Understanding Characteristics and System Implications of DAG-Based Blockchain in IoT Environments

Tianyu Wang, Qian Wang, Zhaoyan Shen, Zhiping Jia, and Zili Shao

***Abstract*—Blockchain is starting to be deployed in the Internet of Things (IoT) to enable autonomous device-to-device transactions. However, traditional block-based blockchain techniques, such as Bitcoin and Ethereum, are not suitable for IoT environments due to their low throughput, high computation overhead, and costly transaction fee. To satisfy the requirements of IoT environments, directed-acyclic-graph (DAG)-based approaches, aiming to provide cheap blockchain services with low latency and high throughput, are emerging. This article presents a set of comprehensive experimental studies on IOTA, a representative DAG-based blockchain. We aim to exhibit its unique characteristics mainly from three aspects: 1) performance; 2) security; and 3) system robustness. We have developed a series of benchmark tools and judiciously selected typical configurations to perform experimental examinations with a real private IOTA network. Our studies reveal several interesting findings: 1) the throughput of IOTA is higher than the traditional block-based blockchain but far less than the reported thousands of transactions per second (TPS) in its whitepaper, even with scaling-up configurations; 2) the database query heavily impacts the performance of IOTA, even more than its mining [i.e., Proof of Work (PoW)] process; and 3) the system robustness of IOTA is closely related to the frequency of the incoming transactions while the milestone sent by the centralized coordinator has little effect on the system robustness. We make our benchmark tools public and expect our works can inspire system architects, application designers, and practitioners with new optimization directions and potential application cases for further exploration.**

***Index Terms*—Benchmark tool, Internet-of-Things (IoT) blockchain, performance evaluation.**

Manuscript received 29 December 2020; revised 17 April 2021 and 25 July 2021; accepted 19 August 2021. Date of publication 30 August 2021; date of current version 8 August 2022. This work was supported in part by the National Science Foundation for Young Scientists of China under Grant 61902218; in part by the National Natural Science Foundation of China under Grant 92064008; in part by the Research Grants Council of the Hong Kong Special Administrative Region, China, under Grant GRF 15224918; and in part by Direct Grant for Research, The Chinese University of Hong Kong under Project 4055151. This article was presented in part at the 16th IEEE International Conference on Embedded Software and Systems (ICESS 2020, Best Paper Award) [DOI: 10.1109/ICESS49830.2020.9301563]. *(Corresponding author: Zhaoyan Shen.)*

Tianyu Wang is with the Department of Computer Science and Technology, Shandong University, Qingdao 266000, Shandong, China, and also with the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: tywang@cse.cuhk.edu.hk).

Qian Wang, Zhaoyan Shen, and Zhiping Jia are with the Department of Computer Science and Technology, Shandong University, Qingdao 266000, Shandong, China (e-mail: daisy_seven@163.com; shenzhaoyan@sdu.edu.cn; jzp@sdu.edu.cn).

Zili Shao is with the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: shao@cse.cuhk.edu.hk).

Digital Object Identifier 10.1109/JIOT.2021.3108527

I. Introduction

INTERNET-OF-THINGS (IoT) devices, in which objects or "things" are augmented with computation and communication capabilities, are increasingly utilized in our daily life [2]–[5]. For instance, there have been over 20 billion IoT devices by 2020, and the number may reach up to 50 billion by 2025 [6], [7]. It becomes important to enable device-to-device transactions such as machine-to-machine (M2M) micro-payments [8]–[11]. With great potential to enable M2M transactions in a more secure and trusted way, blockchain technologies gain great attention from both industry and academia [12]–[16], in which based on a decentralized architecture, transactions are added through a mining process and maintained in a tamper-resistant distributed ledger. As blockchain techniques are starting to be deployed in IoT environments [8], it becomes important to investigate their characteristics and system implications.

In an IoT environment, in order to support massive autonomous M2M transactions for data exchange and processing while assuring data security and operation accountability, high transaction speed, and lightweight consensus mechanisms are required [3], [7], [17]. Traditional block-based blockchain technologies, such as Bitcoin [18] and Ethereum [19], cannot be directly deployed in the IoT environment because they: 1) suffer from low transactions per second (TPS), varying from several to dozens [20], which is far less than the requirement of thousands of TPS in an IoT environment [21], [22]; 2) involve a resource-hungry mining process—Proof of Work (PoW), for which resource-constrained IoT devices may lack sufficient computation power to operate; and 3) require a costly transaction fee for transaction confirmation, which is too expensive for IoT environments with massive small-value transactions among IoT devices.

To address the above issues, directed-acyclic-graph (DAG)-based blockchain techniques are gaining more interest in the distributed ledger field for IoT environments. IOTA is one of the representative techniques and utilizes a DAG structure, called Tangle [8], to organize transactions. For example, as Fig. 1 shows, in a DAG, each node is a transaction, and clients issue all the transactions through a selective PoW process. Leaf nodes (i.e., transactions that have not been approved by latter transactions) are called tips. For a transaction insertion, it must select and approve two tips. During the tip selection and approval process, a random walking algorithm is used to

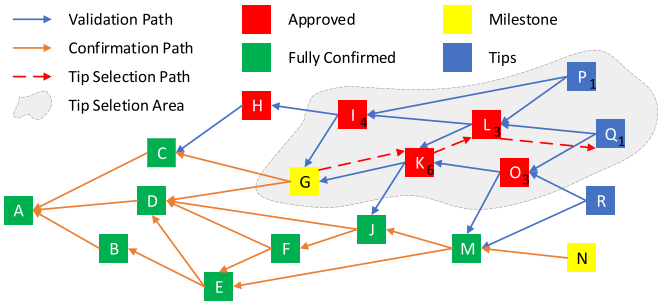


Fig. 1. Tangle in a full node.

choose tips for approval, and a transaction validation algorithm is performed to verify the transactions along the validation path to avoid double-spending. Benefited from this self-propagated process (i.e., the latter transaction helps verify two former transactions), theoretically, the system throughput of IOTA depends on the incoming transaction frequency. The higher the frequency is, the higher the throughput achieves, which can even reach thousands of TPS [22].

Different from the well-benchmarked block-based blockchain systems, more investigations are needed to understand the characteristics and system implications of DAG-based blockchain systems. In this article, we carry out a set of comprehensive experimental studies on IOTA and attempt to gain insights into its unique characteristics. We first build a private IOTA network with typical configurations and then develop a series of benchmark tools that have been released to the public [1] to explore the system characteristics. We examine IOTA from three aspects: 1) performance; 2) security; and 3) system robustness. Our results reveal the following facts.

1) With the scale-up of IOTA, its throughput is higher than the traditional block-based blockchain systems but far less than the reported thousands of TPS. Through analyzing the transaction latency, we find that although PoW and tip selection are time-consuming, database queries are the major bottleneck.
2) IOTA effectively provides IoT security by defending against various attacks, such as the double-spending attack and the off-syncing attack. While these attacks can be detected, how fast they can be detected and their impacts on the system performance deserve further investigation.
3) The system robustness of IOTA is closely related to the frequency of the incoming transactions. Meanwhile, the milestone sent by the centralized coordinator has little effect on system robustness.

We have released our benchmark tools and all the evaluation setups to the public. We expect that our work can inspire system architects, application designers, and practitioners with new optimization directions for further exploration.

The remainder of this article is organized as follows. Section II introduces the background about two types of blockchains and our motivation. Section III presents the experimental setup and environment. Then, we provide our experimental results and the key observations in Section IV. In Section V, we discuss the system implications to system architects and application designers. Related works are presented in Section VI, and Section VII concludes this article.

II. Background and Motivation

A. IoT Environment

In an IoT environment, IoT devices, such as sensors and embedded controllers are connected through IoT technologies [24], [25]. To support the communication requirement between a large number of IoT devices, M2M message becomes one of the basic technologies for IoT [11]. Recently, as the privacy and security issues of IoT become more and more important [26]–[28], the blockchain technology, with its great potential to enable M2M transactions in a more secure and trusted way, has gained a lot of interest from both industry and academia [29], [30]. Specifically, in a blockchain, with its decentralized architecture, M2M transactions can be added to blocks through a mining process and maintained in a tamper-resistant distributed ledger.

