IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 11, 2018, accepted May 29, 2018, date of publication May 31, 2018, date of current version July 6, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2842685

A Review on the Use of Blockchain for the Internet of Things

TIAGO M. FERNÁNDEZ-CARAMÉS, (Senior Member, IEEE), and PAULA FRAGA-LAMAS, (Member, IEEE)

Department of Computer Engineering, Faculty of Computer Science, Campus de Elviña, s/n, Universidade da Coruña, 15071 A Coruña, Spain

Corresponding authors: Tiago M. Fernández-Caramés (tiago.fernandez@udc.es) and Paula Fraga-Lamas (paula.fraga@udc.es)

This work was supported in part by the Xunta de Galicia under Grant ED431C 2016-045, Grant ED341D R2016/012, and Grant ED431G/01, in part by the Agencia Estatal de Investigación of Spain under Grant TEC2015-69648-REDC and Grant TEC2016-75067-C4-1-R, and in part by ERDF funds of EU under Grant AEI/FEDER, UE. The work of P. Fraga-Lamas was supported in part by BBVA and the BritishSpanish Society Grant.

ABSTRACT The paradigm of Internet of Things (IoT) is paving the way for a world, where many of our daily objects will be interconnected and will interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment, and self-maintenance. Such features can be brought by blockchain, a technology born with a cryptocurrency called Bitcoin. In this paper, a thorough review on how to adapt blockchain to the specific needs of IoT in order to develop Blockchain-based IoT (BIoT) applications is presented. After describing the basics of blockchain, the most relevant BIoT applications are described with the objective of emphasizing how blockchain can impact traditional cloud-centered IoT applications. Then, the current challenges and possible optimizations are detailed regarding many aspects that affect the design, development, and deployment of a BIoT application. Finally, some recommendations are enumerated with the aim of guiding future BIoT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BIoT applications.

INDEX TERMS IoT, blockchain, traceability, consensus, distributed systems, BIoT, fog computing, edge computing.

I. INTRODUCTION

The Internet of Things (IoT) is expanding at a fast pace and some reports [1] predict that IoT devices will grow to 26 billions by 2020, which are 30 times the estimated number of devices deployed in 2009 and is far more than the 7.3 billion smartphones, tablets and PCs that are expected to be in use by 2020. Moreover, some forecasts [2] anticipate a fourfold growth in Machine-to-Machine (M2M) connections in the next years (from 780 million in 2016 to 3.3 billion by 2021), which may be related to a broad spectrum of applications like home automation [3], transportation [4], defense and public safety [5], wearables [6] or augmented reality [7], [8].

In order to reach such a huge growth, it is necessary to build an IoT stack, standardize protocols and create the proper layers for an architecture that will provide services to IoT devices. Currently, most IoT solutions rely on the centralized server-client paradigm, connecting to cloud servers through the Internet. Although this solution may work properly nowadays, the expected growth suggests that new paradigms will have to be proposed. Among such proposals, decentralized architectures were suggested in the past to create large Peer-to-Peer (P2P) Wireless Sensor Networks (WSNs) [9]–[11], but some pieces were missing in relation to privacy and security until the arrival of blockchain technology. Therefore, as it is illustrated in Figure 1, in the last years pre-IoT closed and centralized mainframe architectures evolved towards IoT open-access cloud-centered alternatives, being the next step the distribution of the cloud functionality among multiple peers, where blockchain technology can help.

Blockchain technologies are able to track, coordinate, carry out transactions and store information from a large amount of devices, enabling the creation of applications that require no centralized cloud. Some companies like IBM go further and talk about blockchain as a technology for

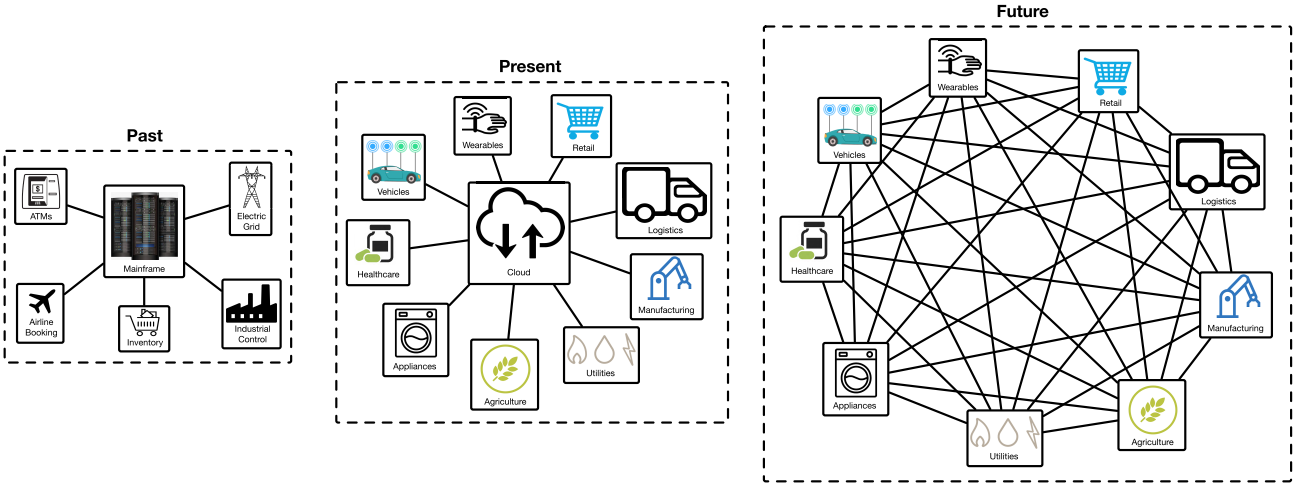

FIGURE 1. Past, present and future IoT architectures.

democratizing the future IoT [12], since it addresses the current critical challenges for its massive adoption:

- Many IoT solutions are still expensive due to costs related to the deployment and maintenance of centralized clouds and server farms. When such an infrastructure is not created by the supplier, the cost comes from middlemen.
- Maintenance is also a problem when having to distribute regular software updates to millions of smart devices.
- After Edward Snowden leaks [13], [14], it is difficult for IoT adopters to trust technological partners who, in general, give device access and control to certain authorities (i.e., governments, manufacturers or service providers), allowing them to collect and analyze user data. Therefore, privacy and anonymity should be at the core of future IoT solutions.
- Lack of trust is also fostered by closed-source code. To increase trust and security, transparency is essential, so open-source approaches should be taken into account when developing the next generation of IoT solutions. It is important to note that open-source code, like closed-source code, is still susceptible to bugs and exploits, but, since it can be monitored constantly by many users, it is less prone to malicious modifications from third parties.

Blockchain technology has been growing at an astounding pace over the past two years. As reported by Statista [15], investments by venture capitalists in blockchain start-ups rose from 93 million to 550 million U.S. dollars from 2013 to 2016. Furthermore, the market for blockchain technology worldwide is forecast to grow to 2.3 billion U.S. dollars by 2021. According to McKinsey & Company, although it is still in a nascent stage, blockchain technology may reach its full potential within the next 4 years based on its current pace of evolution [16]. In addition, as of writing, there are over 1,563 digital coins [17], just a few years after Bitcoin [18], the cryptocurrency that originated the blockchain, was born.

Bitcoin is a digital coin whose transactions are exchanged in a decentralized trustless way combining peer-to-peer file sharing with public-key cryptography. Public keys are alphanumeric strings formed by 27 to 32 characters that are used to send and receive Bitcoins, avoiding the necessity of making use of personal information to identify users. One feature that characterizes Bitcoin is miners, who receive coins for their computational work to verify and store payments in the blockchain. Such payments, like in any other currency, are performed in exchange of products, services or fiat money. This paper is not aimed at detailing the inner workings of Bitcoin, but the interested readers can find good overviews on how Bitcoin works in [19]–[21].

The use of cryptocurrencies based on blockchain technology is said to revolutionize payments thanks to their advantages respect to traditional currencies. Since middlemen are removed, merchant payment fees can be reduced below 1 % and users do not have to wait days for transfers, receiving funds immediately. Modern cryptocurrencies can be divided into three elements [19]: blockchain, protocol and currency. It must be indicated that a coin can implement its own currency and protocol, but its blockchain may run on the blockchain of another coin like Bitcoin or Ethereum [22]. For instance, Counterparty [23] has its own currency and protocol, but it runs on the Bitcoin blockchain.

In the case of a cryptocurrency, the blockchain acts as a ledger that stores all the coin transactions that have been performed. This means that the blockchain grows continuously, adding new blocks every certain time intervals. A full node (a computer that validates transactions) owns a copy of the whole blockchain, which also contains information about user addresses and balances. If the blockchain is public, in can be queried through a block explorer like Blockchain.info in order to obtain the transactions related to a specific address.

Therefore, the key contribution of blockchain is that it provides a way to carry out transactions with another person or entity without having to rely on third-parties. This is possible thanks to many decentralized miners (i.e., accountants) that scrutinize and validate every transaction. This contribution allowed the Bitcoin blockchain to provide a solution to the Byzantine Generals' Problem [24], since it is able to reach an agreement about something (a battle plan) among multiple parties (generals) that do not trust each other, when only exchanging messages, which may come from malicious third-parties (traitors) that may try to mislead them. In the case of cryptocurrencies, this computational problem is related to the double-spend problem, which deals with how to confirm that some amount of digital cash was not already spent without the validation of a trusted third-party (i.e., usually, a bank) that keeps a record of all the transactions and user balances.

IoT shares some common problems with cryptocurrencies, since in an IoT system there are many entities (nodes, gateways, users) that do not necessarily trust each other when performing transactions. However, there are several aspects that differentiate IoT from digital currencies, like the amount of computing power available in the nodes or the necessity for minimizing the energy consumed in devices powered with batteries. Therefore, this paper studies such similarities and analyzes the advantages that blockchain can bring to IoT despite its current practical limitations. Moreover, the main Blockchain-based IoT (BIoT) architectures and improvements that have already proposed are reviewed. Furthermore, the most relevant future challenges for the application of blockchain to IoT are detailed.

Other authors have previously presented surveys on the application of blockchain to different fields. For instance, in [25] it is provided an extensive description on the basics of blockchain and smart contracts, and it is given a good overview on the application and deployment of BIoT solutions. However, although the paper provides very useful information, it does not go deep into the characteristics of the ideal BIoT architecture or on the possible optimizations to be performed for creating BIoT applications. Another interesting work is presented in [26], where the authors provide a generic review on the architecture and the different mechanisms involved in blockchain, although it is not focused on its application to IoT. Similarly, in [27] and [28] different researchers give overviews on blockchain, but they emphasize its application to different Big Data areas and multiple industrial applications. Finally, it is worth mentioning the systematic reviews presented in [29] and [30], which analyze the sort of topics that papers in the literature deal with when proposing the use of blockchain.

Unlike the reviews previously mentioned, this work presents a holistic approach to blockchain for IoT scenarios, including not only the basics on blockchain-based IoT applications, but also a thorough analysis on the most relevant aspects involved on their development, deployment and optimization. It is also the aim of this work to envision the potential contribution of blockchain for revolutionizing the IoT industry and confront today challenges.

The remainder of this paper is organized as follows. Section II describes the basics of blockchain technologies: how they work, which types exist and how to decide if it is appropriate to make use of a blockchain. Section III presents the most relevant BIoT applications. Section IV reviews critical aspects to be optimized in a blockchain in order to adapt it to an IoT application. Section V describes the main shortcomings of current BIoT applications and outlines the primary technical challenges they face. Section VI identifies further medium-term challenges and proposes recommendations for IoT developers. Finally, Section VII is devoted to conclusions.

II. BLOCKCHAIN BASICS

A blockchain is like a distributed ledger whose data are shared among a network of peers. As it was previously mentioned, it is considered as the main contribution of Bitcoin, since it solved a longer-lasting financial problem known as the double-spend problem. The solution proposed by Bitcoin consisted in looking for the consensus of most mining nodes, who append the valid transactions to the blockchain.

Although the concept of blockchain was originated as a tool for a cryptocurrency, it is not necessary to develop a cryptocurrency to use a blockchain and build decentralized applications [31]. A blockchain, as its name implies, is a chain of timestamped blocks that are linked by cryptographic hashes. To introduce the reader into the inner workings of a blockchain, the next subsections describe its basic characteristics and functioning.

A. BLOCKCHAIN BASIC FUNCTIONING

In order to use a blockchain, it is first required to create a P2P network with all the nodes interested in making use of such a blockchain. Every node of the network receives two keys: a public key, which is used by the other users for encrypting the messages sent to a node, and a private key, which allows a node to read such messages. Therefore, two different keys are used, one for encrypting and another for decrypting. In practice, the private key is used for signing blockchain transactions (i.e., to approve such transactions), while the public key works like a unique address. Only the user with the proper private key is able to decrypt the messages encrypted with the corresponding public key. This is called asymmetric cryptography. A detailed explanation of its inner workings is out of the scope of this paper, but the interested reader can obtain further details in [32] and [33].

When a node carries out a transaction, it signs it and then broadcasts it to its one-hop peers. The fact of signing the transaction in a unique way (using the private key) enables authenticating it (only the user with a specific private key can sign it) and guarantees integrity (if there is an error during the transmission of the data, it will not be decrypted). As the peers of the node that broadcasts the transaction receive the signed transaction, they verify that it is valid before retransmitting

it to other peers, thus, contributing to its spread through the network. The transactions disseminated in this way and that are considered valid by the network are ordered and packed into a timestamped block by special nodes called miners. The election of the miners and the data included into the block depend on a consensus algorithm (a more detailed definition of the concept of consensus algorithm is given later in Section IV-D).

