Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places.

António Brandão [1], Henrique São Mamede [2], Ramiro Gonçalves [3]

[1] UAb e UTAD, Portugal, ajmbrandao@gmail.com
[2] UAb - Universidade Aberta, INESC-TEC, Portugal,
[3] UTAD – Universidade Trás-os-montes e Alto Douro, INESC-TEC, Portugal

Abstract. The smart places are vulnerable with corrupted or compromised data, with the false integration of new devices, and devices with firmware versions inconsistent. These risks worsen with the increasing volume and diversity of data, devices, infrastructures and users connected to the Web. The systematic review of the literature were selected 190 documents, which reveals the growing interest on the theme of blockchain technology with the publication of 14 documents in 2014 to about 100 already in 2017. The articles focused on the areas bitcoin (about 40%), IoT (about 30%), financial (about 15%), cryptocurrencies, electronic government (about 12%), smart contracts, smart cities, business (with about 10% each) and health (about 5%). This perspective confirms the generic model study data supported in blockchain technology for smart places, especially when applied to smart cities and the specific field of the mobility ecosystem, with the use of the new concepts of the application of blockchain in IoT, smart contracts and e-governance.

Keywords: smart places; blockchain; literature review; internet of things; smart contracts; e-governance;

1 Introduction

The data generated in the smart places have quality deficiencies and problems of management and governance. Treatment of distributed data aggravates the maintenance of updates, replicate times, security, integrity and reliability of the data. The important question involves whether it is possible to develop a data management platform and information in the context of smart places, based on a generic data model, using a reliable technology.

The smart places, in the case proposed for analysis, smart cities are given ecosystem trying to represent natural ecosystems and find the data in its management and governance the basis for all the structuring of information and knowledge. The integration models, relationship, interaction, participation and access to information in distributed environments require robust connectivity infrastructure to support the growing needs of the various services and applications. The choice of a reliable

technology is crucial to provide anonymity and privacy to all its users, security, and transparency to the data.

The blockchain technology presents itself as proposed solution to the platform in a decentralized transaction environment where all transactions are recorded visibly open to everyone. The goal of blockchain is to provide confidence in data, although these attributes also configure many technical challenges and limitations that need to be addressed.

The blockchain proposed by Satoshi Nakamoto [1] in 2008 with the bitcoin cryptocurrency, intended to present as a ledger, where transactions of bitcoin users were stored, so that different transactions using the same monetary value could not occur without a centralizing entity to validate them. In Nakamoto's proposal, the transactions are visible to the members of the network through a node value transfer to another node on the network, identified in advance. The solution to achieve defense against modifications, tampering or other fraud attempts in the ledger also involves the simple detection by the network users. To get this defense to changes in the elements of the ledger, the blocks are interconnected, forming a chain.

In a simplified way, the blockchain has in its foundation: a distributed peer-to-peer network [2]; the time of creation or modification (timestamp) [3]; the one-way function with the application of applying hash functions; the digital record of the author of the amendment; and the generation of a new mechanism blockchain block.

Limitations of this process consist on the blockchain's high energy consumption with its persistent mechanism for creating new blocks that requires a large computational capacity, which limits its use and creates difficulties in process of scaling it to a large number of transactions per minute.

Architectures associated with blockchain differ from one another mainly in the process of creating new blockchain elements that stand out in the architecture associated with bitcoin and Ethereum [4]. In the case of bitcoin a high period of time is required for the confirmation of financial transactions and a large computational capacity is required as well. The Ethereum was created as an alternative to digital currency bitcoin [5], in a peer-to-peer network of virtual machines, as a platform to build and run smart contracts [6] or decentralized applications on blockchain whose use involves purchasing your own cryptocurrency, Ether. This alternative to the bitcoin limitations also features a high level of complexity, which can hinder their safety and their adoption.

