary programming logic. It is not an actual contract between entities. For IoTs to be used on blockchain, this has to be a fundamental part to consider in order to choose the appropriate blockchain to use. Thus, a smart-contract-supporting-blockchain is one that does not just validate transactions and blocks but also validates the execution of the code contained in each block. This means that any function call to the code repository stored on the blockchain would be executed sequentially in the current block state and the final state is then updated accordingly [25]. In verifying blocks, each node would reexecute the function calls that a given block contains and check its result against what is stored in the block to see if the results are the same. Adding smart contracts on to blockchain gives it enhanced properties such as the following:

(i) Atomicity: an operation is able to run entirely or can fail without affecting the state of the chain

(ii) Immortality: it is only possible to remove the code and the data if a self-destruct operation is performed

(iii) Availability: the code and the accompanying data are always available for all

(iv) Provenance: the executed code can always be traced back to its executor

(v) Synchronous-execution: the code is always executed in a synchronous way

3.2.3. Types of Blockchains. There are different types of blockchains out there. More and more cryptocurrencies are emerging every day which are being built on top of these blockchains. This has also led to the development of more and more Dapps being built and used on these blockchains. The common among these are Bitcoin, Ethereum, Litecoin, and Hyperledger Fabric, just to mention a few.

(1) Bitcoin. The introduction of the Bitcoin blockchain generated a lot of interest among software developers and business moguls. It was created by Satoshi Nakamoto [21]. Bitcoin, as conceived by Satoshi Nakamoto, was an attempt to create a "cryptocurrency" outside the control of governments—a currency that would operate purely on the internet.

The pros of Bitcoin that made it very attractive were its immutable ledger and its pseudonymous nature, which meant that all transactions were accessible to everyone, thus making it very transparent. This transparency was a huge selling point, and a lot of use cases were showcased for industries that demanded high levels of transparency. Later on, in the development cycle of Bitcoin, smart contracts were introduced. The main drawback of Bitcoin was that it was permissionless, and as such, there was uncontrolled transparency. This meant anyone on the chain and anyone who had access to the chain could get access to all transactions. This also exposed the fact that even though nodes on the chain are not referenced by actual names but rather by hashed IDs, a bad actor on the chain can monitor the flow of funds and transactions between nodes to induce node identities. Bitcoin was also plagued with the problems of its slow transaction times (~=10 mins). Apart from this, for one to perform a transaction on the Bitcoin network, cryptocurrency is needed.

Bitcoin was built on a number of key elements as follows:

(i) A distributed file: called a "blockchain ledger" spread to all computers participating in the system

(ii) Proof of work: a complex mathematical procedure ("mining") which gives the "right" to write on the blockchain

(iii) Digital signatures: identity expressed as a number using public-private keys

(iv) Chained hashes

(v) Byzantine consensus: preventing "double spend" of Bitcoins

(2) Ethereum. This is an initiative of Vitalik Buterin and Gavin Wood. The vision for Ethereum [25] was to create a blockchain-based distributed virtual machine which would allow "smart contracts" to run as "distributed autonomous" entities. Ethereum uses a cryptocurrency "ETH" which is publicly traded on cryptocurrency exchanges and an internal "metering unit" called "GAS."

Gas provides a means to provide transaction charges, including running smart contracts, and also allocate incentives for running the Ethereum VM. Ethereum currently uses a "proof of work" mechanism for consensus but has plans to switch to a "proof of stake" methodology [25].

(3) Hyperledger Fabric. It was founded by the Linux Foundation to support business transactions. The chief focus was a technology that would be used for permissioned blockchains that industries and businesses and enterprises need because they did not want to put all their information out in the open on the public blockchains. Hyperledger Fabric [36] allows components, such as consensus and membership services, to be plug-and-play. Partly due to the backing of IBM, Hyperledger has received widespread support and is being used in many different projects, including its use by Walmart in the pork supply chain [37, 38].

A few popular blockchains are compared based on block initialization times and smart contract language. The Bitcoin blockchain, which is the king of all blockchain, has been seen to be very robust and stable. Our findings have revealed that the rate of adoption of blockchain for other applications apart from cryptocurrencies is on the rise. We also found that Ethereum has more DApps running on its blockchain than any other blockchain. This is due to its fast transaction time and block initialization time of 12 sec. We envisaged that this would continue to increase in the future. This is because more and more developers have started to fork the Ethereum blockchain to create their private blockchains. This is partly because Solidity (the programming language for writing smart contracts) is easy to learn. Other languages such as GoLang [39] have also been used to successfully write smart contracts to the Ethereum blockchain, leading to Ethereum's widespread adoption.

3.3. Background to Internet of Things (IoTs). The Internet of Things (IoT) is a concept that has gained popularity and heavy interest over the past few years. The world has seen applications in spheres such as smart healthcare solutions [3], smart and connected agriculture [9, 10], smart homes [11, 12], wearables [13, 14], augmented reality [15, 16], and transportation [17], among others. IoT allows physical devices and objects which in times past had no interconnectivity to communicate with other devices and networks thus enabling them to be smarter, giving them the ability to share information and make decisions. This has been led by a trend known as Machine-to-Machine (M2M) communication [40]. The number of interacting devices using the aforementioned communication was forecasted to grow from 780 million connected devices in 2016 to 3.3 billion devices in 2021. The smart agriculture market has also not been left out of this trend with an expected market growth from 5 billion U.S. dollars in 2016 to $15.3 billion U.S. dollars by 2025. These are all being made possible by enabling technologies such as internet protocols and sensor networks [41].

Current IoT implementations have heavily relied on traditional centralized server-client cloud architectures (see Figure 4) which enable communication via the internet. The current growth and expected forecast of the IoT industry have led to the proposal and development of new architectures and paradigms to handle the shortcomings of centralized server systems. These include large Peer-to-Peer Wireless Sensor Networks (P2P-WSNs) [41, 42]. It has been noted that some aspects with regard to privacy and security still need to be tackled to make these solutions robust [43].

In recent times, IoT applications using the said technology (P2P-WSNs) have been deployed and used for several use cases such as irrigation sensor networks [42] and smart farming [44, 45]. In developing an IoT solution, there are a few challenges that have to be addressed in order to have a successful implementation [46]. These are the following:

(i) *Hardware Challenges*. This has to do with the choice of sensors and meters that would be used in the implementation of the IoT solution. Some common ones that exist and that would be applicable in most use cases for IoT systems are temperature sensors, pressure sensors, gas sensors, grain moisture sensors [47], water quality sensors, etc.

(ii) *Data Analytics Challenges*. The data collected from these smart devices and sensors is enormous, and there is the need to put in place efficient data pipelines to process them and make sense of it. The use of predictive analysis and machine learning has been on the rise in this area, and choosing the right method to use must be closely considered

(iii) *Maintenance Challenges*. This involves the activities to ensure that sensors and IoT devices are functioning well and providing the right data for use. IoT devices and sensors can be quite delicate sometimes and most may also require some form or level of calibration

(iv) *Mobility Challenges*. This challenge comes about due to the mode of use of the IoT implementation. If the IoT solution is going to be used in a large area, then wired connections would not cut it; thus, in such a case, wireless communication approaches have to be employed. It also depends on the positions of your sensors in the sense of whether they are stationary or they will be in some sort of motion like in the case of drones. Choosing the right wireless technology in such as case is a must. Technologies such as 5G, 4G, Wi-Fi, Ultrawide Beacons, and Bluetooth (BLE) Beacons, among others, can be considered

(v) *Infrastructure Challenges*. The networking infrastructure to be used is one to greatly consider. Different types of infrastructural architectures exist that can be used, such as cloud computing, fog computing [13, 48, 49], and network virtualization

(vi) *Privacy and Security Challenges*. One of the aim problems of IoT solutions is the security and privacy. This becomes more prevalent when IoT solutions are being infused with legacy control systems which are built on top of the older protocols such as the

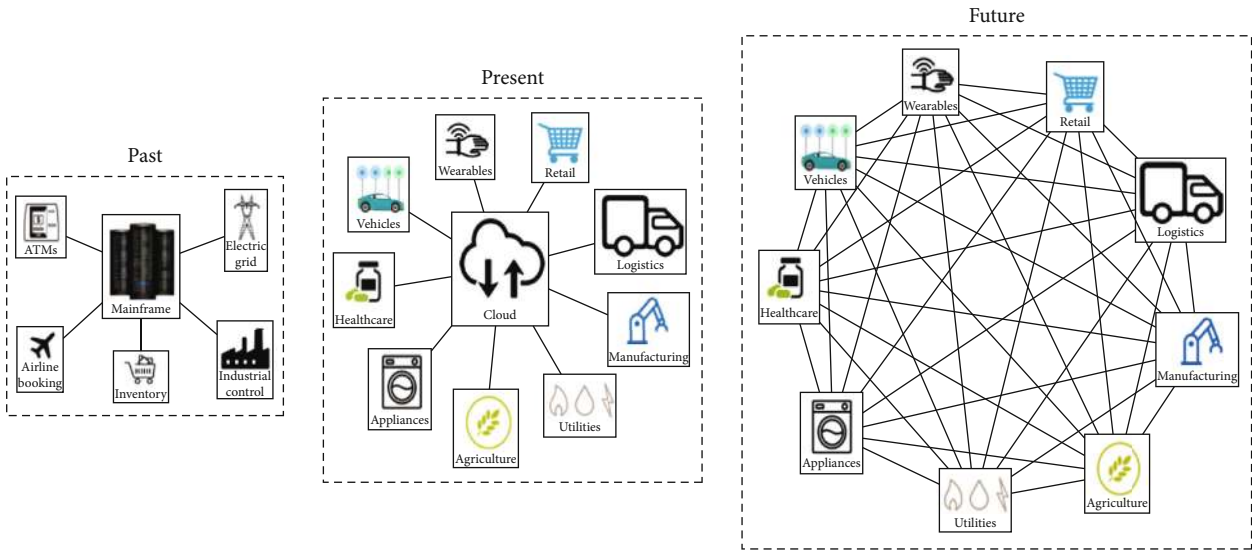

Figure 4: The past, present, and future IoT infrastructural architectures from Fernández-Caramés and Fraga-Lamas [23].

Supervisory Control and Data Acquisition (SCADA) [50] protocol. SCADA has notoriously been found in the past to be quite vulnerable to attacks. This is because SCADA was not originally built with interconnectivity in mind. This raises high security and privacy risks; thus, more secure communications must be sorted out

4. Blockchain IoT (BIoT) Integration

IoT, since its inception and mass adoption, has shown great potential in its ability to transform and optimize manual activities and incorporate them into the digital revolution. The main means by which IoT has become such a superpower is through cloud computing [51]. Cloud computing has provided the core communication and storage integration infrastructure for IoT implementations over the past few years. Through the use of advanced analytics, which can be embedded into cloud computing platforms, real-time actions and knowledge can be derived for the vast amount of information which is produced by IoT devices [52]. This form of integration with cloud computing meant that there had to be centralized architectures in place to ensure that correct data aggregation and distribution is achieved.

