A blockchain-based platform for mobile telcos for the provision of private networks in the context of beyond-5G and 6G

Meroua Moussaoui, Emmanuel Bertin, Noel Crespi

A Blockchain-based Platform for Mobile Telcos for the Provision of Private Networks in the Context of Beyond-5G and 6G

Meroua Moussaoui[1,2] Emmanuel Bertin[1,2] Noel Crespi[2]
[1] Orange Innovation, 14000 Caen, France
[2] SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France.
Emails: {meroua.moussaoui, emmanuel.bertin}@orange.com and noel.crespi@it-sudparis.eu

***Abstract*— Recent technological advancements are increasingly pressuring Telcos to deliver high-performance, customizable networks. One effective solution is to offer private networks tailored to specific use cases. This paper introduces a blockchain-based platform for Telcos for the delivery of private 5G networks as-a-service. The platform serves three functions: a marketplace connecting supply and demand, a network integrator for onboarding and integrating network assets, and a connectivity manager ensuring performance accountability. A proof-of-concept demonstrates the solution's feasibility.**

Keywords—blockchain, Smart Contracts, mobile operators, Telcos, 5G, 6G, platform.

I. INTRODUCTION

Beyond 5G/6G networks are expected to support a wide range of emerging applications and use cases with rigorous and differentiated Quality of Service (QoS) demands. Network capabilities will be enhanced through fine-grained connectivity customization, extensive heterogeneity management, and technological openness. As a result, next-generation networks are anticipated to be open, multi-vendor, multi-tenant, and multi-service [1]. These networks can be collaboratively established and managed by multiple stakeholders.

In particular, verticals place pressing demands on Mobile Network Operators (MNOs) for precise customization, extending beyond mere services, to necessitate the tailoring of the underlying connectivity to meet specific use-case requirements. Effectively, 5G technology promises to facilitate vertical operations by providing high-performance cellular connectivity with QoS customization capabilities. To maximize the advantages of this potential, various enterprises have opted for the establishment of private 5G networks. However, multiple challenges arise in managing the multi-tenancy and openness inherent to next-generation networks, as well as in fostering trust and accountability among all involved parties. This underscores the necessity for proficient and agile network governance, orchestration and management [2].

In this paper, we introduce a blockchain-based platform designed to facilitate the delivery of private 5G networks as-a-service, on user demand. The platform serves a triple function: Firstly, it operates as a marketplace, effectively connecting supply-side (network asset providers) with demand-side (vertical enterprises). Secondly, it facilitates the seamless onboarding and integration of the network assets to create customized private 5G networks. Lastly, the platform ensures service compliance to the user's QoS requirements, through transparency and accountability,

Paper contribution. The contributions of this paper are as follows:

- A blockchain-based marketplace to connect providers and clients for the establishment of network-as-a-service.
- Agile onboarding and integration of network assets into an end-to-end private 5G network .
- Dynamic Service Level Agreement (SLA) establishment and enforcement through Smart Contracts (SCs).
- Decentralized trust, transparency and accountability in multi-tenant networks.
- An end-to-end Proof-of-Concept (PoC).

Paper structure. The paper is organized as follows: Section II offers a background on 5G networks. Section III outlines the motivation and requirements for our contribution. Section IV details the architecture of our solution. Section V presents a technical overview of the solution's PoC. Section VI discusses related works, and Section VII concludes the paper by discussing current challenges and future research directions.

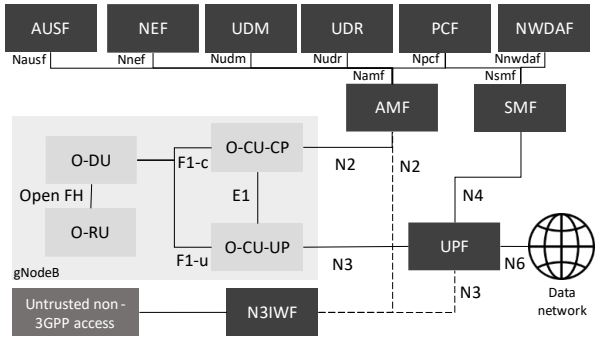
II. BACKGROUND

The 5G network architecture is characterized by its virtualized and modular design, with Network Functions (NFs) communicating via standardized open interfaces. This ensures interoperability among NFs from various providers. This section provides an overview of 5G networks, their deployment methods, and the rise of private 5G networks.

5G core network (CN). To enhance scalability and performance, the 5G core architecture leverages the Control-User Plane Separation (CUPS) principle. The control plane (CP) manages network processes such as authentication, while the user plane (UP) handles user traffic. For CP functions, the 5G core employs a Service-Based Architecture (SBA) where NFs are deployed as microservices, exposing and consuming various services via RESTful APIs. For UP functions, 5G designates a dedicated NF called the User Plane Function (UPF), which adds flexibility and QoS customization

capabilities by allowing the UP to be positioned closer to the user (at the edge) to reduce latency.

