Performance Analysis of the IOTA Chrysalis on Heterogeneous Devices*

Muhammad Waleed[1][0000−0001−9770−6293], Knud Erik Skouby[1][0000−0003−4994−4144], and Sokol Kosta[1][0000−0002−9441−4508]

Aalborg University, Copenhagen, Denmark
{muhammadw,skouby,sok}@es.aau.dk

Abstract. Existing Distributed Ledger Technologies (DLTs) based models like blockchain pose scalability and performance challenges for IoT systems due to resource-demanding Proof of Work (PoW), slow transaction confirmation rates, and high costs. Against a need to adopt a viable approach, especially for low-power IoT devices, IOTA emerges as a promising technology, leveraging the Direct Acyclic Graph (DAG) based approach called Tangle for IoT-focused applications. In this paper, we design a system enabling secure data exchange between IoT devices on IOTA Chrysalis, the latest version. We perform extensive experiments on two machines, a Workstation PC and Raspberry Pi, to demonstrate the performance gap between powerful and low-power devices. Our findings show that even low-power devices, such as Raspberry Pi, perform well with small payload sizes on the Chrysalis network but face challenges with larger payloads. We observe that variation in transmission time increases as payload size grows, indicating the impact of PoW complexity, but it still is feasible for Raspberry Pi. We further validated our experimental setup to ensure the validity and accuracy of our approach through discussions with the IOTA Foundation's technical team.

Keywords: IoT · Distributed Ledger Technology · IOTA Chrysalis · Heterogeneous Devices · Scalability and Data Security.

1 Introduction

Internet of Things (IoT) is growing in our everyday life by connecting people or things with advanced devices to communicate and achieve a common goal in different applications. However, such a rampant explosion of these devices raises concerns for the security and privacy of IoT devices' data. The IoT systems cannot afford a malicious device to participate in the communication leading

* This work was supported by the IoTalentum research program funded by the European Union Horizon 2020 research and innovation program within the framework of Marie Skłodowska-Curie Actions (MCSA) ITN-ETN with grant number 953442. We would also like to thank Thoralf Müller and other members of the IOTA Foundation for their valuable discussion to enhance experiments and good reviews, which led to further improvements.

to the necessity of a secure exchange of information. Further, most devices are resource constrained, where they cannot run complex cryptographic algorithms or store large amounts of data due to low power capabilities. Therefore, these device data must be stored securely, so it cannot be accessible to any malicious device to prevent data abuse.

Initial models for securing IoT devices' data often rely on centralized authorities, introducing vulnerabilities and security risks due to single points of failure [24]. Distributed Ledger Technologies (DLTs), such as Blockchain, have been adopted to eliminate the need for intermediaries in IoT applications [3]. However, scalability issues arise from limited block capacity, and high computation power requirements for Proof of Work (PoW) may not always be applicable, as demonstrated by emerging Proof of Stake (PoS) protocols like Ethereum [23]. Furthermore, this limitation makes traditional blockchain architectures less suitable for deployment on resource-constrained IoT devices. Therefore, developing a lightweight system where IoT devices can communicate and securely store data is demanded. The system should not be confined to powerful devices but also acclimate low-power devices to store their data securely.

The IOTA protocol proposed by the IOTA foundation[1] is a DLT that functions as a Direct Acyclic Graph (DAG) instead of a single chain as in the blockchain [18]. IOTA employs the DAG structure to improve scalability and develop a keystone technology term as a Tangle, a permissionless scalable design focusing on IoT applications [14]. The technology mitigates the mining race and transaction cost by allowing the new transaction to reference two existing tips (i.e., newly attached transactions).

1.1 Contributions

Our contribution involves designing a system based on IOTA Chrysalis to facilitate secure information exchange for resource-constrained IoT devices. The design system utilizes the new IOTA client library *iota.rs* replacing the old one *iota.js* to facilitate communication with the Chrysalis Tangle. We conducted extensive experiments on a real testbed to assess the performance gap between low-power and powerful devices. The experiments stage in two phases: payload creation and payload broadcasting, with 1000 tests performed for each payload size on two machines separately, a workstation PC and Raspberry Pi (RPi). Our analysis includes comprehensive performance data, ranging from small to large payloads (approximately 32 KB), the maximum limit allowed in IOTA Chrysalis. These experiments represent the first real testbed evaluation using the maximum payload size for 1000 tests on the Chrysalis network.

