Distributed Spectrum Coordination using Decoupled Permissioned Blockchains

Alan Veloso[1,2], Jeffson Sousa[1,3], Filipe Saraiva[1], Antônio Abelém[1]

[1] Federal University of Pará (UFPA)
Belém – PA – Brazil

[2]National Education and Research Network (RNP)
Rio de Janeiro – RJ – Brazil

[3]Center for Research and Development in Telecommunications (CPQD)
Campinas – SP – Brazil

aveloso@ufpa.br, jcsousa@cpqd.com.br
saraiva@ufpa.br, abelem@ufpa.br

Abstract. *While decentralized Dynamic Spectrum Access (DSA) improves multi-operator coordination, existing blockchain solutions are slow because they tightly couple consensus mechanisms with time-sensitive radio operations. To overcome this bottleneck, we propose a hybrid architecture that logically decouples these planes, ensuring that only normatively relevant state transitions (e.g., spectrum grants) require synchronous blockchain validation. Informational requests and routine heartbeats are processed entirely off-chain to minimize latency. By using a permissioned blockchain and smart contracts selectively, our system maintains a secure and consistent World State without stalling continuous radio operations. Experimental evaluations demonstrate that confining distributed consensus (averaging 1.8s latency) to critical operations successfully replaces implicit trust with algorithmic guarantees, remaining fully compatible with CBRS/SAS latency budgets.*

1. Introduction

Radio spectrum is a finite natural resource and a critical infrastructure for the digital economy [Akyildiz et al. 2006]. Traditional spectrum management relies on a command-and-control model, where frequency bands are statically assigned to licensed users [Federal Communications Commission 2002]. However, the rapid growth of wireless connectivity driven by 5G and IoT has exposed the inefficiency of this model, leading to artificial scarcity and underutilization of spectrum resources [President's Council of Advisors on Science and Technology 2012].

Dynamic Spectrum Access (DSA) addresses this limitation by enabling opportunistic spectrum sharing. A prominent realization is the Citizens Broadband Radio Service (CBRS), which introduces the Spectrum Access System (SAS) to coordinate spectrum usage among multiple users [Federal Communications Commission 2015]. However, in multi-operator environments, existing coordination mechanisms based on periodic synchronization or peer-to-peer exchange fail to guarantee real-time consistency, leading to temporary divergence in the global spectrum state.

Such inconsistencies may result in overlapping allocations and harmful interference. Moreover, current approaches rely on implicit trust and lack robust mechanisms for

integrity, validation, and auditability, making it difficult for regulators to reliably reconstruct allocation events.

Recent decentralized solutions attempt to address these limitations by introducing blockchain-based coordination. However, many approaches tightly couple distributed consensus with latency-sensitive radio operations, resulting in delays that are incompatible with the requirements of modern wireless systems.

Therefore, the key challenge is to ensure a consistent, secure, and auditable global view of spectrum usage in decentralized multi-operator environments while preserving strict latency constraints. In this context, we investigate how to mitigate the double-spending problem in dynamic spectrum access without compromising system performance.

This work proposes a distributed architecture based on a permissioned blockchain acting as a shared and trusted ledger. The core design principle is the decoupling of radio operations from regulatory governance. Latency-sensitive processing remains local, while spectrum validation and global state synchronization are handled through the blockchain.

Smart contracts enforce spectrum policies, providing immutability, non-repudiation, and consistent state across operators. The main objective is to design and evaluate a blockchain-based architecture that ensures consistency, integrity, and security in multi-operator environments, while maintaining practical latency requirements. The main contributions of this work are:

- **Hybrid Distributed Architecture:** Separation of latency-sensitive radio operations from consistency-oriented governance mechanisms.
- **Deterministic Conflict Prevention:** Smart contract-based model that prevents conflicting spectrum allocations.
- **Efficient Synchronization Model:** Event-driven state propagation that reduces communication overhead.
- **Resilience and Fault Tolerance:** Quorum-based coordination without single points of failure.
- **Performance Evaluation:** Comparative analysis between REST and blockchain-based approaches, quantifying trade-offs between consistency, latency, and scalability.