5G Radio Access Network (RAN). The primary component of the 5G RAN is the gNodeB (gNB), which consists of two main parts: the Radio Unit (RU), responsible for radio transmission and reception, and the Baseband Unit (BBU), for managing radio resources [2]. The RU and BBU communicate via the Fronthaul (FH) interface. The BBU is further divided into a Distributed Unit (DU), for near-real-time radio operations, and a Centralized Unit (CU), for non-real-time radio operations, interconnected via the Middle-haul (MH) interface. These interfaces enable flexible deployment, in separate locations, but often lead to vendor lock-in. To address this, the Open RAN (O-RAN) initiative aims to open and standardize these interfaces. For added flexibility, the CUPS principle splits the CU into a CU-UP and a CU-CP, connected via the E1 interface. Figure 1 shows a full 5G network architecture, comprising 5G core and O-RAN.



AMF: Access and Mobility management Function, **SMF**: Session Management Function, **AUSF**: Authentication Server Function, **UDM**: Unified Data Management, **PCF**: Policy and Charging Function, **NEF**: Network Exposure Function, **UDR**: Unified Data Record, **NWDAF**: Network Data Analysis Function, **UPF**: User Plane Function, **N3IWF**: Non-3GPP Interworking Function, **O-RU**: O-RAN Radio Unit, **O-DU**: O-RAN Distributed Unit, **O-CU**: O-RAN Centralized Unit, **N$_{function}$**: Function's Service-Based Interface, **N$_n$**: Reference Point, **F1-c/F1-u/E1/Open FH**: O-RAN interfaces.

Fig. 1. 5G and O-RAN architecture.

5G deployment model. Advances in Network Function Virtualization (NFV) has led to the creation of Virtual Network Functions (VNFs) by decoupling network software from hardware. To deploy the 5G core, MNOs procure VNFs from NF providers, which they deploy on standard Commercial Off-The-Shelf (COTS) servers. Additionally, these NFs can be encapsulated within containers as Cloud-native Network Functions (CNFs) and deployed within a cloud environment [3]. These NFs are managed and orchestrated by an orchestration and management system. Consequently, MNOs are freed from vendor lock-in when selecting 5G NFs and the underlying hardware infrastructure, as they can be sourced from different providers.

To deploy the 5G RAN, MNOs invest in RAN infrastructure such as towers and antennas. Furthermore, they collaborate with Tower Companies (TowerCos) to lease infrastructure and opt for RAN resource mutualization to further monetize their infrastructure. RUs are typically deployed as Physical Network Functions (PNFs) installed on towers. The BBU components (DU, CU) can be deployed as VNFs/CNFs at specific sites, either closer to or farther from the RU, similar to the deployment of core NFs.

The emergence of compact radio equipment, such as small cells and Reflecting Intelligent Surfaces (RIS), renders them suitable for small and medium-scale networks, eliminating the need for extensive infrastructure and the associated high capital and operational expenditures (CAPEX and OPEX), as well as specialized operational expertise. The virtualization and cloudification of NFs hold promise in rendering 5G deployment more accessible, with various service and cloud providers offering fully functional cloud-native 5G core networks (e.g., Amazon's AWS). Ongoing technological advancements are streamlining the provision of networks and connectivity as-a-service, facilitating on-demand access with customizable QoS parameters.

Non-Public Networks (NPNs). With the increasing demand for network customization, improved coverage, and enhanced confidentiality, NPNs, also known as private networks, have attracted significant interest from both industry and telecom actors. These networks represent small to medium-scale 5G networks and can be deployed using various architectures with differing degrees of reliance on public networks (MNO networks). Some architectures fully or partially rely on MNO NFs for certain operations, while others deploy their own NFs. NPNs offer an excellent opportunity for enterprises to establish their own networks for both indoor and outdoor connectivity (e.g., the initiatives like 5G-ACIA [4]).

III. Motivational scenario and requirements

In this section, we present the motivation for the proposed solution, from which we derive guidelines for our solution.

A. Motivational scenario

Consider the use case of a maritime port enterprise as a motivational scenario. Ports serve as logistical hubs for good transfer and storage. Ports can leverage Information and Communication Technology (ICT) to improve operational efficiency, increase productivity and reduce operational costs.

Outdoors, the enterprise uses fully automated, cable-less cranes to manage cargo movement and shipment, minimizing human error and enhancing safety. High-definition (HD) cameras monitor the movement of people and assets, ensuring surveillance and security. Indoors, operational teams oversee various activities, including remote crane operation and port security. Within warehouses and storage areas, HD cameras and sensors ensure the surveillance of goods, while robots are used for loading and unloading assets. Port employees use handheld devices to monitor and control operations and communicate effectively, while moving throughout the port.

To enhance port operations, the enterprise requires a private 5G network with customized QoS and efficient network management. For the RAN segment, the enterprise would deploy various RUs as on-premises PNFs. Outdoor connectivity would be provided by i) small cells installed on buildings or dedicated poles, or by ii) sharing nearby MNO antennas. Meanwhile, indoor connectivity would be supported by femtocells or RIS-based access points in offices, warehouses, and storage areas. This setup offers flexibility in adapting the RAN to performance constraints through optimal RU placement and densification, improving broadband and reducing latency. Other parts of the RAN, such as the DU and

CU, can be deployed as i) VNFs/CNFs on-premises or ii) on nearby MNO edge infrastructure. The RAN deployment choices are based on the enterprise's performance needs.