The paper is structured as follows: Section 2 provides a background study on DLTs. Section 3 describes the proposed system and its implementation details. Section 4 presents the experimental results, and Section 5 concludes the paper with a discussion and proposed future directions.

[1] https://www.iota.org/

Table 1: Analysis of different DLTs compared to proposed system for IoT.

Reference	DLT (Structure, Consensus)	Analysis	Results	Main Weaknesses
Marzouqi et al. (2022)[16]	Ethereum (Blockchain, PoW)	Scalability	Shows efficiency of transactions from different devices, PC perform better mining to add new blocks fast compared to RPi	High resource demanding, performed only 10 tests, tradeoff between performance and memory consumption
Xuan et at. (2020)[7]	Private Ethereum (Blockchain, PoW)	Scalability	Shows latencies in different workloads, achieved average time of 63.92 ms (without mining time) for one transaction	High resource demanding, tested only with 100 transactions, mining is performed on powerful PC
Zia et al. (2022)[21]	Private Ethereum (Blockchain, PoW)	Scalability	Introduced proof-of-authority to reduce transaction time average transaction time achieved is 487.6 ms	High resource-demanding, one transaction degraded claim of high throughput, not feasible for small devices
Kumar et al. (2021)[13]	Ethereum and Hyperledger Fabric (Blockchain, No info)	Scalability	Internet of Forensic (IoF) framework for secure evidence chain, High transaction throughput, latency achieved is 9.6 sec	High communication cost, low scalability, consensus affect the performance, tested with only 100 transactions, no info on the consensus mechanism provided
Jiaping and Hao (2019)[22]	Monoxide (Blockchain, PoW)	Scalability/ Security	Experiments on testbed for Ethereum and Bitcoin Network, the authors claim 1,000× throughput and 2,000× on each network	High resource demanding, susceptible to attacks due distribution of mining power across zones
Fengyang et al. (2020)[11]	IOTA early version-1.0 (DAG, Tangle reference)	Scalability/ Security	Key findings are that most transactions take around 10 min to attach Tangle, also authors claim that the confirmation rate of 1-5% transaction is exceptionally long	Low transaction confirmation rate (1-10 min), not feasible for delay-sensitive devices, susceptible to attacks such as parasite chain attack
Akhtar, M.M et al. (2021)[2]	IOTA early version-1.0 (DAG, Tangle reference)	Scalability	Enhanced MAM protocol for better communication of IoT data, transactions (small in this case), confirmation time reduced to constant time (5.3 sec)	Experiments performed with small transactions, not on real testbed, MAM library creates overhead in restricted mode
Caixiang et al. (2019)[9]	Private IOTA, IRI 1.5.3 (DAG, Tangle reference)	Scalability	Shows good efficiency in processing transactions, average TPS can reach 1 sec for one transaction, the average time for confirmation of transaction is 0.83 sec	Not tested with maximum data, lack of synchronization time (no info on shifting from private to main Tangle), transaction speed reduces with increase in transactions
Sabah et al. (2020)[19]	IOTA early version-1.0 (DAG, Tangle reference)	Scalability	Shows good throughput for supply chain entities, average time for sending data is 3 sec for a local node, RPi is used to analyze the feasibility of energy consumption on low-power devices	Experiments performed with smaller payloads up to 1000 characters on RPi, large message attach time (average is 23.1 sec)
Our Designed System	IOTA 1.5 (Chrysalis) (DAG, Tangle reference)	Scalability	Shows good efficiency in attaching data to Tangle, performed experiments up to maximum data, average time for largest payload (30,000 char) on PC is 55.7 sec and for RPi it is 1457 sec, implemented on a real testbed, accommodate low-power devices	Need to extend it for real sensors, to perform experiments for a large time (24 hrs for each payload) to analyze behaviour of Chrysalis in different timings, support up to 32 KB of data, Note: These limitations are considered as part of the future work

2 Related Work

DLTs are introduced in recent IoT environments to enable secure exchange of information. One motivation behind bringing attention to DLTs is the problem of a single point of failure with the centralized authority; however, these models also pose various issues, such as scalability and performance are the critical ones.

