Future Generation Computer Systems 88 (2018) 173–190

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

On blockchain and its integration with IoT. Challenges and opportunities

Ana Reyna *, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz

Department of Languages and Computer Science, University of Málaga, Boulevar Louis Pasteur 35, 29071 Málaga, Spain

HIGHLIGHTS

- Challenges to address the integration of the IoT with blockchain.
- Analysis of blockchain potential benefits for the IoT.
- Blockchain IoT applications and platforms for the development of IoT solutions.
- Possible topologies to that integration.
- Evaluation of blockchain nodes in IoT devices.

ARTICLE INFO

Article history:
Received 21 December 2017
Received in revised form 3 April 2018
Accepted 21 May 2018
Available online 24 May 2018

Keywords:
Internet of Things
Blockchain
Smart contract
Trust

ABSTRACT

In the Internet of Things (IoT) vision, conventional devices become smart and autonomous. This vision is turning into a reality thanks to advances in technology, but there are still challenges to address, particularly in the security domain e.g., data reliability. Taking into account the predicted evolution of the IoT in the coming years, it is necessary to provide confidence in this huge incoming information source. Blockchain has emerged as a key technology that will transform the way in which we share information. Building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IoT among them. Disruptive technologies such as big data and cloud computing have been leveraged by IoT to overcome its limitations since its conception, and we think blockchain will be one of the next ones. This paper focuses on this relationship, investigates challenges in blockchain IoT applications, and surveys the most relevant work in order to analyze how blockchain could potentially improve the IoT.

1. Introduction

The rapid evolution in miniaturization, electronics and wireless communication technologies have contributed to unprecedented advances in our society. This has resulted in an increase in the number of suitable electronic devices for many areas, a reduction in their production costs and a paradigm shift from the real world into the digital world. Therefore, the way in which we interact with each other and with the environment has changed, using current technology to gain a better understanding of the world. The Internet of Things (IoT) has emerged as a set of technologies from Wireless Sensors Networks (WSN) to Radio Frequency Identification (RFID), that provide the capabilities to sense, actuate with and communicate over the Internet [1]. Nowadays, an IoT device can be an electronic device from a wearable to a hardware development platform and the range of applications where it can be used encompass many areas of the society. The IoT plays a central role in turning current cities into smart cities, electrical grids into smart grids and houses into smart homes, and this is only the beginning. According to various research reports, the number of connected devices is predicted to reach anywhere from 20 to 50 billion by 2020 [2] mainly due to the vast number of devices that the IoT can place on the scene.

The IoT visualizes a totally connected world, where things are able to communicate measured data and interact with each other. This makes possible a digital representation of the real world, through which many smart applications in a variety of industries can be developed. These include: Smart homes, Weareables, Smart cities, Healthcare, Automotive, Environment, Smart water, Smart grid, etc. IoT solutions are being deployed in many areas, optimizing production and digitizing industries. IoT applications have very specific characteristics, they generate large volumes of data and require connectivity and power for long periods. This, together

* Corresponding author.
E-mail addresses: reyna@lcc.uma.es (A. Reyna), cmf@lcc.uma.es (C. Martín), hfc@lcc.uma.es (J. Chen), esc@lcc.uma.es (E. Soler), mdr@lcc.uma.es (M. Díaz).

https://doi.org/10.1016/j.future.2018.05.046

with the limitations in memory, computer capacity, networks and limited power supply pose a high number of challenges.

The huge expansion of the IoT has to be supported by standard mechanisms and protocols in order to reduce the existing heterogeneity in the field. This heterogeneity leads to vertical silos and reduces the adoption of the IoT. However, aside from the heterogeneity and integration challenges present in the IoT, the trustworthiness of its data is also an important issue to bear in mind. Nowadays, we trust in the information of financial entities and the government among others, but can we be sure that the information provided by them and by other external entities, such as IoT companies, has not been tampered/altered/falsified in any way? This is a difficult question to answer in centralized architectures. Untrusted entities can alter information according to their own interests, so the information they provide might not be completely reliable. This brings about the need to verify that the information has never been modified.

One way to provide trustworthiness in IoT data is through a distributed service trusted by all its participants that guarantees that the data remains immutable. If all participants have the data and they have the means to verify that the data have not been tampered with since the first definition, trustworthiness can be achieved. Moreover, having a system that guarantees data reliability would allow governments to share and securely transfer information with citizens.

In many areas where an exhaustive traceability of assets during their life cycle is required by regulations, data immutability becomes a key challenge. Concretely, European Union (EU) regulations require food producers to trace and identify all raw materials used in the elaboration of their food products in addition to the final destination of each of them. For example, in the case of a large food company with thousands of manufacturing suppliers and millions of clients, the information needs to be digitized and its processing automated to comply with regulation. One example of strong regulation in terms of traceability is the pork supply, regulated in many countries. In this scenario, in addition to tracing the raw material used in pig feed and treatments and the final destination of the pork, the transportation of the animals between factories must also be registered by law. These scenarios involve many participants, some of them still relying on non-automated information handling methods. In the case of food contamination, which has been an important issue for the world population's health throughout history, information that is lost or difficult to find implies delays in the location of the problem's focus. This can also result in the public's mistrust of the contaminated products and a large decrease in their demand. According to the World Health Organization (WHO), it is estimated that every year around 600 million people in the world suffer illness from eating contaminated food, of which 420,000 die from the same cause [3]. So, missing or inaccessible information can affect food security and customer health. In these kinds of scenarios the IoT has the potential to transform and revolutionize the industry and society, digitizing the knowledge so that it can be queried and controlled in real time. This technology can be used to improve current processes in many areas such as cities, industry, health and transportation.

Although the IoT can facilitate the digitization of the information itself, the reliability of such information is still a key challenge. In this sense, a new technology that was born as the first decentralized cryptocurrency has the potential to offer a solution to the data reliability problem: Bitcoin, which has revolutionized the mechanisms in money transfers. The Bitcoin cryptocurrency, and many of its upcoming variants, can be globally transferred without financial entities and foreign exchanges, with a digital and nontransferable wallet. Bitcoin is supported by a protocol that details the infrastructure responsible for ensuring that the information remains immutable over time. This protocol is known as the blockchain. It has been applied to many other areas, and the information immutability is guaranteed in applications that go beyond the cryptocurrencies. Blockchain has revolutionized trustworthiness of information as well. For instance, this technology has been used in voting systems by government entities, renting and data storage among others [4].

In this paper the current challenges of IoT and blockchain and the potential advantages of their combined use will be analyzed.

Disruptive applications in this area will be highlighted in addition to a review of the available blockchain platforms to address these challenges.

The main contributions of the paper are:

1. Survey on blockchain technology, analyzing its unique features and open challenges.
2. Identification and analysis of the different ways of integrating IoT and blockchain.
3. Study of challenges, potential benefits and open issues of the integration of blockchain and IoT.
4. Study of existing blockchain–IoT platforms and applications.
5. Evaluation and comparison of the performance of different blockchains in an IoT device.

The rest of the paper is organized as follows. Section 2 introduces the blockchain technology and analyzes its main challenges. In Section 3 IoT and blockchain integration is addressed, analyzing the challenges that this integration involves. A state of the art in blockchain platforms for IoT and IoT–blockchain applications is presented in Section 4. Lastly, our conclusions and future work are presented in Section 5.

2. Blockchain

The problem of trust in information systems is extremely complex when no verification nor audit mechanisms are provided, especially when they have to deal with sensitive information, such as economic transactions with virtual currencies. In this context, Satoshi Nakamoto, in 2008 [5] presented two radical concepts that have had a great repercussion. The first of these is Bitcoin, a virtual cryptocurrency that maintains its value without support from any centralized authority or financial entity. Rather, the coin is held collectively and securely by a decentralized P2P network of actors that make up an auditable and verifiable network. The second of the concepts, whose popularity has gone even further than the cryptocurrency itself, is blockchain.

Blockchain is the mechanism that allows transactions to be verified by a group of unreliable actors. It provides a distributed, immutable, transparent, secure and auditable ledger. The blockchain can be consulted openly and fully, allowing access to all transactions that have occurred since the first transaction of the system, and can be verified and collated by any entity at any time. The blockchain protocol structures information in a chain of blocks, where each block stores a set of Bitcoin transactions performed at a given time. Blocks are linked together by a reference to the previous block, forming a chain.

To support and operate with the blockchain, network peers have to provide, the following functionality: routing, storage, wallet services and mining [6]. According to the functions they provide, different types of nodes can be part of the network. Table 1 summarizes the most common node types in the Bitcoin network.

The routing function is necessary to participate in the P2P network, this includes transaction and block propagation. The storage function is responsible for keeping a copy of the chain in the node (the entire chain for full nodes, and only a part of it for light nodes). Wallet services provide security keys that allow users to order transactions, i.e., to operate with their Bitcoins. Finally the mining function is responsible for creating new blocks by solving the proof

Table 1
Bitcoin nodes and functionality.

Wallet	Storage	Mining	Routing	
x	x	x	x	Bitcoin core
	x		x	Full node
	x	x	x	Solo miner
x			x	Light wallet

of work. The nodes that perform the proof of work (or mining) are known as miners, and they receive newly generated bitcoins, and fees, as a reward. The concept of proof of work is one of the keys to enable trustless consensus in blockchain network. The proof of work consists of a computationally intensive task that is necessary for the generation of blocks. This work must be complex to solve and at the same time easily verifiable once completed.

Once a miner completes the proof of work, it publishes the new block in the network and the rest of the network verifies its validity before adding it to the chain. Since the generation of blocks is carried out concurrently in the network, the block chain may temporarily fork in different branches (produced by different miners). This discrepancy is solved by considering that the longest branch of blocks is the one that will be considered as valid. This, together with the intensive nature of the block generation process provides a novel, distributed-trustless-consensus mechanism. It is very computationally expensive for a malicious attacker to modify a block and corrupt the block chain since the rest of the trusted miners would outrun the attacker in the block generation process and therefore the trusted branch of blocks will invalidate the one generated by the attacker. In technical terms, in order for a manipulated block to be successfully added to the chain, it would be necessary to solve the proof of work faster than the rest of the network, which is computationally too expensive — it requires having control of at least 51% of the computing resources in the network. Due to the large computational capacity needed to modify the blockchain, the corruption of its blocks is practically impossible. This means that, even if the participants are not completely honest about the use of Bitcoin, a consensus is always reached in the network as long as most of the network is formed by honest participants. The solution proposed by Nakamoto was a great revolution in the reliability of unreliable actors in decentralized systems. More details about the blockchain architecture can be found in [5,7].

Blockchain has also provided a technology where the concept of smart contract can be materialized. In general terms, a smart contract refers to the computer protocols or programs that allow a contract to be automatically executed/enforced taking into account a set of predefined conditions. For example, smart contracts define the application logic that will be executed whenever a transaction takes place in the exchange of cryptocurrency. In smart contracts, functions and conditions can be defined beyond the exchange of cryptocurrencies, such as the validation of assets in a certain range of transactions with non-monetary elements, which makes it a perfect component to expand blockchain technology to other areas. Ethereum [8] was one of the pioneer blockchains to include smart contracts. Today smart contracts have been included in the majority of existing blockchain implementations, such as Hyperledger [9], a blockchain designed for companies that allows components to be deployed according to the needs of users (smart contracts, services or consultations among others) with the support of large companies such as IBM, JP Morgan, Intel and BBVA.

All of this has contributed to the expansion of blockchain technology to a large number of areas where the features offered by this technology are needed: reliability, immutability and auditability. In fact, blockchain is currently one of the top research topics of recent times, with more than 1.4 billion dollars invested by startups alone in the first 9 months of 2016 according to PwC [10].

2.1. Challenges

Although the key idea of blockchain is simple, its implementation poses a great number of challenges. This section introduces the main ones that its use brings about.

2.1.1. Storage capacity and scalability

Storage capacity and scalability have been deeply questioned in blockchain. In this technology, the chain is always growing, at a rate of 1MB per block every 10 min in Bitcoin, and there are copies stored among nodes in the network. Although only full nodes (a node that can fully validate transactions and blocks) store the full chain, storage requirements are significant. As the size grows, nodes require more and more resources, thus reducing the system's capacity scale. In addition, an oversized chain has negative effects on performance, for instance, it increases synchronization time for new users.

Transaction validation is a key component of the distributed consensus protocol as nodes in the blockchain network are expected to validate each transaction of each block. The number of transactions in a block and the time between blocks, modulate the computational power required and this has a direct effect on transaction confirmation times. Hence, the consensus protocol has a direct effect on the scalability of blockchain networks.

Taking into account the trust model of Bitcoin and its scalability limitations, Bitcoin-NG [11] proposes a new Byzantine-fault-tolerant blockchain protocol which improves the consensus latency with respect to Bitcoin. Litecoin [12] is technically identical to Bitcoin, but features faster transaction confirmation times and improved storage efficiency thanks to the reduction of the block generation time and the proof of work, which is based on scrypt, a memory intensive password-based key derivation function. GHOST [13] is intended to improve the scalability of Bitcoin by changing its chain selection rule. Off-chain solutions [14] are intended to perform transactions off the chain, increasing the bandwidth at the same time as it increases the probability of losing data. Another proposal suggests reducing the propagation delay [15] in the Bitcoin protocol, however it can compromise the security of the network. Rather than increasing the scalability on blockchain, BigchainDB [16] adds blockchain characteristics to a big data distributed database. BigchainDB combines the high throughput and low latency characteristics of big data distributed databases with the immutability and decentralized system of blockchain. Another important development is the Inter Planetary File System (IPFS) [17]. IPFS is a protocol designed to store decentralized and shared files enabling a P2P distributed file system to make the web safer, faster and more open. IPFS is intended to increase the efficiency of the web at the same time as it removes duplication and tracks version history for each file.

