Exploring the Intellectual Cores of the Blockchain-Internet of Things (BIoT)

Abstract:

Purpose – Due to the rapid growth of blockchain technology in recent years, the fusion of blockchain and the Internet of Things (BIoT) has drawn considerable attention from researchers and industrial practitioners and is regarded as a future trend in technological development. Although several authors have conducted literature reviews on the topic, none have examined the development of the knowledge structure of BIoT, resulting in scattered research and development (R&D) efforts.

Design/methodology/approach - This study investigates the intellectual core of BIoT through a co-citation proximity analysis-based systematic review (CPASR) of the correlations between 44 highly influential articles out of 473 relevant research studies. Subsequently, we apply a series of statistical analyses, including exploratory factor analysis (EFA), hierarchical cluster analysis (HCA), k-means clustering (KMC) and multidimensional scaling (MDS) to establish the intellectual core.

Findings – Our findings indicate that there are nine categories in the intellectual core of BIoT: (i) data privacy and security for BIoT systems, (ii) models and applications of BIoT, (iii) system security theories for BIoT, (iv) frameworks for BIoT deployment, (v) the fusion of BIoT with emerging methods and technologies, (vi) applied security strategies for using blockchain with the IoT, (vii) the design and development of industrial BIoT, (viii) establishing trust through BIoT, and (ix) the BIoT ecosystem.

Originality – We use the CPASR method to examine the intellectual core of BIoT, which is an under-researched and topical area. The paper also provides a structural framework for investigating BIoT research that may be applicable to other knowledge domains.

Keywords: blockchain, Internet of Things, co-citation proximity analysis, intellectual core, systematic review

1. Introduction

Blockchain and the Internet of Things (IoT) are two promising and emerging technologies that an increasing number of businesses apply to meet industrial and financial objectives. On the one hand, blockchain was a foundational element in the development of cryptocurrency; it was extended for use in various industrial scenarios to build trust and consensus within distributed systems. Blockchain-enabled systems and services have improved authentication, integrity and immutability (Crosby et al., 2016). On the other hand, the IoT originated in the radio frequency identification (RFID)

The following publication Tsang, Y.P., Wu, C.H., Ip, W.H. and Shiau, W.-L. (2021), "Exploring the intellectual cores of the blockchain–Internet of Things (BIoT)", Journal of Enterprise Information Management, Vol. 34 No. 5, pp. 1287-1317 is published by Emerald and is available at https://doi.org/10.1108/JEIM-10-2020-0395.

infrastructure, although no standardised definition of the IoT has been developed (Wortmann and Flüchter, 2015). IoT solutions focus on connecting various physical objects through Internet protocols and networking technology. Existing IoT applications that use centralised approaches are facing challenges related to security, privacy, data storage and scalability (Khan and Salah, 2018). In recent years, more and more research studies have focused on the integration of blockchain and the IoT, i.e. blockchain–IoT (BIoT), to improve the practicality and adaptability of existing IoT applications, particularly with regards to data reliability, security, trustworthiness, and autonomy (Novo, 2018; Reyna, 2018). Such integration would also provide advantages related to mobility, accessibility, concurrency, being lightweight, scalability and transparency. Furthermore, the trustworthiness of IoT data can be established within a distributed network. Due to the massive expansion of IoT use in numerous industries, the number of IoT devices is expected to increase dramatically. Therefore, blockchain promises to play an essential role in addressing the vulnerabilities and effective control of numerous IoT devices. Hence, BIoT research is a promising area, and an investigation of the topic's intellectual core is necessary to support and guide research and development (R&D).

Numerous research studies have described and demonstrated BIoT, and some review studies have summarised the key dimensions and directions of this research (Alladi et al., 2019; Wang et al., 2020). However, there has been no systematic investigation of the intellectual core and knowledge structure of BIoT research. It is essential to categorise the existing BIoT research to identify trends and implications to support future R&D activities. Co-citation analysis is a promising technique for describing BIoT's emerging intellectual core (Wang et al., 2016; Ng et al., 2018; Shiau et al., 2019). Nevertheless, it cannot examine the relationships among influential research studies, let alone evaluate such relationships' strength. Moreover, BIoT research is still preliminary; relevant studies go back only to 2015. A systematic review provides a reliable and comprehensive process for examining specific research objectives, while citation analysis and co-citation proximity analysis can identify and group highly influential research work effectively. This study combines these methods via co-citation proximity analysis-based systematic review (CPASR) to identify BIoT research trends that are relevant to both academia and industrial practitioners. We seek to answer the following two research questions:

a. What is the structural formulation of the CPASR method?
b. What is the intellectual core of BIoT that has emerged from existing research?

To apply the CPASR method to BIoT research, we collected a group of highly influential research studies from Web of Science, a well-known publication database. During the statistical analysis process, exploratory factor analysis (EFA) and hierarchical cluster analysis (HCA) were applied to categorise the intellectual core of BIoT, while k-means clustering (KMC) was used to identify strong relationships among highly influential research studies. After formulating the intellectual core's categories, we used multidimensional scaling (MDS) to visualise the categorisation and the levels of similarity among highly influential research studies. Using this categorisation, we identified various trends and implications to support current and future R&D activities in the field of BIoT. This study makes two main contributions. First, it provides a structural framework via citation analysis, co-citation proximity analysis and a series of statistical analyses, (including EFA, HCA, KMC, and MDS) to investigate research domains' intellectual cores. Second, this study examines BIoT, a topical research domain in the field of information management to accelerate the development of industrial and enterprise solutions. Also, the high applicability of the proposed method fosters the future analysis on other knowledge domains. By analysing relevant research publications in a five-year time frame from 2015 to 2019, nine intellectual cores of BIoT are constructed to evaluate its knowledge diffusion and to support future research on blockchain and IoT technologies.

The remainder of this paper is organised as follows. Section 2 reviews research studies concerning blockchain, the IoT, literature review methods and co-citation proximity analysis. Section 3 describes the CPASR methodology. Section 4 presents the results of our application of CPASR to evaluate the knowledge structure of BIoT technologies. Section 5 discusses the trends and implications identified in the systematic review. Finally, concluding remarks are drawn in Section 6.

2. Literature Review

In this section, we review two areas of the literature relevant to this study: BIoT and literature review methods.

2.1 Overview of BIoT Technologies

In the era of digitalisation, IoT and blockchain are regarded as two emerging technologies with complementary characteristics that can generate a synergy to support technological advances. c Also, complete transparency in a blockchain may cause data privacy challenges, threatening the users' anonymity. Therefore, the integration of blockchain and IoT was proposed to improve system capabilities, including scalability, autonomy, identification, reliability, security and service variety. Since BIoT research

is still preliminary, it is likely that BIoT R&D will grow rapidly in the near future. To facilitate such R&D, the knowledge structure of BIoT must be investigated to identify the trends and implications emerging from preliminary research studies.

To summarise, BIoT is defined as 'a peer-to-peer system network of interconnected objects and users with a unique authentication and consensus mechanism, in which transmitted data in blocks are chained in a decentralised manner to create trust in the network.'

2.2 Overview of Literature Review Methods

There are several review methods, including literature and systematic reviews, that can be used to organise existing studies to identify trends and generate insights for future research. Paré and Kitsiou (2017) summarise six generic procedures for conducting a literature review, namely: (i) formulating research questions and objectives, (ii) searching the existing literature, (iii) literature screening and filtering, (iv) a quality assessment of primary studies, (v) data extraction and (vi) data analysis. Several literature review methods have been developed from this framework to analyse the past literature on BIoT in a qualitative manner, including narrative, mapping and critical reviews (Chowdhury et al., 2018; Hughes et al., 2019; Viriyasitavat et al., 2019; Burton-Jones et al., 2020). These methods summarise the advantages, disadvantages, limitations and applications of a specific topic while analysing the status quo and future directions. Apart from literature reviews, systematic reviews have also been developed for quantitative data collection and research study appraisals. In a systematic review, pre-defined research questions are brought into focus through summarising and synthesising empirical evidence. The review protocol and search strategy are clearly defined to provide reliable findings with minimal bias (Munn et al., 2018). Based on the systemic review, rapid and umbrella reviews were developed to conduct the review process quickly and to consider the multiple factors involved in research studies, such as citation and bibliographic coupling (Khangura et al., 2012; Aromataris et al., 2015). Among systematic review techniques, citation analysis is a well-known method for identifying highly influential research studies in a specific domain using search keywords and a citation threshold (Hug et al., 2017). Moreover, co-citation analysis is a promising method for investigating the correlations between research studies in emerging research areas by evaluating binary co-citation indexes (Hausberg et al., 2020). In order to reflect actual correlations, co-citation proximity analysis focuses on the non-binary closeness of research studies cited in a document (Kim et al., 2016), which can effectively evaluate the proximity of the research studies. Compared with traditional co-citation analysis, it obtains a higher precision to pinpoint the degree of

proximity in chapters, sections and paragraphs within the research documents to establish their intellectual cores. In this review study, citation analysis and co-citation proximity analysis are integrated to construct a systematic review of BIoT, while a series of statistical analyses are performed to evaluate the research findings objectively.

3. CPASR Methodology

To explore the existing research in the BIoT field, we propose a co-citation proximity analysis-based systematic review (CPASR) that integrates citation analysis, co-citation proximity analysis and statistical analysis. First, we establish a structural framework for CPASR (Figure 1). The framework consists of three main tiers: (i) data collection, (ii) citation and co-citation proximity analysis and (iii) statistical analysis and evaluation.

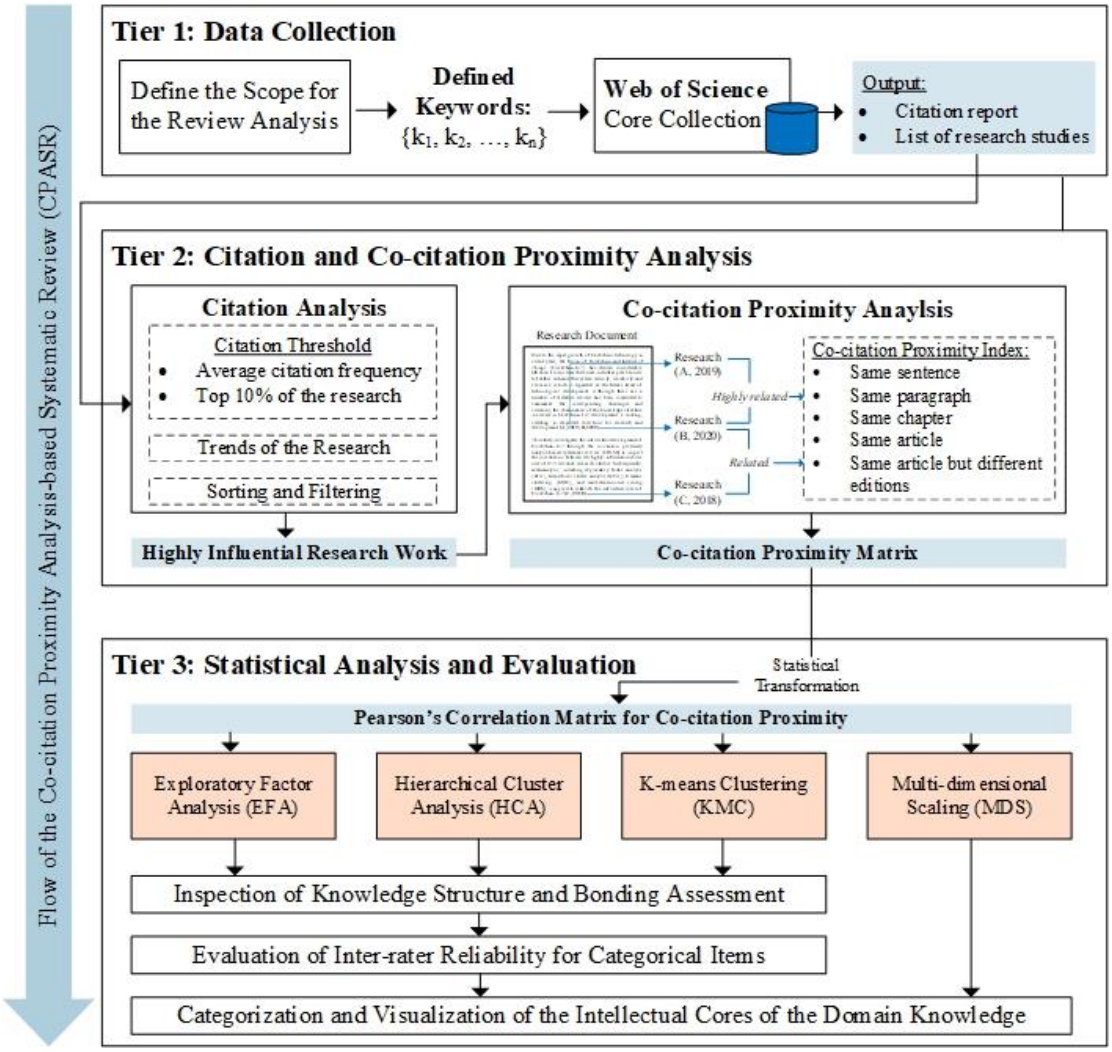

Figure 1. Structural framework for CPASR.

