# Blockchain and IOT integrated Smart City Architecture

**Dr. Chaitanya Singh[a], Dr. Rohit Tripathi[b], Dr. Ranjan Walia[c], Ms. Deepika Chauhan[d], and Ms. Anju Asokan[e]**

[a]
Associate Professor, Department of Computer Science & Engineering, Shivajirao
Kadam Institute of Technology and Management, Indore, M.P, India
[b]Electronics Engineering Department J. C. Bose University of science and technology, YMCA, FARIDABAD-121006, HARYANA, India
[c]Associate Professor, Electrical Engineering Department, Model Institute of
Engineering and Technology, Jammu and Kashmir, India
[d]Assistant Professor, Department of Computer Science & Engineering, Shivajirao Kadam Institute of Technology and Management, Indore, M.P, India
[e]Assistant Professor, Sri Krishna College of Technology, Golf Rd, Arivoli Nagar, Vivekanandapuram, Kovaipudur, Tamil Nadu, India

**Article History**: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

**Abstract:** Recently, the concept of "Smart Cities" has been greatly improved with the growth and development of the Internet of Things as a new form of sustainable development. Smart cities rely on independent and distributed infrastructure that includes information processing and control systems, diverse network infrastructure, and ubiquitous sensitivity that includes millions of information sources. Due to the continued growth of data volume and the number of connected IoT devices, however, issues such as high delays, bandwidth barriers, security and privacy, and scalability emerge from the current smart city network construction. Designing an efficient, secure and scalable distributed architecture by bringing computer and storage resources closer to endpoint is needed to address the limitations of today's smart city network. In this paper, we propose a hybrid network design for an intelligent city using the emerging technologies of Software Defined Networking and blockchain technology. To achieve efficiency and address current constraints, our paper is divided into two parts: the main network and the edge network. In this we proposed hybrid architecture which inherits the capability of both centralized and decentralized network integrated with proof of work for the security and privacy. To evaluate the feasibility and performance of our proposed model, we simulate our model and evaluate it based on various performance metrics. The result of the evaluation shows the effectiveness of our proposed model.

**Keywords**: IoT, Blockchain, Hybrid Architecture, PoW, Bitcoin

## 1. Introduction

The Internet of Things (IoT) has a vision and provides a promising future for traditional Internet industries and communities, and the realization of smart cities is also tied to the IoT vision. By using low-cost sensors and a variety of smart devices to collect data on public infrastructure, a smart city increases efficiency, shares information with the public, and improves quality of life, cost of living, and government services and the environment [1] [2] [3]. Nowadays, a huge wave of urban migration around the world and people moving to cities due to economic growth and social change. Recently, the United Nations predicted that 86% of developed countries and 64% of developing countries would be included in cities by 2050 [4]. Gartner's report predicts that 30% of smart city health care applications will have intelligent robots and equipment, while 10% of smart cities will use street lights as the backbone of a smart cities network by 2020 [5]. That means billions of devices and systems will be integrated in the future, from end-user devices to smart transport, health care, industry, buildings and facilities. Therefore, the facto expectations of the smart cities network to analyze large amounts of data generated by IoT devices, increase security and privacy, see better use of network bandwidth to avoid congestion, support real-time applications, etc.

Recently, blockchain technology has attracted many participants in many industries such as agriculture, cryptocurrency, real estate, etc. IoT technology and blockchain technology are felt throughout our daily lives. Gartner's report predicts that $ 3.1 trillion in business value will be added by 2030 [6]. By taking advantage of the blockchain process on the IoT network, we can offer new ways to change business processes without the need for expensive and sophisticated IT infrastructure. This will help us build trust between devices and users, reduce the risk of fraud and costs, eliminate middleware, and reduce transaction payment time. To simplify business processes, realize cost savings, and improve user experience, blockchain-based IoT solutions are well-suited. On the other hand, Software Defined Networking (SDN) is gaining traction between technologies and its disruptive quality. As an emerging network builder, it eliminates the control of network from traditional hardware devices. SDN-based solutions can assist with meeting needs such as scalability and seamless, efficient, and cost-effective transportation in the architectureof the IoT network [7].

