FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

Security and Privacy Challenges using IoT-Blockchain Technology in a Smart City: Critical Analysis

Zhang Xihua[1,2], Dr. S. B. Goyal[3]
[1,3]City University, Petaling Jaya, Malaysia, [1,2]103718606@qq.com , [3]drsbgoyal@gmail.com
[2]Baicheng Normal University, Baicheng, CHINA

***Correspondence:** Dr. S. B. Goyal; Email: drsbgoyal@gmail.com

ABSTRACT- A smart city is a comprehensive concept created by multiple digital industries. Smart city is a new generation of information technologies such as the Internet of Things, cloud computing, big data, and geospatial information to promote smart new ideas for urban planning, construction, management and services, power city operation and administrative management, industrial development, and public services in various fields. It is a modern high-end urban development form. A smart city is to establish a city center system by connecting terminals, applying information technology and network, and ultimately promoting the efficiency improvement and economic structure optimization in various fields. However, in the construction of smart cities, due to the sharing of a large amount of data, a lot of data leakage is caused, and data protection faces many challenges. The article first introduces the structure of smart cities, the challenges faced by smart cities in data protection and data privacy protection; then summarizes the characteristics, applications, and challenges of blockchain technology in the application of blockchain in smart cities, and makes reference to references. The corresponding comparisons are made, and the future challenges are finally summarized and proposed.

General Terms: Blockchain, IoT.

Keywords: Internet of Things (IoT), Smart city, Blockchain, Security and Privacy.

ARTICLE INFORMATION

Author(s): Zhang Xihua and Dr. S. B. Goyal

Special Issue Editor: Dr. Sandeep Kautish
Received: 12/04/2022; **Accepted**: 04/05/2022; **Published**: 30/05/2022;
e-ISSN: 2347-470X;
Paper Id: 0222SI-IJEER-2022-06
Citation: 10.37391/IJEER.100224
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100224.html

This article belongs to the Special Issue on **Novel Architecture and Methods in Industrial IoT and Wireless Sensor Network for Sustainable Computing**

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

In recent years, Statistics provided by the United Nations show that the growth of the world's urban population has seriously affected people's lives [1]. Many researchers started to look for new and intelligent ways to improve people's quality of life. These intelligent methods are the source of the concept of smart city. There are different opinions on the concept of smart city, the most accepted definition is that they are "methods of developing sustainable cities using modern advanced INFORMATION and communication technology services to improve the standard of living of the masses [2]". The focus of this study is to protect smart cities using emerging blockchain technology.

Back in 2008, an article about bitcoin: The article "A Point-to-point Electronic Cash System" [3] has attracted wide attention in the academic circle. The form of human social activities will be subverted by blockchain in a broad sense, bringing profound changes to finance, science and technology, culture, politics and other fields. Blockchain technology, which is almost impossible to tamper with due to its immutable decentralized edge, is suitable for protecting smart cities. This decentralized ledger is a chain structure consisting of one associated block with a block header, transaction counters, and transactions [4]. Applications of smart city need transparent transactions, automatic making decision, no single points of failure, and data protection to ensure transaction integrity and authorization. The information collected by sensors and other relevant sources constitutes an intelligent database system. The main function of intelligent control system is to organize and schedule resources. Intelligent interfaces are designed to provide citizens with access to information. The application of blockchain technology is security to ensure to every component. Meanwhile, the application blockchain technology protects data collected from all devices in smart database systems [5].

2. SMART CITY OVERVIEW AND ARCHITECTURE

2.1 Base layer

The basic layer includes: equipment layer, urban network, computational storage;

Equipment layer: refers to all kinds of terminal equipment.Access to the urban system through the Internet of Things.
Urban network: refers to the basic network construction in the city.
Computational storage: refers to the use of cloud computing technology for the operation and management of large-scale software, hardware and data.The detailed content of the base

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

layer is shown in *figure 1*:

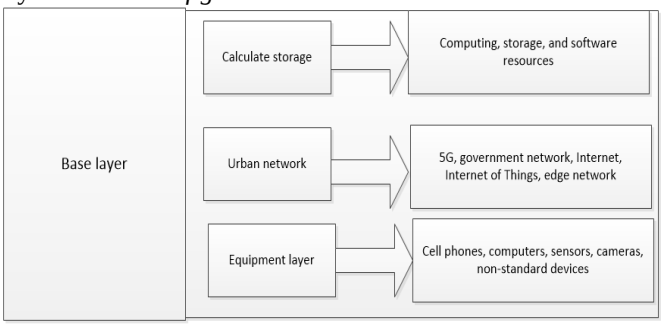

Figure 1: Base layer

2.2 Data Layer

The data layer includes: basic data, subject data. The detailed content of the data layer is shown in *figure 2*:

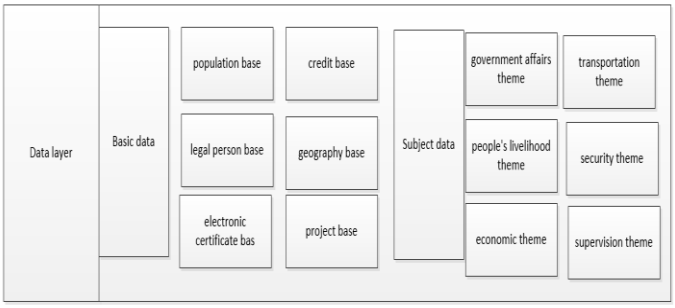

Figure 2: Data Layer

Basic data: refers to the general bottom of the data, such as population data, legal person data.

Subject data: refers to the special data after data governance and analysis.

2.3 Platform layer

Platform layer includes: application support platform, big data platform and public support platform. The detailed content of the Platform layer is shown in *figure 3*:

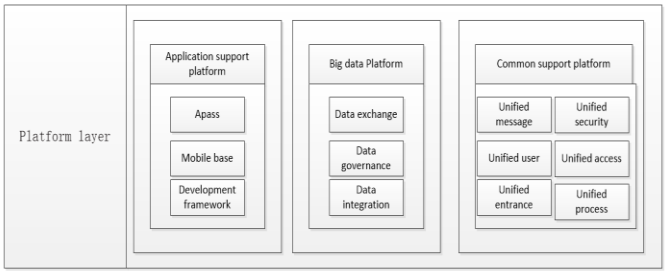

Figure 3: Platform layer

(1) Application support platform

Refers to the unified application services provided for the upper-level business or product.

Apass: mainly used to quickly build the upper-level business.
Mobile base: providing the ability of rapid development and deployment online for mobile programs.

Development framework: to provide standard development process and framework.

(2) Big data platform

Mainly from the data collection, data governance, data computing, data sharing of these four aspects of comprehensive processing. There are three concept names, data center, data center, data center, data exchange center, it is easy to be confused.

Data middle platform is to integrate data from various business departments into a platform from the aspects of data collection, governance, computing, etc., and open it as an interface for external sharing.

Data exchange refers to data in the form of open permissions to support upper-level services to call lower-level data, realizing "multiple data runs" in a real sense.

The data center, generally referred to as the "city brain center," is a basic base, a connector, responsible for integrating the interfaces of the underlying data into the center. It also does not handle the data, while providing the data call capability for the upper level business.

(3) Public support platform

It refers to the ability to provide a standard for the upper-class business from the perspective of public support.The public support platform can be continuously expanded with the capacity of access to share the standard capacity of each manufacturer.

Unified messaging: refers to unified messaging notifications within an application.

Unified user: a user can obtain the permissions of all upper-layer applications with one account.

Unified gateway: refers to a single gateway to all business modules.

Unified security: refers to the three-level end-to-end, tube-cloud security standard.

Unified access: Third-party services are connected to the system in a unified manner.

Unified process: refers to the unification of process business standards to realize the collaboration between data and business.

2.4 Application layer

The application layer refers to the specific performance of the final product in each industry. The detailed content of the Application layer is shown in *figure 4*:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

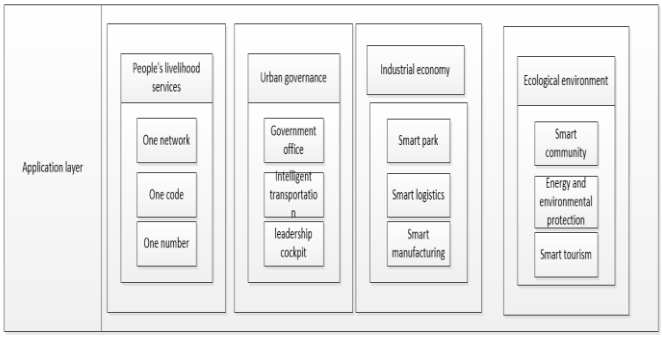

Figure 4: Application layer

People's livelihood services, c-terminal user applications. The representative products are "Zhili Ban", "Health code", "city service" and so on.