3.1 Tier 1: Data Collection

With regard to data collection, a clear focus of a knowledge domain, e.g. BIoT, is

required for the review analysis, and the corresponding keywords $\mathbf{K} = \{k_1, k_2, \ldots, k_z\}$ must be selected carefully to guide the search process. To search for high-quality research studies, we used the Web of Science (WoS) Core Collection, an academic database containing multidisciplinary information. It includes citation data for 21,000 journals, books and conference proceedings published worldwide and is updated daily to ensure accuracy (Clarivate Analytics, 2020). The database covers six citation indexes: the science citation index, expanded (SCIE); social sciences citation index (SSCI); arts and humanities citation index (A&HCI); conference proceedings citation index (CPCI); book citation index (BCI) and emerging sources citation index (ESCI). The WoS acceptance rate is about 10–12% for the SCIE, SSCI and A&HCI indexes, which implies that the collection has relatively rigorous standards compared to other academic databases, for instance Google Scholar and Scopus. Furthermore, the quality of the research work cited in the WoS Core Collection is guaranteed, which improves reliability and validity. We excluded review articles from the search process, as they contribute less to the theoretical and intellectual development of BIoT than original research. Thus, we generated a set **R** of the research studies and their corresponding citations for the citation and co-citation proximity analyses.

3.2 Tier 2: Citation and Co-Citation Proximity Analyses

In this tier, citation and co-citation proximity analyses are performed to evaluate the correlations between highly influential BIoT research studies. The selection of highly influential research studies from **R** is based on two criteria: (i) average citation frequency and (ii) approximately top 10% of the research studies with respect to the number of citations; the sets $\mathbf{R_f}$ and $\mathbf{R_{top}}$ can be determined based on the two criteria, respectively. Any research item with zero citations in the set **R** is excluded from $\mathbf{R_f}$ because such items' significance is uncertain. Research trends can be inspected as the studies in sets $\mathbf{R_f}$ and $\mathbf{R_{top}}$ are sorted and filtered to remove duplicate studies. Consequently, a set of highly influential research studies, $\mathbf{R_h}$, can be obtained, where $\mathbf{R_h} = \min\{\mathbf{R_f}, \mathbf{R_{top}}\} \subseteq \mathbf{R}$. Secondly, an $n \times n$ co-citation proximity matrix $\mathbf{M_{ij}}$ is formulated to evaluate the co-citation proximity index (CPI) for the set of highly influential research studies, where n is the cardinality of the set $\mathbf{R_h}$. Every study in **R** is then inspected to determine whether it is cited in more than one item in $\mathbf{R_h}$. If a document in **R** cites two research items in $\mathbf{R_h}$, a CPI value is assigned to express their proximity and similarity (Yaghtin et al., 2019). As shown in Table 1, each CPI value depends on the occurrence of the cited research work, and the index value is weighted by $1/(2^m)$, where m refers to the proximity level between in-text citations. When highly influential research documents are cited more than once, the closest correlation (i.e. the highest CPI value) between the two studies is assigned, such that CPI_{ij} =

$\max\{CPI_{ij1}, CPI_{ij2}, \ldots, CPI_{ijk}\}$, where k refers to the number of proximate combinations. After constructing the CPI values for the set R, the co-citation proximity matrix is formulated to structure the intellectual core of the knowledge domain.

Table I. CPI value assignments for the co-citation proximity analysis

Occurrence of cited research work	CPI Value
Within the same sentence	$1/2^0 = 1$
Within the same paragraph	$1/2^1 = 0.5$
Within the same section	$1/2^2 = 0.25$
Within the same journal edition	$1/2^3 = 0.125$

3.3 Tier 3: Statistical analysis and evaluation

Once the co-citation proximity matrix is obtained, a series of statistical analyses are conducted to assess the highly influential research studies systematically. In this study, four statistical methods are considered: EFA, HCA, KMC and MDS. EFA, HCA and MDS are widely applied to analyse the correlation between research documents to explore the intellectual structure of a knowledge domain (Shiau et al., 2019). Intellectual structures can be clustered with EFA and HCA, while MDS examines clustering feasibility. To further validate clustering performance, KMC is added to identify the bonding of members in the intellectual cores to identify studies with high similarity. Before the statistical analyses are conducted, the co-citation proximity matrix is converted to a Pearson's correlation matrix. This matrix contains the Pearson product-moment correlation coefficients necessary to measure the correlation between any two highly influential research studies. In this study, EFA (which reveals the underlying structure among measured variables) and HCA (which groups similar items into clusters) were applied to obtain an intermediate knowledge structure containing several clusters of highly influential BIoT studies. Intra-cluster bonds between cluster group members are assessed via KMC to identify the bonding intensities between highly influential research studies inside specific clusters. It is essential to provide support and evidence when constructing categorical labels for clusters. When categories for the highly influential research studies are determined, the inter-rater reliability is examined to ensure the consistent assignment of appropriate categorical labels to clusters. Consequently, a final categorisation of highly influential research studies can be obtained. In addition to the categorisation, the clustering results are visualised using MDS to uncover the degree of similarity among the research studies. Grouping the highly influential research studies systematically using the methods mentioned above formulates the intellectual core, making it possible to identify the trends and implications of the knowledge domain.

4. Results and Analysis

In this section, the CPASR method is used to evaluate the knowledge structure of BIoT. To search for research studies related to BIoT, the set of keywords was defined as **K** = {'blockchain,' 'IoT,' 'Internet of Things'}; 'IoT' is the commonly recognised abbreviation for 'Internet of Things.' If only the keyword 'IoT' is used to represent the IoT domain, then some terminologies that involve the letter combination 'iot' may be included, such as biotechnology, radiotelemetry, and bibliotherapy. Subsequently, we used three keywords, 'blockchain,' 'IoT' and 'Internet of Things,' locating their intersection in BIoT-related studies. As a result, we collected a total of 473 research studies (including journal and conference papers) from the WoS Core Collection on 31 December 2019, and 2,807 citations were obtained from these papers. Figures 2 and 3 depict the trends in publications and citations in the BIoT field, respectively. The results indicate that BIoT research remains preliminary but is growing rapidly, necessitating a systematic investigation of its intellectual core.

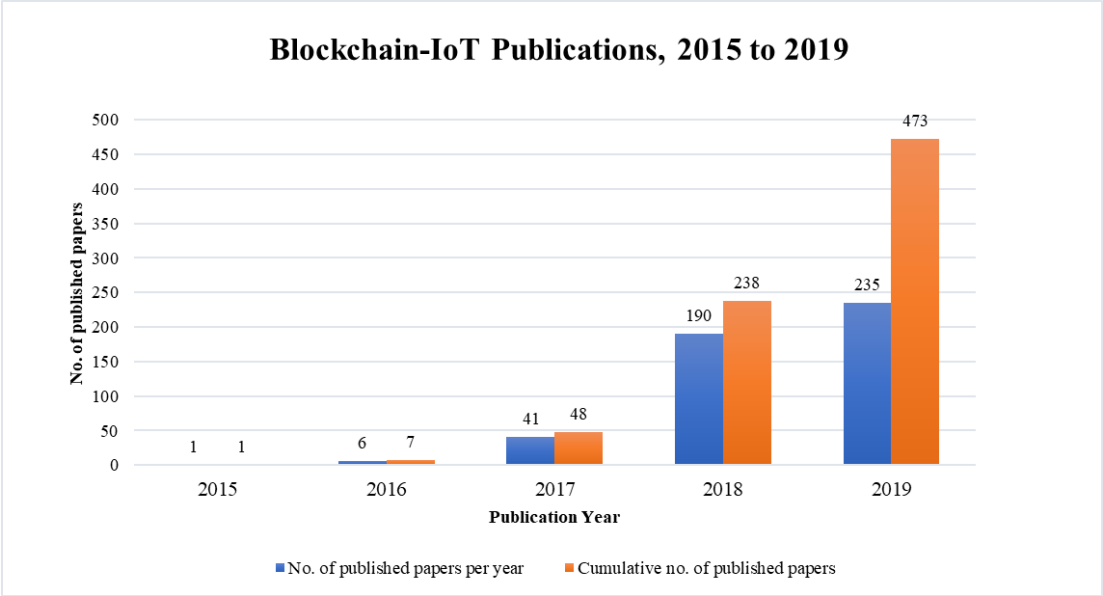

Figure 2. Publication trend for BIoT papers for 2015 to 2019.

The highly influential research studies were selected using the sets $\mathbf{R_f}$ and $\mathbf{R_{top}}$ rather than a fixed citation threshold. For $\mathbf{R_f}$, the 473 research studies were cited 12.2043 times on average, which was rounded up to 13 citations in order to extract the research studies which were cited by more than 12.2043 times. Compared to a fixed citation threshold, the above citation analysis provides greater flexibility for identifying influential research studies in some new and developing research areas, such as blockchain. Citation thresholds such as 100 or 300 citations can be used once research domains are well-developed with a long history. Subsequently, 44 research studies were extracted

for the set $\mathbf{R_f}$, which accounted for the top 9.3% of all research studies. In addition, the set $\mathbf{R_{top}}$ covered the citation performances of the top 47 research studies. By combining $\mathbf{R_f}$ and $\mathbf{R_{top}}$, 44 papers were selected as highly influential research studies and placed in $\mathbf{R_h}$. Table 2 summarises the core objectives or scopes of these studies. The selected studies are classified into system analyses, surveys, conceptual frameworks, case studies and experimental studies. Of the 44 selected BIoT studies, most are system analysis papers about designing and modelling blockchain-based solutions to manage IoT devices and data while preserving security and privacy. Since they have contributed to the development of the intellectual structure of BIoT, the following analysis and interpretation also cover the above three studies. Next, a 44×44 co-citation proximity matrix was formulated through the evaluation of the CPI values. In order to conduct the statistical analysis for the co-citation proximity matrix, it was converted to a Pearson's R correlation matrix to show the correlation loadings between highly influential research studies. The diagonal of the co-citation proximity matrix was treated as missing data so that average co-citation proximity values were considered in this study. The study results are presented in the following four sub-sections: (i) investigation of the knowledge structure, (ii) intra-cluster bonding assessment, (iii) evaluation of inter-rater reliability and (iv) categorisation and visualisation of the intellectual core.

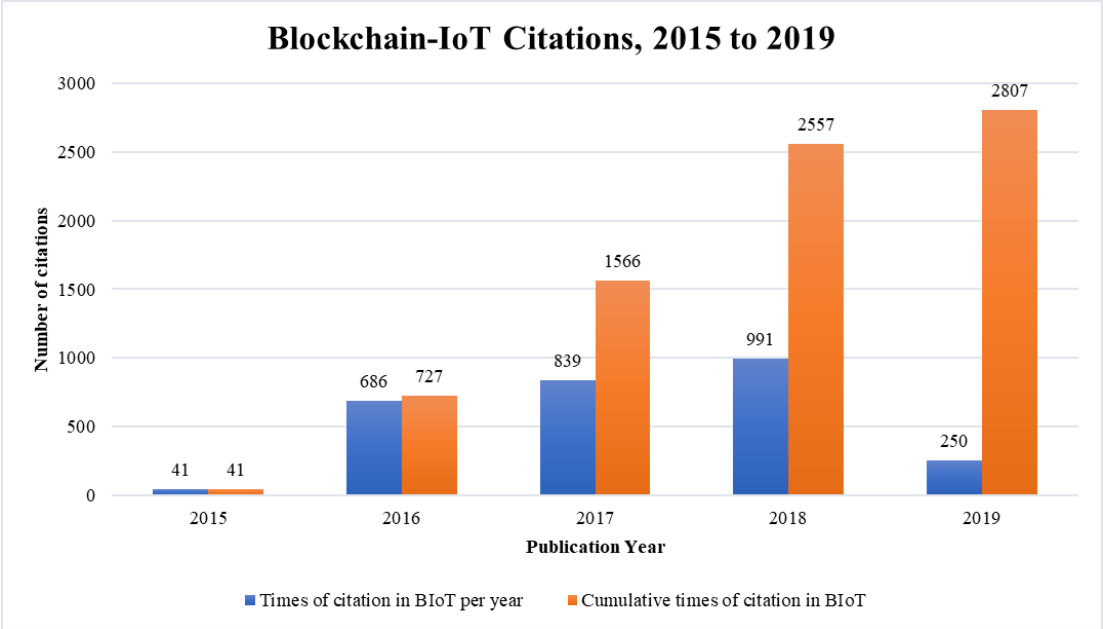

Figure 3. Citation trend for BIoT papers for 2015 to 2019.

