Ethereum Based Storage Aware Mining for Permissioned Blockchain Network

Ikechi Saviour Igboanusi *IEEE Student Member*, Allwinnaldo, Revin Naufal Alief, Muhammad Rasyid Redha Ansori, Jae-Min Lee *IEEE Member*, Dong-Seong Kim *IEEE Senior Member*
Networked System Laboratory, IT Convergence Engineering,
Kumoh National Institute of Technology,Gumi, South Korea.
ikechisaviour@gmail.com, winnaldo@outlook.com, revinnaufal, rasyidred, ljmpaul, dskim(@kumoh.ac.kr)

***Abstract*—This work aims to reduce transaction time by integrating the mining process with the sending of transactions to reduce overall transaction time. This work also decreased the overhead of mining in a private network, by reducing the production of empty blocks in the network which saves energy, storage space, network bandwidth and computational complexity. We proposed an Auto Integrated Mining (AIM) algorithm which starts the mining process only when there is at least one pending transaction in the network, and stops mining as soon as the pending transactions are mined. The results show that the AIM algorithm reduced the number of mined blocks in a 12 hour period by producing only 24% of the original number of blocks. The proposed algorithm is also able to reduce the storage used to save chaindata by 16%. The experiment shows that the mining latency of AIM varied between 200-650*ms* when the number of pending transactions was between 1-1,000, and had a latency between 350-1,350*ms* when there were 1,000-10,000 pending transactions in the private blockchain network.**

***Index Terms*—Auto integrated mining (AIM), Blockchain, low latency, real time, storage efficiency, wireless network.**

I. Introduction

The growing connectivity of things has disrupted many areas of the society from security to financial transactions to communication etc [1], [2]. This level of disruption is further amplified by the Internet of Things (IoT). For new network technologies to penetrate into all kinds of devices, its energy, security, and computational (e.g. storage, and processing) features should be efficient. Blockchain inherently has security as its feature, but energy and computation requirements limits its adoptability.

The energy needed for mining is significant especially for a Proof of Work (PoW) consensus. Although it is one of the most secure and popular consensus algorithms, its energy requirement is making it less attractive, hence making other consensus algorithms with less decentralization to be considered in both permissioned and permissionless blockchain networks. But energy consumption is not the only problem associated with mining, it is also computationally intensive. The computation requirement during the mining process can overwhelm many computers. Also, if a network has low transaction traffic, the continuous mining operation is just a waste of energy, computation, bandwidth, and storage space by mining empty blocks. The downloading of empty blocks affects network bandwidth negatively. These limitations further make scalability another hindrance to blockchain adoption.

Authors in [3] identified decentralized systems' biggest issue to be scalability causing its lag in adoption compared to centralized systems. Their work proposed a theoretical scalable blockchain technology solution. An InterPlanetary File System (IPFS) distributed storage system is used to increase throughput and to avoid the storing liability. By using the dual-blockchain method, the reference of the main block is put in place of the original block, which serves as the main feature of the blockchain. The result shows a 25.8 time increase in throughput and about 1685 times decrease in ledger size in comparison with the Bitcoin Core. Energy consumption is one of the biggest problems associated with blockchain mining especially in PoW consensus algorithms. The authors in [4] considered how to reduce energy consumption in mining of cryptocurrencies. They stated that energy consumption for blockchain mining should be deemed as an opportunity for renewable energy sources. However, energy efficiency is important, not minding whether the source of energy is renewable or not. In article [5], the authors used PoW with a static low difficulty setting to achieve low transaction time. In their paper, they proposed an artificial intelligence based face recognition. They used edge computing to reduce latency which achieved 33-39 milliseconds latency.

Summarized below are the main contributions of this paper: This letter proposed an integrated mining technique, which combines the sending process of transaction with mining, to improve latency. An Auto Integrated Mining (AIM) algorithm was proposed to save energy, computation, storage space and network bandwidth. Also, there is real world implementation of the proposed AIM model.

The remaining parts of this work are organized as follows. Section II presents the blockchain preliminaries and problem formulation. The proposed AIM model is presented in Section III. After that, the experimental results and analysis of the proposed model is presented in Section IV. Finally, the conclusion is presented in Section V.

