In search of lost security. A systematic literature review on how blockchain can save the IoT revolution

Riccardo Occa[1], Yari Borbon-Galvez[1,2], Fernanda Strozzi[1] *

[1] Centro sulla Logistica e il Supply Chain Management, LIUC Università Carlo Cattaneo, Via Corso Matteotti 22, 21053 – Castellanza – Italy (yborbon@liuc.it; fstrozzi@liuc.it; rocca@liuc.it)

[2] University of Antwerp, Department of Transport and Regional Economics. Prinsstraat 13, 2000 Antwerpen, Belgium (yari.borbon@uantwerpen.be)

** Corresponding author*

Abstract: The Internet of Things (IoT) is one of the technologies belonging to the 4.0 industry environment that has found the greatest application in recent years. The large amount of data collected and analysed through the use of a multitude of different types of sensors are, in fact, the basis of some of the main innovations that have crossed the business world in recent years. So far, its diffusion has been limited by several factors. Among these is the important role played by cyber security issues and the possible vulnerability of the Internet of Things to cyber threats. This criticality originated from several elements, such as the large amount of data generated after the adoption of the technology, but also the need to transmit the very same data. In addition, there is the great variety of sensors and devices adopted exposed to risk. Among the possible solutions, one of the most promising is the adoption of the blockchain, which may contribute to the provision of elements such as privacy, security, non-repudiation, all necessary for the proper functioning of an IoT system. The objective of this research is to understand whether the adoption of a blockchain to support IoT devices can actually solve the safety issues that otherwise exist. In order to understand how the blockchain can be a tool used to increase the security of IoT adoption in enterprises, this paper presents a systematic review of the literature on blockchain proposals and solutions currently implemented or planned, thus overcoming the current limitations in IoT deployment. Several proposals based on different approaches and architectures have been identified, such as the integration of IoT Blockchain and cloud computing, fog computing, or the benefits of using smart contracts in the IoT world.

Keywords: IOT, Internet of things, Blockchain, Distributed systems

1.Introduction

The Internet of things (IoT) is a type of network connected to the internet under stipulated protocols by way of sensors to exchange information to achieve smart recognitions, positioning, tracing, monitoring, and administration (Patel, Patel and Scholar, 2016). Thus, IoT enables the development and management of increasing amounts of data to potentially improve processes or create new services and products.

With the spread of the IoT on the market, the interest of the scientific world in the subject has also grown, as can be seen from the graph in Figure 1.

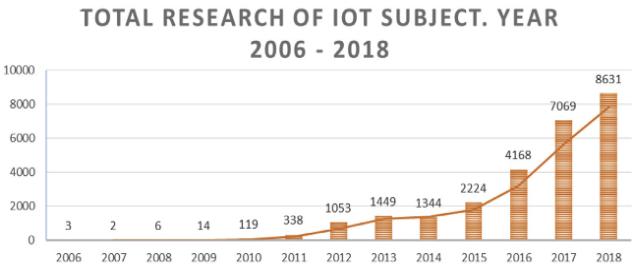

Figure 1: Research IoT subject adapted by Dachyar (2019)

1.1 The Internet of Things characteristics and threats

There is no standard and unique architecture and model for the application of the IoT to date. This is due to several factors, on the one hand the diversity of application areas and uses of IoT equipment, on the other the great variability of architectures, technologies and models that make up the varied world of IoT. (Ala *et al.*, 2015) analysed the elements that most commonly make up IoT infrastructures and summarized some of the most used elements. Between these elements it is possible to identify:

- Identification elements (Naming and addressing), such as EPC, uCode or IPV4 / IPV 6 standards.
- Sensing elements, like Smart sensors or wearable sensors, actuators or RFID tags.
- Computation Elements (both Hardware than Software), such as smartphone, smart things, Arduino and OS and clous softwares.
- Communication elements as RFID, NFC, WiFI
- Service elements, as identity related IoT or information aggregation IoT (as in Smart grids) or ubiquitous IoT (eg. Smart cities applications)
- Semantic elements, as code languages or ontologies as RDF, OWL orEXI.

