

Security and privacy in smart city: a secure e-voting system based on blockchain

Fatima Zahrae Chentouf, Said Bouchkaren

ERMIA Team, Department of Computer Science, ENSAT, Abdelmalek Essaadi University, Tangier, Morocco

Article Info

Article history:

Received May 28, 2022

Revised Sep 20, 2022

Accepted Oct 14, 2022

Keywords:

Blockchain

Cybersecurity

Ethereum

Internet of things

Smart city

Smart contract

ABSTRACT

In recent years, the internet of things (IoT) growth has brought about many technological changes, including the emergence of the notion of the smart city. The development of a smart city requires the integration of IoT devices and information and communication technologies to improve the quality of lives of citizens in many areas such as health, economy, business, agriculture, and transport. However, with this evolution, many cybersecurity risks and challenges have been raised, so it is necessary to develop these technologies in a protected way to avoid being compromised by attackers. Blockchain, being a new technology based on cryptographic principles, can play an important role in securing smart cities. In this survey, we discussed different applications of blockchain technology in smart cities and also studied how blockchain features (transparency, democracy, decentralization, and security) can help in the improvement of smart city services. This analysis will help us to implement an electronic voting model using a smart contract based on the Ethereum blockchain to highlight how blockchain technology can be implemented in smart cities to promote security.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Said Bouchkaren

Department of computer science, ENSAT, Abdelmalek Essaadi University

BP 1818, Route Ziaten 90000 Tanger

Email: sbouchkaren@uae.ac.ma

1. INTRODUCTION

People have recently witnessed a tremendous change in communication technology. In this new world, inside every connected thing there is a computer, which makes it a smart connected thing. Along with the Internet of things (IoT) and information and communication technologies (ICT) that have become part of our lives, in this recent decades another concept received attention which is a smart city. This concept is about transforming urban cities into smart ones to facilitate daily life and provide smart services. To improve these smart services, it is important to collect data from the environment, infrastructures, events, and people. To fulfill this requirement, IoT is considered to be the engine of smart cities [1].

Let us imagine that someone must stay at work for a late hour, but unfortunately, it is time to bring his son from school. Here comes the role of smart city technology, so, he can use a smart application to send an autonomous car to his son's school to bring him home. After the kid gets in the car the father will know how and when he came home using global positioning system (GPS) signals on his son's smartphone, thus, he can be sure that his son went home safely. Also, their smart house system checks the son's arrival and provides him with the best climate condition [2]. The problem here is that the child's data are stored in a service database, which gives an opportunity to hackers to steal his private information, for example, what he eats and which road he takes.

A smart city is a safer and faster place where networks are efficient and telecommunication technologies are used for the benefit of its citizens [3]. The objective of a smart city is to raise the standard of

living of its inhabitants to ensure their long-term development, safety, and health [4]. What leads to the development of Smart cities is the combination of technological trends with urban sustainability by taking advantages of ICT [5]. A smart city is a system that contains subsystems, which means this system is based on different sectors interacting via ICT, also a big amount of data is collected by sensors and stored in the city data storage. In fact, smart cities need to integrate ICT and IoT to improve the standard of living [6]. This implies that smart cities will improve many areas such as health care, education, economics, trading, and so on.

To benefit from smart city services, citizens must apply and participate, to do so, they need to be sure that their information and activities are well protected and secured. That is why smart cities must be secure, so it is necessary to develop security frameworks on it to enhance privacy and security. Moreover, blockchain technology plays a key role in IoT security solutions. Blockchain, in sooth, is a system that delivers a shared ledger technology that permits each network member to view one ledger system, where the data blocks contain all transactions and a hash to the previous block. All transactions in the public ledger are validated as a majority of minor nodes, and the data blocks are immutable and cannot be modified or deleted [7].

In this study, we have sought the importance of blockchain as an incoming technology, which takes a leading role in securing different smart city services, which means the integration of blockchain technology in smart cities can enforce security by the help of a trusted public ledger without requiring a third party. In view of this, many companies invested in deploying blockchain technology, and also much research has been carried out in the field of blockchain in the past few years, including IBM that launched its blockchain framework, and it is used in banks, supply chain systems, and cargo shipping companies [8]. In like manner, blockchain also can be integrated with e-governance to facilitate and secure government services for citizens in smart cities. E-voting can be one of the main e-government services that need security and democracy, which are the main features of blockchain technology.

