Towards Enabling Blockchain-based Circuit Allocation in MEICAN for Secure Auditing and Network Governance

Gessica Franciéle Mendonça Azevedo[1], **Muriel Figueredo Franco**[2], **Lisandro Z. Granville**[1], **Eder John Scheid**[1]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre – RS – Brazil

[2]Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)
Porto Alegre – RS – Brazil

{gessica.azevedo, granville,ejscheid}@inf.ufrgs.br

muriel.franco@ufcspa.edu.br

Abstract. *This paper presents a solution for managing circuit requests in MEICAN, using smart contracts and decentralized storage through IPFS. The architecture integrates a Solidity smart contract, an API for interacting with the blockchain and IPFS, and web interfaces that simulate the circuit request and approval workflows. The evaluation was conducted in terms of gas consumption, demonstrating the feasibility of the approach for recording requests in a transparent, auditable, and immutable manner across inter-domain environments.*

Resumo. *Este artigo apresenta uma proposta de uma solução para o gerenciamento de solicitações de circuitos no MEICAN, utilizando contratos inteligentes e armazenamento descentralizado via IPFS. A arquitetura integra um contrato inteligente em Solidity, uma API, para interação com a blockchain e o IPFS, e interfaces web para simular os fluxos de requisição e aprovação de circuitos. A avaliação foi conduzida em termos de consumo de gas, demonstrando a viabilidade da abordagem para registrar solicitações de forma transparente, auditável e imutável em ambientes interdomínios.*

1. Introduction

The growing interconnectivity among academic and research institutions has created a need for solutions that can securely and efficiently maintain network circuits, particularly when these circuits traverse multiple administrative domains [Asharov et al. 2017]. The Management Environment of Inter-domain Circuits for Advanced Networks (MEICAN) project, for example, is a system designed to provide orchestration and automation of network circuit reservations between institutions [Wickboldt et al. 2018]. However, the current process for registering and approving circuits is performed in a centralized manner and does not provide an immutable mechanism for verification or public auditing. Moreover, centralized systems inherently concentrate control and data, which can introduce single points of failure and increase the risk of compromise [Goel and Rahulamathavan 2024].

Similar challenges arise in Federated Coalition Networks (FCNs), where entities from multiple nations must cooperate while retaining control over their respective systems. This scenario requires enhanced security, trust, and resilience in multi-domain

management [Álvaro González et al. 2025]. In response to the inherent difficulties of ensuring integrity and traceability, particularly in decentralized or multi-domain processes, technologies such as blockchain and smart contracts have emerged as promising solutions [Akter et al. 2024].

Therefore, this paper proposes a blockchain-based governance layer for MEICAN that records each step of the circuit management lifecycle on an immutable ledger while storing the associated policy artifacts in a verifiable manner. This approach enhances transparency and trust across heterogeneous administrative domains. The proposed layer combines the security guarantees provided by blockchain with the existing MEICAN workflow. Such integration represents a significant step toward more efficient multi-domain network governance, as it makes the decision-making process auditable and encourages end-user participation by ensuring record immutability and increased confidence in data integrity.

The remainder of this paper is structured as follows. Section 2 presents a discussion on the state-of-the-art on the topic. Section 3 details the proposed blockchain-based layer for MEICAN, while Section 4 presents an evaluation in terms of gas cost. Finally, Section 5 concludes the paper and presents future work.

2. Related Work

In recent decades, the convergence of emerging technologies such as blockchain and new paradigms that provide greater programmability and flexibility to computer networks (*e.g.*, Software-Defined Networking - SDN and Network Function Virtualization - NFV) has fueled extensive scientific research into new architectures and models for efficient, secure, and decentralized network management. In this section, we reviewed examples of works that benefit from blockchain's architectures and characteristics to improve security and auditability in NFV and SDN.

2.1. Blockchain and NFV

The use of blockchain in NFV has been widely explored to ensure security, automation, and decentralization in the orchestration and management processes of these functions. [Bondan et al. 2019] proposed FENDE, a marketplace ecosystem focused on the distribution and lifecycle management of Virtual Network Functions (VNF). Although the proposal does not integrate blockchain directly, it introduces relevant issues pertaining to scalability and innovation in the NFV domain.