The IoT, unfortunately, also poses many risks that stem from multiple sources. For one thing, the large amount of data and information generated also corresponds to an equal amount to be protected (Miorandi et al., 2012),

while the same information risks being intercepted or modified during its transfer (Weber, 2010). Additionally, the extreme variety of components, protocol elements and processes that the IoT is composed of leads to the union of their weaknesses (Gubbi et al., 2013).

1.2 Blockchain and IoT

The blockchain is a peer to peer decentralized paradigm created to ensure privacy and security. It also provides interesting features, such as data immutability, verifiability, transparency and audibility (Shrestha and Kim, 2019).

Since its inception by Satoshi Nakamoto in 2008, the technology has continued to grow (Nakamoto, 2008.); although its fame is often linked to the thematic wing of cryptocurrency (in particular Bitcoin), the blockchain's applications extend to many areas, from smart contract to distributed ledger to product traceability, constituting a new area of great interest.

In recent years, there has also been a strong focus on possible interactions between Blockchain and the Internet of Things (Dorri, Kanhere and Jurdak, 2017; Rakovic *et al.*, 2019; Shrestha and Kim, 2019).

1.3 Research question

The objective of this paper is to understand how and to what extent the adoption of the blockchain can lead to a perception of improved IT security and, therefore, to a wider adoption of IoTs.

The rest of the paper is organised as follows: methodology, Systematic Literature Review (SLR), Bibliographic Network Analysis (BNA), conclusions and managerial implications.

2 Methodology

A Systematic Literature Network Analysis (SLNA) is the methodology used to answer the research question above.

A SLNA consists of two different phases: in the first one, asystematic literature review is carried out in order to identify the correct group of papers on which to carry out the analysis; then, an analysis of the network of citations and keywords is carried out on the identified papers (Strozzi et al., 2017).

This methodology is particularly suited to the study of a vastly expanding topic such as IoT because it makes it possible to identify, within a growing amount of scientific documentation, the elements that are most shared and that make up the most established component of research discoveries. Moreover, the use of paper selection methods based on specific parameters and not on personal preferences of the author allows to increase the reproducibility and future comparability of the results obtained. In this specific paper, the use of this methodology also makes it possible to verify whether security is actually a widely perceived issue, and, above all, whether solutions that include the use of blockchain-related methodologies have aroused interest in the scientific community or have been used as a basis for further research and development.

3 The SLR Analysis

3.1 Scope of the analysis

In this paper, models and results of the application of the blockchain in conjunction with IoT technologies have been analysed. As previously reported, both the IoTs and the Blockchain are two issues that have received a growing interest from both the scientific and economic world, and their possible union is beginning to be a topic that is becoming more and more discussed.

3.2 Locating studies, study selection and evaluation

The set of identified keywords follows: (TITLE-ABS-KEY ("Blockchain*") AND (TITLE ("Internet of thing*" OR "IOT") OR KEY ("Internet of thing*" OR "IOT")) AND (KEY ("security" OR "cyber risk* " OR "risk*") OR TITLE ("security" OR "cyber risk*" OR "risk*"))).

The choice of keywords was guided by the need to focus the research on a restricted area of integration between blockchain and IOT, that of security. For this reason, we searched only for papers containing the keywords chosen for security issues (security, cyber risk* and risk*) only within the title or keywords, and no longer generically in abstracts.

The identified keywords were used as search terms in Scopus in late January 2020.

The result was a selection of 622 papers, without distinction between journal or peer-reviewed conference papers. These papers were all published between 2016 and 2020, showing the novelty and interest in the topic. It is notable the exponential growth of the research, passing from 4 publications in 2016 to 352 in 2019.

4. Bibliographic network analysis

The Bibliographic network analysis (BNA) consists of a Citation Network Analysis (can) and Author Keywords Analysis (AKA). 622 papers resulting from the SLR process were included in the CNA in order to investigate and comprehend the process of creation and development of knowledge in the area of Blockchain implications for IOT security.

4.1 Citation Network Analysis

A citation network makes it possible to show the flow of knowledge, as the cited papers are linked with the documents that quote them, thus allowing for graphically highlighting the path that the information has taken over time. This methodology leads to the exclusion of papers that show no connection between them as isolated.

Analysing the 622 papers selected emerged a single large connected component made up of 266 papers.