The evolution of the versions of blockchain from the underlying version 1.0 of the bitcoin currency to the underlying version 2.0 to smart contracts 2.0 [7] and, more recently, to 3.0 with the introduction of new architectures and their combination intends to overcome some of the limitations of blockchain, by increasing the number of transactions per minute, the possibility of combining various types of registers and native exchange with other currency types.

With these new releases, the intensification of the number of investigations, increased investment, particularly in the areas of IoT, financial, e-governance and health, enhance the resolution of a number of limitations, extend this technology to new areas and introduce new possibilities and new architectures that create expectation. The use of blockchain in IoT applications can approach two "worlds" that could revolutionize the model of society and the way we interact and work.

A systematic review of the literature that follows describes allowed the consolidation s of some concepts, the verification of the extent of its application and the prospection of the challenges that result from the limitations of this technology.

2 Research Methodology

The methodology chosen for this work will be the Design Science (DS), the approach centered design and development, following the model presented by Peffers et al. [8] for the development of information technology artifact. The methodology will build an artifact resulting from the proposal for a generic data model to be applied in smart cities and the use of reliable technology for data.

Reliable proposed technology will be supported the blockchain which intrinsically provide the desired attributes as the anonymity and privacy to all its users and security and transparency to the data in a distributed environment.

3 Systematic review of the literature blockchain

To assess the maturity and areas of application proposals for scientific papers on blockchain also conducted a systematic review of the literature.

As the study carried out in 2016 on this same area, blockchain technology [9], where it decided to follow the process of systematic mapping [10] followed the research methodology used in this review and orientations for the systematic literature [11] for an overview of the search area, check for evidence of research and be able to quantify the evidence.

All research questions that follow were revised, keeping them essentially with the same objectives, with the exception of Q1 issue that was added.

Q1: What is the evolution over the years in the number of publications on blockchain?

Q2: What are the main features of research analyzed in research on blockchain?

Q3: What are the application areas of blockchain technology?

Q4: What are the limitations in current research in blockchain research?

Q5: What are the future trends and challenges to search for blockchain?

These questions allow globally characterize form major features revealed by research on blockchain, the trends in the application areas that perspectives, the limitations and meet the challenges that the recommendations guide us.

3.1 Research and results

The completion of the survey allowed us to collect the most relevant databases and through a systematic research, supported solely on blockchain word as word single search key, search the databases of IEEE Xplore, Springer Link, ScienceDirect, the YMCA, and the catalog Google Scholar of literature that also allowed more expeditious access to these and to other databases.

The documents were reviewed, ranked and selected systematically and we compiled a list with the following fields, document Number, Document Type, Year, Authors, Title, Abstract, Keywords and Publisher.
The documents included a number of texts outside the specific field of information sciences with the clear objective of verifying the mainstreaming of this issue and its applications. The review had repeatedly doubts about the relevance or otherwise of the document using several times the summaries and the text itself.
They selected texts only in English or Portuguese, available in digital PDF format, complete and available in the catalogs mentioned above.
The initial review contained 202 documents, but after an analysis of the content of the summary and the text 12 documents were excluded, and 190 documents analyzed (the 190 documents – ID1 to ID190 - are available in an attached list).
The analysis could have been more demanding in some documents, but sought in this study reinforce the embryonic aspects and reveal the appearance of this theme in other areas of knowledge.
To the first question, Q1 grouped and quantified the publications selected for years and resulted in the following table (Table 1).

Table 1. Evolution over the years

Year	**Qty**
2008	1
2013	1
2014	13
2015	28
2016	47
2017	100
Grand total	**190**

The analysis by year of publication reveals that this issue arises in 2008 and then in 2013 begins to grow and in 2017 (October 2017) appeared longer texts than in all previous years revealing the relevance and growing importance of the issue.
To answer questions Q2 and Q3 we considered keywords that have emerged repeatedly in the titles and abstracts, and can be found respectively in Tables 2 and 3 below.
To the question, Q2 considered the following as keywords, whose research abstracts of all selected documents resulted in the following table (Table 2).