This has led to confidence issues and concerns on the path of IoT implementors. The main concern about these centralized architectures is that their data storage and retrieval are shown as black boxes to these IoT implementors. Cloud providers usually do not give clear insights into how the data is being stored on their platforms, but they rather make vague claims about the security of their systems which cannot always be verified. IoT implementors also tend to raise further concerns about who has access to their data.

Blockchain, as discussed earlier in Section 3.2, is built on the foundation of trust, confidence, data immutability, and decentralization. These features of blockchains can serve as major advantages and key revolutionary solutions to issues faced by IoTs if integrated properly. This type of integration can prove useful in cases where IoT data is to be shared among many participants. The main concerns that blockchain can readily help solve in the IoT paradigm include secure data access control and data sharing, enhanced data transparency, scalability, privacy, and reliability issues [51].

4.1. Blockchain IoT Infrastructure Design Architectures. IoT peer device communication is one aspect that cannot be ignored in IoT implementations. It forms the core of IoT interactions [20]. This leads to the formation of P2P networks for IoT device interactions where each IoT device is represented as a node in the network. In the case of integrating IoTs with blockchain, it is necessary to make the core design decision at which level or stage their P2P interactions can take place, i.e., through the blockchain, directly from one IoT peer to another peer or within a hybrid design architecture [53]. These interaction types are shown in Figure 5.

The advances that have been made with fog computing [54] have led to its incorporation and usage in hybrid design architectures leading to even better integration of IoTs and blockchains. The various design methodologies are expanded upon as follows:

(i) *IoT Peer to IoT Peer Architecture Design*. This design methodology is employed in scenarios where low latency and high performance are required. In such a case, only the metadata of transactions between IoT peer devices are stored on the blockchain but all other data is transferred between IoT peer devices directly. This architecture requires extensive routing and discovery techniques. This would ensure that the data from one IoT peer device find its way to the other IoT peer device in an efficient way. This architecture will work best in cases where devices belong to a single domain or are located in the same

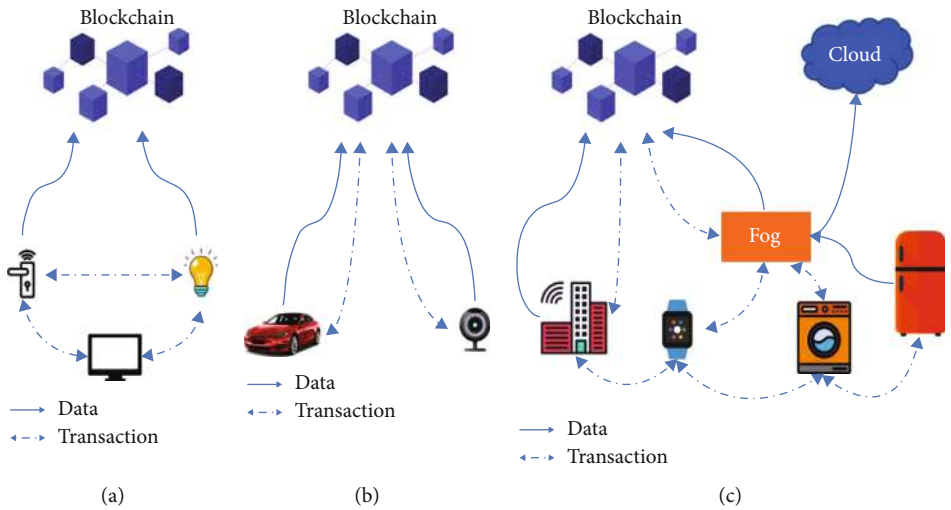

Figure 5: The different IoT peer device interactions.

area or are on the same network. This would help to reduce the complexity of discovery and routing required

(ii) *IoT Peer to Blockchain Architecture Design*. In this design scheme, all IoT peer devices do not have a direct link or means of connection between each other. All interactions and communications are done via the blockchain. This means that all the data that is associated with an interaction between two or more IoT peer devices can be logged and captured onto the blockchain. Thus, the blockchain can help to achieve the purpose of monitoring and verification of transactions between IoT devices. This helps to provide high traceability and transparency of the interactions between devices. This type of architecture can be essentially used for BIoT applications that provide trading and renting services such as Slock.it [55]. This could also be beneficial for IoT peer devices that are from different domain domains which require high fidelity of the data that is shared among them during transactions.

The downside of this architecture would be the high bandwidth and data requirements that would be needed by IoT peer devices to work and communicate in such a manner. Low latency is a requirement for IoT applications, but blockchains are notoriously known to have scalability and latency issues [56]. Thus, the latency of interactions would be increased for this type of design architecture because all information would have to be stored on the blockchain.

Implementing this type of architecture would also mean that IoT peer devices would have to act as nodes in the blockchain. This would require the devices to have the required computational resources to act as nodes in the blockchain. This can get more complicated due to the different types of consensus algorithms that can be used on blockchains. Figure 5(b) shows different devices in different locations and from different domains communicating over the blockchain. The blockchain is thus acting as a transaction verifier as well as storage repository for the data from IoT peer communications

(iii) *Hybrid Architecture Design*. The early years of IoT infrastructure development did not intend for IoT peer devices to be doing a lot of data processing and analysis. This has changed in recent years due to an approach called edge computing [57]. This allows for advanced intercommunication and processing of more data on IoT devices. The hybrid architecture design leverages the power of technologies such as artificial intelligence [57], fog computing [54], and edge computing to create a seamless environment for interaction for IoT devices. Even though edge computing has led to the production of IoT devices with increased computational power and resources, there are still not on that level to function as effective blockchain nodes (as noted as part of the challenges of the IoT peer to blockchain design). Thus, fog computing helps to reduce the energy consumption and computational load needed by IoT devices. It can also help to alleviate some of the bandwidth and latency issues discussed earlier. The fog computing layer which is incorporated into this type of architecture would do all the heavy lifting when it comes to the blockchain interactions such as mining (if needed). It also provides a platform for AI algorithms to run, and this can help to make critical decisions about these IoT peer devices. The strength of this design is that not all IoT interactions would go straight to the blockchain. This means all blockchain interactions would be done by the fog computing layer as well as serve as nodes on the blockchain. There can be an extra source of redundancy where the fogs may be connected to a cloud infrastructure (as shown in Figure 5(c))

4.1.1. A Proposed Update to the Hybrid Architecture. In our proposed update to the hybrid IoT architecture, the fog

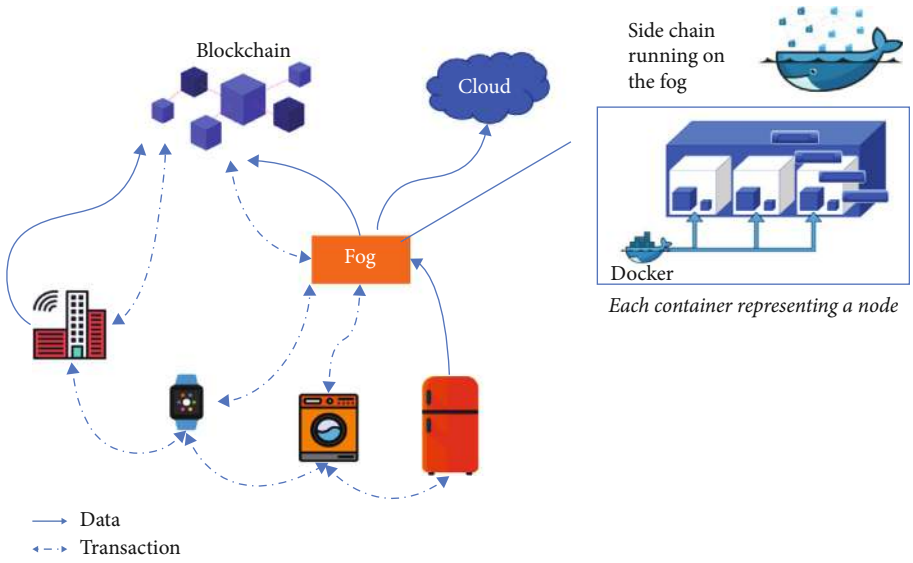

Figure 6: The proposed update to the hybrid architecture design.

computing node would not just be a node that would be connected to the blockchain. The fog node would rather run a side chain for the devices that are connected to it. In such a case, completed transactions on the side chain are going to be sent to the main chain. The blockchain mining process and interactions are still going to be abstracted from the IoT peer devices. The fog will not employ a traditional service-oriented monolithic architecture [58], and the nodes of the blockchain would not be the IoT peer devices. The way the side chain would operate would be by using microservices. Thus, there would be multiple microservices running as containers on the fog that would act as nodes on the sidechain. These containers would take up the mining activities from the IoT devices.

Each IoT device would be randomly assigned to a node in the sidechain (i.e., a container). Separate containers would not be created for each IoT device but rather a pool of IoT devices would be assigned to a node at a time. The depiction of this proposed update is shown in Figure 6.

Owing to a small number of container nodes, only a limited amount of delay is introduced for message propagation through the sidechain which ensures high throughput of transactions and this would be best suited for high transaction-high performance IoT implementations.

Leveraging this proposed update would provide various benefits to implementors of this architecture, and these benefits include the following:

(i) This update to the hybrid architecture would add advantages of microservices such as its loose-coupling features [59] and enhanced security to the already robust architecture

(ii) It would add an extra layer of security to the fog without comprising on performance and throughput. It would increase throughput since IoT peer device would not need to wait for transactions to be made on the main chain but rather on the side chain which would have a shorter resolution time

4.2. Analytics and Monitoring for Blockchain IoT Integrations. With all the data that would be produced from IoT peer devices, there has to be an effective monitoring and management framework that would aid IoT implementors to manage data traffic, sense events, and keep track of transactions that occur on these IoT devices. The major requirement for such a framework is modularity. In [53], the standard blockchain monitoring framework for IoT (SBMF-IoT) is proposed. It was based on a use case where three tracks connected to a blockchain were monitored using monitoring agents. These monitoring agents feed data into a blockchain monitoring system. The framework is described and shown in more detail in Figure 7.

Transparent end-to-end IoT transactions better control in performance and throughput as well as dynamically enabled nonintrusive monitoring routines were highlighted as major benefits of using the SBMF-IoT.

