UNICO I+D Project
6G-DATADRIVEN-01

6G-DATADRIVEN-01-E7

Initial system architecture

Abstract

This report describes the first overall system architecture to achieve in-network computing and integration of different edge platforms in Industry 4.0 environments. The initial system architecture focusses on the integration of different edge platform using the concept of federation that is performed in an automatic manner using DLT. The initial architecture is presented together with the proposed applicability of DLT for multi-edge federation. In addition, the exiting challenges in performing dynamic federation are presented and some federation scenarios where DLT can be applied.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia

Document properties

Document number	6G-DATADRIVEN-01-E7
Document title	Initial system architecture
Document responsible	Milan Groshev (UC3M)
Document editor	Milan Groshev, Carlos J. Bernardos (UC3M)
Editorial team	Milan Groshev, Carlos J. Bernardos (UC3M)
Target dissemination level	Public
Status of the document	Final
Version	1.0
Delivery date	31/12/2023
Actual delivery date	31/12/2023

Production properties

Reviewers	Carlos J. Bernardos (UC3M)

Disclaimer

This document has been produced in the context of the 6G-DATADRIVEN Project. The research leading to these results has received funding from the Spanish Ministry of Economic Affairs and Digital Transformation and the European Union-NextGenerationEU through the UNICO 5G I+D programme.

Contents

List of Figures

No table of figures entries found.

List of Acronyms

QoS: Quality of Service

KPI: Key Performance Indicators

GSMA: Global System for Mobile Communications Association

OP: Operator Platform

NBI: North Bound Interface

DLT: Distributed Ledger Technology

W/EBI: West/East Bound Interface

CI/CD: Continuous Integration/Continuous Deployment

UE: User Equipment

UNI: User to Network Interface

GPU: Graphic Processing Units

VPU: Vision Processing Units

NPU: Neural Processing Units

FPGA: Field Programmable Gate Arrays

VM: Virtual Machine

AD: Administrative Domain

SLA: Service Level Agreement

V2X: Vehicle-to-everything

AR/VR: Augmented Reality / Virtual Reality

Resumen Ejecutivo

Este documento proporciona la versión inicial del diseño del sistema para el 6G-DATADRIVEN-01. El documento detalla los componentes del sistema y explica los desafíos y la solución de la problemática de la federación.

Los principales aportes de este entregable son:

- el análisis de los desafíos existentes para la federación dinámica en el denominado *cloud continuum*;
- la propuesta de tecnología Blockchain para la ejecución del Rol de Gerente de Federación;
- el análisis de diferentes posibilidades de implementación y casos de negocio detrás de la Federación basada en DLT

En línea con la solución propuesta, la siguiente investigación se ha realizado en el contexto de la Industria 4.0 utilizando la tecnología Blockchain. En particular, estas son las publicaciones científicas producidas:

- Applying Blockchain consensus mechanisms to Network Service Federation: Analysis and performance evaluation (Kiril Antevski, 2023).
- Performance evaluation of Private and Public Blockchains for multi-cloud service federation (Zahir, et al., 2024).

El resto del documento está redactado en inglés, de cara a maximizar el impacto del trabajo realizado en este proyecto.

Executive Summary

This document provides the initial version of the system design for the 6G-DATADRIVEN-01. The document details the components of the system, and explains the federation challenges and solution.

The main contributions of this deliverable are:

- the analysis of existing challenges for dynamic federation in the compute continuum.
- the proposal of Blockchain technology for executing the Federation Manager Role;
- the analysis of different deployment possibilities and business cases behind the DLT based Federation.

In line with the proposed solution, the following research has been carried out in the context of Industry 4.0 using Blockchain technology. In particular, these are the produced scientific publications:

- Applying Blockchain consensus mechanisms to Network Service Federation: Analysis and performance evaluation (Kiril Antevski, 2023).
- Performance evaluation of Private and Public Blockchains for multi-cloud service federation (Zahir, et al., 2024).

1. Introduction

In the era of 5G, operators possess a noteworthy chance to capitalize on their network capabilities. Furthermore, leveraging their established partnerships with industrial sector, extensive local presence, adherence to digital sovereignty principles, and proficiency in delivering highly reliable services, the key aspect yet to be addressed is the capacity to package and present their networks in a scalable manner across various public and private networks and operators. In addition to the networking capabilities, another important factor is the offering of computing capabilities in the entire compute continuum from hyperscale cloud service provider to private industrial edge computing.

