Indonesian Journal of Electrical Engineering and Computer Science
Vol. 34, No. 2, May 2024, pp. 806~813
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v34.i2.pp806-813

Improved DAG in blockchain tangle for IOTA

Eugene Rhee[1], Jihoon Lee[2]
[1]Department of Electronic Engineering, College of Engineering, Sangmyung University, Cheonan, Republic of Korea
[2]Department of Smart Information and Telecommunication Engineering, Sangmyung University, Cheonan, Republic of Korea

Article Info

Article history:

Received Jan 25, 2024
Revised Feb 4, 2024
Accepted Feb 16, 2024

Keywords:

Blockchain
Directed acyclic graph
IoT
IOTA
Tangle

ABSTRACT

The internet of things (IoT) enables machine-to-machine communication without human intervention. Consequently, every object connected to the internet can exchange information with each other. Internet of things application (IOTA) has undertaken a project to address the high transaction fees inherent in traditional blockchain systems and enhance the efficiency of microtransactions between machines by combining blockchain and IoT. IOTA employs its unique Tangle technology, which introduces a novel transaction consensus method, addressing the fee issues, limited scalability, and the inability to conduct offline transactions associated with traditional blockchains. This paper provides a detailed overview of the characteristics of the Tangle structure and the concepts applied in IOTA. Additionally, it explores potential approaches for integrating blockchain into IoT.

Corresponding Author:

Jihoon Lee
Department of Smart Information and Telecommunication Engineering, Sangmyung University
Cheonan, Republic of Korea
Email: vincent@smu.ac.kr

1. INTRODUCTION

Globally, it is predicted that approximately one billion devices will be connected through internet of things (IoT). However, the current state of IoT has limitations such as scalability issues, high management costs, and security vulnerabilities inherent to the convenience-centric development of centralized systems [1]–[3]. To overcome these limitations, research is being conducted to apply blockchain technology. Blockchain provides a decentralized system where each user retains transaction records, preventing forgery through its hash chain structure and enabling transparent transactions [4]–[6]. Nevertheless, applying first-generation blockchain systems, like Bitcoin, directly to IoT poses challenges. The transaction verification speed of traditional blockchains is slower than that of centralized systems [7]–[9]. For IoT services requiring rapid processing, the transaction handling of conventional blockchains is impractical. Additionally, many IoT devices lack computing power, making it difficult to implement proof-of-work algorithms used in first-generation blockchains [10]–[12]. To address scalability and transaction verification speed issues, the emergence of third-generation blockchain technology, known as Tangle, has taken place [13]–[15].

In this context, distributed ledger technology and blockchain have gained recognition as innovative technologies providing reliable transaction records and decentralized platforms. Among them, internet of things application (IOTA) stands out as a project seeking to go beyond the limitations of blockchain, presenting a new direction [16]–[18]. IOTA tackles the constraints and fee issues of blockchain by introducing a unique distributed ledger technology called Tangle, flipping the existing paradigm [19]–[21]. This paper will briefly explain first-generation blockchain technology and focus primarily on Tangle technology. And this paper will explore how IOTA's Tangle technology operates, its distinctions from traditional blockchain, and particularly the advantages it offers in IoT environment. Furthermore, it will provide insights into how the technical features of IOTA could impact future decentralized transaction systems and the IoT ecosystem. Through this paper, we anticipate gaining insights into how the new paradigm proposed by IOTA and Tangle could revolutionize the digital economy and social structures.

2. IOTA

IOTA is a German startup focused on blockchain research. IOTA is a cutting-edge microtransaction cryptocurrency platform optimized for the IoT, connecting various devices securely through microtransactions [22]–[24]. With IOTA, values and data can be quickly and tamper-proof transmitted in a distributed manner across many nodes. It is based on its proprietary technology called Tangle, which is considered a third-generation blockchain. Tangle utilizes a directed acyclic graph (DAG), a multi-directional, non-cyclic graph, rather than a traditional blockchain [25]–[27]. When issuing a new transaction in Tangle, there is no need for miners, eliminating the energy consumption associated with traditional proof-of-work algorithms. This helps reduce power waste and authenticate transactions faster than traditional blockchains. One of the advantages of IOTA is the absence of transaction fees.