According to the analysis above, new network design is required to address the current limitations of smart city network building using the emerging SDN capabilities and blockchain technology. In this paper, we propose to build a hybride novel of a smart city network that uses SDN techniques and blockchain strategies to address these issues. We discuss the current architecturechallenges we face in finding a smart city network. We are launching the Argon2 based Proof-of-work (PoW) program in our proposed distributed city network architecture. We also describe the mining process for our proposed buildings in the main network. To test the availability and performance over the proposed model, test analysis was performed based on different parameters.

The whole paper is structured as follows: In Section 2, we discuss the challenges of building a smart city network, a summary of Proof-of-Work and Argon2, and blockchain and IoT related activities; in Section 3, we present our proposed model to address the current limitations of an intelligent city network; in Section 4, we assess the feasibility and performance of our proposed model based on different performance metrics; Finally, we present the conclusions of our study in Section 5.

Architecture challenges in Smart City

In the architectural design of the smart city network, the global population transition to cities puts increasing pressure on urban areas in terms of race, delays, network bandwidth usage, data privacy and security challenges. In the future with large cities, cities can offer a higher standard of living by smart walking, smart living, smart walking, smart energy, and smart business models to support everything. Here, we discuss some of the challenges facing the art of building a modern city network and what we need to address with a smart city network that is sustainable:

1. Low Delays and High Rates: Due to the simultaneous services requested by multiple devices in various locations in the smart city, a strict requirement - such as low delays and high mobility - is being introduced. Addressing the challenges presented by smart city applications requires an effective network construction
2. Structural downturns: Downgrade is another smart city network challenge that we need to address when building smart city infrastructure. This asset allows the system to grow when needed without the need for major changes in network configuration.
3. Network bandwidth constraints: In the case of a smart city application, solutions based on architecture are not appropriate due to network bandwidth. For alternative architecture, we must send all data collected by IoT devices to the main network, which will require a large amount of network bandwidth. To address the bandwidth problem and reduce bandwidth usage, we need to design a structure that allows data performance and analytics performance locally and only sends filtered data to the main network where needed.
4. Privacy and security: Due to the rapid increase in the number of devices connected to the Internet, our smart city network infrastructure offers many security and privacy issues and challenges. Like information databases and networks, the architectureof smart city networks should be able to protect data from destruction, alteration, disclosure, unauthorized access, and cyber attacks.
5. Points of Failure: Building a smart city network can have a large number of single points of failure due to the continuous growth of various networks, which can also undermine the services considered by a smart city. Providing a faulty network requires network configurations that do not interfere with intelligent city applications.

Proof-of-Work with Argon2

In cryptocurrensets and blockchain technology, PoW is a key component that enables large-scale community-led ledgers. Because of the difficulty of building statistics, it is very difficult to measure and manage trust. Initially, PoW was proposed to reduce the spam problem and later used it in the Bitcoin protocol by Nakamoto [8]. In Bitcoin, PoW is usually based on the repetition of two cryptographic functions SHA-256 until the result indicates a special lucky number. The functions of PoW are easy to observe but difficult to quantify [9].

As a difficult task to remember password hashing and other applications, Argon2 was selected as the winner of the Password Hashing Competition in July 2015 [10]. Biryukov, et al. [11] proposed a PoW-based memory scheme using the Merkle hash tree over the Argon2 hash series. Contains disk encryption and strengthening parameters for cryptocurrency applications. For the same members, the PoW schema creates the Merkle tree and the pseudo- randomly selects a set of leaves based on the tree's hash root as a computation proof. In the Argon2 chain, it is very difficult for the invaders to show the knowledge of the proper properties of the Argon2 chain and their proper methods in the Merkle tree. Therefore, if some attackers try to copy and retain a small portion of the Argon2 chain, they are more likely to be caught.

Blockchain and IoT related activities

In our previous work, we suggested that the blockchain structure was distributed through the smart city network structure [12]. Here, we introduce the idea of building safe and reliable transport management structures. We also suggest that the DistBlockNet model, IoT mesh network architecture uses SDN and blockchain [13]. In this model, we also propose a flow rules update system to securely update and validate the flow rules tables in the messaging network. Later, we expanded our work and proposed blockchain-based cloud-based distribution for SDN fog nodes for a scalable IoT network [14]. Bahga, et al. [15] proposed a platform allocated to the Industrial IoT (IIoT) platform using a blockchain process to remove a trusted link and build a peer-to-peer network. Christidis, et al. [16] reviewed blockchains applications and smart IoT contracts. Distribution of unreliable trust data among cloud service providers using blockchain proposed by Xia, et al. [17]. Provides shared data for cloud storage and enables book auditing, data recognition, and management of shared shared data. Li, et al. [18] proposed a secure IIoT power trading system.

