The Blockchain-based Internet of Things Development: Initiatives and Challenges

Sergio F. T. de O. Mendonca[1,2], Joao F. da Silva Junior[1] and Fernanda M. R. de Alencar[1]
[1]Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brazil
[2]Unidade Acadêmica de Garanhuns, Universidade Federal Rural de Pernambuco, Garanhuns, Brazil
e-mail: sergio.mendonca@ufpe.br, joao.fsilva2@ufpe.br, fmra@ufpe.br

***Abstract*—The Internet was originally built based on trust. After several leaks of information, new risks and challenges are introduced. In recent years, we have used even more new devices based on the Internet. Among the main concerns reported on the literature, we need some special attention to trust, protection of data and privacy. In this scenario, a new paradigm has emerged, some information security based on transparency instead of current models of information security on closed and obscure approaches. Some initiatives have been emerging with Blockchain methods and technologies. In this paper, we propose to build an initial view of the model, as a result of our preliminary investigations, described in the Methodology as systematic mapping. The initial results allowed the perception of the initial requirements involved and open problems. We report on some frameworks, models, approaches, and other Blockchain-based Internet of Things (IoT) initiatives. We also evaluate the adherence of each paper to ten IoT key requirements. This work contributes to the new and still developing body of knowledge in the areas of security, privacy and trust. Our findings are useful not only for future studies in the Academy but also for companies from various sectors present in the Internet ecosystem. They can benefit from the consolidated knowledge and use it to guide the definition of their development processes geared to the new paradigms of the IoT.**

***Keywords*—Blockchain; Internet of Things; IoT; Ontology; Privacy; Security.**

I. Introduction

The Internet of Things (IoT) is an application domain that integrates different technological and social fields. Despite the diversity of research on IoT, its definition remains fuzzy [1]. With the increase in demand and production of the new devices based on the IoT paradigms, trust and privacy can be even harder for the engineering field. Security flaws in the IoT might lead, for instance, to malicious attacks on secrecy and authentication, silent attacks on service integrity, or attacks on network availability, such as the Denial of Service (DoS). However, privacy and anonymity, on the other hand, are no less severe issues and must be integrated into the design to give users control over their privacy.

In this respect, a new approach has arisen in the security and transparency of information, which takes the place of current models of information security and is based on closed and obscure approaches. Some initiatives have come up with Blockchain methods and technologies [2].

Among the problems of building devices (or embedded systems) based on the IoT paradigm, we can highlight the absence of formalism, language or modeling architecture that enables the unified development and integration among the various disciplines of the Semantic Web Stack. We are faced with certain difficulties; in addition to complexity and scalability, there are also time latency problems (currently 10 minutes in the Bitcoin network) and the number of confirmations that must be required for transactions, contradicting IoT conceptions regarding real-time processing [1]. The transactions in the Bitcoin network are visible to all nodes. That presents some difficulties (i.e., transactions carried out only for a few nodes of the network), when we need devices for controlled environments [3].

In this context, it is fundamental to comprehend how the traditional software development could be adapted or evolved to support those new Blockchain-based IoT requirements. What consolidated knowledge is, which factors influence on device development are.

To achieve the goal of this study, we are conducting a systematic mapping of critical factors in IoT paradigms-based, embedded systems building. In this research, we are looking for answers to the following questions: i) has Blockchain-based IoT been constructed to stand on development processes? Also, ii) which Blockchain-based IoTs characteristics, principles or requirements have been considered in Blockchain-based IoT development processes? These research questions will be answered in Section IV.

The main objective of this research is to understand Blockchain-based IoT domains as well as best practices in the field, and to present the latest research about the construction of devices (or things). In addition, this effort contributes to the very new and still growing knowledge regarding security, privacy and trust (areas still very undeveloped) of the IoT. This study is useful not only for future studies in academia but also for companies from various sectors operating in the Internet ecosystem. These companies can benefit from the consolidated knowledge and use it to guide the definition of their development processes geared to the new paradigms of the IoT.

The remainder of this paper is organized as follows. In Section II, a briefing about the state of the art is presented. Section III presents the planning, conduction, and reporting of the Systematic Mapping. Section IV presents the preliminary studies results. Section V presents current trends and challenges; and in Section VI, conclusions and future work are discussed.

II. STATE OF THE ART

In this section, we present initial concepts for the understanding of this paper. The IoT and the Blockchain and its ontology overviews are briefly presented below.

