Secure- Reliable Blockchain-Based Data Access Control and Data Integrity Framework in The Environment of Smart City

Alexander A. Varfolomeev¹, Liwa H. Alfarhani², Zahraa Ch. Oleiwi³

¹ BMSTU, NRNU MEPhI, RUDN, Information Security Department, Moscow, Russia
² PhD Student at Academy Engineering, RUDN University. Email: liwarussia@gmail.com
³ Faculty of Science, University of Al-Qadisiyah. Email: zahraa.chaffat@qu.edu.iq

Abstract. The most important concern of smart cities and electronic governments that provide their services through smart applications and modern technology is security, reliability and privacy management. Therefore, it has become an effective research area. The open access environment that the Smart City idea offers suffers from the issue of data access and integrity rights. Encryption, Sequence Detection, and other traditional techniques may be somewhat unable to maintain the required level of security. In this paper, we suggest a practical framework based on blockchain technology and how its positive advantages will be reflected to provide a secure, reliable, integrity and controlled data access system. The main idea presented by the research is to manage access rights and protect privacy according to blockchain strategies. The analytical results showed a high level of protection, decentralization and reliability of the proposal based on blockchain technology and its advantages.

Keywords
Smart City, Smart Contract, Data Access Control, Data Security, Privacy Management.

1. Introduction

In light of the accelerating trend towards smart open environment in providing services and managing various aspects of life, everyone strives for content that is available to everyone according to the security scripts and systematic management of privacy [1]. Problems remain and challenges are difficult despite dozens of technologies based on different safety environments, including high coding and decoding techniques, techniques for detecting hostile behavior, anti-intrusion, and unwanted piracy [2]. Everyone is searching for safety and privacy because the technology has shifted from the polling stage to the stage of work, trade, financial transfer, sale and purchase, management of important aspects of the economy and trade, and management of state institutions and their various services under the tent of the so-called smart city environment and e-government [3]. In this paper, we present a framework to demonstrate the efficiency and reliability of the work based on Blockchain technology through a set of important advantages of this technology, which have contributed greatly to reducing security concerns.

A blockchain system is a group of devices, each device that connects to the system is called a node. Each of these nodes performs a specific task, for example storing information about the operations performed within the system. These nodes are linked in a chain, so that each node is connected to the node before and after it. Where data and processes are distributed between every two nodes on a set of blocks that are protected by encryption algorithms. To avoid any kind of circumvention, the system groups operations into blocks, and when a payment order is issued, an encrypted block is created. But to issue another order to cancel the payment, the system creates another block that depends on its encryption key on the block that
precedes it, and this means that the blocks are linked to each other, hence the name "chain of blocks", and any sudden change that requires the system to verify the legitimacy of that process. In the coming sections, we will expand on the details of this technology, which is now considered one of the rich research points [4].

2. Blockchain technology
Before 1991, no one knew or used a term. The idea started from a group of researchers when they wanted to create a tool for setting a time marker or similar. The purpose was to prevent tampering or altering or modifying digital files. This means that the primary goal of innovation was information security. So, the researcher Satoshi Nakamoto in 2008, who relied on his idea to establish the first cryptocurrency based on a blockchain technology called Bitcoin. Major important advantages of this technology are the most important of them decentralization and transparency high-level security and. Its importance is also reflected in its high efficiency and cost pressure. So, we see it now as a great research point for many applications and ideas based on it [5].

2.1 Work mechanism
The basics of blockchain technology work can be illustrated by reviewing its fundamentals. The fundamental elements or ideas of blockchain technology illustrated in figure 1[6]. We have explained above the reason for calling it a block, but its function is to record all transactions and status results that occur over a period, a consensus on the current ledger status. Transaction is an operation of a reconciliation book that results in a change in the status of the ledger, such as the addition of a transfer record while a chain is the log records of change in the state of the entire ledger, which are appear as series by chunks in the order in which they occur[7].

As shown in figure 2, in the implementation of blockchain technology, first assume that there is a distributed data record ledger, which is only allowed to be added, not allowed to be deleted. The underlying structure of the ledger is a linear list including a series of blocks followed by the block. Adding a new data required basic steps done to do this process. Firstly, the new data must be placed in a new block. Checking and verifying process used to test the legality of the new block. also, the transaction in the new block can be quickly verified by calculating hash. Any legal node can propose a new legal block, but the blockchain technology algorithm which called consensus mechanism which represent the final decision of the block addition [8].