To the best of our knowledge, research work on smart city and blockchain is very limited in literature. Much of the work focuses on using blockchain technology to benefit the IoT in a standard or straightforward manner. Building a new construction platform dedicated to a smart city network is necessary, taking into account all aspects of current and future challenges.

## 2. Proposed Architecture

The smart city has become a emerging concept for IoT growth and development. It is very important to consider sub-network considerations when designing a smart city network design. An example is a smart structure where the sensor is connected to a lighting line that can be part of a large architectureapplication. A smart building and can be part of a network of smart cities. In this regard, we must take into account the fact that the data is not only transmitted locally but also a large network of buildings and ultimately to a large network of cities. The design of new smart city networks is needed to address the current network building constraints as discussed in previous sections. In this section, we propose a blockchain-based hybrid network network design for a smart city and discuss the specific details of the proposed model.

(a) Architecture design overview

Achieving efficiency and decline in IoT network hope management, Kim, et al. [19] introduced the concept of trust management that is widely distributed around the world. They thought the infrastructure to prove the authenticity and authorization of IoT to be centralized and distributed globally. In our previous work, we proposed Dist BlockNet, a blockchain-based architecture distributed across the SDN architecture of the IoT network [13]. We have used the power of structures proposed by Kim, et al. [19] and Sharma, et al. [13], we suggest a hybrid architectureof a smart city network with blockchain strategies and Software Defined Networking (SDN) strategies to overcome the limitations of the current smart city network infrastructure.

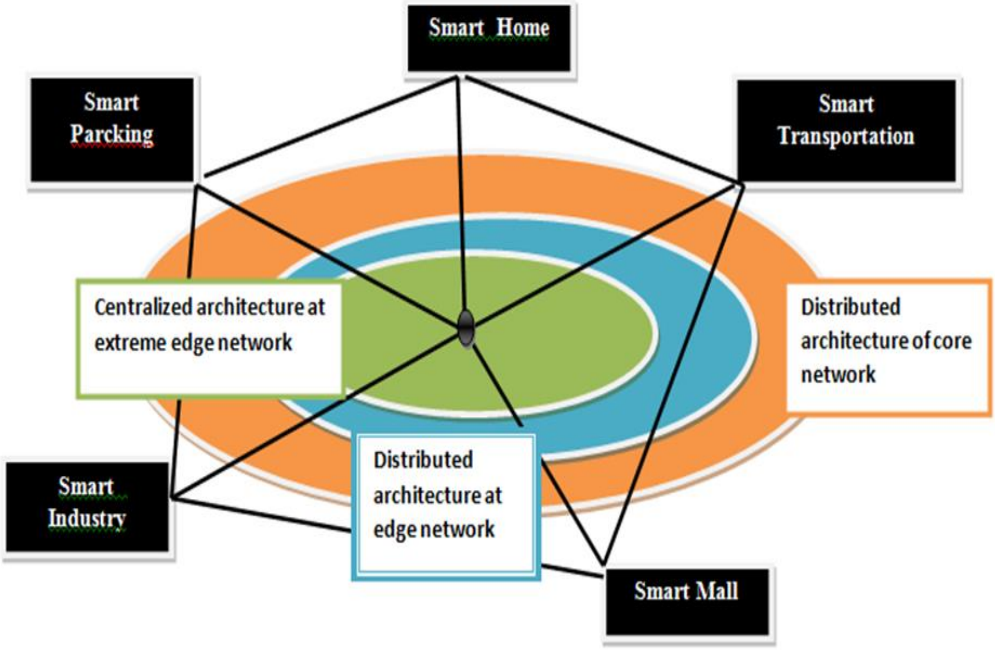
Smart Home
Smart Parcking
Smart Transportation
Centralized architecture at extreme edge network
Distributed architecture of core network
Distributed architecture at edge network
Smart Industry
Smart Mall

