Chapter 10
Can Blockchain Technology Enhance Security and Privacy in the Internet of Things?

Georgios Spathoulas, Lydia Negka, Pankaj Pandey, and Sokratis Katsikas

Abstract The Internet of Things (IoT) has changed the traditional computing models. While it has enabled multiple new computing applications, it has also raised significant issues regarding security and privacy. We are gradually shifting to using extended computing architectures, the nodes of which may be lightweight devices limited in hardware resources, scattered in terms of network topology and too diverse in terms of hardware and software to be efficiently administered and managed. Additionally, such nodes usually store, process and transmit sensitive private data of their users; thus, the risk of a security breach is significantly high. Blockchain technology, introduced through Bitcoin, enables the development of secure decentralized systems. It offers guarantees regarding data integrity, application logic integrity and service availability, while it lags behind in terms of privacy and efficiency. Because of the decentralized architecture of blockchain systems, there seems to be a good fit between blockchain and the IoT. Blockchain systems can be employed to develop solutions to some of the main security and privacy issues encountered in the IoT domain. In this chapter we discuss the convergence of the two technologies, we analyze possible use cases, where blockchain technology can enhance internet of things security and privacy, and we propose enhancements of blockchain technology to make it appropriate for application in the IoT domain.

Keywords Blockchain · Internet of things · Security · Privacy

G. Spathoulas · L. Negka
Department of Computer Science and Biomedical Informatics,
University of Thessaly, Lamia, Greece
e-mail: gspathoulas@uth.gr

L. Negka
e-mail: lnegka@uth.gr

P. Pandey · S. Katsikas
Center for Cyber and Information Security,
Norwegian University of Science and Technology, Gjøvik, Norway
e-mail: pankaj.pandey@ntnu.no

S. Katsikas (✉)
School of Pure and Applied Sciences, Open University of Cyprus, Nicosia, Cyprus
e-mail: sokratis.katsikas@ntnu.no; sokratis.katsikas@ouc.ac.cy

G. A. Tsihrintzis and M. Virvou (eds.), *Advances in Core Computer Science-Based Technologies*, Learning and Analytics in Intelligent Systems 14,
https://doi.org/10.1007/978-3-030-41196-1_10

10.1 Introduction

Blockchain technology, a shared Peer-to-Peer distributed ledger, is the underlying phenomenon of crypto-currencies that started with the proposal of a digital asset and payment system called "Bitcoin", which was introduced as an open source software in 2009 [39]. In a blockchain network there is no intermediary and the transactions are verified by a network of nodes before being recorded over a distributed ledger called blockchain [39]. Blockchains have begun to have a significant influence in the IoT domain and present a wide variety of opportunities for risk management. Blockchain technology and blockchain-based Smart Contracts have been well researched and some use cases have been proposed that adopt them in a range of applications in the IoT, including but not limited to the following: automated distribution and management of service-level information; automated management of warranty and maintenance information; management of ownership and transfer details; securing data records; protecting integrity of device software, and so on. Conoscenti et al. [14] provide a systematic literature review on the application of blockchain in IoT. Their work addresses the following six Research Questions (RQ):

- *RQ1)* What are the use cases of the blockchain beyond cryptocurrencies?
- *RQ2)* Are there any use cases applicable to the IoT?
- *RQ3)* What are the implementation differences with respect to the Bitcoin blockchain?
- *RQ3.1)* Which data are stored in the blockchain?
- *RQ3.2)* Which mining techniques are used?
- What is the degree of integrity (RQ4), anonymity (RQ5) and adaptability (RQ6) of the blockchain?

RQ1 and RQ2 aimed at reviewing the literature on the uses of blockchain technology beyond the initially developed Bitcoin and cryptocurrencies, and at identifying the blockchain applications that are applicable in the IoT context. RQ3 aimed at identifying the implementation choices that can be made in an IoT system, choices that are also different from the Bitcoin blockchain. For RQ4, ISO 25010 [2] was taken as the reference point for defining integrity, and characterizing the attacks that affect the blockchain and lead to undermining the integrity of the IoT. RQ5 addressed the need to protect the privacy of users by avoiding the linkage of IoT devices to their owners. RQ6 aimed at exploring whether the blockchain is adaptable to the number of transactions. For RQ6, the authors adopted the generic definition of adaptability from [2] and narrowed it down by defining the adaptability of the blockchain as its ability to scale with the number of transactions.

Conoscenti et al. [14] published their survey paper on the application of blockchain in the IoT about three years ago; since then there has been a tremendous growth in research and development in the domain, which has not, at the time of writing this chapter been fully. This chapter addresses this gap in the literature; it discusses the convergence of the two technologies, namely blockchain and IoT, it analyzes the potential use cases for leveraging blockchain in strengthening the security and

privacy in the IoT, and proposes enhancements in blockchain that are required for its efficient and effective application in IoT. This chapter is divided into six sections. Section 10.1 presents an Introduction that highlights the context and background of the subject; Sect. 10.2 presents IoT Security and Privacy issues; Sect. 10.3 presents an overview of blockchain technology; the State of the Art is presented in Sect. 10.4; Sect. 10.5 presents an Analysis of the State of the Art; and Sect. 10.6 concludes the paper.

10.2 IoT Security and Privacy

The Internet-of-Things (IoT) has changed and continues to change the way we live in todays digitally connected society. IoT devices are increasingly finding applications in a range of contexts, from smart homes to smart cities, to smart grids, to smart farming, to the Internet-of-Medical-Things (IoMT), to the Internet-of-Military-Things (IoMiT), to the Internet-of-Vehicles (IoV), etc. At the same time, the pervasiveness of IoT devices raises concerns on security and privacy. For example, over 100,000 consumer devices were reported to have been compromised in 2014 to send over 750,000 phishing and spam emails [3]. In several application cases of IoT e.g. the Internet-of-Medical-Things and the Internet-of-Battlefield-Things, data confidentiality is crucial; thus, ensuring cyber-physical security of the data and devices, and privacy of data and computations becomes critical. A cyber-physical threat to the IoT system in any application area could be a result of ill-designed security. For instance, the entire IoT network is usually controlled by a team of Information Technology (IT) practitioners. In such a situation, it is not reasonable to expect that the IT team has detailed knowledge about the individual devices in the network, even though the team have been managing the network with full rights to install patches, remote access to devices, etc. Furthermore, centralized IoT networks have a higher risk of a single point of failure, thus hindering the scalability, and raising security and privacy concerns. In such a scenario, users depend upon third-party entities for data handling and for enforcing necessary security and privacy policies. Further, there is a risk of third-party entities indulging into mass surveillance, misuse of data etc. In this context, blockchain technology appears to be an important link in building a trusted, decentralized and secure environment for IoT applications.

10.3 Blockchain Technology

In 1991, Stuart Haber and W. Scott Stornetta were the first to present their work on a cryptographically secured chain of blocks [23]. Later, Bayer, Haber and Stornetta incorporated Merkle trees to the blockchain in 1992; this was to improve the efficiency so as to collect several documents into one block [7]. The concept of distributed blockchain was first introduced by an anonymous person or group known

as Satoshi Nakamoto, in 2008, by publishing a whitepaper titled "Bitcoin: A Peer-to-Peer (P2P) Electronic Cash System" [39]. Blockchain (Bitcoin) was born when Satoshi Nakamoto solved a complex Game Theory conundrum called the Byzantine Generals Problem [34]; this ensured that, at a particular time, a block of assets could be transferred to only one other person, without the need for a third-party check. In 2009, the concept of distributed blockchain was implemented and released as an open-source software as a core component of the bitcoin digital currency. Bitcoin became the first digital currency (crypto currency) to solve the double spending problem through a blockchain, without requiring a trusted administrator [9]. The words *block* and *chain* were used separately in the original paper by Satoshi Nakamoto [39]; when the term moved into wider use it was still originally *block chain* [9] before becoming the single word "blockchain", by 2016.

Blockchain technology computationally answers the "Byzantine Generals Problem" [34]. In other words, blockchain answers the question of how individual users secure their data from non-trusted actors. The Byzantine Generals problem originates from a thought-experiment called the Two Generals Problem. The problem is illustrated by a scenario where two or more generals are to siege a city from opposite sides and they must coordinate their attack to be successful (to win). Let us assume that the General on one side, called *General A*, sends a message to the General on the other side, called *General B*, stating "attack at noon tomorrow", but the challenge is that the General *A* has no way to verify if General *B* has actually received the message; the risk is that if General *B* has not received the message, then if General *A* attacks in the afternoon, in absence of General *B*'s support he could potentially be marching towards defeat. On the other hand, if General *B* indeed receives the message sent by General *A*, General *B* has no way to verify if the message is authentic or a trap laid by the enemy. Let us assume that General *B* considers the message authentic and sends a response to confirm the planned attack. However, General *B* is now in the same situation as the one that General *A* was in before, i.e he has no way to verify if General *A* has received his response. Thus, there is a risk that General *A* will not be able to attack as planned, implying that General *B* will be the only one attacking as per the plan, risking his and his troops' lives. Nevertheless, General *A* could again send a message to General *B* to confirm the receipt of his acknowledgement message, but General *A* still has no way to verify if the message has reached General *B*, or even if the message was authentic in the first place. This puts General *A* in the same spot where General *B* was just in. This problem bounces back and forth into perpetuity like a never-ending loop, with neither of the Generals being ever confident about the authenticity and delivery of messages [27]. To relate the Byzantine Generals Problem to the blockchain we can illustrate it as follows: Person A can store almost anything of value into a 'digital lock box'. The content inside of the box can only be opened and changed with a unique private key. The information inside this box can then be shared on demand without the possibility of it being altered, changed, or replicated from its original form [22].