A secure e-voting system based on blockchain is presented in this paper. The proposed system is implemented on Ethereum blockchain platform, this method will solve the problem of centralized systems, because the data stored in centralized servers and databases can be manipulated, otherwise, the data are immutable on the blockchain. That is why we built a decentralized application (DApp) for voting to ensure that our vote system is secured and the number of votes is counted properly with no changes, also to be sure that a voter can only vote once. A client-side application is made to talk to the blockchain, and a smart contract written with solidity programming language contains all the code that makes us read and write data on the blockchain, and we can connect to it using personal accounts with an Ethereum wallet on the browser.

The rest of this paper is organized as. Section 2 presents some related works. Then, the concepts of smart cities and blockchain are briefly discussed in section 3. In section 4, the motivations for using blockchain technology in smart cities. Section 5 contains the proposed scheme for electronic voting. Finally, the work is concluded in section 6 with some conclusions.

2. RELATED WORKS

In this section, we present some related works concerning security and privacy in smart cities. For a safer city, Lacinak and Ristvej [4] mentioned some possibilities to use in crisis management such as the creation of a comprehensive directory of dangerous materials, databases of sources, individuals, and potential threats, and also supporting decision-making and salvage operations coordination. Bahga and Madiseti [9] proposed a blockchain-based framework for industrial internet of things (IIoT) which is used to interact with the blockchain network and the cloud. Also, Christidis and Devetsikiotis [10] discussed the advantages of blockchain technology for IoT, and describe an outline in which blockchain might automate energy purchasing and selling among IoT devices such as smart meters. In their survey dealing mainly with the topic of smart city, Sharma and Park [11] explained the relationship between blockchain and IoT environments and proposed a new hybrid network architecture for the smart city by taking advantage of the power of growing software defined networking (SDN) and blockchain technology. Nowadays, online social network (OSN) represents the main source for collecting data, on the other hand, it can bring several threats and risks that can affect security and privacy in a smart city. Moustaka *et al.* [6] studied privacy and security on OSN and identify how it can impact smart people and smart living dimensions, by determining the boundaries between them and investigating behavioral patterns of individuals on OSN to transform them into smart people and increasing their substantial engagement in smart cities through social networking.

Farahat *et al.* [12] proposed a method to share information in a secure way via Wi-Fi by encrypting data in a source using an advanced encryption standard (AES) algorithm with a rotate key and decrypt it in a destination with an authentication method for authorized people only. Saracevic *et al.* [13] discussed different methods and cryptographic systems that can solve the security gaps in IoT devices, suggesting a cryptographic method based on Catalan numbers. This method is suitable to encrypt text and images, also clarified the convenience of this method in different IoT applications and smart city services, namely,

e-health, since medical data is considered to be critical and sensitive, Catalan numbers algorithm can be used in encrypting and hiding these data. So, in general, this method can be used to solve the problem of storage and processing data in smart cities.

Exchanging keys in cryptography is classed as a major security problem. Catalan numbers are also used in addition to the lattice path to offer a secure way for exchanging secret keys, the proposed scheme is made of three main steps, the first step is to generate Catalan values, the second step is to determine the lattice path movement space, and the final step is to identify the key equalization rules [14]. This method of exchanging secret keys can serve in smart city applications to exchange keys between entities, actually, in smart cities, citizens' data must stay secure and private so that they can trust a smart city system and participate in its services. Blockchain can also be an appropriate solution for securing smart city applications by preserving the integrity, confidentiality, and anonymity, as long as the private keys are maintained secret by users. Besides using Fuss-Catalan numbers as a cryptographic method for exchanging keys, it may be applied to improve technologies such as IoT and blockchain [15].

Biometric authentication can be viewed as a sensitive issue in smart cities. Rajasekar *et al.* [16] addressed this subject in their study and suggested a multimodal biometric technique for smart cities that is based on machine learning and functions with both iris and fingerprint biometrics, the method applies the score-level fusion technique based on an optimized fuzzy genetic algorithm (OFGA) in order to obtain better recognition, fuzzy procedure, and a genetic algorithm is combined in this system for the purpose of providing a powerful fusion approach and authentic biometric recognition.

Xie *et al.* [17] mentioned the importance of blockchain technology in providing security in smart cities. They discussed using cases concerning different smart city services that are based on blockchain, for example, distributed electronic health records (EHR) presented in [18] to solve such a problem. In this solution, IoT devices are used to collect patients' data, and the data is stored on the blockchain-based BigChainDB using big data tools.