In contrast to Bitcoin, where miners compete, consuming power to connect blocks to the blockchain and receive fees as compensation, IOTA has a tip selection algorithm that does not consume power when validating transactions. The absence of transaction fees is a notable advantage of IOTA. Bitcoin miners approving transactions for blocks that offer higher fees can lead to delays for blocks with lower fees. IOTA, however, designed a distributed ledger without the need for a blockchain, utilizing cryptographic technology. This enables the processing of thousands of transactions per second, emphasizing the elimination of the need for traditional blockchain structures. For instance, when A wants to send a transaction to B for approval, A must first approve two random transactions. In essence, A sends data to B, receives IOTA in return, and for this transaction to be validated on the network, A must validate two prior transactions from unknown parties. As more devices participate in IOTA, the network stability increases, as more devices can verify various transactions. Unlike traditional blockchains, IOTA operates without the need for miners, eliminating the requirement for transaction fees.

3. TANGLE

Tangle is a distributed ledger technology and a type of DAG used in the context of cryptocurrencies, notably associated with the IOTA cryptocurrency [28]–[30]. Unlike traditional blockchain structures, Tangle does not rely on a chain of blocks. Instead, it forms a DAG where each transaction approves two previous transactions, creating a web-like structure. This eliminates the need for miners and allows for parallel and real-time processing of transactions. In Tangle, when a participant wants to make a transaction, they need to validate two previous transactions, adding a level of decentralized verification. This structure is designed to enhance scalability, eliminate transaction fees, and potentially increase security by making the network more resilient to certain types of attacks. IOTA, a cryptocurrency built on the Tangle technology, is particularly focused on applications in IoT, where microtransactions, scalability, and low resource requirements are essential.

3.1. DAG

DAG is a graph that is not cyclic but acyclic. In other words, in DAG algorithms, there is no existence of cycles, and it strictly follows a single direction. What makes DAG algorithms more intricate is the fact that the acyclic structure is randomly generated [31]–[33]. While Bitcoin’s blockchain forms blocks in a linear, directional fashion, DAG algorithms exhibit blocks in a random and acyclic structure. In blockchain, each subsequent block verifies the complete transaction history of the preceding block, but in DAG algorithms shown in Figure 1, one block is involved in verifying multiple blocks simultaneously.

DAG algorithms exhibit advantages over traditional blockchain algorithms due to several distinctive characteristics. Firstly, in DAG, there is no concept of block formation as in Bitcoin. Since one block verifies other blocks below it, the transaction processing speed can increase exponentially. Unlike Bitcoin, where the creation of one block must precede the creation of another, DAG allows for real-time and parallel processing without time constraints, resulting in faster transaction processing. Secondly, Bitcoin’s high fees exist as a concept of compensation for the engine driving the blockchain network-miners. As the number of transactions increases, miners have more work to process, and their computational power naturally grows. This led users to pay higher fees. In DAG algorithms, there is no concept of miners forming blocks, resulting in minimal fees [34]–[36]. For example, IOTA, adopting DAG algorithm, incurs fees close to zero. Thirdly, as the number of transactions increases, there is an increased possibility of verifying future transactions. Metcalfe’s Law, which asserts that the value of a network experiences exponential growth as the number of users increases, is prominently observable in DAG networks.