For the core segment, the enterprise has various deployment options. If it requires stringent security and confidentiality for its data and traffic, on-premises management of the UP and user data becomes necessary. This involves deploying NFs such as the UPF and the User Data Management (UDM) on on-premises servers. Meanwhile, the remaining core NFs can be deployed as i) shared MNO NFs or ii) on private/public cloud/edge platforms with exclusive access rights. Alternatively, the enterprise has the option to deploy a full 5G core: i) on-premises, ii) on a private/public cloud/edge infrastructure, or iii) share the entire MNO core.

The network operates on either a dedicated spectrum, a shared MNO spectrum, or utilizes unlicensed bands (e.g., CBRS). The NFs are provided by different NF providers according to the port's requirements. Additionally, The employees' handheld devices and the connected industrial equipment are equipped with dedicated eSIMs.

B. Requirements

The aforementioned scenario highlights several requirements for our proposed solution. The cellular network serving the port needs to provide both indoor and outdoor coverage. This network is deployed as an end-to-end 5G network that supports the seamless integration of various types of NFs (physical, virtual, and cloud-native), provisioned on-demand and as-a-service from different providers. Moreover, it is crucial to customize the QoS to meet the specific requirements of this use case. This involves dynamically establishing SLAs and ensuring their enforcement through accountability, thus facilitating SLA violation detection. Lastly, the network must ensure principles of decentralized trust and distributed governance across the network to handle the multitenant nature of the network and foster reliability.

Addressing these requirements involves encouraging greater openness to ecosystem players (mainly NF providers), enhancing operational agility and dynamism, optimizing and securing the connections in multi-tenant environments, and establishing trust through transparency and accountability.

IV. A BLOCKCHAIN-BASED PLATFORM FOR THE PROVISION OF PRIVATE NETWORKS

We introduce a blockchain-powered platform where MNOs provide private 5G networks as-a-service with on-demand customized QoS. This platform performs three key functions: it seamlessly connects supply and demand through agile smart-contract-based SLAs, fostering distributed trust among stakeholders. Additionally, it supports dynamic service integration and provision by providing essential tools for supervision and monitoring. Finally, it ensures network performance by continuously tracing user experience indicators.

This section outlines the platform architecture, detailing the SCs and system interactions. Before delving into this, we present the solution's assumptions and identify key stakeholders.

Stakeholders. The actors interacting with the platform are the following:

- *Platform Owner*: The MNO, which owns the platform and oversees its stability and coherence.
- *Platform Supply-Side (Providers)*: These include NF providers, cloud/edge providers, TowerCos, active/passive infrastructure providers, and open-source network providers. They offer various services, customized into differentiated offers to enhance flexibility and adaptability.
- *Platform Demand-Side (Clients)*: Enterprises that require customized connectivity services.

Assumptions. In presenting this solution, we assume the following: a) NFs supplied by multiple vendors can interact through standardized interfaces and protocols. b) The platform has a technician team to ensure the physical installation of the network modules (PNFs, on-premises COTS servers) if needed. c) NFs are equipped with embedded observability algorithms that report telemetry data. d) The client possesses sufficient networking knowledge to compose a complete network offer by selecting different NFs from various providers. e) We leverage 5G architecture as a reference network architecture, but the solution is also applicable to next-generation network architectures. f) The network operates on a dedicated spectrum band. g) The platform can be backed by a financial system that converts the digital tokens into conventional currency. It is also possible to create a platform-specific cryptocurrency, as is the case in Decentralized Wireless (DeWi) networks [5]. h) We consider the subscription payment model.

Architecture. The platform comprises three key functional elements:

- A *marketplace*, which manages the advertisement of NFs, and acts as the commercial and legal interface between clients and providers, establishing and enforcing SLAs.
- A *network integrator,* which integrates the requested NFs into an end-to-end private network. It oversees the dynamic onboarding, provisioning and activation of network resources, as well as the orchestration and management of the network.
- A *connectivity manager*, which monitors network QoS, ensuring adherence to the SLA terms.

Blockchain is leveraged to register stakeholder profiles, the advertised NFs, as well as the network performance telemetry and QoS data. SCs are leveraged to establish and enforce SLAs between clients and providers and well as to monitor different network orchestration and management functions. We annotate SCs as SC_{role}. Figure 2 presents an overview of the architecture. In the following sub-sections, we present the functioning of the three key functional elements of our proposed solution, and their respective SCs.

