IoT-Enabled Smart Cities: A Review of Security Frameworks, Privacy, Risks and Key Technologies

Bushra Al Barwani, Esraa Al Maani, and Basant Kumar(✉)

Modern College of Business and Science, Muscat, Oman
basant@mcsb.edu.om

Abstract. Smart cities are becoming increasingly popular worldwide as cities grow; technology evolves and improves daily. The internet of things devices are used in smart cities that are all interconnected to run critical systems that a city requires to function correctly. The Internet of Things controls traffic lights, security cameras, weather, infrastructure, meters, and other data collection devices to run the city. Because technological devices do not sleep, eat, or take breaks like humans, the systems can be relied on to operate continuously. Blockchain is a system of decentralized and immutable electronic ledgers or databases in which anyone can securely store and access public records while maintaining information integrity. Blockchain offers a method of communication, transactions, security, and governance that is transparent and available to all members of a town or society, which are several advantages of a smart city. This paper reviews how blockchain can aid in developing a smart city and proposes a security framework based on layers.

Keywords: Blockchain · Smart City · IoT

1 Introduction

WITH their fast-paced lives, most people prefer to live in cities, and this trend is expected to continue in the coming years. As a result, smart cities have begun to simplify people's lives by integrating technologies into the infrastructure. One could argue that modern cities resemble future cities without robots or flying cars. By leveraging blockchain technology to conduct verifications and secure transactions on the Internet, this technology will revolutionize smart city management by promoting transparency, efficiency, and privacy in the coordination, integration, and regulation of many cities' services.

Considering its technological nature, many concerns have been raised regarding smart city security. Consequently, the implementation encountered several challenges both at the government and administrative levels. Hence, there should be a collaboration among the residents, private organizations, and government when implementing this infrastructure. Replacing the outdated infrastructure and converting it into modern goods needed to be paid by the government large sums of money to build and fund

N. Bacanin and H. Shaker (Eds.): ICIITB 2022, ACSR 104, pp. 83–95, 2023.
https://doi.org/10.2991/978-94-6463-110-4_8

infrastructure. A cybersecurity threat and the right to privacy are also concerning, where infiltration of security systems is one of the main obstacles, a hackers can control financial and transportation services and citizens' and others' information. Privacy and security concerns are associated with sensors, devices, etc., connected to the Internet. Most smart applications generate a large amount of data from various sources continuously.

Blockchain is a network of an incorruptible digital record of information exchange that may store everything of value rather than just the history of financial transactions as bitcoin is renowned for. Likewise, blockchain is a chain based on cryptographic principles that may record any valuable object, such as accounting books, voting, copyright, property, and anything else that can be stated in code. The old Internet could only transfer information; however, blockchain is built to communicate importance to the network and is regarded as the future generation of global credit certification and Internet validity. It lowers the cost of credit with excellent efficiency, openness, security, transparency, and traceability. It enables two untrustworthy people to trust one another without needing third-party credit approval. Blockchain is a cryptographic technology that might help us develop smart cities in the future with the help of IoT systems [1, 2].

Information systems in smart cities are only one of the numerous fields where blockchain technologies have already been adopted. This paper proposes an improved framework for smart cities that considers security aspects, particularly privacy of data collection and sharing via IoT systems and blockchain applications. The following is how the paper is structured. Section 2 will present IoT in smart cities with an overview of IoT and smart cities with their applications. Section 3 presents the literature review. Section 4 addresses the challenges and issues that may arise in Smart Cities. Section 5 will show related work on the framework of smart cities. Section 6 highlights the solutions with an algorithm. Finally, Sect. 7 concludes the paper.

2 IoT in Smart Cities

2.1 Smart Cities Overview

SmART cities are the new way of life; there is no single definition for these cities. However, they all have one thing in common: they constantly strive to improve citizens' lives, increase efficiency and productivity, reduce costs, and reduce consumption of available resources by utilizing ICT to enhance various aspects of city operation and management. It becomes smart when a set of advanced smart technologies is used (software and hardware). However, the city cannot be smart solely through technology; these are merely enablers; the city must sustain economic, social, cultural progress, and environmental through technology [3][4].