4.3. Future Integration Scenarios for BIoT. There are many ways by which blockchain can be integrated with IoT to solve specific problems. The following are a few scenarios that show this:

(i) *Extending Address Space for IoT Devices*. The number of IoT devices that are put online continues to rise day-by-day. Each device requires an IP address for routing communications and interactions to it. The IPv4 address space is limited and cannot cater for this increase. IPv6 has been employed in many IoT deployments [60]. IPv6 has worked well for IoT scenarios, since it has a 128-bit address space as compared to the 32-bit address space provided by IPv4, but still, the number of IoT devices keeps rising. Blockchain utilizes advanced cryptographic

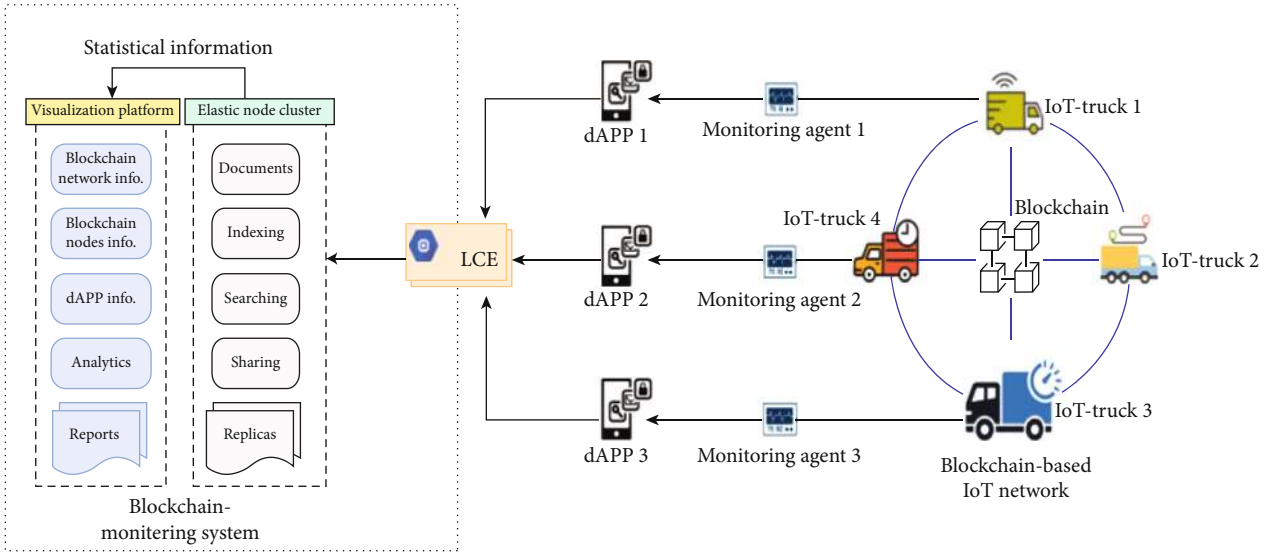

Figure 7: Standard blockchain monitoring framework for IoT (SBMF-IoT) proposed by Torky and Hassanein [53].

algorithms which employ a public key-private key scheme (see Section 4.5). The public key generated by the Elliptic Curve Signature Algorithm, for instance, has a 160-bit length (i.e., 20 bytes) [61]. This effectively means that if a 160-bit public address is used for addressing IoT devices, there would be about 1.46×10^{18} address spaces [18] for IoT nodes. This would be good enough to provide a unique identifier to IoT nodes and devices. If such a thing is implemented, there would be no need for an Internet Assigned Number Authority (IANA) [62] to assign IP addresses since all of this would be on the blockchain and managed by smart contracts from DApps. This would help to solve some of the scalability and security issues that would be faced in future IoT deployments

(ii) *Smart Contract-Based Access Control and Data Sharing for IoT Systems*. In [63], a smart contract-based framework was proposed to perform the task of access control for IoT devices. This framework is meant to solve the issue of having bad actors mimic other IoT devices and to prevent them from performing malicious activities. The framework is made up of three main components: Access Control Contracts (ACCs), Judge Contracts (JCs), and Register Contracts (RCs). A standard operation of the framework is to have multiple ACCs, one JC, and one RC on the blockchain. Each ACC performs the task of granting each subject-object pair an access control method. The ACC validates the access rights for each subject-object pair by performing two types of validation tasks: a dynamic access right validation and a static access right validation. The static access right validation is done based on predefined policies, and the dynamic access right validation checks subject behaviour. The JC receives reports from the dynamic ACC and performs misbehaviour-judging and penalizes offending subjects. In [64], a model to improve the penalty structure of the JC was proposed. This proposed design, shown in Figure 8, gives penalties to offending parties in the form of time-restricted periods of no ability to execute transactions. The RC registers all activities from the ACC and JC as well as the execution of management methods such as registrations, updates, and deletion that are performed by the ACCs and JC. The working of this framework is shown in Figure 8

4.4. BIoT Applications. BIoT is a term formed by combining blockchain with IoT applications. Due to some of the privacy and security concerns of IoT solutions as well as the sensitivity of the data that is obtained from them, especially in areas like healthcare [1] and supply chain management [1], some current implementations have infused blockchain into their IoT systems. Some examples of these include applications in wearables [65, 66], healthcare [3], data storage [67], smart transportation system, and smart cities [68].

The area of smart IoT agriculture has also seen some great applications. In [9], a food traceability blockchain system made use Radio Frequency Identification (RFID) as the authentication scheme to help identify food products as well as all the participants of the food supply chain. In [43], the researchers also proposed a fog computing architecture to help power blockchain-based agriculture IoT applications. The main argument was based on the low computational capacity of IoT devices, and thus, using the fog architecture proved to be very beneficial so that IoT devices serve as just nodes for transfer, and the heavy lifting (mining and validation) is done by the fog node (see Figure 9).

In [28], the authors propose a solution for secure over-the-air firmware updates for IoT devices. This would work in such a way that a manufacturer would have all its IoT devices as participants on the same blockchain network. The manufacturer would then have a smart contract on the

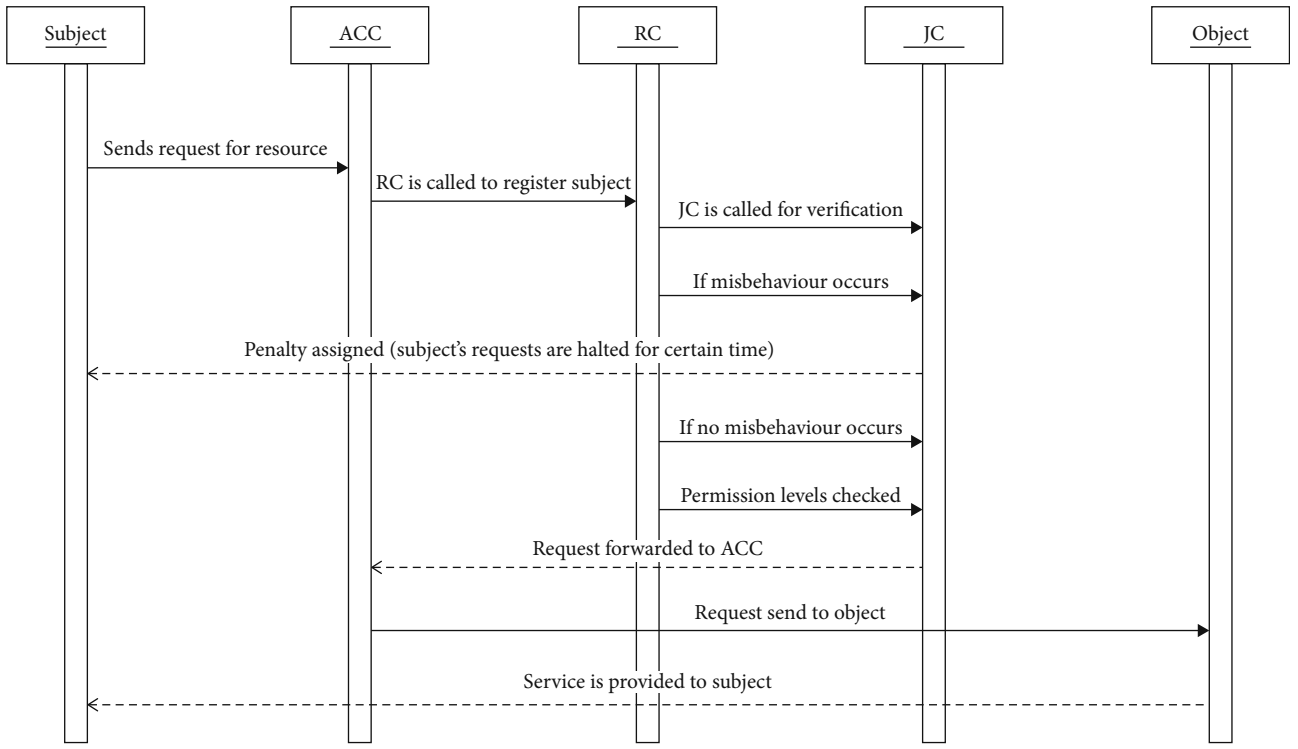

Figure 8: Flow diagram of the proposed system model for smart contract-based access control by Sultana et al. [64].

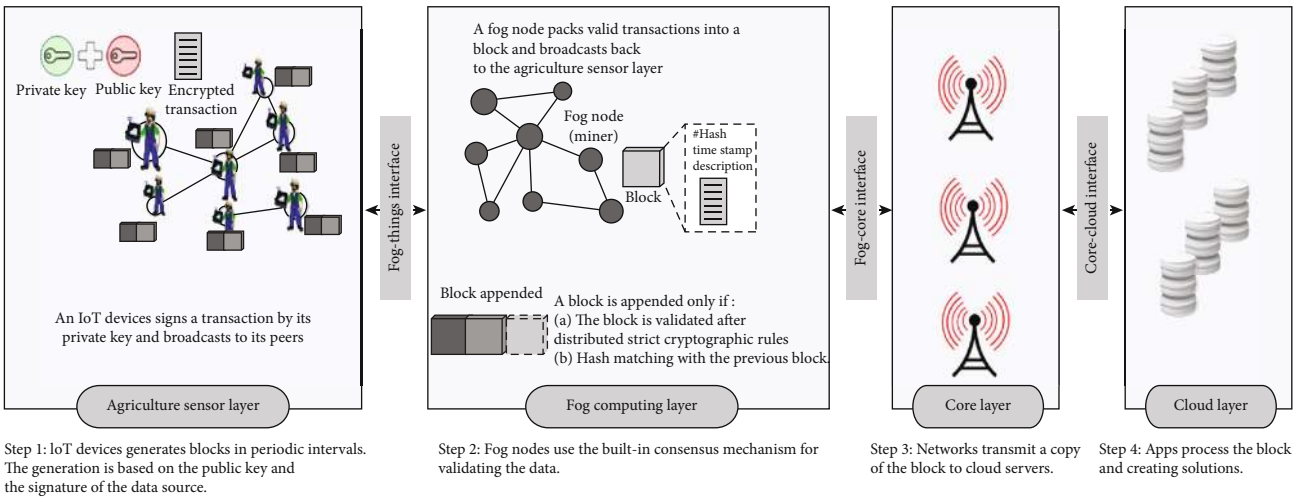

Figure 9: Fog computing architecture proposed by Ferrag et al. [43] for IoT-based agriculture solutions.

blockchain which will execute firmware updates, and the hash of that smart contract would come baked into the IoT devices. These devices can periodically query the contract to check for new firmware updates, then request the current update by its hash, and receive it via a distributed peer-to-peer filesystem [55, 69]. This would greatly improve the security and availability of firmware updates on these devices because even if the manufacturer's node is not available or even if the manufacturer has stopped pushing out that update for the device, because that device is on the blockchain, it can receive the update it needs from other IoT devices on the blockchain.

In [70], the authors introduce a children incentive token system for use in homes. This research provided a framework that parents can use as a source of motivation and a reward system to get their children to do the right thing at home. This system is to run on a private home blockchain. In such a case, the parents would have access to all tokens and then reward a child's home blockchain account with tokens when the child completes a task (such as doing his homework or doing the dishes).