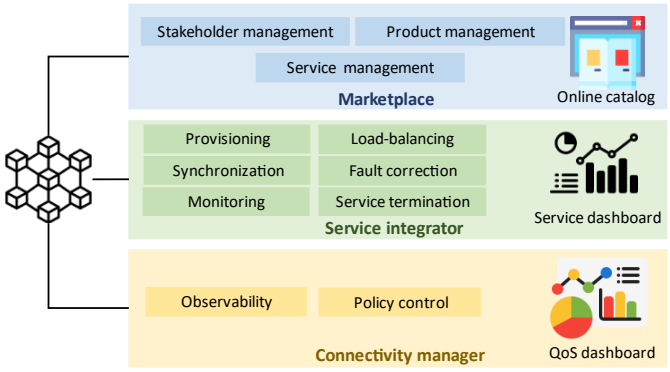


Fig. 2. The platform architecture.

1) The marketplace

The marketplace serves as the interface between the stakeholders. Providers use the marketplace to advertise their offers, which encompass various network components and services: VNFs, PNFs, CNFs, active and passive infrastructure, edge/cloud infrastructure, complete 5G core networks, full RAN networks, end-to-end private networks, and more. Detailed information about these offers (such as performance characteristics and costs) is published in an online catalog for clients to browse. Subsequently, clients have three options: i) they can request individual offers that they integrate into their existing private networks (here the platforms does not handle the service integration), ii) compose their own private network offer by selecting the necessary components and requesting their integration into a fully functional end-to-end private network, or iii) request a full end-to-end private network as-a-service, customized to their specific requirements. To enable fine-grained customization, clients can further fine-tune their QoS requirements within the defined range set by the provider for each component and the overall network service.

All service specifications, along with legal and commercial terms (including payment models and conflict resolution procedures), are encompassed within an SLA. In this paper, we consider a subscription payment model, where clients pay upon SLA establishment for a defined service duration. Nevertheless, our solution can be easily adapted to other payment models (e.g., pay-per-use). The SLA is established and agreed upon by all the concerned parties, the client pays the provider for the service and the platform owner (MNO) earns a commission from each transaction.

When the client selects different network modules from different providers, the platform owner actively participates in the service. This is because the platform owner provides the end-to-end network service that integrates the various modules subscribed to by the client. Therefore, when establishing the SLA, the client agrees to service terms with each individual provider for their respective offers, as well as with the MNO (as a third party) for the integration service and the provided end-to-end network. In the scenario where the client only requests an offer from a provider, the SLA is established between the provider, client, and the MNO, which here, acts as a regulator to ensure that the SLA terms align with the platform's policies.

After all parties have validated the SLA, the service can begin as scheduled. Throughout the service period, both clients and providers have access to a dashboard connected to the network/service orchestration and management system, allowing them to visualize service performance and network QoS, promoting enhanced accountability and transparency. Figure 3 summarizes the overall interactions taking place within the marketplace.

Leveraging blockchain and SCs, the marketplace ensures the following functions.

Stakeholder management. The marketplace manages the different parties (providers and clients), leveraging the following SCs.

- *Stakeholder Registration contracts* ($SC_{P\text{-}registration}$ for providers and $SC_{C\text{-}registration}$ for clients). These SCs are called when a client/provider accesses the platform for the first time, and asks to sign up to the platform. It registers the stakeholder's profile, containing information required by the platform, assigns a unique ID to each profile, and initializes their token wallet balance as specified by the user. The user profile, user ID and user wallet are then stored on the blockchain. These SCs keep a list of the registered stakeholders.
- *Stakeholder Wallet contract* ($SC_{S\text{-}wallet}$). This SC manages payment processes, handling transactions for SLA establishment, SLA compensation and the periodical subscription payments.

Offer management. The marketplace handles the registration and advertisement of various network offers provided by the providers through the use of the following SC:

- *Offer Registration contract* ($SC_{O\text{-}registration}$). This SC is called when a provider requests to register an offer on the marketplace. The provider must supply all necessary information for the offer's registry. Based on this information, the SC creates an offer profile, assigns it a unique ID, and stores both the offer profile and its ID on the blockchain.

Once registered to the blockchain, the offer is advertised on the marketplace's catalog.

Service management. The marketplace oversees service establishment between providers and clients and tracks service Key Performance Indicators (KPIs) and QoS to enforce SLAs. This is facilitated by the following SCs:

- *SLA Establishment contract* ($SC_{SLA\text{-}establishment}$). When a client subscribes to a service, they can further customize it to their QoS requirements within a predefined range of parameters supported by the offer. This SC fills the service SLA template with the client's requirements, creating the service SLA and initiating the signing process by the stakeholders. Once signed, it triggers the payment process handled by $SC_{S\text{-}wallet}$ and transfers the service requirements to the *network integrator*, along with a notification to commence service integration.

- *SLA Conflict contract ($SC_{SLA\text{-}conflict}$)*. This SC manages disputes according to the established clauses in the SLA, specifying the actions to be taken in case of a violation, such as financial compensation (which triggers $SC_{S\text{-}wallet}$) .

