

Blockchain solutions for Internet of Things Systems

NGUYEN KHOI TRAN, The University of Adelaide, Australia

MUHAMMAD ALI BABAR, The University of Adelaide, Australia

Internet of Things (IoT) systems lay the foundation for the future computing. They fuel the decision making and machine learning pipelines and then feeds these decisions back to the physical world. As a result, IoT systems must be trustworthy. However, they are vulnerable.

In the past few years, Distributed Ledger Technologies, specifically Blockchain (BC), have been increasingly used to address these challenges. BC provides a decentralised, immutable source of truth, upon which many solutions have been proposed. By 2018, over 400 peer-reviewed primary studies on BC-IoT integration have been published. This wealth of efforts 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 such as tactical, emergency response, and common operating picture. In this article, we present a systematic review of 90 prominent primary studies on BC-IoT integration. Our review focuses on three questions: Why do IoT systems integrate blockchains? How do IoT systems integrate blockchains? and What optimisations were performed to blockchains for run on IoT infrastructure? These questions aim at the technical problems posed by IoT systems and the solutions offered by BC. Thus, they are relevant across IoT verticals and beyond.

CCS Concepts: • **Information systems** → **Web search engines**; *Information retrieval*;

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

ACM Reference Format:

Nguyen Khoi Tran and Muhammad Ali Babar. 2017. Blockchain solutions for Internet of Things Systems. *ACM Comput. Surv.* 0, 0, Article 01 (January 2017), 23 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 values and cooperate. Internet of Things technologies allow physical entities to listen and talk to other physical and digital entities which might not be trustworthy. The convergence of two technology is imminent. Its 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

Authors' addresses: Nguyen Khoi Tran, The University of Adelaide, Adelaide, SA, 5005, Australia; Muhammad Ali Babar, The University of Adelaide, Adelaide, SA, 5005, Australia.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.

0360-0300/2017/1-ART01 \$15.00

<https://doi.org/0000001.0000001>

IoT devices? How 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 those 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 creates 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 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 BC network has been setup, optimized, and used in IoT system.

This playbook is synthesized from BC-related IoT systems in the academic literature. We assessed 375 related research works starting from the first IoT-BC 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 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 [45]. 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, potentially malicious. Multiple applications can share an IoT system's sensing infrastructure, perhaps for a fee. This sharing emerges during the operation of an IoT infrastructure, differentiating it from traditional industrial control systems.

Most IoT systems revolve around a centralized IoT platform. This platform (i) monitors and configures IoT devices, (ii) provides an interface to interact with IoT devices, (iii) stores data generated by IoT devices, (iv) helps analyze and visualize IoT data for events and actions, and (v) secures IoT system from malicious data and requests. Cloud-based platforms make managing IoT system and developing IoT systems simpler. *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 signal must travel multiple hops across the Internet.

Blockchains help decentralise IoT systems. With blockchains, all participants of an IoT system of 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 in addition can use additional logic in form of Smart Contracts. As a cryptographically secured system, blockchains rely on cryptography for security. Each block 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 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 right 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 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 METHODOLOGY

We employed Systematic Literature Review (SLR) method to conduct the study. A systematic literature review (SLR) synthesis existing work in a manner that is fair and seen to be fair [32]. SLRs are driven by explicit and documented review protocols. These protocols specify the research questions and the methods to conduct the review to answer those questions.

¹<https://github.com/ethereum/wiki/wiki/White-Paper>

The review methods comprise five steps [32]:

- (1) Identify potential primary studies from credible sources, such as peer-reviewed academic journals.
- (2) Excluding the studies that are irrelevant to the research questions.
- (3) Filtering the potential studies based on their quality. The remaining studies become the input of the SLR.
- (4) Extracting the data from the selected primary studies. The research questions determine the features to be extracted from the studies.
- (5) Synthesizing the answers to the research questions from the data and report the SLR.

Research questions drive the review methods. They determine the types of papers that would be needed, which in turn influence the query for papers and the selection criteria upon them. They also control the knowledge that we can get out of the review process by determining the features to be extracted and synthesized from the primary studies. To be systematic, review questions, queries, criteria, and extractions features are all predefined and documented prior to the conduct of the review.

3.1 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 is where blockchains and their smart contracts fit into an IoT system, physically and logically (RQ2.1). The second aspect concerns with the data and logic that blockchains and smart contracts handle for IoT systems (RQ2.2). The third aspect is how the integrated blockchains have been configured (RQ2.3). These three aspects constitute a complete 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. For instance, IoT devices lack the computing capability, storage, and network bandwidth to participate in blockchain networks. This research question helps identify the optimisations to blockchain systems to satisfy the constraints of IoT systems. These optimisations can be transferred to other cases of blockchain integration.

3.2 Study Identification and Selection

We followed a five-step process to identify and select primary studies for the review.