We will list the steps to explain the basics of blockchain technology as follows:
I. The generation of the transaction.
by using the private key, the current owner starts to sign a digital signature on the previous transaction and the next owner, and attach the signature to the end of the currency to make a trade order. Any new transaction proposed must firstly broadcast to other nodes which participating in the blockchain network [9].
I. The spread of the transaction
Proof-of-Work represent the gate of checking in blockchain technology which also called PoW. It is the original consensus algorithm in a Blockchain network used to perform two essential steps first it is used to confirm transactions and second it is used to produce new blocks to the other nodes in the chain. With Proof-of-Work (PoW), miners contest against each other to complete transactions on the network and get rewarded. The transaction sheet is broadcasted to the entire network by current owner, and several unverified transaction hash values into the block are collected via each node, each containing transactions about thousands or hundreds. POW the node that completes pow as quickly as possible propagates its own blocks to other nodes [10].

II. Proof of workload
Each node acquires the power to create new blocks and competes for rewards for digital currencies through a workload proof mechanism equivalent to solving a math problem. Each node performs the
calculation of the workload proof to determine who can validate the transaction, and the node that calculates the result as quickly as possible to validate the transaction is the practice of achieving consensus [11].

III. Full-node validation
When a node finds the intercept, it broadcasts to the whole network all the time-stamped transactions recorded by the block, and by the other nodes of the network check, other nodes will confirm whether the transaction contained in the block is valid, confirm that the block has not been repeatedly spent and has the effective digital seal, accept the block, at this time the block is officially connected to the blockchain, can no longer tamper with the information[12].

IV. Blockchain records
Other nodes across the network check the block bookkeeping correctness, and after no errors they will compete for the next block after the legal block, thus forming a legitimate billing block

2.2 Distributed Consensus Mechanism
The core of the blockchain system is the competition of the nodes in the system to keep accounts. This competitive process is called a consensus mechanism. There are four parts in the bottom layer of the blockchain components, as shown in figure 3, a distributed database is used to store past and future transaction data, and the cryptographic public-private key system is used. To confirm the identity of both parties to the transaction, the P2P network is used to broadcast and spread various types of messages (such as node join messages, node failure messages, and get mining data message) and the consensus mechanism used to determine the node's accounting rights[13].

Figure 3. Consensus Mechanism
3. Blockchain-Based Access Control Framework

The proposed data access control framework based on the advantages of blockchain technology which present a solution to the problems of existing centralization techniques which also used to develop the technology environment of work, any node participant in it can exchange value under this framework.

![Diagram: Publishing Tasks Based Blockchain Technology Platform]

**Figure 4.** Publishing Tasks Based Blockchain Technology Platform

In the practical application process, whether for the task publisher or for the task recipient, before accessing this basic platform, will be blocked, using the trusted technical characteristics of blockchain, to determine whether the current user has this right to access, only through authentication and the contract access control conditions, can be followed up. On this platform, we can clearly represent published tasks with data, and the publisher of the task can be defined as the owner of the data, who can define the rules for access to the data according to his needs. The task recipient can be treated as a visitor to the data, and certain conditions need to be met to access and operate the owner's data as shown in figure 4. Combined with the above on how to achieve business operations in an open environment in a blockchain network, a blockchain-based data access control framework is proposed as shown in figure 5.
Figure 5. Blockchain-Based Data Access Control Framework

In an open environment, the data owner will define the data access control rules [DEF (data)] according to the sensitivity of the data, and form the access rules in the form of smart contracts, and deploy to the blockchain network submit (contract). Visitor according to the data, the identity verification V(ID) needs to be performed first. If it passes the identity verification and meets the contract condition C(condition), it can be obtained to the identity token (T), for example T = {V(ID) AND C(condition)}, the data accessor can hold this token to access the data object. In this framework, anyone can post tasks and receive tasks, without the so-called centralized thought. In the decentralized environment, the owner of the data can customize the data access rights, that is, the requirements of the task, the visitor according to their own conditions, if you think you are competent, you can apply for it. After passing the complex blockchain verification, you can access the execution data (task). No third party with the intervention, both parties can complete the peer-to-peer transaction in a free environment.

3.1 Smart Contract Design
The data owner formulates the contract according to the access rules, and the smart contract of the blockchain gives the ledger programmable features, which is also the realization of user data [14].
The concept pattern diagram of smart contracts is shown in figure 6. In general, the smart contract encapsulation defines a number of states, transition rules, trigger conditions and response actions, etc., after the signing of the parties in the form of program code attached to the blockchain data, after peer-to-peer computer network propagation and node verification recorded in the distributed ledger of each node, blockchain can real-time monitor the status of the entire smart contract, after verifying that the external data source confirms that specific trigger conditions are met, to activate and execute the contract. The definition and description of these relational data in the contract is the key to the whole system, and it is necessary to specify the representation of the contract in design to satisfy the expression of the reading and writing rules in an open environment.