In order to more clearly identify the flow of knowledge, it was therefore decided to apply the key-route algorithm

(Liu, 2013) using the Pajek software to build a "main path", a set of papers composed of the articles that most cite or are cited by the other papers of the connected component constituting the fundamental structure of the research and contents of the component itself. The key-route algorithm allows for identifying the nodes that cite or have been cited by the largest number of papers that compose the sample to be analysed, thus allowing for both the identification of the paper most relevant for the development of the theory, representing the most consolidated research in the field, and the papers that are more suitable to summarise and describe the contents of the field. The analysis of the main path allows, therefore, for building a clear knowledge flow and will be a valid tool to identify trends and variations that could not have been very visible in the general set of papers.

The application of the algorithm has allowed for the identification of a main path composed of 33 papers. These papers are reported using Pajek software with the name of the first author and the year of publication in Figure 2.

The papers are concentrated in a period from 2017 to 2020.

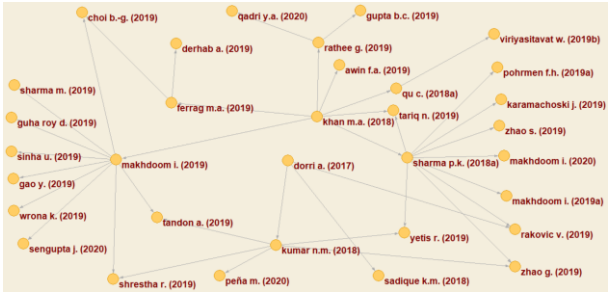

Figure 2: Papers included in the Main Path

The main path does not present a single flow of a discussion, but rather as an intersection of different themes.

The first theme that emerges within the main path is the criticality of the blockchain in being inserted in IoT systems and possible solutions to these critical issues; this topic has been present since appearing in the first paper that composes the main path: Dorri *et al.* (2017).

Dorri *et al.* (2017) present a possible application of a model that takes into consideration the inability of IoT systems to cope with the necessary high computing capacity for the operation of a blockchain when applied in the smart home sector. This model is based on a hierarchical architecture based on centralized private Immutable Ledger (IL) at the local IoT network level with the aim to reduce the problematics connected with the overhead for the systems. The simulations carried out show how the proposed model generates overheads significantly lower than the traditional blockchains, being more adherent and compatible with the needs and characteristics of IoT systems.

The conclusions drawn by Dorri *et al.*, (2017) are then taken from different reviews on the critical issues of the use of the blockchain in the IoT, which admit that there are still open issues in the full implementation of the blockchain in the IoT. To the problems highlighted previously, Rakovic, Karamachoski, Atanasovski, & Gavrilovska (2019) also add the possible impact of the human factor, as the lack of knowledge regarding the blockchain could reduce its effectiveness in the implementation phase. Sadique et al. (2018) instead focus on the need to build a clearer framework of possible types of existing IoT architectures in order to develop solutions that can be widely effective. For this reason, (Sadique, Rahmani and Johannesson, 2018) present a 6-layer framework that represents all possible IoT applications.

Another interesting finding is present in Qu & Tao, (2018), who propose a new methodology to solve the problems of credibility verification. The methodology is based on the subdivision of IoT devices into devices and manager servers, with the devices constituting a plurality of blockchain networks, called a Blockchain Structure.

The manager servers provide the devices with elements, such as private and public keys needed for encryption activities, which are responsible for transmitting and updating the information in the Blockchain Structure. Since the network is divided into different subsystems, it is not necessary to update each structure with all the information generated, but it can be compartmentalized to reduce the load of information to be processed for each device. Operatingscheme is shown in Figure 3.