II. Preliminaries and Problem Formulation

A. Preliminaries

Blockchain transactions follow five steps of processes to complete a transaction [6] as shown in Fig. 1. The five steps are as follows:

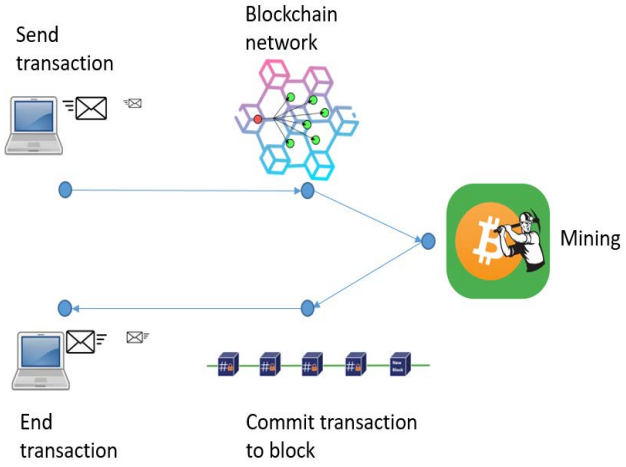

Fig. 1. The blockchain transaction process.

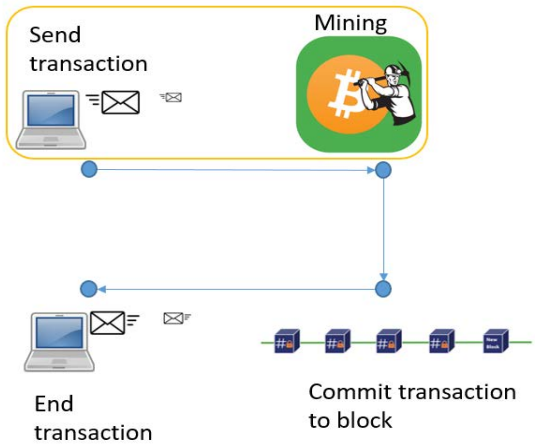

Fig. 2. The proposed AIM blockchain transaction process.

1 Send transaction: The sender initiates the transaction request to send a certain information to the receiver.
2 Blockchain network broadcast: After sending a transaction, it is broadcast so that all available miners in the network has the ability to mine this pending transaction.
3 Mining: Available miners compete to mine pending transactions by completing the requirement of the consensus algorithm and including the transaction in a new block.
4 Committing transaction to block: Mined transactions are included into the blockchain ledger in the last block on the blockchain network. The block is downloaded by all capable nodes in the network.
5 End transaction: The sent transaction reflects in the receiver account and the transaction is ended.

B. Problem formulation

The current blockchain sends transactions and broadcasts it into the network before it is mined. Some amount of delay is introduced between the time of sending transaction, broadcasting and mining by one of the miners. The problem of mining time and how it affects a network speed has also been explored by *Shisheng et al* in [7]. The proposed integrated model combines the transaction sending and mining process as shown in Fig. 2, thereby eliminating the delays associated with broadcasting the transactions. To the best of our knowledge there is no previous work that has explored an integrated mining technique. We have explored the concept of auto mining in our previous work [8] However there was no explanation on the principle of its workings and analysis of its results.

Another limitation of the current blockchain network is that the miners mine new blocks continuously in the network, whether or not there are available pending transactions. This creates unnecessary computational overhead and energy consumption during such mining. Also, the bandwidth of the network is used to transmit information of mined blocks to all the nodes in the network. Even though the mined blocks are empty and consume minimal storage, over an extended period of time they will occupy significant storage space. The

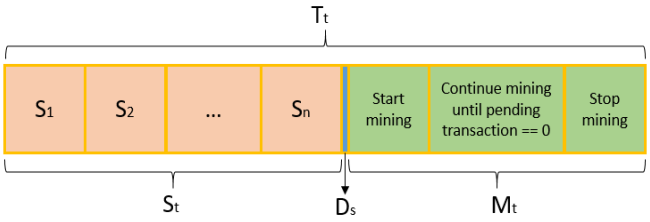

Fig. 3. The time properties of AIM blockchain transactions.

proposed AIM architecture starts the mining once a transaction is initiated and stops the mining as soon as the transaction has been successfully mined as illustrated in Fig. 3. Thereby preventing the use of unnecessary bandwidth and storage.

III. System Model

This section presents the assumptions and formulation of the proposed AIM architecture. Some simple mathematical expressions are also used to illustrate the features of this proposed model.

A. Assumptions

The proposed model can only work efficiently when these assumptions below are met.

