Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18931-4

Blockchain-enabled Smart Contracts and the Internet of Things: Advancing the research agenda through a narrative review

Arun C. R.[1] · **Ashis K. Pani**[1] · **Prashant Kumar**[1]

Received: 30 October 2022 / Revised: 4 March 2024 / Accepted: 13 March 2024

Abstract
The combination of blockchain-enabled smart contracts and the Internet of Things (IoT) is an emerging research area with a potential for far-reaching impact on our daily lives. While existing literature reviews explore current and future research states, most do not investigate the intellectual foundation. This study is a database-assisted narrative review of the smart contract and IoT combination using the TCM (Theme-Context-Method) framework that explores the past, present, and future. By reviewing 227 relevant peer-reviewed articles across 69 Scopus-listed journals, the authors profile the existing research, identify the foundational roots of literature, review the current state of research, and identify implications for research, practice, and society. The origins of the literature include themes such as decentralised data management, service orchestration, and distributed trust management. Themes in current research include the convergence of blockchain and the IoT, security, and privacy. Open research directions along the technology-legal-organisational triad, such as interoperability, dispute resolution, and skill gap assessment, have also been elucidated. This study synthesises extant literature to serve as a foundation for future academic research and practitioner exploration.

Keywords Smart contract · Blockchain · Internet of Things · Literature review · TCM framework

1 Introduction

Smart contracts are technology-driven, tamper-evident agreements that can self-execute a negotiated contract through a computer protocol [1]. Smart contracts are mostly blockchain-based and can automatically transfer digital assets based on arbitrary pre-specified logic specified as rules without a trusted third party [2]. While a vending machine is the oldest demonstrated example of a smart contract [3], technological advancements have made more sophisticated implementations possible. Smart contracts are deployed in

✉ Arun C. R.
r18003@astra.xlri.ac.in; arun.cr@gmail.com

[1] XLRI - Xavier School of Management, Jamshedpur, Jharkand, India

various sectors, including medical care, finance, energy, and the Internet of Things (IoT) [4–6]. IoT is a connected ecosystem of virtual and physical objects that automatically generate and communicate big data [7]. Smart contracts aid the interconnectivity between devices by managing such interactions without requiring that the objects trust each other.

A literature search of databases (Scopus and Google Scholar) confirms that both 'smart contracts' and the 'IoT' have become topics discussed extensively, with interest increasing significantly since 2015 onwards. Scholars have undertaken several literature reviews exploring the integration of blockchain with adjacent technologies, including edge computing [8], artificial intelligence [9] and the IoT [10]. Other studies include an exploration of blockchain as a technology [11], sector-focussed evaluations such as in healthcare [12], and a detailed exploration of smart contracts [13]. These studies discuss the current state of research, the challenges/risks of integration, and directions for future research. However, they do not explore the intellectual structure of the respective areas to understand the foundation. Database-assisted studies in this area are further limited; studies such as [14] have investigated blockchain-based digital twins in asset lifecycle management and [15] identified the developmental trajectories of blockchain. [16] evaluated supply chain visibility with blockchain, [17] explored decentralised access control, and [18] assessed cyber-physical smart contracts. These studies also explored the current and future status but did not explore the foundation. The authors of such studies have leveraged databases such as Scopus, Web of Science, IEEE Xplore, Google Scholar, Springer, and ACM in their studies. The methods include systematic reviews using the PRISMA guidelines, mapping reviews, citation analysis, and bibliometric analysis. However, none of these studies leveraged the TCM (Theme-Context-Method) framework utilised in previous reviews such as [19].

An analysis of the extant literature confirms that only a few (five) database-assisted literature reviews of SC-IoT have been conducted. The existing studies discuss the current state of research and identify future research directions using methods such as systematic literature reviews and bibliometric analyses. However, they do not explore the foundations of this emerging topic. Motivated by this research gap, the authors propose a Scopus-based narrative review of the smart contract-IoT combination (SC-IoT) using the TCM framework. Unlike the previous studies, this narrative review examines the past, the present, and the future in the same study. This study identifies the foundational roots of the literature on the SC-IoT combination (past), examines the current state of research (present), and identifies directions for further research (future). In addition, this study also profiles the existing research. To the best of the authors' knowledge, this is the first study in the SC-IoT space that utilizes this approach. Specifically, the following research questions are addressed by this review: 1) RQ1: What has the publication performance been in terms of authors, journals, and countries? 2) RQ2: What are the foundational research topics in smart contracts and the IoT? 3) RQ3: Which themes are the focus of current research? and 4) RQ4: What are the implications for future research and practice?

Our study builds upon and expands the extant SC-IoT literature. The main contributions of our study can be summarized as follows: 1) Synthesises and organises the existing SC-IoT knowledge base; 2) Provides a strong foundation for future scholars to conduct further research in this inter-disciplinary topic; and 3) Serves as an informed reference point for other stakeholders such as consumers, practitioners, governments, and policymakers. Our study profiles the existing research by shortlisting 227 relevant peer-reviewed articles and identifies the influential articles, journals, authors, countries, and publication trends. It further comprehends the intellectual foundation of the related literature by analysing the shortlisted articles' references. The authors subsequently review the current state of research by critically examining the contributions of the 227 articles and identifying future

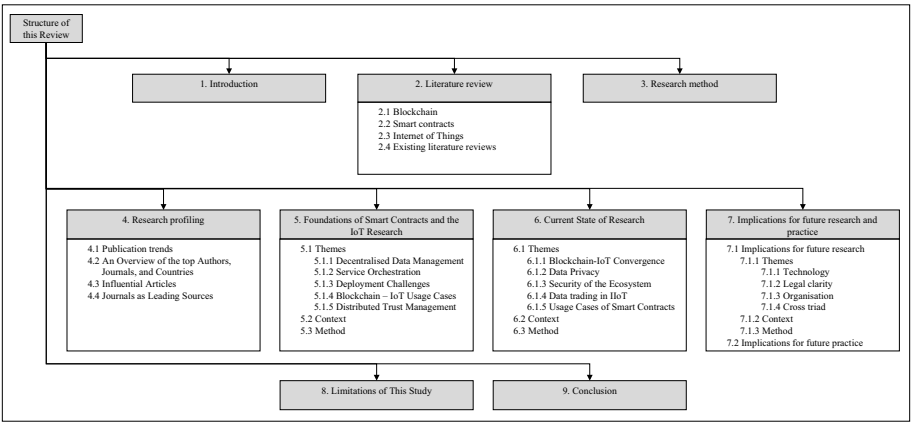

Fig. 1 Organisation of this Review

directions for research, practice, and society. The findings of this research study are presented by utilizing the TCM framework.

The remainder of the article is organised as follows. Firstly, the authors explain the concepts of blockchain, smart contracts, and the IoT, followed by an analysis of the existing literature reviews. Secondly, the authors discuss the method adopted by this study to conduct the analysis. Thirdly, the authors profile the shortlisted research papers, discuss the foundation on which the SC-IoT research is based, and analyse the current research status and directions for future research. The study ends with the Limitations of the study and the Conclusion. Figure 1 explains the organisation of this review, similar to the one followed in [20].

2 Literature review

The following section briefly explains the three topics of interest – blockchain, smart contracts, and the IoT, and the reviews undertaken so far. This section has been structured along the lines of the review in [21] to enable the reader to better appreciate the concepts and their relationships.

2.1 Blockchain

Blockchain is a distributed system comprising a network of peers that can read or write and a consensus protocol specifying the basis of adding new transactions to the chain [22]. In such a linked list of records, new blocks validated by peers using cryptographic means are appended to the end of the list, with each block pointing to the previous block through a hash value [23, 24]. In addition to the hash value, each block contains a timestamp and a random number used to verify the hash. Consensus algorithms in blockchain ensure the integrity, confidentiality, and security of the platform – they enable the blockchain to reach a "consensus" on the order in which the transactions are listed in the block. While several consensus algorithms exist for different blockchains, the prominent ones are Proof of Work (POW), Proof of Stake (PoS), Byzantine fault-tolerant (BFT), Proof of Authority (PoA),

and Proof of Elapsed Time (PoET), Among them, POW is the most popular. In POW, which is used for permissionless blockchains, the miner solves mathematical computations on the new block before validating the block [25]. POW is intentionally made compute-intensive and is key to making the blockchain immutable. Any node that finds the right random number (nonce) in the block header by solving the puzzle earns the right to validate the next block [22, 26]. Blockchain facilitates a network of computers to periodically arrive at a consensus on a distributed ledger's actual state that contains shared data secured through cryptography without the need for any trusted nodes [27]. The result is an immutable chain of records or blocks that can be either public or private. Some industries amenable to blockchain implementation include banks, finance, money transfers, micropayments, identity/privacy, and the IoT. Blockchain offers several advantages, such as eliminating the need for separate reconciliation, ensuring data provenance, quick settlement of transactions, and a robust security model [28]. Addressing the adoption barriers such as security risks, privacy risks, higher investment costs, lack of organisational policies/structure, and inadequate knowledge management systems could open further avenues for expansion [29]. A blockchain that supports Bitcoin-style transactions can facilitate asset transfers; however, one that supports smart contracts may extend the support for transactions between parties that do not trust each other [26].

2.2 Smart contracts

Smart contracts are mostly deployed on blockchains, as they provide a decentralised architecture enabling multiple technologies and communication patterns [18]. Conceptualised by Nick Szabo in the '90 s, smart contracts are programs running on blockchain nodes, and correspond to the protocols and user interfaces that formalise and secure relationships over computer networks [3]. Although introduced in 1994, some objectives such as verifiability, enforceability, observability, and privity were described in 1996 [30]. Smart contracts started gaining increased attention after Satoshi Nakamoto introduced Bitcoin in 2008. Multiple definitions of smart contracts exist today—from a technological perspective, they may be defined as event and state-driven programs that run on a platform to administer assets [31]. From a legal perspective, smart contracts may be defined as self-executing, tamper-proof agreements [32]. Smart contracts are utilised in a variety of industries such as real estate (e.g., purchase and lease agreements), finance (e.g., stock trading), healthcare (e.g., electronic health record management), construction (e.g., automated payments) and energy (e.g., electricity trading) [33]. Smart contracts offer several benefits including accuracy, autonomy, cost savings, and execution speed [34]. Although smart contracts are promising, several challenges remain to enhance their adoption, such as performance issues (low throughput, data storage difficulties), privacy issues (artificial stealing, node vulnerabilities), and security issues (contract loopholes, leakage of users' information) [35].

Based on preliminary investigation, smart contracts are more suited to industries with quantifiable terms of engagement and built on a system with clear rules [36]. While smart contracts enable general-purpose transactions, they add the most value in managing data-driven interactions between multiple non-trusting entities within a network. Once hosted and verified on the network, the smart contract will provide the same result for the same input each time, and the execution cannot be stopped, in theory. The execution also leaves an audit trail, and the potential of a dispute is minimised since the contracting parties would have agreed on the terms before the contract's execution. Not surprisingly, one of the most prominent applications of smart contracts is in the context of the IoT.

2.3 Internet of things

The Internet of Things (IoT), first coined by Kevin Ashton in 1999, refers to embedded computing devices that collect and store information without human intervention [37]. The IoT is an interconnected network of objects that are identified by an exclusive identifier and communicate over a network [38]. The IoT network consists of four layers: sensors (primary identification and tracking), networking (sharing of information between devices), services (integration of services and applications through middleware), and the user interface (user interaction) [37]. The technological advancement in communication protocols and the rapid advancements in adjacent technologies have enabled these devices to communicate and generate large amounts of data. Some common applications of the IoT are seen in the smart city, retail, healthcare, agriculture, and manufacturing sectors [39]. Several challenges must be resolved to improve adoption, including data privacy, network/IoT security, scalability, energy efficiency, and interoperability [40].

Security and privacy-related attacks on IoT devices are becoming more sophisticated and prominent with each passing day due to the increased availability of computing power [41]. The attacks impact not just the physical security (e.g., node capture, replay, side channel) but also the network (e.g., spoofing, man-in-the-middle attack, and denial of service) and application (e.g., phishing, trust management, malicious scripts) security too [42]. Instances of users being impacted include situations where users receive images from other people's homes in smart security cameras, and hackers play disturbing music and change the room temperature in smart homes. Researchers have also demonstrated the vulnerability of IoT devices by stealing device passcodes through an acoustic side channel attack on a smartphone's microphone, stealing data from a fax machine, and hacking a smart speaker during a live demonstration at the DEFCON security conference [43].

A secure IoT system must ensure the confidentiality of data, integrity of data, and network availability. Several approaches have been deployed to resolve security and privacy-related issues, including the use of blockchain, artificial intelligence, cloud, fog computing, edge computing, and various combinations of the above [20, 41, 44, 45]. Owing to its immutable, decentralized, and transparent properties, blockchain offers a promising solution to address security and privacy-related issues [46]. Blockchain records data securely on blockchain and facilitates safe and transparent data sharing between connected devices [47]. Blockchain-related solutions that have gained traction include secure unique identification (assigning a unique blockchain-based address to each IoT device using public keys) and secure communication (using lightweight protocols since no key management or key distribution needs to be maintained in the blockchain). Other measures include enabling privacy through authorization (implementing data access policies through a smart contract) and ensuring data integrity (the immutable nature of blockchain makes refuting a committed transaction difficult and enables non-repudiation) [42]. However, several challenges remain, such as the lack of consensus protocols resulting in limited adaptability of the integrated blockchain-IoT (BC-IoT) paradigm and transaction validation challenges owing to IoT devices' distributed nature and heterogeneity. Other challenges include implementing frequent software/firmware updates due to the decentralized nature of blockchain, limited interoperability due to the varying properties of blockchains / IoT devices, and sub-optimal network performance on parameters such as timeliness and power consumption.

Blockchain aids the development of a secure, decentralised, and trustworthy IoT ecosystem. Smart contracts and consensus protocols are foundational components of blockchain technology. Smart contracts and PoW share a supportive relationship as both rely on

a common platform – blockchain, but serve different purposes. While smart contracts automate participant interactions based on the data collected, consensus protocols such as PoW are the backbone of block propagation and facilitate secure and transparent interactions between the objects. Smart contracts are not solely dependent on PoW as other alternatives exist (such as PoS), and PoW cannot independently make or manage smart contracts—PoW facilitates a secure environment, and smart contracts utilize this to enhance the IoT ecosystem [48, 49]. A smart contract is a powerful multiplier for the capabilities of the IoT devices since both the code and agreements are replicated across the network elements. It is well-positioned to harness the large amount of data that is transmitted over the network and, at the same time, facilitates a set of actions based on predefined rules.