However, different from other peer-to-peer applications like cryptocurrency, an IoT environment raises particular challenges for secure M2M transactions as follows. First, to support massive autonomous M2M transactions for data exchange and processing, it requires much higher throughput, e.g., thousands TPS [21], [22]. Second, many IoT devices are resource-constrained and lack sufficient computation power to process resource-hungry consensus protocol such as PoW. Third, for M2M communications, it is important to support low cost (or zero cost) transactions (called microtransaction). High transaction fees will severely limit the usage of blockchains in IoT environments [11].

DAG-based blockchains are emerging as a promising direction to tackle the above challenges. Different from traditional block-based blockchains, in which the throughput is limited with fixed parameters (e.g., block size and block interval), a DAG-based blockchain organizes all transactions in a DAG structure. Without block-based limitations, it can achieve higher throughput. Moreover, lightweight consensus protocols in DAG-based blockchains avoid resource-hungry computation, so they are suitable for resource-constrained IoT devices. Finally, transactions with a DAG structure can be self-propagated, which can help reduce transaction fees. Thus, microtransactions in IoT environments can be efficiently supported.

B. Block-Based Blockchain

Traditional block-based blockchain systems, such as Bitcoin [18] and Ethereum [19], utilize a distributed public ledger technology that stores transactions with a linked list of blocks. Blocks are generated and shared over the entire blockchain network to defend against system failure, data manipulation, and cyber attacks [31], [32]. These systems generally adopt a mining process (e.g., PoW, which requires solving a computation and energy-hungry puzzle) [33] to generate new blocks. A newly generated block will be broadcast

to the whole network to achieve consensus. The mining process heavily limits the scalability of block-based blockchain systems and makes them suffer from low throughput. For example, the throughput of Bitcoin and Ethereum are only tens per second. Besides, every transaction is carried out with a certain transaction fee, and the transaction fee is expensive and keeps increasing.

There are currently two major approaches to improving the throughput of the block-based blockchain systems: 1) accelerating the block generation time and 2) enlarging the block size. Accelerating the block generation time means decreasing the nonce accuracy during the mining process, which will sacrifice the blockchain system's security. Besides, this approach increases the possibility that multiple miners solve the PoW puzzle simultaneously, aggravating the blockchain forks. For the second approach, a larger block size requires longer generation time and broadcasting time across the network. Thus, this approach only achieves slight improvement in system throughput [14], [34]. All these disadvantages make it hard to apply the block-based blockchain in IoT environments.

C. DAG-Based Blockchain

DAG-based blockchains provide a promising solution to enable secure autonomous transactions in IoT environments [8], [35]. Instead of packing transactions into a linked block list, a DAG-based blockchain maintains transactions with the DAG structure. In this article, we use IOTA to illustrate its working principle. IOTA has been applied in multiple industrial environments, such as healthcare and smart sensing [11], [36]–[38]. The DAG structure of IOTA is called Tangle, in which each node is a transaction. Leaf nodes of Tangle (i.e., transactions that have not been approved) are called tips. For a transaction to be added to Tangle, it must select and approve two tips and do a light-weighted PoW to complete the attached transaction. The whole Tangle is stored in full nodes that running the IOTA reference implementation (IRI) service. Other participators that launch transactions are called light nodes.

Fig. 1 shows the snapshot of a Tangle in a full node. In IOTA, transactions are issued by light nodes and attached to the Tangle through a selective PoW process, which includes tip selection and validation processes. For example, in Fig. 1, Q is a newly attached transaction (i.e., a tip), L and O are two old tips approved by Q. The tip selection process uses a Markov Chain Monte Carlo (MCMC) algorithm to perform a random walking on the DAG. The algorithm begins with a former milestone (e.g., G). Then, based on probability, it selects another transaction that approves it (the chosen probability of each approver is relative to its accumulated weight—the number on the node's bottom right indicating how many transactions have approved it directly or indirectly). The algorithm stops until it reaches a tip and is performed twice for another tip selection. After that, the newly attached transaction needs to verify the transactions approved by these two selected tips recursively (along the validation path) until a fully confirmed transaction. When a transaction has been verified by a predefined large number of transactions or indirectly approved by a milestone (a transaction with a significant weight issued by the IOTA foundation), it becomes fully confirmed. Once a new transaction is attached to the DAG, the full node will synchronize the updated DAG to its neighbors to promise the Tangle's consistency.

As reported by the IOTA foundation [39], it can satisfy the requirement of an IoT environment since its performance is related to the number of users. That is, the more incoming truncations served, the higher throughput it achieves. Specifically, a higher incoming transaction frequency will accelerate approving tips and speed up the transaction confirmation process. However, in IOTA, in the beginning, it will take a long time for transactions to be confirmed if there are not enough users. Thus, the IOTA foundation maintains a centralized coordinator sending milestones (yellow nodes in Fig. 1) to confirm those tips periodically. Tips directly or indirectly approved by milestones will be confirmed immediately. The frequency of sending milestones is vitally crucial for the latency of confirming those transactions.

D. Motivation

Currently, block-based blockchain systems, such as Bitcoin and Ethereum, have been well investigated, and many works have been performed for benchmarking these systems. For instance, Pongnumkul *et al.* [40] conducted a performance analysis of Hyperledger Fabric and Ethereum in terms of execution time, latency, and throughput, to provide adoption hints of the blockchain technology in their IT systems. Dinh *et al.* [41] developed an evaluation framework for analyzing private blockchains, serving a fair way for comparing different platforms, and enabling a deeper understanding of different system design choices. Baliga *et al.* [42] characterized the performance features of Quorum, a permissioned blockchain platform built from the Ethereum codebase. They use several micro-benchmarks to study the throughput and latency characteristics of Quorum. Gervais *et al.* [16] introduced a novel quantitative framework to compare PoW blockchains objectively. They characterize different PoW blockchains and evaluate their performance and security.

However, due to the lack of well-designed evaluation tools, DAG-based blockchains need more investigation. Thus, based on IOTA, we develop a series of benchmark tools and aim to exhibit its intrinsic characteristics in this article.

In this work, we strive to explore and understand the intrinsic characteristics of IOTA by answering the following questions.

1) How are the performance characteristics of IOTA, including throughput, latency, and scalability?
2) How robust for IOTA to defend against security attacks such as double-spending? What will happen if one of the full nodes is attacked and off synced from the whole network?
3) The shape of the Tangle reflects the system robustness of IOTA. What factors will influence the shape (robustness) of the Tangle?
4) How milestones influence IOTA, including performance, security, and system robustness?

Fig. 2. Private IOTA blockchain network.

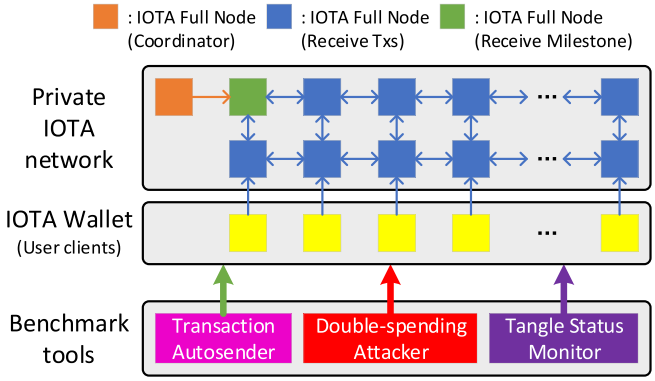


Fig. 3. Private IOTA system architecture.

