The Journal of Korean Institute of Communications and Information Sciences '24-01 Vol.49 No.01
https://doi.org/10.7840/kics.2024.49.1.124

Vehicle Routing Based Mining for Proof-of-Useful-Work Blockchain

Philip Tobianto Daely◆, Jae Min Lee*, Dong-Seong Kim°

ABSTRACT

Blockchain gains tremendous attraction recently as the appearance of cryptocurrencies that can serve as an alternative of transaction between two entities that does not require a third party to intermediate the transaction. Blockchain is designed as an immutable digital ledger, consisting of a chain of blocks, with each block storing the information of transactions that happened between nodes in the blockchain network. Proof-of-Work (PoW) is the most popular consensus protocol to mine blocks in public blockchain, where participating nodes (miners) will use its computation resource to solve computational problems. However, the problems being solved in many PoW blockchains can be considered not useful, as they are designed to have high complexity but the output does not exactly serve any meaningful purpose, leading to massive energy waste. Proof-of-Useful-Work (PoUW) is a variant of PoW, where the miners mine blocks by solving more useful problems, having a more meaningful purpose for the output. This paper proposes the optimization of the Vehicle Routing Problem (VRP) as a block mining mechanism for PoUW blockchain. The proposed PoUW produces a new block by having miners solve VRP instances competitively. Particle Swarm Optimization (PSO) is used by miners to solve the VRP instance. The VRP instances are provided by external parties that also provide rewards for successfully mining the new block. The proposed PoUW blockchain can convert the computational effort to solve more useful problems, which serve a better purpose for the spent energy.

Key Words Blockchain, block mining, proof-of-useful-work, proof-of-work, vehicle routing problem

Ⅰ. Introduction

Blockchain technology has become extremely popular in recent years due to its innovative features. Blockchain, at its core, is a distributed ledger that permits private, open, and unchangeable transactions between parties without the involvement of intermediary like banks or other financial organizations. Blockchain is decentralized, as opposed to conventional transaction ledgers, which are centralized and managed by a single entity[1]. As a result, a peer-to-peer network of users share and maintain the blockchain. This makes the system more secure and impervious to hacking and other harmful attempts by ensuring that no single party has total control over it[2]. Blockchain technology

※ "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, 50%) and the Ministry of Science and ICT (MSIT) under the Innovative Human Resource Development for Local Intellectualization Support Program (IITP-2024-2020-0-01612, 50%) supervised by the Institute for Information & communications Technology, Planning, & Evaluation (IITP)."
◆ First Author : Kumoh National Institute of Technology, Department of IT Convergence Engineering; Institut Teknologi Telkom Surabaya, Department of Information Technology, philip.daely@kumoh.ac.kr, 학생회원
° Corresponding Author : Kumoh National Institute of Technology, Department of IT Convergence Engineering, dskim@kumoh.ac.kr, 종신회원
* Kumoh National Institute of Technology, Department of IT Convergence Engineering, ljmpaul@kumoh.ac.kr, 종신회원
논문번호 : 202303-059-C-RE, Received March 29, 2023; Revised October 24, 2023; Accepted December 14, 2023

has the potential to significantly change a variety of industries in the years to come, with uses in everything from voting and healthcare to finance and supply chain management.

One important aspect of blockchain is its method in achieving consensus between nodes to mine a new block. In the case of public blockchain, the most utilized consensus protocol is Proof-of-Work (PoW). It is a process that enables nodes in a blockchain network to come to an agreement over the ledger's current status by confirming transactions and adding new blocks to the chain, without any node acting as a central node to coordinate or synchronize this process over the network[3]. The oldest and most wellknown blockchain based cryptocurrency, Bitcoin, is introduced in 2009, with PoW as its consensus protocol. Since then, more cryptocurrency and blockchain projects have adopted it.