The initial explosion of Blockchain as a DLT has minimal use in IoT like bitcoin and Litecoin are not viable for IoT due to limited block size, low transaction rate and high transaction costs [17]. Following that, in [12], the authors proposed a model based on Ethereum for IoT devices; however, the concept is based on a limited number of devices, which needs to be clarified in relation to more transactions. Further, it is not feasible for low-power IoT device [7].

However, many researchers have recently worked towards improving performance and throughput in traditional Blockchain. An interesting work is presented in [22], called Monoxide for IoT systems. They made different zones, where an independent PoW is assigned to each zone to enable running PoW in parallel. However, the interaction of different zones with deploying cross-zone algorithms leads to security issues between zones as it weakens the mining power for sub-blockchains in the single system [15]. In one of the other works [20], the authors proposed an optimal node algorithm to analyze Blockchain's throughput and transaction success rate for IoT systems. However, the model needs to show feasibility for low-power devices.

Previous research has examined DAG-based IOTA to assess transaction confirmation time and system performance. Notably, a study on an early version of IOTA observed delays in attaching transactions to the Tangle [11]. Another simulation-based investigation highlighted the superior performance of IOTA compared to traditional blockchains, particularly in terms of transaction confirmation rate and computational requirements [5]. However, these experiments focused on smaller data sizes and made certain unrealistic assumptions [11]. In

a separate study, an offline IOTA network was deployed to analyze performance with varying data amounts. However, the maximum data used and synchronization with the online Tangle were not explicitly addressed [9]. Table 1 provides an analysis of different DLTs related to the research. Recent experiments have focused on energy consumption in the future network of IOTA [10], known as Coordicide. However, these experiments are limited to energy analysis and do not cover the variations in data sizes. It is important to note that Coordicide is still in the development stage.

To the best of our knowledge, the performance gap between low-power and powerful devices on the recent version of IOTA, the Chrysalis, is not investigated in the literature, which is the main contribution addressed in this work.

2.1 IOTA Chrysalis

The IOTA foundation recently released the updated version of IOTA, named Chrysalis[2], with potential improvements to optimize the protocol and enhance the usability of the IOTA legacy for IoT applications. Chrysalis is improved in numerous aspects: *i)* the tip selection algorithm has been substituted with a new algorithm called Weighted Uniform Random Tip Selection (W-URTS), significantly reducing the time in nominating new tips [8]; *ii)* The Winternitz One Time Signature (W-OTS) scheme is replaced with the Edwards-curve (Ed25519) signature scheme to reduce signatures size and time for validation [4]; *iii)* the unspent transaction output (UTXO) model; and *iv)* the integration of atomic transactions with the protocol [8]. This work aims to analyze the impact of these new significant additions in terms of performance overhead on different types of devices.

3 System Architecture

The proposed system is designed on the lightweight DLT IOTA Chrysalis to secure the IoT devices' data. The system aims to evaluate its potential for creating and broadcasting data from powerful and low-power IoT devices. We have set up a powerful workstation PC and a low-power device like RPi. We use the Chrysalis public Hornet node, which is fully functional with the Chrysalis network. The proposed system architecture is shown in Figure 1, while Table 2 provides more details about the components' specs.

IOTA has been utilized in several applications [1, 6]; however, they were based on the IOTA legacy version, where the old libraries have been used, inducing complications in employing them with different programming languages. Further, the IOTA legacy version also raises issues while including new messages, such as the Random Walk tip selection algorithm's inefficiency in selecting new tips (i.e., messages), later improved with Chrysalis's new tip selection algorithm called Restricted Uniform Random Tip Selection (R-URTS) algorithm [14].

[2] https://chrysalis.iota.org/

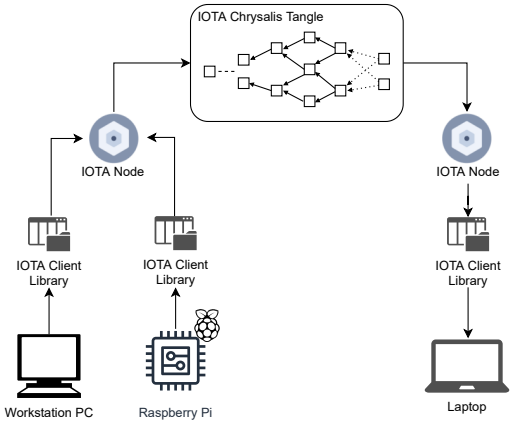


Fig. 1: Designed system architecture.