- **Assumption 1: All the nodes in the network can mine.** Private blockchain networks for offices, institutions, and companies are usually dominated by personal computers and server computers which are very capable to handle mining operations. However in some cases, less capable computers are used for IoT operations like surveillance of the environment and actuation in the industries. We considered Jetson Nano to be the smallest device to participate in our network, which was able to handle the mining operation in the network.
- **Assumption 2: The network is not constantly having a transaction to mine.** A private network is expected to have periods of frequent transactions and periods of little or no transactions. Transactions will be frequent when

there are many active users of the network, like during the working hours. However, at night there may be limited transaction processing in the network.

- **Assumption 3: The mining nodes are the only initiators of transactions.** It is assumed that accounts like smart contract do not make transactions on their own, except prompted by one of the nodes, which will mine any transaction created with the prompt.
- **Assumption 4: One miner is sufficient to mine transactions.** The consensus algorithm can determine if a single miner in a network with multiple miners can mine transactions successfully.

B. Proposed Model

The system model of our work compressed three entities (the sender, the node, and the miner) into one entity, referred to as node throughout in this paper.

1) Integrating sending and mining process: The motive of integrating the process of sending and mining transaction is to minimize time spent before a transaction is included into the blockchain. Transaction time (T_t) is expressed as:

$$T_t = \sum_{i=1}^{n} S_i + D_S + D_{N1} + B_t + D_{N2} + \sum_{j=1}^{m} M_i, \quad (1)$$

where S_i is the time for sending a single transaction. B_t is the time to broadcast the transaction into the blockchain network. M_i is the time for mining an individual transaction. T_t is the total time spent between sending and mining a transaction. D_s is the system delay, and D_{N1} and D_{N2} are network delays before and after mining respectively.

$$S_t = \sum_{i=1}^{n} S_i, \quad (2)$$

S_t is the time spent to send multiple transactions.

$$M_t = \sum_{i=1}^{n} M_i, \quad (3)$$

M_t is the total time of mining all pending transactions. For simplicity let D_{N1} and D_{N2} be equal.

$$2D_N = D_{N1} + D_{N2}, \quad (4)$$

Substituting equations (2), (3), (4) into (1) we have:

$$T_t = S_t + D_s + B_t + 2D_N + M_t. \quad (5)$$

By integrating the sending and mining process request in a single code, B_t and network delays are eliminated. Hence equation (5) becomes:

$$T_t = S_t + D_s + M_t. \quad (6)$$

S_t depends on the number of transactions sent and the capacity of the device used. Hence the delay it introduces is external to the blockchain network. The actual time a transaction spends on the blockchain network in our proposed model are D_s and M_t.

2) Auto mining process: Blockchain networks have at least one miner working at each point in time to mine all transactions broadcasted into the network. However, this work proposed an auto mining model by including an instruction to start mining immediately after the send transaction instruction in the code. The code ends with a stop mining instruction once the last pending transaction is mined. Algorithm 1 presents the pseudo code of the mining process. The AIM implementation code is developed using JavaScript and can be accessed on Networked Systems Lab website in [9].

Algorithm 1: Auto Mining process

```
Initiate a send transaction from one node to another
if check pending transaction > 0 then
    start miner
end
else
    check pending transaction == 0
    stop miner
end
```

TABLE I
SPECIFICATION OF USED DEVICE.

Item	Specification
Computer	Mac Air 2020
Memory	16Gb RAM
Storage	1TB
Processor	M1 (8 core CPU and 8 Core GPU)
Operating System	macOS Big Sur

3) Implementation: This work implemented the AIM system model on an Ethereum private network running on a PoW consensus algorithm. It was run on several machines to test its versatility. Trials were done in devices including Macbook, Windows 10 laptop, and Jetson Nano board, and all gave successful results. The results used for analysis in this letter came from a Macbook Air with specifications as shown in Table I.