A commercial startup, Slock.it [55], has put out a product that makes use of both smart contracts and cryptocurrencies on the Ethereum blockchain. Slock.it works with smart

electronic locks called "Slocks" that enable anyone to efficiently share property (like renting an apartment) or share items by using their safe deposit boxes. A slock can only be unlocked by a device that has the appropriate token. The owner of the slock can put his car or apartment up for rent (secured by the slock), and any interested party would have to download the slock app and then communicate with the slock via the Whisper peer-to-peer communication protocol [71]. This would unlock the slock, and the owner of the property does not need to be concerned about the tenant or the person who is renting the property defaulting on their payment or running away with their money because the amount for the rent would be automatically charged from that person's Ethereum (cryptocurrency) wallet.

4.4.1. Key Technical Choices to Consider when Choosing a Blockchain Technology for an IoT Application. It is very important for any developer or researcher to understand the underworking of blockchains and how to deploy it for an IoT application. From our findings, we observed that a blockchain implementation may not always be the best for use in an IoT project. It might be better to consider a traditional database or an implementation using Directed Acyclic Graph (DAG) ledgers [72]. Thus, it is necessary to determine if the following features would be required for any project in order to make the correct technical decisions as to whether blockchain should be used or not.

(i) *Peer-to-Peer (P2P) Communication*. In a traditional IoT application architecture, the nodes communicate with gateways that transfer the data from those nodes to a remote server or cloud. Thus, if P2P communication is not a preference and is not essential to the application, then other forms of communication techniques among nodes can be considered

(ii) *Decentralization*. A traditional blockchain demands a high sense of decentralization to ensure trust among participating nodes which usually demands that nodes have a copy of the ledger transactions on the chain [22]. This is something that must be considered due to the low computation power and limited storage of IoT devices

(iii) *Payment System*. Most IoT applications do not require economic transactions between third parties or external entities, but some do. Thus, a blockchain IoT implementation can be strongly considered if a trusted economic transactional channel is needed. The other option exists to integrate traditional payment solutions, but that demands that the banks and financial institutions involved must be trusted

(iv) *Microtransaction Collection*. In [40, 73], a few IoT applications are mentioned that need to record and keep track of each transaction to maintain traceability for auditing purposes or for data mining activities [74, 75]. It is recommended in the plasma whitepaper [76, 77] to make use of sidechains for such a purpose. In cases such as agricultural remote sensing, where communications are done at time intervals, it would be efficient to have a storage facility or a fog computing infrastructure to keep the data from sensors and later make one big transaction to the blockchain at least once a day

If these questions above are answered and you decide to go with a blockchain, then the following must be considered in choosing the best blockchain for the IoT implementation:

(i) Permission design, i.e., whether permission is needed to access the blockchain (see Figure 10). A permissioned blockchain needs some form of authorization before it can be used, whereas permissionless blockchains let anyone participate and read data stored on it

(ii) Choice of consensus algorithm, i.e., how a new block is added to the blockchain

(iii) Whether or not to use smart contract, i.e., whether to use the blockchain as a virtual machine where programs representing business processes are run

(iv) Whether or not to use cryptocurrency, i.e., whether the consensus algorithm and smart contract operations depend on an artificial currency or not

4.4.2. Considerations for IoTs. The type of blockchain used depends on the managed data and on the actions to be performed by a user. In dealing with blockchain, it is easy to see articles and research papers describing a blockchain as public/permissionless and private/permissioned (see Figure 10). As this may be true for cryptocurrencies, it does not necessarily apply the same way when using blockchain in IoT implementations. This is because in dealing with IoT devices you would want to decide what the IoT device can do on the blockchain (permissionless or permissioned) and who can access the data that has been put on the blockchain by that IoT device.

(1) Public vs. Private Blockchains. Public blockchains allow anyone to join without any approval from a governing body or third parties. Once on the blockchain, one is able to act simply as a node or a miner (a validator). Public blockchains usually provide incentives by means of cryptocurrencies to miners (validators), e.g., Bitcoin, Ethereum, and Litecoin [78].

Private blockchains on the other hand are permissioned and require access rights by a governing body or an owner. This leads to the efficient control of who is able to read and see the transactions on the blockchain, perform or execute smart contracts, or act as a miner (validator). Examples of such blockchains are Hyperledger Fabric [36] and Ripple [26]. It is also possible to fork a permissionless blockchain such as Ethereum and build a private permissioned blockchain on it.

Blockchains can also be distinguished based on the token system (Figure 10). Some blockchains make use of tokens like Ripple while some others like Hyperledger Fabric do not.

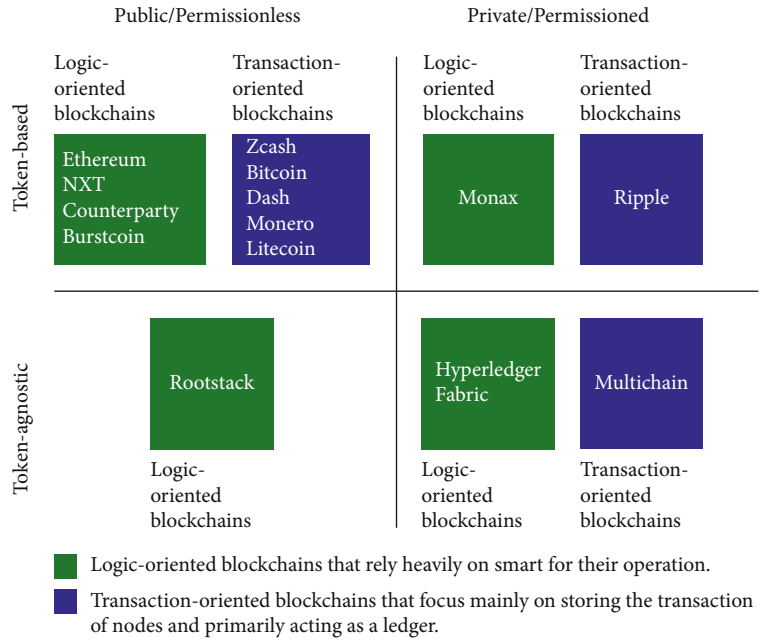

Figure 10: Blockchain taxonomy and practical examples.

These tokens are not necessarily related to cryptocurrencies but can be used as receipts to show that an event has occurred. It can also be used to show the transfer of a digital asset representing a physical asset in the real world (like a diamond—Everledger [79]) from one person to another.

4.5. Cryptographic Algorithms for BIoT Applications. It is worth noting that blockchains have two main cryptographic implementations that support them which are as follows:

(i) Hashing functions

(ii) Public-key cryptography

4.5.1. Public-Key Cryptography. As mentioned earlier, the computational power of IoT devices is limited and IoT devices may have a hard time implementing the standard public-key cryptography that is essentially used to provide security and privacy in blockchain. The Rivest-Shamir-Adleman (RSA) algorithm is a very powerful cryptographic scheme, but the resource allocation, in terms of power needed to implement it, is quite high [33]. IoT devices will be slower at implementing it. It is essential that in choosing a cryptographic algorithm (scheme) for an IoT device, the following should be considered:

(i) *The Computational Load.* It is a well-known fact that the computational processing power that exists on IoT devices is quite limited due to the fact that these devices are usually made to have a smaller form factor. Since IoT devices are made for specific applications and they are usually fitted with application-specific integrated circuits (ASICs) to handle computational tasks, they are not usually intended for general purpose use and applications. Thus, in choosing an algorithm, the computational load that would be exerted on the IoT device should be considered

(ii) *Memory Requirements.* IoT devices do not come premade with a lot of memory. A cryptographic scheme chosen for any BIoT application should be one that has memory requirements that IoT devices are capable of handling

(iii) *Energy Consumed.* Energy and power consumption is directly related to the computational power that is used by IoT devices, and most devices run on batteries. Thus, if a cryptographic scheme with a suitable computational load is chosen for a BIoT application, it would further help reduce energy consumption

(1) Limitations of using RSA for IoT. In the past, there have been different implementations of RSA key sizes. The most common ones being the 768-bit and 1024-bit implementation (which were broken in 2010 [80, 81]) as well as the current standard which is the 2048-bit implementation. In Table 1, we outlined the recommendation that has been made by the Federal Office for Information Security, BSI [83] for asynchronous encryptions schemes from 2020-2022. We envisage that any party interested in the undertaking research regarding the use of RSA in a BIoT implementation should pay close attention to the key length. This is because as the key length increases the computational cost also increases. We suggest the key length should be kept under 2048-bit for IoT devices.

It is possible to use 2048-bit keys and certificates on IoT devices, but then, it comes at the cost of quite a large overhead as well as heavy computational resource requirements. This can be a challenge on IoT resource-constrained devices.

Table 1: Recommended asynchronous encryption schemes and their key lengths (l) recommended for 2020-2022 by BSI [83].

Method	ECIES	DLIES	RSA
l	250	>2000	>2000

An alternative to RSA which has been suggested in literature is the Elliptic Curve Cryptography (ECC) which is lighter and has been proven to perform better in terms of power requirements and speed [83] on low computational power devices. In 2015, the National Security Agency (NSA) gave a recommendation to stop the use of ECC-based cryptographic schemes due to advancements that had been made in the area of quantum cryptography, citing it as a better option [84].

A recent research performed by [83] shows higher security levels and lower power consumption by an ECC-based cryptographic scheme called ECDSA (see Figure 11 and Table 2). It outperformed RSA when the security level was increased. This still needs further research and evaluation.

(2) Hashing Functions. Hash functions play a very vital role in blockchains because they are used to sign transactions. It is important that whatever hash function is used on an IoT device must be fast, lightweight, have low power consumption, and must be secure (in order to prevent collisions).

The popular hash function used in blockchains is KECCAK-256 (used by the Ethereum SHA3 function), SHA-256d (used by Bitcoin), SHA-256 (used by Emercoin), and Scrypt (used by Litecoin). SHA-256 has been tested on a number of IoT devices including wearables [85] even though much older, but newer schemes presented in [86, 87], respectively, suggest that AES should be used for IoT devices due to its low power requirements. In [88], other researchers have suggested ciphers like Simon. A possible consideration that has gained a lot of traction is the BLAKE2x hash function that comes in two flavours (BLAKE2b for 64-bit platforms and BLAKE2s for 8 to 32-bit platforms) [89]. In Figure 12, it was shown to outperform MD5, SHA-1, SHA-2, and SHA-3. The power requirements are still an area open to further research and evaluation.

4.5.2. Consensus Algorithms and Its Effect on IoTs. A consensus is an important part of any blockchain. It is essentially the way nodes in blockchain are able to come to an agreement on what to or what not to accept as a valid transaction on the blockchain. The nodes on a blockchain can be said to have "reached a consensus" when such a decision is made. Since no central authority exists on public blockchains, coupled with its distributed nature, the nodes need a strategy of validating transactions. This is what is referred to as the byzantine generals' problem. The byzantine problem is one that has its roots from the early 1920s. It has come to be known as a computer science description for any occurrence that involves two or more parties that have to agree on an action to be taken to avoid failure but has one or more of the parties involved corrupting and spreading false information [90].

