Towards Blockchain-Based Architecture for Smart Cities Cyber-Security

Abla El bekkali [1] [2], Mohammed Boulmalf [2], Mohammad Essaaidi [1], Driss El majdoubi [1]

[1] ENSIAS, Mohammed V University of Rabat, ISRT
[2] UIR, International University de Rabat, TICLAB
{abla.elbekkali@uir.ac.ma, mohammed.boulmalf@uir.ac.ma, m.essaaidi@ieee.com, drisensias@gmail.com}

***Abstract*— The rapid development of urbanization poses many economic, social and environmental problems. The smart city brings smart solutions that are effective and sustainable in different areas: transportation, environment, energy and government affairs. The Internet of Things (IoT) is the basis of the structure of a smart city to interconnect all devices together. At present, and despite the potential benefits presented, IoT is still not secure by design, making its applications particularly vulnerable to security threats such as: Confidentiality and data integrity. However, there is the risk of creating urban environments with compromised data. The Blockchain has recently been proposed as a revolutionary technology that can be integrated and resolves many vulnerabilities in IoT applications. In this work, we analyze the applicability of the Blockchain to ensure the security of the data transmitted and received by the nodes of an IoT network. The purpose of this article is to integrate the Blockchain with IoT to create a secure decentralized architecture to provide a secure communication platform in a smart city.**

Keywords—Smart city, IoT, Confidentiality, Integrity, Blockchain

I. Introduction

Urbanization is a global phenomenon. By 2050, the United Nations predicts that 68% of the world's population will reside in urban areas, a figure that is rising sharply compared to the 55% of our urban population today.

Urbanization has improved the standard of living of citizens in many areas, such as: education, health, transport, economy, living and working environments [1]. Yet there are still many problems and challenges. However, cities are focusing on smarter approaches in trying to reduce costs, use resources optimally and also create a sustainable urban environment with a better quality of life [3]. Appearing in the wake of tremendous advances in the field of connected objects (IoT), software systems and information and communication technologies, Smart Cities help them meet the challenge. While the development of IoT and wireless communications have facilitated the interconnection of multiple devices as well as the ubiquitous transmission of data, even from remote sites [3]. On the other hand, the researches always affirm the existence of several limitations of the devices IoT especiallywith regard to security.

This article proposes an architecture that takes into account the limitations and capabilities of IoT devices, by integrating Blockchain technology, which is a distributed and secure transaction database, to manage Smart City data exchange.

The rest of the document is structured as follows: In Section II, context and motivation where we demonstrate the state of security in smart cities, the important role of IoT in the smart city and the difference between centralized architecture and decentralized. Then we present the Blockchain technology, its benefits and limitations for the smart city. Section III, related works where we present the existing work with an analysis. Section IV, we propose an architecture that could make the system more secure and efficient. Finally we conclude our article in sectionV.

II. Context and motivation

A. Security in smart city

Smart cities will play a significant role in different aspects of life [5]. Growth is widespread and various dimensions need to be taken into account before they can be considered a sustainable solution. Equipped with sensors collecting data, relying on information systems to optimize their services, favoring a growing use of digital, smart cities are increasingly connected.

A smart city is vulnerable to multiple security attacks because of the heterogeneous nature of devices with limited resources.

In a smart city, the cyber risk is increased by the presence of connected objects, pillars of the innovative services offered by the city. In order to preserve the functioning of the city and its services, but also to protect the personal data of their citizens, the identification of the threats and their consequences is essential as well as to design an effective solution. We then identify threats to availability regarding the maintenance of resources, integrity including unauthorized modification of data such as information corruption or manipulation, confidentiality by disclosing sensitive information by an unauthorized entity, authenticity with unauthorized access to sensitive resources and information [3].

978-1-7281-4341-5/20/$31.00 ©2020 IEEE

i. Role of the Internet of Things in the smart city

At a time when the IoT is exploding, urbanism is also making its digital transformation by putting connected objects in the service of a smarter city. IoT is a major pillar of smart cities and the IoT detection devices that are used to detect and monitor in real-time operation of various scenes in the city, are a very important part of the connection of network communication devices. [2]. The Internet of Things is therefore an indispensable component of the Smart City for data collection. Thanks to the sensors, it is indeed possible to analyze in real time information with the aim then to improve the everyday life of the inhabitants. They also help to reduce operational costs and optimize certain operations in the city.