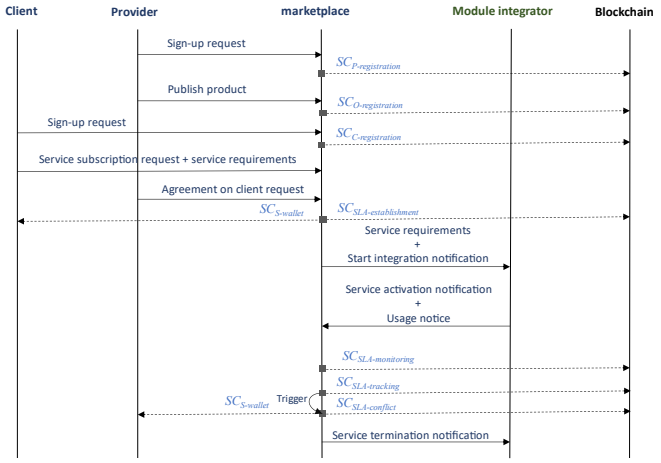


Fig. 3. The marketplace functionalities.

2) The network integrator

The *network integrator* assembles the various services subscribed to by the client into a fully functional end-to-end network. It leverages the standardized interfaces and protocols for vendor interoperability. Furthermore, it dynamically replaces network modules on demand and handles configuration, onboarding, provisioning, and activation of services. The performance of both individual modules and the overall network can be optimized through provisioning and orchestration and management, which help adjust factors such as module placement (physical, cloud/edge), computing resources, and deployment technologies. Some scenarios may require human interaction, like PNF installation (e.g., RUs).

We assume that modules are equipped with self-orchestration and management algorithms, along with observability algorithms to collect telemetry data. This data aids in internal management (self-diagnosis, self-healing) or external transfer via predefined interfaces. Network probes are deployed in various network segments to gather performance telemetry data. Figure 4 summarizes the functioning of the *network integrator*. The *network integrator* ensures the following orchestration and management functionalities:

Provisioning. The *network integrator* configures the network modules based on the parameters specified in the SLA. These parameters are translated into technical settings to determine module placement and allocate all necessary resources for integration and activation. This process also activates the self-orchestration and management capabilities embedded within the network modules.

Upon receiving a notification from the *marketplace* to start service integration, the *network integrator* proceeds with service onboarding and provision by configuring the physical and virtual modules according to the required service performance. Once the service is configured and provisioned, the *network integrator* creates the module profiles and network profile associated with the service, using the following SCs.

- *Module Registration contract ($SC_{M\text{-}registration}$)*. It generates the module profile linked to the client's subscribed offer, filling it with necessary module details (placement, owner, etc.), along with an ID, QoS requirements, and performance KPIs as per the SLA terms. Everything is stored on the blockchain, and the SC maintains the list of module profiles.
- *Network Registration contract ($SC_{N\text{-}registration}$)*. It generates a network profile with details such as QoS requirements and performance KPIs, along with a list of the integrated modules' IDs. After assigning a network ID, it stores this data on the blockchain and maintains a list of network profiles.

Subsequently, the service is activated, initiating the self-orchestration and management tools within the modules. Upon activation, the *network integrator* notifies the *marketplace* to indicate the service launch and sends the service usage notice.

Synchronization. In scenarios involving dynamic module replacement, this ensures the smooth termination of the current module and seamless integration of the new one. When adding a new service, provisioning occurs, with activation following synchronization and updating the network profile with the new module ID and QoS requirements.

Load-balancing. This functionality manages the instances of a module, balancing traffic and computing load to optimize and fine-tune network performance.

Monitoring. The platform monitors module and network resource consumption to ensure KPI adherence, initiating load-balancing and fault correction for performance issues. It tracks parameters like energy use, computing, and storage (this data can be leveraged to support new payment models based on consumption). This data is visualized by clients and providers via a service dashboard and is periodically logged to the blockchain using SCs.

- *Module Monitoring contract ($SC_{M\text{-}monitoring}$)*. This SC is periodically called to record the performance data generated by the self-orchestration and self-management tools within the module.
- *Network Monitoring contract ($SC_{N\text{-}monitoring}$)*. This SC is periodically called to log the network performance data using the data retrieved from the network probes and output by the modules.

Fault correction. This functionality analyzes the monitoring data to detect faults and provides proactive and reactive fault correction.

- *Network Fault Correction contract ($SC_{N\text{-}fault}$)*. This SC periodically accesses telemetry data from $SC_{M\text{-}monitoring}$ and $SC_{N\text{-}monitoring}$, comparing it to the KPIs and QoS requirements in the blockchain-stored

module and network profiles. If a fault is detected, it feeds the data to algorithms for proactive and reactive correction.

Service termination. Upon the SLA termination date, the *network integrator* gracefully terminates the service and its components. The following SCs are used:

- *Module Termination contract* ($SC_{M\text{-}termination}$). This SC marks the module as terminated in its profile, rendering it ineligible usage.
- *Network Termination contract* ($SC_{N\text{-}termination}$). This SC marks the network as terminated in its profile, preventing further network usage.