Table 2. Characteristics

Features	**190**	
Security	60	32%
Trust	44	23%
Privacy	34	18%
Anonymity	34	18%
Scalability	14	7%

By analyzing the table above, we see the importance of safety features, trust, privacy and anonymization of work on blockchain.

The following question, Q3, considered the following applications, whose research in all selected abstracts of documents resulted in the following table (Table 3).

Table 3. Application.

Applications	**190**	
Bitcoin	73	38%
IoT (Internet of Things)	54	28%
Financial	27	14%
Cryptocurrency	23	12%
Government	23	12%
Smart contracts	19	10%
City or Cities	17	9%
Business	17	9%
Health	10	5%
Ethereum	4	2%

By analyzing these applications, which disclose the study documents, it appears that the number of new applications or application areas themselves extend. We highlight the relative decrease in bitcoin currency 38%, with the appearance of other cryptocurrencies 12% the growing importance of Internet of Things (IoT) with 28%, the application in the financial sector with 14% of e-governance with 12% of smart contracts with 10%, the smart cities and businesses both 9% and health with 5%.

4 Search Analysis

At this point, we are looking to respond to Q4 and Q5 issues presenting the issues, constraints and challenges, with the use of selected texts that the features and applications reveal.

The analysis of applications and features began by being treated independently and to each of its ratings, but the progress of the work led to the need to relate the features to the applications. Since the characteristics are transverse to the various applications verifying the documents the identification of common constraints and challenges that focus on changes or new models, architectures and algorithms.

From the selected documents we review the IoT applications, E-Governance, Smart contracts, Smart Cities, and other applications, relating them to the security (integrity, confidentiality, availability, authenticity and accountability) more trust, anonymization and scalability. We synthesized some of the responses mentioned in the review literature, guided by the limitations and challenges.

Cryptocurrencies were not focused, in particular the bitcoin, given the extensive analysis and review already conducted on these topics.

4.1 Internet of Things (IoT)

The challenge of numerous and growing devices connected to the Internet through the IoT creates needs of private and secure infrastructure, which according to [12] presents an array of threats to security and privacy in IoT to identify the platform requirements IoT and middleware, the middleware available and that security.

The IoT application is presented in [13] a network model of multiple layers based on blockchain technology, to overcome the actual implementation of difficulty of blockchain technology, we divided the network at various levels and adopted blockchain technology in which each level of the network uses security. Another model presented in [14] an architecture based on blockchain technology to access IoT, distributed cloud based with low cost of access, safe and that fits infrastructure computing needs to make IoT network more economical and competitive. Creating a distributed cloud infrastructure, the proposed model allows high performance and economical computing, where performance improvement and at the same time reduces the response time, increasing the ability to reveal real-time attacks on IoT network.

The study [15] analyzes the application of blockchain and IoT, with BigchainDB concept with a traceability system in the chain of food supplies for tracking food in real time, based on the hazard analysis and critical control points. Through an information platform for all members of the supply chain neutrality, transparency, reliability and security for these decentralized systems was allowed and could be scaled.

The changing of business models induced by IoT and e-business and simultaneously by the two reveal several model proposals referred to in [16], with the inherent problems in the reliability of the data, such as the model of e-Business of IoT, the new designs of traditional models transformed into electronic business, the trades with P2P payments IoT, that may be solved with the use of smart base contracts and blockchain technology.

The smart home based on blockchain presented in [17] and IoT reveals its security over the confidentiality, availability and integrity and simulates traffic consumption, processing time and power consumption comparing them with the solutions without blockchain.

The qualitative assessment of the architecture, presented in [18], based on blockchain on common models threat reveals its effectiveness in security and privacy of IoT applications.

Decentralized essence of blockchain minimizes the scope for fraud and manipulation by participants, through identity and access systems management that are based on blocks providing possible solutions presented in [19] to the main challenges related to the security of IoT.

The DistBlockNet solution presented in [20] allows you to discover the IoT network attacks in real time with performance and low cost, to meet the requirements to an IoT network.