In a PoW consensus protocol, miners compete to solve complex mathematical problems to verify transactions and add new blocks to the blockchain. The miner who solves the problem first and adds the new block to the chain is rewarded with a certain amount of cryptocurrency, usually in the form of transaction fees and newly created coins. For example, in Bitcoin, all miners compete to find a hash in SHA-256 format for the new block, which must be lower than a predetermined difficulty target[4]. The process of solving these problems is computationally intensive and requires significant amounts of energy and processing power, making it expensive and timeconsuming[5].

To address these issues, a newer consensus protocol called Proof-of-Useful-Work (PoUW) has been proposed. PoUW seeks to leverage the computational power of miners to solve real-world problems that can benefit society, such as scientific research or data processing. By doing so, PoUW aims to reduce the energy consumption required for mining, while also incentivizing miners to contribute to projects that have a positive impact on society[6]. Unlike PoW, which only rewards miners for solving mathematical problems, PoUW rewards miners for solving useful problems that contribute to society. This can encourage a more diverse group of participants to join the network, reducing the risk of centralization and promoting a more decentralized system. Furthermore, PoUW can provide a more sustainable and environmentally friendly solution by harnessing the computational power for useful purposes, such as scientific researches or organization activities[7].

In this paper, we proposes a more useful work for miners, which is solving Vehicle Routing Problem (VRP) instance. VRP is a combinatorial optimization problem that involves optimizing the delivery of goods or services to multiple locations using a fleet of vehicles. VRP's main objective(s) can be to minimize overall traveled distance by vehicles, travel durations of vehicles from and back to depot, or other metrics pertaining to the problem instance provider. The complexity of VRP depends mainly on the number of vehicles and the number of destinations to visit[8]. It further increases when other parameters or constraints are considered, e.g. vehicle capacity or time windows to visit each destination. In the proposed PoUW blockchain, several nodes are designated as problem pool, sharing list of available VRP instances from external parties such as private companies, governmental bodies, or academic institutions. Miners will try to solve one VRP instance at a time to mine a new block. When a miner successfully mine a new block, it will broadcast the block to the whole network and it will also send the problem instance and the solution to a problem pool. Other nodes that receive the new block will verify that block and append it to its blockchain if the block is verifiable.

The remaining of this paper is organized as follows. Section II provides literature reviews related to PoUW and VRP. Section III provides details on the proposed PoUW blockchain. Section IV provides simulation results and analysis on the performance of proposed PoUW blockchain. Lastly, Section V conclude this paper.

Ⅱ. Related Works

PoUW is a type of consensus mechanism used in some blockchain systems to validate transactions and create new blocks. It requires network participants to perform a specific computational task, such as solving a mathematical puzzle or performing a useful computation, to prove that they have expended a significant amount of computational effort. This approach is designed to be more energy-efficient than other proof-of-work mechanisms, as it encourages participants to perform useful work that can be applied to real-world problems, rather than simply solving meaningless puzzles. Proof of useful work is still an emerging concept and is not widely used in blockchain systems yet, but it has the potential to address some of the scalability and environmental concerns associated with traditional proof-of-work mechanisms.

Huang et al.[9] proposed a new approach to enhance trustworthiness in mobile crowdsensing (MCS) by using a blockchain-based solution called BlockSense. BlockSense employs a PoUW approach named Proof-of-Data (PoD) to ensure the authenticity and integrity of data collected by mobile devices in MCS applications. The proposed system also addresses the privacy concerns of participants by allowing them to control the sharing of their data. The authors evaluated BlockSense through experiments and simulations, showing that it provides better security and privacy compared to existing MCS solutions. The results demonstrate the potential of BlockSense to facilitate trustworthy and efficient MCS applications in various domains, including smart cities, healthcare, and transportation.