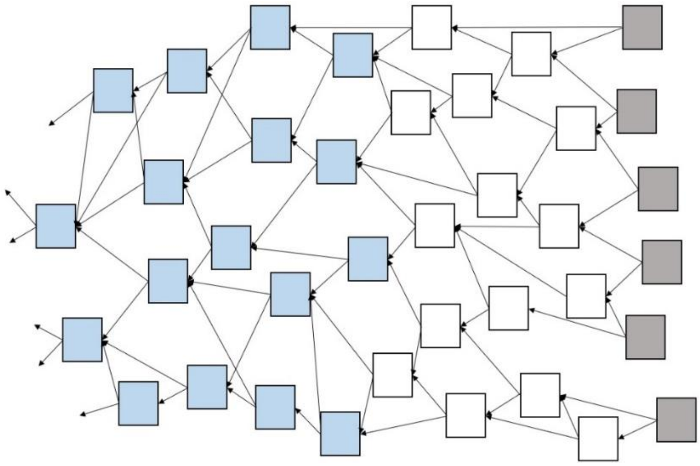

Figure 1. Typical DAG algorithms

3.2. Selection algorithm

In the Tangle network, a node issuing a new transaction utilizes the properties of a DAG to select transactions. The selection algorithm in Tangle influences how nodes verify transactions and choose new transactions: i) Transaction verification and approval: a new transaction needs to be referenced and verified by other transactions. The more references a new transaction receives from previous transactions, the higher the likelihood of quick confirmation and selection. ii) Transaction selection priority: priority is assigned based on the attributes of a transaction. For instance, a node may give higher priority to transactions with attached fees or those meeting specific conditions. iii) Connection between transactions and nodes: a new transaction integrates into the Tangle network by establishing connections with existing transactions. Transactions with more connections to previous transactions are more likely to be selected. The Tangle selection algorithm ensures consistent distribution across the network by considering the relative reliability and connectivity of transactions [37]–[39].

In consideration of a scenario where a node publishes a new transaction on the Tangle network, initially, the node signs the transaction with its private key. The node is not required to achieve unanimous consensus on what valid transactions should be recorded on the ledger. However, in the presence of conflicting transactions, the node must determine which transaction will become orphaned. The primary rule that a node follows for conflicting transactions is as follows: the node employs the tip selection algorithm multiple times and checks which transaction is more consistently approved by the selected tips. For instance, after performing the tip selection algorithm over 100 times, if a transaction is selected 99 times, it can be confidently stated that it has been approved with 99% confidence.

4. CONSENSUS AND CUMULATIVE WEIGHT

In Tangle, every node has the capability to participate in consensus. Nodes perform only lightweight tasks that do not require significant processing power. Users can set up nodes with minimal cost and actively contribute to network security at a minimal expense [40]–[42]. The consensus mechanism ensures network consistency by determining how nodes collectively agree on which transactions are trustworthy. In the current implementation of IOTA, nodes trust and reference transactions approved by the coordinator, a centralized “finality device,” to secure the network, especially in its early stages. To scale IOTA, this paper employed a temporary consensus mechanism, the coordinator, and engage voluntary participants to address security concerns. Every two minutes, a milestone transaction is issued and approved by the IOTA Foundation, considering all transactions approved by it immediately as having a 100% confirmation confidence. This serves as a protective mechanism as the IOTA network transitions towards a fully decentralized Tangle-based consensus algorithm. At the point when the network matures enough without the need for the coordinator, the IOTA foundation removes it, and Tangle evolves independently. This iterative process occurs repeatedly, and each time the network matures through the removal of the coordinator, it becomes more efficient at scale.

To address the issue of slow tips, one possible solution is to enforce participants to only approve recent transactions. However, this approach contradicts the principles of decentralization, as everyone should have the ability to approve transactions. Additionally, since there is no reliable way to precisely notify the system of the arrival of each transaction, enforcing specific rules becomes challenging. A resolution to this challenge involves configuring the system to naturally discourage behaviors that go against this principle by incorporating inherent incentives. The strategy is to introduce randomness to the process, reducing the likelihood of consistently choosing slow tips. The weight of a transaction is proportional to the amount invested by the issuing node. In practice, the weight is assumed to follow the formula 3 to the power of *n*, where *n* is a positive integer. Cumulative weight indicates how crucial a transaction is, calculated as the sum of the weight of the transaction itself and the weight of all transactions directly or indirectly approving it.

5. VALIDATION

5.1. Initial state of tangle

The origin of IOTA lies in the first transaction called the genesis transaction within Tangle, where all IOTAs were generated. Additional IOTAs are not created. Since the beginning of the genesis, IOTAs have been transferred to the accounts of the original investors in the project, matching the amount of their initial investment. Subsequently, they sold some of their IOTAs to other individuals, ultimately establishing the network. Initial transactions, excluding the genesis transaction, can be categorized into three types: i) Confirmed transactions: transactions are considered confirmed if they are directly or indirectly referenced by all tips. There is consensus on these transactions. ii) Pending/unconfirmed transactions: these are transactions that are awaiting confirmation. iii) Tip transactions: these are newly attached transactions that have not yet been referenced by other transactions.

