Blockchain solutions for Internet of Things Systems

NGUYEN KHOI TRAN, The University of Adelaide, Australia
M. ALI BABAR, The University of Adelaide, Australia
JONATHAN BOAN, Defence Science and Technology Group, Australia

Internet of Things (IoT) systems bring about tremendous improvements in efficiency and effectiveness. With their data, they fuel the analytics pipeline for decision making and with their actuators, they realise these decisions in the physical world. As a result, IoT systems must be secure and trustworthy. However, they are vulnerable due to their large number of distributed resource-constrained endpoints and their reliance on centralised backends.

In the past few years, Distributed Ledger Technologies, specifically Blockchain (BC), have been increasingly used to address the problems posed by IoT systems. BC provides a decentralised, immutable source of truth, upon which many solutions have been built. By 2018, over 400 peer-reviewed primary studies on BC-IoT integration have been published. This wealth of studies enables and demands a comprehensive, rigorous review. A playbook that synthesises their findings would guide not only the next generation of IoT systems but also related systems in domains such as tactical and emergency response. In this article, we present a systematic review of 90 prominent primary studies on BC-IoT integration, which focuses on three foundational questions: Why do IoT systems integrate blockchains? How do IoT systems integrate blockchains? What optimisations were performed to blockchains for run on IoT infrastructure? These questions aim at the technical problems posed by IoT systems and their corresponding BC-based solutions. Thus, they are relevant across IoT verticals and beyond.

CCS Concepts: • **Computer systems organization** → **Peer-to-peer architectures**; • **Software and its engineering** → **Peer-to-peer architectures**; • **Security and privacy** → *Software and application security*; • **Information systems** → Collaborative and social computing systems and tools; Reputation systems;

Additional Key Words and Phrases: Blockchain, Distributed Ledger, Smart Contract, Web of Things, Internet of Things, Systematic, Review

ACM Reference Format:
Nguyen Khoi Tran, M. Ali Babar, and Jonathan Boan. 2019. Blockchain solutions for Internet of Things Systems. *ACM Comput. Surv.* 0, 0, Article 01 (January 2019), 28 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

On the first days of 2009, Satoshi Nakamoto mined the genesis block of bitcoin and the number of Internet-connected devices exceeded the World's population for the first time. On those days, two disruptive technologies were born: *Blockchain (BC)* and the *Internet of Things (IoT)*. Blockchains allow parties who do not trust each other to exchange value and cooperate. Internet of Things technologies allow physical entities to listen and talk to other physical and digital entities which

Authors' addresses: Nguyen Khoi Tran, The University of Adelaide, Adelaide, SA, 5005, Australia; M. Ali Babar, The University of Adelaide, Adelaide, SA, 5005, Australia; Jonathan Boan, Defence Science and Technology Group, Adelaide, SA, 5111, Australia.

0360-0300/2019/1-ART01 $15.00
https://doi.org/0000001.0000001

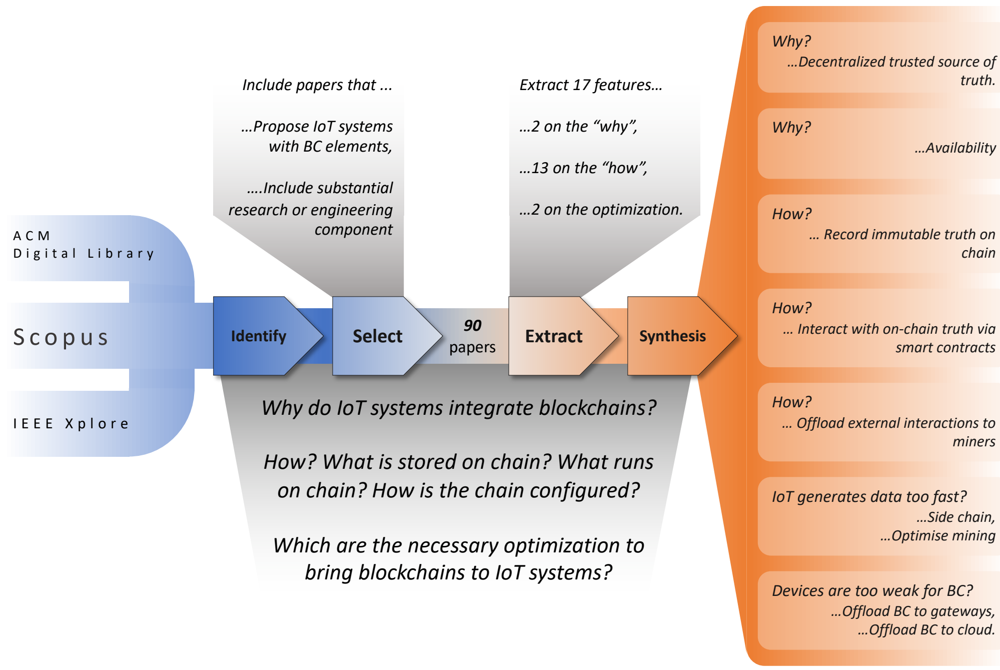


Fig. 1. The research questions, review process and key findings.

might not be trustworthy. The convergence of two technology is imminent and the result is *BC-integrated IoT systems (BC-IoT)*.

IoT systems pose challenging questions. For instance, how to establish reliable communications between IoT devices and digital services over untrusted channels? How to prevent IoT devices from joining Botnets? How to ensure the integrity of data generated by IoT devices? How to maintain evidences of misconducts in IoT systems? How to allow individuals to own and sell resources of IoT devices? How to deliver firmware updates to IoT devices in a secured and scalable manner? *More importantly, how to do them all without relying on a trusted third party?*

Blockchain technologies offer some answers to these problems. *First, blockchains provide tamper-proof transaction storages* which can be used to guarantee the integrity of data generated by IoT systems. They can act as secure channels for interaction between and within IoT systems. They can also maintain forensic evidences of tampering of IoT systems. This integrity guarantee to create the necessary trust to employ IoT systems in critical situations such as tactical and operational planning, maintaining common operating pictures, pollution monitoring, city automation and smart health care. *Second, blockchains provide tamper-proof code execution in the form of smart contracts.* These smart contracts can implement different types of logic, such as assessing the integrity of IoT devices, authorizing IoT devices to prevent them from joining botnets, and delivering software updates to IoT devices. These smart contracts also allow parties to exchange IoT resources, such as electricity, sensing data, and processing capability. *Finally, blockchains enable decentralized trustless systems.*

This work establishes a playbook to employ BC technology in IoT and similar systems. It describes technical problems of IoT that BC has been applied to solve; and the way the blockchain solution has been setup, optimized, and used in IoT system.

This playbook is synthesized from BC-IoT systems in the academic literature. We assessed *375 related research works* starting from the first BC-IoT paper in 2015 and studied in detail **90 prominent works**. From these research prototypes, we extracted and synthesized three types of information: (i) The type of problem in an IoT system that they use BC to solve, (ii) how they use BC and SC to solve those problems, and (iii) optimizations that they need to bring BC and SC into IoT infrastructure.

2 BACKGROUND

A Blockchain-integrated IoT (BC-IoT) System is an IoT system that uses Blockchain and Smart Contracts.

An IoT System is a computer system that involves physical devices, such as electronic tags, sensors, and actuators over the Internet. These devices enable physical entities (Thing) to send data and events to generate insights and actions to improve business or processes [53]. A distinctive feature of IoT Systems is that the communications within and between them happen over the Internet. This communication channel is open, not-trustworthy, and potentially malicious. Moreover, multiple applications can share an IoT system's sensing infrastructure, perhaps for a fee. This sharing emerges organically during the operation instead of the design phase of IoT systems, differentiating them from traditional industrial control systems.

Most IoT systems revolve around a centralized IoT platform. This platform monitors and configures IoT devices, provides an interface to interact with IoT devices, stores data generated by IoT devices, helps analyze and visualize IoT data for events and actions, and secures IoT system from malicious data and requests. Cloud-based platforms simplify the management and development of IoT systems. *On the flip side, IoT systems become dependent on the cloud platform.* This reliance creates a single point of corruption and failure. It also leads to silos where IoT devices do not talk to each other. Relying on the cloud also hampers the response time of IoT systems, as sensor data and control signals must travel multiple hops across the Internet.

Blockchains help decentralise IoT systems. With blockchains, all participants of an IoT system can keep a local ledger and verify all transactions themselves. Blockchains provide IoT systems non-repudiation of transactions. They also help remove the single point of failure and sole authority over IoT data. Finally, they can bring some intelligence of IoT systems to the edge in a secured and trusted manner.

A Blockchain is a cryptographically secured transactional singleton machine with shared state[1]. As a singleton machine with shared state, a blockchain system maintains a single truth for everyone in the network. For Bitcoin, the single truth is the set of unspent transaction outputs (UTXO). For Ethereum, the state of all accounts on the network. As a transactional system, a blockchain system processes transactions to transit between states. Bitcoin uses a restricted script to process transactions, while Ethereum and Hyperledger Fabric can use additional logic in the form of Smart Contracts. As a cryptographically secured system, blockchains rely on cryptography for security. Each block of transactions contains the hash of the previous block, thus block "chain". Users sign transactions with their private cryptography key. Addresses of users on blockchains are double-hashes of their public keys.

Blockchain systems differ in the ledger they maintain, their protocols, access rights, and off-chain elements around them. Ledgers records all transactions going through a blockchain. Ledgers vary in their data structure and the state that they maintain. Propagation protocols specify how transactions and blocks are spread across a peer-to-peer blockchain network.

Consensus protocols specify the rules that participants follow to maintain a blockchain. Specifically, they dictate how a transaction or a block can be considered valid. They also specify how to

[1]https://github.com/ethereum/wiki/wiki/White-Paper

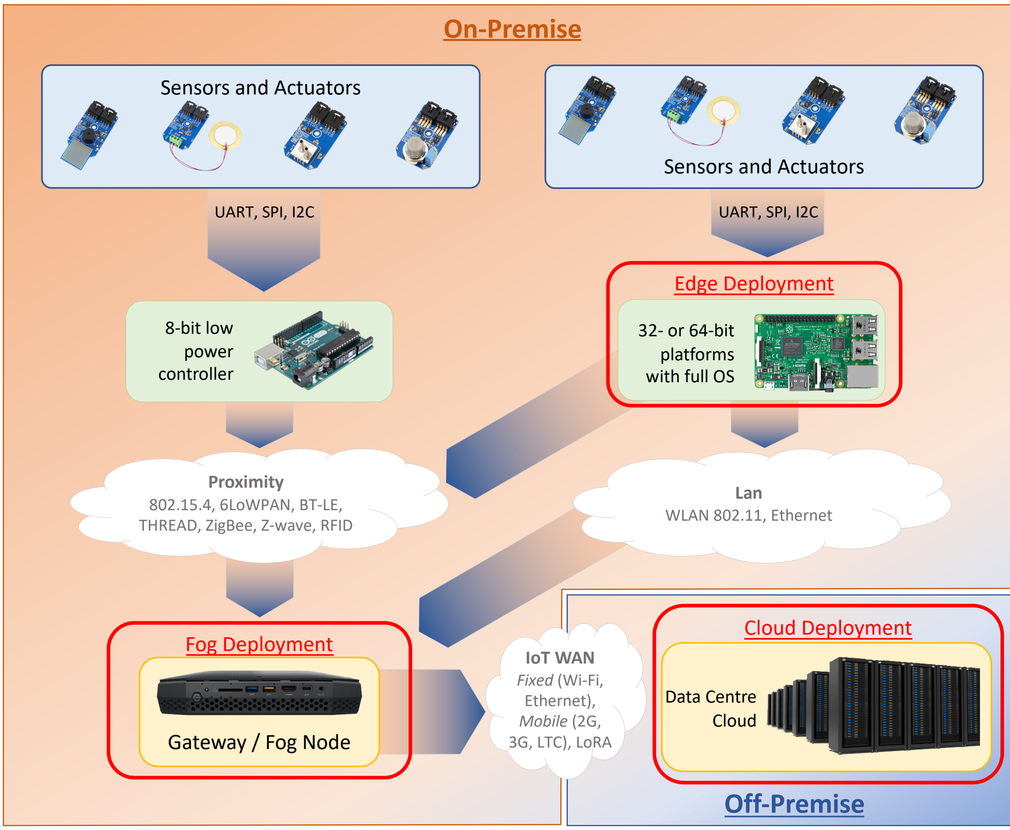


Fig. 2. Typical Edge-Fog-Cloud Architecture of IoT Systems.

select a participant to add a block to the blockchain (*Mining*). Purposes of this selection include preventing Sybil attack and making the system Byzantine Fault Tolerant. Proof-of-work, proof-of-stake, and Redundant Byzantine Fault Tolerance (RBFT) are some common miner selection protocols. Finally, consensus protocols also decide the main chain in case a blockchain forks. *Nakamoto consensus* is the most common protocol. It states that the blockchain with the most proof-of-work (longer) is the main chain.