Haouari et al.[10] proposed PoUW consensus mechanism for a blockchain system designed to store transportation transactions. The authors argue that traditional PoW and Proof-of-Stake (PoS) mechanisms are not ideal for this domain due to scalability and environmental concerns, and that a PoUW approach that incentivize useful work could provide a more sustainable and efficient alternative. The proposed PoUW mechanism requires network participants to perform a useful computation related to supply chain, that is, minimizing transportation cost between sea ports. They discuss the potential applications of their blockchain system in various domains, including smart cities, logistics, and transportation. The authors conclude that their PoUW-based blockchain system has the potential to address some of the scalability and environmental concerns associated with traditional blockchain consensus mechanisms while providing a more sustainable and efficient solution for transportation transactions.

Fitzi et al.[11] proposed a novel PoUW consensus protocol called Ofelimos for blockchain systems. The authors argue that existing PoUW protocols are not provably secure and that Ofelimos provides a more secure alternative by leveraging combinatorial optimization problems. The proposed protocol requires network participants to solve these problems as a form of useful work, and the difficulty of the problems is adjusted dynamically based on network performance. The authors provide a formal security analysis of the Ofelimos protocol and demonstrate its effectiveness through simulation results. They also discuss the potential applications of Ofelimos in various domains, including finance, healthcare, and logistics. The authors conclude that Ofelimos provides a more secure and efficient consensus mechanism for blockchain systems by incentivizing useful work and leveraging combinatorial optimization problems.

Du et al.[12] proposed a novel approach to accelerate blockchain-enabled distributed machine learning by introducing the concept of PoUW. The PoUW protocol leverages the computing power used in blockchain mining to perform useful work related to machine learning tasks. This approach aims to reduce the computational and energy costs associated with distributed machine learning while maintaining the security and decentralization properties of blockchain. The authors present a proof-ofconcept implementation of the PoUW protocol and show its effectiveness in accelerating distributed machine learning tasks. Overall, the paper introduces a promising approach for enhancing the efficiency of blockchain-enabled machine learning systems.

Davidović et al.[13] proposed a new consensus algorithm called Consensus using Optimized Computation and PoUW (COCP), which utilizes the computing power required for blockchain mining to perform useful work that is related to real-life applications. The authors argue that traditional PoW algorithms are energy-inefficient and propose COCP as a more sustainable alternative. The COCP protocol leverages the computational power used in blockchain mining to solve real-world problems, such as optimizing energy distribution and traffic management. The paper presents a proof-of-concept implementation of COCP and evaluates its performance in terms of energy efficiency and speed. In general, the authors show that COCP is a promising approach to improving the sustainability of blockchain systems while maintaining their decentralization and security properties.

Previous related works have proposed several solutions to replace PoW with their own version of the PoUW consensus protocol. But some disadvantages are introduced with these PoUW protocols. The work by Huang et al.[9] added data perturbation and also encryption for the data that will be used in PoUW, increasing the computational complexity when checking data quality, thus not suitable for blockchain network with low computation resources. The work of Haouari et al.[10] designed a PoUW that requires a parameter synchronization process between nodes, basically increasing message exchanges between nodes, making it difficult to scale the blockchain network without reducing the quality of the service. The work of Fitzi et al.[11] implemented a Doubly Parallel Local Search algorithm and zero-knowledge protocol for its PoUW, which would be difficult for devices without parallel computation capability and low specification. The work of Du et al.[12] that incorporated PoUW with distributed machine learning resulted in a rather long block time, which will further increase the time needed to achieve the finality of the transactions saved on the blockchain. The work of Davidović et al.[13] proposed COCP for blockchain but did not designate a specific combinatorial optimization problem and allows different types of combinatorial optimization problems to be submitted and solved in blockchain network, thus can lead to complication in maintaining desired block time and adjusting mining difficulty. In this work, we proposed a PoUW framework with adequate complexity for mining but simple process for validation, each node does not need to synchronize any parameter during mining process thus reducing traffic in the network, no requirement for each node to have specific computing features, low block time, and specified type of problem to solve to simplify difficulty adjustment and maintain fair competition between mining nodes.