4.2 Smart contracts.

The electronic contract signing protocol between two parties, supported blockchain, presented in [21], is simple, efficient and scalable because not ask a trusted third party mediator, to ensure equality between the two signing parties.

The proof of concept, held in [22], the decentralized energy trading system uses the blockchain technology with anonymous messages and multiple signatures, enable peers anonymously negotiate the energy values and effect securely business transactions with performance assessment and safety analysis in the context of privacy and security requirements.

To address the issues of transparency, trust and confidence, using smart blockchain and contracts, these may come to facilitate decentralized coordination between not confident agents.

4.3 E-governance.

The blockchain technology applied to electronic government and its services in China, said in [23], provides a more efficient and effective way to provide the services, processes, standardization, the management system and responsibility between the parties, the government and the citizen, with the promotion of their application.

4.4 Other Application Areas.

Application areas multiply as they are resolved some limitations and that renew architectures and models.

The blockchain technology also expands its applications to new practical tools for record keeping, validation and access control, presented in [24], to increase confidence, security and compliance in a variety of industry settings.

The blockchain implementations in clinical trials described in [25], appear as new methods and modern to ensure the reliability, privacy and security.

The application of blockchain technology in the financial services referred to in [26], begin to address the costs of operations, the security and privacy issues, although some challenges remain.

In control of firmware versions associated with devices, come check and update requirements when a new device is added and necessary firmware upgrade required from us a blockchain network, you get a response to determine whether the firmware is updated or not . The proposal presented in [27] ensures that the firmware added device updated, without falsification, minimizing attacks on firmware vulnerabilities in embedded devices.

The implementation of a protocol presented in [28], which transforms a blockchain an automated access control manager without the need to require reliance on third parties.

4.5 Models and architectures

At this point, we analyze the conceptual aspects that drive several investigations with the change, evaluation, comparison and presentation of new models, architectures and algorithms to overcome the limitations of blockchain.

The new consensus algorithms, the new models, and the new blockchain architectures attempt to address the limitations of this technology.

The decentralized data sharing with numerous untrusted Web participants have impact on major design decisions, as referred to in [29] and implies major architectural aspects of quality of systems and performance based on blockchain.

The "traditional" model blockchain, compared to the other models that allow the deletion of blocks and blockchain data, cannot affect the safety of the proposed new model in the study presented in [30].

The blockchain architectures have consensus algorithms that were compared in [31] and that allow arrive at the possible future trends for blockchain technology.

The feasibility study of blockchain as data processing platform distributed was analyzed in [32] and are identified several critical bottlenecks, how to achieve better platforms.

Kerberos implementations has several drawbacks that may be overcome with the use of blockchain technology, referred to in [33] in distributed environments and can also increase the safety associated with Big Data.

5 Generic Data Model with or without blockchain

The adoption of blockchain technology as trusted technology have to be demonstrated and verified with a comparative review of other technologies similar. Although the blockchain technology have with unique characteristics. This technology can be regarded as a distributed database that maintains a list of records, wherein each block contains a list of records, and each block is connected with the previous blockchain. The blockchain are replicated over the network, so that at any node one can read the records validated by each block. The records are validated through trust and are irreversible and unalterable. Confidence in the distributed network requires consensus among servers to allow transactions between unknown entities and through automatic processes prevents duplicate or conflicting transactions.

The literature review has strengthened the future of blockchain as reliable technology in areas such as the IoT, smart contracts and e-governance in decentralized environment, using the processing in cloud computing with security guarantees and transparency of data and privacy its users.

In this context, we intend to propose a generic data model to be applied in smart places, which will be in the study base to develop in the context of smart cities, focusing their review and structuring the data management aspects and its governance that will allow viable alternatives dematerialization of natural ecosystems or their subsystems.

The generic data model supported in blockchain technology for smart places, specifically applied to smart cities and in the specific domain of the mobility ecosystem,

with the use of new concepts of applying blockchain in IoT, smart contracts and e-governance.