A. The Internet of Things overview

The IoT consists of a global network of billions of uniquely identifiable and addressable objects, embedded with sensors, actuators, and controllers. Those are connected to the Internet in wireless mode [4]. The IoT is a "dynamic global network infrastructure that can self-configure using standards and using interoperability protocols where things (physical and virtual) have identities, attributes, and uniqueness, feature intelligent interfaces, and it can be seamlessly integrated into the network" [2].

The IEEE presents IoT as an application domain that incorporates different technological and social fields. IEEE described the phrase Internet of Thing as a network of items each embedded with sensors which are connected to the Internet [5]. It is a (non-approved) description of the Internet of Things. However, this statement is treating just one of the physical aspects of Internet of Things [6].

B. The Blockchain overview

The Blockchain is a universal digital ledger that works at the core of decentralized financial systems, such as Bitcoin and many other decentralized systems. The blockchain keeps a record of all transaction made by each participant. Cryptography is used to verify operations and keep information on the blockchain private. Several participants verify each transaction, providing highly redundant verification and are rewarded for the computational work required.

The Blockchain technology has the ability to make the organizations that use it transparent, democratic, decentralized, secure, and efficient. The Blockchain can be used to access to financial services, it presents the primary advantages of the traditional correspondent banking system: i) consistent process standards; ii) more long-range global reconnaissance.

C. The Blockchain Ontology

A first effort to standardize this technology is the BLONDIE (Blockchain Ontology with Dynamic Extensibility) ontology. This OWL ontology can be used to express in RDF different fields of the structures of Ethereum or Bitcoin. It can also be extended to cover other Blockchain technologies. In addition, BLONDIE being OWL has the ability to make explicit knowledge available [3].

Ugarte [3] says that an ideal scenario would be that everyone would use only the original Bitcoin technology, or forks with minimum modifications. The protocol itself is already standardized and well-defined, but since Bitcoin presents many limitations and was not designed for other functionalities besides financial transactions, it is not a realistic scenario.

Currently, the interoperability between Blockchain technologies is one of the most discussed issues in the Blockchain world and this is where we must focus our efforts on. The devices would be able to communicate to each other directly to update software, manage bugs, and monitor energy usage.

III. METHODOLOGY

The research methodology was divided into four steps. In this paper, we will present only Step #2 (Systematic Mapping) of this Doctoral research, as shown in Fig. 1, and described in detail as follows.

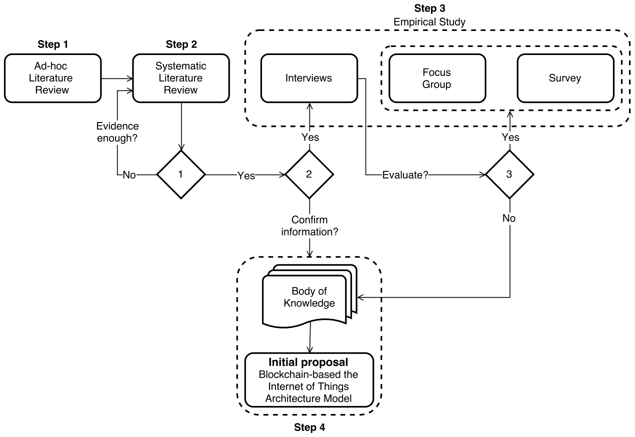

Figure 1. Scientific methodology steps. Adapted from [7].

A. Step 2—Systematic Mapping

The systematic mapping study was deemed warranted after an initial foray into the discussed topic. Before starting a systematic mapping, we came across a very broad question. To obtain an overview of this research topic and identify evidence to provide the best positions on the issues of research, we have established a systematic mapping [8],], as shown a summarization in Fig. 2. The authors still saying that the systematic mapping allows:

- Mapping the evidence of a domain at a high level of granularity;
- The identification of clusters and void of evidence to enable future systematic reviews; and
- Discover areas to conduct new primary studies.

B. Blockchain-based Internet of Things: a Systematic Mapping

1) Protocol: We have conducted this study based on the conscious guidelines and procedures. This protocol specifies the basis for the study research questions, search strategy, selection criteria, and data extraction and synthesis. The protocol was mainly developed by one of the researchers and reviewed by two of the senior researchers aiming to mitigate any bias [8].