Ⅲ. Proposed PoUW

The proposed PoUW framework is designed with VRP solving as the core of the block mining process. The choice to utilize VRP is based on its intrinsic qualities that correspond to the objectives of our PoUW framework. VRP, unlike other problems, intrinsically entails optimizing routes, allocating resources, and efficiently utilizing assets. These elements are essential for developing a practical and effective Proof of Useful Work (PoUW) consensus process.

Resource efficiency: VRP inherently focuses on optimizing the allocation of resources, which is consistent with the purpose of this PoUW framework to motivate and compensate participants for their contributions of useful work. This framework guarantees that computing resources dedicated to addressing intricate routing issues have a significant impact on the blockchain network by using VRP.

Real-world applicability: VRP is a widely recognized issue in the fields of logistics and transportation. Its incorporation within the PoUW framework demonstrates a commitment to ensuring practical relevance. This distinguishes this work from other PoUW frameworks that may concentrate on theoretical or conjectured issues, rendering this paradigm more concrete and applicable to real-life situations.

Scalability and complexity: The introduction of

VRP brings about a degree of complexity that poses a hurdle to the scalability of conventional PoUW techniques. This PoUW framework showcases its scalability by tackling a real-world optimization problem and effectively managing sophisticated routing scenarios. This highlights its potential for larger and more demanding blockchain networks.

In summary, the decision to utilize VRP in this PoUW framework is a conscious selection aimed at aligning with tangible optimization problems, improving resource effectiveness, and fostering practical usability. This approach sets this work apart from existing PoUW frameworks and establishes it as a potential alternative for blockchain networks that demand effective and meaningful proof of work.

The simplified diagram of the proposed PoUW blockchain is illustrated in Fig. 1. It consists of four types of node: client node, miner node, problem pool node, and external party node. Client node is a node that store blockchain. When a new block is received by client node, it will verify the new block, and add it to its blockchain if the new block is verifiable. The client node also stores unverified transactions that happen between blockchain nodes. The miner node has the same function and capability as the client node, with the addition of being able to mine (create) a new block. The problem pool node acts as storage of problem instances received from external party nodes. These problem instances are stored permanently only by the problem pool nodes and given priority in the order of pool based on the time of acquisition and problem fee. The miner nodes will sometimes request a problem instance from the closest problem pool node in the network to mine a new block. The external party nodes only communicate with the problem pool nodes, where they post new problem instances to solve and retrieve the solutions produced by the miner nodes. Problem pool nodes also share problem instances and problem solutions that they receive with each other so that every miner nodes can have access to the same set of problem instances.

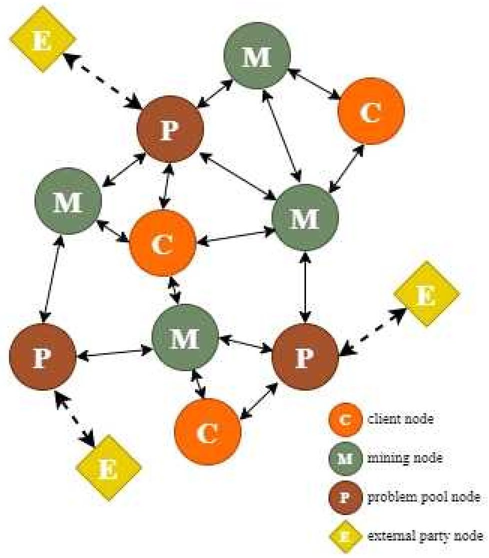

Fig. 1. Simplified network diagram of proposed PoUW blockchain. Solid arrow represents peer-to-peer connection between two node in blockchain network, whereas dashed arrow represents connection between an external party node and a problem pool node.