A few factors are required for smart cities to perform efficiently. First, data collection involves collecting data from various digital sources, monitoring, and communicating via multiple sensitivities that serve the smart city environment, assisting in better decision-making and outcomes. As a result, smart city data leads to more accurate decisions. Second, data communication is critical in developing and managing networks that organize connection guidelines between devices, servers, and major smart city points. It allows data to flow from various parts and data sources. Third, data analysis and action support decision-making based on collected and saved data and human interference. Through a

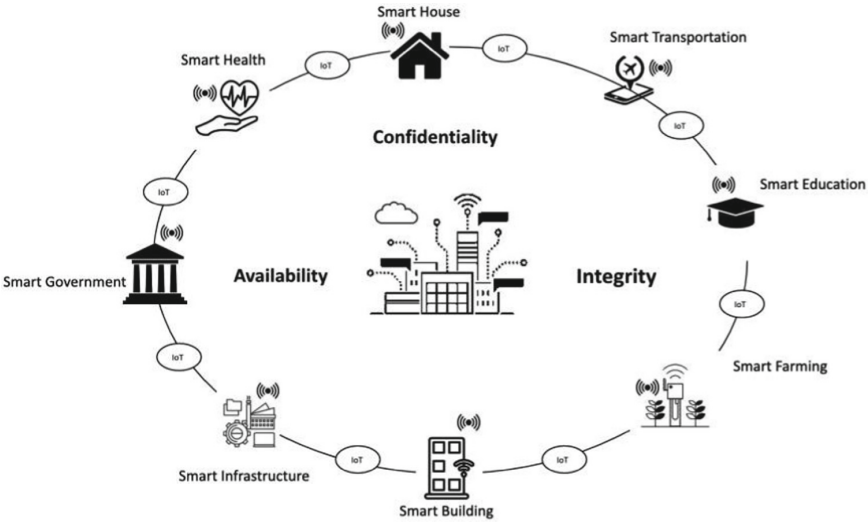

Fig. 1. Smart City Applications

central analysis, data consists of real-time data combined with a set of archived historical data. After it is issued, the final decision is transmitted to the appropriate entities [4]. Figure 1 shows some smart city applications.

Smart Transportation. One of the most severe problems that people face is traffic congestion. Smart city solutions offer ideal applications and transportation services. Using data from cameras, satellites, drones, parking sensors, and other multimedia, a comprehensive view of city transportation is provided, allowing for real-time tracking of passing traffic and a new routing algorithm to improve energy efficiency and route stability. Additionally, Drivers can also receive advance notice before entering the parking area by using the smart parking system [4–6].

Smart Governance. The government must be involved in improving security and privacy concerns. A civil partnership may support smart city project design, execution, and evaluation processes. The smart city concept has changed citizens' interactions with their governments. Citizens can now engage in decision-making and voice their opinions clearly and concisely, thanks to the e-government system. Smart governments should be technologically progressive, with smart governance and policies. Cloud-based information system services should support the need for sustainable governance of facilities in smart cities. [4, 6].

Smart Healthcare. Since lives are always on the line, healthcare requires the accuracy and dependability of results in real-time. A health service system known as "smart healthcare" connects individuals, resources, and organizations involved in providing healthcare through technology. Smart healthcare may encourage interaction among all healthcare entities. Remote monitoring from patients' homes or hospitals can improve their health [7].

2.2 Internet of Things (IoT) Overview

The Internet of Things (IoT) aims to securely connect and transport data between everyday objects, transforming the world into a massive information system, allowing them to send and receive data. Even though people can engage with them to set up or retrieve the data, most work is done without human intervention [1]. IoT allows interaction between the physical and digital worlds using actuators and sensors. Sensors are used to store and process all necessary information. Data processing occurs at the network's edge or on a remote server or cloud. IoT data must be secured at rest and in transit to ensure data integrity. Security solutions are executed in a way that makes it possible for them to identify unauthorized intrusions to thwart malicious attacks on the communication layer. [8].

2.3 Smart Cities' Relation in IoT

The development of smart cities necessitates the use of communication and information technologies. They facilitate connectivity and data collection, allowing smart cities to be smart. Almost every aspect of smart city operation is improved by communication architecture. IoT is a necessary element for a smart city to be smart, and it plays a vital and effective role in meeting the needs of citizens by providing and restoring essential services. The city and its residents' development would benefit from the IoT technology and smart city combination, considering IoT analytics is crucial for data analysis and improving decision-making ability. IoT deployments in smart cities certainly improve quality of life. Creating a smart city by centralizing and connecting all the city's applications would be accomplished using IoT since IoT sensors may transform any object into a smart object. One of the most important new digital technologies is the Internet of Things platform, which will be around for the foreseeable future [9, 10].