IV. Experiment Results and analysis

Practical implementation results from real world tests have been generated. In the data gathering, each parameter setting is iterated ten times, and the average is calculated as given in equation (7) used for this analysis.

$$Y_i = \frac{1}{10} \sum_{J=1}^{10} X_i. \quad (7)$$

After setting the number of transactions to be performed, we recorded the number of blocks mined during the transaction, time to send transaction (S_t), mining time (M_t), total transaction time (T_t), and the system delay (D_s). D_s is calculated by rearranging equation (6) to have $D_s = T_t - (M_t + S_t)$. We calculated the time for a single transaction for all used iterations. The iteration was carried out in four stages which are: single digit number of sent transactions, in tense, in hundreds, and in thousands. Table II shows the time cost of

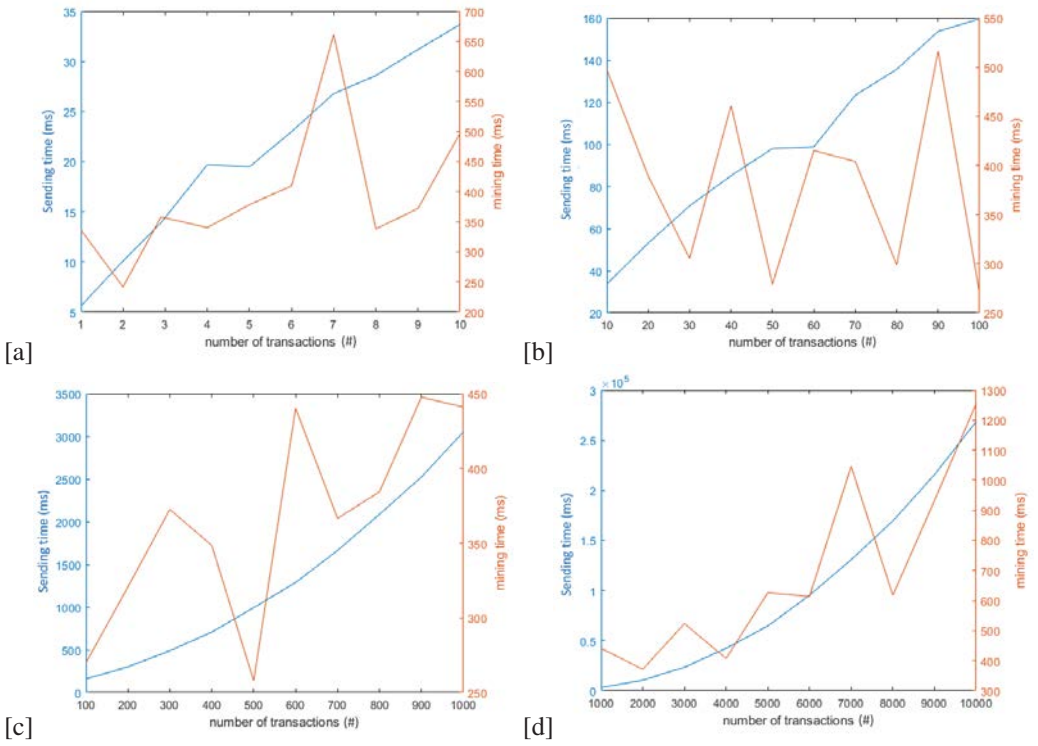

Fig. 4. The comparison of sending time ($S_t ms$) and mining time ($M_t ms$) against number of transactions (N).
[a] for N ranging from 1 to 10, [b] for N ranging from 10 to 100, [c] for N ranging from 100 to 1000, and [d] for N ranging from 1,000 to 10,000.

each transaction. The single transaction time in table II follows a gradient descent pattern as given by authors in [10].

A. System delay (D_s)

The elimination of the broadcast phase has made the time delay between S_t and the M_t process to be minimized. D_s for all experiments below 1000 transactions varies between 5.4*ms* and 15.4*ms*. From 1,000-10,000 transactions the delay rose gradually from 13.8-105.2*ms*. All experiments were conducted 10 times and the average is used for this analysis (See D_t in Table II).

B. Sending time (S_t)

In other works, there is no distinction of S_t from T_t, everything is usually measured as blockchain transaction time, whereas S_t is sending time in the device. Our experiment t shows that S_t is significant in a transaction. The graphs in Fig 4 (a-d) shows how S_t (Sending time) increase with increase in number of transactions (N). In Table II, the average time cost of a single sending $S_{\bar{t}}$ is calculated. It is seen that $S_{\bar{t}}$ decrease as N increased from 1 to 200 transactions with least $S_{\bar{t}}$ of 1.5*ms* at 200 transactions. As the number of transaction increase after N = 200, $S_{\bar{t}}$ increased.