The first step is to *identify potential primary studies*. We chose Scopus as the primary source of scholarly peer-reviewed articles. We use IEEE Xplore and ACM Digital Library as supplementary sources. The reason is that in our pilot search, we found that Scopus has a broader coverage than the other two. Another reason is that Scopus provides better support for structured query and also for reproducing search queries. We decided not to include Google Scholar as a source due to the lack of structured query capability and lack of reproducibility. To find studies that lie at the intersection between Blockchains and Internet of Things research, we used the following query:

[“Blockchain” OR “block chain”]
AND

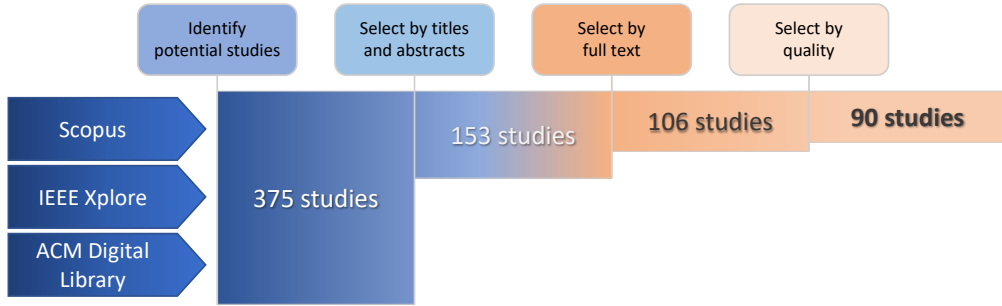


Fig. 1. Study Identification and Selection Process.

ternet of Things” OR “IoT” OR “Web of Things” OR “WoT” OR “Industrial Internet of Things”

Query results were filtered by their field of study and language. We assessed only English-written studies in the field of Computer Science, Engineering, and Mathematics.

The next step is to *preprocess and aggregate potential studies*. From the result lists, we removed entries that represent collections of work, such as conference proceedings. We combined lists of articles from all three sources into an aggregated list. Finally, we remove duplicates in the aggregated list.

The third step is to *assess the relevance of potential studies*. We conducted the relevance assessment in two rounds. The first round is on title and abstract of the potential studies. The second round is on the full text of the remaining studies. In both rounds, we apply criterion 1 and 2 of the selection criteria, which we will describe later in this section.

The fourth step is to *appraise the quality of potential studies*. We applied the criterion 3 of the selection criteria. The remaining studies after this step became the input of the review process.

The last step is to *cross-validate and adjust the selection*. 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 that the first author made. Results from co-authors were then compared. Adjustment would be done if the agreement is less than 85.

We assessed each potential study against three following criteria:

- 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.

By following the described process, we identified 375 *potential studies* and narrowed them down to a *review set of 90* (Fig. 1). The query on digital libraries returned 375 results. By assessing titles and abstracts of the studies against criterion 1 and 2, we reduced the number of potential studies to 153. Further assessment on full text of the remaining studies reduced the potential studies to 106. Finally, we applied criterion 3 to assess the quality of the studies and generated the final set of 90 studies. These studies became the input of the literature review process.

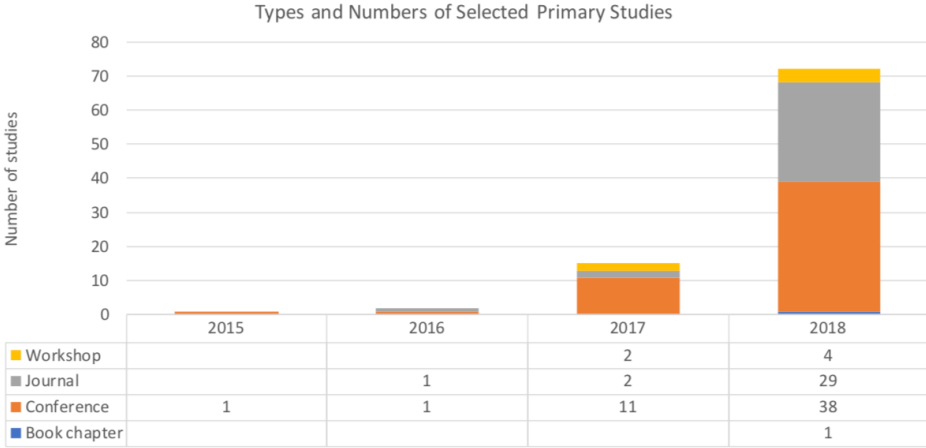


Fig. 2. Distribution of the selected studies by publication year and type.

The earliest work on BC-IoT integration that we found and included in the set was from 2015. It was about 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. 2).

3.3 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 functional modules of an IoT system that a blockchain replaces or enhances represent its logical position. The physical position of a blockchain denotes the placement of its elements onto hardware nodes of an IoT system. We considered four types of blockchain elements. A miner node collects transactions and generates new blocks to expand a blockchain. A wallet node stores the private keys of a user and creates new transactions with these keys. A full node stores the entire blockchain in its local storage. It might also act as a miner. A light weight node stores only the metadata (i.e., headers) of a ledger. It might also act as a wallet. These elements of blockchains are deployed on three types of nodes in an IoT system. Edge devices are low-power computing nodes with sensing and actuating capability. Fog devices locate on-premise, one-hop away from edge devices. Cloud nodes locate off-premise and require Internet-routing to reach.