Table II. List of highly influential research studies on BIoT

ID	Authors (Year)	Core Objective/Scope	Methodology Type	Citations
S1	Zhang and Wen (2015)	To propose an IoT e-business model with the help of P2P trade based on the blockchain and smart contract.	System analysis	41
S2	Sun et al. (2016)	To investigate the contributions of blockchain technology for developing sharing services in smart cities.	Conceptual framework	51
S3	Ouaddah et al. (2016)	To propose a blockchain-based access control framework (FairAccess) for the IoT.	System analysis	65
S4	Singh and Singh (2016)	To discuss the outlook of the role of blockchain in the future of banking, finance, and IoT.	Case study	21
S6	Christidis and Devetsikiotis (2016)	To explore a blockchain-IoT combination to facilitate the sharing economy and to automate business workflows in a cryptographically verifiable manner.	Survey	492
S7	Biswas and Muthukkumaras amy (2016)	To propose a security framework that integrates blockchain and smart devices to establish a secure communication platform in a smart city.	Conceptual framework	51
S8	Kshetri (2017)	To evaluate the role of blockchain in strengthening cybersecurity and privacy protection for industrial scenarios.	Case study	47
S10	Outchakoucht et al. (2017)	To propose a dynamic and fully distributed security policy for access control in the context of IoT.	System analysis	15
S11	Zhang and Wen (2017)	To establish an IoT e-business platform that adopts distributed autonomous corporations to conduct P2P trade.	System analysis	59
S12	Lee and Lee (2017)	To propose a novel firmware update scheme for IoT devices using blockchain technology.	System analysis	47
S13	Huh et al. (2017)	To manage devices in IoT systems by using Rivest-Shamir-Adleman (RSA) public key cryptosystems with the hybrid use of Ethereum and local storage.	System analysis	101
S14	Shae and Tsai (2017)	To design a blockchain platform for clinical trial and precision medicine for big data analytics, IoT device management and data-sharing schemes.	System analysis	21
S15	Zheng et al. (2017)	To provide an overview of blockchain technology and to compare blockchain mechanisms.	Survey	178
S17	Ahram et al. (2017)	To innovate healthcare services and applications, namely Healthchain, with blockchain technology.	Case study	27
S19	Stanciu (2017)	To formulate a platform-hierarchical and distributed control system to facilitate edge computing.	System analysis	36
S25	Samaniego and Deters (2017)	To utilise a permission-based blockchain protocol to manage an extensive Internet of Smart Things.	Experimental	15
S26	Liu et al. (2017)	To propose a blockchain-based framework for a data integrity service to replace the role of third-party auditors.	System analysis	32
S27	Boudguiga et al. (2017)	To investigate the use of blockchain infrastructure to meet the requirements of confidentiality, integrity and availability.	System analysis	20
S31	Karafiloski and Mishev (2017)	To discuss decentralised management in the big data revolution for personal data protection, digital property, IoT and healthcare.	Survey	34
S34	Lin et al. (2017)	To propose an open, trusted, decentralised and tamper-proof system for long-range wide-area network (LoRaWAN).	System analysis	13
S35	Teslya and Ryabchikov (2017)	To integrate the Smart-M3 information sharing platform and blockchain technology to build trust between stakeholders and to control resource distribution.	System analysis	13
S38	Hwang et al. (2017)	To introduce the energy prosumer service model by using blockchain technology to improve energy efficiency.	System analysis	17

Table II. (continued)

ID	Authors (Year)	Core Objectives/Scopes of the Studies	Methodology Type	Citations
S39	Conoscenti et al. (2017)	To develop a decentralised private-by-design IoT for storing IoT data in a P2P network to achieve better user privacy protection.	System analysis	13
S42	Dorri et al. (2017)	To demonstrate a lightweight blockchain in the smart home scenario to strengthen IoT security and privacy.	Case study	21
S43	Ouaddah et al. (2017)	To develop a decentralised pseudonymous and privacy-preserving authorisation management framework for better access control on IoT devices.	System analysis	44
S48	Xu et al. (2017)	To propose a privacy-respecting approach for blockchain-based sharing economy applications to leverage a zero-knowledge scheme.	System analysis	13
S49	Yu et al. (2018a)	To investigate typical security and privacy issues in IoT, and develop a blockchain-IoT framework for better assurance of IoT data.	System analysis	13
S54	Reyna et al. (2018)	To analyse the opportunities and challenges in blockchain–IoT applications, and improve the IoT by using blockchain.	Survey	70
S60	Hammi et al. (2018)	To propose a decentralised identification and authentication system (bubbles of trust) for IoT devices to enhance data integrity and availability.	System analysis	34
S62	Sharma and Park (2018)	To propose a hybrid network architecture for the smart city that integrates software-defined networking and blockchain technologies to ensure data security and privacy.	System analysis	21
S66	Banerjee et al. (2018)	To discuss blockchain technology in relation to the integrity of sharing IoT datasets.	Survey	32
S69	Yu et al. (2018b)	To demonstrate the applicability of blockchain to IoT devices and data management for establishing end-to-end trust for trading.	Case study	15
S70	Griggs et al. (2018)	To deploy blockchain-based smart contracts to facilitate secure analysis and IoT sensor management in the healthcare scenario.	System analysis	25
S73	Joshi et al. (2018)	To synthesise the structures and consensus algorithms of blockchain technology.	Survey	17
S75	Novo (2018)	To propose a novel architecture for arbitrating roles and permissions in a fully distributed access control system for IoT based on blockchain technology.	System analysis	90
S76	Kshetri (2018)	To examine the effect of using blockchain in supply chain management objectives, such as cost, quality, speed, dependability, risk reduction, sustainability and flexibility.	Case study	71
S210	Sharma et al. (2018)	To propose a blockchain-based distributed cloud architecture with software-defined networking that enables fog nodes at the edge of the network.	System analysis	81
S211	Xu et al. (2018)	To synthesise state-of-the-art technologies in the area of Industry 4.0, including blockchain and IoT.	Survey	120
S212	Zheng et al. (2018)	To introduce the blockchain taxonomy, consensus algorithms and applications from both technological and application perspectives.	Survey	75
S231	Zhou et al. (2018)	To propose a blockchain-based threshold IoT service system (BeeKeeper) to process user data by performing homomorphic computations.	System analysis	15
S236	Cha et al. (2018)	To design a blockchain-connected gateway for user privacy preferences on IoT devices.	System analysis	23
S237	Jesus et al. (2018)	To analyse the use of blockchain for IoT security and privacy by considering a stalker attack.	Survey	18
S344	Ferrag et al. (2019)	To analyse the application domains of blockchain technology in IoT, and classify threat models for blockchain protocols in IoT networks.	Survey	14
S358	Dwivedi et al. (2019)	To propose a decentralised privacy-preserving healthcare blockchain model for IoT.	Case study	23

4.1 Investigation of the Knowledge Structure

We conducted EFA and HCA in the SPSS software environment to analyse the correlation loadings between highly influential research studies, formulating intermediate knowledge structures for BIoT. For the EFA, the threshold for factor extraction was set as one eigenvalue, while the rotation method was set to varimax to maximise the loading dispersion within factors. Consequently, we obtained eight factors that explained 89.948% (almost 90%) of the variability (Table 3). Factor 4 was excluded in the further analysis, as only one item was assigned to this cluster, indicating that the factor was inadequate. The remaining seven factors explained 82.790% of the variability, which is sufficient for explaining the knowledge structure. On the other hand, only relying on a statistical method (i.e. EFA) is insufficient to describe a knowledge structure. Therefore, HCA was also applied to group similar items into clusters. The results from EFA and HCA were then aggregated to facilitate the construction of the intellectual core of BIoT research. Ward's method was selected to conduct the HCA. Therefore, the HCA results were visualised in a dendrogram (Figure 4). The clusters were identified according to the lowest level of the rescaled distance (i.e. approximately 1.4 units) in the dendrogram to form the maximum number of research study groups (i.e. 13 groups). However, several studies (S31, S38 and S73) could not be grouped in such fine-grained clusters because only one study in the group cannot reveal any closeness and relationship with other research studies. Therefore, ten clusters were generated for the classification of the highly influential research studies, as shown in Figure 4.

Table III. EFA exploration of the knowledge structure of BIoT

Factor	Member (ID)	Eigenvalue	% of Variance	Cumulative % of Variance
1	S1, S4, S11, S12, S13, S14, S15, S34, S42, S54, S66, S75	20.129	45.747%	45.747%
2	S2, S3, S6, S7, S10, S19, S26, S27, S39, S43, S48, S76, S210, S231, S236	5.332	12.119%	57.865%
3	S25, S60, S62, S69, S237, S344	3.956	8.990%	66.856%
4	S49	3.150	7.158%	74.014%
5	S31, S212, S358	2.509	5.703%	79.717%
6	S38, S73	1.843	4.188%	83.904%
7	S8, S17	1.626	3.695%	87.600%
8	S70, S35, S21	1.033	2.348%	89.948%

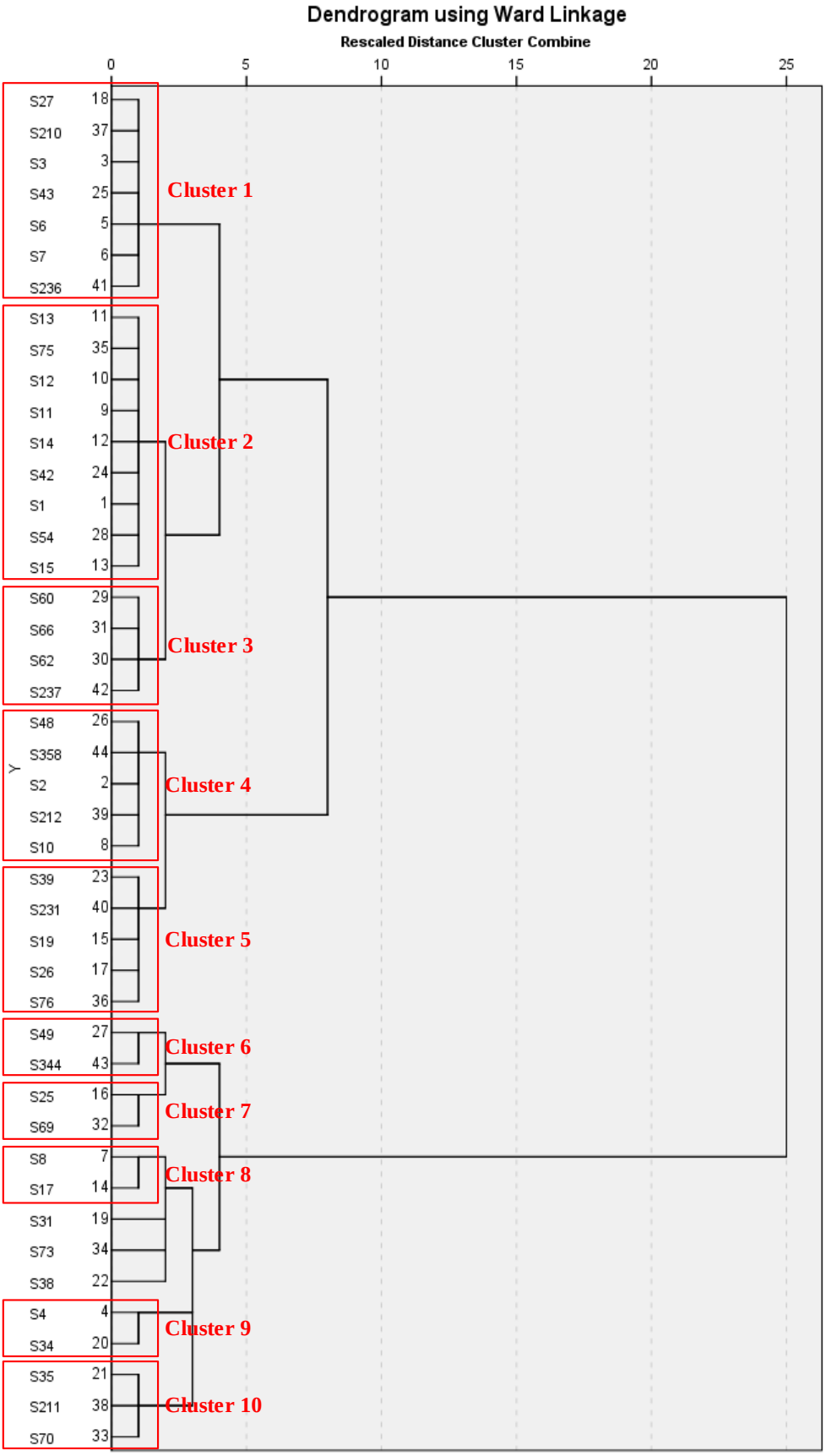

Figure 4. HCA exploration of the knowledge structure for BIoT.

To aggregate the results from EFA and HCA, the research studies identified in EFA factor construction and HCA clustering were grouped into a number of categories representing the BIoT knowledge structure. Nine categories were formulated to group similar research studies, while the remaining uncategorised items were grouped in an un-clustered category (Figure 9). The nine identified categories, all of which have drawn considerable attention from scholars and industrial practitioners, constitute the intellectual core of the BIoT field.