5.2. Adding a new transaction

To add the new transaction 19 to the Tangle, the user must randomly select two tips, 15 and 16, as shown in Figure 2, and verify them. Verification involves checking the signatures and proof-of-work of the selected tips and ensuring there are no conflicts with past transactions referenced directly or indirectly by the tips. If there are no issues with the selected tips, the user adds the new transaction 19, referencing the two tips, 15 and 16, to the Tangle. Transactions 11, 14, 17, and 18, which are not directly or indirectly referenced by the selected tips 15 and 16, are not verified during the process of adding transaction 19 to the Tangle. These transactions will be verified later when other transactions are added.

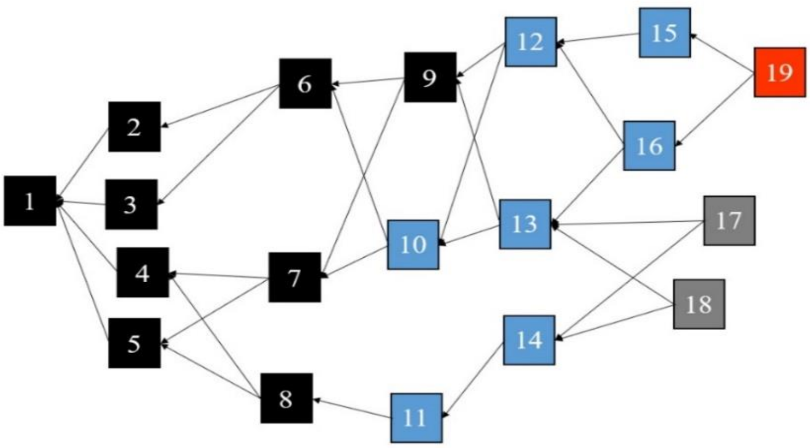

Figure 2. New transaction

5.3. Double spending

In the context of Bitcoin, “double spending” is a critical security concern. It refers to attempts by users to spend the same Bitcoin more than once, essentially trying to use the same Bitcoin for multiple transactions. Bitcoin functions through a decentralized peer-to-peer (P2P) network, where transactions are documented on a public ledger known as the blockchain [43]–[45]. However, to prevent double spending, these transactions need to be propagated and confirmed by the network [46]–[48]. Key mechanisms to prevent double spending are as follows: i) Blockchain confirmation: miners verify the validity of transactions before adding them to a block. Attempts to reuse Bitcoins that have already been spent are rejected during this verification process. ii) Mining process: the Bitcoin network employs a competitive mining process where miners race to create a block. Only valid transactions are included in the block. When one block becomes longer than others (due to more computational work), the transactions within it are considered final and valid. iii) Mining difficulty: Bitcoin adjusts the mining difficulty periodically to regulate the time it takes to create a new block. This ensures that the network remains stable, making it difficult for attackers to attempt double spending with rapid changes. Through these mechanisms, Bitcoin effectively prevents double spending and maintains its security.

In the event that a user initiates two conflicting transactions, denoted as 18 and 19, within distinct regions of the Tangle, as illustrated in Figure 3. Subsequently added transactions may potentially include only one of these conflicting transactions, either 18 or 19, in the verification path due to tip selection. For instance, a user adding transaction a to the Tangle and another user adding transaction c might not be aware of the conflict between 18 and 19. Consequently, they may perceive 18 and 19 as non-conflicting valid transactions. However, the conflict is soon discovered. For example, when a new transaction e referencing both a and c is added, it will include both 18 and 19 in its verification path, enabling e to detect the conflict. Therefore, e would refrain from selecting a and c, opting for two non-conflicting tips instead. This way, e can be verified as a valid transaction when later added to the Tangle.

According to the tip selection algorithm and the Tangle process, many users may include only one of the conflicting transactions, 18 or 19, in the verification path before the conflict becomes apparent. Consequently, there is a possibility that some users might recognize 18 and 19 as valid transactions without detecting the conflict. However, ultimately, based on which set of tips, those including 18 or those including 19, users add more new transactions to, either 18 or 19 will be confirmed, and the other one will be discarded. Transactions added to the discarded side, while unaware of the conflict, are discarded together. However, these transactions are not entirely removed from the Tangle. Instead, they have the chance to be selected and added back to the Tangle by other users, gaining an opportunity for verification.