The remainder of this paper is organized as follows. Section 2 reviews existing approaches to spectrum coordination, with emphasis on decentralized solutions. Section 3 presents the proposed architecture and its operational model. Section 4 describes the experimental methodology and presents the performance results. Finally, Section 5 concludes the paper, discussing practical implications and outlining future research directions.

2. Related Work

Existing approaches for dynamic spectrum access can be categorized as centralized, federated, and decentralized. Centralized models (e.g., TV White Space and Licensed Shared Access, LSA) rely on a single authority, ensuring control but introducing a single point of failure and requiring implicit trust. Federated models, such as CBRS/SAS, distribute

control across multiple administrators, but rely on periodic synchronization, leading to eventual consistency and limited auditability.

Recent research has shifted toward decentralized approaches, which replace implicit trust with cryptographic guarantees and distributed consensus [Al-Matari et al. 2024]. These architectures use shared ledgers to maintain a global view of spectrum usage across operators.

As shown in Table 1, existing decentralized solutions either lack robust global state synchronization or tightly couple consensus with latency-sensitive radio operations. In contrast, this work explicitly decouples radio control from distributed consensus while maintaining strong consistency and supporting multi-operator environments.

Table 1. Comparison of decentralized approaches for dynamic spectrum access.

Work	System	Technology	Prototype	State Sync	Evaluation	Multi-Operator	Decoupling
[Curran et al. 2019]	Radio Allocation	SMPC	Yes	No	Simulation	Partial	No
[Wu et al. 2022]	Trusted Coordination	TEE + SMPC	Yes	No	Experimental	Yes	No
[Grissa et al. 2019]	SAS (CBRS)	Permissioned Blockchain	Yes	Yes	Experimental	Partial	No
[Xiao et al. 2023]	SAS (CBRS)	Permissioned Blockchain	Yes	Partial	Prototype	Yes	No
[Wang et al. 2024]	Inter-tier CBRS	Blockchain	Yes	Partial	Performance Test	Yes	No
[Li et al. 2023]	LSA	Blockchain	No	No	Simulation	Yes	No
[Muntaha et al. 2025]	5G SA Sharing	Hybrid DLT	Yes	No	Experimental	Yes	No
[Yan et al. 2026]	6G DSS	Sharded DLT	No	No	Simulation	Yes	No
[Zhang et al. 2022]	6G IoT DSS	DAG-based Ledger	No	No	Simulation	Yes	No
[Ye et al. 2022]	IoT DSS	Blockchain	No	No	Simulation	Yes	No
This Work	Decoupled SAS	Permissioned Blockchain	**Yes**	**Yes**	**Experimental**	**Yes**	**Yes**

Decentralized solutions can be grouped into non-DLT and DLT-based approaches. Non-DLT techniques, such as SMPC and TEEs, improve privacy and correctness but do not provide an immutable and globally verifiable history, limiting their use for regulatory auditing.

DLT-based solutions, particularly blockchain, provide auditability, transparency, and non-repudiation. Systems such as TrustSAS and BD-SAS use smart contracts to automate allocation and enforce policies. However, these approaches often tightly couple consensus with radio operations, introducing delays incompatible with time-sensitive wireless systems and raising scalability concerns.

These limitations highlight an unresolved trade-off between consistency, latency, and scalability. This work addresses this gap by proposing a hybrid architecture that decouples radio control from distributed consensus, enabling strong consistency and auditability while preserving latency requirements.

3. Proposed Architecture

This work proposes a distributed architecture for dynamic spectrum coordination based on a permissioned blockchain acting as a shared and trusted ledger. The architecture ensures global consistency and auditability in multi-operator environments while preserving the operational requirements of radio access networks.

