Blockchain for the Internet of Things: Present and Future

Francesco Restuccia, *Member, IEEE*, Salvatore D'Oro, *Member, IEEE*, Salil S. Kanhere, *Senior Member, IEEE,* Tommaso Melodia, *Fellow, IEEE*, and Sajal K. Das, *Fellow, IEEE*

***Abstract*—One of the key challenges to the IoT's success is how to secure and anonymize billions of IoT transactions and devices per day, an issue that still lingers despite significant research efforts over the last few years. On the other hand, technologies based on blockchain algorithms are disrupting today's cryptocurrency markets and showing tremendous potential, since they provide a distributed transaction ledger that cannot be tampered with or controlled by a single entity. Although the blockchain may present itself as a cure-all for the IoT's security and privacy challenges, significant research efforts still need to be put forth to adapt the computation-intensive blockchain algorithms to the stringent energy and processing constraints of today's IoT devices. In this paper, we provide an overview of existing literature on the topic of blockchain for IoT, and present a roadmap of research challenges that will need to be addressed to enable the usage of blockchain technologies in the IoT.**

***Index Terms*—Internet of Things, Research, Challenges, Blockchain, Security, Anonymity, Privacy**

I. Introduction

It is hard to mention a technology that will impact and benefit our lives more than the Internet of Things (IoT). In a few years, cars, kitchen appliances, televisions, smartphones, utility meters, intra-body sensors, thermostats, and almost anything we can imagine will be absorbed into the Internet and accessible from anywhere on the planet [1]. The revolution brought by the IoT will be unmatched – some say it will be similar to the building of roads and railroads which powered the Industrial Revolution of the 18th to 19th centuries [2] – and will take by storm every human sector and industry, ranging from education, health-care, smart home and smart city, to manufacturing, mining, commerce, transportation, and surveillance, just to mention a few [3].

Over the last few years, researchers have mainly focused their attention on addressing IoT's computation and communication scalability issues [4–6]. While these topics are certainly paramount to IoT's success and need to be thoroughly investigated, the community has now widely acknowledged that they have to be considered "low-hanging fruits" with respect to the towering issues of IoT security and privacy, which are unprecedented in scope and magnitude [7–11] and will require considerable research effort to be overcome. It is easy to imagine, indeed, that once humans, sensors, cars, robots, and drones are able to seamlessly interact with each other from any side of the globe, a number of threats that we cannot even imagine today will be unveiled.

As currently envisioned, the IoT will implement a centralized, client-server based access model in which IoT transactions (*i.e.*, data, money, or any other object of value) between IoT entities (*i.e.*, any computing device or stakeholder connected to the IoT) is entrusted to monolithic, centralized service providers [12]. This model clearly simplifies the interactions between IoT entities and facilitates the data collection process. However, it ultimately makes the IoT vulnerable to a number of spinous security and privacy issues. Specifically, centralized service providers can make illegitimate use of IoT data, for example, mass-surveillance programs [13]. Even more importantly, centralized data collection models can expose the system to hacking by malicious activities, with nefarious consequences for citizens, as unveiled in [14–17]. Another major challenge is the authentication of IoT entities that will be mostly deployed *in the wild* with little supervision [18; 19]. If not addressed, IoT authentication issues can generate botnets (*e.g.*, Mirai [20]) and hard-to-tackle sybil attacks [21].

The key intuition to address the challenges above is to *orchestrate IoT transactions in a decentralized fashion*, so that no single entity has control over them. Not only will decentralization provide security and privacy by design, but also empower users with the choice of sharing or selling their sensor data with third party entities without intermediaries. Decentralized control also implies scalability – which has plagued the IoT from its very inception [22; 23]. The end goal, therefore, is to investigate decentralized data access models for the IoT, which will ensure that user-data is not entrusted to centralized entities or companies, but instead is made the property of the users themselves. To this end, technologies and systems based on the concept of *blockchain* have enabled the cryptocurrency market, and may prove crucial to achieve the stringent security and privacy goals of the IoT [24]. Although the key algorithms and principles behind the blockchain have been known since the 70's (*i.e.*, Merkle trees [25], consensus algorithms [26]), the first practical application of the blockchain was originally proposed in 2008 as part of the Bitcoin cryptocurrency [27]. Since then, it has been widely applied to a wide range of non-monetary applications, including transportation, energy management, smart cities,

F. Restuccia, S. D'Oro and T. Melodia are with the Institute for the Wireless Internet of Things, Department of Electrical and Computer Engineering, Northeastern University, Boston, MA, 02115 USA e-mail: {frestuc, salvatoredoro, melodia}@northeastern.edu.
S.S. Kanhere is with the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052, Australia. E-mail: salil.kanhere@unsw.edu.au.
S. K. Das is with the Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65401 USA. Email: sdas@mst.edu.
Manuscript received December 15, 2017; revised January 1, 2018.

drones/robots, and manufacturing; we survey existing literature on the topic in Section III.