Access rights of a blockchain specify who can read from and write to a blockchain on both block- and transaction-level. Based on access rights, blockchains can be classified into public, private, and consortium chains. *A public chain is open to everyone.* Its consensus protocols of a public chain are predetermined and open to everyone. Bitcoin is an example of a public chain. *A private chain is controlled by an organization.* This organization determines the consensus protocol and carries out the mining. *A consortium chain is a private chain which is controlled by a group of organizations.* These organizations agree on the consensus protocols and mine the blockchain together. Consortium members do not necessarily trust each other. However, they need to cooperate.

A blockchain system might also have some off-chain components. For instance, oracles help injecting context data. Key managers create and distribute key pairs among blockchain participants. Access services enforce access rights of a blockchain.

A BC-IoT system can be described by how it uses blockchains and how those blockchains are built. The way an IoT-BC system uses blockchains can be described by three features: (i) the components of an IoT system that blockchains replace or enhance, (ii) the type of information stored in transactions and accounts on blockchains, and (iii) the type of logic that runs as a Smart Contract on blockchains. The deployment structure of blockchains on an IoT infrastructure also describes the way a blockchain fits into an IoT system. The construction of a blockchain can be specified by its ledger, protocols, access rights, and off-chain elements.

3 RELATED WORK

As BC-IoT systems garnered more attention, the interest in positioning and reviewing this topic has also grown. Using the same systematic selection process that we employed in this review, we identified a number related reviews and position papers [12, 13, 18, 38, 50, 60, 67, 92]. These works tend to approach BC-IoT systems from a blockchain-centric, speculative perspective. They asked the question of what blockchain can do and then deduce its applicability to IoT systems. Few of them followed an explicit review protocol. Their primary outcomes were curated lists of primary studies and potential options to use BC in IoT contexts. In other words, they *speculated and mapped* the BC-IoT integration field.

This review, on the other hand, *aims at the synthesis*. Instead of starting from what blockchain can do and working backward to the IoT context, we begin with the "why": Why have IoT systems been integrating blockchain? For what purpose? To solve what technical problem? Then, we work forward to the "how" of BC-IoT integration. We base the answers not on deduction but on the IoT problems that the *published primary studies* tackled and the BC-based solutions that they proposed. Each primary study represents a vote for a particular IoT problem and a corresponding BC solution. Its "proof-of-work" is the effort spent on designing, developing, and evaluating the BC-IoT prototype. To ensure completeness and correctness of the review, we employed an explicitly and systematic protocol to select, appraise, extract, and synthesise these results into the answers.

Comparing to two existing systematic surveys on BC-IoT, this review exceeds in both size and resolution (Table 1). The two- to three-fold larger sample reveals not only alternatives of BC-IoT uses and designs but also the relative weights of those alternatives. The larger sample also reveals *outliers*. These black swan cases highlight some unique problems and solutions. For instance, we found studies that use BC as a source of time to synchronise the distributed IoT devices [22]. We found studies that use BC to give IoT devices the ability to question the integrity of commands that they receive. As smart, autonomous vehicles become a reality, this might become critical for our safety.

Table 1. Comparison between this review and previous systematic surveys on BC-IoT systems.

Review	Size	Features	Primary Question
Conoscenti, et. al., 2017	35 studies	6	Can the blockchain foster a private-by-design IoT?
Panarello, et. al., 2018	51 studies	6	What are usage of BC-related approaches and technologies in IoT context?
This review	**90 studies**	**17**	*Why, and how have IoT systems integrated blockchains?*

4 METHODOLOGY

We conducted the study following an explicit protocol in order to ensure its comprehensiveness, correctness, and fairness. The review process consists of four steps (Fig. 1):

(1) Identifying potential primary studies from credible sources using a structured query, which is derived from our research questions.
(2) Selecting the potential studies based on their quality and relevance to the research questions.
(3) Extracting data from the remaining studies on a set of features, which are derived from the research questions.
(4) Synthesizing the data to answer the research questions. The narrative synthesis method was employed.

The following sections provide more details of this process.

4.1 Research Questions

Research questions drive the review process. They determine the types of papers that would be needed, which in turn influence the query and the selection criteria. They also determine the features to be extracted and synthesized from the relevant studies. Our review addresses the three following research questions:

RQ1: Why do IoT systems integrate blockchains? With this question, we look for the objectives to improve IoT systems that lead to blockchain integration. We also look for technical problems of IoT systems that drive the blockchain integration. This information can help transfer the BC-IoT solutions in this review to other systems that have similar objectives and technical problems.

RQ2: How do IoT systems integrate blockchains? We consider the "how" part of BC-IoT integration on three aspects. The first aspect (RQ2.1) is where blockchains and their smart contracts fit into an IoT system, physically and logically. The second aspect (RQ2.2) concerns with the data and logic that blockchains and smart contracts handle for IoT systems. The third aspect (RQ2.3) is how the integrated blockchains have been configured . Together, these aspects constitute a comprehensive description of a blockchain solution for IoT systems.

RQ3: What optimisations were performed on blockchains for them to run on IoT infrastructure? IoT presents some unique challenges to blockchain systems. For instance, the rate that IoT systems generate data can exceed the throughput of blockchains by orders of magnitude. Moreover, IoT devices lack the computing capability, storage, and network bandwidth to participate in blockchain networks. This research question aims to identify the optimisations to BC that have been proposed by the existing studies to address these constraints.

4.2 Study Identification and Selection

The first two steps of the review process, namely study identification and selection, can be considered a filtering procedure in which we narrow down the literature on BC and IoT to a set of relevant studies. We conducted this filtering in four iterations (Fig. 3).

The first iteration is to *identify potential primary studies*. We chose Scopus as the primary source of scholarly peer-reviewed articles, and IEEE Xplore and ACM Digital Library as supplementary sources. Our decision was motivated by our pilot queries which showed that Scopus has a broader coverage and provides a better support for structured query as well as reproduction of search results. Google Scholar, which is a common source used by related surveys on BC-IoT, was excluded due to the lack of structured query support and reproducibility of results. We utilised the following query to identify potential studies from the chosen sources.

["Blockchain" OR "block chain"]
AND
["Internet of Things" OR "IoT" OR "Web of Things" OR "WoT"
OR "Industrial Internet of Things"]

Only English-written studies in the field of Computer Science, Engineering, and Mathematics were considered. We also removed entries that represent collections of work, such as conference proceedings. Results from all three sources were aggregated and duplicates were removed to form a set of *375 potential studies*.

The second iteration is a *coarse-grained filtering* of the potential studies based on their titles and abstracts. The third iteration continued with a *fine-grained filtering* based on their full text. In both iterations, we apply the first two of the following selection criteria:. By the end of the third iteration, *106 relevant studies* were identified.

- *Criterion 1:* Include works that address specific improvement objectives or technical problems of IoT systems with blockchains and smart contracts.
- *Criterion 2:* Include works that adapt or optimise elements of BC, such as architecture, consensus mechanism, and mining, to make it suitable for IoT uses.
- *Criterion 3:* Include only studies that contain substantial research or engineering component. Accordingly, we exclude all secondary studies, short and position papers. We also exclude all primary studies that offer speculations without substantial design or engineering components to back them up.

The forth iteration is to *appraise the quality of the relevant studies*. We applied the criterion 3 and filtered out 16 studies, leaving *a final set of 90 relevant BC-IoT studies* for the data extraction and synthesis steps that follow. The earliest work on BC-IoT integration that we found and included in the set was from 2015. It was about a business model for exchanging resources in IoT systems using blockchain as an orchestrator. The number of relevant works has grown exponentially over the years. By 2018, the number of BC-IoT studies grew to 72. On average, 6 out of 10 studies appeared in conferences, and 3 out of 10 studies have been published in journals (Fig. 4).

In order to minimize inaccuracy and bias, the following *cross-validation and adjustment mechanism* were introduced into the procedure. The first author generated and circulated a random sample of studies among co-authors. Co-authors applied the selection criteria on the studies, without knowing the assessment by the first author made. Results from co-authors were then compared and adjustment would be done if the agreement was less than 85%.

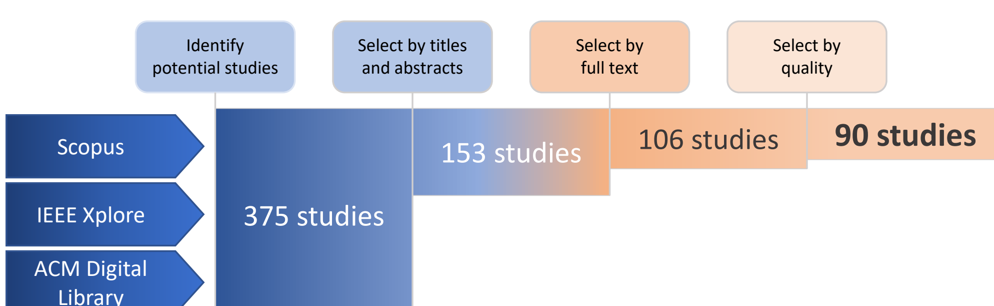


Fig. 3. Study Identification and Selection Process.

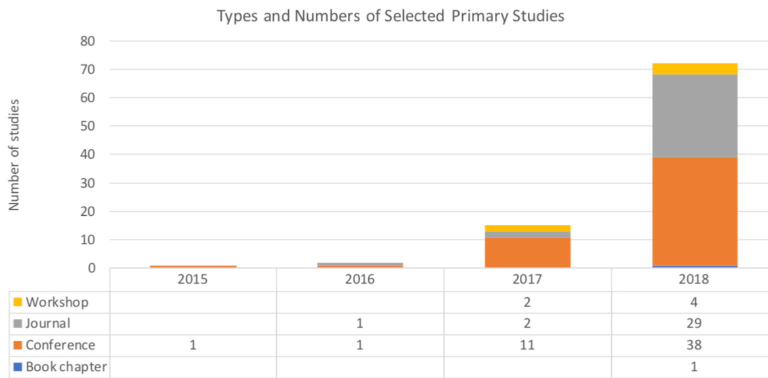


Fig. 4. Distribution of the selected studies by publication year and type.

4.3 Extraction Features

We extracted *17 features from the 90 selected studies* to answer the research questions.

For RQ1, we extracted *improvement objectives* and *technical problems* of IoT systems that were mentioned in the studies. An improvement objective denotes the aim to improve an IoT system that drove a BC-IoT research. These objectives either fall into giving an IoT system a new functionality or improving its qualities. A technical problem denotes a design or engineering challenge posed by an IoT system in the pursuit of the improvement objective. Improvement objectives and technical problems are agnostic of the vertical that an IoT system serves. Improvement objectives and technical problems represent the questions posed by IoT systems, which blockchains offer some potential answers.

For RQ2.1, we extracted the *logical and physical position of blockchains within IoT systems*. The logical position of a blockchain denotes the functional modules of an IoT system that it replaces or enhances. The physical position of a blockchain denotes the placement of its nodes onto hardware nodes of an IoT system. Each blockchain that is integrated in an IoT system comprises a set of nodes, which fall into four types: miner, full, wallet, and lightweight nodes. These blockchain nodes can be spread across various hardware nodes of an IoT system including edge devices, fog devices, and cloud nodes. The physical position of a blockchain is constituted by the positions of its nodes in the IoT system that it supports.

For RQ2.2, we extracted *on-, off-chain data and on-, off-chain logic*. On- and off-chain data are self-explanatory. On-chain logic denotes the logic of IoT systems run in on-chain smart contracts or in chain codes that govern the state transitions of blockchains. Off-chain logic denotes the IoT systems' logic that is offloaded to miners or other elements of a blockchain system. For instance, BC-IoT systems can offload the calculation of population scores, generation of key pairs, and authentication of devices to miner nodes of the integrated blockchains.