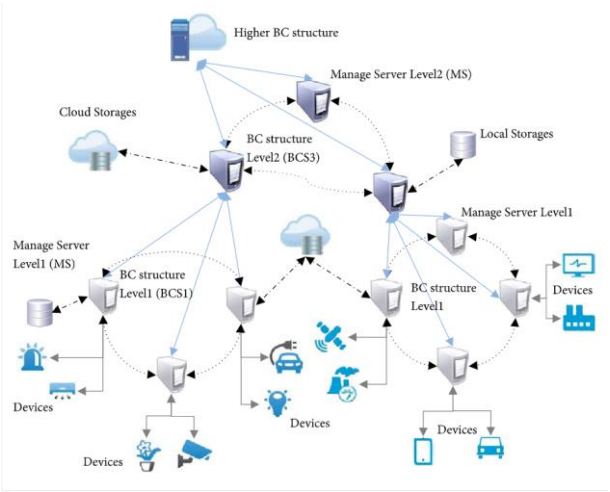

Figure 3: A credibility verification framework for IoT (Qu and Tao, 2018)

In analysing the applications of blockchain and IoT in the food sector, Peña & Llivisaca (2019) argue that a high level of collaboration between the different partners of a supply chain is a facilitator for the introduction of blockchain in IoT systems. A second theme that is widespread among the papers of the main path is the impact of blockchain in smart cities. Smart cities make extensive use of IoT systems, and the adoption of Blockchain is considered a possible solution to the resulting security problems.

Sharma & Park (2018) have proposed a possible blockchain solution designed to be implemented in the

development of Smart Cities. The solution provides a hybrid between traditional blockchain and Software Defined Networking (SDN), a technique derived from cloud computing that involves centralizing network intelligence in a separate component, disassociating the process of sending and routing data packets in order to optimize system efficiency. This solution, however, still had some critical issues, such as the efficient deployment of edge nodes and enabling of caching technique at the edge nodes.

Makhdoom, Zhou, et al. (2019) propose a different solution, based on a multi-channel approach. The hypothetical network manages the data of 11 different types of participants, including energy suppliers, banks, insurance companies and other actors. Depending on the privacy and security requirements, the data can be routed through different channels. The first channel is assumed to be constituted and managed by a government authority, and in addition to being the level with the highest security, it contains within it the parameters for the creation and control of the lower level. The scheme is repeated for each level. The different levels of security in the different channels, therefore, allow for optimizing the data flow according to the actual needs required, increasing the scalability of the architecture.

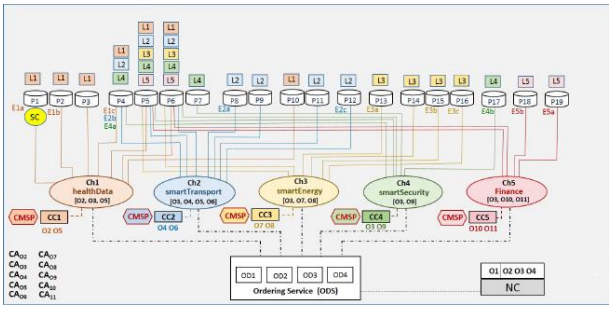

Figure 4: 5 channels model, adapted by Makhdoom, Zhou, et al. (2019)

One last theme within the main path is the possible applications of the union between Blockchain and IoT. In addition to the sectors mentioned in the above papers, such as food (Peña and Llivisaca, 2019), health, and energy (Sadique, Rahmani and Johannesson, 2018), there are some papers that specifically focus on other areas of application.

Wrona & Jarosz (2019) focus on military applications, showing how some blockchain protocols can be integrated with NATO protocols.

Sinha, Hadi, Faika, & Kim (2019), instead, present the possible security advantages to implementing the blockchain in micro solar inverter control systems.

Finally, Rathee et al. (2019) have developed a framework for the adoption of the blockchain in the field of self-driven vehicles, thus bringing safety to that specific part of the IoT market, also known as the Internet of Vehicles (IoV).

4.2 Author keywords analysis

Author Keywords analysis searches for news and emerging trends within the whole set of papers analysed. In order to develop this analysis, a co-occurrence network (Callon, Courtial and Laville, 1991) was implemented.

The co-occurrence keyword network was then analysed using VOSviewer software (van Eck and Waltman, 2010), which implements the Visualisation Of Similarities clustering technique (VOS) thatdetermines the locations of keywords in a map using a function depending on a similarity measure that is minimised. To develop the analysis, the authors' keywords that appear together for at least ten times between the 622 papers were selected. As a result, 5 clusters emerged, which we titled: 1) Blockchain Characteristic and Typologies, 2) Blockchain Management and Architectures, 3) Privacy and Security Issues, 4 Trust, 5 Smart Cities. The keywords composing the different clusters are summerized in table 1.The next subsections describe each of the clusters.