In a nutshell, a blockchain maintains a collection (or *ledger*) of transactions in a decentralized fashion – we describe in details what a blockchain is in Section II. The ledger is *immutable*, meaning that past transactions cannot be modified by any entity registering transactions in the blockchain[1], and is shared and synchronized across all participating nodes. This way, the blockchain guarantees that the ledger cannot be tampered with, and that all the data held by the blockchain is trustworthy. A *consensus algorithm*, which involves solving a hard-to-solve (*i.e.*, resource-demanding) yet easy-to-verify puzzle called proof-of-work (PoW), is used for appending (*mining*) new blocks into the blockchain, and thus establish a *secure trusted network among untrusted entities*. For identification purposes, blockchain nodes may choose to employ changeable public keys to prevent tracking. Multiple transactions are merged together to form a block which is appended to the ledger by following the consensus algorithm. Each block includes the hash of the previous block in the ledger (hence the name *blockchain*). Any modifications to a block (and thus transactions) can be readily detected as the hash maintained in the subsequent block will not match.

The combination of blockchain and IoT has disruptive potential. Indeed, the blockchain may help the IoT's expansion into our society by providing the following key advantages:

- *Anonymity.* IoT entities can participate to the blockchain with a public/private key, which (if so desired) does not reveal in itself the real identity of the entity;
- *Decentralization.* Traditional centralized systems require each transaction be validated through a centralized authority (*e.g.*, a central bank) – which inevitably translates into a performance bottleneck. Conversely, third-party validation is no longer needed in the blockchain, since consensus algorithms maintain data consistency;
- *Non-repudiation.* The blockchain ensures that (i) transactions can be easily validated; and (ii) invalid transactions are not admitted – it is nearly impossible to delete or roll back transactions once included in the blockchain.

Although the blockchain may look as a panacea to the IoT's security and privacy issues, there are still many research challenges that prevent its off-the-shelf application to most of today's IoT networks. Indeed, most of the algorithms used by today's blockchain-based systems were not designed to be run on devices with extremely stringent computation/energy/bandwidth constraints as in the IoT. Several key challenges (discussed in detail in Section V) need to be addressed, including: (i) scalability issues that stem from the need to achieve consensus among potentially billions of miners; (ii) high computation demands due to the use of proof-of-work (or similar) algorithms; and (iii) high delays due to anti-double spending mechanisms (issue which may not necessarily apply to the IoT).

[1]Many works refer to the blockchain as an immutable data structure, however it is technically imprecise to define it as immutable. In fact, there are precedents where entries in the blockchain have been changed after attacks or misbehavior of the network [28]. In this paper, the word immutable is intended to be used to represent the *hard-to-change* structure of the blockchain [29].

The focus of this paper is to provide an overview of the state of the art pertaining to the application of blockchain-based system to address IoT's security and privacy issues, and offer a roadmap of novel and exciting research challenges to the research community. We point out that an in-depth survey and comparison of existing blockchain-based IoT systems is not the ultimate objective of this paper. Instead, our main goal is to prime the readers and stimulate their research efforts toward the development of next-generation secure-by-design blockchain-based IoT systems.

II. What is a Blockchain?

From a computational viewpoint, a *blockchain* is a data structure where entries (also called *blocks*) are stored and linked to one another in sequential order. As shown in Fig. 1, the concept of blockchain is very similar to that of a linked list, where each entry is linked to the next one by means of a pointer. Although the two structures above are conceptually the same, their implementation differs in several major aspects.

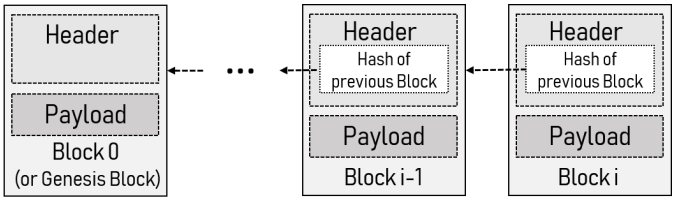

Figure 1. The structure of a blockchain.

Each block is composed by a header and a data payload. While the payload is generally used to store a list of transactions among users of the blockchain, the header is used to convey useful information with respect to the block, such as its length and content. Furthermore, the header stores the 32-bit SHA256 [30] hash value of the previous block. The importance of such a field is twofold: this way, (i) each block is immutably linked to the previous one; and (ii) the hash value of the i-th block will depend on the hash value of block $i-1$. The first feature provides a very efficient mechanism to interconnect all blocks of the blockchain, while the second one, as discussed later, is used to prevent malicious attacks.

To understand this latter statement, it is important to first understand how the blockchain is generated and maintained over time.