Search string. The standard version of search string was designed to include variations and synonym terms related to

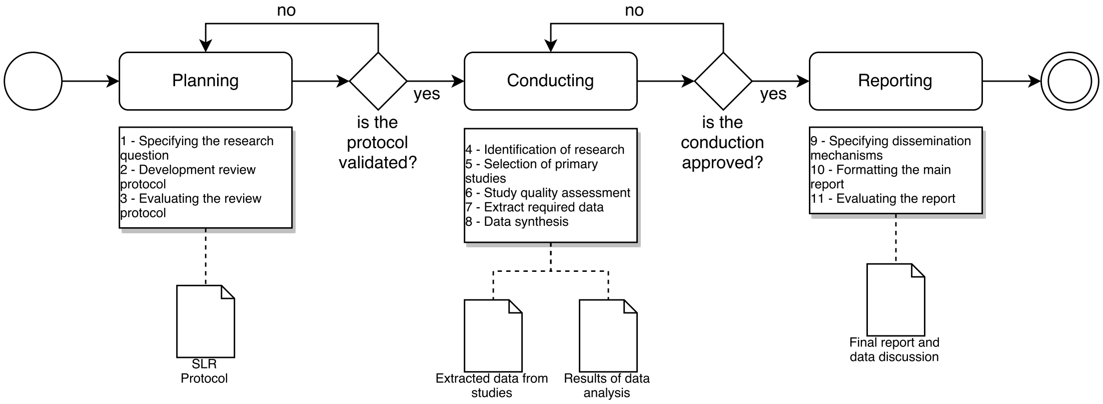
no
no
Planning
yes
is the protocol validated?
Conducting
yes
is the conduction approved?
Reporting
1 - Specifying the research question
2 - Development review protocol
3 - Evaluating the review protocol
4 - Identification of research
5 - Selection of primary studies
6 - Study quality assessment
7 - Extract required data
8 - Data synthesis
9 - Specifying dissemination mechanisms
10 - Formatting the main report
11 - Evaluating the report
SLR Protocol
Extracted data from studies
Results of data analysis
Final report and data discussion

Figure 2. Systematic Literature Mapping. Adapted from [8]

"Internet of Things", "Blockchain" and their "Development Processes".

(((model OR framework OR architecture OR process OR method OR approach OR design OR procedure) AND (development)) AND ((internet of things OR iot OR internet of everything OR web of things OR smarter planet))) AND (blockchain)

Search strategy. We selected the following search engines: ACM Digital Library, IEEE Xplorer, ISI Web of Science Science Direct, Scopus, Engineering Village. We have considered opinion of experts, gray literature, and related works of the included studies.

Inclusion and exclusion criteria. The studies were selected according to the inclusion and exclusion criteria described below. In order to select suitable studies to answer our research questions, we established the following Inclusion (IC) and Exclusion Criteria (EC):

- IC_1. The study discusses Blockchain-based IoT development processes.
- IC_2. The study addresses Blockchain-based IoT characteristics, requirements, problems or activities related to Blockchain-based IoT development processes.
- EC_1. The study is not related to Blockchain-based IoT.
- EC_2. The study does not discuss any Blockchain-based IoT development process.
- EC_3. The complete study is not available.

2) Conduction of the Research: Once the protocol had been agreed, the review review itself can be initialized. However, as noted previously, researchers were expected to try each of the steps described in this section when they construct their research protocol [8].

The author [9] recommends the adoption of effective criteria for inclusion and exclusion of relevant studies to answer the research questions. Some of the criteria are essential for the collection of a rigorous and defensible set of data for evaluation.

Therefore, we applied the inclusion and exclusion criteria involved in the analysis of the parameters 1) title and keywords check out, it was applied one 2) summary of the analysis in the work identified in the previous phase, if there are questions, reading the introduction and conclusion; and 3) the complete reading of the paper.

IV. Preliminary Studies Results

The results are reported in the systematic mapping as follows.

Table I shows the selection of studies by database (source studies). The initial search resulted in 25 works. In the first analysis, we excluded 2 items, 23 papers remaining. In the second selection, applying the criteria of inclusion and exclusion in the reading of the summary, the number of articles was reduced to 21. Upon complete reading of each of the other items, two papers, which had the same content or similar (duplicate), were found, resulting in their exclusion, leaving at the end 17 papers with strong and relevant indications to the area of investigation.

TABLE I. PRIMARY STUDIES INCLUEDED FOR SEARCH STRATEGY.