2.4 Existing literature reviews

Both 'smart contracts' and the 'Internet of Things' (generally written as IoT) have recently become topics discussed extensively in the academic and practitioner world. A simple search (during early 2022) of Scopus's journal articles on the 'Internet of Things' returned 311,047 results, and 'smart contracts' returned 19,006 results. More than 99% of the articles on 'smart contracts' and 92% on the 'Internet of Things' were published after 2015, indicating recent significant levels of interest. A similar search in Google Scholar revealed comparable observations—80% of the articles on "smart contracts" and 71% on the "Internet of Things" were published after 2015. A search on the Scopus database (during early 2024) for reviews or surveys on the combination of smart contracts and the Internet of Things returned 81 records [Scopus search query: TITLE-ABS-KEY ("smart contract" AND ("internet of thing" OR "iot") AND (survey OR review)) AND (LIMIT-TO (DOCTYPE, "ar")) AND (LIMIT-TO (LANGUAGE, "English"))]. The authors reviewed the titles and abstracts of these articles carefully for alignment with the topic and 45 were apt. Table 1 provides a summary of the papers.

While many referred to integrating blockchain with concepts such as artificial intelligence, edge computing, or the IoT, some focussed on sectors such as healthcare, agriculture, and smart homes. Only a few articles explored the development, challenges, and languages of smart contracts in detail, and some explored blockchain in general. [10] investigated the integration between blockchain and the IoT, the challenges in developing applications, and ideated on how blockchain could better enable the IoT ecosystems. [49] considered BC-IoT integration as a new paradigm, introduced an architecture for the Blockchain of Things (BCoT), and discussed potential issues regarding future implementations. [8] reported on the progress of edge intelligence-blockchain integration and the associated benefits of computing power management, data administration, and model optimization. More recently, authors have considered the integration of artificial intelligence with blockchain – [9] reviewed federated learning methods for holistically securing the IoT ecosystems; [50] examined federated learning frameworks from process decentralisation and reward mechanism perspectives and [51] conducted an in-depth evaluation of ensemble learning methodologies in the blockchain network.

Authors have also conducted sector-specific explorations—[12] reviewed applications of blockchain technology in healthcare and proposed workflows for better data management using Ethereum, and [52] explored concepts such as explainable blockchains while evaluating blockchain-based healthcare systems. Agriculture-focussed studies such as [53] studied blockchains in the agricultural sector, including technical elements, categorised the existing blockchain applications, and identified key challenges, and [54] evaluated the potential of

Table 1 Surveys/Reviews on SC-IoT

#	Category	2018	2019	2020	2021	2022	2023	2024	Total	Focus areas in exemplar papers
1	Blockchain integration	1	2		3	6	3		15	Integration with AI/Edge/IoT; federated learning, and security
2	Smart contract focus		1		1	5	3	1	11	Development, challenges, digital twin, cyber-physical systems, and languages
3	Sector focus			2	4	1	2		9	Healthcare, agriculture, aerospace, oil & gas, and smart home
4	Blockchain - general	2			3				5	Applications, issues, potential, and open research questions
5	Others		1	1		1	2		5	Metaverse, supply chain, governance, and data sharing
	Total	3	4	3	11	13	10	1	45	

blockchain to enable food traceability, protect workers' rights, limit the power of intermediaries, and protect market prices. Authors have also investigated the applicability of blockchain in aerospace and oil and gas sectors; [55] explored the potential of blockchain to revolutionise aerospace using multiple usage cases such as battlefield operations management, border protection, and swarm assistance for rescue operations and [56] discussed the applicability of blockchain in managing the exploration, production, supply chain, and logistics in the oil and gas industry.

Some studies have explored blockchain technology in general and smart contracts specifically—[11, 57] discussed the taxonomy, consensus algorithms, categories, applications, and technical challenges of blockchain; [13] discussed the application of smart contracts in Industry 4.0, [58] reviewed the development and opportunities of smart contract deployment through an explanation of the working principles and the status of application research, and [59] examined recent developments in smart contracts across the categories of platforms, risks, and solutions. Other studies have included applications of blockchain in the metaverse [60] and how blockchain can resolve issues in governance [61].

The authors further filtered the review articles to identify database-assisted studies that explored the SC-IoT combination—summarised in Table 2. [14] explored blockchain-based digital twins in asset lifecycle management and established that blockchain-based digital twins can support digitalisation initiatives through a systematic literature review supported by a quantitative survey. [15] identified blockchain's developmental trajectories and themes through citation analysis. Four stages of development included the challenges to Bitcoin, smart contract issues, opportunities, challenges, and development in blockchain, and smart contract applications; themes included e-healthcare, energy, Bitcoin, security of Bitcoin, financial applications of Bitcoin, Ethereum smart contracts, security, and privacy in the IoT. While [16] evaluated supply chain visibility with blockchain through a bibliometric analysis identifying five knowledge clusters, [17] explored decentralised access control through a study of the challenges of centralised access control on securing the IoT devices, and [18] assessed cyber-physical smart contracts through a mapping review of the underlying architectures from the dimensions of cyber-physical architectures, infrastructure failures, and the technical challenges. The databases explored for the studies include Scopus, Web of Science, IEEE Xplore, Google Scholar, Springer, and ACM. The authors have adopted systematic reviews using the PRISMA guidelines, citation or cluster analysis, and mapping reviews. However, none of the studies used the TCM (Theme– Context–Method) framework.

3 Research method

An effective review of prior, relevant literature builds a strong base to advance existing knowledge and, at the same time, facilitates theory development [62]. A standalone literature review creates a starting point for scholars interested in a particular field [63]. Such a review could be undertaken for several reasons in order – to evaluate the progress of a specific research stream, aggregate the findings by previous studies, review the application of a theory or methodology. or to enable theory building. Some commonly undertaken literature reviews include narrative reviews, systematic reviews, meta-analyses, and bibliometric analyses. While systematic literature reviews are often performed manually on a narrow set of articles, meta-analyses, and bibliometric analyses rely on quantitative tools to cover more articles. Meta-analyses are commonly used as theory extension tools, while bibliometric analyses summarise the bibliometric and

Table 2 Database-assisted studies that explore SC-IoT combination

#	Review article	No. of papers	Databases	Focus	Method	Findings of the review	Topics for future work
1	Tseng et al [15]	2,478	Web of Science	Developmental trajectories of blockchain technology and its major themes	Citation analysis using Main path analysis and Girvan-Newman clustering	• Development stages included challenges to Bitcoin, smart contract issues, opportunities, challenges, and development in blockchain and smart contract applications • Identified six major themes—bitcoin security, bitcoin financial applications, e-healthcare, Ethereum smart contracts, security and privacy in IoT, and energy	• Additional articles and topics (e.g., deepfake, digital twin) • Impact of COVID-19 and 5G on blockchain • Combine citation analysis and text analysis
2	Sahoo et al [16]	308	Scopus	Blockchain technology in supply chains	Bibliometric analysis using PageRank analysis and Content mining	• Identified five knowledge clusters—blockchain for food supply chain transparency; distributed ledger for sustainable supply chains; traceability systems using smart contracts; IoT for logistics, and the emergence of Ethereum and Hyperledger in supply chains	• Integration with emerging technologies • Scalability and interoperability challenges • Industry-specific applications

Table 2 (continued)

#	Review article	No. of papers	Databases	Focus	Method	Findings of the review	Topics for future work
3	Noor et al [17]	81	ScienceDirect, IEEE, Springer, and ACM	Decentralised access control in smart farming/IoT	Systematic literature review	• Commonly used authorisation and authentication methods include key management schemes (e.g., symmetric/asymmetric cryptography) • Frequently used access control models include role-based and attribute-based access controls • Gaps identified include lack of standardisation, privacy, and security	• Enhancement of smart contract design for access control • Validation of designs through simulations

Table 2 (continued)

#	Review article	No. of papers	Databases	Focus	Method	Findings of the review	Topics for future work
4	Alfuhaid et al [18]	50	Scopus, Web of Science, IEEE Xplore, and Google Scholar	Use of cyber-physical smart contracts (CPSCs) for compliance monitoring	Mapping review using the PRISMA guidelines	• Several platforms, development tools, and data carriers exist to develop, deploy, and invoke CPSCs • CPSCs require external components to verify, produce, and consume compliance monitoring data • Several infrastructure failure risks arise due to centralisation and attacks; potential mitigation by integrating with digital ledger technologies or distributing data storage • Identified challenges, such as security, availability, data privacy, and robustness	• Compliance monitoring using other architectures that address the limitations of blockchain • Reference monitoring model of data and events for compliance monitoring • Research challenges such as availability, robustness, privacy, and legal and regulatory aspects
5	Götz et al [14]	46	Scopus and ScienceDirect	Applicability, interoperability, and integrability of a blockchain-based digital twin in asset lifecycle management	Systematic literature review using the PRISMA guidelines and a Quantitative survey	• Blockchain-based digital twins can support digitalization initiatives • User-friendliness, accessibility, and manuals (user- and implementation-) are necessary for successful implementation	• Think tank discussions with industry professionals • Organisational prerequisites to enhance adoption • Map technologies, data ontology solutions, and usability alignment with digital twin

Table 2 (continued)

#	Review article	No. of papers	Databases	Focus	Method	Findings of the review	Topics for future work
6	Our paper	227	Scopus	Smart contract and IoT	Narrative review using the TCM framework	• Profiled the existing research in terms of top journals, articles, authors, and countries • Identified intellectual foundations of research such as decentralised data management, service orchestration, deployment challenges, BC-IoT use cases, and distributed trust management • Highlighted themes in the current state of research such as BC-IoT convergence, data privacy, ecosystem security, data trading in IIoT (Industrial IoT), and smart contract use cases	• Future research directions include interoperability, technical characteristics, and legal and organisational issues are identified • Monitor the research model using advanced techniques

intellectual structure by analysing the social and structural relationships between different research constituents [64]. In contrast, narrative reviews attempt to uncover what has already been written about a particular subject.

The authors chose narrative review since they found this to be the most suitable review method, given the status of research on SC-IoT. The extant literature is not mature enough to warrant a systematic literature review. Furthermore, it includes only a few empirical studies; hence, meta-analysis is not preferred. Since the literature has picked up the pace only during the recent decade, a bibliometric analysis may not help glean relevant insights. This narrative review is divided into four sections – the first profiles the existing research, the second uncovers the intellectual foundations of the research, the third analyses the current state of research, and the fourth discusses some implications for future research. The authors reviewed the articles referenced in the shortlisted papers to determine the foundations of SC-IoT. Then, they reviewed the shortlisted articles to understand the current state of research. While reviewing, the articles were grouped into themes based on the observed commonalities. The resultant groupings helped determine the individual clusters in each of the areas. While one author reviewed and identified the themes, the other authors evaluated the themes and suggested revisions to the groupings and themes. The authors conducted brainstorming sessions based on the identified themes to determine the implications for future research and practice. For each of the three sections, the authors also identified the relevant context in which the research was conducted and the methods employed.

The authors chose the Scopus database to conduct the narrative review. Scopus is among the largest citation and abstract databases of scientific peer-review literature, including 23,000 titles from publishers, and guarantees the data's completeness and reliability [65]. The search was conducted in January 2022 using the search string 'smart contract' AND 'internet of thing'; it was limited to English, and the period was set as all research artefacts published until December 31, 2021. The search returned 1,072 records that included 596 conference papers, 385 articles, 32 book chapters, 28 conference reviews, 27 reviews, two books, one editorial, and one note. Research articles from only the following fields were used for further analysis to ensure relevance to the Information Systems field: ABDC—Information systems, Management, Marketing/Tourism/Logistics, Accounting, Other commerce, management, tourism, and services; Scopus—Business Management & Accounting, Social Sciences, Decision Sciences, Economics, Econometrics, and Finance; Scimago—Information Systems, Information Systems and Management, Management Information Systems, Business Management and Accounting (Miscellaneous), Decision Sciences (Miscellaneous); Web of Science—All categories/sub-categories containing Information system and Information science. The above shortlisting process resulted in 227 articles for further review.

Table 3 Number of papers by year

Year	2016	2017	2018	2019	2020	2021	Total
Number of papers	1	3	11	45	45	122	227

4 Research profiling

This section addresses RQ1—What has the publication performance been in terms of the authors, journals, and countries?

4.1 Publication trends

Smart contracts, as a concept have existed for a while; however, their application in the context of IoT has picked up interest recently. While only one article was published in 2016, 45 were published in both 2019 and 2020, and in 2021, the number more than doubled, indicating the increasing interest in this area. Please refer Table 3 for the summary.

4.2 An overview of the top authors, journals, and countries

Table 4 represents the most productive authors, journals, and countries, with productivity being measured by their respective total publications (TP). Seven hundred and forty-nine authors have published 227 articles, with 95% having authored two or fewer articles. Sixty-nine Scopus-listed journals have published articles on smart contracts in the IoT context. Of the 69, 12 are IEEE-related journals—IEEE Internet of Things and IEEE Access, and IEEE Transactions on Industrial Informatics journals form the top three contributing journals. These three contribute 44% (99) of the overall number of articles. Like the authors, the journals also exhibited a long tail, with ~ 60% of the journals contributing only one article each. Authors from 51 countries have published articles related to smart contracts in the IoT's context, with the top three countries represented in ~ 67% of the articles. Cumulatively, China, the United States of America, and the United Kingdom are represented in 151 articles.

4.3 Influential articles

Table 5 lists the top 15 influential papers. With five papers cited more than 250 times; cumulatively, these 15 papers have been cited more than 3.500 times (3,788). [11] stands out, with more than 900 citations. The authors conducted a comprehensive survey on blockchain technology, discussed its taxonomy, consensus algorithms, and reviewed the application areas and technical challenges. The authors also identified five areas for future research, including smart contracts, blockchain testing, centralisation avoidance, artificial intelligence, and big data analytics. [48] introduced a new blockchain-based, fully distributed access control system for the IoT and supported this with a proof-of-concept implementation. [66] proposed an IoT e-business model that helped realize smart property transactions and paid data on the IoT with the help of peer-to-peer trade based on smart contracts.