A. Consensus Mechanisms

The purpose of the blockchain [27] is to enable peer-to-peer transactions that are validated, organized into blocks, and then stored inside a distributed ledger. To achieve this objective, the blockchain is regulated by decentralized consensus algorithms that determine how and when a group of transactions can be included in the ledger. Specifically, each new block can be appended to the blockchain only if the majority of nodes in the network agrees upon its inclusions, that is, only if consensus among users of the blockchain is reached. Each node in the network keeps a local copy of the blockchain. When a new block achieves a consensus, it is broadcast over the network.

Thus, each node appends the new block to its local copy of the blockchain. These mechanisms make it possible to create multiple consistent copies of the blockchain, such that as soon as the majority of nodes possesses the same copy of the blockchain, the network can be considered as reliable and trusted.

Consensus is an extremely important concept for the blockchain. The first implementations of the blockchain adopted the proof-of-work (PoW) consensus mechanism [31], which provides a distributed mechanism to maintain and validate the blockchain. The idea behind PoW is to achieve consensus among nodes of the network through hard-to-compute, but easy-to-verify, computational puzzles. For example, the Bitcoin blockchain asks its users (also called *miners*) to find a 4-byte random number, *i.e.*, the *nonce*, such that the SHA256 hash value of a new block is equal to or less than a given threshold. While the computation of the nonce is hard and computational-hungry, verifying that a nonce satisfies the threshold requirement is computationally very inexpensive. Accordingly, the first node that finds a candidate nonce notifies the blockchain network and broadcasts the new block. The obtained nonce, which represents the PoW of the miner, is tested by other nodes that determine whether or not the nonce is an actual solution of the hashing puzzle. When the validation of the nonce is successful, nodes add the new block to their locally stored blockchain and start working on a new block.

B. Computational Aspects

Although PoW is a very effective mechanism to achieve consensus, it requires overwhelming amounts of energy and computational power, which increase every year as more and more miners and transactions add up to the blockchain [32]. For this reason, other consensus mechanisms [33] have been considered in many blockchain architectures. As an example, Proof-of-Stake (PoS) mechanisms [34; 35] use deterministic rules based on the amount of coins, *i.e.*, the *stake*, to select which node in the network will append the next block to the blockchain. Similarly, the proof-of-importance (PoI) considers the stake as an important metric as well – however, it accounts also for metrics that measure the miner's involvement in the network, such as number and volume of transactions.

As shown in Fig. 1, the hash value of each block depends on the hash value of the previous blocks. Thus, a change in any of the already existing blocks of the blockchain would produce a different hash value for that block, that will then generate a cascading effect on all subsequent blocks and their hash values. The newly generated hash values will be different from those already stored by all other nodes in the network, and thanks to the consensus algorithm, the corrupted blocks will be rejected from the blockchain.

C. Security Aspects

In general, consensus algorithms guarantee the trustworthiness of a blockchain. However, there are cases where malicious users can leverage the blockchain structure to change, duplicate or delete blocks [36]. Specifically, it is sufficient for an attacker to possess more than the 50% of the nodes in the network to take control of the whole blockchain. This attack, also referred to as the 51% *attack*, aims at governing the consensus mechanism to manipulate a blockchain. These attacks have been shown to be effective against many minor crypto-currencies such as Verge, Bitcoin Gold and Zencash [37] – however, they have as well threatened even widespread crypto-currencies such as Bitcoin [38; 39]. Double-spending [40; 41], which consists in the replication of one or more transactions, is the main purpose of 51% attacks. However, it has been shown that double-spending can be achieved even without approaching the 50% threshold [42].

To mitigate 51% attacks, ever more blockchain-based systems are adopting better security strategies. For example, real-time validators can be used to increase the attack threshold to 99% [43], which means that an attacker can take control over the blockchain network only if it has access to almost all nodes in the network. Another approach is to use PoS consensus mechanisms where the importance given to the possession of coins (rather than of computational power) makes the 51% attack unprofitable for the attacker and less likely to happen.

III. Overview of Blockchain-based IoT Systems

In this section, we provide a survey of the most relevant blockchain-based IoT systems investigated so far in literature. As shown in Table I, we divide the papers by categories, each named after the most common IoT applications nowadays available, *i.e.*, smart energy, smart environments, robotics, transportation, and supply chain.

Application of Blockchain to IoT	Papers
Smart Energy	[44–50]
Smart Environments	[51–55]
Robotics	[56–59]
Transportation	[60–70]
Supply Chain	[71–73]
Others	[74–78]

Table I
Summary of Blockchain-based IoT Systems.