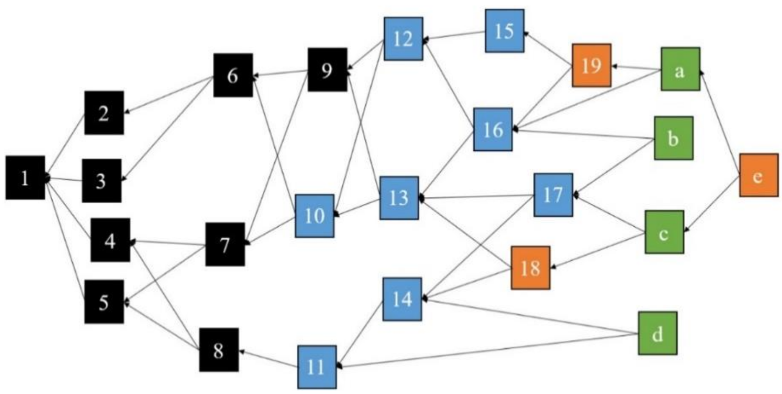

Figure 3. Double spending

5.4. Offline tangle

Offline Tangle refers to the use of Tangle technology to process transactions even when the internet connection is unavailable [49], [50]. Typically, Tangle is utilized in a decentralized network to confirm transactions and form blocks on the ledger. However, offline Tangle allows for the creation and signing of transactions within an internal network, even in the absence of an external internet connection. Transactions in offline Tangle possess distinctive features, such as the absence of miners and no transaction fees, unlike traditional blockchain systems. Instead, users validate their transactions and those of others in the network. The system becomes more efficient as more users participate, and it exhibits relatively lower scalability issues. Offline Tangle is particularly useful in environments with unstable or limited internet connectivity. This makes it a potential solution for scenarios where infrastructure is constrained, such as in the context of IoT devices.

Tangle users can continue to append transactions even in an offline network not connected to the main Tangle network. For this to happen, transactions must be generated and connected according to the protocol-defined conventions. An offline network refers to a network in a state where external internet connection is unavailable to connect to the main Tangle network, but internal connections, similar to an intranet, are possible. For a transaction that was in the offline network to achieve a fully confirmed state, it must not conflict with transactions in the main Tangle network, just like transactions present in the main Tangle network. If there is any conflict with transactions in the main Tangle network, the transaction cannot be confirmed. Subsequent transactions need to be added to the Tangle network for it to be discovered by all tips in the main Tangle.

6. CONCLUSION

This paper discussed IOTA and its technology Tangle, proposed to address the limitations of first-generation blockchains when applied to IoT. Tangle, as described in this paper, offers advantages such as faster transactions with an increasing number of users and zero fees due to the absence of miners. Additionally, the significant reduction in bottlenecks results in improved scalability without scalability issues. Thanks to these benefits, IOTA has the potential to be widely used as a micro-payment method in IoT. However, IOTA remains a solution for the future, and it will take time for machine-to-machine communication to adopt it extensively. While Tangle has addressed scalability and overhead issues, which were limitations of first-generation blockchains applied to IoT, it introduces a special central node called the coordinator. This has led to criticism, considering IOTA as a cryptocurrency in a semi-decentralized state rather than a fully decentralized one. Further research is needed to enhance the security of internal information, and it is predicted that once these aspects are improved, blockchain technology applied to IoT will become more viable.

REFERENCES

[1] K. Fizza, P. P. Jayaraman, A. Banerjee, N. Auluck, and R. Ranjan, "IoT-QWatch: a novel framework to support the development of quality-aware autonomic IoT applications," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 17666–17679, Oct. 2023, doi: 10.1109/JIOT.2023.3278411.

[2] N. Nabeel, M. H. Habaebi, and M. D. R. Islam, "Security analysis of LNMNT-lightweight crypto hash function for IoT," *IEEE Access*, vol. 9, pp. 165754–165765, 2021, doi: 10.1109/ACCESS.2021.3133097.

[3] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[4] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[5] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang, and L. Gao, "A lightweight and attack-proof bidirectional blockchain paradigm for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371–4384, Mar. 2022, doi: 10.1109/JIOT.2021.3103275.