Urban governance: application for 5G terminal users. Government affairs office, intelligent transportation, leadership cockpit, representative products and so on.

Industrial economy, for the application of b-end industries. Smart park, smart logistics, smart manufacturing, smart water, etc. Representative products are "park access", "face access control" and so on.

Ecological environment, oriented to the application of ecological environmental protection, harmonious life. Smart community, energy and environmental protection, smart tourism, etc. Representative products are "qing Qing online", "one button parking".

3. CHALLENGES OF SECURITY AND PRIVACY IN SMART CITIES

In recent years, the development of smart cities has made a great contribution to improving the environment, but almost every smart application is vulnerable. For example, smart metering infrastructure in smart grid can monitor residents' private life, including their living habits and working hours [6]. Similarly, in smart homes and healthcare, device manufacturers and service providers have access to sensitive data [7]. In addition, a large amount of trajectory information collected by intelligent mobility applications can be used to infer the location and mobility patterns of users [8]. In addition, there are hacker attacks such as background knowledge attacks, collusive attacks, Sybil attacks, eavesdrop attacks, spam attacks, likability attacks, inside curious attacks, outside forgery attacks, identity attacks. According to the above issues, the security and privacy of smart cities are classified:

(1) *Security challenges*: refers to the list of intentional and unintentional issues and challenges in IoT and cloud-based smart city architectures (such as sensing, transmission, storage and processing layer) that unauthorized parties can use to attack systems.

(2) *Privacy challenges*: In general, the privacy debate involves considering acceptable practices for obtaining and disclosing citizens' personal and sensitive information in the context of data perception and data analysis [9].

4. BASICS OF BLOCKCHAIN PRINCIPLES

4.1 The characteristics of blockchain

4.1.1 De-centration

The concept of blockchain decentralization is as follows: the entire operation process of blockchain is based on the joint completion of all nodes of the entire distributed system, and the trust relationship between distributed nodes is dependent on pure mathematical methods rather than central institutions, so that the distributed system becomes a decentralized and trusted system [10]. In contrast to centralized applications, users are both information providers and information participants.

4.1.2 Immutable

Use hash value chain to ensure that the block chain data cannot be tampered with, each a block the size of blocks in the chain of preservation with a block size of the hash value, and the bigger contains stored in all transactions in this block, once one of the deals have been tampered with, hash value is bound to change, must get rid of all the hash value of the block size to stay behind, This creates a huge amount of work for tampering with data [11].

4.1.3 Trusty

The blockchain's data exchange relies entirely on mathematical algorithms, or the computing power of each node, to form a powerful system that can defend against external attacks without human intervention. Participants can complete transactions without trust, even in complete anonymity. Blockchain protects the privacy of both parties and guarantees the security and credibility of both parties. In addition, each node on the blockchain stores all transactions in their entirety, and as long as no more than 51 percent of all nodes in the blockchain are manipulated by hackers, the data in the blockchain is trusted.

4.2 Type of blockchain

According to the characteristics of blockchain, we usually divide blockchain into public chain, federation chain and private chain, as shown in *Table 1*.

Table 1. Comparison of Blockchain Types

Features	Public	Private	Consortium
Nature	Permissionless	Restrictions	Merging
Transparency	Less	More	More
Energy sage	More	Less	Less
Scalable	Yes	Yes	Not much
Efficiency	Less	More	More

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

4.3 The key technology of blockchain

4.3.1 Consensus mechanism

Consensus mechanism [11] is the core content of blockchain. In a centralized network, there is only one central node, so there is almost no need to consider the issue of consensus. However, in a distributed system, it is difficult for nodes to reach consensus to ensure data consistency. Proof-of-work (PoW), the consensus mechanism used by the original Bitcoin, is most commonly used in blockchains to ensure consistency of data between ledgers and prevent forks in the blockchain. Consensus mechanism of thought is through the block between nodes in the chain of the data to calculate force competition agreement, all nodes can be involved in the "dig" contest, by calculating a random number (Nonce), so that the size of the double SHA256 hash value less than or equal to a certain value, the rapid calculation of the random number node to get the billing and the piece reward.