Table 4 Top 15 authors, journals, and countries

Rank	Author	TP	Select topics covered in exemplar papers	**Journal**	**TP**	**Select topics covered in exemplar papers**	Country	TP
1	Zhang Y	7	IoT electric business model, blockchain-internet of things integration, access control, service provisioning schemes, and multi-server authentication protocol	**IEEE Internet of Things Journal**	**47**	**BC-IoT integration, edge-IoT integration, IoT access control management, data privacy, security, data and electricity trading, and sector focus—smart cities, energy**	China	94
2	Viriyasitavat W	7	Service composition in Industry 4.0, collaborative Internet-of-Things, blockchain for business processes in the digital economy, system design perspective to BC-IoT integration, and quality of services for blockchain-based IoT services	**IEEE Access**	**36**	**Sector focus—smart city, healthcare, and energy, BC-IoT integration, trust, IIoT, and authentication**	United States of America	35
3	Yang Y	7	Game theoretic approach to blockchain, network slicing service quality computing model, energy trading, resource allocation, and multi-chain trusted reputation scheme for charging platform	**IEEE Transactions on Industrial Informatics**	**16**	**Data trading, blockchain-edge integration, and trust**	United Kingdom	22
4	Xu L.D	7	Blockchain for business processes in the digital economy, collaborative Internet-of-Things, service composition in Industry 4.0, system design perspective to BC-IoT integration, and quality of services for blockchain-based IoT services	**Wireless Communications and Mobile Computing**	**12**	**Blockchain-based secure network computing services, sector focus—healthcare, and authentication**	India	21

Table 4 (continued)

Rank	Author	TP	Select topics covered in exemplar papers	**Journal**	**TP**	**Select topics covered in exemplar papers**	Country	TP
5	Wang H	6	Review of blockchain and challenges, food safety traceability system, and privacy-preserving transactive energy management	**Sensors**	**10**	**BC-IoT integration, security, and privacy**	Australia	18
6	Chen X	6	Review of blockchain and challenges, provable data possession model for smart cities, and blockchain for mobile device cloud	**IEEE Transactions on Computational Social Systems**	**5**	**BC-IoT integration**	South Korea	12
7	Bi Z	6	System design perspective to BC-IoT integration, service composition in Industry 4.0, and blockchain for business processes in the digital economy	**Future Internet**	**5**	**Open-source ecosystem-based IoT**	Saudi Arabia	11
8	Salah K	6	IoT data monetization, reputation system for IoT public fog nodes, and cross-device federated learning in IIoT	**Security and Communication Networks**	**5**	**Blockchain-based services in IoT**	Canada	10
9	Wang Y	6	Game theoretic approach to blockchain, resource allocation in IoT, and special vehicles priority access guarantee	**IEEE Network**	**4**	**Blockchain-based IoT frameworks**	United Arab Emirates	9
10	Wang G	5	Service provisioning schemes, special vehicles priority access guarantee, and optimal smart contract execution	**International Journal of Recent Technology and Engineering**	**4**	**Smart contract usage cases**	Spain	9
11	Zhao Y	5	IoT scalability and security, data trading, and privacy-preserving schemes	**Peer-to-peer Networking and Applications**	**3**	**New BC-IoT-based business models**	Thailand	8

Table 4 (continued)

Rank	Author	TP	Select topics covered in exemplar papers	**Journal**	**TP**	**Select topics covered in exemplar papers**	Country	TP
12	Li J	5	Data trading, resource allocation, and privacy-preserving authentication protocols	**Computers and Security**	**3**	**Data privacy**	France	8
13	Yu Y	5	Data trading, provable data possession model for smart cities, and self-tallying voting system	**Journal of Information Security and Applications**	**3**	**Data security**	Japan	6
14	Chen Y	5	Game theoretic approach to blockchain, IIoT data sharing, and energy trading	**Computer Communications**	**3**	**Authentication and access management**	Pakistan	5
15	Li H	5	Provable data possession model for smart cities, blockchain in the construction sector, and network slicing service quality computing model	**IEEE Systems Journal**	**3**	**Lightweight BC-IoT instantiations**	Taiwan	5

Table 5 Top 15 Influential papers

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
1	Zheng Z., Xie S., Dai H.-N., Chen X., Wang H.	Blockchain challenges and opportunities: A survey [11]	2018	International Journal of Web and Grid Services	901	• Lack of a comprehensive survey of blockchain from technological and application perspectives	• Explained blockchain taxonomy, consensus algorithms, applications, technical challenges, recent advances, and future directions	• In-depth investigation of smart contracts
2	Novo O.	Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT [48]	2018	IEEE Internet of Things Journal	530	• Scalability issues in managing access to IoT devices	• Proposed a new architecture that is scalable and easy-to-manage for arbitrating roles and permissions in IoT. • Developed a Proof-of-Concept and evaluated its performance.	• System-related limitations such as higher transaction processing times
3	Zhang Y., Wen J.	The IoT electric business model: Using blockchain technology for the Internet of things [66]	2017	Peer-to-Peer Networking and Applications	294	• Unsuitability of traditional business models for IoT electric business	• Proposed an E-business architecture specifically designed for IoT using DACs. • Experimentally verified the IoT E-business model.	• Development of smart devices equipped with NFC module. • Design uniform format and API for paid data. • Construct IoT data exchange platform.

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
4	Griggs K.N., Ossipova O., Kohlios C.P., Baccarini A.N., Howson E.A., Hayajneh T.	Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring [182]	2018	Journal of Medical Systems	268	• Use of a private blockchain-based smart contract for secure analysis and management of medical sensors	• Proposed use of smart contracts to execute real-time analysis and logging of transaction metadata of medical sensors in WBAN. • Evaluated the information collected based on customised threshold values using a permissioned consortium-managed blockchain. • Coded smart contracts in Solidity as a proof-of-concept.	• Hyperledger implementations. • Privacy of patients by utilising anonymizers.
5	Dai H.-N., Zheng Z., Zhang Y.	Blockchain for Internet of Things: A Survey [49]	2019	IEEE Internet of Things Journal	267	• Convergence of Blockchain and IoT as a new paradigm	• Explained Internet of Things (IoT) and blockchain technology. • Evaluated BC-IoT convergence and proposed an architecture. • Discussed applications, challenges, and open research issues of BCoT.	• Research scalability and security vulnerabilities. • System development considering resource constraints and privacy leakage. • Incentive mechanisms.

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
6	Kim H.M., Laskowski M.	Toward an ontology-driven blockchain design for supply-chain provenance [183]	2018	Intelligent Systems in Accounting, Finance and Management	249	• Use of ontologies in blockchain design for supply chain provenance	• Developed a proof-of-concept implementation of a provenance evaluating blockchain on Ethereum using Solidity. • Analysed select assumptions and data models of TOVE traceability ontology. • Translated TOVE traceability ontology axioms into smart contracts.	• Other traceability constructs (formal axioms and informal data models). • Systematic conversion of ontology representations to blockchain code.
7	Sun J., Yan J., Zhang K.Z.K.	Blockchain-based sharing services: What blockchain technology can contribute to smart cities [184]	2016	Financial Innovation	242	• Lack of understanding of how information technology can support the development of smart cities	• Proposed a conceptual framework comprising human, technology, and organisation factors to explore smart cities for a sharing economy. • Discussed the potential contribution of blockchain in developing sharing services in smart cities.	• Design and adoption of blockchain-based sharing services for smart cities

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
8	Kshetri N.	Blockchain's roles in strengthening cybersecurity and protecting privacy [107]	2017	Telecommunications Policy	235	• Security and privacy concerns in existing systems	• Examined the role of blockchain in strengthening privacy and improving cybersecurity. • Evaluated privacy and security aspects of blockchain against cloud computing.	• Blockchain-based identity and access management systems.
9	Zhang Y., Kasahara S., Shen Y., Jiang X., Wan J.	Smart contract-based access control for the Internet of Things [153]	2019	IEEE Internet of Things Journal	230	• Feasibility of distributed and trustworthy access control in IoT network	• Designed a smart contract-based framework to implement trustworthy and distributed access control in IoT devices using multiple access control contracts, one judge contract, and one register contract. • Evaluated the performance of the framework through a case study.	• Could not be ascertained

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
10	Xu Y., Ren J., Wang G., Zhang C., Yang J., Zhang Y.	A blockchain-based nonrepudiation network computing service scheme for industrial iot [111]	2019	IEEE Transactions on Industrial Informatics	106	• Challenges in applying traditional non-repudiation solutions in the IIoT context	• Developed a fair blockchain-based non-repudiation service provisioning scheme. • Demonstrated the use of homomorphic-hash-based service verification method. • Developed smart contracts for dispute resolution.	• Performance evaluation of real-world deployments. • Integration of deposit and reputation mechanisms. • Non-repudiation dispute resolution mechanisms.
11	Rahman M.A., Rashid M.M., Shamim Hossain M., Hassanain E., Alhamid M.F., Guizani M.	Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City [185]	2019	IEEE Access	106	• Challenges of coordinating cognitive and intelligent processing at the edge of the network	• Designed a framework for a sustainable IoT-enabled sharing economy in smart cities. • Detailed the deployment and implementation of the framework. • Enabled parties to transact without a third party by leveraging intelligence at the edge and seamlessly coordinate with IoT devices.	• Performance evaluation in different sharing economy scenarios at a large scale, such as Hajj

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
12	Lin Q., Wang H., Pei X., Wang J.	Food Safety Traceability System Based on Blockchain and EPCIS [186]	2019	IEEE Access	100	• Issues with traditional food traceability systems, such as data tampering, disclosure of sensitive details, and invisibility of data	• Developed the design and prototype of a food traceability system based on blockchain and EPCIS. • Designed an enterprise-level smart contract to prevent disclosure of sensitive information and data tampering. • Defined a dynamic management method to control data explosion.	• Optimisation of peer-to-peer network by implementing the fragmentation node. • Fine-tuning the consensus algorithm to enhance system performance. • Information clipping to reduce the amount of data.
13	Fernandez-Carames T.M., Fraga-Lamas P.	A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories [13]	2019	IEEE Access	95	• Lack of a comprehensive approach to studying the applicability of blockchain to Industry 4.0 technologies	• Reviewed the benefits and challenges of applying blockchain to Industry 4.0. • Provided a reference guide for Industry 4.0 developers on the suitability of blockchain.	• Scalable architectures. • Energy-efficient algorithms. • Data privacy, integrity, and certification. • Interoperability and standardisation of devices. • Regulatory and legal aspects.

Table 5 (continued)

#	Authors	Title	Year	Journal	Cites	Motivation	Contribution	Future work
14	Pan J., Wang J., Hester A., Alqerm I., Liu Y., Zhao Y.	EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts [100]	2019	IEEE Internet of Things Journal	90	• Scalability and security challenges of existing IoT devices	• Developed the design and prototype of EdgeChain - an edge-IoT framework based on smart contracts. • Demonstrated use of credit-based resource management system. • Defined policy enforcement methods to regulate IoT device behaviour.	• IoT proxy, intelligent resource provisioning for mechanisms for diverse applications, and enhanced regulations for IoT device behaviour
15	Lin X., Li J., Wu J., Liang H., Yang W.	Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach [187]	2019	IEEE Transactions on Industrial Informatics	75	• Lack of sufficient studies on knowledge trading among IoT devices	• Developed an implementation architecture of the knowledge market to enable efficient knowledge sharing and trading. • Proposed a new environmentally conscious consensus mechanism - Proof-of-Trading. • Proposed a knowledge pricing strategy based on a non-cooperative game.	• Economic models that consider data/information and knowledge trading

DAC Decentralised Autonomous Corporations, *NFC* Near Field Communication, *API* Application Programming Interface, *WBAN* Wireless Body Area Networks, *EPCIS* Electronic Product Code Information Services

Since blockchain is the platform, and smart contracts reside on the platform enabling functionalities, most papers explore smart contracts from the perspective of blockchain and its integration with the IoT. Hence, few papers provide an exclusive and in-depth focus on smart contracts. Although blockchains and smart contracts have existed for a while, they have only recently captured the imagination of academicians and practitioners.

4.4 Journals as leading sources

Both smart contracts and IoT are based on technological developments as reflected in the list of the most productive journals. The aims/purpose/scope sections of the most productive journals below reveal that they all have a significant technological focus. The articles that have been published include literature reviews, applications in use examples, and the exploration of concepts. Although the journals welcome process, technology, and theory papers, there is little evidence of papers regarding theory development being published.

H-index and average citations per paper (Total citations divided by Total publications; abbreviated as TC/TP) may be considered as key criteria for a journal's influence [67]. Higher values would identify the most relevant journals published in the literature concerning smart contracts and the IoT. TC/TP and publication output follow a similar trend in journals that have published more than ten papers, (bar one, IEEE Transactions on Industrial Informatics). However, the TC/TP and H-index do not follow the same pattern as the journals. While Sensors and IEEE Access are the top two in terms of H-index, IEEE Transactions on Computational Social Systems and the IEEE Internet of Things Journal are the TC/TP top two among the top 15 journals. Please refer Table 6 for details.

5 Foundations of smart contracts and the IoT research

The authors have utilised the TCM (Theme-Context-Method) framework to present the findings on the foundations, current state of research and the direction for future research. The themes correspond to the underlying commonalities, the context refers to the sector/industry in which the referenced studies were conducted, and the methods represent the approach followed in conducting those studies. The authors explored the articles listed as references of the shortlisted articles to understand the foundations of the SC-IoT research (RQ2). The authors uncovered five key elements. The foundational articles explore the applicability of blockchain in the context of the IoT– this provides fertile development grounds for smart contracts since blockchain is the platform on which smart contracts reside. While one explores decentralised data management, the second addresses orchestrating the relevant services to achieve a coordinated outcome. The other three pillars addressed the key challenges regarding deployment, relevant usage cases, and decentralised trust management. The following sections explore the themes, contexts, and methods of the foundational aspects.

5.1 Themes

5.1.1 Decentralised data management

IoT applications are characterised by the large amounts of data they generate. While the challenge of storing and processing large volumes of data can be addressed by integrating

Table 6 Citation structure of top 15 journals

#	Source	TP	TC	TC/TP	H-index	> = 50	> = 20	> = 10	> = 5	> = 1
1	IEEE Internet of Things Journal	47	1,419	30	119	4	4	8	5	8
2	IEEE Access	36	829	23	158	6	7	7	2	8
3	IEEE Transactions on Industrial Informatics	16	449	28	151	4	2	2	2	4
4	Wireless Communications and Mobile Computing	12	112	9	69	1	1	1	0	3
5	Sensors	10	28	3	196	0	0	1	1	4
6	IEEE Transactions on Computational Social Systems	5	178	36	33	1	3	1	0	0
7	Future Internet	5	36	7	38	0	0	2	1	2
8	Security and Communication Networks	5	20	4	50	0	0	1	0	1
9	IEEE Network	4	47	12	135	0	1	0	0	3
10	International Journal of Recent Technology and Engineering	4	6	2	23	0	0	0	0	4
11	Peer-to-peer Networking and Applications	3	307	102	36	1	0	1	0	1
12	Computers and Security	3	84	28	102	1	0	1	1	0
13	Journal of Information Security and Applications	3	23	8	45	0	0	1	0	1
14	Computer Communications	3	17	6	109	0	0	0	2	0
15	IEEE Systems Journal	3	7	2	88	0	0	0	0	3

TP and *TC* Total publications and citations, *TC/TP* Average citation per paper; $\geq 50, \geq 20, \geq 10, \geq 5, \geq 1$ = the number of papers with equal or more than 50, 20, 10, 5, and 1 citations respectively

with cloud technologies, the resultant centralisation leads to concerns regarding security and privacy. Integrating the IoT with blockchain enables decentralised data sharing at scale and addresses security and privacy challenges. The extant literature includes several review and survey articles that studied the integration of blockchain with the IoT—while [68] and [69] focussed on the security and privacy aspects, [10, 70] and [11] analysed the integration of blockchain and the IoT solutions in general, including their development, deployment, and optimisation. Specific solutions to address the security and privacy issues included a distributed secure SDN architecture for the IoT using blockchain (DistBlockNet) [71] and secure key management schemes in vehicular communication systems [72]. Adaptations of the Elliptic Curve Digital Signature Algorithm [73] are implemented in signature schemes, including lattice-based signature schemes that can resist quantum attacks [74] and attribute-based signature schemes [75] that enhance security. In addition to introducing the blockchain architecture, consensus algorithms, and typical applications, the reviews also discuss the technical challenges, limitations of the IoT devices, secure code deployment, and several other factors. The authors have explored blockchain's data storage and processing capabilities further in sectors such as energy and healthcare and found that the performance of blockchain-based solutions is comparable [76] or superior [72]. Several recent advancements, such as mobile edge computing [77], fog computing [78], and consortium blockchains [79] have improved decentralised data management and applicability of blockchain-enabled IoT devices. Additional research directions have highlighted several aspects that include work on interoperability, standardisation, energy-efficient communications, development of design principles for the future, and organisational/regulatory considerations.