III. Measurement Environment

In this work, we develop a series of IOTA benchmark tools, mainly including three parts: 1) an automatic transaction initiator; 2) a real-time status monitor; and 3) a double-spending attacker. We implement our automatic transaction initiator with multithreading *NodeJS*, utilizing APIs provided by the IOTA foundation. Each initiator will automatically send transactions with the preconfigured sender's seed and receiver's address. The monitor is implemented with *Golang* for high performance. All the tools have been released to the public [23].

The evaluations are performed based on a distributed private IOTA blockchain network. We have recorded the shape of the IOTA Tangle after running IOTA for three days (the Tangle graphic view can be found at).[1] In our environment, the network consists of 35 Intel next unit of computings (NUCs), and each NUC is equipped with i5-6200u CPU, 4-GB DDR3 memory, and 128-GB NVMe storage. Fig. 2 shows the private IOTA blockchain system.

The NUCs are divided into several roles. As edge devices can choose to participate in all transaction certifications (as a full node) or not (as a light node), to simulate it, one NUC is used as a coordinator to send milestones to the private IOTA network (the orange one in Fig. 3), while the others perform as full nodes (the blue ones) or clients (the yellow ones). All the clients are installed with our automatic transaction initiator (the pink module) to continuously initiate transactions and send them to the whole IOTA network in a configured frequency. All the full nodes are equipped with IRI 1.5.5 (IRI, version 1.5.5) to receive and handle those transactions. Thus, we can adjust the whole IOTA network's load by simply increasing or decreasing the number of clients.

As Fig. 3 shows, a real-time status monitor is installed on an NUC to monitor all changes of transaction status (the purple module), from *tips* to *approved* then *confirmed* ones, and record the latency including inherent and confirmation latencies. The real-time status monitor also collects the CPU and memory usage for performance analysis and the tip/confirmed transaction ratio for system robustness analysis.

Because both receiving milestone transactions and broadcasting transaction status will occupy resources in the IOTA full nodes, we separate one full node (the green one) from the other full nodes to serve as the milestone receiver and the status broadcaster. Thus, we can isolate its influence on the other full nodes.

One NUC is selected from all the clients to serve as a double-spending attacker (the red module) by maliciously sending two transactions using the same amount of money. By monitoring all the IOTA full nodes' status, we can observe the behavior after the full node detects the double-spending attack—one of the major security issues in a private IOTA network.

In this work, we configure the private IOTA system with several typical setups, including the different number of full nodes, clients, and milestone intervals, and judiciously evaluate the representative DAG-based blockchain system from three aspects: 1) performance; 2) security; and 3) system robustness.

IV. Experimental Examination

A. Performance

Throughput: The system throughput indicates how many transactions the blockchain network can handle per second. We evaluate the system throughput with both a single full node and multiple full nodes scenarios. When testing the system throughput, we gradually increase the incoming transaction speed (TPS).

Fig. 4(a) shows the system throughput when there is only one full node. When the incoming transaction speed is less than 15, the system can easily accommodate all incoming transactions. Thus, the system throughput is equal to the incoming transaction speed. Once the incoming transaction speed exceeds 15, the system throughput is bounded to 16 TPS. This phenomenon is because when attaching a transaction to the Tangle, both memory and computation resources are required from the full node, as described in Section II-C. Thus, when there is only one full node, with the increment of the incoming transaction speed, the resources of the full node will finally run out, and the system throughput is limited to 16 TPS.

We further evaluate the system throughput by configuring the system with multiple full nodes. In this test, we fix each

[1]IOTA Tangle graphical view: https://www.youtube.com/channel/UCj0muwSgKr2bn2BybLkw3kQ.

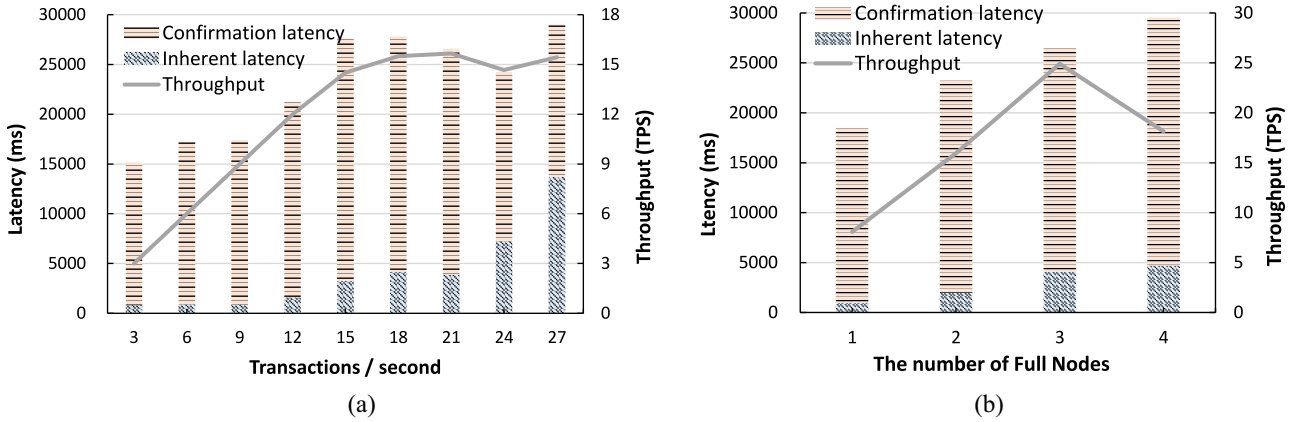


Fig. 4. Latency and throughput in different configurations. (a) Single full node. (b) Multiple full nodes.

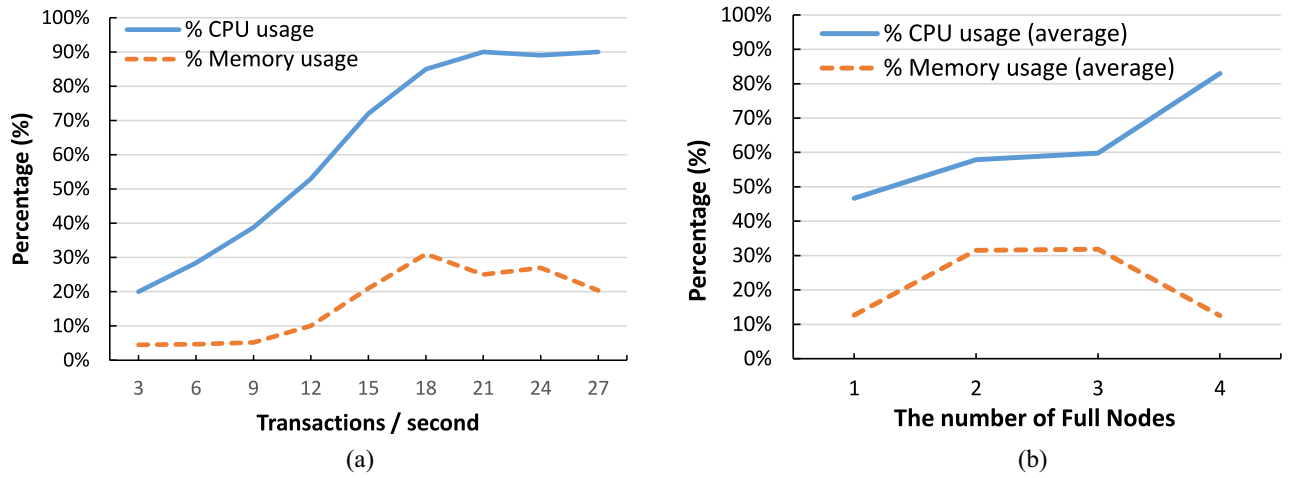


Fig. 5. Resource usage in different configurations. (a) Single full node. (b) Multiple full nodes.

full node to receive eight incoming TPS and then increase the full node number to test the private IOTA network's scalability. The results are as shown in Fig. 4(b). It can be observed that the highest system throughput is about 25 TPS when there are three active full nodes and drops back a little with four active full nodes. The reason that limits the system throughput is the network synchronization overhead. When a new transaction is attached to the Tangle, it needs to be synchronized to all the full nodes. Thus, although we can add more full nodes to handle more transactions, the system throughput is still limited.