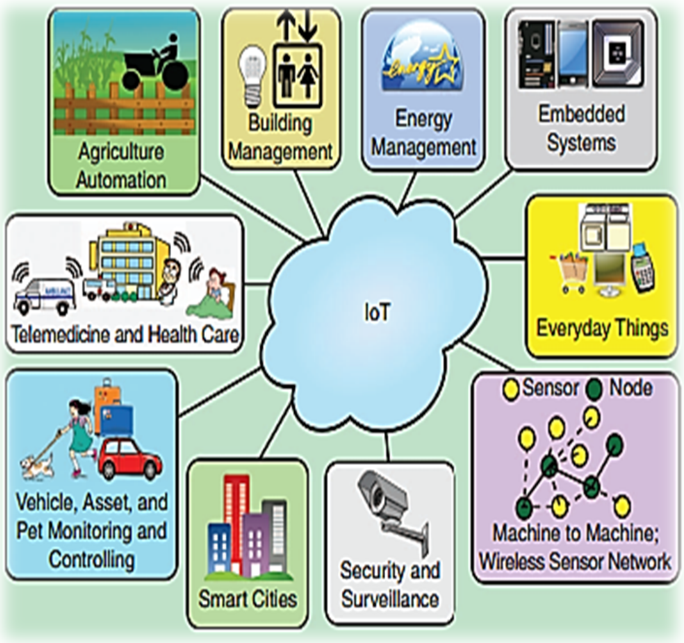
Agriculture Automation
Building Management
Energy Management
Embedded Systems
Telemedicine and Health Care
IoT
Everyday Things
Sensor
Node
Vehicle, Asset, and Pet Monitoring and Controlling
Smart Cities
Security and Surveillance
Machine to Machine; Wireless Sensor Network

Fig. 1. IoT in smart cities [24]

ii. Centralized Architecture of IoT

The IoT is at the heart of the smart city, these devices consist of network nodes, whether they are connected to a server or a computer, so they are connected to share their data. The collection of data is done by the sensors then these data are stored, processed and then presented. Currently the IoT architecture is presented by a centralized model called server / client model. This centralized model connected a large number of computer peripherals for many years, they can not communicate with each other but address a centralized gateway. This model will not be able to meet the expansion needs of the IoT system in the future, and therefore the amount of communication to manage costs will increase exponentially. Although the costs and communication issues are managed, the server / client model will remain a point of failure that can interrupt the entire network. Thus this centralized model is vulnerable to data manipulation [8]. What amplifies the complexity of security and privacy mechanisms is the heterogeneous nature of IoT. These centralized architecture models that have been used so far to authenticate, authorize, and connect different nodes in an IoT network. These centralized systems may fail when the centralized server becomes unavailable due to the growing number of devices [9].

A decentralized approach to IoT would provide a solution to many of these problems. Blockchain is one of the popular techniques of decentralization.

B. *Blockchain background*

In 2009 (Nakamoto), Blockchain technology was created as a primary payment network for Bitcoin cryptocurrency [3]. Blockchain is a system that manages transactions between partners of a distributed network such as the transfer of currencies, exchanges, writing of reports in a register, or traceability to operate on actions such as sales, purchases, tracking or movement of objects, acts of manufacture or distribution.

The implementation of a Blockchain system relies on a sequence of records chained and stored in a distributed database integrating an innovative mechanism of replication. A Blockchain-type network is therefore a distributed registry offering a high level of security, based on very specific encryption algorithms, and containing all the transactions carried out since the origin of the network creation. It is shared by all participants who each have a local copy through the replication mechanism. The network is managed by rights and permissions, so that each participant sees only the appropriate transactions [10]. Blockchain technology is based on the following [3]:

Cryptography: Used to protect the content of blocks and thus ensure that each participant sees only the relevant data for him.

Consensus protocol: Blockchain which is a decentralized distributed network offering immutability, confidentiality, security and transparency. In order to verify and validate transactions, no central authority exists, however each transaction in the Blockchain is well verified and secure thanks to the consensus protocol which is at the heart of any Blockchain network. Blockchain consensus protocols impose a system of agreement between different parties within a distributed network, thereby preventing malicious operation of the system. So Blockchain consensus protocols guarantee synchronization between all nodes on the network. The Blockchain consensus mechanism is an internal and automatic audit of its network. This protocol is therefore essential:

- It allows the Blockchain to be updated while ensuring that each block in the chain is valid.
- It prevents a single entity from having control of the entire network and therefore guarantees its decentralization.