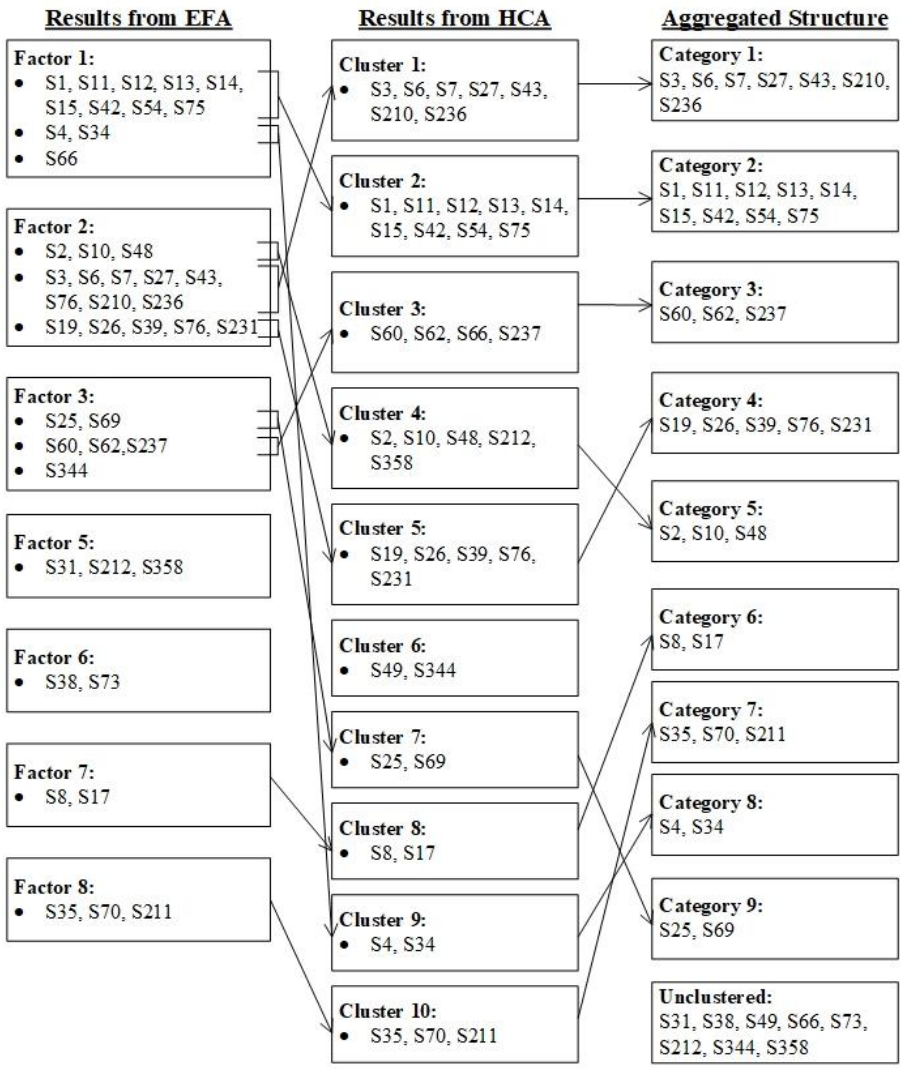

Figure 5. Aggregated knowledge structure for BIoT based on EFA and HCA.

4.2 Intra-cluster Bonding Assessment

We investigated the intra-cluster bonding assessments between cluster members through k-means clustering to facilitate the labelling process for the nine categories. The Pearson's correlation matrix was analysed and partitioned into nine clusters via k-means clustering (Figure 6). The common classification results were highlighted to explore the strongly bonded members within the categories. When the classifications

of highly influential research studies using KMC and the aggregated structure were the same, the member–member bonding was considered relatively strong. Strongly bonded members were identified with an asterisk (*) to assist in labelling the categories effectively. Therefore, the themes of the nine identified categories were established through in-depth investigations of the categories' core members, considering that the nine categories should be independent of each other.

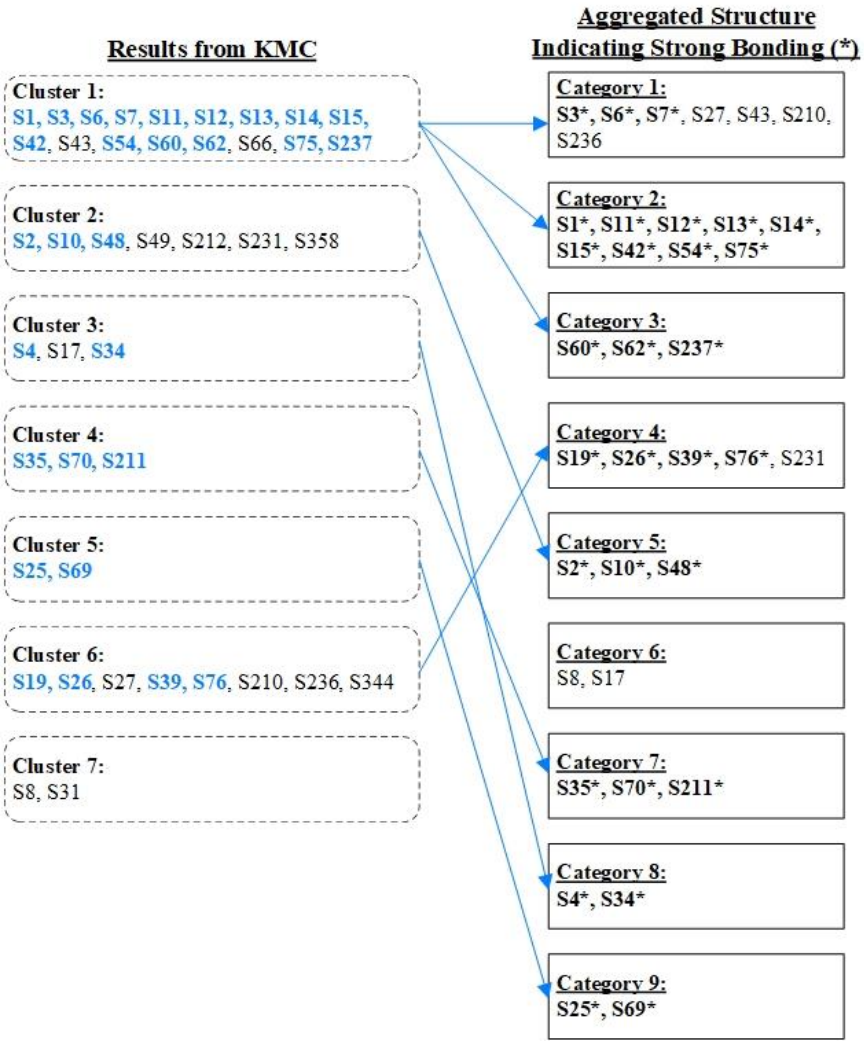

Figure 6. KMC evaluation of member bonding within categories.

4.3 Evaluation of inter-rater reliability

In order to assign the appropriate theme to each category, a list of draft categorisations was prepared, assessed and classified by a group of raters, all of whom were domain experts in the field of BIoT. For cluster 1 (S3, S6, S7, S27, S43, S210, S236), the studies considered various access control methods to secure data privacy and data management; thus, this cluster was named 'Data Privacy and Management for BIoT Systems' (category 1). Cluster 2 (S1, S11, S12, S13, S14, S15, S42, S54, S75) centred on

numerical models and applications in various domains, and this cluster was named ‘Models and Applications of BIoT’ (category 2). In cluster 3 (S60, S62, S237), novel frameworks and architectures for system security were introduced for decentralisation and secure authentication mechanisms; therefore, this cluster was named ‘System Security Theories for BIoT’ (category 3). Cluster 4 (S19, S26, S39, S76, S231) focused on the fusion of blockchain and IoT, including the key components for building BIoT systems, and so this cluster was named ‘Frameworks for BIoT Deployment’ (category 4). The studies in cluster 5 (S2, S10, S48) discussed how other emerging methods and technologies such as machine learning and artificial intelligence could generate new synergies in BIoT systems; thus, this cluster was named ‘Fusion of BIoT with Emerging Methods and Technologies’ (category 5). Cluster 6 (S8, S17) concentrated on applications of BIoT-driven security theories to strengthen business cybersecurity and user privacy protections; the cluster was named ‘Applied Security Strategies for Using Blockchain in IoT’ (category 6). In cluster 7 (S35, S70, S211), the potential of BIoT was further aligned with emerging technological trends such as industry 4.0 and smart health; hence, this cluster was named ‘Design and Development of Industrial BIoT’ (category 7). Cluster 8 (S4, S34) focused on digitalising society and the economy using BIoT and considered trust on the Internet to be a key research topic; thus, this cluster was named ‘Establishing Trust with BIoT’ (category 8). The studies in Cluster 9 (S25, S69) provided overviews of BIoT deployments, summarising features, benefits and potential development trends; this cluster was named ‘BIoT Ecosystem’ (category 9). Table 4 summarises the above results.

The raters, five scholars who possessed PhD-level qualifications and were engaged in BIoT research, were invited to conduct the inter-rater reliability analysis by evaluating the intraclass correlation coefficients (ICC). ICCs can reflect the variations between domain experts who measure the categorisation of intellectual cores with consistent themes (Koo and Li, 2016). This technique is useful for ensuring the reliability of the categorisation process for the nine intellectual cores; it uses domain experts’ views to determine whether the cores’ themes are appropriate. The raters judged the level of matching between the nine suggested themes and their corresponding categories on a three-point scale (1: match, 2: neutral, 3: not match). Since the measured data are ordinal for all 18 items, Krippendorff’s alpha was used to calculate the inter-rater reliability (Hayes and Krippendorff, 2007). The five scholars are randomly selected and invited from the the population, and the categories were assessed consistently by the scholars. As shown in Table 5, the five raters assigned the scores to the items (C1 to C9 and M1 to M9) in a random order using their own professional judgements. When analysing the ICC in the SPSS software environment, the kalpha function was used

(SPSS macro syntax: *kalpha judges = R1 R2 R3 R4 R5/level = 2/detail = 0/boot = 10000*). Therefore, the ICC value was 0.7486 (0.5600–0.9057, 95% confidence interval), demonstrating that the theme assignments for the nine groups had acceptable reliability. In summary, the suggested themes were appropriate for the nine categories.

Table IV. Intellectual core formulation results

#	Factors in EFA	Clusters in HCA	Clusters in KMC	Conceptual theme	Members
1	Partial 2	1	Partial 1	Data Privacy and Management for BIoT Systems (1)	S3, S6, S7, S27, S43, S210, S236
2	Partial 1	2	Partial 1	Models and Applications of BIoT (2)	S1, S11, S12, S13, S14, S15, S42, S54, S75
3	Partial 3	3	Partial 1	System Security Theories for BIoT (3)	S60, S62, S237
4	Partial 2	5	Partial 6	Frameworks for BIoT Deployment (4)	S19, S26, S39, S76, S231
5	Partial 2	4	Partial 2	Fusion of BIoT with Emerging Methods and Technologies (5)	S2, S10, S48
6	7	8	N/A	Applied Security Strategies for Using Blockchain in IoT (6)	S8, S17
7	8	10	4	Design and Development of Industrial BIoT (7)	S35, S70, S211
8	Partial 1	9	Partial 3	Establishing Trust with BIoT (8)	S4, S34
9	Partial 3	7	5	BIoT Ecosystem (9)	S25, S69

Table V. Raters' theme assignments for inter-rater reliability analysis

#	Item	Rater 1	Rater 2	Rater 3	Rater 4	Rater 5
1	C1	1	1	1	1	1
2	C2	1	1	1	1	1
3	C3	1	2	1	1	1
4	C4	1	1	1	1	1
5	C5	2	1	2	2	2
6	C6	1	1	1	1	1
7	C7	1	1	1	1	1
8	C8	2	2	2	2	2
9	C9	1	1	1	1	1

Remark: C1–C9 represent the nine categories identified with the CPASR method; 3-point scale: 1 for 'match,' 2 for 'neutral,' 3 for 'no match.'

4.4 Categorisation and visualisation of the intellectual core

The intellectual core of BIoT can be systematically established using the nine groups of highly influential research studies discussed above. To visualise the above categorisation, we used MDS to convert distances between research studies into distances in Cartesian space. The goodness of fit of 3-D MDS was better than that of 2-D MDS (Table 6). The overall performance of 3-D MDS was between 'good' and 'excellent,' following Mair (2016). In particular, the normalised raw stress of the 3-D MDS can be decreased by 54.45% to 0.02123, indicating excellent goodness of fit. In terms of the stress measures, including normalised raw stress, stress-I, stress-II and S-stress, the reductions in stress in 3-D MDS outperformed the reductions in 2-D MDS by an average of 39.23%. With regards to S-stress, Dugard et al. (2010) suggested that S-stress values between (i) 0.05 and 0.099 and (ii) 0.025 and 0.049 indicate good and excellent performances, respectively. Thus, using 3-D MDS (with an S-stress value of 0.03754) to measure the differences between the observed similarity matrices is preferable to using 2-D MDS (with an S-stress value of 0.07130). Moreover, the dispersion accounted for (DAF) and Tucker's coefficient congruence were improved by approximately 2% when using the 3-D MDS, which indicates a high degree of similarity in the research studies. Therefore, it is appropriate to visualise the nine categories of the intellectual core in 3-D Cartesian space to examine their proximity graphically (Figure 7).