The system is organized into two logically decoupled planes (Figure 1): (i) a *radio control plane*, responsible for local spectrum analysis and device interaction, and (ii) a *coordination plane*, responsible for validation, synchronization, and global state persistence through the blockchain network. The architecture is composed of four main components:

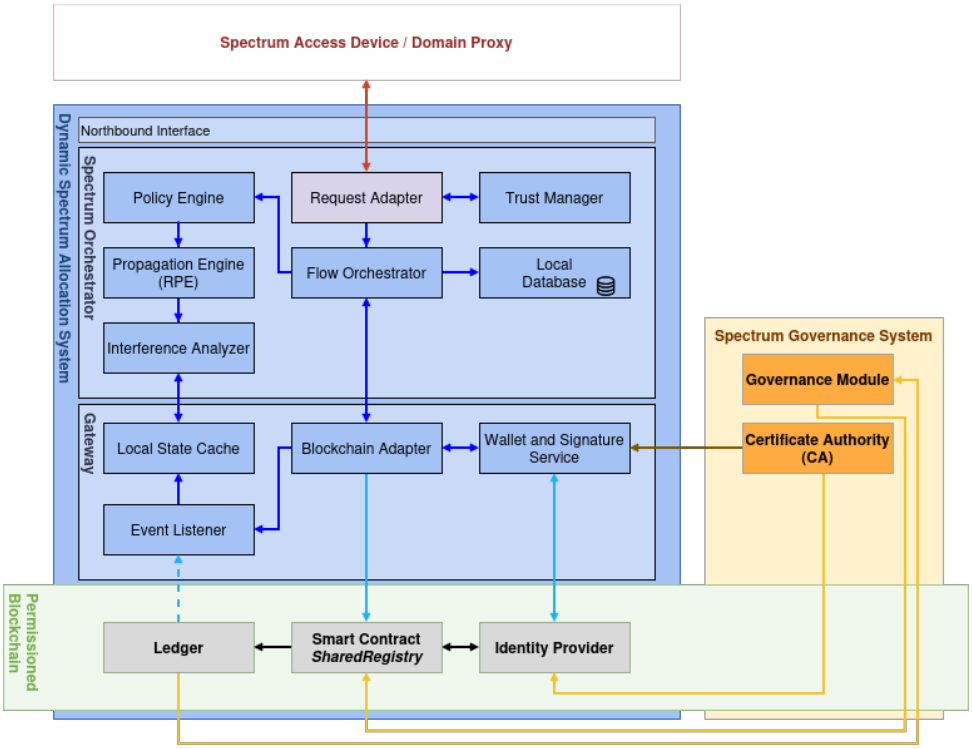


Figure 1. Proposed distributed architecture with decoupled radio control and blockchain-based coordination.

- **Spectrum Orchestrator:** Responsible for radio decision-making and spectrum allocation based on local conditions. It processes device requests, applies interference mitigation mechanisms, and enforces regulatory constraints at the operational level.
- **Gateway:** Acts as the integration layer between the radio domain and the blockchain network. It translates spectrum management operations into blockchain transactions, manages cryptographic identities, and maintains cached state to optimize local performance.
- **Permissioned Blockchain:** Provides a distributed and immutable ledger that maintains a globally consistent view of spectrum usage. Smart contracts validate allocations, enforce conflict constraints, and ensure transaction ordering across operators.
- **Spectrum Governance System (SGE):** Defines and enforces regulatory policies, manages system participation, and controls the trust infrastructure (e.g., PKI). It can issue governance actions, such as revoking operator permissions or updating regulatory parameters, which are recorded on-chain.

3.1. Operational Model

The system follows a hybrid off-chain/on-chain workflow, where only normatively relevant operations require blockchain validation. The main operations are defined as follows:

- **Spectrum Inquiry:** A device requests candidate channels from the local operator. This operation is purely informational and does not modify the global state, being handled entirely off-chain with latency dominated by local processing.