Source Studies	Retrieved	Duplicated	First Phase	Second Phase	Included
ACM Digital Library	6	-	6	5	5
IEEE Xplore	1	1	-	-	-
ISI Web of Science	1	1	-	-	-
Science Direct	3	-	1	-	-
Engineering Village	2	-	2	2	2
Manually	5	-	5	5	4
Snowballing	7	-	7	7	6
Total	25	2	21	19	17

Based on the analysis of the 17 primary studies included, we have addressed the Research Questions (RQ). In this section, we will be addressing these Questions.

RQ_1. *Has Blockchain-based IoT been constructed to stand on development processes?*

We have identified 17 initiatives of Blockchain-based IoT development as shown the Table I. Three of these initiatives are classified by the authors as Frameworks, four as Models, six as Approaches, and four as Other Initiatives. For the other studies, we created the classification Other Initiatives to Blockchain-based IoT Development, which includes single initiative of methodology, description, [re]engineering, ontology, or simulation platform for Blockchain-based IoT.

TABLE II. LIST OF INCLUDED PRIMARY STUDIES.

Study ID	Included Study	Source
S1	[10]	ACM
S2	[11]	ACM
S3	[12]	ACM
S4	[13]	ACM
S5	[6]	IEEE
S6	[14]	IEEE
S7	[15]	Snowballing
S8	[4]	Manually
S9	[16]	Snowballing
S10	[17]	Manually
S11	[5]	Manually
S12	[18]	Manually
S13	[19]	Manually
S14	[20]	Snowballing
S15	[21]	Snowballing
S16	[22]	Snowballing
S17	[23]	Snowballing

RQ_2. Which Blockchain-based IoT's characteristics, principles or requirements have been considered in Blockchain-based IoT development processes?

We reported on some frameworks, models, approaches, and other Blockchain-based IoT initiatives that reflect adherence to well-known development processes to build an initial Body of Knowledge. We detected key requirements in the IoT and we determined whether they were functional and non-functional requirements. Authors of the primary studies classified their works as follows: four as Frameworks, four as Models, two as Methods, and three as Approaches. We classified four papers as Other Initiatives addressed in initial descriptions or superficial studies.

Uckelmann, Harrison and Michahelles described key requirements (kR) that need to be considered in the IoT, as seen in Table III.

We summarized the domain type: six as generic, eight as specific, and three as non-specific. We then identified essential characteristics, processes, modeling phases, tasks and products. Most of these works (16) emphasized domain analysis, but just seven these presented a domain design, into three discussed architecture design and only two presented a detailed and comprehensive design. These papers addressed the product modeling: ten as a domain model, five as an architectural model, and one as agent model. The community still has no better support for the design, architecture, integration and testing processes to build Blockchain-based IoT.

Considering the IoT key requirements by [19], Table III depicts 100% of all studies addressed the kR1 (meet key societal needs for the IoT including open governance, security, privacy and trustworthiness). This was followed by 70.6% which addressed both kR2 (bridge the gap between B2B, business-to-consumer (B2C) and machine-to-machine (M2M) requirements through a generic and open IoT infrastructure) and kR3 (design an open, scalable, flexible and sustainable infrastructure for the IoT). Requirement kR4 (develop migration paths for disruptive technological developments to the IoT) is covered by 64.7% and kR5 (excite and enable businesses and people to contribute to the IoT) is covered by 58.8%, followed by 52.9% for both kR6 (enable businesses across different industries to develop high added value products and services) and kR8 (provide an open solution for sharing costs, benefits and revenue generation in the IoT). The other IoT key requirements did not achieve at least 50%.

We have also evaluated the adherence of each paper. In this analysis, the papers are evaluated against the ten IoT key requirements described in Table III. We highlight the importance of the studies S1, S8, S14, S15 and S16. They discuss some main activities or artifacts or modeling of design, but they did not explicitly address these activities or artifacts or modeling design in their propositions. However, they did mention some essential IoT characteristics and processes. On the other hand, we considered that studies S2, S3, S4, S5, S6, S7, S9, S10, S11, S12, S13 and S17 covered 50% or less and therefore did not explicitly address all of the IoT fundamental processes.

V. Current Trends and Challenges

The main trends and challenges discussed by the authors of the included papers about Blockchain-based IoT are described in this section.

One author [4] says that security flaws in the IoT may lead, for instance, to malicious attacks on secrecy and authentication, silent attacks on service integrity, or attacks on network availability such as the DoS. Privacy and anonymity, on the other hand, are no less serious issues. IoT devices are natural "collectors and distributors of information", so they represent a unique challenge to individual privacy.