[6] H. M. Kim, H. Turesson, M. Laskowski, and A. F. Bahreini, "Permissionless and permissioned, technology-focused and business needs-driven: understanding the hybrid opportunity in blockchain through a case study of insolar," *IEEE Transactions on Engineering Management*, vol. 69, no. 3, pp. 776–791, Jun. 2022, doi: 10.1109/TEM.2020.3003565.

[7] Y. Ren, C. Wang, Y. Chen, M. C. Chuah, and J. Yang, "Signature verification using critical segments for securing mobile transactions," *IEEE Transactions on Mobile Computing*, vol. 19, no. 3, pp. 724–739, Mar. 2020, doi: 10.1109/TMC.2019.2897657.

[8] N. Kokash and F. Arbab, "Formal design and verification of long-running transactions with extensible coordination tools," *IEEE Transactions on Services Computing*, vol. 6, no. 2, pp. 186–200, Apr. 2013, doi: 10.1109/TSC.2011.46.

[9] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Joint transaction relaying and block verification optimization for blockchain empowered D2D communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 828–841, Jan. 2020, doi: 10.1109/TVT.2019.2950221.

[10] M. Baza *et al.*, "Detecting sybil attacks using proofs of work and location in VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 39–53, Jan. 2022, doi: 10.1109/TDSC.2020.2993769.

[11] F. Wilhelmi, S. Barrachina-Munoz, and P. Dini, "End-to-end latency analysis and optimal block size of proof-of-work blockchain applications," *IEEE Communications Letters*, vol. 26, no. 10, pp. 2332–2335, Oct. 2022, doi: 10.1109/LCOMM.2022.3194561.

[12] B. Alangot, D. Reijsbergen, S. Venugopalan, P. Szalachowski, and K. S. Yeo, "Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1659–1672, Jun. 2021, doi: 10.1109/TNSM.2021.3069502.

[13] Y. Chen, Y. Guo, M. Wang, E. Xu, H. Xie, and R. Bie, "Securing IOTA blockchain against tangle vulnerability by using large deviation theory," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1952–1965, Jan. 2023, doi: 10.1109/JIOT.2023.3283788.

[14] S. Zheng, Y. Jiang, X. Ge, Y. Xiao, Y. Huang, and Y. Liu, "Cooperative spectrum sensing and fusion based on tangle networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3614–3632, Sep. 2022, doi: 10.1109/TNSE.2022.3174688.

[15] K. Xue, X. Luo, Y. Ma, J. Li, J. Liu, and D. S. L. Wei, "A distributed authentication scheme based on smart contract for roaming service in mobile vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5284–5297, May 2022, doi: 10.1109/TVT.2022.3148303.

[16] J. Chen, H. Masaki, K. Nguyen, and H. Sekiya, "QoE provisioning system for voip and video streaming using software-defined networking and IOTA micropayment," *IEICE Communications Express*, vol. 12, no. 12, pp. 587–590, Dec. 2023, doi: 10.23919/comex.2023col0002.

[17] F. Guo, X. Xiao, A. Hecker, and S. Dustdar, "A theoretical model characterizing tangle evolution in IOTA blockchain network," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1259–1273, Jan. 2022, doi: 10.1109/JIOT.2022.3207513.

[18] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, and N. Ottakath, "Evolution of internet of things from blockchain to IOTA: a survey," *IEEE Access*, vol. 10, pp. 844–866, 2022, doi: 10.1109/ACCESS.2021.3138353.

[19] V. S. Naresh, V. V. L. D. Allavarpu, and S. Reddi, "Blockchain IOTA sharding-based scalable secure group communication in large VANETs," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5205–5213, Mar. 2023, doi: 10.1109/JIOT.2022.3222382.