Table 2: System description.

System and Environment Description	
Workstation	Intel® Xeon(R) W-2133 CPU @ 3.60GHz×12, Ubuntu 22.04.1 LTS, 32 GB RAM, 512 GB
Language for development	JavaScript (Node.js)
IoT device	RPi 4 Model B (ARMv7), Raspbian GNU/Linux 11

3.1 Implementation Details and Procedures

The communication of IoT devices with the Chrysalis network is facilitated by utilizing the new IOTA client library, specifically the `iota.rs`[3] library. This library allows for direct integration with Rust or enables binding with other programming languages. In our system, we have integrated the IOTA client library with Node.js. This integration allows us to convert requests into REST API format and send them to the node for processing. It provides a convenient way to interact with the IOTA network. For this research, we utilize the Chrysalis public Hornet node[4], a robust and capable node that supports full node functionalities. It is designed to be compatible with low-power devices such as the RPi. The selected Hornet node interacts with the Chrysalis network, including the operational network (mainnet) and the network for testing purposes (devnet).

In our design system, we leverage the client libraries and the Hornet node to interact specifically with the Chrysalis devnet. This enables us to conduct thorough testing and research activities in a controlled environment. Additionally, we include a laptop, as shown on the right side in Figure 1 of the setup. Its role is to verify the reception of data transmitted by the IoT devices. Although our primary focus is on data creation and broadcasting, we include the laptop to

[3] https://github.com/iotaledger/iota.rs
[4] https://wiki.iota.org/hornet/welcome

ensure that data is correctly attached to the Tangle and can be received on the other side. By using the address and message indexation, we verify the successful transmission and retrieval of data. It serves as a validation step in our experimental setup. Further, in our testbed, we have set the devices to perform PoW locally. This allows us to assess the feasibility of executing PoW on low-power devices within the IOTA network. Additionally, the validation process verifies and confirms transactions on the IOTA Tangle. It checks transaction structure, data consistency, and completion of the required PoW. The IOTA nodes, including the Hornet node we used, perform this validation to maintain network integrity and security.

4 Experimental Results

In our study, we conducted two phases of experiments to assess the impact of IOTA Chrysalis on both powerful and low-power devices. In the first phase, we created data payloads with varying sizes, ranging from 10 to 30,000 characters, on both the workstation PC and RPi. This allowed us to examine the performance of each device in generating payloads of different magnitudes. In the second phase, we transmitted these payloads and attached them to the Chrysalis Tangle. By doing so, we analyzed the effectiveness and suitability of the IOTA Chrysalis technology for small, low-power devices. Through these experiments, we aimed to gain insights into how the IOTA Chrysalis implementation meets different devices' requirements and capabilities, providing a comprehensive understanding of its support and applicability.

4.1 Measuring Overhead of Data Creation

The first phase of experiments is set up to create various data/payloads. Different payloads are created, ranging from small (10 characters) to large (30,000 characters). Two devices, a workstation PC and a RPi (detailed description in Table 2), are used to conduct the experiments. The payloads are created on both machines using the IOTA Node.js client library.

For each of the six payload creations, we perform 1000 tests on each machine. The results of the experiments for the workstation PC and the RPi are shown in Figure 2. Furthermore, statistical details of the results are shown in Table 3.

From the experiments, we notice that, when considering small payloads (up to 1000 characters), the difference in creation time between the workstation and the RPi is relatively small. Both devices are able to create payloads in less than 1 ms, with the workstation being slightly faster due to its higher processing capabilities. However, a significant performance gap becomes apparent as the payload size increases beyond 1000 characters. The workstation consistently outperforms the RPi, completing the payload creation process 3-5 times faster. Additionally, the time variations for small payloads are generally lower compared to large payloads. The workstation exhibits greater stability in all measurements, particularly with larger payloads. This is evident from the smoother curves and smaller standard deviation values, indicating a more consistent performance.

Table 3: Experimental results on Workstation (left) and RPi (right) for creation different payload sizes (1000 times).

