IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MOBILE SERVICE COMPUTING WITH INTERNET OF THINGS

Received April 8, 2019, accepted April 25, 2019, date of publication May 3, 2019, date of current version May 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914675

Analysis of Blockchain Solutions for IoT: A Systematic Literature Review

SIN KUANG LO[1,2], YUE LIU[3], SU YEN CHIA[4], XIWEI XU[1,2], QINGHUA LU[1,2], LIMING ZHU[1,2], AND HUANSHENG NING[4]

[1]Data61, CSIRO, Canberra, ACT 2601, Australia
[2]School of Computer Science and Engineering (CSE), University of New South Wales (UNSW), Sydney, NSW 2052, Australia
[3]China University of Petroleum (East China), Qingdao 266580, China
[4]University of Science and Technology Beijing, Beijing 100091, China

Corresponding author: Sin Kuang Lo (sinkuang.lo@data61.csiro.au)

ABSTRACT The Internet of Things (IoT) aims at connecting things to the Internet in a peer-to-peer paradigm for data collecting and data sharing in our daily life. A blockchain is an immutable append-only ledger maintained by a peer-to-peer network, where the whole network needs to reach a consensus on the transactional data stored on the ledger. With the decentralization nature, the design of IoT and blockchain aligns with each other well. Blockchain has been integrated with the IoT to solve the existing IoT problems. Our research focuses on analyzing the solutions proposed in academia and the methodologies used to integrate blockchain with the IoT. Through conducting a systematic literature review (SLR) on peer-reviewed, published articles on blockchain-based solutions for IoT, we gather the knowledge on current technical approaches implemented to integrate blockchain into the IoT. Majority of the research in this space is either at a conceptual level or at a very early stage. However, we only found 35 published papers with the real implementation of blockchain in the IoT platforms. We elicit the challenges of the IoT that were being addressed, and the detailed design of the blockchain-based solutions from two perspectives, namely data management and thing management. The evaluation methods and metrics used by those works are also being recorded and analyzed. In addition to the analysis of the literature, we provide our insights on improving the existing solutions and research methodology based on our expertise and experience on the blockchain.

INDEX TERMS Internet of Things, blockchain, data privacy, identity management systems.

I. INTRODUCTION

Internet of Things (IoT) aims at building smart space by connecting Things to internet and exchanging the collected data in a peer-to-peer paradigm [1]. Industry projects have been building IoT platforms in domains such as supply chain, manufacturing and energy grid. However, the development and management of IoT platforms are challenging for developers [2]. An IoT platform consists of mass of Things, and generally all the connected Things are controlled by a central node. Such a centralized architecture introduces single-point of failure. Second, it is inefficient for centralized servers to handle all the data collected by the Things in the IoT platform as heavy computing resources are required [3], [4]. Third, the management of Things is complicated as there is no established standard for managing the Things to address the issues including data privacy, data security, Thing security, as well as system maintenance for a large number of connected Things [5].

A blockchain is an immutable distributed ledger maintained by a peer-to-peer network, where the network participants must reach a consensus on the states of transactions submitted to the blockchain network to make the transactions valid [6]. The operation of the blockchain network does not rely on any centralized trusted third-party. Moreover, every participant of a blockchain network contains a local replica of all the historical transactions, which provides data transparency to network participants and ensures high availability of the system.

The decentralization nature of blockchain and the unique properties provided by blockchain attract researchers to investigate the potential of using blockchain to solve the existing challenges in IoT [7]. However, most of the existing works in this area either focus on the conceptual level or

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

still at a very early stage of integrating both technologies. Therefore, in this paper, we conduct a systematic literature review (SLR) to systematically study the current research to understand how blockchain has been applied to IoT. On one hand, we investigate what roles blockchain can play to address the existing issues of IoT such as access control, data storage and Thing-to-Thing communication. On the other hand, we explore the potential challenges that blockchain brings to the solutions due to blockchain's unique properties. Based on our study, we provide suggestions on how to address those challenges in applying blockchain to IoT. In addition, we analyze the methodology followed by the researchers to integrate both technologies, and we give suggestions on further improvement. Specifically, the contributions of this paper are mainly five-folds:

- A summary of the existing IoT issues and the roles blockchain played to address the issues;
- A summary of the blockchain infrastructure chosen and implemented for IoT in the literature;
- Investigation of IoT management that covers both data and Things aspects;
- Analysis of the evaluation methods and metrics used to evaluate the solutions in the papers, which reflect the technical maturity of the solution;
- Suggestions on the design decisions to address common design defects in the integration of blockchain with IoT.

The remainder of the paper is organized as follows. Section II discusses other reviews and surveys on similar topics, and also points out the differences between our study and the existing works. Section III introduces our methodology on the paper selection and data collection processes. Section IV presents the study results after the data collection process. The data is analyzed in Section V, where interesting and promising research points are discussed. Section VI concludes the paper.

II. RELATED WORK

We found 11 studies that reviewed the state-of-art of integrating blockchain with IoT. Table 1 lists out the surveys, SLRs or mapping studies on similar topics. Two of the papers focused on a single aspect of blockchain, namely, smart contract and consensus protocol, while four papers discussed blockchain as a holistic solution. There are two papers focused on the security properties of the solutions and three papers mainly discussed the use cases. These related works are classified into five groups based on their focus, including smart contract, consensus algorithm, holistic, use cases, and security.

Christidis and Devetsikiotis [43] focused on smart contract and claimed that the integration of smart contract and IoT technique can bring new business models to the existing systems and improved current working processes. Yeow *et al.* [44] analyzed the different consensus protocols being applied in IoT.

Diverse IoT scenarios that can be facilitated by blockchain are summarized and analyzed in the studies of Panarello *et al.* [45], Fernández-Caramés and Fraga-Lamas [46], and Conoscenti *et al.* [50]. Panarello *et al.* [45] discussed usage pattern and development process of existing solutions on IoT interacting blockchain, while Fernández-Caramés and Fraga-Lamas [46] gave suggestions on optimizing some aspects (system architecture, cryptographic algorithm and message timestamping) of the existing solutions.

TABLE 1. Scope of related works.

	Smart contract	Consensus	Use cases	Security	Holistic
Survey	[43]	[44]	[45], [46]	[7]	[47], [48], [49]
SLR			[50]		
Mapping Study				[51]	[52]

Khan and Salah [51], and Banerjee *et al.* [7] analyzed the blockchain state-of-art from the security perspective. Specifically, Banerjee *et al.* [7] focused on intrusion detection and prevention, and the collaborative security approaches using blockchain.

Reyna *et al.* [47], Atlam *et al.* [48], and Ali *et al.* [49] treated blockchain as a holistic solution. Reyna *et al.* [47] provided network typology alternatives to support such integration. Ali *et al.* [49] compiled a list of existing literature about blockchain. In addition, Sergio *et al.* [52] conducted a mapping study that helps researchers to understand the features, processes, existing solutions and challenges of blockchain-based IoT development.

The existing review and survey papers cover a list of relevant academic papers in this space. However, most of them do not provide new insight on the state-of-art. Our study is different because we put a heavier weight on quality than quantity of the included paper. There is a lack of established standards or checklist to assess the quality of the blockchain and IoT article to date. Hence, for quality assessment, we considered the venue of the paper, the proposed solution, and the methodology the researchers followed. For example, we only shortlisted peer-reviewed published paper from good conferences and journals that had been examined and reviewed by experts. Besides, we excluded papers that only give vision without concrete system design, and papers without proper evaluation of their proposed solution. In addition, we analyzed both the proposed solution and the methodology of the included papers in our discussion. During the analysis phase, we leveraged the blockchain knowledge of the researchers participated in this study and identified the limitations of the proposed solution and its evaluation. We further gave our own suggestions on how to address these limitations or improve the design of the system.