Miner nodes start the mining process by retrieving header of the latest block, a problem instance from problem pool node, and unverified transactions from its mempool. The Merkle Root for the new block is calculated from the unverified transactions. The latest block's hash is generated

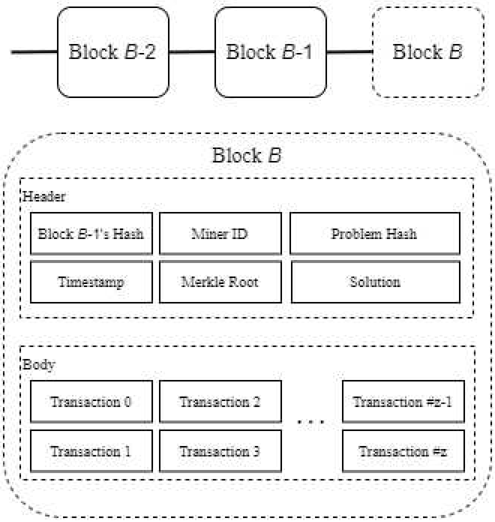

Fig. 2. Block structure of the proposed PoUW blockchain.

from the latest block's header. Then, the solution for the problem instance is determined using PSO. After a solution is found, the new block is created and appended to the blockchain. Miner node also broadcasts this new block to all other nodes. The solution for the problem instance is send back to problem pool node. The block structure of the proposed PoUW blockchain is shown in Fig. 2. The flowchart of proposed PoUW blockchain is shown in Fig. 3.

The new block is mined by solving a VRP instance. The objective function of VRP is formulated as

$$\begin{aligned} \min \quad & \sum_{i\in V}\sum_{J\in V} c_{ij}x_{ij}, \\ \text{s.t.} \quad & \sum_{i\in V} x_{ij} = 1, \\ & \sum_{j\in V} x_{ij} = 1, \\ & \sum_{i\in V\backslash\{0\}} x_{i0} = K, \\ & \sum_{j\in V\backslash\{0\}} x_{0j} = K, \\ & x_{ij} \in 0,1. \end{aligned} \tag{1}$$

In this formulation, c_{ij} represents the cost of going from destination i to destination j. x_{ij} is a binary variable that has value 1 if the arc going from i to j is considered as part of the solution and 0 otherwise. K Is the number of available vehicles. 0 is depot identifier in location set V. Constraint 1 and 2 state that exactly one arc enters and exactly one leaves each vertex associated with a customer, respectively. Constraints 3 and 4 say that the number of vehicles leaving the depot is the same as the number entering. Finally, constraints 5 are the integrality constraints.

Ⅳ. Simulation Results and Analysis

4.1 Usefulness Rate Comparison

We simulated our proposed PoUW blockchain in Python environment. We assumed 20 nodes acting as miners, 1 problem pooling node, and 1 external party node. We run the blockchain for 10 minutes repeatedly. The summarized results is shown in Table 1. The results shows that although VRP has rather high complexity, PSO can provide a fast solution, thus resulting in relatively short block time. This will lead to higher confirmed transaction rate for clients. We also provide usefulness rate, a percentage of how much time in mining process allocated for useful work. The metric usefulness rate is inspired from one used in work of Fitzi et al.[11], but instead of calculating computation step ratio, we based it on ratio of time spent for solving the 'useful work' over the whole computation time of a mining process, with assumption that energy consumption rate during one mining process is constant. As Bitcoin is a Hashcash based PoW, there

Table 1. Comparison between Proposed PoUW blockchain and Bitcoin.

Blockchain	Block Time	Block Size	Usefulness Rate (%)
Proposed PoUW	~1 min	3 MB	90
Bitcoin	~10 min	1 MB	0