4.3.2 Intelligent contract

Smart contract [13, 14] can be understood as a computer program that can be automatically executed and deployed in blockchain. Smart contract can be programmed according to the needs of developers, which is a core part of blockchain-related application development at present. According to the definition of smart contract, Cao Binyan et al. [13] put forward the operation principle model of smart contract, as shown in *figure 1*. Blockchain-based smart contract technology can be applied to multiple scenarios [15], such as sharing economy, Internet of Things, financial asset processing, digital payment, multi-signed contract, cloud computing and other application scenarios. Current smart contracts use if-then contracts that follow a fixed set of logic and are not intelligent. In the future, with the continuous development of artificial intelligence technology, the contract mode of IFTHEN will be replaced by the mode of What-if [12], making the smart contract more intelligent to meet more complex demand scenarios in the future.The detailed content of Smart contract model is shown in *figure 5*:

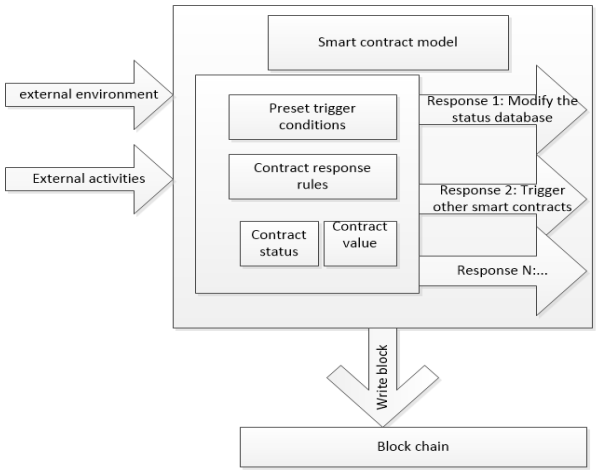

Figure 5: Smart contract model

4.3.3 Merkle Tree

The nodes with billing rights package legitimate transactions in the system into blocks and add the blocks to the blockchain. The Merkle tree in the blockchain contains the Root Hash, as well as the individual branch hashes and the individual leaf hashes that make up the branch hashes, the leaves being each individual transaction. This structure enables Merkle trees to verify the existence and integrity of transaction data in blocks.

4.3.4 Asymmetric Encryption

Asymmetric encryption in cryptography requires a key pair, namely public key and private key, in which the public key can be disclosed compared with the private key, while the private key can only be known to the owner, and the private key cannot be calculated from the public key. Common asymmetric encryption algorithms include RSA, Rabin, Elgamal, elliptic curve cryptography and digital signature. The sender of a message encrypts the plaintext with a public key or private key and sends the ciphertext to the receiver, who can decrypt it with the corresponding key.

5. APPLICATIONS OF IOT AND BLOCKCHAIN IN SMART CITIES

The following advantages of blockchain technology are used in cities. First, in access control of the blockchain, each participant has access to the database. In smart cities, data generation is very laborious due to the participation of many devices, and blockchain can provide partial/complete/no access to lots of data in a single database without raising any security and privacy issues. Second, an incentive mechanism that can be used to motivate citizens was created by blockchain technology, to use different smart city-based applications. Third, blockchain technology can help detect abnormal users by looking at users who are trying to change their data. At present, intelligent system is applied in many aspects, security and privacy issues must be considered.

5.1 Smart Healthcare

Licensed blockchains make it easier to keep track of healthcare providers' professional certificates and any other necessary information, and when local provider information is updated in one place, it is automatically updated across all areas of the blockchain. Using blockchain for this purpose can also reduce the operating costs of keeping directories up to date while keeping information secure.

(1) Electronic health Record

Moving electronic health records between healthcare facilities has always been a difficult and time-consuming task, but getting that information on a blockchain could make the process simpler and more convenient. With these new delivery modes, patients have greater control over their medical history data and can more easily manage and understand that data. Placing electronic health records on the blockchain also assigns patients an identification code so that their data is always associated with their local identifier.

(2) Drug tracking

In addition to blockchain sharing of medical history data, drug information can be stored and transferred via blockchain to track prescriptions, identify stolen or counterfeit drugs, and publicly share clinical trial results. Each new thing added to

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

the block in the drug traceability category is immutable and time-stamped, making it easy to track the drug and ensure that the information does not change.

(3) Health care process

From drug manufacturing, to clinical trials, patient data management, and medical insurance reimbursement, blockchain technology is actively promoting. The priority use cases are efficiency and office day after tomorrow, with an emphasis on improving processes by simplifying and reducing costs. These are conservative use cases that can prove the efficacy of blockchain. The plan for the future is to open up the network to any organization that can benefit from participating, extending it to all healthcare payers and providers worldwide.