For RQ2.2, we extracted *on-, off-chain data and on-, off-chain logic*. On-chain 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

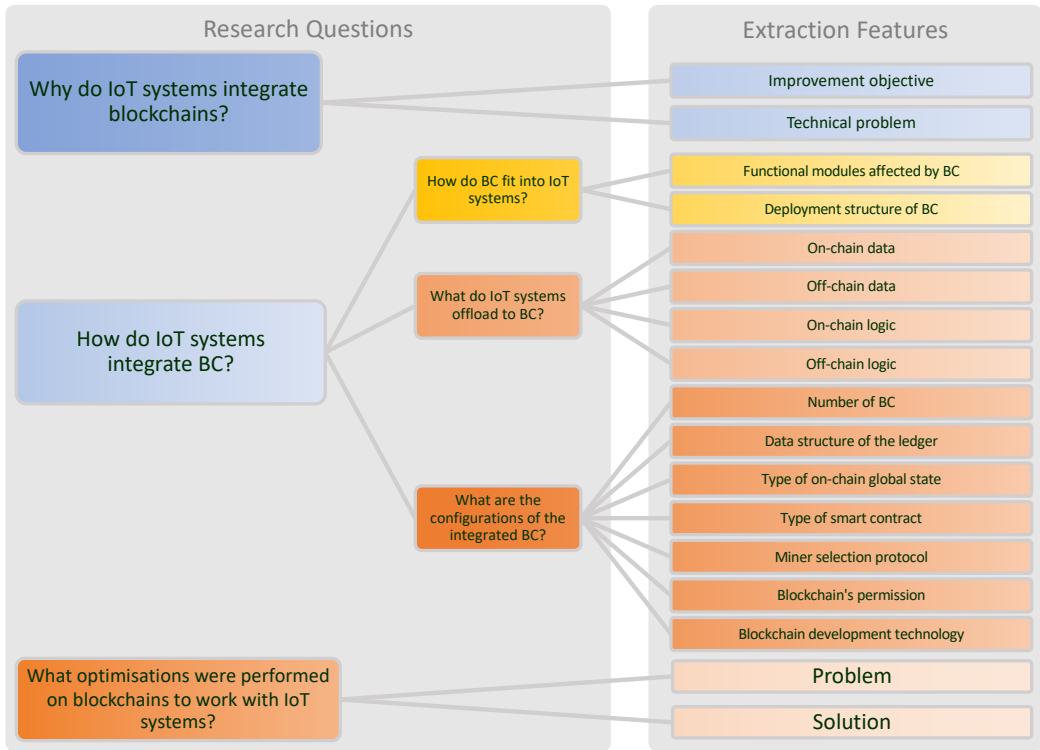


Fig. 3. Extraction features of the investigated research questions.

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 that represent key variabilities of blockchain systems*. These key variabilities act as a condensed description of blockchain systems. To identify these features, we started with a set of potential features based on the architecture of Bitcoin, Ethereum, and Hyperledger Fabric. Then, we simplified these features as we assessed the primary studies until we came up with a minimal feature set that can describe most blockchains that BC-IoT research prototypes used. 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 Unspent Transaction Output (UTXO) and Account models. The former was used by Bitcoin, while the latter was used by Ethereum. 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 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

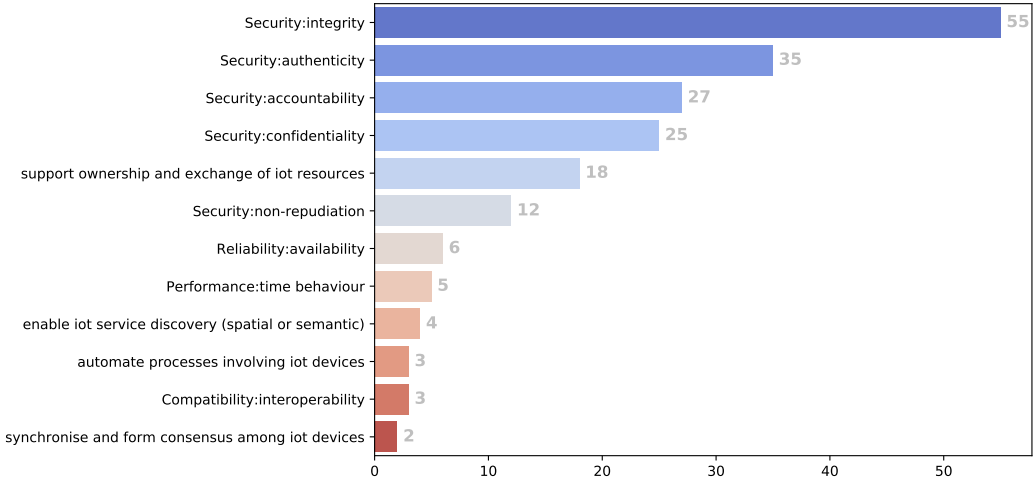


Fig. 4. Distribution of improvement objectives.

technology feature captures the information on how 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. These challenges are reported in the primary studies. We did not include speculated challenges. We only included challenges from studies that also propose the solutions to those challenges.

4 IoT PROBLEMS AND BLOCKCHAIN SOLUTIONS

4.1 Objectives of Blockchain Integration

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

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 [11, 29, 38, 42, 46, 49, 52, 62, 72, 81, 83]. Smart contracts on blockchains can orchestrate and incentivise the exchange of resources. Blockchains can keep immutable records of transactions. Blockchains and smart contracts can also store and maintain registry for services that IoT devices offer [3, 12, 31, 59]. Smart contracts running on blockchains can be also used to represent business processes that involve IoT devices in different platforms [16, 22, 53]. 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 [17].