C. Mining time (M_t)

The mining operation mines all the pending transactions in the network. All sent transactions were mined and the average mining time of ten trials of each number of transactions is shown in Fig. 4 (a-d). Mining transactions less than 1,000 transactions have a fluctuating value between 250*ms* and 660*ms*. However the M_t increased gradually in a zig-zag manner between 400*ms* and 1,250*ms* for N between 1,000 and 10,000. The mining time for a single transaction $M_{\bar{t}}$ decreased continuously with increase in N.

D. Transaction time (T_t)

The transaction time T_t is the total time spent from start of sending to end of mining operation. Table II shows how sending mining time influences T_t with a smaller number of N, the M_t influenced T_t significantly until an equilibrium point is reached at about 250 N, where both S_t M_t have approximately the same influence. If N is more than 250 transactions, the S_t gradually increases its influence on T_t. The value of $T_{\bar{t}}$ has a downward trend until N is about 500 and starts an upward trend.

E. Energy and computational complexity

The energy consumption and computational complexity is directly proportional to the mining process, which can be ascertained by measuring the number of generated blocks. In the course of running the experiment, 270 operations were initialized with a total number transaction (N) of 599,950. A single operation has between 1 and 10,000 transactions ($1 \leq N \leq 10,000$). The operations generated 513 blocks. However, without using AIM model, the network generated 2,138 additional blocks within 12 hours of mining operation,

TABLE II
TIME OF TRANSACTIONS

No of transactions (N)	1	10	100	1000	10000
No of blocks generated	1	1	1	1.1	1.8
S_t (*ms*)	5.6	33.7	159.5	3050.9	268485
M_t (*ms*)	336.3	497.4	269.9	440.9	1254.9
T_t (*ms*)	349.3	537.3	436.1	3505.6	269845.9
D_s (*ms*)	7.4	6.2	6.7	13.8	105.2
$S_{\bar{t}} = S_t/N$ (*ms*)	5.6	3.4	1.6	3.1	26.8
$M_{\bar{t}} = M_t/N$ (*ms*)	336.3	49.7	2.7	0.4	0.1
$T_{\bar{t}} = T_t/N$ (*ms*)	349.3	53.73	4.4	3.5	27.0

with no transaction sent for mining, having over 300% block generation with no extra pending transaction ($N = 0$) mined. The genesis block is set to have low difficulty for fast mining operation.

F. Storage and bandwidth

All the transactions using the AIM model occupied a total of 80.1*Mb* in storage. Without the proposed AIM, the storage occupied an additional 12.8*Mb* by mining empty blocks that had no transactions (N = 0) for 12 hours. Since the size of network storage is directly proportional to the bandwidth requirement to download a full node, the proposed AIM reduced bandwidth requirement, at the same rate it reduced storage.

G. Consensus speed and Scalability

After each transaction is mined it is included in the block and can be downloaded by other nodes in the blockchain network. Hence, the proposed model has no effect on consensus speed. Since AIM reduced storage and bandwidth requirement without negatively affecting consensus, AIM model can be inferred as scalable with increase in network size.

V. CONCLUSION

This work presented AIM, an automatic integrated mining for private blockchain networks. The major concept is that the send transaction request is combined with mining instruction, which reduces storage, bandwidth, energy and computational complexity. The approach eliminated broadcast of transactions, hence making delay between sending and mining transaction very minimal. The practicability of this model has been demonstrated by implementing it on a real world private blockchain network.

In the future, improvements will be made on the model by proposing solutions that work for all consensus algorithms. Also future auto mining solutions should be capable of not requiring every node to be a miner.

VI. ACKNOWLEDGMENT

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(MEST)(2018R1A6A1A03024003), and the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program(IITP-2022-2020-0-01612) supervised by the IITP(Institute for Information & communications Technology Planning Evaluation).

REFERENCES

[1] A. Rovira-Sugranes and A. Razi, "Optimizing the age of information for blockchain technology with applications to iot sensors," *IEEE Communications Letters*, vol. 24, no. 1, pp. 183–187, 2020.

[2] T. Kwon, S. W. Choi, and Y.-H. Shin, "A comprehensive design framework for network-wide cost reduction in random access-based wireless iot networks," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1576–1580, 2019.

[3] M. S. H. Sohan, M. Mahmud, M. A. B. Sikder, F. S. Hossain, and M. R. Hasan, "Increasing throughput and reducing storage bloating problem using ipfs and dual-blockchain method," in *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 2021, pp. 732–736.

[4] D. Rusovs, S. Jaundālders, and P. Stanka, "Blockchain mining of cryptocurrencies as challenge and opportunity for renewable energy," in *2018 IEEE 59th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, 2018, pp. 1–5.