A consensus algorithm is a procedure by which all peers in the Blockchain network reach a common agreement in the distributed register. Thus consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment [22]. There are different consensus algorithms:

- POW: Proof-of-Work is the first and most used consensus algorithm of all. Network nodes are called miners. The latter in order to validate a transaction must solve a complex mathematical problem requiring significant computing power. They therefore use a hash function allowing the transaction data to be written into the blocks and connected to each other. Once the hash registered in the blockchain, it is however falsifiable. PoW therefore ensures that miners can only validate a new transaction block and add it to the blockchain if the distributed nodes of the network reach a consensus and agree that the block hash provided by the minor is valid proof of work.

- POS: Proof-of-Stake, or proof of stake developed in 2011 as an alternative to PoW. The participants of this consensus can be assimilated to shareholders of a business entity having the right to participate in its consensus mechanism. In order to validate a block, the nodes must prove their possession of a certain amount of cryptocurrency by requiring to pledge them on the network and which will be destroyed in the event of fraud. The more this quantity is important, the node will be more likely to be chosen to update the registry of a Blockchain.

The Proof of Work, Proof of Stake are the main Blockchain consensuses. There are many others: Proof of Importance (POI), Delegated Proof of Stake (DPOS), Proof of Authority (PoA), Proof of Elapsed Time (PoET), etc.

Shared Ledger: The replicated and distributed registry is tamper-proof and contains transaction history in the form of individual records chained to each other and time stamped.

Smart Contracts: Is the second founding concept after the registry. Defines the conditions of the transaction or transfer, it is embedded in the replicate database. The participants of the network agree on the verification conditions of the transaction by applying the rules of the contract to each of them.

There are two types of Blockchain:

Public blockchains or unpermissioned**:** Do not require access permission, and are those whose transaction log is readable by everyone. Each network member has the ability to view transaction history, create smart contracts and decentralized applications. The transactions that are stored in these "Ledgers" are neither deletable nor modifiable, readable by all, well secured by cryptography, decentralized and without a central governance body [10] [11].

Private blockchains or permissioned: Request permission to access it. In order to access this type of blockchain and become a member you need an invitation and the creator of the network or user-moderator who sets the rules can approve or reject, and existing members of the network can also confirm or reject this access. The control mechanism is variable and depends on the rules. For operations, only direct participants can access them [7] [11].

i. Advantages of integrating Blockchain into the smart city

Blockchain technology is a simple and powerful way to make the city truly sustainable and smart. Trust and control in the circulation and use of data will be guaranteed, so it brings out a new economy of access. Data from different origins can thus be shared without being displaced and thus contribute in a measurable way to the emergence of new solutions [10]. Integrating the blockchain into smart city devices will create a common platform for all devices to communicate in a secure distributed environment.

The blockchain offers two key advantages over traditional centralized databases: it guarantees traceability and integrity of data in real time, allowing users to exchange information efficiently and transparently. It also allows the automation and security of processes thanks to intelligent contracts with efficiency gains [10] [14]. Blockchain helps to limit the risk of piracy during the development of a digital recording connecting thousands of computers. Indeed, the combination of the Blockchain and the IoT will allow devices to be more powerful and this will create more transparency, immutability and security in smart cities [12] [13].

ii. Limitations of integrating Blockchain into the smart city

Blockchain technology has created hope in the ICT community that it could provide a long-awaited solution to several ongoing security vulnerabilities [5]. Applications of Blockchain technology are still in their infancy and several challenges must be overcome to ensure its wider development. The first issue is a scalability issue, its lack of maturity and its security vulnerabilities that constitute an obstacle to its development in smart cities. In the future, the blockchain, possibly coupled with other new technologies, could become one of the technological pillars of the smart city, based on an increasingly integrated and automated ecosystem and a more collaborative economy [15].

III. RELATED WORKS

A. Presentation of existing works

The smart city its goal is to improve the quality of life and the services of a city, as well as to convert it into a more sustainable space, through the integration of new services based on information technologies, communication and more generally digital in the daily lives of citizens. These new services are based on technologies and concepts such as Big Data, the Internet of Things (IoT) that cities and communities must understand to achieve these objectives. Cities everywhere are facing 4 major challenges: growing urbanization, aging infrastructure, quality of life and security. Several researchers present solutions to deal with its problems. In this section after a long study of all the solutions proposed in this field we have chosen precisely to discuss and analyze the solutions of these researchers knowing that they are the most recent and which approaches the good secure and decentralized architecture with minimal risks.