- **Grant Request:** The operator performs local validation based on radio conditions and regulatory constraints. If admissible, the request is submitted to the blockchain, where smart contracts validate conflict conditions and persist the allocation. The grant becomes effective only after ledger confirmation.
- **Heartbeat:** Periodic updates are processed locally as long as they do not introduce changes to the global state. Blockchain interaction is only required when relevant state transitions occur.
- **Relinquishment:** The device may immediately stop transmission locally. The release of spectrum resources is propagated asynchronously through the blockchain, ensuring eventual global consistency without blocking the operation.

The smart contract (e.g., `SharedRegistry`) enforces policies through deterministic validation rather than heavy radio physics calculations. It employs a discrete geospatial indexing system (such as S2[1] or H3[2]) to map the space-frequency binomial into unique hashes, it strictly prevents double-spending. Any simultaneous attempts to allocate the same index are deterministically rejected via read/write set version conflicts during consensus. Finally, the contract verifies the proposing system's authorization before persisting allocations to the World State.

4. Experimental Evaluation

This section evaluates the performance of the proposed decentralized spectrum coordination architecture, comparing a permissioned blockchain implementation (Hyperledger Besu with QBFT consensus) against a traditional centralized REST-based approach.

4.1. Methodology

This evaluation compares a permissioned blockchain-based architecture (Hyperledger Besu with QBFT consensus) with a traditional centralized REST-based approach, focusing on latency, throughput, and synchronization efficiency.

Experiments were conducted in a controlled virtualized environment using QEMU/KVM. The setup consists of four virtual machines acting as independent spectrum administrators and blockchain validators (2 vCPUs, 4 GiB RAM each), and a dedicated load generator (16 vCPUs, 8 GiB RAM). One node also hosts the application Gateway, which translates REST requests into blockchain transactions.

The blockchain network was configured with QBFT consensus, a 2-second block interval, and pre-allocated accounts to ensure uninterrupted execution. These parameters were selected to provide a stable and representative baseline rather than an optimized configuration. Workloads were generated using Apache JMeter to capture end-to-end behavior, including middleware and communication overhead. The load scales from 2 to 100 concurrent virtual devices across five scenarios (*Low*, *Medium*, *High*, *Stress*, and *Extreme*), executed under burst conditions (zero ramp-up).

Only operations that result in persistent state changes (e.g., grant and relinquishment) were included in the critical path. Informational operations such as inquiry and routine heartbeat messages were excluded, as they do not consistently require blockchain

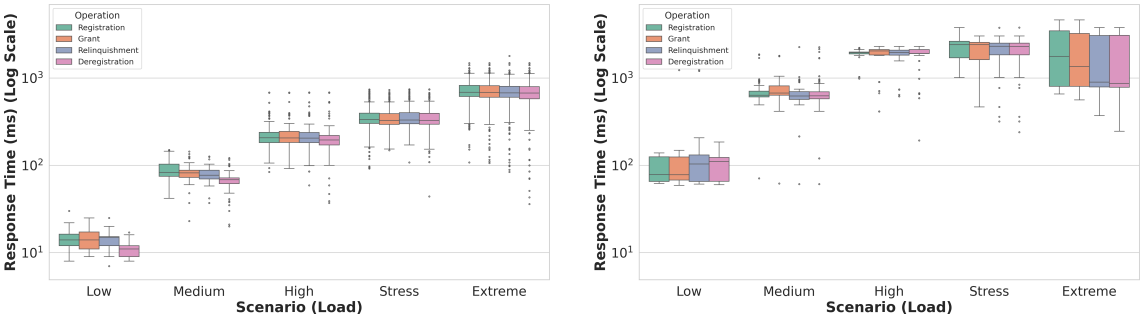
[1] `https://s2geometry.io/`

[2] `https://www.uber.com/en-BR/blog/h3/`

interaction. Latency measurements capture the full execution path, from REST request reception at the Gateway to transaction confirmation in the blockchain.