Blockchain technology could help in improving vehicles' communication management because of its distributed nature. Yang *et al.* [19] presented a decentralized and self-managed network of ad hoc vehicles (VANET) and used smart contracts to encourage the development of decentralized VANET applications. Dorri *et al.* [20] proposed a solution for smart homeowners to control communication between devices, this solution consists of the use of a private blockchain where communication histories between local devices are recorded as transactions on the blockchain. Lemieux [21] mentioned the collaboration between the Government of Honduras and Factom (a blockchain company) that consists of providing a blockchain-based registration system to store land related information in order to enhance mutual trust between citizens and the government. Furthermore, e-voting can be another smart government service that requires the application of blockchain technology. A blockchain-based e-voting system was proposed to enhance security by providing integrity, non-repudiation, and authenticity during the voting process where votes are stored on an Ethereum blockchain by using smart contracts [22]. In summary, implementing security on IoT devices faces several challenges, including limited resources, Heterogeneous devices, security protocols Interoperability, Single points of failure, hardware/firmware vulnerabilities, trusted updates and administration, as well as various blockchain concerns, related to the method relying on miner hashing being exposed, allowing attackers to host the blockchain [7].

3. BACKGROUND

3.1. Smart city

The smart city is the ability to acquire and integrate data using sensors, household appliances, personal devices, and similar sensors. These data are integrated into a processing platform that allows information to be shared among various city departments in order to make better decisions. In the field of urban planning, "smart city" is frequently qualified as an ideological dimension that being smarter implies strategic directions. Governments and public bodies at all levels adopt the concept of intelligence to make their policies and programs stand out of targeting long-term development, economic improvement, better standards of living, and happiness creation. In order to develop a smart town, it must be livable, efficient, sustainable, and safe. Smart can be viewed in four main areas: smart planning, smart environment, smart estate, and services and smart living as shown in Figure 1.

3.1.1. Smart city pillars

Institutional infrastructure (citizens-based decision, citizens advisory committee, ICT-based service delivery, transparency accountability, environment sustainability), physical infrastructure (waste management, power water supply, multi-modal transport, connectivity, housing), social infrastructure (education, healthcare, environment, inclusive planning), and economic infrastructure (job creation, market growth,

livelihood activities, gross domestic product (GDP) contribution) are considered the four pillars/themes of a smart city.



Figure 1. Smart city characteristics

- Institutional infrastructure: institutional infrastructure is on top of smart cities governance, it combines decision-making involvement, social services, transparency, governance, political strategies, and perspectives.
- Physical infrastructure: natural resources and manufactured infrastructure make up physical infrastructure. The physical infrastructure pillar assures that resources are available and sustainability to continue city operations now and in the future. The quality of ICT infrastructure builds on the performance of a smart city.
- Social infrastructure: the social infrastructure of a smart city includes intellectual and human capital and quality of life. Citizen awareness, accountability, and engagement are essential in promoting the notion of smart cities.
- Economic infrastructure: the smart economy includes new innovations in ICT, the manufacture and provision of ICT-related services, and the integration of sophisticated technologies that improve the economic management's dependability and performance.

3.1.2. Architecture

Smart city architecture has 4 layers as shown in Figure 2: sensing layer contains devices to collect data from the environment. The data collection layer is responsible for transmitting collected data to the local or remote database. The data processing layer performs data per-processing strategies on the basis of the smart city applications. The smart processing and application layer is responsible for exchanging data between operators, and smart applications are also charged for analyzing data in order to make a global decision and providing raw data for smart city applications [23].

3.1.3. Services

In this section, we present some of the services that could be made possible by an urban IoT paradigm to improve quality of life and provide an economic benefit to the city administration in terms of reduced operational costs. To begin with, smart energy is the main application of smart cities that aims to provide efficient control of energy and use renewable energy sources and it relies on resource system integration, access to energy services, resilience, energy efficiency, clean energy, and sustainable economy. Second, the smart building where ICT plays a key role in the growth and administration of smart buildings, and it aims to manage energy equipment to decrease energy use and improve energy resilience. Third, smart mobility aims to provide a comfortable transportation service for citizens. Smart governance aims to provide a productive way to simplify and plan a decision-making-based ICT tool. Smart education helps students by

using modern technologies and e-learning. Smart healthcare, consist of providing health services using ICT infrastructure and context-aware network. The smart citizen can participate in decision-making and apply smart solutions in daily activities. Finally, smart traffic, as we know traffic congestion can affect badly on economic development and also can cause pollution and waste of time, that's why smart traffic can manage these problems by taking decisions quickly and collecting data from sensors and closed-circuit television (CCTV).