Biswas and Muthukkumarasamy presented a security solution in order to make communication channels and platforms secure in smart cities, this solution is based on the integration of Blockchain in smart IoT devices. Researchers confirm that to secure smart cities, distributed ledger technologies and Blockchain have become very important because they secure communication protocols, devices, and channels [3].

Sun et al. proposed a conceptual framework containing three main factors (man, technology, and organization) focusing on the integration of Blockchain sharing services and how they contribute to smart cities. The factors are arranged to create a peer-to-peer when integrating the Blockchain in smart cities to enjoy the benefits of their services. However, this framework contributes to sharing services based on the Blockchain [16].

Watanabe et al. propose a process based on a hybrid consensus algorithm to improve the security of the Blockchain against the risks of monopolization. This mechanism has been used to manage smart contracts. This hybrid consensus algorithm uses a credibility score algorithm and proof of participation to prevent attackers from monopolizing resources and thereby maintaining Blockchain security [17].

Ruta et al. their objective was to present a service-oriented architecture (SOA) which could improve the scalability of the IoT, and which may use smart cities in several fields by integrating a semantic layer into the Blockchain. According to the researchers, using consensus algorithms, this example will improve the validation of resources, as well as the efficiency of smart contract operations within the network [20].

Ibba et al. offer "CitySense" which is a solution for data immutability in smart cities. These researchers wanted the data collected using sensors using the IoT to be stable and not modifiable. This is the reason why they set up the Blockchain. Researchers agree that implementing Blockchain in smart cities has several advantages [18]. Xu et al. present "Sapphire" which is a new model for smart cities integrating a Blockchain-based storage system to process data in IoT. These researchers thus propose a smart contract protocol called "OSD-based intelligent contract" which is an object-based storage device introduced in the "Sapphire". Researchers show that this new system helps to analyze data and reduce indirect costs [21].

B. *Analysis of existing works*

The studies of the above-mentioned researchers have been reviewed and evaluated according to certain measurement and evaluation criteria, presented in Table 1: Cost, Scalability, Immutability, Applies smart contracts or not, if a consensus protocol is used and which one "POW, POS, DPOS, POI, PoET, POA, etc".

TABLE 1. An analysis of the existing work of researchers

Authors	Contribution	Cost	Scalability	Immutability	Smart Contracts	Consensus Protocol
1. Biswas and Muthukkumarasamy [3]	Introducing a new security framework for smart city communications by implementing the Blockchain on smart IOT devices.	**Low**	**High**	**Yes**	**Yes**	**POW**
2. Sun et al. [16]	Present a framework on the contribution of Blockchain sharing services in smart cities.	**Medium**	**High**	**Yes**	**No**	**POW**
3. Watanabe et al. [17]	Suggests a new consensus protocol for the registration of smart contracts using Blockchain technology.	**Low**	**High**	**Yes**	**Yes**	**POS**
4. Ruta et al. [20]	Offer a service-oriented architecture (SOA) that can be used to improve the scalability of the IoT.	**Low**	**High**	**Yes**	**Yes**	**POW/UTXO**
5. Ibba et al. [18]	Offer a solution for the immutability of data in smart cities that applies Blockchain and using IoT.	**Low**	**High**	**Yes**	**Yes**	**PoET**
6. Xu et al. [21]	Introduction of a Blockchain-based storage system to analyze data in IoT.	**Low**	**High**	**Yes**	**Yes**	**NO**

IV. PROPOSED ARCHITECTURE

In this section we will propose "Secuchain" an architecture based on Blockchain technology that takes into account the limitations and capabilities of IoT devices. We are securing this architecture with the integration of a token-based access control solution Fig. 2.

Device Layer: The role of this layer is to monitor different public infrastructure environments and then transfer the filtered data to the next layer. It is composed of several sensor nodes that detect and collect information about the surroundings. This covers several applications and areas in smart cities: Health, Transport, etc.

Fog Computing Layer: In this layer each of the nodes is connected to a group of sensors, after the data collection carried out at the device layer, they pass to the following stages: The application of a method "the sign share" which realizes the Hidden data filtering, it is used to analyze the collected data without decrypting the messages using cryptology which ensures that only the desired destination can decipher the content. Then the data is sorted into sensitive data and normal data. Normal data is stored separately to be accessible to everyone, and sensitive data is routed to larger services in the next layer, the Blockchain. With the introduction in addition to a high-performance distributed SDN controller. This will allow the integrity and confidentiality of the data. Thus, thanks to this filtration method, it will reduce the overhead of the upper layer and improve the latency performance of the system.