III. METHOD

In this section, we state the method used to conduct this study, which includes the research questions, eligibility criteria,

TABLE 2. Inclusion and exclusion criteria.

No	Criteria	Justification
1	The study must be original research paper instead of a review/survey paper.	We investigate the adoption level of blockchain in IoT. Review and survey papers or papers without being peer-reviewed do not always contain sufficient description of their solution.
2	The solution developed must be aimed to solve problems on IoT platform.	The objective of this review is to inform the audience on how to implement blockchain in IoT. Hence, the accepted paper must be attempting to use blockchain to solve IoT issues. Articles that aims to solve issues on the blockchain while using IoT as a domain or a motivating example will not provide relevant insight in our context.
3	The proposed solution must be evaluated.	This review is to inform the audience on applicable and feasible solution instead of just showing the trend or vision without considering the technical feasibility of the solution.
4	The study must be English written articles.	English is the common language for all four researchers that conducted this SLR.
5	The study must be a full-length paper.	Short paper in general could not cover all sufficient detail of the proposed solution, and is normally without strong evaluation.

information sources and search, and study selection and data collection.

A. RESEARCH QUESTION

The research questions address by this study are as follows:

RQ1. What existing IoT issues the author tried to solve with blockchain?
RQ2. What is the role of blockchain in solving those issues?
RQ3. How IoT data is being managed in the blockchain-based system?
RQ4. How Things are being managed in the blockchain-based system?
RQ5. What is the evaluation result of the proposed solution?

RQ1 aims to gather all the current IoT issues that could be potentially tackled by leveraging blockchain technology. In this study, we specifically look at studies with developed proof-of-concept (PoC) instead of just idea or vision papers. There are many vision papers or white-papers being published on using blockchain for IoT but our main goal is to give readers real applicable insight on how they could implement blockchain in the IoT domain. RQ2 informs what role the blockchain technology is being used in the IoT platform.

There are two main concerns in IoT, which are the Things and the data. RQ3 is to investigate how large stream of IoT data is being managed as the blockchain solution is not as scalable and efficient as a centralized system for a large amount of data. Similarly, the Things connected to the IoT network are not scalable and in general, have less computing power. Managing a large number of Things have always been another main concern with IoT platforms, so RQ4 is to see how these studies manage connected Things on blockchain-based IoT platform.

We have filtered out all blockchain for IoT studies without evaluation of the proposed solution in their studies. RQ5 is aimed to extract the limitations found during integrating blockchain for IoT. This would provide readers with insights and principles to build proper blockchain-based IoT solutions.

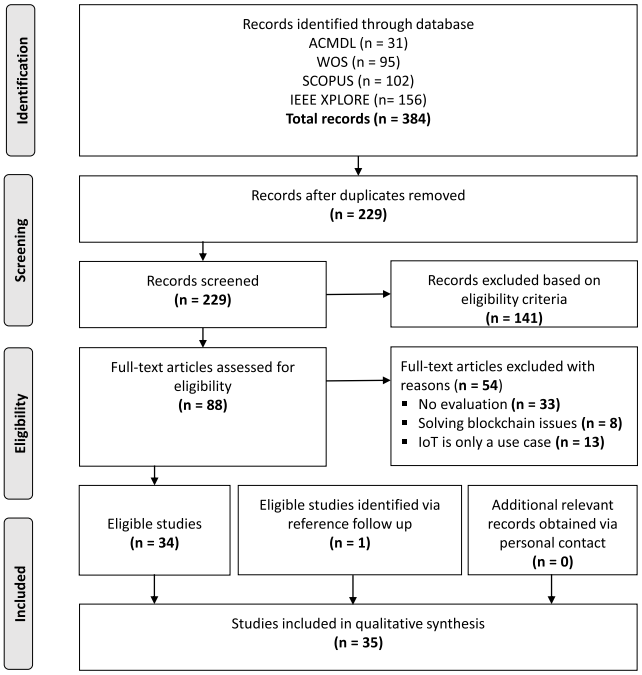

FIGURE 1. PRISMA flow diagram.

B. PROTOCOL AND PHASES OF THE STUDY

This review was conducted according to the Preferred Reporting Items for SLRs and Meta-Analyses (PRISMA) statement [53] and incorporated with the standard guidelines proposed by Kitchenham [54], to tailor this SLR for computer science domain. The process is illustrated in Fig. 1.

C. INCLUSION AND EXCLUSION CRITERIA

Published peer-reviewed articles that fulfill the predefined criteria were included. There are five key criteria a study needs to achieve to be eligible for this review. The criteria and the corresponding justification is shown in Table 2.

D. INFORMATION SOURCES AND SEARCH PROCESS

The search process was manually conducted by searching through four databases. The selected databases are:

- Web of Science
- Scopus

- IEEE Xplore Digital Library
- ACM Digital Library

Two main concepts were used to search for relevant articles: IoT AND Blockchain. The complete search terms can be found in Appendix A. In addition to database searching, the reference lists of retrieved studies were hand searched in order to identify any additional relevant studies to be included in this review.

E. STUDY SELECTION AND DATA COLLECTION PROCESSES

The data collection were conducted by four researchers, two senior researchers, and two junior researchers. The two senior researchers are leading experts in blockchain and IoT, while the two junior researchers are currently working towards research degrees in the area of blockchain.

After extracting relevant articles from the databases, each study title and abstract was screened independently for eligibility by four researchers. Researchers were encouraged to be inclusive in cases of doubt concerning the eligibility of a paper. Disagreements regarding eligibility were resolved through discussion between all researchers to reach consensus. Similarly, the full text of all potentially relevant studies identified based on the titles and abstracts were subsequently retrieved and further examined for eligibility independently by all.

For data extraction, a framework was formed by the research team based on system development principles as well as discussions with SLR experts. The framework consists of two parts, which are the characteristics of the included studies and technical characteristics of the blockchain and IoT platform. The framework was used to develop the data extraction form using Microsoft Excel. The form was pilot tested with eight randomly selected included papers and revised iteratively. The data extraction form was used by four researchers to extract the data from the included articles independently.

The data extracted from each study were:

- Study details including first author, country, year and type of paper
- Description of the PoC (name, purpose, attempted IoT issues, methods and the blockchain infrastructure).
- IoT data (size, query, process, retrieve, store).
- Things (types, number, operation).
- Evaluation of the PoC and learning experience.

Four researchers formed a group of two. In each group, one researcher extracted the data and another checked the extraction. After both groups complete data extraction. Several follow-up discussions are conducted to cross-check the extracted data and achieve consensus among the researchers. Another independent researcher, Su Yen Chia reviewed and checked the integrity of data extracted with the original articles. An initial analysis was generated by Su Yen Chia and further discussed and refined together with all seven researchers.

TABLE 3. IoT Domains and Issues.

Domain	No.	Issue	No.
Generic IoT platform	22	Centralized key management	27
Manufacturing	3	Lack of standard guidelines	4
Internet of vehicles (IoV)	2	Integrity of data and Things' state	6
Energy grid	2	Limited thing computation capability	9
Electricity trading	2		
EHealth	1	Interoperability	4
Smart home	1		

IV. RESULTS

In this section, we present the results of data collection, on the distribution of the answers for each of the research questions. Please note that we only report what is found in the reviewed paper. We do not tailor the collected data.