[20] A. N. Bikos and S. A. P. Kumar, "Securing digital ledger technologies-enabled IoT devices: taxonomy, challenges, and solutions," *IEEE Access*, vol. 10, pp. 46238–46254, 2022, doi: 10.1109/ACCESS.2022.3169141.
[21] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "Pay as you go: a generic crypto tolling architecture," *IEEE Access*, vol. 8, pp. 196212–196222, 2020, doi: 10.1109/ACCESS.2020.3034299.
[22] W. Zhao, I. M. Aldyaflah, P. Gangwani, S. Joshi, H. Upadhyay, and L. Lagos, "A blockchain-facilitated secure sensing data processing and logging system," *IEEE Access*, vol. 11, pp. 21712–21728, 2023, doi: 10.1109/ACCESS.2023.3252030.
[23] A. Cullen, P. Ferraro, C. King, and R. Shorten, "On the resilience of DAG-based distributed ledgers in IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7112–7122, Aug. 2020, doi: 10.1109/JIOT.2020.2983401.
[24] L. Vigneri, T. Spyropoulos, and C. Barakat, "Quality of experience-aware mobile edge caching through a vehicular cloud," *IEEE Transactions on Mobile Computing*, vol. 19, no. 9, pp. 2174–2188, Sep. 2020, doi: 10.1109/TMC.2019.2921765.
[25] Z. Xie, S. Dang, and Z. Zhang, "On convergence probability of direct acyclic graph-based ledgers in forking blockchain systems," *IEEE Systems Journal*, vol. 17, no. 1, pp. 1121–1124, Mar. 2023, doi: 10.1109/JSYST.2022.3201777.
[26] J. Liang, J. Wang, G. Yu, W. Guo, C. Domeniconi, and M. Guo, "Directed acyclic graph learning on attributed heterogeneous network," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 10, pp. 10845–10856, Oct. 2023, doi: 10.1109/TKDE.2023.3266453.
[27] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019, doi: 10.1109/TIA.2019.2919820.
[28] F. Chen, H. Jia, K. Liu, W. Tang, J. Zhu, and W. Guo, "A new attack method for malicious nodes in tangle network," in *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, IEEE, Nov. 2020, pp. 84–87. doi: 10.1109/SmartCloud49737.2020.00024.
[29] A. Kumari and I. Sharma, "Augmentation of internet of things security and privacy with IOTA tangle network," in *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*, IEEE, Oct. 2023, pp. 1–5. doi: 10.1109/gcat59970.2023.10353394.
[30] G. Li, Q. Zhao, M. C. Zhou, and H. Liang, "An on-chain smart contract protocol for tangle," in *ICNSC 2022 - Proceedings of 2022 IEEE International Conference on Networking, Sensing and Control: Autonomous Intelligent Systems*, IEEE, Dec. 2022, pp. 1–5. doi: 10.1109/ICNSC55942.2022.10004163.
[31] X. Tang, J. Zhou, Y. Qiu, X. Liu, Y. Shi, and J. Zhao, "One edge at a time: a novel approach towards efficient transitive reduction computation on DAGs," *IEEE Access*, vol. 8, pp. 38010–38022, 2020, doi: 10.1109/ACCESS.2020.2975650.
[32] H. T. Zhang, Z. Chen, and X. Mo, "Effect of adding edges to consensus networks with directed acyclic graphs," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4891–4897, Sep. 2017, doi: 10.1109/TAC.2017.2692527.
[33] J. Chen, Y. Yang, C. Wang, H. Zhang, C. Qiu, and X. Wang, "Multitask offloading strategy optimization based on directed acyclic graphs for edge computing," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9367–9378, Jun. 2022, doi: 10.1109/JIOT.2021.3110412.
[34] Z. Chen and Z. Ge, "Directed acyclic graphs with tears," *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 4, pp. 972–983, Aug. 2023, doi: 10.1109/TAI.2022.3181115.
[35] V. Krishnamurthy and M. Hamdi, "Mis-information removal in social networks: Constrained estimation on dynamic directed acyclic graphs," *IEEE Journal on Selected Topics in Signal Processing*, vol. 7, no. 2, pp. 333–346, Apr. 2013, doi: 10.1109/JSTSP.2013.2245630.
[36] S. Cho, T. Elhourani, and S. Ramasubramanian, "Independent directed acyclic graphs for resilient multipath routing," *IEEE/ACM Transactions on Networking*, vol. 20, no. 1, pp. 153–162, Feb. 2012, doi: 10.1109/TNET.2011.2161329.
[37] S. Arora, H. Singh, M. Sharma, S. Sharma, and P. Anand, "A new hybrid algorithm based on grey wolf optimization and crow search algorithm for unconstrained function optimization and feature selection," *IEEE Access*, vol. 7, pp. 26343–26361, 2019, doi: 10.1109/ACCESS.2019.2897325.
