Secure and Authorized Data Sharing among different IoT Network Domains using Beez blockchain

1st Enrico Zanardo
Universitas Mercatorum
Rome, Italy
University of Nicosia
Nicosia, Cyprus
enrico.zanardo@studenti.unimercatorum.it

2nd Barbara Martini
Universitas Mercatorum
Rome, Italy
barbara.martini@unimercatorum.it

***Abstract*—This paper explores the feasibility of a novel concept aimed at enabling secure and authorized data sharing among different IoT networks belonging to different organizations or owners (i.e., domains), each hosting a multitude of Internet of Things (IoT) sensors. These sensors are capable of collecting various data points, including temperature, liquid levels, and environmental conditions, which can be used to represent specific objects (e.g., temperature, cup of coffee). The challenge lies in facilitating data exchange between sensors and objects residing on different networks while ensuring security and authorization for a predetermined period.**

To address this challenge, we propose a solution that leverages blockchain technology. Specifically, the permission and content of data sent from sensors or objects are stored in dedicated nodes, referred to as storage nodes, within a blockchain network. The rules governing access to this data are managed by seed nodes, also within the blockchain network. This innovative approach enables the management of permissions for external clients, such as web applications, to access the content of data transmitted by sensors, all while adhering to predefined rules encoded as custom transactions within the blockchain system. A proof-of-concept prototype is presented that has been developed and tested in a preliminary test campaign. The first round of experiments shows promising results in terms of scalability, throughput, and latency.

***Index Terms*—5G Cybersecurity, Blockchain, IoT access management**

I. Introduction

The fusion of Internet of Things (IoT) devices with high-speed, low-latency 5G (and upcoming 6G) networks, alongside the integration of Edge computing, has unleashed a new realm of data generation and pervasive intelligence. This convergence enables a spectrum of innovative services and applications across diverse sectors, spanning from industrial environments to smart cities, healthcare, and agriculture [1] [2]. The expansion of IoT has led to the creation of networks of devices that have resulted in a wealth of data that, if harnessed effectively, can drive innovation and efficiency [3].

Nevertheless, the rapid expansion of IoT devices has resulted in the development of fragmented networks, each producing significant amounts of data. This highlights the urgent requirement for secure and transparent methods of sharing data between different IoT domains. However, in the absence of a resilient framework for securely and openly exchanging data, there is the risk of constraining the full potential of IoT technology [4]. Indeed, sharing data among heterogeneous IoT networks is essential to gain meaningful insights, make informed decisions, and develop new intelligent applications [5]. On the other hand, this poses challenges related to privacy, security, and data governance [6].

This paper delves into the imperative challenge of facilitating secure and authorized data exchange among disparate IoT networks. Specifically, our focus is to bridge the gap between isolated Local Area Networks (LANs) housing myriad IoT sensors, each diligently gathering valuable information [7]. The aim of this work is to enable seamless and secure data interchange while upholding stringent security and authorization standards, particularly emphasizing the role of the Beez blockchain [8] in augmenting these capabilities.

Our proposed solution leverages the intrinsic strengths of blockchain technology, primarily focusing on the distinctive features of the Beez blockchain network, which was created by the main author of the proposed paper [8]. The Beez blockchain facilitates fine-grained control over data access, ensuring tamper-proof records of data transactions and establishing a trustworthy environment for all stakeholders involved in IoT data sharing.

In delineating the contributions of this study, we emphasize the novel adaptation and utilization of the Beez blockchain, specifically tailored for secure data sharing among IoT networks. It's important to clarify that our work extends beyond mere utilization; we introduce innovative enhancements or adaptations atop the Beez blockchain framework to address the challenges inherent in cross-network data sharing among IoT domains.

II. State of Art

In the swiftly evolving landscape of 5G/6G networks and Internet of Things (IoT) ecosystems, establishing robust data

access control mechanisms within blockchain systems has received considerable attention from academia and industry [9]–[12].

Recent research efforts in access control within blockchain networks have concentrated on enhancing granularity, crucial in the dynamic and heterogeneous nature of IoT environments on 5G/6G networks [13]–[16]. Advancements utilize smart contracts [17] to facilitate data sharing for IoT-based applications and implement complete access control in private blockchain settings [18]. Blockchain's decentralized and immutable ledger capabilities have heralded the utilization of smart contracts to codify access control rules [19]. They enable fine-grained access permissions, allowing data owners to define access conditions, potentially mitigating single points of failure and reducing reliance on centralized authorities.