The blocks packed by a miner are then broadcast back into the network. Then the blockchain nodes verify that the broadcast block contains valid transactions and that it references the previous block of the chain by using the corresponding hash. If such conditions are not fulfilled, the block is discarded. However, if both conditions are verified successfully, the nodes add the block to their chain, updating the transactions.

B. TYPES OF BLOCKCHAINS

There are different types of blockchains depending on the managed data, on the availability of such data, and on what actions can be performed by a user. Thus, it can be distinguished between public and private, and permissioned and permissionless blockchains.

It is important to indicate that some authors use the terms public/permissionless and private/permissioned as synonyms, what may be coherent when talking about cryptocurrencies, but that is not the case for IoT applications, where it is important to distinguish between authentication (who can access the blockchain; private versus public) and authorization (what an IoT device can do; permissionless versus permissioned). Nonetheless, note that such distinctions are still in debate and the definitions given next might differ from others in the literature.

In public blockchains anyone can join the blockchain without the approval of third-parties, being able to act as a simple node or as miner/validator. Miners/validators are usually given economic incentives in public blockchains like Bitcoin, Ethereum or Litecoin [34].

In the case of private blockchains, the owner restricts network access. Many private blockchains are also permissioned in order to control which users can perform transactions, carry out smart contracts (a concept defined later in Section III) or act as miners in the network, but note that not all private blockchains are necessarily permissioned. For instance, an organization can deploy a private blockchain based on Ethereum, which is permissionless. Examples of permissioned blockchains are the ones used by Hyperledger-Fabric [35] or Ripple [36].

It can also be distinguished between blockchains aimed exclusively at tracking digital assets (e.g., Bitcoin) and blockchains that enable running certain logic (i.e., smart contracts). Moreover, there are systems that make use of tokens (e.g., Ripple), while others do not (e.g., Hyperledger). Note that such tokens are not necessarily related to the existence of a cryptocurrency, but they may be used as internal receipts that prove that certain events happened at certain time instants.

As a summary, the different types of blockchains are depicted in Figure 2 together with several examples of implementations.

C. DETERMINING THE NEED FOR USING A BLOCKCHAIN

Before delving into the details on how to make use of a blockchain for IoT applications, it must be first emphasized that a blockchain is not always the best solution for every IoT scenario. Traditional databases or Directed Acyclic Graph (DAG) based ledgers [37] may be a better fit for certain IoT applications. Specifically, in order to determine if the use of a blockchain is appropriate, a developer should decide if the following features are necessary for an IoT application:

- Decentralization. IoT applications demand decentralization when there is not a trusted centralized system. However, many users still trust blindly certain companies, government agencies or banks, so if there is mutual trust, a blockchain is not required.
- P2P exchanges. In IoT most communications go from nodes to gateways that route data to a remote server or cloud. Communications among peers at a node level are actually not very common, except for specific applications, like in intelligent swarms [38] or in mist computing systems [39]. There are also other paradigms that foster communications among nodes at the same level, as it happens in fog computing with local gateways [40], [41].
- Payment system. Some IoT applications may require to perform economic transactions with third parties, but many applications do not. Moreover, economic transactions can still be carried out through traditional payment systems, although they usually imply to pay transaction fees and it is necessary to trust banks or middlemen.
- Public sequential transaction logging. Many IoT networks collect data that need to be timestamped and stored sequentially. Nonetheless, such needs may be easily fulfilled with traditional databases, especially in cases where security is guaranteed or where attacks are rare.
- Robust distributed system. Distributed systems can also be built on top of clouds, server farms or any form of traditional distributed computing systems [42]. The need of this feature is not enough to justify the use of a blockchain: there also has to be at least a lack of trust in the entity that manages the distributed computing system.
- Micro-transaction collection. Some IoT applications [43], [44] may need to keep a record of every transaction to maintain traceability, for auditing purposes or because Big Data techniques will be applied later [45], [46]. In these situations, a sidechain may be useful [47]. However, other applications do not need to store every collected value. For example, in remote agricultural monitoring, where communications are

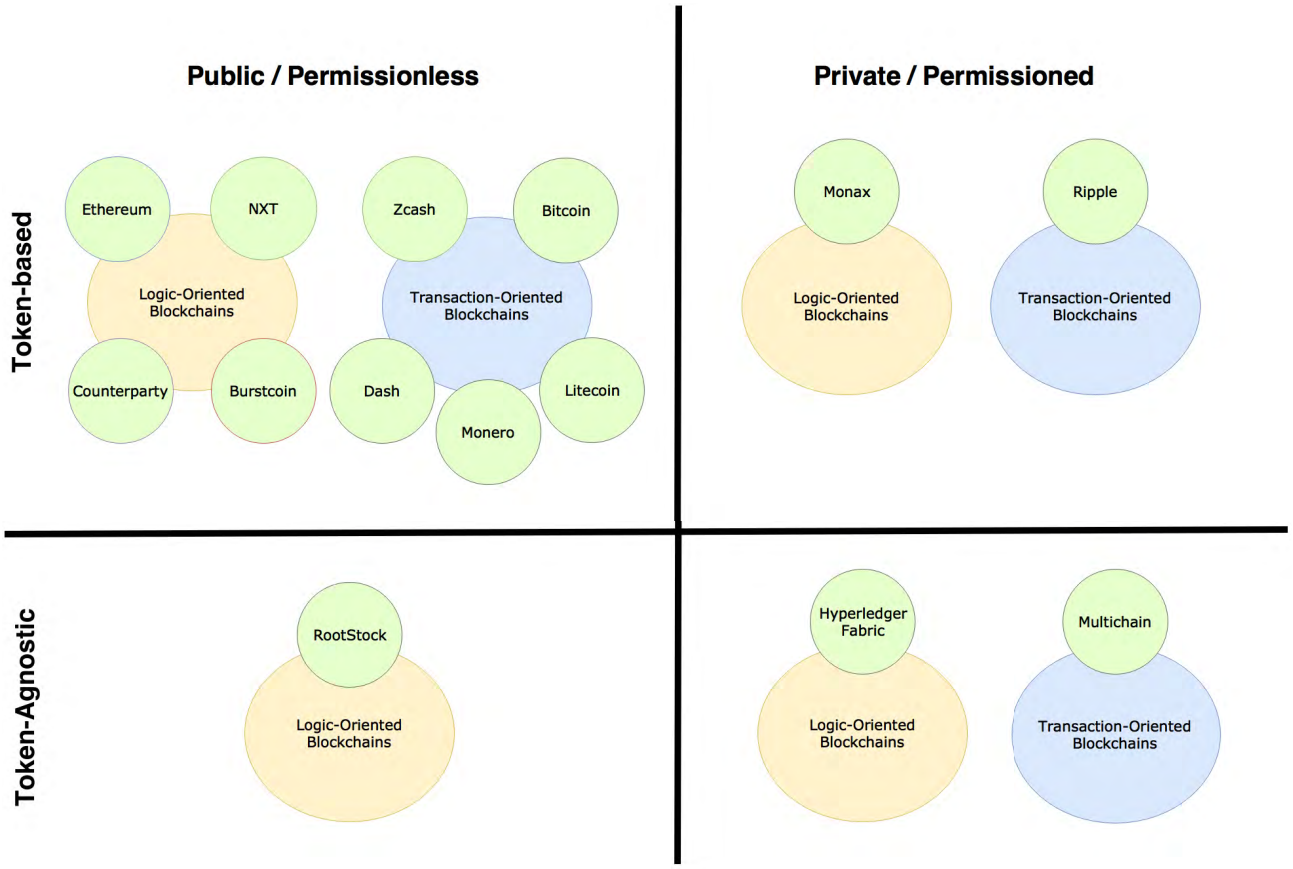

FIGURE 2. Blockchain taxonomy and practical examples.

expensive, it is usual to make use of IoT nodes that wake up every hour to obtain environmental data from sensors. In such cases, a local system may collect and store the data, and once a day it transmits the processed information altogether in one transaction [48].

Figure 3 shows a generic flow diagram that allows for determining the type of blockchain that is necessary depending on the characteristics of an IoT system.

III. BIoT APPLICATIONS

Blockchain technology can be applied in many fields and use cases. Swan [19] suggested that blockchain applicability evolution started with Bitcoin (blockchain 1.0), then evolved towards smart contracts (blockchain 2.0) and later moved to justice, efficiency and coordination applications (blockchain 3.0).

Regarding smart contracts, they are defined as pieces of self-sufficient decentralized code that are executed autonomously when certain conditions are met. Smart contracts can be applied in many practical cases, including international transfers, mortgages or crowd funding [49].

Ethereum is arguably the most popular blockchain-based platform for running smart contracts, although it can actually run other distributed applications and interact with more than one blockchain. In fact, Ethereum is characterized by being Turing-complete, which is a mathematical concept that indicates that Ethereum's programming language can be used to simulate any other language. A detailed explanation on how smart contracts work is out of the scope of this paper, but the interested reader can find a really good description in Section II.D of [25].

Beyond cryptocurrencies and smart contracts, blockchain technologies can be applied in different areas (the most relevant are shown in Figure 4) where IoT applications are involved [29], like sensing [50], [51], data storage [52], [53], identity management [54], timestamping services [55], smart living applications [56], intelligent transportation systems [57], wearables [58], supply chain management [59], mobile crowd sensing [60], cyber law [61] and security in mission-critical scenarios [62].

Blockchain can also be used in IoT agricultural applications. For example, in [63] it is presented a traceability system for tracking Chinese agri-food supplies. The system is based on the use of Radio Frequency Identification (RFID) and a blockchain, being its aim to enhance food safety and quality, and to reduce losses in logistics.

Other researchers focused on managing IoT devices through a blockchain [64]. Such researchers proposed a system able to control and configure IoT devices remotely. The system stores public keys in Ethereum while private

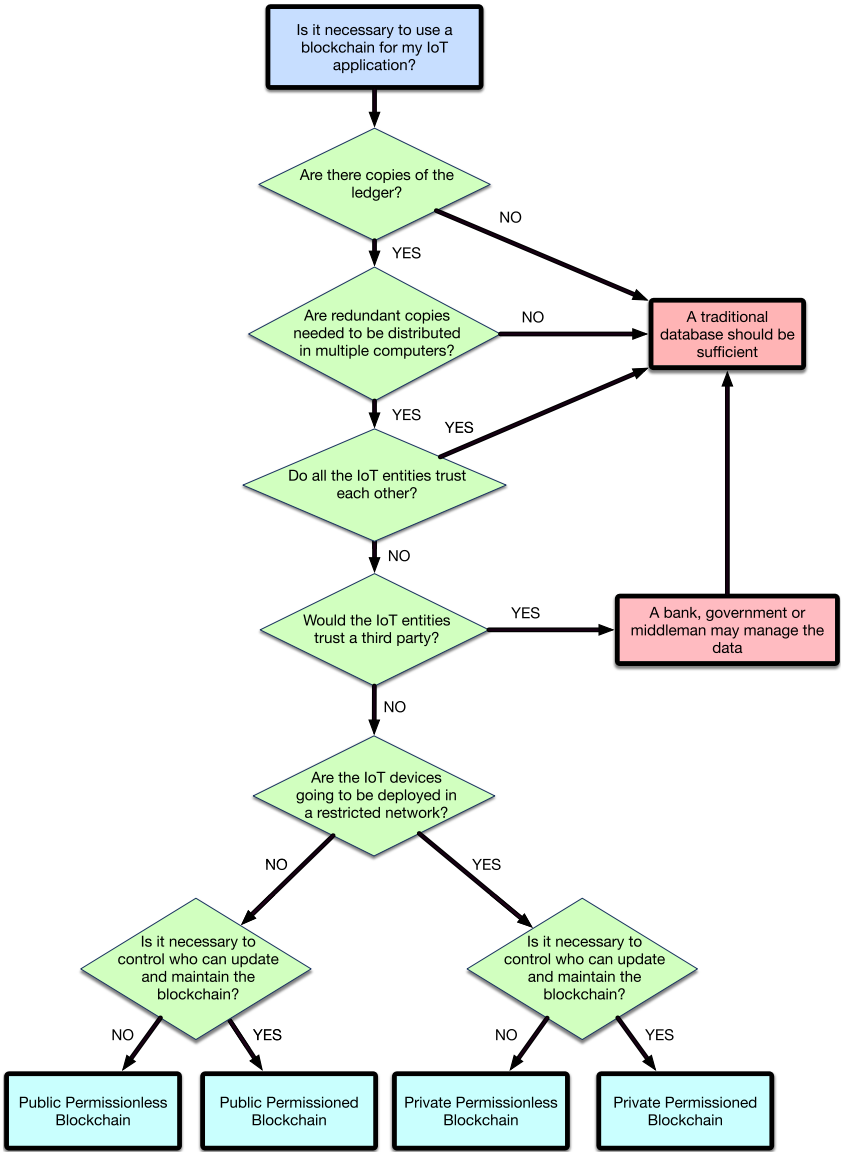

FIGURE 3. Flow diagram for deciding when to use blockchain in an IoT application.

keys are saved on each IoT device. The authors indicate that the use of Ethereum is essential, since it allows them to write their own code to run on top of the network. Moreover, updating the code on Ethereum modifies the behavior of the IoT devices, what simplifies maintenance and bug corrections.