[38] A. J. Rabash, M. Z. A. Nazri, A. Shapii, and M. K. Hasan, "Non-dominated sorting genetic algorithm-based dynamic feature selection for intrusion detection system," *IEEE Access*, vol. 11, pp. 125080–125093, 2023, doi: 10.1109/ACCESS.2023.3328395.
[39] B. Ahadzadeh, M. Abdar, F. Safara, A. Khosravi, M. B. Menhaj, and P. N. Suganthan, "SFE: a simple, fast, and efficient feature selection algorithm for high-dimensional data," *IEEE Transactions on Evolutionary Computation*, vol. 27, no. 6, pp. 1896–1911, Dec. 2023, doi: 10.1109/TEVC.2023.3238420.
[40] Y. Yin and L. Wei, "Hyperspectral image classification using comprehensive evaluation model of extreme learning machine based on cumulative variation weights," *IEEE Access*, vol. 8, pp. 187991–188003, 2020, doi: 10.1109/ACCESS.2020.3030649.
[41] H. M. Salih and R. S. Al Mahdawi, "The security of RC4 algorithm using keys generation depending on user's retina," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 1, pp. 452–463, Oct. 2021, doi: 10.11591/ijeecs.v24.i1.pp452-463.
[42] C. Jie, L. A. Prashanth, M. Fu, S. Marcus, and C. Szepesvári, "Stochastic optimization in a cumulative prospect theory framework," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 2867–2882, Sep. 2018, doi: 10.1109/TAC.2018.2822658.
[43] H. Abdullah and A. H. Ibrahim, "Blockchain technology opportunities in kurdistan, applications and challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 405–411, Apr. 2019, doi: 10.11591/ijeecs.v18.i1.pp405-411.
[44] N. Tripathy, S. Hota, and D. Mishra, "Performance analysis of bitcoin forecasting using deep learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1515–1522, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1515-1522.
[45] A. Houria, B. M. Abdelkader, and G. Abderezzak, "A comparison between the secp256r1 and the koblitz secp256k1 bitcoin curves," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 3, pp. 910–918, Mar. 2019, doi: 10.11591/ijeecs.v13.i3.pp910-918.
[46] L. Van Der Horst, K. K. R. Choo, and N. A. Le-Khac, "Process memory investigation of the bitcoin clients electrum and bitcoin core," *IEEE Access*, vol. 5, pp. 22385–22398, 2017, doi: 10.1109/ACCESS.2017.2759766.
[47] N. Aljojo, A. Alshutayri, E. Aldhahri, S. Almandeel, and A. Zainol, "A nonlinear autoregressive exogenous (NARX) neural network model for the prediction of timestamp influence on bitcoin value," *IEEE Access*, vol. 9, pp. 148611–148624, 2021, doi: 10.1109/ACCESS.2021.3124629.
[48] N. Tovanich, N. Soulie, N. Heulot, and P. Isenberg, "The evolution of mining pools and miners' behaviors in the bitcoin blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3633–3644, Sep. 2022, doi: 10.1109/TNSM.2022.3159004.

[49] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, “Tangle the blockchain:towards connecting blockchain and DAG,” in *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, IEEE, Oct. 2021, pp. 63–68. doi: 10.1109/WETICE53228.2021.00023.
[50] F. Guo, X. Xiao, A. Hecker, and S. Dustdar, “Characterizing IOTA tangle with empirical data,” in *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322220.

BIOGRAPHIES OF AUTHORS

Eugene Rhee received the Ph.D. degree in electronics from Hanyang University, Korea, in 2010. He was a visiting professor at Chuo University, Japan from 2010 to 2011. Since 2012, he has been with Sangmyung University, Korea, where he is currently a full professor in the Department of Electronic Engineering. His research area includes microwave, electromagnetic compatibility, electromagnetic interference, and reverberation chamber. He can be contacted at email: eugenerhee@smu.ac.kr.

Jihoon Lee received B.S., M.S, and Ph.D. degrees in electronics engineering from Korea University in 1996, 1998, and 2001, respectively. From 2002 to 2011, he worked at Samsung Electronics as a senior research member. He is currently a full professor in the Department of Smart Information and Telecommunication Engineering, Sangmyung University, Korea. His research interests include edge computing, secure M2M, and network security. He can be contacted at email: vincent@smu.ac.kr.