5.1.2 Service orchestration

Services form the building blocks that execute activities of the business process of any ecosystem [80]. Through service workflows, also known as business processes, the ecosystem utilises services to improve dynamic interoperation among its constituents to achieve its functionalities [81]. Functionalities are viewed as services that are orchestrated by service workflows [82]. Service selection in a service workflow (which specifies the composition, sequence, and execution path) is based on several parameters, such as service quality, experience, and reputation. The service requirements are developed through service workflow specification languages (examples include SWSpec and Self-Adaptive Configuration based on HMS[1]BAM[2] and CTR[3]).

Blockchain is appropriate for complex workflows [83] such as in an IoT context—with technological advancements, the BC-IoT combination presents several opportunities for automation, effective data sharing, and business transformation [84]. Integrating blockchain into business processes will help to mitigate the risks associated with security, privacy, trust, automation, and interoperability issues—examples include FairAccess [85] and "Bubbles of Trust" [86]. While FairAccess provided a pseudonymous and privacy-preserving authorisation management framework, Bubbles of Trust enabled robust identification

[1] Holonic Multi-agent Systems;

[2] Business Application Modeler.

[3] Concurrent Transaction Logic.

and authentication of devices. Blockchain is also architected to integrate with other service (or business process) components to resolve traditional problems of time inconsistency and consensus bias to improve the overall trust levels. BC-IoT integration must be carefully orchestrated, since several challenges must be overcome (please refer to Section 5.1.3). The authors have also identified several open research challenges in this emerging area, including resource limitations of the IoT devices, the heterogenous nature of the IoT devices, hardware/firmware vulnerabilities, development of green IoT technologies, and employment of artificial intelligence and cloud computing [87–89].

5.1.3 Deployment challenges

While the BC-IoT combination can help to achieve the true potential of the IoT, close attention needs to be paid to several potential challenges. [26] highlighted several such issues and suggested potential solutions. The inherent nature of blockchain leads to slower transaction processing than a centralised system, hence reduced throughput. Since the transactions are replicated transparently across nodes, sophisticated actors can analyse the transactions to make informed inferences, thereby compromising privacy. As a solution, devices can use separate keys for each transaction or separate keys per transacting party to limit exposure. Homomorphic encryption or Zero Knowledge Proofs can also help to achieve transactional privacy. Miners should be chosen carefully—although miners cannot create fraudulent transactions, they can prevent a truthful one from being recorded. Since regulations are still catching up with this new technology, legally enforcing smart contracts remains challenging. Another issue that needs to be tackled is "complete autonomy." Smart contracts are executed automatically according to compliance with certain pre-defined conditions. Hence, measures should be taken to avoid unintended consequences such as faulty smart contract coding. Access to the blockchain-integrated IoT system should be monitored carefully– if malicious actors gain unauthorised access, they can create unwanted problems for the entire ecosystem. [48] proposed a scalable and easy-to-access management system and demonstrated its efficiency through a proof-of-concept prototype. The energy consumption by blockchain-based methods is higher than by traditional methods, and development of mechanisms to reduce the energy requirements are ongoing. Additionally, coordination costs of integrating blockchain into the IoT context can sometimes be considerable; thus, optimal methods to reduce these need to be developed. Other key challenges include double-spending [90], transaction malleability, and pooled mining [91]. In addition, significant delays and computational overheads introduce several design challenges that practitioners need to resolve.

5.1.4 Blockchain – IoT usage cases

With its unique advantages, the BC-IoT combination, termed the Blockchain of Things (BCoT) [17], may be applied in many industries. Dai et al. explain that smart manufacturing, supply chain management, food industry, smart grids, healthcare, the Internet of Vehicles (IoV), and unmanned aerial vehicles (UAVs) are prominent among such applications. In smart manufacturing, BCoT aids interoperability by enabling data sharing by forging connections between the IoT systems in a peer-to-peer network, which enables better security and privacy, reduces security maintenance costs, and enhances data quality assurance. In supply chain management, it helps establish the provenance of the parts used in the supply chain and reduces counterfeits. Thus, it reduces the cost and risk elements

and increases the velocity of the supply chain. BCoT can enhance the traceability of food products by integrating RFIDs in the food industry. In smart grids, BCoT facilitates secure energy trading among peers, enabling the rise of a new class of prosumers (producers and consumers), reducing trading costs, and protecting the confidentiality of transactions. Integrating blockchain into healthcare data (such as that generated through wearables) helps to preserve privacy and enables tracing the origin of pandemic outbreaks. BCoT also enables secure energy trading in electric vehicles and resolves the challenges of heterogeneity and non-trustworthiness of data compared to traditional implementation in the context of IoVs and UAVs. Blockchain may also be utilized in other usage cases, such as in smart homes [92], authentication systems [86], medical data access/permission management, and implementation of role-based access controls [93]. While Dorri et al. demonstrated through a case study that a blockchain-based smart home framework can ensure the triad of confidentiality, integrity, and availability, Hammi et al. implemented a decentralised authentication system using C++and Ethereum and established its capabilities of robust device identification and authentication.

5.1.5 Distributed trust management

The distributed nature of blockchain enables any participant node in a network to transact in a decentralised, trusted manner within various environments, including vehicular networks and electronic health records (EHR). However, confidentiality, scalability, and the reliance on third parties require addressing. [84] proposed a decentralized trust management system for vehicular networks using joint Proof of Work and Proof of Stake consensus mechanisms. The vehicles in the network use the Bayesian inference model to validate the messages received and generate ratings to assess the credibility of the messages. Thus, trust values are generated and aggregated in roadside units (RSUs) that maintain a concurrent, reliable, and consistent trust blockchain. Since data is stored in a decentralised manner, security and access control become crucial. [85] proposed a framework to address the problems of data integrity, security, and management that utilises off-chain storage, enabling scalability, and provides secure storage, and defines granular access rules for EHRs. Along similar lines, [86] introduced a blockchain-based framework for a data integrity service for the IoT that does not rely on third-party auditors. The prototypes are found effective based on the performance evaluation results – authors establish the system's effectiveness through simulation, and prove that their pay-per-transaction data integrity service provides a reliable and scalable solution that supports decentralised data trading. Another decentralised trust management perspective is integrating two technological ecosystems; blockchain and artificial intelligence [87]. The authors have provided a detailed discussion on the taxonomy, compared common blockchain implementations, and identified challenges in enabling decentralised AI (including privacy, scalability and side chains, security, smart contract vulnerabilities, and AI-specific consensus protocols).

5.2 Context

Table 7 summarises the sectors in which the studies were conducted. More than two-thirds of the studies do not refer to any specific sector. The findings in such studies are likely applicable uniformly across sectors – reviews (discussed in 5.3) constitute more than 40% of such sector-agnostic studies. Some studies refer to multiple sectors such as healthcare,

Table 7 Context of Foundational Studies

#	Context	Number of studies	Exemplar studies
1	Multi-sector focus	36	Christidis and Devetsikiotis, 2016 [26]; Khan and Salah, 2018 [87]; Banerjee et al., 2018 [68]; Liu et al., 2017 [188]; Dinh et al., 2018 [189]; Fernandez-Carames and Fraga-lamas, 2018 [70]; Xu et al., 2014 [88]; Dai et al., 2019 [49]
2	Energy	4	Li et al., 2018 [79]; Kang et al., 2017 [190]
3	Healthcare	4	Guo et al., 2018 [75]; Xia et al., 2017 [76]
4	Transportation	3	Lei et al., 2017 [72]
5	Others – smart home, manufacturing, disaster warning system	3	Bahga and Madisetti, 2016 [191]; Dorri et al., 2017 [92]

Table 8 Methods followed in Foundational studies

#	Method	Number of studies	Exemplar studies
1	Review	19	Christidis and Devetsikiotis, 2016 [26]; Khan and Salah, 2018 [87]; Banerjee et al., 2018 [68];
2	Framework	18	Viriyasitavat and Hoonsopon [84]; Sharma et al., 2017 [71]; Li et al., 2018 [79]
3	Prototype	10	Novo, 2018 [48]; Aitzhan and Svetinovic, 2018 [192]; Hammi et al., 2018 [86]
4	Others – Opinion and MCDM	3	Kshetri, 2017 [83]; Viriyasitavat, 2016 [80]

logistics, smart cities, food supply chain, mining production, transportation and logistics, and firefighting. Other prominent sectors referenced in the literature include energy, healthcare, and transportation.

5.3 Method

The methods utilised in the foundational studies are provided in Table 8. Frameworks are the most used method among the studies, with circa 40% of the studies utilising this method. The authors have defined architectures, algorithms, or service workflow specification languages. For example, Viriyasitavat and Hoonsopon defined an architecture to integrate blockchain into business process management, and Sharma et al. developed a secure distributed SDN architecture for the IoT using blockchain technology. A considerable number of studies are positioned as reviews. While they may be comprehensive [94], the authors do not explicitly clarify the method used to identify the literature. Many studies have also developed prototypes – a miniature, working version of the artefact. For example, Novo has developed a proof-of-concept implementation for scalable access management in the IoT; Bahga and Madisetti have implemented BPIIoT (Blockchain Platform for Industrial Internet of Things) to enable decentralised, trustless interaction in a peer-to-peer

network. Some other articles are positioned as opinions, and one article deployed a multi-criteria decision method (analytical hierarchical processing) to select services in service workflows.

6 Current state of research

This section addresses RQ3—Which themes are the focus of the current research? The authors have reviewed the shortlisted articles and uncovered five key themes in the published literature. While the first discusses the convergence of blockchain and the Internet of Things, the following three discuss different aspects of data – data security, data privacy, and how the data generated may be monetized. Sufficient attention is also provided to promising application areas of smart contracts. Each theme is discussed in detail in the following section.

6.1 Themes

6.1.1 Blockchain-IoT convergence

An IoT network comprises several resource-light devices (memory and computing power) [95], which cannot perform extensive computations. Integrating emerging technologies such as blockchain and the cloud-edge paradigm can enable efficient aggregation and processing of the huge data generated by the IoT nodes [96]. Current instances of IoT networks demonstrate a high degree of centralisation [97], often leading to a single point of failure/compromise [98], and the potential for manipulating the IoT data [99]. Integrating blockchain and the IoT is increasingly used to resolve challenges such as centralisation, trust, scalability, security, and privacy [100, 101]. The decentralised blockchain-based approach helps to enable credible information transmission [102], improves authentication efficiency [103], enables autonomous transaction settlement [104], preserves privacy [105], enhances trustworthiness [106], and can contain an IoT security breach in a targeted way after it is discovered [107]. Blockchain can be integrated through service-oriented architectures [108], and services/resources can be orchestrated [109] through workflows to enable interoperability of the IoT services. Blockchain further offers the facility of aggregating users' evaluation of the various component nodes and computing the reputation of each, thereby establishing a reputation management framework [98]. This framework is, in turn, utilised to ensure an adequate quality of service (QoS) in the network. The identity of nodes can be established through decentralised versions of constructs, such as self-sovereign identity that decouples the digital identity from the owner, to facilitate large-scale cooperation [110]. Other measures to ensure QoS include nonrepudiation service provisioning schemes [111], reporting service quality as penalties based on any differences between the expected and actual values [112], and decentralised QoS measurement through collectively trusted sub-networks [113]. Blockchain can also help resolve the potential issue of siloed storage—the on-chain network is used to process transactions, and an integrated off-chain network is utilised for storage and complex data processing [114]. However, this integration can also lead to performance concerns due to additional storage and computing requirements, and

communication overheads. Efforts are underway to create more efficient system designs to address these concerns by leveraging advancements such as zero-knowledge proofs [115].

6.1.2 Data privacy

An IoT ecosystem helps users access personalised services based on analysing the data sensed from the devices, which often includes data shared by the end users, but who are oblivious of how the data may be utilised [116]. While a considerable amount of data is generated owing to the large number of IoT devices, the devices cannot process the data due to resource limitations. Hence, the network depends on external environments, such as cloud-based networks to process this data [117], thereby amplifying privacy-related concerns. Data privacy includes anonymity, untraceability, unlinkability, unforgeability, and confidentiality [118], all needing to be preserved. Several approaches exist to ensure privacy in an IoT network including (i) Segregating the blockchain network into multiple channels, where each channel processes a specific data type and comprises a certain fixed number of authorised organisations; (ii) The use of cryptographic techniques [119], both within a domain and across domains [120]; (iii) The use of a privacy-preserving framework [105] to ensure data authentication and mitigation of data poisoning attacks [121]; (iv) Federated learning where the local data samples at the edges are used to train, and data models are shared instead of sharing raw data [122]; (v) Edge computing architectures in which the processing is moved to the edge of the network [123]; (vi) By storing the sensitive data off-chain [124] and (vii) By defining hierarchical smart-contract based access control [125]. The exchange of data can occur within one IoT network and across various IoT networks where the data sets could be shared to improve the overall efficiency of the ecosystem, such as for IIoT or Internet of Medical Things (IoMT) [126, 127]. Smart contracts can also be used as a governance mechanism, a data attestation service provider, or reputation management to enhance network privacy [128–130]. The authors have suggested that increased training for the stakeholders, financial investments in smart contracts, and regulatory support will help address privacy-related concerns in the long run [107].

6.1.3 Security of the ecosystem

The proliferation of intelligent devices has created the security risk of the IoT network being compromised, as bad actors can exploit networks through malicious devices or network capture [131]. A secure IoT system corresponds with the security of physical devices and networks and has a bearing on the relevant processes, technologies, and measures [132]. The network's security can be assured through several approaches: (i) The use of identity and access management systems that limit access only to authorised devices within the network, implemented through smart contracts [105, 107]. These could be based on measures such as the computed reputation scores of nodes [130, 133], or context-aware authorization management as a service [134], or multi-signature smart contracts [122] (ii) An interoperable trust framework among different blockchains [106] (iii) Lightweight agents at IoT installations to collaboratively detect distributed denials of service [135] (iv) Physical unclonable functions (PUFs) as an authentication barrier [136] and (v) Encryption methods such as two-phase encryption [137], hierarchical cryptographic key generation [138] or interplanetary file system (IPFS) to store ciphertext [126]. While the security of the network is important across all sectors, sectors such as the IoMT, Healthcare IoT, smart city, and agriculture [105, 106, 119, 139, 140] have received much attention of late.