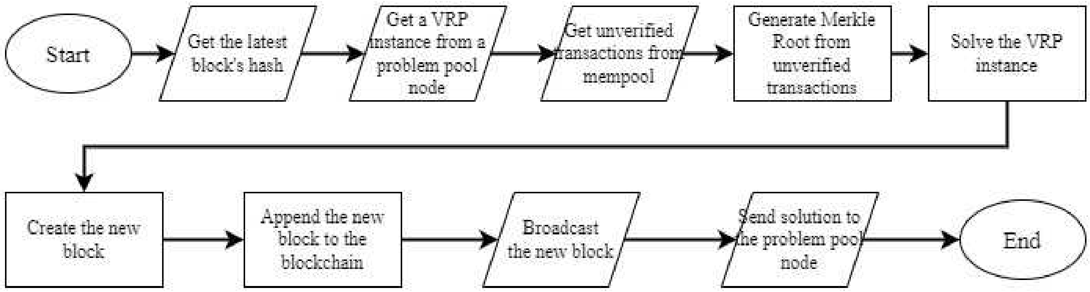

Fig. 3. Flowchart of block mining for miner node.

is no time used for work that is deemed useful. On the other hand, our proposed PoUW blockchain can achieve 90%, with the 10% of the mining time is used to generate random numbers for PSO and other functions outside finding the solution.

4.2 Features Comparison

Features of Proposed PoUW Framework were compared and analyzed in terms of type of useful work executed in mining process, real-world applicability, and scalability. The comparison summary is shown in Table 2. PoUW frameworks proposed by Fitzi et al. and Davidović et al. have low realworld applicability as they are not designed for a specific type of optimization problem. Some of NPhard optimization problems are still theoretical in nature and can only be provided by research organizations that rarely needs blockchain based processing solution to solve their problems, as they usually already equipped with devices intended for solving their own particular problem. These frameworks are deemed moderate in scalability because some of NP hard problems still can be processed by devices available to public, while some other problems will required higher specification. PoUW framework by Du et al. is considered low in real-world applicability and scalability because it requires each miner node to have extensive resources to store and process training data, which will also increase traffic when distributed across the network. PoUW frameworks by Huang et al. and Haouari et al. have high real-world applicability because each of them has specific problem to solve by miner nodes and highly related to public sector. PoUW by Haouari et al. has low scalability as it requires parameter synchronization between miner nodes when they are mining a new block which will increase message overhead in the network. PoUW by Huang et al. has moderate scalability as the mining process are quite fast, altough will be difficult to expand as the data being validated are confidential and need further encryption process. Compare to previous related works, our proposed PoUw framework have high real-world applicability for its specific target problem to solve by each miner node and high scalability for the mining process is not difficult to performed by devices available to public and independent towards other miner nodes' mining process.

4.3 Security Threat Analysis

Our proposed PoUw Blockchain has similar consensus mechanism with Hashcash based blockchain, and there are only a several attack possibilities analyzed as follows.

1) Denial of Service: The problem pooling node communicates the problem to all miners. As previously discussed, a problem pooling node can refuse service at any time or be attacked by hackers attempting to disrupt the blockchain. A problem pooling node can also deliberately withhold service to specific users, which can be used as a penalty against a group of people or to empower a malicious party with more than 50% of the blockchain's computational capacity, allowing them to erase transactions. This can be avoided by making Hashcash cryptographic puzzle available as an additional challenge for miners to solve in order to add new blocks. Because we want to incentivize solving important problems, we can keep the difficulty of the cryptographic puzzle high enough that miners can solve it.

2) Deliberately deviating from promised difficulty: The problem pooling nodes can also have their own mining nodes, and they can improve their rewards obtained by regulating difficulty based on the fraction of computation power they have. For example, when the number of miners is low and the problem pooling node has 25% of the network's calculation power, they can boost the block publishing rate more than when the number of miners is high and the problem pooling node's power is only 10% of the network.

It is possible to argue that any attack by the problem creator is self-sabotage because the network is dedicated to solving their problem. Bad behaviour will reduce trust in their blockchain, reducing the number of miners mining in their blockchain and decreasing the network's compute capacity. Additional hacker attacks can be avoided with strong

Table 2. Feature comparison between Proposed PoUW and previous works.