This document proposes the initial system architecture to ensure network and compute capabilities Industry 4.0 scenarios over different network operators and compute service providers. Instead of designing yet another architecture, in this project we will re-use the GSMA Operator Platform proposed architecture [(Association, 2021)] because it fulfills the main requirements for this project.

The GSMA proposed architecture is further extended with the concept of DLT based federation, as main enabler for in network computing integration between different service providers in the complete compute continuum. The GSMA Operator Platform has three main that are described in this document: 1) Capabilities Exposure Role, 2) Federation Manager Role and 3) Service Resource Manager Role. While in the 6G-DATADRIVEN-01-E9 deliverable we are focusing on the main requirements for the NBI and the Capabilities Exposure and Service Resource Management Role, in this document we are elaborating in detail the WEBI and Federation Manager, proposing the applicability of DLT for a such a role in operator's network.

The document is structured as follows. First, it presents the overall GSMA Operator Platform Initial Roles and Interfaces for an Industry 4.0. Then it explains in detail the Federation Manager Role with its main characteristics. After describing the Federation Manager Role, this document presents the main federation challenges and proposes the applicability of Blockchain technology for dynamic federation. Finally, before concluding the document, it discusses different deployment scenarios using the proposed DLT federation.

2. Initial system design

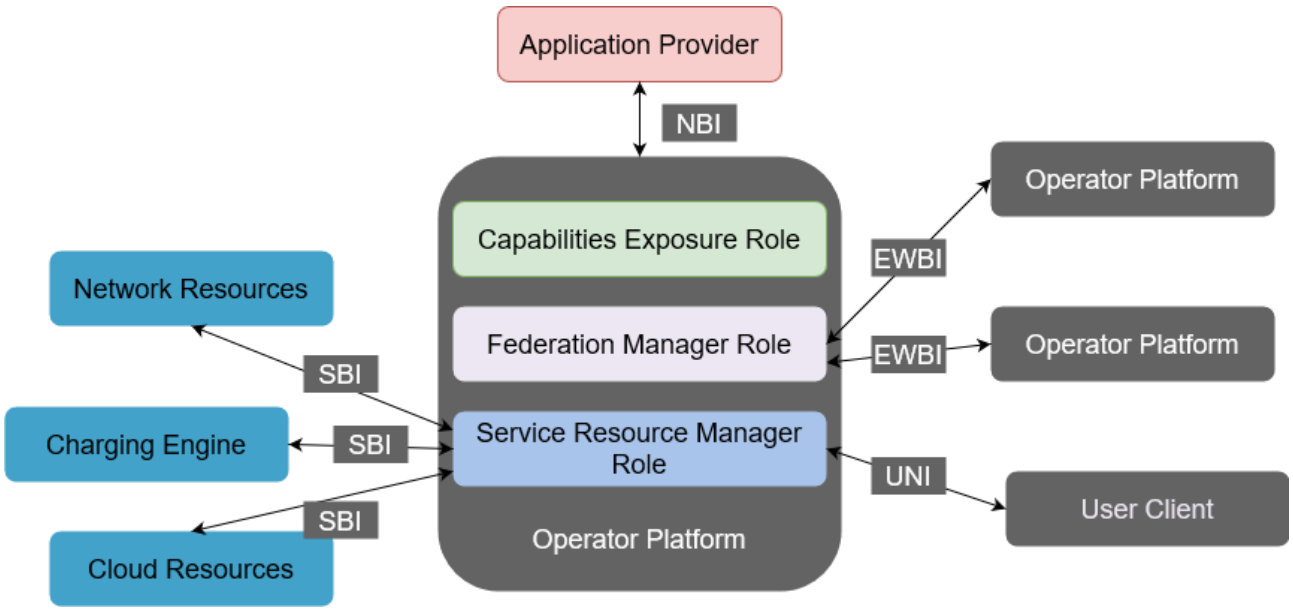

FIGURE 1: OP ROLES AND INTERFACES REFERENCE ARCHITECTURE (ASSOCIATION, 2021)