Table VI. Goodness of fit evaluation for 2-D and 3-D MDS

	2-D MDS	3-D MDS
Normalised raw stress	0.04661	0.02123
Stress-I	0.21588	0.14570
Stress-II	0.47007	0.36385
S-stress	0.07130	0.03754
Dispersion accounted for	0.95339	0.97877
Tucker's coefficient of congruence	0.97642	0.98933

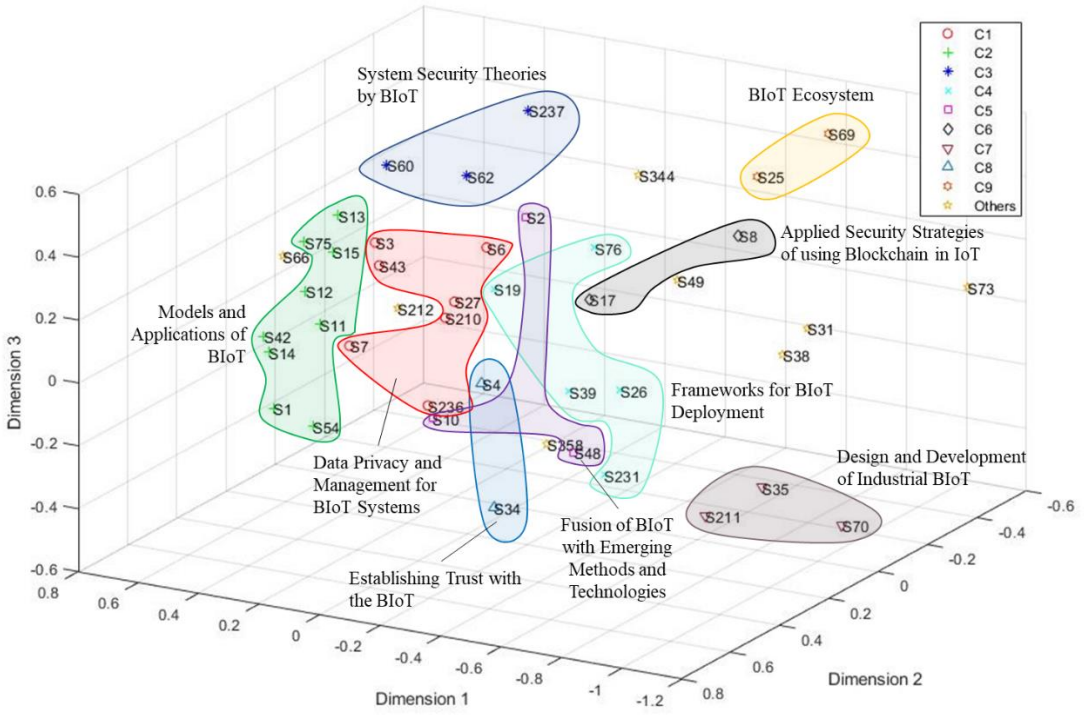

Figure 7. Graphical illustration of 3-D multidimensional scaling of the categories

5. Discussion and Future Directions for BIoT

In this section, we discuss the future directions for BIoT according to the categories of the intellectual core identified via the CPASR method. The highly influential research studies within each category are synthesised to formulate the trends and future directions in BIoT research.

5.1 Data Privacy and Management for BIoT Systems (C1)

The area of data privacy and management has drawn substantial attention. The concept of a decentralised access control framework for IoT authorisation was proposed to alleviate ethical and privacy problems for end users while granting them full control over their data (Ouaddah et al., 2016; Ouaddah et al., 2017; Cha et al., 2018). The secure management and access control of IoT devices can be strengthened through the deployment of digital signatures and smart contracts using blockchain. Only authorised IoT nodes can participate in decentralised networks, which can guarantee information accuracy and reliability. Also, BIoT can facilitate the secure sharing of data, resources and services between IoT devices, allowing the automation of industrial workflows (Biswas and Muthukkumarasamy, 2016; Christidis and Devetsikiotis, 2016). The decentralisation and immutability of BIoT can make the data within a network highly transparent and traceable. Consequently, the IoT's availability, reliability, fault tolerance capability, scalability and resilience can be enhanced to generate new business models and achieve digital transformations (Boudguiga et al., 2017; Sharma et al.,

2017). According to the research studies in this category, data privacy and management are the key concerns when deploying BIoT systems, yielding the following three primary directions and implications:

(i) Data authentication

BIoT systems provide a robust and secure mechanism for managing data created by IoT devices in the physical world to interconnect them with the digital world. However, the input of fake data cannot be effectively prevented with blockchain and IoT. Once fake data are forged in the blockchain, the blockchain's decentralisation and immutability help spread the fake data to the whole network. Data authentication, which is used to confirm the origin and integrity of data, is still under-researched. The data to be input into BIoT systems should be obtained from authorised entities, and the data's integrity should also be validated. Given modern IoT developments such as cyber-physical systems and digital twins, the authentication of data and products can be integrated to achieve comprehensive authentication in BIoT systems (Hammi et al., 2018; Alzahrani and Bulusu, 2020). Authenticated data can be established by identifying and verifying that physical objects possess their claimed identities. Consequently, the data accuracy of BIoT systems can be guaranteed for all BIoT applications.

(ii) Lightweight systems and vaporisation

Managing data in terms of size, frequency, and type requires balancing storage capabilities and completeness. Lightweight systems and vaporisation are two characteristics that are increasingly considered in system formulations (Tsang et al., 2019; Fu et al., 2020). A lightweight system stores only minimal data and their corresponding keys in the blockchain because the entire data payload can be stored in other permitted servers or the cloud. The lightweight approach can effectively shorten the time spent mining and forging blocks, which involves solving complex mathematical problems of varying difficulty levels. As a result, the practicality and adaptability of a system can be further enhanced by making it lightweight. In vaporisation, the data are separated from the blockchain applications and moved to the cloud for long-term storage and management once the blockchain's lifecycle ends. The resources and storage in the blockchain are thus released for managing incoming data and transactions.

(iii) Decentralised identity

To enhance access control in BIoT systems, a decentralised identity can be created for the objects (e.g. people and machines) involved in the system environment. All the events related to the objects can be recorded in decentralised systems to alleviate

problems arising from multiple identities for various IoT services, such as difficulties in event verification and data incompleteness (Bouras et al., 2020). Relatedly, Sousa et al. (2020) explored the potential of using blockchain for identity management in the context of IoT, evaluating the privacy and usability of practical systems. The concept of a decentralised identity can be further extended to applied research into industrial applications and theoretical studies on consensus algorithms. Such research can improve the self-ownership and censorship resistance of industrial systems, allowing trust to be built between the systems and their users.

5.2 Models and Applications of BIoT (C2)

To deploy BIoT technology for its intended purposes, several BIoT models have been formulated in various application domains. The level of blockchain involvement in IoT systems varies across three interaction types: IoT–IoT, IoT–blockchain and the hybrid approach (Huh et al., 2017; Zheng et al., 2017; Reyna et al., 2018). Recent research has shown that blockchain is a promising technology in the logistics, supply chain management, finance and healthcare industries (Erol et al., 2020). Blockchain has a data management role in IoT devices and services to ensure the practicality and adaptability of BIoT in various industries. It is not necessary to store all IoT data associated with real-time events in the blockchain. Thus, it is possible to achieve a configuration of system resources and requirements that leverages the benefits of the interaction of blockchain and the IoT. To demonstrate the applications of BIoT, some examples that combine blockchain and IoT are shown below. These examples may inspire further applications of BIoT in other domains.

(i) E-business and supply chain management

BIoT has converted the electronic business (e-business) model to a new IoT e-business model (Zhang and Wen, 2015; Zhang and Wen, 2017). The government–company–customer relationships in the traditional e-business environment have evolved into relationships between customers and decentralised autonomous corporations (DACs). The centralised control exerted by governments has been eliminated in the new IoT e-business model, in which DACs coordinate the trading of IoT data and commodities. In the new model, cryptocurrencies are used for transactions, and smart contracts define the relationships between DACs and customers. Consequently, the supply chain in the IoT e-business environment has been simplified and provides a secure connection between upstream and downstream stakeholders. Implementing BIoT in supply chain management can also strengthen transparency and traceability, facilitating the development of new business models (Zheng et al., 2018; Wong et al., 2020).

(ii) Healthcare

Shae and Tsai (2017) discuss the deployment of blockchain technology in medical decision-making to improve cost-effectiveness and patient care. They stress that the components related to data sharing, identities, data storage and computing paradigms should be emphasised in healthcare-related BIoT systems. Trusted datasets obtained through BIoT can enhance the reliability of decision-making and data analytics and guarantee the security of IoT wearables and devices. Moreover, Dwivedi et al. (2019) used blockchain technology to mitigate the privacy risks of wearable IoT technology for remote patient monitoring. Furthermore, blockchain technology in Internet of Healthcare Things enables the secure management and analysis of healthcare-related big data (Farouk et al., 2020). Patient anonymity, particularly regarding the use of IoT devices, can be maintained, and data transmission can be secured to establish advanced electronic medical records. In addition, Farahani et al. (2018) discuss the connection between the IoT and medical big data, arguing that the existing challenges of IoT in healthcare, (e.g. data management, scalability and security) may be overcome by integrating blockchain into the system architecture. Concerning data security, the decentralised feature is promising for managing heterogeneous medical data by facilitating interoperability between different healthcare platforms and workflows (Kaur and Alam, 2018).

(iii) Smart cities

Concerning the development of smart cities, Dorri et al. (2017) present a blockchain-based smart home framework for managing several smart devices securely and privately. Under the suggested framework, each smart home is assigned a cluster head, which is a smart home miner that can create and validate transactions regarding the smart home's activities. In addition, an overlay network is established to achieve communications between the cluster heads of smart homes. Another study developed a transparent and safe energy prosumer model featuring BIoT technology (Hwang et al., 2017). In this model, BIoT provides room to realise energy prosumer technology for lighting control, cooling and heating control, environmental monitoring and power monitoring. Finally, the energy efficiency of smart cities can be improved by analysing the energy usage patterns of households (Yahaya et al., 2020).

(iv) Device management

BIoT can also facilitate device management. Lee and Lee (2017) developed a remote firmware update scheme that utilises blockchain technology in the IoT environment. The latest firmware for IoT devices is shared in a decentralised peer-to-peer network that features secure checking and updating, thus maintaining firmware integrity.

Relatedly, Novo (2018) designed an access control architecture to manage IoT devices in a decentralised manner. Management hubs have been suggested as interfaces between IoT devices and blockchain nodes to manage tremendous amounts of real-time data from wireless sensor networks, thus striking a balance between computational resources and blockchain network effectiveness (Xiong et al., 2020). The authors also proposed that these management hubs control the permissions for lightweight nodes and miner nodes in the blockchain network to optimise hardware resources.

5.3 Frameworks for BIoT Deployment (C4)

Due to the rapid growth of BIoT technology, most research studies suggest their own deployment schemes and frameworks for achieving their designated purposes and needs. Thus, some studies in this category propose standardised protocols and frameworks for deployment, identifying their key components and elements. Stanciu (2017) implemented the IEC61499 standard for the integration of blockchain and IoT technologies to create a distributed control system through the use of function blocks and service interface function blocks. The standard coordinates data transmission and function execution between edge nodes and cloud services. Liu et al. (2017) constructed a framework for a blockchain-enabled data integrity service designed to connect data owner applications and data consumer applications in the cloud environment. The authors formulated protocols for using BIoT to execute data integrity verifications in cloud storage services. In another study, blockchain's presence in IoT systems boosted the development of peer-to-peer (P2P) networks, and the P2P cloud became a promising data management paradigm (Conoscenti et al., 2017). Considering BIoT deployment in real-life business environments, Kshetri (2018) developed six strategic objectives for building BIoT solutions: cost, speed, dependability, risk reduction, sustainability and flexibility. These objectives represent explicit benefits for industries, such as supply chain management. Zhou et al. (2018) proposed a threshold secure multi-party computing protocol for BIoT systems to perform homomorphic computations on data, with the additional advantage that external computing resources could be used to enhance system performance. The above studies demonstrate essential elements and considerations for frameworks and protocols, demonstrating that the IoT's service-oriented (or layered) architecture can be modified with blockchain elements. Figure 8 shows that the service-oriented architecture for BIoT is formulated with five layers: perception, network, decentralisation, service and access. Physical objects and users (i.e. the system nodes) are connected to the digital system in the perception layer, while data transmission proceeds through wireless communication technologies and machine-to-machine (M2M) communication protocols. In the decentralisation layer, the P2P network is established via a consensus algorithm, verification mechanism, smart

contracts and a distributed system. The IoT platform and hybridisation of the cloud databases are formulated in the service layer to create BIoT applications. Ultimately, the access layer controls user privileges for the P2P network and defines whether a public, consortium or private blockchain is used (Du et al., 2020).