Security frameworks in an IoT network are also subject to continuous improvement using emerging technologies such as artificial intelligence [141] through techniques including federated learning [130] and XGBoost [142]. Authorised parties could also be enabled to audit the behaviours of the auditors [143], thereby encouraging the desirable behaviour of the auditors to address post facto concerns regarding security. Implementation of security considerations should achieve an optimal balance between the security and performance of the network and incorporate energy-efficient mechanisms [144]. The security implementation should also explore various mechanisms such as a post-quantum approach given the resource constraints of the IoT devices [13].

6.1.4 Data trading in IIoT

Development of the Industrial Internet of Things (IIoT) has led to large-scale data creation, thereby enhancing the possibilities for data trading [127]. The data generated may be traded by establishing a digital data marketplace [145]. Data trading has assumed considerable significance given its potential economic impact on efficiency, decision making, and the customer's experience [146]. A good data trading model should establish the trustworthiness of the trading partners, data availability for the consumers, privacy for the data providers, transparent value creation for the suppliers and demanders, and a dispute arbitration model to resolve disagreements [147, 148]. Current data trading models are plagued by high latency, leading to poor service quality [127] and a lack of trading fairness [149]. Fair and efficient data trading protocols [127, 148], which are scalable and autonomous transaction settlement systems [104], should help to overcome such challenges. The data trading platforms can trade data packets and analytic services by utilising public and consortium blockchains [150]. Another commonly cited hindrance in the data trading market is unauthorised access to data. Several blockchain-based approaches can resolve this through measures such as traceable aggregate signature schemes [151], hybrid access control mechanisms [152], multiple access control contracts [153], attribute-based encryption schemes [154], and a combination of security by contracts, manufacturer usage description (MUD) based behavioural fingerprinting and software-defined networking [133]. Artificial intelligence and machine learning techniques are also used to optimise the analytics services in the IIoT landscape. Examples include chatbots and intelligent assistants for public engagement as part of GovTech systems [155], an AI-based data analytics framework integrated with blockchain for 5G networks [141], a deep learning-based anomaly detection engine for smart agricultural UAVs [121], and a cognitive micro natural gas industrial ecosystem [156].

6.1.5 Usage cases of smart contracts

Limited successful prototypes and a lack of critical mass have impeded large-scale adoption of smart contracts in the context of the IoT. However, some prominent applications are beginning to emerge in IIoT and several other sectors (discussed in detail in 6.2). While healthcare, energy, transportation/logistics, smart home, and agriculture show promise, several industry-agnostic applications are also being developed. Several privacy-preserving solutions are being implemented in areas such as authentication protocols [96], medical data sharing [157], parking platforms [158], consortium-based PHR (patient health record) management [126] and smart agricultural UAVs [121]. Smart contracts are also being used to build various scalable access management models [48], including ones based on

entitlement [159], attributes, access authority authentication schemes [120], hybrid access [152] and adaptive risk-based access control [160]. Other usage cases include smart grids for energy distribution [161], the use of elastic smart contracts to aid analytics/decision-making both in and between multiple IoT blockchains [162], the design of a smart healthcare system through the integration of Blockchain 3.0 and Healthcare 4.0 [163], peer-to-peer electricity trading [164], and self-tallying voting systems [165]. Smart contracts are also being integrated with other emerging technologies in usage cases such as information sharing in AI-enabled 5G networks [141], spectrum auctions for 6G mobile networks [166], the development of secure fitness frameworks integrated with machine learning approaches [167], and the auditing of the auditors' behaviour [143]. Although not widespread, usage cases are also being developed in sectors such as government (algorithmic government) [155], engineering/construction (information traceability), and tourism (integrated reservations systems based on smart contracts) [168].

6.2 Context

The sectors in which the studies were conducted are provided in Table 9. Most studies (144) analysed as part of the current state of research do not focus on any specific sector, as in the foundational studies. Most such studies have either developed a framework or a prototype. Many of the remaining 83 studies focussed on healthcare, energy, transportation/logistics, smart city/home, and agriculture. Compared to the foundational literature, while the number of studies focusing on specific sectors has increased, the percentage has reduced marginally from 72% to 63%.

6.3 Methods

The methods utilised in the studies in current state are provided in Table 10. Like the foundational studies, most studies (~70%) have developed frameworks, such as architectures [169] (an architecture for monetizing data using smart contracts), protocols [170] (a contractual routing protocol for IoT devices using smart contracts), and algorithms [171] (an algorithm for content caching). Around 15% of the studies have developed prototypes based on platforms such as Ethereum (e.g., [172]), or Hyperledger (e.g., [167]). Sixteen studies have conducted reviews based on the extant literature and identified research opportunities. Other methods include case studies, game theory, systems design, and action research.

7 Implications for future research and practice

This section addresses RQ4: What are the implications for future research and practice? The implications for future research are discussed using the TCM framework.

7.1 Implications for future research

7.1.1 Themes

The authors present seven themes (Table 11) for developing promising future research questions. Recognising that blockchain-enabled smart contracts and IoT are

Table 9 Context of Current state of research

#	Context	Number of studies	Exemplar studies
1	Multi-sector focus	144	Zheng et al. [11]; Novo [48]; Dai et al. [49] Kim and Laskowski [183]; Kshetri [107]
2	Healthcare	16	Griggs et al. [182]; Garg et al. [193]; Abou-Nassar et al. [106]
3	Energy	15	Zhang and Wen [66]; Afzal et al. [194]; Khattak et al. [161]
4	Transportation and Logistics	13	Yin et al. [195] ; Wang et al. [196]; Betti et al. [197]
5	Smart home / Smart city	10	Sun et al. [184]; Makhdoom et al. [105]; Lin et al. [198]
6	Agriculture	5	Kumar et al. [121]
7	Financial services	4	Singh et al. [199]
8	Food	4	Lin et al. [186]
9	Others – Telecom; Engineering Procurement and Construction; Oil and Gas; Government; Audit and Accounting; Tourism; Manufacturing and Education	16	Liu et al. [166]

Table 10 Methods of Current state of research

#	Method	Number of studies	Exemplar studies
1	Framework	157	Xu et al. [111]; Rahman et al. [185]; Lin et al. [187]; Garg et al. [193]; Guo et al. [103]
2	Prototype	37	Lin et al. [186]; Pan et al. [100]; Arachchige et al. [200]
3	Review	16	Zheng et al. [11]; Dai et al. [49]; Fernandez-Carames and Fraga-Lamas [13]
4	Case study	6	Sandner et al. [201]
5	Game theory	6	Kundu [128]
6	Others – Systems design, Action research, Opinion	5	Viriyasitavat et al. [97]

interdisciplinary topics, the authors have identified these across the technological-organisational-legal triad. While themes one to three (interoperability, technical characteristics, and integration with emerging technologies) correspond to the technology triad element, theme four (legal clarity) corresponds to the legal triad element. Theme five (organisational enablers) comprises research questions on the organization triad element. The concluding themes – six and seven (adoption-related studies and theoretical exploration) comprise cross-sectional questions that may be applied across any of the three triad elements.

Technology Although the smart contract was introduced in the '90 s and offers unique advantages, it is still in the early stages of development [35]. The increasing number of research papers on smart contracts year-on-year points to progressive investigation into smart contracts as a research area [6]. Developments such as advanced cryptographic schemes are leading to improvements in security and privacy considerations, and new IoT-specific protocols, such as IOTA, are focussing on reducing energy consumption, aiding sustainable growth. With the development of several newer and adjacent technologies, such as artificial intelligence [173], quantum computing [10], and 5G/6G, their integration with smart contract/blockchain and the IoT offers enormous potential. In addition, several alternative blockchains exist, and they are expected to consolidate over time. Among the existing options, there are already signs of consolidation and cooperation to enable cross-platform interoperability [174]. The interoperability of smart contracts and blockchain continues to be a relatively less explored but important research area.

Legal clarity The extant literature does not address smart contracts' legal and regulatory considerations, specifically in context of the IoT. However, some legal considerations are addressed at the generic level of smart contracts [175]. Areas such as the impact of this new ecosystem on cross-border commerce, its (mis-)alignment with existing legal statutes, and the implications concerning consumer rights have not been fully explored. This offers a fertile area for impactful cross-disciplinary research.

Organisation From the organisational perspective, limited inquiries into whether the current organisational structure is conducive to new-age industries involving smart contracts and the IoT exist. With this advanced technological intervention, the conduct of business

Table 11 Future research directions

#	Theme	Research questions
1	Interoperability	a. How can interoperability between different blockchain environments be ensured? b. How can authentication be implemented in a multi-chain smart contract? c. How can industry-wide standards be developed for the IoT and smart contracts? d. How can security and incentive mechanisms be ensured for cross-domain transactions?
2	Technical characteristics	a. What steps must be taken to reduce electricity consumption and make it eco-friendly? b. How can transaction speed be improved? c. How can the blockchain be made more scalable, given that the process of mining blocks is getting slower with the growing network? d. How can efficient big-data management of IoT devices using the cloud and blockchain be ensured? e. How can privacy in the SC-IoT combination be further enhanced? f. How can security be further enhanced by leveraging advances in cryptography?
3	Integration with emerging technologies	a. How can the SC-IoT combination be integrated with other technologies like Artificial Intelligence and Quantum computing?
4	Legal clarity	a. How can domiciling and jurisdiction-related issues be made unambiguous to aid in faster dispute resolution? b. What is the legal recourse in case of criminal and civil contract breach? c. What impact does the SC-IoT technological combination have on consumer rights? d. How can blockchain's anonymity feature impact compliance with applicable legal frameworks? e. What legal statutes need to be considered in different jurisdictions? How is it different between developed and developing countries? f. How will alignment with securities law be ensured?
5	Organizational enablers	a. How will enterprises have to restructure themselves to align with the changes in the ways of doing business induced by the SC-IoT combination? b. What must organizations do to address the skill gap in smart contracts and IoT? c. How can organizations enable larger participation in the network to ensure critical mass? d. Given the negative press associated with blockchain, how can organizations keep their reputation and customer base intact while encouraging adoption?
6	Adoption related studies	a. How can the adoption of blockchain and smart contracts be improved? b. How do different market contexts affect the drivers of adoption? c. How can the lack of education and awareness of smart contracts, blockchain, and IoT be addressed? d. How can the benefits be quantified to improve awareness and adoption? e. What industries will drive the next wave of SC-IoT adoption?

Table 11 (continued)

#	Theme	Research questions
7	Theoretical exploration	a. How can the user experience be enhanced using a Design Science Research perspective? b. How can game-theoretical approaches be implemented to enhance the adoption of smart contracts in the IoT context? c. How can the SC-IoT combination be used to solve problems of data asymmetry in specific use cases, e.g., agriculture and cross-border supply chains?

can be expected to transform significantly. Therefore, organisations need to be structured to enable such an industry. Questions about whether the workforce understands (or does it need to?) this area, how can that advance businesses, whether the current structure of the organisations enables such an industry, and how can (positive) awareness be enhanced continue to be interesting exploration areas.

Cross triad While technological, organisational, and legal dimensions could be traversed to unravel the potential of the SC-IoT combination, some streams run across all the triad components. Given the newness of the topic, adoption-related studies have not taken off. A few have already been undertaken [176, 177], but there is ample scope for furthering this initiative. Similarly, theoretical investigations into smart contracts in general have been very limited, e.g., game theory [177], given the nascent nature of this area.

7.1.2 Context

More than three-fifths of the articles demonstrated a multi-sector focus in both the foundational and current state of research. This multi-sector focus is justified since the smart contract -IoT combination is nascent. In both the foundation and current state, the articles focus on healthcare, energy, and transportation as the next three most focused sectors. As the area matures, studies should take a broader approach by moving away from multi-sector studies and address the nuances of individual sectors. Further studies should build on the groundwork laid in these three sectors and, at the same time, evaluate other sectors suitable for the application of smart contracts and the IoT.

7.1.3 Method

While reviews (38%) emerge as the most used method in foundational studies, frameworks (69%) emerge as the most popular option in the current state of research. In the current state of research, prototypes emerge as the second most used method, with reviews taking up the third position. This increased utilisation of frameworks and prototypes serves this area well, and can be interpreted as a sign of increasing maturity. Going forward, authors should focus on theory testing and building, and evaluating the usability of existing theories, as they were developed in an entirely different environment. The pace at which technological interventions are being introduced is unprecedented and calls for developing new theories. More empirical studies and case studies should also be undertaken to evaluate the efficacy of this powerful combination.

7.2 Implications for practice

Blockchain could be considered as one of the most important technological advancements since the Internet [178] that offers fundamentally transformative benefits. However, despite the hype, it is also seen by many as a yet-to-mature technology [179]. The onus is on practitioners to ensure that enterprises can grow this transformative technology, particularly around the applications of smart contracts in the IoT and other contexts, to its full potential – the current adoption levels are not commensurate with the potential. Since the adoption ratio of new technologies hundreds of years ago is believed to impact the current development levels [180], today's technology adoption will drive the development of tomorrow. Although this combination has applicability across several industries, it has been adopted

by only a few. Practitioners should focus on extending the prototypes already developed to full implementations, converting promising usage cases into prototypes, and conceiving interesting applications. Practitioners should also focus on communicating the benefits of smart contracts, given the negative press that the underlying technology has attracted. Given the lack of a critical adoption mass, practitioners could consider forming industry consortiums that help to develop common standards and, thereby drive adoption. Practitioners should also collaborate closely not only with each other but also with academia.

While our work has significant implications for practitioners and academicians, several facets of this work are useful to society. We believe our work will help improve public awareness of the SC-IoT combination. It will make the public aware of the benefits of such a powerful technological intervention and the related considerations (e.g., security, privacy, and interoperability). By highlighting the interdisciplinary nature of the SC-IoT combination, this review is also a call for action for stakeholders to collaborate to enhance its impact. Our work can be a reference point for governments, policymakers, venture capitalists, and ESG (environmental, social, and governance) proponents. The governments of different countries should collaborate to develop a unifying regulatory framework applicable to cross-border transactions. Policymakers should define policies that encourage innovative implementations of this novel technology without exposing the public to too much risk. In the current economic environment where funding is hard to come by, venture capitalists should not avoid investing in meaningful research endeavours and encouraging promising start-ups that address opportunities that can generate long-term value. Given the growing prominence of ESG considerations, ESG proponents could reference our work to ensure that the SC-IoT applications are environmentally friendly (e.g., optimise energy consumption and minimise electronic waste).