In the domain of data security within blockchain systems, numerous works have addressed securing IoT data in the context of 5G/6G networks, employing novel cryptographic techniques [20]–[22]. Techniques like zero-knowledge proofs and homomorphic encryption enable secure computations on encrypted data, preserving confidentiality while facilitating authorized data sharing [23], [24]. Additionally, the integration of hardware-based security modules and consortium blockchains has strengthened overall security against adversarial attacks and unauthorized access [25]–[27].

User-centric data management solutions are gaining traction within blockchain systems, especially concerning IoT and 5G/6G networks [28]. These solutions prioritize user agency and control over data, allowing data owners to autonomously manage data-sharing preferences through blockchain-enabled frameworks [29]–[31]. Decentralized identity frameworks rooted in blockchain technology offer users greater control over their identities and data access permissions, aligning with privacy by design principles [32], [33].

However, while these existing works have made significant strides, there remains a need for scalability and user-centric data management solutions. Many scalable blockchains do provide fine-grained access control (e.g., projects from the Hyperledger foundation), but our proposed solution aims to offer a highly scalable blockchain architecture that efficiently manages consensus processes, ensuring responsive data sharing within the rapidly expanding IoT ecosystem. Moreover, our approach empowers users to define and enforce access rules, offering an elevated level of privacy and security unique to our proposal. Additionally, our solution uniquely integrates with 5G/6G networks, leveraging their low-latency and high-throughput capabilities to provide real-time data sharing, effectively addressing crucial gaps identified in the state of the art.

The objective of this study is to facilitate uninterrupted data transfer between isolated local area networks (LANs), ensuring stringent security measures and authorization protocols. This task involves enabling the exchange of data among sensors and objects located on distinct LANs within the IoT ecosystem.

III. Proposed Solution

The architectural framework, as depicted in Figure 1, introduces a solution addressing secure and authorized data sharing among disjoint LANs housing IoT sensors. This section outlines the architectural framework, functionality of key components, and sequential process from sensor data generation to management within the proposed blockchain network.

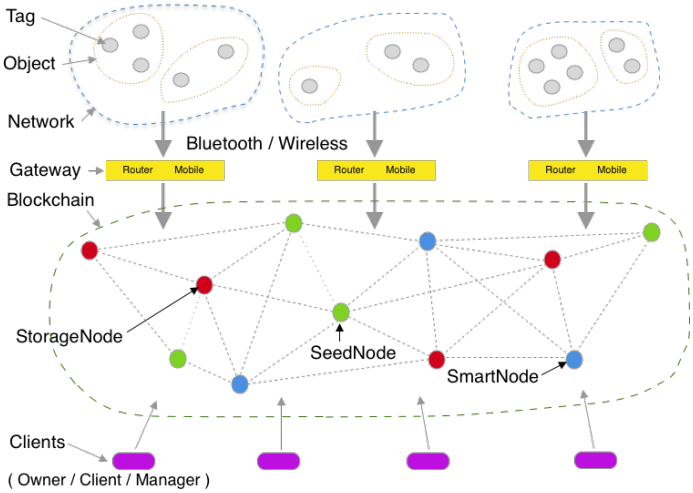

Fig. 1. Architectural Framework

A. Background and Beez blockchain Functioning

The proposed solution integrates the Beez blockchain as a fundamental element for data management and access control (depicted in Figure 1). Within this blockchain, three distinct node types exist: *Seed Nodes* responsible for consensus, *Storage Nodes* storing data, and *Smart Nodes* intended for domain-specific knowledge, currently non-operational.

The Beez consensus algorithm facilitates transactional consensus without a leader node, accommodating potential adversarial nodes and adverse network conditions. The protocol is asynchronous and can reach consensus with f failed nodes (including complete takeover by an attacker) as long as N is greater than $3*f$. Operating in distinct epochs, nodes engage in encrypted data transaction transmission and consensus establishment, ensuring consistency across nodes. It does not make any timing assumptions about message delivery. An adversary can control network scheduling and delay messages without impacting consensus. In order to achieve consensus, the Beez consensus protocol operates at distinct epochs. During each epoch, the nodes that are involved in the process engage in the act of transmitting a collection of encrypted data transactions to one another and subsequently reach a consensus regarding the specific contents of those transactions. In an ideal networking setting, the output encompasses the transmission of data from every individual node. Within a challenging context, the resulting outcome is a mutually accepted subset of information. Regardless of the approach taken, the output

obtained will consist of a set of transactions that are ensured to maintain consistency across all nodes.