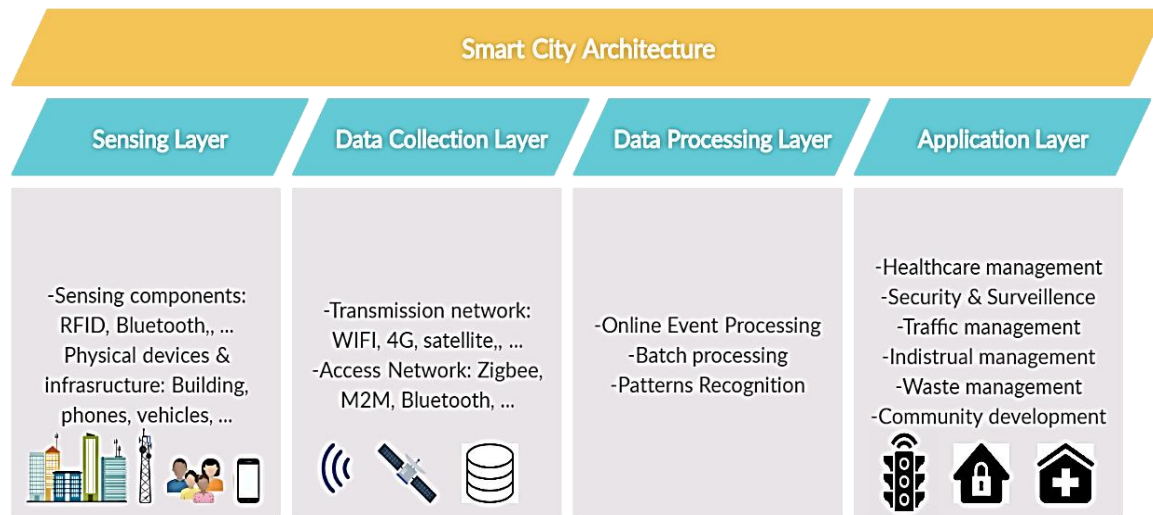


Figure 2. Smart city architecture

3.2. Blockchain

3.2.1. What is a blockchain?

The power of modern communication makes us think of a technology that is decentralized, which means removing middlemen and allowing users to interact with each other directly through a global network. Actually, decentralization becomes the leading technology in the past 10 years, and it can aid in costs and barriers reduction, single point of failure elimination, censorship prevention and the reinforcement of transparency and confidence between all parties engaged in a transaction. Blockchain technology provides a solution to this problem by offering a shared ledger that allows every network member to see the same system ledger. In other terms, blockchain is a peer-to-peer network that allows users to share a digital ledger that records transactions. The ledger, which is distributed to all network members' nodes, permanently preserves data blocks in cryptographically linked blocks, allowing them to be structured and chained together. The data are arranged and connected together in chunks. Blockchain technology attracts many stakeholders from variant fields such as agriculture, and cryptocurrency [11]. So, using blockchain technology can let businesses benefit from the more efficient transfer of services. The technological research and consulting firm Gartner report [24] expected that by 2030, \$3.1 trillion in business value will be added. So simply, blockchain is a distributed ledger technology (DLT), that is transparent and secure for data storage and transfer in a decentralized database that can work without a third party [17].

As shown in Figure 3, the blockchain forms a register composed of small blocks connected to each other. Each block holds a list of transactions, linked to the previous block by a cryptographic process. This system is based on 3 principles: i) a block can only be generated when a certain amount of time has passed after the previous block; ii) the network as a whole-has mostly a good intention; and iii) each block contains the imprint of the previous one.

3.2.2. The block

After creating a proof of work (POW), the node picks the transactions from the transaction queue to include them in its newly created block. So, it assembles a number of transactions, adds to this the proof of work created, its reward, and the imprint of the previous block, and records it in a database. The newly created block is distributed over the network for all other nodes to write it into their copy of the database. They check the content and that the fingerprint of the previous block, written in this new block, is correct and that the proof of work is correct.