8 Limitations of this study

This paper has two primary research limitations. Firstly, blockchain, the platform on which smart contracts currently reside, is a nascent and developing technology. Although the IoT has existed for a long time, the potential benefits of its integration with smart contracts have recently picked up prominence. Consequently, the research topics and directions are yet to mature. Hence, the richness of the body of literature is limited, and as academicians explore other areas, the body of literature will mature. Secondly, the articles for this review were chosen from the Scopus database. Therefore, the compilation may have missed some relevant articles in other databases (e.g., Web of Science). Additionally, this dataset also does not include any conference publications. Since the topic is comparatively nascent, interesting concepts and developments discussed in such publications may have been omitted by this study.

9 Conclusion

Over the next few years, it is reasonable to posit that blockchain-enabled smart contracts and the IoT will transform how consumers and enterprises conduct business. Through this study, the authors have conducted a database-assisted narrative review of the SC-IoT combination and presented their findings based on the TCM framework. Based on 227 articles

extracted from Scopus, the authors have profiled the existing research (authors, journals, papers, and countries), explored the intellectual foundation of the literature, reviewed the current state of research, and identified future implications for research and practice.

This area has recently spiked academia's interest, with more than half of the articles published in 2021. IEEE-related journals emerge as the primary source of related articles, with over half of the articles being authored from China and the USA. The authors identified the fundamental roots of the literature by reviewing the references of the shortlisted articles. Decentralised data management, service orchestration through workflows, deployment challenges of BC-IoT, its usage cases, and distributed trust management comprise the underlying themes in the foundational literature. Most studies in such literature have a multi-sector focus, with a few focussing on energy, healthcare, and transportation. Most studies take the form of reviews, followed by frameworks and prototypes. The current state of research further explored the themes of BC-IoT convergence, data privacy, ecosystem security, data trading in IIoT, and specific usage cases of smart contracts. Like the foundational studies, most studies apply a multi-sector focus. Sector-focussed studies include healthcare, energy, transportation, smart homes, agriculture, and financial services. Most studies in the current state utilise frameworks and prototypes, with reviews at a distant third. Case studies, game theory, systems design, and action research have also been utilised to explore this area.

Being a relatively young area, this offers tremendous potential for further research. The authors propose seven themes across the technology-organisation-legal triad that scholars should research in future studies. Interoperability between different environments, the development of common standards, and defining authentication and security mechanisms present an interesting area of research within the technology element. Technology-related factors such as reducing energy consumption, enhancing transaction speed, scalability, efficient big data management, privacy, and security should also be thoroughly examined. The potential of blockchain to integrate with other adjacent technologies, such as artificial intelligence and cloud computing, should be examined to consider both the advantages and disadvantages. Limited studies have been undertaken in the regulatory space, and further studies should address issues around domiciling and jurisdiction, dispute resolution, consumer rights, and the applicability of existing regulatory frameworks. Through an organisational lens, studies should address how enterprises should restructure themselves to leverage this combination, apply steps to address existing skill gaps, and introduce organisational measures to contain any negative impact by bad press more effectively. Future studies should also focus on adoption-related exploration using existing adoption models, and develop new models better suited to evaluating emerging technologies. Future studies should encourage a more holistic application, testing, and development of the theoretical constructs. While existing theories should be tested and validated, this is also a call for scholars to develop new theories that align with this emerging area. As the area matures, studies should be more sector-focussed and consider nuances of specific industries – they should build on the existing studies (e.g., healthcare, energy, and transportation) and expand to other adjacent and relevant sectors. Work on developing prototypes and evaluating their performance should continue when they demonstrate the suitability of the SC-IoT to address specific gaps.

Given the nascency of the SC-IoT combination, this field will evolve rapidly, and new perspectives will continue to emerge. Hence, the authors plan to work on another study about five years from now to monitor how the technology has evolved. This future study will evaluate the body of knowledge at that point in time and help chart the new direction for research. The authors expect to leverage emerging technologies for data preparation,

visualization, and analysis processes by exploring the suitability of newer techniques such as MLOps for data extraction [181], VosViewer for data visualisation, and Python for data analysis.

Acknowledgements The authors wish to thank the Editor and the three anonymous reviewers for their valuable feedback which has helped improve the quality of the manuscript considerably. The authors also wish to thank Andrew Lochhead for proofreading the manuscript.

Funding No funding was received for conducting this study.

Data Availability The datasets generated during and/or analysed during the current study are available from the corresponding author upon reasonable request

Declarations

Conflict of Interest The authors declare that they have no known conflict of interest.

References

1. Cieplak J and Leefatt S (2016) Smart Contracts: A smart way to automate performance. Georgetown Law Technology Review. [Online]. Available: http://www.treasurer.ca.gov/cdiac/reports/rateswap04-12.pdf. Accessed 28 Jan 2024.
2. Buterin V (2014) Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. *Etherum*, 1–36.
3. Szabo N (1997) Formalizing and Securing Relationships on Public Networks. First Monday
4. Kumari A, Tanwar S (2022) Multiagent-based secure energy management for multimedia grid communication using Q-learning. Multimed Tools Appl 81(25):36645–36665. https://doi.org/10.1007/s11042-021-11491-x
5. Eenmaa-Dimitrieva H, Schmidt-Kessen MJ (2019) Creating markets in no-trust environments: The law and economics of smart contracts. Comput Law Secur Rev 35(1):69–88. https://doi.org/10.1016/j.clsr.2018.09.003
6. Ante L (2021) Smart contracts on the blockchain – A bibliometric analysis and review. Telematics Inform 57:101519. https://doi.org/10.1016/j.tele.2020.101519
7. Yen B (2016) The internet of things (IOT): Shaping the future of e-commerce
8. Wang X, Ren X, Qiu C, Xiong Z, Yao H, Leung VCM (2022) Integrating edge intelligence and blockchain: what, why, and how. IEEE Commun Surv Tutorials. https://doi.org/10.1109/COMST.2022.3189962
9. Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z (2023) Blockchain-based federated learning for securing internet of things: a comprehensive survey. ACM Comput Surv 55:9. https://doi.org/10.1145/3560816
10. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. Challenges and opportunities. Futur Gener Comput Syst 88(2018):173–190. https://doi.org/10.1016/j.future.2018.05.046
11. Zheng Z, Xie S, Dai HN, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 14(4):352. https://doi.org/10.1504/ijwgs.2018.10016848
12. Khatoon A (2020) A blockchain-based smart contract system for healthcare management. Electronics (Switzerland) 9(1):94. https://doi.org/10.3390/electronics9010094
13. Fernandez-Carames TM, Fraga-Lamas P (2019) A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. IEEE Access 7:45201. https://doi.org/10.1109/ACCESS.2019.2908780
14. Götz CS, Karlsson P, Yitmen I (2022) Exploring applicability, interoperability and integrability of Blockchain-based digital twins for asset life cycle management. Smart Sustain Built Environ 11(3):532–558. https://doi.org/10.1108/SASBE-08-2020-0115
15. Tseng FM, Palma Gil EIN, Lu LYY (2021) Developmental trajectories of blockchain research and its major subfields. Technol Soc 66:101606. https://doi.org/10.1016/j.techsoc.2021.101606

16. Sahoo S, Kumar A, Mishra R, Tripathi P (2024) Strengthening supply chain visibility with blockchain: A PRISMA-based review. IEEE Trans Eng Manag. https://doi.org/10.1109/TEM.2022.3206109
17. Noor NM, Razali NAM, Malizan NA, Ishak KK, Wook M, Hasbullah NA (2022) Decentralized access control using blockchain technology for application in smart farming. Int J Adv Comput Sci Appl 13(9):788–802. https://doi.org/10.14569/IJACSA.2022.0130993
18. Alfuhaid S, Amyot D, Anda AA, Mylopoulos J (2023) A mapping review on cyber-physical smart contracts: architectures, platforms, and challenges. IEEE Access 11:65872–65890. https://doi.org/10.1109/ACCESS.2023.3290899
19. Paul J, Alhassan I, Binsaif N, Singh P (2023) Digital entrepreneurship research: A systematic review. J Bus Res 156:113507. https://doi.org/10.1016/j.jbusres.2022.113507
20. GK Walia, M Kumar, SS Gill (2023) ai-empowered fog/edge resource management for IoT applications: a comprehensive review, research challenges and future perspectives. IEEE Commun Surv Tutorials:1–1. https://doi.org/10.1109/comst.2023.3338015.
21. Akkem Y, Biswas SK, Varanasi A (2023) Smart farming using artificial intelligence: A review. Eng Appl Artif Intell 120:105899. https://doi.org/10.1016/j.engappai.2023.105899
22. Ghiro L et al. What is a blockchain? a definition to clarify the role of the blockchain in the internet of things. arXiv preprint, Feb. 2021. [Online]. Available: http://arxiv.org/abs/2102.03750. Accessed 24 Jan 2024.
23. Mathur G, Pandey A, Goyal S (2023) A review on blockchain for DNA sequence: security issues, application in DNA classification, challenges and future trends. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-15857-1
24. Szabó I, Ternai K, Fodor S (2022) Affordances in blockchain-based financial recommendations concerned with life events and personalities. Enterp Inf Syst. https://doi.org/10.1080/17517575.2022.2081935
25. Gugueoth V, Safavat S, Shetty S, Rawat D (2023) A review of IoT security and privacy using decentralized blockchain techniques. Comput Sci Rev 50:100585. https://doi.org/10.1016/j.cosrev.2023.100585
26. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
27. Church Z (2022) Blockchain, explained. Ideas made to matter. [Online]. Available: https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained. Accessed 7 Feb 2022.
28. Lacity MC (2018) Addressing key challenges to making enterprise blockchain applications a reality. MIS Q Exec 17(3):201–222
29. Alshamsi M, Al-Emran M, Shaalan K (2022) A systematic review on blockchain adoption. Applied Sciences (Switzerland) 12(9):4245. https://doi.org/10.3390/app12094245
30. Kemmoe VY, Stone W, Kim J, Kim D, Son J (2020) Recent advances in smart contracts: a technical overview and state of the art. IEEE Access 8:117782–117801. https://doi.org/10.1109/ACCESS.2020.3005020
31. Luu L, Chu DH, Olickel H, Saxena P, Hobor A (2016) Making Smart contracts smarter. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 254–269
32. Lauslahti K, Mattila J, Seppala T (2017) Smart contracts - How will blockchain technology affect contractual practices? ETLA Reports, vol. 68. https://doi.org/10.2139/ssrn.3154043.
33. Bohyer K, Hayajneh T (2023) Modernizing contracts across industries: a review of smart contract applications and the evolving legal landscape. EAI Endorsed Transactions on Scalable Information Systems, vol. 10, no. 5. European Alliance for Innovation, pp. 1–11 https://doi.org/10.4108/eetsis.3299.
34. Irei A, Scarfone K. Smart contract benefits and best practices for security. techtarget.com. Accessed: Jan. 24, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Smart-contract-benefits-and-best-practices-for-security
35. Wu C, Xiong J, Xiong H, Zhao Y, Yi W (2022) A review on recent progress of smart contract in blockchain. IEEE Access 10:50839–50863. https://doi.org/10.1109/ACCESS.2022.3174052
36. ChainTrade. 10 Advantages of Using Smart Contracts. Medium.com. [Online]. Available: https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a. Accessed 29 Aug 2021.
37. Rezaee N, Zanjirchi SM, Jalilian N, Hosseini Bamakan SM (2023) Internet of things empowering operations management a systematic review based on bibliometric and content analysis. Telemat Inform Rep 11:100096. https://doi.org/10.1016/j.teler.2023.100096
38. Kiran DR (2019) Chapter 35 - Internet of Things. In: Production Planning and Control - A Comprehensive Approach 495–513.

39. Balaji S, Nathani K, Santhakumar R (2019) IoT technology, applications and challenges: a contemporary survey. Wireless Personal Commun 108:363–388. https://doi.org/10.1007/s11277-019-06407-w
40. Furstenau LB et al (2023) Internet of things: Conceptual network structure, main challenges and future directions. Digit Commun Networks 9(3):677–687. https://doi.org/10.1016/j.dcan.2022.04.027. (KeAi Communications Co)
41. Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M (2021) Security and privacy in IoT using machine learning and blockchain: threats and countermeasures. ACM Comput Surv 53:6. https://doi.org/10.1145/3417987
42. Mohanta BK, Jena D, Ramasubbareddy S, Daneshmand M, Gandomi AH (2021) addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J 8(2):881–888. https://doi.org/10.1109/JIOT.2020.3008906
43. CISOMAG. 10 IoT Security Incidents That Make You Feel Less Secure. CISOMAG.com. Accessed: Feb. 26, 2024. [Online]. Available: https://cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/
44. Iftikhar S et al (2023) AI-based fog and edge computing: a systematic review, taxonomy and future directions. Internet Things 21:100674. https://doi.org/10.1016/j.iot.2022.100674
45. Samriya JK, Kumar M, Gill SS (2023) Secured data offloading using reinforcement learning and Markov decision process in mobile edge computing. Intl J Network Manag 33:5. https://doi.org/10.1002/nem.2243
46. Kumar M, Raj H, Chaurasia N, Gill SS (2023) Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet Things Cyber-Phys Syst 3:309–322. https://doi.org/10.1016/j.iotcps.2023.05.006
47. Samriya JK et al (2023) Blockchain and reinforcement neural network for trusted cloud-enabled IoT network. IEEE Trans Consum Electron. https://doi.org/10.1109/TCE.2023.3347690
48. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195. https://doi.org/10.1109/JIOT.2018.2812239
49. Dai HN, Zheng Z, Zhang Y (2019) Blockchain for internet of things: a survey. IEEE Internet Things J 6(5):8076–8094. https://doi.org/10.1109/JIOT.2019.2920987
50. Witt L, Heyer M, Toyoda K, Samek W, Li D (2023) Decentral and incentivized federated learning frameworks: a systematic literature review. IEEE Internet Things J 10(4):3642–3663. https://doi.org/10.1109/JIOT.2022.3231363
51. Hisham S, Makhtar M, Aziz AA (2022) Combining multiple classifiers using ensemble method for anomaly detection in blockchain networks: a comprehensive review. [Online]. Available: www.ijacsa.thesai.org. Accessed 25 Jan 2024.
52. Suaib Akhter AFM, Zubair S, Ahmed M, Barkat Ullah ASSM (2021) Yet another investigation on blockchain in smart healthcare. Intl J Agile Syst Manag 14(4):614. https://doi.org/10.1504/ijasm.2021.10043920
53. Lin W et al (2020) Blockchain technology in current agricultural systems: from techniques to applications. IEEE Access 8:143920–143937. https://doi.org/10.1109/ACCESS.2020.3014522
54. Mirabelli G, Solina V (2022) Blockchain-based solutions for agri-food supply chains: A survey. Int J Simul Process Model. https://doi.org/10.1504/IJSPM.2021.120838
55. Wasim Ahmad R, Hasan H, Yaqoob I, Salah K, Jayaraman R, Omar M (2021) Blockchain for aerospace and defense: Opportunities and open research challenges. Comput Ind Eng 151:106982. https://doi.org/10.1016/j.cie.2020.106982
56. Ahmad W, Salah K, Jayaraman R, Yaqoob I, Omar M (2022) Blockchain in oil and gas industry: applications, challenges, and future trends. Technol Soc. https://doi.org/10.1016/j.techsoc.2022.101941
57. Lu Y (2018) Blockchain: A survey on functions, applications and open issues. J Indust Integ Manag. https://doi.org/10.1142/S242486221850015X
58. Lin SY, Zhang L, Li J, L. li Ji, and Y. Sun, (2022) A survey of application research based on blockchain smart contract. Wireless Netw 28(2):635–690. https://doi.org/10.1007/s11276-021-02874-x
59. Sharma P, Jindal R, Borah MD (2023) A review of smart contract-based platforms, applications, and challenges. Cluster Comput. https://doi.org/10.1007/s10586-021-03491-1
60. Huynh-The T et al (2023) Blockchain for the metaverse: a review. Futur Gener Comput Syst 143:401–419. https://doi.org/10.1016/j.future.2023.02.008
61. Razzaq A et al (2019) Use of Blockchain in governance: a systematic literature review. Int J Adv Comput Sci Appl 10(5):685–691. https://doi.org/10.14569/ijacsa.2019.0100585
62. Webster J, Watson RT (2002) Analyzing the past to prepare for the future: Writing a literature review. MIS Q 38(12):1662–1666. https://doi.org/10.1016/j.freeradbiomed.2005.02.032