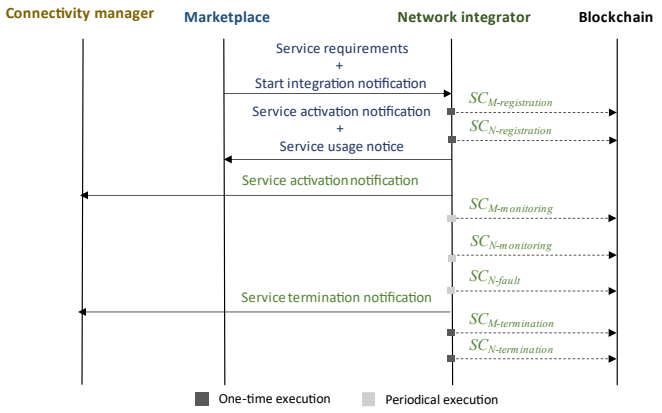


Fig. 4. The network integrator functionalities.

B. The connectivity manager

The *connectivity manager* monitors network QoS parameters to enforce SLA clauses and network policies. Upon service activation, it initiates observability and policy control functions. Upon SLA expiration, the *network integrator* signals the connectivity manager to terminate operations. Figure 5 summarizes the functioning of the *connectivity manager* which leverages the following SCs:

Observability. This function deploys probes across network segments to collect performance statistics. It aggregates this data with telemetry from multiple network modules to create comprehensive observability data. It leverages the following SCs:

- *Module Performance contract* ($SC_{M\text{-}performance}$). After activation, the component periodically logs performance data using its self-orchestration and management feature, storing it on the blockchain.
- *Network Performance contract* ($SC_{N\text{-}performance}$). This SC interacts with the network probes to log the collected data on the blockchain.

The logged performance data is easily accessible to both the client and the provider, visible on their dashboards.

Policy control. This functionality controls and enforces network policies and QoS based on the client's SLA requirements, leveraging the following SC:

- *Network Policy Enforcement contract* ($SC_{N\text{-}policy}$). After service activation, this SC reads performance KPIs and QoS requirements from the module profile on the blockchain. It then retrieves network and module observability data periodically, comparing it to SLA values. Discrepancies trigger analysis algorithms for QoS correction. In case of confirmed SLA violation, the SC logs the details on the blockchain for further use by $SC_{SLA\text{-}conflict}$.

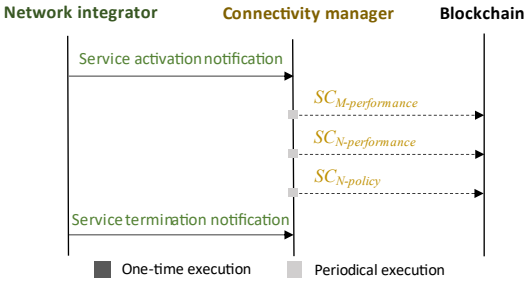


Fig. 5. The connectivity manager functionalities.

The main functionalities of this solution encompass several key aspects: a marketplace for network function providers to advertise their assets, a blockchain-based system for the dynamic establishment and enforcement of SLAs, and the dynamic onboarding, provision, integration, and activation of network services. Additionally, it leverages blockchain to manage access rights and governance over network components and data, and provide tools for enhancing service supervision, orchestration, and management, and mechanisms for SLA violation detection. The solution ensures immutable data storage and traceability, thereby enhancing transparency and accountability, while providing QoS monitoring.

V. Technical Implementation and Evaluation

In this section, we outline our proposed blockchain-based platform's technical implementation to demonstrate its feasibility. Figure 6 provides a comprehensive diagram of our PoC testbed.

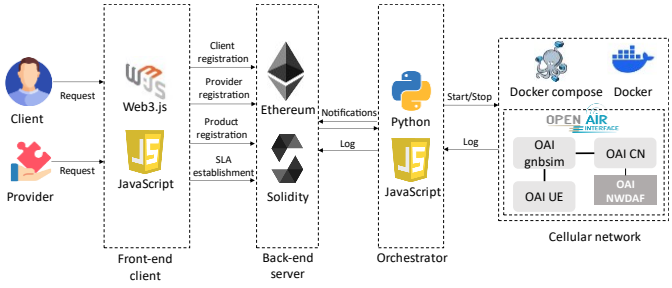


Fig. 6. A high-level overview of the technical implementation.

A. Testbed description

The implementation of our blockchain-based solution comprises the following three functional layers:

The blockchain layer. This layer consists of a private blockchain network, deployed on Truffle, and includes two

SCs written in Solidity: Marketplace.sol and PerformanceLog.sol.

- Marketplace.sol. This SC ensures the primary functionalities of the marketplace. It includes functions for the registration of clients, providers, and offers, maintaining lists of each. It also validates SLA contracts between clients and providers, processes corresponding payments, and keeps a record of established SLAs. Upon SLA validation, it emits an event. After the SLA expiration, the client can provide a service rating from 1 to 5.
- PerformanceLog.sol. This SC has a function that receives performance data and logs it to the blockchain.

The management layer. This layer consists of multiple scripts that interface between the user and the blockchain layer, as well as between the blockchain layer and the service layer.