Blockchain layer & token-based access control: Its role is the processing of data received from the previous layer. The blockchain examines the received data, and converts it into a transaction using the verification decoding phase of the sign share approach. In order to manage transactions between block chains, we will integrate a POW consensus mechanism, as well as the use of digital signatures and hashes. We will also add an access control solution based on smart contracts with personalized tokens.

Basically any customer can transfer some of their chips to another customer using the transfer function (Token transfer), this client could therefore perform a malicious operation with its tokens, it is then a security threat that exists in legacy access control systems based on tokens. However, with smart contracts, a customer is allowed to transfer their tokens only to the owner. This transfer is activated to support features such as "offsets" when a customer is authorized to perform a transaction only for a given period of time (which corresponds to their team) and then transfers through their owner his authorization to the client of the next post. This means that off-line token transfers will be impossible. Thus, in smart contracts, a customer is allowed to transfer his chips only to the owner.

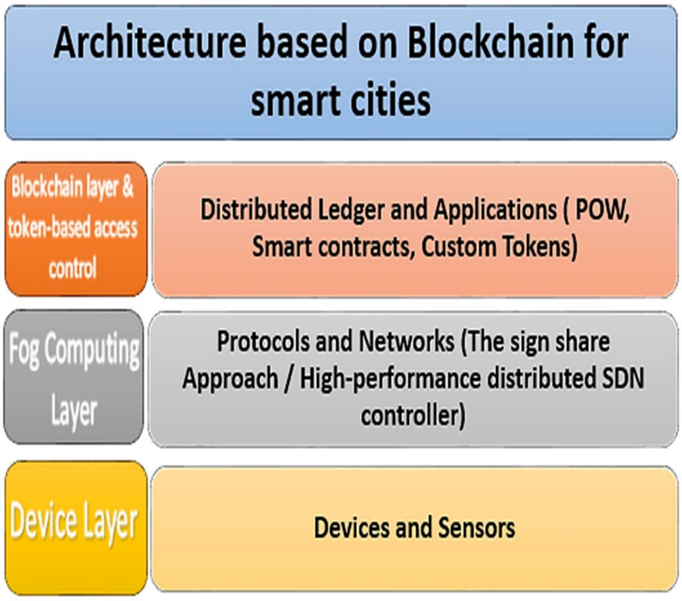
Architecture based on Blockchain for smart cities
Blockchain layer & token-based access control
Distributed Ledger and Applications (POW, Smart contracts, Custom Tokens)
Fog Computing Layer
Protocols and Networks (The sign share Approach / High-performance distributed SDN controller)
Device Layer
Devices and Sensors

Fig. 2. “Secuchain” Architecture based on Blockchain for smart cities

A. Security analysis

After an analysis of the Secuchain architecture that we proposed in the previous section, we find that it has the following characteristics: decentralization, low latency, flexibility, low cost, high scalability, immutability, smart contracts, POW consensus protocol. Knowing that the POW consensus protocol is not vulnerable to the following attacks: Short Range attack, Long Range attach, Precomputing attack, Denial of Service (Dos), Sybil attack. This architecture therefore offers a high level of security, which we will prove in our next article with an implementation of this architecture using Solidity which is the programming language of the most well-known and most used decentralized application platform Ethereum.

V. CONCLUSION

There is no doubt that technology has always played a major role in the evolution of cities. A smart city based on IoT its objective is to make the quality of life of citizens better, with a city that meets their needs and that is sustainable. The smart city requires several efforts and above all a large amount of resources. Smart cities have many challenges to overcome, so the integration of Blockchain technology could very well serve the intended purpose and help governments create effective smart cities. The blockchain, which already streamlines various industries based on its unlimited benefits, also plays an essential and major role in the development of smart cities and the security of citizens' data in different fields and applications.

For this we have proposed in this article a "Secuchain" architecture based on the blockchain to secure smart cities. Future work in this research will therefore include the implementation and testing of this architecture with a general analysis and comparison of the results obtained compared to those of other researchers.

REFERENCES

[1] J. Xie et al., « A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges », IEEE Commun. Surv. Tutorials, vol. 21, no 3, p. 2794□2830, 2019.