Cluster 1: Blockchain Characteristic and Typologies	**Blockchain Characteristic and Typologies (Bitcoin, Blockchain, Cryptocurrency, Data Security, Decentralization, Ethereum, Internet of Things, Network Security, Smart Contracts, Smart Home).**
Cluster 2: Blockchain Management and Architectures	**Blockchain Technology, Cloud Computing, Cybersecurity, Distributed Systems, Edge computing, Fog Computing, Internet of Things (IoT), IoT security, Machine learning, Smart cities**
Cluster 3: Privacy and Security Issues	**Authentication, Block Chain, Cryptography, Healthcare, IoT, Privacy, Security**
Cluster 4: Trust	**Access Control, Distributed Ledger, Smart Contract, Trust**
Cluster 5: Smart cities	**Security and Privacy, Smart city**

Table 1: Author keywords analysis clusters

Cluster 1 focuses on the main features of blockchain and IoT technologies and their perspectives. The keywords that make up the cluster are often used to indicate literature reviews describing both the evolution of the blockchain concept (Acharjamayum, Patgiri and Devi, 2018) and the IoT (Hirsch, 2019) and the possibilities represented by the union of the two technologies, but also to indicate several surveys on possible perspectives of these technologies, identifying the perceptions of the economic actors concerned, or the use of the first cryptocurrency systems developed by substituting the currency for authorised tokens for data transmission and access. The surveys identified show that over 93% of blockchain solution developers believe that these projects have a higher emphasis on security issues. (Ouaddah, Elkalam and Ouahman, 2017; Bosu *et al.*, 2019).

Cluster 2 takes a similar approach to cluster 1, with the presence of reviews and application cases of blockchain and IoT. The difference between the two clusters is the high relevance of solutions that cluster 2 keyword papers

provide to other architectures for data transmission and management, fog computing and edge computing.

These methods "provide a way to distribute some of the computing functions to the edge of the network where most of the data originates and is consumed" (Zahid, Hussain and Ferworn, 2019), resulting in increased system efficiency and reduced overall data transmission needs.

Integrating the fog computing model into the blockchain and IoT can then be the way to provide high availability, real-time data delivery, scalability, security, resilience, and low latency (Sharma, Chen and Park, 2018).

Cluster 3 focuses mainly on privacy and security; in addition to demonstrating how the blockchain can be more efficient than the standards currently used to ensure our digital identity and privacy, it shows how it can also increase the security of digital transactions (Kravitz and Cooper, 2017). From the keywords of this cluster, it is possible to trace back to papers that give great emphasis to possible applications in healthcare, where the need to ensure maximum confidentiality of sensitive patient information and data can easily be traced back to the use of the blockchain (Padmavathi and Rajagopalan, 2019), and where wearable IoT devices are becoming increasingly popular today. The importance of the blockchain's healthcare applications is also linked to the further possibility of effectively tracking stocks of medicines, thus preventing alteration or abuse of the same, or ensuring their correct disposal.

However, most of the research currently carried out is limited to a theoretical estimate of the impact of the proposed solutions, and the wide interest of the academic world has been followed by a more limited number of real applications (Padmavathi and Rajagopalan, 2019).

The combination of IoT and Blockchain can also facilitate the spread of patterns of self-treatment and self-management of chronic diseases, such as diabetes, by providing patients with real-time information on their parameters to indicate the correct dosages and treatment times (Azbeg *et al.*, 2018).

The content of cluster 4 is focused on the concept of trust, that may not be present for several reasons.

A first cause of the lack of trust can be identified in the variability of IoT systems, which are based on different protocols that often fail to be made secure by simplified PKI models; blockchain-based trust models can help to overcome this criticality (Di Pietro *et al.*, 2018).

Another criticality related to trust is the use of systems belonging to third party companies, as in the case of cloud or fog computing. Also in this case, possible blockchain solutions have been developed that show their benefits in increasing trust between partners (Kochovski *et al.*, 2019).