[5] K. P. Dirgantoro, J. M. Lee, and D.-S. Kim, "Generative adversarial networks based on edge computing with blockchain architecture for security system," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2020, pp. 039–042.

[6] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/8/2575

[7] S. Hu, Y. Pei, and Y.-C. Liang, "Sensing-mining-access tradeoff in blockchain-enabled dynamic spectrum access," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 820–824, 2021.

[8] I. S. Igboanusi, K. P. Dirgantoro, J.-M. Lee, and D.-S. Kim, "Blockchain side implementation of pure wallet (pw): An offline transaction architecture," *ICT Express*, vol. 7, no. 3, pp. 327–334, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959521000928

[9] I. S. Igboanusi, R. N. Alief, M. R. R. Ansori, Allwinnaldo, and D.-S. Kim, "Aim: Auto integrated mining," 2021. [Online]. Available: http://nsl.kumoh.ac.kr/include/sub.php?m=134&mode=Read&serial_no=202112080001&com_id=bi0001&menu_cd=30&class_cd=106&Page_Num=&left=&item=&find=&m=134

[10] Team, "Ml cheatsheet documentation," ML Glossary, Sep. 02, 2021 [Online]. [Online]. Available: https://ml-cheatsheet.readthedocs.io/en/latest/gradient_descent.html

Igboanusi Ikechi Saviour received his B. Tech degree in Physics from Federal University of Technology Owerri, Nigeria in 2013. He received his M.Eng degree from the department of IT Convergence Engineering from Kumoh National Institute of Technology, South Korea. He is currently working towards his PhD degree in IT Convergence Engineering, at Kumoh National Institute of Technology, Gumi, South Korea. He is a researcher in Networked Systems Lab since 2018 and has been a IEEE member since 2011. His interest research area include Blockchain, Network load balancing, real-time networks, and machine learning.

Revin Naufal Alief earned his Bachelor degree in Telecommunication Engineering from Telkom University, Indonesia in 2020. He is currently pursuing master's degree in IT Convergence Engineering in the Kumoh National Institute of Technology, Gumi, South Korea. He is also a researcher in Network System Laboratory, one of the laboratory in Kumoh National Institute of Technology. His research interest is regarding blockchain, real-time systems, information and security, and machine learning.

Muhammad Rasyid Redha Ansori earned his Bachelor's degree in Telecommunication Engineering from Telkom University, Indonesia in 2020. He is currently pursuing Master's degree in IT Convergence Engineering and is a researcher in the Kumoh National Institute of Technology's Networked System Lab in Gumi, South Korea. His research interests include blockchain, information and security, real-time systems, and machine learning.

Allwinnaldo also known as Allwin earned his Bachelor of Engineering degree in Telecommunication Engineering from Telkom University, Indonesia in 2020. He is currently pursuing master's degree in IT Convergence Engineering and also as a researcher in Kumoh National Institute of Technology's Networked System Lab (NSL) in Gumi, South Korea. His research interests include Blockchain, Digital Signal Processing, Audio Watermarking and Machine Learning

Jae-Min Lee received the Ph.D. degree in Electrical and Computer Engineering from the Seoul National University, Seoul, Korea, in 2005. From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, Korea. From 2015 to 2016, he was a Principle Engineer in Samsung Electronics, Suwon, Korea. Since 2017, he has been an assistant professor with School of Electronic Engineering and Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gyeongbuk, Korea. He is a member of IEEE. His current main research interests are industrial wireless control network, performance analysis of wireless networks, and TRIZ.

Dong-Seong Kim received his Ph.D. degree in Electrical and Computer Engineering from the Seoul National University, Seoul, Korea, in 2003. From 1994 to 2003, he worked as a full-time researcher in ERC-ACI at Seoul National University, Seoul, Korea. From March 2003 to February 2005, he worked as a postdoctoral researcher at the Wireless Network Laboratory in the School of Electrical and Computer Engineering at Cornell University, NY. From 2007 to 2009, he was a visiting professor with Department of Computer Science, University of California, Davis, CA. He is currently a director of kit Convergence Research Institute and ICT Convergence Research Center (ITRC and NRF advancd reserch center program) supported by Korean government at Kumoh National Institute of Technology. He is a senior member of IEEE and ACM. His current main research interests are real-time IoT and smart platform, industrial wireless control network, networked embedded system and Fieldbus.