- marketplace.js. Written in JavaScript using the web3.js library, this decentralized application (dApp) interacts with the SCs in the blockchain layer. It manages the frontend for clients and providers, allowing them to sign up, advertise offers, and subscribe to services. It sends necessary information to the Marketplace.sol SC to register clients, providers, and offers, and to establish SLAs. Upon SLA establishment, it receives an event with contract details and forwards these to provision.py.
- provision.py. This Python script receives notifications from marketplace.js with SLA details and launches the requested service by activating the necessary Docker containers (OAI 5G core, gnbsim and UE containers) for the specified duration. It also activates the network observability module (OAI NWDAF) and sends collected data periodically to performanceLog.js. Upon SLA expiration, it shuts down the Docker containers.
- performanceLog.js. Also written in JavaScript and leverages the web3.js library, this script logs observability information received from provision.py to the blockchain using the PerformanceLog.sol SC.

The service layer. This layer is set up using a Docker Compose environment to deploy an OAI 5G core, including the main 5G core NFs, the OAI gnbsim to simulate the RAN and a simulated UE, all deployed as NF as Docker containers. The network is appended with an OAI NWDAF (deployed through multiple Docker containers) for capturing both network analytics (e.g., number of connected UEs, PDU sessions) and network events (e.g., anomalies, UE mobility).

To deploy this solution, we used an Ubuntu 18.04 system with a Core i7 CPU, 16GB RAM, and a 512GB hard disk. Technically, the layers are deployed as follows: the service layer through the cellular network component, the management layer through the frontend client and orchestrator, and the blockchain layer through the backend server.

VI. State-of-the-Art

Several studies have examined the integration of blockchain technology and SCs to efficiently connect supply and demand in the telecommunications field through decentralized marketplaces designed to facilitate the sale and trade of NFs.

Kapassa et al. [6] propose a blockchain-based NFV marketplace for the storage, publication and licensing of VNFs within a 5G infrastructure. However, this work lacks a technical implementation. Meanwhile, Weerasinghe et al. [7] propose a Blockchain-as-a-Service platform for Local 5G Operators, comprising various customizable blockchain-based services, including a marketplace for buying and selling network assets, a reputation system, agreement establishment, and payment settlement. Additionally, Fernández-Fernández et al. [8] define a dual-blockchain-enabled 5G marketplace for sharing heterogeneous 5G resources among operators and service providers. This solution employs two separate blockchains: a governance platform for managing identities and permissions and a marketplace platform for handling the offer lifecycle and SLAs. Furthermore, Giupponi et al. [9] propose to enrich the O-RAN architecture with new blockchain-based functional blocks for automatic, dynamic and auditable sharing of RAN resources. Additionally, they introduce a blockchain-based marketplace for operators to advertise O-RAN VNFs. Finally, Xevgenis et al. [10] leverage blockchain for resource pooling among network providers, allowing them to share unused resources without relying on a central trusted authority.

On the other hand, Yrjölä et al. [11], [12] explore the concept of MNO platformization from both engineering and economic perspectives. They propose a comprehensive framework for MNO platformization and explain how blockchain technology can enhance this model in the context of 6G. These studies offer guidelines for transforming MNOs into platforms, leaving it to researchers to adapt the proposed framework to their specific use cases.

While these studies included technical implementations, their primary focus was on the functionalities of the marketplace and the performance of the deployed blockchain and SCs. To the best of our knowledge, none of the aforementioned studies have technically implemented the network asset aspects, such as VNF onboarding, integration, configuration, and activation. In contrast, our work offers a comprehensive end-to-end implementation that spans from the blockchain layer to the service layer. We not only facilitate the integration of NFs and other assets but also ensure the complete orchestration and management of network services through auditability, providing a more holistic and functional solution. Our technical implementation is designed to be functional in real-life use cases.

VII. Discussion, challenges and future directions

The MNO owns and manages the platform, ensuring its stability and coherence. It fosters an environment that balances cooperation and competition among various providers, enhancing growth and value capture. By maintaining this equilibrium, the MNO creates a robust ecosystem where providers can effectively collaborate and compete, driving innovation and creating network effects [13]. MNOs should explore innovative methods and leverage tools like ML-based data analysis to understand platform dynamics and harness these effects. Blockchain's immutability and traceability provide a clear snapshot of the platform's state at any given time, enabling deeper insights and data-driven decisions to enhance performance and growth. Additionally, MNOs should study offer pricing and consider including pricing regulators as active nodes on the platform [14].

Another obstacle to deploying on-demand private networks as a service is spectrum availability. Spectrum regulations often remain inflexible in granting access to non-MNOs (despite progress in some countries like Germany, which has begun allocating spectrum to non-MNOs) [15]. Sharing spectrum with MNOs can be a provisional solution to this regulatory inflexibility, but it can hinder the performance of private networks. This rigidity limits the effectiveness and reliability of private networks, posing significant challenges to their deployment and operation.