The energy sector can also be benefited from the application of a blockchain to IoT or to the Internet of Energy (IoE) [65]–[67]. An example is detailed in [68], where the authors propose a blockchain-based system that allows IoT/IoE devices to pay each other for services without human intervention. In the paper it is described an implementation that shows the potential of the system: a smart cable that connects to a smart socket is able to pay for the electricity consumed. In addition, to reduce the transaction fees of cryptocurrencies like Bitcoin, the researchers present a single-fee micro-payment protocol that aggregates several small payments into a larger transaction.

Healthcare BIoT applications are found in the literature as well. For instance, in [69] it is presented a traceability application that makes use of IoT sensors and blockchain technology to verify data integrity and public accessibility to temperature records in the pharmaceutical supply chain. This verification is critical for the transport of medical products in order to ensure their quality and environmental conditions (i.e., their temperature and relative humidity). Thus, every shipped parcel contains a sensor that transfers the collected data to the blockchain where a smart contract determines whether the received values remain within the allowed range. Another healthcare BIoT application is detailed in [70], where it is presented the architecture of a blockchain-based platform for clinical trials and precision medicine. It is also

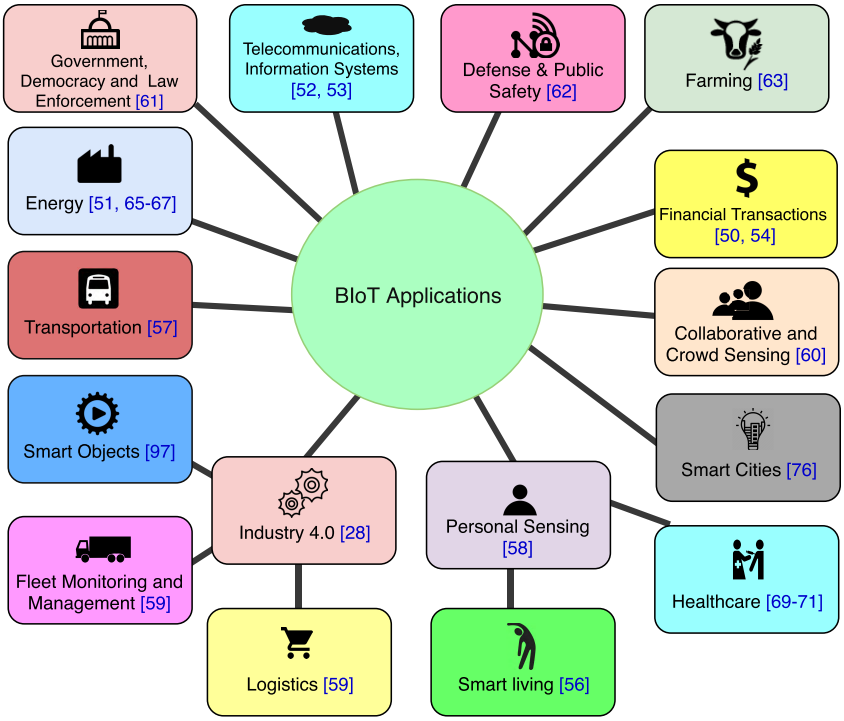

FIGURE 4. BIoT applications.

worth mentioning the work described in [71], which presents a generic smart healthcare system that makes use of IoT devices, cloud and fog computing [72], a blockchain, Tor [73] and message brokers.

IoT low-level security can also be enhanced by blockchain technology. Specifically, it can be improved remote attestation, which is the process that verifies whether the underlying Trusted Computer Base (TCB) of a device is trustworthy [74]. This verification can be performed by managing the TCB measurements obtained by using ARM TrustZone [75] and a blockchain, where they are stored securely.

Other already proposed BIoT applications are related to smart cities [76] and industrial processes [28]. In the case of [76] it is proposed a framework that integrates smart devices in a secure way for providing smart city applications. In [28], different blockchain-based industrial applications are reviewed, including their connection to Industrial IoT (IIoT) networks.

Finally, it should be mentioned that Big Data can be leveraged by blockchain technology (i.e., to ensure its trustworthiness), so some researchers [27] reviewed the main blockchain-based solutions to gather and control massive amounts of data that may be collected from IoT networks.

IV. DESIGN OF AN OPTIMIZED BLOCKCHAIN FOR IoT APPLICATIONS

Blockchain technologies can bring many benefits to IoT, but, since they have not been devised explicitly for IoT environments, the different pieces that make them up should be adapted. In order to optimize them, several authors studied BIoT performance in different scenarios. They analyzed a number of influential aspects, but they mainly focus on the performance of consensus algorithms.

An example of performance evaluation is detailed in [77]. Specifically, the paper analyzes whether the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm (described later in Section IV-D) could be a bottleneck in networks with a large amount of peers. Actually, the tests described make use of up to 100 peers that interact with a blockchain based on IBM's Bluemix. The experiments measure the average time to reach a consensus and it can be observed how it grows as the number of peers increases.

The scalability of Proof-of-Work (PoW) and Byzantine Fault Tolerance (BFT) based consensus methods is compared in [78]. The author points out that, although Bitcoin has been a clear success, its poor scalability makes no sense today, since there are modern cryptocurrency platforms like Ethereum. In the paper it is suggested to improve PoW performance by mixing it with a BFT protocol. In addition, it is stated that the implementation of the consensus protocols in hardware is probably the most promising way for improving the performance of any consensus method.

Besides the consensus algorithm, other elements of the blockchain can be adapted to be used in IoT networks. Thus, in the next subsections the different parts of a blockchain are analyzed in order to determine possible optimizations.

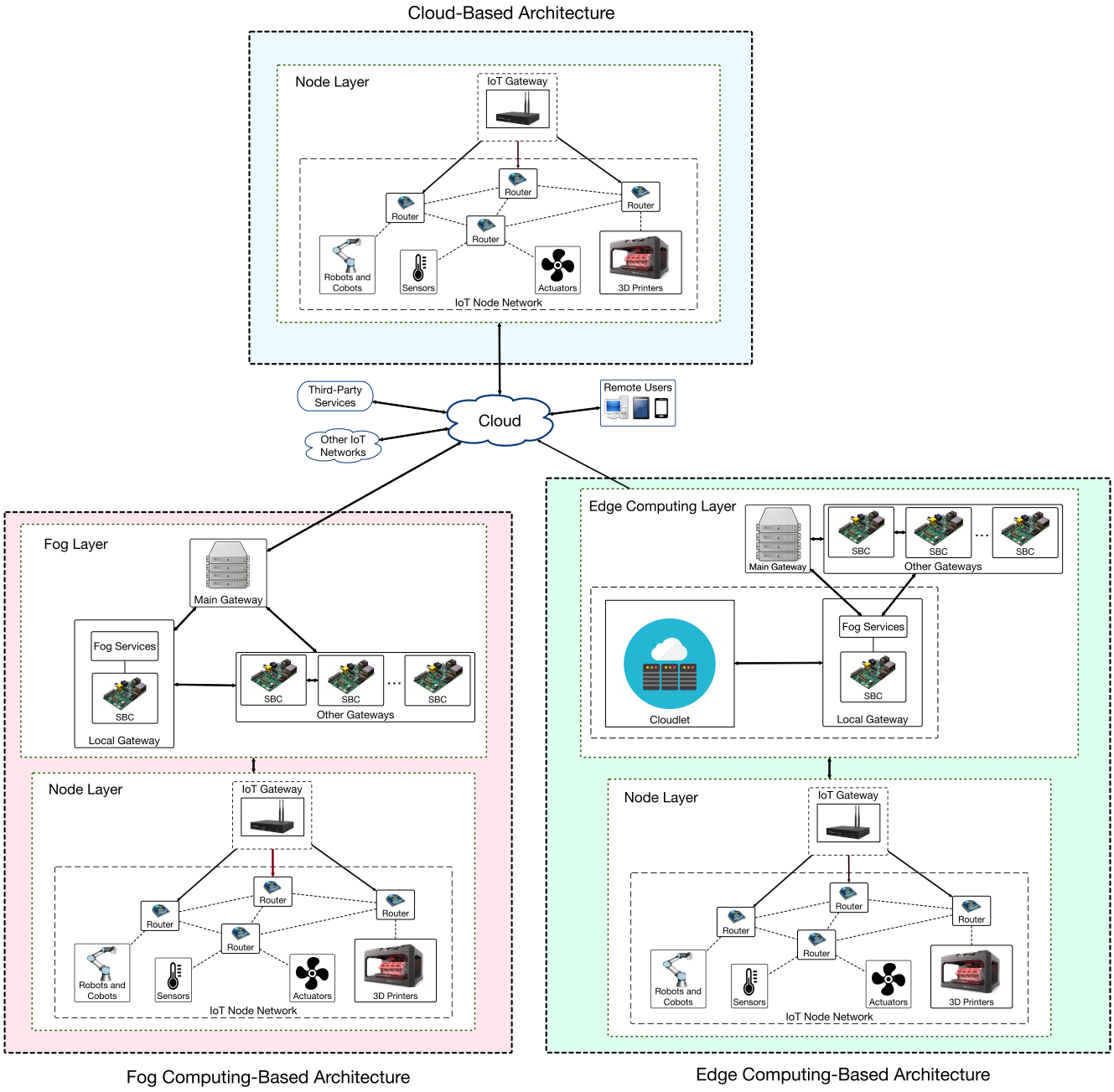

FIGURE 5. Traditional IoT architecture evolution.

A. ARCHITECTURE

The architecture that supports a blockchain used for IoT applications should have to be adapted to the amount of traffic that such applications usually generate. This is a concern for traditional cloud-based architectures, which, as it is illustrated in Figure 5, evolved towards more complex edge and fog computing-based architectures. In such a Figure it can be observed that three architectures depend on a cloud, although, in practice, the dependency degree varies a great deal. In the case of a cloud-based architecture, the data collected by the Node Layer are forwarded directly to the cloud through IoT gateways without further processing that the one needed for protocol conversion (in case it is needed). There are also gateways that perform more sophisticated tasks (e.g., sensor fusion [79]), but in most cloud-centered applications, most processing is carried out in the cloud.

However, note that traditional cloud-centered IoT architectures have certain inherent vulnerabilities [59], being the most relevant the fact that the cloud is a point of failure: if the cloud is down due to cyberattacks, maintenance

or software problems, the whole system stops working. In addition, it is important to emphasize that if a single IoT device is compromised, it may disrupt the whole network by performing Denial of Service (DoS) attacks [80], eavesdropping private data [81], altering the collected data [82] or misleading other systems [83]. Therefore, once an IoT device connected to the cloud or to a central server is breached, the rest of the nodes may be compromised. In contrast, blockchain-based systems do not rely on a unique central server or cloud. Moreover, transactions are verified cryptographically, so when malicious activities from a compromised device are detected, the system can reject its blockchain updates.

The other two architectures depicted in Figure 5 are more recent and offload part of the processing from the cloud to the edge of the network. This offloading is key for IoT applications, since it is estimated that if the number of IoT connected devices keeps on growing at the same rate [1], the amount of communications to be handled by a cloud will increase remarkably and, therefore, the cloud network capacity will have to be expanded. Thus, Edge and fog computing can be used to support physically distributed, low-latency and QoS-aware applications that decrease the network traffic and the computational load of traditional cloud computing systems.

Fog computing is based on a set of local gateways able to respond fast to IoT node requests through specific services. Such nodes can also interact with each other and, when required, with the cloud (for instance, for long term storage). In Figure 5, fog local gateways are represented by Single-Board Computers (SBCs), which are low-cost and low-energy consumption computers that can be installed easily in a reduced space. Examples of popular SBCs are the different versions of Raspberry Pi [84] or BeagleBone [85].

Fog computing is actually considered a subset of edge computing [72], which has recently been presented as a valid architecture for supporting blockchain and blockchainless DAG IoT applications [86]. As it can be observed in Figure 5, in the Edge Computing Layer, besides fog gateways there is a cloudlet, which in practice consists in one or more high-end computers that act like a reduced version of a cloud. The main advantage of cloudlets is that they can provide high-speed responses to compute-intensive tasks required by the Node Layer (e.g., running a full node of a blockchain), which cannot be delivered effectively when using resource-constrained fog gateways.

There are other architectures that have been explored in the past in order to tackle the architectural issues that arise when providing BIoT services. A brief but good compilation of alternatives can be found in [87]. In such a paper the advantages and disadvantages of four different architectures (that the authors call Fully Centralized, Pseudo-Distributed Things, Distributed Things and Fully Distributed) are discussed. The researchers conclude that a BIoT architecture should be as close as possible to the Fully Distributed approach, but that, in some scenarios where computational power or cost are limiting factors, other approaches may be more appropriate.

An interesting platform that promotes decentralization for IoT systems is IBM's ADEPT. Such a platform was conceived for secure, scalable and autonomous peer-to-peer IoT telemetry. According to the authors, ADEPT is presented more as a starting point for discussion than as an implementation, but its white paper [88] provides a detailed description on the requirements for the platform. For instance, the researchers point out that an IoT device should be able to authenticate autonomously and to self-maintain, leaving to the manufacturers the responsibility of registering new devices in the blockchain. In addition, ADEPT's vision of mining is different from the one implemented in Bitcoin. Mining is necessary in Bitcoin to restrict currency issuance, but IBM considers that such a limitation restricts scalability and imposes an increasing computational cost. Therefore, ADEPT uses Proof-of-Stake (PoS) and PoW, which guarantee network integrity and security, but which do not impose additional limitations. Furthermore, it is worth mentioning that IBM's architecture for ADEPT distinguishes among three types of IoT devices (Light Peers, Standard Peers and Peer Exchanges), which differ in their role and computational capabilities. Finally, the authors of the white paper indicate the software selected for implementing ADEPT (Telehash [89], BitTorrent [90] and Ethereum) and describe different practical use cases of the system, like a washer that buys detergent automatically when it is low.