2.1.2. Security: weaknesses and threats

The Bitcoin protocol has been thoroughly analyzed [18], and various vulnerabilities and security threats have been discovered.

The most common attack is the 51% attack or majority attack [19].

This attack can occur if a blockchain participant is able to control more than 51% of the mining power. In this situation he/she can control the consensus in the network. The boom and fast evolution of mining pools (with GHash.io4 temporarily reaching 51% of the Bitcoin mining power in 2014), has increased the probability of this attack happening, which in turn could compromise the integrity of Bitcoin. In addition, the authors in [20] discuss the possibility of reaching a majority of mining power through bribery. The solo mining incentive or P2P mining would help alleviate this problem. Many other consensus mechanisms proposed for blockchains are also susceptible to majority attacks, especially those that centralize the consensus among a limited number of users.

The double-spend attack consists in spending the same coin twice [21]. In Bitcoin a transaction should be considered confirmed only after the block where the transaction is stored has a certain depth in the blockchain, typically 5 or 6. This takes between 20 and 40 min on average [22]. There is a large variance in the confirmation time since it depends on many factors. In fast payment scenarios the trader cannot afford this wait. Therefore, in these scenarios, double-spend attacks are still possible.

Similarly, race attacks can work in these scenarios. To carry out this attack the user sends a transaction directly to the merchant, who accepts the transaction too quickly. Then the user sends multiple conflicting transactions to the network transferring the coins of the payment to himself. The second transaction is more likely to be confirmed, and the merchant is cheated. Similarly, the Finney [23] attack is a more sophisticated double spend, since it requires the participation of a miner.

The well-known attacks Denial of Service(DoS), Man in the Middle (MitM) or Sybil can also obstruct the network operation. Most P2P protocols and IoT infrastructures are vulnerable to these kinds of attacks, since they strongly rely on communications. In the eclipse attack [24], attackers can monopolize a node's connections, isolating it from the rest of the network and altering the view of the network for this node.

Code updates and optimization in blockchain networks are usually supported by part of the cryptocurrency community and are intended to improve their underlying protocols. These improvements are known as soft and hard forks in blockchain terminology. On the one hand, soft forks provide an update of the software protocol that recognizes backward-compatibility with the previous blocks. This requires an upgrading of the majority of the miners to the new software. However, upgraded functionality can also be rejected by the majority of the nodes keeping to the old rules. On the other hand, hard forks bring a radical change to the protocol, with no compatibility with previous blocks and transactions. Consequently, all the nodes have to upgrade to the latest update, and nodes with older versions will no longer be accepted. The community can be divided when a hard fork happens, resulting in two different forks of the network. Hard forks can also be canceled if they have not built sufficient consensus like SegWit2x [25]. Noted examples of that division are Ethereum and Ethereum Classic; and Bitcoin, Bitcoin Cash and Bitcoin Gold. The aforementioned hard forks have progressed at the same time as the original networks and nowadays they are competing with each other. Nodes and users have to decide on a version, and the fork continuity will depend on these decisions. Hence forks, especially hard ones, can divide the community into two completely different blockchains and this can represent a risk to the blockchain users.

A common problem of virtual currencies, beyond the controversy surrounding their real value, is the problem of coin loss. If the wallet key is forgotten, there is no mechanism to operate with these coins. It has been estimated that 30% of bitcoins are lost.

Finally, quantum computing could be seen as a threat to Bitcoin, since the computing power of these computers could break the security of digital signatures. Furthermore, technology progresses over time and every day new bugs and security breaches are discovered. These improvements and bugs can compromise public blockchains with encrypted data since blockchain data is immutable.

2.1.3. Anonymity and data privacy

Privacy is not enforced in the Bitcoin protocol by design. A key feature of Bitcoin is its transparency. In blockchain each transaction can be checked, audited and traced from the system's very first transaction. This is indeed an unheard of new level of transparency that doubtlessly helps to build trust. However this transparency has a knock-on effect on privacy, even though there is no direct relationship between wallets and individuals, user anonymity seems to be compromised despite the mechanisms that Bitcoin provides, such as pseudonymous and the use of multiple wallets. In this sense, some effort has been made to provide stronger anonymity features in Bitcoin. On the other hand not just open virtual currencies, but many applications based on public blockchain technology require a higher level of privacy in the chain, specifically those that deal with sensitive data.

Popular attempts to tackle the anonymity problem in Bitcoin are Zerocash [26] and Zerocoin [27] which propose that Bitcoin extensions have completely anonymous transactions, hiding the sender, the receiver and the information itself. Monero [28] uses a ring of signatures to make transactions untraceable, so that they cannot be easily traced back to any given person or computer.

Similarly, transaction mixing services or tumblers, provided by Bitcoin Fog [29] and Bit Laundry can increase the anonymity. These services break up transactions into smaller payments and schedule them to obfuscate transactions for a fee. However, these kinds of services are said to be prone to theft. Likewise, the coin-mixing approach, originally proposed in CoinJoin [30] helps to anonymize Bitcoin. The idea is that users agree on joint payments, so that it can no longer be assumed that transaction inputs are from the same wallet. However the previous negotiation required between users, typically performed by mixing servers, could lack the required anonymity depending on the implementation. Later, this approach inspired Dark Wallet [31], a browser plugin that allows completely private anonymous Bitcoin transactions; Dash [32], known as the first cryptocurrency focused on anonymity and privacy; MixCoin [33], that adds cryptographic accountability mechanisms and randomized mixing fees to increase security; CoinShuffle [34] that proposes a modification of CoinJoin in order to increase security; CoinSwap [35] that proposes a four-transactions mechanism based on the inclusion of intermediaries that receive coins and make the payment with unconnected coins; and Blindcoin [36] that increases the anonymity of the mixing server. In general, these attempts to increase anonymity in Bitcoin typically embrace the idea of maintaining a deregulated Bitcoin, and are therefore usually accused of encouraging illicit activities, such as the acquisition of illegal products on the Darknet or money laundering.

In order to increase privacy, data in the blockchain can be encrypted. Hawk [37] stores encrypted transactions. The Hawk compiler is responsible for translating the generic code written by programmers into cryptographic primitives that enable information anonymity in transactions. The Enigma project [38], in addition to encryption, splits data into unrecognizable chunks and distributes them through the network, in a way that no node ever has access to the data. It uses a decentralized off-chain distributed hash-table (DHT) accessible through the blockchain to store data references.

The problem of privacy in private blockchains can be tackled differently, since by definition they must provide authentication and authorization mechanisms. However, even inside a private blockchain, participants want to preserve the privacy of their data. Quorum [39] for instance, is a private permissioned blockchain based on Ethereum that uses cryptography to limit the visibility of sensitive data and segmentation to increase privacy of data. Multichain [40] integrates user permissions to limit visibility and to introduce controls over which transactions are allowed and which users can mine. Rockchain [41] is also based on Ethereum and follows a data-centric approach, where public calculations can be performed on private data, accumulative results can be obtained preserving data privacy. This approach offers a distributed file system that allows users to manage data privacy through smart contracts in Ethereum. Hyperledger Fabric [9] provides a distributed and scalable ledger focused on enterprise environments. To provide blockchain networks with privacy control, Hyperledger Fabric provides an identity control service and access control lists

through private channels where users can control and restrict the access to their shared information in the network. Thanks to this mechanism, members of the network know each other through their public identities, but they do not have to know the information that it is shared in the network.

Another approach to tackle data privacy is to store sensitive data outside the chain, commonly referred to as the off-chain solution [42]. This kind of solution favors systems that manage large amounts of data, since it would be impractical to store them inside the blockchain. In addition, they are particularly suitable for systems that deal with highly sensitive data that should have a tighter access control, such as health care applications. In this way the public blockchain can be used to store anchor data, so that proof to verify the integrity and time stamps of data is available. Users can verify data without relying on authorities, just by checking the blockchain, and data are safely stored outside. Obviously, these off-chain sources must be fault tolerant and should not introduce bottlenecks or single points of failure. In [43] the authors propose using a Kademlia, a well-known DHT to store key–value pairs (user identities and permissions) to access, control and storage data. In [44] a pointer and a hash to validate the data obtained are stored in the chain. In this way, the data in the chain are links to the private data, and the hash is the mechanism that verifies that the information obtained has not been altered. Access control mechanisms for off-chain sources are provided to ensure that only authorized parties can access the information. The information can therefore be obtained from external sources in a secure and verified way with blockchain.

2.1.4. Smart contracts

In 1993, Nick Szabo defined the smart contract as "A computerized transaction protocol that executes the terms of a contract". One of the key features of a smart contract is that it has a way to enforce or self-execute contractual clauses. Until the emergence of blockchain technology, this was technologically unviable. Blockchain has turned out to be the ideal technology to support smart contracts. In addition, smart contracts have contributed significantly to the momentum of blockchain, moreover this coupling has led to a second generation of blockchains, commonly known as Blockchain 2.0. The combination of automatically executed contracts in a trusted environment without centralized control promises to change the way current business is done.

Basically, the smart contract code is stored on the blockchain, and each contract is identified by a unique address, and for users to operate with it, they just send a transaction to this address. The correct execution of the contract is enforced by the blockchain consensus protocol. Smart contracts introduce a set of advantages such as cost reduction, speed, precision, efficiency, and transparency that have fostered the appearance of many new applications in a wide variety of areas. Although Bitcoin offers a basic scripting language, it has turned out to be insufficient, which has led to the emergence of new blockchain platforms with integrated smart contract functionality.

The most prominent smart contract blockchain platform is Ethereum [8]. Ethereum is a blockchain with a built-in Turing-complete programming language, that allows the definition of smart contracts and decentralized applications. The code in Ethereum's contracts is written in "Ethereum virtual machine code", a low-level, stack-based bytecode language.

Frequently, financial smart contracts require access to data about real-world states and events. This data is provided by the so-called oracles. These entities are crucial for the successful integration of smart contracts within the real world, but they also create more complexity, since authentication, security and trust in oracles have to be provided [45].

The advantages of smart contracts do not come without cost, as they are vulnerable to a series of attacks [46–48] that bring new exciting challenges. Delegating contract execution to computers brings with it some problems, since it makes them vulnerable to technical issues such as hacking, bugs, viruses or communication failures. Bugs in contract coding are especially critical because of the irreversibly and immutable nature of the system. Mechanisms to verify and guarantee the correct operation of smart contracts are necessary for them to be widely and safety adopted by clients and providers. The formal validation of the contract logic, and its correctness are research areas where contributions are expected to be made in the years to come [49].

In addition, real-life contracts usually have clauses or conditions that are not quantifiable. In this sense, there is still a lot of work to be done in order to model the conditions of the contracts in smart contracts, so that they are representable and quantifiable for a machine to execute them. Additionally, efforts to provide tools for users to be able to specify and understand smart contracts are needed [50].

2.1.5. Legal issues

The absence of a central authority, the non-existent minting entity, and therefore the total dearth of censorship in Bitcoin is an attractive and at the same time dangerous peculiarity. Bitcoin users are commonly accused of using the network for fraudulent purposes, and thus the technology is suspected of promoting or facilitating illegal conduct. Bitcoin, as the first decentralized cryptocurrency has generated a lot of dispute [51]. On the one hand, with regard to its value, some experts claim it is a fraud [52] and that it will totally collapse [53], while at the same time others estimate that its value will reach 100.000 dollars in 10 years [54]. The European Central Bank, has warned of its volatility risk but have also admitted its potential as a financial innovation [55]. However, with regard to the lack of governance, many countries are developing new laws in an attempt to regulate the use of virtual currencies (a map of Bitcoin regulation status is available at [56]). This situation creates a lot of uncertainty, and seems to be the reason behind its recent fall [57].

Banks and governments will have their say as to whether or not the currency becomes legal tender. Legal implications in the context of currencies is an important concern, as they can directly and negatively affect blockchain applications based on that currency.

Many private and permissioned blockchain applications have recently emerged. These are blockchains that grant write permissions to a predefined peer or set of peers. This can bring some benefits to authorization and authentication mechanisms, for instance key recovery or transaction redemption, and can also contribute to simplifying the problem of privacy and to reducing transaction latency. In fact, interesting market opportunities have arisen in insurance coverage for Bitcoins that would no longer be necessary if the authorities handled this responsibility. The threat of mining pools controlling the network, together with other vulnerabilities, favors the development of such blockchains, and governments are obviously interested in a regulated and controlled use of this technology in many applications. However, this means that the trustless network will regress to a third-party trust network, losing part of its essence. In addition, this can potentially create bottlenecks if solutions include centralized entities. The features of these blockchains are closer to the features of distributed databases.