The model proposed for development purposes and the application will focus on the ecosystem of mobility and transport, processes and subsystems involving ticketing and e-ticketing, with:

- The design a generic data model to support the concept of smart cities to lead and enable the alignment of the application of data ecosystems with natural ecosystems, applied to processes and subsystems involving ticketing or e – ticketing.
- Structuring relationships between ecosystems, participants and data to facilitate the use of blockchain technology in data management, security and privacy;
- The privacy mechanisms and reliable data management.

The use of technology as blockchain will allow a decentralized and redundant model, with the use of cloud computing models in support of the IoT and the blockchain as confidence and security layer.

The challenge of a generic data model, developed in layers, will also allow the accession process of new users can made with the use of smart contracts also supported in blockchain technology.

The model will propose the ticketing dematerialization, with protecting the privacy of users, with transparency, consistency and reliability of equipment and of the data generated.

6 Conclusions

The blockchain technology is spreading beyond the financial sector as evidenced by the 190 selected articles, whose application areas have not only bitcoin and cryptocurrencies. The various industries and various solutions are also trying to find ways to use this technology, reinventing and pushing new models, new architectures, new protocols, new algorithms that seek to overcome its limitations and challenges arise as science computing.

The features focus on security aspects, confidence, privacy, scalability and anonymization revealing its application mainly for solutions where there may be potentially unreliable aspects or where trust needs to strengthened.

The systematic literature review identified limitations, trends and challenges that are briefly described on the following items.

Some of the disclosed limitations are:

- The limiting scalability there given the requirements placed involved systems, by requiring a substantial computing power and consequent high power consumption, to verify and confirm each transaction unit.
- While allowing access to transactional information, as the transactions are public, to ensure transparency, cannot allow access to the identification of the participants in the network, to ensure confidentiality.

- Limited possibilities of data management, given the need for a decentralized service to avoid relying solely on central bodies.
- The stage of blockchain technology should also understood as a basic level protocol and limited and not as a complete business solution.

Then identifies some trends:

- The trend of centralization may come to seen given the growing need for computing capacity to verify the transactions, which can begin to change the concept of blockchain as a decentralized system, may begin to control the upgrade of the distributed record.
- The use of bockchain technology in IoT, in which with the ability to route transactions of any size, in any form, with security and confidence, can result in reliable use of IoT devices and applications.
- This technology brings the opportunity to renew the monitoring of ecosystems, especially financial, or completely change the cost structure of operations in the various businesses, although the nature of distributed registration may still appear as a threat in terms of disintermediation.

Some of the challenges are:

- Platforms with current blockchain technology is still limited and still not reach the requirements of a range and global distribution platform, requiring enhance the development of functional capabilities of this technology.
- That new solutions can develop blockchain use technology to add confidence to a non-secure environment, applying this trust model especially in unreliable parts.
- Only the Bitcoin and Ethereum platform tested on a large scale, although there are several platforms with blockchain technology to meet this challenge.
- These systems involving multiple parties will involve new governance approaches, security and economy with other technical, organizational, political and legal.

This review also allowed strengthening and verifying the potential application of a generic data model supported in blockchain technology for smart places, specifically applied to smart cities and the specific field of the mobility ecosystem, using cloud for dynamic processing and new concepts of applying blockchain in IoT, smart contracts and e-governance.

As future work, we intend to consolidate the concept of smart places, review generic data models for smart cities, and adapt to a model that describes natural ecosystems in data ecosystems, in IoT scenarios, with layers information aggregation, allowing an architecture supported in blockchain technology. As analysis system, we will apply a transport ticketing´s platform within the mobility ecosystem.

References

1. Nakamoto, S.: Bitcoin. A Peer-to-Peer Electronic Cash System (2008).
2. Decker, C., Wattenhofer, R.: Bitcoin transaction malleability and MtGox. In: European Symposium on Research in Computer Security. pp. 313–326. Springer (2014).