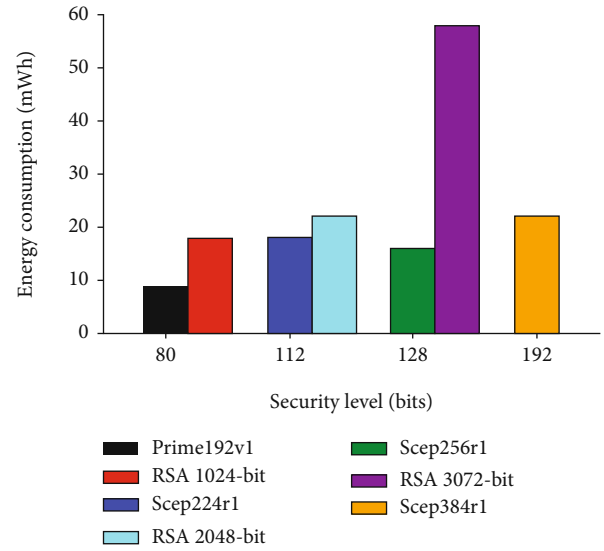

Figure 11: The graph showing the energy consumption of the RSA against ECDSA.

Table 2: The security level and key size and its equivalent ECC curve.

Security level	Symmetric key algorithms	RSA key size	ECC curve
80	2TDEA	1024 bits	prime192v1
112	3TDEA	2048 bits	secp224rl
128	AES-128	3071 bits	scep256r1
192	AES-192	7680 bits	Scep384r1

The ideal way of dealing with a consensus is to give each miner in the blockchain network the same amount of voting rights, and then by counting the majority votes, a decision can be taken on what action to perform. This is a mechanism that is very vulnerable to Sybil attacks; thus, if one user has access to multiple nodes and thus multiple identities, that user will control the chain.

(1) Proof of Work. The most popular consensus algorithm which became well-known with Bitcoin was proof-of-work (PoW). This was an attempt to prevent Sybil attacks by requiring validators to perform a task called mining, thus the term miner. This meant that each miner on the network had to perform a complex mathematical problem which consists of finding a random number which is known as nonce. The result of this operation was to make the SHA-256 hash have a required number of zeros at the start of it. Once this operation is performed in the right manner, it makes it easy for other nodes to verify the obtained results. This had serious drawbacks which were evident in its high-power consumption, low throughput, and scalability [91]. These are issues that are not desirable in any IoT application.

Owing to the problems faced by the proof-of-work algorithm, other methods of consensus have been developed to

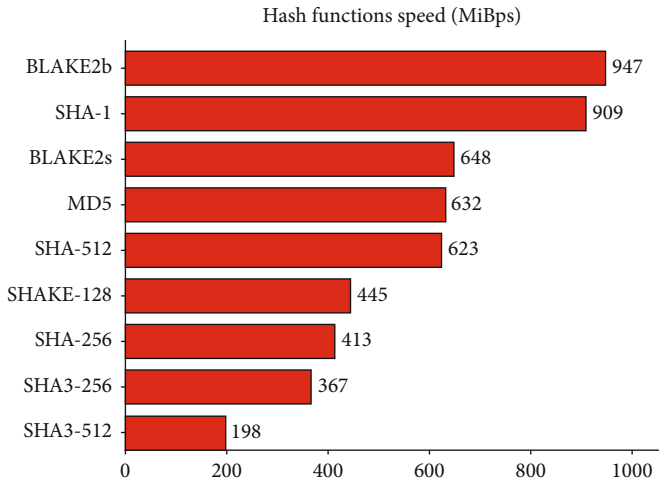

Figure 12: Speed of BLAKE2 hashing function compared to other cryptographic ciphers [90].

help solve the issue. The most promising of these are as follows:

(i) *Proof-of-Stake*. This has been shown to have a lower power consumption rate than PoW. There have been multiple approaches to the PoS strategy. One approach is to view the miners on the network and determine which of them has a high participation rate. This can be proven on a public cryptocurrency blockchain by seeing how much currency a miner has. Based on this, it can be said that that miner is less likely to attack the network; thus, that miner can be allowed to mine more blocks. This has been seen as unfair as the richest miners would control the chain. The other approach taken by Peercoin is to consider the age of the currency of the miner. The older and the more the coins the miner has, the higher the likelihood of the miner to mine a block. This improves throughput very much and scales well

(ii) *Delegated Proof of Stake (DPoS)*. In this scheme, stakeholders and nodes delegate certain miners to validate blocks instead of doing it themselves. This scales very well because there are less nodes involved in the validation process. This process is secured by the fact that, since less nodes are validating transactions, it is easy to identify if a miner or a node behaves dishonestly and a decision can easily be taken to kick that node off the network

(iii) *Proof-of-Activity (PoAC)*. This approach was developed as a build-up on the PoS scheme. A miner may have old coins and might have become passive on the network; thus, the age of the coins as well as its time of activity is checked before that node earns the right to mine a block

(iv) *Practical Byzantine Fault Tolerance (PBFT)*. In [92], the authors describe how this consensus algorithm solves the byzantine generals' problem. PBFT assumes that one 1/3 of the nodes on the network are malicious and thus a leader miner is selected for validating the transaction and 2/3 of all actively known nodes on the network must be in agreement of that leader

(v) *Delegated BFT (DBFT)*. It works in a similar fashion to DPoS. Some particular nodes are selected for mining transactions and if they show any signs of dishonesty, they are kicked out

(vi) *Bitcoin-NG* [93]. This implements a variant of the Bitcoin consensus algorithm which is meant to improve scalability, throughput, and latency

In Table 3, we outlined the various consensus algorithms with their limitation. We also propose ways in which these consensus algorithms can be used in BIoT applications to still make them effective. The list of the consensus algorithms listed in Table 3 is not exhaustive but provides a good means of adaption of the mentioned ones for IoT applications. Researchers should also be looking along the lines of finding effective means of adaption for BIoT applications.

5. Current Challenges Faced in BIoT Applications

There are many benefits of using blockchains in IoT applications, but it also comes with its own set of challenges. IoTs, in recent years, have had emerging advancements in the technologies that power them. These advances have been in the area of communication technologies such as 4G/5G communications [94, 95], Authentication and Security Schemes such as RFID and NFC [9, 96], and Cyber-Physical Systems (CPS) [97, 98]. Adding blockchain to IoT introduces issues that affect scalability, processing power and time, storage, privacy, and the overall throughput of such implementations. BIoT flaws and shortcomings are discussed as in the subsequent subsection.

Table 3: Comparison between the different consensus algorithms and the blockchains that implement them.

Consensus algorithm	Blockchain-based adaptation	Type	Performance	Limitation	Adaptation for IoT
Proof-of-work (PoW)	Bitcoin [21]	Competition consensus	Robust against DDoS and spam attacks Resistance against Sybil attacks	High-power consumption Low throughput and scalability Double spend risk	Access points would serve as miners instead of individual nodes (IoT devices). Thus, taking the computational load of IoT devices
Proof-of-stake (PoS)	Peercoin [99] Nxt [100]	Competition consensus	Difficult and more costly to attack Lower power consumption	Unfair as the richest miners would control the chain	All IoT devices can be selected as validators
Proof-of-activity (PoAC)	Decred [101]	Competition consensus	Enhanced network topology Lower power consumption	Susceptible to double-spend attack	Fog network architecture can be adapted. Each fog layer would have one miner node which creates an empty block header. IoT devices derive N pseudorandom stakeholders using the hash of the block header
Practical Byzantine Fault Tolerance (PBFT)	Ripple [26] Hyperledger Fabric [36] Stellar [102]	Cooperative consensus	(i) Less power consumption (ii) Low variance of the reward	(i) High number of communications between nodes, thus increased number of nodes will result in increased messages sent (ii) Communication overhead increases exponentially when a new node is added	Fog network architecture would be preferred in this case. Communications would take place between fog nodes
Delegated BFT (DBFT)	Neo [103]	Competition consensus	(i) Less power consumption (ii) Low computational power required	(i) Delegated nodes operate under real identities	(i) A voting system should be implemented among nodes with a randomised decision of which node to delegate

Table 4: Blockchain-based machine learning privacy solutions for IoT devices and networks.

Ref.	Attack	Use case	Metric	Algorithm	Blockchain used	Description
Shen et al. [114]	Data privacy (ciphertext model, known as the background model)	Smart cities	Accuracy	SVM (secureSVM)	—	A secure SVM training algorithm in multipart scenarios was created on IoT data. Proof-of-work consensus algorithm was used. Accuracy: 93.89%
Mendis et al. [108]	Data leakage	Multipurpose/general	Accuracy	CNN	Ethereum	Proof-of-stake consensus algorithm used. This research looked at training machine learning models in a distributed fashion on multiple Raspberry Pi 3's.
Arachchige et al. [115]	Data privacy	Industrial IoT		Federated ML	Ethereum	A framework was introduced called PriModChain that prevents leak of sensitive data from IoTs to adversarial networks.

5.1. Privacy. Blockchain anonymity is something that is implied but not assured. This is because devices and users of blockchains are identified by their public key or their hash. Thus, attackers and third parties can study their public keys and hashes and deduce the identities of the nodes or participants [104]. This is a serious concern when it comes to IoT devices because these devices usually store or transmit sensitive and personal information, and once such a trace can be achieved, it puts the devices and their owners at risk [105]. Due to the transparency that public blockchains provide, it makes privacy a challenge. It has been suggested in [106] to use permissioned blockchains instead, for sensitive applications. This would have an identity certification authority allowing users and nodes to participate on the blockchain. We see this as having both pros and cons. The advantage of this would be that a permissioned blockchain with an authority would provide some protection to nodes, but this can also be very dangerous because once an attacker gets hold of the node acting as the certificate authority, the whole system can be compromised. The only solution to this problem is to have a private blockchain that would be properly implemented such that the certificate authority would need to execute a smart contract to add a new node. This must also be followed by a consensus by all nodes for all changes to be effected.

Automatic identity authentication systems for IoT applications are also mentioned in [107], where the researchers presented a blockchain-based system for IoT application that would obtain the IoT device signatures automatically thereby identifying devices and users. There have been some blockchain-based machine learning solutions that have been presented for IoT solutions, and these are listed in Table 4.

Our findings that are listed in Table 4 show the effectiveness of using machine learning-based approaches in privacy solutions. The solution provided by Mendis et al. [108] uses a deep learning approach. This works in a distributed manner so that all the training does not happen on one device (Raspberry Pi). We found no implementation that uses reinforcement learning for such privacy preservation. We envisage that researchers can be looking along these lines as a building block unto the work done in [108]. This is because once the training can be done in a distributed fashion, then it would only be prudent to effectively have an implementation that retrains the produced model in a similar manner.