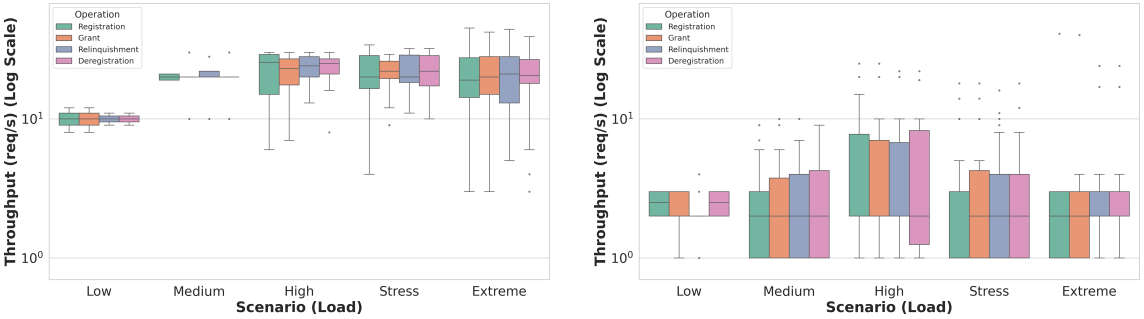
4.2. Latency and Throughput Results

Figure 2 presents the latency distributions, while Figure 3 shows the throughput behavior for both REST and blockchain-based approaches across different load scenarios. Under extreme conditions, the REST-based system stabilizes at approximately 22 requests per second (req/s), while the blockchain-based architecture achieves around 3.3 req/s. The REST approach maintains an average latency of approximately 700 ms in the extreme scenario. In contrast, the blockchain-based system presents latencies between 1.7 s and 2.1 s (approximately 1.8 s on average), with peaks reaching up to 16 s during synchronized bursts of requests.



(a) REST **(b) Blockchain**

Figure 2. Latency distribution across different load scenarios.



(a) REST **(b) Blockchain**

Figure 3. Throughput distribution across different load scenarios.

The REST system behaves similarly to a classical queuing system under continuous demand, supporting increased load through a linear degradation in latency while maintaining stable throughput. In contrast, the blockchain-based system degrades nonlinearly due to its batch-based processing model, with a fixed block interval of 2 seconds. Under peak load, latency is dominated by the accumulation of transactions in the mempool, which may require multiple block cycles for inclusion.

The latency observed in the blockchain-based approach is compatible with spectrum coordination systems such as CBRS/SAS, where timing constraints allow heartbeat

intervals of up to 240 s. However, the computational cost of distributed consensus renders the current architecture unsuitable for strict near-real-time control loops requiring sub-second responses.

While the proposed architecture successfully enforces global consistency, the observed latency peaks (up to 16 s) under extreme load expose the inherent scalability limitations of the baseline QBFT consensus in high-density deployments. It is crucial to clarify, however, that this latency does not lead to simultaneous allocations or harmful interference. Because the decoupled operational model dictates that a spectrum grant only becomes effective after on-chain confirmation, the penalty for processing delays is strictly an extended waiting period for the requesting device, preventing any collision state. Nevertheless, in a massive operational deployment with thousands of simultaneous users, this access delay could trigger application-layer timeouts. Mitigating this limitation requires transitioning to high-throughput execute-order-validate architectures or exploring layer-2 scaling solutions to handle massive concurrent requests without stalling the spectrum access.

5. Conclusion

This work demonstrated the feasibility of replacing implicit trust in multi-operator environments with an algorithmic, blockchain-based architecture that decouples radio operations from governance. Since Section 4.2 already discusses these numbers and the queuing behavior, the conclusion does not need to repeat them. Simply state conclusively that the tests validate that the latency meets the time budgets of CBRS/SAS, making it ideal for fixed infrastructure, but inadequate for sub-second control loops like Open RAN.