Finally, there is the issue of access control. As the number of connected devices and the services based on them increases, it is necessary to create control systems that are reliable not only from the point of view of security, but also of resilience, thus avoiding, for example, the possibility that a single node makes it impossible to access the network in case of malfunction. The use of distributed control systems developed through blockchain can be the answer to these needs. Also in this case the discussion on the proposed solutions still seems to be limited to the academic field, without an effective implementation phase in companies. (Drame-Maigne, Laurent and Castillo, 2019).

The content of the fifth cluster focuses primarily on the impact that integration between Blockchain and IoT can have on security in the development of smart cities. Two different types of content can be discerned in this cluster.

The first concerns the generic types of architectures proposed to mitigate the risks of devices (Biswas and Muthukkumarasamy, 2016) or more generically sensors and elements that mark the transition from a traditional to a smart city. Makhdoom, Zhou, et al. (2019) is one of the articles that has already appeared in the main path.

Instead, the second group of papers focuses on the development of architectures dedicated to specific services that identify smart cities. Among these services, we can find the production and transport of energy (Chaudhary *et al.*, 2019): this is particularly critical in terms of security and for the functionality of urban systems. Indeed, the increase in the number of electric means of mobility and the high amount of sensors and devices involved are elements that create the need for a more efficient and high-performance electrical distribution network, which the blockchain can help to develop (Chaudhary *et al.*, 2019).

In addition to the issue of information security, in this case the blockchain offers solutions that are able to increase the efficiency of smart grids (Alladi *et al.*, 2019) a fundamental step to making them sustainable and effectively implementable. In the SmartGrid sector, the blockchain has already had many real-life applications, its use in conjunction with the IoT has made it possible, for example, to implement systems for the exchange and evaluation of renewable energy produced by individual users.

5. Conclusions and managerial implications

Blockchain and IoT are two topics that have been at the centre of scientific research and have also received considerable interest from the economic world. Their integration is a new area of research that has seen growing interest in recent years. This article is an attempt to rationalise the content of research developed in the context of the integration of the IoT and Blockchain.

The study revealed how the growing interest from the scientific world has been followed by the growth of possible areas of application of integrated blockchain and IoT, thus showing the considerable potential of these technologies. The integration between blockchain and IoT has shown to be recognized as a valuable step in a large number of sectors, at least by the scientific world. However, a real sharing of this perspective by the business world is not confirmed at the moment. in some specific areas, however, such as the energy market, it shows how technology can actually be considered an effective

solution even by players in the business world. Finally, a positive view of the possible impacts by developers and companies working on the implementation of blockchain technologies is widely diffused.

However, it emerged that this integration is not without difficulties, as there are still some complexities arising from various factors, such as the need for high scalability of solutions, the problems related to the low computing capacity of the IoT and the high demand for data transmission typical of blockchain infrastructures that usually need to transmit updated information to all nodes that make up the same, with the result of multiplying transmission activities. These critical issues lead to develop specific solutions for use in IoT systems.

The first specific solutions developed usually tend to address only some of these problems but the simulations carried out during their development suggest that they may actually mitigate the problems and have allowed for testing the first real applications. Therefore, they can be considered a promising step in the process of creating a comprehensive model, whereby integrating the different approaches may lead to the realization of a fully functional blockchain that integrates with IoT systems.

If in the coming years attempts to build functional blockchain architectures continue successfully along the path taken and the problems identified above are definitively eliminated, then they can bring significant benefits to many areas and contribute to the decisive affirmation of the IoT in many areas of daily life, from healthcare to transport, and participate in the evolution of the management of the cities we live in.

The managerial implications of our analysis are of two different types. First, the identification of blockchain models that can also be applied to IoT systems can increase confidence in this technology and encourage its faster and more widespread adoption, with the consequence of increasing the benefits that the use of IoT can bring, such as the development of new market segments based on digital interaction or the development of new products and services (Miorandi *et al.*, 2012).

Secondly, the presentation of the different problems and solutions currently existing in the application of blockchain and IoT can facilitate a faster development of architectures and models that can be applied massively on the market, thus making large-scale applications, such as those assumed by Makhdoom *et al.* (2019), possible. With the integration of digital services of multiple companies made feasible, the potential would be created for the development of supply chains, cities and systems with very high connection and real-time integration increasing the efficiency of the systems.