Another BIoT architecture is proposed in [91] and [92]. In such papers the authors devise a theoretical lightweight architecture with security and privacy in mind, which reduces the communications overhead introduced by the use of a blockchain. The presented system is oriented towards home automation and its architecture is divided into three layers: the smart home layer, where there are sensors, actuators and local storage; an overlay network of peers and shared storage; and a cloud, which also provides remote storage. In the lower layers (smart homes and overlay network) storage is composed by traditional storage servers and blockchains, either public or private. The reduction in overhead is carried out by removing the PoW consensus mechanism, so every block is mined and appended to the blockchain without additional efforts. Every transaction is also appended to a block and is assumed that it is a true transaction, being the owner the one responsible for adding/removing devices. This simplification eases the blockchain functioning and, although the researchers studied the impact of different attacks on the system, it is not clear that the proposed scheme would withstand attacks performed by compromised IoT nodes whose contribution (e.g., collected sensor values), which is assumed to be true by default, may alter the behavior of other subsystems.

IoT is also gaining traction thanks to its global vision where devices are interconnected seamlessly among them and with the environment. For such a purpose, in [93] it is presented a theoretical blockchain-based architecture focused

both on providing IoT services and connecting heterogeneous devices. The proposed architecture makes use of hierarchical and multi-layered blockchains, which enable building a contextual service discovery system called CONNECT.

A multi-layer IoT architecture based on blockchain technology is described in [94]. The proposed architecture decreases the complexity of deploying a blockchain by dividing the IoT ecosystem in levels and making use of the blockchain in each one. The researchers state that the architecture harnesses both the power of a cloud and the security and reliability of the blockchain.

A slightly different approach is presented in [95], where it is evaluated the use of a cloud and a fog computing architecture to provide BIoT applications. The authors indicate that the architecture is proposed because is really difficult to host a regular blockchain on traditional resource-constrained IoT devices. Thus, the researchers measure empirically the performance of the system proposed by using IoT nodes based on Intel Edison boards and IBM's Bluemix as blockchain technology. The obtained results show that, under high transaction loads, the fog system latency response is clearly faster than in a cloud-based system. Following similar ideas, the same authors presented another two works. In [96] they describe the implementation of RESTful microservices on the architecture, while in [97] they extend the architecture to a paradigm they call the Internet of Smart Things.

Another architecture based on edge computing is presented in [98], which describes ongoing research on the development of a hierarchical and distributed platform based on the IEC 61499 standard [99], which supports distributed automation control systems. Such systems can be structured in two layers: a bottom layer that controls devices and processes, and a top layer that supervises the bottom layer. For the top layer, the platform uses a blockchain based on Hyperledger Fabric [35] that implements smart contracts to perform supervision tasks. The edge nodes conform the bottom layer and are based on a micro-service architecture that makes use of Docker containers [100] and Kubernetes [101].

Software Defined Networking (SDN) has been also suggested for implementing BIoT architectures. For instance, in [102] it is proposed a novel blockchain-based architecture that makes use of SDN to control the fog nodes of an IoT network. The system makes use of a cloud to perform compute-intensive tasks, while providing low-latency data access through fog computing. The fog nodes are the ones that are distributed, providing services and interaction with the blockchain. The results obtained by the authors indicate that the architecture reduces delays, increases throughput and it is able to detect real-time attacks on the IoT network. In the specific case of a flooding attack, the architecture is able to balance the load between the fog nodes thanks to the use of the blockchain and an SDN algorithm. In addition, the same authors describe in [103] a similar SDN-based approach.

B. CRYPTOGRAPHIC ALGORITHMS

Public-key cryptography is essential for providing security and privacy in a blockchain. However, resource-constraint IoT devices struggle with the computing requirements of modern secure cryptographic schemes [104]. Specifically, asymmetric cryptography based on Rivest–Shamir–Adleman (RSA) is slow and power consuming when implemented on IoT devices [41]. Therefore, when choosing the right cryptographic scheme, it should be taken into account not only the computational load and the memory requirements, but also the energy consumed.

The most common public-key based cipher suites are RSA and Elliptic Curve Diffie-Hellman Exchange (ECDHE), which are the ones recommended by the National Institute of Standards and Technology (NIST) [105] for Transport Layer Security (TLS) [106]. RSA-based cipher suites use RSA [107] as the key exchange algorithm, while the ECDHE-based ones use an algorithm that makes use of Ephemeral Diffie-Hellman based on Elliptic Curves [108].

Current RSA key sizes are not practical for most IoT devices. A 2048-bit key is the minimum size considered secure, since 768-bit and 1024-bit RSA implementations were broken in 2010 [109], [110]. Although possible, the use of a 2048-bit certificates on an ephemeral key exchange algorithm introduces heavy overhead and computing requirements, which are very difficult to accommodate on the constrained hardware capabilities of most IoT nodes.

In contrast, Elliptic Curve Cryptography (ECC) represents a much lighter alternative to RSA [111], [112]. It has already been shown that, when implemented on resource-constrained devices, ECC outperforms RSA in terms of speed [113]–[115] and power consumption [116]–[119]. However, note that in August 2015 the National Security Agency (NSA) recommended stopping the use of Suite B, an ECC-based algorithm, apparently, because of the progress recently made on quantum cryptography [120].

Regarding hash functions, they are also key in a blockchain-based system, since they are required to sign transactions. Therefore, hash functions for IoT applications have to be secure (i.e., they should not generate collisions [121]), fast and should consume the smallest possible amount of energy.

The most popular blockchain hash functions are SHA-256d (used by Bitcoin, PeerCoin or Namecoin), SHA-256 (used by Swiftcoin or Emercoin) and Scrypt (used by Litecoin, Gridcoin or Dogecoin). The performance of SHA-256 has been evaluated in different IoT devices, like wearables [122]. However, researchers that evaluated the footprint and energy requirements of SHA-256 in ASICs, concluded that, for low-power secure communications, it is more efficient to make use of Advanced Encryption Standard (AES) [123]. Due to such power limitations, other researchers suggested using ciphers like Simon [124], but further research and empirical evaluations on real BIoT applications are still needed.

C. MESSAGE TIMESTAMPING

In order to track modifications on the blockchain, transactions have to be both signed and timestamped. This last task should be performed in a synchronized way, so timestamping servers are commonly used.

Different timestamping mechanisms can be used. Traditional schemes rely on having trustworthiness on the server, which signs and timestamps transactions with its own private key. Nonetheless, no one deters the server from signing past transactions. For such a reason, diverse authors have proposed secure mechanisms. For instance, the method implemented by Bitcoin is inspired by one of the solutions proposed in [125], where each timestamp includes a hash of the previous timestamp, what maintains the order of the transactions (even when the clocks are inaccurate) and makes it difficult to insert fake transactions in the already linked chain. In addition, timestamping can be distributed, hence avoiding the problem of having a single point of failure. Although such a distributed system is prone to Sybil attacks [126], Bitcoin solves them by linking blocks and using the PoW mechanism.

Other authors recently proposed the use of a decentralized timestamping service [127] or the distribution of its keys [128], but the topic has still to be studied in detail when decentralizing the service among devices of an IoT network.

D. CONSENSUS MECHANISMS, MINING AND MESSAGE VALIDATION

Consensus is key for the proper functioning of a blockchain. It basically consists in a mechanism that determines the conditions to be reached in order to conclude that an agreement has been reached regarding the validations of the blocks to be added to the blockchain [26]. In practice, the problem is the Byzantine Generals Problem previously described in the Introduction.

The most egalitarian (and idealistic) consensus mechanism consists in giving to all the miners the same weight when voting and then deciding according to the majority of the votes. This scheme may be possible to implement in a controlled environment, but, in a public blockchain, this mechanism would lead to Sybil attacks, since a unique user with multiple identities would be able to control the blockchain [126].

In practice, in a decentralized architecture, one user has to be selected to add every block. This selection could be performed randomly, but the problem is that random selection is prone to attacks. PoW consensus algorithms are based on the fact that if a node performs a lot of work for the network, it is less likely that it is going to attack it. Specifically, the solution proposed by PoW-based blockchains makes it difficult to perform Sybil attacks by requiring miners to perform computationally expensive tasks that, theoretically, cannot be carried out by a single entity. The work performed usually involves doing some calculations until a solution is found, a process that is commonly known as mining. In the case of the Bitcoin blockchain, mining consists in finding a random number (called nonce) that will make the SHA-256 hash of the block header to have at the beginning certain number of zeroes. Therefore, miners have to demonstrate that they have performed certain amount of work to solve the problem. Once the problem is solved, it is really easy for other nodes to verify that the obtained answer is correct. However, this mining process makes the blockchain inefficient in throughput, scalability [78], and in terms of energy consumption, what is not desirable in an IoT network.

Due to the problems previously mentioned, several alternative consensus methods have been proposed. The following are the most relevant:

- PoS is a consensus mechanism that requires less computational power than PoW, so it consumes less energy. In a PoS-based blockchain it is assumed that the entities with more participation on the network are the ones less interested in attacking it. Thus, miners have to prove periodically that they own certain amount of participation on the network (e.g., currency). Since this scheme seems unfair, because the wealthiest participants are the ones ruling the blockchain, other variants have been proposed. For example, Peercoin's consensus algorithm [129] takes coin age into account: the entities with the oldest and largest sets of coins would be more likely to mine a block. Because of the advantages of PoS, some blockchains like Ethereum are planning to move from PoW to PoS.
- Delegated Proof-of-Stake (DPoS) [130] is similar to PoS, but stakeholders instead of being the ones generating and validating blocks, they select certain delegates to do it. Since less nodes are involved in block validation, transactions are performed faster than with other schemes. In addition, delegates can adjust block size and intervals, and, if they behave dishonestly, they can be substituted easily.
- Transactions as Proof-of-Stake (TaPoS) [131] is a PoS variant. While in PoS systems only some nodes contribute to the consensus, in TaPoS all nodes that generate transactions contribute to the security of the network.
- Proof-of-Activity (PoA) consensus algorithms were proposed due to the main limitation of PoS systems based on stake age: it is accumulated even when the node is not connected to the network. Thus, PoA schemes have been proposed to encourage both ownership and activity on the blockchain [132], rewarding stakeholders who participate instead of punishing passive stakeholders. A similar approach is proposed by Proof-of-Stake-Velocity (PoSV) [133]. It is implemented by Reddcoin [134], which is based on the concept of velocity of money. Such a concept indicates how many times a unit of currency flows through an economy and is used by the members of a society during a

certain time period. Usually, the higher the velocity of money, the more transactions in which it is used and the healthier the economy.

- PBFT [135] is a consensus algorithm that solves the Byzantine Generals Problem for asynchronous environments. PBFT assumes that less than a third of the nodes are malicious. For every block to be added to the chain, a leader is selected to be in charge of ordering the transaction. Such a selection has to be supported by at least 2/3 of the all nodes, which have to be known by the network.
- Delegated BFT (DBFT) is a variant of BFT where, in a similar way to DPOS, some specific nodes are voted to be the ones generating and validating blocks.
- The Ripple consensus algorithm [136] was proposed to reduce the high latencies found in many blockchains, which are in part due to the use of synchronous communications among the nodes. Thus, each Ripple's server (i.e., miner) relies on a trusted subset of nodes when determining consensus, what clearly reduces latency.
- Stellar Consensus Protocol (SCP) is a implementation of a consensus method called Federated Byzantine Agreement (FBA) [137]. It is similar to PBFT but, whilst in PBFT every node queries all the other nodes and waits for the majority to agree, in SCP the nodes only wait for a subset of the participants that they consider important.
- BFTRaft [138] is a BFT consensus scheme based on the Raft algorithm [139], which is aimed at being simple and easy to understand for students. Such an aim makes Raft assume simplifications that rarely hold in practice, like the fact that nodes only fail by stopping. Thus, BFTRaft enhances the Raft algorithm by making it Byzantine fault tolerant and by increasing its security against diverse threats.
- Sieve [140] is a consensus algorithm proposed by IBM Research that has already been implemented for Hyperledger-Fabric. Its objective is to run non-deterministic smart contracts on a permissioned blockchain that makes use of BFT replication. In such a scenario, Sieve replicates the processes related to non-deterministic smart contracts and then compares the results. If a divergence is detected among the results obtained by a small number of processes, they are sieved out. However, if the number of divergent processes is excessive, the whole operation is sieved out.
- Tendermint [141] is a consensus algorithm that can host arbitrary application states and can only tolerate up to a 1/3 of failures. In Tendermint, blockchain participants are called validators and they propose blocks of transactions and vote on them. A block is validated in two stages (pre-vote and pre-commit) and it can only be committed when more than 2/3 of the validators pre-commit it in a round.
- Bitcoin-NG [142] implements a variant of the Bitcoin consensus algorithm aimed at improving scalability, throughput and latency. The developers performed experiments with 1,000 nodes and concluded that Bitcoin-NG scales optimally, only limited by the bandwidth of the nodes and the latency related to the propagation time of the network.
- Proof-of-Burn (PoB) is a consensus method that requires miners to show proof of their commitment to mining by burning some cryptocurrency through an unspendable address. The idea behind PoB is that, instead of burning resources (e.g., energy in the case of many PoW implementations), cryptocurrency is burnt as it is considered as expensive as such resources.
- Proof-of-Personhood (PoP) [143] is a consensus mechanism that makes use of ring signatures [144] and collective signing [145] to bind physical to virtual identities in a way that anonymity is preserved. A very similar concept is Proof-of-Individuality (PoI), which is currently being developed on Ethereum by the PoI Project [146].