In the field of security and reliability, [Scheid et al. 2019] presented BUNKER, a trusted VNF package repository that uses blockchain to ensure package integrity, thereby obviating the necessity for trusted intermediaries. Subsequently, [Scheid et al. 2022] proposed VeNiCE, an architecture that automates VNF lifecycle management based on smart contract events, demonstrating practical feasibility with prototypes based on Ethereum and OpenStack.

Other research, such as that of [Taskou et al. 2021], introduced frameworks such as NFVChain, which aims at the efficient allocation of energy and financial resources in blockchain-based NFV networks. This model employs optimized algorithms that contribute to cost and latency reduction, although challenges such as computational overhead and scalability persist.

To complement these endeavors, [Franco et al. 2019] carried out the development of the BRAIN (Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service) concept, which is focused on the reverse auction mechanism to promote competition among infrastructure providers in hosting VNFs.

2.2. Blockchain and SDN

Integrating blockchain with SDN has become a rapidly growing research area. [Alharbi 2020] presented a detailed study on the use of the blockchain principle to secure and make the SDN network more efficient. Nevertheless, as the authors note, their study is mainly focused on the theoretical part and does not provide actual validation.

[Latah and Kalkan 2022] highlighted the BC-Sec-SDN architecture, which aims to distribute power and provide security functions by smart contracts, as well as blockchain-based authentication methods in SDN networks. Similarly, [Oktian et al. 2022] envisioned a decentralized system for bandwidth negotiation in SDN edge networks that is more efficient and flexible for all involved users. The paper not only presents the benefits of the approach but also identifies remaining challenges, such as the high transaction per second rates in public networks like Ethereum.

In terms of practical implementations, [Kovacs et al. 2024] demonstrated the feasibility of integrating blockchain into the control of large-scale SDN/NFV networks, focusing on the validation of functions and Internet Service Provider (ISP) environments. However, aspects related to performance and scalability still require further examination.

2.3. Key Findings

The literature analysis underscores the revolutionary potential of the integration between blockchain, SDN, and NFV, especially with regard to security, automation, and decentralization in network management. However, challenges persist, notably about scalability, latency, and computational costs, which must be thoroughly evaluated in future implementations. These aspects are especially pertinent for initiatives such as the integration of blockchain into MEICAN, which have the potential to improve the management of inter-domain circuits through distributed and secure mechanisms enabled by smart contracts.

3. Blockchain-based Circuit Allocation

The proposed architecture, depicted in Figure 1, integrates the MEICAN system with blockchain technology and decentralized storage through the InterPlanetary File System (IPFS), providing enhanced transparency, security, and auditability in the management of inter-domain circuit requests.

Users and operators interact with MEICAN through a web interface, where they submit and evaluate circuit requests. These operations are handled by the internal Request Manager module, which controls the request workflow within the MEICAN infrastructure. An Application Programming Interface (API) layer provides the functionalities required for request management, including modules for encryption, integration with IPFS, and interaction with the Ethereum blockchain. Before being uploaded to IPFS, the policy file and associated metadata undergo an encryption process to ensure data confidentiality.

The smart contract deployed on the blockchain is responsible for maintaining an immutable record of circuit requests. It stores the relevant request information, the hash

of the policy file, the IPFS link to the file, and the corresponding approval or rejection status. Additionally, an event mechanism allows MEICAN, through the API layer, to monitor changes in the request status in real time.