10.3.1 Blockchain Types

Buterin [10] categorized blockchains into three categories: Public Blockchain; Private Blockchain; and Hybrid Blockchain.

Public Blockchain

A fully open public ledger has no limitations with regards to reading- and writing permissions. Anyone can connect to the network, can access and add information. Anyone connected to the network has the right to participate in the consensus protocol, to verify the newly added blocks and ensure that they are not conflicting with previous blocks in the chain. The consensus protocol needs to be based on a cryptoeconomic mechanism, because of the open nature of the system and due to lack of trust between the nodes. A public ledger blockchain system operates without the requirement of trust between users; hence, it is considered to be fully decentralized.

Some of the state-of-the-art open source public blockchain platforms are Bitcoin, Ethereum, and Monero. The main characteristics of a public blockchain are as follows:

- Open to anyone for participation, without the need for any permission.
- Open to anyone to download the source code and run a public node on their local machine, validate the transactions in the network, and contribute to the consensus process. The consensus process is to determine the blocks that would be added to the (block)chain and their current state.
- Open to anyone to initiate transactions over the network and expect to see them added to the blockchain, after validation.
- Open to anyone to read transactions over a public block explorer. Transactions are transparent, but anonymous/pseudonymous.

Private Blockchain

A private blockchain enforces certain limitations on the reading- and writing permissions and is more tightly controlled than a public blockchain. Only a centralized group of participants, for example an organization, is granted the right to modify, add or read information. In a private blockchain system, a consensus protocol is usually not required, because of the trusted nodes. Private blockchain networks allow faster access to information, low cost transactions, and possibility to control the privacy level. Example applications of a private blockchain network include auditing, database management, etc. which are largely internal to a single organization; hence, public access to that information is not necessary in many cases. In other cases, public audit ability is desired. Private blockchains (such as MONAX, Multichain) exploit the blockchain technology by setting up internally verifiable groups and participants to approve the transactions. On the other hand, this has the risk of security breach like a traditional centralized system but has advantages in terms of scalability and compliance to data privacy rules and regulations.

Hybrid or Federated or Consortium Blockchains

As the name suggests, a hybrid blockchain, also called a consortium ledger, has some features of a public blockchain and some features of a private blockchain. In a consortium blockchain network, the consensus protocol is usually predetermined and managed by a predefined group of institutions [10]. A consortium blockchain system could e.g. have 25 participant institutions controlling one node, and every newly added block must be validated by at least 18 participant institutions before it can be added to the network. A hybrid blockchain system is thus partially decentralized. In a hybrid blockchain system, reading permissions could be granted to anyone or restricted to a group of participants. Furthermore, there is a hybrid solution to granting reading permissions as well, such that some parts of the information are open to the public while other parts are not.

Federated Blockchains (such as R3 (Banks), EWF (Energy), B3i (Insurance), Corda), operate under the leadership of a group, not allowing any other individual or institution to participate in the network transaction validation process. Federated Blockchains are much faster than public and private blockchains and provide much more privacy to transactions.

10.4 State of the Art

A lot of research on the convergence of blockchain and IoT technologies has been recently done. In this section research efforts relevant to applying blockchain solutions to enhance privacy and security for IoT ecosystems are reviewed and analyzed along three dimensions, namely (i) the security properties that the proposed systems aim to protect; (ii) the application domain in which these systems operate; and (iii) the technical maturity of the used blockchain infrastructure. Additionally, the main flaws or drawbacks of these proposals are identified, in order to define a clear path ahead for adapting blockchain technology to make it appropriate for solving IoT privacy and security issues.

10.4.1 Analysis Dimensions

10.4.1.1 Security Properties

We have identified five main security properties that blockchain solutions aim to protect; these are strongly coupled to fundamental security properties or combinations of these:

- **Confidentiality**: One of the main security issues in the IoT is the handling of sensitive personal data captured by IoT devices. On the other hand, the initial concept of blockchain is based on a publicly available ledger; therefore, any data

stored on blockchain networks is by default available to more than the strictly required users. Even though cryptography may be used to protect the data, this is not trivial in the context of the technical limitations imposed by blockchain technology.

- **Integrity**: The integrity of both data and procedures is crucial for any system, including the IoT ecosystem. Integrity is one of the main characteristics of blockchain technology as data that has been appended to the blockchain in the past cannot be removed or altered. Additionally, some blockchain solutions offer the ability to implement functionality; in this case, the integrity of the latter is also ensured.
- **Availability**: Systems need to be available to provide service to the end users. One of the main advantages of blockchain networks is that they are theoretically always available, or in other words their availability is not directly dependent on a single or a few points of failure. In this respect, blockchain technology has been extensively used to increase the availability of IoT systems and services.
- **Authentication**: Surprisingly, it is also common to use blockchain technology in order to implement authentication mechanisms in the IoT. Authentication is commonly achieved by means of challenging and proving the possession of a private key; given the restricted resources of IoT systems, this is not always easily forthcoming.
- **Non-repudiation**: Last, several blockchain/IoT research efforts provide non-repudiation mechanisms. Such mechanisms ensure that system actors are not able to argue on the content or the very existence of interactions with the system, to maliciously gain some benefit. This is also one of the straightforward applications of blockchain technology, as the integrity of past transactions is ensured by the protocol itself.

10.4.1.2 Application Domain

Research efforts that aim to improve IoT security through blockchain usually refer to a specific application domain. However, proposals addressing more than one domains are not uncommon. The main application domains we have identified are:

- **Smart home/city**: There are multiple proposals that address either smart home or smart city environments. These have been the first domains into which IoT applications were developed and the corresponding security and privacy issues were the first to be identified.
- **Supply chain**: Supply chain management is another domain where the application of IoT seems to offer added value. Integrating blockchain technology in such use cases can ensure the integrity of information collected along the whole supply chain, and thus increase trust in the process.
- **Data communication**: Data communication between IoT devices or between an IoT device and a central node is another common use case. Either through authentication schemes or access control mechanisms based on blockchain, several authors propose to enhance the security of such communications.

- **Data marketplace**: There are also some efforts to integrate blockchain technology with data marketplaces. IoT-produced data may be useful to other actors eager to pay in return for getting access to collected data. Blockchain technology is by design coupled with financial transactions, as its mechanics mainly work around a valuable token, the flow of which governs users' behavior.
- **Counterfeits**: Along with the growth in the usage of IoT devices, a new problem has emerged, related to counterfeit devices that either have low quality components or are maliciously designed to function differently than initially intended. Such devices may cause significant security or privacy issues. Blockchain technology has been proposed as a means of controlling IoT devices supply chains, to ensure that no counterfeit devices reach the end user.
- **Healthcare**: A critical domain to which IoT has started being applied to is healthcare. Due to the nature of this domain both availability of devices and data, and confidentiality of information are critical. There are multiple research efforts that relate to applying blockchain technology to healthcare IoT systems to make the latter more secure and safe.
- **Generic**: Finally, several proposals that are not domain-specific, and could theoretically fit any of the domains mentioned above, exist.

10.4.1.3 Technical Maturity

Due to the diversity in hardware, firmware and communication protocols and the limitations of computational resources in the IoT ecosystem, integrating any other technology with IoT systems is not trivial. Particularly when integrating a novel and relatively immature technology such as blockchain with IoT systems, technical validation of the outcome is of high importance. Merely proposing the use of blockchain in IoT systems is not enough, as the feasibility of the solution has to be demonstrated and validated.

For this reason, we have created a scale of 1 (less mature) to 5 (most mature) to rate the technical maturity of each one of the research efforts reviewed herein. This categorization is depicted in Fig. 10.3.

10.4.2 Literature

In this subsection the relevant literature sources are reviewed, categorized per the main security property or service they pertain to.

10.4.2.1 Generic (Several Properties/Services)

It was more common in the past, but is still happens to encounter research efforts that are too generic. Usually the authors reason about applying blockchain technology

in IoT systems, in order to resolve any possible issue and without tackling any limitations.

The authors in [17] propose a lightweight, centrally managed architecture, based on that of the Bitcoin Blockchain, optimized for use in IoT ecosystems. Three tiers have been created (smart home, overlay network, cloud storage), with features that aim to eliminate the disadvantages of the blockchain (scalability problem, high resources, high delay) while maintaining its security level, and also improving availability and accountability in IoT ecosystems. Whilst the authors mix a lot of interesting ideas, their proposal is not mature enough to be applied to real world applications. The same authors propose a more detailed application of the same concept for a smart home case [19]. The description of the proposed system is more thorough and aims to ensure all three security properties for the IoT installation of the smart home, namely confidentiality, integrity and availability. The design is based on a single central node, called home miner, that facilitates the functioning of the system. Because of this approach the system is similar to a traditional centralized system rather than to a truly decentralized system. Using blockchain terminology, such as transactions or mining, is not enough to protect the IoT system. The same authors have further elaborated their approach [18] and presented the Lightweight Scalable Blockchain (LSB). To address scalability problems, computational costs and delays, they implemented a lightweight consensus algorithm, applied a distributed trust method and a distributed throughput management strategy, and separated the flow of the data from the transaction traffic. They also made a lot of progress in terms of evaluating their solution.