Latency: The system latency can be divided into two parts: one part is the time from the transaction initialization to it is attached to the Tangle; at that time, another part of latency begins counting until the transaction has been confirmed. We name the former one as *inherent latency* and the latter one as *confirmation latency*. Both two latencies are evaluated as follows.

Inherent Latency: In the single full node scenario, the trend between the latency and the incoming transaction speed is shown in Fig. 4(a). With the increment of the incoming transaction speed, the inherent latency increases correspondingly. When the throughput reaches its upper bound, the inherent latency boosts to an extremely high level as the incoming transaction speed increases. We will further analyze the inherent latency later to obtain how much latency that each task consumes.

For the multiple full nodes environment, the results are as shown in Fig. 4(b). When we activate three full nodes, its throughput reaches the upper bound while the inherent latency increases. It represents that the computation resources in the full nodes are running out. When four full nodes are activated, the throughput declines while the latency continues increasing. Overall, the peak throughput cannot be further improved.

Confirmation Latency: Presently, IOTA still depends on milestones to confirm transactions, so we fix the milestone interval to 20 s during the whole test. As shown in Fig. 4(a), the confirmation latency slowly increases when the incoming transaction speed rises. The total latency reaches the maximum at 18 TPS, but it drops back slightly when the incoming transaction speed further increases. We measure each incoming transaction's confirmation latency and draw the distribution diagram in Fig. 6 to analyze this phenomenon in terms of tip selection and validation.

Analysis: Fig. 5(a) shows the resource usage in the single full node scenario. When we continue increasing the incoming transaction speed, the CPU usage of the full node increases rapidly. It exceeds 90% when the incoming transaction speed

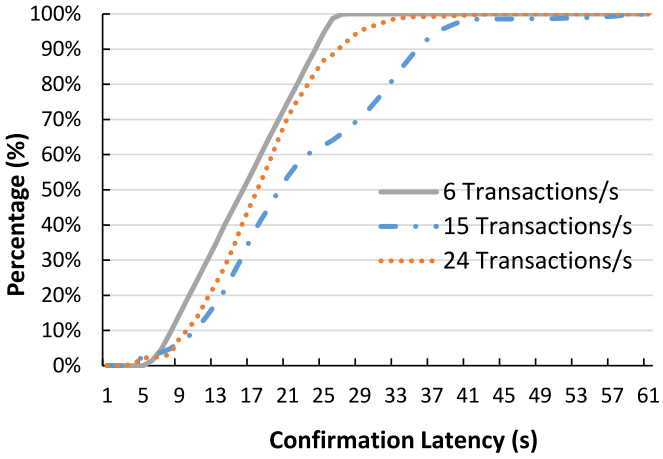


Fig. 6. Distribution of the confirmation latencies.

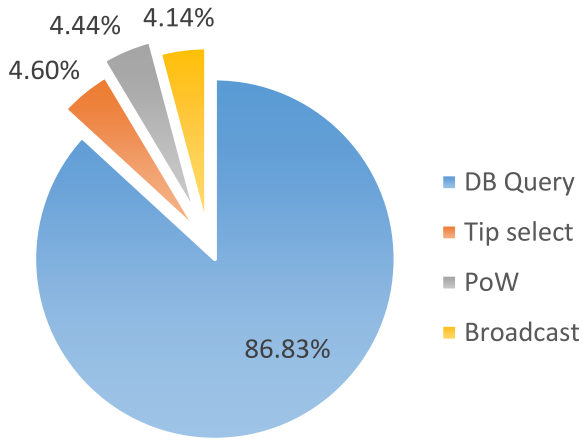


Fig. 7. Inherent latency composition.

reaches 18 TPS. The computation resource becomes the bottleneck which vitally limits its performance. Combining Fig. 4(a) for analysis, the throughput stops increasing when the incoming transaction speed reaches 18 TPS, exactly matching the CPU usage shown in Fig. 5(a). However, the full node's memory usage does not exceed 30%, which reveals that the tasks running in the full node are not memory intensive.

As Fig. 5(b) shows, although the CPU usage of one full node is not too high at the beginning, with the full node number increases, the average CPU usage of each full node also increases. Since we do not increase the incoming transaction speed of one full node, the increase in CPU usage is mainly due to the communication cost. Once a full node receives a transaction, it needs to broadcast the transaction to all the other full nodes in the whole private IOTA network, which is a costly process. Thus, both the computation-intensive tasks and the network communication cost influence the private IOTA network's throughput by consuming its full nodes' computation resources, limiting the system throughput to less than 30 TPS.

The confirmation latency is highly related to the milestone interval. Because the random walk process starts at three milestones ago, the confirmation latency cannot exceed triple the milestone interval (i.e., 60 s). During the tip selection process, it chooses the next transaction based on the trust value of transactions. The more transactions connected behind this transaction, the higher trust value this transaction will get, making it more likely to be chosen at the next step of the random walk algorithm. A milestone is trusted due to its centralization, maintaining a significantly higher trust value than all other transactions. Suppose there are many tips connected to the Tangle simultaneously with a milestone. In that case, all these tips are less likely to be approved by following tips because they prefer connecting to the milestone more.

For the confirmation latency, it is worth noting that we only count valid records. That is, the transactions with infinite confirmation latency will not be recorded. Fig. 6 shows the distribution of the confirmation latency from each transaction. The confirmation latency linearly increases when the incoming transaction speed is 6. However, when the incoming transaction speed increases to 15, the confirmation latency distribution is divided into two stages: 1) 9–25 s and 2) 29–41 s. This distribution is mainly due to the lack of computation resources in the single full node, which will cause a transaction to be blocked until the second or the third milestone comes. All those transactions with the confirmation latency ranged from 29 to 41 s are the blocked ones. If the incoming transaction speed further increases, the average confirmation latency begins to drop back. It seems good, but actually, it sacrifices the stability of the Tangle. With the increasing number of blocked transactions, the milestone can only confirm a fraction of those transactions, leaving many transactions not confirmed forever. Therefore, these transactions will have an infinite confirmation latency; as they are not valid records, the confirmation latency distribution at 24 TPS does not include those isolated transactions.

Bottleneck: According to the previous works [39], [43]–[47], during the whole transaction initialization process, the most costly parts are the tip selection and the validation processes, both of which are handled by the full nodes. When the incoming transaction speed increases, the full nodes will become too busy to handle these tasks incurred by incoming transactions. However, except for those two tasks, we find another annoying factor that greatly impacts the performance.

Fig. 7 shows the composition of the inherent latencies of the transactions. We can see that the bottleneck of initiating a transaction is neither the tip selection process nor the validation process but database queries. In IOTA, during the transaction initiation period, one address can only be used once. Thus, it needs a unique address checking process to check if an address has been used before. IOTA implements this process by reading all transactions from the database and checking if the specific address has been used. As the database size grows larger and larger, this query process consumes more and more time, which severely: 1) degrades the full nodes' performance; 2) makes the inherent latency continue increasing; and 3) limits the private IOTA network's throughput. To the best of our knowledge, this is the first time that the database query cost is evaluated and identified as the performance bottleneck in the private IOTA network.

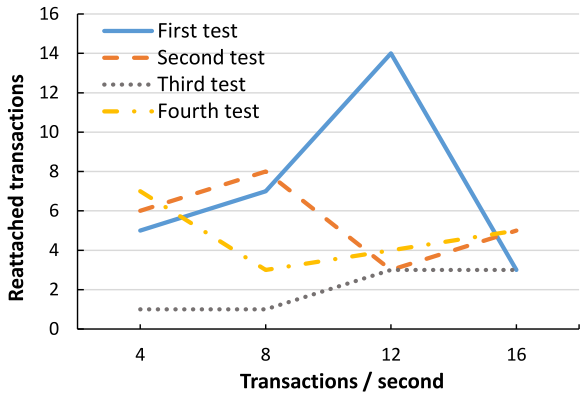


Fig. 8. Reattached transactions in the double-spending attack.