Finally, it is worth noting that private blockchains, which control user access, reduce the probability of Sybil attacks, so they do not require costly mining algorithms and economic incentives are removed.

E. BLOCKCHAIN UPDATING/MAINTENANCE AND PROTOCOL STACK

The construction of an IoT network requires deploying a huge number of devices. Such devices embed certain firmware that is usually updated to correct bugs, prevent attacks [147] or just to improve some functionality. Traditionally, IoT devices had to be updated manually or with Over-The-Air (OTA) updates [148]. According to some researchers [149] these updates can be performed by using a blockchain, which enables IoT devices to spread securely new firmware versions.

Regarding the protocol stack, some authors suggested changes on the traditional OSI stack to adapt it to blockchain technologies. The most relevant is the so-called ''Internet of Money'' (IoM) [150], which proposes a set of five layers that operate on TCP/IP (shown in Figure 6). Such five layers include:

- A Ledger Layer that creates ledgers and issues assets.
- A Payment and Exchange Layer.
- A Pathfinding Layer that calculates the optimal set of atomic operations to be executed for the desired value transfer or exchange.
- A Contract Layer that controls balances through certain running code.
- An Application Layer that allows for developing applications and user interfaces.

More research is still needed in order to study the need for specific stacks and to analyze their performance in comparison to other traditional OSI-based stacks.

V. CURRENT CHALLENGES FOR BIoT APPLICATIONS

Today, emerging technologies in the IoT ecosystem like Cyber-Physical Systems (CPS) [151]–[153], RFID [154],

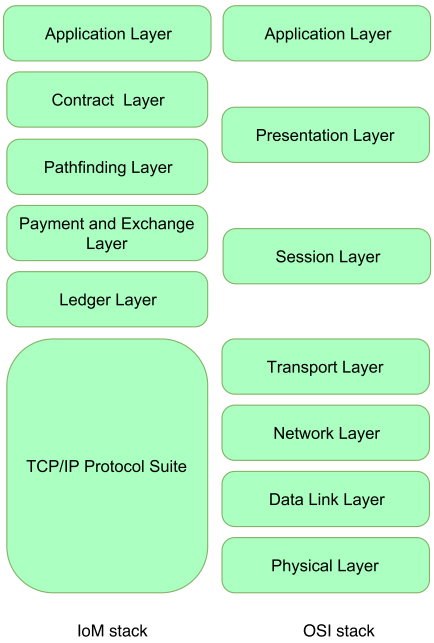

FIGURE 6. IoM versus traditional OSI protocol stack.

telemetry systems [155] or 4G/5G broadband communications [156], [157] have to face several challenges. Specifically, the case of mission-critical scenarios [158] rise additional concerns. Adding blockchain to the mix implies further operational and technical requirements since the development of BIoT applications is a complex process that is affected by many aspects that are interrelated. The main factors are described in the next subsections and are depicted in Figure 7.

A. PRIVACY

All the users of a blockchain are identified by their public key or its hash. This means that anonymity is not guaranteed and, since all transactions are shared, it is possible for third-parties to analyze such transactions and infer the actual identities of the participants [159], [160]. Privacy is even more complex in IoT environments, since IoT devices can reveal private user data that could be stored in a blockchain whose privacy requirements differ from one country to another [161]. Therefore, in contrast to traditional online payments, which are usually only visible to transacting parties and to a middleman (e.g., financial institutions, government), the transparent transactions fostered by blockchain are a challenge in terms of privacy.

Identity certification may also be a problem in IoT: if an identity provider is responsible for authorizing entities, it can also be able to block them. To address such a challenge, in [162] it is proposed the use of a permissioned blockchain for securing and managing multiple IoT nodes. The proposed system provides a distributed identity management solution that increases security and protection against attacks by rotating asymmetric keys. Such keys are generated locally on the device and they are never moved from it. To verify the identity of a user while rotating keys, the system makes use of a mechanism called Device Group Membership (DGM) that includes in a group all the devices that belong to a user and, when a user carries out a transaction, it is reflected on the blockchain as it was performed by a device that belonged to the user's group. The proposed solution also enhances security by using a certificate system for authentication and by enabling the hash function substitution if it is compromised. It is also worth mentioning that the system can be tweaked to limit the amount of temporal data stored, which is useful for IoT devices with little storage space (for instance, it could only be stored the data from the previous 24 hours).

Another approach focused on solving the privacy and robustness problems derived from using centralized identity management systems is described in [92]. There the authors emphasize the need for providing automatic authentication systems for IoT applications where scalability is needed and where device heterogeneity and mobility are common. To deal with such challenges, the researchers present a blockchain-based system for IoT smart homes that extracts appliance signatures automatically in order to identify both the appliances and their users.

Access management to IoT networks is challenging as well. Some researchers [163] suggested improving it by defining a blockchain-based multi-level mechanism, which would specify capabilities, access lists and access rights. However, note that, in many IoT applications anonymity is not necessary, but the privacy of the transactions is required in certain scenarios when the collected data may allow for monitoring and predicting people behavior or habits. This has already been an issue in fields like RFID-based transportation card systems, where the stored information (i.e., trips, balance, personal data) is supposedly anonymous, but in practice it may be collected by third parties [164]–[166]. The issue is even more problematic when adding a blockchain, since transactions are shared among peers, what in certain fields like industry or financial systems, allows for monitoring the activity of competitors.

Therefore, solutions have to be proposed to mitigate these privacy issues. For example, in the case of public blockchains a user does not need to know the address of every user, just the one of the counterparty he/she is dealing with. If a blockchain participant makes use of a new address for every transaction, data analysis would become more difficult. This is similar to what smartphones manufacturers have implemented to avoid Wi-Fi tracking [167], [168]. A more practical but less anonymous solution would consist in using a unique address for each counterparty.

In a private blockchain, since access controls are performed, there is at least one node that knows who accesses the system. Assuming the neutrality of the access controller, it is possible to reduce exposure by establishing an independent blockchain with every entity a user is collaborating with. This setup increases communications complexity, but

FIGURE 7. Most relevant factors that condition the development of a BIoT application and their main relationships.

isolates the user from non-desired monitoring. For instance, Multichain [169] provides a solution for deploying private blockchains (it can work with different blockchains at the same time) that ensures that the activities on the blockchain can be monitored by chosen participants.

Mixing techniques can also help to enhance privacy. Such techniques can collect transactions from diverse IoT devices and output events or other transactions to different addresses that are not linked to the original devices. These techniques increase privacy, but they are not perfect, since they may be de-anonymized through statistical disclosure attacks [170]. Moreover, the mixing service has to be trusted, since a malicious mixer may expose users and, in the case of economic transactions, it may end up stealing coins. To tackle these issues different proposals suggested exposing theft through an accountability mechanism [171] or hiding the input/output address mapping from the mixing server [172].

Privacy can also be increased through zero-knowledge proving techniques like the ones used by Zerocoin [173], Zerocash [174] or Zcash [175]. A zero-knowledge proof is a method that allows for proving to a counterparty that a user knows certain information without revealing such an information [176]. In the case of IoT applications, zero-knowledge proofs can be used for authentication or during regular transactions in order to avoid revealing the identity of a user or a device. However, note that these proofs are not immune to attacks [177]. In fact, like in the case of mixing techniques, they are susceptible to de-anonymization through statistical

disclosure attacks, but they improve mixing techniques by avoiding the necessity for a mixing server, which can pose a security or performance bottleneck.

It must be also remarked the privacy-focused efforts performed by several initiatives like Bytecoin [178] or Monero [179], which are based in CryptoNote [180]. CryptoNote is a protocol that makes use of ring signatures and whose transactions cannot be followed through the blockchain in order to determine who performed them. The only people that can access the transaction information are the parties that carry it out or whoever knows one of the two private keys. One of the keys of CryptoNote is its implementation of the concept of ring signature [144], which makes it possible to specify a set of possible signers without revealing who of them actually produced the signature.

Another possible solution for preserving privacy is the use of homomorphic encryption [181], [182]. Such a kind of encryption allows third-party IoT services to process a transaction without revealing the unencrypted data to those services. Several researchers have suggested variations on the Bitcoin protocol to make use of homomorphic commitments [183], [184].

Finally, note that part of the mechanisms previously mentioned require a relevant number of computational resources, so its applicability to resource-constrained IoT devices is currently limited.

B. SECURITY

Traditionally, three requirements have to be fulfilled by an information system in order to guarantee its security:

- Confidentiality. The most sensitive information should be protected from unauthorized accesses.
- Integrity. It guarantees that data are not altered or deleted by unauthorized parties. It is also usually added that, if an authorized party damages the information, it should be possible to undo the changes.
- Availability. Data can be accessed when needed.

Regarding confidentiality, the part related to the transaction data is associated with their privacy, which has been already analyzed in the previous subsection. With respect to the infrastructure that supports the stored data, it can be stated that current IoT applications tend to centralize communications in a server, in a farm of servers or in a cloud. Such an approach is valid as long as the administrators of the centralized infrastructure are trusted and while the system remains robust against attacks [185], [186] and internal leaks. In contrast, blockchain technologies are characterized by being decentralized, so, although one node is compromised, the global system should keep on working.

For an individual user, the key for maintaining confidentiality is a good management of his/her private keys, since it is what an attacker needs in conjunction with the public key to impersonate someone or steal something from him/her. An interesting initiative related to this topic is CONIKS [187], a key management system created to liberate users from encryption key management. In such a system the user first has to ask for a public key to a provider, which only requires a user name to register in the CONIKS system. When a user wants to send a message to another user, his/her CONIKS client looks for the counterparty's key in the key directory. In order to avoid key tampering from the service provider (which might become compromised), before sending any message, two verifications are performed: it is checked that the public key of the receiver is the one used by other clients when communicating with the same user, and that such a key has not changed unexpectedly over time. Similar solutions have been proposed for IoT devices, making use of blockchain technology to strengthen their identity and access management, since blockchains provide a defense against IP spoofing and forgery attacks [59].

Certificates are also essential when guaranteeing security on the Internet. Therefore, certificate authorities that make use of a public-key infrastructure have to provide trust to third-parties. However, such authorities have proven to fail in certain occasions [188], then having to invalidate certificates previously issued. Some recent initiatives are aimed at fixing certain structural flaws found in the SSL certificate system. Specifically, Google's Certificate Transparency [189] provides a framework for monitoring and auditing SSL certificates in almost real time. The solution uses a distributed system based on Merkle hash trees that allows third-parties to audit and verify whether a certificate is valid.

With respect to integrity, it must be indicated that the foundations of a blockchain are designed to store information that cannot be altered (or that it is very costly to do it) once it is stored. Nonetheless, note that in the past there were certain situations when this principle was ignored. For instance, in 2014, in an event that it is still to be clarified, the currency exchange platform MintPal notified its users that a hacker had stolen almost 8 million Vericoins, what was about 30% of the total coins of such a platform. To prevent the loss of investor funds and the fact that an actor would control 30% of the coin's proof-of-stake network capacity, the Vericoin developers decided to hard fork the blockchain, reversing the damage (a hard fork is a permanent divergence from the previous version of the blockchain). Therefore, although many information sources indicate that blockchains are a permanent storage for data that cannot be altered, it is actually not true in practice for preserving integrity in very exceptional cases. In IoT applications, data integrity is also essential and it is usually provided by third-parties. To avoid such a dependence, in [190] it is proposed a data integrity service framework for cloud-based IoT applications that makes use of blockchain technology, thus eliminating the need for trusting such third-parties.

The third characteristic of security is availability, but it is actually the most straightforward to be fulfilled by blockchains, since they are conceived by design to be distributed systems, what allows them to keep on working even when some nodes are under attack. Nevertheless, availability can be compromised through other types of attacks.

The most feared attack is a 51-percent attack (also called majority attack), where a single miner can control the whole blockchain and perform transactions at wish. In this situation, data are available, but the availability for performing transactions can be blocked by the attacker that controls the blockchain. Obviously, this kind of attack also affects data integrity.

C. ENERGY EFFICIENCY

IoT end-nodes usually make use of resource-constrained hardware that is powered by batteries. Therefore, energy efficiency is key to enable a long-lasting node deployment. However, many blockchains are characterized by being power-hungry. In such cases most of the consumption is due to two factors:

- Mining. Blockchains like Bitcoin make use of massive amounts of electricity due to the mining process, which involves a consensus algorithm (PoW) that consists in a sort of brute force search for a hash.
- P2P communications. P2P communications require edge devices that have to be powered on continuously, which could lead to waste energy [191], [192]. Some researchers proposed energy efficient protocols for P2P networks [193]–[195], but the issue still has to be studied further for the specific case of IoT networks.