- *Smart Energy.* This field has attracted significant attention from the IoT community over the last years [79]. The majority of the proposed IoT systems leverage the blockchain to (i) preserve the privacy of the users along with their personal information; and (ii) protect the system from malicious transaction such as users attempting to sell or buy unreasonable amount of energy [45; 46; 49]. The authors in [44; 47] propose auction systems where users can sell to the highest bidder their excessive energy based on an auction defined in a smart contract, hence eliminating the need for a third-party auctioneer. Moreover, Hahn *et al.* [44] implemented the auction on a campus-level energy grid. Yan *et al.* [50] explored the use of blockchain to reconstruct the current distributed energy transaction patterns to allow decentralized real-time transactions and intelligent energy trading contracts using an automatic trust mechanism.
- *Smart Environments.* Smart environments have been extensively in industrial settings [80], for smart healthcare

[81], smart cities [82] and smart homes [52; 55; 83]. In this context, the blockchain is used to ensure the availability and unrepudiability of sensed data collected in the wild, *e.g.*, a farm area [53; 54].

- *Robotics.* Existing work in this area leverages the blockchain as a system to support secure and reliable unmanned air vehicles (UAV) communications. Indeed, UAVs need to reliably coordinate their actions, exchange data and collaboratively make decisions. Sharma *et al.* [59] present a system where drones are programmed to use the blockchain to securely relay information. Moreover, Ferrer *et al.* [56] investigate the use of the blockchain to provide security, autonomy and collective decision-making in swarm robotic systems. The authors in [58] leverage a combination of blockchain and cloud storage to protect the integrity of drone-collected data.
- *Transportation.* Over the last years, many IoT concepts have been used to design next-generation transportation systems [84–86]. The most promising aspect is that smart vehicles will likely not be as computationally constrained as other IoT devices, such as sensor platforms. Therefore, the blockchain is a strong candidate to become a system for tamper-proof data exchange among smart vehicles, as proposed by Steger *et al.* [68]. Similarly, Ceba *et al.* [60] monitor vehicle-related data (*e.g.*, maintenance information and vehicle diagnosis reports) by using the blockchain. Yuan *et al.* [70] use the blockchain to design a full-fledged intelligent transportation system architecture, which includes application, contract, incentive, consensus, data, physical, and network layers. The blockchain has also been leveraged to implement systems to handle the public keys of the vehicles [63], and in general share data without third-party centralized management [61; 64]. Li *et al.* [62] propose *CreditCoin*, a privacy-preserving system to share relevant information (*e.g.*, accident, traffic) between vehicles, where participants are rewarded through monetary tokens. Yang *et al.* [66] proposed a blockchain-based reputation system that estimates the trustworthiness of received messages.
- *Supply Chain & Others.* Some systems have been proposed to enhance the functionality of cloud-based and on-demand manufacturing [71; 73]. A blockchain-based distribution framework to share knowledge and services across enterprises is presented in [72]. A set of papers [74–78] address edge computing, virtualization of IoT resources, among others.

IV. Blockchain technologies for the IoT

In this section, we discuss the most important blockchain technologies and features, and we discuss their application to the IoT.

A. Smart Contracts

One of the key challenges of the IoT is to enable and control autonomous and self-organized machine-to-machine (M2M) communications. In this specific context, it is of paramount importance to design management mechanisms such that (i) interactions are automatically initiated; and (ii) there is no need to individually control and verify the trustworthiness of each interaction/communication. The above problem is definitely not trivial, and its complexity is further exacerbated by the large number of connected devices and their heterogeneous design. It is worth mentioning that the above problem is not peculiar of the IoT only, but it also affects all of those network architectures and systems where the lack of centralized entities that perform centralized network control and management call for self-organized and automated protocols.

The best example is the blockchain, a system where distributed entities are required to autonomously reach consensus by locally executing complex algorithms. In this context, *smart contracts* [87] has been shown to be effective to solve the above challenges.

In a nutshell, smart contracts are software programs that specify and automatically enforce contracts among two or more parties. To understand how smart contracts work, we consider the case where Alice rents a house to Bob. Bob is required to send a monthly payment to Alice. In the context of the blockchain, the above transaction can be easily encoded into a smart contract. As an example, in Ethereum's blockchain each smart contract is represented by a series of computational operations that are expressed via a programming language that is specified by an Application Binary Interface (ABI). Indeed, it is sufficient to write a few lines of code to generate and link the contract to Bob, such that the monthly payment can be automatically triggered by a software program when the monthly deadline is over. Therefore, smart contracts implement effective mechanisms to send/receive payments (i.e., the rent) to/from other entities when one or more conditions (i.e., monthly deadline) are satisfied.

Although the previous example is very simple, contracts can generally implement very complex operations and can also be linked one to another, thus generating a nested structure (*e.g.*, sublease). The advantages of smart contracts are numerous, and their impact on IoT networks is considerable, as discussed in [87]. First, since contracts are stored inside the blockchain, their content is trusted among parties as it cannot be modified or corrupted after its inclusion in the blockchain. Second, each contract is assigned an unequivocal address in the blockchain and can be directly accessed from the Internet, thus making smart contracts well-suited to be accessed by remotely connected IoT devices. Finally, contracts consist of few lines of code that devices can easily understand and execute.