In particular, the challenges include the ubiquitous interaction of users with smart objects and groups of things, as well as the uncontrolled concentration of such data on platforms lacking in transparency, perhaps systematically exposing users to several threats, such as identification, localization, monitoring, tracking, surveillance, manipulation, profiling, targeted advertising, data linkage, and even social engineering.

The authors in [16] investigated which are the main factors affecting the levels of integrity, anonymity, and adaptability of the blockchain. They should further analyze what are the security properties provided by the Proof of Work, which up to now is one of the key factors allowing for the achievement of distributed consensus.

The Ethereum platform supports a feature to encode rules or scripts for processing transactions through smart contracts. The authors in [10] investigated the security of running smart contracts based on Ethereum in an open distributed network. According to the authors [10][11]there are several new security problems. These bugs suggest subtle gaps in the understanding of the distributed semantics of the underlying platform. Those authors propose ways to enhance the operational semantics to make contracts less vulnerable through a symbolic execution tool called Oyente.

Blockchain has recently attracted the interest of stakeholders from the most varied sectors, from finance and health-care to utilities, real estate, and the government sector. That explosion

TABLE III. IoT KEY REQUIREMENTS ADHERENCE OF THE INCLUDED STUDIES.

Key Requirements	Frameworks				Models				Methods		Approaches			Other Initiatives				%
	S2	S14	S15	S16	S1	S5	S6	S11	S4	S7	S3	S9	S10	S17	S8	S12	S13	
1. Meet key societal needs for the Internet of Things including open governance, security, privacy and trustworthiness.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	100,0
2. Bridge the gap between B2B, business-to-consumer (B2C) and machine-to-machine (M2M) requirements through a generic and open Internet of Things infrastructure.	x	x	x	x	x		x	x	x	x			x	x	x			70,6
3. Design an open, scalable, flexible and sustainable infrastructure for the Internet of Things.		x	x	x	x	x		x		x	x	x	x		x		x	70,6
4. Develop migration paths for disruptive technological developments to the Internet of Things.		x	x	x	x		x	x	x	x		x		x			x	64,7
5. Excite and enable businesses and people to contribute to the Internet of Things.	x	x	x	x	x	x					x		x		x		x	58,8
6. Enable businesses across different industries to develop high added value products and services.		x	x	x		x	x	x	x						x	x		52,9
7. Encourage new market entrants, such as third party service and information providers, to enter the Internet of Things.		x	x	x					x			x						29,4
8. Provide an open solution for sharing costs, benefits and revenue generation in the Internet of Things.	x	x			x	x	x			x			x	x	x			52,9
9. Public initiatives to support the usage of the Internet of Things for social relevant topics.		x	x															11,8
10. Enable people to seamlessly identify things to access as well as contribute related information.		x	x	x											x			23,5
Total adherence	40,0	100,0	90,0	80,0	60,0	50,0	50,0	50,0	50,0	50,0	30,0	40,0	50,0	40,0	70,0	20,0	40,0	

of interest in Blockchain-based applications has happened because we need applications that can run only through a trusted intermediary. And, with the adoption of Blockchain strategies, we can operate without the need for a central authority [17].

The authors in [24] also say we can then create some knowledge basis by defining individual instances of these classes, filling in specific slot value information and additional slot restrictions.

A. *Threats to Validity*

We have detected some threats to validity in this Systematic Mapping:

- **The specific group of interest:** This Systematic Mapping used a specific group of search engines considered the most relevant. However, some primary studies may be missing. To mitigate this threat, we adopted the opinion of experts and snowballing.
- **The choice of primary studies:** The classification of the authors was the only evaluation criterion to select each study, restricted to IoT and Blockchain. No other nomenclature was considered.
- **Placebo effects or courtesy bias or inadequate survey instrument:** Anything that seemed to be real research, containing results without errors.
- **Number of reviewers:** SM was conducted by one researcher. We considered adopting the support of experts.
- **Study not available**: Six primary studies were not available.
- **Data extraction doubts:** Some information was not clearly available and it was very difficult to interpret. Discussions with experts were considered.

VI. Concluding Remarks and Future Work

We conducted a Systematic Mapping to investigate which primary development processes have been used in, and which factors have been influencing Blockchain-based IoT building. The ultimate goal of our research is to present the current panorama about best practices outlined in the literature to develop an initial Blockchain-based ontology model for IoT projects. The Blockchain-based IoT research area is so new and most of the papers and publications (such as a book, a technical report and others works) are concentrated in the last five years (i.e., 17 of the studies that were considered, and seen in Table II).