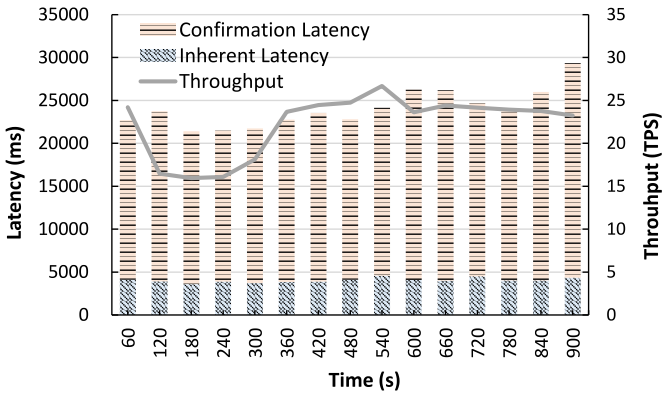


Fig. 9. Performance during the off-syncing attack.

B. Security

To evaluate the private IOTA network's security, we have simulated two types of attacks, double-spending, and off syncing. Double-spending means that one user tries to spend the same amount of money twice with two different receivers. Off syncing is a consistency attack by which attackers attempt to make one of the full nodes offline, thus creating an inconsistency among the full nodes. The evaluation results for these two types of attacks are shown as follows.

Double-Spending Attack: According to the white paper of IOTA [8], it can detect the double-spending attack and remove illegal transactions from the Tangle. To examine this, for the double-spending attack, we directly send two transactions spending the same amount of money and wait until the full nodes detect the attack. There will be many transactions connecting to the illegal transaction before the double-spending attack is detected. Those transactions need to be removed together with the illegal transaction. The later a double-spending attack is detected, the more transactions it will influence. Thus, we record the number of transactions which need to be reattached to the Tangle due to the double-spending attack (the y-axis) with different incoming transaction speed (x-axis). The results are shown in Fig. 8.

It can be observed that the results are not related to the incoming transaction speed. The double-spending attack can be detected once a transaction is directly or indirectly attached to both the two double-spending transactions. Then, one of the two double-spending transactions will be marked as illegal and removed from the Tangle. According to the results, the time of detecting the double-spending attack is uncertain, and the number of transactions influenced by the double-spending attack is ranged from 1 to 14. We have observed no more than 14 transactions to be influenced during the whole test, revealing that the private IOTA network can detect the double-spending attack. However, how can a double-spending attack be detected faster and its impact on the system performance need further investigation.

Off-Syncing Attack: The private IOTA network has several full nodes providing service to user clients. Each full node stores the whole Tangle, and all of the full nodes need to be maintained in a consistent status. However, suppose one of them suffers from attacks and is not synchronized with the whole network. In that case, the system performance will be degraded, as shown in the performance experiment results in Section IV-A. When the nonsynchronized full node rejoins the network, the synchronization process will restart, which will incur more performance overhead. To simulate the off-syncing attack situation, we activate three full nodes that work normally and turn off one full node in the cluster. We continue monitoring the performance during off-syncing and resyncing periods. The results are shown in Fig. 9.

We fix each full node to receive eight incoming TPS and wait until the Tangle reaches stable status. Then, we shut down one full node at 60 s and restart it at 120 s. Meanwhile, we clean the off-synced full node's database, thereby maximizing the number of resynced transactions. We repeat the test three times and then take the average throughput data for analysis. As expected, at 60 s, the throughput suddenly drops down from 24 to 16 TPS. At 120 s, the number of transactions to be resynced is about 4200. The throughput maintains low until 300 s, and it climbs back to about 24 TPS at 360 s, representing that the synchronization process is accomplished. Although the private IOTA network suffers from a throughput degradation, its performance only takes around 240 s to bounce back to the normal level. After all the full nodes are synchronized at 480 s, the private IOTA network continues providing service normally.

We can see that both the confirmation latency and inherent latency are stable during the whole experiment, revealing that the private IOTA network is stable during the whole test. With continuous service, the recovery speed is about 23 TPS (using 180 s to recover 4200 transactions), which is acceptable compared to its normal performance.

C. System Robustness

Tip Ratio and Confirmed Transaction Ratio: The system robustness of IOTA is highly related to its tip ratio and confirmed transaction ratio. Tips represent newly attached transactions, whose ratio should be stable in a healthy private IOTA network. If the tip ratio continues increasing, it represents that too many transactions attach to the stale state of the Tangle or wait to be processed. Under this condition, if the incoming transaction speed is still high, the full nodes will finally crash.

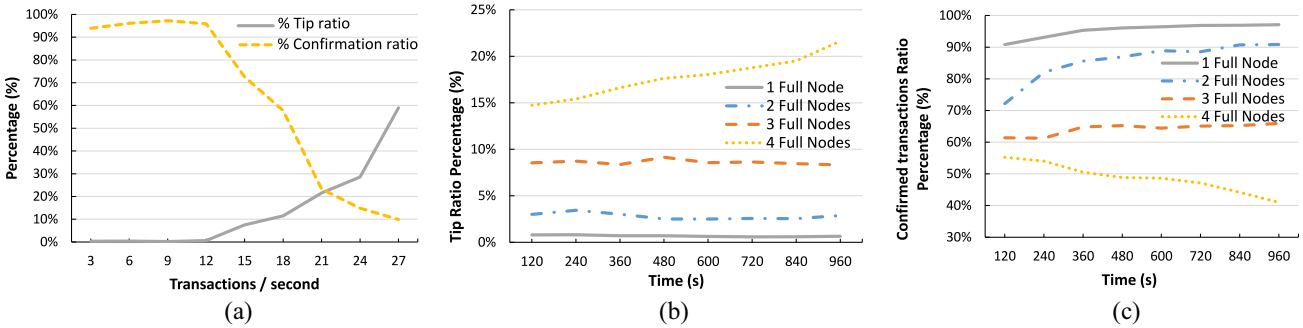


Fig. 10. System robustness with different configurations. (a) Single full node. (b) Tip ratio in multiple full nodes. (c) Confirmation ratio in multiple full nodes.

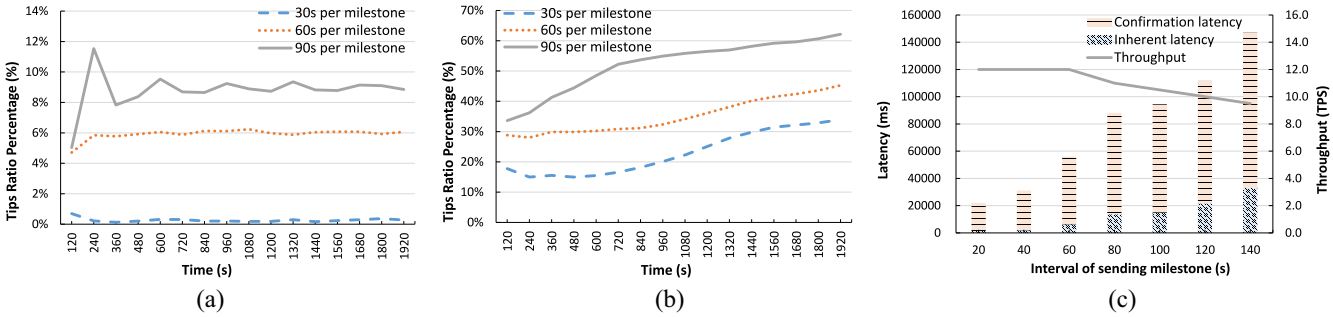


Fig. 11. Influence with different milestone intervals. (a) Tip ratio with eight incoming TPS. (b) Tip ratio with 16 incoming TPS. (c) Performance.