Figure 1 depicts the proposed target architecture outlined by GSMA, tailored to meet the requirements of this project. The central element of this architecture is the Operator Platform (OP), designed with the primary objective of offering a universal and standardized method for exposing specific services to external Application Providers. This exposure can occur either through a direct connection from the resource owner to the end consumer or by utilizing intermediate integration platforms. Within the OP environment, various actors coexist, collaborating to achieve end-to-end service delivery, resource sharing, and footprint expansion. This collaboration necessitates the establishment of a common framework for facilitating interactions among these actors. In the following section, we present the GSMA OP architecture and its primary components at a relatively high level. When detailing OP-specific concepts, the concepts are presented as roles, functionalities, and interfaces. This approach ensures that we capture the fundamental behavior required by OPs while allowing the architecture to align with existing standards and permitting vendors to introduce innovative solutions without constraints.

2.1. Roles and Functional Definitions

The operational functionality of the Operator Platform (OP) is actualized through a variety of roles. These roles empower an OP instance to engage with and enact scenarios involving other entities within the OP ecosystem, including Application Providers, other OP instances, Cloud Resources, and Network Resources. A singular OP can integrate all roles and their corresponding functionalities, or distinct instances can specialize in different roles (e.g., one OP instance handling the Service Resource Manager Role and another addressing the Capability Exposure Role). This section outlines these roles and elucidates their principal functions.

Capabilities Exposure Role

The Capabilities Exposure Role within the Operator Platform (OP) is tasked with revealing the OP's capabilities to Application Providers through the NBI. The Capabilities Exposure role facilitates various scenarios, including:

- Edge Cloud Infrastructure Endpoint Exposure;
- Application Onboarding;
- Application Metadata/Manifest Submission;
- Application CI/CD Management DevOps;
- Application Lifecycle Management;
- Application Resource Consumption Monitoring;
- Edge Cloud Resource Catalogue exposure;
- The geographical footprint reachable via the OP (either via own resources or partner OP resources).

Service Resource Manager Role

The role of the Service Resource Manager within the Operator Platform (OP) involves the management of Cloud and Network resources originating from Edge Cloud(s) through the SBI and UNI interfaces. The Service Resource Manager role facilitates various scenarios through these interfaces, including:

- SBI:
    - Inventory, Allocation and Monitoring of Compute resources from Edge Cloud
    - Infrastructure via the Southbound Interface – Cloud Resources (SBI-CR);
    - Orchestration of Application instances on the Edge Cloud Infrastructure via the SBI-CR interface;
    - Cloud resource reservation managed by the OP,
    - Configuring UE traffic management policies to accomplish the application's requirements, e.g. as described in 3GPP TS 23.502, or the UE's IP address shall be maintained;
    - Exposure of usage and monitoring information to operator's charging engine via the Southbound Interface – Charging functions (SBI-CHF) to enable operators to charge for the OP's services.

    - Interacting with the Mobile Network via the Southbound Interface – Network Resources (SBI-NR), for example to:
        - Fetch Cloudlet locations based on the mobile network data-plane breakout location;
        - Subscribe and receive notifications on UE Mobility events from the network to assist applications.
        - Configure traffic steering in the Mobile Network towards Applications orchestrated in Edge Clouds;
        - Receive statistics/analytics, e.g. to influence Application placement or mobility decisions.
        - Receive information related to the network capabilities, such as QoS, policy, network information, etc.
- UNI:
    - Application Instantiation/Termination, e.g. based on triggers from the UNI;
    - Application Endpoint exposure towards User Clients via the UNI;
    - Application Placement decisions, e.g. based on measurements/triggers from the UNI.

Federation Broker and Federation Manager Roles

The Federation Broker and Manager roles in the OP are responsible for interfacing with other OPs via the East-West Bound Interface. Typical scenarios enabled by the Federation Manager role are:

- Federation Interconnection Management;
- Edge Cloud Resource Exposure and Monitoring towards partner OPs;
- Application Images and Application metadata transfer towards partner OPs;
- Application Instantiation/Termination towards partner OPs;
- Application Monitoring towards partner OPs;
- Service Availability in visited networks.

The Federation Broker is an optional role. It acts as a broker to simplify the federation management between multiple OPs.

