Future Generation Computer Systems 86 (2018) 650–655

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Blockchain based hybrid network architecture for the smart city

Pradip Kumar Sharma, Jong Hyuk Park *

Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech), Seoul 01811, Republic of Korea

HIGHLIGHTS

- We discuss the architectural challenges in the smart city network.
- We propose a novel hybrid architecture for the smart city network using SDN and blockchain techniques.
- We introduce the PoW scheme for a securely distributed smart city network.

ARTICLE INFO

Article history:
Received 26 February 2018
Received in revised form 19 April 2018
Accepted 19 April 2018
Available online 2 May 2018

Keywords:
Internet of Things
Smart city
Blockchain
Software Defined Networking

ABSTRACT

Recently, the concept of "Smart Cities" has developed considerably with the rise and development of the Internet of Things as new form of sustainable development. Smart cities are based on autonomous and distributed infrastructure that includes intelligent information processing and control systems heterogeneous network infrastructure, and ubiquitous sensing involving millions of information sources Due to the continued growth of data volume and number of connected IoT devices, however, issues such as high latency, bandwidth bottlenecks, security and privacy, and scalability arise in the current smart city network architecture. Designing an efficient, secure, and scalable distributed architecture by bringing computational and storage resources closer to endpoints is needed to address the limitations of today's smart city network. In this paper, we propose a novel hybrid network architecture for the smart city by leveraging the strength of emerging Software Defined Networking and blockchain technologies. To achieve efficiency and address the current limitations, our architecture is divided into two parts: core network and edge network. Through the design of a hybrid architecture, our proposed architecture inherits the strength of both centralized and distributed network architectures. We also propose a Proof-of-Work scheme in our model to ensure 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.

1. Introduction

The Internet of Things (IoT) envisions and offers a promising future for traditional Internet industries and societies, and the realization of smart cities is tightly bound to the IoT outlook. By deploying low-cost sensors and various types of smart objects to collect data in public infrastructure, a smart city increases operational efficiency, shares information with the public, and improves the quality of life, cost of living, and government services as well as the environment [1–3]. Nowadays, the biggest wave of urbanization around the world and people are moving toward cities because of economy growth and social transformation. Recently, the United Nations has predicted that 86% of developed countries and 64% of the developing countries will be urbanized by 2050 [4]. Gartner's report forecast that 30% of smart cities' healthcare applications will have robotics and smart machines, and 10% of smart cities will use streetlamps as the backbone for a network of smart cities by 2020 [5]. Such implies that billions of devices and systems will be integrated in the future, ranging from end-user devices to smart transportation, healthcare, industry, buildings, and environments. Thus, the de facto expectation for a network of smart cities is to analyze a huge volume of data generated by IoT devices, increase security and privacy, realize optimal use of network bandwidth to avoid congestion, support real-time applications, etc.

Recently, blockchain technology has attracted the attention of many stakeholders in many industries such as agriculture, cryptocurrency, supply chain, etc. IoT technology and blockchain technology are felt throughout our daily lives. The Gartner report predicts that $ 3.1 trillion in business value will be added by 2030 [6]. By taking advantage of the blockchain technique in the IoT network, we can offer new ways to automate business processes without the need for costly and complex centralized IT infrastructure.

* Corresponding author.
E-mail addresses: pradip@seoultech.ac.kr (P.K. Sharma), jhpark1@seoultech.ac.kr (J.H. Park).

https://doi.org/10.1016/j.future.2018.04.060
0167-739X/

This will help us build trust between devices and users, reduce the risk of falsification and cost, eliminate middlemen, and shorten the transaction settlement time. To simplify business processes, realize significant cost savings, and improve the user experience, blockchain-based IoT solutions are ideally suited. On the other hand, Software Defined Networking (SDN) is gaining prominence among technologies for its disruptive quality. As an emerging network architecture, it decouples control of the network from traditional hardware devices. SDN based solutions can be useful in meeting requirements such as scalability and seamless, efficient, and cost-effective deployment in the IoT network architecture [7].

Based on the analysis above, designing a new network architecture is needed to address the current limitations of the smart city network architecture by leveraging the strength of emerging SDN and blockchain technologies. In this paper, we propose a novel hybrid architecture for the smart city network using SDN and blockchain techniques to address these problems. We discuss the current architectural challenges that we are facing to realize a sustainable smart city network. We introduce the Argon2 based Proof-of-work (PoW) scheme into our proposed architecture for a securely distributed smart city network. We also explain the mining process of our proposed architecture at the core network. To evaluate the feasibility and performance overhead of the proposed model, experimental analysis is performed based on different parameters.