The main limitation in this study is related to the lack of primary data available from the business world. The type of analysis, focused on the evidence of scientific research, allows in fact to have a clear picture of the developments of this research, but does not allow to directly analyze the impressions and the evolution of the topic within the entrepreneurial world. Further future studies carried out through interviews with entrepreneurs, panels of experts or focus groups could help to broaden the field of observations to the realities on the market.

7. References

Acharjamayum, I., Patgiri, R. and Devi, D. (2018) 'Blockchain: A Tale of Peer to Peer Security', in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, pp. 609–617. doi: 10.1109/SSCI.2018.8628826.

Ala, A.-F. *et al.* (2015) 'A Survey on Social Internet of Things', *IEEE Communications Surveys & Tutorials*, 17(4), pp. 2347–2376.

Alladi, T. *et al.* (2019) 'Blockchain in smart grids: A review on different use cases', *Sensors (Switzerland)*, 19(22), pp. 1–25. doi: 10.3390/s19224862.

Azbeg, K. *et al.* (2018) 'Blockchain and IoT for Security and Privacy: A Platform for Diabetes Self-management', *2018 4th International Conference on Cloud Computing Technologies and Applications, Cloudtech 2018*. IEEE, pp. 1–5. doi: 10.1109/CloudTech.2018.8713343.

Biswas, K. and Muthukkumarasamy, V. (2016) 'Securing Smart Cities Using Blockchain Technology', in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, pp. 1392–1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

Bosu, A. *et al.* (2019) 'Understanding the Motivations, Challenges and Needs of Blockchain Software Developers: A Survey. (arXiv:1811.04169v2 [cs.SE] UPDATED)', *arXiv Computer Science*. Empirical Software Engineering. doi: arXiv:1811.04169v2.

Callon, M., Courtial, J. P. and Laville, F. (1991) 'Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemsitry', *Scientometrics*, 22(1), pp. 155–205. doi: 10.1007/BF02019280.

Chaudhary, R. *et al.* (2019) 'BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system', *Computers & Security*, 85, pp. 288–299. doi: 10.1016/j.cose.2019.05.006.

Dorri, A. *et al.* (2017) 'Blockchain for IoT Security and Privacy: The Case Study of a Smart Home', in.

Dorri, A., Kanhere, S. S. and Jurdak, R. (2017) 'Towards an optimized blockchain for IoT', in *Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week)*. Association for Computing Machinery, Inc, pp. 173–178. doi: 10.1145/3054977.3055003.

Drame-Maigne, S., Laurent, M. and Castillo, L. (2019) 'Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts', *2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019*, pp. 1582–1587. doi: 10.1109/IWCMC.2019.8766478.

van Eck, N. J. and Waltman, L. (2010) 'Software survey:

VOSviewer, a computer program for bibliometric mapping', *Scientometrics*, 84(2), pp. 523–538. doi: 10.1007/s11192-009-0146-3.

Gubbi, J. *et al.* (2013) 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 29(7), pp. 1645–1660. doi: 10.1016/j.future.2013.01.010.

Hirsch, P. B. (2019) 'The goose that laid the golden eggs: personal data and the Internet of Things', *Journal of Business Strategy*, 40(1), pp. 48–52. doi: 10.1108/JBS-10-2018-0176.

Kochovski, P. *et al.* (2019) 'Trust management in a blockchain based fog computing platform with trustless smart oracles', *Future Generation Computer Systems*. Elsevier B.V., 101, pp. 747–759. doi: 10.1016/j.future.2019.07.030.

Kravitz, D. W. and Cooper, J. (2017) 'Securing user identity and transactions symbiotically: IoT meets blockchain', in *2017 Global Internet of Things Summit (GIoTS)*. IEEE, pp. 1–6. doi: 10.1109/GIOTS.2017.8016280.

Liu, X. (2013) 'Full-Text Citation Analysis : A New Method to Enhance', *Journal of the American Society for Information Science and Technology*, 64(July), pp. 1852–1863. doi: 10.1002/asi.

Makhdoom, I. *et al.* (2019) 'PrivySharing : A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities', *Computers & Security*. Elsevier Ltd, p. 101653. doi: 10.1016/j.cose.2019.101653.