Regarding mining, some authors suggested that the power consumed by proofs of work could be used for something useful while providing at the same time the required PoW [196]. Obtaining such proofs should have certain degree of difficulty, while its verification should be really fast. Some initiatives based on blockchains, like Gridcoin [197], reward volunteer scientific research computing with coins (although, as a consensus algorithm, Gridcoin uses PoS). Another interesting example is Primecoin [198], whose PoW mechanism looks for chains of prime numbers. Thus, a massive infrastructure like the one involved in IoT could also be harnessed to solve problems while making use of a blockchain.

Proof-of-Space (PoS) (also known as Proof-of-Capacity (PoC)) has also been suggested as a greener alternative to PoW [199]. PoS systems require users to show a legitimate interest in a specific service by allocating certain amount of memory or disk. This mechanism has already been implemented by cryptocurrencies like Burst-coin [200]. Other consensus methods have been proposed to reduce energy consumption respect to PoW, like Proof-of-Stake or Practical Byzantine Fault Tolerance (both described in Section IV-D).

In relation to P2P communications, they are essential for a blockchain to communicate peers and distribute blocks, so the more updates a blockchain receives, the more energy consumption is dedicated to communications. To reduce the number of updates, mini-blokchains [201] may allow IoT nodes to interact directly with a blockchain, since they only keep the latest transactions and lower the computational requirements of a full node.

In terms of hashing algorithms, SHA-256 is the reference due to being the one used by Bitcoin, but new algorithms like Scrypt [202] or X11 [203] are faster and thus can reduce mining energy consumption. Other hashing algorithms have been suggested, like Blake-256 [204], and some blockchains are able to make use of different hashing algorithms (e.g., Myriad [205]), but further analyses should be carried out on the performance and optimization of modern hash functions to be used on IoT devices.

D. THROUGHPUT AND LATENCY

IoT deployments may require a blockchain network able to manage large amounts of transactions per time unit. This is a limitation in certain networks. For instance, Bitcoin's blockchain has a theoretical maximum of 7 transactions per second [78], although it can be increased by processing larger blocks or by modifying certain aspects of the node behavior when accepting transactions [206]. In comparison, other networks are remarkably faster. For instance, VISA network (VisaNet) can handle up to 24,000 transactions per second [207].

Regarding latency, it is important to note that blockchain transactions take some time to be processed. For example, in the case of Bitcoin, block creation times follow a Poisson distribution with a 10-minute mean [18], although, for avoiding double-spend, merchants are recommended to wait for about an hour, since five or six blocks usually need to be added to the chain before the transaction is confirmed. This latency requires only a few seconds in the case of VISA [207].

In relation to the consensus latency, it can be stated that the complexity of the consensus process is more important in terms of latency than individual hashing, but different blockchains, like the one that supports Litecoin [34], have opted for using scrypt, a hashing algorithm that is slightly faster than SHA-256.

E. BLOCKCHAIN SIZE, BANDWIDTH AND INFRASTRUCTURE

Blockchains grow periodically as users store their transactions, what derives into larger initial download times and in having to make use of more powerful miners with larger persistent memories. Blockchain compression techniques should be further studied, but the truth is that most IoT nodes would not be able to handle even a small fraction of a traditional blockchain. Moreover, note that many nodes have to store large amounts of data that are of no interest for them, what can be regarded as a waste of computational resources. This issue could be avoided by using lightweight nodes, which are able to perform transactions on the blockchain, but who do not have to store it. However, this approach requires the existence in the IoT hierarchy of certain powerful nodes that would maintain the blockchain for the resource-constrained nodes, what implies a certain degree of data centralization.

Another alternative would consist in the use of a mini-blockchain [183], [201]. Such a kind of blockchain introduces the use of an account tree, which stores the current state of every user of the blockchain. Thus, only the most recent transaction has to be stored on the blockchain together with the account tree. Therefore, the blockchain only grows when new users are added to the blockchain.

In addition, note that transaction and block size have to be scaled according to the bandwidth limitations of IoT networks: many small transactions would increase the energy consumption associated with communications, while a few large ones may involve big payloads that cannot be handled by some IoT devices.

Regarding the infrastructure, certain elements are required to make the blockchain work properly, including decentralized storage, communication protocols, mining hardware, address management or network administration. Part of these needs are being fulfilled by the industry progressively, creating specific equipment for blockchain applications. For instance, miners have evolved from simple CPU-based systems, to more sophisticated equipment that harnesses the power of Graphics Processing Units (GPUs), Field-Programmable Gate Arrays (FPGAs) or Application-Specific Integrated Circuits (ASICs) [208].

F. OTHER RELEVANT ISSUES

1) ADOPTION RATE

One of the factors that may prevent a wide adoption of a BIoT application is the fact that a blockchain enables pseudo-anonymity (i.e., users or devices are identified by addresses, but they are not clearly linked to them). Governments may demand a strong link between real-world and online identity. Moreover, since IoT transactions can be carried out internationally, it may not be clear who should perform the identification.

In addition, note that the value and security of a blockchain increases with the number of users, also being more difficult to perform the feared 51-percent attacks.

Moreover, note that miner adoption rate also influences the capacity of a network to process transactions, so, in a BIoT deployment, the computational power brought by miners should be high enough to handle the transactions received from the IoT devices.

2) USABILITY

In order to ease the work of developers, blockchain access Application Programming Interface (APIs) should be as user-friendly as possible. The same should be applied to the APIs to manage user accounts.

3) MULTI-CHAIN MANAGEMENT

In some cases, the proliferation of blockchains has derived into the necessity of having to deal with several of them at the same time. This can also happen in an IoT scenario, where, for instance, sensor values may be stored in a private blockchain, while financial transactions among nodes that provide services may be supported by Ethereum's or Bitcoin's blockchain.

4) VERSIONING AND FORKS

Blockchains can be forked for administrative or versioning purposes. Once a blockchain is forked, it is not easy to carry out transactions between both chains.

5) MINING BOYCOTT

Miners end up deciding which transactions are or are not stored in the blockchain, so they are able to censor certain transactions for economic or ideological reasons. This issue can happen when the number of conspiring miners are above 51 percent of the total, so small chains and blockchains that delegate their decisions on a subset of miners are susceptible to this kind of boycotts. Therefore, miners have to be chosen wisely and, when smart contracts have been signed, misbehaviors should be sanctioned.

6) SMART CONTRACT ENFORCEMENT AND AUTONOMY

Legal rules have still to be developed to enforce smart contracts and resolve disputes properly. Some work is being performed for binding real-world contracts with smart contracts [161], but this is still an issue to be further studied.

VI. FURTHER CHALLENGES AND RECOMMENDATIONS

Despite the promising benefits and the brilliant foreseen future of BIoT, there are significant challenges in the development and deployment of existing and planned systems that will need further investigation:

- Complex technical challenges: there are still issues to be addressed regarding the scalability, security, cryptographic development and stability requirements of novel BIoT applications. Moreover, blockchain technologies face design limitations in transaction capacity, in validation protocols or in the implementation of smart contracts. Furthermore, methods to solve the tendency to centralized approaches should be introduced.
- Interoperability and standardization: the adoption of BIoT will require the compromise of all stakeholders in order to achieve full interoperability (i.e., from data to policy interoperability) and integration with legacy systems. The adoption of collaborative implementations and the use of international standards for collaborative trust and information protection (i.e., access control, authentication and authorization) will be needed. For instance, authentication across multiple authorities or organizations requires Federated Identity Management (FIM) [209]. At an international scale, such a FIM currently exists only at a low Level of Assurance (LoA). The required LoA (from LoA 1 to LoA 4), as defined by the ISO/IEC 29115:2013 standard, is mainly based on risks, on the consequences of an authentication error and/or the misuse of credentials, on the resultant impact,

and on their likelihood of occurrence. Thus, higher LoAs will be needed.

- Blockchain infrastructure: it will be needed to create a comprehensive trust framework or infrastructure that can fulfill all the requirements for the use of blockchain in IoT systems. Many state-of-the-art approaches that address issues such as trust depend on inter-domain policies and control. For instance, the governments should set up a blockchain infrastructure to support use cases of public interest.
- Organizational, governance, regulatory and legal aspects: besides technological challenges, shaping the regulatory environment (i.e., decentralized ownership, international jurisdiction) is one the biggest issues to unlock the potential value of BIoT. For instance, it is possible that some developers fake their blockchain performance in order to attract investors driven by the expected profits.
- Rapid field testing: in the near future, different types of blockchains for diverse applications will need to be optimized. Moreover, when users want to combine blockchain with IoT systems, the first step is to figure out which blockchain fits their requirements. Therefore, it is necessary to establish a mechanism to test different blockchains. This approach should be split into two main phases: standardization and testing. In the standardization phase, after a wide understanding of the supply chains, markets, products, and services, all the requirements have to be analyzed and agreed. When a blockchain is created, it should be tested with the agreed criteria to verify if the blockchain works as needed. In the case of the testing phase, different criteria should be evaluated in terms of privacy, security, energy efficiency, throughput, latency, blockchain capacity or usability, among others.

VII. CONCLUSIONS

The transition to a data-driven world is being accelerated by the pace of the technological advances of an Internet-enabled global world, the rise of societal challenges, and an increasing competition for scarce resources. In this ecosystem, blockchain can offer to IoT a platform for distributing trusted information that defy non-collaborative organizational structures.

This review examined the state-of-the art of blockchain technologies and proposed significant scenarios for BIoT applications in fields like healthcare, logistics, smart cities or energy management. These BIoT scenarios face specific technical requirements that differ from implementations involving cryptocurrencies in several aspects like energy efficiency in resource-constrained devices or the need for a specific architecture.

The aim of this work was to evaluate the practical limitations and identify areas for further research. Moreover, it presented a holistic approach to BIoT scenarios with a thorough study of the most relevant aspects involved in an optimized BIoT design, like its architecture, the required cryptographic algorithms or the consensus mechanisms. Furthermore, some recommendations were provided with the objective of giving some guidance to future BIoT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BIoT applications.

We can conclude that, as in any technological innovation, there is no one-size-fits-all solution for a BIoT application. Nevertheless, the adoption of the paradigm opens a wide area of short- and medium-term potential applications that could disrupt the industry and probably, the economy, as we know it today. The global reality is a complex mix of different stakeholders in the IoT ecosystem, therefore it is necessary to reassess the different activities and actors involved in the near-future economy. We can conclude that BIoT is still in its nascent stage, and beyond the earliest BIoT developments and deployments, broader use will require additional technological research advances to address the specific demands, together with the collaboration of organizations and governments.

REFERENCES

[1] *Forecast: The Internet of Things, Worldwide, 2013*, Gartner, Stamford, CA, USA, Nov. 2013.
[2] *White Paper: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021*. San Jose, CA, USA, Mar. 2017.
[3] M. Suárez-Albela, P. Fraga-Lamas, T. M. Fernández-Caramés, A. Dapena, and M. González-López, "Home automation system based on intelligent transducer enablers," *Sensors*, vol. 16, no. 10, no. 1595, pp. 1–26, Sep. 2016.
[4] P. Fraga-Lamas, T. M. Fernández-Caramés, and L. Castedo, "Towards the Internet of smart trains: A review on industrial IoT-connected railways," *Sensors*, vol. 17, no. 6, no. 1457, pp. 1–44, Jun. 2017.
[5] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A review on Internet of Things for defense and public safety," *Sensors*, vol. 16, no. 10, p. 1644, Oct. 2016.
[6] S. J. Barro-Torres, T. M. Fernández-Caramés, H. J. Pérez-Iglesias, and C. J. Escudero, "Real-time personal protective equipment monitoring system," *Comput. Commun.*, vol. 36, no. 1, pp. 42–50, 2012.
[7] Ó. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and M. A. 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.
[8] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.
[9] P. Triantafillou, N. Ntarmos, S. Nikoletseas, and P. Spirakis, "NanoPeer networks and P2P worlds," in *Proc. 3rd Int. Conf. Peer-Peer Comput.*, Linkoping, Sweden, Sep. 2003, pp. 40–46.
[10] M. Ali and Z. A. Uzmi, "CSN: A network protocol for serving dynamic queries in large-scale wireless sensor networks," in *Proc. 2nd Annu. Conf. Commun. Netw. Services Res.*, Fredericton, NB, Canada, May 2004, pp. 165–174.
[11] S. Krco, D. Cleary, and D. Parker, "P2P mobile sensor networks," in *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci.*, Big Island, HI, USA, Jan. 2005, p. 324c.
[12] *Device Democracy: Saving the Future of the Internet of Things*, IBM, New York, NY, USA, 2015.
[13] S. Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations," *IEEE Security Privacy*, vol. 11, no. 4, pp. 54–63, Jul. 2013.
[14] S. Landau, "Highlights from making sense of Snowden, Part II: What's significant in the NSA revelations," *IEEE Security Privacy*, vol. 12, no. 1, pp. 62–64, Jan. 2014.

[15] Markets and Markets; Statista Estimates. *Market for Blockchain Technology Worldwide*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size

[16] *Blockchain Technology Report to the U.S. Federal Advisory Committee on Insurance*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf

[17] *Crypto-Currency Market Capitalizations*. Accessed: Apr. 10, 2018. [Online]. Available: https://coinmarketcap.com/

[18] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Apr. 10, 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[19] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Newton, MA, USA: O'Reilly Media, Jan. 2015.

[20] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *Proc. 2nd Int. Conf. Contemporary Comput. Inf. (IC3I)*, Noida, India, Dec. 2016, pp. 463–467.