The rest of this paper is organized as follows: In Section 2, we discuss the architectural challenges in the smart city network, brief overview of Proof-of-Work and Argon2, and blockchain and IoT related works; in Section 3, we present our proposed model to address the current limitations of the smart city network; in Section 4, we evaluate the feasibility and performance of our proposed model based on different performance metrics; finally, we present the conclusions of our research in Section 5.

2. Preliminaries

2.1. Architectural challenges in the smart city

In the architectural design of the network of smart cities, the shift of the global population to cities is putting increasing pressure on urban areas in terms of scalability, latency, network bandwidth usage, data privacy, and security challenges. In a highly urbanized future, cities can offer the best quality of life through intelligent transportation, smart living, smart mobility, smart energy, and smart business models to finance everything. Here, we discuss some of the challenges faced by today's smart city network architecture and which we need to address for a sustainable smart city network

Low latency and high mobility: Due to the on-demand services simultaneously requested by multiple devices at different locations in the smart city, a set of stringent requirements – such as low latency and high mobility – is introduced. Addressing these constraints introduced by smart city applications requires an effective network architecture.

Structural scalability: Structural scalability is another challenge for the smart city network that we need to address when designing the architecture for a sustainable smart city network. This property allows a system to grow when needed without requiring significant changes in the network architecture.

Network bandwidth constraints: For smart city application scenarios, centralized architecture-based solutions are not appropriate due to network bandwidth limitations. In the centralized architecture, we have to send all the data collected by the IoT devices to the core network, which will require a huge amount of network bandwidth. To address the bandwidth constraint and reduce bandwidth usage, we need to design an architecture that allows data processing and analytics operations locally and sends only filtered data to the core network when needed.

Privacy and security: Due to the rapid increase in the number of devices connected to the Internet, our smart city network infrastructure gives rise to a number of security and privacy issues and challenges. As a paradigm of information and networks, the architecture of smart city networks should be able to protect information against destruction, modification, disclosure, unauthorized access, and cyberattacks.

Single points of failure: The smart city network architecture can have a large number of single points of failure due to the continued growth of heterogeneous networks, which in turn can degrade the services envisioned for the smart city. Providing a fault-tolerant network requires a tamper-proof network architecture for smart city applications.

2.2. Proof-of-Work and Argon2 overview

In cryptocurrencies and blockchain technology, PoW is the core part that enables large distributed public ledgers. Due to the difficulty in forging mathematical computations, it is very hard to quantify and manage trust. Initially, PoW was proposed to mitigate the spam problem and was later used in the Bitcoin protocol by Nakamoto [8]. In Bitcoin, PoW was often based on the iteration of double cryptographic functions SHA-256 until the result shows a special lucky number. PoW functions are easy to check but hard to compute [9].

As a memory hard function for password hashing and other applications, Argon2 has been selected as the winner of the Password Hashing Competition in July 2015 [10]. Biryukov, et al. [11] proposed a memory-hard PoW scheme using Merkle hash tree on top of the Argon2 hash chain. It consists of disk encryption and instantiation parameters for cryptocurrency applications. On an array, the PoW schema constructs a Merkle tree and pseudo-randomly selects a subset of leaves based on the root hash of the tree as proof of computation. In the Argon2 chain, it is very hard for attackers to demonstrate knowledge of the proper Argon2 chain elements with their correct paths in the Merkle tree. Thus, if some attackers attempt to cheat and store only a fraction of the Argon2 chain, they are very likely to be caught.

2.3. Blockchain and IoT related works

In our previous work, we proposed a blockchain based distributed vehicular network architecture in the smart city [12]. Here, we introduce the idea of building a secure and reliable distributed architecture for the transport management system. We also propose the DistBlockNet model, a distributed mesh network architecture for IoT using SDN and blockchain [13]. In this model, we also propose the flow rule update scheme to update securely and verify the flow rule tables in the mesh network. Later, we extended our work and proposed a blockchain based distributed cloud architecture enabled with SDN fog nodes for a scalable IoT network [14]. Bahga, et al. [15] proposed a decentralized platform for Industrial IoT (IIoT) using the blockchain technique to remove the trusted intermediary and build a peer-to-peer network. Christidis, et al. [16] reviewed the applications of blockchains and smart contracts for IoT. Trustless medical data sharing among cloud service providers using blockchain was proposed by Xia, et al. [17]. It provides shared medical data in cloud storage and enables auditing, data provenance, and control for shared medical data. Li, et al. [18] proposed a secure energy trading system for IIoT.