For RQ2.3, we extracted *seven features which represent a condensed description of a blockchain system*. These features represent key variations among blockchain systems. They were identified iteratively as we processed the relevant BC-IoT studies. Among these features, the number of integrated blockchains feature is self-explanatory. The data structure of the ledger feature captures and assesses the use of non-Blockchain ledger designs such as Hash Graph and Tangle. The type of global state feature captures and compares the use two dominant models: Unspent Transaction Output (UTXO) and Account. The type of smart contract feature captures and assesses the use of on-chain smart contracts (i.e., Ethereum style) versus installed smart contracts that manage

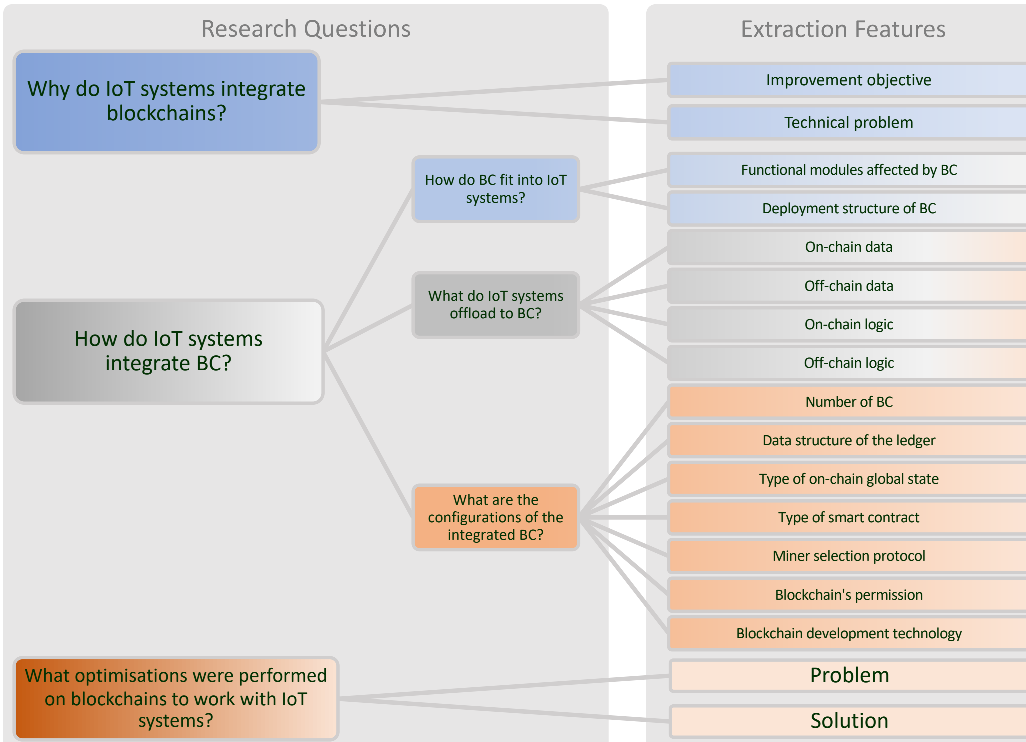


Fig. 5. Extraction features of the investigated research questions.

state transitions of the ledger (i.e., Hyperledger Fabric style). The miner selection protocol feature captures the mechanism to select the miner to extend the blockchain, such as Proof-of-Work and Proof-of-Stake. These protocols are sometimes called "consensus protocols", even though they are only one of the components that make up consensus protocols. The blockchains' permission feature captures the access rights of the integrated blockchains. Finally, the blockchain development technology feature captures the information on the software stack that was used to build the integrated blockchain.

Finally, for RQ3, we extracted the *challenges and the optimisations* necessary to integrate blockchains into IoT systems. Speculative challenges were excluded. We considered and reported only challenges from studies that also propose and develop solutions.

5 IOT PROBLEMS AND BLOCKCHAIN SOLUTIONS

5.1 Objectives of Blockchain Integration

The surveyed research uses blockchains either to improve some qualities of IoT systems or to give them new functionalities (Fig. 6).

Only two out of ten use blockchain to provide new functionality to IoT systems. Blockchains help create market places for sensing data, electricity, as well as spare data storage and computing capability from private users [15, 34, 45, 49, 54, 57, 61, 72, 83, 93, 95]. Smart contracts on blockchains can orchestrate and incentivise the exchange of resources. Blockchains can keep immutable records of

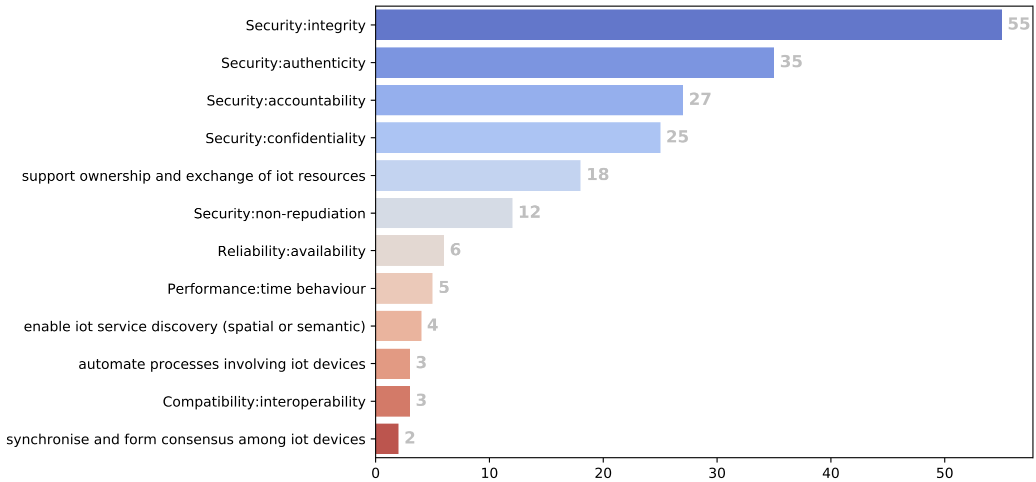


Fig. 6. Distribution of improvement objectives.

transactions. Blockchains and smart contracts can also store and maintain a registry for services that IoT devices offer [3, 16, 36, 69]. Smart contracts running on blockchains can be also used to represent business processes that involve IoT devices in different platforms [21, 27, 62]. Blockchains can act as a source of truth to synchronise distributed IoT devices. For instance, blockchains can store the "current time" of a distributed system and prevent malicious nodes from introducing time errors into the synchronisation process [22].

Eight out of ten reviewed papers aim to improve the quality of IoT systems with blockchains. Nearly all BC-IoT research prototypes aim to improve some aspects of IoT systems' security. Blockchains can act as a tamper-proof source of truth of IoT systems. Because blockchain is immutable, it can keep indisputable records of interactions to and from IoT systems. Because blockchains are open for multiple parties to verify, they can detect and prevent tampering of data collected by IoT systems. Integrity, accountability, and non-repudiation improvements then can be achieved by placing sensitive IoT data and transactions directly on blockchains [3, 27, 48, 55, 70]. Blockchains can even store hashes of devices' configurations and firmware to detect tampering [24]. Authenticity improvement can be achieved by building authentication mechanisms on top of blockchains [8, 20, 25]. For example, blockchains can act as a second channel for two-factor authentication [85]. Confidentiality improvement can be achieved by building new authorization mechanisms on top of blockchains [52, 59, 71]. For example, blockchains and smart contracts can be used to implement an OAuth-like mechanism.

Around one out of ten BC-IoT research prototypes aim to improve the reliability of IoT systems with blockchains. Availability is the degree to which, in the event of an interruption or a failure, a system can recover the data directly affected and re-establish the desired state of the system. BC-IoT research prototypes rely on the decentralised nature of blockchains to improve the availability of IoT systems. One approach is to deploy a blockchain near the edge of an IoT system to host some data and logic [70]. This blockchain helps the system function when its loses the connectivity to the cloud backend. Another approach is to replace centralised cloud backends with blockchains to negate the single point of failure in IoT systems [88, 96]

One out of ten BC-IoT research prototypes on average use blockchains to improve the performance of IoT systems. Specifically, they improve the time behavior of IoT systems, which is the degree to which the response and processing time and throughput rates of a product or system, when performing its functions, meet requirements.BC-IoT research prototypes use blockchain to place some data and logic of IoT systems on their edge nodes to remove the round trip to the backend. Alternatively, they can deploy blockchains at the edge of the network and run the logic of IoT systems on them as smart contracts.

One out of thirty BC-IoT research prototypes on average use blockchains to increase the compatibility between IoT systems. Specifically, they target the interoperability of IoT systems, which is the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged. They use blockchain to maintain trust assessment between parties so that they can communicate with each other [8, 17] instead of to perform data transformation or similar tasks to enable syntactic and semantic interoperability.

5.2 Problems posed by IoT Systems

Regardless of the objective, each BC-IoT research prototype addresses a subset of sixteen technical problems of IoT systems (Fig. 7). These technical problems can be classified into five categories (Fig. 8).

The first problem category is to operate IoT systems without relying on centralised backends that stores the data and control the devices. Some surveyed research aim to replace the centralised backends of IoT systems with blockchains and smart contracts [29, 34, 87, 95]. Others use blockchains to regulate and keep the backends accountable [3, 89]. These works pursue decentralisation for different objectives:

- Increasing the integrity of the data collected by IoT devices. This is critical for IoT systems whose data has large social and legal implications, such as pollution level [55]
- Increasing the reliability of the system by replacing a single point of failure with a decentralised system that is arguably more resilient to failure and attacks.
- Increasing the performance of IoT systems by moving data and logic closer to the edge of the network.

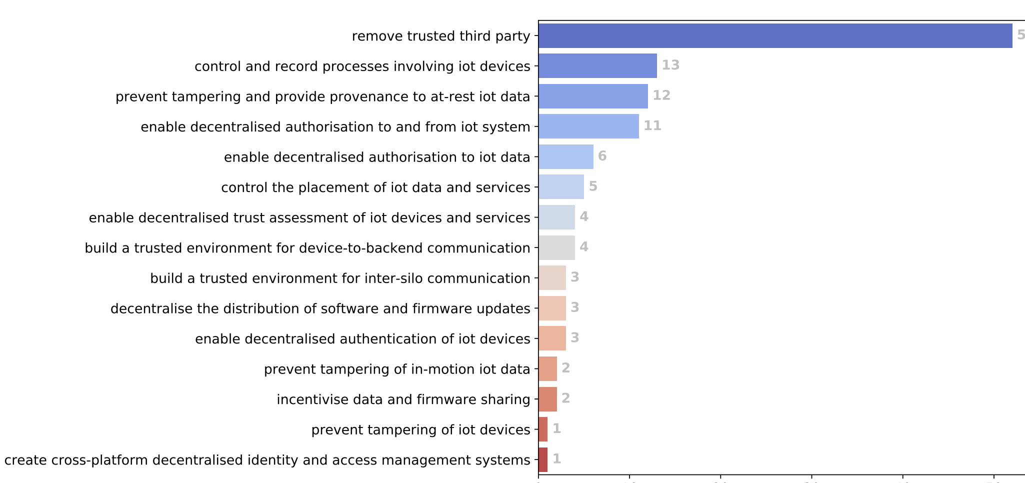
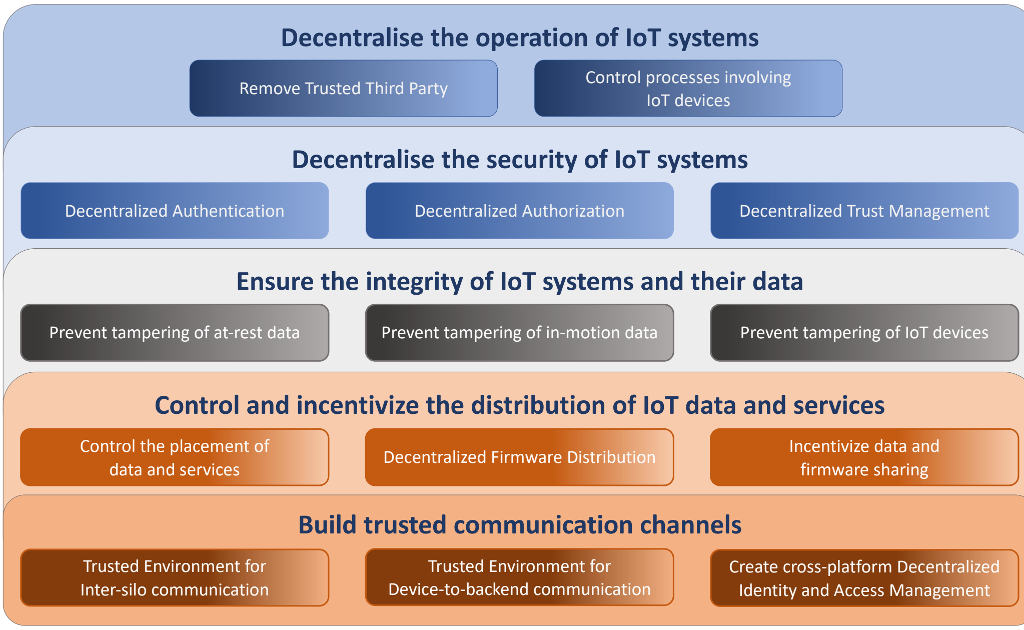
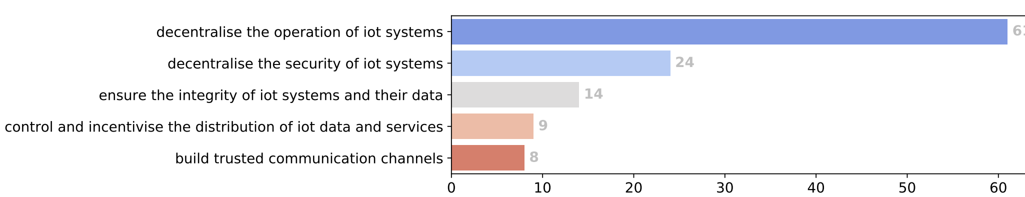


Fig. 7. Technical problems posed by IoT systems.