63. Pare G, Trudel M, Jaana M, Kitsiou S (2015) Synthesizing information systems knowledge : A typology of literature reviews. Inform Manag 52:183–199. https://doi.org/10.1016/j.im.2014.08.008
64. Donthu N, Kumar S, Mukherjee D, Pandey N, Lim WM (2021) How to conduct a bibliometric analysis: An overview and guidelines. J Bus Res 133:85–296. https://doi.org/10.1016/j.jbusres.2021.04.070
65. Harzing AW, Alakangas S (2016) Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison. Scientometrics 106(2):787–804. https://doi.org/10.1007/s11192-015-1798-9
66. Zhang Y, Wen J (2017) The IoT electric business model: Using blockchain technology for the internet of things. Peer Peer Netw Appl 10(4):983–994. https://doi.org/10.1007/s12083-016-0456-1
67. Mishra AN, Raj A, Pani AK (2020) Construal level research in decision making: analysis and pushing forward the debate using bibliometric review and thematic analysis. Am Business Rev 23(1):106. https://doi.org/10.37625/abr.23.1.106-135
68. Banerjee M, Lee J, Choo KKR (2018) A blockchain future for internet of things security: a position paper. Digit Commun Networks 4(3):149–160. https://doi.org/10.1016/j.dcan.2017.10.006
69. Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 4(5):1250–1258. https://doi.org/10.1109/JIOT.2017.2694844
70. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. IEEE Access 6:32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685
71. Sharma PK, Singh S, Jeong YS, Park JH (2017) DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag 55(9):78–85. https://doi.org/10.1109/MCOM.2017.1700041
72. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z (2017) Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J 4(6):1832–1843. https://doi.org/10.1109/JIOT.2017.2740569
73. Johnson D, Menezes A, Vanstone S (2001) The elliptic curve digital signature algorithm (ECDSA). Int J Inf Secur 1(1):36–63. https://doi.org/10.1007/s102070100002
74. Yin W, Wen Q, Li W, Zhang H, Jin Z (2017) An anti-quantum transaction authentication approach in blockchain. IEEE Access 6:5393–5401. https://doi.org/10.1109/ACCESS.2017.2788411
75. Guo RUI, Shi H, Zhao Q, Zheng D (2018) Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6:11676. https://doi.org/10.1109/ACCESS.2018.2801266
76. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M (2017) MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5:1–10. https://doi.org/10.1109/ACCESS.2017.2730843
77. Xiong Z, Zhang Y, Niyato D, Wang P, Han Z (2018) When mobile blockchain meets edge computing. IEEE Commun Mag 56(8):33–39. https://doi.org/10.1109/MCOM.2018.1701095
78. Sharma PK, Chen MY, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124. https://doi.org/10.1109/ACCESS.2017.2757955
79. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y (2018) Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans Industr Inform 14(8):3690–3700. https://doi.org/10.1109/TII.2017.2786307
80. Viriyasitavat W (2016) Multi-criteria selection for services selection in service workflow. J Ind Inf Integr 1:20–25. https://doi.org/10.1016/j.jii.2016.03.003
81. Viriyasitavat W, Da Xu L, Viriyasitavat W (2014) Compliance checking for requirement-oriented service workflow interoperations. IEEE Trans Industr Inform 10(2):1469–1477. https://doi.org/10.1109/TII.2014.2301132
82. Viriyasitavat W, Martin A (2017) The reviews and analysis of the state-of-the-art service workflow specification languages. J Ind Inf Integr 8:1–7. https://doi.org/10.1016/j.jii.2017.07.002
83. Kshetri N (2017) Can blockchain strengthen the internet of things? IT Prof 19(4):68–72. https://doi.org/10.1109/MITP.2017.3051335
84. Viriyasitavat W, Hoonsopon D (2019) Blockchain characteristics and consensus in modern business processes. J Ind Inf Integr 13(2018):32–39. https://doi.org/10.1016/j.jii.2018.07.004
85. Ouaddah A, Abou Elkalam A, Ait Ouahman A (2016) FairAccess: a new Blockchain-based access control framework for the internet of things. Sec Commun Networks 9(18):5943–5964. https://doi.org/10.1002/sec.1748
86. Hammi MT, Hammi B, Bellot P, Serhrouchni A (2018) Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput Secur 78:126–142. https://doi.org/10.1016/j.cose.2018.06.004

87. Khan MA, Salah K (2018) IoT security: Review, blockchain solutions, and open challenges. Futur Gener Comput Syst 82:395–411. https://doi.org/10.1016/j.future.2017.11.022
88. Da Xu L, He W, Li S (2014) Internet of things in industries: A survey. IEEE Trans Industr Inform 10(4):2233–2243. https://doi.org/10.1109/TII.2014.2300753
89. Atlam HF, Alenezi A, Alassafi MO, Wills GB (2018) Blockchain with internet of things: benefits, challenges, and future directions. Intl J Intell Syst Appl 10(6):40–48. https://doi.org/10.5815/ijisa.2018.06.05
90. S. Nakamoto, "bitcoin: a peer-to-peer electronic cash system." Accessed: Feb. 04, 2024. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf
91. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun Surv Tutorials 18(3):2084–2123. https://doi.org/10.1109/COMST.2016.2535718
92. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE Intl Conf Pervasive Comput Commun Workshops, PerCom Workshops 2017:618–623
93. Cruz JP, Kaji Y, Yanai N (2018) RBAC-SC: Role-based access control using smart contract. IEEE Access 6:12240–12251. https://doi.org/10.1109/ACCESS.2018.2812844
94. Kitchenham B (2005) Procedures for Performing Systematic Reviews. [Online]. Available: https://www.researchgate.net/publication/228756057. Accessed 19 Jan 2024.
95. Gonzalez-Amarillo C, Cardenas-Garcia C, Mendoza-Moreno M, Ramirez-Gonzalez G, Corrales JC (2021) Blockchain-iot sensor (Biots): A solution to iot-ecosystems security issues. Sensors 21(13):1–22. https://doi.org/10.3390/s21134388
96. Zhang Y, Li B, Liu B, Hu Y, Zheng H (2021) A privacy-aware pufs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2021.3068410
97. Viriyasitavat W, Xu LD, Bi Z, Hoonsopon D (2019) Blockchain technology for applications in internet of things—mapping from system design perspective. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2019.2925825
98. Debe M, Salah K, Rehman MHU, Svetinovic D (2019) IoT public fog nodes reputation system: a decentralized solution using ethereum blockchain. IEEE Access 7:178082–178093. https://doi.org/10.1109/ACCESS.2019.2958355
99. Lockl J, Schlatt V, Schweizer A, Urbach N, Harth N (2020) Toward trust in internet of things ecosystems: design principles for blockchain-based IoT applications. IEEE Trans Eng Manag 67(4):1256–1270. https://doi.org/10.1109/TEM.2020.2978014
100. Pan J, Wang J, Hester A, Alqerm I, Liu Y, Zhao Y (2018) EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts. IEEE Internet Things J. [Online]. Available: http://arxiv.org/abs/1806.06185. Accessed 21 Jan 2024.
101. Jiang Y, Zhong Y, Ge X (2019) Smart contract-based data commodity transactions for industrial internet of things. IEEE Access 7:180856–180866. https://doi.org/10.1109/ACCESS.2019.2959771
102. Liu L, Zhang JZ, He W, Li W (2021) Mitigating information asymmetry in inventory pledge financing through the internet of things and blockchain. J Enterp Inf Manag 34(5):1429–1451. https://doi.org/10.1108/JEIM-12-2020-0510
103. Guo S, Hu X, Guo S, Qiu X, Qi F (2020) Blockchain meets edge computing: a distributed and trusted authentication system. IEEE Trans Industr Inform 16(3):1972–1983. https://doi.org/10.1109/TII.2019.2938001
104. Liu C, Xiao Y, Javangula V, Hu Q, Wang S, Cheng X (2019) NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce. IEEE Internet Things J 6(3):4680–4693. https://doi.org/10.1109/JIOT.2018.2877634
105. Makhdoom I, Zhou I, Abolhasan M, Lipman J, Ni W (2020) PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Comput Secur 88:33. https://doi.org/10.1016/j.cose.2019.101653
106. Abou-Nassar EM, Iliyasu AM, El-Kafrawy PM, Song OY, Bashir AK, El-Latif AAA (2020) DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8:111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468
107. Kshetri N (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecomm Policy 41(10):1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003
108. Viriyasitavat W, Da Xu L, Bi Z, Sapsomboon A (2019) New blockchain-based architecture for service interoperations in internet of things. IEEE Trans Comput Soc Syst 6(4):739–748. https://doi.org/10.1109/TCSS.2019.2924442

109. Nunez-Gomez C, Caminero B, Carrion C (2021) HIDRA: A distributed blockchain-based architecture for fog/edge computing environments. IEEE Access 9:75231–75251. https://doi.org/10.1109/ACCESS.2021.3082197
110. Samir E, Wu H, Azab M, Xin C, Zhang Q (2021) DT-SSIM: A decentralized trustworthy self-sovereign identity management framework. IEEE Internet Things J 9(11):7972–7988. https://doi.org/10.1109/JIOT.2021.3112537
111. Xu Y, Ren J, Wang G, Zhang C, Yang J, Zhang Y (2019) A blockchain-based nonrepudiation network computing service scheme for industrial iot. IEEE Trans Industr Inform 15(6):3632–3641. https://doi.org/10.1109/TII.2019.2897133
112. Maiti A, Raza A, Kang BH, Hardy L (2019) Estimating service quality in industrial internet-of-things monitoring applications with blockchain. IEEE Access 7:155489–155503. https://doi.org/10.1109/ACCESS.2019.2948269
113. Viriyasitavat W, Da Xu L, Bi Z, Hoonsopon D, Charoenruk N (2019) Managing QoS of internet-of-things services using blockchain. IEEE Trans Comput Soc Syst 6(6):1357–1368. https://doi.org/10.1109/TCSS.2019.2919667
114. Bai L, Hu M, Liu M, Wang J (2019) BPIIoT: A light-weighted blockchain-based platform for industrial IoT. IEEE Access 7:58381–58393. https://doi.org/10.1109/ACCESS.2019.2914223
115. Boo E, Kim J, Ko J (2021) LiteZKP: lightening zero-knowledge proof-based blockchains for IoT and edge platforms. IEEE Syst J. https://doi.org/10.1109/JSYST.2020.3048363
116. Daidone F, Carminati B, Ferrari E (2021) Blockchain-based privacy enforcement in the IoT domain. IEEE Trans Dependable Secure Comput. https://doi.org/10.1109/TDSC.2021.3110181
117. Li H, Han D, Tang M (2022) A privacy-preserving storage scheme for logistics data with assistance of blockchain. IEEE Internet Things J 9(6):4704–4720. https://doi.org/10.1109/JIOT.2021.3107846
118. Attarian R, Hashemi S (2021) An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. Comput Netw 190:11. https://doi.org/10.1016/j.comnet.2021.107976
119. Lakhan A et al (2021) Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors 21(12):1–21. https://doi.org/10.3390/s21124093
120. Xuan S, Xiao H, Man D, Wang W, Yang W (2021) A cross-domain authentication optimization scheme between heterogeneous IoT applications. Wirel Commun Mob Comput 2021:1–14. https://doi.org/10.1155/2021/9942950
121. Kumar R, Kumar P, Tripathi R, Gupta GP, Gadekallu TR, Srivastava G (2021) SP2F: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. Comput Netw 187:1–14. https://doi.org/10.1016/j.comnet.2021.107819
122. Feng C, Liu B, Yu K, Goudos SK, Wan S (2021) Blockchain-empowered decentralized horizontal federated learning for 5g-enabled UAVs. IEEE Trans Industr Inform 18(5):3582–3592. https://doi.org/10.1109/TII.2021.3116132
123. Firdaus M, Rahmadika S, Rhee KH (2021) Decentralized trusted data sharing management on internet of vehicle edge computing (Iovec) networks using consortium blockchain. Sensors 21(7):2410. https://doi.org/10.3390/s21072410
124. Satamraju KP, Malarkodi B (2021) A decentralized framework for device authentication and data security in the next generation internet of medical things. Comput Commun 180:146–160. https://doi.org/10.1016/j.comcom.2021.09.012
125. Chang J, Ni J, Xiao J, Dai X, Jin H (2021) SynergyChain_A multichain-based data sharing framework with hierarchical access control. IEEE Internet of Things. https://doi.org/10.1109/JIOT.2021.3061687
126. Wang Y, Zhang A, Zhang P, Qu Y, Yu S (2021) Security-aware and privacy-preserving personal health record sharing using consortium blockchain. IEEE Internet Things J:1–5 2021 https://doi.org/10.1109/JIOT.2021.3132780.
127. Zhang X et al (2021) A data trading scheme with efficient data usage control for industrial IoT. IEEE Trans Industr Inform 18(7):4456–4465. https://doi.org/10.1109/TII.2021.3123312
128. Kundu D (2019) Blockchain and trust in a smart city. Environ Urban ASIA 10(1):31–43. https://doi.org/10.1177/0975425319832392
129. Debe M, Salah K, Jayaraman R, Yaqoob I, Arshad J (2021) Trustworthy blockchain gateways for resource-constrained clients and IoT devices. IEEE Access 9:132875–132887. https://doi.org/10.1109/ACCESS.2021.3115150
130. ur Rehman MH, Dirir AM, Salah K, Damiani E, Svetinovic D (2021) TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT. IEEE Trans Industr Inform 17(12):8485–8494. https://doi.org/10.1109/TII.2021.3075706