B. Node Functionalities

In this context, in our proposed solution, the process commences with IoT sensors deployed across different LANs collecting diverse data points, such as temperature, liquid levels, and environmental conditions (gray dots in Figure 1). These sensors are tasked with representing specific objects (orange sets in Figure 1), thereby generating data of varying types. For instance, consider the scenario where a set of sensors monitors the temperature of a cup of coffee while another set measures room temperature in a separate LAN (blue sets in Figure 1).

As already mentioned above, the Beez blockchain is composed of three distinct types of nodes that, in the considered scenario, work as follows:

Seed Nodes: Maintain the blockchain ledger, facilitate consensus, and oversee access control rules, serving as governance guardians. They are in charge of communicating and gathering the data that the IoT devices send.

Storage Nodes: Securely store data transmitted by IoT sensors, ensuring availability and accessibility based on predefined access control rules. Encryption mechanisms protect stored data.

Smart Nodes: Intended knowledge repository utilizing a custom DSL for querying applications. They derive their knowledge from the syntactic data that the raw sensors send to the storage nodes.

C. Sequential Process Overview

The process flow within the Beez blockchain is as follows:

1) *Generation and Transmission of Sensor Data*: IoT sensors across distinct LANs collect data, relying on gateways for transmission to storage nodes.
2) *Blockchain Implementation*: Storage nodes process incoming data, encrypt it, and securely store it within the blockchain.
3) *Access Control and Permissions*: Seed nodes validate access requests based on encoded smart contract permissions, granting authorized users access to encrypted sensor data.
4) *Encryption and Data Retrieval*: Authorized users retrieve and decrypt data, ensuring secure and authorized access.

For instance, the sequential nature of this process can be demonstrated through the following example:

1) IoT sensors in LAN 1 record the temperature of a cup of coffee and transmit this data to a storage node within the blockchain.
2) IoT sensors in LAN 2 record the room temperature and transmit this data to a storage node within the blockchain.
3) The storage nodes process the incoming data, encrypt it, and store it securely on the blockchain.
4) The seed nodes are responsible for validating the authorizations of devices to transmit data and generating a new blockchain block.
5) A user or external client, such as a mobile app, seeks access to this temperature data. An access request is sent to a seed node for verification.
6) The seed node, acting as an access control authority, checks the permissions encoded in the blockchain's *smart contract*.
7) If the access request aligns with the predefined rules (e.g., authorized user, specific time frame), the seed node grants access to the encrypted temperature data from the sensors that are operating on two different LANs.
8) The authorized user retrieves the data, decrypts it, and displays the current temperature of the coffee and of the room.

In this case, the suggested blockchain-based architecture protects the data created by IoT sensors, only allows authorized users to access it, and keeps the data's privacy. This allows for safe and authorized sharing of data across different LANs and IoT environments in 5G/6G networks.

D. Achieving Secure Data Management

The proposed blockchain-based architecture ensures secure data storage, authorized access, and data privacy by employing encryption mechanisms, access control rules governed by smart contracts, and consensus-driven validation. However, detailed insights into the cryptographic methods employed, smart contract functionalities, and encryption mechanisms are further elaborated in subsequent subsections to provide a more comprehensive understanding of the proposed solution.

1) Cryptographic Methods Employed: The storage nodes have a crucial function in securely storing the data generated by IoT sensors within the Beez blockchain. In order to guarantee the confidentiality and integrity of data, the storage nodes utilize widely accepted encryption methods like Elliptic Curve Cryptography (ECC) [34]. Upon receiving sensor data, it is subjected to encryption using asymmetric encryption algorithms, resulting in the generation of encrypted data, which is then stored. Ensuring data confidentiality and integrity during storage, offering an extra level of protection against unauthorized access or tampering.

2) Smart Contract Functionalities: Smart contracts embedded within the Beez blockchain enforce access control policies. They contain predefined rules and permissions that govern data access by external entities or users. The smart contracts define the conditions under which data can be accessed, specifying parameters such as authorized users, time frames, and access rights. When an access request is made by an external client or user, the seed nodes interact with the smart contracts to validate the request against these predefined rules. If the request aligns with the encoded permissions, the seed nodes grant access to the encrypted sensor data stored across different LANs.

3) Encryption Mechanisms and Cryptography: Apart from the encryption employed within storage nodes, the proposed

solution ensures encrypted data transmission from IoT sensors to the storage nodes. When IoT sensors collect data, this data is encrypted before transmission to storage nodes through a secured gateway. This end-to-end encryption mechanism safeguards the data during its transit across LANs, preventing unauthorized interception or tampering. Moreover, the Beez consensus algorithm incorporates cryptographic mechanisms to facilitate secure transactions and consensus establishment. It utilizes cryptographic hashing functions [35] to ensure the integrity of transactions and consensus-related communication between nodes and between the communication from the IoT devices and the seed nodes. The algorithm employs cryptographic hashing to create a unique hash for each transaction, ensuring that data remains unchanged and verifiable across the blockchain network.