5.2. Security. For any BIoT system to be considered to be secure, it must meet the following conditions and requirements:

(i) *Integrity*. This is the property of the system that guarantees that once an attacker or unauthorised party gains access to the system and changes or deletes any data, then it should be possible to undo those changes and go back to the previous state of the system. This is essentially one of the areas that the early blockchain concepts frowned upon because one of the main selling points of blockchains is that they are immutable, but that may not be necessary in some cases and in some BIoT implementations. In 2014, an event was reported in [109] where 8 million Vericoins [110] were stolen from the MintPal platform. This prompted the creators of Vericoin to perform a hard fork to help retrieve the stolen coins. Thus, it is known that blockchains are a source of permanent storage but that can be amended in very exceptional cases. In IoT applications, data integrity is an essential aspect to consider if it is being provided by external parties. In [111], the authors proposed a solution to help to eliminate external data integrity providers by making use of blockchain technology for an IoT cloud-based application. To have a robust BIoT implementation, data integrity must be considered

(ii) *Confidentiality*. For IoT applications, it is essential for the data to be protected from unauthorised access by external services and users. This is due to the fact that most of the data that is produced from IoT devices, like wearables and smart home devices, are very sensitive and private to their owners. With regard to the data that is produced and stored in IoT applications, it has been observed over the years that the system architectures and solutions have been built around centralized communications and

Table 5: Literature on different security approaches that have been considered for BIoT applications.

References	Area of study	Research contribution
Ding et al. [116], Ali et al. [117]	Access control	Researchers employed a blockchain-permissioned delegation approach to help control the access of data from IoT devices. This was to help protect the vital information from IoT devices.
Mohanta et al. [118], Huh et al. [119], Xie et al. [120], Maw et al. [121]	Trust assurance	Many IoT applications run on centralized systems where the integrity of the data is provided by third parties. The authors in these papers proposed better trust management processes to help main the integrity of data in BIoT implementations.
Li et al. [22], Biswas et al. [56], Dorri et al. [122]	Scalability	Scalability issues in BIoT applications were tackled by these authors who provided frameworks on how to make them more scalable.
Shen et al. [114], Lv et al. [123], Hassan et al. [124], Sagirlar et al. [125], Xu et al. [2]	Data privacy preservation	The authors in these papers provide blockchain-based encryption techniques to help preserve the privacy of the users and nodes on the blockchain.
Liu and Seo [126], Mohanta et al. [127], Hammi et al. [128], Mohsin et al. [129], Lin et al. [130], Gope et al. [131], Zhang et al. [132], Conti et al. [133]	Authentication	Device authentication is one of the important factors considered in these papers. The authors used different approaches to tackle the authentication issue from RFID-based authentication schemes, delegated authentication schemes, PSO-AES, mutual authentication, and distributed authentication for IoT implementations.
Si et al. [134], Li et al. [135], Roy et al. [136], Danzi et al. [137], Pan et al. [138], Zhou et al. [139], Yang et al. [140], Li et al. [141]	Information exchange	The authors in these papers discussed and proposed blockchain-based information exchange as part of IoT application implementations.

solutions, such as physical servers, server farms, or centralized cloud solutions. These infrastructures and architectures are good for the job, if they can be trusted and can withstand attacks [112, 113]. If centralized systems cannot be trusted, then blockchains offer a decentralized system or approach that incorporates many nodes, that means no down times, and if one node is comprised, the others can keep the system running efficiently

(iii) *Availability*. This is an aspect of information systems that looks at the data on the system being available whenever needed. Blockchains by design are made to be distributed and decentralized. Thus, data can be made available even if one node is down or under attack. As noted earlier from [22], the 51-percent attack is one of the many means by which a full-replicated blockchain can be put under attack. This attack implies that one miner (attacker) has control of 51-percent of the nodes on the chain and thus can block the availability of the chain to process new transactions

Multiple approaches have been considered for ensuring security for BIoT applications. Some have used machine learning approaches, and others have gone with more conventional approaches. These can be seen in Table 5. Our findings brought to light different ways in which security has been ensured in some BIoT implementations. Some of these approaches used schemes such as access control, trust assurance, and even authentication. We found the literature concerning the maintenance of security while improving the scalability of the blockchain to be very interesting and an area that still demands more research. The papers outlined look into the implications of making BIoT solutions more scalable while maintaining a high standard of security. Once a BIoT application is made more scalable, it is usually done at the expense of an aspect of the blockchain which in turn can cause security vulnerabilities.

5.3. Scalability, Throughput, and Latency. Scalability is a major issue that has plagued blockchains over the years of the technology's existence. This is a problem caused by many factors such as the high level of cryptography that is used and the consensus algorithms used (which usually require high computational power). This is an aspect that is of concern when considering BIoT implementation due to the limited resources that exist on these IoT devices.

All of this goes to affect the throughput of blockchain networks as we know it. Despite its enhanced security features, the number of transactions that can be carried on a blockchain has been a thing of concern for people who want to use blockchains for main stream implementations and applications. IoT solutions require that a large amount of transactions be executed at every given time, but some blockchain networks such as Bitcoin are only capable of performing 7 transactions per second [21]. Improvements have been presented by researchers in [22, 142], where the throughput was said to have increased when larger blocks were

Table 6: Taxonomy of blockchain scalability solutions and how they impact blockchain.

Proposed technology	References	Claimed TPS	Layer	Category	Notes
Plasma	Poon and Buterin [76]	5000	Layer 2	Side chain	Side chain is created for faster transactions. Only completed and validated blocks from the side chain are added on to the main chain.
Sharding	Li et al. [22], Klarman et al. [143], Zamani et al. [144], Kokoris-Kogias et al. [145], Luu et al. [146]	45000	Layer 1	On-chain	Partition blockchain into K-independent subchains to have smaller full replication systems for faster transactions.
Raiden red eyes	[147]	1000000	Layer 2	Payment channel	Payment solution that allows one to run smart contracts off-chain.
Lightning network	Poon and Dryja [142]	1000000	Layer 2	Payment channel	Solution uses cross-chain atomic swabs and has been tested on the bitcoin blockchain.
Jidar	Dai et al. [148]	—	Layer 1	Block data (data storage size reduction)	A data reduction approach for Bitcoin system. The main idea of Jidar is to allow users only to store relevant data they are interested in and thus release the storage pressure of each node.
Erlay	Naumenko et al. [149]	—	Layer 0	Data propagation (bandwidth savings)	Reduce the overall bandwidth consumption while increasing the propagation latency.
bloXroute	Klarman et al. [143]	200000	Layer-0	Data propagation	Helps individual nodes to propagate transactions and blocks more quickly.

processed, other than the 1 MB block size limit usually given on blockchains such as Bitcoin, or by modifying how nodes accept and process transactions.

Latency in blockchains has also being proven to be high. For example, Bitcoin takes almost 10 minutes to complete a transaction. The issue of latency is caused by the type of consensus algorithm that is chosen for a particular blockchain. The more complex the consensus process, the more time is needed to process the transaction. The hashing algorithm used on blockchains also adds more time unto the time taken for transactions. Litecoin [78] uses a blockchain that uses Scrypt instead of SHA-256 which is relatively faster. An adopted taxonomy, summarized in Table 6, has been used to differentiate the various technologies.

5.4. Computation, Processing, Blockchain Size, Bandwidth, and Infrastructure. There is quite a high cost in maintaining blockchain networks across a vast number of nodes (peers). These costs stem from the computational power, energy, storage, and memory that is needed to participate in a blockchain network [56, 150]. In [150], the blockchain ledger was almost 196 GB in 2018 and this has since increased to 306.86 GB as at May 2020. This is a serious concern for IoT solutions. This limitation accounts for the reason why most IoT devices would have poor transaction times and poor scalability. There have been proposed solutions by researchers to offload the computational tasks for these IoT devices to centralized servers (or cloud servers) or a fog server, but these were seen to cause network latencies [51, 150].

6. Future Directions and Recommendations

In light of the advancement that has been made in past years in BIoT implementation and solutions, there are still some areas that need further consideration. To further enhance BIoT applications and solutions, further research and investigation must take place in some areas to make deployments safe, secure, and scalable. These areas include the following:

(i) *Machine Learning-Based Solutions for Privacy and Security of BIoT Applications.* Some machine learning implementations for BIoT privacy and security have already been discussed in this paper, but it would be insightful to try out other machine learning algorithms such as K-NN and other deep learning and clustering techniques to perform better intrusion detection and privacy preservation

(ii) *Technical Challenges with Decentralization.* Due to issues in scalability, security, and privacy, most of the BIoT applications that have been proposed so far had to add some form of centralization to the blockchain. Investigations and research must be carried out that would help to reduce the tendency for centralization and move in the direction of truly decentralized architectures that are scalable for BIoT applications

(iii) *Blockchain Infrastructure.* Trust is an essential part of using IoTs on blockchains; thus, it is essential to have a blockchain system that truly solves the issue of trust in BIoT implementations, since IoT devices produce very sensitive data. Many approaches have been given to this issue, but they mostly depend on interdomain policies and control systems. We need more research into this area that is devoid of this

(iv) *Governance, Regulations, and Legal Aspects.* The blockchain world, due to its high level of

Table 7: Cross-cutting analysis of surveys and related work on blockchain and IoT.

Ref.	Blockchain	IoT security	IoT privacy	Deep learning-based BIoT privacy
Restuccia et al. [151]	✗	✓	✗	✗
Reyna et al. [51]	✓	✓	✗	✗
Xin et al. [152]	✗	✓	✗	✗
Khan and Salah [18]	✓	✓	✗	✗
Al-Rubaie and Chang [153]	✗	✗	✓	✗
Aich et al. [7]	✓	✗	✗	✗
Hussain et al. [19]	✗	✓	✓	✓
Alam and Benaida [154]	✓	✗	✗	✗
Ferrag et al. [43]	✓	✓	✓	✗
This review	✓	✓	✓	✓

decentralization, is seen by many as "no-man's land." There are no major regulations and legal aspects that bind the use of blockchains and their implementation. IoT being added to a system that lacks this form of governance can be very dangerous. We are not suggesting that blockchains should have centralized authorities entirely, but there should be at least guidelines to follow to implement solutions and applications that would involve IoTs

7. Contribution

We live in a data-driven world that is advancing speedily in technology. These technological advancements have been spearheaded by the widespread usage of the internet and the increase in research and investigation into societal problems and challenges. A lot of brilliant proposals and implementations have been realized over the years and among those is IoT. A lot can be done with IoT on its own, but blockchain serves to bring a more robust, secure and distributed structure to IoT implementations that defy centralized and noncollaborative organizational structures.

This review examined the state-of-the-art in the BIoT world and looked at the advancements that have been made in research and in the industry. The review had the focus to examine BIoT applications and their challenges. We looked at implementations and proposed solutions in wearables [65, 66], healthcare [3], agriculture, and smart cities [68, 114]. The work dived deep into the technical and technological aspects to show the similarities between all BIoT applications. This is to say that the implementation details, infrastructure, and architectural details outlined in this review, if followed, can be applied to any BIoT solution especially in the food sector. It was also clearly brought to light that there are specific technical requirements that are needed for BIoT applications that differ significantly from using blockchains as just cryptocurrency solutions. The resource limitations of IoT devices were clearly outlined, and proposals were made to show how they can be used in such cases. A hybrid BIoT integration scheme was proposed in this paper that made use of microservices. This proposed scheme is one that would definitely help to improve the scalability of a BIoT application if implemented.

The aim of the research was also to look into the limitations of current BIoT applications and suggest areas of research that still need to be worked on. This was achieved by taking a deep dive into the consensus algorithms, cryptographic algorithms, and the security and privacy aspects. These are of serious concern to BIoT implementations due to the sensitive data that is produced or transmitted by IoT devices. Further information was also provided for developers and researches on the areas that need attention if they plan to deploy and roll out BIoT solutions.