Future work will investigate execute-order-validate architectures (e.g., Hyperledger Fabric) to improve parallelism and throughput, as well as extend the evaluation to geographically distributed testbeds to assess consensus behavior under WAN conditions and integration with real radio systems. Additionally, it will characterize resource consumption (CPU, memory, and I/O) under long-term operation to define deployment requirements, and perform sensitivity analysis of blockchain parameters (e.g., block interval and gas limits) to identify optimal configurations for different regulatory scenarios.

Acknowledgements

This work was supported in part by the National Council for Scientific and Technological Development (CNPq) under Grants 403539/2020-0 and 400111/2023-3; by the Coordination for the Improvement of Higher Education Personnel (CAPES); and by the São Paulo Research Foundation (FAPESP) under grants 2023/00811-0, 2023/00673-7, 2021/00199-8 (CPE SMARTNESS), 2020/04031-1, and 2018/23097-3. It also received support from the Fund for the Technological Development of Telecommunications (Funttel), the Funding Authority for Studies and Projects (Finep) – Ministry of Science, Technology, and Innovation, and the Telecommunications Research and Development Center (CPqD).

References

Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., and Mohanty, S. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks*, 50(13):2127–2159.

Al-Matari, N. Y., Zahary, A. T., and Al-Shargabi, A. A. (2024). A survey on advancements in blockchain-enabled spectrum access security for 6g cognitive radio iot networks. *Scientific Reports*, 14(30990).

Curran, M., Liang, X., Gupta, H., Pandey, O., and Das, S. R. (2019). Procsa: Protecting privacy in crowdsourced spectrum allocation. In *Proceedings of Privacy Enhancing Technologies*.

Federal Communications Commission (2002). Spectrum Policy Task Force Report. Technical Report ET Docket No. 02-135, FCC, Washington, D.C.

Federal Communications Commission (2015). Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band. Report and Order FCC 15-47, FCC, Washington, D.C.

Grissa, M., Yavuz, A. A., and Hamdaoui, B. (2019). Trustsas: A trustworthy spectrum access system for the 3.5 ghz cbrs band. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 1495–1503.

Li, Z., Wang, W., Wu, Q., and Wang, X. (2023). Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework. *IEEE Transactions on Cognitive Communications and Networking*, 9(1):3–15.

Muntaha, S. T., Ahmed, Q. Z., Khan, F. A., Zaharis, Z. D., and Lazaridis, P. I. (2025). Hybrid blockchain-based multi-operator resource sharing and sla management. *IEEE Open Journal of the Communications Society*, 6:362–377.

President's Council of Advisors on Science and Technology (2012). Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth. Technical report, Executive Office of the President of the United States, Washington, D.C.

Wang, S., Sun, C., Li, H., and Cui, T. (2024). Cross-tier coordination in spectrum sharing: A blockchain approach. In *2024 International Conference on Computing, Networking and Communications (ICNC)*, pages 910–914.

Wu, P., Ning, J., Shen, J., Wang, H., and Chang, E.-C. (2022). Hybrid trust multi-party computation with trusted execution environment. *IEEE Access*.

Xiao, Y., Shi, S., Lou, W., Wang, C., Li, X., Zhang, N., Hou, Y. T., and Reed, J. H. (2023). Bd-sas: Enabling dynamic spectrum sharing in low-trust environment. *IEEE Transactions on Cognitive Communications and Networking*, 9(4):842–855.

Yan, K., Ma, W., Sun, S., and Wang, W. (2026). Blockchain-based dynamic spectrum sharing for service-centric 6g networks: An evolutionary approach. *IEEE Transactions on Network Science and Engineering*, 13:485–500.

Ye, J., Kang, X., Liang, Y.-C., and Sun, S. (2022). A trust-centric privacy-preserving blockchain for dynamic spectrum management in iot networks. *IEEE Internet of Things Journal*, 9(15):13263–13278.

Zhang, H., Leng, S., Wu, F., and Chai, H. (2022). A dag blockchain-enhanced user-autonomy spectrum sharing framework for 6g-enabled iot. *IEEE Internet of Things Journal*, 9(11):8012–8023.