The work in [13] aims to enable device owners to manage the data they share in a community scenario where entities need to exchange private information generated by IoT devices. The proposed design has three main layers: A P2P network (e.g. network of IoT devices) for generating and storing private data; a blockchain layer used for certifying IoT devices and offering a way to check data integrity; and a set of access rules at the application layer for owners to set their desired privacy levels. Again, this is a relatively immature work without a technical implementation.

The authors in [8] propose a blockchain-based security architecture for smart cities, divided into four layers (Physical, Communication, Database, Interface).They provide a way to store and share IoT data from devices integrated into the smart city environment and to enable secure communication and data exchange between different smart cities. Their work is at early stages, without specifications or evaluation methodology.

In [35], the authors divide the IoT ecosystem in two layers (high level and edge level) and implement blockchain technology in both of them. This aims to facilitate blockchain adoption for IoT ecosystems and to lower the complexity and computation required for its use, without sacrificing the provided level of security. Eventually, the goal is to provide a secure wide-area network of Internet of Things. There is no implementation and no justification for the validity of the proposal.

The work in [20] presents a hybrid system comprising five layers, that aims to solve the majority of existing security and privacy issues of the IoT, especially in the healthcare domain. A patient-centric approach is assumed, to give patients control

over their EMRs (Electronic Medical Records). Blockchain technology and several other cryptographic techniques are employed to that end. The first layer is the Overlay Network, that recognizes certified IoT devices as nodes and groups them into clusters, to increase scalability. Each of the clusters is associated to a Cluster Head, responsible for key management of devices, patients, and healthcare providers. Next, a Cloud Storage layer is used for storing patient data. It is connected to and cooperates with the Overlay Network for verification purposes. Smart Contracts are another layer, charged with alerting responsible parties when abnormal data is obtained from a patient. The remaining two levels are the main actors of the platform. These include healthcare providers, patients, or wearable IoT devices. The authors provide a very detailed analysis of their approach, without however providing information on how this can be practically applied to the healthcare domain.

A framework to enable secure data transmission between connected nodes, in this case IoMT devices, is presented in [16]. The project also aims at reducing the gigantic volumes of storage required by IoMT devices to process medical records in real time, as well as the replacement of cloud services that are currently being used for storage, since the cloud is a low security and privacy solution. The solution has hashes of all data, obtained either through real time or remote observation of patients, uploaded to the blockchain. The actual data is stored off-chain, since the blockchain cannot accommodate its size. Physicians and health practitioners, as well as care givers have access to the EMRs (Electronic Medical Records).

10.4.2.2 Authentication

An interesting technical implementation is presented in [31], where the authors discuss the risks of creating a single SSH key that is copied to every device a user needs to have access to. They address the key management problem by proposing a custom, private blockchain that will have a block added to it when an SSH public key is added, rotated or revoked. The approach combines collective signing and a custom blockchain to create a secure and easy-to-use, decentralized SSH-key management system.

For the purposes of identity management, the authors of [61] present the Blockchain-based Identity Framework for IoT (BI-FIT). This framework stores device-owner identities on the blockchain and correlates them with the device identities via a signature that has been created with the owner's private key. The signatures are used for authentication and device identification purposes. The whole scheme is user-centric and aims to facilitate the application of security mechanisms and real time monitoring.

The authors in [47] explore the scenario of an information distribution system that is blockchain-assisted, but all blockchain related operations are performed by a gateway which then provides IoT devices with an API. The scheme is presented as a secure way to identify and locate IoT devices. The authors point out security prerequisites for such a system, and explore whether these can be met using blockchain and smart contracts and how current security schemes can be empowered through blockchain.

The goal of [21] is to present a protocol that fulfills both authentication and authorization purposes, and is also sufficiently scalable for widespread use in the IoT domain. The proposed scheme implements blockchain technology and allows seamless integration of new devices (no physical intervention required), while it can adapt to existing authentication techniques. Additionally, it enables continuous identity verification and authorization of devices at the gateway level, even when these are moving.

A blockchain-based, multi layered ID-management framework is proposed by the authors of [48]. In this architecture, all IoT devices are considered to be nodes on the blockchain, but may belong to different categories (lightweight, full, communication), based on the intensity of the computations they can handle and on their connection life. Easy identity verification is achieved though the generation of a unique ID for each IoT device, that is also coupled with the blockchain wallet ID. Attackers are discouraged from repeatedly creating fake IDs because of the cost of such a practice. No proof-of-concept implementation is discussed.

The authors in [49] propose a blockchain-based method for identity and credibility verification for IoT that makes use of self-organizing Blockchain Structures (BCS) to counter the problems that Blockchain-IoT integration presents, such as computational requirements or network throughput. Devices are assigned an identification id and a private key to be used for credibility verification, generated by a Manage Server (MS). Manage Servers also have ids and private keys and are responsible for providing calculation and storage. BCS are small blockchain networks, each managed by a MS. All actions, such as adding or deleting a device, are recorded on the BCS the device was part of. Different BCSs may have a hierarchical relationship to each other. This flexible structure enables IoT devices to form blockchain networks that may not overwhelm their functioning. On the other hand the security guarantees of the approach need to be furthered researched.

In [59], the concept of a physical-logical link through physical chip identification is presented with the purpose of preventing illegal spoofing of physical addresses. The authors advocate replacing the SSD controllers' cash memories with Identification RAMs (IDRAMs), and using them to generate a secret key to pair with the IoT devices public key. The authors confirm that blockchain technology can be utilized to protect data between logical addresses, and by extension, thanks to the link, physical addresses as well.

10.4.2.3 Privacy

Enigma [63] offers the novel opportunity to execute data computation while keeping it private. It is designed to connect to an existing blockchain and load private and intensive computation to an off-chain network. The blockchain stores proof of correct computations for verification purposes, while the off-chain storage and computations are also linked to the blockchain. Enigma offers a management overlay for multi-party computation to enhance its integrity and efficiency.

Another interesting approach is the ChainAnchor [25] architecture which is a blockchain-based, privacy-preserving platform for the commissioning of IoT devices into a cloud ecosystem. It supports device owners who sell their devices' data to service providers, and incentivizes both parties to use the framework. ChainAnchor builds on EPID (Enhanced Privacy ID), and utilizes the blockchain as a means to anonymously register devices for commissioning and decommissioning. It also enables devices to prove that they are genuine without requiring the involvement of a trusted third party. While the concept seems promising, the level of technical implementation is too low.

The work in [15] utilizes a smart contract-based access control architecture previously proposed for the IoT, enhanced in terms of privacy. The authors present an ecosystem comprising service providers, devices (or a cluster of), and storage devices for storing the collected data. The smart home that all the IoT devices are connected to, and the user-owner of the smart home are also identified as main actors of the system. Moving the storage location of the data to trusted nodes and utilizing blockchain to manage access, offers increased privacy.

The authors of [51] propose a network model that aims to preserve privacy and to enable access control by combining attribute-based encryption and blockchain technology. Cluster devices have an important role in the framework. They are defined as devices capable of handling intense computations that are responsible for the processing of data that other IoT devices transmit to them. Miners are necessary for the verification of transactions and are rewarded with tokens that enable them to access data. Attribute Authorities exist to provide Attribute Based Encryption (ABE) and as a way to specify access rights. The approach is interesting, but not much in terms of implementation is provided.

Beekeeper 2.0 [60] was created to mitigate the risk of leaking sensitive information in the context of blockchain-enabled IoT systems. It is a novel approach that simultaneously enables devices to trade data with each other, servers to perform homomorphic multiplications of any degree, as well as additions of encrypted data without ever having access to plaintext data of the devices. The main actors of this framework are the IoT devices, the servers, and the blockchain validators. Servers come to use for devices by processing encrypted data, when being requested to do so. They communicate with the devices through blockchain transactions. The validators of the blockchain, in addition to the usual general verification duties, are also responsible for verifying commitments. Any dishonest behaviour by a server is detected by the data owner and by the blockchain validators.

The blockchain based framework presented in [6] is broken down in three tiers. The first tier includes the Devices, as constrained or unconstrained nodes, as well as the Patient, which functions either as a gateway or as an aggregator. A private blockchain per patient is employed, and this tier is responsible for the creation of new Electronic Health Records (EHR). Data from IoT devices is used for completion of block attributes and the registration, after which the private key of the patient is generated. Before a device can send data, it needs to be authenticated by the patient system. The second tier, made up from Authorities (Hospitals, Labs etc.), is responsible for both accessing existing EHRs and the generation of new blocks. It is

implemented in a public blockchain. A block is added to the authority's chain after it has been visited by a patient, and the same block is sent to the cloud. Authorities can access patient data, but are unable to tamper with it, since it, is recorded in an established block. To achieve perfect privacy, Pseudonym Based Encryption (PBE) is brought into service. The third tier is described as a public blockchain to ensure the compliance of various cloud servers, but is not explored further in this work.