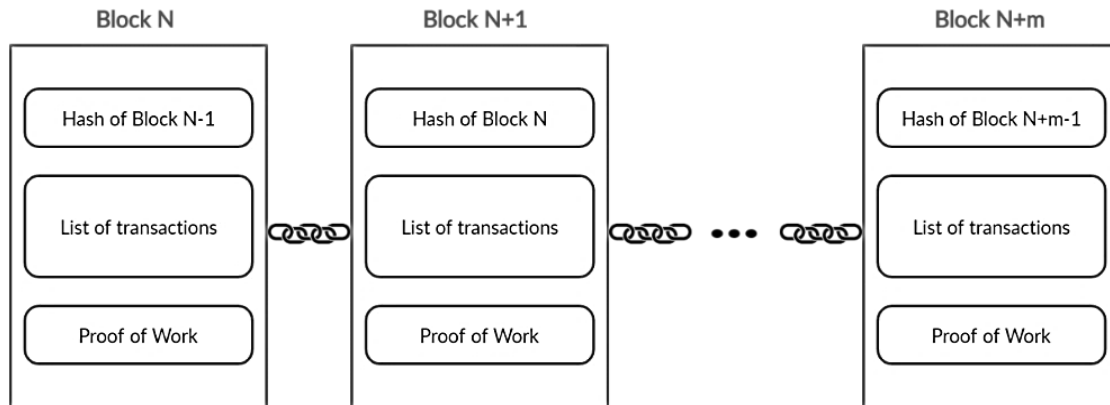


Figure 3. Blockchain

3.2.3. Transactions

When one person wants to send money to another, they create a transaction. The transaction is an instruction: “Person A transfers value X to person B”, but that is not all; person A, in order to collect the amount to be sent, first goes to his receipts, so, he creates what we call an “entry”; that is, a list of old transactions whose value he has not yet spent. Then person A defines a list of addresses among which to share the collected value. In this way, it is possible to trace the origin of a coin back to the block where it was generated, in this way, authenticity is verified.

3.2.4. Transaction verification

Since the system requires a POW for an actor to create a block and add it to the blockchain. When a person creates a transaction, they broadcast it to nodes in the network. A node will therefore listen and receive the transactions thus created. For each transaction, it will trace the origin of the parts and make sure that each one is authentic and in the possession of the recipient, therefore, it is not necessary to know or record the “balance” of an account. If there is a concern, the transaction is rejected. If everything is in order, the node will hold it pending.

3.2.5. Distributed consensus

A decentralized network depends on consensus algorithms to make an agreement between distributed nodes so that they can make a decision to accept the transactions. The reason for this is that all transactions in a blockchain must be confirmed by most nodes of the network. Simply put, storage using a distributed ledger implies that each entity that owns a copy of the ledger can potentially have a different fork, i.e., the state, of the blocking chain. Therefore, all peers in the distributed network will eventually agree with the correct version.

3.2.6. Smart contract

Smart contracts are autonomous, self-running programs that are run on the basis of the defined condition by a programmer [25]. These contracts enable, enforce, and establish agreements between two entities using block strings. In contrast to traditional contracts, which require the intervention of a third party, intelligent contracts allow independent activity among anonymous entities with minimal costs. As an illustration, it is possible to pay room rent at the end of the month without engaging a bank in the meantime. Smart contracts can be used in a multitude of applications, like real estate, shares or bonds trading in distributed markets. In addition, it can also be used for a stand-alone transparent digital voting system or a stand-alone digital notary contract system. In this context, companies such as Ethereum and Codius allow intelligent contracts using block strings to support these applications.

3.2.7. Blockchain systems

Blockchain systems can be classified into private blockchain, public blockchain, and consortium blockchain [17]. A public blockchain is one without permission, which means anyone can join the network such as Ethereum which support decentralized applications, and Bitcoin which is a crypto-currency system created in 2008, these two systems are the most famous blockchain systems, while other systems require permission. Permissioned systems contrariwise need permission even in reading transactions, this kind of blockchain system is used in businesses such as Hyperledger.

Table 1 presents a comparison between some blockchain systems. Compared to the private blockchain, the public blockchain is paying, and the validation of transactions takes much more time. On the other hand, allowing a total decentralization of the system, and good scalability of the network are the major advantages of the public blockchain. One of the main objectives of a public blockchain is that the participating objects do not need to go to authenticator to perform transactions, because the blockchain itself ensures the legitimacy of its transactions.

Table 1. Comparison between some blockchain systems

| Blockchain systems | Application | Permission | Smart contract language | Smart contract execution | Consensus |
|---------------------|---------------------|------------|-------------------------|--------------------------|--------------|
| Bitcoin [26] | Crypto currency | No | Golang, C++ | Native | PoW |
| Ethereum [27] | General application | No | Solidity, Serpent | EVM | PoW, PoS |
| Litecoin [28], [29] | Crypto currency | No | Golang, C++ | Native | PoW |
| Ripple [30], [31] | Digital assets | Yes | Golang, C++ | XRP | Ripple |
| Hyperledger [32] | General application | Yes | Golang, Java | Dockers | PBFT |
| Quorum [33] | General application | Yes | Golang | EVM | Quorum-Chain |
| ZCash [34] | Crypto currency | No | C++ | Native | PoW |
| Monax [35], [36] | General application | Yes | Solidity | EVM | Tendermint |