We monitor the tip ratio in each test and observe several unstable situations which might cause the full nodes crashing. Fig. 10(a) shows the condition of the single full node scenario. The *x*-axis shows the incoming transaction speed. We can see that when we increase the incoming transaction speed to 24, the tip ratio boosts to an extremely high level, while the confirmed transaction ratio decreases to less than 20%. At that time, the full node is already overloaded. Suppose we keep the workload at such intensity for a while. In that case, the whole IOTA network will crash, rejecting all the incoming transactions, which severely damages the system robustness of the private IOTA network.

For the multiple full node scenarios, we fix each full node's incoming transaction speed at 8. Fig. 10(b) and (c) reveal the tip ratio and confirmed transaction ratio with different configurations. It can be observed that when there are less than four full nodes activated, the tip ratio maintains relatively low while the confirmed transaction ratio is kept high. It reveals that the Tangle is in a very healthy state. However, with four full nodes, the situation is different. The tip ratio starts at around 15% at 120 s and rises to more than 20% at 960 s with a continuously increasing trend. The confirmed transaction ratio drops from more than 50% to around 40%. As time goes by, the full nodes become unstable and finally crash.

The result exhibits that when a full node does not struggle to deal with the incoming transactions, the private IOTA network's health can remain at a relatively normal status. Nevertheless, once the full nodes run out of resources, there will be more and more incoming transactions waiting to be processed, which will finally cause a system crash.

Milestone Interval: Another critical factor that will influence the tip ratio is the milestone interval. According to the confirmation mechanism of IOTA, if a transaction is not approved directly or indirectly by a recent milestone, it will remain unconfirmed until the next milestone comes. Furthermore, if a transaction is not approved during three milestones, it will not be confirmed anymore. That means each milestone may leave some transactions in the Tangle to be tips forever. Thus, the total tip number will increase continuously, but the tip number between two milestones, which is highly related to the tip ratio, will be stable.

We use one full node configuration for this test. The tip ratio influences incurred by different milestone intervals are shown in Fig. 11(a) and (b). When we fix the incoming transaction speed at 8, different milestone intervals incur different tip ratios. After a short unstable time initially, no matter how we change the milestone interval, the tip ratio is maintained stable. However, a longer milestone interval will lead to a higher tip ratio, mainly due to one milestone's limited confirmation ability.

When we fix the incoming transaction speed at 16, the results are different. From Fig. 11(b), we can see that all three lines are increasing. Although shorter milestone intervals cause lower tip ratios, all of them are not stable. As time goes by, the tip ratio increases slowly, which indicates that each milestone leaves more and more tips unconfirmed, degrading the stability of the whole IOTA network. The main reason is that 16 TPS is the upper limit of one full node's throughput. Thus, the overloaded full node degrades the system robustness.

Besides the system robustness, the milestone interval can also affect system performance. We monitor the performance

of the private IOTA network as we change the milestone interval. We first fix the incoming transaction speed at 8. Fig. 11(c) shows its performance. When we slow down the milestone speed, the throughput of the private IOTA network decreases a little, and the latency also grows higher. It is because the tip selection and validation processes will cover more transactions. Furthermore, the full node needs to utilize more resources to handle the computation-intensive tasks when the milestone interval prolongs.

The above evaluations show that whether or not the tip ratio is stable is highly associated with the private IOTA network's status, and many factors will influence the tip ratio. The most crucial factor is the incoming transaction speed. Too many incoming transactions will make the full nodes run out of their resources, and finally, crash. Meanwhile, the milestone interval is also very important, and its changes may influence various behaviors of the private IOTA network, especially the performance.

V. System Implications

We will summarize some system implications and promising optimization directions in this section after the comprehensive exploration of the IOTA's characteristics.

Performance: The performance upper bound of the private IOTA network is highly related to the system configurations. The existing public IOTA network contains more than one hundred full nodes, and the milestone interval is set to 1 min. However, this configuration only makes the throughput of the public IOTA network reach about 10 TPS [48]. To further improve the IOTA's throughput, reducing the IOTA full nodes' workload is the top priority. From our experiment, we can see that when generating a transaction, besides the tip selection and the validation processes, the database query also incurs a lot of storage overhead and prolongs the internal latency. Thus, improving the database query performance will contribute a lot to the IOTA's performance [49]. Furthermore, if the tip selection and validation processes can be accelerated [46], [47], it will also enhance the full nodes' capability of processing incoming transactions.

For the transaction confirmation process, the confirmation latency is fully dependent on the milestone interval. If milestones are issued more frequently, transactions can be confirmed more quickly, reducing the confirmation latency. Thus, if we employ the private IOTA network in an IoT environment, a smaller milestone interval will enhance the system performance.

Another potential optimization is to mitigate the network communication overhead between multiple full nodes. The communication cost limits the private IOTA network's scalability and causes the degradation of its performance. Once a transaction is attached, the updated Tangle needs to be broadcasted to all the other full nodes, incurring heavy network traffic. In our experiments, when the full node number reaches 4, the network traffic will seriously degrade the system performance.

Security: The IOTA's security can be promised when facing double-spending and off-syncing attacks. However, for off-syncing attacks, the whole IOTA network's recovery speed is slow, at around 20 TPS. Improving the recovery speed can reduce the period of performance thrashing, enhancing the private IOTA network's stability.

For the double-spending attack, the detection time is not guaranteed, which is an uncertain factor when employing IOTA in an IoT environment. Although we do not find more than 14 transactions that need to be reattached during the double-spending attack experiments, it is worthwhile to enhance the efficiency of double-spending detection.

System Robustness: The system robustness of the private IOTA network is not satisfactory. Many situations can cause changes in the Tangle's tip ratio. Once the tip ratio presents an upward trend, the whole IOTA network will be at the risk of crashing. One interesting optimization direction can be developing new scheduling algorithms to prevent the IOTA full nodes from being overloaded and make the tip ratio more stable to improve system robustness.

Controlling the milestone intervals is also a promising approach for enhancing the system robustness since the actual number of tips in the private IOTA network is highly related to the milestone interval. According to our experiments, setting a smaller milestone interval when employing IOTA in the IoT environment will be a better choice. Furthermore, the milestone mechanism can also be replaced by other efficient consensus mechanisms to control the transactions' confirmation.

VI. Related Work

In this section, we will introduce closely related works that focus on optimizing and benchmarking block-based blockchain systems and DAG-based blockchain systems. We also list several works concentrating on the blockchain technique in IoT environments.

Block-Based Blockchain: Many techniques have been proposed for block-based blockchain systems to optimize the PoW consensus mechanism. Several studies propose to translate the huge energy consumption of PoW into meaningful work. For example, Primecoin [50] replaces hash calculation with the search of prime sequence, and Gapcoin [51] searches for large prime gaps. Hardware accelerators are designed for accelerating the PoW process, such as GPU, FPGA, ASIC, and ReRAM [52]–[55], to improve the performance of the blockchain system. GPU platforms experience higher power consumption and higher price. ASIC is application-specific and cannot be used once the mining algorithm is updated. FPGA suffers from complicated unfavored programming. ReRAM implementations are not widely adopted by the industry yet. Hence, the performance optimization of block-based blockchain systems still needs more effort.

Benchmarking block-based blockchain systems have been widely investigated. For instance, Gervais *et al.* [16] presented a novel quantitative framework to compare PoW blockchains. They characterize different PoW blockchains and evaluate their performance and security. Hao *et al.* [56] and Sukhwani *et al.* [57] targeted how consensus protocols influence the performance. Different consensus algorithms

are compared to show their impact on the performance of the blockchain system. Rouhani and Deters [58], and Nasir *et al.* [59] evaluated the performance of a private blockchain and perform transaction analysis on Ethereum and hyper ledger fabric, respectively. Dinh *et al.* [41] and Zheng *et al.* [60] focused on the benchmark tools for standard block-based blockchains. They propose performance monitoring and benchmarking frameworks and present comprehensive analysis for different system design choices.