A novel architecture with built-in privacy and adaptability, called modular consortium blockchain architecture for IoT and blockchains, is what the authors of [4] have proposed and implemented. This scheme aims to secure IoT devices communication and data exchange on top of a software stack of blockchains on the IPFS (Inter-Planetary File System). To address scalability problems, the authors have divided the workload on many smaller private blockchains called sidechains, that join up to form a consortium network, which they can be added to or removed from at any given time. The sidechains log hashes for all activity related to sensor data from sidechain members and the data itself is stored on the IPFS, while a public blockchain run by the whole network keeps records of all access requests between consortium members, and their outcome, to enable accountability. This distribution helps overcome privacy issues. Each IoT network associated with a sidechain has IoT devices and a single validator as its members. Devices send encrypted data to the validator, who in turn logs the data and its hash to the IPFS and to the blockchain respectively. A smart contract is activated to enforce access control in the sidechain; to ensure that only data by authorized origins reaches the validator; and to store the public keys of requesters with access rights along with the public keys of the data they have access to. A similar, Access Control performing smart contract, runs on the consortium blockchain and also stores the devices that are entitled to submit access requests. To become a requester, one must first join the network, then sign a request transaction with their private key, and if they end up receiving the IPFS file hash, decrypt it with their private key to access the information.

10.4.2.4 Access Control

The authors of [62] have designed a platform that grants users of mobile phones access over data provided by service-providing entities. For that purpose, a blockchain is being used as an access control manager, storing a pointer to the data and sending the actual information to a distributed, private, key-value data store. The proposed approach is interesting, but the authors do not provide information on the practical specifications of the proposed blockchain implementation, such as the number of nodes or the security of the consensus mechanism.

The authors of [24] introduce Bubbles of Trust, a decentralized system based on blockchain, which aims to facilitate the authentication of devices against each other. The proposed system creates virtual secure zones (bubbles) around master IoT devices. Follower devices are identified by signing object IDs with the associated private keys and are given authentication tickets. Devices with tickets can request to be associated with a bubble, in order to be considered trusted by other bubble

members. A bubble is protected and non-member devices cannot access it. Member IoT devices should only communicate with other members of their bubble, as those are the only verified trusted devices. All communications are practically associated with blockchain transactions and must therefore be validated according to bubbles' membership. The proposal is technically thorough and sufficiently tested.

The authors in [30] present a framework for access control based on smart contracts. The application comprises three different kinds of smart contracts. Several Access Control Contracts (ACCs) are implemented, each offering a different access control method for a subject-object pair. ACCs provide two kinds of access control verification, namely static, based on predefined rules; and dynamic, based on the object's behavior. Information about misbehavior is sent to a single Judge Contract (JC), which is responsible for imposing penalties. Finally, registering and updating of allowed interactions is achieved through the Register Contract (RC). The proposed framework has been implemented by using the Ethereum platform and Rpi3 as IoT devices, in order to showcase its validity.

The authors of [46] have developed the ControlChain system, which relies heavily on blockchain technology. It is a scalable, user friendly and compatible to existing access control mechanisms model for authentication and authorization optimization. It utilizes an off-chain side channel, for the propagation of time-sensitive data, as well as four different blockchains. The Relationships Blockchain is responsible for storing the public data and relationships of all entities. The Context Blockchain stores contextual info on users and devices that are then taken into account in authorization decisions, and the Accountability Blockchain holds all information about entity behavior, actions performed and access control permissions. Finally, the Rules Blockchain stores authorization guidelines by owners to objects, or objects to themselves. While the authors describe general blockchain implementations, they present E-ControlChain, a proof of concept implementation to be deployed on the Ethereum network.

EdgeChain [45] is an edge-IoT framework that aims to connect the account of every IoT device to edge cloud resources. The main idea is to regulate how light devices may access and utilize offered resources in a secure way. Blockchain technology is used to record all transactions and activities, and smart contracts are brought in as means to enforce rules and regulate device behavior. The authors aim to construct a framework that will drive efficient utilization of resources from IoT devices by controlling their activity through behavioral economics. While testing has been done on a private blockchain, the scheme has been built on the Ethereum network.

In [41], a framework that utilizes blockchain technology to enforce access control policies in IoT networks is presented. It is a lightweight, mobile, scalable design that does not directly integrate the blockchain functionality into the devices, thus ensuring that even those with the most limited resources can be part of the network. Entities named managers interact with the contract to add and update access control rules. They do not need to be continuously connected to the network and have no requirements to meet in terms of computational strength or memory. Management control hubs are a special type of node in wireless sensor networks that, while not part of the blockchain, are continuously connected to a blockchain node. They need to

have high performance capability, as they handle all the requests for information on access control policies on behalf of devices with limited resources. Each IoT device needs to be registered under a hub, and to use a public key as its unique identity. The whole scheme, while tested on a private Ethereum network, is meant to be carried by a public blockchain.

The authors in [50] secure information exchange in the healthcare ecosystem, and hand information access control over to the patients, through a blockchain-dependent framework. They propose the use of mobile edge computing (MEC) for securing in-home therapy management. They combine this with a blockchain infrastructure to offer low-latency, secure, anonymous, and always-available therapeutic data communication. They propose trustless nodes of two kinds; edge nodes, that analyze and share with the cloud the data that IoT devices forward to them, and cloudlet server nodes, that reinforce the data processing, storing and analysis. Trusted nodes have the duty of verifying the therapy transactions within the blocks. While the authors discuss the use of a blockchain system and a tor layer that can enhance data exchange in such scenarios, they do not analyze how this blockchain system practically functions. They provide some use case implementations but with limited technical documentation.

A prototype for tracking the supply chain and detecting counterfeits by bringing blockchain technology and Physical Unclonable Functions (PUFs) into service is being proposed by the authors in [28]. They make use of a custom private blockchain to store PUF data and info for each Integrated Circuit (IC) to enable authentication. On each block, verified transactions are stored to record the transfer of ownership for an IC between owners. The protocol enhances security by enabling only legitimate IP address owners to profess themselves initial owners of an IC, and only current owners to fire a transferring transaction.

In their first two works on the FairAccess framework [42, 43], the authors describe its earliest and most simplified version. According to their design, any subject identified with a requester address wishing to access protected data will be able to submit a request through its wallet, which is acting as a Policy Enforcement Point (PEP) and is charged with regulating the protected resources. The PEP expresses the request through a GetAccess transaction and shares it with the miners, who will evaluate it and rule whether the request is to be accessed or denied. The evaluation is done by comparing the transactions unlocking script to the GetAccess locking script. Transactions deemed valid will be recorded on the blockchain. The authors extend their approach in [44], but the justification of their approach suffers from insufficient analysis.

The authors of [52] introduce the concept of the Internet of Smart Things, where Smart Things are defined to be devices that have been provisioned with Artificial Intelligence (AI) features that enable them to be autonomous. A permission-based blockchain protocol (Multichain), that offers secure communication at low cost, is employed to create a network of such devices. While the contribution of the work is unclear, the authors present an implementation of their approach.

The work in [54] describes an auditable, resilient, integrity preserving, blockchain-based framework for sharing and storing IoT data. Resources are organized in streams, per which ownership and sharing rights are defined. They are stored off-

chain (on-premise storage/cloud/distributed P2P network), while a corresponding identifier is stored on the blockchain, making it tamper-proof. End-to-end encryption of the data takes place before data is stored. Access control is enforced through blockchain, on which the access permissions are stored for each data stream. A blockchain transaction contains information on the ownership of the stream and its corresponding access permissions. Stealth addresses are used to preserve privacy. Storage nodes, in the case of an access request, consult the blockchain to determine whether to grant access or not.

10.4.2.5 Integrity

A blockchain-based framework is proposed as a means to provide a Data Integrity Service for transactions of IoT data for both data owners and consumers [37]. Both of them act as blockchain nodes. The proposed system is built on the blockchain and implemented in a smart contract, while cloud storage services are used as general purpose data storage. The proposed service framework is reliable and able to handle an increasing number of clients that trade for IoT data. The implementation is based on a custom blockchain network, while a significant part of the functionality has been left as future work.

In [40], through an Ethereum Smart Contract, an application that enables the detection of Counterfeit IoT devices is realized. This is achieved by tracking the ICs that IoT devices will consist of down the supply chain, logging their owners until they are ultimately part of a device. Furthermore, authentication is made possible, since all ICs and IoT devices are linked to their own PUF-derived unique ID. The authors provide a proof of concept implementation for the blockchain functionality of their approach.

The authors of [38] present a three-level blockchain solution for ensuring data integrity and identity verification. The first blockchain layer, named IoT, includes devices like sensors and gateways. It is secure, time predictable, and achieves energy-efficient communication, through a Proof of Trust protocol, which is based on the Trustful Space-Time Protocol (TSTP). Fog is the second blockchain level of this architecture, and its based on the Proof of Luck consensus algorithm. It enables secure communication between gateways and the cloud storage and the blockchain, and protects against data loss. The final blockchain level is the cloud. It provides semi-trusted data storage and identity verification and can function with any agreement algorithm. The authors have systematically approached the problem of securing the whole IoT ecosystem stack, but the implementation they provide does not prove the concept.