This combination of encryption mechanisms, smart contract functionalities for access control, and cryptographic methods within the Beez blockchain ensures robust security, data confidentiality, and authorized access to sensor-generated data across disparate LANs. These measures collectively contribute to the secure and authorized data sharing capabilities of the proposed solution within the context of 5G/6G networks and IoT environments.

IV. Experimental Evaluation

The experimental evaluation aims to validate and analyze the performance, security, and feasibility of the Beez blockchain concerning secure and authorized data sharing among disconnected IoT networks in 5G/6G environments.

A. Experimental Setup

The experimental setup, tailored for assessing the Beez blockchain within the context of the specific IoT application, is instantiated in Figure 1 (a specialized diagram for the chosen experimental configuration). This diagram illustrates the configured hardware components and their interconnections, providing a visual representation of the setup utilized for the experimental evaluation.

The main machine hosts the Beez blockchain, consisting of seed nodes and storage nodes deployed using Docker containers. The gateway, an iPhone Pro, collects Bluetooth data from IoT devices (Arduino BLE 33) and transmits it via a 5G network to the blockchain network for storage and access control evaluation. The IoT devices generate data packets simulating sensor data within the experimental setup.

The security evaluation of the Beez blockchain in this context encompasses assessing various aspects such as cryptographic strength, access control mechanisms, resistance to unauthorized access, and data integrity preservation during transmission and storage.

B. Data Generation and Access Control Policies

In the experimental setup, the Arduino BLE 33 microcontroller was programmed to generate data mimicking real-world scenarios encountered in IoT environments. Specifically, data packets encapsulating images captured by the OV7675

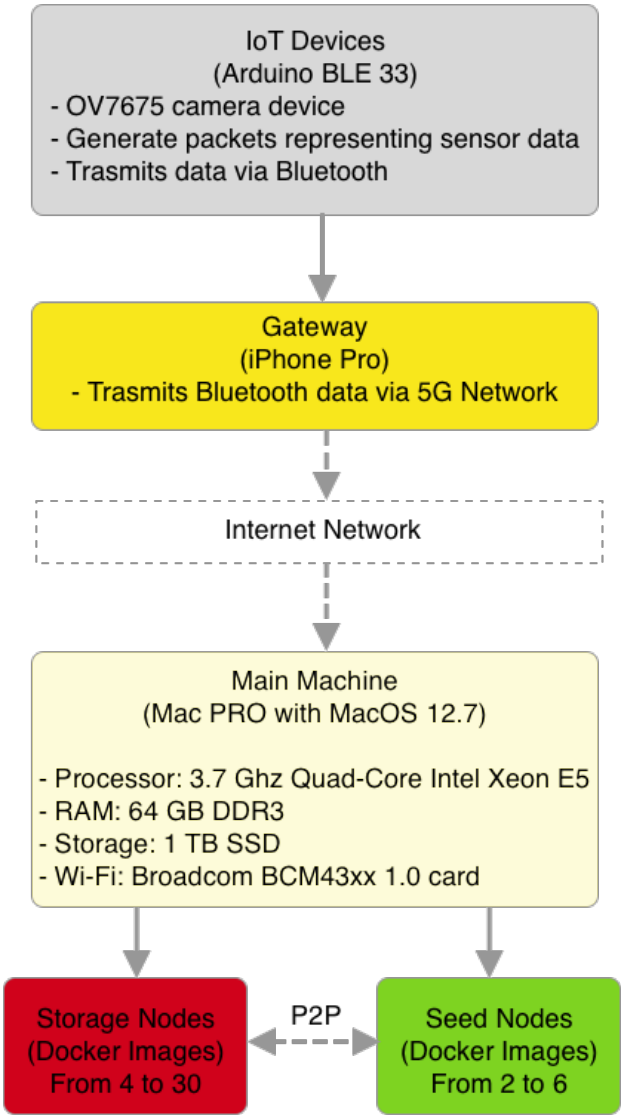

Fig. 2. Experimental Configuration

camera device were generated at a frequency of 1 image every 3 seconds, each image being about 350 kilobytes in size. This setup aimed to emulate typical data output from IoT sensors, providing a realistic basis for evaluating the blockchain's handling of sensor-generated data.