Eight out of ten reviewed research 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, 22, 41, 47, 60]. Blockchains can

even store hashes of devices' configurations and firmware to detect tampering [19]. Authenticity improvement can be achieved by building authentication mechanisms on top of blockchains [8, 15, 20]. For example, blockchains can act as a second channel for two-factor authentication [74]. Confidentiality improvement can be achieved by building new authorization mechanisms on top of blockchains [44, 51, 61]. 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 product or 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 [60]. This blockchain helps the system function when it loses the connectivity to the cloud backend. Another approach is replacing centralised cloud backends with blockchains to negate the single point of failure in IoT systems [77, 84]

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 logics 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, 13] instead of to perform data transformation or similar tasks to enable syntactic and semantic interoperability.

4.2 Problems posed by IoT Systems

Regardless the objective, each BC-IoT research prototype addresses a subset of sixteen technical problems of IoT systems (Fig. 5). These technical problems can be classified into five categories (Fig. 6).

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 [24, 29, 76, 83]. Others use blockchains to regulate and keep the backends accountable [3, 78]. These works pursue decentralisation for different objectives:

- Increasing the integrity data collected by IoT devices. This is critical for IoT systems whose data has large social and legal implications, such as pollution level [47]
- 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.

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

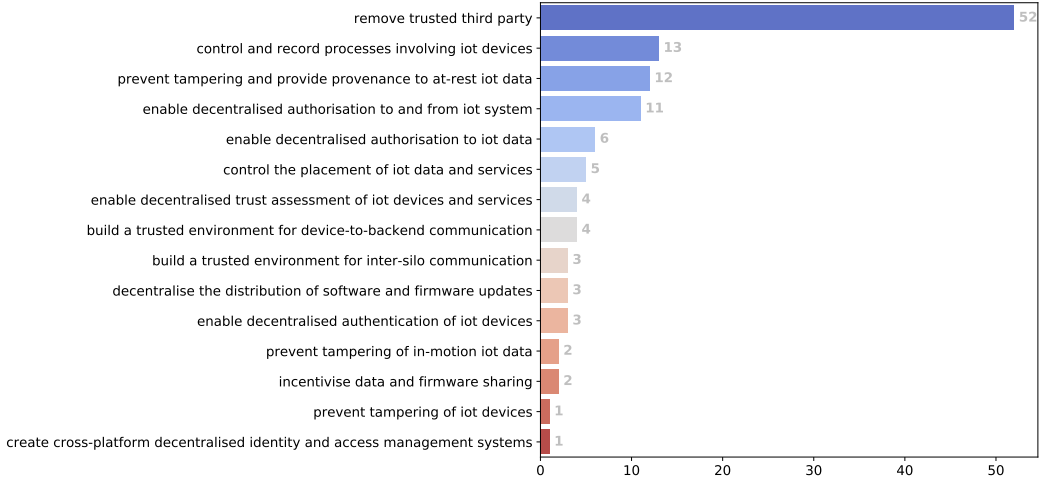


Fig. 5. Technical problems posed by IoT systems.

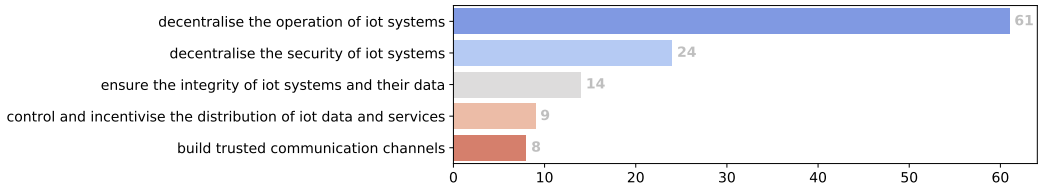


Fig. 6. Category of technical problems posed by IoT systems.

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 as an immutable, decentralised source of trust to store reputation rating [28, 80], incidents [68], or access requests [9, 15, 63, 70]. Smart contracts then can use the trusted records in the ledger to authenticate, authorise [51], and assess the reputation of parties in IoT systems [68].

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 [19]. 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, 41] or signatures of IoT data [19, 33] 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 [56, 60, 65]. 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 [34]. Maintaining up-to-date firmware is critical to the security of IoT systems. However, manufacturers might 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 [39, 43, 61]. 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, 13, 78].

4.3 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. 7). 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 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. 8). 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