A. DOMAIN AND ATTEMPTED ISSUES

1) DOMAIN

Out of 35 studies, three [17], [21], [40] were building blockchain-based IoT platform for *manufacturing* domain, follows by domain of *IoV* [26], [32], *electric trading* [20], [29] and *energy grid* [37], [41] having two studies each. There is one study [42] that focused on applying blockchain-based IoT solution on *eHealth* while one [8] is on *smart home*. The rest of the 22 studies were focusing on generic blockchain-based IoT solutions.

2) ISSUE

There are 27 out of the 35 studies [9]–[23], [25], [26], [28], [29], [32], [34], [36]–[41] that used blockchain to solve the central key management issue on IoT platform. There are four [8], [12], [17], [40] to solve the lack of standards with the use of blockchain. Six studies [10], [12], [20], [25], [27], [35] leveraged blockchain to solve the integrity issues such as integrity of the collected data from sensors and integrity of Things' state. There are nine studies [9], [12], [30]–[33], [36], [40], [42] that attempted to solve the limited computational capability of Things on IoT platform. For example, Things connected to the IoT network do not have the capability to carry out encoding of the collected data. Four studies [24], [35], [37], [40] used blockchain to achieve interoperability between IoT platforms. A summary of the results is illustrated in Table 3.

B. BLOCKCHAIN INFRASTRUCTURE

1) BLOCKCHAIN PLATFORM

There are 16 out of 35 studies used Ethereum [8], [10]–[12], [14], [19], [20], [23], [24], [27], [32], [34], [36]–[38], [42] while four used Bitcoin network [22], [28], [30], [34]. Out from the remaining 35, four used Multichain [21], [30], [33], [39], followed by three studies that used Hyperledger [15], [31], [40] and one used Monax [33].

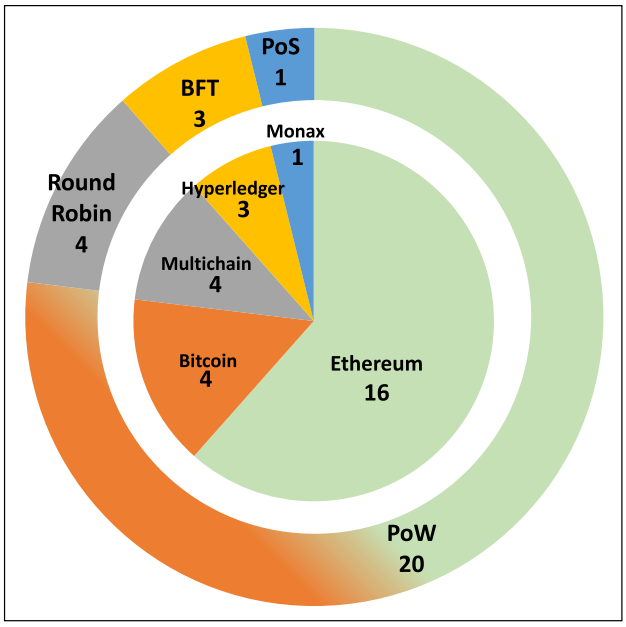

FIGURE 2. Blockchain platform and consensus.

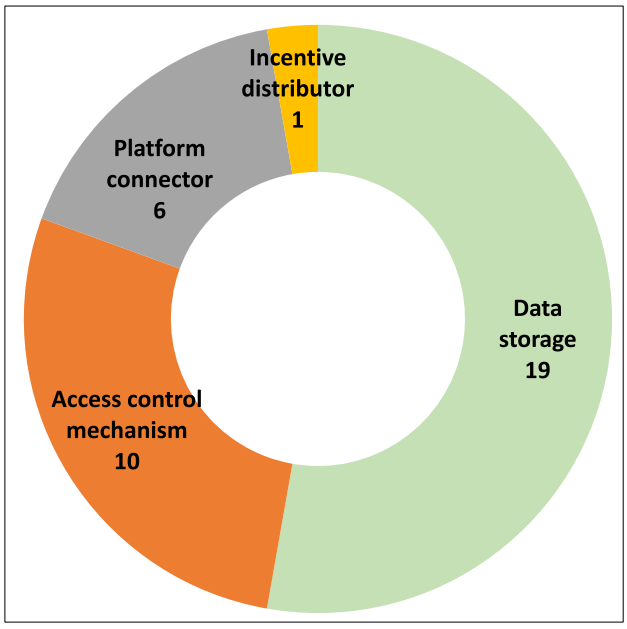

FIGURE 3. Roles of blockchain.

TABLE 4. IoT thing type, identity model, connection method and operation.

Type	No.	Connection method	No.
PC	15	Blockchain client	12
Single board computer	11	Connector	7
Sensor	7	Manual approach	2
Home applicances	3	**Operation**	**No.**
Camera	2	Identity registration	7
Smartphone	2	Identity revocation	1
Vehicle	1	Identity update	2
Identity model	**No.**	Authentication	14
PKI mechanism	22	Policy modification	2
Ontology classification	1	Behavior detection	1
Hierarchical management	1	Software upgrade	1

2) CONSENSUS

Twenty studies [8], [10]–[12], [14], [19]–[21], [23], [24], [27], [30], [32]–[34], [36]–[39], [42] implemented blockchain solutions that use Proof-of-Work (PoW) consensus for their IoT platform while three studies [15], [31], [40] selected to use blockchain with Byzantine-Fault Tolerance (BFT) consensus. There are one study [33] that used Proof-of-Stake (PoS) consensus and 4 studies [21], [30], [33], [39] used round robin consensus.

3) BLOCKCHAIN ROLE

Out of 35 studies, 19 used blockchain as a data storage [8]–[16], [20], [29], [30], [32], [35], [36], [39]–[42], follows by [8], [18], [19], [22]–[25], [28], [34], [38] (n = 10) that used blockchain as access control mechanism. There are six studies that used blockchain as platform connector [17], [21], [23], [27], [33], [37] to interconnect between the sensors and the high computing nodes. Only one study [26] used blockchain to distribute incentive to keep user motivated to use the proposed blockchain-based IoT solution. A summary of the results is illustrated in Fig 2 and Fig 3.

C. DATA MANAGEMENT

1) RECORDING METHOD

Out of 35 studies, 29 recorded data collected from Things into the blockchain via transactions. Within the 29, there are 27 that used blockchain nodes connected to those Things to create the transaction while two studies submitted transactions via Things directly. Seven studies [11], [20], [22], [23], [32], [33], [35] created transactions via smart contract on Ethereum network.

2) DATA SIZE

The range of data size varies among all the studies [8], [11], [23], [30], [33], [35], [36]. The largest data size per transaction reported was 0.022MB while the smallest data size per transaction was 0.00007MB. 28 out of the 35 studies did not mention the size of the data.

3) DATA OPERATION

There are five studies talk about data generation [13], [17], [18], [24], [27], 11 studies talk about data transfer [12], [13], [15], [20], [21], [24]–[27], [32], [33], and six studies talk about data verification [10], [12], [14], [18], [21], [27]. A summary of the results is illustrated in Table 5.

D. THING MANAGEMENT

1) THING TYPE

PC (n = 15) and single board computer (n = 11) are the most used Thing types, followed by sensor (n = 7), home

TABLE 5. Data size, recording methods and operations.

Size (bytes)	No.	Operation	No.
1024	2	Generation	5
22000	1	Transfer	11
629	1	Verification	6
148	1	**Recording method**	**No.**
125	1	Transactions	29
74	1	Smart contract	7

appliance (n = 3), camera (n = 2), smartphone (n = 2), and vehicle(n = 1). There are nine out of 35 paper did not mention what kind of Things are used in their studies.