3 Literature Review

For this research, the method used will be a review based on which many papers will be read and analyzed. With that, a table will be generated for comparison to develop the model, which would be based on a combination of those papers.

According to [11], using blockchain in smart cities, it will secure the communication of data and services between the cities. The author suggested an application called "orthus," a blockchain platform in smart cities that will help to solve the security issues in smart cities. Moreover, they have mentioned how the platform works, the requirement to build blockchain platforms, and how it will work.

According to [12], new issues and difficulties regarding data governance and storage facilities are brought up by smart technology. Also, one of the major focuses was data integrity, to which access to information must be regulated, for what purpose, and how it is stored and protected. To secure data sharing between various entities, it suggested "SmartPrivChain," a solution that combines data audit mechanisms and access control.

Based on [13] Modern cities prioritize technology to maximize resource utilization, cut expenses, and create a more livable environment. A smart city is vulnerable to a variety of security threats. Identifying these threats and potential consequences is critical

to design an effective solution. Cybercriminals may access personal and financial information from IoT devices in smart cities. As a result, new solutions and communication platforms must be developed based on the nature of the data (private or public) to provide privacy, integrity, and data confidentiality. This paper proposes a blockchain-based security framework that allows communication between entities in a smart city while maintaining privacy and security.

As stated in Li's research paper [2], the most significant issues that smart cities face are lack of security in IoT devices, high cost for maintenance and equipment of the data center, and no privacy for users' data. The author's proposed solution involves using P2P, a distributed network technology based on cryptography, to address the massive cost of blockchain data storage. To solve the lack of privacy and security in IoT devices in smart cities, blockchain validation and consensus procedures will be used to identify genuine IoT nodes and prevent rogue or harmful node active devices from accessing the network.

After reading and analyzing multiple research papers, it has been concluded that the most common issues faced in smart cities are security based and the above papers show that with the proper framework this issue could be solved.

4 Issues and Challenges

SmART cities have a lot of information and technological infrastructure running simultaneously and constantly [14], The systems need to be reliable, or the city might become chaotic if some systems fail. There are sensors all over the city to collect data like temperature, humidity, wind speeds, traffic, and many other environmental factors. If the traffic lights and cameras were to fail, it would create a lot of congestion in the streets and potentially cause serious accidents to which emergency services would probably be unable to respond due to all the traffic jams. Provided the systems sensors and the physical layer of the infrastructure hold together and work seamlessly, data privacy, networks, and interfaces are still vulnerable and need measures to keep them secure [14][15].

Security is among the most critical concerns in any smart city and society [14]. Smart cities collect and use a lot of data to help manage financial, physical, and social infrastructures, and this data needs to be secured while being accessible to the public. With the interconnection of multiple systems and networks comes the threat of data breaches and unauthorized access to the data. There are also a lot of concerns about privacy for the users. There is a need to keep some details private to prevent many dangers like stalking, identity theft, corporate espionage, and other threats. There is a dilemma in technology because it is almost impossible to give people total privacy while offering them the best security [6]. Blockchain has the potential to provide protection, keep public records accessible, and preserve confidential information. Blockchain proved an efficient way to secure all the data while still making it accessible to all the parties and stakeholders involved [14, 16]. IoT devices collect heterogeneous data, making the system vulnerable in several ways.

Availability is on availability of information related to the upholding of resources. The information must always be available to the users/stakeholders so the system runs smoothly. Nevertheless, the data must also be secured and locked to prevent unauthorized manipulation or deletion by third parties.

Data Integrity. Data integrity concerns the wholeness and completeness of data and protects against corruption and manipulation [14]. Data in a system needs to be whole and void of errors. Unauthorized access to the data may compromise the data integrity. Therefore, it is protected from malicious users. The database should also have self-checking and correcting mechanisms to continuously comb over the system to correct any errors as they occur.

User authenticity. It is centered on the authenticity of the users [16, 17]. Measures must be employed to ensure that anyone who accesses the data in the database is authorized. The use of complex passwords and two-stage authentication is an example of providing that the users trying to access the data are indeed allowed to do so.