On the other hand, the key to increasing confidence in this technology could be the involvement of governments and/or large consortiums of companies in their development. Ongoing initiatives in this direction will be helpful [58,59]. Currently, personal information is distributed among different entities: government, universities, companies and so on. The information is spread across many entities and accessing it is time consuming, even when said entities answer to the same authority, e.g., the government. This leads to obstacles in accessing information in addition to a

lack of a trustworthy service that guarantees the information. A trustworthy and global identity service with the information of each person would be disruptive at the present time. Nevertheless, each country has its own laws and regulations.

Initiatives such as Alastria [60] aim to involve multiple entities in the development of a national regulated blockchain, from public notaries to universities and private companies. They plan to enable a public and legal wallet for each person. Companies can also be part of the network. Therefore, each personal wallet could be a digital proof of possessions, companies where he/she has worked, college degrees and so on. This information could be used in a legal and trustworthy way for many services. For instance, in the case of a job interview, candidates could share their college degrees and work experience information with the interviewers. This information is reliable and verifiable by definition. These initiatives are the key to expanding blockchain inside government institutions, and the first step in creating a common and regulatory framework for blockchain systems. Moreover, this could also facilitate the administrative transactions of the population to obtain their information, the data transfer between countries, the reduction of corrupt information and a seamless integration between population, companies, government and universities. However, this also brings about an easy way to obtain highly private information, so the privacy and security considered in the rest of the paper should necessarily go hand in hand with these initiatives.

2.1.6. Consensus

Consensus mechanisms [61–63] are responsible for the integrity of the information contained in blockchain, while defending against double-spend attacks, and therefore are an essential part of blockchain technology. The final goal is to achieve consensus in a distributed network without central authorities and with participants who do not necessarily trust each other.

The consensus based on the proof of work (PoW), which has worked so successfully in Bitcoin, forces miners to solve a computationally-intensive easily-verifiable task in order to create a new block. Once solved, the solution is published and the new block is added to the chain. The new block is spread across the network and the rest of the participants verify it and append it to its local blockchain copy. This process can simultaneously occur in different parts of the network. This is why the chain is in fact a tree. There are several, valid branches existing simultaneously in the blockchain network. When peers append a new block, they also have to check that the branch is the one with the most accumulated work (difficulty), that is, the longest chain which is assumed to be the valid one. This allows consensus to be achieved quickly. A key drawback is that PoW makes Bitcoin dependent on energy consumption. The aforementioned 51% attack is a potential attack on the Bitcoin protocol. Additionally, the incentives in PoW are unexpectedly promoting centralization as the proliferation of mining pools confirm. This together with the mint reduction, reward diminution and fee increase could compromise the system [64] in the future. Certainly, PoW has certain drawbacks such as high latency, low transaction rates and high energy expenditure that makes it unsuitable for many applications. As stated, the latency, or block frequency of 10 min may also be impractical in many scenarios. Despite this, some platforms do use or have adapted PoW, such as NameCoin, LiteCoin, Ethereum, DogeCoin and Monero. Primecoin, for instance, mitigates the energy loss by proposing useful computationally-intensive tasks, such as the prime numbers search that can have applications alongside.

Not surprisingly many attempts to change PoW have recently been proposed, probably underestimating the complexity that this change implies, nevertheless it is not clear if they expose the security properties in the same way as PoW. The most popular alternative approach to consensus in blockchain is the Proof of Stake (PoS). It is based on the fact that those users who own more coins, are more interested in the survival and the correct functioning of the system, and therefore are the most suitable to carry the responsibility of protecting the system. Basically, the idea behind using PoS is to move the opportunity costs from outside the system to inside the system. The algorithm randomly determines the user responsible for the creation of each block, based on the number of coins he/she owns. A common critique is that this approach does not provide incentives for nodes to vote on the correct block (known as the nothing-at-stake problem). Additionally, it is negative in the sense that it promotes enrichment of the rich. PoS was originally used by Peercoin and later in Nextcoin, Nxt [65], Crave and Ethereum. A variant of PoS is the Delegate PoS (DPoS) of BitShares, Monax, Lisk or Tendermint. In BitShares [66], a number of selected witnesses validate signatures and time stamps of transactions by including them in blocks. The election is performed by voting, and each time a witness successfully produces a block it is rewarded. This approach allows delegates to set the block latency, block size and confirm transactions in just a second.

The Leased Proof of Stake (LPoS) allows users to lease funds to other nodes, so that they are more likely to be selected for block creation, increasing the number of electable participants, and therefore reducing the probability of the network being controlled by a single group of nodes. Rewards are proportionally shared.

The Proof of Burn (PoB) [67] proposes burning coins, that is, sending them to a verifiable unspendable address, in order to publish a new block. Like PoW, PoB, is hard to do and easy to verify, but in contrast requires no energy consumption. In addition, PoB has some economic implications that contribute to a more stable ecosystem.

Nem's [68] approach to consensus, called Proof of Importance (PoI), associates an importance value with each account, in this way building a reputation system in the network. The chance of being chosen to create a block depends on this value, the computation of it also takes into account the number of coins and the number of transactions performed. In other words, productive network activity is also rewarded, not just the amount, promoting the useful behavior of the users.

Other extended variants are the activity test (PoA), a hybrid approach that combines both PoW and PoS, and the Elapsed Time Test (PoET) developed by IBM that uses a random choice of manager to mine each block based on runtimes within reliable execution environments. The Proof of Capacity (PoC) [69], also known as proof of storage or space, uses available hard drive space instead of computing resources. This approach is used in Permacoin, SpaceMint and Burstcoin.

Private blockchains have specific features, since the number of participants is usually lower than public blockchains and are semi-reliable. They are usually registered in the system with a predefined set of permissions. These systems, therefore, require specific consensus mechanisms that fit these characteristics.

Some of these alternative mechanisms are Paxos [70], developed by Lamport and Microsoft based on state machine replication; Chubby [71], based on the former and developed by Google, which is defined as a distributed blocking service. These approaches have the advantage that they are adaptations of formal algorithms, and therefore their features have been formally proved. RAFT [72] which separates key elements of consensus such as choice of leaders, record replication and security, and forces a greater degree of consistency to reduce the number of states that need to be considered. The Practical Byzantine Fault Tolerance (PBFT) algorithm, which is based on state machine replication and replicate voting for consensus on state change, is used in Hyperledger and Multichain. SIEVE [73], treats the blockchain as a black box, executing operations and comparing the output of each replica. If there are divergences between the replicas, the operation

is not validated. Another variant of the PBFT is the Byzantine agreement Federated Byzantine Agreement (FBA). In FBA each participant maintains a list of trusted participants and waits for these participants to agree on a transaction before being considered liquidated. It is used in Ripple [74]. Stellar [75] is another variant that employs the quorum and partial quorum concept. The quorum is a set of nodes, enough to reach an agreement, the partial quorum is a subset of a quorum with the ability to convince another given node about the agreement. HDAC [76] is a system, currently being implemented, which proposes an IoT Contract & M2M Transaction Platform based on Multichain. HDAC is specially tailored to IoT environments. It uses the ePow consensus algorithm whose main goals are to motivate the participation of multiple mining nodes and to prevent excessive energy waste.

Finally, the HC Consensus, proposed in Hydrachain, is based on a list of validators of which no more than one-third are unreliable.

To sum up, consensus mechanisms in public blockchains have been widely proposed but poorly, formally proved. It is mandatory to understand the guarantees they offer and their vulnerabilities prior to using them [77]. In this sense, the research community together with the industry have to work towards the validation of these mechanisms in order to demonstrate their legitimacy. To the contrary, private blockchains have adopted formal well-known solutions, but the limited list of participants in these blockchains also limit the diversity and potential of applications.

3. IoT and blockchain integration

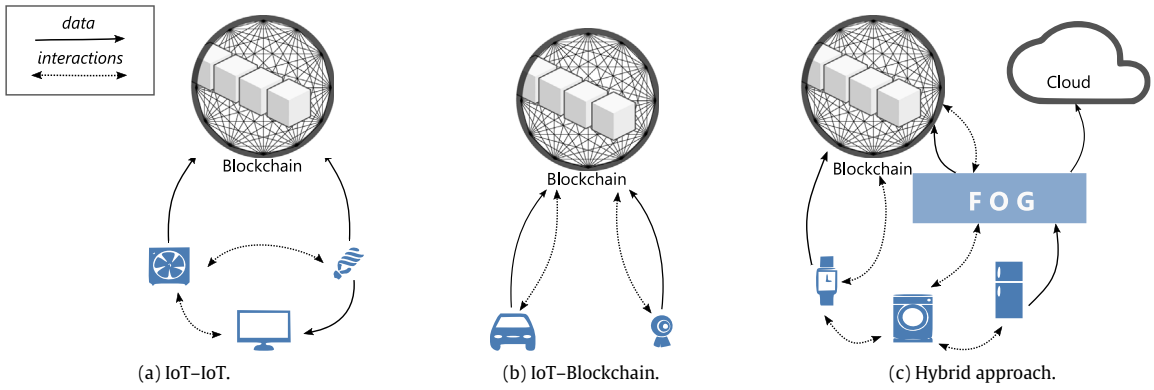
The IoT is transforming and optimizing manual processes to make them part of the digital era, obtaining volumes of data that provides knowledge at unheard of levels. This knowledge is facilitating the development of smart applications such as the improvement of the management and the quality of life of citizens through the digitization of services in the cities. Over the last few years, cloud computing technologies have contributed to providing the IoT with the necessary functionality to analyze and process information and turn it into real-time actions and knowledge [1]. This unprecedented growth in the IoT has opened up new community opportunities such as mechanisms to access and share information. The open data paradigm is the flagship in these initiatives. However, one of the most important vulnerabilities of these initiatives, as has occurred in many scenarios, is the lack of confidence. Centralized architectures like the one used in cloud computing have significantly contributed to the development of IoT. However, regarding data transparency they act as black boxes and network participants do not have a clear vision of where and how the information they provide is going to be used.

The integration of promising technologies like IoT and cloud computing has proven to be invaluable. Likewise, we acknowledge the huge potential of blockchain in revolutionizing the IoT. Blockchain can enrich the IoT by providing a trusted sharing service, where information is reliable and can be traceable. Data sources can be identified at any time and data remains immutable over time, increasing its security. In the cases where the IoT information should be securely shared between many participants this integration would represent a key revolution. For instance, an exhaustive traceability in multiple food products is a key aspect to ensure food safety. Food traceability could require the involvement of many participants: manufacturing, feeding, treatment, distribution, and so on. A data leak in any part of the chain could lead to fraud and slow down the processes of the search for infection which can seriously affect citizen's lives and incur huge economic costs to companies, sectors and countries in the case of a foodborne outbreak [78]. A better control in these areas would increase food safety, improving the data sharing between participants and reducing the search time in the case of a foodborne outbreak, which can save human lives. Moreover, in other areas such as smart cities and smart cars, sharing reliable data could favor the inclusion of new participants in the ecosystems and contribute to improve their services and their adoption. Therefore, the use of blockchain can complement the IoT with reliable and secure information. This has started to be recognized as mentioned in [79], where blockchain technology is identified as the key to solve scalability, privacy, and reliability problems related to the IoT paradigm.

From our point of view IoT can greatly benefit from the functionality provided by blockchain and will help to further develop current IoT technologies. It is worth noting that there are still a great number of research challenges and open issues that have to be studied in order to seamlessly use these two technologies together and this research topic is still in a preliminary stage.

More specifically, improvements that this integration can bring include (but are not limited to):

- **decentralization and scalability**: the shift from a centralized architecture to a P2P distributed one will remove central points of failures and bottlenecks [80]. It will also help prevent scenarios where a few powerful companies control the processing and storage of the information of a huge number of people. Other benefits that come with the decentralization of the architecture are an improvement of the fault tolerance and system scalability. It would reduce the IoT silos, and additionally contribute to improving the IoT scalability.
- **identity**: using a common blockchain system participants are able to identify every single device. Data provided and fed into the system is immutable and uniquely identifies actual data that was provided by a device. Additionally, blockchain can provide trusted distributed authentication and authorization of devices for IoT applications [81]. This would represent an improvement in the IoT field and its participants.
- **autonomy**: blockchain technology empowers next-gen application features, making possible the development of smart autonomous assets and hardware as a service [82,83]. With blockchain, devices are capable of interacting with each other without the involvement of any servers. IoT applications could benefit from this functionality to provide device-agnostic and decoupled-applications.
- **reliability**: IoT information can remain immutable and distributed over time in blockchain [84]. Participants of the system are capable of verifying the authenticity of the data and have the certainty that they have not been tampered with. Moreover, the technology enables sensor data traceability and accountability. Reliability is the key aspect of the blockchain to bring in the IoT.
- **security**: information and communications can be secured if they are stored as transactions of the blockchain [85]. Blockchain can treat device message exchanges as transactions, validated by smart contracts, in this way securing communications between devices. Current secure standard-protocols used in the IoT can be optimized with the application of blockchain [86].
- **market of services**: blockchain can accelerate the creation of an IoT ecosystem of services and data marketplaces, where transactions between peers are possible without authorities. Microservices can be easily deployed and micro-payments can be safety made in a trustless environment [87–89]. It would improve IoT interconnection and the access of IoT data in blockchain.
- **secure code deployment**: taking advantage of blockchain secure-immutable storage, code can be safety and securely pushed into devices [80,90]. Manufacturers can track states



(a) IoT–IoT. (b) IoT–Blockchain. (c) Hybrid approach.