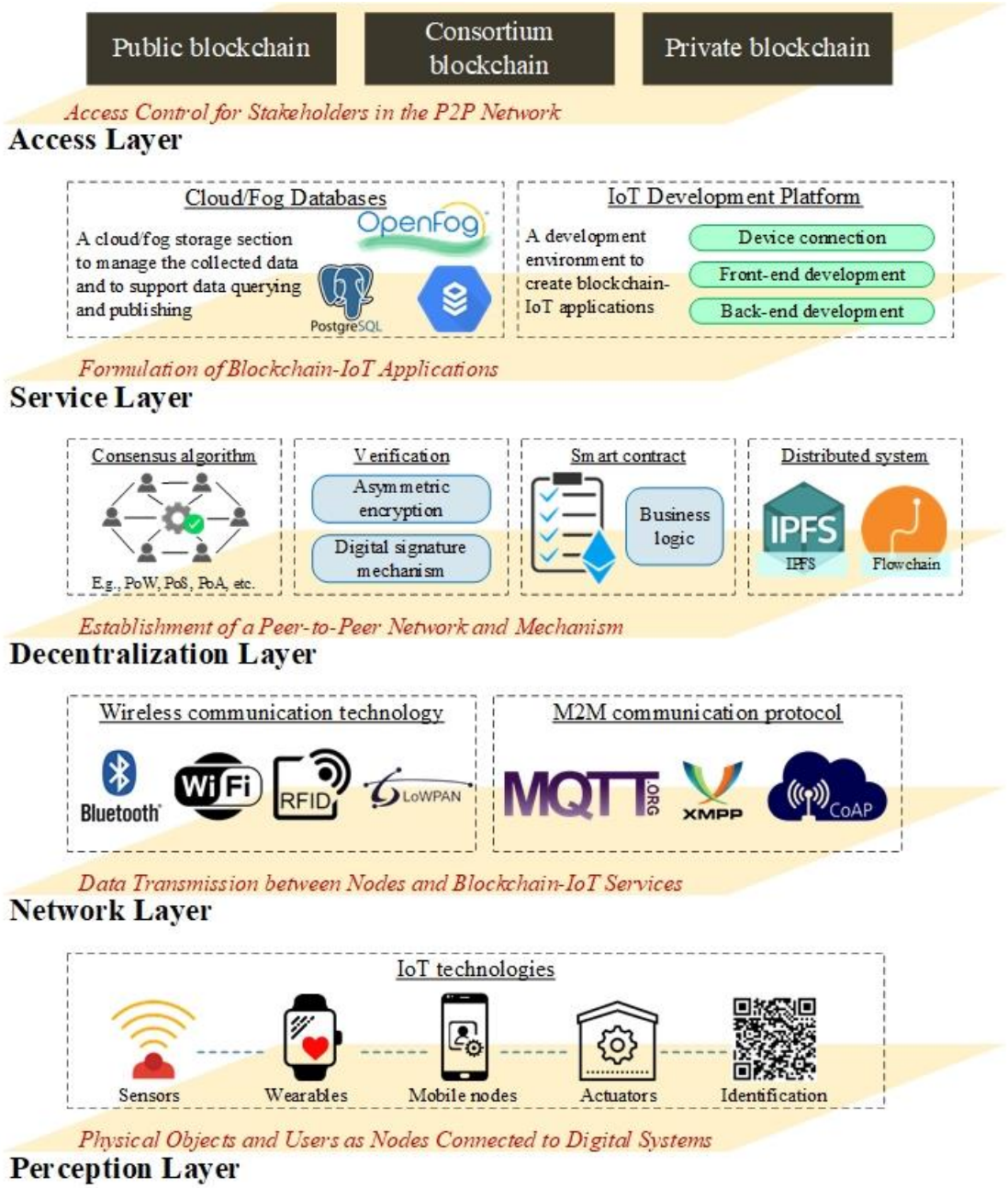

Figure 8. Service-oriented architecture for BIoT.

5.4 Fusion of BIoT with Emerging Methods and Technologies (C5)

With respect to the interaction of blockchain and the IoT, Reyna et al. (2018) observe that a hybrid approach featuring fog and cloud computing can leverage the advantages of blockchain and real-time IoT interactions. In this approach, only a small portion of

the interactions and data are managed in the blockchain, while the rest are shared in the IoT environment. The fusion of BIoT with emerging methods and technologies was motivated by novel business models, such as smart homes, smart cities and the sharing economy (Sun et al., 2016; Xu et al., 2017). This technological fusion provides additional synergies and strengthens the capabilities of BIoT. Outchakoucht et al. (2017) combined BIoT with a reinforcement learning algorithm (a type of machine learning method) to develop a dynamic, optimised and self-adjusted security policy. As a result, the flexibility and adaptability of smart contracts can be improved to suggest appropriate actions based on environmental states and reinforcement weights. Hwang et al. (2017) proposed an integrated platform involving IoT, blockchain, cloud computing and big data for an energy prosumer application. Larson and Chang (2016) synthesised agile principles with business intelligence and data science; they found that the entire agile business intelligence delivery framework can be strengthened through the deployment of BIoT. Yang et al. (2019) explored IoT-based healthcare big data with privacy-preserving and self-adaptive characteristics. The possibility of deploying a robust smart deduplication mechanism was explored for big data applications. Under a hybrid environment, big data is used to analyse the data and interactions stored in the cloud with techniques such as text mining, opinion mining, social network analytics and cluster analysis. This approach could be extended to other methods and techniques such as artificial intelligence (AI) and optimisation to enhance system functionalities and capabilities for industrial purposes. In the future, additional 'intelligence' can be embedded in BIoT applications; for example, smart contracts can become intelligent enough to execute decision-making functions in response to environmental states.

5.5 System Security Theories for BIoT (C3)

System security theories used to address cybersecurity concerns can be improved by integrating blockchain with IoT. Hammi et al. (2018) suggested a robust identification and authentication system to create secure virtual zones in the IoT environment, thus creating a security model, i.e. "bubble of trust". IoT devices can communicate securely in the P2P network in public blockchain applications using threat models designed to eliminate malicious nodes. Enhancements in real-time interactions, initialisation and cryptocurrency mechanisms can improve security models. Sharma and Park (2018) formulated a blockchain-based hybrid network architecture for sustainable development comprising core and edge networks; the architecture addresses existing challenges including high latency, bandwidth bottlenecks, security, privacy and scalability in a smart city network. The core network executes the blockchain mechanism in a decentralised manner through mining and verification, while the edge network manages various services in a centralised way. The raw data collected in the

edge network from IoT devices are forged into blocks in the core network to ensure the smart city network's security. Jesus et al. (2018) summarise the methodologies used to provide security and privacy for BIoT. BIoT is resistant to typical attack modes and threat models, as enormous computational power is required for attacks. However, stalker attacks, which benefit from hindering the verifications of blocks, should also be considered. Even though stalker attackers cannot directly benefit from the BIoT network, broken transactions and business relationships may affect businesses in other ways, such as mergers and acquisitions (M&A) and company reputation. It was found that stalker attacks can be alleviated by increasing the target hash power. With a higher target hash power, more blocks are published to create more forks in the network, making it difficult for attackers to create the same number of blocks. In the future, additional attack modes involving consensus algorithms and verification processes can be researched to strengthen BIoT system security theories.

5.6 Applied Security Strategies for Using Blockchain in IoT (C6)

Based on the security theories for BIoT, security strategies and policies can be formulated to generate impacts on the various application domains. Kshetri (2017) summarises blockchain's role in enhancing cybersecurity and privacy protection in the healthcare industry and supply chain management. When integrated with the IoT, blockchain-based security strategies can facilitate the interoperability of medical data and can be extended to electronic healthcare records (eHRs). In such a system, patients can control their own data, and changes in their medical records are transparent and traceable within the network. A new culture for addressing the privacy, security and integrity of healthcare data should be investigated in future studies. Similarly, BIoT plays an essential role in enhancing security for both upstream and downstream supply chain parties. More importantly, item ownership and traceability changes can be achieved independently while fostering trust in the supply chain network. Fair information practices (FIPs) have also been investigated (particularly in the big data environment) to provide transparency, security, individual participation and accountability. Furthermore, Ahram et al. (2017) illustrated agile value chains, faster product innovations and effective customer relationships for multiple industrial applications, developing a corresponding health chain. BIoT can also be used to address many cybersecurity concerns. For instance, the lifecycle of protected health information (PHI) in a healthcare network can be monitored, and PHI records can be consolidated in a decentralised network for better traceability and security. In the future, both financial and non-financial industries (e.g. industrial manufacturing) can benefit from the security strategies developed on the basis of BIoT.

5.7 Design and Development of Industrial BIoT (C7)

Some authors have researched industrial applications and industrial IoT (IIoT), which is regarded as the evolution of the distributed control system, to automate and optimise industrial processes. Teslya (2017) foresees the industrial revolution beyond industry 4.0 in terms of integrating the IIoT and blockchain to form the industrial BIoT. This integration should strengthen security, fault tolerance, durability, public accessibility and consensus, all of which are shortcomings of current IIoT applications. In addition, blockchain should support business process management, in which manufacturing steps and processes are controlled and optimised (Xu et al., 2018). The increase in BIoT use has also proven that blockchain's role in industry 4.0 is to promote resilience, scalability, security and autonomy. The suggested primary foci for industrial BIoT development are as follows:

(i) Emerging paradigms for BIoT

The concept of overlay has been proposed to connect multiple blockchain systems. Overlay generates a global P2P network in accordance with the distributed architecture (Dorri et al., 2017). It is particularly essential in cyber-physical systems for the construction of inter-network communications, allowing the cluster heads of local blockchains to communicate with each other to create a global blockchain environment (Griggs et al., 2018). When industrial BIoT facilitates the recording and sharing of data related to physical objects and processes in the digital world, digital twins (real-time digital replicas) can be created for modelling, prognostics and diagnostics in industrial scenarios (Hasan et al., 2020).

(ii) Consensus algorithms

Since blockchain was created to handle cryptocurrency, several well-known consensus algorithms were developed for financial applications, including the proof of work (PoW), proof of stake (PoS) and practical Byzantine fault tolerance (pBFT) algorithms, (Nguyen and Kim, 2018). Consensus algorithms should be customised according to industries' unique characteristics in order to reach mutual agreement among all peers in industrial scenarios. Instead of providing incentives to peers, stakeholders should sustain blockchain applications through block forging and validation, which is of the utmost importance for establishing trust in P2P networks. Therefore, novel consensus algorithms should be developed or selected to encourage stakeholder participation and maintain network sustainability (Lao et al., 2020).

5.8 Establishing Trust With BIoT (C8)

Building trust is one of BIoT's most valuable benefits. Blockchain provides the advantages of high security and immutability, as records can be verified in a distributed P2P network (Singh and Singh, 2016; Lin et al., 2017). Since published blocks are difficult to modify, data stored in the blockchain is trustworthy. Although a 51% attack on a blockchain may be a threat, a group of malicious nodes must control more than 50% of a network's power, such as computational resources (PoW) or wealth (PoS). The threshold to perform a 51% attack is relatively high, particularly in a large-scale permissionless blockchain application. As a result, trust is gradually established in a trustless decentralised network, where consensus algorithms and blockchain protocols are two crucial elements used to foster trust. For the permissioned blockchain, trust between stakeholders and systems can be sustained to establish a culture of collaboration within a P2P network. If malicious nodes create fake data that could damage the trustworthiness of permissioned BIoT systems, such nodes are removed from the network to ensure a positive culture in the BIoT environment. In future, a scheme should be proposed to support trust delegation without breaching security and privacy concerns (Yu et al., 2018b). Yang et al. (2018) introduced decentralised trust management in the Internet of vehicles, calculating trust value offsets for the messages sent by vehicles in order to generate the next blocks. This technique effectively assesses IoT devices' credibility for the establishment of a safe and reliable P2P network. She et al. (2019) designed a blockchain trust model to detect malicious nodes in wireless sensor networks, embedding a consortium blockchain for quadrilateral measurement and localisation. The malicious nodes were determined by considering the node states, processing delay, forwarding rate and response time. In general, human-centric trust models in IoT can be developed to provide effective data security and privacy in P2P networks, in which security risks can be mitigated through proper strategies and policies.