3. Federation management

The Federation Management feature within the Operator Platform (OP) allows it to engage with other OP instances, often situated in diverse geographical locations. This interaction expands the access for Application Providers to a broader range of Edge Clouds, a larger pool of subscribers, and diverse Operator capabilities. The following prerequisites are essential for activating the federation model:

- Operators need to have an agreement to share Edge Cloud resources;
- Operators need to agree on an Edge Cloud resource sharing policy;
- Operators need to enable connectivity between the OP instances over which East/West Bound Interface signaling flows.

Federation Management serves as the control center through the Management Plane. This plane encompasses a range of functionalities provided to both Application Providers and OPs, enabling them to oversee and regulate resources and applications within the federation they oversee. The Management Plane functionality is implemented through various functional blocks within an OP instance, as detailed in the subsections below. Communication of management actions occurs through interfaces, namely NBI, SBI, and E/WBI.

The Management Plane operates on two domain levels: application and infrastructure (resources). Each domain supports management at two pivotal stages in the life cycle of managed entities: configuration and runtime management.

3.1. Federation Interconnect Management

The OP's Federation Interconnect Management functional block is responsible for initiating and maintaining the Federation Interconnect (E/WBI) between different OP instances. The Federation Interconnect employs secure transport, incorporating features like integrity protection for E/WBI messaging exchanged between OP instances. In the process of establishing the Federation Interconnect, the Federation Managers of the involved OPs engage in mutual authentication to verify each other's identities. Additionally, the functionality of Federation Interconnect Management ensures that the partnering OP is authorized to establish and uphold the interconnect in accordance with the agreed-upon federation terms between the participating OPs/Operators.

3.2. Resource Catalogue Synchronization and Discovery

Operators have the capability to incorporate edge resources into the available resources of the Operator Platform (OP) through the SBI. The OPs are required to exchange and manage information regarding the types of resources they provide to one another (E/WBI). This exchange encompasses details about Availability Zones, including:

- A Region identifier (e.g. geographical area);
- Compute Resources Offered: e.g. a catalogue of resources offered (CPUs, Memory, Storage, Bandwidth in/out);

- Specialized Compute Offered: catalogue of add-on resources, e.g. Graphic Processing Units (GPU), Vision Processing Units (VPU), Neural Processing Units (NPU), and Field Programmable Gate Arrays (FPGA).
- Network QoS supported by the zone: maximum values of latency, jitter, packet loss ratio.
- Supported virtualization technology: only VMs, only containers, both.
- Costs associated with the use of resources. This information can influence the Availability Zone selection (e.g. the use of several small zones, that combined, cover the needed Region and are offered by different partners, instead of a more extensive and expensive zone offered by another partner)

This information is subject to change and can be modified through the E/WBI whenever alterations occur in the geographical area or the types of resources presented to an OP by a partner, as a result of operational or administrative events (e.g., scheduled maintenance). To facilitate this, a subscription/notification mechanism is facilitated via the E/WBI.

3.3. Application and Resources Management

This process involves forwarding a northbound request from one operator to facilitate the accommodation of an Edge Application or resource booking in another operator's Cloudlets. The authorization for deployment or reservation is contingent upon the availability of resources and compliance with the federation agreement. In a Federated model, a single OP can collaborate with partner OPs to support application onboarding, deployment, and monitoring in the partner OP Edge Clouds. Consequently, the E/WBI interface must possess capabilities to facilitate resource reservation, as well as application onboarding, deployment, and monitoring in partner OP Edge Clouds.

Application Providers interact with a specific OP instance, submitting their requests through the NBI and indicating the geographical Regions they intend to target. The OP instance then translates these NBI interactions to the E/WBI. The Application Provider's request includes essential information, such as required CPU, memory, storage, and bandwidth, specified in an application manifest. It may also encompass optional characteristics indicating additional needs of the application, such as latency, prioritization, or reservation. Multiple models for orchestrating applications via the E/WBI may be possible.

In a federation relationship, the Partner OP decides where to deploy applications or which Cloudlet provides the resources available for a reservation, based on the Availability Zone/Region preferences indicated by the Application Provider. The partner OP uses the Application Provider's criteria, received through the E/WBI, to inform its decision. While the application provider's criteria about Availability Zone/Region are considered, ultimately, it is the Operator Platform that determines which edge cloud resources best align with the application requirements (QoS) and the associated costs.