We reported on some frameworks, models, approaches, and other Blockchain-based IoT initiatives that present adherence to well-known development processes and endeavor to build an initial body of knowledge. We detected key requirements on the IoT and, we sorted them by functional and non-functional requirements. We also evaluated the adherence of each paper. In this analysis, the papers are evaluated against the ten IoT key requirements.

Thus, the main contribution of this paper is the understanding of the realm of Blockchain-based IoT development, and we aim to establish best practices in the construction of devices (or things) that inspire more confidence in their use (or transactions). These are the essential requirements for building a Blockchain-based IoT, and we have identified as well as characteristics, processes, former initiatives and current challenges of Blockchain-based IoT.

Our future work will address the main characteristics, models and tasks to integrate existing approaches and scalable blockchains, and in designing an architecture for IoT applications which addresses integrity, trust and security issues. Moreover, we will concentrate on building an initial body of knowledge about Blockchain-based IoT devices. We intend to conduct semistructured interviews with specialists to evaluate the original understanding.

References

[1] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" *SSRN Electronic Journal*, pp. 1–37, 2015. [Online]. Available: papers.ssrn.comhttp://www.ssrn.com/abstract=2709713

[2] M. Pilkington, "Blockchain technology: Principles and applications," pp. 1–39, Sep. 2015. [Online]. Available: http://papers.ssrn.com/abstract=2662660

[3] H. Ugarte. (2016, Nov.) Semantic blockchain: Semantic web on/with the blockchain. [Online]. Available: https://semanticblocks.wordpress.com/

[4] M. Atzori, "Blockchain-based architectures for the internet of things: A survey," Oct. 2016. [Online]. Available: https://ssrn.com/abstract=2846810

[5] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered iot users," in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2016, pp. 13–24.

[6] Y. Zhang and J. Wen, "The iot electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Apr. 2016. [Online]. Available: http://dx.doi.org/10.1007/s12083-016-0456-1

[7] A. C. Dias-Neto, R. O. Spnola, and G. H. Travassos, "Developing software technologies through experimentation: experiences from the battlefield," in *XIII Ibero-American Conference on Software Engineering*. XIII Congreso Iberoamericano en Software Engineering, May 2010.

[8] B. A. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University, Keele, Newcastle ST5 5BG, UK, techreport 2.3, Jul. 2007. [Online]. Available: https://pdfs.semanticscholar.org/e62d/bbbbe70cabcde3335765009e94ed2b9883d5.pdf

[9] T. Meline, "Selecting studies for systematic review: Inclusion and exclusion criteria," *Contemporary issues in communication science and disorders*, vol. 33, pp. 21–27, Mar. 2006.

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 254–269. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978309

[11] L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, "Demystifying incentives in the consensus computer," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: ACM, 2015, pp. 706–719. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813659

[12] P. Vigna and M. J. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York, NY, USA: St. Martin's Press, Inc., Jan. 2015.

[13] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 15–29. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660379

[14] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Feb 2015, pp. 184–191.

[15] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2Nd ACM International Workshop on IoT Privacy, Trust, and Security*, ser. IoTPTS '16. New York, NY, USA: ACM, 2016, pp. 29–36. [Online]. Available: http://doi.acm.org/10.1145/2899007.2899012

[16] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov 2016, pp. 1–6.

[17] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[18] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, no. Supplement C, pp. 461 – 466, 2016, the 7th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2016)/The 6th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2016)/Affiliated Workshops. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916322190

[19] D. Uckelmann, M. Harrison, and F. Michahelles, *An Architectural Approach Towards the Future Internet of Things*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1–24. [Online]. Available: https://doi.org/10.1007/978-3-642-19157-2_1

[20] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, "Adept: An iot practitioner perspective," IBM, techreport, 2015.

[21] A. Norta, *Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations*. Cham: Springer International Publishing, 2015, pp. 3–17. [Online]. Available: https://doi.org/10.1007/978-3-319-21915-8_1

[22] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.

[23] G. Zyskind, O. Nathan, and A. . Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.

[24] N. F. Noy and D. L. McGuinness. (2001, Feb.) Ontology development 101: A guide to creating your first ontology. [Online]. Available: http://liris.cnrs.fr/amille/enseignements/Ecole_Centrale/What%20is%20an%20ontology%20and%20why%20we%20need%20it.htm

ISBN: 978-1-61208-590-6