Machine learning and artificial intelligence are aspects that are greatly important for the optimization and efficiency of BIoT applications. The aspect of machine learning with regard to the security and privacy of BIoT solutions was also closely studied, and suggestions for future implementations in that area were provided.

There have a number of reviews and literature on BIoTs, but none of them have considered using deep learning approaches for privacy protection. Restuccia et al. in [151] reviewed papers on IoT security based on a combination of well-known notions in network security like software-defined networking, security-by-design, and polymorphism. The concept of blockchain described in this paper looked at blockchain as a double-edged sword for IoT devices. It considered blockchain as a tool to ensure IoT security by using its enhanced cryptographic properties and in turn considered the high level of automation provided by IoT devices to help to ensure the credibility of data that is put on blockchains since data is almost persistent on a blockchain. This paper also considered machine learning approaches to ensure the security of IoT devices on a network.

Reyna et al. in [51] looked at the feasibility of using IoT devices as BIoT nodes. Experiments were performed using a Raspberry Pi v3 with different blockchains to evaluate IoT-based blockchain nodes and the limitations that the IoT devices will face. The authors thoroughly looked at the issue of legislation and regulations that have to be implemented to ensure that businesses, companies, and governments have confidence in both technologies so as to adopt them for use. Aich et al. in their conference paper [7] focused on the use of blockchain in supply chains across different industries such as the automotive, pharmaceutical, food industry, and the retail sector. The authors provided a clear

understanding of the blockchain technology with the purpose of helping people across different sectors to see the benefits for their industries. Hussain et al. in [19] reviewed the current security solutions that exist for IoT networks. The authors also looked into the security requirements and the most potent attack vectors of IoT devices on networks. They discussed existing machine learning and deep learning solutions for addressing security problems in IoT networks.

This literature on the other hand considers the blockchain technology and its integration into IoT networks as well as the key technical choices that are needed to ensure the success of any BIoT project. This paper also looks into deep learning and federated learning approaches to address the privacy issues in BIoT networks. Table 7 summarizes the focus of our contribution.

8. Conclusion

We conclude that IoT, as we know it, has come to stay and BIoT implementations would soon become widespread, but we want to make it known that there is no one-size-fits-all answer for BIoT applications in terms of architectural choices and network structure. The technology is still maturing, and we can boldly say that this will give more room in the future for the development of some applications that would disrupt industries and businesses. But in moving forward, we foresee that the broader use of this technology will require the collaboration and cooperation of stakeholders, governments, and other technological institutions and unions to be able to provide the right governance, organizational structure, and regulatory and legal aspects to be able to truly harness the power of BIoT applications and avoid misuse.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] "BitShares 4.0 | OSS Solutions for finance and business management based on blockchain technology," June 2020, https://bitshares.org/.

[2] J. Xu, K. Xue, S. Li et al., "Healthchain: a blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[3] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, pp. 1–10, 2020.

[4] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2040–2050, 2021.

[5] L. Ge, C. Brewster, J. Spek, A. Smeenk, and J. Top, *Blockchain for agriculture and food (findings from the pilot study)*, Wageningen Economic Research, 2017.

[6] J.-H. Huh and S.-K. Kim, "Verification plan using neural algorithm blockchain smart contract for secure P2P real estate transactions," *Electronics*, vol. 9, no. 6, article 1052, 2020.

[7] S. Aich, S. Chakraborty, M. Sain, H. 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 *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 138–141, PyeongChang, Korea (South), 2019.

[8] M. Queiroz, R. Telles, and S. Bonilla, "Blockchain and supply chain management integration: a systematic review of the literature," *Supply Chain Management Intenational Journal*, vol. 25, no. 2, pp. 241–254, 2019.

[9] F. Tian, "An agri-food supply chain traceability system for China based on RFID & Blockchain technology," in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, Kunming, China, June 2016.

[10] N. Ahmed, D. De, and I. Hussain, "Internet of things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[11] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[12] H. Nguyen-An, T. Silverston, T. Yamazaki, and T. Miyoshi, "Generating IoT traffic in smart home environment," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2020.

[13] P. F.-L. M. Suárez-Albela, T. Fernández-Caramés, and L. A. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, article 1978, 2017.

[14] L. Celic and R. Magjarevic, "Seamless connectivity architecture and methods for IoT and wearable devices," *Automatika*, vol. 61, no. 1, pp. 21–34, 2020.

[15] P. F.-L. Ó. Blanco-Novoa, T. FernáNdez-Caramés, and M. Vilar-Montesinos, "A practical evaluation of commercial industrial augmented reality systems in an Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 8201–8218, 2018.

[16] Ó. B.-N. P. Fraga-Lamas, T. FernáNdez-Caramés, and M. Vilar-Montesinos, "A review on industrial augmented reality systems for the Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.

[17] M. Hammoudeh, G. Epiphaniou, S. Belguith et al., "A service-oriented approach for sensing in the internet of things: intelligent transportation systems and privacy use cases," *IEEE Sensors Journal*, p. 1, 2020.

[18] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[19] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[20] P. Danzi, A. E. Kalor, R. B. Sorensen et al., "Communication aspects of the integration of wireless IoT devices with distributed ledger technology," *IEEE Network*, vol. 34, no. 1, pp. 47–53, 2020.

[21] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin*, https://bitcoin.org/bitcoin.pdf.

[22] S. Li, M. Yu, C. Yang, A. S. Avestimehr, S. Kannan, and P. Viswanath, *PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously*, Cornell University, 2020.

[23] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[24] Statista, *Size of the blockchain technology market worldwide from 2018 to 2025, Statista*, https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/.

[25] V. Buterin, "Ethereum Whitepaper," *Ethereum*, https://ethereum.org/whitepaper/.

[26] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," *Ripple*, https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[27] J. Palmer and S. Nakamoto, "Dogecoin," *The Dogecoin Project*, https://dogecoin.com.

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

[29] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: a literature review," in *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, Ohrid, Macedonia, 2017.

[30] J. Al-Jaroodi and N. Mohamed, "Industrial applications of blockchain," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2019.

[31] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 99–114, 2020.

[32] T. Alam, "Blockchain and its role in the internet of things (IoT)," *SSRN Electronic Journal*, 2019.

[33] N. Tahat, A. A. Tahat, M. Abu-Dalu, B. R. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimeh, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical and Computer Engineering*, vol. 10, pp. 1430–1437, 2020.

[34] S. Srilaya and S. Velampalli, "Cryptography: the key technology for security management," *International Journal of Research and Analytical Reviews*, vol. 7, no. 1, 2020.

[35] A. Tar, "Smart Contracts, Explained," *Cointelegraph*, 2017, https://cointelegraph.com/explained/smart-contracts-explained.

[36] L. Community, "HyperLedger Fabric White Paper," *Linux Foundation*, 2018, https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf.

[37] M. Castillo, *Walmart Blockchain Pilot Aims to Make China's Pork Market Safer - CoinDesk*, CoinDesk, 2016, http://www.coindesk.com/walmart-blockchain-pilot-china-pork-market/.

[38] S. Higgins, *Walmart: Blockchain Food Tracking Test Results Are 'Very Encouraging' - CoinDesk*, CoinDesk, 2017, http://www.coindesk.com/walmart-blockchain-food-tracking.

[39] "Go Ethereum," August 2020, https://geth.ethereum.org/.

[40] Z. Wu, Z. Meng, and J. Gray, "IoT-based techniques for online M2M-interactive itemized data registration and offline information traceability in a digital manufacturing system," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2397–2405, 2017.

[41] E. Olakunle, T. A. Rahman, I. Orikumhi, C. Y. Leow, and N. M. H. D. Hindia, "An overview of internet of things (IoT) and data analytics in agriculture: benefits and challenges," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.

[42] L. J. Klein, H. F. Hamann, N. Hinds et al., "Closed loop controlled precision irrigation sensor network," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4580–4588, 2018.

[43] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[44] P. Abouzar, D. G. Michelson, and M. Hamdi, "RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6638–6650, 2016.

[45] M. A. Zamora-Izquierdo, J. Santa, J. A. Martínez, V. Martínez, and A. F. Skarmeta, "Smart farming IoT platform based on edge and cloud computing," *Biosystems Engineering*, vol. 177, pp. 4–17, 2019.

[46] A. Chalimov, "IoT in Agriculture: 8 Technology Use Cases for Smart Farming (and Challenges to Consider)," 2020, https://easternpeak.com/blog/iot-in-agriculture-5-technology-use-cases-for-smart-farming-and-4-challenges-to-consider/.

[47] "GrainMate GM-101 grain moisture meter," *Sesi Technologies*, June 2020, https://sesitechnologies.com/grainmate-gm-101-grain-moisture-meter-2/.

[48] M. Goudarzi, H. Wu, M. S. Palaniswami, and R. Buyya, "An application placement technique for concurrent IoT applications in edge and fog computing environments," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[49] T. Alam, "IoT-fog: a communication framework using blockchain in the internet of things," *International Journal of Recent Technology and Engineering*, vol. 7, 2019.

[50] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[51] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[52] M. M. Othman and A. El-Mousa, "Internet of things cloud computing internet of things as a service approach," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, pp. 318–323, Irbid, Jordan, 2020.

[53] M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges," *Computers and Electronics in Agriculture*, vol. 178, article 105476, 2020.

[54] H. Zahmatkesh and F. Al-Turjman, "Fog computing for sustainable smart cities in the IoT era: caching techniques and enabling technologies - an overview," *Sustainable Cities and Society*, vol. 59, article 102139, 2020.

[55] Slock it, "Slock.it website," June 2020, https://slock.it/.

[56] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, 2019.

[57] X. Liu, J. Yu, J. Wang, and Y. Gao, "Resource allocation with edge computing in IoT networks via machine learning," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3415–3426, 2020.

[58] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved, "BlendMAS: a blockchain-enabled decentralized microservices

architecture for smart public safety," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 564–571, Atlanta, GA, USA, 2019.

[59] S. Li, H. Zhang, Z. Jia et al., "Understanding and addressing quality attributes of microservices architecture: a systematic literature review," *Information and Software Technology*, vol. 131, article 106449, 2020.

[60] R. Liu, Z. Weng, S. Hao, D. Chang, C. Bao, and X. Li, "Addressless: enhancing IoT server security using IPv6," *IEEE Access*, vol. 8, pp. 90294–90315, 2020.

[61] "The case for IPv6 as an enabler of the internet of things - IEEE internet of things," November 2020, https://iot.ieee.org/newsletter/july-2015/the-case-for-ipv6-as-an-enabler-of-the-internet-of-things.html.

[62] "Internet assigned numbers authority," November 2020, https://www.iana.org/.

[63] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[64] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Applied Sciences*, vol. 10, no. 2, p. 488, 2020.

[65] M. Siddiqi, S. T. All, and V. Sivaraman, "Secure lightweight context-driven data logging for bodyworn sensing devices," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1–6, Tirgu Mures, Romania, 2017.

[66] X. Qian, H. Chen, H. Jiang, J. Green, H. Cheng, and M.-C. Huang, "Wearable computing with distributed deep learning hierarchy: a study of fall detection," *IEEE Sensors Journal*, vol. 20, no. 16, pp. 9408–9416, 2020.