131. Hameed K, Garg S, Amin MB, Kang B (2021) A formally verified blockchain-based decentralised authentication scheme for the internet of things. J Supercomp 77(12):14461–14501. https://doi.org/10.1007/s11227-021-03841-1
132. ARM, "What Is IoT Security?," ARM website. Accessed: Feb. 01, 2022. [Online]. Available: https://www.arm.com/glossary/iot-security
133. Krishnan P, Jain K, Achuthan K, Buyya R (2021) Software-Defined Security-by-Contract for Blockchain- Enabled MUD-Aware Industrial IoT Edge Networks. IEEE Trans Industr Inform:1–7 https://doi.org/10.1109/TII.2021.3084341.
134. Sylla T, Mendiboure L, Chalouf MA, Krief F (2021) Blockchain-based context-aware authorization management as a service in iot. Sensors 21(22):1–21. https://doi.org/10.3390/s21227656
135. Spathoulas G, Giachoudis N, Damiris GP, Theodoridis G (2019) Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. Future Internet 11(11):226. https://doi.org/10.3390/fi11110226
136. Patil AS, Hamza R, Hassan A, Jiang N, Yan H, Li J (2020) Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. Comput Secur 97:2020–2023. https://doi.org/10.1016/j.cose.2020.101958
137. Islam A, Kader MF, Shin SY (2019) BSSSQS: A blockchain-based smart and secured scheme for question sharing in the smart education system. J Inform Commun Conv Eng 17(3):174–184. https://doi.org/10.6109/jicce.2019.17.3.174
138. Saha R et al (2021) The blockchain solution for the security of internet of energy and electric vehicle interface. IEEE Trans Veh Technol 70(8):7495–7508. https://doi.org/10.1109/TVT.2021.3094907
139. Pranto TH, Noman AA, Mahmud A, Haque AB (2021) Blockchain and smart contract for IoT enabled smart agriculture. PeerJ Comput Sci 7:1–29. https://doi.org/10.7717/PEERJ-CS.407
140. Liu C, Guo S, Guo S, Yan Y, Qiu X, Zhang S (2021) LTSM: lightweight and trusted sharing mechanism of IoT data in smart city. IEEE Internet Things J 9(7):5080–5093. https://doi.org/10.1109/JIOT.2021.3110097
141. El Azzaoui A, Singh SK, Pan Y, Park JH (2020) Block5GIntell: blockchain for AI-enabled 5G networks. IEEE Access 8:145918–145935. https://doi.org/10.1109/ACCESS.2020.3014356
142. Deebak BD, Turjman FAL (2021) Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. J Inform Secu Appl. 58:2021–2023. https://doi.org/10.1016/j.jisa.2021.102749
143. Lin Y, Li J, Kimura S, Yang Y, Ji Y, Cao Y (2021) Consortium blockchain-based public integrity verification in cloud storage for IoT. IEEE Internet Things J 9(5):3978–3987. https://doi.org/10.1109/JIOT.2021.3102236
144. Zhang W et al (2022) A trustworthy safety inspection framework using performance-security balanced blockchain. IEEE Internet Things J 9(11):8178–8190. https://doi.org/10.1109/JIOT.2021.3121512
145. Dixit A, Singh A, Rahulamathavan Y, Rajarajan M (2021) FAST data: a fair, secure and trusted decentralized IIoT data marketplace enabled by blockchain. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2021.3120640
146. Xiong W, Xiong L (2019) Smart contract based data trading mode using blockchain and machine learning. IEEE Access 7:102331–102344. https://doi.org/10.1109/ACCESS.2019.2928325
147. Chuang I-H, Huang S-H, Chao W-C, Tsai J-S, Kuo Y-H (2020) TIDES: A trust-aware IoT data economic system with blockchain-enabled multi-access edge computing. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2991267
148. Zhao Y, Yu Y, Li Y, Han G, Du X (2019) Machine learning based privacy-preserving fair data trading in big data market. Inf Sci (N Y) 478:449–460. https://doi.org/10.1016/j.ins.2018.11.028
149. Li Y, Li L, Zhao Y, Guizani N, Yu Y, Du X (2021) Toward decentralized fair data trading based on blockchain. IEEE Netw 35(1):304–310. https://doi.org/10.1109/MNET.011.2000349
150. Fan S, Zhang H, Zeng Y, Cai W (2020) Hybrid blockchain-based resource trading system for federated learning in edge computing. IEEE internet things J 8(4):2252–2264. https://doi.org/10.1109/JIOT.2020.3028101
151. Li T, Wang H, He D, Yu J (2021) Permissioned blockchain-based anonymous and traceable aggregate signature scheme for industrial internet of things. IEEE Internet Things J 8(10):8387–8398. https://doi.org/10.1109/JIOT.2020.3045451
152. Saha R et al (2021) DHACS: Smart contract-based decentralized hybrid access control for industrial internet-of-things. IEEE Trans Industr Inform 18(5):3452–3461. https://doi.org/10.1109/TII.2021.3108676

153. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2019) Smart contract-based access control for the internet of things. IEEE Internet Things J 6(2):1594–1605. https://doi.org/10.1109/JIOT.2018.2847705
154. Xia Q et al (2019) Secured fine-grained selective access to outsourced cloud data in IoT environments. IEEE Internet Things J 6(6):10749–10762. https://doi.org/10.1109/JIOT.2019.2941638
155. Engin Z, Treleaven P (2019) Algorithmic government: automating public services and supporting civil servants in using data science technologies. Computer J 62(3):448–460. https://doi.org/10.1093/comjnl/bxy082
156. Miao Y, Song J, Wang H, Hu L, Hassan MM, Chen M (2021) Smart Micro-GaS: a cognitive micro natural gas industrial ecosystem based on mixed blockchain and edge computing. IEEE Internet Things J 8(4):2289–2299. https://doi.org/10.1109/JIOT.2020.3029138
157. Chen Y, Meng L, Zhou H, Xue G (2021) A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection. Wirel Commun Mob Comput 2021:1–12
158. Li Z, Alazab M, Garg S, Hossain MS (2021) PriParkRec: Privacy-preserving decentralized parking recommendation service. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2021.3074820
159. Sabrina F, Jang-Jaccard J (2021) Entitlement-based access control for smart cities using blockchain. Sensors 21(16):5264. https://doi.org/10.3390/s21165264
160. Atlam HF, Walters RJ, Wills GB, Daniel J (2021) Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. Mobile Networks Appl 26(6):2545–2557. https://doi.org/10.1007/s11036-019-01214-w
161. Khattak HA, Tehreem K, Almogren A, Ameer Z, Din IU, Adnan M (2020) Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. J Inform Secu Appl 55:1–7. https://doi.org/10.1016/j.jisa.2020.102615
162. Dustdar S, Fernandez P, Garcia JM, Ruiz-Cortes A (2021) Elastic Smart contracts in blockchains. IEEE/CAA J Automatica Sinica 8(12):1901–1912. https://doi.org/10.1109/JAS.2021.1004222
163. Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E (2020) A Novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access 8:118433–118471. https://doi.org/10.1109/ACCESS.2020.3004790
164. Royo PM, Rodriguez-Molina J, Garbajosa J, Castillejo P (2021) Towards blockchain-based internet of things systems for energy smart contracts with constrained hardware devices and cloud infrastructure. IEEE Access 9:77742–77757. https://doi.org/10.1109/ACCESS.2021.3081932
165. Han G, Li Y, Yu Y, Choo K-KR, Guizani N (2020) Blockchain-based self-tallying voting system with software updates in decentralized IoT. IEEE Netw. https://doi.org/10.1109/MNET.001.1900439
166. Liu M, Wu Q, Hei Y, Li D, Hu J (2021) Fair and smart spectrum allocation scheme for IIoT based on blockchain. Ad Hoc Netw 123:1–12. https://doi.org/10.1016/j.adhoc.2021.102686
167. Jamil F, Kahng HK, Kim S, Kim DH (2021) Towards secure fitness framework based on iot-enabled blockchain network integrated with machine learning algorithms. Sensors 21(5):1–31. https://doi.org/10.3390/s21051640
168. Demirel E, Karagöz ZS, Hakan K (2021) Smart contracts in tourism industry: a model with blockchain integration for post pandemic economy. Curr Issue Tour. https://doi.org/10.1080/13683500.2021.1960280
169. Suliman A, Husain Z, Abououf M, Alblooshi M, Salah K (2019) Monetization of IoT data using smart contracts. IET Networks 8(1):32–37. https://doi.org/10.1049/iet-net.2018.5026
170. Ramezan G, Leung C (2018) A Blockchain-Based contractual routing protocol for the internet of things using smart contracts. Wirel Commun Mob Comput, 2018, https://doi.org/10.1155/2018/4029591.
171. Cui L et al (2020) CREAT: blockchain-assisted compression algorithm of federated learning for content caching in edge computing. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.3014370
172. Dai H, Shi P, Huang H, Chen R, Zhao J (2021) Towards trustworthy IoT: A blockchain-edge computing hybrid system with proof-of-contribution mechanism. Secu Commun Networks 2021:1. https://doi.org/10.1155/2021/3050953
173. Hughes L, Dwivedi YK, Misra SK, Rana NP, Raghavan V, Akella V (2019) Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. Int J Inf Manage 49:114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

174. Lacity MC, Van Hoek R. What we've learned so far about blockchain for business. MIT Sloan Management Review. Accessed: Feb. 04, 2024. [Online]. Available: https://sloanreview.mit.edu/article/what-weve-learned-so-far-about-blockchain-for-business/?og=Home+Tiled
175. Drummer D, Neumann D (2020) Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. J Inf Technol. https://doi.org/10.1177/0268396220924669
176. Badi S, Ochieng E, Nasaj M, Papadaki M (2020) Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint. Const Manag Econ 39:36. https://doi.org/10.1080/01446193.2020.1819549
177. Ullah F, Al-Turjman F (2021) A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. Neural Comput Appl 35:5033. https://doi.org/10.1007/s00521-021-05800-6
178. Crosby M, Nachiappan P, Pattanayak SV, Kalyanaraman V (2016) Blockchain technology: Beyond bitcoin. Appl Innov Rev 27(45):222–228
179. Carson B, Romanelli G, Walsh P, Zhumaev A (2018) Blockchain beyond the hype: What is the strategic business value?. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. Accessed 24 Jul 2022.
180. Comin D, Hobijn B (2010) An exploration of technology diffusion. Accessed: Feb. 04, 2024. [Online]. Available: https://www.nber.org/system/files/working_papers/w12314/w12314.pdf
181. Y Akkem, SK Biswas, A Varanasi (2023) Smart farming monitoring using ML and MLOps. In: International conference on innovative computing and communications, Springer Science and Business Media Deutschland GmbH, https://doi.org/10.1007/978-981-99-3315-0_51.
182. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):1–7. https://doi.org/10.1007/s10916-018-0982-x
183. Kim HM, Laskowski M (2018) Towards an ontology-driven blockchain design for supply chain provenance. *Intelligent Systems in Accounting*. Finance Manag. https://doi.org/10.1002/isaf.1424
184. Sun J, Yan J, Zhang KZK (2016) Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innov 2(1). https://doi.org/10.1186/s40854-016-0040-y.
185. Rahman MA, Rashid MM, Shamim Hossain M, Hassanain E, Alhamid MF, Guizani M (2019) Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7:18611–18621. https://doi.org/10.1109/ACCESS.2019.2896065
186. Lin Q, Wang H, Pei X, Wang J (2019) Food safety traceability system based on blockchain and EPCIS. IEEE Access 7:20698–20707. https://doi.org/10.1109/ACCESS.2019.2897792
187. Lin X, Li J, Wu J, Liang H, Yang W (2019) Making knowledge tradable in edge-ai enabled IoT: a consortium blockchain-based efficient and incentive approach. IEEE Trans Industr Inform. https://doi.org/10.1109/TII.2019.2917307
188. Liu B, Yu XL, Chen S, Xu X, Zhu L (2017) Blockchain based data integrity service framework for IoT data. Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017 468–475, 2017 https://doi.org/10.1109/ICWS.2017.54.
189. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J (2018) Untangling blockchain: A data processing view of blockchain systems. IEEE Trans Knowl Data Eng 30(7):1366–1385. https://doi.org/10.1109/TKDE.2017.2781227
190. Kang J, Yu R, Huang X, Maharjan S, Zhang Y, Hossain E (2017) Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans Industr Inform 13(6):3154–3164. https://doi.org/10.1109/TII.2017.2709784
191. Bahga A, Madisetti VK (2016) Blockchain platform for industrial internet of things. J Softw Eng Appl 09(10):533–546. https://doi.org/10.4236/jsea.2016.910036
192. Aitzhan NZ, Svetinovic D (2018) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secure Comput 15(5):840–852. https://doi.org/10.1109/TDSC.2016.2616861
193. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G (2020) anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 8:159402–159414. https://doi.org/10.1109/ACCESS.2020.3020513
194. Afzal M, Huang Q, Amin W, Umer K, Raza A, Naeem M (2020) Blockchain enabled distributed demand side management in community energy system with smart homes. IEEE Access 8:37428–37439. https://doi.org/10.1109/ACCESS.2020.2975233

195. Yin A et al (2019) An efficient collaboration and incentive mechanism for Internet of Vehicles (IoV) with Secured Information Exchange Based on Blockchains. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2019.2949088
196. Wang Y, Yu J, Yan B, Wang G, Shan Z (2020) BSV-PAGS: blockchain-based special vehicles priority access guarantee scheme. Comput Commun. https://doi.org/10.1016/j.comcom.2020.07.012
197. Betti Q, Khoury R, Hallé S, Montreuil B (2019) Improving hyperconnected logistics with blockchains and smart contracts. IT Prof. [Online]. Available: http://arxiv.org/abs/1904.03633. Accessed 22 Jan 2024.
198. Lin C, He D, Kumar N, Huang X, Vijayakumar P, Choo KKR (2020) HomeChain: a blockchain-based secure mutual authentication system for smart homes. IEEE Internet Things J 7(2):818–829. https://doi.org/10.1109/JIOT.2019.2944400
199. Singh H, Jain G, Munjal A, Rakesh S (2020) Blockchain technology in corporate governance: disrupting chain reaction or not? Corp Govern (Bingley) 20(1):67–86. https://doi.org/10.1108/CG-07-2018-0261
200. Arachchige PCM, Bertok P, Khalil I, Liu D, Camtepe S, Atiquzzaman M (2020) A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Trans Industr Inform 16(9):6092–6102. https://doi.org/10.1109/TII.2020.2974555
201. Sandner P, Lange A, Schulden P (2020) The role of the CFO of an industrial company: An analysis of the impact of blockchain technology. Future Internet 12(8):128. https://doi.org/10.3390/FI12080128