(a) Mapping of problems to categories.



(b) Distribution of categories.

Fig. 8. Category of technical problems posed by IoT systems.

The second problem category is to decentralise the security of IoT systems. The security mechanisms that existing BC-IoT systems decentralise include authentication, authorisation, and trust management. Authentication determines whether a user or a device is the one that it claim to be. Authorisation assesses whether a user or a device is allowed to do a certain thing in an IoT system. Trust management keeps track of incidents and reputation of users and devices to assess the trustworthiness of incoming messages. IoT systems generally rely on their centralised backends for security. This approach limits the scaling of IoT systems. It also reduces the reliability of the system, as devices would be unusable or vulnerable when losing connection to the backend. This approach also assumes that centralised, closed IoT cloud backends are secured and trustworthy. This might not always be the case.

On average, three out of ten surveyed research aim at decentralising the security mechanisms of IoT systems with blockchains. They use ledgers on blockchains an immutable, decentralised source of trust to store reputation rating [33, 91], incidents [79], or access requests [10, 20, 73, 81]. Smart contracts then can use the trusted records in the ledger to authenticate, authorise [59], and assess the reputation of parties in IoT systems [79].

The third problem category is to ensure the integrity of IoT systems and their data. The first problem in this category is to detect and prevent tampering of IoT devices. These devices generally lack the protection against physical tampering and malware. Their compromise led to serious consequences. For instance, the DDoS attack (Mirai) on Dyn that took down a large portion of the Internet was caused by infected IoT devices. Tampering of camera sensors in a smart city can violate privacy of citizen and lead to legal repercussions [24]. Blockchains can help to detect tampering by maintaining immutable records of device configurations. The second problem in this category is to prevent tampering and provide provenance to at-rest IoT data. Due to its potential social and economic impacts, the incentive to modify it to cover up wrongdoings is strong. Existing BC-IoT research use blockchains to maintain immutable records [1, 8, 48] or signatures of IoT data [24, 40] to prevent tampering. The third problem in this category is to prevent tampering of IoT data as it moves through the networks. Existing IoT-BC research use blockchains as the communication channels between different parties in an IoT system [65, 70, 75]. Miners can verify the announcements from devices and ensure the integrity of messages.

The forth problem category is to control and incentivise the distribution of IoT data and services. One problem is controlling the placement of IoT data and services on fog- or edge-nodes to help IoT systems respond quicker to the external stimuli. Another is to enable a trustworthy, sustainable delivery of firmware to IoT devices [41]. Maintaining up-to-date firmware is critical to the security of IoT systems. However, manufacturers might not be able to keep all operational devices up-to-date due to their large number, variety, and potentially long life-time. One solution is to have volunteers to host and share firmware, and use blockchains to orchestrate the process. Blockchains and digital signatures can guarantee the integrity of firmware in the absence of a central authority. Cryptocurrency and smart contracts can incentivize the volunteers and penalize malicious acts.

The fifth problem category is to build trusted communication channels within and between IoT systems. Within an IoT system, the communication might not be secured because it travels over wireless networks and the Internet. Essentially, the backend cannot trust the data from the devices and the devices cannot trust the commands from the backend. To address this problem, existing BC-IoT research use blockchains as the trusted intermediary to validate and audit the communication between devices and backends [46, 51, 71]. Similarly, the interactions between IoT systems are also unsecured yet unavoidable in many applications of IoT. Blockchains, specifically consortium variation, can act as a trusted communication to orchestrate various IoT systems [8, 17, 89].

5.3 Positions of the integrated blockchains

From the perspective of an IoT system, an integrated blockchain is characterised by where it is, logically and physically (RQ2.1), and what it holds (RQ2.2).

The functional modules which a blockchain adds or replaces represent its logical position in an IoT system (Fig. 9). The most common use of blockchain is, unsurprisingly, to orchestrate business processes among independent parties. This fits the role of the blockchain as a decentralised immutable ledger of transactions Another common use of blockchain is to use as an immutable, decentralised storage. This can be used for sensor data (15/90), interactions and security incident records (11/90), trust and reputation rating for trust management system (7/90), and configuration of devices for integrity verification (9/90). Another use of blockchain is a trusted communication channel between parties that cannot trust each other, such as different silos of IoT systems (8/90). This can be used for many purposes, including delivery of firmware updates to IoT devices (2/90). Another use of blockchain is accountable execution of application logic, based on smart contracts running on blockchains. This is used for implementing authorisation policies (22/90). Some works

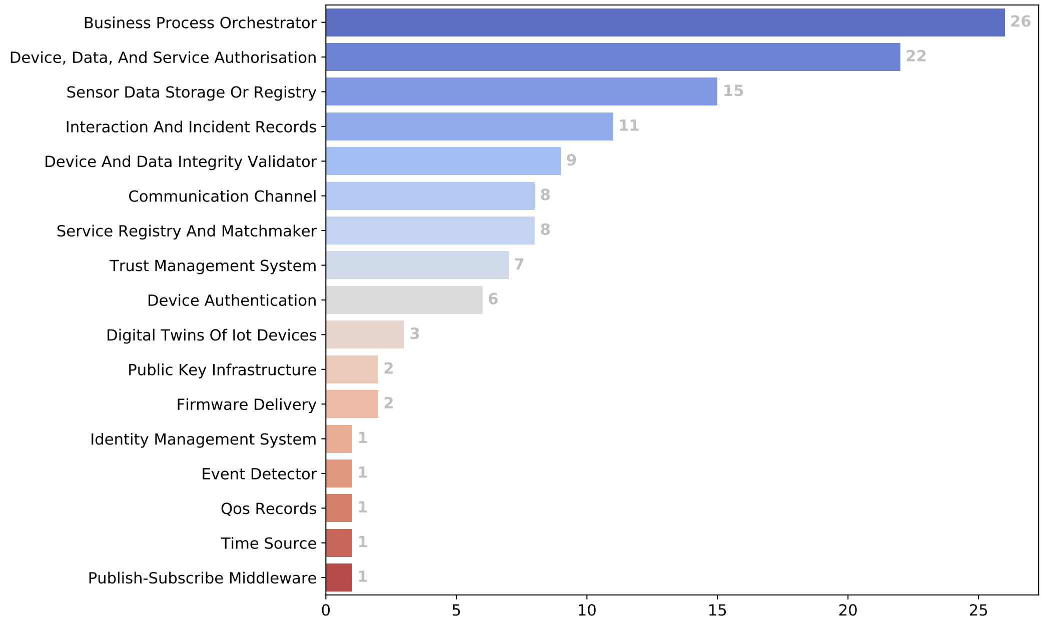


Fig. 9. Functional modules of IoT systems added or replaced by integrated blockchains.

even use this ability to implement digital twins of IoT devices (3/90). Recall that digital twin is the virtual representation of IoT devices on computer systems, generally on the Web so that computer software can interact with devices more easily. Some other less common use of blockchain is as a decentralised source of truth. One use case is using blockchain as a time source for synchronising IoT devices. SDN flow table to synchronise different SDN controller nodes are also supported by blockchain.

The type of computing nodes that create transactions, mine new blocks, run smart contracts, and hold the blockchain represents its physical position in an IoT system (Fig. 10). Cloud is the dominant form of BC. A reason is that it would be easier to deploy and run blockchain this way, as Proof-of-work of blockchains are resource demanding. Or it also means that blockchain is reachable over the Internet, outside the premise of IoT sensors in the application. In this case, the blockchain is generally

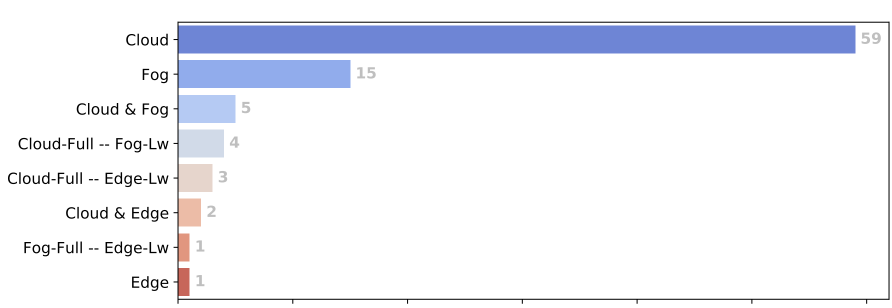


Fig. 10. Distribution of deployment structures of the integrated blockchains.

Ethereum or Bitcoin. Cloud means blockchain can run on cloud as a service. Fog is the second form of deployment. It means that ledgers and miners are deployed on the fog nodes of IoT systems. These fog nodes then form a blockchain network. Edge is the least common. This is understandable as edge devices in IoT have very limited resources to run blockchain. Works that use edge in our review generally modify blockchains extensively, use private chain, and use devices that are more capable than usual edge devices. Some works use a combination. They offload full blockchain nodes (with full ledger and mining capability) to more powerful computing nodes, and let weaker nodes use light weight clients to interact with the ledger.

The on- and off-chain data presents a more nuanced perspective on the functional position of an integrated blockchain. *On-chain data* are transactions. They drive the state of the integrated blockchain and present immutable records for future provenance and audits. The most common types of on-chain data in the reviewed BC-IoT studies fit the expectation (Fig. 11):

- Resource exchange records which support business process orchestration (21 out of 90) [6, 15, 17, 29, 34, 36, 41, 43–45, 49, 54, 57, 61, 80, 83, 87, 89, 93, 95]
- Device interaction records (14 out of 90) [2, 3, 8, 11, 19, 21, 23, 28, 30, 31, 42, 48, 64]
- Sensor readings (13 out of 90) [1, 35, 42, 55, 62, 66, 71, 82, 86, 88, 96]
- Authorisation requests and responses, which drive the authorisation mechanisms (12 out of 90) [4, 5, 7, 20, 26, 33, 56, 58, 59, 73, 81, 94]
- Service interaction records (11 out of 90) [3, 19, 27, 28, 32, 36, 70, 75, 76, 93, 96]
- Hashes of sensor readings (11 out of 90) [4, 7, 24, 40, 44, 46, 47, 51, 68, 74, 84]

Some unexpected types of on-chain data types can be found at the tail of the distribution. For instance, the chain can hold SDN flow tables to synchronise SDN controllers [63, 75, 77], current time to synchronise decentralised IoT devices [22], and device configurations to verify their integrity [24, 42]. Off-chain data is only used by one out of 90 reviewed work to store the source code of smart contracts.

The on- and off-chain logic offers another perspective on the functional position of an integrated blockchain. *On-chain logic* is the trusted, auditable codes that blockchain runs (Fig. 12. Recall that blockchains can support smart contracts, to control the state transition in a different way than the original bitcoin protocol. Interestingly, 47 out of 90 works do not support any form of on-chain logic. For the chains that support, the most common uses by far are authorisation mechanisms (15/90) and establishing contracts between providers and consumers of IoT resources, be it data, services, or electricity (14/90). Some interesting uses are digital twins, data indexes, and service match making.

Some works run additional logic on miner nodes, or some specialised computing nodes that they add to as a part of a blockchain system. These *off-chain logic* are not common (Fig. 13). 66 over 90 do not have them. The most common use is to interact with the outer world in the way that blockchain and smart contracts cannot. For example to authenticate users and devices, or to discover devices, or to interface with various cloud-based IoT systems. Other use is to offload computation that are simply too heavy to run on blockchain. For example, off-chain logic run cryptographic key generation, reputation score calculation, reasoning engine, deriving device configurations from its readings, clustering blockchains, etc. Off-chain logic can even be used to manage the life cycle of on-chain smart contracts.