Several studies have been conducted to optimize application-specific blockchain systems. Sagirlar *et al.* [17] produced a novel IoT-oriented hybrid blockchain architecture, and the performance evaluation proves the validity of their design under the sweet-spot guidelines. Novo [61] developed a distributed IoT management system based on blockchain, overcoming the limitations on the applicability in scenarios with numerous IoT devices. Suankaewmanee *et al.* [62] focused on analyzing mobile blockchains' performance and exploring potential applications.

Blockchain in IoT Environment: To make IoT environment more secure and trusted, several works propose to adopt blockchain techniques. Mohanta *et al.* [30] proposed an Ethererum-based blockchain system in a smart IoT system to tackle security and privacy issues. Cui *et al.* [29] introduced CoDAG, a blockchain protocol based on a compacted directed acyclic graph, to improve the blockchain throughput. CoDAG in an Industrial Internet-of-Things (IIoT) system significantly outperforms Bitcoin and Ethererum.

He *et al.* [63] focused on optimizing the security of the edge computing architecture in an IoT environment, which uses block-based blockchains to maintain trust between IoT devices and edge computing nodes (ECNs). They also design a machine-learning algorithm to efficiently allocate edge computing resources, which is implemented with smart contracts in a private blockchain network. Cui *et al.* [64] study trusted edge computing in an IoT environment and construct a decentralized platform with blockchains to enhance the trust and the incentive of each participant. In [65], a containerized edge computing platform, called CUTE, is developed to provide low latency computation services for the Internet of Vehicles. CUTE has been deployed in the China Mobile Network and the results show that CUTE outperforms traditional container scheduling policies.

DAG-Based Blockchain: Researches on DAG-based blockchain systems are still at their early stage. IOTA foundation [39] presents several simulation results for the Tangle structure and evaluates the trend of the cumulative weight parameter and number of tips. The presented data confirm the results in the IOTA whitepaper. Attias and Bramas [45] proposed a multiagent network model to test the stabilization of IOTA and also propose two Tangle compression algorithms to reduce the inherent latency. Pervez *et al.* [66] presented a comparative analysis of several DAG-Based blockchains, including Nxt, IOTA, Orumesh, DagCoin, Byteball, Nano, and XDAG. Wang *et al.* [67] constructed three types of attack strategies and test IOTA security with these attacks. Cao *et al.* [68] focused on the performance analysis between different consensus algorithms. They compare PoW, PoS, and DAG-based blockchains and the results indicate that PoW and PoS are more sensitive to the change of network resource while DAG is more sensitive to network load conditions. Li *et al.* [69] used the Markov chain model to formulate the consensus process of IOTA. They also design a typical double-spending attack in the consensus process and use a stochastic model to examine the probability of launching a successful attack under different loads.

Only a few works are focusing on optimizing DAG-based blockchains. Wang *et al.* [46], [47] proposed an ReRAM-based accelerator for IOTA blockchain, including speeding up both the PoW process and validation process. By offloading those two processes to parallel execution on ReRAM, the CPU usage can be reduced significantly, thus improving the performance. Shafeeq *et al.* [70] reduced the IOTA address generation time by adopting a cuckoo bloom filter to mitigate some database overhead.

One reason with few works on optimizing DAG-based blockchains is the lack of a full-functional benchmarking tool. Dong *et al.* [71] proposed a performance evaluation framework for DAG-based blockchains. Park *et al.* [72] also analyzed the performance of DAG-based blockchains. However, those works only focus on the performance characteristics of DAG-based blockchain, neglecting other metrics, such as security and system robustness.

In this article, we aim to bridge this gap by developing a full-functional benchmarking tool and investigating not only the performance characteristics but also the security and system robustness of DAG-based blockchains.

VII. Conclusion

DAG-based blockchains are emerging, aiming to provide trustworthy and secure device-to-device transactions for IoT environments with high throughput. In this article, based on IOTA, we build a private DAG-based blockchain system and develop a series of benchmark tools, including a transaction initiator, an IOTA status monitor, and a double-spending attacker. All the benchmark tools are open-sourced to the public. Based on these benchmark tools, we examine IOTA in terms of performance, security, and system robustness. Although the security of IOTA can be promised, both its performance and robustness need more improvements. We further analyze the underlying reasons and summarize several system implications and optimization directions for further IoT security design based on DAG-based blockchain technologies.

References

[1] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding intrinsic characteristics and system implications of dag-based blockchain," in *Proc. IEEE Int. Conf. Embedded Softw. Syst. (ICESS)*, Shanghai, China, 2020, pp. 1–6.

[2] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?" in *Proc. Hamburg Int. Conf. Logist. (HICL)*, 2017, pp. 3–18.

[3] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *Sci. Res. Publ. J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

[4] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Oxford Univ. Press J. Amer. Med. Informat. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[5] S. Park and H. Kim, "DAG-based distributed ledger for low-latency smart grid network," *Multidiscipl. Digit. Publ. Inst. Energies*, vol. 12, no. 18, p. 3570, 2019.

[6] S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT network," in *Springer Data Communication and Networks*. Singapore: Springer, 2020.

[7] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of Things (IoT) enabling technologies, requirements, and security challenges," in *Springer Advances in Data and Information Sciences*. Singapore: Springer, 2020.

[8] S. Popov, "The tangle," IOTA Foundation, Austin, TX, USA, White paper, vol. 1, p. 3, 2016.

[9] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proc. IEEE Asia South Pac. Design Autom. Conf. (ASP-DAC)*, Macao, China, 2016, pp. 519–524.

[10] N. Cam-Winget, A.-R. Sadeghi, and Y. Jin, "Can IoT be secured: Emerging challenges in connecting the unconnected," in *Proc. ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Austin, TX, USA, 2016, pp. 1–6.

[11] N. Zivic, C. Ruland, and J. Sassmannshausen, "Distributed ledger technologies for M2M communications," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Kuala Lumpur, Malaysia, 2019, pp. 301–306.

[12] W. Jiang, P. Pop, and K. Jiang, "Design optimization for security- and safety-critical distributed real-time applications," *Microprocess. Microsyst.*, vol. 52, pp. 401–415, Jul. 2017.

[13] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[14] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Springer Int. Conf. Finan. Cryptogr. Data Security*, 2016, pp. 106–125.

[15] T. Chen *et al.*, "Understanding Ethereum via graph analysis," *ACM Trans. Internet Technol.*, vol. 20, no. 2, pp. 1–32, 2020.

[16] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 3–16.

[17] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-IoT: Hybrid blockchain architecture for Internet of Things—PoW sub-blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 1007–1016.

[18] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: www.bitcoin.org

[19] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project, Zug, Switzerland, Yellow Paper, vol. 151, pp. 1–32, 2014.

[20] A. Rossow. (2018). *Ethereum Founder Acknowledges Promising Solution to Blockchains' Scalability Problem*. [Online]. Available: https://www.forbes.com/sites/andrewrossow

[21] R. Singh, A. D. Dwivedi, and G. Srivastava, "Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," *Sensors*, vol. 20, no. 14, p. 3951, 2020.

[22] IOTA-Foundation. (2020). *What Is IoTA?*. [Online]. Available: https://www.iota-services.com/what-is-iota

[23] T. Wang. (2019). *IoTA-Benchmark-Tool*. [Online]. Available: https://github.com/wty715/IOTA-Benchmark-Tool

[24] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of Things: A definition & taxonomy," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl. Serv. Technol.*, Cambridge, U.K., 2015, pp. 72–77.

[25] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.

[26] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[27] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[28] M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, Helsinki, Finland, 2017, pp. 246–251.

[29] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4134–4145, Jun. 2020.

[30] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, Jan. 2021.

[31] G. Zyskind, O. Nathan, and A. 'S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180–184.

[32] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1229–1241, Jun. 2020.

[33] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Proc. Springer Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2017, pp. 643–673.

[34] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Springer Int. Workshop Open Problems Netw. Security*, 2015, pp. 112–125.

[35] A. Churyumov. (2016). *Byteball: A Decentralized System for Storage and Transfer of Value*. [Online]. Available: https://byteball.org/Byteball.pdf

[36] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020.