Fig. 1. Blockchain IoT interactions.

and updates with the highest confidence [85]. IoT middlewares can use this functionality to securely update IoT devices.

Another aspect to take into account is related to the IoT interactions, i.e., the communication between the underlying IoT infrastructure. When integrating blockchain, it needs to be decided where these interactions will take place: inside the IoT, a hybrid design involving IoT and blockchain, or through blockchain. Fog computing [91] has also revolutionized the IoT with the inclusion of a new layer between cloud computing and IoT devices and could also facilitate this integration. Below, these alternatives (shown in Fig. 1) are described together with their advantages and disadvantages:

- **IoT–IoT**: this approach could be the fastest one in terms of latency, and security since it can work offline. IoT devices have to be able to communicate with each other, which usually involves discovery and routing mechanisms. Only a part of IoT data is stored in blockchain whereas the IoT interactions take place without using the blockchain (Fig. 1a). This approach would be useful in scenarios with reliable IoT data where the IoT interactions are taking place with low latency.
- **IoT–Blockchain**: in this approach all the interactions go through blockchain, enabling an immutable record of interactions. This approach ensures that all the chosen interactions are traceable as their details can be queried in the blockchain, and moreover it increases the autonomy of IoT devices. IoT applications that intend to trade or rent such as Slock.it can leverage this approach to provide their services. Nevertheless, recording all the interactions in blockchain would involve an increase in bandwidth and data, which is one of the well-known challenges in blockchain (Fig. 1b). On the other hand, all IoT data associated with these transactions should also be stored in blockchain.
- **Hybrid approach**: lastly, a hybrid design where only part of the interactions and data take place in the blockchain and the rest are directly shared between the IoT devices. One of the challenges in this approach is choosing which interactions should go through the blockchain and providing the way to decide this in run time. A perfect orchestration of this approach would be the best way to integrate both technologies since it leverages the benefits of blockchain and the benefits of real-time IoT interactions. In this approach fog computing could come into play and even cloud computing, to complement the limitations of blockchain and the IoT. For example, fog computing involves fewer computationally-limited devices such as gateways and it is a potential place where mining can take place in the same way as other initiatives that use IoT devices [92,93] (Fig. 1c).

In a typical IoT deployment, limited-resource devices are used as end nodes that communicate with a gateway that is responsible for forwarding sensor data to upper layers (cloud or server). When integrating blockchain, if end nodes have to interact with the blockchain, cryptographic functionality could be provided in IoT devices. This is key to realize IoT autonomy, which comes at a cost of a more sophisticated hardware and higher computational expense (in Section 4.1.1 an evaluation of the cost of using blockchain in IoT devices is presented). Integrating gateways in these solutions is also plausible, in the same way as traditional deployments do, however the benefits of using blockchain in this way are fewer. Despite the expansion of blockchain, it would make no sense to use it in many applications, where databases provide enough functionality. Deciding when it is worth using a blockchain will mainly depend on the requirements of the application. For instance, when high performance is required, blockchain alone may not be the right solution, but a hybrid approach could be applied to optimize it. In [94] the authors present a methodology to identify whether a blockchain is useful depending on problem requirements. Next we focus on how this can be technically achieved for IoT devices.

Alliances between well-known companies have started to appear, like the Trusted IoT Alliance [59], to bridge the gap between the IoT and blockchain. Also there are an increasing number of devices with integrated blockchain capabilities available on the market such as [92,93,95]. EthEmbedded [92] enables the installation of Ethereum full nodes on embedded devices such as Raspberry Pi, Beaglebone Black and Odroid. Raspnode [93] and Ethraspbian [96] both support the installation of Bitcoin, Ethereum and Litecoin full nodes on a Raspberry Pi. [95] Antrouter R1-LTC [95] is a Wi-Fi router that also enables mining Litecoin. Therefore, this type of router could be installed in smart homes and be part of a fog computing ecosystem. Raspnode also enables wallet support for Bitcoin and Litecoin. As stated by Raspnode, mining can be done on IoT devices, but it would be useless. Mining has become a specialized task for certain hardware (ASIC chips) and it is useless to try it on IoT devices. That is the main reason why there is little work on mining for IoT devices. There is still a lot of research to be done for enabling a wide integration of IoT devices as blockchain components. Table 2 shows a summary of the surveyed IoT devices to be used as part of blockchain platforms.

Full nodes must store the entire blockchain (currently more than 150 and 46 GB in Bitcoin and Ethereum, respectively) for a full validation of transactions and blocks, thus their deployment can be very limited in IoT devices. As stated, mining would be useless in the IoT due to its specific requirements. The consensus protocol could be relaxed to facilitate the inclusion of IoT devices, however this could compromise the security of the blockchain implementation. This could be used in consortium blockchains where consensus protocols are relaxed. In the deployment of lightweight nodes

Table 2
IoT devices to be used as blockchain components.

Source	IoT device	Mode	Blockchain
EthEmbedded Ethraspbian	Raspberry Pi BeagleBone Black Odroid XU3/XU4 Wandboard Ethcore Parity	Full node	Ethereum
Raspnode	Raspberry Pi	Light node	Bitcoin
		Full node	Litecoin
Bitmain	Antrouter R1-LTC	Miner	

the authenticity of the transactions is validated without having to download the entire blockchain, therefore they can contribute to blockchain and are easy to run and maintain in IoT devices. These nodes can be used in the IoT to be part of the blockchain network, reducing the gap between the two technologies. This always has to be backed up with full nodes to validate transactions and blocks. Nevertheless, many blockchains do not yet provide support for lightweight nodes as is the case of Ethereum, which it is under development. In any case, blockchain could be used as a external service to provide a secure and reliable storage.

One clear alternative to the integration of blockchain with the IoT is the integration between the IoT and cloud computing [1]. This integration has been used in the last few years to overcome the IoT limitations of: processing, storage and access. However, cloud computing usually provides a centralized architecture, which in contrast to blockchain, complicates reliable sharing with many participants. The integration between blockchain and the IoT is intended to address previous limitations in addition to maintaining reliable data. Fog computing aims to distribute and bring the computing closer to end devices, following a distributed approach like blockchain. This can incorporate more powerful devices than the IoT such as gateways and edge nodes, which can then be reused as blockchain components. Therefore, fog computing could ease the integration of the IoT with blockchain.

3.1. Challenges in blockchain–IoT integration

This section studies the main challenges to be addressed when applying blockchain technology to the IoT domain. The integration of blockchain technology with the IoT is not trivial. Blockchain was designed for an Internet scenario with powerful computers, and this is far from the IoT reality. Blockchain transactions are digitally signed, and therefore devices capable of operating with the currency must be equipped with this functionality. Incorporating blockchain into the IoT is challenging. Some of the identified challenges are presented in this section.

3.1.1. Storage capacity and scalability

As stated, storage capacity and scalability of blockchain are still under debate, but in the context of IoT applications the inherent capacity and scalability limitations make these challenges much greater. In this sense, blockchain may appear to be unsuitable for IoT applications, however there are ways in which these limitations could be alleviated or avoided altogether. In the IoT, where devices can generate gigabytes (GBs) of data in real time, this limitation represents a great barrier to its integration with blockchain. It is known that some current blockchain implementations can only process a few transactions per second, so this could be a potential bottleneck for the IoT. Furthermore, blockchain is not designed to store large amounts of data like those produced in the IoT. An integration of these technologies should deal with these challenges.

Currently, a lot of IoT data are stored and only a limited part is useful for extracting knowledge and generating actions. In the literature different techniques to filter, normalize and compress IoT data with the aim of reducing them have been proposed. The IoT involves embedded devices, communication and target services (blockchain, cloud), thus savings in the amount of data that the IoT provides can benefit multiple layers. Data compression can lighten transmission, processing tasks and storage of the high volume of IoT data generated. Normal behaviors do not usually require extra, necessary information, unlike anomalous data.

Last but not least, blockchain, and especially its consensus protocol which causes its bottleneck, could also be adapted to increase the bandwidth and decrease the latency of its transactions thereby enabling a better transition to the IoT demonstrated by the case of Bitcoin-NG [11].

3.1.2. Security

IoT applications have to deal with security problems at different levels, but with an additional complexity due to the lack of performance and high heterogeneity of devices. In addition, the IoT scenario comprises a set of properties that affect security, such as mobility, wireless communication or scale. An exhaustive analysis of security in IoT is beyond the scope of this paper but detailed surveys can be found in [97–100].

The increasing number of attacks on IoT networks, and their serious effects, make it even more necessary to create an IoT with more sophisticated security. Many experts see blockchain as a key technology to provide the much needed security improvements in IoT. However, one of the main challenges in the integration of the IoT with blockchain is the reliability of the data generated by the IoT. Blockchain can ensure that data in the chain are immutable and can identify their transformations, nevertheless when data arrives already corrupted in the blockchain they stay corrupt. Corrupt IoT data can arise from many situations apart from malicious ones. The well-being of the IoT architecture is affected by many factors such as the environment, participants, vandalism and the failure of the devices. Sometimes the devices themselves and their sensors and actuators fail to work properly from the start. This situation cannot be detected until the device in question has been tested, or sometimes it works properly for a while and changes its behavior for some reason (short circuit, disconnection, programmed obsolescence, and so on). In addition to these situations, there are many threats that can affect the IoT such as eavesdropping, denial of service or controlling [98]. For that reason, IoT devices should be thoroughly tested before their integration with blockchain and they should be located and encapsulated in the right place to avoid physical damage, in addition to including techniques to detect device failures as soon as they happen.

These devices are more likely to be hacked since their constraints limit the firmware updates, preventing them from actuating over possible bugs or security breaches. Moreover, it is sometimes difficult to update devices one by one, as in global IoT deployments. Therefore, run-time upgrading and reconfiguration mechanisms should be placed in the IoT to keep it running over time. Initiatives such as GUITAR [101] and REMOWARE [102] enable network and firmware updates in run time and are essential to ensure a secure integration of the IoT with blockchain over time.

The IoT and blockchain integration can also have repercussions on the IoT communications [86]. Currently, IoT application protocols such as CoAP and MQTT make use of other security protocols such as TLS or DTLS to provide secure communications. These secure protocols are complex and heavy in addition to requiring a centralized management and governance of key infrastructure, typically with PKI. In the blockchain network each IoT device would

have its own GUID (Global Unique Identifier) and asymmetric key pair installed once connected to the network. This would simplify current security protocols which usually have to exchange PKI certificates and would allow them to be used in devices with lower capabilities.

One notable IoT project in terms of security with a blockchain adoption is Filament [83]. Filament is a hardware and software solution that provides functionality for Bitcoin-based payments and smart contracts in IoT. Filament devices have embedded cryptoprocessors that support five protocols: Blockname, Telehash and smart contracts to operate, and additionally Pennyback and Bittorrent protocols. The device identity management is done with Blockname, while Telehash, an open source implementation of Kademlia DHT, provides secure encrypted communications, and smart contracts define the way in which a device can be used.

3.1.3. Anonymity and data privacy

Many IoT applications work with confidential data, for instance when the device is linked to a person, such as in the e-health scenario, it is essential to address the problem of data privacy and anonymity. Blockchain is presented as the ideal solution to address identity management in IoT, however as in Bitcoin, there may be applications where anonymity needs to be guaranteed. This is the case of a wearable with the ability to hide the identity of the person when sending personal data, or smart vehicles that safeguard the privacy of the itineraries of users.

The problem of data privacy in transparent and public blockchains has already been discussed, together with some of the existing solutions. However, the problem of data privacy in IoT devices entails more difficulty, since it starts at data collection and extends to the communications and application levels. Securing the device so that data are stored securely and not accessed by people without permission is a challenge since it requires the integration of security cryptographic software into the device. These improvements should take into account the limitation of resources of the devices and the restrictions related to economic viability. Many technologies have been used to secure communications using encryption (IPsec, SSL/TLS, DTLS). IoT device limitations often make it necessary to use less-constrained devices such as gateways to incorporate these security protocols. The use of cryptographic hardware could accelerate cryptographic operations and avoids the overload of complex secure software protocols.

Protection of data and privacy are key challenges for IoT, using blockchain technology the problem of identity management in IoT can be alleviated. Trust is another key feature of the IoT where the integration of blockchain can play a role. In [103] the importance of trust in IoT systems is identified as one of the primary goals to ensure its success. Data integrity techniques are another option to ensure data access at the same time as they avoid overloading blockchain with the huge amount of data generated by the IoT. This can result in public systems, but with an efficient and restricted access control. MuR-DPA [104] provides dynamic data updates and efficient verification though public auditing verification. In [105] the authors ensure the data content through another privacy-preserving public auditing system. For a broad review of integrity verification techniques, refer to [106].

Last but not least, there are laws that regulate data privacy, such as the EU's data protection directives that will need to be revised to cover the new models that the technology makes possible. The adoption of blockchain as a legal platform should address these regulations so as to ensure data privacy following the law.