[21] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[22] *Ethereum*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.ethereum.org

[23] *Counterparty*. Accessed: Apr. 10, 2018. [Online]. Available: www.counterparty.io

[24] L. Lamport, R. Shostack, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

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

[26] Z. Zheng, S. Xie, H. Dai, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data, Big Data Congr.*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[27] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE Int. Conf. Smart Technol.*, Ohrid, Macedonia, Jul. 2017, pp. 763–768.

[28] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *Proc. IEEE Technol., Eng. Manage. Conf. (TEMSCON)*, Santa Clara, CA, USA, Jun. 2017, pp. 137–141.

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

[30] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016.

[31] S. Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*, 1st ed. Newton, MA, USA: O'Reilly Media, Aug. 2016.

[32] H. X. Mel and D. Baker, *Cryptography Decrypted*. Reading, MA, USA: Addison Wesley, 2001.

[33] N. Ferguson and B. Schneier, *Practical Cryptography*. Hoboken, NJ, USA: Wiley, 2003.

[34] *Litecoins*. Accessed: Apr. 10, 2018. [Online]. Available: https://litecoin.com

[35] *Hyperledger-Fabric*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.hyperledger.org/projects/fabric

[36] *Ripple's*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.ripple.com

[37] *IOTA's*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.iota.org

[38] T. Gui, C. Ma, F. Wang, and D. E. Wilkins, "Survey on swarm intelligence based routing protocols for wireless sensor networks: An extensive study," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Taipei, Taiwan, Mar. 2016, pp. 1944–1949.

[39] J. S. Preden, K. Tammemäe, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015.

[40] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," presented at the 1st edition MCC Workshop Mobile Cloud Comput., Helsinki, Finland, Aug. 2012, pp. 13–16.

[41] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, p. 1978, Aug. 2017.

[42] D. Datla *et al.*, "Wireless distributed computing: A survey of research challenges," *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 144–152, Jan. 2012.

[43] 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 Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2397–2405, Oct. 2017.

[44] R. K. Lomotey, J. Pry, S. Sriramoju, E. Kaku, and R. Deters, "Wearable IoT data architecture," in *Proc. IEEE World Congr. Services (SERVICES)*, Honolulu, HI, USA, Jun. 2017, pp. 44–50.

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

[46] M. Marjani *et al.*, "Big IoT data analytics: Architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[47] A. Back *et al. Enabling Blockchain Innovations With Pegged Sidechains*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.blockstream.com/sidechains.pdf

[48] J. Pérez-Expósito, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "VineSens: An eco-smart decision-support viticulture system," *Sensors*, vol. 17, no. 3, p. 465, Feb. 2017.

[49] T. Swanson. *Consensus-as-a-service: A Brief Report on the Emergence of Permissioned, Distributed Ledger System*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[50] D. Wörner and T. von Bomhard, "When your sensor earns money: Exchanging data for cash with Bitcoin," in *Proc. UbiComp Adjunct*, Seattle, WA, USA, Sep. 2014, pp. 295–298.

[51] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of Bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw.*, Paris, France, Feb. 2015, pp. 184–191.

[52] S. Wilkinson *et al. Storj a Peer-to-Peer Cloud Storage Network*. Accessed: Apr. 10, 2018. [Online]. Available: https://storj.io/storj.pdf

[53] G. Ateniese, M. T. Goodrich, V. Lekakis, C. Papamanthou, E. Paraskevas, and R. Tamassia, "Accountable storage," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, Kanazawa, Japan, Jul. 2017, pp. 623–644.

[54] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using Bitcoin and the blockchain," in *Proc. Int. Conf. Netw. Syst. Secur.*, New York, NY, USA, Nov. 2015, pp. 368–375.

[55] B. Gipp, N. Meuschke, and A. Gernandt, "Decentralized trusted timestamping using the crypto currency Bitcoin," in *Proc. iConf.*, Newport Beach, CA, USA, Mar. 2015, pp. 1–5.

[56] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," in *Proc. Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, Jeju Island, South Korea, Dec. 2017, pp. 1165–1167.

[57] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[58] M. Siddiqi, S. T. All, V. Sivaraman, "Secure lightweight context-driven data logging for bodyworn sensing devices," in *Proc. 5th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Tirgu Mures, Romania, 2017, pp. 1–6.

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

[60] C. Tanas, S. Delgado-Segura, and J. Herrera-Joancomartí, "An integrated reward and reputation mechanism for MCS preserving users' privacy," in *Proc. 10th Int. Workshop Data Privacy Manage., Secur. Assurance*, vol. 9481. New York, NY, USA: Springer-Verlag, 2016, pp. 83–99.

[61] A. Wright and F. P. De. (Mar. 2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Accessed: Apr. 10, 2018. [Online]. Available: https://ssrn.com/abstract=2580664

[62] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[63] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Kunming, China, Jun. 2016, pp. 1–6.

[64] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Bongpyeong, South Korea, Feb. 2017, pp. 464–467.
[65] Y. R. Kafle, K. Mahmud, S. Morsalin, and G. E. Town, "Towards an internet of energy," in *Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON)*, Wollongong, NSW, Australia, Sep./Oct. 2016, pp. 1–6.
[66] O. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "An electricity-price aware open-source smart socket for the internet of energy," *Sensors*, vol. 17, no. 3, p. 643, Mar. 2017.
[67] T. M. Fernández-Caramés, "An intelligent power outlet system for the smart home of the Internet of Things," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 11, p. 214805, 2015, doi: 10.1155/2015/214805.
[68] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[69] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Lisbon, Portugal, May 2017, pp. 772–777.
[70] Z. Shae and J. J. P. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Atlanta, GA, USA, Jun. 2017, pp. 1972–1980.
[71] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, Jul. 2017.
[72] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[73] *Tor Project*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.torproject.org
[74] J. Park and K. Kim, "TM-Coin: Trustworthy management of TCB measurements in IoT," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Kona, HI, USA, Mar. 2017, pp. 654–659.
[75] *ARM TrustZone*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.arm.com/products/security-on-arm/trustzone
[76] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 14th Int. Conf. Smart City*, Sydney, NSW, Australia, Dec. 2016, pp. 1392–1393.
[77] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Rel. Distrib. Syst. (SRDS)*, Hong Kong, Sep. 2017, pp. 253–255.
[78] M. Vukolić. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.vukolic.com/iNetSec_2015.pdf
[79] M. Bahrepour, N. Meratnia, and P. J. M. Havinga, "Sensor fusion-based event detection in wireless sensor networks," in *Proc. 6th Annu. Int. Mobile Ubiquitous Syst. Netw. Services MobiQuitous*, Toronto, ON, Canada, 2009, pp. 1–8.
[80] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *Proc. Int. Conf. Comput., Commun. Signal Process. (ICCCSP)*, Chennai, India, Jan. 2017, pp. 1–4.
[81] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[82] X. Li, H. Wang, Y. Yu, and C. Qian, "An IoT data communication framework for authenticity and integrity," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Pittsburgh, USA, Apr. 2017, pp. 159–170.
[83] T. Yu, X. Wang, and A. Shami, "Recursive principal component analysis-based data outlier detection and sensor data aggregation in IoT systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2207–2216, Dec. 2017.
[84] *Raspberry Pi*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.raspberrypi.org
[85] *BeagleBoards*. Accessed: Apr. 10, 2018. [Online]. Available: http://beagleboard.org
[86] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
[87] C.-F. Liao, S.-W. Bao, and C.-J. Cheng, "On design issues and architectural styles for blockchain-driven IoT services," in *Proc. IEEE Int. Conf. Cons. Electron.-Taiwan (ICCE-TW)*, Taipei, Taiwan, Jun. 2017, pp. 351–352.
[88] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, "ADEPT: An IoT practitioner perspective," IBM Inst. Bus. Value, New York, NY, USA, White Paper, 2015, pp. 1–18.
[89] *Telehash*. Accessed: Apr. 10, 2018. [Online]. Available: http://telehash.org
[90] *BitTorrent*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.bittorrent.com
[91] A. Dorri, S. S. Kanhere, and R. Jurdak. (Aug. 2016). "Blockchain in Internet of Things: Challenges and solutions." [Online]. Available: https://arxiv.org/abs/1608.05187
[92] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Pittsburgh, PA, USA, Apr. 2017, pp. 173–178.
[93] V. Daza, P. R. Di, and I. S. M. Klimek, "CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT," in *Proc. IEEE Int. Conf. Commun.*, Paris, France, May 2017, pp. 1–6.
[94] C. Li and L.-J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Honolulu, HI, USA, Jun. 2017, pp. 33–41.
[95] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Chengdu, China, Dec. 2016, pp. 433–436.
[96] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Nadi, Fiji, Dec. 2016, pp. 116–119.
[97] M. Samaniego and R. Deters, "Internet of smart things-IoST: Using blockchain and CLIPS to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Honolulu, HI, USA, Jun. 2017, pp. 9–16.
[98] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci.*, Bucharest, Romania, May 2017, pp. 667–671.
[99] *IEC 61499 Standard*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.iec61499.de
[100] *Docker*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.docker.com
[101] *Kubernetes*. Accessed: Apr. 10, 2018. [Online]. Available: https://kubernetes.io
[102] P. K. Sharma, M.-Y. Chen, and J.-H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, Sep. 2017.
[103] P. K. Sharma, S. Singh, Y.-S. Jeong, and J.-H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.
[104] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 4, pp. 359–370, Oct./Dec. 2017.
[105] *NIST*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.nist.gov
[106] T. Polk, K. McKay, and S. Chokhani, "Guidelines for the selection and use of transport layer security (TLS) implementations," in *Proc. NIST*, vol. 1, Jun. 2005, pp. 1–30.
[107] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[108] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), vol. 8437, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2014.
[109] T. Kleinjung *et al.*, "Factorization of a 768-bit RSA modulus," in *Proc. 30th Annu. conf. Adv. Cryptol.*, Santa Barbara, CA, USA, Aug. 2010, pp. 333–350.
[110] A. Pellegrini, V. Bertacco, and T. Austin, "Fault-based attack of RSA authentication," in *Proc. Design, Automat., Test Eur. Conf., Exhib.*, Dresden, Germany, Mar. 2010, pp. 855–860.
[111] A. Levi and E. Savas, "Performance evaluation of public-key cryptosystem operations in WTLS protocol," in *Proc. 8th IEEE Symp. Comput. Commun.*, Kemer-Antalya, Turkey, Jun./Jul. 2003, pp. 1245–1250.

[112] M. Habib, T. Mehmood, F. Ullah, and M. Ibrahim, "Performance of WiMAX security algorithm (the comparative study of RSA encryption algorithm with ECC encryption algorithm)," in *Proc. Int. Conf. Comput. Technol. Develop.*, Kota Kinabalu, Malaysia, Nov. 2009, pp. 108–112.

[113] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, Cambridge, MA, USA, Aug. 2004, pp. 119–132.

[114] M. Savari, M. Montazerolzohour, and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," in *Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic*, Kuala Lumpur, Malaysia, Jun. 2012, pp. 49–53.

[115] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, "Comparison of ECC and RSA algorithm in resource constrained devices," in *Proc. Int. Conf. IT Converg. Secur.*, Macau, China, Dec. 2013, pp. 1–3.

[116] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun.*, Kauai Island, HI, USA, Mar. 2005, pp. 324–328.

[117] E. Noroozi, J. Kadivar, and S. H. Shafiee, "Energy analysis for wireless sensor networks," in *Proc. 2nd Int. Conf. Mech. Electron. Eng.*, Kyoto, Japan, Aug. 2010, pp. V2-382–V2-386.

[118] P. R. de Oliveira, V. D. Feltrim, L. A. F. Martimiano, and G. B. M. Zanoni, "Energy consumption analysis of the cryptographic key generation process of RSA and ECC algorithms in embedded systems," *IEEE Latin Amer. Trans.*, vol. 6, no. 6, pp. 1141–1148, Sep. 2014.

[119] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," in *Proc. Int. Conf. Adv. Comput., Commun. Informat.*, Jaipur, India, Sep. 2016, pp. 1725–1729.

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

[121] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *Proc. 11th Fast Softw. Encryption*, vol. 3017. Berlin, Germany: Springer-Verlag, 2004, pp. 371–388.

[122] A. Ometov *et al.*, "Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Sydney, NSW, Australia, Mar. 2016, pp. 1–6.

[123] M. Feldhofer and C. Rechberger, "A case against currently used hash functions in RFID protocols," in *Proc. Move Meaningful Internet Syst. Workshops*, Montpellier, France, Oct./Nov. 2006, pp. 372–381.

[124] B. Degnan, G. Durgin, and S. Maeda, "On the Simon Cipher 4-block key schedule as a hash," in *Proc. IEEE Int. Conf. RFID*, Phoenix, AZ, USA, May 2017, pp. 36–40.

[125] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991.

[126] J. R. Douceur, "The Sybil attack," in *Proc. 1st Int. Workshop Peer-Peer Syst. (IPTPS)*, Cambridge, MA, USA, Mar. 2002, pp. 251–260.

[127] M. Sato and S. Matsuo, "Long-term public blockchain: Resilience against compromise of underlying cryptography," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Vancouver, BC, Canada, Jul./Aug. 2017, pp. 42–49.

[128] A. Takura, S. Ono, and S. Naito, "A secure and trusted time stamping authority," in *Proc. Internet Workshop*, Osaka, Japan, Feb. 1999, pp. 88–93.