[67] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, pp. 902–911, 2020.

[68] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: architecture, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 8–14, 2020.

[69] C. Karapapas, I. Pittaras, N. Fotiou, and G. C. Polyzos, "Ransomware as a service using smart contracts and IPFS," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–5, Toronto, ON, Canada, May 2020.

[70] S. A. Suchaad, K. Mashiko, N. B. Ismail, and M. H. Z. Abidin, "Blockchain use in home automation for children incentives in parental control," in *Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence - MLMI2018*, pp. 50–53, Ha Noi, Viet Nam, 2018.

[71] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "PSTRM: privacy-aware sociopsychological trust and reputation model for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1505–1525, 2020.

[72] H. Hashgraph, "Hedera Hashgraph Whitepaper," *Hedera Hashgraph*, 2019, https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf.

[73] P. Parthasarthy and S. Vivekanandan, "A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm," *International Journal of Computers and Applications*, pp. 222–333, 2018.

[74] M. Anbarasana, K. O. Boateng, and J. D. Gadze, "Detection of flood disaster system based on IoT, big data and convolutional deep neural network," *Computer Communications*, vol. 150, pp. 150–157, 2020.

[75] H. Cai, B. Xu, L. Jiang, and A. Vasilakos, "IoT-based big data storage systems in cloud computing: perspectives and challenges," *IEEE Internet Things Journal*, vol. 4, no. 1, pp. 75–87, 2017.

[76] J. Poon and V. Buterin, "Plasma: scalable autonomous smart contracts," 2017, http://plasma.io/.

[77] A. Back, M. Corallo, L. Dashjr et al., *Enabling blockchain innovations with pegged sidechains*, 2014, http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.

[78] "Litecoin - open source P2P digital currency," June 2020, https://litecoin.org/.

[79] Everledger, *Everledger Website*, 2020, https://www.everledger.io/.

[80] T. Kleinjung, K. Aoki, J. Franke et al., "Factorization of a 768-bit RSA modulus," in *Advances in Cryptology*, pp. 333–350, Springer Berlin Heidelberg, 2010.

[81] A. Pellegrini, V. Bertacco, and T. Austin, "Fault-based attack of RSA authentication," in *2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010)*, pp. 855–860, Dresden, Germany, 2010.

[82] BSI, *Cryptographic Mechanisms: Recommendations and Key Lengths*, Technical Guideline, 2020.

[83] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical performance comparison of ECC and RSA for resource-constrained IoT devices,," in *2018 Global Internet of Things Summit (GIoTS)*, pp. 1–6, Bilbao, Spain, 2018.

[84] N. Koblitz and A. Menezes, "A riddle wrapped in an enigma," *IEEE Security Privacy*, vol. 14, no. 6, pp. 34–42, 2016.

[85] W. Y. Bin Saleem, H. Ali, and N. AlSalloom, "A framework for securing EHR management in the era of internet of things," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–5, Riyadh, Saudi Arabia, 2020.

[86] L. Fu, X. Shen, L. Zhu, and J. Wang, "A low-cost UHF RFID tag chip with AES cryptography engine," *Security and Communication Networks*, vol. 7, no. 2, pp. 365–375, 2014.

[87] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[88] R. Anand, A. Maitra, and S. Mukhopadhyay, "Grover on *SIMON*," *Quantum Information Processing*, vol. 19, no. 9, article 340, 2020.

[89] "BLAKE2," June 2020, https://blake2.net/.

[90] O. Alfandi, S. Otoum, and Y. Jararweh, "Blockchain solution for IoT-based critical infrastructures: Byzantine fault tolerance," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–4, Budapest, Hungary, 2020.

[91] D. J. Moroz, D. J. Aronoff, N. Narula, and D. C. Parkes, "Double-spend counter-attacks: threat of retaliation in proof-of-work systems," *Cryptoeconomic Systems*, vol. 1, no. 1, 2020, https://cryptoeconomicsystems.pubpub.org/pub/cb2oh2jw/release/3.

[92] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operat. Syst. Design Implement*, pp. 1–14, New Orleans, LA, USA, 1999.

[93] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: a scalable blockchain protocol," in *13th USENIX*

Symposium on Networked Systems Design and Implementation (NSDI 16), pp. 45–59, Santa Clara, CA, 2016, https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal.

[94] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60–67, 2018.

[95] N. Kumar and R. Khanna, "A compact multi-band multi-input multi-output antenna for 4G/5G and IoT devices using theory of characteristic modes," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 30, no. 1, article e22012, 2020.

[96] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for internet of things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.

[97] P. Fraga-Lamas, T. M. Fernández-Caramés, D. Noceda-Davila, and M. Vilar-Montesinos, "RSS stabilization techniques for a real-time passive UHF RFID pipe monitoring system for smart shipyards," in *2017 IEEE International Conference on RFID (RFID)*, pp. 161–166, Phoenix, AZ, USA, May 2017.

[98] P. Fraga-Lamas, "Enabling automatic event detection for the pipe workshop of the shipyard 4.0," in *2017 56th FITCE Congress*, pp. 20–27, Madrid, Spain, 2017.

[99] S. King and S. Nadal, "PPCoin: peer-to-peer crypto-currency with proof-of-stake," *Chain Extranet*, https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf.

[100] "Nxt Whitepaper - Introduction: Nxt Whitepaper," June 2020, https://nxtdocs.jelurida.com/Nxt_Whitepaper.

[101] "Decred documentation," June 2020, https://docs.decred.org/.

[102] "Stellar Consensus Protocol - Stellar," June 2020, https://www.stellar.org/papers/stellar-consensus-protocol?locale=en.

[103] neo-project, "Neo documentation," June 2020, https://docs.neo.org/docs/en-us/basic/whitepaper.html.

[104] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[105] J. Angwin, *Own a Vizio Smart TV? It's Watching You*ProPublicaJune 2020, https://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you?token=Gg58888u2U5db3W3CsuKrD0LD_VQJReQ.

[106] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *2017 Global Internet of Things Summit (GIoTS)*, pp. 1–6, Geneva, Switzerland, 2017.

[107] N. Shi, L. Tan, C. Yang et al., "BacS: a blockchain-based access control scheme in distributed internet of things," *Peer-to-Peer Networking and Applications*, vol. 13, 2020.

[108] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, and R. Roche, "Blockchain as a service: a decentralized and secure computing paradigm," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2020.

[109] "8 Million Vericoin hack prompts hard fork to recover funds," *CoinDesk*, 2014, June 2020, https://www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach.

[110] Vericoin, *VeriCoin & Verium - Official Site | Home*June 2020, https://vericoin.info/.

[111] G. Dong and X. Wang, "A secure IoT data integrity auditing scheme based on consortium blockchain," in *2020 5th IEEE International Conference on Big Data Analytics (ICBDA)*, pp. 246–250, Xiamen, China, 2020.

[112] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Pyeong-Chang, Korea (South), 2016.

[113] A. O. F. Atya, Z. Qian, S. V. Krishnamurthy, T. L. Porta, P. McDaniel, and L. Marvel, "Malicious co-residency on the cloud: attacks and defense," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.

[114] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[115] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[116] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[117] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in internet of things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, 2019.

[118] B. K. Mohanta, S. S. Panda, U. Satapathy, D. Jena, and D. Gountia, "Trustworthy management in decentralized IoT application using blockchain," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–5, Kanpur, India, 2019.

[119] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 464–467, PyeongChang, Korea (South), 2017.

[120] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[121] A. Maw, S. Adepu, and A. Mathur, "ICS-BlockOpS: blockchain for operational data security in industrial control system," *Pervasive and Mobile Computing*, vol. 59, article 101048, 2019.

[122] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: a lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[123] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IOT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, 2019.

[124] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[125] G. Sagirlar, B. Carminati, and E. Ferrari, "Decentralizing privacy enforcement for internet of things smart objects," *Computer Networks*, vol. 143, pp. 112–125, 2018.

[126] Z. Liu and H. Seo, "IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms," *IEEE Transactions*

on Information Forensics and Security, vol. 14, no. 3, pp. 720–729, 2018.

[127] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena, and D. Gountia, "Decauth: decentralized authentication scheme for IoT device using Ethereum blockchain," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, pp. 558–563, Kochi, India, 2019.

[128] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: a decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[129] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan et al., "Based blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication," *Computer Standards & Interfaces*, vol. 66, article 103343, 2019.

[130] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018.

[131] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, vol. 83, pp. 629–637, 2018.

[132] X. Zhang, C. Liu, S. Poslad, and K. K. Chai, "A provable semi-outsourcing privacy preserving scheme for data transmission from IoT devices," *IEEE Access*, vol. 7, pp. 87169–87177, 2019.

[133] M. Conti, M. Hassan, and C. Lal, "BlockAuth: blockchain based distributed producer authentication in ICN," *Computer Networks*, vol. 164, article 106888, 2019.

[134] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[135] Z. Li, L. Liu, A. V. Barenji, and W. Wang, "Cloud-based manufacturing blockchain: secure knowledge sharing for injection mould redesign," *Procedia CIRP*, vol. 72, pp. 961–966, 2018.

[136] D. G. Roy, P. Das, D. De, and R. Buyya, "QoS-aware secure transaction framework for internet of things using blockchain mechanism," *Journal of Network and Computer Applications*, vol. 144, pp. 59–78, 2019.

[137] P. Danzi, A. E. Kalør, C. Stefanovic, and P. Popovski, "Delay and communication tradeoffs for blockchain systems with lightweight IoT clients," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2354–2365, 2019.

[138] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, 2018.

[139] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: a blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[140] J. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *Journal of Systems Architecture*, vol. 87, pp. 36–48, 2018.

[141] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 4719–4732, 2018.

[142] J. Poon and T. Dryja, "The Bitcoin lightning network," *BitcoinLightning.com*, 59, https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf.

[143] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "bloXroute: a scalable trustless blockchain distribution network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur*, p. 15, Toronto, Canada, 2019.

[144] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 931–948, Toronto, Canada, 2018.

[145] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: a secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 583–598, San Francisco, CA, USA, 2018.

[146] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–30, Vienna, Austria, 2016.

[147] "Raiden network," June 2020, https://raiden.network/.

[148] X. Dai, J. Xiao, W. Yang, C. Wang, and H. Jin, "Jidar: a jigsaw-like data reduction approach without trust assumptions for Bitcoin System," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1317–1326, Dallas, TX, USA, 2019.

[149] G. Naumenko, G. Maxwell, P. Wuille, A. Fedorova, and I. Beschastnikh, "Erlay: efficient transaction relay for Bitcoin," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 817–831, London, UK, 2019.

[150] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, pp. 169–174, Paris, France, 2018.

[151] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[152] Y. Xin, L. Kong, Z. Liu et al., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[153] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: threats and solutions," *IEEE Security Privacy*, vol. 17, no. 2, pp. 49–58, 2019.

[154] T. Alam and M. Benaida, "Blockchain, fog and IoT integrated framework: review, architecture and evaluation," *Technology Reports of Kansai University*, 2020.