Miorandi, D. *et al.* (2012) 'Internet of things: Vision, applications and research challenges', *Ad Hoc Networks*. Elsevier B.V., pp. 1497–1516. doi: 10.1016/j.adhoc.2012.02.016.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: www.bitcoin.org.

Ouaddah, A., Elkalam, A. A. and Ouahman, A. A. (2017) 'Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT', in Rocha Á., Serrhini M., F. C. (ed.) *Europe and MENA Cooperation Advances in Information and Communication Technologies. Advances in Intelligent Systems and Computing, vol 520*. Springer, Cham, pp. 523–533. doi: 10.1007/978-3-319-46568-5_53.

Padmavathi, U. and Rajagopalan, N. (2019) 'A research on impact of blockchain in healthcare', *International Journal of Innovative Technology and Exploring Engineering*, 8(9 Special Issue 2), pp. 35–40. doi: 10.35940/ijitee.I1007.0789S219.

Patel, K. K., Patel, S. M. and Scholar, P. G. (2016) 'Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges', *International Journal of Engineering Science and Computing*. doi: 10.4010/2016.1482.

Peña, M. and Llivisaca, J. (2019) 'Blockchain and Its Potential Applications in Food Supply Chain Management in Ecuador', 3, pp. 101–112. doi: 10.1007/978-3-030-32022-5.

Di Pietro, R. *et al.* (2018) 'A blockchain-based trust system for the internet of things', *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*, pp. 77–83. doi: 10.1145/3205977.3205993.

Qu, C. and Tao, M. (2018) 'Blockchain Based Credibility Verification Method for IoT Entities', 2018.

Rakovic, V. *et al.* (2019) 'Blockchain Paradigm and Internet of Things', *Wireless Personal Communications*. Springer New York LLC. doi: 10.1007/s11277-019-06270-9.

Rathee, G. *et al.* (2019) 'A blockchain framework for securing connected and autonomous vehicles', *Sensors (Switzerland)*, 19(14), pp. 1–15. doi: 10.3390/s19143165.

Sadique, K. M., Rahmani, R. and Johannesson, P. (2018) 'Towards security on internet of things: Applications and challenges in technology', in *Procedia Computer Science*. Elsevier B.V., pp. 199–206. doi: 10.1016/j.procs.2018.10.168.

Sharma, P. K., Chen, M. Y. and Park, J. H. (2018) 'A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT', *IEEE Access*. Institute of Electrical and Electronics Engineers Inc., 6, pp. 115–124. doi: 10.1109/ACCESS.2017.2757955.

Sharma, P. K. and Park, J. H. (2018) 'Blockchain based Hybrid Network Architecture for the Smart City', *Future Generation Computer Systems*. Elsevier B.V. doi: 10.1016/j.future.2018.04.060.

Shrestha, R. and Kim, S. (2019) 'Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities', in *Advances in Computers*. Academic Press Inc., pp. 293–331. doi: 10.1016/bs.adcom.2019.06.002.

Sinha, U. *et al.* (2019) 'Blockchain-Based Communication and Data Security Framework for IoT-Enabled Micro Solar Inverters', *2019 IEEE CyberPELS, CyberPELS 2019*. IEEE, pp. 1–5. doi: 10.1109/CyberPELS.2019.8925096.

Strozzi, F. *et al.* (2017) 'Literature review on the "smart factory" concept using bibliometric tools', *International Journal of Production Research*. Taylor and Francis Ltd. doi: 10.1080/00207543.2017.1326643.

Weber, R. H. (2010) 'Internet of Things - New security and privacy challenges', *Computer Law and Security Review*. Elsevier Ltd, 26(1), pp. 23–30. doi: 10.1016/j.clsr.2009.11.008.

Wrona, K. and Jarosz, M. (2019) 'Use of blockchains for secure binding of metadata in military applications of IoT', *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, pp. 213–218. doi: 10.1109/WF-IoT.2019.8767315.

Zahid, J. I., Hussain, F. and Ferworn, A. (2019) 'A Model of Computing and Communication for Public Safety Integrating FirstNet, Edge Computing, and Internet of Things', *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*. Doi: 10.1109/IEMCON.2019.8936153.