With this architecture, the proposed solution provides a secure and distributed environment for storing data and recording administrative decisions, thereby reinforcing trust among domains involved in the circuit authorization process. The complete source code of the implemented solution is publicly available in the following GitHub repository: `https://github.com/gmazevedo/meican-smart-contract-api`

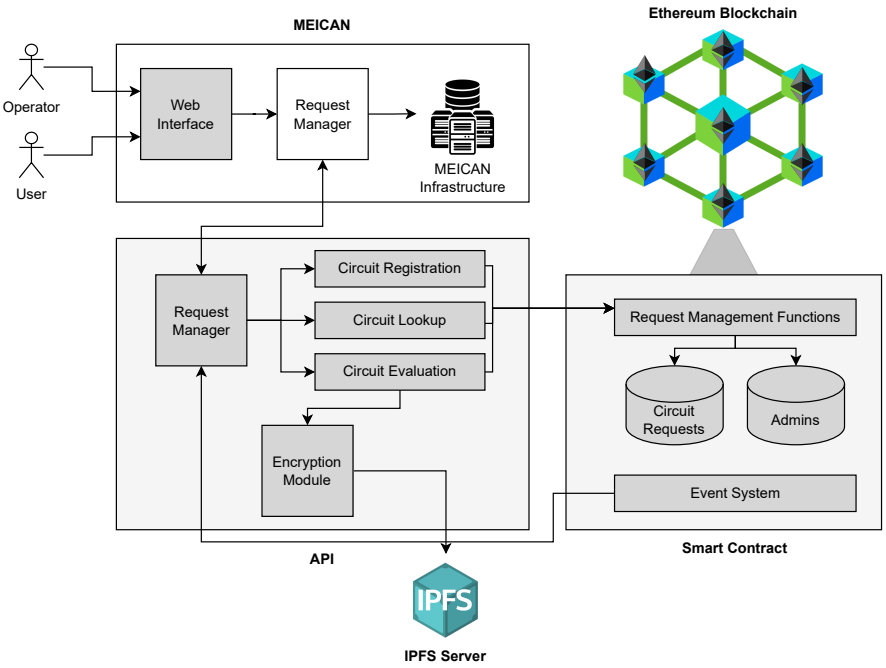

Figure 1. Solution's Proposed Architecture

The system connects to the Ethereum blockchain through a remote node, whose address is specified via environment variables. Authentication and authorization of blockchain transactions are performed using a private key, also defined in the execution environment. The backend interacts directly with a previously deployed MEICAN smart contract via its Application Binary Interface (ABI), stored in a local JSON file. The smart contract is responsible for managing inter-domain circuit requests.

4. Evaluation

To estimate the financial cost of executing the smart contract functions on the public Ethereum network, the gas consumption was evaluated by considering the average *Gas Price* and the exchange rate of *ether* (ETH) against the US dollar (USD). For this study, a *Gas Price* of 0.43 Gwei was assumed, corresponding to the average value observed on the Ethereum Mainnet in June 2025. Table 1 presents the gas consumption computed for each function, along with the estimated cost in ETH and the approximate cost in USD.

During the tests conducted in the Ganache environment, each smart contract function was executed in isolation to obtain precise measurements of gas consumption. The

Table 1. Gas Used and Estimated Cost per Function (Gas Price: 0.43 Gwei)

Function	Gas Used	Estimated Cost (ETH)	Estimated Cost (USD)
`requestCircuit()`	277,152	0.000119176	$0.27
`approveCircuit()`	100,734	0.000043316	$0.10
`rejectCircuit()`	100,770	0.000043331	$0.10
`addAdmin()`	47,791	0.000020550	$0.05
`removeAdmin()`	25,700	0.000011051	$0.03

results indicate that the `requestCircuit` function exhibited the highest gas consumption, reflecting the complexity of the operation, which involves creating a new data structure and emitting an event. Simpler state update functions, such as `addAdmin` and `removeAdmin`, showed significantly lower consumption. The `approveCircuit` and `rejectCircuit` functions, which require multiple storage updates and event emissions, consume intermediate levels of gas.

5. Conclusion and Future Work

This work presented the design and evaluation, in terms of gas cost, of a solution to enable a blockchain-based circuit allocation system in MEICAN. The proposed approach leverages smart contracts to provide transparent and auditable registration of inter-domain circuit requests and uses IPFS for decentralized storage of policy artifacts. The integration of these technologies into the MEICAN workflow demonstrates the feasibility of building a secure and immutable system capable of improving governance, auditability, and end-user confidence in circuit reservation processes.