To the best of our knowledge, research work on smart city and blockchain is very limited in literature. Majority of the work focuses on using blockchain technology to benefit IoT either in a very general way or specific to a problem. Designing a new architecture platform specific to the smart city network is needed, taking into account all aspects of current and future challenges.

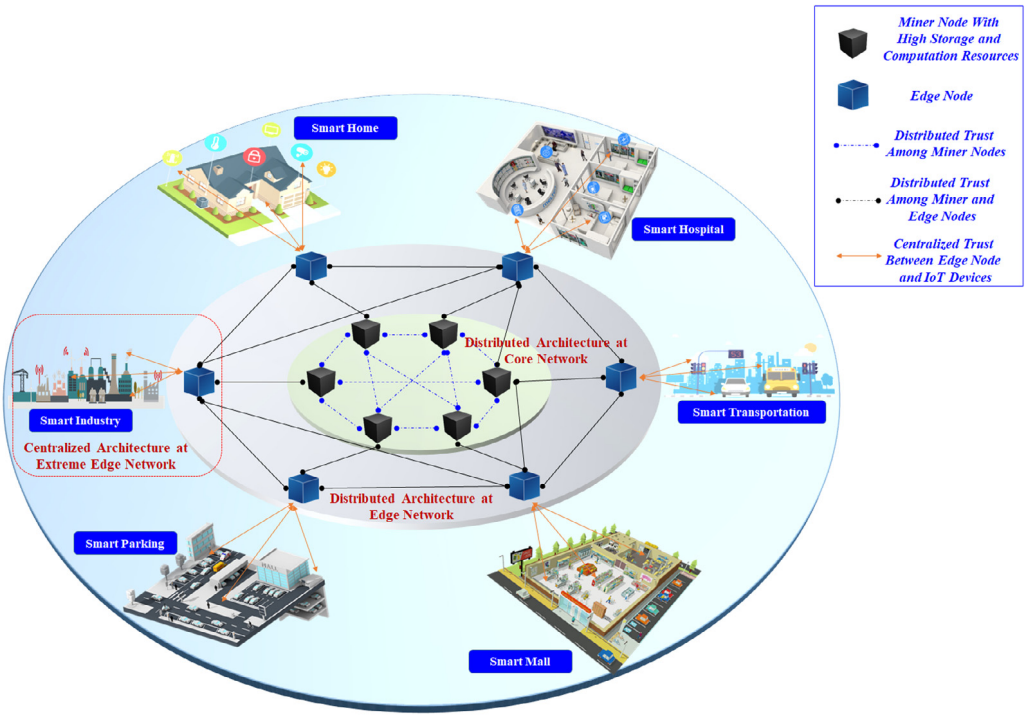

Fig. 1. Proposed hybrid network architecture for a sustainable smart city network.

3. Proposed smart city architecture

The smart city has become an emerging paradigm with the growth and advancement of IoT. It is very important to consider the downstream processing of the network when designing the architecture of a smart city network. An example is a smart building wherein a sensor is connected to a lighting fixture that can be part of a larger building application. The smart building can also be part of a network of smart cities. In this case, we must consider the fact that the data is transmitted not only locally but also to a larger network of buildings and finally to a larger network of cities. The design of a new smart city network architecture is required to address the limitations of current network architectures as discussed in previous sections. In this section, we propose a novel blockchain-based hybrid network architecture for the smart city and discuss the detailed specification of the proposed model.

3.1. Architecture design overview

To achieve efficiency and scalability in trust management for the IoT network, Kim, et al. [19] introduced the concept of globally distributed and locally centralized trust management. They envisioned the authentication and authorization infrastructure for the IoT to be centralized locally and distributed globally. In our previous work, we proposed DistBlockNet, a blockchain-based distributed secure SDN architecture for the IoT network [13]. Taking advantage of the strength of the architectures proposed by Kim, et al. [19] and Sharma, et al. [13], we propose a hybrid architecture for a scalable smart city network with blockchain and Software Defined Networking (SDN) techniques to overcome the limitations of the current smart city network architectures.