5.9 BIoT Ecosystem (C9)

Numerous BIoT studies propose ecological designs to support the development of software sustainability and eco-innovation. Samaniego and Deters (2017) suggest improving autonomous IoT (AIoT) via blockchain while complying with the principles of self-configuration, self-optimisation, self-healing and self-protection. The authors formulated a permission-based protocol to manage real-time transmissions in the AIoT environment. Yu et al. (2018b) examined several ways that blockchain changes the IoT ecosystem; the authors see it as a new data-sharing model that eliminates the challenges of trust, communication, cost and ownership. More importantly, the use of blockchain eliminates single points of failure in the BIoT ecosystem, while blockchain nodes can be synchronised regularly to detect any malicious nodes in the network (Lockl et al.,

2020). Moreover, Siegfried et al. (2020) suggested six dimensions to map the blockchain technology on the industrial IoT: performance, reliability, IT security, scalability, compatibility and adaptability. Figure 9 depicts a BIoT ecosystem that summarises the essential elements of this study. Based on the solid foundation of blockchain and IoT technologies, BIoT covers a wide range of features, including decentralisation, immutability, autonomy, scalability, trust, security, privacy, durability, access control and fault tolerance. In addition, emerging methods (e.g. AI, business intelligence, big data analytics and optimisation) and technologies (e.g. digital twins, cyber-physical systems (CPSs), the physical Internet and 5G) can be synthesised in BIoT to establish designated platforms for the industries discussed in this paper. Furthermore, BIoT has the potential to be applied to aviation, government, media and entertainment (Abeyratne, 2020; Chen et al., 2020; Geneiatakis et al., 2020). The benefits from various emerging technologies can be leveraged in the BIoT environment to add value for the market and customers, as the features of decentralisation and real-time connection can be embedded in specific solutions and services. With the extensive development of data, technologies and analytical methodologies leading the digital revolution, eco-sustainable innovations in the BIoT services can be developed further through its standardised service-oriented architecture. As a result, these technologies promise a new era for information systems and advanced technological development.

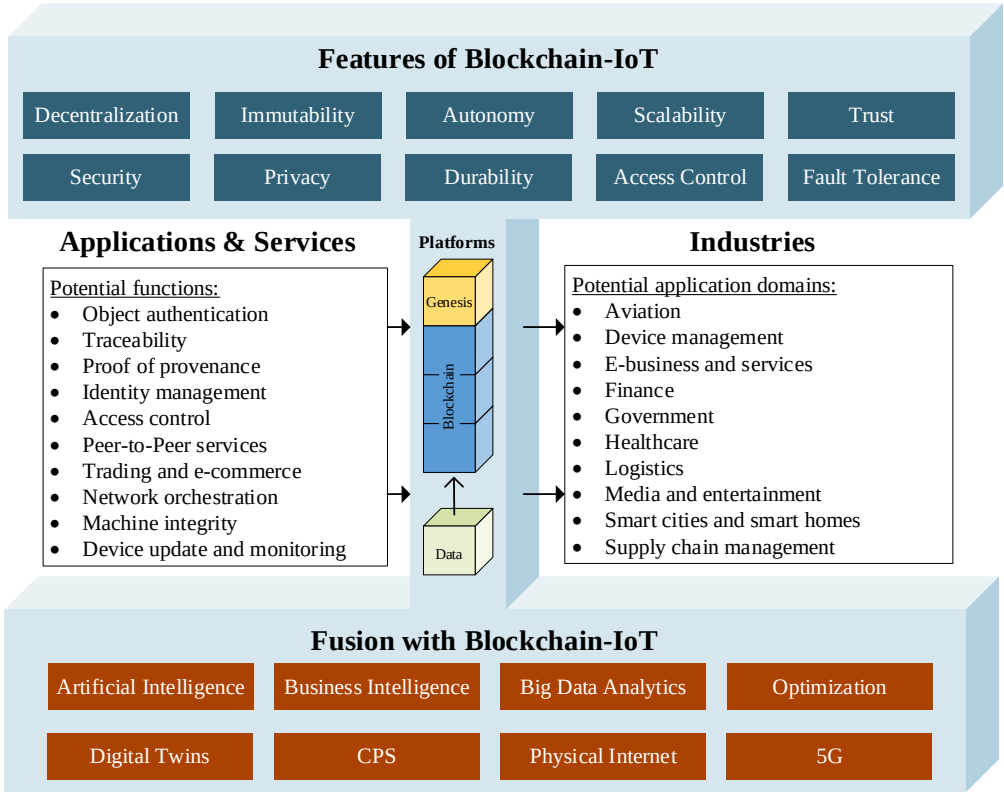

Figure 9. BIoT ecosystem.

6. Concluding Remarks

To conclude, we address the two research questions posed in Section 1. First, we have successfully developed the CPASR method to examine the intellectual core of BIoT, which is an under-researched and topical area. Citation analysis, co-citation proximity analysis and a series of statistical analyses are integrated as a whole in the CPASR method. Second, we applied the structured CPASR method to investigate 44 highly influential research studies, identifying nine categories that describe the trends and implications of BIoT. This study contributes to near-future R&D by providing foundations and future directions for new BIoT paradigms and applications. In short, this study introduces the CPASR method, which integrates citation analysis, co-citation proximity analysis and a series of statistical analyses to examine the intellectual cores of the designated knowledge domain. Moreover, the CPASR method is applied to identify nine intellectual cores of BIoT, which is an under-researched but topical area in the context of information management, to support the future research directions in the field of BIoT, as follows:

a. **BIoT Design and Deployment:** The core objectives for implementing blockchain in IoT systems are to enhance data security and privacy by effectively managing IoT devices. Therefore, it is necessary to develop a customised BIoT deployment scheme that considers blockchain protocols, the design of consensus algorithms, security strategies, system architectures and data management to strengthen frameworks in the Internet of Everything (IoE).

b. **Novel BIoT Applications:** Apart from enriching BIoT implementations in finance, healthcare and supply chain management, BIoT can be deployed in various industries, such as aviation, government, logistics engineering, media and entertainment. Such applications leverage the benefits of trust establishment from the decentralisation and P2P network, enhancing data privacy and security. The novel applications can also boost technological development globally in an eco-sustainable manner.

c. **Fusion with Emerging Aspects:** BIoT consolidates the frameworks for IoT data exchange in P2P networks, improving data integrity and reliability. It also strengthens the capabilities of AI and data analytics under BIoT architecture. Instead of formulating standalone AI or data analytics models, improving data availability for model training and validation can foster collaboration between existing models to create an industrywide solution.

This study is limited to a five-year timeframe from 2015 to 2019, as the development of BIoT is still in a preliminary stage. The number of research studies and citations are expected to grow rapidly within the decade. In future, the CPASR method can be used to examine the intellectual structure for BIoT again (e.g. using a ten-year timeframe) to validate and amend the intellectual cores. Moreover, the proposed CPASR method can also be applied to examine the intellectual structure of other knowledge domains.

References:

Abeyratne, R. (2020). Blockchain and Aviation. In *Aviation in the Digital Age* (pp. 109-120). Springer, Cham.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B. (2017), "Blockchain technology innovations", In *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, IEEE, pp. 137-141.

Alladi, T., Chamola, V., Parizi, R. M. and Choo, K. K. R. (2019), "Blockchain applications for industry 4.0 and industrial IoT: A review", *IEEE Access*, Vol. 7, pp. 176935-176951.

Alzahrani, N. and Bulusu, N. (2020), "A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol", *Concurrency and Computation: Practice and Experience*, Vol. 32 No. 12 e5232. doi: 10.1002/cpe.5232.

Aromataris, E., Fernandez, R., Godfrey, C. M., Holly, C., Khalil, H. and Tungpunkom, P. (2015), "Summarizing systematic reviews: methodological development, conduct and reporting of an umbrella review approach", *International journal of evidence-based healthcare*, Vol. 13 No. 3, pp. 132-140.

Banerjee, M., Lee, J. and Choo, K. K. R. (2018), "A blockchain future for internet of things security: a position paper", *Digital Communications and Networks*, Vol. 4 No. 3, pp. 149-160.

Biswas, K. and Muthukkumarasamy, V. (2016), "Securing smart cities using blockchain technology", In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems*, IEEE, pp. 1392-1393.

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

Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H. (2020), "Distributed ledger technology for eHealth identity privacy: State of the art and future

perspective", *Sensors*, Vol. 20 No. 2. doi: 10.3390/s20020483.

Burton-Jones, A., Akhlaghpour, S., Ayre, S., Barde, P., Staib, A. and Sullivan, C. (2020), "Changing the conversation on evaluating digital transformation in healthcare: Insights from an institutional analysis", *Information and Organization*, Vol. 30, No. 1. doi: 10.1016/j.infoandorg.2019.100255

Cha, S. C., Chen, J. F., Su, C. and Yeh, K. H. (2018), "A blockchain connected gateway for BLE-based devices in the internet of things", *IEEE Access*, Vol. 6, pp. 24639-24649.

Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M. and Al Ridhawi, I. (2020), "An incentive-aware blockchain-based solution for internet of fake media things", *Information Processing & Management*, Vol. 57 No. 6, 102370.

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J. and Sarda, P. (2018), "Blockchain versus database: a critical analysis", In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering*, IEEE, 1348-1353.

Christidis, K. and Devetsikiotis, M. (2016), "Blockchains and smart contracts for the internet of things", *IEEE Access*, Vol. 4, pp. 2292-2303.

Clarivate Analytics. (2020), "Web of Science: Summary of Coverage", available at: https://clarivate.libguides.com/webofscienceplatform/coverage (accessed 15 July 2020)

Conoscenti, M., Vetro, A. and De Martin, J. C. (2017), "Peer to Peer for Privacy and Decentralization in the Internet of Things", In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion*, IEEE, 288-290.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016), "Blockchain technology: Beyond bitcoin", *Applied Innovation*, Vol. 2, pp. 6-19.

Dorri, A., Kanhere, S. S., Jurdak, R. and Gauravaram, P. (2017), "Blockchain for IoT security and privacy: The case study of a smart home", In *2017 IEEE international conference on pervasive computing and communications workshops*, IEEE, 618-623.

Du, M., Wang, K., Liu, Y., Qian, K., Sun, Y., Xu, W. and Guo, S. (2020), "Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security", *IEEE Wireless Communications*, Vol. 27 No. 3, pp. 38-45.

Dugard, P., Todman, J. and Staines, H. (2010), *Approaching multivariate analysis: A practical introduction*. Routledge/Taylor & Francis Group.

Dwivedi, A. D., Srivastava, G., Dhar, S. and Singh, R. (2019), "A decentralized privacy-preserving healthcare blockchain for IoT", *Sensors*, Vol. 19, No. 2. doi: 10.3390/s19020326.

Erol, I., Ar, I. M., Ozdemir, A. I., Peker, I., Asgary, A., Medeni, I. T., & Medeni, T. (2020). Assessing the feasibility of blockchain technology in industries: evidence from Turkey. *Journal of Enterprise Information Management*. DOI: 10.1108/JEIM-09-2019-0309.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N. and Mankodiya, K. (2018), "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare", *Future Generation Computer Systems*, Vol. 78, pp. 659-676.

Farouk, A., Alahmadi, A., Ghose, S. and Mashatan, A. (2020), "Blockchain platform for industrial healthcare: Vision and future opportunities", *Computer Communications*, Vol. 154, pp. 223-235.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L. and Janicke, H. (2018), "Blockchain technologies for the internet of things: Research issues and challenges", *IEEE Internet of Things Journal*, Vol. 6 No. 2, pp. 2188-2204.

Fu, J., Wang, N. and Cai, Y. (2020), "Privacy-Preserving in Healthcare Blockchain Systems Based on Lightweight Message Sharing", *Sensors*, Vol. 20 No. 7. doi: 10.3390/s20071898.

Geneiatakis, D., Soupionis, Y., Steri, G., Kounelis, I., Neisse, R. and Nai-Fovino, I. (2020), "Blockchain Performance Analysis for Supporting Cross-Border E-Government Services", *IEEE Transactions on Engineering Management*, Vol. 67 No. 4, pp. 1310-1322.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A. and Hayajneh, T. (2018), "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring", *Journal of medical systems*, Vol. 42. doi:10.1007/s10916-018-0982-x.

Hammi, M. T., Hammi, B., Bellot, P. and Serhrouchni, A. (2018), "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT", *Computers & Security*, Vol. 78, pp. 126-142.

Hasan, H. R., Salah, K., Jayaraman, R., Omar, M., Yaqoob, I., Pesic, S., Taylor, T. and Boscovic, D. (2020), "A Blockchain-Based Approach for the Creation of Digital Twins", *IEEE Access*, Vol. 8, pp. 34113-34126.

Hausberg, J. P. and Korreck, S. (2020), "Business incubators and accelerators: a co-citation analysis-based, systematic literature review", *The Journal of Technology Transfer*, Vol. 45 No. 1, pp. 151-176.

Hayes, A. F. and Krippendorff, K. (2007), "Answering the call for a standard reliability measure for coding data", *Communication methods and measures*, Vol. 1 No. 1, pp. 77-89.

Hug, S. E., Ochsner, M. and Brändle, M. P. (2017), "Citation analysis with microsoft

academic", *Scientometrics*, Vol. 111 No. 1, pp. 371-378.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V. and Akella, V. (2019), "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda", *International Journal of Information Management*, Vol. 49, pp. 114-129.