One limitation of our solution is the on-chain storage of logs, which can quickly saturate the network and degrade overall system performance. A potential alternative is to use off-chain storage solutions like IPFS for log storage. This approach not only alleviates network congestion but also enhances log confidentiality. By leveraging off-chain storage, we can significantly improve both the efficiency and security of the system.

The deployment of 5G requires substantial capital investment from MNOs, a financial burden that they find challenging to meet. Consequently, an increasing number of MNOs are engaging in resource sharing and mutualization to better monetize their infrastructure. Our proposed platform serves as a catalyst for resource mutualization, encompassing various types of network resources. Through our platform, MNOs can share their assets with other stakeholders, creating new revenue streams, particularly as MNOs earn commissions on every transaction conducted via the platform. While our current solution addresses private networks, our approach can be extended to public networks, where MNOs become clients in need of diverse network assets. These assets can be sourced from other MNOs through resource sharing or from other stakeholders and resource providers.

The interworking between public and private networks necessitates thorough exploration. Blockchain technology can offer numerous advantages in this context by ensuring trust, integrity verification, and provenance tracking. These capabilities can be leveraged to connect multiple private networks via a public network, which is particularly beneficial for enterprises with geographically dispersed sites.

Future research directions include evaluating the performance of our solution by assessing the marketplace and the dynamic replacement of NFs. Additionally, it is essential to implement a system for detecting SLA violations, as well as a conflict resolution mechanism.

References

[1] C. De Alwis *et al.*, “Survey on 6G frontiers: Trends, applications, requirements, technologies and future research,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.

[2] M. Moussaoui, E. Bertin, and N. Crespi, “5G shortcomings and Beyond-5G/6G requirements,” in *International Conference on 6G Networking (6GNet)*, 2022.

[3] A. Khichane, I. Fajjari, N. Aitsaadi, and M. Gueroui, “Cloud native 5G: an efficient orchestration of cloud native 5G system,” in *NOMS 2022-2022 IEEE/IFIP network operations and management symposium*, IEEE, 2022, pp. 1–9. Accessed: Apr. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9789856/

[4] “WP_5G_NPN_2019_01.pdf.” Accessed: May 17, 2024. [Online]. Available: https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf

[5] M. Moussaoui, E. Bertin, and N. Crespi, “Decentralized Wireless (DeWi): which perspectives for Blockchain-based mobile networks?,” in *5th Conference on Blockchain Research & Applications for Innovative Networks and Services, BRAINS 2023*, 2023.

[6] E. Kapassa, M. Touloupos, D. Kyriazis, and M. Themistocleous, “A Smart Distributed Marketplace,” in *Information Systems*, vol. 381, M. Themistocleous and M. Papadaki, Eds., in Lecture Notes in Business Information Processing, vol. 381. , Cham: Springer International Publishing, 2020, pp. 458–468. doi: 10.1007/978-3-030-44322-1_34.

[7] N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere, and M. Ylianttila, “A novel blockchain-as-a-service (BaaS) platform for local 5G operators,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 575–601, 2021.

[8] A. Fernández-Fernández *et al.*, “Multi-party collaboration in 5G networks via DLT-enabled marketplaces: A pragmatic approach,” in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 550–555. Accessed: Apr. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9482487/

[9] L. Giupponi and F. Wilhelmi, “Blockchain-enabled network sharing for O-RAN in 5G and beyond,” *IEEE Netw.*, vol. 36, no. 4, pp. 218–225, 2022.

[10] M. Xevgenis, D. G. Kogias, P. Karkazis, H. C. Leligou, and C. Patrikakis, “Application of blockchain technology in dynamic resource management of next generation networks,” *Information*, vol. 11, no. 12, p. 570, 2020.

[11] S. Yrjölä, P. Ahokangas, and M. Matinmikko-Blue, “Platform-Based Business Models in Future Mobile Operator Business,” *J. Bus. Models*, vol. 9, no. 4, pp. 67–93, 2021.

[12] S. Yrjölä, “How could blockchain transform 6G towards open ecosystemic business models?,” in *2020 IEEE international conference on communications workshops (ICC workshops)*, IEEE, 2020, pp. 1–6.

[13] M. Moussaoui, E. Bertin, and N. Crespi, “Divide and Conquer: A Business Model Agenda for Beyond-5G and 6G,” *IEEE Commun. Mag.*, vol. 61, no. 7, pp. 82–88, 2023.

[14] M. Moussaoui, E. Bertin, and N. Crespi, “Blockchain and Smart Contracts for Telecommunications: The Whys and Wherefores,” in *Blockchain and Smart-Contract Technologies for Innovative Applications*, N. El Madhoun, I. Dionysiou, and E. Bertin, Eds., Cham: Springer Nature Switzerland, 2024, pp. 259–279. doi: 10.1007/978-3-031-50028-2_9.

[15] M. Moussaoui, E. Bertin, and N. Crespi, “Telecom Business Models for Beyond 5G and 6G networks: Towards Disaggregation?,” in *2022 1st International Conference on 6G Networking (6GNet)*, IEEE, 2022, pp. 1–8.