The basic representation is:

i. The custom data model of the contract corresponds to the specific relationships in the network.

ii. The functional method of the contract corresponds to the reading, writing, and updating of network data.

iii. The logical design in the contract corresponds to the rules that exist in the network data.

Data owners can flexibly define smart contracts to meet their own business needs, depending on their wishes.

3.2 Participant rights management
We have reviewed the advantages of blockchain technology and its most important. Under the shadow of these features, it has become easy to deal with all previous problems related to authentication and personal coordination with the technical features of the blockchain. Individuals gain a good level of freedom to create encrypted digital IDs, manage the topic of username and passwords and change and modify them according to requirements. The subscriber as this technology provides more comprehensive security features that reflects on the overall performance of the system and saves customers and institutions valuable time and resources. Another process of issuing digital certificates to identify users is another feature of Blockchain technology and enhances user authentication procedures. If the new visitor to the network gets blockchain authentication, he will move to the second stage of the smart contract recall process that we explained earlier. A quick audit processes are used to check the status and, in the event, that the conditions and rules set for this contract are met by the data owner, meaning that he will cross to the third stage that includes obtaining the final communication code that enables him to reach the final result of that type of contract[15].

4. Blockchain-Based Data Integrity Framework

Normally blockchain work as distributed system using the consensus systems as well as cryptography algorithms to provide digitalised trust instead of centralize party. This mechanism distributes transactions into a group of blocks. Each block contains information and an identification number. The identifier is encrypted using the hash function, and each block must contain the hash of the previous blocks. Based on this mechanism, data integrity is obtained with a high rate. Any attempt to attack, change, delete or add to information from a block leads to a change in its hash and is therefore be not specific and validate to the next subsequent block [16]. This makes it difficult for the attacker to penetrate all the copied data without being detected, as he must accumulate all the nodes to reach the full whole information, but once he breaks through one of the nodes, his presence will be alerted by the rest of the nodes. Below equations illustrate the complexity and time the hacker required to attack information in blockchain based system

Let C refers to complexity and cost, T refers to time, N total number of blocks in blockchain between to object in the smart city, I refer to information in each block.

So, in blockchain based system

\[
\text{whole information} = I_{n1} \parallel I_{n2} \parallel \ldots \ldots \parallel I_N
\]

Total time of attack = \[T(I_{n1}) + T(I_{n2}) + \ldots \ldots + T(I_N)\] (1)

Total cost of attack = \[C(I_{n1}) + C(I_{n2}) + \ldots \ldots + C(I_N)\] (2)

According to equation (2) then

Total time of completed process between two objects \ll Total time of attack.

As compared with centralized system:

\[
\text{whole information} = I_N
\]

Total time of attack = \[T(I_N)\] (4)

Total cost of attack = \[C(I_N)\] (5)

Total time of attack in blockchain \gg Total time of attack one database in centralized system

5. Comparative Analysis

In order to explain the advantages of the blockchain technology and its impacts to present a reliable and secure working environment, we will make a comparative analysis by focusing on very important points data security, privacy management, trust mechanism, and other evaluation measurements.

5.1 Data security and vulnerabilities

Comparing with the commonly used access models, a centralized server proposed to complete the authorization decision. and the Internet of Things (IoT) access control model present a distributor
architecture, but it is not safe to place access control decisions on weaker IoT devices, it is vulnerable to a single point of attack by hackers and cannot be satisfied application requirements in an open environment. In other side, the decentralized blockchain technology solves the data security problems brought by centralization very well. It not only ensures the safety and reliability of the information on the chain, and also bring new vitality to access control in the internet development environment [17].

So, the data security, collection and analysis of data in the smart city is based on the strength of the security of the blockchain technology, as a result of its decentralization property that causes an increase in the cost and complication for the attacker.

5.2 Reliability

In today's internet environment, data owners are generally played by third-party organizations because they have the ability to provide adequate computing and storage resources. But leaving data access control power to third-party agencies can lead to a crisis of confidence, such as data tampering, rule-making, data breaches, and so on. Blockchain technology is designed to solve the trust problem of the Internet, which solves the disadvantages of central monopoly rule based on trust from a technical point of view [18].

5.3 Privacy Management

One piece of data per node strategy makes Blockchain has highly redundant storage. privacy-protected point represents another strong advantage of blockchain also it is decentralized and secure. All these points make it particularly suitable for storing and protecting critical privacy data to avoid large-scale data loss or leakage due to attacks on centralized organizations or improper rights management. Any data can be generated by hash operations and Merkle packaged into the blockchain. the security is guaranteeing through the calculation and asymmetric encryption of the consensus nodes within the system. The access control strategy defined by each data owner is recorded on the blockchain, which is more secure and reliable due to the decentralization and tamper-proof nature of the blockchain. After authentication, visitors have secure access to data if they have access to the contract. The use of blockchain access control ensures the security of data access by participants in an open environment [19].