Fig 1: proposed complete hybrid architecture

Figure 1 shows the proposed complete hybrid architecture of an intelligent city network. In the proposed model, the smart city network is divided into two distinct groups - the main network and the network network - using the blockchain process. The main network consists of nodes with high counting and end-to-end resources, while the boundary node has limited storage capacity and computational power. Miner nodes will be responsible for building blocks and verifying proof of performance. Each node is powered by an SDN controller to achieve maximum speed and security, reduce hardware management costs, and experience ease of deployment on intelligent city network infrastructure. Here, we have used the security capabilities of the FS-Open Security SDN model from our previous work [20]. In our proposed infrastructure, each edge node acts as a central server for a particular public infrastructure to provide essential services and local implementation. Maintains access policies and guarantees for its registered organizations in the repository and helps achieve lower delays and reduce network bandwidth. Distributed status of the proposed the model can do the whole system is able to withstand and limit the impact of the attack anytime node is compromise. In other words, if the node at the edge is damaged, the resulting effect should be limited to the local area.

(b) Proposed model workflow

In a smart city, IoT devices produce large amounts of data and require real-time processing. In our proposed model, edge nodes offer real-time performance with low latency and network bandwidth usage and distributed across the network. Border node has limited computer capacity and processes raw data that can be loaded with storage devices to filter data and get useful information. When the data is pre-processed, the boundary node transmits the encrypted data to the main intelligent city network if necessary. The mining node in the core network will continue to analyze previously processed data, make decisions, validate and validate PoW, and produce blocks. To ensure the integrity of the data stored on the main network, we use a digital signature and store store hashes in the blockchain. This speed in blockchain is immutable, which serves as proof of the authenticity of the data. Figure 2 shows the workflow of our proposed model, in which we have implemented an Argon2-based hashing system.

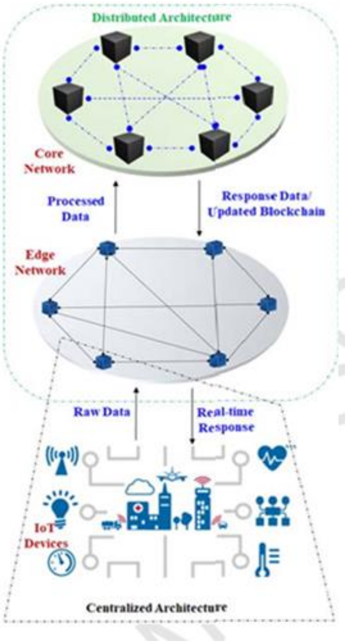

Fig 2: Workflow of proposed model

(c) PoW Algorithm

In today's cryptocurrensets and blockchains, PoW is a key component. By solving the difficulty of measuring and managing reliability with sophisticated statistical computers, these methods allow large books to be distributed publicly. For our proposed model, we use a complex PoW scheme called "Itsuku PoW," proposed by Coelho. et al. [21]. Itsuku PoW system is inspired by MTP-Argon2 [22]. Fixes issues such as unintended retrieval attacks, memory storage, random false listing, parallel searches, and robust input attacks by adding new functions and modifying MTP-Argon2 parameters to improve memory complexity. Table 1 shows the fake code of the Itsuku PoW scheme algorithm. The scheme assumes the challenge of inserting me, and the difficulty d, and the result of the search algorithm is (N, 亞, b, Æ), where T is the number of fixed objects, L is the length of a single search, HS is a variable hash size function, 亞 indicators of selected leaves, b of selected leaves, and Æ combined evidence of the Merkle tree of both selected leaves and their contraindications, if any. A detailed description and detailed analysis of the Itsuku PoW program is provided in [21].

(d) Mining process at the core network

After receiving the transaction on the main node from the edge node, the mining process is started. Due to resource constraints in the buttocks, we are making the mining process in the main network in our proposed model. The mining process includes the following steps:

Step 1: Anytime edge node receives a new transaction application with the necessary services by the IoT device / user, sends a transaction request to each miner on the main network.