Accountability. There is a threat around accountability, including correct claims of transmission and reception of data. When data is sent across a network, there must be a mechanism to relay that the data has been received by the intended recipient and not anyone else. Cryptographic encryption keys are commonly used to authenticate that the data has been received and viewed by the intended use and that no data breaches have occurred.

5 Related Work

DubAI is an excellent example of a smart city currently implementing blockchain systems [12]. The city is linking crucial systems and making them available to all citizens via the internet. Residents may now pay fines and report crimes without visiting police stations, saving time, space, and transportation costs to the police stations. Other services like driverless cars and automated traffic systems are active in the city, economic systems, automatic power grids, and many other benefits. The entire smart city infrastructure taps into new 5G networks to make the Internet of Things (IoT) devices communicate quickly and efficiently. By adopting blockchain, the city resident hopes to provide a secure platform to perform all kinds of transactions securely and transparently. As Dubai is one of the leading tourist attractions in the world, this will boost tourism and attract investors. Blockchain technology will also come in handy as the city aims to be a cashless society soon. Blockchain has proved to be a valuable tool for monetary transactions with cryptocurrency [18].

6 Solutions

6.1 Blockchain Technology

As stated by [2], A blockchain comprises a collection of blocks, every block with its own header and body. The hash, previous hash, timestamp (block creation time), nonce, and Merkle root are all included in the block header. By submitting the preceding block's header to a hash function, the hash value is computed. The blockchain grows as new blocks are generated and connected, with the hash of the previous block saved in the current block. If an attacker attempts to modify the value of a transaction in a block, the hash of that block will be incorrect as well.

Furthermore, this guarantees that any interference with the prior block is discovered quickly. The block body contains a collection of transactions that include the hash value and sender and receiver identities. The chain begins with a genesis block, which serves as the foundation of blockchains; it is the first block in the chain upon which subsequent blocks are added [19], as shown in Fig. 2. There is a growing interest in blockchain technology, particularly in the financial sector. Since 2009, bitcoin transactions have been performed without a central organization or institution using blockchain technology. Using computer protocols, the blockchain enables immutability, confidentiality, transparency, and high degrees of trust by creating chains of timestamped transactions using the following mechanisms that have been mentioned by [2, 12, 20] in their research papers:

A consensus algorithm. It is a mechanism for achieving consensus in a blockchain network. Nodes of blockchain networks must agree on the validity of generated transactions because they are not dependent on a central authority; hence, consensus algorithms are needed. Monitoring the protocol rules ensures that all transactions are safe and reliable. Various nodes in a blockchain system must reach a consensus using a consensus algorithm. A consensus algorithm specifies the criteria for reaching an agreement among several nodes in a blockchain network. The node identification, energy usage, data model, and application of each blockchain consensus technique differentiate it. There are several consensus algorithms, the extremely common of which are Proof-of-Work and Proof-of-Stake. Each has pros and cons regarding security, functionality, and scalability.

Smart contracts. It consists of autonomous electronic transactions or digital contracts that incorporate rules and operate on distributed blockchain networks. To ensure the legality of contracts, the primary objective is to ensure that they are enforceable. In a legal sense, it would take longer, but it would be done directly by computer code. A smart contract ensures the transparency, traceability, irreversibility, and reliability of contracts and transactions.

Digital signatures are one of the most significant components of asymmetric cryptographic signatures, which means a digital signature is a mathematical approach used to authenticate a signature. Hellman created the first digital signature mechanism, which included communicative parties sharing a secret key. He invented asymmetric cryptography, which is used in blockchain technology. Digital signatures are classified into two categories; the private key is for signing the transaction, while the public key is for validating transactions.

Hash Function. Converts a variable-length input into a fixed-length to a small practical integer value using a hash algorithm and a mathematical function. The mapped integer value in the hash table is an index to the hash value of the hash function's input string results. Three characteristics must be present to achieve cryptographic security: collision resistance, hiding, and puzzle friendliness. By transforming input into a hash code or value, this function encodes data. The hash algorithm limits the possibility of two inputs having the same hash value [2, 12].