An architecture meant to be integrated into a Smart Factory environment in order to increase data privacy and ensure its integrity is proposed in [58]. It is broken down in 5 layers with specific responsibilities. The sensor layer includes the IoT sensor devices, along with a microcomputer with sufficient computing power, that collects information from factory equipment. The entities of the Management Hub layer are the blockchain nodes and are record blocks. They are also responsible for parsing,

encrypting and packaging collected data, and for including it in the blocks they generate. The Storage layer is where blockchain technology comes in, in the form of a private network. The Application layer is responsible for providing services to users, and last but not least, the Firmware layer encompasses the technologies required to guarantee the smooth cooperation of all layers. To ensure data integrity and information privacy, the SHA256 hashing algorithm and Elliptic Curve Cryptography are employed. A use case scenario is provided, without however any actual implementation.

The authors in [26] present an attribute-based blockchain model for the management of IoT devices. In this framework there are two types of nodes, each with their respective set of attributes. Primary nodes are responsible for block generation and for storing transactions in them, while backup nodes handle the creation of new transactions, and read transaction information from a block, provided they have the right attributes that enable them to decrypt the data. Blocks are classified in different categories, such as a New Transaction Block (NTB) which is generated for each new IoT device to be traded, carrying a unique identifier for it, as well as all device and transaction related info. Device Maintenance Blocks (DMtB) are created when maintenance is required for a device; they come with maintenance related info, and the device's identifier. Access Control and other security policies are stored in Device Management Blocks (DMgB). The main actors in this case are manufacturers, sellers, purchasers and administrators. Manufacturers produce and trade IoT devices, and may need to maintain equipment. Thus, they have the right to interact with NTBs and DMtBs. Sellers also trade IoT devices and can send messages to NTB blocks. The Purchasers are the ones that receive ownership of a device and can write into NTBs. An Administrator is an entity that is responsible for regulating IoT devices, and managing Access control policies; they interact with DMgBs. An Authority Agency is the point where users (manufacturers, sellers, purchasers) apply to join the network. This entity has to verify the applicants' identities, and then distribute public parameters and a master key to each of the accepted ones. All of this information is then included in an Authority Agency-signed certificate.

The authors of [11] focus on laying out the requirements, principles and design for a blockchain-based Sensor Data Protection System (SDPS). Furthermore, they have implemented a SDPS system using Ethereum, that satisfies the aforementioned criteria. Their scheme combats odometer fraud on mileage data gathered from cars, and makes the collection, processing and exchange processes of that data inviolable, in a scalable, economically feasible manner. The architecture is called CertifiCar and through it data is collected from sensors, cross-validated and transmitted via blockchain transactions. Raw data is stored in secure mass storage, and hashes derived from it are stored in the blockchain. Through the comparison of stored hashes to hashes calculated from raw information, data consistency can be verified. The authors went through three possible implementations before settling on the final prototype. The end product can detect continuous odometer fraud, has a smartphone app that gives data owners the options of sharing with clients only the current odometer value, thus protecting any detailed car usage information, and also lets them share historic

data to establish trust. The product was evaluated in a field test with 100 cars and by a focus group of 16, as well as through various interviews and workshops.

DroneChain [36] is a blockchain-based architecture used for ensuring data integrity in a scenario where drones are collecting data from IoT devices. The main entities of this system are the drones, which are enrolled as data collecting nodes and are identified by a unique ID. Their functions are to collect sensor data and send it to a Control System (CS), from which they also receive commands. Control Systems in this framework are also identified by an ID. After receiving data from the drones, they are charged with hashing it, and sharing hashed data and with the blockchain network and original data with the cloud server. Blockchain can then be used to ensure the integrity of exchanged data or commands.

The authors in [5] present a design that replaces the single server of the ACE authorization framework [53] with a blockchain, and utilizes the OSCAR security model [57] to build a more secure access control architecture for the IoT. The components of the scheme are: Recourse Servers (RS) that generate and store protected resources; Proxy Servers that store encrypted data if necessary; and Recourse Owners (RO) that legally claim the RS and the data they generate. Blockchain is used to manage the authorization requests and grant access in a secure way. The framework was tested and evaluated using a private Ethereum network.

The difficulties of merging blockchain technology with the IoT are analyzed, and popular techniques for achieving the integration are showcased in [55]. The authors present a Hyperledger Fabric-based system, structured in five distinct layers. The first layer consists of sensors, connected to Raspberry Pi devices, which make up the second layer, namely the Edge Device layer. Raspberry Pi devices function as peer nodes and structure data acquired from sensors into transaction format. After those transactions have been peer validated, they are sent to the Orderer nodes, that exist in the Cloud layer and unburden Raspberry Pi devices of block creation. Valid data is encompassed in blocks and committed blocks are broadcast back to peers.

The utilization of Ethereum smart contracts and PUFs is being proposed in [29] for the purpose of preventing attackers from impersonating IoT devices or tampering with the data sent by legitimate devices to spread malicious software. IoT devices can register to the BlockPro network, through smart contracts. Two smart contracts have been designed for this system. One is charged with ensuring safe communication between registered IoT devices, by acting as an intermediary between the devices and the servers of the network, by checking the legitimacy of participating devices. The second smart contract can only be invoked by the first, and is responsible for manipulating information, uploading to and receiving from the blockchain already verified data. Servers/miners are the nodes that deploy the smart contracts and are registered as trusted hosts. They are also responsible for maintaining optimal blockchain operation.

IoT data integrity is protected through the use of blockchain technology in a series of works [12, 32, 33, 56] related to the GHOST research project [1] which deals with the security of smart home installations. Three different use cases are described that are related to forms of consent, software integrity and IP blacklisting. In each installation a smart home gateway functions as a blockchain node, equipped with an

account (pair of keys) coupled to the home owner. In the first use case, traditional forms of consent have been replaced by a blockchain mechanism. Through this smart home users accept the terms of use for their installation set up by their service provider. The users are not able to use the system, without having accepted the terms of use. The second use case is related to ensuring software integrity for the system itself. The hash of the software installed on the device is periodically calculated and it is compared to the valid software's hash stored in the blockchain. Finally, the reputation of each external IP is built upon reports submitted by all installed gateways. Specifically, each gateway is equipped with a risk engine component that calculates risks associated with each connection and thus each IP. If this risk is high, the gateway reports the specific IP as malicious to the blockchain. The reputation score for each IP is calculated upon multiple factors, such as time, number of different gateways reporting the IP as malicious or requests to remove the reports. The platform of choice is a private Ethereum network built by using smart home gateways as nodes.

10.5 State of the Art Analysis

10.5.1 Trends in State of the Art

An extensive literature review was conducted to identify papers that have been published over the last four years and are relevant to the employment of blockchain technology to resolve privacy or security issues in the IoT domain. Searched databases were the ACM Digital Library, IEEE Xplore, and Springer. Google Scholar was also employed for retrieving additional research results published elsewhere. Combinations of the following keywords, were used to identify works relevant to this study: *blockchain, IoT, security, privacy, integrity, authentication, availability* and *non-repudiation*. Papers related to IoT, blockchain, and at least one of security, privacy, integrity, authentication, availability were studied. The references of these papers were also analyzed to identify additional relevant publications. This exhaustive search resulted in the identification of 73 papers relevant to this subject. A more detailed analysis of those led to discarding several papers, either because of low relevance or of very low quality. This procedure reduced the number of the papers to be analyzed to 49. For all these, the following have been analyzed:

- Security goals
- Main security goal
- Relevant application domains
- Technical maturity.

From Fig. 10.1 it is obvious that there is an increasing trend in the number of publications, starting in the early 2017. Before then one or two papers per semester appear. Starting from the first semester of 2017 the number of published papers is continuously increasing. The lower number in the first semester of 2019 is due to

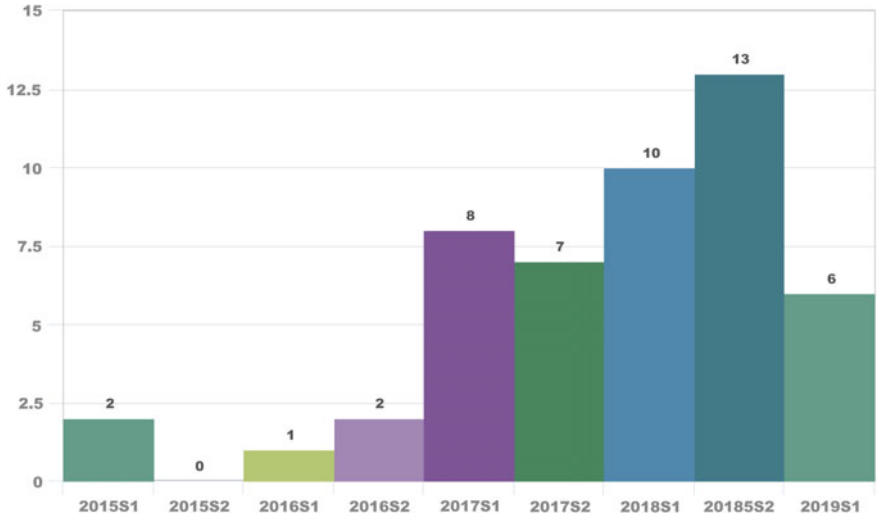

Fig. 10.1 Papers per semester

the fact that we have been able to analyze publications only in the first three months of the semester, at the time of conducting our survey. It is, however, evident that applying blockchain to IoT systems in order to enhance privacy and security is a hot topic and we expect to see more publications in the coming years.