[37] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jul. 2018.

[38] O. Lamtzidis and J. Gialelis, "An IOTA based distributed sensor node system," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, UAE, 2018, pp. 1–6.

[39] B. Kusmierz, "The first glance at the simulation of the tangle: Discrete model," IOTA Found., Berlin, Germany, White Paper, 2017.

[40] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. IEEE Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, 2017, pp. 1–6.

[41] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data (SIGMOD)*, 2017, pp. 1085–1100.

[42] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," 2018. [Online]. Available: arXiv:1809.03421.

[43] B. Kusmierz, P. Staupe, and A. Gal, "Extracting tangle properties in continuous time via large-scale simulations," IOTA Found., Berlin, Germany, Working Paper, 2018.

[44] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "IOTA feasibility and perspectives for enabling vehicular applications," in *Proc. IEEE Globecom Workshops*, Abu Dhabi, UAE, 2018, pp. 1–7.

[45] V. Attias and Q. Bramas, "Tangle analysis for IOTA cryptocurrency," 2018. [Online]. Available: https://vidal-attias.io/

[46] Q. Wang, T. Wang, Z. Shen, Z. Jia, M. Zhao, and Z. Shao, "Re-tangle: A ReRAM-based processing-in-memory architecture for transaction-based blockchain," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Westminster, CO, USA, 2019, pp. 1–8.

[47] Q. Wang *et al.*, "A highly parallelized PIM-based accelerator for transaction-based blockchain in IoT environment," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4072–4083, May 2020.

[48] IOTA-Foundation. (2021). *IOTA Tangle Explorer*. s[Online]. Available: https://thetangle.org

[49] T. Wang, W. Zhu, Q. Ma, Z. Shen, and Z. Shao, "ABACUS: Address-partitioned bloom filter on address checking for uniqueness in IoT blockchain," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, San Diego, CA, USA, 2020, pp. 1–7.

[50] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," vol. 1, no. 6, Jul. 2013.

[51] S. King. (2014). *Gapcoin*. [Online]. Available: https://gapcoin.org

[52] Y. Long, T. Na, and S. Mukhopadhyay, "ReRAM-based processing-in-memory architecture for recurrent neural network acceleration," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2781–2794, Dec. 2018.

[53] Y. Sakakibara, K. Nakamura, and H. Matsutani, "An FPGA NIC based hardware caching for blockchain," in *Proc. 8th Int. Symp. Highly Efficient Accelerators Reconfigurable Technol. (HEART)*, 2017, pp. 1–6.

[54] H. Cho, "ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," *IEEE Access*, vol. 6, pp. 66210–66222, 2018.

[55] S. Morishima and H. Matsutani, "Acceleration of anomaly detection in blockchain using in-GPU cache," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl. Ubiquitous Comput. Commun. Big Data Cloud Comput. Soc. Comput. Netw. Sustain. Comput. Commun. (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, Melbourne, VIC, Australia, 2018, pp. 244–251.

[56] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Changshu, China, 2018, pp. 280–285.

[57] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE Symp. Rel. Distrib. Syst. (SRDS)*, Hong Kong, 2017, pp. 253–255.

[58] S. Rouhani and R. Deters, "Performance analysis of Ethereum transactions in private blockchain," in *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. (ICSESS)*, 2017, pp. 70–74.

[59] Q. Nasir, I. A. Qasse, M. A. Talib, and A. B. Nassif, "Performance analysis of hyperledger fabric platforms," *Security Commun. Netw.*, vol. 2018, Sep. 2018, Art. no. 3976093.

[60] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *Proc. IEEE/ACM Int. Conf. Softw. Eng. Softw. Eng. Pract. Track (ICSE-SEIP)*, Gothenburg, Sweden, 2018, pp. 134–143.

[61] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4694–4701, Jun. 2019.

[62] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance analysis and application of mobile blockchain," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, Maui, HI, USA, 2018, pp. 642–646.

[63] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, "Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2226–2237, Feb. 2021.

[64] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, and M. Xu, "A decentralized and trusted edge computing platform for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3910–3922, May 2020.

[65] L. Cui *et al.*, "A blockchain-based containerized edge computing platform for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2395–2408, Feb. 2021.

[66] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of DAG-based blockchain architectures," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Lahore, Pakistan, 2018, pp. 27–34.

[67] B. Wang, Q. Wang, S. Chen, and Y. Xiang, "Security analysis on tangle-based blockchain through simulation," in *Proc. Aust. Conf. Inf. Security Privacy*, 2020, pp. 653–663.

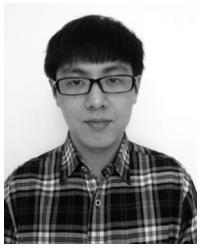
[68] B. Cao *et al.*, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 480–485, 2020.

[69] Y. Li *et al.*, "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, Aug. 2020.

[70] S. Shafeeq, S. Zeadally, M. Alam, and A. Khan, "Curbing address reuse in the IOTA distributed ledger: A cuckoo-filter-based approach," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1244–1255, Nov. 2020.

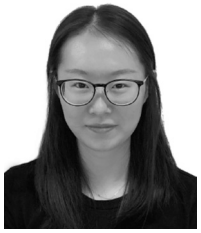
[71] Z. Dong, E. Zheng, Y. Choon, and A. Y. Zomaya, "DAGBENCH: A performance evaluation framework for DAG distributed ledgers," in *Proc. IEEE Int. Conf. Cloud Comput. (CLOUD)*, Milan, Italy, 2019, pp. 264–271.

[72] S. Park, S. Oh, and H. Kim, "Performance analysis of DAG-based cryptocurrency," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Shanghai, China, 2019, pp. 1–6.



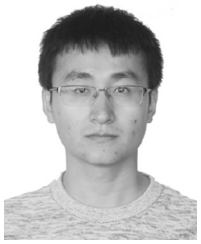
Tianyu Wang received the B.E. degree from the School of Electronics and Information Engineering, Tongji University, Shanghai, China, in June 2016, and the M.S. degree from the School of Computer Science and Technology, Shandong University, Qingdao, China, in June 2019.

His main research interests include storage systems, nonvolatile memory, and blockchain techniques.



Qian Wang received the B.E. degree from the School of Data Science and Software Engineering, Qingdao University, Qingdao, China, in June 2017. She is currently pursuing the M.S. degree with the School of Computer Science and Technology, Shandong University, Qingdao.

Her research interests include emerging nonvolatile memory and Blockchain techniques.



Zhaoyan Shen received the B.E. and M.E. degrees from the Department of Computer Science and Technology, Shandong University, Qingdao, China, in 2012 and 2015, respectively, and the Ph.D. degree from the Department of Computing, Hong Kong Polytechnic University, Hong Kong, in 2018.

He is currently an Assistant Professor with Shandong University. His research interests include big data systems, storage systems, embedded systems, system architecture, and hardware/software codesign.

Zhiping Jia received the master's from the School of Computer Science, Shandong University, Jinan, China, in 1989, and the Ph.D. degree from the School of Control Science, Shandong University in 2007.

In July 1989, he was with the Department of Computer Science and Technology, Shandong University, Qingdao, China, where he has been a Professor since 2002. He has published more than 70 research papers in refereed conferences and journals and served as program committee members in numerous international conferences.

Dr. Jia received the Shandong Province Award and the Teaching Award.

Zili Shao received the B.E. degree in electronic mechanics from the University of Electronic Science and Technology of China, Sichuan, China, in 1995, and the M.S. and Ph.D. degrees from the Department of Computer Science, University of Texas at Dallas, Dallas, TX, USA, in 2003 and 2005, respectively.

In 2018, he was with the Department of Computing, The Hong Kong Polytechnic University, Hong Kong, where has been serving since 2005. He is currently an Associate Professor with the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong. His current research interests include big data systems, storage systems, embedded software and systems, and related industrial applications.