Given the similarities between the IoT and the blockchain, and looking at the success and effectiveness of smart contracts in blockchain applications, it is reasonable to assume that smart contracts can find useful applications in the IoT to support autonomous and self-organized interactions. Although the application of smart contracts to the IoT is still being investigated, preliminary results already show that several IoT applications would benefit from blockchain technologies such as smart contracts. For example, the application of smart contracts to devise access control mechanisms that regulate the access to the IoT network has been shown to be beneficial for the IoT [88–92]. These works leverage the immutability of the blockchain to generate real-time access control lists that also regulate and describe access policies to device resources.

Another example is the work in [87], where authors discuss the possibility to achieve smart supply chain monitoring by means of smart contracts. They show that, not only smart contracts can be used to regulate transactions and fees related to the production and shipment processes of goods, but they can also be used to keep track of their position.

B. Software and Content Validation

The IoT system is well-known to be a heterogeneous environment where substantially different devices (in terms of hardware and offered services) interact with both users and other devices. In this challenging scenario, it is crucial to guarantee that the software embedded in each device (*e.g.,* firmware, scripts) is always up-to-date and satisfies regulations and security requirements of the network. Although the sheer number of devices in the network complicates the design of mechanisms that meet the above requirements in large-scale heterogeneous networks, the blockchain already provides useful embedded features that completely, or partially, address the above issues.

As shown in [75; 93], the distributed nature of the blockchain may be leveraged to store and disseminate secure and verified firmware updates over the network. Specifically, the blockchain can be used to (i) store either the firmware update itself, or the address of a safe and trusted location where the updated code can be downloaded and installed; and (ii) use PoW (or similar tools) to determine when a device possesses an updated and verified firmware, thus deciding whether or not a device can be trusted. Since the blockchain is maintained through consensus mechanisms, it is possible to generate trusted blockchains that store all trusted and up-to-date firmware updates [75] that can be easily identified and downloaded by network nodes.

Another interesting application of blockchain technologies to IoT systems is the possibility to provide reliable license validation tools to avoid piracy and preserve copyrights of software/hardware developers [94] and content creators [95]. Indeed, IoT devices are nowadays capable of performing heterogeneous sensing and computational tasks, and can be reprogrammed by dynamically loading different software applications coming from different developers. Although open-source software is now widely used in many IoT environments, there are still several applications whose code can be purchased from the Internet through licensing. The purpose of [94] is to leverage blockchain technologies to provide effective licensing validation tools for a software developer to enforce their copyright.

V. The Road Ahead

We now propose a roadmap of research challenges pertaining to the application of blockchain algorithms to the IoT.

A. Addressing Blockchain Scalability Issues

Applying blockchain technologies to the IoT implies that scalability issues must be addressed. Most importantly, existing blockchain tools require all nodes in the network to either approve each transaction/block, or store them locally. While these tasks are easy for personal computers or workstations, they may be prohibitive for small sensors with limited storage and computational resources. This issue is further exacerbated by the fact that the amount of data transmissions, and thus required transactions, to be stored in the blockchain is large and exponentially increasing over time [24; 96–98]. In other words, existing consensus algorithms that rely on PoW and PoS are not directly applicable to address long-term, reliable and scalable solutions for blockchain-based IoT systems.

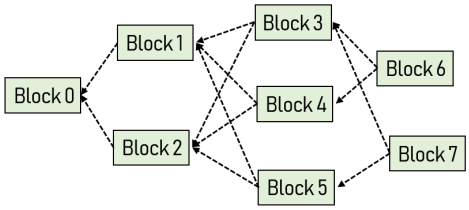

Figure 2. DAG blockchain (or Tangle).

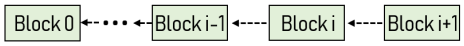

Figure 3. Traditional linear blockchain

The most widely used approach to address scalability issues is to leverage clustering algorithms to reduce communication and computation overheads [52; 90]. For example, Novo [90] proposes a scalable blockchain solution for IoT systems. At the cost of additional communication delay, the proposed solution relies on a management hub that handles a group of IoT devices, thus reducing the number of interactions between things and the blockchain, effectively producing a scalable blockchain design. A similar approach is instead proposed by Dorri *et al.* [52], where the authors design a scalable secure and privacy-preserving blockchain for IoT applications.