Fig. 1 shows the overall proposed hybrid architecture of the scalable smart city network. In the proposed model, the smart city network is divided into two different groups – the core network and the edge network – using the blockchain technique. The core network consists of miner nodes with high computation and storage resources, whereas the edge node has limited storage and computation power. Miner nodes will be responsible for creating blocks and verifying proof-of-work. Each node is enabled with SDN controller to achieve high agility and security, reduce hardware management cost, and realize ease of deployment in the smart city network infrastructure. Here, we leveraged the security strength of the FS-OpenSecurity SDN model from our previous work [20]. In our proposed architecture, each edge node acts as a centralized server for specific public infrastructure to provide essential services and achieve localizations. It stores the access policies and credentials of its locally registered entities in its database and helps achieve low latency and reduce network bandwidth. The distributed nature of the proposed model can make the whole system more resilient and limit the impact of attacks even when the node is compromised. In other words, if the edge node is compromised, the resulting effect must be limited to the local area.

3.2. Proposed model workflow

In the smart city, IoT devices generate a large volume of data and require real-time processing. In our proposed model, edge nodes offer real-time processing with low latency and network bandwidth usages and get deployed at the edge of the network. The edge node has limited storage and computation power and preprocesses the raw data uploaded by the end devices to filter the data and obtain useful information. Once data is pre-processed, the edge node transfers the pre-processed encrypted data to the core network of the smart city if necessary. The miner node in the core network will further analyze the pre-processed data, make decisions, validate and verify the PoW, and generate blocks. To ensure the integrity of data stored in the core network, we use digital signature and store hashes in blockchain. These hashes in blockchain are immutable, serving as evidence to prove the integrity of the data. Fig. 2 demonstrates the workflow of our proposed model, where we used the Argon2 based hashing scheme.

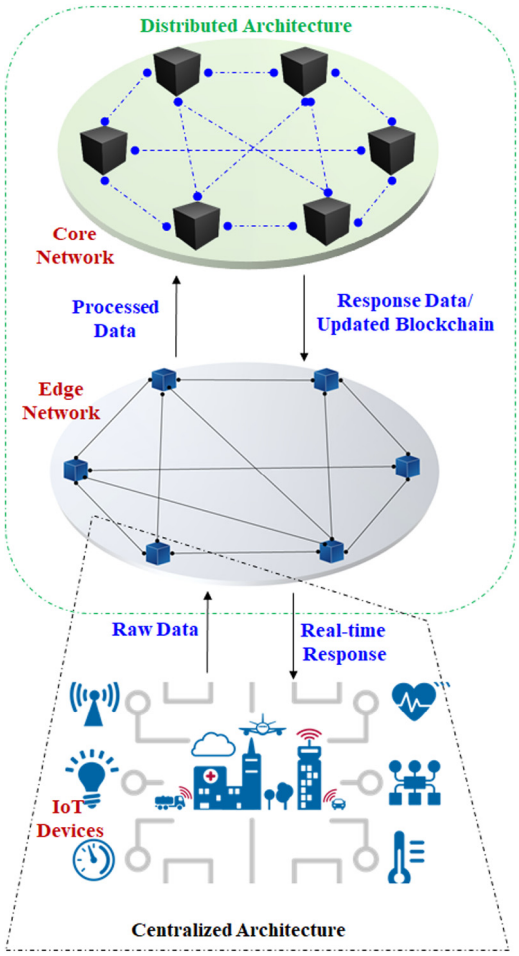

Fig. 2. Hybrid network architecture workflow.

3.3. PoW scheme algorithm

In today's of cryptocurrencies and blockchains, PoW is the core component. By resolving the difficulty of quantifying and managing trust with hard-to-forge mathematical computations, these techniques enable large public distributed ledgers. In our proposed model, we use a memory-hardened PoW scheme called "Itsuku PoW", proposed by Coelho. et al. [21]. The Itsuku PoW scheme is inspired by MTP-Argon2 [22]. It fixes issues such as raw recomputation attack, memory saving, pseudo-random array, parallel searches, and hash composability attacks by adding new operations and modifying the MTP-Argon2 parameters to improve memory hardness. Table 1 shows the pseudo-code of the Itsuku PoW scheme algorithm. The scheme takes as input challenge I, and difficulty d, and the output of the search algorithm is $(\mathrm{N}, \mathbb{I}, \mathbb{L}, \mathbb{Z})$, where T is the number of elements in array, L is the length of one search, H_S is the variable-size hash function, $\mathbb{I}$ is the indexes of selected leaves, $\mathbb{L}$ is the selected leaves, and $\mathbb{Z}$ is the collective Merkle tree proof of both selected leaves and their antecedents, if any. A detailed description and the complexity analysis of the Itsuku PoW scheme are given in [21].