2) CONNECTION METHOD

Out of 35 studies, 12 studies [10], [12], [14], [19], [23], [25], [27], [28], [30]–[33] connected Things to the blockchain network by the client and protocol provided by a specific blockchain, while [9], [11], [13], [18], [24], [34], [38] through connector (n = 7), [8] and [20] applied manual approach, and 14 studies did not have a clear description.

3) IDENTITY MODEL

Eleven out of 35 paper did not present identity model for the Things. In the remaining 24 studies, PKI mechanism is applied in [9], [11], [13], [14], [16], [18]–[28], [31], [32], [34], [38], [39], [41] (n = 22), while ontology classification is proposed in [8], and a hierarchical smart thing management is used in [15].

4) THING OPERATION

In terms of the supported operations for IoT thing management, [8], [13], [27], [28], [31], [34], [38] discussed identity registration, while [8] also covers identity revocation, [8] and [13] covers identity update. Authentication is supported in [9], [11], [14]–[16], [18], [19], [22], [23], [25]–[28], [34], and policy modification is supported in [16] and [38]. [8] supports behavior detection and [27] focused on software upgrade. A summary of the results is illustrated in Table 4.

E. EVALUATION

1) EVALUATION METHOD

Majority (n = 29) of the studies conducted experiment and developed PoC (Proof-of-Concept) as a form of evaluation. Three studies [26], [29], [42] conducted simulation and three [17], [21], [31] conducted case study to evaluate their proposed solution. There are six studies [16], [18], [19], [28], [29], [38] that conducted scenario-based analysis and two [27], [30] that carried out model checking.

2) EVALUATION METRIC

28 of the reviewed studies conducted performance analysis while five [10], [12], [24], [26], [36] of them performed feasibility analysis. Six out of 35 [14], [17], [19], [21], [26], [41] evaluated their blockchain-based IoT solution with security analysis while six studies [8], [14], [19], [20], [24], [25] conducted cost analysis. A summary of the results is illustrated in Table 6.

TABLE 6. Evaluation method and metric.

Method	No.	Metric	No.
Proof of Concept	29	Performance	28
Simulation	3	Feasibility	5
Case study	3	Security	6
Scenario-based analysis	6	Cost	6
Model checking	2		

V. DISCUSSION

In this section, we analyze the extracted data in the previous section from their technical solution till the corresponding evaluation, and give our own insights on the solution design, research methodology and research opportunities that are currently missing in the state-of-art. This section contains five subsections that answer all our research questions. Subsection V-A is the answer for RQ1. Subsection V-B covers consensus and platforms, which is the answer for RQ2. Subsection V-C and subsection V-D is the answers for RQ3 and RQ4 respectively. Finally, Subsection V-E is the answer for RQ5.

A. ATTEMPT ON IOT ISSUES

Majority of the studies leveraged the immutability and integrity properties provided by blockchain to deal with the existing security issues in IoT, and utilized the decentralized computational infrastructure of blockchain to manage data and Things. The current issues being targeted in the studied papers are as follows (Please refer to section IV-A):

- Heavy resource consumption for security through encoding the collected sensor data;
- Single point of failures due to the centralized management servers managing all the Things and keys;
- Difficulties in streamlining control the integrity of large volume of connected Things and data generated by Things;
- Lack of established standard on managing Things on IoT;
- Providing Interoperability between IoT platforms is challenging.

By storing the collected sensor data on the blockchain via transactions, authors stated that fewer resources are required to achieve security as blockchain infrastructure can provide the required security attributes for the whole system.

As sensors or edge devices are generally Things with low computing power, there is a need to have additional nodes with higher computational capability to carry out heavy computation. Most of the IoT solutions use another device (or server) to provide extra computational capability. Such a

centralized design creates a single point of failure. Thus, some of the reviewed studies leverage the computational infrastructure provided by blockchain to extend the computational capability of IoT system, and get rid of the central management to avoid single point of failure, because the computation is based on a peer-to-peer network with decentralized design in nature.

Some of the reviewed studies use blockchain to enable distributed access control on a large number of devices across the network in a decentralized way. The access control is implemented in smart contracts, which are running on a physically distributed but logically centralized platform. Thus, it is more efficient for the devices interacting with the smart contracts autonomously rather than being configured one by one.

Other studies also use blockchain platform to enable real-time monitoring of all the connected devices while ensuring all are on the same state as blockchain ensures integrity among all connected devices. One study gives a solution to support concurrent software update for all the devices connected on the same blockchain network.

B. BLOCKCHAIN INFRASTRUCTURE

Blockchain has been used as a replacement for traditional data storage. Using public blockchain as the sole data storage is not practical due to the high cost of sending transactions (those that are using Bitcoin and public Ethereum) that includes the data and limited storage of the transaction (restricted by *gas* limit for example). However, none of the reviewed studies discuss the issues of cost and data size. Also, blockchain is used in a paper as incentive distributor to distribute token to motivate users to forward announcements on the condition of traffic anonymously and reliably (Please refer to Section IV-B).

Ethereum[1] is the most experimented platform in the studies reviewed as it is one of the most accessible blockchain platforms with a lot of documentation available. It is the first blockchain platform that provides a Turing complete programming language for smart contract. Bitcoin[2] is after Ethereum, although Bitcoin is the first blockchain with the largest market capitalization. Bitcoin is used much less due to limited smart contract support. Ethereum has a public testnet, which is aimed to provide a test environment for decentralized applications before they are being deployed on public Ethereum. The Ethereum testnet uses Proof-of-Stake consensus protocol instead of the Proof-of-Work on public Ethereum, so the latency on the testnet is much lower than the latency on the public Ethereum.

Multichain[3] and Hyperledger Fabric[4] are two permissioned blockchains, which require one or more authorities to act as a gate for permission granting. This may include permission to join the network (and thus read information from the blockchain), permission to initiate transactions, or permission to mine. Multichain also allows more fine-grained permissions, such as permission to create assets. Moreover, Multichain supports off-chain storage by default. With this feature, Multichain achieves better scalability but sacrifices security because the integrity of the off-chain data cannot be guaranteed.

Hyperledger[5] is an open-source blockchain platform from Linux foundation initiatives. Hyperledger currently has five different frameworks that are designed for different purposes. For example, Hyperledger Indy is designed to cater for blockchain-based identity management. Hyperledger Fabric is a business blockchain framework, intended as a foundation for developing blockchain-based applications with a modular architecture, so that data can be stored in multiple formats, and various consensus algorithms can be configured.

C. IoT DATA

The largest size of data being mentioned in those studies is 0.022MB and smallest is 0.00007MB. At 2019 January, to store 0.022MB data on public blockchain, it costs 7.50USD on Bitcoin and costs 0.24USD on Ethereum, hence storing a large amount of IoT data on public chain is not economically feasible, as IoT solution in general produces a large stream of real-time data from various devices or sensors. Unless the majority of the data is being stored off-chain, else a consortium or private blockchain suits IoT use case better (Please refer to Section IV-C).

Due to the limited computational power of blockchain, all of the reviewed studies used blockchain only for storing and transferring data without further processing.

D. THINGS

Things in IoT are responsible to generate, process, and sometimes analyze a large amount of IoT data. Consequently, the management of these Things is significant. Things can be categorized into two layers [56], namely, the physical layer and edge layer. The physical layer refers to the sensor devices, and their descriptions, which is missing in most of the reviewed papers. Authors of some of the reviewed works stated that they stored the device information on-chain. The edge layer refers to the intermediate which is a standalone server or a computing Thing to connect and manage a group of sensors or devices. Majority of the reviewed papers use Things in the physical layer (single board computer, home appliance, sensor, camera, and vehicle) as light nodes, while using PC and smartphone in edge layer as full nodes (Please refer to Section IV-D).