Other approaches choose to revisit the structure of consensus mechanisms and the blockchain itself to provide ad-hoc solutions for the IoT. Glaring examples are the crypto-currencies IoT Chain (ITC) [99] and IOTA [100]. These currencies are built to provide lightweight blockchain technologies for the IoT. Specifically, together with other coins such as Byteball [101], ITC and IOTA aim at reshaping the linear structure of the blockchain to obtain a *tangled* [100] network represented by a direct acyclic graph (DAG). The differences between traditional (linear) blockchain approaches and the DAG-based one are shown in Figs. 2 and 3. In the DAG-based architecture (also called *tangle*), blocks represents vertices of the DAG and edges are used to validate transactions. Specifically, to be included in the DAG, each new transaction A must approve any two transactions B and C already included in the DAG. Approval of transactions is represented through directed edges going from a transaction to another. Accordingly, when A is included in the DAG, it automatically generates two edges $A \rightarrow B$ and $A \rightarrow C$ that extend the DAG incrementally. The synergic usage of DAGs and blockchain technologies allows to dispose of the linear structure of traditional blockchains,

facilitate transaction verification times and eliminate the need for mining as transactions are in charge of validating other transactions.

B. IoT-tailored Security and Reliability

Being able to remotely access one or more devices, together with the possibility to let them communicate and coordinate with each other autonomously is with no doubt a very useful and remarkable feature. However, this inevitably poses several concerns from the security and reliability viewpoints [7; 41]. The IoT is vulnerable to a wide variety of network attacks that undermine the confidentiality, integrity, authentication and availability. These aspects are fundamental requirements of any modern communication network and a variety of solutions for have been proposed in the literature [7; 10; 41; 102; 103]. These surveys provide an exhaustive literature review of already existing solutions to design secure and reliable IoT systems. At the same, however, they show that many security solutions are not general enough and require ad-hoc solutions that involves new algorithms and software.

The blockchain already implements several mechanisms such as public/private encryption, hashing, consensus and fault-tolerance whose effectiveness in terms of security has been widely investigated and verified for many networking scenarios. For this reason, the blockchain has been identified as a pivotal technology to design secure and reliable IoT systems [52; 67; 104; 105].

- *Confidentiality:* data confidentiality is achieved when a given information (*e.g.,* sensing data, transaction) can be accessed by intended devices only. In this context, public key encryption used to perform transactions in the blockchain can be seamlessly used to encrypt communications and data to be stored, thus effectively achieving confidentiality;
- *Integrity:* to guarantee that data accessed and stored by IoT devices is reliable, integrity of contents must be ensured at all times. Again, the blockchain comes in help by providing useful mechanisms to guarantee integrity of data. Recall that the integrity of each block in the blockchain is verified by computing its hash value, and that the hash value of any block depends on the hash of previous blocks. Accordingly, not only hashing in the blockchain ensures integrity of a new block, but it also extends the integrity check to all previous blocks. As shown in [67], the same concept can be used in blockchain-based IoT networks to check the integrity of sensing data, transmitted data and transactions among devices and users;
- *Authentication and Non-repudiation:* by leveraging on the already embedded public key encryption it is possible to implement signature-based security mechanisms, which are well-known to jointly provide authentication and non-repudiation [106]. Recall that any node B possessing the public key of a given device A can i) decode messages encrypted by using A's private key; and ii) encrypt messages with the public key of A. Since the private key of A is known to A only, public key encryption makes it possible to use private keys to generate an electronic signature of A. This signature is used to authenticate A when it communicates with other nodes (each node can verify the signature by using A's public key); and can be used for non-repudiation purposes to sign all the transactions included in the blockchain that involve A, thus effectively providing proofs of A's activity on the blockchain.

VI. Conclusions

In this paper, we have provided an overview of existing literature on the topic of blockchain for IoT, and presented a roadmap of research challenges that will need to be addressed to enable the usage of blockchain technologies in the IoT. First, we have briefly introduced the concept of blockchain in Section II, followed by an overview of existing blockchain-based IoT applications in Section III. Then, we have presented the major blockchain technologies for the IoT in Section IV. We have concluded the paper by discussing several research challenges in Section V.

References

[1] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things – A survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[2] Glen Martin (Forbes), "How The Internet Of Things Is More Like The Industrial Revolution Than The Digital Revolution," https://www.forbes.com/sites/oreillymedia/2014/02/10/more-1876-than-1995/#674c4e0b66d2.

[3] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[4] O. Bello and S. Zeadally, "Communication issues in the internet of things (iot)," in *Next-Generation Wireless Technologies*. Springer, 2013, pp. 189–219.

[5] S. Tayeb, S. Latifi, and Y. Kim, "A survey on iot communication and computation frameworks: An industrial perspective," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–6.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, 2018.

[8] C. Bekara, "Security issues and challenges for the iot-based smart grid," *Procedia Computer Science*, vol. 34, pp. 532–537, 2014.

[9] M. FRUSTACI, P. Pasquale, A. Gianluca, and G. FORTINO, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of Things Journal*, 2017.