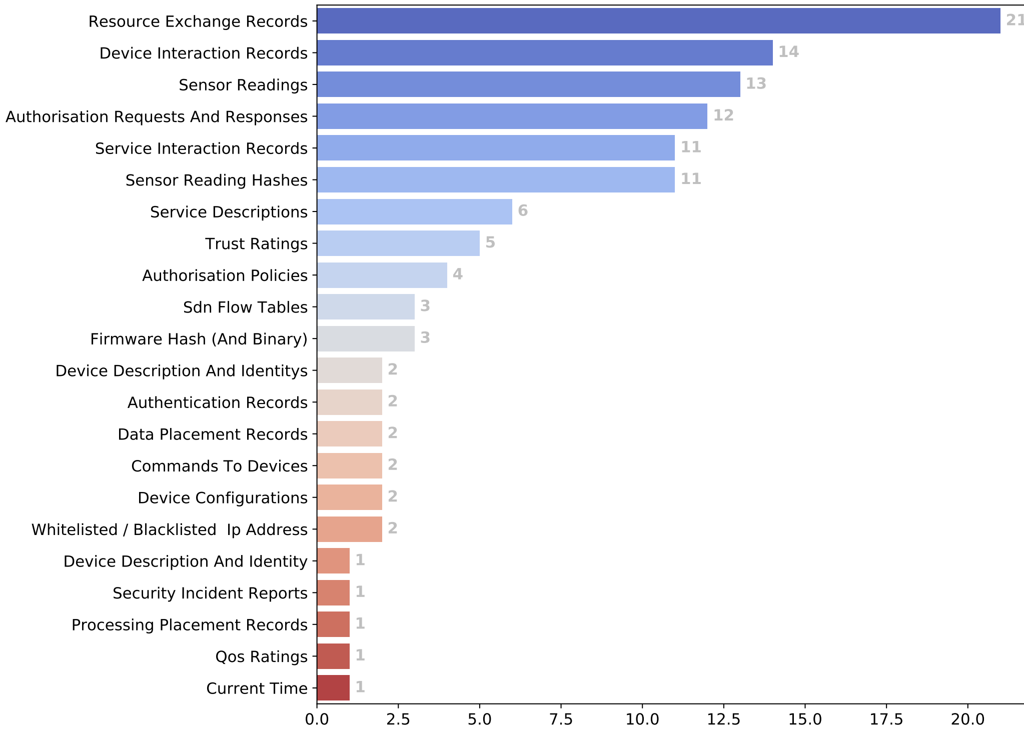


Fig. 11. Distribution of on-chain data types among BC-IoT prototypes.

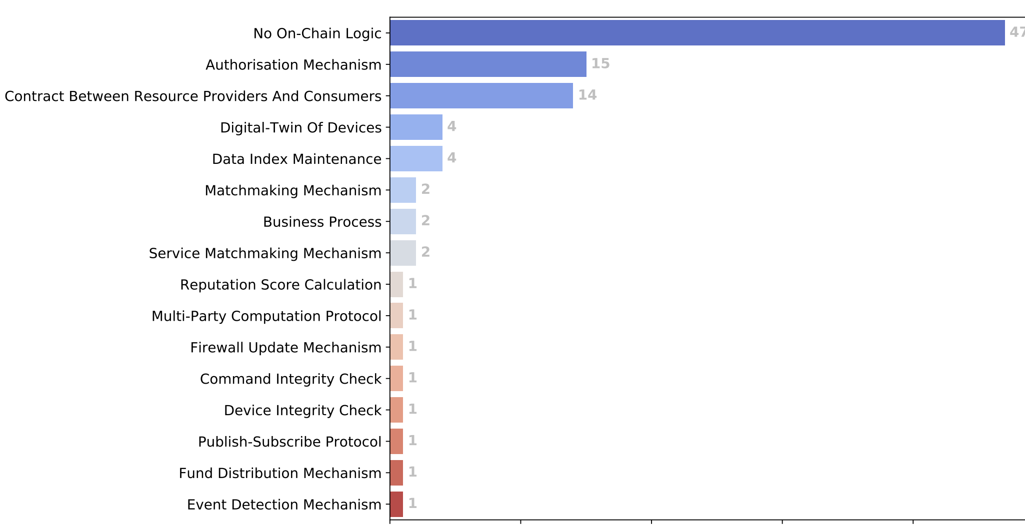


Fig. 12. Distribution of on-chain logic types among BC-IoT prototypes.

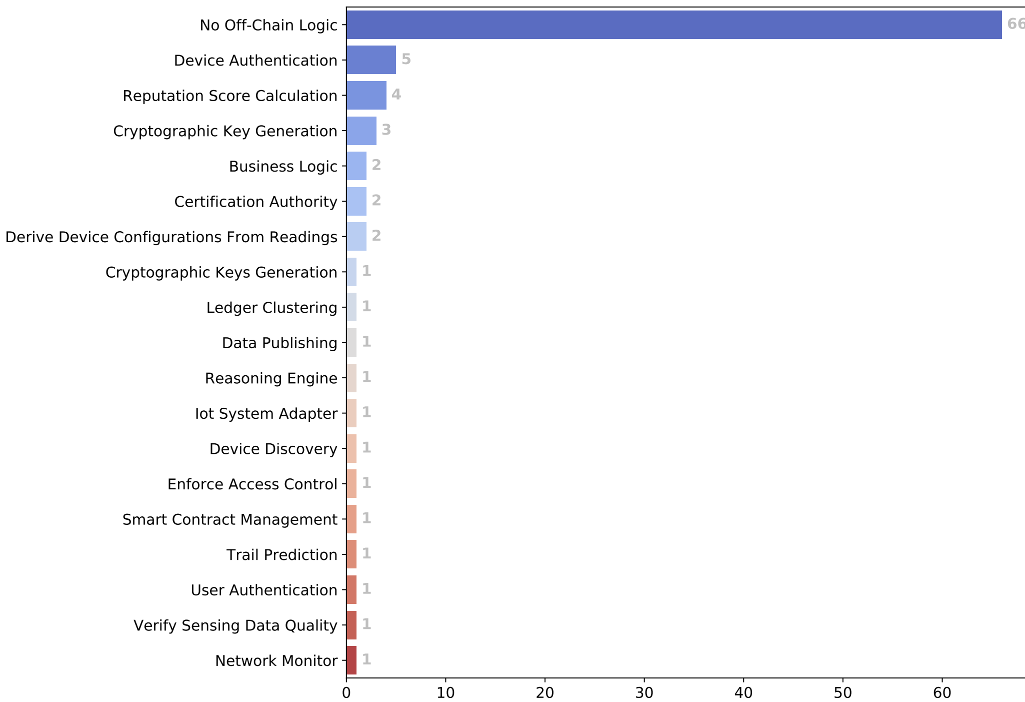


Fig. 13. Distribution of off-chain logic types among BC-IoT prototypes.

5.4 Configurations of the integrated blockchains

Configuration offer a detailed, technical perspective on the integrated blockchain (RQ2.3). The first feature we considered is the *number of blockchains being used* in a BC-IoT system. Only 9 out of 90 reviewed BC-IoT prototypes employed more than one blockchain [4, 8, 16, 17, 19, 51, 65, 75, 82]. Some works however use the concept of side chains. Some works deploy a faster or more private chain on all fog nodes, and then another chain on the cloud nodes (a mechanism similarly to the current Fog - Cloud interaction). Other works uses multiple private chains, each for one geographical area or one user, and then a public chain to interconnect these private chains. All the remaining studies used only one chain.

The second feature is the *type of permission* of the integrated blockchains (Fig. 14. Public chain is still the most common form of blockchain (7 out of 10 works on average). Private and consortium chains are used but to a lesser degree, and usually as a part of a multi-chain setup, as we mentioned previously.

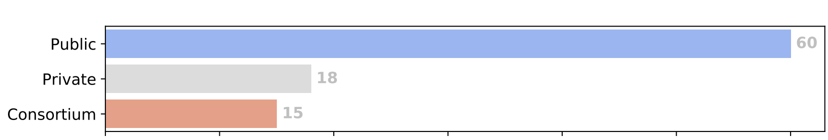


Fig. 14. Distribution of permission types of blockchains in the reviewed BC-IoT research prototypes.

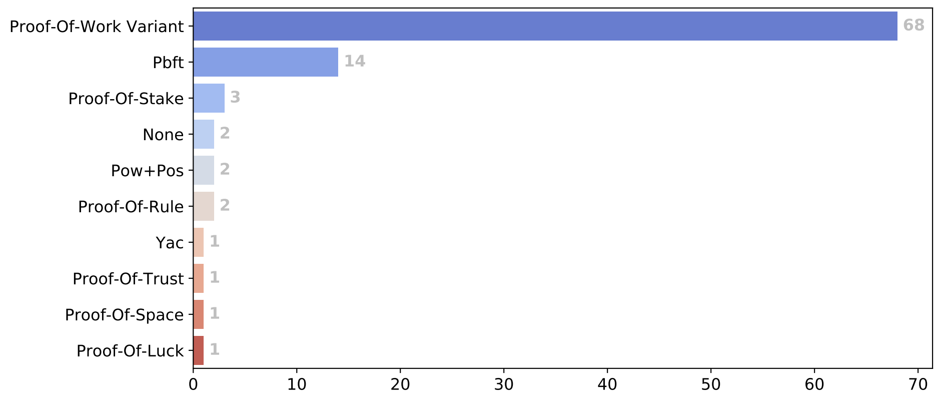


Fig. 15. Distribution of consensus schemes in the reviewed BC-IoT prototypes.

The next feature is the *consensus scheme, specifically the protocol to select a miner* to extend a chain (Fig. 15. An overwhelming number of papers use some variants of Proof-of-work. In Bitcoin proof-of-work protocol, miners race to find a number (i.e., “nonce”) that will make the hash of a block smaller than a threshold value. The first miner to find the nonce can append his block and receive the mining rewards and the transaction fees within a block. The probability of winning a mining round depends on the total hash rate of a miner. Ethereum proof-of-work protocol operates on a similar basis. To minimise the energy consumption of PoW in an IoT system, selective Proof-of-work has been proposed [82]. In this protocol, clients rank miners by trust rating. For every set of transactions, there is only one miner working at one time to solve the PoW . Practical Byzantine Fault Tolerance is a common alternative to PoW in private and consortium chains. As participants are vetted in these chains, PBFT does not have to prevent sybil attacks as on public chains and therefore can be faster. Other alternatives rely on hardware-enabled Trusted Execution Environment [51] (e.g., Software Guard Extensions (SGX) in Intel’s CPUs), or a combination of PoW with Proof-of-Stake [75, 90]. Interestingly, some BC-IoT prototypes dropped consensus protocol entirely and rely on other mechanisms such as distributed trust assessment [19].

The next feature is the *technology used* to build the integrated blockchain (Fig. 16. Ethereum is the most common technology to build integrated blockchains. Its early arrival, matured technology stacks, and support for private chains might be the key factor of its wide adoption. Hyperledger Fabric is emerging in the research field. Its modular structure and support for private chains might be the key factors. In the tail of the distribution, we have technologies such as Multichain, Monax, Eric, and Iroha. Finally, many works involve proprietary blockchain implementation. We classified them all under the label of in-house BC systems.

Other features that we extracted include the data structure, global state model of the chain, and the type of smart contracts. Most BC-IoT prototypes did not deviate from the norms and defaults of BC technologies. Therefore, we did detect any unexpected results for these features. For example, if a BC-IoT system uses Ethereum, then its blockchain generally follows the account-based model with on-chain smart contract. If it uses Hyperledger, then its model is automatically transaction logs with installed smart contract. The data structure of the ledger also did not deviate from the blockchain structure. We did not detect any alternatives, such as Tangle or HashGraph.

In summary, *the configurations of the integrated blockchain in the reviewed prototypes mostly align with the common blockchain development technologies*. Figure 17 shows the top five patterns.

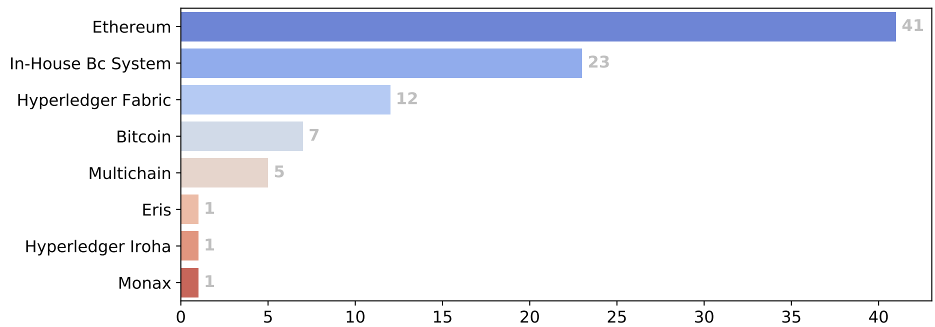


Fig. 16. Blockchain development technology employed by the BC-IoT research prototypes.