1) CONNECTION METHOD

When using blockchain in IoT, Things need to be linked to blockchain directly or indirectly. There are three different ways to connect with blockchain, including using blockchain

[1] https://www.ethereum.org/
[2] https://bitcoin.org/en/
[3] https://www.multichain.com/
[4] https://www.hyperledger.org/projects/fabric
[5] https://www.hyperledger.org/

Insight for Section V-A: Attempt on IoT issues

Data Privacy: The cryptographic techniques and consensus process used by blockchain guarantee data integrity and immutability on blockchain. But blockchain sacrifices confidentiality in order to achieve data integrity. If the sensor data is confidential, the collected data should be either encrypted before submitting to blockchain or kept off-chain with only a representation (like the hash of the data) kept on the blockchain.

Dynamic Behaviour: Smart contract, as a type of data, is also immutable after being deployed on blockchain. Using smart contracts to implement access control needs to consider the dynamism of the IoT network, where new Things can join, and existing Things can leave at any time. In the case where dynamic behavior of the Things is out of the pre-defined policies, the smart contract should be extensible to support the adaptation of access control.

Security of Computation: Although blockchain can extend the IoT network with a neutral computational platform to support additional functions that cannot be implemented on the resource-constrained Things, the computational capability of blockchain is still limited. Depending on the type of blockchain, there might be technical constraints on computation execution, like *gas* limit on Ethereum, which restricts the complexity of the programs running on blockchain. Blockchain has inherent limitations when being used as a computational infrastructure, but it can be used to ensure the security of off-chain computation. Any computation, like data processing or device upgrading, is implemented by a piece of code. Code is a type of data, which can execute in the corresponding execution environment. The integrity of the code can be ensured by adding a representation of the code on the blockchain.

Monitoring: Due to the latency caused by the consensus process on public blockchain, a system with blockchain cannot support real-time monitoring. There is always a delay of at least one block interval before the state is updated on the blockchain and available publicly. In the case that real-time monitoring is required, a permissioned blockchain using Practical Byzantine Fault Tolerance (PBFT) consensus is more appropriate due to the much less latency caused by the consensus process.

client, manual approach, and via a connector. Most Things automatically connect to blockchain via client or interface provided by the blockchain platform. Due to the limited computational capacity, the client installed on Things is the lightweight client which doesn't maintain a full copy of historical data, but relies on other full nodes for many operations. There are some works that require the owner of Things to manually send the identity of Things and generated data to blockchain. The owner of the thing is a participant of the blockchain network with a blockchain address. The remaining works use a connector, which can be a special Thing with strong computing capability, such as PC. The connector maintains a full node of blockchain and takes the responsibility to connect other Things to blockchain. Such a centralized connector introduces a single point of failure.

2) IDENTITY MODEL

Identity model is critical for Thing-to-Thing and human-to-thing communication and interaction. Identity is a symbol or mark that can be used as a unique identification of a Thing, for example, the address in blockchain. Only a few papers propose particular identity models to manage Things, as most of the reviewed paper use PKI (Public Key Infrastructure) to facilitate identity management. The inherent key infrastructure provided by blockchain is applied, an alternative is using a particular thing to generate key pairs. The public key of a Thing can be accessed by everyone, while private key is used by the Thing to sign a transaction and should be kept securely. An Ontology-based Things' identity management defines two classes, namely, ''physical space'' for the physical entities participated in the network, and ''information space'' for the computational resources. Hierarchical identity management is a combination of a hierarchical Thing architecture and the PKI mechanism, where the Things at lower layer are controlled by the ones at the higher layer, and the corresponding identities can be chased from top to bottom. Although specific identity model exists, we found that a mature solution for identity management is still missing.

3) OPERATION

Majority of the reviewed researches support operations related to access control. There are user-oriented operations supported in the reviewed studies, for example, users locking and unlocking a Bluetooth device [11]. In [9], authentication is applied to prove that a Thing is believable, which focuses on the identity validity of a Thing. Access control operations include the following:

- Identity management – In most cases, the inherent PKI mechanism in blockchain infrastructure is used to manage the identity of Things. The current identity management life cycle includes basic operations on blockchain addresses, like registration, revocation, and update.
- Authentication – There is no privilege user in blockchain for manipulating and managing blockchain. Every participant can access blockchain, submit transactions, deploy and invoke smart contract. Such a model may cause chaos in an IoT system, consequently, extra authentication implemented in smart contract is required to guarantee the role of each Thing and prevent possible attacks.

Insight for Section V-B: Blockchain infrastructure

Permissioned blockchain: Permissioned blockchains, like Multichain and Hyperledger Fabric, are more suitable for IoT use case. On permissioned blockchains, normally no transaction cost is required for recording data and executing programs because the permissioned blockchains are maintained by a group of authorities rather than public. A financial incentive is unnecessary for the authorities to operate and maintain the blockchain. However, permissionless blockchains, like Ethereum and Bitcoin, are not suitable for storing or streaming a large amount of data or executing complex computation due to the inherent transaction cost of storing data on chain and constraints of computation complexity. It should store only representation of data or metadata, rather than the raw data itself.

Permissionless blockchain: If public permissionless blockchains are desired, other strategies are needed to limit the size of on-chain data and computation. One possible strategy is to use anchoring mechanisms. For example, Weber *et al.* [55] proposed a scalable platform architecture for multi-tenant blockchain systems. In their design, each tenant is given an individual blockchain, and all tenant chains are anchored to a public blockchain periodically. The anchoring uses a combined root of all tenant chains, thus achieving data integrity, low cost, and performance and data isolation. This architecture can also be applied to many situations requiring multiple blockchains, e.g. a long-lived and a short-lived blockchain for long and short-running business needs, or a separate blockchain per year.

Consensus protocol: Proof-of-Work is not suitable for IoT due to the requirement of computational power of the node. Gateways with more computational capacity might be able to join blockchain using Proof-of-Work. Proof-of-Stake and PBFT are more suitable consensuses considering the characteristics of IoT. Furthermore, immutability provided by Proof-of-Work on public blockchain is probabilistic. There is a probability, although very low, that the historical transaction is changed. For example, the public Ethereum experienced a 51% attack on 8 January 2019[6].

IOT specific blockchain platform: IOTA[7] is a blockchain initiative specifically built for IoT, which uses a DAG (Directed Acyclic Graph) instead of a blockchain to store its ledger. There is no block, the vertices of the DAG represent transactions, and edges represent validation of transactions. IOTA provides better scalability because there is no built-in maximum throughput. However, security is worse since it is susceptible to 33% (rather than 51%) attack.

- Policy modification – In some of the proposed solutions, the network participants are able to modify the access control policies, which increases the adaptability of the Thing management.

Maintenance is also significant in the management of Things. Things can work for many years if being maintained properly. In addition, maintenance also reflects the privacy and security of a system to some extent. In the reviewed paper, we identified two types of maintenance:

- Behavior detection – Things may work abnormally when being attacked or affected by environment. When an abnormal behavior is found, preset actions of the Thing can be triggered to mitigate the impact. Such operation is for the physical safety of the Things.
- Software upgrade – The software upgrade package may suffer ''man-in-the-middle attack'' in an IoT system. Blockchain can be used as a secure and convenient channel to support the upgrade of the Things.

E. EVALUATION

This SLR focuses only on published studies with evaluation section, we are able to extract the following information from all the accepted studies: *evaluation method*, *evaluation metric*, and *evaluation result* (Please refer to section IV-E).