4. MOTIVATION OF USING BLOCKCHAIN

Recently, there are many initiatives from different countries for smart city projects. Singapore is one of the first countries that aims to build a smart nation. The smart city of Trikala is another example, so Trikala city architecture follows a model with four layers where the first layer contains the physical environment such as people, vehicles, and buildings, and the second layer concerns the telecommunication and electronics infrastructures like CCTV systems and IoT, the third layer includes information technology infrastructures, the final layer contains infrastructure-based sectors and service-based sectors [6]. Many other cities are pursuing their strategies such as Amsterdam, Madrid, and Manchester. There are many challenges in addressing the implementation of smart cities. Xie *et al.* [17] classified smart city challenges into two categories, technological ones such as data collection, number of devices, sharing data and city management, and non-technological such as financial investment. Blockchain technology seems to be an ideal solution for such challenges due to its features such as decentralization, pseudonymity, transparency, democracy, security, and immutability. That means blockchain technology can make us build a secure, democratized, and trusted smart city. Many cities proposed blockchain as a solution for implementing smart cities. The Government of Dubai has declared its plan for enabling government transactions and documents on the blockchain, which makes it the first blockchain city by 2020 [37].

5. THE PROPOSED SCHEME FOR ELECTION

In this part, we present our model of a blockchain-based e-voting system in order to clarify how blockchain technology can be applied to develop secure, trusted, and democratized smart city services. Figure 4 shows the use case of our solution, the administrator creates the election and defines the candidates proposed with the rules of the election, and then adds the list of the legitimate voters. When the admin starts the election, voters can cast their vote transactions, smart contracts do the number of votes counting according to the transactions that are stored on the blockchain. When the admin ends the election no one can cast a vote.

- Admin: the person who creates the election using a decentralized application (DApp) and manages the election process and the candidates' list.
- Voters list: the list that contains the legitimate persons who have the right to vote.
- Smart contract: a contract where Ethereum blockchain enables us to run codes on Ethereum virtual machine (EVM), in other words, it is where the code of our DApp lives, and it is written with Solidity programming language.
- Blockchain: it is where all the transactions of our smart contract are broadcast.

The use case of the system is as follows.

- Create election: the administrator of the election creates the vote by deploying the smart contract to the blockchain.
- Add voters: the administrator can define the list of voters that have the right to cast a vote, each voter has his own unique wallet.
- Start vote: when the admin starts the voting process, no one can be registered to vote only the voters that are registered already before the election starts.

- d. Vote transaction: when a voter chooses the candidate and casts a vote, the smart contract verifies if the address wallet belongs to a legible voter from the voters' list and also has not voted previously if it is the case the vote will be confirmed and the transaction broadcast to the blockchain.
- e. Vote counting: the smart contract automatically counts the vote's transactions that are recorded on the blockchain.
- f. End vote: when the election is done, the admin can close the election and stop anyone from voting.
- g. Vote verification: The voter can use his transaction ID to see his transaction information and the election results.