Merkle tree. It is a secure, efficient, and tamper-proof data storing technique. The Merkle tree allows for the safe verification of large volumes of data. Moreover, it organizes transactions within a block and uses cryptographic hashing to record transactions

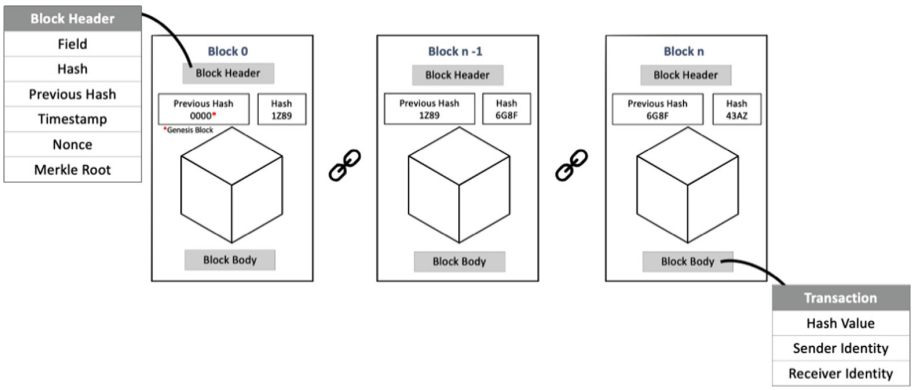

Fig. 2. Blockchain Structure

in an immutable manner. The Merkle tree's root is included in the block header. The block header is timestamped and contains the hash of the previous block, producing a sort of chain. Blockchain transactions are signed with a digital signature using asymmetric cryptography.

Smart cities have systems that must follow the CIA triad framework to be secure. The CIA triad represents three components: confidentiality, integrity, and availability. Confidentiality concerns making the data private, meaning only authorized users can access and manipulate data in the system database. Integrity pertains to the correctness and completeness of the data in the database. The data should have no errors or redundancies for the system to operate smoothly. Finally, availability ensures that data is available and functional when it should be, at the appropriate time, and to the right person. Authorized users are assigned authentication identification methods like usernames and unique passwords to ensure they can access the data in the system at any time. Unauthorized users are kept out of the system to preserve the integrity of the data. Blockchain is great technology to address these components of a system.

At its core, blockchain employs peer-to-peer distributed ledger/database technology on which agreements, contracts, sales, and transactions are stored and are available for access. The system is so efficient that for a hacker or an unauthorized user to corrupt the database successfully, they would have to compromise 51% of the records (Fig. 3).

Security Framework and Mechanism. [19, 20]

1. Physical Layer: This layer has IoT devices in the real world, like sensors, cameras, actuators, and microphones, which collect data and forward it to the upper layers [21, 22]. This layer's primary function is to gather data. The main security mechanisms in this layer are related to the safety and unyielding measure put in the physical world to make sure that the equipment is not damaged. It involves actions like installing cameras in high-up positions so that they can capture everything and are not damaged by the environmental elements. Insulating the equipment from malicious people and environmental factors is the most important security mechanism in this layer.
2. Communication Layer: This layer houses communication network infrastructure like Wi-Fi, Bluetooth, Ethernet, and wireless networks that communicate and transmit

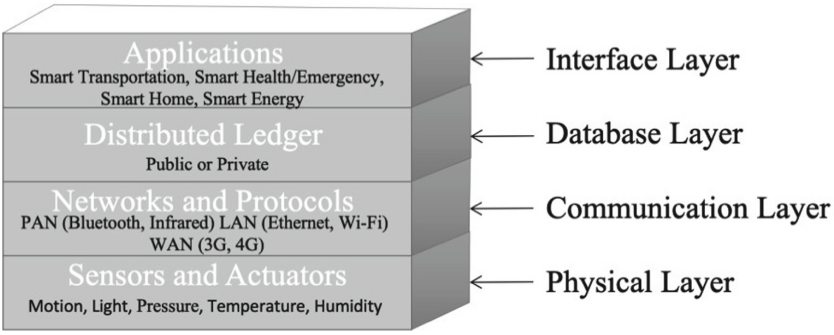

Fig. 3. Smart City Layers Based Security Framework

information across different layers [21, 22]. This layer has a few security mechanisms to protect the data being sent through the network. Internet security protocols like hyper ledgers, multichain, quorum, and Corda are protocols used to ensure information is not altered while in transit from the sender to the recipient in a blockchain system [23].