Development of a PoC system is the most common method conducted to evaluate the proposed blockchain-based IoT solution in all the studies. However, the conducted experiments could not reflect the system behavior in the production environment due to the following reasons:

- Available test environment might use different consensus from production environment;
- Only a small number of IoT things are being used;
- Not all the corner cases can be easily covered in the simulation method.

In the studies, majority of the PoCs are deployed on a test environment or local environment due to the monetary cost for using the public blockchain. In a test environment, such as Ethereum testnet, is using a different consensus mechanism than the public Ethereum. The public Ethereum is using PoW but two of the most frequently used Ethereum testnets, Kovan and Rinkeby, are using PoA (Proof-of-Authority). There is another testnet uses PoW, Ropsten, which is not being used by any of the studies. Hence, the result shown in the evaluation is inaccurate as the latency on the testnet is very different from the public Ethereum.

Most of the developed PoCs use less than five IoT devices, so the request from devices could not reflect the real world

[6]https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped

[7]https://www.iota.org/

Insight for Section V-C: IoT data

The conventional IoT solution and the blockchain-based solution is compared at different stages along the life-cycle of sensor data.

Data collection: Conventional IoT solution and blockchain-based solution can use the same data collection mechanism. Things with enough computational power can directly send the generated data to the data storage or blockchain. The data generated by Things with limited computational capacity is first aggregated by a gateway, which is a delegate that sends the aggregated data to a conventional data storage or wraps the aggregated data into transactions, which are then submitted to blockchain.

Storage and Sharing: Conventional IoT solution stores data in a centralized place, either a local data storage or cloud. In a blockchain-based solution, data is partially stored in blockchain based on the characteristics of the data and the blockchain. The critical data requires a high level of integrity should be stored on blockchain, as unstructured data in transactions or structured data in a smart contract. The data requires a medium level of integrity can be stored in a content-addressable peer-to-peer data storage, like IPFS (InterPlanetary File System)[8], which also guarantees the data integrity without strong immutability or full replication across the whole network. The remaining uncritical data can be kept in conventional data storage.

Access control: Conventional IoT solution relies on a centralized permission control layer to control the access to the data stored in the data storage. The blockchain-based solution uses smart contract to provide a distributed access control for data processing. The data on-chain is by default visible to all the participants of the blockchain network. As discussed earlier (Section V-A), the dynamic behavior of the IoT network should be considered by the access control layer.

Data processing: Conventional IoT solution processes the collected data in centralized services, which are trusted by the users who use the services. As discussed in Section V-A, blockchain can be used to ensure the integrity of data processing.

Insight Section V-D: Things

Connection: Smart contract enables Thing-to-Thing communication if the Things have their own blockchain accounts. Manually binding Things with blockchain restricts the interaction between the Things and blockchain because the computational platform provided by blockchain is not fully utilized.

Trading: Blockchain provides a trading infrastructure for IoT, which enables many business scenarios. If the Things have their own blockchain accounts, they can transact autonomously with each other for data trading or service provision.

Identity management: A public key infrastructure (PKI) [57] denotes that a centralized role holding pre-defined rules to create, distribute, and revoke digital identities which is in the form of key pairs. Blockchain provides pseudo-anonymous identity to the current IoT system. Furthermore, the idea of Self-Sovereign Identity (SSI) [58] can provide flexibility to identity management, which aims to give one to have complete control over its identity. Decentralized Identifier (DID)[9] is a new concept in the implementation of SSI, identifying the entities in the network, existing solutions include uPort[10] and Hyperledger Indy[11].

situation realistically as IoT would have hundreds to thousands of devices collecting streams of real-time data.

For studies that used simulation to evaluate the performance of the blockchain-based system, the mining process and block confirmation waiting time are generally being omitted. However, those factors are very important for the performance of the blockchain-based system. The behavior of the connected peer also affects the blockchain-based system, but it is hard to simulate all ranges of those behaviors. For example, sporadic attacks from malicious nodes towards the blockchain network can impact the performance of the blockchain. Peers that submit their smart contract by paying a large amount of gas can push their transactions to be included faster than transactions with standard gas cost. There is no standard approach that could be used to cover all potential corner cases of peers' activities.

Performance is the metric being evaluated the most. Majority of the result is a positive result because the experiments are looking at the contract and transaction creation speed rather than the complete time for the transaction to be included into the blockchain and committed. Although a number of studies mentioned that the block confirmation time can affect the performance but they did not specifically discuss how long block confirmation time affects the usability of their solution. *X-confirmation* is one of the essential security strategy

[8]https://ipfs.io/
[9]https://w3c-ccg.github.io/did-spec/
[10]https://www.uport.me/
[11]https://www.hyperledger.org/projects/hyperledger-indy

Insight for Section V-E: Evaluation

Cross-checking: Simulation might not be able to cover all the edge cases. By developing a working PoC and cross check the result with the simulation, the differences between both methods can be used to fine tune the simulation to reflect real world more realistically. Ropten testnet should be used for PoC when Ethereum is desired. It is the closest test environment with the public Ethereum.

Performance: Performance analysis should be conducted from end-to-end, starting from submission time till the time when the corresponding block is included in the blockchain and a sufficient number of blocks are built on top of it.

Security: For understanding the behavior of the system from the security perspective, attack analysis or mutation analysis can be conducted. The behavior of the blockchain-based IoT system can be monitored and checked to identify any potential deviation from the expected output.

Feasibility: There are three types of feasibility analysis, which are technical feasibility, operational feasibility, and economic feasibility [59]. Integrating existing systems with blockchain introduces additional technical complexity and more cost towards the development and maintenance process. In term of understanding the feasibility of developing a blockchain-based IoT system, all three feasibility analysis should be conducted. In term of the economic feasibility, an organization needs to consider the cost of storing data on public blockchain and the cost of smart contract deployment and execution. Operational feasibility needs to be considered too, as the operation mode of blockchain differs from traditional cloud system and blockchain has different trade-offs. For example, commercial confidentiality on public blockchain is natively impossible. Due to the immutable nature of blockchain, to update or change smart contract on blockchain requires extra consideration [60].

Cost: Cost analysis is another important factor that needs to be evaluated. There are different components that need to be considered when cost is calculated. The first is the monetary cost to store data and execute a smart contract on blockchain. The second is the cost to maintain the blockchain node(s) used by the blockchain-based application. Although maintaining blockchain nodes are not required, owning blockchain nodes can largely improve the read latency because the read is from local nodes. Besides, if considering the cost of maintaining the blockchain infrastructure as a whole, the cost is high when Proof-of-Work is used.

used by blockchain-based applications to ensure immutability of transaction [60]. So, the performance of the whole PoC should be analyzed from end to end, from transaction being submitted until the transaction being included and committed.

Six studies with PoC conducted scenario-based cost analysis. The cost analysis measured the average transaction cost rather than the total cost of storing a large volume of data. Unless the IoT solution is cater for a few devices that transfer a small amount of data, or else storing stream of data is very costly. Hence, it is not economically feasible to store all the collected data on blockchain. One possible solution is to store the raw data off-chain while storing on-chain an address that links to the off-chain data.

VI. CONCLUSION

The main challenges being target on IoT are centralized key management, lack of standards, integrity of Things' states, limited Thing computation capability and interoperability between Things. In this paper, we conducted an SLR to analyze how blockchain has been applied to IoT to address these challenges. The SLR covers 35 blockchain solutions found in the peer-reviewed academic papers. Performance and scalability are the main problems while integrating blockchain with IoT platform due to the high volume of data collected by IoT Things. Permissioned blockchain would be more suitable than public blockchain for IoT platform. According to our knowledge and experience on blockchain and IoT, we identified some design defects in the existing solutions and methodology which the works followed. Based on our observation, we provided insights about what factors to consider when integrating blockchain with IoT. The main issues are the majority of the solutions were being implemented and evaluated on the test environment. Blockchain test environment is using a different consensus protocol, hence it would not be able to realistically evaluate the performance of the solutions. We have recommended alternatives for both solution design and evaluation.