3.4. Edge Node Sharing

Two operators may choose to share edge nodes to enhance their edge presence. For instance, Partner A deploys edge sites in the country's North Region, while Operator B deploys them in the

South Region. In this setup, Operator B can deploy an application on Partner A's edge node, offering connectivity to end-users through their own radio network.

Edge node sharing allows end-users to access the Edge Cloud service, even if Operator B lacks its own edge resources in this region. Instead, Operator B's Edge Cloud service is hosted on Partner A's edge node. The connection between the two operators is facilitated through the E/WBI interface.

The East/Westbound interface allows Operator B's OP to retrieve application instance access information and deliver it to the user, enabling service discovery and delivery similar to when the application originates from a Cloudlet in Operator B's network. When a subscriber of Operator B requests an Edge-Enhanced or Edge-Native Application, Operator B's OP, upon identifying that the most suitable edge node is in Partner A, requests the Edge Cloud service through the E/WBI to Partner A's OP. Due to their long-running partnership, these operators have pre-established commercial agreements, security relationships, and policy decisions, such as QoS-related measures. Assuming adequate edge resources, Partner A can respond with the application endpoint, allowing the subscriber to connect to the application.

It's important to note that network resources remain under the management of Operator B, the provider of the actual mobile network connection to the user. IP connectivity between Partner A's edge node and Operator B is managed to ensure end-to-end QoS delivery for the subscriber. The responsibility for managing edge cloud resources depends on the agreement between the partners, with Operator B likely having a long-term allocation of resources in Partner A's cloudlets and managing them for its subscribers seeking access to the edge service.

Authentication between OPs in a federation interconnect is necessary, requiring authentication information provisioned in the OP. This authentication mechanism can be mutually agreed upon between the involved operators initially, and a more universal solution based on a Certificate.

An OP can authorize a partner OP for a limited duration based on a federation agreement or specific Availability Zones where they possess Edge Cloud resources. This authorization information must be provisioned during partner provisioning. An OP should provide controls to the operator to specify Availability Zones made available to a partner OP, allowing for the sharing of all or part of the resources based on the existing Federation agreement.

3.5. Edge Cloud resource monitoring

The Operator Platform (OP) is required to provide application providers and operators with the ability to monitor resources, including:

- Usage metrics such as compute, memory, storage, and bandwidth (both ingress and egress).
- Event tracking, alarms/faults, and logs.
- Performance metrics.

Default monitoring parameters include usage data for resources consumed, categorized by partner or application. However, specific events, alarms, logs, and metrics should be defined either by the

application provider (for application-related aspects) or by the federation contract between operators (for shared resource-related aspects).

The OP monitors the consumption of Edge Cloud resources by Edge Applications, encompassing applications from partner OPs. Additionally, the OP communicates the resource consumption statistics of its applications to the partner OP through the E/WBI. Resource usage is identified per Operator and Edge Application and may be reported per Availability Zone. This information serves as input for billing, audit, and settlement purposes.

3.6. Operational visibility

The Operator Platforms (OPs) must possess an operational perspective of each other, enabling Fault Management and Performance Management within the boundaries outlined in their federation contracts. This management is reliant on information gathered through the monitoring process. Given the volume of exchanged information, a subscription/notification mechanism should be in place to facilitate filtering of relevant information for Fault and Performance Management.

3.7. Automation Capabilities

The Operator Platform (OP) is required to provide application providers with the automation of routine actions concerning the lifecycle management of resources across a federation. Harmonization of information assets used in a federation is necessary for enabling this automation, as outlined in the Common Data Model. Several key scenarios for automation include:

- Instantiating new application instances.
- Reconfiguration of resources and network to uphold SLAs.
- Executing application policies.
- Reserving and releasing of resources.