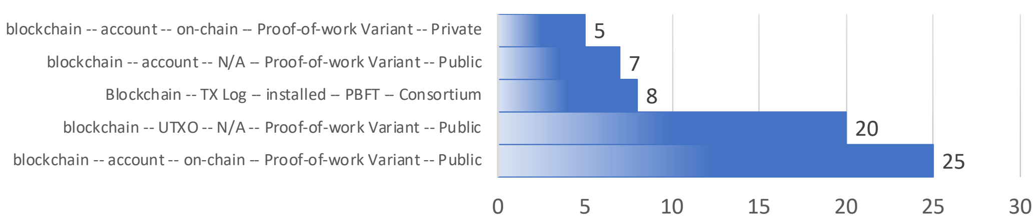


Fig. 17. Common configurations of blockchain in BC-IoT systems.

5.5 IoT-specific optimizations to blockchains

A common problem is that IoT devices *lack the computing resources to store and mine a blockchain*. Lightweight blockchain node is the most common solution [36, 80, 96]. A lightweight node holds only the block headers and therefore 1000 times less space than a full node. It can generate transactions but has only limited capability in validating the incoming transactions of the transaction. Another solution [27] is to migrate the whole blockchain to cloud-based virtual machine, and then having the IoT devices to subscribe or connect directly to these machines. From an IoT device's perspective, a blockchain backend is indistinguishable from a cloud back end.

The lack of resources also means that IoT devices *cannot execute smart contract by themselves*. Instead, they rely on other nodes that participate in a blockchain to run the smart contract and tell them what to do. This approach assumes that the nodes are trusted, which is not always the case. Split-virtual machine [21] has been proposed to address this problem. It extended the Ethereum virtual machine with a part that runs directly on resource-constrained devices. This architecture removes the questionable intermediaries. The lack of resources also mean that IoT devices *cannot perform complex security measures*. One of them is stealth address protocol, which prevents linking and revealing the identity of the key owner via transactions on blockchains. A fast dual-key stealth address protocol has been proposed to address this problem [23].

Another common problem that drives blockchain optimisations is the *massive influx of IoT data*. We identified three approaches to this problem in the literature. The first approach is to make the consensus process faster and less costly. It has been done by altering the Proof-of-work protocol [82], replacing it with more efficient consensus protocols such as Proof-of-stake [62] and Proof-of-trust [51], or to removing it altogether [19]. The second approach is to reduce the amount of data injecting into blockchain. It has been done by either aggregating [49] or filtering sensor

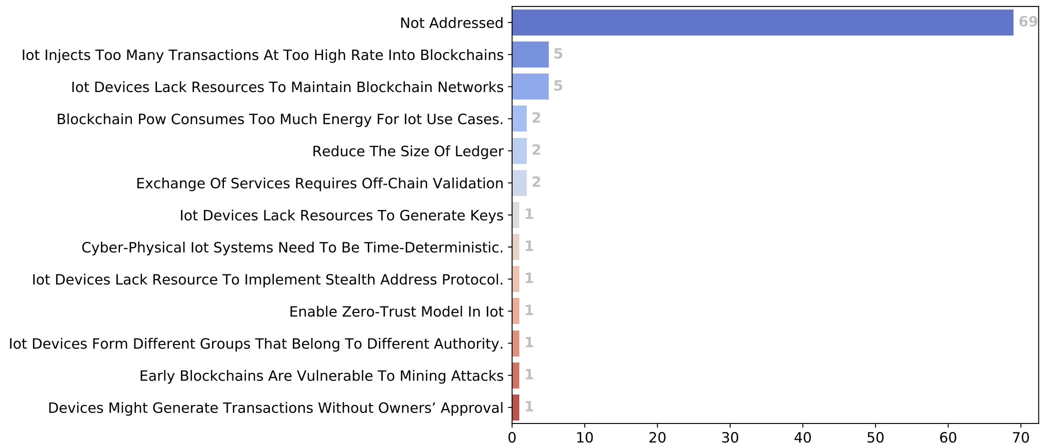


Fig. 18. Problems of IoT systems that drove the optimisation of blockchains.

data [86] before submitting to the chain. The third approach is employing multiple chains [4, 8, 71]. Fast, private chains can absorb the incoming traffic, while slower, public chains can coordinate and audit the fast chains.

The *large and ever-increasing size of IoT data on-chain* also drove the optimisation. One approach is to offload old transactions to external storage. This can be done by modifying the data structure of blockchain to make the transaction log modifiable [48]. Another approach is to partition the blockchain network into clusters, and have each cluster to maintain only a subset of the chain relevant to them. Hypergraph theory has been used in this task [64].

Another challenge is *off-chain verification of resource exchanges*. For instance, on-chain smart contracts need to verify the delivery of an IoT service, electricity, or firmware. Alternative consensus protocols that take off-chain validation into account have been proposed, including Proof-of-delivery [41] and proof-of-service [75]. Another challenge is protecting early blockchains. This is relevant to many of the reviewed BC-IoT prototypes, as they involve new blockchains with low participation. One approach was to use a joint PoW-PoS protocol, such as 2-hop blockchain.

6 CONCLUSIONS

6.1 A Case for BC: Decentralised Trusted Source of Truth

IoT systems require a trusted *source of truth* to coordinate their various moving components: IoT devices, fog nodes, cloud services, and other IoT systems. This truth represents what IoT systems consider the current facts, such as requests and responses for authorisation [56, 59, 73, 81, 94], records of resource exchanges [49, 54, 87, 89, 95], trust ratings [78, 90, 91], and even the current time [22]. Traditionally, an IoT system relies on an entity that it deems trustworthy to maintain the truth. This entity is generally a cloud backend of n IoT system, or an intermediary between systems in resource exchange use cases. It has a global view of the involving IoT systems and uses this view to maintain an up-to-date truth. This approach works, with some caveats. Single point-of-failure and reduced reaction time to external stimuli are some well-documented drawbacks. The other caveat, which we believe to be even more critical, is that this model *operates upon assumed trust* which might not be guaranteed.

To trust another party is to believe that it would provide the service as per the agreement. A party is trusted when others considers it to be trustworthy enough to transact businesses. In an IoT system with centralised truth, the entity that maintains the truth is trusted. Vice versa, the devices that provide inputs to the truth and act upon it are also trusted. There might be a handshake in the beginning and perhaps frequent security checks that follow. However between these checks, the involving parties are trusted. Due to the nature of IoT, everything can be compromised and masqueraded. Therefore, the devices should not assume that commands, firmwares, nor the truth that they perceive from the trusted entity are completely trustworthy. The backend should not assume that IoT devices are trusted either. Operating upon assumed trust is dangerous.

Blockchains offer a mean to maintain a decentralised trusted source of truth. This truth is stored as the state of the ledger and the transactions that drive the state changes. The trust in blockchain emerges from three factors. The first one is the cryptographic primitives that it uses, specifically public-key cryptography and digital signature. They guarantee that the transactions were unaltered and came from the holder of the corresponding private key. They provide nonrepudiation and provenance. The second factor is the blockchain data structure, which embeds the hash of each transaction block into its immediate subsequent block. Because a small change in the input leads to large change in the hash, and because the hash of each block becomes a part to calculate the hash of the following block, any tampering would be apparent unless all the subsequent hashes are recalculated. However, if a node operates by itself, it would be able to recalculate these hashes to cover up the tampering, even if there is a proof-of-work puzzle lock in each block. Therefore, the trustworthiness of BC hinges on the third factor: decentralisation with complete redundancy.

A BC network can be considered a collection of paranoid participants. They trust neither the network nor their peers. Instead, they maintain a complete copy of the truth and verify everything coming their way: announcements, transactions, blocks. As a result, a malicious entity can only overwrite the truth with the compromised one if it can control 51% of the network. This is considerably more difficult, given that every node in the network has its own agenda and vesting in the system. The more of these trust-less nodes that a BC possesses, the more resilient and therefore trustworthy the truth it maintains become. Maintaining a decentralised trusted source of truth is by far the most common case for BC integration among the reviewed studies.

6.2 A Case for BC: Availability

In 2014, Jibo - the world's first family robot was announces with much fanfare, raising over $3 million crowdfund. It can greet the parents, read to the children, send reminders, deliver personal reports, and dance. Thus, Jibo was warmly welcomed to families when it finally arrived in 2017. Then in 2018, the company behind Jibo went bankrupt and the Jibo gave its farewell dance as its server shut down. This is just an example of the precarious nature of IoT systems whose brains live in remote cloud services. Their availability hangs on the survival and, to some degree, good will of service providers. Even if the service is still around, the availability is still not guaranteed, as the Internet connectivity of the devices might still be lost. This is also true in tactical systems and emergency response systems in disaster struck areas where the communication has been knocked down.

Blockchains can increase the availability of IoT systems, due to their complete redundancy. Each full node in blockchain network holds a complete copy of both the data and the logic, which means that there is not a single node that maintain the total control over the data and logic of a system. If a node is lost, the remaining nodes in the blockchain can continue to function. In case of Jibo, a blockchain hosted by dedicated volunteers might have been able to save a part of its brain so that it can continue to operate. If such chains can be established at the perimeter of IoT systems among their edge or fog nodes, then the systems might even be able to operate when the Internet connectivity is lost.

Availability is considered a case for BC integration by many of the reviewed papers [9, 11, 39, 42, 52, 80].

6.3 A Case against BC: Performance and Scalability

Decentralised trusted truth and availability of BC come at severe costs. *The first case against BC integration is performance.* To provide decentralised trusted truth, blockchain networks rely on cryptographic primitives, data structure, and decentralisation with complete redundancy. All of these have negative impacts on the performance of the chain (i.e., throughput, latency, bootstrap time [14]. In the case of Bitcoin, the maximum rate at which it can confirm transactions is 3.3 to 7 transactions per second [14]. It takes on average 10 minutes for a Bitcoin transaction to be included in a block, and 60 minutes for a transaction to be finalised. Bootstrapping a blockchain full node is also a long process, clocking nearly four days in Bitcoin. Anecdotally, we observed a similar bootstrap time on Ethereum network when we set up a full node on a workstation with an 80 Mbps Ethernet connection.

In other words, *public blockchains are generally slow. And costly.* As high as $6.2 USD per transaction confirmation in Bitcoin network [14].

This level of performance cannot keep up with the traditional payment systems, and is vastly outpaced by the influx of IoT data. For instance, an IoT-based security camera can record up to 60 samples per second, while an microphone sensor can record from 8000 to more than 5 million samples per second. The reviewed papers proposed some solutions to bridge this performance gap. The first one is to reduce the data before committing to the chain [49, 86]. The second one is to make the blockchain faster by altering its parameters and consensus protocols [19, 51, 62, 82]. The third one is to use faster private chains to absorb the incoming traffic from IoT devices [4, 8].

The second case against BC integration is scalability. The complete redundancy which offers trust assurance and availability also means the ledgers on all full nodes are large and will grow without bound as an IoT system grows. Imagine we have a smart home that hosts a full node to run its automation logic. Even though the number of devices in our home does not increase, the software that run our smart home would keep getting slower and the data it requires would keep getting larger because more smart homes are brought online across the globe. This problem is exacerbated by the amount of data that IoT generates. Cisco estimates that by 2021, all people, machine, and things would generate nearly 850 zettabytes, or 850 billion terabytes

Until these performance and scalability limitations are mitigated, practical BC integration in a production level might be limited.

6.4 Looking Forward: Faster Chains

Scaling blockchains means finding the optimal compromise of the *Impossible Triangle: Security - Scalability - Decentralization.* Recall that a factor for the trustworthiness of blockchain is the decentralisation with complete redundancy. The more full nodes there are in the network to keep track of others, the more secure and anti-fragile the BC network becomes. But the more decentralised, the more redundancy is introduced into the network and the slower it becomes. The efforts to increase the performance of blockchain tends to lead to centralisation, which might compromise its security. An example would be Ripple network, which replaces miners with a preselected 16 servers that handle the ledger update.

