Impacts of RBB Topology on Blockchain Scalability

Jeffson Celeiro Sousa*†, Bruno Evaristo*†, Antonio Mateus de Sousa*, Ismael Ávila* and Rayan G. Lima*
*Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
†Universidade Federal do Pará (UFPA)
Emails: {jcsousa, elderb, amateus, avila_an, rayang}@cpqd.com.br

***Abstract*—Decentralized Digital Identity (DDI) solutions are constantly evolving, and national-scale blockchain networks are beginning to develop their solutions. This article discusses the performance impact of the Indy Besu DDI framework deployed on the Rede Blockchain Brazil (RBB).**

***Index Terms*—Rede Blockchain Brazil, Blockchain, Scalability, Topology**

I. Introduction

The escalating demand for secure and interoperable digital services has propelled the adoption of governance models predicated on decentralized digital identities (DDIs), also known as Self-Sovereign Identity (SSI). In contrast to conventional centralized systems, SSI empowers individuals and organizations with direct control over their credentials and identities, fostering autonomy, portability, and enhanced security [1], [2].

Indy Besu is a framework that furnishes the requisite logic for managing decentralized digital identities within smart contracts executable on EVM-compatible blockchains, such as Besu itself. Its recent surge in exploration stems from its inherent flexibility, superior integration capabilities with extant systems, and leveraging the extensive developmental work already accrued on EVM-compatible networks.

Numerous government initiatives have emerged to implement DDI frameworks to protect citizens' data, exemplified by eIDAS 2.0 in the European Union. In Brazil, the Rede Blockchain Brazil (RBB), a permissioned public blockchain infrastructure established for the deployment of public interest applications, serves as a platform where DDI solutions based on IndyBesu are being developed.

The RBB implements a network topology based on the architecture proposed by LACChain [3]. Building upon the findings presented in [4], this article analyzes the potential impact of the network topology adopted by the RBB on the performance of Indy Besu smart contracts.

Specifically, this article elucidates how the RBB's topology, inspired by the LACChain architecture, influences the performance of the Indy Besu framework—a contemporary and EVM-compatible alternative for the management of decentralized digital identities (DDI).

II. RBB Architecture

In [5], a network topology was proposed specifically for permissioned public blockchains. This framework categorizes nodes into two main groups, each further divided into two types. Core Nodes are essential for the network's operation; without them, the blockchain cannot function. These nodes can be:

- Validator Nodes: These nodes actively participate in the network's consensus mechanism.
- Boot Nodes: These nodes act as a crucial connection point between the validator nodes and the satellite nodes.

Satellite Nodes extend the network's reach and functionality, and they are divided into:

- Writer Nodes: These nodes have write permissions on the network. They are typically responsible for submitting transactions, often originating from decentralized applications (DApps) and end-users.
- Observer Nodes: These nodes only have read permissions on the network. Critically, any entity can operate this type of node and connect to the network, which helps ensure its public nature.

Figure 1 illustrates the connections and interactions among these various node types within this architecture.

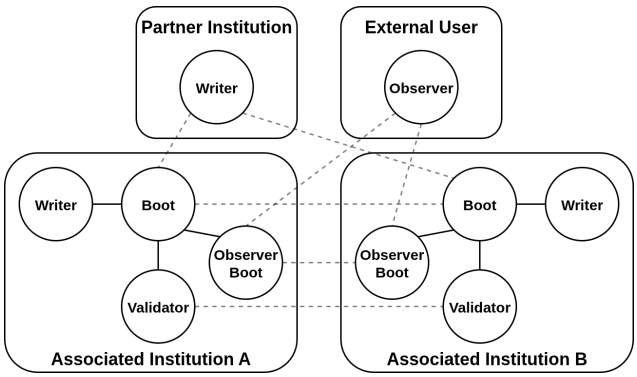

Fig. 1. RBB Topology

This topology significantly enhances legal accountability and promotes regulatory clarity. By restricting transaction initiation to Writer Nodes only, it simplifies the traceability of any transaction that might violate regulations such as GDPR (or Brazil's LGPD, which addresses private user data). Furthermore, this design also bolsters the security of Validator Nodes by reducing their exposure to external attacks, as they are exclusively connected to other participating institutions within the network.

2994-810X/25/$31.00 ©2025 IEEE
DOI 10.1109/ISSREW67781.2025.00057

III. Indy Besu Performance

The study [4] aimed to assess the performance of Indy Besu in comparison to Hyperledger Indy, specifically in terms of confirmed DDI operations per second on the network. To achieve this, two distinct simulation environments were configured, one for each DDI solution.