Additionally, through a REST API, external applications and users simulated access requests to sensor data kept on the Beez blockchain. Access control policies were configured using a role-based access control (RBAC) model (written into the smart contract), where permissions were defined based on user roles and specific data categories. For instance, authorized users with specific roles (e.g., administrators, analysts) were granted read or write access to designated data categories during predefined time intervals. These access control policies aimed to evaluate the granularity and effectiveness of the blockchain's access control mechanisms in enforcing predefined rules for data access.

V. Experiments and Results

Given the outlined evaluation framework, several experiments can be conducted to comprehensively assess the efficacy of the proposed blockchain-based solution for facilitating secure and authorized data sharing among disconnected Internet of Things (IoT) networks within the context of 5G/6G networks. The conducted experiments will yield empirical data and quantitative metrics, which can be utilized to construct graphical representations in the discussion section.

A. Throughput Level between the Network

The primary aim of this experiment is to assess the correlation between the data throughput of the system and the incremental growth in the number of IoT devices.

Procedure:

- Gradually increase the number of IoT devices (Arduino BLE 33 micro-controllers) in the testbed.
- Continuously generate and transmit data packets, mimicking sensor data, to the designated gateway.
- Record the data throughput (measured in Mbps) at different levels of IoT device saturation.

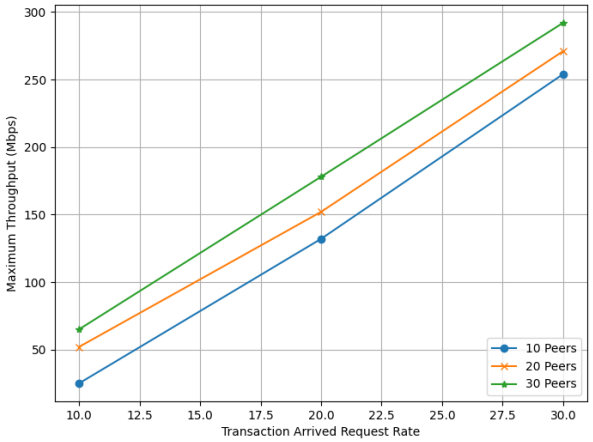

Fig. 3. Throughput Level between the Network

The illustration in Figure 3 depicts the IoT Device Processes executed by the distributed model that has been developed. When examining the process of identity verification and assessing transactions, the system's median execution time is a key factor that is considered. The duration of IoT Device Registration is predominantly occupied by the involvement of validator nodes, which are tasked with organizing, authorizing, and validating transactions. This observation has been made. The process of identifying IoT devices gets quicker due to the efficient storage of IoT node data within the blockchain network, ensuring immediate accessibility across all devices. IoT device authentication is characterized by its minimal time requirement.

Many Internet of Things (IoT) applications do not necessitate high data throughput. However, for devices that involve tasks such as streaming video or transmitting real-time data, speed becomes crucial [36]. The significance of data throughput becomes evident when considering the delivery of remote firmware updates, which serve to enhance device security, address software glitches, and introduce additional functionalities.

B. Network Latency

The objective of this experiment is to assess the system's latency performance under varying levels of load. Procedure:

- Simulate high loads on the blockchain network by continuously generating access requests from simulated users and external applications.
- Measure the response time (latency) for access requests to be processed by the storage nodes.
- Vary the load to simulate different traffic conditions.

In the conducted experiments, a block size of 201 KB was utilized to mitigate the impact of varying block sizes on network performance. This specific block size was chosen as a standardized parameter to maintain consistency and to avoid fluctuations in the block size, which could potentially affect the measured network performance metrics such as latency and throughput. By keeping a consistent block size across different conditions, the experiments aim to isolate the impact of other factors, ensuring that any observed changes in performance are attributed to the specific variables being tested (e.g., number of nodes, network load), rather than differences in block sizes. Figure 4 illustrates the network delay experienced by Beez blockchain during the completion of a consensus cycle, while the number of seed nodes ranges from 4 to 16.