APPENDIX
A COMPLETE SEARCH TERMS
A. SEARCH STRING FOR WEB OF SCIENCE

TOPIC:(blockchain OR "distributed ledger technology" OR "distributed ledger technologies" OR "distributed-ledger technology" OR "distributed-ledger technologies" OR "smart contract" OR "smart contracts" OR "Smart-Contracts" OR "blockchain-based" OR DLT) AND TOPIC: ("edge device" OR "edge devices" OR "smart vehicle" OR "smart vehicles" OR "IOV" OR "Internet of Vehicle" OR "Internet of vehicles" OR "edge computing" OR "fog computing" OR "smart city" OR "smart cities" OR "smart space" OR "smart spaces" OR "smart home" OR "smart house" OR "smart houses" OR "IoT" OR "internet of thing" OR "internet of Things")

B. SEARCH STRING FOR SCOPUS

TITLE(blockchain OR "distributed ledger technology" OR "distributed ledger technologies" OR "distributed-ledger technology" OR "distributed-ledger technologies" OR "smart contract" OR "smart contracts" OR "Smart-Contracts" OR "blockchain-based" OR DLT) AND TITLE("edge device" OR "edge devices" OR "smart vehicle" OR "smart vehicles" OR "IOV" OR "Internet of Vehicle" OR "Internet of vehicles" OR "edge computing" OR "fog computing" OR "smart city" OR "smart cities" OR "smart space" OR "smart spaces" OR "smart home" OR "smart house" OR "smart houses" OR "IoT" OR "internet of thing" OR "internet of Things")

C. SEARCH STRING FOR IEEE XPLORER DIGITAL LIBRARY

("Document Title":blockchain OR "Document Title":"distributed ledger technology" OR "Document Title":"distributed ledger technologies" OR "Document Title":"distributed-ledger technology" OR "Document Title":"distributed-ledger technologies" OR "Document Title":"smart contract" OR "Document Title":"smart contracts" OR "Document Title":"Smart-Contracts" OR "Document Title":"blockchain-based" OR "Document Title":DLT) AND ("Document Title":"smart houses" OR "Document Title":IoT OR "Document Title":"internet of thing" OR "Document Title":"internet of things") AND ("Document Title":blockchain OR "Document Title":"distributed ledger technology" OR "Document Title":"distributed ledger technologies" OR "Document Title":"distributed-ledger technology" OR "Document Title":"distributed-ledger technologies" OR "Document Title":"smart contract" OR "Document Title":"smart contracts" OR "Document Title":"Smart-Contracts" OR "Document Title":"blockchain-based" OR "Document Title":DLT) AND ("Document Title":"edge device" OR "Document Title":"edge devices" OR "Document Title":"smart vehicle" OR "Document Title":"smart vehicles") AND ("Document Title":blockchain OR "Document Title":"distributed ledger technology" OR "Document Title":"distributed ledger technologies" OR "Document Title":"distributed-ledger technology" OR "Document Title":"distributed-ledger technologies" OR "Document Title":"smart contract" OR "Document Title":"smart contracts" OR "Document Title":"Smart-Contracts" OR "Document Title":"blockchain-based" OR "Document Title":DLT) AND ("Document Title":IOV OR "Document Title":"Internet of Vehicle" OR "Document Title":"Internet of vehicles" OR "Document Title":"edge computing") AND ("Document Title":blockchain OR "Document Title":"distributed ledger technology" OR "Document Title":"distributed ledger technologies" OR "Document Title":"distributed-ledger technology" OR "Document Title":"distributed-ledger technologies" OR "Document Title":"smart contract" OR "Document Title":"smart contracts" OR "Document Title":"Smart-Contracts" OR "Document Title":"blockchain-based" OR "Document Title":DLT) AND ("Document Title": "fog computing" OR "Document Title":"smart city" OR "Document Title":"smart cities") AND ("Document Title":blockchain OR "Document Title":"distributed ledger technology" OR "Document Title":"distributed ledger technologies" OR "Document Title":"distributed-ledger technology" OR "Document Title":"distributed-ledger technologies" OR "Document Title":"smart contract" OR "Document Title":"smart contracts" OR "Document Title":"Smart-Contracts" OR "Document Title":"blockchain-based" OR "Document Title":DLT) AND ("Document Title":"smart space" OR "Document Title":"smart spaces" OR "Document Title":"smart home" OR "Document Title":"smart house")

D. SEARCH STRING FOR ACMDL

recordAbstract:(blockchain OR "distributed ledger technology" OR "distributed ledger technologies" OR "distributed-ledger technology" OR "distributed-ledger technologies" OR "smart contract" OR "smart contracts" OR "Smart-Contracts" OR "blockchain-based" OR DLT) OR recordAbstract:("edge device" OR "edge devices" OR "smart vehicle" OR "smart vehicles" OR "IOV" OR "Internet of Vehicle" OR "Internet of vehicles" OR "edge computing" OR "fog computing" OR "smart city" OR "smart cities" OR "smart space" OR "smart spaces" OR "smart home" OR "smart house" OR "smart houses" OR "IoT" OR "internet of thing" OR "internet of Things") AND acmdlTitle:(blockchain OR "distributed ledger technology" OR "distributed ledger technologies" OR "distributed-ledger technology" OR "distributed-ledger technologies" OR "smart contract" OR "smart contracts" OR "Smart-Contracts" OR "blockchain-based" OR DLT) OR acmdlTitle:("edge device" OR "edge devices" OR "smart vehicle" OR "smart vehicles" OR "IOV" OR "Internet of Vehicle" OR "Internet of vehicles" OR "edge computing" OR "fog computing" OR "smart city" OR "smart cities" OR "smart space" OR "smart spaces" OR "smart home" OR "smart house" OR "smart houses" OR "IoT" OR "internet of thing" OR "internet of Things")

REFERENCES

[1] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[2] R. Van Kranenburg and A. Bassi, "Iot challenges," *Commun. Mobile Comput.*, vol. 1, no. 1, p. 9, 2012.

[3] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.

[4] T. Qiu, R. Qiao, and D. O. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[5] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, "SIGMM: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2019.

[6] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, Inc., 2015.