- Indy Besu: A Hyperledger Besu blockchain network was deployed on a dedicated server featuring Ubuntu 22.04, 32 GB of RAM, and 12 CPU cores. The network was configured with four validator nodes utilizing the QBFT consensus mechanism and two bootnodes, adhering to the official documentation's recommendations for production environments.
- Hyperledger Indy: Following the methodology presented in [6], a Hyperledger Indy network was deployed across four virtual machines, each with the following specifications: 4 vCPUs (Intel Xeon E312xx at 2.0 GHz), 4 GB of RAM, running Ubuntu 20.04. These nodes were configured as RBFT validators within a permissioned network.

Subsequently, the Hyperledger Caliper benchmarking tool was employed to generate the workload for both environments and collect the transaction throughput metric.

The results indicate that Indy Besu is more scalable than Hyperledger Indy in permissioned networks, demonstrating up to a 600% gain in throughput for DDI operations. This shows that Indy Besu's advantages extend beyond flexibility, interoperability, and standard compliance; it also boasts superior scalability compared to Hyperledger Indy. However, the network's topology can significantly affect this performance, especially in high-demand scenarios like those envisioned by national and international DDI initiatives.

IV. Impacts of RBB Topology on Blockchain Scalability

This work underscores the importance of performance evaluations as a key technical criterion for adopting decentralized digital identity (DDI) solutions in large-scale environments, with a particular focus on the Indy Besu framework. Initiatives like eIDAS 2.0 in the European Union and Brazil's Rede Blockchain Brazil (RBB) both face the challenge of providing infrastructure for millions of users, making scalability a central requirement.

While blockchain scalability is widely discussed in literature, with solutions like sharding (layer-1) and rollups (layer-2), these approaches rarely consider the specifics of permissioned networks. These include access restrictions, role separation, and controlled topologies.

A blockchain network's topology directly influences its performance in terms of scalability. It dictates how messages—transactions and blocks—circulate among nodes. In poorly distributed networks or those with bottlenecks, block propagation can be slow, limiting the number of transactions confirmed per second (TPS). This impact is even more pronounced in topologies with communication concentration, such as those based on central nodes or star models, which are prone to overload.

Furthermore, in permissioned networks that adopt role separation, as used in the RBB, scalability can be structurally constrained. Delegating write permissions solely to specific Writer Nodes enhances governance and legal security, but it sacrifices the ability to parallelize input operations, potentially creating bottlenecks. The presence of bootnodes as intermediaries between Writers and Validators also increases communication hops, which can affect throughput, especially if these intermediaries are poorly sized or distributed.

Another significant factor is the geographical distribution of nodes. When topology disregards the physical proximity between participants, latency increases, and consensus time can be compromised, hindering scalability even in networks with efficient consensus mechanisms. Additionally, an excessive number of connections (like in fully connected mesh networks) might offer resilience but also introduce communication overhead, necessitating a balance between efficiency and fault tolerance.

Therefore, when evaluating blockchain performance—especially in contexts like decentralized digital identities—it's crucial to consider not just the consensus algorithm or smart contract logic, but also how the network is structured and interconnected. Topology, often overlooked, can be decisive for the success of large-scale solutions.

V. Conclusion

The results from [4] show significant performance gains with Indy Besu, but they also highlight the need for more in-depth studies on the impact of network topology, especially within architectures like the one proposed by [5]. The maturity of these solutions hinges not only on technical advancements but also on understanding how the network model affects the ability to scale securely and efficiently.

References

[1] C. Allen, "The path to self-sovereign identity," *Life with Alacrity Blog*, 2016. [Online]. Available: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[2] W3C, "Verifiable credentials data model 1.1," https://www.w3.org/TR/vc-data-model/, 2022, w3C Recommendation.

[3] M. Allende López, "Lacchain framework for permissioned public blockchain networks: From blockchain technology to blockchain networks," 2021. [Online]. Available: https://doi.org/10.18235/0003747

[4] J. Sousa, B. Evaristo, A. Sousa, and I. Ávila, "Avaliação de performance de contratos de identidade digital descentralizada em redes blockchain baseada em ethereum," in *Anais do VIII Workshop em Blockchain: Teoria, Tecnologias e Aplicações*. Porto Alegre, RS, Brasil: SBC, 2025, pp. 57–69. [Online]. Available: https://sol.sbc.org.br/index.php/wblockchain/article/view/35467

[5] M. A. López, "Lacchain framework for permissioned public blockchain networks: From blockchain technology to blockchain networks," 2021.

[6] M. Bastos, A. Veloso, J. Sousa, B. Evaristo, D. Abreu, and A. Abelém, "Minindy: Automating the deployment and management of hyperledger indy networks," in *11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2024.