Payload (nr. chars)	Min. Time (ms)	Max. Time (ms)	Avg. Time (ms)	St. dev. (ms)
10	0.034	0.184	0.047	0.011
100	0.030	0.901	0.066	0.058
1000	0.084	0.984	0.226	0.139
10000	0.594	6.127	1.679	0.347
20000	1.407	7.135	3.713	0.446
30000	2.229	11.251	5.020	0.644

Payload (nr. chars)	Min. Time (ms)	Max. Time (ms)	Avg. Time (ms)	St. dev. (ms)
10	0.028	0.389	0.076	0.031
100	0.044	0.579	0.129	0.045
1000	0.264	2.268	0.644	0.246
10000	2.317	29.925	6.008	1.473
20000	4.688	32.727	10.724	3.435
30000	7.159	48.021	16.509	4.987

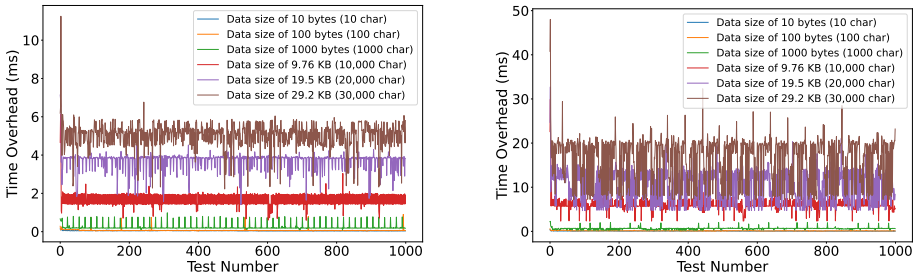


Fig. 2: Data/payload creation (1000 tests performed for each payload) on (a) Workstation and (b) RPi.

4.2 Overhead of Data Transmission on the IOTA Chrysalis Tangle

In our study's second phase, we conduct experiments to measure the time overhead of broadcasting payloads to the Chrysalis Tangle on both machines. We capture accurate time variance by repeating the process and attaching each payload to the Tangle 1000 times. The time taken for each message depends on the complexity of the required PoW. In the legacy IOTA implementation, users manually set the PoW difficulty when issuing messages. However, in Chrysalis, the PoW complexity is automated and adjusted based on message size. This dynamic PoW mechanism ensures efficient and scalable PoW computations tailored to each message. Looking forward, IOTA Coordicide introduces Adaptive PoW as a further advancement. Adaptive PoW dynamically adjusts the PoW process based on the rate of message issuance. It serves as a safeguard against transaction bursts, preventing spam attacks and congestion within the network.

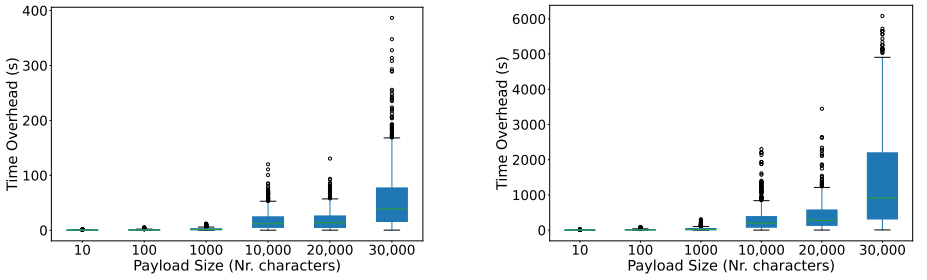
Figure 3 shows the results of these experiments on the workstation and RPi. The results of the 1000 measurements are presented as boxplots showing the minimum, the first quartile, the median, the third quartile, and the maximum. The statistical facts of the outcomes are shown in Table 4.

Based on our experiments, several key findings emerged; firstly, the broadcasting time for data on the IOTA Tangle is significantly faster for powerful devices compared to resource-constrained IoT devices. This can attribute to the

Table 4: Experimental results on Workstation (left) and RPi (right) for broadcasting different payload sizes (1000 times).