4. DLT based federation concept using OP

Distributed Ledger Technologies (DLTs) such as Blockchain can be seen as a secure and failure-resistant platform for both negotiation and execution of the Federation Management feature of an OP. The main advantages of applying blockchain in the federation management include:

- **Security.** The transaction data within each block of the blockchain is timestamped, tamper-proof, and immutable. Any attempts to modify the data would require the collaboration of at least 51% of the nodes being malicious or compromised.
- **Integrity, and trust.** All participants can easily verify the state of the blockchain by confirming that they have observed an equivalent state of the blockchain.
- **Smart Contracts.** Programmable applications that run as autonomous entities or members and are built on top of a blockchain platform, such as Ethereum. These applications contain predefined rules and conditions that automatically execute and enforce transactions or actions when specific conditions are met. This functionality enables them to incorporate business logic and rules, similar to traditional contract agreements.
- **Privacy and transparency.** All transactions, state transitions, and block creations are transparent. Using cryptography, private data can be encrypted and kept confidential while still preserving the specified transition rules.
- **Third-party absence.** The consensus mechanism enables a trustworthy collaboration among anonymous members, eliminating the need for a third-party authority to guarantee the integrity of the participants.

4.1. Federation Challenges

The main challenges associated with multi-domain federation in dynamic environments are presented in Table 1, identifying how these challenges are addressed based on their interconnection approach. In addition, it is emphasized how blockchain as a technology can serve as a fundamental solution to these challenges. Let's first focus on how the multi-domain federation is currently done for the centralized and decentralized-peering types of solutions:

- **Admission Control.** In an open federation, administrative domains have the freedom to join or leave at any time. In a centralized interconnection model, a central authority manages admission control, deciding which domains are allowed to join or leave the network. In contrast, with a decentralized-peering approach, the access can be completely open depending on each individual AD. In both cases, the main challenge is to balance the trade-off between domain openness and preserving privacy, security, and trust. Highly secure frameworks and message exchanges may introduce higher delays or congestion in the federation interaction, while completely open admission could expose ADs to passive spoofing.
- **Availability.** The number of participating ADs changes over time in dynamic environments. Centralized approaches offer easier monitoring of participants but may introduce inconsistencies if there are sporadic failures, as centralized systems are susceptible to single

points of failure. This can lead to the federation becoming unavailable. Decentralized-peering solutions inherently provide more resilience to failures, but the task of tracking the ADs is more complex and may introduce spoofing risks.

- **Dynamic pricing and billing.** ADs seek to increase profits by adjusting the federation price offerings, especially in dynamic environments. A central entity, acting as an auctioneer, can modify federation offerings and oversee the billing process. However, participating domains must voluntarily trust this federation control and pay for it. In the decentralized-peering scenario, the ADs autonomously set the price offerings. The challenge here lies in quickly establishing secure agreements in the form of dynamic SLAs that serve as a baseline for reliable billing. Additionally, implementing mechanisms to identify other domains and securely handle the charging process is costly.
- **Multi-domain quality of service (QoS).** Ensuring QoS across federating domains is particularly challenging in dynamic environments. Both decentralized-peering and decentralized-distributed approaches encounter difficulties in establishing dynamic SLAs and maintaining unbiased monitoring data. Disagreements on monitored data among domains often lead to disputes, requiring third-party entities for SLA monitoring. In the centralized option, a centralized entity is responsible for establishing QoS across domains, controlling and monitoring the entire process.
- **Security and privacy.** Within a centralized interconnection model, ADs rely on the central entity. To enhance security, the central entity might request more information from each AD, which comes at the cost of reduced privacy per domain. On the other hand, a decentralized-peering solution may achieve higher privacy (exchanging less information with peering domains) at the cost of lower-security policies employed.

TABLE 1: FEDERATION CHALLENGES

Challenges	Interconnections		
	Centralized	Decentralized peering	Blockchain
Admission control	Central	Open	Distributed; consensus voting
Availability	High single point of failure	Unknown; fail-safe	Balanced; fail-safe; Incentive to participate
Dynamic pricing and billing	Central auctioneer; single-point control	Autonomous; no control; no billing	Autonomous by default; token-based billing
Multi-domain QoS	Central control and monitoring (dynamic SLAs)	None	Smart contract as dynamic SLAs;
Security and Privacy	High security; Low privacy	Low security; High privacy	High security; High privacy

4.2. Federation using DLT

Just by looking at the main characteristics of blockchain technology mentioned earlier, most of the federation challenges enumerated in Table 1 can be addressed by deploying a non-customized (vanilla) version of a permissioned blockchain network (Ethereum, Hyperledger, Cosmos, etc).

Admission control relies on the blockchain governance policy. Permissioned blockchains typically involve member acceptance through voting. While some domains may act maliciously and reject the entry of new members, they generally have an incentive to increase participation. If it is not the case, multiple blockchain instances may run in parallel.