3. Ateniese, G., Faonio, A., Magri, B., De Medeiros, B.: Certified bitcoins. In: International Conference on Applied Cryptography and Network Security. pp. 80–96. Springer (2014).
4. Butgereit, L., Martinus, C.: A comparison of two blockchain architectures for inspiring corporate excellence in South Africa. In: Information Communication Technology and Society (ICTAS), Conference on. pp. 1–6. IEEE (2017).
5. de Lucena, A.U., Henriques, M.A.A.: Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum.
6. Fremantle, P., Scott, P.: A survey of secure middleware for the Internet of Things. PeerJ Computer Science. 3, e114 (2017).
7. Anjum, A., Sporny, M., Sill, A.: Blockchain Standards for Compliance and Trust. IEEE Cloud Computing. 4, 84–90 (2017).
8. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24, 45–77 (2007).
9. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where Is Current Research on Blockchain Technology?—A Systematic Review. PloS one. 11, e0163477 (2016).
10. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic Mapping Studies in Software Engineering. In: EASE. pp. 68–77 (2008).
11. Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M.: Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software. 80, 571–583 (2007).
12. Min, X., Li, Q., Liu, L., Cui, L.: A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size. In: Trustcom/BigDataSE/ISPA, 2016 IEEE. pp. 90–96. IEEE (2016).
13. Li, C., Zhang, L.-J.: A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. Presented at the June (2017).
14. Nakashima, H., Aoyama, M.: An Automation Method of SLA Contract of Web APIs and Its Platform Based on Blockchain Concept. Presented at the June (2017).
15. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. pp. 184–191. IEEE (2015).
16. Dennis, R., Owenson, G., Aziz, B.: A temporal blockchain: a formal analysis. In: Collaboration Technologies and Systems (CTS), 2016 International Conference on. pp. 430–437. IEEE (2016).
17. Sun, J., Yan, J., Zhang, K.Z.K.: Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation. 2, (2016).
18. Fu, D., Fang, L.: Blockchain-based trusted computing in social network. In: Computer and Communications (ICCC), 2016 2nd IEEE International Conference on. pp. 19–22. IEEE (2016).
19. Kshetri, N.: Can Blockchain Strengthen the Internet of Things? IT Professional. 19, 68–72 (2017).

20. Sharma, P.K., Singh, S., Jeong, Y.-S., Park, J.H.: DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. IEEE Communications Magazine. 55, 78–85 (2017).
21. Wan, Z., Deng, R.H., Lee, D.: Electronic Contract Signing Without Using Trusted Third Party. In: International Conference on Network and System Security. pp. 386–394. Springer (2015).
22. Zhumabekuly Aitzhan, N., Svetinovic, D.: Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing. 1–1 (2016).
23. Hou, H.: The Application of Blockchain Technology in E-Government in China. In: Computer Communication and Networks (ICCCN), 2017 26th International Conference on. pp. 1–4. IEEE (2017).
24. Patel, D., Bothra, J., Patel, V.: Blockchain exhumed. In: Asia Security and Privacy (ISEASP), 2017 ISEA. pp. 1–12. IEEE (2017).
25. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187. (2016).
26. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 4, 2292–2303 (2016).
27. Benchoufi, M., Ravaud, P.: Blockchain technology for improving clinical research quality. Trials. 18, (2017).
28. Zyskind, G., Nathan, O., Pentland, A. “Sandy”: Decentralizing Privacy: Using Blockchain to Protect Personal Data. Presented at the May (2015).
29. Fukumitsu, M., Hasegawa, S., Iwazaki, J., Sakai, M., Takahashi, D.: A Proposal of a Secure P2P-Type Storage Scheme by Using the Secret Sharing and the Blockchain. Presented at the March (2017).
30. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A Secure Sharding Protocol For Open Blockchains. Presented at the (2016).
31. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A Taxonomy of Blockchain-Based Systems for Architecture Design. Presented at the April (2017).
32. Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.-L.: BLOCKBENCH: A Framework for Analyzing Private Blockchains. Presented at the (2017).
33. Samaniego, M., Deters, R.: Blockchain as a Service for IoT. Presented at the December (2016).