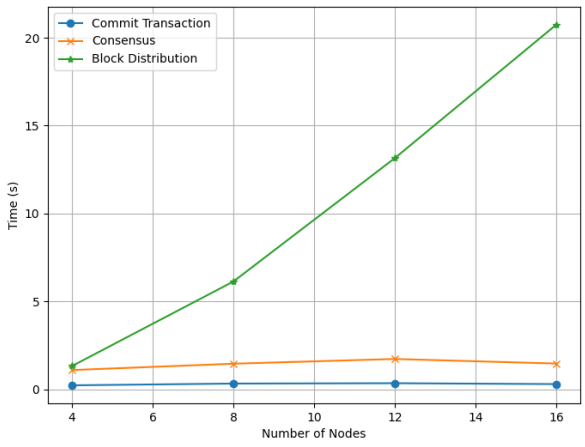

Fig. 4. Latency Times under Different Load Conditions

The latency of committing a transaction T_{ct} is used for evaluating the time for all nodes of the dynasty to accept a broadcasted transaction. Since the communication complexity of broadcasting transactions is $\mathcal{O}(K)$. The latency of block distribution is a linear scale to seed nodes K, and it varies from 132 ms to 207 ms, as the green line at the top of Fig 4 shows.

The orange line in the middle of Fig 4 indicates the latency of block consensus T_{bp} process. It evaluates how long the candidate blocks could be generated and verified by the forger. Since the consensus algorithm is proportional to the stake distribution D with expectation $E(D)$, the latency of block proposal is scale to communication complexity $\mathcal{O}(\frac{K^2}{E(D)})$, which varies from 1.09 s to 1.72 s. Finally, the latency of committing transaction distribution T_{tb} is the time it takes the broadcast a transaction among all nodes. The T_{tb} seams not influenced by the number of nodes. The time required for a transaction to be committed to a network consisting of 16 seed nodes was measured to be 0.29 seconds, whereas in the scenario with only 4 nodes, the latency was approximately 0.22 seconds.

C. Confidence Intervals

Confidence intervals are statistical tools utilized to quantify the degree of uncertainty or precision inherent in empirical data. Within the framework of our experimental investigations, the computation of confidence intervals serves the purpose of establishing a range of values that is highly probable to encompass the true population parameter.

Table I presents the confidence intervals, at 95%, for the experiment in section V-A under different conditions, namely 10 Nodes, 20 Nodes, and 30 Nodes. It is worth noting that in order to obtain more accurate confidence interval values, a larger sample size of data points is required.

TABLE I
95% CONFIDENCE INTERVAL - EXPERIMENT SECTION V-A

Nodes	Confidence Interval
10 Nodes	7.3384 – 266.6615
20 Nodes	34.2670 – 282.3995
30 Nodes	49.8955 – 306.7710

Table II presents the computed values of the 95% confidence intervals for each condition, namely Commit Transaction, Consensus, and Block Distribution. The calculation of values necessitates the inclusion of additional data and the adjustment of network settings to obtain a comprehensive understanding.

TABLE II
95% CONFIDENCE INTERVAL - EXPERIMENT SECTION V-B

Transaction	Confidence Interval
Commit Transaction	0.2089 – 0.3760
Consensus	1.0181 – 1.841
Block Distribution	-3.1400 – 23.8100

The accuracy of confidence intervals is contingent upon both the magnitude of the sample size and the extent of variability observed within the data collected during experimental procedures. Increasing the number of data points has the potential to enhance the accuracy of estimations and reduce the width of confidence intervals. The utilization of confidence intervals, in conjunction with hypothesis tests, facilitates a comprehensive statistical analysis of the experimental outcomes.

D. Comparative Evaluation

In order to conduct a comparative evaluation between Beez blockchain and established blockchain platforms, a series of experimental test cases were also performed on two blockchain benchmarks, namely Tendermint [37] and Ethereum [38]. In the context of the Tendermint test network, we established a network configuration consisting of 16 Docker containers running on the same main machine. These Docker containers were built on the Alpine Linux Arm64/v8 platform and served as validators. Additionally, we deployed a private Ethereum network comprising six Docker containers as miners and two separate machines as nodes. These Docker containers were also based on the Alpine Linux Arm64/v8 platform. In order to assess the overall efficacy of transaction execution on a blockchain, we define a specific testing scenario wherein a node initiates a batch of 2,000 transactions and subsequently monitors their successful inclusion in the blockchain. We perform a total of 100 test iterations using a predefined test scenario and subsequently analyze the outcomes with respect to various critical performance metrics. Table III presents a comprehensive assessment through the execution of test scenarios on various blockchain platforms.