5.4 Performance measurements

The characteristics of the blockchain related to energy consumption and hardware (resource consumption) have a direct positive impact on the performance of the processing system in the smart city, as the blockchain is characterized by relying on the algorithms in it with less reliance on materials, which saves less cost and time and thus is faster in performance than centralize technologies[20][21].

The other feature that the blockchain adds to the smart city environment is the ability to deal with an increasing amount of work, which is known as scalability, as the principle of blockchain work, which relies on variable size blocks, has the effect of adding the scalability feature to the smart city environment[22].

6. Conclusions

Over time, Blockchain technology demonstrates its transparency and efficiency. Studies based on demonstrating the advantages of this positive technology also demonstrate that it provides a reliable work environment. The data access control model we discussed in this paper illustrates the good level of data management security based on the distributed nature of this technology that leads to good protection and marginalization of the impact of human error, and even protection from intentional attacks as well. We have come to speak of true digital freedom under blockchain technology. Freedom makes the user the decision-maker in the administration without decentralization from anyone and
without guardianship. All these features have made blockchain technology very suitable for the market aspirations. Its current development, evidence of its compatibility with the future vision of successful technology.

References

[1] H. Samih, "Smart cities and internet of things", Journal of Information Technology Case and Application Research, 2019.

[2] S. Sengan et al., "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network", Future Generation Computer Systems, Volume 112, Pages 724-737, November 2020.

[3] F. Dai et al., "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues", 4th International Conference on Systems and Informatics (ICSAI). Hangzhou, China: IEEE, 2017.

[4] A. Alketbi, Q. Nasir, and M. Abu Talib, "Blockchain for government services — Use cases, security benefits and challenges", 15th Learning and Technology Conference (L&T). Jeddah, Saudi Arabia: IEEE, 2018.

[5] M. Graglia, and C. Mellon, "Blockchain and property in 2018: At the end of the beginning", Annual World Bank Conference on Land and Poverty. Washington, DC, 2018.

[6] F. Daniel, and L. Guida, "A service-oriented perspective on blockchain smart contracts", IEEE Internet Computing, 2019.

[7] S. M. H. Bamakan, A. Motavali, A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria", Expert Systems With Applications, Elsevier, 2020.

[8] S. Aggarwal, et.al. "Blockchain for smart communities: Applications, challenges and opportunities", Journal of Network and Computer Applications, 2019.

[9] S. Thompson, "The preservation of digital signatures on the blockchain", University of British Columbia iSchool Student Journal, 2017.

[10] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms", Paper presented at the 2018 41st International Convention on Information and Communication Technology. Electronics and Microelectronics (MIPRO), 2018.

[11] I. Bentov et al., "Proof of activity: Extending Bitcoin’s Proof of Work via Proof of Stake", IACR Cryptology ePrint Archive, 2014.

[12] A. Winnicka, and K. Kesik, "Idea of using blockchain technique for choosing the best configuration of weights in neural networks", Algorithms, 12(8), 163, 2019.

[13] W. Wang, et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks", IEEE Access, 7, 2019.

[14] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology", 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Bangalore, India: IEEE, 2018.

[15] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", Journal of Network and Computer Applications, 143, 167–177, 2019.
[16] K. Biswas, and V. Muthukumarasamy, "Securing smart cities using blockchain technology", In Proceedings of the 14th IEEE International Conference on Smart City High Performance Computing and Communications, pages 1392–1393, 2016.

[17] K. Alachkar, and D. Gaastra, "Blockchain-based Sybil Attack Mitigation: A Case Study of the I2P Network", https://www.os3.nl/_media/2017-2018/courses/rp2/p97_report.pdf, 2018.

[18] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?" Available at SSRN, 2709713, 2015.

[19] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home", In Proceedings of the 2nd IEEE Workshop on Security, Privacy, and Trust in the Internet of Things (PERCOM), Hawaii, USA, 2017.

[20] F. Haidar, A. Kaiser, and B. Lonc, "On the performance evaluation of vehicular pki protocol for v2x communications security", In Proceedings of the 86th IEEE Vehicular Technology Conference (VTC-Fall), pages 1–5, 2017.

[21] J. Li et al. "Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies", Energy, 168, 160–168, 2019.

[22] J. Poon, and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments", https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf, 2016.