3. Database Layer: This decentralized ledger records all the data and is accessible to all the information stakeholders. Each record has a unique time stamp and a cryptographic signature for security. The ledger is the main security mechanism that blockchain uses as it is straightforward to access and track all the transactions carried out in the system [23–25]. The ledger is decentralized, making it extremely difficult to alter or delete any information without being discovered.
4. Interface Layer: This layer has careful integration of the layers where the different applications of the system can access information in the database and make decisions based on the available data [24]. Most of the security mechanisms are found in this layer. Security mechanisms include features like cryptographic hashing and the use of Merkle trees. Hashing is converting any form of data into a unique string of characters to store and access information more efficiently. Merkel trees are verification mechanisms used to summarize enormous chunks of data that can be verified easily. The users can verify transactions easily using Merkel trees, and any transactions not included in the chain are flagged as fraudulent activity in the system [24]. The interface layer has much of the computational burden of the blockchain system, and hence it is the most important along with the database layer.

System Architecture and operations. Let's explore how the system operates with one specific sub-system within the more extensive city-wide system, like the parking IoT allocation system [26, 27].

1. Block approval: A parking lot user requests a spot, and the system assigns a block through one of the gateways in the parking IoT. The interface handles the request, the optimal place to park is issued to the user, and the information is added to the ledger as the latest entry.

2. Spot reservation: the spot has been found, and now it has to be reserved. The system assigns a sequence number and links it to the latest blockchain. The process is complete, and the system indicates that the spot is reserved for the user.

Algorithms 1 for parking spot reservations for users I [2, Algorithm 1]
while *user*$_i$ *received* valid *request* = True **do**
if user identity authentication = True **then**
m ← *request*
multicasts pre-prepare to other members.
end if
end while
while *user*$_i$ received valid *prepare* = True **do**
if number of valid prepare > 2f **then**
multicasts commit to other members.
end if
end while
while *user*$_i$ received valid *commit* = True **do**
if number of valid commit > 2f **then**
send reply message to the client.
end if
end while

6.2 Discussion

All the nodes in this system have identical blockchains, and the system can easily detect unwanted requests [16, 22]. A malicious node is not allowed to request a block as all submissions are assigned to their respective blocks in the chain. Other types of malicious activity, like requesting two or more parking space reservations, can be easily detected, and all the other nodes can deny them as they are all accessing the same ledger in real-time. If the reservation process fails, the user may try again after a ransom timer countdown and if it hasn't already been allocated to another user, use the same sequence number.

7 Conclusion

Blockchain has many potential uses in a smart city setting. This paper proposes a security system framework with a blockchain-based database to operate multiple systems like parking lots and access to buildings. Blockchain has many advantages, the most lucrative being that it is very secure and takes a lot to manipulate data within the database without necessary permissions. With more people moving into cities, there is a demand for more resources and a system to distribute the resources equally. As more people rush into the cities, problems arise like congestion, financial burdens, housing concerns, and many other issues arise. There is a need for a system that uses blockchain technology to manage all these systems in an integrated infrastructural system. It is also very reliable, and all the stakeholders of the information being stored can access the information easily.

People's privacy is respected while keeping the right information public, and the database is protected from malicious users. Networks are also getting better and faster and can support more devices and have the potential to hold multiple modes of communication like video, audio, documents, and complex transactions. The future will now focus on designing collective systems that are interoperating and scalable across all functions of a smart city.