Step 2: After receiving the transaction request, the miner node checks and verifies whether the transaction has been changed or not and whether the transaction is in blockchain or not. If the action is not changed, and is not in block, miner node proceeds to step 3. Besides, the miner node cancels the mining process and broadcasts the report to the main network.

Step 3: In this step, the miner node returns the previous block ID and starts the PoW process. In the case of the genesis block, the previous block ID is zero. The genesis block is the first block in the blockchain. In the PoW process, the miner node will create a new block by translating details, including previous ID, generated ID, date and time stamp, verified transactions, and the miner's digital signature using the Itsuku PoW algorithm mentioned above.

Step 4: Once a block is created, to ensure the integrity of the details of all blocks in the blockchain, the nodes check and verify all existing blocks.

Step 5: In the final step, the mining node sends the updated blockchain to all Edge nodes and provides the requested services to IoT devices / users.

Algorithm:

Input: input challenge (I), difficulty (d), independent segment (P), and segment length (l) Output: (N, 亞, b, Æ) Begin

```
Step 1    Build challenge-dependent memory XI[1… T] as P independent segments of length l
Step 2    Compute the root φ of the Merkle hash tree X
Step 3    Select nonce N
Step 4    Compute Y0 = HS(N‖φ‖I)
Step 5    For 1 1 ≤ j ≤ L Do
ij–1 = Yj–1mod T
Yj = HS(Yj–1‖XI[ij–1]⊕I)
Step 6    Back sweep over intermediates hashes in reverse order P = HS(YL‖… ‖Y1–L mod 2 ⊕ I)
Step 7    If P has d binary leading zeros Then
Step 8    return (N, 亞, b, Æ)
Step 9    Goto Step 3
End
```

## 3. Results

At this stage, we emulate our proposed model on private etherium blockchain network to assess the feasibility of our proposed architecture. Here, we discuss the test results set and test based on various parameter metrics. All tests are performed on an Intel Core i5 CPU 3.40 GHz with 16 GB memory running on Windows 10.

We used go-Ethereum to set up our own private blockchain network and installed a Mist browser to enable the distributed property of network architecture. We defined our own custom genesis block and used the Argon2 hashing technique discussed in the previous section. Ethereum testnet is used to debug and test our model. We used Mininet at each edge and miner nodes to build SDN-enabled controller nodes. Here, we generate random data as raw IoT data and consider its hashes as the blockchain transaction.

## 4. Performance Analysis:

PoW is an important form of blockchain technology. Internally, PoW-based work should be difficult to resolve. This often comes down to a random process of trying to find a solution to a puzzle such as a hash collision, we observe difficulty, rate of hashing, the number of transactions per second for the variable block size in our proposed model and compared it with another system. Figure 3 shows the difficulty and level of hash of our proposed system. Indicates that the hash scale is continuously adjusted according to the level of difficulty in the proposed system.

Figure 4 shows how the size of a block affects the amount of action per second in our proposed model. Our match data is based on actual sales from the Bitcoin blockchain component [23]. The result shows that, compared to other systems, our proposed model achieves better performance.

We also found that the average block times behaved relative to the time frame and compared to the desired product (e.g. 10 minutes). Figure 5 shows the results of the block time behaviour by reorganization interval. We can see that this is also changing a lot, and yet our proposed model looks solid again near the normal blocking time. Initially, wild volatility appears to be due to large changes in hash values.

Fig 7 and 8 shows the test was performed based on a variety of peer numbers, both single and equal mines, using different levels of difficulty. Here, the difficulty level refers to the minimum number of consecutive eggs required at the beginning of an acceptable hash. Figures represent the results of the mines based on single and equal mines. Here, intermediate time (average) time refers to the average time required to resolve a block in seconds. This is calculated after performing several tests under the same conditions and taking into account the total results. Identification resolution, indicator, timestamp, transaction hash, previous hash and nonce are considered input. Here, in the case of mines alone, the time stamp and the previous hash are the same with a particular block for all miners. In terms of the same mines and this data, the trading hash is also the same for all miners of a particular block.