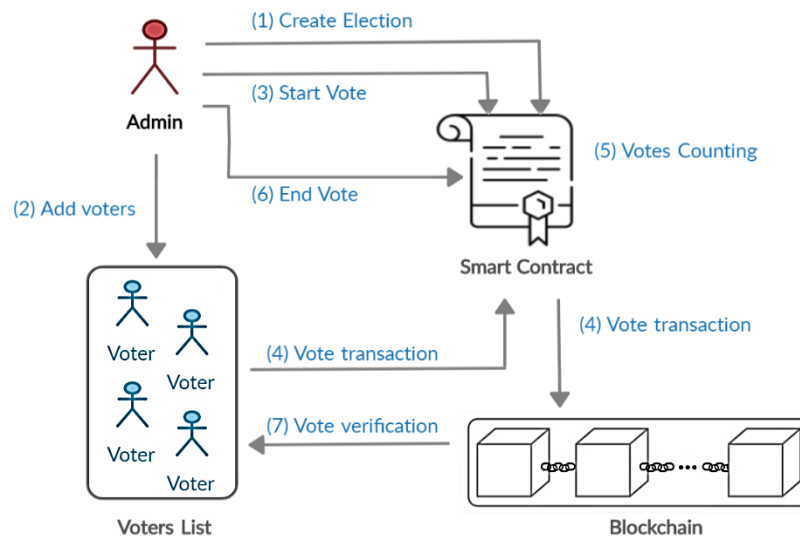


Figure 4. E-voting use case

6. CONCLUSION

In smart cities, there are several objects that are linked and connected to each other, to be specific, a set of electronic equipment that is interconnected with the help of sensors. Indeed, equipment and technologies allow us to be smarter and make our life easier. In this work, we focused on the problem of security in smart cities, and we discussed different solutions from different surveys. The major focus of our work is on blockchain technology as a solution to enhance security and privacy in smart city services. We proposed an electronic voting system which is the main service in smart cities that can ease voting service for citizens, our solution is based on blockchain technology that will help us not only create a decentralized and secure electronic voting system, but also a transparent and accurate one. After all, an e-voting system that is based on a decentralized technology can have some flaws, since it is still a new technology that demands more investigation and analysis. So, this system still can be defenseless to some attacks, thus Sybil's attack is classified among attacks that can threaten an e-voting system, this vulnerability can permit a voter to create more than one identity on a blockchain network. To avoid that in our system, the list of legitimate users is added by an administrator and a smart contract controls the process of voting by allowing a voter to cast only one vote. In the work ahead, we aspire to strengthen this system by ameliorating the authentication process and to develop blockchain-based systems for other smart city services.

We have implemented our e-voting system on Ethereum platform, and our suggested solution architecture is made up of three core parts: an Ethereum wallet, smart contracts, and Ethereum blockchain. User authentication is handled via an Ethereum wallet by creating encryption materials (public and private keys). The public key is available to all peers and the private key is kept undercover by the user. These couple of keys serve as user credentials, allowing the network to check and confirm the user's validity using the public key. Smart contracts implement the core logic of the user voting process and counting the votes of users. The Ethereum blockchain is considered to be the engine of our e-voting system, after the network establishes consensus, transactions are authenticated and verified, resulting in the creation of the transaction block, which is then added to the blockchain. When a block is appended to the blockchain network, it permanently changes the network and is published and spread across nodes. It also ensures that voters are legitimate, the contract transactions are distributed and decentralized, and these transactions can be checked by everybody on the network, however, only the owner can decrypt them.