Blockchain scaling can be done on 2 layers. *Layer-1 scaling indicates the optimisation done to the blockchain itself.* It is done by altering parameters of the blockchain network and changing its consensus protocols [19, 51, 62, 82]. In Ethereum, Layer-1 scaling is done by introducing Proof-of-Stake (PoS) via the Casper protocol.

Layer-2 scaling indicates optimisation done to the protocols built on top of blockchain, which can be created and modified without altering the blockchain itself. There are three major approaches: side-chain, off-chain computation, and sharding. Side-chain approach involves employing faster, less secured chains to absorb the incoming transactions (e.g., [4, 8], Lightning Network payment protocol, and Ethereum's Plasma). Off-chain computation approach involves a offloading complex calculation off-chain in a way that is verifiable by the main-chain (e.g., TrueBit[2]). Sharding involves dividing data across multiple servers[3]. Layer-1 scaling might drive the early innovation in public blockchain scaling; however eventually the public chain must stabilise and layer-2 scaling would become dominant[4].

6.5 Foreseeable Future: The Post-Quantum Cryptography World

By 2014, a quantum computer can factorise 56153 into its prime factors (233*241). While the number is by no mean large, what is notable is that this factorisation algorithm ran in polynomial time. As quantum computing continues to mature, it is not unreasonable to expect that in foreseeable future, three hard mathematical problems underlying the current popular cryptography algorithms - integer factorisation, discrete logarithm, and elliptic-curve discrete logarithm - would be solved. And by then, we would enter a post-quantum cryptography world in which the trusted cryptographic primitives might not protect our IoT system anymore.

One research direction relevant to BC-IoT systems is to secure the blockchain against the quantum attacks. Public-key cryptography is the most vulnerable. Proof-of-work would also be threatened by quantum computers. While it is true that the difficulty threshold of the blockchains can adjust itself automatically to match with the available hash rate to ensure regular block time (10 minutes in case of bitcoin), quantum computers can still compromise public blockchains by forcing centralisation. Specifically, if some hypothetical superpowers have access to a functional quantum-based miner, they can drive the difficulty threshold so high that they effectively lock other miners out of the network and assume control of the chain. However, the risk to blockchain is not that severe, as its protocol can evolve quickly to replace the vulnerable primitives with quantum-proof ones.

Low-power-long-living IoT devices along with legacy systems that IoT systems interact with, however, do not enjoy such luxury. They would be the most vulnerable, the weakest chains of IoT ecosystem in the post-quantum world. Can blockchain offers a decentralised security mechanism to protect these devices? Would blockchain evolve from keeping IoT cloud backends accountable to protecting the IoT ecosystem?

Or would a new technology emerge and take its place?

[2]https://truebit.io
[3]https://github.com/ethereum/wiki/wiki/Sharding-roadmap
[4]vitalik.ca/general/2018/08/26/layer_1.html

REFERENCES

[1] M. Y. Afanasev, A. A. Krylova, S. A. Shorokhov, Y. V. Fedosov, and A. S. Sidorenko. 2018. A Design of Cyber-physical Production System Prototype Based on an Ethereum Private Network. In *Proceedings of the 22nd Conference of Open Innovations Association (FRUCT)*. 3–11. DOI: http://dx.doi.org/10.23919/FRUCT.2018.8468296

[2] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar. 2018. Continuous Security in IoT Using Blockchain. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 6423–6427. DOI: http://dx.doi.org/10.1109/ICASSP.2018.8462513

[3] A. A. Ali, I. A. El-Dessouky, M. M. Abdallah, and A. K. Nabih. 2017. The quest for fully smart autonomous business networks in iot platforms. In *ACM International Conference Proceeding Series*. 13–18. DOI: http://dx.doi.org/10.1145/3178298.3178301

[4] M. S. Ali, K. Dolui, and F. Antonelli. 2017. IoT data privacy via blockchains and IPFS. In *ACM International Conference Proceeding Series*. DOI: http://dx.doi.org/10.1145/3131542.3131563

[5] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli. 2018. IoTChain: A blockchain security architecture for the Internet of Things. In *Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC*, Vol. 2018-April. 1–6. DOI: http://dx.doi.org/10.1109/WCNC.2018.8377385

[6] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren. 2018. A blockchain-based decentralized security architecture for Iot. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10972 LNCS. 3–18. DOI: http://dx.doi.org/10.1007/978-3-319-94370-1_1

[7] G. Ayoade, V. Karande, L. Khan, and K. Hamlen. 2018. Decentralized IoT data management using blockchain and trusted execution environment. In *Proceedings of the 19th IEEE International Conference on Information Reuse and Integration for Data Science, IRI 2018*. 15–22. DOI: http://dx.doi.org/10.1109/IRI.2018.00011

[8] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang. 2018. A Scalable Blockchain Framework for Secure Transactions in IoT. *IEEE Internet of Things Journal* (2018), 1–1. DOI: http://dx.doi.org/10.1109/JIOT.2018.2874095

[9] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey. 2017. Towards better availability and accountability for IoT updates by means of a blockchain. In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017*. 50–58. DOI: http://dx.doi.org/10.1109/EuroSPW.2017.50

[10] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh. 2018. A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. *IEEE Access* 6 (2018), 24639–24649. DOI: http://dx.doi.org/10.1109/ACCESS.2018.2799942

[11] S. S. Choi, J. W. Burm, W. Sung, J. W. Jang, and Y. J. Reo. 2018. A Blockchain-based Secure IoT Control Scheme. In *Proceedings of the International Conference on Advances in Computing and Communication Engineering (ICACCE)*. 74–78. DOI: http://dx.doi.org/10.1109/ICACCE.2018.8441717

[12] K. Christidis and M. Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* 4 (2016), 2292–2303. DOI: http://dx.doi.org/10.1109/ACCESS.2016.2566339

[13] M. Conoscenti, A. Vetro, and J. C. De Martin. 2017. Blockchain for the Internet of Things: A systematic literature review. In *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. DOI: http://dx.doi.org/10.1109/AICCSA.2016.7945805

[14] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, and Emin Gün Sirer. 2016. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer, 106–125.

[15] P. Danzi, A. E. Kalør, C. Stefanović, and P. Popovski. 2018. Analysis of the communication traffic for blockchain synchronization of IoT devices. In *IEEE International Conference on Communications*, Vol. 2018-May. DOI: http://dx.doi.org/10.1109/ICC.2018.8422485

[16] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini. 2017. CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In *Proceedings of IEEE International Conference on Communications*. DOI: http://dx.doi.org/10.1109/ICC.2017.7996641

[17] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard. 2018. A blockchain-based trust system for the internet of things. In *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*. 77–83. DOI: http://dx.doi.org/10.1145/3205977.3205993

[18] A. Dorri. 2019. Blockchain in internet of things: Challenges and Solutions. (2019). https://arxiv.org/abs/1608.05187v1

[19] A. Dorri, S. S. Kanhere, and R. Jurdak. 2017. Towards an optimized blockchain for IoT. In *Proceedings of the 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week)*. 173–178. DOI: http://dx.doi.org/10.1145/3054977.3055003

[20] C. Dukkipati, Y. Zhang, and L. C. Cheng. 2018. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In *ABAC 2018 - Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control, Co-located with CODASPY 2018*, Vol. 2018-January. 61–69. DOI: http://dx.doi.org/10.1145/3180457.3180458

[21] J. Ellul and G. J. Pace. 2018. AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things. In *Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018*, Vol. 2018-January. 1–4. DOI: http://dx.doi.org/10.1109/NTMS.2018.8328732

[22] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang. 2018. Blockchain-based Secure Time Protection Scheme in IoT. *IEEE Internet of Things Journal* (2018), 1–1. DOI: http://dx.doi.org/10.1109/JIOT.2018.2874222

[23] X. Fan. 2018. Faster dual-key stealth address for blockchain-based Internet of Things systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10974 LNCS. 127–138. DOI: http://dx.doi.org/10.1007/978-3-319-94478-4_9

[24] P. Gallo, S. Pongnumkul, and U. Quoc Nguyen. 2018. BlockSee: Blockchain for IoT Video Surveillance in Smart Cities. In *Proceedings of the IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / ICPS Europe)*. 1–6. DOI: http://dx.doi.org/10.1109/EEEIC.2018.8493895

[25] M. T. Hammi, P. Bellot, and A. Serhrouchni. 2018. BCTrust: A decentralized authentication blockchain-based mechanism. In *Proceedings of IEEE Wireless Communications and Networking Conference, WCNC*, Vol. 2018-April. 1–6. DOI: http://dx.doi.org/10.1109/WCNC.2018.8376948

[26] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni. 2018. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security* 78 (2018), 126–142. DOI: http://dx.doi.org/10.1016/j.cose.2018.06.004

[27] M. G. M. Mehedi Hasan, A. Datta, M. Ashiqur Rahman, and H. Shahriar. 2018. Chained of Things: A Secure and Dependable Design of Autonomous Vehicle Services. In *Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 02. 498–503. DOI: http://dx.doi.org/10.1109/COMPSAC.2018.10283

[28] M. Hossain, Y. Karim, and R. Hasan. 2018. FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. In *Proceedings of the IEEE International Congress on Internet of Things (ICIOT)*. 33–40. DOI: http://dx.doi.org/10.1109/ICIOT.2018.00012

[29] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie. 2018. A decentralized solution for IoT data trusted exchange based-on blockchain. In *Proceedings of the 3rd IEEE International Conference on Computer and Communications, ICCC 2017*, Vol. 2018-January. 1180–1184. DOI: http://dx.doi.org/10.1109/CompComm.2017.8322729

[30] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar. 2018. Mitigating IoT device based DDoS attacks using blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018*. 71–76. DOI: http://dx.doi.org/10.1145/3211933.3211946

[31] Y. Kaga, M. Fujio, K. Naganuma, K. Takahashi, T. Murakami, T. Ohki, and M. Nishigaki. 2017. A secure and practical signature scheme for blockchain based on biometrics. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10701 LNCS. 877–891. DOI: http://dx.doi.org/10.1007/978-3-319-72359-4_55

[32] E. Kak, R. Orji, J. Pry, K. Sofranko, R. Lomotey, and R. Deters. 2018. Privacy Improvement Architecture for IoT. In *Proceedings of IEEE International Congress on Internet of Things (ICIOT)*. 148–155. DOI: http://dx.doi.org/10.1109/ICIOT.2018.00028

[33] Anas Abou El Kalam, Aissam Outchakoucht, and Hamza Es-Samaali. 2018. Emergence-Based Access Control: New Approach to Secure the Internet of Things. In *Proceedings of the 1st International Conference on Digital Tools and Uses Congress*. ACM, 3240136, 1–11. DOI: http://dx.doi.org/10.1145/3240117.3240136

[34] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang. 2018. A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid. In *Proceedings of the 3rd International Conference on Computer and Communication Systems (ICCCS)*. 472–476. DOI: http://dx.doi.org/10.1109/CCOMS.2018.8463317

[35] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang. 2018. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. *IEEE Internet of Things Journal* (2018), 1–1. DOI: http://dx.doi.org/10.1109/JIOT.2018.2875542

[36] Bo Youn Kim, Seong Seok Choi, and Ju Wook Jang. 2018. Data Managing and Service Exchanging on IoT Service Platform Based on Blockchain with Smart Contract and Spatial Data Processing. In *Proceedings of the 2018 International Conference on Information Science and System*. ACM, 3209916, 59–63. DOI: http://dx.doi.org/10.1145/3209914.3209916

[37] Barbara Ann Kitchenham and Stuart M. Charters. 2007. *Guidelines for performing systematic literature reviews in software engineering.*

[38] N. Kshetri. 2017. Can Blockchain Strengthen the Internet of Things? *IT Professional* 19, 4 (2017), 68–72. DOI: http://dx.doi.org/10.1109/MITP.2017.3051335

[39] B. Lee and J. H. Lee. 2017. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *Journal of Supercomputing* 73, 3 (2017), 1152–1167. DOI: http://dx.doi.org/10.1007/s11227-016-1870-0

[40] C. H. Lee and K. H. Kim. 2018. Implementation of IoT system using block chain with authentication and data protection. In *Proceedings of the International Conference on Information Networking*, Vol. 2018-January. 936–940. DOI: http://dx.doi.org/10.1109/ICOIN.2018.8343261

[41] O. Leiba, Y. Yitzchak, R. Bitton, A. Nadler, and A. Shabtai. 2018. Incentivized Delivery Network of IoT Software Updates Based on Trustless Proof-of-Distribution. In *Proceedings of the 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*. 29–39. DOI: http://dx.doi.org/10.1109/EuroSPW.2018.00011