Payload (nr. chars)	Min. Time (s)	Max. Time (s)	Avg. Time (s)	St. dev. (s)
10	0.117	1.985	0.421	0.248
100	0.136	5.648	0.825	0.633
1000	0.145	12.280	2.164	1.974
10000	0.211	120.131	17.250	16.586
20000	0.256	130.552	18.624	17.409
30000	0.312	386.629	55.786	55.534

Payload (nr. chars)	Min. Time (s)	Max. Time (s)	Avg. Time (s)	St. dev. (s)
10	0.147	21.304	3.269	3.207
100	0.211	90.639	12.315	13.092
1000	0.235	257.607	17.667	25.591
10000	1.126	2302.348	295.868	324.819
20000	2.460	3446.051	402.049	391.866
30000	6.574	6080.719	1457.376	1399.201



(a) (b)

Fig. 3: Broadcasting payloads (1000 tests performed for each payload) from (a) Workstation and (b) RPi on Chrysalis Tangle.

faster execution of PoW required for each payload attachment by the more capable devices. When considering small payloads (up to 1000 characters), the RPi can perform the PoW and transmit the data without significant hindrance. However, the RPi remains slower than the workstation by an average factor of ten. However, for larger payloads (more than 1000 characters), the performance gap becomes more pronounced, with the RPi being 17-26 times slower than the workstation on average. In terms of stability, smaller payloads exhibit minimal time variation and higher system stability. However, as the payload size increases, the variance in transmission time also increases for both the workstation and the RPi.

These findings provide valuable insights into the performance differences between powerful and low-power devices when broadcasting data on the IOTA Tangle.

5 Conclusion and Future Work

Secure storage of IoT devices' data is imperative in numerous IoT applications. In this paper, we have designed a system based on the nascent DLT IOTA Chrysalis that enables communication and securely stores heterogeneous devices' data. The system is not limited to powerful devices but can accommodate low-power devices such as RPi. We conducted detailed experiments by creating

and broadcasting different payloads from two machines to compare and analyze the support of IOTA Chrysalis. Results show practical compatibility of IOTA Chrysalis for low-power devices that can effectively create and broadcast different payloads, especially small ones typical for IoT devices, on the Chrysalis network without hindrance.

In the future, we will extend the designed system to accommodate more low-power IoT devices, such as sensors (i.e., CC2650 sensortag), to collect a large amount of real data and see its impact on the system.

References

1. Abdullah, S., Arshad, J., Khan, M.M., Alazab, M., Salah, K.: Prised tangle: a privacy-aware framework for smart healthcare data sharing using iota tangle. Complex & Intelligent Systems pp. 1–19 (2022)
2. Akhtar, M.M., Rizvi, D.R., Ahad, M.A., Kanhere, S.S., Amjad, M., Coviello, G.: Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy. Sensors **21**(13) (2021). https://doi.org/10.3390/s21134354, https://www.mdpi.com/1424-8220/21/13/4354
3. Bera, B., Saha, S., Das, A.K., Vasilakos, A.V.: Designing blockchain-based access control protocol in iot-enabled smart-grid system. IEEE Internet of Things Journal **8**(7), 5744–5761 (2021). https://doi.org/10.1109/JIOT.2020.3030308
4. Bernstein, D.J., Duif, N., Lange, T., Schwabe, P., Yang, B.Y.: High-speed high-security signatures. Journal of cryptographic engineering **2**(2), 77–89 (2012)
5. Bottone, M., Raimondi, F., Primiero, G.: Multi-agent based simulations of block-free distributed ledgers. In: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). pp. 585–590 (2018). https://doi.org/10.1109/WAINA.2018.00149
6. Brogan, J., Baskaran, I., Ramachandran, N.: Authenticating health activity data using distributed ledger technologies. Computational and Structural Biotechnology Journal **16**, 257–266 (2018). https://doi.org/https://doi.org/10.1016/j.csbj.2018.06.004, https://www.sciencedirect.com/science/article/pii/S2001037018300345
7. Chen, X., Nguyen, K., Sekiya, H.: Characterizing latency performance in private blockchain network. In: Mobile Networks and Management: 10th EAI International Conference, MONAMI 2020, Chiba, Japan, November 10–12, 2020, Proceedings 10. pp. 238–255. Springer (2020)
8. Conti, M., Kumar, G., Nerurkar, P., Saha, R., Vigneri, L.: A survey on security challenges and solutions in the iota. Journal of Network and Computer Applications **203**, 103383 (2022). https://doi.org/https://doi.org/10.1016/j.jnca.2022.103383, https://www.sciencedirect.com/science/article/pii/S1084804522000467
9. Fan, C., Khazaei, H., Chen, Y., Musilek, P.: Towards a scalable dag-based distributed ledger for smart communities. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). pp. 177–182 (2019). https://doi.org/10.1109/WF-IoT.2019.8767342
10. Foundation, I.: Energy consumption of iota 2.0: Continued energy efficiency with new protocol components (May 25, 2022), https://blog.iota.org/energy-consumption-of-iota-2-0/ (Accessed on 20 December, 2022)