[10] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[11] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*. IEEE, 2014, pp. 1–8.

[12] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, 2017, p. 14.

[13] Julia Powles (The Guardian), "Internet of things: the greatest mass surveillance infrastructure ever?" https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance, 2013.

[14] Dan Goodin, Ars Technica, "9 Baby Monitors Wide Open to Hacks that Expose Users' Most Private Moments," http://tinyurl.com/ya7w43e9, 2015.

[15] Jerry Hirsch, Los Angeles Times, "Hackers Can Now Hitch a Ride on Car Computers," http://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html, 2015.

[16] Kelsey D. Atheron, Popular Science, "Hackers Can Tap Into Hospital Drug Pumps To Serve Lethal Doses To Patients," available at: http://tinyurl.com/qfscthv, 2015.

[17] Darren Pauli, ITNews, "Hacked Terminals Capable of Causing Pacemaker Deaths," http://tinyurl.com/ycl4z9xf, 2015.

[18] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.

[19] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, 2018.

[20] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[21] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[22] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini, "Spatiotemporal stochastic modeling of iot enabled cellular networks: Scalability and stability analysis," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3585–3600, 2017.

[23] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[24] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*. IEEE, 2016, pp. 1–6.

[25] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, 1980 IEEE Symposium on*. IEEE, 1980, pp. 122–122.

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, June 2017, pp. 557–564.

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[28] K. D. Werbach, "Trust, but verify: Why the blockchain needs the law," 2017.

[29] A. Walch, "The path of the blockchain lexicon (and the law)," *Rev. Banking & Fin. L.*, vol. 36, p. 713, 2016.

[30] F. I. P. S. PUBLICATION, "Secure Hash Standard (SHS)," *FIPS PUB 180*, vol. 4, 2012.

[31] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference*. Springer, 1992, pp. 139–147.

[32] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 2014.

[33] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2018, pp. 1545–1550.

[34] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov, "A provably secure proof-of-stake blockchain protocol." *IACR Cryptology ePrint Archive*, vol. 2016, p. 889, 2016.

[35] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Big Data (BigData Congress), 2017 IEEE International Congress on*. IEEE, 2017, pp. 557–564.

[36] D. Bradbury, "The problem with bitcoin," *Computer Fraud & Security*, vol. 2013, no. 11, pp. 5–8, 2013.

[37] Alyssa Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular," https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular, 2018.

[38] Daniel Cawrey, "Are 51% Attacks a Real Threat to Bitcoin?" https://www.coindesk.com/51-attacks-real-threat-bitcoin, 2014.

[39] Roop Gill, "CEX.IO Slow to Respond as Fears of 51% Attack Spread," https://www.coindesk.com/cex-io-response-fears-of-51-attack-spread, 2014.

[40] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 906–917.

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

[42] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, p. 2, 2015.

[43] Vitalik Buterin, "A Guide to 99% Fault Tolerant Consensus," https://vitalik.ca/general/2018/08/07/99_fault_tolerant.html, 2018.

[44] A. Hahn, R. Singh, C.-C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized transactive energy auctions," in *Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2017 IEEE*. IEEE, 2017, pp. 1–5.

[45] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," in *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, 2017, p. 13.

[46] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids," in *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET, 2018, pp. 1–6.

[47] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[48] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Control Technology and Applications (CCTA), 2017 IEEE Conference on*. IEEE, 2017, pp. 2164–2171.

[49] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Resilience Week (RWS), 2017*. IEEE, 2017, pp. 18–23.

[50] H. Yan, B.-B. Huang, and B.-W. Hong, "Distributed energy transaction pattern and block chain based architecture design," *DEStech Transactions on Environment, Energy and Earth Sciences*, no. epee, 2017.

[51] R. A. Michelin, A. Dorri, R. C. Lunardi, M. Steger, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," *arXiv preprint arXiv:1807.01980*, 2018.

[52] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," *arXiv preprint arXiv:1712.02969*, 2017.

[53] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A framework for blockchain based secure smart green house farming," in *Advances in Computer Science and Ubiquitous Computing*. Springer, 2017, pp. 1162–1167.

[54] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "Citysense: blockchain-oriented smart cities," in *Proceedings of the XP2017 Scientific Workshops*. ACM, 2017, p. 12.

[55] A. Palai, M. Vora, and A. Shah, "Empowering light nodes in blockchains with block summarization," in *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on*. IEEE, 2018, pp. 1–5.

[56] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," *arXiv preprint arXiv:1608.00695*, 2016.

[57] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," in *Research, Education and Development of Unmanned Aerial Systems (RED-UAS), 2017 Workshop on*. IEEE, 2017, pp. 84–89.

[58] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*. IEEE, 2017, pp. 261–266.