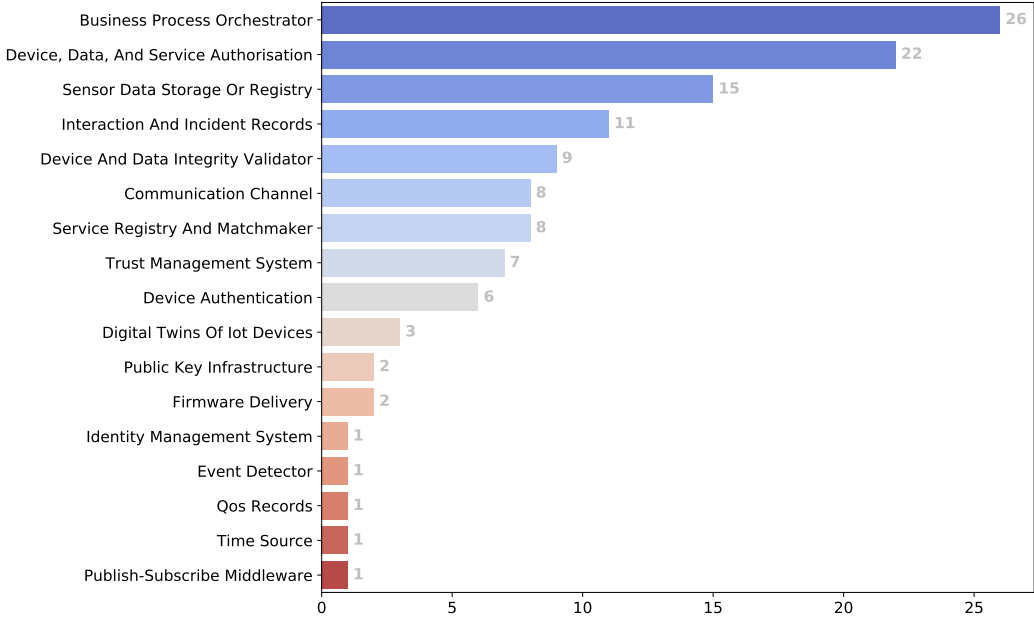


Fig. 7. Functional modules of IoT systems added or replaced by the integrated blockchains.

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. 9):

- Resource exchange records which support business process orchestration (21 out of 90) [6, 11, 13, 24, 29, 31, 34, 36–38, 42, 46, 49, 52, 69, 72, 76, 78, 81, 83]
- Device interaction records (14 out of 90) [2, 3, 8, 10, 14, 16, 18, 23, 25, 26, 35, 41, 55]
- Sensor readings (13 out of 90) [1, 30, 35, 47, 53, 57, 61, 71, 75, 77, 84]
- Authorisation requests and responses, which drive the authorisation mechanisms (12 out of 90) [4, 5, 7, 15, 21, 28, 48, 50, 51, 63, 70, 82]
- Service interaction records (11 out of 90) [3, 14, 22, 23, 27, 31, 60, 65, 66, 81, 84]
- Hashes of sensor readings (11 out of 90) [4, 7, 19, 33, 37, 39, 40, 43, 58, 64, 73]

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 on the chain to synchronise SDN controllers [54, 65, 67], current time to synchronise decentralised IoT devices [17], and device configurations to verify their

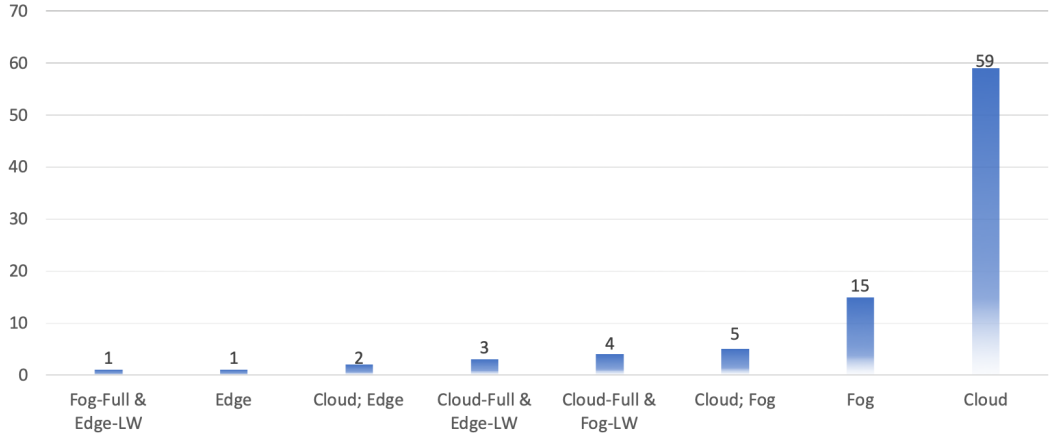


Fig. 8. Distribution of deployment structures of the integrated blockchains.