[42] C. Li and L. J. Zhang. 2017. A blockchain based new secure multi-layer network model for internet of things. In *Proceedings of the 2nd IEEE International Congress on Internet of Things, ICIOT 2017*. 33–41. DOI: http://dx.doi.org/10.1109/IEEE.ICIOT.2017.34

[43] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun. 2018. Blockchain For Large-Scale Internet of Things Data Storage and Protection. *IEEE Transactions on Services Computing* (2018). DOI: http://dx.doi.org/10.1109/TSC.2018.2853167

[44] Z. Li, A. V. Barenji, and G. Q. Huang. 2018. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing* 54 (2018), 133–144. DOI: http://dx.doi.org/10.1016/j.rcim.2018.05.011

[45] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. 2018. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3690–3700. DOI: http://dx.doi.org/10.1109/TII.2017.2786307

[46] X. Liang, J. Zhao, S. Shetty, and D. Li. 2017. Towards data assurance and resilience in IoT using blockchain. In *Proceedings of IEEE Military Communications Conference MILCOM*, Vol. 2017-October. 261–266. DOI: http://dx.doi.org/10.1109/MILCOM.2017.8170858

[47] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu. 2017. Blockchain Based Data Integrity Service Framework for IoT Data. In *Proceedings of the IEEE 24th International Conference on Web Services, ICWS 2017*. 468–475. DOI: http://dx.doi.org/10.1109/ICWS.2017.54

[48] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo. 2018. Distributed access control on IoT ledger-based architecture. In *Proceedings of the IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*. 1–7. DOI: http://dx.doi.org/10.1109/NOMS.2018.8406154

[49] T. Lundqvist, A. De Blanche, and H. R. H. Andersson. 2017. Thing-to-thing electricity micro payments using blockchain technology. In *Proceedings of the Global Internet of Things Summit, GIoTS 2017*. DOI: http://dx.doi.org/10.1109/GIOTS.2017.8016254

[50] Ferrag A. M. 2019. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. (2019).

[51] C. Machado and A. A. Frohlich. 2018. IoT data integrity verification for cyber-physical systems using blockchain. In *Proceedings of the 21st IEEE International Symposium on Real-Time Computing, ISORC 2018*. 83–90. DOI: http://dx.doi.org/10.1109/ISORC.2018.00019

[52] Diego M. Mendez Mena and Baijian Yang. 2018. Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. International World Wide Web Conferences Steering Committee, 3241853, 7–12. DOI: http://dx.doi.org/10.1145/3241815.3241853

[53] Microsoft. 2018. Microsoft Azure IoT Reference Architecture v2.1. *Technical Report* (2018).

[54] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati. 2017. Mind My Value: A decentralized infrastructure for fair and trusted IoT data trading. In *ACM International Conference Proceeding Series*. DOI: http://dx.doi.org/10.1145/3131542.3131564

[55] S. R. Niya, S. S. Jha, T. Bocek, and B. Stiller. 2018. Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and LoRaWAN. In *Proceedings of the IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*. 1–4. DOI: http://dx.doi.org/10.1109/NOMS.2018.8406329

[56] O. Novo. 2018. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal* 5, 2 (2018), 1184–1195. DOI: http://dx.doi.org/10.1109/JIOT.2018.2812239

[57] O. Odiete, R. K. Lomotey, and R. Deters. 2018. Using blockchain to support data and service management in IoV/IoT. In *Advances in Intelligent Systems and Computing*. Vol. 733. 344–362. DOI: http://dx.doi.org/10.1007/978-3-319-76451-1_33

[58] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks* 9, 18 (2016), 5943–5964. DOI: http://dx.doi.org/10.1002/sec.1748

[59] A. Z. Ourad, B. Belgacem, and K. Salah. 2018. Using blockchain for IOT access control and authentication management. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10972 LNCS. 150–164. DOI: http://dx.doi.org/10.1007/978-3-319-94370-1_11

[60] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito. 2018. Blockchain and iot integration: A systematic survey. *Sensors (Switzerland)* 18, 8 (2018). DOI: http://dx.doi.org/10.3390/s18082575

[61] A. Pieroni, N. Scarpato, L. Di Nunzio, F. Fallucchi, and M. Raso. 2018. Smarter City: Smart energy grid based on Blockchain technology. *International Journal on Advanced Science, Engineering and Information Technology* 8, 1 (2018), 298–306. DOI: http://dx.doi.org/10.18517/ijaseit.8.1.4954

[62] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini. 2018. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors (Switzerland)* 18, 1 (2018). DOI: http://dx.doi.org/10.3390/s18010162

[63] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao. 2018. Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach. *IEEE Internet of Things Journal* (2018), 1–1. DOI: http://dx.doi.org/10.1109/JIOT.2018.2871394

[64] C. Qu, M. Tao, and R. Yuan. 2018. A hypergraph-based blockchain model and application in internet of things-enabled smart homes. *Sensors (Switzerland)* 18, 9 (2018). DOI: http://dx.doi.org/10.3390/s18092784

[65] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan. 2018. Blockchain based credibility verification method for IoT entities. *Security and Communication Networks* 2018 (2018). DOI: http://dx.doi.org/10.1155/2018/7817614

[66] Y. Rahulamathavan, R. C. W. Phan, M. Rajarajan, S. Misra, and A. Kondoz. 2018. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In *Proceedings of the 11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*. 1–6. DOI: http://dx.doi.org/10.1109/ANTS.2017.8384164

[67] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz. 2018. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems* 88 (2018), 173–190. DOI: http://dx.doi.org/10.1016/j.future.2018.05.046

[68] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher. 2018. Towards using blockchain technology for IoT data access protection. In *Proceedings of the 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband, ICUWB 2017*, Vol. 2018-January. 1–5. DOI: http://dx.doi.org/10.1109/ICUWB.2017.8251003

[69] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, A. Pinto, and E. Di Sciascio. 2018. A Blockchain Infrastructure for the Semantic Web of Things. In *Proceedings of the CEUR Workshop*, Vol. 2161. 1DUMMY. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051857332&partnerID=40&md5=3c3579e550f1afc33d6b5941acc29ec4

[70] M. Samaniego and R. Deters. 2016. Using blockchain to push software-defined IoT components onto edge hosts. In *ACM International Conference Proceeding Series*. DOI: http://dx.doi.org/10.1145/3010089.3016027

[71] M. Samaniego and R. Deters. 2018. Zero-Trust Hierarchical Management in IoT. In *Proceedings of the IEEE International Congress on Internet of Things (ICIOT)*. 88–95. DOI: http://dx.doi.org/10.1109/ICIOT.2018.00019

[72] E. R. Sanseverino, M. L. D. Silvestre, P. Gallo, G. Zizzo, and M. Ippolito. 2018. The blockchain in microgrids for transacting energy and attributing losses. In *Proceedings of the IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, Vol. 2018-January. 925–930. DOI: http://dx.doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.142

[73] M. Saravanan, R. Shubha, A. M. Marks, and V. Iyer. 2018. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In *Procedings of the 11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*. 1–6. DOI: http://dx.doi.org/10.1109/ANTS.2017.8384099

[74] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy. 2017. Towards blockchain-based auditable storage and sharing of iot data. In *Proceedings of the 2017 Cloud Computing Security Workshop, co-located with CCS 2017*. 45–50. DOI: http://dx.doi.org/10.1145/3140649.3140656

[75] P. K. Sharma, M. Y. Chen, and J. H. Park. 2018. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access* 6 (2018), 115–124. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2757955

[76] P. K. Sharma and J. H. Park. 2018. Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems* 86 (2018), 650–655. DOI: http://dx.doi.org/10.1016/j.future.2018.04.060

[77] P. K. Sharma, S. Rathore, Y. Jeong, and J. H. Park. 2018. Energy-Efficient Distributed Network Architecture for Edge Computing. *IEEE Communications Magazine* (2018), 2–9. DOI: http://dx.doi.org/10.1109/MCOM.2018.1700822

[78] M. Singh and S. Kim. 2018. Trust Bit: Reward-based intelligent vehicle commination using blockchain paper. In *Proceedings of the IEEE World Forum on Internet of Things, WF-IoT 2018*, Vol. 2018-January. 62–67. DOI: http://dx.doi.org/10.1109/WF-IoT.2018.8355227

[79] G. Spathoulas, A. Collen, P. Pandey, N. A. Nijdam, S. Katsikas, C. S. Kouzinopoulos, M. Ben Moussa, K. M. Giannoutakis, K. Votis, and D. Tzovaras. 2018. Towards Reliable Integrity in Blacklisting: Facing Malicious IPs in GHOST Smart Contracts. In *Proceedings of the Innovations in Intelligent Systems and Applications (INISTA)*. 1–8. DOI: http://dx.doi.org/10.1109/INISTA.2018.8466327

[80] H. Sun, S. Hua, E. Zhou, B. Pi, J. Sun, and K. Yamashita. 2018. Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10974 LNCS. 3–17. DOI: http://dx.doi.org/10.1007/978-3-319-94478-4_1

[81] N. Tapas, G. Merlino, and F. Longo. 2018. Blockchain-Based IoT-cloud authorization and delegation. In *Proceedings of the IEEE International Conference on Smart Computing, SMARTCOMP 2018*. 411–416. DOI: http://dx.doi.org/10.1109/SMARTCOMP.2018.00038

[82] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian. 2018. Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access* 6 (2018), 32700–32726. DOI:http://dx.doi.org/10.1109/ACCESS.2018.2846779

[83] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang. 2018. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access* 6 (2018), 17545–17556. DOI:http://dx.doi.org/10.1109/ACCESS.2018.2805837

[84] B. Wen, Z. Luo, and Y. Wen. 2018. Evidence and trust: IoT Collaborative security mechanism. In *Proceedings of the 8th International Conference on Information Science and Technology, ICIST 2018*. 98–103. DOI:http://dx.doi.org/10.1109/ICIST.2018.8426148

[85] L. Wu, X. Du, W. Wang, and B. Lin. 2018. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. In *Proceedings of the International Conference on Computing, Networking and Communications, ICNC 2018*. 769–773. DOI:http://dx.doi.org/10.1109/ICCNC.2018.8390280

[86] C. Xie, Y. Sun, and H. Luo. 2017. Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking. In *Proceedings of the 3rd International Conference on Big Data Computing and Communications, BigCom 2017*. 45–50. DOI:http://dx.doi.org/10.1109/BIGCOM.2017.43

[87] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han. 2018. When mobile blockchain meets edge computing. *IEEE Communications Magazine* 56, 8 (2018), 33–39. DOI:http://dx.doi.org/10.1109/MCOM.2018.1701095

[88] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong. 2018. A blockchain-based storage system for data analytics in the internet of things. In *Studies in Computational Intelligence*. Vol. 715. 119–138. DOI:http://dx.doi.org/10.1007/978-3-319-58190-3_8

[89] J. Yang, Z. Lu, and J. Wu. 2018. Smart-toy-edge-computing-oriented data exchange based on blockchain. *Journal of Systems Architecture* 87 (2018), 36–48. DOI:http://dx.doi.org/10.1016/j.sysarc.2018.05.001

[90] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung. 2018. Blockchain-based Decentralized Trust Management in Vehicular Networks. *IEEE Internet of Things Journal* (2018), 1–1. DOI:http://dx.doi.org/10.1109/JIOT.2018.2836144

[91] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung. 2018. A blockchain-based reputation system for data credibility assessment in vehicular networks. In *Procedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, Vol. 2017-October. 1–5. DOI:http://dx.doi.org/10.1109/PIMRC.2017.8292724

[92] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko. 2017. Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access* 6 (2017), 1513–1524. DOI:http://dx.doi.org/10.1109/ACCESS.2017.2779263

[93] Y. Zhang, Y. Han, and J. Wen. 2018. SMER: a secure method of exchanging resources in heterogeneous internet of things. *Frontiers of Computer Science* (2018). DOI:http://dx.doi.org/10.1007/s11704-018-6524-3

[94] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. 2018. Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal* (2018). DOI:http://dx.doi.org/10.1109/JIOT.2018.2847705

[95] Y. Zhang and J. Wen. 2015. An IoT electric business model based on the protocol of bitcoin. In *Proceedings of the 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*. 184–191. DOI:http://dx.doi.org/10.1109/ICIN.2015.7073830

[96] L. Zhou, L. Wang, Y. Sun, and P. Lv. 2018. BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation. *IEEE Access* 6 (2018), 43472–43488. DOI:http://dx.doi.org/10.1109/ACCESS.2018.2847632

Received Month 2019; revised Month 2019; accepted Month 2019