3.4. Mining process at the core network

After receiving a transaction at the core node from the edge node, the mining process is initiated. Due to the limitation of resources at the edge node, we perform the mining process at the core network in our proposed model. The mining process includes the following steps:

Step 1: Whenever the edge node receives a new transaction request for the services required by the IoT device/user, it sends a transaction request to each miner in the core network.

Step 2: Upon receiving the transaction request, the miner node checks and verifies if the transaction is modified or not and whether the transaction exists in blockchain or not. If the transaction is not modified, and it does not exist in blockchain, the miner node moves to Step 3. Otherwise, the miner node aborts the mining process and broadcasts the report in the core network.

Step 3: In this step, the miner node retrieves 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 iteratively hashing the information, which includes the previous ID, created block ID, date and time stamp, verified transaction, and digital signature of the miner using the Itsuku PoW algorithm discussed above.

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

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

4. Experimental analysis

In this section, we simulate our proposed model to assess the feasibility of our proposed architecture. Here, we discuss the experimental setup and evaluation results based on various parameter metrics. All the experiments are simulated on Intel Core i5 CPU 3.40 GHz with 16 GB memory running on Windows 10.

We simulated our proposed model on top of a private Ethereum blockchain network. 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.

4.1. Performance analysis of the core network architecture

PoW is a crucial module of blockchain technology. Intrinsically, the task based on PoW must be difficult to solve and trivial to verify. This often comes down to a random process of trying to find a solution to a puzzle like a hash collision. Here, we observed the difficulty and hashing rate obtained in our proposed scheme. Fig. 3 shows the difficulty and hash rate of our proposed scheme. It shows that the hash rate is continuously adjusted according to the difficulty level in the proposed scheme.

We also observed the result on the number of transactions per second for the variable block size in our proposed model and compared it with another system. Fig. 4 shows how the size of a block affects the number of transactions per second in our proposed model. The data for our simulations are based on actual transactions from part of the Bitcoin blockchain [23]. The result shows that, compared to the other system, our proposed model achieves better performance.

We also observed that the average block times behave in relation to the retargeting interval and compared to the desired output (i.e. 10 min). Fig. 5 shows the results of the average block time behavior with a retargeting interval. We can see that even that

Table 1
PoW scheme algorithm.

	Input: *input challenge* (I), *difficulty* (d), *independent segment* (P), and *segment length* (l)
	Output: (N, $\mathbb{I}$, $\mathbb{L}$, $\mathbb{Z}$)
	Begin
Step 1	**Build** challenge-dependent memory X_I [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 $Y_0 = H_S(N \|\varphi\| \mathrm{I})$
Step 5	**For** 1 1 $\leq j \leq L$ **Do**
	$i_{j-1} = Y_{j-1} mod T$
	$Y_j = H_S\left(Y_{j-1} \left\| X_I\left[i_{j-1}\right] \bigoplus I\right.\right)$
Step 6	Back sweep over intermediates hashes in reverse order $\vartheta = H_S\left(Y_L \| \ldots \| Y_{1-Lmod2} \oplus I\right)$
Step 7	**If** ϑ has d binary leading zeros **Then**
Step 8	**return** (N, $\mathbb{I}$, $\mathbb{L}$, $\mathbb{Z}$)
Step 9	**Goto** Step 3
	End

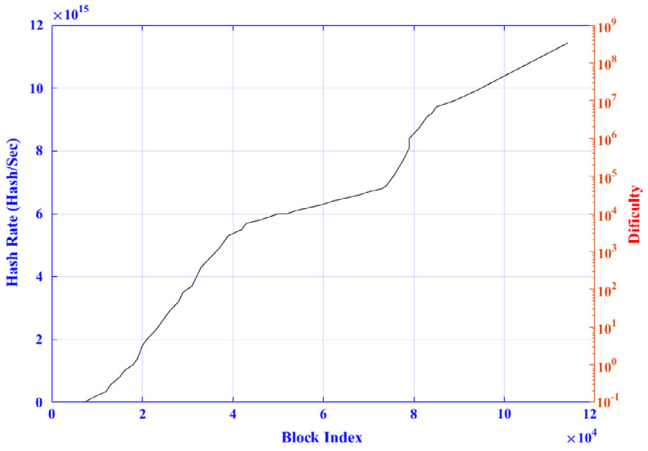

Fig. 3. Hash rate vs. Difficulty.