[2] S. Li, « Application of Blockchain Technology in Smart City Infrastructure », in 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi’an, 2018, p. 276□2766.

[3] K. Biswas et V. Muthukkumarasamy, « 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), Sydney, Australia, 2016, p. 1392□1393.

[4] B. Wadii et A. Boulmakoul, « Blockchain technology in IoT applications security service for secure smart cities », 2019, p. 8.

[5] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, et S. B. Mandal, « IoT Based Secure Smart City Architecture Using Blockchain », in 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), Changsha, 2018, p. 215□220.

[6] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, et G. C. Polyzos, « Secure IoT access at scale using blockchains and smart contracts », arXiv:1907.03904 [cs], juill. 2019.

[7] Blockchain France, La Blockchain décryptée: les clefs d’une révolution. 2016.

[8] Electronic and Computer Science Dept., University of Southampton, Southampton, UK, H. F. Atlam, A. Alenezi, M. O. Alassafi, et G. B. Wills, « Blockchain with Internet of Things: Benefits, Challenges, and Future Directions », IJISA, vol. 10, no 6, p. 40□48, juin 2018.

[9] M. Maroufi, R. Abdolee, et B. M. Tazekand, « On the Convergence of Blockchain and Internet of Things (IoT) Technologies », JSIS, vol. 14, no 1, mars 2019.

[10] Livre blanc - Civis blockchain, Rendre la Smart City aux citoyens grâce à la Blockchain, 2018, p. 29.

[11] O. Labazova, T. Dehling, et A. Sunyaev, « From Hype to Reality: A Taxonomy of Blockchain Applications », p. 10.

[12] F. Restuccia, S. D. andSalil S. Kanhere, T. Melodia, et S. K. Das, « Blockchain for the Internet of Things: Present and Future », arXiv:1903.07448 [cs], mars 2019.

[13] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, et S. S. Kanhere, « A Trust Architecture for Blockchain in IoT », arXiv:1906.11461 [cs], juin 2019.

[14] E. Nagel, J. kranz, P. Sandner, S. hopf, How blockchain facilitates smart city applications– development of a multi-layer taxonomy, Association for Information Systems AIS Electronic Library (AISeL), ECIS 2019 Proceedings, p. 18.

[15] C. Dukkipati, Y. Zhang, et L. C. Cheng, « Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things », in Proceedings of the Third ACM Workshop on Attribute-Based Access Control - ABAC’18, Tempe, AZ, USA, 2018, p. 61□69.

[16] A. G. Ghandour, M. Elhoseny, et A. E. Hassanien, « Blockchains for Smart Cities: A Survey », in Security in Smart Cities: Models, Applications, and Challenges, A. E. Hassanien, M. Elhoseny, S. H. Ahmed, et A. K. Singh, Éd. Cham: Springer International Publishing, 2019, p. 193□210.

[17] Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J (2016) Blockchain contract: securing a blockchain applied to smart contracts. In: 2016 IEEE international conference on consumer electronics (ICCE). IEEE, pp 467–468

[18] Ibba S, Pinna A, Seu M, Pani FE (2017) CitySense: blockchain-oriented smart cities. In: Proceedings of the XP2017 Scientific Workshops. ACM, p 12

[19] Sharma PK, Moon SY, Park JH (2017) Block-VN: a distributed blockchain based vehicular network architecture in smart city. J Inf Process Syst 13(1):184–195

[20] Ruta M, Scioscia F, Ieva S, Capurso G, Loseto G, Gramegna F, Pinto A, Di Sciascio E (2017) Semantic-enhanced blockchain technology for smart cities and communities. In: 3rd Italian conference on ICT

[21] Xu Q, Aung KMM, Zhu Y, Yong KL (2017) A blockchain-based storage system for data analytics in the internet of things. In: New advances in the internet of things. Springer, Cham, pp 119–138

[22] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/

[23] Y. Yu, Y. Li, J. Tian, et J. Liu, « Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things », IEEE Wireless Commun., vol. 25, no 6, p. 12‑18, déc. 2018, doi: 10.1109/MWC.2017.1800116.

[24] S. P. Mohanty, U. Choppali, et E. Kougianos, « Everything you wanted to know about smart cities: The Internet of things is the backbone », IEEE Consumer Electron. Mag., vol. 5, no 3, p. 60 ‑70, juill. 2016, doi: 10.1109/MCE.2016.2556879.