TABLE III
COMPARATIVE EVALUATION ON DIFFERENT BLOCKCHAIN PLATFORMS

	Beez	Tendermint	Ethereum
Transaction (tx) committed time (s)	3.12	2.85	4.63
CPU usage (%)	5	28	100
Memory usage (MB)	24	66	1240

Tendermint utilizes a Byzantine Fault Tolerant (BFT) consensus protocol in order to attain deterministic finality. Consequently, the time taken for transaction commitment remains relatively consistent, approximately 3.12 seconds, which is notably lower compared to Beez blockchain and Ethereum. However, Beez blockchain exhibits advantages in terms of resource consumption, specifically in CPU and memory usage, as evidenced by the data presented in Table III. By employing a computationally demanding Proof-of-Work (PoW) consensus algorithm, the mining procedure in Ethereum effectively utilizes a significant portion of the CPU's processing capabilities and consumes approximately 1.24 GB of memory. Hence, the deployment of Ethereum miners on IoT devices with limited resources is deemed unsuitable. The utilization of lightweight consensus protocols enables Beez blockchain and Tendermint to attain efficiency in resource consumption on the host machine. Nevertheless, Beez blockchain demonstrates superior performance compared to Tendermint, as it consumes fewer resources on edge devices. For instance, Beez blockchain utilizes only 5% of CPU usage, which is equivalent to one-fifth of the resources consumed by Tendermint. Additionally, Beez blockchain requires a mere 24 MB of memory, which is less than half the amount utilized by Tendermint.

VI. Conclusions and Future works

The study presents an exhaustive evaluation of the Beez blockchain, highlighting its fine-grained access control, scalability, and adept latency management within the burgeoning IoT ecosystem. The assessment encompassed diverse experiments that shed light on functionality, performance, security, and constraints. Key insights from the findings include:

1) Scalability and Throughput: Beez demonstrated commendable scalability, showcasing increased data throughput with the expansion of IoT devices and seed nodes. This scalability is pivotal in accommodating the burgeoning IoT ecosystem within 5G/6G networks, facilitating efficient data sharing.

2) Latency Management: Even under varying load conditions, the system exhibited robust latency management, maintaining acceptable latency levels. This responsiveness is crucial for real-time applications, ensuring timely interactions despite high-load scenarios.

The Beez blockchain presents potential benefits for IoT applications, especially in user-centric data management and fine-grained control, addressing security and privacy concerns. However, challenges remain, particularly concerning efficiency and resource management.

A. Future Works

Future research endeavors could delve into an in-depth analysis of the targeted IoT application to extract underlying assumptions and specific security and functional requirements. Given the diverse specifics and unique requirements across different IoT networks, designing an architectural framework that accommodates and respects these assumptions and fulfills these varied requirements is crucial. Tailoring the Beez blockchain to meet such diverse demands would enhance its applicability and effectiveness within distinct IoT environments.

B. Conclusion and Prospects

The proposed blockchain-based solution holds promise for secure and authorized data sharing in 5G/6G-capable IoT environments, addressing challenges posed by IoT proliferation. Yet, practical implementation requires addressing resource needs, integration complexities, and blockchain latency. Future efforts should focus on these aspects to fully leverage blockchain technology for IoT data sharing. The Beez approach uniquely integrates with 5G/6G networks, leveraging their low-latency and high-throughput capabilities for real-time data sharing. This integration fills a critical gap in the current state of the art.

In summary, while the Beez blockchain demonstrates potential for IoT data sharing, overcoming challenges in resource management, integration, and latency is crucial for widespread adoption. Further research and development efforts should concentrate on addressing these challenges to fully harness blockchain technology's potential in the dynamic IoT and advanced network landscape. Integrating tailored solutions for diverse IoT network requirements would fortify the Beez blockchain's utility and relevance across various IoT domains.

References

[1] S. Noto, M. Gharbaoui, M. Falcitelli, B. Martini, P. Castoldi, and P. Pagano, "Experimental evaluation of an iot-based platform for maritime transport services," *Applied System Innovation*, vol. 6, no. 3, 2023.

[2] C.-Y. Chang *et al.*, "Performance isolation for network slices in industry 4.0: The 5growth approach," *IEEE Access*, vol. 9, pp. 166 990–167 003, 2021.

[3] S. Ugwuanyi, G. Paul, and J. Irvine, "Survey of iot for developing countries: Performance analysis of lorawan and cellular nb-iot networks," *Electronics*, vol. 10, p. 2224, 09 2021.

[4] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. PP, pp. 1–1, 03 2020.

[5] J. Byabazaire, G. O'Hare, and D. Delaney, "Data quality and trust: Review of challenges and opportunities for data sharing in iot," *Electronics*, vol. 9, no. 12, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/12/2083

[6] J. Zhou, Z. Cao, X. Dong, and A. Vasilakos, "Security and privacy for cloud-based iot: Challenges," *IEEE Communications Magazine*, vol. 55, pp. 26–33, 01 2017.