5.2 Smart Logistics and Supply Chains

As the logistics industry faces a lack of transparency throughout the supply chain, blockchain offers an opportunity to transform the supply chain and the industry as a whole. Specifically, Bitcoin aligns well with the fundamental need for reliability and integrity in the supply chain.

5.3 Smart Home

Internet of Things technology and Internet appliances related to smart city have made important contributions to the development of smart home. New technologies to improve life quality through home network [16, 17], smart home reflects the continuous development of diversified use and integration.

The benefits of integrating blockchain technology into your smart home are clear. Ferdous et al. [18] pointed out that blockchain contributes to trust and traceability in smart home. With environmental sensing, smartphone apps and iot sensors can easily generate data, including user activity, energy use, security measures and human physiology. All data can be recorded on the blockchain and can also be used for sharing economy services [19]. Digital signatures can be used to detect suspicious activity and securely assign each smart home device its own identity [20]. The decentralized, transparent, and secure features of blockchain provide a unique platform for smart home sensors, actuators, and devices to communicate seamlessly and easily share information across platforms. Makhdoom et al. [21] studied the advantages of this technology in multiple applications such as smart home and developed an innovative privacy protection platform based on blockchain called "Private Sharing". In addition, blockchain has the potential to address the lack of interoperability between smart home objects. This is a prerequisite for smart home integration, communication and proper functioning. In this regard, Park et al. [22] highlight the key role of blockchain in facilitating interactions between smart homes, facilitating automated energy trading activities within smart homes, and facilitating more sustainable practices between smart homes and within smart cities.

5.4 Smart Education

As information communication technology (ICT) permeates education extensively, the digitization of educational records increases the pressure to ensure the security and privacy of online storage using IoT [25], [26], [27]. Education has witnessed great challenges because of the need to protect personal data, which is rich in important details such as citizenship, immigration, financial and social information collected by educational institutions. Concerns about the use of student information have risen as the collection of learning analysis and big data has become more common in higher education [23], [28]. Blockchain technology provides a highly secure design for processing large amounts of educational data. Thus, this technology represents a secure educational ledger file, such as student transcripts, certificates, and degrees that allows everyone to own and share his/her own digital certificates on peer-to-peer networks [24]. Blockchain is helping to transform the higher education model into a sustainable platform for lifelong learning.

6. DISCUSSION

With wisdom city construction, based on the application of intelligent city block chain is also more and more, in the future, chain technology should be able to manage the block chain complex operations, including consensus, intelligent contract execution, a large transaction concurrency management, fair and efficient mining of reward mechanism and rapid processing of heterogeneous data types/format data. Each smart city application has its own special requirements based on its nature. Therefore, in smart city applications which develop a robust blockchain is a challenging task. Blockchain architecture should be intelligent, reliable, fast, and scalable. Additional research work is needed to design a robust blockchain architecture that is highly secure, less complex, and protects privacy.

7. CONCLUSION & FUTURE WORK

Based on research questions and to achieve research objectives, we will follow the major methodology steps as follow Blockchain technology is used to realize different applications such as smart cities, smart homes, smart transportation systems, healthcare systems, agricultural fields, supply chain systems and so on. Innovations in smart devices with wireless connectivity, storage space and some processing power allow them to use them in real time. However, security and privacy concerns for IoT systems exist at different levels.

Based on research questions and to achieve research objectives, we will follow the major methodology steps as follows:

First, a smart city can be vulnerable to many security attacks and threats, Integrity, confidentiality, authenticity, and accountability etc. We will do the state-of the art about the existing data security& data privacy issues in various subparts of smart cities like urban planning, to waste management using compound heterogeneous network of interconnected multiple sensors, devices, protocols, tools and software.

Second, we need to depth literature survey of different blockchain applications to applicable security in various context in smart cities like healthcare, manufacturing

International Journal of Electrical and Electronics Research (IJEER)
Survey Report | Volume 10, Issue 2 | Pages 190-195 | e-ISSN: 2347-470X

industries, waste management, energy generation, public services etc.

Thirdly, we need to analyze different security and privacy aspects of existing protocols, methods and prove their pros and cons faced while applying in various sections of smart cities as well to identify different open issues and consider blockchain as a major security solution for smart cities.