Huh, S., Cho, S. and Kim, S. (2017), "Managing IoT devices using blockchain platform", In *2017 19th international conference on advanced communication technology*, IEEE, pp. 464-467.

Hwang, J., Choi, M. I., Lee, T., Jeon, S., Kim, S., Park, S. and Park, S. (2017), "Energy prosumer business model using blockchain system to ensure transparency and safety", *Energy Procedia*, Vol. 141, pp. 194-198.

Jesus, E. F., Chicarino, V. R., de Albuquerque, C. V. and Rocha, A. A. D. A. (2018), "A survey of how to use blockchain to secure internet of things and the stalker attack", *Security and Communication Networks*, Vol. *2018*. doi: 10.1155/2018/9675050.

Joshi, A. P., Han, M. and Wang, Y. (2018), "A survey on security and privacy issues of blockchain technology", *Mathematical Foundations of Computing*, Vol. 1 No. 2, pp. 121-147.

Karafiloski, E. and Mishev, A. (2017), "Blockchain solutions for big data challenges: A literature review", In *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, IEEE, pp. 763-768.

Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K. and Chang, V. (2018), "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment", *Journal of medical systems*, Vol. 42 No. 156, pp. 1-11.

Khangura, S., Konnyu, K., Cushman, R., Grimshaw, J. and Moher, D. (2012), "Evidence summaries: the evolution of a rapid review approach", *Systematic reviews*, Vol. 1, pp. 10. doi: 10.1186/2046-4053-1-10.

Khan, M. A. and Salah, K. (2018), "IoT security: Review, blockchain solutions, and open challenges", *Future Generation Computer Systems*, Vol. 82, pp. 395-411.

Kim, H. J., Jeong, Y. K. and Song, M. (2016), "Content-and proximity-based author co-citation analysis using citation sentences", *Journal of Informetrics*, Vol. 10 No. 4, pp. 954-966.

Koo, T. K. and Li, M. Y. (2016), "A guideline of selecting and reporting intraclass correlation coefficients for reliability research", *Journal of chiropractic medicine*, Vol. 15 No. 2, pp. 155-163.

Kshetri, N. (2017), "Blockchain's roles in strengthening cybersecurity and protecting privacy", *Telecommunications policy*, Vol. 41 No. 10, pp. 1027-1038.

Kshetri, N. (2018), "1 Blockchain's roles in meeting key supply chain management

objectives", *International Journal of Information Management*, Vol. 39, pp. 80-89.

Lade, P., Ghosh, R. and Srinivasan, S. (2017), "Manufacturing analytics and industrial internet of things", *IEEE Intelligent Systems*, Vol. 32 No. 3, pp. 74-79.

Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S. and Yang, Y. (2020), "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling", *ACM Computing Surveys*, Vol. 53 No. 1. doi: 10.1145/3372136.

Larson, D. and Chang, V. (2016), "A review and future direction of agile, business intelligence, analytics and data science", *International Journal of Information Management*, Vol. 36 No. 5, pp. 700-710.

Lee, B. and Lee, J. H. (2017), "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment", *The Journal of Supercomputing*, Vol. 73 No. 3, pp. 1152-1167.

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N. and Harth, N. (2020), "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications", *IEEE Transactions on Engineering Management*. doi: TEM.2020.2978014.

Lin, J., Shen, Z. and Miao, C. (2017), "Using blockchain technology to build trust in sharing LoRaWAN IoT", In *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, ACM, 38-43.

Lin, I. C. and Liao, T. C. (2017), "A survey of blockchain security issues and challenges", *IJ Network Security*, Vol. 19 No. 5, pp. 653-659.

Liu, B., Yu, X. L., Chen, S., Xu, X. and Zhu, L. (2017), "Blockchain based data integrity service framework for IoT data", In *2017 IEEE International Conference on Web Services*, IEEE, pp. 468-475.

Mair, P., Borg, I. and Rusch, T. (2016), "Goodness-of-fit assessment in multidimensional scaling and unfolding", *Multivariate behavioral research*, Vol. 51 No. 6, pp. 772-789.

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A. and Aromataris, E. (2018), "Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach", *BMC medical research methodology*, Vol. 18 No. 143. doi: 10.1186/s12874-018-0611-x.

Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system", available at: https://bitcoin.org/bitcoin.pdf (accessed July 15 2020)

Ng, C. K., Wu, C. H., Yung, K. L., Ip, W. H. and Cheung, T. (2018), "A semantic similarity analysis of Internet of Things", *Enterprise Information Systems*, Vol. 12 No. 7, pp. 820-855.

Nguyen, G. T. and Kim, K. (2018), "A Survey about Consensus Algorithms Used in Blockchain", *Journal of Information processing systems*, Vol. 14, pp. 101-128.

Nord, J. H., Koohang, A. and Paliszkiewicz, J. (2019), "The Internet of Things: Review and theoretical framework", *Expert Systems with Applications*, Vol. 133, pp. 97-108.

Novo, O. (2018), "Blockchain meets IoT: An architecture for scalable access management in IoT", *IEEE Internet of Things Journal*, Vol. 5 No. 2, pp. 1184-1195.

Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A. (2016), "FairAccess: a new Blockchain-based access control framework for the Internet of Things", *Security and Communication Networks*, Vol. 9 No. 18, pp. 5943-5964.

Ouaddah, A., Elkalam, A. A. and Ouahman, A. A. (2017), "Towards a novel privacy-preserving access control model based on blockchain technology in IoT", In *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Springer, Cham, pp. 523-533.

Outchakoucht, A., Hamza, E. S. and Leroy, J. P. (2017), "Dynamic access control policy based on blockchain and machine learning for the internet of things", *International Journal of Advanced Computer Science and Applications*, Vol. 8 No. 7, pp. 417-424.

Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A. (2018), "Blockchain and iot integration: A systematic survey" *Sensors*, Vol. 18 No. 8. doi: 10.3390/s18082575.

Papert, M. and Pflaum, A. (2017), "Development of an ecosystem model for the realization of internet of things (IoT) services in supply chain management", *Electronic Markets*, Vol. 27 No. 2, pp. 175-189.

Paré, G. and Kitsiou, S. (2017), "Methods for literature reviews", In *Handbook of eHealth Evaluation: An Evidence-based Approach*. University of Victoria.

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. (2018), "On blockchain and its integration with IoT. Challenges and opportunities", *Future generation computer systems*, Vol. 88, pp. 173-190.

Samaniego, M. and Deters, R. (2017), "Internet of smart things-iost: Using blockchain and clips to make things autonomous", In *2017 IEEE international conference on cognitive computing*, IEEE, pp. 9-16.

Shae, Z. and Tsai, J. J. (2017), "On the design of a blockchain platform for clinical trial and precision medicine", In *2017 IEEE 37th International Conference on Distributed Computing Systems*, IEEE, pp. 1972-1980.

Sharma, P. K., Chen, M. Y. and Park, J. H. (2017), "A software defined fog node based distributed blockchain cloud architecture for IoT", *IEEE Access*, Vol. 6, pp. 115-124.

Sharma, P. K. and Park, J. H. (2018), "Blockchain based hybrid network architecture for the smart city", *Future Generation Computer Systems*, Vol. 86, pp. 650-655.

She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B. and Liu, W. (2019), "Blockchain trust model for malicious node detection in wireless sensor networks", *IEEE Access*, Vol. 7, pp. 38947-38956.

Shiau, W. L., Yan, C. M. and Lin, B. W. (2019), "Exploration into the intellectual structure of mobile information systems", *International Journal of Information Management*, Vol. 47, pp. 241-251.

Siegfried, N., Rosenthal, T., & Benlian, A. (2020). Blockchain and the Industrial Internet of Things. *Journal of Enterprise Information Management*. DOI: 10.1108/JEIM-06-2018-0140.

Singh, S. and Singh, N. (2016), "Blockchain: Future of financial and cyber security", In *2016 2nd international conference on contemporary computing and informatics*, IEEE, pp. 463-467.

Sousa, P. R., Resende, J. S., Martins, R., & Antunes, L. (2020). The case for blockchain in IoT identity management. *Journal of Enterprise Information Management*. DOI: 10.1108/JEIM-07-2018-0148.

Stanciu, A. (2017), "Blockchain based distributed control system for edge computing", In *2017 21st International Conference on Control Systems and Computer Science*, IEEE, pp. 667-671.

Sun, J., Yan, J. and Zhang, K. Z. (2016), "Blockchain-based sharing services: What blockchain technology can contribute to smart cities", *Financial Innovation*, Vol. 2, pp. 26. doi: 10.1186/s40854-016-0040-y.

Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S. and Lam, H. Y. (2019), "Blockchain-driven IoT for food traceability with an integrated consensus mechanism", *IEEE Access*, Vol. 7, pp. 129000-129017.

Teslya, N. and Ryabchikov, I. (2017), "Blockchain-based platform architecture for industrial IoT", In *2017 21st Conference of Open Innovations Association*, IEEE, 321-329.

Viriyasitavat, W., Da Xu, L., Bi, Z. and Hoonsopon, D. (2019), "Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective", *IEEE Internet of Things Journal*, Vol. 6 No. 5, pp. 8155-8168.

Wang, Q., Zhu, X., Ni, Y., Gu, L. and Zhu, H. (2020), "Blockchain for the IoT and industrial IoT: A review", *Internet of Things*, Vol. 10, pp. 100081.

Wang, N., Liang, H., Jia, Y., Ge, S., Xue, Y. and Wang, Z. (2016), "Cloud computing research in the IS discipline: A citation/co-citation analysis", *Decision Support Systems*, Vol. 86, pp. 35-47.

Wong, L. W., Tan, G. W. H., Lee, V. H., Ooi, K. B. and Sohal, A. (2020), "Unearthing the determinants of Blockchain adoption in supply chain management", *International Journal of Production Research*, Vol. 58 No. 7, pp.

2100-2123.

Wortmann, F. and Flüchter, K. (2015), "Internet of things", *Business & Information Systems Engineering*, Vol. 57 No. 3, pp. 221-224.

Xiong, Z., Zhang, Y., Luong, N. C., Niyato, D., Wang, P. and Guizani, N. (2020), "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things", *IEEE Network*, Vol. 34 No. 1, pp. 166-173.

Xu, L. D., Xu, E. L. and Li, L. (2018), "Industry 4.0: state of the art and future trends", *International Journal of Production Research*, Vol. 56 No. 8, pp. 2941-2962.

Xu, L., Shah, N., Chen, L., Diallo, N., Gao, Z., Lu, Y. and Shi, W. (2017), "Enabling the sharing economy: Privacy respecting contract based on public blockchain", In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, ACM, pp. 15-21.

Yaghtin, M., Sotudeh, H., Mirzabeigi, M., Fakhrahmad, S. M. and Mohammadi, M. (2019), "In quest of new document relations: evaluating co-opinion relations between co-citations and its impact on Information retrieval effectiveness", *Scientometrics*, Vol. 119 No. 2, pp. 987-1008.

Yahaya, A. S., Javaid, N., Alzahrani, F. A., Rehman, A., Ullah, I., Shahid, A. and Shafiq, M. (2020), "Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism", *Sustainability*, Vol. 12 No. 8. doi: 10.3390/su12083385.

Yang, Y., Zheng, X., Guo, W., Liu, X. and Chang, V. (2019), "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system", *Information Sciences*, Vol. 479, pp. 567-592.

Yang, Z., Yang, K., Lei, L., Zheng, K. and Leung, V. C. (2018), "Blockchain-based decentralized trust management in vehicular networks", *IEEE Internet of Things Journal*, Vol. 6 No. 2, pp.1495-1505.

Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J. and Ranjan, R. (2018a), "Trust chain: Establishing trust in the iot-based applications ecosystem using blockchain", *IEEE Cloud Computing*, Vol. 5 No. 4, pp. 12-23.

Yu, Y., Li, Y., Tian, J. and Liu, J. (2018b), "Blockchain-based solutions to security and privacy issues in the Internet of Things", *IEEE Wireless Communications*, Vol. 25 No. 6, pp. 12-18.

Zhang, Y. and Wen, J. (2015), "An IoT electric business model based on the protocol of bitcoin", In *2015 18th international conference on intelligence in next generation networks*, IEEE, pp. 184-191.

Zhang, Y. and Wen, J. (2017), "The IoT electric business model: Using blockchain technology for the internet of things", *Peer-to-Peer Networking and Applications*,

Vol. 10 No. 4, pp. 983-994.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017), "An overview of blockchain technology: Architecture, consensus, and future trends", In *2017 IEEE international congress on big data*, IEEE, 557-564.

Zheng, Z., Xie, S., Dai, H. N., Chen, X. and Wang, H. (2018), "Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services*, Vol. 14 No. 4, pp. 352-375.

Zhou, L., Wang, L., Sun, Y. and Lv, P. (2018), "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation", *IEEE Access*, Vol. 6, pp. 43472-43488.