3.1.4. Smart contracts

Smart contracts have been identified as the killer application of blockchain technology, but as mentioned there are several challenges yet to be tackled. IoT could benefit from the use of smart contracts, however the way they fit into IoT applications is diverse.

From a practical point of view, a contract is a collection of code (functions) and data (states) that reside in a specific blockchain address. Public functions in a contract can be called by devices. Functions can also fire events, applications can listen for them in order to properly react to the event fired. To change the state of the contract, that is, to modify the blockchain, a transaction has to be published in the network. Transactions are signed by senders and have to be accepted by the network.

The IoT has the ability to sense and actuate over the Internet in many areas [1]. In the food traceability example, food packaging would be equipped with sensors with the capability to measure environmental conditions and connect to the blockchain (sign transactions). In the blockchain a contract would provide functions to start shipping, finish shipping and log and query measurements. When measurements exceeded a predefined threshold, an event would be fired. Management applications would be listening to these events, and the shipping company, retailers, manufacturers and clients would be informed. If no events were raised, then the blockchain would guarantee that the shipment was carried out in optimal conditions. Smart contracts would provide a secure and reliable processing engine for the IoT, recording and managing all their interactions. Actions would be the result of a reliable and secure processing. Therefore, smart contracts can securely model the application logic of IoT applications. However, the following challenges should be addressed in that integration.

On the one hand, working with smart contracts requires the use of oracles which are special entities that provide real-world data in a trusted manner. Validating these smart contracts could be compromised since the IoT can be unstable. Moreover, accessing multiple data sources could overload these contracts. Nowadays, smart contracts are distributed and decentralized, but they do not share resources to distribute tasks and address a large amount of computation. In other words, execution of smart contracts is done in just a single node whereas simultaneously the code execution is done by multiple nodes. This distribution is only done for the validation process, instead of using it to distribute tasks. The IoT has leveraged the distributed capabilities of cloud computing and big data to increase its processing power. Since then, data mining techniques have been able to address the IoT data as a whole, enabling a better understanding of the IoT, i.e, the processing power enlarged by cloud computing. Big data has enabled the processing of large amounts of data simultaneously, allowing knowledge to be extracted from large datasets, which was previously very hard to do. In the integration of IoT with blockchain, smart contracts should leverage their distributed nature to enable the processing capabilities provided in other paradigms (big data and cloud computing) and needed in the IoT.

Smart contracts should also take into account the heterogeneity and constraints present in the IoT. Filtering and group mechanisms should be complemented by smart contracts to enable applications to address the IoT depending on the context and requirements. A discovery mechanism could enable device inclusion on the fly, making these applications more powerful. Lastly, actuation mechanisms directly from smart contracts would enable faster reactions with the IoT.

3.1.5. Legal issues

The vision of an unregulated blockchain is part of its essence, and partly responsible for the success of Bitcoin. As seen, blockchain, specifically in the context of virtual currencies, has brought with it a lot of controversy regarding legality. The need, or opportunity, to introduce control elements over the network has come in the form of permissioned, private and consortium blockchains.

The IoT domain is also affected by a country's laws or regulations regarding data privacy, for instance the data protection

directive. Most of these laws are becoming obsolete and need to be revised, especially since the emergence of new disruptive technologies such as blockchain. The development of new laws and standards can ease the certification of security features of devices, and in this way help build the most secure and trusted IoT network. In this sense, laws that deal with information privacy and information handling are still a big challenge to be tackled in IoT and will therefore be an even bigger challenge if used in combination with blockchain.

As stated, the lack of regulation creates disadvantages, because mechanisms for private key retrieval or reset, or transaction reversion are not possible. Some IoT applications envision a global, unique blockchain for devices, however it is unclear if this type of network is intended to be managed by manufacturers or open to users. In any case, it is expected it will require legal regulation. These regulations will have an influence on the future of blockchain and IoT and as such could possibly disrupt the decentralized and free nature of blockchain by introducing a controlling, centralized participant such as a country.

3.1.6. Consensus

In the context of IoT applications, the limited-resource nature of devices makes them unsuitable for taking part in consensus mechanisms, such as PoW, directly. As stated, there are a wide variety of proposals for consensus protocols, although they are, in general, immature and have not been tested enough. Resource requirements depend on the particular type of consensus protocol in the blockchain network. Typically, solutions tend to delegate these tasks to gateways, or any other unconstrained device, capable of providing this functionality. Optionally off-chain solutions, which move information outside the blockchain to reduce the high latency in blockchain, could provide the functionality

Although there are initiatives to incorporate blockchain full nodes into IoT devices [92,93], mining is still a key challenge in the IoT due to its limitations. IoT is mainly composed of resource-constrained devices but globally the IoT has a potentially huge processing power, taking into account that it is expected that the number of devices in it will reach anywhere between 20 and 50 billion by 2020. Research efforts should focus on this field and leverage the distributed nature and global potential of the IoT to adapt the consensus in the IoT.

In Babelchain [107] a novel consensus protocol called Proof of Understanding (PoU) that aims to adapt PoW for IoT applications is proposed. With less energy consumption, the protocol, instead of using miners to solve hash puzzles, proposes translating from different protocols. In this way the effort is more concentrated on useful computation while simultaneously tackling a key problem in IoT communications. Peers in the network instead of agreeing on transaction status, agree on message meaning (format, content and action). Additionally, the blockchain data provide information to learn, like a learning set.

4. Platforms and applications

Recently blockchain platforms and applications have emerged from many diverse areas, due to the advantages that this technology offers. This section surveys the most representative applications and platforms that combine the IoT and blockchain.

4.1. Blockchain platforms for IoT

Blockchain has been identified as a disruptive technology that can strongly affect many industries. The number of platforms is so high and in constant change that it is impossible to analyze them all, in this section we focus on the most popular and most suitable for IoT domains.

Bitcoin was the first cryptocurrency and the first blockchain platform. It provides a mechanism to carry out monetary transactions in a fast, cheap and reliable way, which can be integrated into applications as a secure payment system. In IoT domain, autonomous devices can use Bitcoins to perform micro-payments, working mainly as wallets. In general when the use of blockchain is limited to micro-payments, applications are attached to the currency, which can be a drawback, since depreciation of the coin can negatively affect the application. As stated using smart contracts is a common solution when integrating blockchain with IoT. Bitcoin includes a scripting language that allows specific conditions to be set when carrying out transactions. However, the scripting is quite limited compared with other smart contract platforms.

As mentioned one of the platforms that has had an important impact in recent times is Ethereum [8]. Ethereum was one of the pioneer blockchains in including smart contracts. Ethereum can be described both as a blockchain with a built-in programming language (Solidity), and as a consensus-based virtual machine running globally (Ethereum Virtual Machine EVM). The inclusion of smart contracts moves the blockchain away from currencies and facilitates the integration of this technology in new areas. This along with its active and broad community makes Ethereum the most popular platform for developing applications. Most IoT applications use Ethereum or are compatible with it (see Table 6). The simplest approach is to define a smart contract where devices can publish their measures and policies that react to changes.

Hyperledger [9] has also had a great impact. Hyperledger is an open-source platform on which various projects related to blockchain have been developed, among them Hyperledger Fabric, a blockchain deprived of permissions and without cryptocurrency on which commercial implementations like IBM's Blockchain platform are based. It provides different components for consensus and membership. Distributed application can be developed in the blockchain using general purpose languages. IoT devices can supply data to the blockchain through the IBM Watson IoT Platform, which manages devices and allows data analysis and filtering. IBM's Bluemix platform eases the integration of blockchain technology by offering it as a service. The use of this platform speeds up application prototyping, and several use cases have been developed. There is an ongoing project on food traceability that uses this platform [108].

The Multichain platform allows the creation and deployment of private blockchains. Multichain uses an API that extends the core of the original Bitcoin API with new functionality, allowing the management of portfolios, assets, permissions, transactions, etc. In addition, it offers a command-line tool for interacting with the network, and different clients that can interact through JSON-RPC with the network such as Node.js, Java, C # and Ruby. Multichain is a fork of Bitcoin Core, its source code compiles for 64 bit architectures. In [109] multichain blockchain cluster is deployed on three nodes, one of them an arduino board, as a proof of concept of an IoT–blockchain application.

Litecoin [12], as stated, is technically identical to Bitcoin, but features faster transaction confirmation times and improved storage efficiency thanks to the reduction of the block generation time (from 10 min to 2.5) and the proof of work, which is based on scrypt, a memory intensive password-based key derivation function. This means that the computational requirements of Litecoin nodes are lower, so it is more suitable for IoT.

Lisk [110] offers a blockchain platform in which sub-blockchains or sidechains can be defined with decentralized blockchain applications and a choice of cryptocurrencies to use (e.g. Bitcoin, Ethereum, etc.). Known as the blockchain platform for javascript developers, Lisk also offers support to create and deploy decentralized applications within the platform to be used directly by end users, creating an ecosystem of interoperable blockchain

Table 3
Blockchain platforms for creating blockchain applications.

Platform	Blockchain	Consensus	Crypto currency	Smart contracts
Ethereum	Public and permission-based	PoS	Ether (ETH)	yes
Hyperledger Fabric	Permission-based	PBTF/SIEVE	None	yes
Multichain	Permission-based	PBTF	Multi-currency	yes
Litecoin	Public	Scrypt	litecoins (LTC)	no
Lisk	Public and permission-based	DPoS	LSK	yes
Quorum	Permission-based	Multiple	ETH	yes
HDAC	Permission-based	ePoW,Trust-based	Multiasset	yes

services. The applications developed can use LSK currency or can create custom tokens. Lisk uses Delegated proof of stake consensus. Lisk is working with Chain of Things to examine whether blockchain technology can be effective in establishing security within IoT.

Quorum [39] is a blockchain platform developed to provide the financial services industry with a permissioned implementation of Ethereum with support for transaction and contract privacy. It allows multiple consensus mechanisms and achieves data privacy through cryptography and segmentation. The platform has recently integrated ZeroCash technology to obscure all identifiable information about a transaction. The Quorum platform has been used by Chronicled [111] to create secure links between physical assets and blockchain.

HDAC [76] is an IoT contract and M2M transaction platform based on Blockchain currently under development. The HDAC system uses a combination of public and private blockchains, and quantum random number generation to secure these transactions. The HDAC cryptocurrency-enabled public blockchain can be effectively used with multiple private blockchains. Hdac IoT contract proof of concept will be launched this year.

Table 3 shows a comparison of the blockchain platforms for creating IoT applications surveyed in this section. Smart contracts are present in most platforms, thus enabling application logic beyond cryptocurrency transactions. In the case of a blockchain deployment, there is a dualism among blockchains with and without a cryptocurrency. An established platform with a cryptocurrency like Ethereum can provide the needed infrastructure for a blockchain application. This can be seen as deploying your own cloud infrastructure or using AWS Amazon or Google Cloud Platform. However, in the case of blockchain the distribution is the linchpin of its trustworthiness. On the other hand, using a non-cryptocurrency platform like Hyperledger Fabric requires joining a consortium and infrastructure to start a blockchain. PBTF and PoS are the most used consensuses. Permissions and privacy are in most platforms, therefore consortium and global applications can be created from them.

4.1.1. Evaluation

To test the viability of running blockchain platforms on IoT devices we installed and ran different nodes from different platforms on a Raspberry Pi 3 model B with Raspbian Stretch OS and Linux kernel 4.9.59-v7+. To perform these experiments the device was equipped with an SD card of 128GB (Samsung EVO PLUS MB-MC128GA/EU). Raspberry was connected to the Internet through Ethernet. The different types of nodes were installed and run, connected to the public network. We measured energy consumption and collected some measurements related to task performance for 30 min for each test. The energy consumption was obtained by measuring the current between the power source and the Raspberry Pi, with a Moteino Mega equipped with the INA219 DC current sensor. The results were obtained on a PC through a serial connection with the Moteino Mega. To evaluate the task performance, a background process was run collecting the following task data: percentage of use of cpu and memory, amount of virtual memory required by the task, and the bandwidth consumption (sent and received bytes). This was done with the top.[1] Unix command and the monitor per process network bandwidth usage tool nethogs[2] Table 4 summarizes the results. CPU measurement is 100% for each core, so the maximum for our quad core device is 400%.

Note that the different types of nodes implement different functionalities, and the same types of nodes in different blockchains also perform different tasks. Nodes were connected to public blockchain networks such as Bitcoin, Ethereum and Litecoin to test the device in real working conditions. In addition, when connected to the public network we had no control of the status of the network,i.e., the number of transactions published during each experiment were not the same. Therefore, this evaluation is not intended to be an exhaustive comparison of the performance of the different implementations, but rather to provide an idea of the viability of using blockchain nodes on IoT and to state technical difficulties.

The nodes chosen for the experiment were those with Raspberry Pi compatibility that run in public networks, so the nodes can take part of the routing protocol. To be able to compare the results we also measured the energy consumption of the Raspberry running Raspbian and without any node installed, obtaining 272.09 mA. Raspberry Pi is powered with 5 V.