The distribution of the application domains to which examined papers apply is depicted in the pie chart of Fig. 10.2. It has to be mentioned that multiple papers proposed systems or methodologies applicable to more than one application domains. A large portion of the papers stated that the proposed methods are domain agnostic and can function in every scenario. Apart from that, there were two dominant application domains, namely smart home/cities and data communication. Our view is that smart home/cities is the most common use case for IoT systems, so it is normal to have more blockchain integration efforts in that domain. Regarding the data communication it seems that there is a good fit that enables to provide enhanced communication schemes between IoT devices by using blockchain technology. Integrity of data and immutable access control mechanisms are the main benefits of this approach. The remaining papers are split among other domains. The only domain that is statistically more significant than others is healthcare, presumably due to the criticality of its applications.

A good overview of the results we found is depicted in Fig. 10.3. Most of the papers had more than one security goals but in order to classify those we have identified the main security goal for each one. Out of 49 papers, 14 were mainly related to integrity, 13 to access control, 7 to privacy, 7 to authentication, while 8 of the papers equally aimed to multiple security goals so they were classified as generic. The majority of the papers mainly deal with integrity, as blockchain can secure data and offers an immutable storage resource, although there are significant limitations

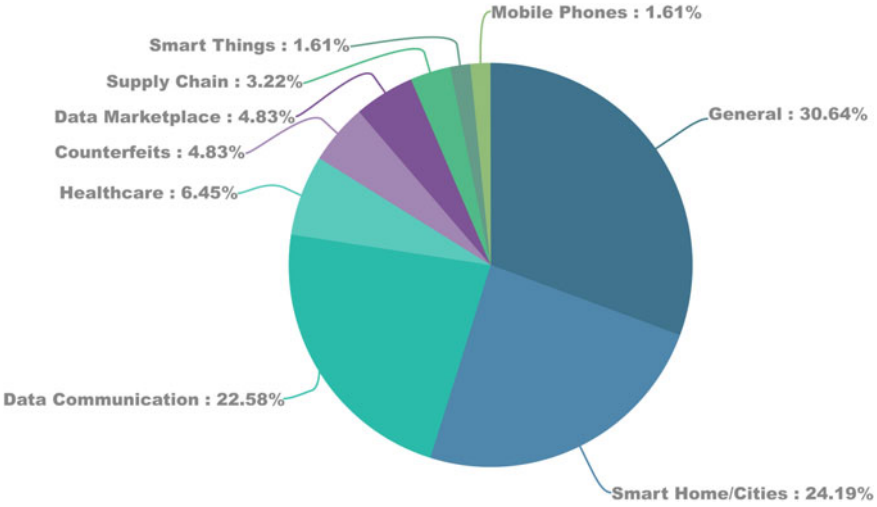

Fig. 10.2 Application domains distribution

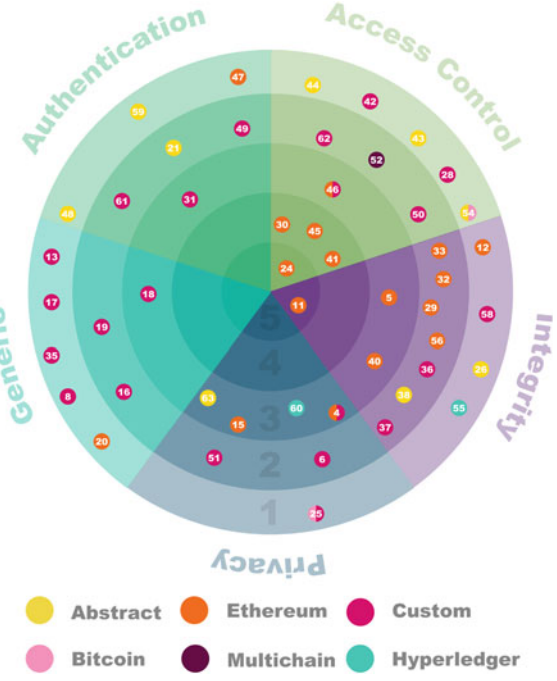

Fig. 10.3 Technology radar for blockchain application to IoT security and privacy

in terms of size and efficiency. Equally frequent are papers that set up access control mechanisms over blockchain technology. Theoretically, blockchain offers a trusted decentralized architecture that can apply access control rules, without any actor in the system being able to maliciously alter or cease this functionality. There are some efforts that aim to protect user privacy, mainly by combining blockchain mechanisms with cryptographic workflows, in order to create private workflows the integrity of which is also assured. There is another medium-sized group of papers that deals with authentication. Authentication schemes usually rely on a central node against which other nodes authenticate. This is problematic and inefficient for heterogeneous networks of numerous IoT devices, thus some blockchain related approaches have been proposed throughout the last years. Finally there is an important portion of papers that propose holistic solutions that aim to solve more than one security problems for IoT ecosystems.

Figure 10.3 depicts all papers analyzed through a technology radar approach. Specifically, the circle is split into five different triangular subareas (each one differently colored) which correspond to the five different taxonomies identified according to the main security goal of each paper: integrity, access control, privacy, authentication and generic. The five rings in the circle represent the five different levels of technical maturity (1–5) of the papers. Each paper is denoted on the figure with a small circle placed at the proper triangular subarea and the proper ring. Additionally, the color of the paper circle corresponds to the blockchain implementation employed in each one of the papers, to depict any correlations. The different options for blockchain implementation are Ethereum, Bitcoin, Hyperledger, Multichain or custom implementations. There are some papers that only present abstract implementations and some others that state that the approaches presented can be applied to any blockchain. Both cases seem problematic, as papers that belong to those do not technically justify their claims.

It is obvious that the average technical maturity of the proposed solutions is very low. Out of 49 papers only 5 are in the two inner rings (technical maturity 4 or 5). This means that most of the papers, approximately 90%, propose unjustified schemes that even if theoretically sound, come with a relatively high risk of not being applicable to real world IoT systems. Additionally, it is evident that the more technically mature a proposed approach is, the more likely it is that this approach is implemented in one of the ready to use blockchain platforms (mainly Ethereum). Papers that discuss the custom blockchain implementations tend to be located in the outer rings of the circle. Building a custom secure blockchain system is a difficult procedure that requires a lot of effort and should be avoided in the first place. It is also evident that the main security goal of the paper is correlated to some extend to the technical maturity of the paper. Papers aiming to access control seem to be of a higher technical level, papers aiming to generic solutions seem to be of a lower technical level and papers in the other taxonomies seem to be of a medium technical level.

It is evident that trying to apply blockchain technology to appropriate specific problems is more successful in general than trying to apply it to any generic problem. Additionally, trying to employ already built and tested platforms is also beneficial for the proposed approach than trying to build everything from scratch.

10.5.2 Common Problems

Through conducting an extensive analysis of papers regarding the incorporation of blockchain technology into the Internet of Things, we have identified patterns of disadvantageous approaches to the problem. Those precarious practices are presented and discussed in this subsection.

10.5.2.1 Blockchain Limitations

While some would argue that the most appropriate approach for a secure, decentralized application would be to use an established blockchain network, under no circumstances can it be said that this comes without drawbacks, and those unavoidably affect any design that chooses to adopt them. Ethereum is the most popular platform for implementations that require anything more than simple transactions, but the security it provides comes at a cost. Fees for single transactions may sum up to high amounts that make the proposed applications too expensive to be deployed.

Currently, Ethereum can process 15 transactions per second. Keeping in mind that there is a significant number of applications running on it, many of which require an equally large amount of transactions to go through each day, and factoring in the individuals that are also using the blockchain, we end up with a considerable scalability problem. Thankfully, there is a number of both proposed and recently activated solutions for this predicament. It must be noted that such problems are not exclusive to the Ethereum network. The Bitcoin network has a maximum block size that severely limits its throughput and results in an average of 3–7 transactions per second, meaning it is also suffering from scalability issues.

Another platform that is relatively frequently opted for is Hyperledger Fabric. While it is more scalable than other major blockchain networks, its consensus algorithm is not viewed as particularly secure, it does not offer a miner incentive and does not provide complete transparency or immutability. This makes it suitable for quite a limited variety of use cases that only allow trusted parties to participate.

When proposing the use of any of these platforms for deploying a blockchain application, the aforementioned limitations should be taken into account. This is not the case in most of the analyzed papers, as the authors neglect these issues during the design of the proposed methodologies and end up with schemes that are inefficient or even inapplicable to the IoT.

10.5.2.2 Custom Blockchain Implementations

In an effort to escape scalability limitations, delays, and most importantly, costs, many opt for creating a custom blockchain instead of using an existing one. This is a choice that almost unavoidably means sacrificing security. While such a route could function acceptably in a very targeted or privatized framework, it is unlikely to

be beneficial in any other context. A blockchain network requires numerous nodes in order to operate the way it is supposed to. It has to be a vigorous network, with nodes that are widely dispersed, otherwise it cannot reach its full potential. Custom blockchains can rarely claim to have the required number of nodes to guarantee the level of security they are supposed to be providing. Most rely on achieving it as the network grows, which still leaves them quite vulnerable during their early life, and possibly longer, since there is no guarantee that the implementation will be adopted widely enough to achieve the number of desired participants.