[7] J. Kang, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. PP, pp. 1–1, 10 2018.

[8] E. Zanardo, "Learningchain. a novel blockchain-based meritocratic marketplace for training distributed machine learning models," in *Software Engineering Application in Systems Design*, R. Silhavy, P. Silhavy, and Z. Prokopova, Eds. Cham: Springer International Publishing, 2023, pp. 152–169.

[9] B. Martini, P. Mori, F. Marino, A. Saracino, A. Lunardelli, A. L. Marra, F. Martinelli, and P. Castoldi, "Pushing forward security in network slicing by leveraging continuous usage control," *IEEE Communications Magazine*, vol. 58, no. 7, pp. 65–71, 2020.

[10] V. Messié, G. Fromentoux, X. Marjou, and N. L. Omnes, "Baladin for blockchain-based 5g networks," in *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2019, pp. 201–205.

[11] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. PP, pp. 1–1, 10 2019.

[12] K. Shafique, B. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios," *IEEE Access*, vol. PP, pp. 1–1, 01 2020.

[13] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. PP, pp. 1–1, 06 2018.

[14] W. Wang, H. Dinh Thai, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. PP, pp. 1–1, 01 2019.

[15] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A blockchain-enabled decentralized capability-based access control for iots," 07 2018.

[16] 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 of Things Journal*, vol. PP, pp. 1–1, 11 2020.

[17] D. Prata, H. Araújo, C. Santos, and P. Patel, "A literature review about smart contracts technology," *SSRN Electronic Journal*, vol. 8, pp. 1–4, 02 2021.

[18] D. Neyadi, D. Puthal, J. Dutta, and E. Damiani, *Role-Based Access Control in Private Blockchain for IoT Integrated Smart Contract*, 10 2023, pp. 227–245.

[19] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. PP, pp. 1–1, 10 2018.

[20] S. Bhatia, B. Mallikarjuna, D. Gautam, U. Gupta, S. Kumar, and S. Verma, "The future iot: The current generation 5g and next generation 6g and 7g technologies," 03 2023, pp. 212–217.

[21] N. Manoj Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in iot," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 06 2018.
[22] J. Sengupta, S. Ruj, and S. Dasbit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, 11 2019.
[23] C. Gentry, J. Groth, Y. Ishai, C. Peikert, A. Sahai, and A. Smith, "Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs," *Journal of Cryptology*, vol. 28, 04 2014.
[24] R. Lagendijk, E. Zekeriya, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, vol. 30, pp. 82–105, 01 2013.
[25] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, 06 2018.
[26] D. O'Leary, "Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems," *Intelligent Systems in Accounting, Finance and Management*, vol. 24, pp. 138–147, 10 2017.
[27] M. S. Ali, K. Dolui, and F. Antonelli, "Iot data privacy via blockchains and ipfs," 10 2017.
[28] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. PP, pp. 1–1, 07 2019.
[29] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 10 2017.
[30] Y. Ezawa, S. Kakei, Y. Shiraishi, M. Mohri, and M. Morii, "Blockchain-based cross-domain authorization system for user-centric resource sharing," *Blockchain: Research and Applications*, vol. 4, p. 100126, 01 2023.
[31] V. Jaiman, L. Pernice, and V. Urovi, "User incentives for blockchain-based data sharing platforms," *PLOS ONE*, vol. 17, p. e0266624, 04 2022.
[32] I. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. Qureshi, "Health-id: A blockchain-based decentralized identity management for remote healthcare," *Healthcare*, vol. 9, p. 712, 06 2021.
[33] A. Zwitter and J. Hazenberg, "Decentralized network governance: Blockchain technology and the future of regulation," *Frontiers in Genetics*, vol. 3, p. 12, 03 2020.
[34] A. Guru, H. Mohapatra, B. Mohanta, C. Altrjman, and A. Yadav, "A survey on consensus protocols and attacks on blockchain technology," *Applied Sciences*, vol. 13, p. 2604, 02 2023.
[35] X. Luo, H. Wang, D. Wu, C. Chen, M. Deng, J. Huang, and X.-S. Hua, "A survey on deep hashing methods," *ACM Transactions on Knowledge Discovery from Data*, vol. 17, 04 2022.
[36] R. Patan, K. Suresh, and M. Babu, "Real-time smart traffic management system for smart cities by using internet of things and big data," 10 2016, pp. 1–7.
[37] E. Buchman, J. Kwon, and Z. Milosevic, "The latest gossip on bft consensus," 2019.
[38] V. Buterin *et al.*, "Ethereum white paper."