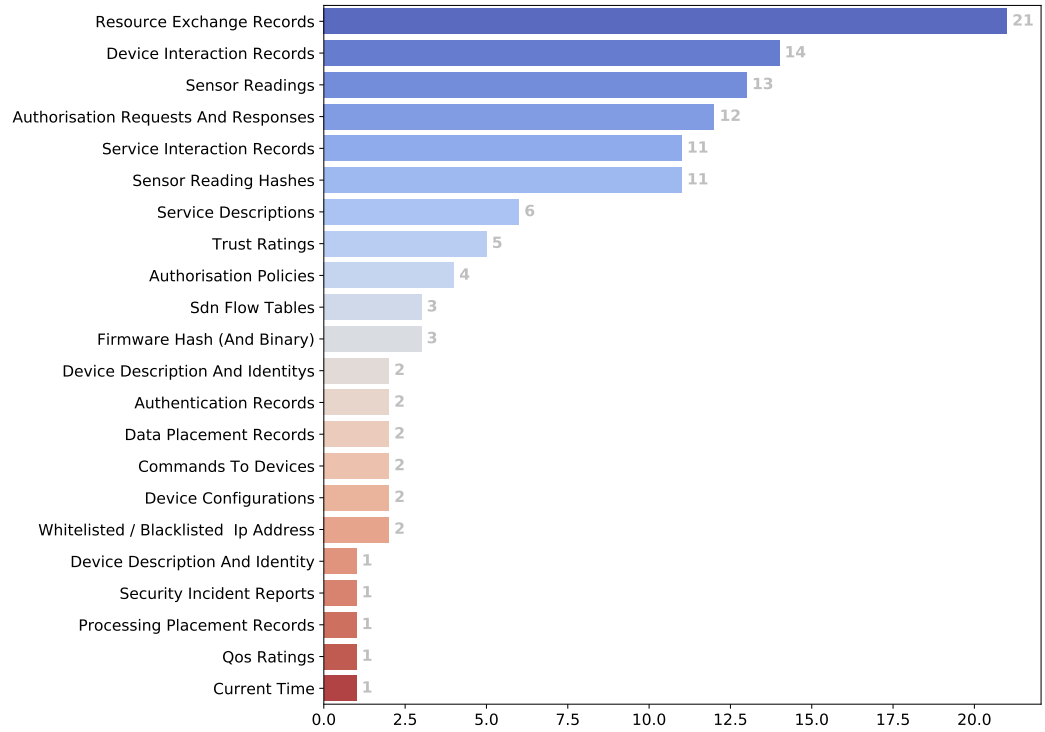


Fig. 9. Distribution of on-chain data types among BC-IoT prototypes.

integrity [19, 35]. Off-chain data is only used by one out of 90 reviewed work to store 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. 10. Recall that

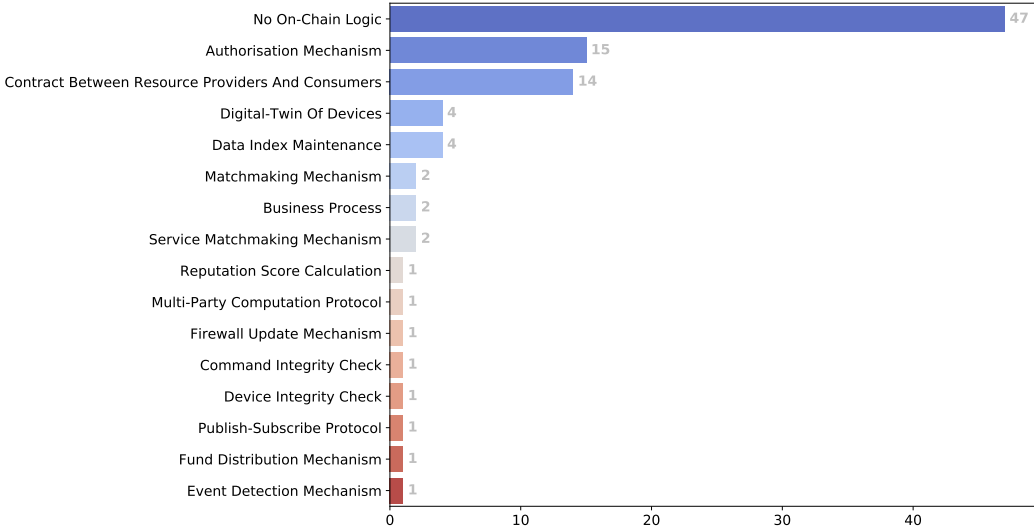


Fig. 10. Distribution of on-chain logic types among BC-IoT prototypes.

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 the system as a part of the blockchain system. These *off-chain logic* are not common (Fig. 11). 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.

4.4 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 (Fig. 12). Only 9 out of 90 reviewed BC-IoT prototypes employed more than one blockchain [4, 8, 12–14, 43, 56, 65, 71]. 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. 13). Public chain is still the most common form of blockchain (7 out of 10 works on average). Private and consortium