REFERENCES

- [1] V. Moustaka, A. Vakali, and L. G. Anthopoulos, "A systematic review for smart city data analytics," *ACM Computing Surveys*, vol. 51, no. 5, pp. 1–41, Sep. 2019, doi: 10.1145/3239566.
- [2] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499–507, May 2018, doi: 10.1016/j.scs.2018.02.039.
- [3] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, Jul. 2016, doi: 10.1109/MCE.2016.2556879.
- [4] M. Lacinák and J. Ristvej, "Smart city, safety and security," *Procedia Engineering*, vol. 192, pp. 522–527, 2017, doi: 10.1016/j.proeng.2017.06.090.
- [5] L. G. Anthopoulos, "The rise of the smart city," in *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?*, 2017, pp. 5–45.
- [6] V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos, "Enhancing social networking in smart cities: Privacy and security borderlines," *Technological Forecasting and Social Change*, vol. 142, pp. 285–300, May 2019, doi: 10.1016/j.techfore.2018.10.026.
- [7] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.
- [8] F. Z. Chentouf and S. Bouchkaren, "Blockchain for cybersecurity in IoT," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, 2021, pp. 61–83.
- [9] A. Bahga and V. K. Madiseti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 09, no. 10, pp. 533–546, Oct. 2016, doi: 10.4236/jsea.2016.910036.
- [10] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [11] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, Sep. 2018, doi: 10.1016/j.future.2018.04.060.
- [12] I. S. Farahat, A. S. Tolba, M. Elhoseny, and W. Eladrosy, "Data security and challenges in smart cities," in *Security in Smart Cities: Models, Applications, and Challenges*, A. E. Hassanien, M. Elhoseny, S. H. Ahmed, and A. K. Singh, Eds. Cham: Springer International Publishing, 2019, pp. 117–142.
- [13] M. H. Saračević *et al.*, "Data encryption for internet of things applications based on Catalan objects and two combinatorial structures," *IEEE Transactions on Reliability*, vol. 70, no. 2, pp. 819–830, Jun. 2021, doi: 10.1109/TR.2020.3010973.
- [14] M. H. Saračević, S. Ž. Adamović, N. Maček, A. Selim, and S. H. Pepić, "Source and channel models for secret-key agreement based on Catalan numbers and the lattice path combinatorial approach," *Journal of Information Science and Engineering*, vol. 37, no. 2, pp. 69–482, 2021, doi: 10.6688/JISE.202103_37(2).0012.
- [15] M. Saračević, S. Adamović, N. Maček, M. Elhoseny, and S. Sarhan, "Cryptographic keys exchange model for smart city applications," *IET Intelligent Transport Systems*, vol. 14, no. 11, pp. 1456–1464, Nov. 2020, doi: 10.1049/iet-its.2019.0855.
- [16] V. Rajasekar *et al.*, "Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm," *Scientific Reports*, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-021-04652-3.
- [17] J. Xie *et al.*, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019, doi: 10.1109/COMST.2019.2899617.
- [18] M. Simić, G. Sladić, and B. Milosavljević, "A case study IoT and blockchain powered healthcare," in *The 8th PSU-UNS International Conference on Engineering and Technology (ICET-2017)*, 2017, pp. 1–5.
- [19] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019, doi: 10.1109/JIOT.2018.2836144.
- [20] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2017, pp. 173–178.
- [21] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," *Records Management Journal*, vol. 26, no. 2, pp. 110–139, Jul. 2016, doi: 10.1108/RMJ-12-2015-0042.
- [22] E. Yavuz, A. K. Koc, U. C. Cabuk, and G. Dalkilic, "Towards secure e-voting using Ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Mar. 2018, pp. 1–7, doi: 10.1109/ISDFS.2018.8355340.
- [23] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: A survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019, doi: 10.1109/COMST.2018.2867288.
- [24] Gartner, "Forecast: blockchain business value, Worldwide, 2017-2030," *Gartner Research*. 2017. <https://www.gartner.com/en/documents/3627117/forecast-blockchain-business-value-worldwide-2017-2030> (accessed Aug. 13, 2020).
- [25] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2018, pp. 1–4, doi: 10.1109/ICCCNT.2018.8494045.
- [26] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.
- [27] D. D. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.
- [28] T. Gibbs and S. Yordchim, "Thai perception on Litecoin value," *International Journal of Social, Education, Economics and Management Engineering*, vol. 8, no. 8, pp. 2613–2615, 2014.
- [29] M. Haferkorn and J. M. Q. Diaz, "Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, Litecoin and Namecoin," in *International Workshop on Enterprise Applications and Services in the Finance Industry*, 2014, pp. 106–120.
- [30] M. Benji and M. Sindhu, "A study on the corda and ripple blockchain platforms," in *Advances in Big Data and Cloud Computing*, 2019, pp. 179–187.
- [31] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc. White Paper*, vol. 5, no. 8, 2014.
- [32] E. Androutaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.
- [33] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance Evaluation of the Quorum Blockchain Platform," *ArXiv Prepr. ArXiv180903421*, Jul. 2018.
- [34] E. Ben Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and*





- Privacy*, May 2014, pp. 459–474, doi: 10.1109/SP.2014.36.
- [35] M. S. Ali, K. Dolui, and F. Antonelli, “IoT data privacy via blockchains and IPFS,” in *Proceedings of the Seventh International Conference on the Internet of Things*, Oct. 2017, pp. 1–7, doi: 10.1145/3131542.3131563.
- [36] M. Bartoletti and L. Pompianu, “An empirical analysis of smart contracts: platforms, applications, and design pattern,” in *Financial Cryptography and Data Security*, 2017, pp. 494–509.
- [37] A. Bin Bishr, “Dubai: A city powered by blockchain,” *Innovations Technology Governance Global*, vol. 12, no. 3/4, pp. 4–8, 2018.

BIOGRAPHIES OF AUTHORS



Fatima Zahrae Chentouf     is currently pursuing her Ph.D. degree with the Department of Systems and Computer Science, ENSAT, ERMIA Team, Abdelmalek Essaadi University, Tangier, Morocco. Her current research interests include internet of things security and blockchain. She received her master’s degree in cybersecurity and cybercrime from the National School of applied sciences of Tangier (ENSAT) of the University Abdelmalek Essaadi, Morocco, in 2020. She can be contacted at fatimazahrae.chentouf.97@gmail.com.



Said Bouchkaren     received his engineer degree and Ph.D. from the National School of Applied Sciences of Tangier (ENSAT) in 2010 and 2016, respectively. He worked as an IT instructor from 2011 to 2018, and from 2018 till now as an associate professor in the Mathematics and Computer Science Department, ENSAT. He is a member of the ERMIA research team. His main research field is cryptography, blockchain, the Internet of things, and system security. He can be contacted at sbouchkaren@uae.ac.ma.