Finally, we need to propose a blockchain based mechanism for smart cities to handle different sections like garbage management, healthcare, industries, energy, etc. of smart cities to integrate with security concerns and offer a reliable atmosphere for user data authentication & accountability etc. for user's data transaction.

In process, there are several milestones will be written as paper and then issued at publications and conferences of proceedings. Finally, thesis will be presented for reviewed and discussion.

REFERENCES

[1] UN, "Population Division"; https://www.un.org/en/development/desa/population/index.asp, 2017, accessed 23 July 2018.

[2] J. Xie et al., "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," IEEE Commun. Surveys & Tutorials, vol. 21, no. 3, 3rd qtr. 2019, pp. 2794–2830.

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: http://bitcoin. org / bitcoin. pdf, 2009.

[4] A. Kosba et al., "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," Proc. 2016 IEEE Symp. Security and Privacy, 2016, pp. 839–58.

[5] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," IEEE Communications Magazine, vol. 55, no. 5, pp. 16–55, 2017.

[6] R. Kitchin, "Getting smarter about smart cities: Improving data privacy and data security," 2016.

[7] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1732–1745, 2014. [102] Z. Ni

[8] M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter 2019, doi: 10.1109/COMST.2018.2867288.

[9] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions [J]. Computer Standard & Interfaces, 2019, 64.

[10] Yuan Yong, Wang Fei-yue. Current Status and Prospect of blockchain technology [J]. Acta automatica sinica, 2016, 42 (04): 481-494.

[11] Ouyang Liwei, Wang Shuai, Yuan Yong, et al. Intelligent contracts: architecture and progress [J]. Acta automatica sinica, 2019, 45 (03): 445-457.

[12] Ma Chunguang, AN Jing, BI Wei, et al. Smart contracts in blockchain [J]. Information Network Security, 2018(11): 8-17.

[13] Cao Binh, Lin Liang, Li Yun, et al. A review of blockchain research [J]. Journal of chongqing university of posts and telecommunications (natural science), 2020, 32 (01):1-14.

[14] Yang Lu.The blockchain : State-of-the-art and research challenges [J].Journal of Industrial Information Integration, 2019, 15.

[15] Sripan, M.; Lin, X.; Petchlorlean, P.; Ketcham, M. Research and thinking of smart home technology. In Proceedings of the International Conference on Systems and Electronic Engineering (ICSEE'2012), Phuket, Thailand, 18–19 December 2012; pp. 61–63.

[16] Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. 2020, 135, 106382.

[17] Fadeyi, O.; Krejcar, O.; Maresova, P.; Kuca, K.; Brida, P.; Selamat, A. Opinions on sustainability of smart cities in the context of energy challenges posed by cryptocurrency mining. Sustainability 2020, 12, 169.

[18] Pavithran, D., Shaalan, K., Al-Karaki, J.N. et al. Towards building a blockchain framework for IoT. Cluster Comput 23, 2089–2103 (2020).

[19] Ortiz-Fournier, L.V.; Márquez, E.; Flores, F.R.; Rivera-Vázquez, J.C.; Colon, P.A. Integrating educational institutions to produce intellectual capital for sustainability in Caguas, Puerto Rico. Knowl. Manag. Res. Pract. 2017, 8, 203–215.

[20] Ismagilova, E.; Hughes, L.; Dwivedi, Y.K.; Raman, K.R. Smart cities: Advances in research—an information systems perspective. Int. J. Inf. Manag. 2019, 47, 88–100.

[21] Vu, P.; Adkins, M.; Henderson, S. Aware, but don't really care: Students' perspective on privacy and data collection in online courses. J. Open Flex. Distance Learn. 2020, 23, 42–51.

[22] Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry 2019, 11, 1198.

[23] Zhou, Z.; Hu, C. Research on the risk identifification of academic information system based on the comprehensive weighting method. Inf. Sci. 2017, 8, 29.

[24] Filvà, D.A.; García-Peñalvo, F.J.; Forment, M.A.; Escudero, D.F.; Casañ, M.J. Privacy and identity management in Learning Analytics processes with Blockchain. In Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality, Salamanca, Spain, 24–26 October 2018; Association for Computing Machinery: Salamanca, Spain, 2018; pp. 997–1003.

[25] Aamir, M.; Qureshi, R.; Khan, F.A.; Huzaifa, M. Blockchain based academic records verifification in smart cities. Wirel. Pers. Commun. 2020, 113, 1397–1406.