First, we measured the performance of light nodes. The Bitcoin light node (Electrum implementation), for instance, increased the energy consumption by less than 4%, with respect to the Raspberry base measurement (272.09 mA). Very similar to the values obtained for the Litecoin light node (Electrum implementation) which reached a 5% increase. The Ethereum light node was not tested because it is currently under development. Regarding the task performance, the CPU usage and virtual memory were also quite similar for both light nodes. There was more difference in the use of memory, where Bitcoin consumed 2% additional memory. Bandwidth consumption mainly differed in received bytes, where Litecoin downloaded almost 36 Kb more. Results show that these light nodes run comfortably on the Raspberry Pi, they provide the functionality to make secure transactions, which is enough to benefit from blockchain features, and do not require an excessive amount memory, nor high energy consumption. The next section introduces several solutions where these types of nodes are used in IoT–blockchain applications.

Next the experiments were performed with full nodes: the Ethereum full node (Go implementation), the Bitcoin full node (Bitcoin core implementation) and the Litecoin full node (Litecoin core implementation). As stated, the functionality of the Ethereum full node is not the same as the Bitcoin one. First of all, the different consensus protocols, PoS and PoW, have radically different computational requirements. In addition, full nodes require a synchronization process to download the full chain, during this process the computational requirements are expected to be higher. To evaluate the different consumption requirements, measurements were taken during the synchronization and after it. At the moment

[1] https://linux.die.net/man/1/top.
[2] https://github.com/raboof/nethogs.

Table 4
Blockchain nodes evaluation on Raspberry Pi v3 (Synchronizing (s), after synchronization (as))

	Avg energy (mA)	Avg %CPU	Avg %Mem	Avg VIRT (MB)	Total sent MB	Total received MB
Bitcoin light node	283.45	2.19	9.6	288	0.074	0.068
Litecoin light node	275.53	2.05	7.6	209	0.081	0.104
Ethereum full node (s)	599.72	256.82	85.96	1490	78.9	490
Ethereum full node (as)	371.26	47.39	29.36	1280	15.3	80.3
Bitcoin full node (s)	429.05	55.47	27.55	405	48	912
Litecoin full node (s)	437.62	117.80	19.36	341	17.1	546
Litecoin full node (as)	280.04	7.01	51.7	679	1.22	2.06

of testing Litecoin's blockchain size was 14.03 Gb, 49.47 Gb for the Ethereum chain, and 155.8 Gb for the Bitcoin chain. Note that the full Bitcoin node after the synchronization could not be tested since the current Bitcoin chain size exceeds the memory of our test scenario. The Ethereum synchronization took about 5 days (with several reboots, due to system failures), and Litecoin about 2 days. Moreover, after a couple of days of being close to a full synchronization (fewer than 100 blocks to reach it), we decided to evaluate the Ethereum full node in its current state, 99.99% for a full synchronization. We considered that 99.99% is a good approximation for a full synchronization. The number of new blocks generated and the limited capabilities of the Raspberry Pi for that full node made it difficult to reach a full synchronization.

When compared with light nodes, the additional functionality that full nodes implement, which is mainly the storage, is observed in higher consumption values, both in memory and CPU. Most values obtained after the synchronization were lower than during it, as expected. In the Ethereum full node after synchronizing, the average CPU used was 5 times lower, and average memory use 2.8 times lower, with respect to the values during the synchronization.

The energy consumption, when compared with the Raspberry base measurement (272.09 mA), increased by 120% in the Ethereum node during synchronization, whereas Bitcoin full node does it with 57% and Litecoin with 60%. These values after the synchronization were 36% increase for Ethereum and less than 3% for Litecoin. The use of CPU and memory also rose in full nodes, especially during the synchronization, the highest consumption values were the Ethereum node that reached an average of 256% of CPU usage and 86% of memory. However, after the synchronization those values decreased to 47% and 29% respectively. For Litecoin, CPU usage was 117% during synchronization and only 7% after synchronization. Block validation is CPU intensive, so the CPU usage drop is normal after the chain synchronization. In contrast memory usage in Litecoin increased from 19% to 51% after synchronization. This is probably due to its memory intensive consensus protocol. As expected bandwidth values soared, when compared with light nodes, since they stored the full chain. Whereas for light nodes bandwidth values were in the order of Kb, for full nodes were in the order of Mb. Bitcoin full node received 13 thousand times more bytes than its light node, and the Litecoin full node during synchronization, 5 thousand times more than its light version, and barely 20 times more after synchronization.

There are very few scenarios where it makes sense to use a full node IoT. We have not found any application that uses it in IoT. It could be used in private deployments and for test purposes, but we understand that in final applications there would be other more suitable devices to run these nodes. The evaluation results show that the feasibility of using these nodes on the IoT is very limited. As stated, light nodes are a far better fit for limited resource devices such as those in the IoT.

The most noteworthy problems during the tests were the difficulties in finding up-to-date information about the different node implementations on the pages found for IoT devices, along with the high installation times in some cases and very high synchronization times for full nodes. Moreover, the correct configuration for IoT devices has been necessary in some cases, such as Ethereum, otherwise the full node would collapse the Raspberry. The official documentation and implementations have been very useful for the deployment of the aforementioned nodes.

4.2. Blockchain applications

In finances, there has been a notable emergence of alternative cryptocurrencies (altcoins, 1486 according to coinmarketcap) that have built a new market and have enabled new forms of payment and investment. Examples of them are Ripple [74], Litecoin [12], Nxt [65], Peercoin [112], Bitshares [66], Dogecoin [113], Namecoin [114], Dash [32], and Monero [28]. This new market has also led to the appearance of new applications for payment, exchange and trading infrastructures for these new currencies.

Beyond finances, the distributed and trustless ledger of blockchain has been identified as an ideal solution for traceability systems. What were economic transactions in Bitcoin, have become changes of the plotted objects. In this way the chain stores the objects and all their changes, allowing a complete, open and reliable traceability, only possible through this technology. There are some ongoing projects from prominent companies such as IBM, Unilever, Walmart and Nestle collaborating for food traceability [108] or Renault to track vehicle maintenance history [115].

Identity verification has also become a popular application of the technology, blockchain provides an open trusted distributed ledger that can be used to store identities. This makes the global management of identities possible. In the field of e-government many countries have proposed the use of blockchain technologies for instance: for passports in Dubai [116], e-identity in Estonia [117], Illinois to digitize birth certificates [118] and in India for land registration [119].

Additionally, the integration of smart contracts opens up a world of possibilities for many industries: energy, insurance, mortgages, music royalty payments, real estate, gambling, betting, etc. Cloud storage, education, or e-health are other areas in which blockchain applications have been proposed. Table 5 lists some of these applications in different areas.

4.2.1. IoT–blockchain applications

Although the use of blockchain in the IoT is relatively recent, there are already a large number of proposals where this technology is used in different ways to improve current IoT technology. A summary of some of these proposals is shown in Table 6.

In fact, IoT can join forces with blockchain in many scenarios. Almost all traceability applications can benefit from the inclusion of IoT devices, for instance, sensors that are attached to the product to be traced can provide information during its distribution. Similarly, many applications that digitize the world by providing sensed data can be enriched with blockchain technology. It can help to increase data legitimacy or reliability and moreover provide distributed identity, authentication and authorization mechanisms without the need for central authorities.

Blockchain could be a powerful candidate to make the smart city concept a reality. The concept of the smart city is based on smart IoT devices that can work autonomously. Blockchain can increase the autonomy of devices since it eases interaction and

Table 5
Blockchain applications.

Application	Classification
Ripple [74] Litecoin [12] Nxt [65] Peercoin [112] Dogecoin [113] Namecoin [114] Dash [32] Monero [28]	Cryptocurrency
BitPay [120] Abra [121]	New payment infrastructures
BitNation [122] Onename [123] Keybase [124] ShoCard [125]	Identity verification
Passport management [116] e-identity [117] Birth certificates [118] Land registration [119] Follow my vote [126]	e-government
Tierion [127] Proof of Existence [128] Factom [129] Everledger [130] MIT's digital diploma [131]	Verification of ownership or provenance
Provenance.org [132] SkuChain [133] IBM Food traceability [108] Renault vehicle maintenance history tracking [115]	Product traceability
Robomed [134] Medrec [135]	e-health
Synechron [136]	Energy, insurance and mortgages
Ubitquity [137] Atlant [138]	Real estates
Slock.it [85]	Renting, sharing and selling
DAO.Casino [139] Peerplays [140] Wagerr [141]	Gambling and betting
Storj [142]	Cloud storage
Sony education history [143]	Education
Ujo [144] Resonate [145]	Music royalty payments

coordination by providing a distributed open ledger where devices can query trusted information with reliability. Moreover, the autonomy that blockchain enables, favors the creation of new IoT marketplaces. [85,87–89].

As Table 6 shows, Ethereum is the most popular platform for IoT–blockchain applications. Ethereum provides more features than Bitcoin, the inclusion of smart contracts greatly expands the possible applications.

In LO3 Energy [87] an energy microgrid that uses blockchain has been demonstrated in Brooklyn (USA), southern Germany and South Australia. Microgrids are localized groupings of electricity generation, energy storage, and electrical loads. The project builds a community energy marketplace that creates a decentralized P2P energy network that is coordinated with the broader power grid. It is the first ever energy-blockchain-platform, that allows devices at the grid edge to securely and directly transact for energy sales among microgrid participants. A hybrid device measures a building's energy production in use and sends data to the network.

The project for Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) led by IBM and Samsung [80] aims to promote device autonomy, and to this end they use blockchain technology to ensure code execution on edge devices. ADEPT uses three protocols: Telehash, Bittorrent and Ethereum, for messaging, file sharing and blockchain, respectively. Blockchain technology provides authentication, engagement, contracts and checklists. Their proof of concept consists in smart washing machines that use smart contracts to buy detergent supplies from retailers.

The blockchain framework proposed by Slock.it [85] aims to address security, identity, coordination and privacy over billions of IoT devices. The objective is to build a sharing economy where each IoT asset can be rented securely and quickly without the need for any authority. They are working on a variety of projects, for instance a marketplace to provide a charging infrastructure for electric vehicles, called Blockcharge. This solution uses a smart-plug, a mobile application to activate the plug and control the charge, and the blockchain to pay for the services. They are also working on a smart lock to automate apartment renting.

Aigang [88] is an autonomous insurance network for IoT assets. Aigang has deployed smart contracts over the Ethereum test-bed that issue policies, conduct risk assessment and process claims automatically. They have also created a custom virtual currency (AIX). They offer investment opportunities in different products with different risk levels and potential gains. Smart contracts connect intelligent devices with insurance policies. Through these contracts the devices can order maintenance and insurance payment can be automated. With the inclusion of Oracles to report events, claim handling can be automatically handled.

Table 6
IoT–Blockchain applications.

Application	Classification	Platform
LO3 Energy [87]	Energy microgrid	Ethereum
ADEPT [80]	Smart contracts involving IoT devices	Ethereum
Slock.it [85]	Renting/Selling/Sharing smart objects	Ethereum
Aigang [88]	Insurance network for IoT assets	Ethereum
MyBit [89]	Investment in IoT devices	Ethereum
AeroToken	Sharing airspace market for drone navigation	Ethereum
Chain of things [146]	Identity, security and interoperability	Ethereum
Chronicled [111]	Identity, data provenance and automation	Multiplatform
Modum [84]	Data integrity for the supply chain	Multiplatform
Riddle and Code [147]	Sharing and machine economy	Multiplatform
Blockchain of things [82]	Secure connectivity between IoT devices	Multiplatform

MyBit [89] plans to build an ecosystem of services where IoT assets (from drones to cars) are owned by a group of people, and the revenues are shared. A new financing model and investment opportunity open to anyone. Ethereum smart contracts are used to automate processes: when the IoT devices generate revenue the investors automatically receive a share of the profits proportionate to their ownership stake. A central smart contract is responsible for the control, maintenance and updating of the platform. The platform defines different asset types, and IoT devices are linked to assets, once installed they send and request information through an API. Oracles are used to connect devices to the network.

AeroToken [148] aims to create a real-time navigation and property access authorization system for low-altitude commercial drone services. They provide a solution to drone navigation by voluntarily sharing airspace over properties. This helps to solve the problem of drone operation permission, building a new sharing marketplace. Property owners offer their airspace using smart contracts in the blockchain, and drone service providers pay for a temporary access. The application has been developed using Ethereum smart contracts.

The Chain of Things [146] is a blockchain-enabling IoT research lab that proposes Maru, an integrated blockchain and IoT hardware solution. Blockchain provides devices with universal identity from birth, security and interoperability. Three case studies are presented: Chain of Security, focused on providing security to IoT through blockchain; Chain of Solar, that aims to connect solar panels to the blockchain to store produced energy for a variety of applications and Chain of Shipping, that plans to improve security in the shipping and logistics industry. Data logging devices are used to send data to the network. The proof of concept has been developed over the Ethereum network.

Chronicled [111] has developed several IoT products provided with cryptographic capabilities with the objective of creating the world's most trusted IoT and supply chain ecosystems. Chronicled platform includes a blockchain synchronization server capable of synchronizing with multiple blockchain systems such as Quorum, Ethereum and Hyperledger. Registration and verification of device identity is performed through smart contracts.