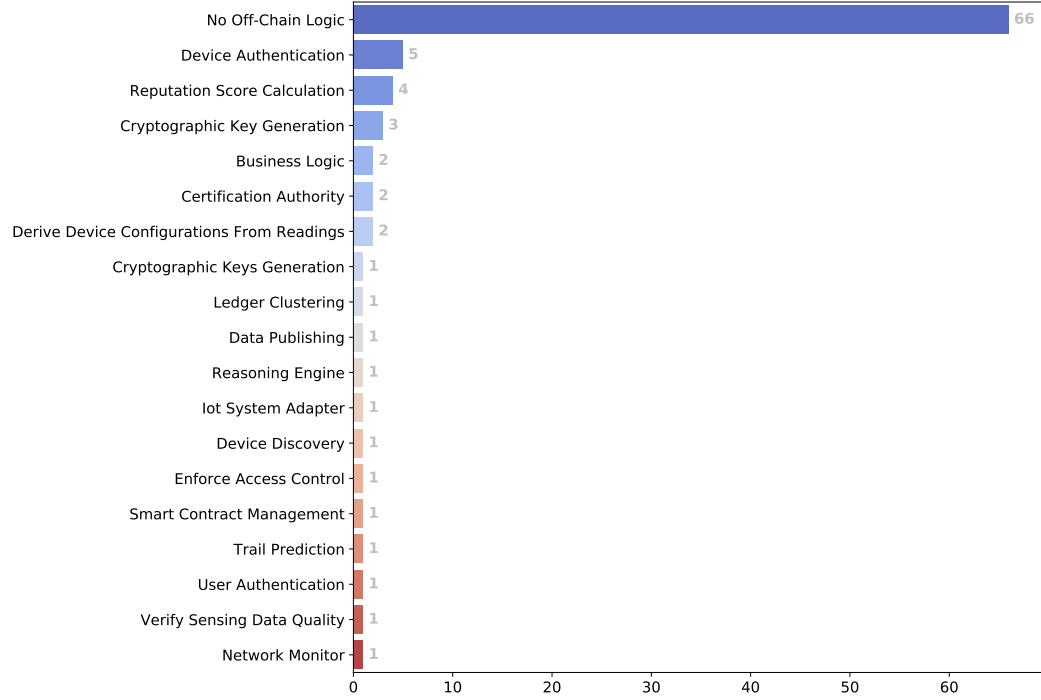


Fig. 11. Distribution of off-chain logic types among BC-IoT prototypes.

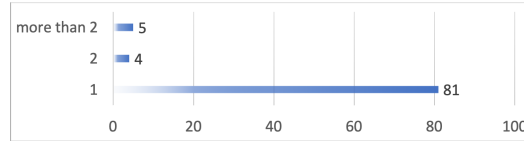


Fig. 12. Number of blockchains in the reviewed BC-IoT research prototypes.

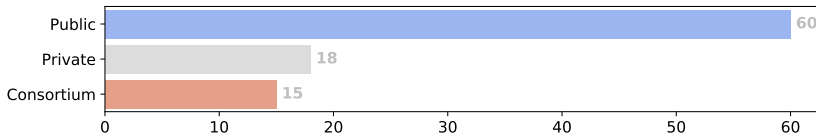


Fig. 13. Distribution of permission types of blockchains in the reviewed BC-IoT research prototypes.

chains are used but to a lesser degree, and usually as a part of a multi-chain setup, as we mentioned previously.

The next feature is the *consensus scheme*, specifically the *protocol to select a miner* to extend a chain (Fig. 14). An overwhelming number of works use some variants of Proof-of-work. In Bitcoin proof-of-work protocol, miners race to find a nonce that will make the hash of the 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 the block. The probability of winning a mining round

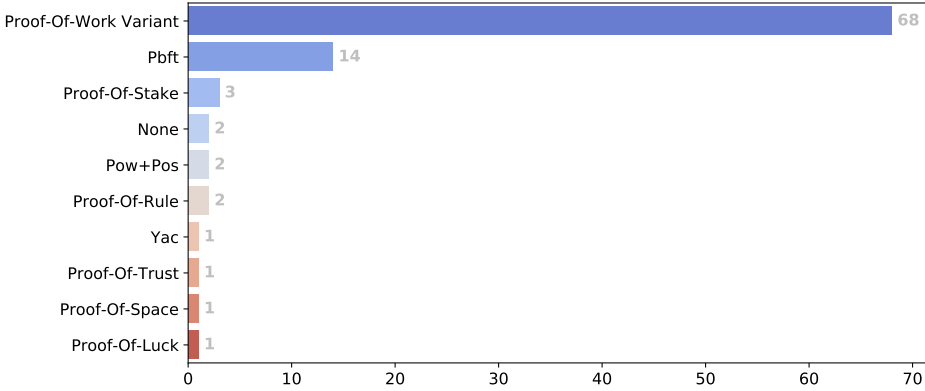


Fig. 14. Distribution of consensus schemes in the reviewed BC-IoT prototypes.

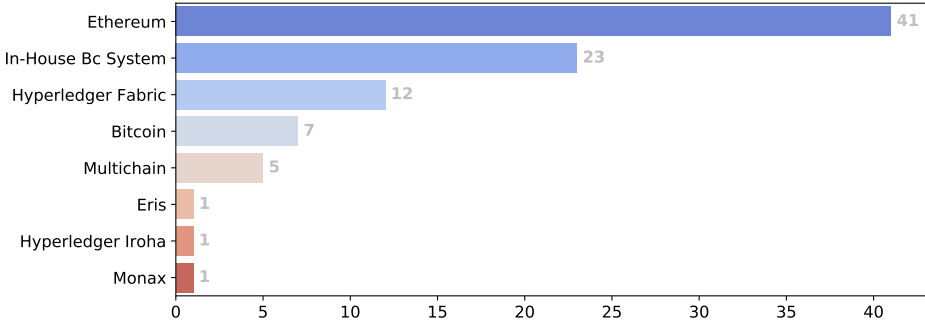


Fig. 15. Blockchain development technology employed by the BC-IoT research prototypes.

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 [71]. In this protocol, clients rank miners by trust rating. For every set of transaction, 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 [43] (e.g., Software Guard Extensions (SGX) in Intel's CPUs), or a combination of PoW with Proof-of-Stake [65, 79]. Interestingly, some BC-IoT prototypes dropped consensus protocol entirely and rely on other mechanisms such as distributed trust assessment [14].

The next feature is the *technology used* to build the integrated blockchain (Fig. 15). 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 this 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.