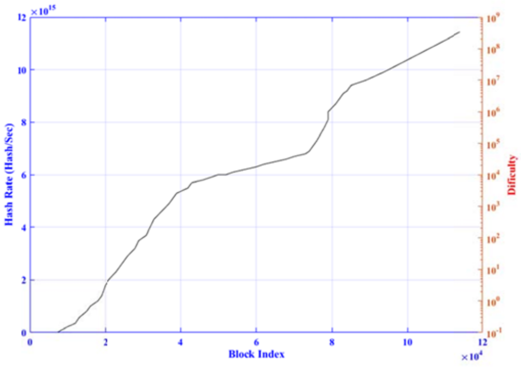

**Fig 3: Hash rate verses Difficulty**

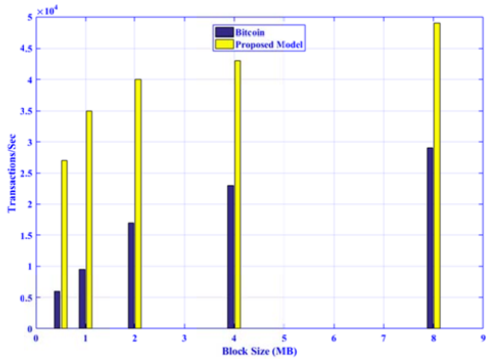

**Fig 4: Block size vs. Transactions/Sec**

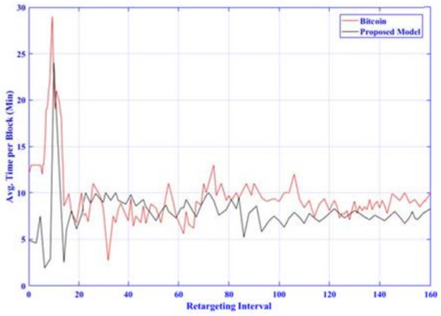

**Fig 5: Average time per block and public Ethereum BC**

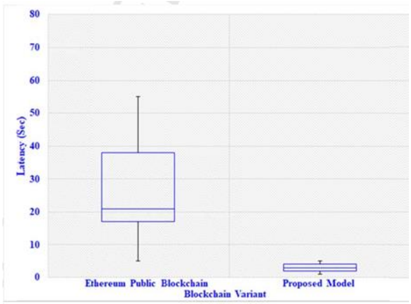

**Fig 6 : Results of latency in our proposed model**

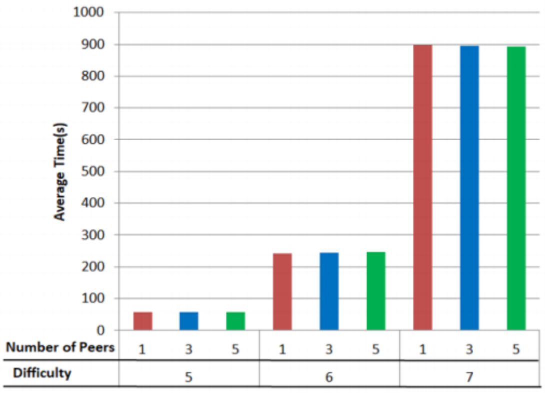

Fig 7: Test results for solo mining.

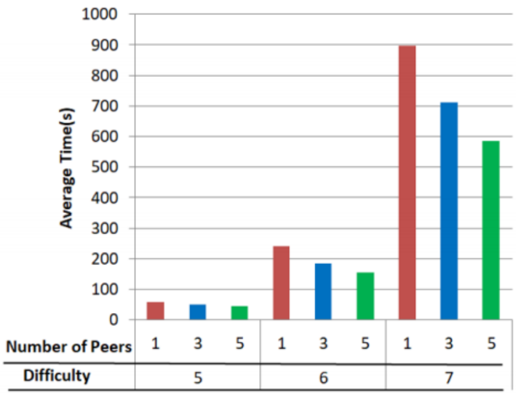

Fig 8: Test results for parallel mining.

For difficulty levels 1, 2, 3 and 4, there is no significant difference between solo mining and parallel mining. However, for difficulty levels 5, 6 and 7, there is improvement in parallel mining, and, as Figures 6 and 7 depict, this improvement becomes significant with the increase in the difficulty level and the number of miners. In solo mining, the average time depends only on the level of difficulty, but, in parallel mining, the average time depends on both the difficulty level and the number of peers. If the level of difficulty increases, the average time required increases. Again, if the number of peers increases, the average time decreases because the miners are working in parallel and no two miners perform the same work. Another important aspect to notice is that the average time taken for one peer in parallel mining is almost the same as that in solo mining regardless of the number of peers. This is because, when there is only one miner in parallel mining, no parallel work is taking place. The improvement reaches 34% for five miners compared to one miner. It should be noted that the results may vary based on the processing power allocated to the miners.