The Modum [84] blockchain solution aims to provide data integrity for physical products, focused on improving supply chain processes. The Modum sensors record environmental conditions during shipments. Modum has been designed to work with different platforms. A solution for the distribution of medical products has been developed using Ethereum blockchain. Ethereum smart contracts are used to verify sensor data each time goods change ownership, the contract validates that the transaction meets the customer's standards. The solution integrates sensor tags that collect measurements during transit, a mobile application, used to connect and activate sensors and change ownership, and a dashboard to analyze sensor collected data after shipment reception.

Twin of Things is a solution for securing the ownership and provenance of everyday objects [147] developed by Riddle and Code. The solution combines blockchain and cryptography to generate a hardware-based digital identity for all connected physical objects. Communication and transactions between devices is autonomously and securely performed thanks to blockchain. A highly secure crypto chip enables each device to become a blockchain node. The chip is produced in the form of an adhesive non-removable NFC tag and an Android application is used to carry out a blockchain transaction to register the unique, tamper-proof identity of the chip. Once validated in the network, it can interact with other devices. The solution has been designed to be blockchain agnostic, it can currently work with Ethereum, Bitcoin and BigchainDB blockchains.

The Blockchain of Things [82] provides a secure open communication platform for industrial IoT integration. They propose Catenis, a web service layer for rapid Bitcoin blockchain integration, with end-to-end encryption. It can also be adapted to Ethereum, Hyperledger and other blockchains. In Catenis, each IoT device is represented as a virtual device in a Catenis Hub and Gateways (with increased security). Each virtual device will manage a host of Catenis services for the IoT device.

5. Conclusion and future work

Disruptive technologies always generate great controversy. Although there are many detractors of virtual currencies, it seems undeniable that the technology that sustains them is a significant technological revolution. Blockchain is here to stay. However, modifying the technology without adequately guaranteeing its operation or applying it to scenarios where the cost does not compensate the improvement are risks into which one can fall easily. Therefore, the benefits of applying blockchain to the IoT should be analyzed carefully and taken with caution. This paper has provided an analysis of the main challenges that blockchain and IoT must address in order for them to successfully work together. We have identified the key points where blockchain technology can help improve IoT applications. An evaluation has also been provided to prove the feasibility of using blockchain nodes on IoT devices. Existing platforms and applications have also been examined to complete the study, offering a complete overview of the interaction between blockchain technology and the IoT paradigm.

It is expected that blockchain will revolutionize the IoT. The integration of these two technologies should be addressed, taking into account the challenges identified in this paper. The adoption of regulations is key to the inclusion of blockchain and the IoT as part of government infrastructures. This adoption would speed up the interaction between citizens, governments and companies. Consensus will also play a key role in the inclusion of the IoT as part of the mining processes and distributing even more blockchains. Nevertheless, a dualism between data confidence and facilitating the inclusion of embedded devices could arise. Lastly, beyond the scalability and storage capacity which affect both technologies, research efforts should also be made to ensure the security and

privacy of critical technologies that the IoT and blockchain can become.

One of the main concerns about blockchain, and especially cryptocurrencies, resides in its volatility which has also been exploited by people to take unfair advantage of this situation. The integration of the IoT and blockchain will greatly increase the use of blockchain, in such a way as to establish cryptocurrencies on the same level as current fiduciary money.

Acknowledgments

This work was funded by the Spanish projects TIC-1572 (MIsT-Ica: Critical Infrastructures Monitoring based on Wireless Technologies, Spain) and TIN2014-52034-R (An MDE Framework for the Design and Integration of Critical Infrastructure Management Systems, Spain).

Author Contributions

Jaime Chen, Cristian Martin and Ana Reyna have written this paper and have done the research which supports it. Manuel Díaz has collaborated in the conception, research and design of the paper. Enrique Soler has reviewed the work.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript.

References

[1] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.
[2] J. Rivera, R. van der Meulen, Forecast alert: internet of things — endpoints and associated services, worldwide, 2016, Gartner (2016).
[3] World Health Organization Food safety fact sheet, 2017. Available online: http://www.who.int/mediacentre/factsheets/fs399/en/. (Accessed 1 February 2018).
[4] 17 Blockchain disruptive use cases, 2016. Available online: https://everisnext.com/2016/05/31/blockchain-disruptive-use-cases/. (Accessed 1 February 2018).
[5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. Available online: https://bitcoin.org/bitcoin.pdf. (Accessed 1 February 2018).
[6] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc., 2014.
[7] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. (2017).
[8] V. Buterin, Ethereum white paper, 2013. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (Accessed 2 April 2018).
[9] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: A distributed operating system for permissioned blockchains, 2018, arXiv preprint arXiv:1801.10228.
[10] J. Kennedy, $1.4bn investment in blockchain start-ups in last 9 months, says PwC expert, 2016. Available online: http://linkis.com/Ayjzj. (Accessed 1 February 2018).
[11] I. Eyal, A.E. Gencer, E.G. Sirer, R. Van Renesse, Bitcoin-NG: a scalable blockchain protocol, in: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.
[12] Litecoin, 2011. https://litecoin.org/. (Accessed 4 February 2018).
[13] Y. Sompolinsky, A. Zohar, Accelerating bitcoin's transaction processing, in: Fast Money Grows on Trees, Not Chains. IACR Cryptology EPrint Archive, vol. 881, 2013.
[14] C. Decker, R. Wattenhofer, A fast and scalable payment network with bitcoin duplex micropayment channels, in: Symposium on Self-Stabilizing Systems, Edmonton, AB, Canada, Springer, 2015, pp. 3–18.
[15] C. Stathakopoulou, C. Decker, R. Wattenhofer, A faster Bitcoin network, Tech. rep., ETH, Zurich, Semester Thesis, 2015.
[16] BigchainDB: The scalable blockchain database powering IPDB, 2017. Available online: https://www.bigchaindb.com/. (Accessed 1 February 2018).
[17] Ipfs is the distributed web, 2017. Available online: https://ipfs.io/. (Accessed 1 February 2018).
[18] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) (in press).
[19] I. Eyal, E.G. Sirer, Majority is not enough: bitcoin mining is vulnerable, in: International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer, 2014, pp. 436–454.
[20] J. Bonneau, E.W. Felten, S. Goldfeder, J.A. Kroll, A. Narayanan, Why Buy when You Can Rent? Bribery Attacks on Bitcoin Consensus, Citeseer, 2016.
[21] G. Karame, E. Androulaki, S. Capkun, Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin, IACR Cryptology ePrint Archive 2012 (248), 2012.
[22] Bitcoin average transction confirmation time, 2017. Available online: https://blockchain.info/es/charts/avg-confirmation-time. (Accessed 1 February 2018).
[23] H. Finney, The Finney attack(the Bitcoin Talk forum), 2011. Available online: https://bitcointalk.org/index.php?topic=3441.msg48384. (Accessed 1 February 2018).
[24] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin's peer-to-peer network., in: USENIX Security Symposium, Washington, D.C., USA, USENIX Association, 2015, pp. 129–144.
[25] SegWit2x backers cancel plans for bitcoin hard fork, 2017. Available online: https://techcrunch.com/2017/11/08/segwit2x-backers-cancel-plans-for-bitcoin-hard-fork/. (Accessed 1 February 2018).
[26] E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: decentralized anonymous payments from bitcoin, in: Security and Privacy (SP), 2014 IEEE Symposium on, San Jose, CA, USA, IEEE, 2014, pp. 459–474.
[27] I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: anonymous distributed e-cash from bitcoin, in: Security and Privacy (SP), 2013 IEEE Symposium on, Berkeley, CA, USA, IEEE, 2013, pp. 397–411.
[28] Monero, 2017. https://getmonero.org/. (Accessed 20 October 2017).
[29] Bitcoin Fog, 2017. Available online: http://bitcoinfog.info/. (Accessed 1 February 2018).
[30] G. Maxwell, CoinJoin: bitcoin privacy for the real world, in: Post on Bitcoin Forum, 2013 Available online: https://bitcointalk.org/index.php?topic=279249.msg2983902#msg2983902. (Accessed 1 February 2018).
[31] A. Greenberg, 'Dark Wallet' is about to make Bitcoin money laundering easier than ever, 2014. URL http://www.wired.com/2014/04/dark-wallet.
[32] Dash, 2017. https://www.dash.org/es/. (Accessed 20 October 2017).
[33] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll, E.W. Felten, Mixcoin: anonymity for bitcoin with accountable mixes, in: International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer, 2014, pp. 486–504.
[34] T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: practical decentralized coin mixing for bitcoin, in: European Symposium on Research in Computer Security, Heraklion, Crete, Greece, Springer, 2014, pp. 345–364.
[35] G. Maxwell, CoinSwap: Transaction graph disjoint trustless trading, CoinSwap: Transactiongraphdisjointtrustlesstrading (October 2013), 2013.
[36] L. Valenta, B. Rowan, Blindcoin: blinded, accountable mixes for bitcoin, in: International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer, 2015, pp. 112–126.
[37] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: Security and Privacy (SP), 2016 IEEE Symposium on, San Jose, CA, USA, IEEE, 2016, pp. 839–858.
[38] G. Zyskind, O. Nathan, A. Pentland, Enigma: Decentralized computation platform with guaranteed privacy, 2015, arXiv preprint arXiv:1506.03471..
[39] Quorum Whitepaper, 2016. Available online: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf. (Accessed 1 February 2018).
[40] G. Greenspan, MultiChain Private BlockchainWhite Paper, 2015. Available online: https://www.multichain.com/download/MultiChain-White-Paper.pdf. (Accessed 1 February 2018).
[41] S. Jehan, Rockchain A distributed data intelligence platform, 2017. https://icobazaar.com/static/4dd610d6601de7fe70eb5590b78ed7cd/RockchainWhitePaper.pdf.(Accessed 20 October 2017).
[42] A. Lazarovich, Invisible Ink: Blockchain for Data Privacy (Ph.D. thesis), Massachusetts Institute of Technology, 2015.
[43] G. Zyskind, O. Nathan, et al., Decentralizing privacy: using blockchain to protect personal data, in: Security and Privacy Workshops (SPW), 2015 IEEE, San Jose, CA, USA, IEEE, 2015, pp. 180–184.
[44] D. Houlding, Healthcare Blockchain: What Goes On Chain Stays on Chain, 2017. Available online:https://itpeernetwork.intel.com/healthcare-blockchain-goes-chain-stays-chain/.(Accessed 1 February 2018).
[45] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: an authenticated data feed for smart contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, ACM, 2016, pp. 270–282.
[46] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab,