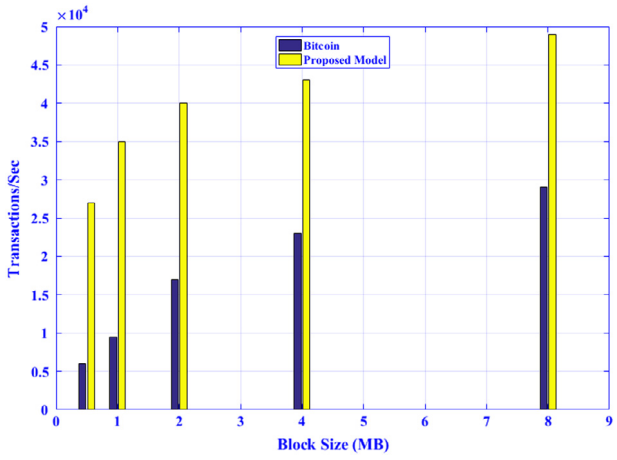

Fig. 4. Block size vs. Transactions/Sec.

fluctuates considerably, whereas but our proposed model seems more robust and closer to the desired average block time. Initially, the wild fluctuations seem to be due to the major changes in the hash rate.

4.2. Evaluation of the performance overhead of the proposed model

To evaluate the performance overhead of our proposed model, we observed the latency and throughput in our experimental analysis. Here, we consider latency to be the total time taken from receipt of the event by the edge node to the time it sends the desired response, transaction hash, generating block, etc. Here, we wrote test scripts to trigger events at the edge node as soon as it receives the response of the previous event. Fig. 6 shows the results of latency observation in our proposed model compared with the public Ethereum blockchain. The mining task is deliberately designed to be difficult to compute, and the duration for a block to be mined depends on the complexity of the mining task. As shown in Fig. 6, the median latency achieved in our simulation using the public Ethereum blockchain is 21 s; in our proposed model, however, we achieved a median latency of 3.9 s, which is suitable for deployment in many smart city applications. Since we inherited the SDN controller security features from our previous work [14,20], we skipped further security analysis of the SDN controller here.

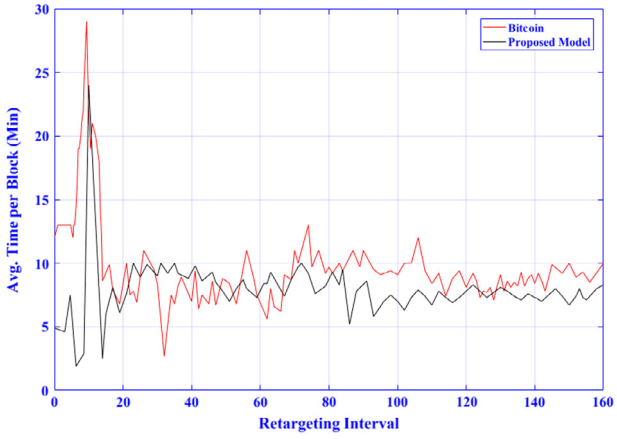

Fig. 5. Average time per block.

5. Conclusions

With IoT advancing and flourishing, a lot of data will be produced by different devices in the context of smart cities. Achieving low latency, reducing bandwidth usage, and improving security and privacy and scalability are the major challenges of smart cities. In this context, we have focused on these limitations by proposing a hybrid distributed architecture for a sustainable smart

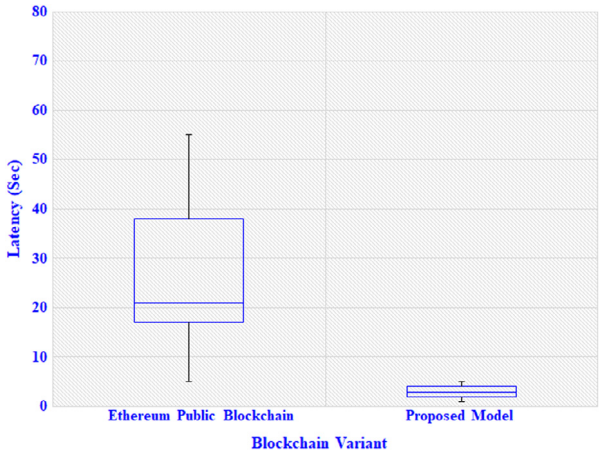

Fig. 6. Results of latency in our proposed model and public Ethereum blockchain.