[59] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain," in *Proceedings of the 2017 International Workshop on Managing Insider Security Threats*. ACM, 2017, pp. 81–84.

[60] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *arXiv preprint arXiv:1802.00561*, 2018.

[61] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*. ACM, 2016, pp. 137–140.

[62] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, July 2018.

[63] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick,

"Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," *arXiv preprint arXiv:1704.02553*, 2017.

[64] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, p. 84, 2017.

[65] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," *arXiv preprint arXiv:1707.07442*, 2017.

[66] Z. Yang, K. Zheng, K. Yang, and V. C. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on*. IEEE, 2017, pp. 1–5.

[67] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[68] M. Steger, A. Dorri, S. S. Kanhere, K. Römer, R. Jurdak, and M. Karner, "Secure wireless automotive software updates using blockchains: A proof of concept," in *Advanced Microsystems for Automotive Applications 2017*. Springer, 2018, pp. 137–149.

[69] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, "B-fica: Blockchain based framework for auto-insurance claim and adjudication," *arXiv preprint arXiv:1806.06169*, 2018.

[70] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*. IEEE, 2016, pp. 2663–2668.

[71] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.

[72] Z. Li, W. Wang, G. Liu, L. Liu, J. He, and G. Huang, "Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing," *Industrial Management & Data Systems*, vol. 118, no. 1, pp. 303–320, 2018.

[73] K. Rabah, "Overview of blockchain as the engine of the 4th industrial revolution," *Mara Research Journal of Business & Management-ISSN: 2519-1381*, vol. 1, no. 1, pp. 125–135, 2017.

[74] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for iot updates by means of a blockchain," in *Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on*. IEEE, 2017, pp. 50–58.

[75] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[76] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge-hosts with blockchain," in *Computer and Information Technology (CIT), 2016 IEEE International Conference on*. IEEE, 2016, pp. 116–119.

[77] ——, "Virtual resources & blockchain for configuration management in iot," *Journal of Ubiquitous Systems & Pervasive Networks*, vol. 9, no. 2, pp. 01–13, 2017.

[78] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Control Systems and Computer Science (CSCS), 2017 21st International Conference on*. IEEE, 2017, pp. 667–671.

[79] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for iot application on smart grids: Survey and research challenges," in *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on*. IEEE, 2016, pp. 63–68.

[80] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart cities and the future internet: Towards cooperation frameworks for open innovation," in *The future internet assembly*. Springer, 2011, pp. 431–446.

[81] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An iot-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

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

[83] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of iot for environmental condition monitoring in homes," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3846–3853, 2013.

[84] X.-Y. Liu and M.-Y. Wu, "Vehicular CPS: an application of IoT in vehicular networks," *Jisuanji Yingyong/ Journal of Computer Applications*, vol. 32, no. 4, pp. 900–904, 2012.

[85] W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1587–1595, 2014.

[86] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 2014, pp. 241–246.

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

[88] C. Lin, D. He, X. Huang, and K.-K. R. Choo, "Secure and privacy-preserving smart contract-based solution for access control in iot," *Newsletter*, 2018.

[89] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[90] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, April 2018.

[91] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A smart contract enabled decentralized capability-based access control mechanism for iot," 2018.

[92] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *arXiv preprint arXiv:1802.04410*, 2018.

[93] C. S. Kouzinopoulos, G. Spathoulas, K. M. Giannoutakis, K. Votis, P. Pandey, D. Tzovaras, S. K. Katsikas, A. Collen, and N. A. Nijdam, "Using blockchains to strengthen the security of internet of things," in *International ISCIS Security Workshop*. Springer, 2018, pp. 90–100.

[94] J. Herbert and A. Litchfield, "A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology," in *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*, vol. 27, 2015, p. 30.

[95] "Po.et: The decentralized protocol for content ownership, discovery and monetization in media ," https://www.po.et/.

[96] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2017, pp. 173–178.

[97] D. Wörner and T. von Bomhard, "When your sensor earns money: exchanging data for cash with bitcoin," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM, 2014, pp. 295–298.

[98] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to betterhow to make bitcoin a better currency," in *International Conference on Financial Cryptography and Data Security*. Springer, 2012, pp. 399–414.

[99] IoT Chain, "White Paper: a high-security lite IoT OS," https://iotchain.io/.

[100] S. Popov, "The tangle," http://blockchainrai.com/papers/iota.pdf.

[101] Byteball, "White Paper: A Decentralized System for Storage and Transfer of Value," https://byteball.org/.

[102] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*. IEEE, 2015, pp. 1–6.

[103] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[104] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[105] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *Wireless Communications and Networking Conference (WCNC), 2018 IEEE*. IEEE, 2018, pp. 1–6.

[106] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE network*, vol. 13, no. 6, pp. 24–30, 1999.