Future work can advance in several directions to enhance the system's capabilities and practicality for production environments. First, additional evaluations focusing on performance should be conducted. Also, it is needed to investigate the overhead and the impact on execution time of encryption in the IPFS upload workflows. Furthermore, a deeper integration between the smart contract and MEICAN's policy workflows could enable automated approval decisions, reducing manual intervention while preserving auditability. Finally, exploring deployment on alternative blockchain platforms, such as Polygon or Binance Smart Chain, could reduce transaction costs and improve scalability. Finally, evaluating deployments on private blockchain platforms such as Hyperledger Besu or Quorum would enable internal governance models for organizations requiring stricter control.

Disclaimer of Generative Artificial Intelligence Use

This paper was edited with the assistance of AI tools. The content has been reviewed and revised by the authors, who remain fully responsible for the accuracy and integrity of the information presented.

References

Akter, S., Hussain, M. I., Bhuiyan, M. K. I., Sumon, S. A., Hossain, M. I., and Akhter, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. Available at `https://ssrn.com/abstract=5041397`.

Alharbi, T. (2020). Deployment of blockchain technology in software defined networks: A survey. *IEEE Access*, 8:9146–9156.

Asharov, G., Demmler, D., Schapira, M., Schneider, T., Segev, G., Shenker, S., and Zohner, M. (2017). Privacy-preserving interdomain routing at internet scale. *Cryptology ePrint Archive*.

Bondan, L., Franco, M. F., Marcuzzo, L., Venancio, G., Santos, R. L., Pfitscher, R. J., Scheid, E. J., Stiller, B., De Turck, F., Duarte, E. P., Schaeffer-Filho, A. E., Santos, C. R. P. d., and Granville, L. Z. (2019). FENDE: Marketplace-Based Distribution, Execution, and Life Cycle Management of VNFs. *IEEE Communications Magazine*, 57(1):13–19.

Franco, M. F., Scheid, E. J., Granville, L. Z., and Stiller, B. (2019). BRAIN: Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service. In *IFIP Networking Conference (IFIP Networking 2019)*, pages 1–9, Warsaw, Poland.

Goel, A. and Rahulamathavan, Y. (2024). A comparative survey of centralised and decentralised identity management systems: Analysing scalability, security, and feasibility. *Future Internet*, 17(1):1.

Kovacs, R., Buzura, S., Iancu, B., Dadarlat, V., Peculea, A., and Cebuc, E. (2024). Practical implementation of a blockchain-enabled sdn for large-scale infrastructure networks. *Applied Sciences*, 14(5):1914.

Latah, M. and Kalkan, K. (2022). When sdn and blockchain shake hands. *Communications of the ACM*, 65(9):68–78.

Oktian, Y. E., Jo, U., Kim, H., et al. (2022). Blockchain-powered bandwidth trading on sdn-enabled edge network. *IEEE Access*, 10:114024–114039.

Scheid, E. J., Franco, M. F., Küffer, F., Kübler, N., Kiechl, P., and Stiller, B. (2022). VeNiCE: Enabling Automatic VNF Management based on Smart Contract Events. In *IEEE Conference on Local Computer Networks (LCN 2022)*, pages 98–105, Edmonton, Canada.

Scheid, E. J., Keller, M., Franco, M., and Stiller, B. (2019). BUNKER: a Blockchain-based trUsted VNF pacKagE Repository. In *Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019)*, pages 1–9. Springer, Leeds, UK.

Taskou, S. K., Rasti, M., and Nardelli, P. H. (2021). Energy and cost efficient resource allocation for blockchain-enabled nfv. *IEEE Transactions on Services Computing*, 15(4):2328–2341.

Wickboldt, J. A., Guerreiro, M. Q., Granville, L. Z., Gaspary, L. P., Schwarz, M. F., Guok, C., Chaniotakis, V., Lake, A., and MacAuley, J. (2018). Meican: Simplifying dcn life-cycle management from end-user and operator perspectives in inter-domain environments. *IEEE Communications Magazine*, 56(1):179–187.

Álvaro González, J., García, A. M. S., and Baeza, V. M. (2025). Blockchain-enabled management framework for federated coalition networks. Avaiable at: `https://arxiv.org/abs/2503.09666`.