## 5. Conclusion

As IoT develops and thrives, more data will be generated on different devices in the context of smart cities. Achieving low latency, reducing bandwidth usage, and improving security and privacy and distribution are major challenges for smart cities. In this case, we are focusing on these issues by proposing hybrid architecture that is distributed to an intelligent city network in this paper. A sophisticated PoW scheme has been applied to our proposed model to ensure security and privacy and to avoid tampering with information by attackers. The results of the test analysis showed the effectiveness of our proposed model. There are still some limitations to our proposed model such as the decentralization of decision-making and enabling the process of temporary preservation at the edge.

**References**

1. Gazis, A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Communications Surveys & Tutorials, 19(1) (2017) 482-511
2. Vanus, et al., Monitoring of the daily living activities in smart home care. Human-centric Computing and Information Sciences 7(1) (2017) 30

A. Khan, and K. Salah, IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 82 (2018) 395-411

3. Merry, Population increase and the smart city. [Available online] https://www.ibm.com/blogs/internet- of-things/increased-population-smart-city/, Accessed date: 25 Feb 2018
4. Panetta, Smart Cities Look to the Future. [Available online] https://www.gartner.com/smarterwithgartner/smart-cities-look-to-the-future/, Accessed date: 25 Feb 2018
5. D. Lovelock, et al. Forecast: Blockchain Business Value, Worldwide, 2017-2030. [Available online] https://www.gartner.com/doc/3627117/forecast-blockchain-business-value-worldwide, Accessed date: 25 Feb 2018
6. Bera, S. Misra, and A. V. Vasilakos, Software-Defined Networking for Internet of Things: A Survey. IEEE Internet of Things Journal 4(6) (2017) 1994-2008
7. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. (2008)
8. Dwork, and M. Naor, M. Pricing via processing or combatting junk mail. In Annual International Cryptology Conference, Springer, Berlin, Heidelberg (1992) 139-147
9. Biryukov, D. Dinu, and D. Khovratovich, Argon2: new generation of memory-hard functions for password hashing and other applications. In Security and Privacy (EuroS&P), 2016 IEEE European Symposium on IEEE (2016) 292-302
10. Biryukov, and D. Khovratovich, Egalitarian Computing. In USENIX Security Symposium (2016) 315- 326
11. Sharma, S. Y. Moon, and J. H. Park, Block-VN: A distributed blockchain based vehicular network architecture in smart City. Journal of Information Processing Systems 13(1) (2017) 184-195
12. K. Sharma, et al. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. IEEE Communications Magazine 55(9) (2017) 78-85
13. K. Sharma, M. Y. Chen, and J. H. Park, A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access 6 (2018) 115-124
14. Bahga, and V. K. Madisetti, Blockchain platform for industrial Internet of Things. Journal of Software Engineering and Applications 9(10) (2016) 533-546
15. K. Christidis, and M. Devetsikiotis, Blockchains and smart contracts for the internet of things. IEEE Access 4 (2016) 2292-2303
16. Xia, et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access 5 (2017) 14757-14767
17. Li, et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2017) DOI: 10.1109/TII.2017.2786307
18. H. Kim, and E. A. Lee, Authentication and Authorization for the Internet of Things. IT Professional 19 (5) (2017) 27-33
19. Sung, et al. FS-OpenSecurity: a taxonomic modeling of security threats in SDN for future sustainable computing. Sustainability 8 (9) (2016): 919-944

20. Coelho, A. Larroche, and B. Colin, Itsuku: a Memory-Hardened Proof-of-Work Scheme. Doctoral dissertation, MINES ParisTech-PSL Research University (2017)
21. Biryukov, and D. Khovratovich, Egalitarian Computing. In USENIX Security Symposium (2016) 315- 326
22. Bitcoin Historical Data. [Available online] https://www.kaggle.com/mczielinski/bitcoin-historical-data, Accessed date: 25 Feb 2018