PoUW Framework	Useful Work	Real-World Applicability	Scalability
Blocksense by Huang et al.[9]	crowdsensing data validation	high	moderate
PoUW by Haouari et al.[10]	maritime transportation allocation	high	low
Ofelimos by Fitzi et al.[11]	NP-hard problem optimization	low	moderate
PoUW by Du et al.[12]	machine learning subproblem solving	low	low
COCP by Davidovic et al.[13]	combinatorial NP-hard problem optimization	low	moderate
Proposed PoUW	vehicle routing	high	high

security techniques implemented by the problem pooling node.

V. Conclusion

We presented a PoUW blockchain with a block mining technique for resolving VRP instances from third parties. Our proposed PoUw blockchain has been proved to be capable of redirecting squandered energy to more productive uses. The relevance of this work is based on overcoming the disadvantage of PoW's inefficient power usage. PoUW has the potential to be a useful mechanism for validating transactions on blockchains used in operations and finance applications. Similarly, the technique permits distributed optimization, which leads to distributed decision-making appropriate to the ecosystem served by the blockchain. A blockchain utilized in finance, for example, with our optimization-based PoUW, would optimize investment portfolios, considerably boosting the blockchain's usefulness beyond serving as a simple distributed ledger. It should be underlined that no other alternative validation technique, such as Proof of Stake, can perform this dual purpose of PoUW (PoS). Not all blockchains are designed to support applications that require optimal decision making. Yet, when used in situations where such challenges exist (such as optimizing operations, financial portfolios, and so on), PoUW can become the stone that kills two birds. As a result of overcoming the major limitation of PoW, PoUW may lead to the expansion of blockchain use cases beyond serving as a ledger and a virtual environment for running smart contracts.

References

[1] B. Farahani, F. Firouzi, and M. Luecking, "The convergence of iot and distributed ledger technologies (DLT): Opportunities, challenges, and solutions," *J. Netw. and Comput. Appl.*, vol. 177, p. 102 936, 2021, ISSN: 1084-8045. (https://doi.org/10.1016/j.jnca.2020.102936)

[2] R. Akter, M. Golam, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "IoMT-Net: Blockchain integrated unauthorized uav localization using lightweight convolution neural network for internet of military things," *IEEE Internet of Things J.*, pp. 1-1, 2022. (https://doi.org/10.1109 / JIOT.2022.3176310)

[3] B. Shrimali and H. B. Patel, "Blockchain Stateof-the-Art: Architecture, use cases, consensus, challenges and opportunities," *J. King Saud University Comput. and Inf. Sci.*, vol. 34, no. 9, pp. 6793-6807, 2022, ISSN: 1319-1578. (https://doi.org/10.1016/j.jksuci.2021.08.005)

[4] B. Wu and B. Wu, "Blockchain: A groundbreaking technology," in *Blockchain for Teens: With Case Studies and Examples of Blockchain Across Various Industries.* Berkeley, CA: Apress, pp. 1-49, 2023, ISBN: 978-1-4842-8808-5. (https://doi.org/10.1007/9781-4842-8808-5_1).

[5] I. S. Igboanusi, A. Allwinnaldo, R. N. Alief, M. R. R. Ansori, J.-M. Lee, and D.-S. Kim, "Smart auto mining (SAM) for industrial IoT blockchain network," *IET Commun.*, vol. 16, no. 18, pp. 2123-2132, 2022.

(https://doi.org/10.1049/cmu2.12465)

[6] M. Todorović, L. Matijević, D. Ramljak, et al., "Proof-of-Useful-Work: BlockChain mining by solving real-life optimization problems," *Symmetry*, vol. 14, no. 9, 2022, ISSN: 2073-8994. (https://doi.org/10.3390/sym14091831)

[7] V. Kohli, S. Chakravarty, V. Chamola, K. S. Sangwan, and S. Zeadally, "An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions," *Digital Commun. and Netw.*, vol. 9, no. 1, pp. 79-89, 2023, ISSN: 2352-8648. (https://doi.org/10.1016/j.dcan.2022.06.017)

[8] F. Torres, M. Gendreau, and W. Rei, "Crowdshipping: An open VRP variant with stochastic destinations," *Transportation Research Part C: Emerging Technologies*, vol. 140, p. 103 677, 2022, ISSN: 0968-090X. (https://doi.org/10.1016/j.trc.2022.103677).