11. Guo, F., Xiao, X., Hecker, A., Dustdar, S.: Characterizing iota tangle with empirical data. In: GLOBECOM 2020 - 2020 IEEE Global Communications Conference. pp. 1–6 (2020). https://doi.org/10.1109/GLOBECOM42002.2020.9322220
12. Huh, S., Cho, S., Kim, S.: Managing iot devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South). pp. 464–467 (2017). https://doi.org/10.23919/ICACT.2017.7890132
13. Kumar, G., Saha, R., Lal, C., Conti, M.: Internet-of-forensic (iof): A blockchain based digital forensics framework for iot applications. Future Generation Computer Systems **120**, 13–25 (2021). https://doi.org/https://doi.org/10.1016/j.future.2021.02.016, https://www.sciencedirect.com/science/article/pii/S0167739X21000686
14. Kusmierz, B., Sanders, W., Penzkofer, A., Capossele, A., Gal, A.: Properties of the tangle for uniform random and random walk tip selection. In: 2019 IEEE International Conference on Blockchain (Blockchain). pp. 228–236. IEEE (2019)
15. Li, Y., Cao, B., Peng, M., Zhang, L., Zhang, L., Feng, D., Yu, J.: Direct acyclic graph-based ledger for internet of things: Performance and security analysis. IEEE/ACM Transactions on Networking **28**(4), 1643–1656 (2020). https://doi.org/10.1109/TNET.2020.2991994
16. Marzouqi, S.A., Baddeley, M., Lopez, M.A.: Benchmarking performance of ethereum blockchain on resource constrained devices. In: 2022 Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench). pp. 12–16 (2022). https://doi.org/10.1109/CPS-IoTBench56135.2022.00009
17. Okegbile, S.D., Cai, J., Alfa, A.S.: Performance analysis of blockchain-enabled data-sharing scheme in cloud-edge computing-based iot networks. IEEE Internet of Things Journal **9**(21), 21520–21536 (2022). https://doi.org/10.1109/JIOT.2022.3181556
18. Popov, S.: The tangle. White paper **1**(3) (2018)
19. Suhail, S., Hussain, R., Khan, A., Hong, C.S.: Orchestrating product provenance story: When iota ecosystem meets electronics supply chain space. Computers in Industry **123**, 103334 (2020). https://doi.org/https://doi.org/10.1016/j.compind.2020.103334, https://www.sciencedirect.com/science/article/pii/S0166361520305686
20. Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B., Imran, M.A.: Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment. IEEE Internet of Things Journal **6**(3), 5791–5802 (2019). https://doi.org/10.1109/JIOT.2019.2905743
21. Ullah, Z., Raza, B., Shah, H., Khan, S., Waheed, A.: Towards blockchain-based secure storage and trusted data sharing scheme for iot environment. IEEE Access **10**, 36978–36994 (2022). https://doi.org/10.1109/ACCESS.2022.3164081
22. Wang, J., Wang, H.: Monoxide: Scale out blockchains with asynchronous consensus zones. In: NSDI. vol. 2019, pp. 95–112 (2019)
23. Wang, P., Xu, N., Zhang, H., Sun, W., Benslimane, A.: Dynamic access control and trust management for blockchain-empowered iot. IEEE Internet of Things Journal **9**(15), 12997–13009 (2022). https://doi.org/10.1109/JIOT.2021.3125091
24. Wang, S., Li, H., Chen, J., Wang, J., Deng, Y.: Dag blockchain-based lightweight authentication and authorization scheme for iot devices. Journal of Information Security and Applications **66**, 103134 (2022). https://doi.org/https://doi.org/10.1016/j.jisa.2022.103134, https://www.sciencedirect.com/science/article/pii/S2214212622000242