10.5.2.3 Partially Decentralized Schemes

The integration of blockchain technology with the IoT is a tricky endeavor, since most commonly used IoT devices are very limited in terms of computational power. Most observed formats opt for sacrificing decentralization to overcome that obstacle. They choose to burden few, but more capable devices with the weight of the calculations required to participate in a blockchain network. Constrained devices are therefore dependent upon those gateways for handling their communication with the blockchain, resulting in a hierarchy in the system.

Additionally, in an attempt to organize authorization and verification processes, many frameworks have resorted to grouping devices and appointing managers that have to coordinate actions and communication, again creating some sort of central management. It is also a common practice to give certain entities the responsibility of granting and revoking permission to participate in such groups or even the whole network itself. Even though it is clear that this is being done for security reasons, it still differentiates one device from another, and creates inequality in an environment that is supposed to be functioning without central authorities.

Such designs are plagued by similar risks as fully centralized systems do, especially if the more powerful nodes are very few. They pose enticing targets for attackers, and the damage caused by a malicious device that has more freedom, power, and is responsible for the regulation of participating devices, is quite difficult to control. A denial of service (DOS) attack against those elevated nodes could render the entire system unusable.

Furthermore, to deal with the fact that storing large amounts of information in the blockchain would come at an extraordinary cost, some choose to store protected, sensitive data the traditional way, using on-site storage, or the cloud. Storing resources in that manner provides malicious entities with a single target that would give them access to the entirety of the sensitive, private information.

10.5.2.4 Unsecured Edge Devices

It comes without saying that an attacker will always go for the weakest component of a whole. In the cases being studied, those are the edge devices of each network. Most of the architectures presented up till now take few to no precautions towards securing

the edge IoT devices, thus undermining most of their work, since the network will always be only as secure as those devices are. At best, means for detecting and isolating a compromised device are provided, and ways to limit the damage it can cause are established, but the designs that actually guard against attackers in the first place are few to nonexistent. While such "tamper-evident" implementations might be able to correct the damage or revert the alterations on the data, they cannot effectively prohibit third parties from accessing it.

On top of that, the vast majority of proposals attempt to ensure data integrity or validity only after data has left the device it was procured from. We have seen an abundance of approaches when it comes to ensuring information is safe, private and remains unchanged after being collected by an IoT device, but a notable lack of measures to verify data and ensure it is tamper proof before it is transferred out of the devices.

10.5.2.5 Lack of implementation

Since almost all of the works are proposing frameworks and architectures to be implemented, some sort of evaluation of the suggestion is expected to identify whether it would be operational and beneficial to the ecosystem. Even through most works include such a section, the vast majority only explores the blockchain side of their scheme, and few to no tests are conducted with regards to the IoT devices. It is hard to simulate an implementation of that scale, and yet necessary, to verify it will continue to work as intended when many entities are using the system. Lack of such testing results in proposals that may very well turn out to be not advantageous at all, or even not applicable in real-world scenarios.

10.5.3 Proposed Approach

While there has been a lot of research with respect to applying blockchain technology to solve IoT security and privacy problems, it seems that it has not been as effective as required. In our view, the main axes around which such research efforts should focus in the near future are :

- **Technical validation**: The IoT ecosystem is characterized by high diversity in terms of hardware devices, firmware and software installed on those, communication protocols and middleware devices used to connect IoT devices to wide area networks. Apart from that, such systems are characterized by limited resources in terms of computational power, storage capacity or energy consumption as many devices operate on batteries. Proposing a blockchain integration scheme for IoT systems may be promising, but until it is implemented and technically validated it can be regarded as non-functional in real world environments. New approaches have to be at least tested against a general IoT setup, to check they

are applicable under IoT limitations. Even if such a test is successful, diversity in IoT environments has also to be taken into account, in order to propose a methodology applicable in the IoT in the long run.

- **Research on the device level**: Another common pattern is methodologies that secure the network communication or the data storage for IoT devices, but in the same time neglect to secure the devices themselves. A system is as secure as its weakest link. It does not make sense to design immutable blockchain systems for managing IoT devices output, if we have not first secured the devices themselves in order to be sure about the integrity of the data those output to our system. There are some interesting research efforts that propose the use of hardware security techniques such as trusted execution environment or the integrity checking of hardware through PUF technology, to ensure that devices function legitimately. Such features have to be integrated into blockchain-based systems in order to establish trust upon the complete workflow.
- **Build upon existing blockchain technology**: Many researchers propose custom blockchain implementations that fit with IoT limitations, at least in the context of specific applications. This approach is problematic as building a secure custom blockchain platform, requires significant effort, that is not usually committed or even available. Additionally, most of the security properties of blockchains stem from the assumption that there are multiple nodes connecting to each other, and maliciously altering information on the system requires the collaboration of too many nodes, which cannot happen. Custom blockchain implementations usually drive to blockchain networks consisting of too few nodes, so this assumption does not hold.
- **Genuinely decentralized design**: Current blockchain technology comes with significant drawbacks that makes its application problematic. The most obvious of those are scalability issues, speed and privacy. It is common to try to overcome these drawbacks by proposing the use of either private blockchain networks or permissioned ones in which some nodes hold more power than others. While these approaches partially resolve blockchain inherent problems, they also come with reduced security guarantees. The right direction is to improve blockchain technology, in order to resolve the existing problems while avoiding to create insecure blockchain networks.

10.6 Conclusions

Blockchain technology, a shared Peer-to-Peer distributed ledger, which is the underlying artefact of crypto-currencies that started with the proposal of a digital asset and payment system, has disrupted the technological development in various domains. Blockchains have begun to have a significant influence in the IoT domain and present a wide variety of opportunities for enhanced security and privacy in IoT. The Internet of Things has changed traditional computing models. While it has enabled multiple new computing applications, it has also created significant issues related to security

and privacy. The world is now gradually moving towards using extended computing architectures, the nodes of which may be lightweight devices limited in hardware resources, scattered in terms of network topology and too diverse in terms of hardware and software, to be efficiently administered and managed. Additionally, such nodes usually store, process and transmit sensitive private data of their users, so the risk of any security event is significantly high. Blockchain technology enables the development of secure decentralized systems. It offers guarantees regarding data integrity, application logic integrity and service availability, while it lacks in terms of privacy and efficiency. In this chapter, we have presented a case for convergence of blockchain technology and the IoT, we have analyzed potential use cases where blockchain technology can be harnessed to enhance security and privacy in the IoT, and we have proposed a set of required features in blockchain technology for it to be effectively applied in the IoT.

References

1. https://www.ghost-iot.eu/
2. ISO/IEC 25010:2011(en) Systems and software engineering Systems and software Quality Requirements and Evaluation (SQuaRE) System and software quality models
3. Proofpoint Uncovers Internet of Things (IoT) Cyberattack (Jan 2014), https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack
4. M.S. Ali, K. Dolui, 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
5. O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, F. Zanichelli, IoTChain: a blockchain security architecture for the Internet of Things. IEEE Wirel. Commun. Netw. Conf. WCNC **2018-April**(October), 1–6 (2018). https://doi.org/10.1109/WCNC.2018.8377385
6. S. Badr, I. Gomaa, E. Abd-Elrahman, Multi-tier blockchain framework for iot-ehrs systems. Proc. Comput. Sci. **141**, 159–166 (2018)
7. D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, in *Sequences Ii* (Springer, 1993), pp. 329–334
8. K. Biswas, V. Muthukkumarasamy, *Securing Smart Cities Using Blockchain Technology* (2017). https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198, https://www.researchgate.net/publication/311716550
9. J. Brito, A. Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center at George Mason University, 2013)
10. V. Buterin, *On Public and Private Blockchains* (2015). https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/
11. M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, Privacy-preserving data certification in the internet of things: leveraging blockchain technology to protect sensor data. J. Assoc. Inf. Syst. (2019)
12. A. Collen, N. Nijdam, J. Augusto-Gonzalez, S. Katsikas, K. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami et al., Ghost-safe-guarding home IoT environments with personalised real-time risk control, in *International ISCIS Security Workshop* (Springer, Cham, 2018), pp. 68–78
13. M. Conoscenti, A. Vetr, J.C. De Martin, Peer to peer for privacy and decentralization in the internet of things, in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)* (2017), pp. 288–290. https://doi.org/10.1109/ICSE-C.2017.60