[9] J. Huang, L. Kong, L. Cheng, et al., "BlockSense: Towards trustworthy mobile crowdsensing via proof-of-data blockchain," *IEEE Trans. Mobile Comput.*, pp. 1-17, 2022. (https://doi.org/10.1109/TMC.2022.3230758)

[10] M. Haouari, M. Mhiri, M. El-Masri, and K. Al-Yafi, "A novel proof of useful work for a blockchain storing transportation transactions," *Inf. Process. & Manag.*, vol. 59, no. 1, p. 102 749, 2022, ISSN:0306-4573. (https://doi.org/10.1016/j.ipm.2021.102749)

[11] M. Fitzi, A. Kiayias, G. Panagiotakos, and A. Russell, "Ofelimos: Combinatorial optimization via proof-of-useful-work," in *Advances in Cryptology CRYPTO 2022*, Y. Dodis and T. Shrimpton, Eds., Cham: Springer Nature Switzerland, pp. 339-369, 2022. (https://doi.org/10.1007/978-3-031-15979-4%5C_12)

[12] Y. Du, C. Leung, Z. Wang, and V. C. Leung, "Accelerating blockchain-enabled distributed machine learning by proof of useful work," in *2022 IEEE/ACM 30th IWQoS*, pp. 1-10, 2022. (https://doi.org/10.1109/IWQoS54832)

[13] T. Davidović, M. Todorović, D. Ramljak, et al., "COCP: Blockchain proof-of-usefulwork leveraging real-life applications," in *2022 Fourth Int. Conf. Blockchain Computing and Applications (BCCA)*, pp. 107-110, 2022. (https://doi.org/10.1109/ BCCA55292.2022.9922117)

Philip Tobianto Daely

Feb. 2015 : B.Eng. degree, Telkom University

Aug. 2017 : M.Eng. degree, Kumoh National Institute of Technology

Jan. 2018~Current : Lecturer, Institut Teknologi Telkom Surabaya

Mar. 2019~Current : Ph.D. student, Kumoh National Institute of Technology

<Research Interest> artificial intelligence, internet of things, vehicle routing

[ORCID:0000-0001-5290-9564]

Jae Min Lee

2005 : Ph.D. Electrical and Computer Engineering, Seoul National University, Seoul, Korea

2005~2014 : Senior Engineer, Samsung Electronics Engineering, Suwon, Korea

2015~2016 : Principal Engineer, Samsung Electronics Engineering, Suwon, Korea

2017~Current : Associate Professor, School of Electronic Engineering, Kumoh National Institute of Technology, Gyeongbuk, Korea

<Research Interests> Blockchain, TRIZ, Smart IoT convergence Application, industrial wireless control network, UAV, Metaverse.

[ORCID:0000-0001-6885-5185]

Dong-Seong Kim

2003 : Ph.D. Electrical and Computer Engineering, Seoul National University, Korea.

2003~-2004 : Postdoctoral Researcher, Cornell University, NY, USA

2007~2009 : Visiting Professor, The University of California, Davis, CA, USA

2004~Current : Professor, Kumoh National Institute of Technology, Korea

2014~Current : Director, ICT Convergence Research Center, Kumoh National Institute of Technology, Korea

2017~2022 : Dean, Industry-Academic Cooperation Foundation and Office of Research, Kumoh National Institute of Technology, Korea

2022~Current : CEO, NSLab co. Ltd., Korea

<Research Interests> Blockchain, Metaverse, Industrial IoT, real-time systems, industrial wireless control network, 5G+, and 6G.

[ORCID:0000-0002-2977-5964]