[7] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018. doi: 10.1016/j.dcan.2017.10.006.
[8] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic identity framework for the Internet of Things," in *Proc. Int. Conf. Cloud Autonomic Comput. (ICCAC)*, Sep. 2017, pp. 69–79.
[9] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Secur. Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 7817614.
[10] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.
[11] S. C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.
[12] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for IoT," in *Internet of Things—ICIOT*, D. Georgakopoulos and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 3–18.
[13] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
[14] H. Huang, K.-C. Li, and X. Chen, "Blockchain-based fair three-party contract signing protocol for fog computing," *Concurrency Comput. Pract. Exper.*, p. e4469, Apr. 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.4469
[15] A. Kashevnik and N. Teslya, "Blockchain-oriented coalition formation by cps resources: Ontological approach and case study," *Electronics*, vol. 7, no. 5, p. 66, 2018.
[16] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, blockchain based access control framework for the heterogeneous Internet of Things," in *Proc. 3rd ACM Workshop Attribute-Based Access Control*, 2018, pp. 61–69.
[17] Z. Li, W. M. Wang, G. Liu, L. Liu, J. He, and G. Q. Huang, "Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing," *Ind. Manage. Data Syst.*, vol. 118, no. 9, pp. 303–320, Feb. 2018.
[18] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo, "Distributed access control on IoT ledger-based architecture," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2018, pp. 1–7.
[19] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in *Internet of Things—ICIOT*, D. Georgakopoulos and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 150–164.
[20] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, "Mind my value: A decentralized infrastructure for fair and trusted IoT data trading," in *Proc. 7th Int. Conf. Internet Things*, 2017, p. 15.
[21] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robot. Comput.-Integr. Manuf.*, vol. 54, pp. 133–144, Dec. 2018.
[22] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, 2017.
[23] S.-C. Cha, K.-H. Yeh, and J.-F. Chen, "Toward a robust security paradigm for bluetooth low energy-based smart objects in the Internet-of-Things," *Sensors*, vol. 17, no. 10, p. 2348, 2017.
[24] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. (2018). "Smart contract-based access control for the Internet of Things." [Online]. Available: https://arxiv.org/abs/1802.04410
[25] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.
[26] L. Li *et al.*, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.
[27] J. Lee, "Patch transporter: Incentivized, decentralized software patch system for wsn and iot environments," *Sensors*, vol. 18, no. 2, p. 574, 2018.
[28] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new Blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2017.
[29] L. W. Park, S. Lee, and H. Chang, "A sustainable home energy prosumer-chain methodology with energy tags over the blockchain," *Sustainability*, vol. 10, no. 3, p. 658, 2018.
[30] Y. Sakakibara, S. Morishima, K. Nakamura, and H. Matsutani, "A hardware-based caching system on FPGA NIC for blockchain," *IEICE Trans. Inf. Syst.*, vol. 101, no. 5, pp. 1350–1360, 2018.
[31] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic blockchain to improve scalability in the Internet of Things," *Open J. Internet Things*, vol. 3, no. 1, pp. 46–61, 2017.
[32] H. Sun, S. Hua, E. Zhou, B. Pi, J. Sun, and K. Yamashita, "Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling," in *Blockchain—ICBC*, S. Chen, H. Wang, and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 3–17.
[33] M. Samaniego and R. Deters, "Using blockchain to push software-defined IoT components onto edge hosts," in *Proc. Int. Conf. Big Data Adv. Wireless Technol.*, 2016, p. 58.
[34] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proc. 7th Int. Conf. Internet Things*, 2017, p. 14.
[35] M. Samaniego and R. Deters, "Internet of smart Things—IoST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Jun. 2017, pp. 9–16.
[36] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.
[37] C. Pop *et al.*, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, Jan. 2018.
[38] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[39] R. D. Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23rd ACM Symp. Access Control Models Technol.*, 2018, pp. 77–83.
[40] J. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *J. Syst. Archit.*, vol. 87, pp. 36–48, Jun. 2018.
[41] Z. Guan *et al.*, (2018). "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities." [Online]. Available: https://arxiv.org/abs/1806.01056
[42] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.
[43] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[44] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
[45] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.
[46] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[47] A. Reyna and C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
[48] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, 2018.
[49] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, to be published.
[50] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov./Dec. 2016, pp. 1–6.
[51] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[52] F. D. O. Sergio, J. F. D. Silva, Jr., and F. M. de Alencar, "The blockchain-based Internet of Things development: Initiatives and challenges," in *Proc. ICSEA*, 2017, p. 39.
[53] A. Liberati *et al.*, "The prisma statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration," *PLoS Med*, vol. 6, no. 7, 2009, Art. no. e1000100.
[54] B. A. Kitchenham and S. Charters, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Jan. 2007.

[55] I. Weber, Q. Lu, A. B. Tran, A. Deshmukh, M. Gorski, and M. Strazds, "A platform architecture for multi-tenant for blockchain-based systems," in *Proc. Int. Conf. Softw. Archit.*, Hamburg, Germany, Mar. 2019, p. 10. [Online]. Available: http://hdl.handle.net/102.100.100/86005?index=1

[56] Y. Xu and A. Helal, "Scalable cloud-sensor architecture for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 285–298, Jun. 2016.

[57] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Boston, MA, USA: Addison-Wesley, 2003.

[58] C. Allen. The path to self-sovereign identity. Life With Alacrity BLOG. Accessed: Apr. 25, 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereignidentity.html

[59] S. M. Ruffer, D. Yen, and S. Lee, "Client/server computing technology: A framework for feasibility analysis and implementation," *Int. J. Inf. Manage.*, vol. 15, no. 2, pp. 135–150, 1995.

[60] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, "A pattern collection for blockchain-based applications," in *Proc. 23rd Eur. Conf. Pattern Lang. Programs (EuroPLoP)*, New York, NY, USA, 2018, p. 3. doi: 10.1145/3282308.3282312.

SIN KUANG LO is currently pursuing the Ph.D. degree with the Architecture and Analytics Platforms (AAP) Team, Data61, CSIRO, Sydney, and the School of Computer Science and Engineering (CSE), University of New South Wales (UNSW). His current research interests include software architecture and blockchain, specifically on the role of blockchain within a larger software systems.

YUE LIU is currently pursuing the master's degree with the College of Computer and Communication Engineering, China University of Petroleum (East China), Qingdao, China. His research interests include blockchain as a service and architecture design of blockchain applications.

SU YEN CHIA received the degree from the University of Malaya, Malaysia. Her research interests include software architecture, blockchain, and federated data platform.

XIWEI XU received the Ph.D. degree from the University of New South Wales (UNSW). She is currently a Senior Research Scientist with the Architecture and Analytics Platforms (AAP) Team, Data61, CSIRO, Sydney, and also a Conjoint Lecturer with the School of Computer Science and Engineering (CSE), UNSW. Her main research interests include software architecture. Since 2015, she has been working on blockchain. She also does research in the areas of service computing, business process, cloud computing, and dependability.

QINGHUA LU received the Ph.D. degree from the University of New South Wales, in 2013. She is currently a Senior Research Scientist with Data 61, CSIRO, Australia. Before joining Data61, she was an Associate Professor with the China University of Petroleum. She formerly worked as a Researcher with NICTA. She has published over 80 academic papers in international journals and conferences. Her current research interests include blockchain application design, blockchain as a service, self-sovereign identity, the IoT, and reliability of cloud computing.

LIMING ZHU is currently the Research Director of Data61, CSIRO. He is also a Conjoint Full Professor with the University of New South Wales (UNSW). He has published over 150 academic papers on software architecture, secure systems, and data analytics infrastructure. His research program has over 300 people innovating in the area of big data platforms, computational science, blockchain, regulation technology, privacy, and cybersecurity. He is the Chairperson of the Standards Australia's Blockchain and Distributed Ledger Committee.

HUANSHENG NING is currently a Professor and the Associate Dean of the School of University of Science and Technology Beijing (USTB). He has presided over many research projects, including the Natural Science Foundation of China (NSFC: 60879025, 61079019, 6131030602, and 61471035), and the National High Technology Research and Development Program of China (863 Project). He has published over 70 journal/conference papers and authored two books on the Internet of Things. His research interests include cybermatics, the Internet of Things, and cyber-physical social systems. He is the Founder and Chair of the Cybermatics and Cyberspace International Science and Technology Cooperation Base, the Co-Founder and Co-Chair of the IEEE Systems, Man, and Cybernetics Society Technical Committee on Cybermatics, and the Co-Founder and Vice Chair of the IEEE Computational Intelligence Society Emergent Technologies Technical Committee Task Force on Smart Word.