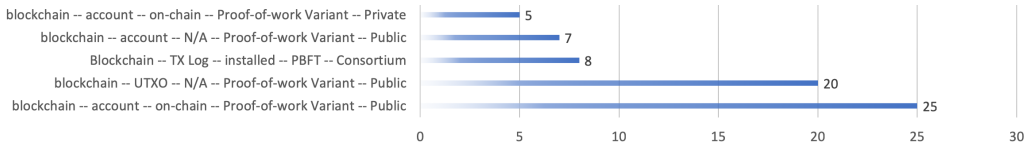


Fig. 16. Common configurations of blockchain in BC-IoT systems.

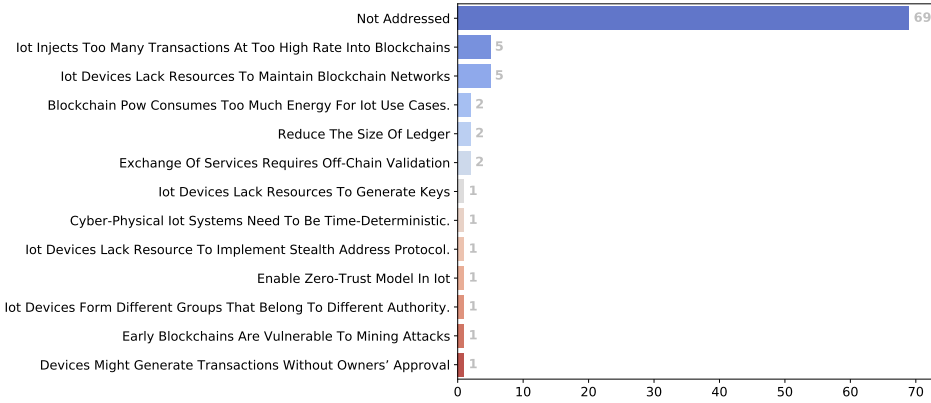


Fig. 17. Problems of IoT systems that drove the optimisation of blockchains.

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 not 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 16 shows the top five patterns.

4.5 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 [31, 69, 84]. 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 [22] 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 mean that IoT devices *cannot execute smart contract by themselves*. Instead, they rely on other nodes that participate in the 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 [16] 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 [18].

Another common problem that drives blockchain optimisations is the *massive influx of IoT data into the system*. 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 [71], replacing it with more efficient consensus protocols such as Proof-of-stake [53] and Proof-of-trust [43], or to removing it altogether [14]. The second approach is to reduce the amount of data injecting into blockchain. It has been done by either aggregating [42] or filtering sensor data [75] before submitting to the chain. The third approach is employing multiple chains [4, 8, 61]. 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 [41]. 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 [55].

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 [34] and proof-of-service [65]. Another challenge is protecting early blockchains. This is relevant to many 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.

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. Ayoadé, 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] 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>
- [10] 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>
- [11] 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>
- [12] 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>
- [13] 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>
- [14] 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>
- [15] C. Dukkupati, 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>
- [16] J. Ellul and G. J. Pace. 2018. AlkyIVM: 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>
- [17] 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>
- [18] 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
- [19] 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>
- [20] 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.2018.8377385>

- <http://dx.doi.org/10.1109/WCNC.2018.8376948>
- [21] 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>
 - [22] 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>
 - [23] 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>
 - [24] 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, ICC 2017*, Vol. 2018-January. 1180–1184. DOI: <http://dx.doi.org/10.1109/CompComm.2017.8322729>
 - [25] 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>
 - [26] 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
 - [27] 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>
 - [28] 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>
 - [29] 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>
 - [30] 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>
 - [31] 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>
 - [32] Barbara Ann Kitchenham and Stuart M. Charters. 2007. *Guidelines for performing systematic literature reviews in software engineering*.
 - [33] 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>
 - [34] 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>
 - [35] 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>
 - [36] 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>
 - [37] 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>
 - [38] 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>
 - [39] 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>

- [40] 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>
- [41] 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>
- [42] 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>
- [43] 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>
- [44] 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>
- [45] Microsoft. 2018. Microsoft Azure IoT Reference Architecture v2.1. *Technical Report* (2018).
- [46] P. Missier, S. Bajoudah, A. Caposelle, 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>
- [47] 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>
- [48] 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>
- [49] 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
- [50] 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>
- [51] 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
- [52] 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>
- [53] 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>
- [54] 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>
- [55] 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>
- [56] 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>
- [57] 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>
- [58] 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>
- [59] 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. IDUMMY. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051857332&partnerID=40&md5=3c3579e550f1afc33d6b5941acc29ec4>
- [60] 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>

- [61] 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>
- [62] 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-CPSCo-SmartData 2017*, Vol. 2018-January. 925–930. DOI : <http://dx.doi.org/10.1109/iThings-GreenCom-CPSCo-SmartData.2017.142>
- [63] M. Saravanan, R. Shubha, A. M. Marks, and V. Iyer. 2018. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. 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.2017.8384099>
- [64] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquenois. 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>
- [65] 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>
- [66] 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>
- [67] 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>
- [68] 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>
- [69] 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
- [70] 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>
- [71] 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>
- [72] 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>
- [73] 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>
- [74] 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>
- [75] 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>
- [76] 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>
- [77] 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
- [78] 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>
- [79] 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>
- [80] 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 *Proceedings 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>
- [81] 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>

- [82] 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>
- [83] 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>
- [84] 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 2017; revised Month 2017; accepted Month 2017