[129] *Peercoin*. Accessed: Apr. 10, 2018. [Online]. Available: https://peercoin.net

[130] *DPOS Description on Bitshares*. Accessed: Apr. 10, 2018. [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html

[131] D. Larimer. *Transactions as Proof-of-Stake*. Accessed: Apr. 10, 2018. [Online]. Available: https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

[132] I. L. C. Bentov, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoin's proof of work via proof of stake [extended abstract]," in *Proc. 9th Workshop Economics Netw., Syst. Comput.*, Austin, TX, USA, Jun. 2014, pp. 34–37.

[133] L. Ren. *Proof of Stake Velocity: Building the Social Currency of the Digital Age*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.reddcoin.com/papers/PoSV.pdf

[134] *Reddcoin*. Accessed: Apr. 10, 2018. [Online]. Available: www.reddcoin.com

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

[136] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs, San Francisco, CA, USA, White Paper, 2014.

[137] D. Mazieres. *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[138] C. Copeland and H. Zhong. *Tangaroa: A Byzantine Fault Tolerant Raft*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf

[139] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. USENIX Annu. Techn. Conf.*, Philadelphia, PA, USA, Jun. 2014, pp. 305–320.

[140] C. Cachin, S. Schubert, and M. Vukolić, "Non-determinism in Byzantine fault-tolerant replication," in *Proc. Int. Conf. Principles Distrib. Syst. (OPODIS)*, Madrid, Spain, Dec. 2016, pp. 24:1–24:16.

[141] J. Kwon. *Tendermint: Consensus Without Mining (v0.6)*. [Online]. Available: https://tendermint.com/static/docs/tendermint.pdf

[142] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement.*, Santa Clara, CA, USA, Mar. 2016, pp. 45–59.

[143] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Paris, France, Apr. 2017, pp. 23–26.

[144] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Gold Coast, Australia, Dec. 2001, pp. 552–565.

[145] E. Syta *et al.*, "Keeping authorities' honest or bust' with decentralized witness cosigning," in *Proc. 37th IEEE Symp. Secur. Privacy*, San Jose, CA, USA, May 2016, pp. 526–545.

[146] *PoI Project*. Accessed: Apr. 10, 2018. [Online]. Available: http://proofofindividuality.online

[147] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT zombie armies," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Baltimore, MA, USA, Oct. 2017, pp. 267–272.

[148] H. Chandra, E. Anggadjaja, P. S. Wijaya, and E. Gunawan, "Internet of Things: Over-the-air (OTA) firmware update in lightweight mesh network protocol for smart urban development," in *Proc. 22nd Asia–Pacific Conf. Commun. (APCC)*, Yogyakarta, Indonesia, Aug. 2016, pp. 115–118.

[149] A. Boudguiga *et al.*, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Paris, France, Apr. 2017, pp. 50–58.

[150] R. Meher. *The Internet of Money*. Accessed: Apr. 10, 2018. [Online]. Available: https://docs.google.com/document/d/1Bc-kZXROTeMzG6-AvH7rrTrUy24UwHoEcgiL7ALHMO0A/pub

[151] P. Fraga-Lamas, D. Noceda-Davila, T. M. Fernández-Caramés, M. Díaz-Bouza, and M. Vilar-Montesinos, "Smart pipe system for a shipyard 4.0" *Sensors*, vol. 16, no. 12, p. 2186, Dec. 2016.

[152] 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 *Proc. IEEE Int. Conf. RFID (IEEE RFID)*, Phoenix, AZ, USA, May 2017, pp. 161–166.

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

[154] S. J. Barro-Torres, T. M. Fernández-Caramés, M. González-López, and C. J. Escudero-Cascón, "Maritime freight container management system using RFID" in *Proc. 3rd Int. EURASIP Workshop RFID Technol.*, La Manga del Mar Menor, Spain, Sep. 2010, pp. 20–27.

[155] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications," *Sensors*, vol. 18, no. 1, p. 57, Dec. 2017.

[156] P. Fraga-Lamas, L. Castedo-Ribas, A. Morales-Méndez, and J. M. Camas-Albar, "Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN," in *Proc. Int. Conf. Military Commun. Inf. Syst. (ICMCIS)*, Brussels, Belgium, May 2016, pp. 1–8.

[157] P. Fraga-Lamas, J. Rodríguez-Piñeiro, J. A. García-Naya, and L. Castedo, "Unleashing the potential of LTE for next generation railway communications," in *Proc. 8th Int. Workshop Commun. Technol. Veh. (Nets4Cars/Nets4Trains/Nets4Aircraft)*, vol. 9066. Sousse, Tunisia, May 2015, pp. 153–164.
[158] P. Fraga-Lamas, "Enabling technologies and cyber-physical systems for mission-critical scenarios," Ph.D. dissertation, Dept. Electrónica Sistemas, Univ. A Coruña, A Coruña, Spain, 2017.
[159] S. Meiklejohn *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names," *Commun. ACM*, vol. 59, no. 4, pp. 86–93, Apr. 2016.
[160] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *Proc. APWG eCrime Res. Summit*, San Francisco, CA, USA, Sep. 2013, pp. 1–14.
[161] N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," in *Proc. Int. Conf. Internet Things Global Community (IoTGC)*, Funchal, Portugal, Jul. 2017, pp. 1–7.
[162] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[163] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement. (IoTDI)*, Berlin, Germany, Apr. 2016, pp. 13–24.
[164] P. Fraga-Lamas and T. M. Fernández-Caramés, "Reverse engineering the communications protocol of an RFID public transportation card," in *Proc. IEEE Int. Conf. RFID (IEEE RFID)*, Phoenix, AZ, USA, May 2017, pp. 30–35.
[165] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications," *Sensors*, vol. 17, no. 1, p. 28, Dec. 2016.
[166] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "A methodology for evaluating security in commercial RFID systems, radio frequency identification," in *Radio Frequency Identification Tales Pimenta*, 1st ed., P. C. Crepaldi and T. C. Pimenta, Eds. Rijeka, Croatia: InTech, 2017.
[167] Z. Li and T. Braun, "Passively track WiFi users with an enhanced particle filter using power-based ranging," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7305–7318, Nov. 2017.
[168] C. Luo, L. Cheng, M. C. Chan, Y. Gu, J. Li, and Z. Ming, "Pallas: Self-bootstrapping fine-grained passive indoor localization using WiFi monitors," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 466–481, Feb. 2017.
[169] *Multichain White Paper*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf
[170] G. Danezis and A. Serjantov, "Statistical disclosure or intersection attacks on anonymity systems," in *Proc. 6th Int. Workshop Inf. Hiding*, Toronto, ON, Canada, May 2004, pp. 293–308.
[171] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.*, Christ Church, Barbados, Mar. 2014, pp. 486–504.
[172] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for Bitcoin," in *Proc. Int. Workshops BITCOIN, WAHC, Wearable*, San Juan, Puerto Rico, Jan. 2015, pp. 112–126.
[173] *Zerocoin*. Accessed: Apr. 10, 2018. [Online]. Available: http://zerocoin.org
[174] *Zerocash*. Accessed: Apr. 10, 2018. [Online]. Available: http://zerocash-project.org
[175] *Zcash*. Accessed: Apr. 10, 2018. [Online]. Available: https://z.cash
[176] M. Schukat and P. Flood, "Zero-knowledge proofs in M2M communication," in *Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Commun. Technol.*, Limerick, Ireland, Jun. 2014, pp. 269–273.
[177] K. Peng, "Attack against a batch zero-knowledge proof system," *IET Inf. Secur.*, vol. 6, no. 1, pp. 1–5, Mar. 2012.
[178] *Bytecoin's*. Accessed: Apr. 10, 2018. [Online]. Available: https://bytecoin.org
[179] *Monero's*. Accessed: Apr. 10, 2018. [Online]. Available: https://getmonero.org
[180] *CryptoNote's*. Accessed: Apr. 10, 2018. [Online]. Available: https://cryptonote.org
[181] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doroz, and B. Sunar, "Practical homomorphic encryption: A survey," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Melbourne, VIC, Australia, Jun. 2014, pp. 2792–2795.
[182] H. Hayouni and M. Hamdi, "Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues," in *Proc. IEEE 13th Int. Conf. Netw., Sens., Control (ICNSC)*, Mexico City, Mexico, Apr. 2016.
[183] B. F. França. (Apr. 2015). *Homomorphic Mini-Blockchain Scheme*. Accessed: Apr. 10, 2018. [Online]. Available: http://cryptonite.info/files/HMBC.pdf
[184] D. Lukianov. (Dec. 2015). *Compact Confidential Transactions for Bitcoin*. Accessed: Apr. 10, 2018. [Online]. Available: http://voxelsoft.com/dev/cct.pdf
[185] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*, Pyeongchang, South Korea, Jan./Feb. 2016.
[186] 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 *Proc. IEEE Conf. Comput. Commun.*, Atlanta, GA, USA, May 2017, pp. 1–9.
[187] *CONIKS*. Accessed: Apr. 10, 2018. [Online]. Available: https://coniks.cs.princeton.edu
[188] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.
[189] *Google's Certificate Transparency*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.certificate-transparency.org
[190] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services*, Honolulu, HI, USA, Jun. 2017, pp. 468–475.
[191] Z. Zhou *et al.*, "EEP2P: An energy-efficient and economy-efficient P2P network protocol," in *Proc. Int. Green Comput. Conf.*, Dallas, TX, USA, Nov. 2014, pp. 1–6.
[192] L. Sharifi, N. Rameshan, F. Freitag, and L. Veiga, "Energy efficiency dilemma: P2P-cloud vs. datacenter," in *Proc. IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, Singapore, Dec. 2014, pp. 611–619.
[193] P. Zhang and B. E. Helvik, "Towards green P2P: Analysis of energy consumption in P2P and approaches to control," in *Proc. Int. Conf. High Perform. Comput., Simulation (HPCS)*, Madrid, Spain, Jul. 2012, pp. 336–342.
[194] S. Miyake and M. Bandai, "Energy-efficient mobile P2P communications based on context awareness," in *Proc. IEEE 27th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Barcelona, Spain, Mar. 2013, pp. 918–923.
[195] C. C. Liao, S. M. Cheng, and M. Domb, "On designing energy efficient Wi-Fi P2P connections for Internet of Things," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.
[196] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan. *Proofs of Useful Work*. Accessed: Apr. 10, 2018. [Online]. Available: https://eprint.iacr.org/2017/203.pdf
[197] *Gridcoin's*. Accessed: Apr. 10, 2018. [Online]. Available: http://gridcoin.us
[198] *Primecoin's*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.primecoin.org
[199] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annu. Cryptol. Conf. Adv.*, Santa Barbara, CA, USA, Aug. 2015, pp. 585–605.
[200] *Burst-Coin*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.burst-coin.org
[201] J. D. Bruce. *The Mini-Blockchain Scheme*. Accessed: Apr. 10, 2018. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/The%20Mini-Blockchain%20Scheme.pdf
[202] *Original Scrypt Function for Tarsnap*. Accessed: Apr. 10, 2018. [Online]. Available: http://www.tarsnap.com/scrypt.html
[203] *X11 Official Documentation for Dash*. Accessed: Apr. 10, 2018. [Online]. Available: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146918/X11
[204] J.-P. Aumasson, L. Henzen, W. Meier, and R. C.-W. Phan. NIST. *SHA-3 Proposal BLAKE*. Accessed: Apr. 10, 2018. [Online]. Available: http://131002.net/blake/
[205] *Myriad*. Accessed: Apr. 10, 2018. [Online]. Available: http://myriadcoin.org
[206] N. T. Courtois, P. Emirdag, and D. A. Nagy, "Could Bitcoin transactions be 100x faster?" in *Proc. 11th Int. Conf. Secur. Cryptogr. (SECRYPT)*, Vienna, Austria, Aug. 2014, pp. 1–6.
[207] *VISA Claims About the Number of Transactions Handled by VisaNet*. Accessed: Apr. 10, 2018. [Online]. Available: https://usa.visa.com/run-your-business/small-business-tools/retail.html

[208] M. B. Taylor, "The evolution of Bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, Sep. 2017.
[209] E. Birrell and F. B. Schneider, "Federated identity management systems: A privacy-based characterization," *IEEE Security Privacy*, vol. 11, no. 5, pp. 36–48, Sep./Oct. 2013.

TIAGO M. FERNÁNDEZ-CARAMÉS (S'08–M'12–SM'15) received the M.Sc. and Ph.D. degrees in computer science from the Universidade da Coruña, Spain, in 2005 and 2011, respectively. Since 2005, he has been a Researcher and a Professor with the Group of Electronic Technology and Communications, Department of Computer Engineering, Universidade da Coruña. His current research interests include Internet of Things systems, radio frequency identification, wireless sensor networks, Industry 4.0, blockchain, and augmented reality.

PAULA FRAGA-LAMAS (M'17) received the M.Sc. degree in computer science from the Universidade da Coruña (UDC) in 2008 and the M.Sc. and Ph.D. degrees from the University of the Basque Country, the University of Cantabria, the University of Zaragoza, the University of Oviedo, and UDC, through the Mobile Network Information and Communication Technologies Joint Program, in 2011 and 2017, respectively. Since 2009, she has been with the Group of Electronic Technology and Communications, Department of Computer Engineering, UDC. She has also been participating in over 20 research projects funded by the regional and national government as well as research and development contracts with private companies. She has co-authored over 30 peer-reviewed indexed journals, international conferences, and book chapters. Her current research interests include wireless communications in mission-critical scenarios, Industry 4.0, Internet of Things, augmented reality, blockchain, radio frequency identification, and cyber-physical systems.