14. M. Conoscenti, A. Vetro, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (IEEE, 2016), pp. 1–6
15. T.L.N. Dang, M.S. Nguyen, An approach to data privacy in smart home using blockchain technology, in *2018 International Conference on Advanced Computing and Applications (ACOMP)* (IEEE, 2018), pp. 58–64
16. N. Dilawar, M. Rizwan, F. Ahmad, S. Akram, Blockchain: securing internet of medical things (iomt). Int. J. Adv. Comput. Sci. Appl. **10**(1), 82–89 (2019)
17. A. Dorri, S.S. Kanhere, R. Jurdak, *Towards an optimized blockchain for IoT* (October), 173–178 (2017). https://doi.org/10.1145/3054977.3055003
18. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, LSB: a lightweight scalable blockchain for IoT security and privacy. Tech. rep. https://arxiv.org/pdf/1712.02969.pdf
19. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (IEEE, 2017), pp. 618–623
20. A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**, 326 (2019)
21. A. Fayad, B. Hammi, R. Khatoun, An adaptive authentication and authorization scheme for IoTs gateways: a blockchain based approach, in *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)* (IEEE, 2018), pp. 1–7
22. P. Francis, *Blockchain, The Byzantine Generals Problem, and The Future of Identity Management* (2016). https://medium.com/@philfrancis77/blockchain-the-byzantine-generalproblem-and-the-future-of-identity-management-6b50a2eb815d
23. S. Haber, W.S. Stornetta, How to time-stamp a digital document, in *Conference on the Theory and Application of Cryptography* (Springer, 1990), pp. 437–455
24. M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018). https://doi.org/10.1016/j.cose.2018.06.004, http://www.sciencedirect.com/science/article/pii/S0167404818300890
25. T. Hardjono, N. Smith, Cloud-based commissioning of constrained devices using permissioned blockchains, in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (ACM, 2016), pp. 29–36
26. Q. He, Y. Xu, Z. Liu, J. He, Y. Sun, R. Zhang, A privacy-preserving internet of things device management scheme based on blockchain. Int. J. Distrib. Sens. Netw. **14**(11), 1550147718808750 (2018)
27. A. Heikkila, *The Blockchain and The Byzantine Generals Problem* (2017). http://techblog.cosmobc.com/2017/03/16/blockchain-byzantine-generals-problem/
28. M.N. Islam, V.C. Patii, S. Kundu, On IC traceability via blockchain, in *2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT)* (IEEE, 2018), pp. 1–4
29. U. Javaid, M.N. Aman, B. Sikdar, Blockpro: blockchain based data provenance and integrity for secure IoT environments, in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems* (ACM, 2018), pp. 13–18
30. X. Jiang, Y. Shen, Y. Zhang, J. Wan, S. Kasahara, Smart contract-based access control for the internet of things. IEEE Internet of Things J. **PP**(c), 1–1 (2018). https://doi.org/10.1109/jiot.2018.2847705
31. L. Kokoris-Kogias, L. Gasser, I. Khoffi, P. Jovanovic, N. Gailly, B. Ford, Managing identities using blockchains and CoSi, in *HotPETs 2016—9th Workshop on Hot Topics in Privacy Enhancing Technologies (EPFL-TALK-220210)* (2016). https://infoscience.epfl.ch/record/220210/files/1_Managing_identities_bryan_ford_etc.pdf
32. C.S. Kouzinopoulos, K.M. Giannoutakis, K. Votis, D. Tzovaras, A. Collen, N.A. Nijdam, D. Konstantas, G. Spathoulas, P. Pandey, S. Katsikas, Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust, in *2018 Innovations in Intelligent Systems and Applications (INISTA)* (IEEE, 2018), pp. 1–6

33. C.S. Kouzinopoulos, G. Spathoulas, K.M. Giannoutakis, K. Votis, P. Pandey, D. Tzovaras, S.K. Katsikas, A. Collen, N.A. Nijdam, Using blockchains to strengthen the security of internet of things, in *International ISCIS Security Workshop* (Springer, Cham, 2018), pp. 90–100
34. L. Lamport, R. Shostak, M. Pease, The byzantine generals problem. ACM Trans. Program. Lang. Syst. (TOPLAS) **4**(3), 382–401 (1982)
35. C. Li, L.J. Zhang, A blockchain based new secure multi-layer network model for internet of things, in *2017 IEEE International Congress on Internet of Things (ICIOT)* (IEEE, 2017), pp. 33–41
36. X. Liang, J. Zhao, S. Shetty, D. Li, Towards data assurance and resilience in IoT using blockchain, in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (IEEE, 2017), pp. 261–266
37. B. Liu, X.L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain based data integrity service framework for IoT data, in *Proceedings—2017 IEEE 24th International Conference on Web Services, ICWS 2017* (2017), pp. 468–475. https://doi.org/10.1109/ICWS.2017.54
38. C. Machado, A.A.M. Fröhlich, IoT data integrity verification for cyber-physical systems using blockchain, in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)* (IEEE, 2018), pp. 83–90
39. S. Nakamoto, *Bitcoin: A Peer-to-peer Electronic Cash System* (2008)
40. L. Negka, G. Gketsios, N.A. Anagnostopoulos, G. Spathoulas, A. Kakarountas, S. Katzenbeisser, Employing blockchain and physical unclonable functions for counterfeit IoT devices detection, in *Proceedings of the International Conference on Omni-Layer Intelligent Systems* (ACM, 2019), pp. 172–178
41. O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet of Things J. **5**(2), 1184–1195 (2018)
42. A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fairaccess: a new blockchain-based access control framework for the internet of things. Secur. Commun. Netw. **9**(18), 5943–5964 (2016)
43. A. Ouaddah, A.A. Elkalam, A.A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT, in *Europe and MENA Cooperation Advances in Information and Communication Technologies* (Springer, 2017), pp. 523–533
44. A. Ouaddah, A.A. Elkalam, A.A. Ouahman, Harnessing the power of blockchain technology to solve IoT security and privacy issues, pp. 1–10, 2018 (2017). https://doi.org/10.1145/3018896.3018901
45. J. Pan, J. Wang, A. Hester, I. AlQerm, Y. Liu, Y. Zhao, Edgechain: an edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet of Things J. (2018)
46. O.J.A. Pinno, A.R.A. Grégio, L.C. De Bona, Controlchain: a new stage on the IoT access control authorization. *Concurrency and Computation: Practice and Experience*, p. e5238
47. G.C. Polyzos, N. Fotiou, Blockchain-assisted information distribution for the internet of things, in *2017 IEEE International Conference on Information Reuse and Integration (IRI)* (IEEE, 2017), pp. 75–78
48. H. Qiu, M. Qiu, G. Memmi, Z. Ming, M. Liu, A dynamic scalable blockchain based communication architecture for IoT, in *International Conference on Smart Blockchain* (Springer, 2018), pp. 159–166
49. C. Qu, M. Tao, J. Zhang, X. Hong, R. Yuan, Blockchain based credibility verification method for IoT entities. Secur. Commun. Netw. **2018** (2018)
50. M.A. Rahman, M.S. Hossain, G. Loukas, E. Hassanain, S.S. Rahman, M.F. Alhamid, M. Guizani, Blockchain-based mobile edge computing framework for secure therapy applications. IEEE Access **6**, 72469–72478 (2018)
51. Y. Rahulamathavan, R.C.W. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption, in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (IEEE, 2017), pp. 1–6
52. M. Samaniego, R. Deters, Internet of smart things-iost: using blockchain and clips to make things autonomous, in *2017 IEEE International Conference on Cognitive Computing (ICCC)* (IEEE, 2017), pp. 9–16

53. L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, H. Tschofenig, Authentication and authorization for constrained environments (ace). Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07 (2017)
54. H. Shafagh, L. Burkhalter, A. Hithnawi, S. Duquennoy, Towards blockchain-based auditable storage and sharing of IoT data, in *Proceedings of the 2017 on Cloud Computing Security Workshop* (ACM, 2017), pp. 45–50
55. J.C. Song, M.A. Demir, J.J. Prevost, P. Rad, Blockchain design for trusted decentralized IoT networks, in *2018 13th Annual Conference on System of Systems Engineering (SoSE)* (IEEE, 2018), pp. 169–174
56. G. Spathoulas, A. Collen, P. Pandey, N.A. Nijdam, S. Katsikas, C.S. Kouzinopoulos, M.B. Moussa, K.M. Giannoutakis, K. Votis, D. Tzovaras, Towards reliable integrity in blacklisting: facing malicious IPS in ghost smart contracts, in *2018 Innovations in Intelligent Systems and Applications (INISTA)* (IEEE, 2018), pp. 1–8
57. M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, Oscar: object security architecture for the internet of things. Ad Hoc Netw. **32**, 3–16 (2015)
58. J. Wan, J. Li, M. Imran, D. Li et al., A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans. Ind. Inform. (2019)
59. H. Watanabe, H. Fan, A novel chip-level blockchain security solution for the internet of things networks. Technologies **7**(1), 28 (2019). https://doi.org/10.3390/technologies7010028, https://www.mdpi.com/2227-7080/7/1/28
60. L. Zhou, L. Wang, T. Ai, Y. Sun, Beekeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation. Sensors **18**(11), 3785 (2018)
61. X. Zhu, Y. Badr, J. Pacheco, S. Hariri, Autonomic identity framework for the internet of things, in *Proceedings—2017 IEEE International Conference on Cloud and Autonomic Computing, ICCAC 2017* (2017), pp. 69–79. https://doi.org/10.1109/ICCAC.2017.14
62. G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing privacy: using blockchain to protect personal data, in *Proceedings—2015 IEEE Security and Privacy Workshops, SPW 2015* (2015), pp. 180–184. https://doi.org/10.1109/SPW.2015.27
63. G. Zyskind, N. Oz, A.S. Pentland, *Enigma: Decentralized Computation Platform with Guaranteed Privacy*. Tech. rep. (2015). https://arxiv.org/pdf/1506.03471.pdf