city network in this paper. A memory-hardened PoW scheme was used in our proposed model to ensure security and privacy and avoid tampering of information by attackers. The result of the experimental analysis showed the effectiveness of our proposed model. There are still some limitations in our proposed model such as efficient deployment of edge nodes and enabling of caching technique at the edge nodes, so we will carry out related future work.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No 2016R1A2B4011069).

References

[1] V. Gazis, A survey of standards for machine-to-machine and the internet of things, IEEE Commun. Surv. Tutor. 19 (1) (2017) 482–511.
[2] J. Vanus, et al., Monitoring of the daily living activities in smart home care, Human-Centric Comput. Inf. Sci. 7 (1) (2017) 30.
[3] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[4] H. Merry, Population increase and the smart city. [Available online] https://www.ibm.com/blogs/internet-of-things/increased-population-smart-city/. (Accessed 25 February 2018).
[5] K. Panetta, Smart cities look to the future. [Available online] https://www.gartner.com/smarterwithgartner/smart-cities-look-to-the-future/. (Accessed 25 February 2018).
[6] J.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 February 2018).
[7] S. Bera, S. Misra, A.V. Vasilakos, Software-defined networking for internet of things: A survey, IEEE Internet Things J. 4 (6) (2017) 1994–2008.
[8] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.
[9] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 1992 pp. 139–147.
[10] A. Biryukov, D. Dinu, 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, pp. 292–302.
[11] A. Biryukov, D. Khovratovich, Egalitarian computing, in: USENIX Security Symposium, 2016, pp. 315–326.
[12] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: A distributed blockchain based vehicular network architecture in smart City, J. Inf. Process. Syst. 13 (1) (2017) 184–195.
[13] P.K. Sharma, et al., DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.
[14] P.K. Sharma, M.Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2018) 115–124.
[15] A. Bahga, V.K. Madisetti, Blockchain platform for industrial internet of things, J. Softw. Eng. Appl. 9 (10) (2016) 533–546.
[16] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[17] Q. Xia, et al., MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[18] Z. Li, et al., Consortium blockchain for secure energy trading in industrial internet of things, IEEE Trans. Ind. Inf. (2017). http://dx.doi.org/10.1109/TII.2017.2786307.
[19] H. Kim, E.A. Lee, Authentication and authorization for the internet of things, IT Professional 19 (5) (2017) 27–33.
[20] Y. Sung, et al., FS-OpenSecurity: a taxonomic modeling of security threats in SDN for future sustainable computing, Sustainability 8 (9) (2016) 919–944.
[21] F. Coelho, A. Larroche, B. Colin, Itsuku: A Memory-Hardened Proof-of-Work Scheme (Doctoral dissertation), MINES ParisTech-PSL Research University, 2017.
[22] A. Biryukov, D. Khovratovich, Egalitarian computing, in: USENIX Security Symposium, 2016, pp. 315–326.
[23] Bitcoin Historical Data. [Available online] https://www.kaggle.com/mczielinski/bitcoin-historical-data. Accessed 25 February 2018.

Mr. Pradip Kumar Sharma is a Ph.D. scholar at the Seoul National University of Science and Technology. He works in the Ubiquitous Computing & Security Research Group under the supervision of Prof. Jong Hyuk Park. Prior to beginning the Ph.D. program, he worked as a software engineer at MAQ Software, India. He worked on a variety of projects, proficient in building large-scale complex data warehouses, OLAP models and reporting solutions that meet business objectives and align IT with business. He received his Master's degree in Computer Science from the Thapar University, in 2014, India. His current research interests are focused on the areas of ubiquitous computing and security, cloud computing, SDN, SNS, and IoT. He is also reviewer of Journal of Supercomputing (JoS), IEEE System Journal, IEEE Transaction of Industrial Informatics, IEEE Internet of Things Journal, IEEE Consumer Electronics Magazine, and IEEE Communication Magazine.

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences — MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, The Journal of Information Processing Systems (JIPS) by KIPS, and Journal of Convergence (JoC) by KIPS CSWRG. He is Associate Editor/Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.