in: International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, Springer, 2016, pp. 79–94.
[47] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, Uppsala, Sweden, Springer, 2017, pp. 164–186.
[48] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[49] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, ACM, 2016, pp. 254–269.
[50] C.K. Frantz, M. Nowostawski, From institutions to code: towards automated generation of smart contracts, in: Foundations and Applications of Self* Systems, IEEE International Workshops on, Augsburg, Germany, IEEE, 2016, pp. 210–215.
[51] C.K. Elwell, M.M. Murphy, M.V. Seitzinger, Bitcoin: questions, answers, and analysis of legal issues, Congressional Research Service, 2013. Available online: https://fas.org/sgp/crs/misc/R43339.pdf. (Accessed 1 February 2018).
[52] Bitcoin is a fraud that will blow up, says JP Morgan boss, 2017. Available online: https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers. (Accessed 1 February 2018).
[53] Bitcoin could be here for 100 years but it's more likely to 'totally collapse', Nobel laureate says, 2018. Available online: https://www.cnbc.com/2018/01/19/bitcoin-likely-to-totally-collapse-nobel-laureate-robert-shiller-says.html. (Accessed 1 February 2018).
[54] Bitcoin could hit $100,000 in 10 years, says the analyst who correctly called its $2,000 price, 2017. Available online: https://www.cnbc.com/2017/05/31/bitcoin-price-forecast-hit-100000-in-10-years.html. (Accessed 1 February 2018).
[55] E.B. Centralny, Virtual currency schemes—a further analysis, Luty, 2015. Available online: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.(Accessed 1 February 2018).
[56] BitLegal, 2017. Available online: http://bitlegal.io/. (Accessed 1 February 2018).
[57] Regulatory fears hammer bitcoin below $10,000, half its peak, 2017. Available online: https://www.reuters.com/article/uk-global-bitcoin/regulatory-fears-hammer-bitcoin-below-10000-half-its-peak-idUSKBN1F60CG. (Accessed 1 February 2018).
[58] R3, 2017. Available online: https://www.r3.com/. (Accessed 1 February 2018).
[59] Trusted IoT Alliance, 2017. Available online: https://www.trusted-iot.org/. (Accessed 1 February 2018).
[60] Alastria: National Blockchain Ecosystem, 2017. Available online: https://alastria.io/. (Accessed 1 February 2018).
[61] C. Cachin, M. Vukolić, Blockchains Consensus Protocols in the Wild, 2017, arXiv preprint arXiv:1707.01873.
[62] A. Baliga, Understanding Blockchain Consensus Models, 2017. Available online: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf.(Accessed 4 April 2018).
[63] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials 18 (3) (2016) 2084–2123.
[64] N.T. Courtois, On the longest chain rule and programmed self-destruction of crypto currencies, 2014, arXiv preprint arXiv:1405.0534.
[65] Nxt White Paper, 2014. Available online: https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf. (Accessed 2018-03-04).
[66] F. Schuh, D. Larimer, Bitshares 2.0: General overview, 2017. Available online: https://bravenewcoin.com/assets/Whitepapers/bitshares-general.pdf. (Accessed 4 March 2018).
[67] I. Stewart, Proof of burn. bitcoin. it, 2012. Available online: https://en.bitcoin.it/wiki/Proof_of_burn. (Accessed 4 March 2018).
[68] A. Nember, NEM Technical Reference, 2018. Available online: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf. (Accessed 4 March 2018).
[69] A. Miller, A. Juels, E. Shi, B. Parno, J. Katz, Permacoin: repurposing bitcoin work for data preservation, in: Security and Privacy (SP), 2014 IEEE Symposium on, San Jose, CA, USA, IEEE, 2014, pp. 475–490.
[70] L. Lamport, et al., Paxos made simple, ACM Sigact News 32 (4) (2001) 18–25.
[71] M. Burrows, The chubby lock service for loosely-coupled distributed systems, in: Proceedings of the 7th Symposium on Operating Systems Design and Implementation, Seattle, WA, USA, USENIX Association, 2006, pp. 335–350.
[72] D. Ongaro, J.K. Ousterhout, In search of an understandable consensus algorithm., in: USENIX Annual Technical Conference, Philadelphia, PA, USA, USENIX Association, 2014, pp. 305–319.
[73] M. Nabi-Abdolyousefi, M. Mesbahi, Sieve method for consensus-type network tomography, IET Control Theory Appl. 6 (12) (2012) 1926–1932.
[74] Ripple, 2017. https://ripple.com/. (Accessed 20 October 2017).
[75] D. Mazieres, The stellar consensus protocol: a federated model for internet-level consensus, Stellar Development Foundation (2015).
[76] HDAC, 2017. Available online: https://hdac.io/. (Accessed 1 February 2018).
[77] V. Gramoli, From blockchain consensus back to byzantine consensus, Future Gener. Comput. Syst. (2017).
[78] J.C. Buzby, T. Roberts, The economics of enteric infections: human foodborne disease costs, Gastroenterology 136 (6) (2009) 1851–1862.
[79] H. Malviya, How Blockchain will Defend IOT, 2016. Available online: https://ssrn.com/abstract=2883711. (Accessed 1 February 2018).
[80] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.
[81] S. Gan, An IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices using Blockchain, Indian Institute of Technology Kanpur, 2017.
[82] Chain of things, 2017. Available online: https://www.blockchainofthings.com/. (Accessed 1 February 2018).
[83] Filament, 2017. Available online: https://filament.com/. (Accessed 1 February 2018).
[84] modum, 2017. Available online: https://modum.io/. (Accessed 1 February 2018).
[85] G. Prisco, Slock. It to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, 2016. Available online: https://bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/.(Accessed 1 February 2018).
[86] M.A. Khan, K. Salah, Iot security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. (2017).
[87] LO3ENERGY, 2017. Available online: https://lo3energy.com/. (Accessed 1 February 2018).
[88] Aigang, 2017. Available online: https://aigang.network/. (Accessed 1 February 2018).
[89] My bit, 2017. Available online: https://mybit.io/. (Accessed 1 February 2018).
[90] M. Samaniego, R. Deters, Hosting virtual iot resources on edge-hosts with blockchain, in: Computer and Information Technology (CIT), 2016 IEEE International Conference on, Yanuca Island, Fiji, IEEE, 2016, pp. 116–119.
[91] M. Aazam, E.-N. Huh, Fog computing and smart gateway based communication for cloud of things, in: Proceedings of the 2nd International Conference on Future Internet of Things and Cloud, FiCloud-2014, Barcelona, Spain, Aug 2014, pp. 27–29.
[92] Ethembedded, 2017. Available online: http://ethembedded.com/. (Accessed 1 February 2018).
[93] Raspnode, 2017. Available online: http://raspnode.com/. (Accessed 1 February 2018).
[94] K. Wüst, A. Gervais, Do you need a blockchain? IACR Cryptology EPrint Archive 2017 (2017) 375.
[95] Ant Router R1-LTC The WiFi router that mines Litecoin, 2017. Available online: https://shop.bitmain.com/antrouter_r1_ltc_wireless_router_and_asic_litecoin_miner.htm. (Accessed 1 February 2018).
[96] Ethraspbian, 2017. Available online: http://ethraspbian.com/. (Accessed 1 February 2018).
[97] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges, Future Gener. Comput. Syst. 78 (2018) 680–698.
[98] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.
[99] J. Lopez, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the internet of things, Future Gener. Comput. Syst. 75 (2017) 46–57.
[100] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to internet of things security: a position paper, Digital Commun. Netw. (2017). http://dx.doi.org/10.1016/j.dcan.2017.10.006. http://www.sciencedirect.com/science/article/pii/S2352864817302900.
[101] P. Ruckebusch, E. De Poorter, C. Fortuna, I. Moerman, Gitar: generic extension for internet-of-things architectures enabling dynamic updates of network and application modules, Ad Hoc Networks 36 (2016) 127–151.
[102] A. Taherkordi, F. Loiret, R. Rouvoy, F. Eliassen, Optimizing sensor network reprogramming via in situ reconfigurable components, ACM Transactions on Sensor Networks (TOSN) 9 (2) (2013) 14.
[103] C. Fernandez-Gago, F. Moyano, J. Lopez, Modelling trust dynamics in the internet of things, Inform. Sci. 396 (2017) 72–82.
[104] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, J. Chen, Mur-dpa: top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud, IEEE Trans. Comput. 64 (9) (2015) 2609–2622.
[105] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: INFOCOM, 2010 Proceedings IEEE, San Diego, California, USA, Ieee, 2010, pp. 1–9.
[106] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and iot: a big picture, Future Gener. Comput. Syst. 49 (2015) 58–67.
[107] Bitcoin Fog, 2016. Available online: http://www.the-blockchain.com/2016/05/01/babelchain-machine-communication-proof-understanding-new-paper/.(Accessed 1 February 2018).

[108] I.A. Naidu R, Nestle, Unilever, Tyson and others team with IBM on blockchain, Reuters, 2017. http://www.reuters.com/article/us-ibm-retailers-blockchain/nestle-unilever-tyson-and-others-team-with-ibm-on-blockchain-idUSKCN1B21B1.(Accessed 20 October 2017).
[109] M. Samaniego, R. Deters, Internet of smart things-iost: using blockchain and clips to make things autonomous, in: Cognitive Computing (ICCC), 2017 IEEE International Conference on, Honolulu, Hawaii, USA, IEEE, 2017, pp. 9–16.
[110] The Lisk Protocol, 2017. Available online: https://docs.lisk.io/docs/the-lisk-protocol. (Accessed 1 February 2018).
[111] Chronicled, 2017. Available online: https://chronicled.com/. (Accessed 1 February 2018).
[112] S. King, S. Nadal, Peercoin–Secure & Sustainable Cryptocoin, 2012. https://peercoin.net/whitepaper. (Accessed 20 October 2017).
[113] B. Markus, Dogecoin, 2013. http://dogecoin.com/. (Accessed 20 October 2017).
[114] Namecoin, 2014. https://namecoin.org/. (Accessed 20 October 2017).
[115] V. Pradeep, Renault partners with Microsoft for blockchain-based digital car maintenance book, MSPoweruser, 2017. https://mspoweruser.com/renault-partners-microsoft-blockchain-based-digital-car-maintenance-book/. (Accessed 20 October 2017).
[116] M. C, The end of passport gates? dubai to test 'invisible' airport checks using facial recognition, in: The Telegraph, 2017 http://www.telegraph.co.uk/technology/2017/06/13/end-passport-gates-dubai-test-invisible-airport-checks-using/.(Accessed 20 October 2017).
[117] e-identity, 2017. https://e-estonia.com/solutions/e-identity/e-residency/. (Accessed 20 October 2017).
[118] How to get an Illinois Birth Certificate online, 2017. https://vital-records.us/order-an-illinois-birth-certificate/. (Accessed 20 October 2017).
[119] C. R, Indian states look to digitize land deals with blockchain, Reuters, 2017. https://www.reuters.com/article/us-india-landrights-tech/indian-states-look-to-digitize-land-deals-with-blockchain-idUSKBN1AQ1T3. (Accessed 20 October 2017).
[120] Bitpay, 2017. https://bitpay.com/. (Accessed 20 October 2017).
[121] Abra, 2017. https://www.abra.com/. (Accessed 20 October 2017).
[122] Bitnation, 2017. https://bitnation.co/. (Accessed 20 October 2017).
[123] OneName, 2017. https://onename.com/. (Accessed 20 October 2017).
[124] Keybase, 2017. https://keybase.io/. (Accessed 20 October 2017).
[125] ShoCard, 2017. https://shocard.com/. (Accessed 20 October 2017).
[126] Follow my vote, 2017. Available online: https://followmyvote.com/. (Accessed 1 February 2018).
[127] Tierion, 2017. https://tierion.com/. (Accessed 20 October 2017).
[128] Proof of Existence, 2017. https://poex.io/. (Accessed 20 October 2017).
[129] Factom, 2017. https://www.factom.com/. (Accessed 20 October 2017).
[130] Everledger, 2017. https://www.everledger.io/. (Accessed 20 October 2017).
[131] MIT Digital Diploma Pilot Program, 2017. http://web.mit.edu/registrar/records/certs/digital.html. (Accessed 20 October 2017).
[132] Provenance, 2017. https://www.provenance.org/. (Accessed 20 October 2017).
[133] Skuchain, 2017. http://www.skuchain.com/. (Accessed 20 October 2017).
[134] Robomed network, 2017. https://robomed.io/. (Accessed 20 October 2017).
[135] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: using blockchain for medical data access and permission management, in: Open and Big Data (OBD), International Conference on, Vienna, Austria, IEEE, 2016, pp. 25–30.
[136] Synechron, 2017. https://www.synechron.com/finlabs/mortgage-lending. (Accessed 20 October 2017).
[137] Ubitquity, 2017. https://www.ubitquity.io. (Accessed 20 October 2017).
[138] Atlant, 2017. https://atlant.io/. (Accessed 20 October 2017).
[139] DaoCasino, 2017. https://dao.casino/. (Accessed 20 October 2017).
[140] Peerplays, 2017. https://www.peerplays.com/. (Accessed 20 October 2017).
[141] Wagerr, 2017. https://wagerr.com/. (Accessed 20 October 2017).
[142] Storj.io, 2017. https://storj.io/. (Accessed 20 October 2017).
[143] R. J, Sony wants to digitize education records using the blockchain, Techcrunch, 2017. https://techcrunch.com/2017/08/09/sony-education-blockchain/. (Accessed 20 October 2017).
[144] ujo, 2017. https://ujomusic.com/. (Accessed 20 October 2017).
[145] resonate, 2017. https://resonate.is/. (Accessed 20 October 2017).
[146] Chain of things, 2017. Available online: https://www.chainofthings.com/. (Accessed 1 February 2018).
[147] Riddle and Code, 2017. Available online: https://www.riddleandcode.com. (Accessed 1 February 2018).
[148] AeroToken, 2017. Available online: https://aerotoken.com. (Accessed 1 February 2018).

Ana Reyna received her M.S. degree in Computer Engineering from the University of Málaga, in 2005. And a Ph.D. degree in Computer Engineering in 2013. She is currently a research assistant in the Department of Computer Sciences and Languages at the University of Málaga and member of ERTIS (Embedded Real Time Systems) research group. Her research interests are in the areas of peer to peer networks, embedded systems and incentive mechanisms.

Cristian Martin received a M.Sc. in Computer Engineering and a M.Sc. in Software Engineering and Artificial Intelligence from the University of Málaga in 2014 and 2015 respectively. Currently, he is a Ph.D student in the ERTIS research group at the University of Málaga. Previously, he has been working as a software engineer in various technological companies with the RFID technology and software development. His research interests focus on the integration of the Internet of Things with cloud computing, and the integration of the Internet of Things with blockchain.

Jaime Chen earned his M.S. and Ph.D. degree in Computer Engineering from the University of Málaga in 2008 and 2013, respectively. He is working in the areas of Wireless Sensor and Actor Networks, IoT and its applications. He is specially involved in the research field of communication protocols for the IoT. He has been a member of the Software Engineering group of the University of Málaga (GISUM) since 2009. He is currently working as a professor at the University of Málaga.

Enrique Soler received his M.S. and Ph.D. degree in Computer Science from the University of Málaga (UMA) in 1990 and 2001, respectively. From 1995 to 2002, he was Assistant Professor at the Dep. of Languages and Computer Science of the University of Málaga where he is an associate professor since 2002. He has published several papers in the field of high performance computing and simulation of complex systems, such as nuclear power plants. He has also worked in image analysis for the detection of defects in the inspection of industrial components and in the field of quality of food. He is also specialized in the design and Administration of Databases and Data Warehouses.

Manuel Díaz is Full Professor in the Computer Science Department at the University of Málaga and Head of the ERTIS research group. His research interests are in distributed and real time systems, Internet of Things and P2P, especially in the context of middleware platforms and critical systems. He has lead several international research projects on those areas and is also co-founder of the company Software for Critical Systems.