References

1. Mustapha, S.: Blockchain Applications in IoT to Smart Homes. (2019).
2. Li, S.: Application of Blockchain Technology in Smart City Infrastructure. 2018 IEEE International Conference on Smart Internet of Things (SmartIoT). (2018). https://doi.org/10.1109/smartiot.2018.00056
3. Ismagilova, E., Hughes, L., Dwivedi, Y., Raman, K.: Smart cities: Advances in research—An information systems perspective. International Journal of Information Management. 47, 88-100 (2019). Doi: https://doi.org/10.1016/j.ijinfomgt.2019.01.004
4. Varfolomeev, A., Alfarhani, L., Oleiwi, Z.: Overview of Five Techniques Used for Security and Privacy Insurance in Smart Cities. Journal of Physics: Conference Series. 1897, 012028 (2021). Doi: https://doi.org/10.1088/1742-6596/1897/1/012028
5. Hajam, S., Sofi, S.: IoT-Fog architectures in smart city applications: A survey. China Communications. 18, 117-140 (2021). Doi: https://doi.org/10.23919/jcc.2021.11.009
6. Kirimtat, A., Krejcar, O., Kertesz, A., Tasgetiren, M.: Future Trends and Current State of Smart City Concepts: A Survey. IEEE Access. 8, 86448-86467 (2020). Doi: https://doi.org/10.1109/access.2020.2992441
7. Tian, S., Yang, W., Grange, J., Wang, P., Huang, W., Ye, Z.: Smart healthcare: making medical care more intelligent. Global Health Journal. 3, 62-65 (2019). Doi: https://doi.org/10.1016/j.glohj.2019.07.001
8. Garg, H., Dave, M.: Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). (2019). Doi: https://doi.org/10.1109/iot-siu.2019.8777334
9. Kaushik, N., Bagga, T.: Smart Cities Using IoT. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). (2021). doi: https://doi.org/10.1109/ICRITO51393.2021.9596386
10. Ilyas, M.: IoT Applications in Smart Cities. 2021 International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB). (2021). Doi: https://doi.org/10.1109/ICEIB53692.2021.9686400
11. Loss, S., Cacho, N., Valle, J., Lopes, F.: Orthus: A Blockchain Platform for Smart Cities. 2019 IEEE International Smart Cities Conference (ISC2). (2019). Doi: https://doi.org/10.1109/ISC246665.2019.9071761
12. MAJDOUBI, D., EL BAKKALI, H., SADKI, S.: Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment. 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech). (2020). Doi: https://doi.org/10.1109/CloudTech49835.2020.9365905
13. Biswas, K., Muthukkumarasamy, V.: Securing Smart Cities Using Blockchain Technology. 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). (2016). Doi: https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

14. Qushtom, H., Misic, J., Misic, V., Chang, X.: Efficient Blockchain Scheme for IoT Data Storage and Manipulation in Smart City Environment. IEEE Transactions on Green Communications and Networking. 6, 1660-1670 (2022). Doi: https://doi.org/10.1109/TGCN.2022.3171397
15. Rahman, M., Rashid, M., Hossain, M., Hassanain, E., Alhamid, M., Guizani, M.: Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. IEEE Access. 7, 18611-18621 (2019). Doi: https://doi.org/10.1109/access.2019.2896065
16. Yazdinejad, A., Srivastava, G., Parizi, R., Dehghantanha, A., Karimipour, H., Karizno, S.: SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). (2020). Doi: https://doi.org/10.1109/vtc2020-spring48590.2020.9129462
17. Misic, J., Misic, V., Chang, X.: Comparison of single- and multiple entry point PBFT for IoT blockchain systems. 2020 IEEE 92nd Vehicular Technology Conference (VTC2020- Fall). (2020). Doi: https://doi.org/10.1109/VTC2020-Fall49728.2020.9348782
18. Lai, O.: Smart City in Dubai: Could Blockchain Technology Be the Game Changer? | Earth.Org, https://earth.org/smart-city-in-dubai/.
19. Liang, Y.-C.: Blockchain for Dynamic Spectrum Management. Dynamic Spectrum Management. 121–146 (2019). Doi: https://doi.org/10.1007/978-981-15-0776-2_5
20. Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.M.A., Salah, K., Hong, C.S.: Blockchain for IOT-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications. 181, 103007 (2021). Doi: https://doi.org/10.1016/j.jnca.2021.103007
21. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W.: PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security. 88, 101653 (2020). Doi: https://doi.org/10.1016/j.cose.2019.101653
22. Yin, M., Malkhi, D., Reiter, M., Gueta, G., Abraham, I.: HotStuff: BFT Consensus in the Lens of Blockchain. (2018).
23. Zhao, H., Bai, P., Peng, Y., Xu, R.: Efficient key management scheme for health blockchain. CAAI Transactions on Intelligence Technology. 3, 114-118 (2018). Doi: https://doi.org/10.1049/trit.2018.0014
24. Sayeed, S., Marco-Gisbert, H.: Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences. 9, 1788 (2019). Doi: https://doi.org/10.3390/app9091788
25. Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., de Ree, M., Ribeiro, J., Mantas, G., Rodriguez, J.: Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. Sensors. 22, 2449 (2022). Doi: https://doi.org/10.3390/s22072449
26. Shahnaz, A., Qamar, U., Khalid, A.: Using Blockchain for Electronic Health Records. IEEE Access. 7, 147782-147795 (2019). Doi: https://doi.org/10.1109/access.2019.2946373
27. Salah, K., Rehman, M., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: Review and Open Research Challenges. IEEE Access. 7, 10127-10149 (2019). Doi: https://doi.org/10.1109/access.2018.2890507