Availability is ensured through each domain's incentive to maintain an active blockchain node. Consequently, this enhances the network security (avoiding 51 percent attacks) and increases the domain's usage budget (e.g., gas in Ethereum). In the event of a node failure, departure, or compromise, the blockchain network remains operational, and the domain can access it via other nodes using its unique blockchain address.

Security and privacy are established by restricting the usage budget and employing cryptography. Newly joined domains have limited usage budgets or a restricted number of federation announcements, preventing them from spoofing or spamming other participating domains. Communications between domains are recorded as immutable transactions on the ledger, with cryptography for preserving data privacy.

Dynamic pricing, billing, and multi-domain QoS require the implementation of dynamic SLAs and QoS monitoring. A promising approach for achieving this integration involves the use of smart contracts. The ETSI PDL specification hints at this approach by describing a scenario where smart contracts represent a specific service with QoS metrics in a marketplace of SLAs. Customers ready to deploy a service from the marketplace must send a payment blockchain transaction to the corresponding smart contract. An external entity acts as an oracle to monitor QoS metrics and record SLA fulfilment directly in the smart contract. If QoS standards are not met, the smart contract automatically issues a blockchain payment transaction to the customer's blockchain address including the penalty amount. Additionally, service providers, acting as smart contract owners, can dynamically adjust prices in each smart contract before customers make deposit transactions.

4.3. DLT based federation deployment using OP

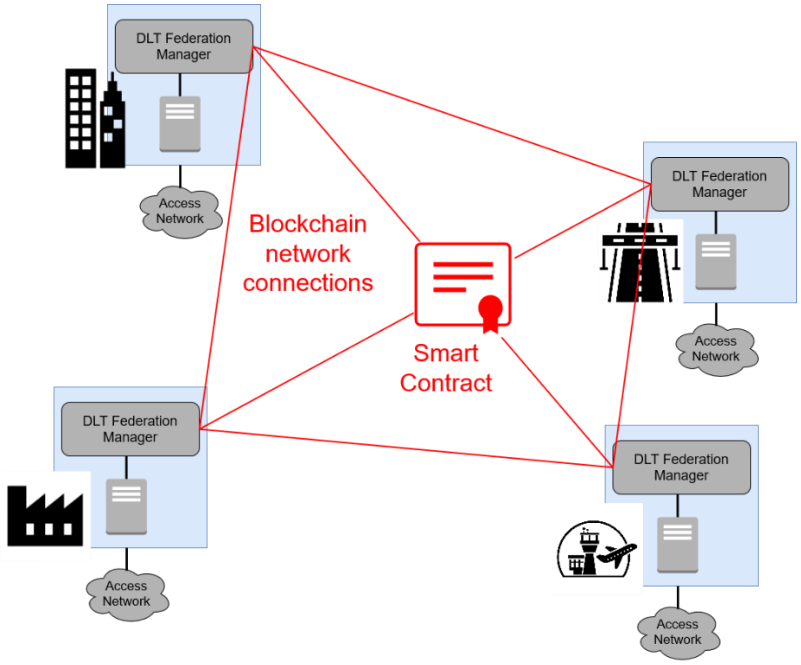

FIGURE 2: OP FEDERATION DEPLOYMNET IN A SINGULAR OPERATOR NETWORK VIA DLT FEDERATOR

Consider the primary scenario for the integrated OP business case, where an OP is deployed at a singular facility such as a factory, hospital, or airport. This OP system is incorporated into the internal operations of the facility owner, potentially for a specific task. Users requiring access within the facility can utilize the OP in these deployments. The deployment at a single facility can be expanded to support users dispersed geographically, utilizing services like V2X or engaging in AR/VR gaming. Utilizing the concept of DLT federation, OP systems from various deployment options can be dynamically integrated (refer to Figure 1). The Federation Manager Role facilitates the connection of individual OP systems through the implementation of DLT capabilities. In a DLT-based federation, each OP must deploy a DLT node. Implementing this concept in a federation scenario involves creating a new smart contract for each federation of services or resources. These smart contracts act as dynamic federation Service Level Agreements (SLAs) ensuring Quality of Service (QoS) between consumer and provider domains.

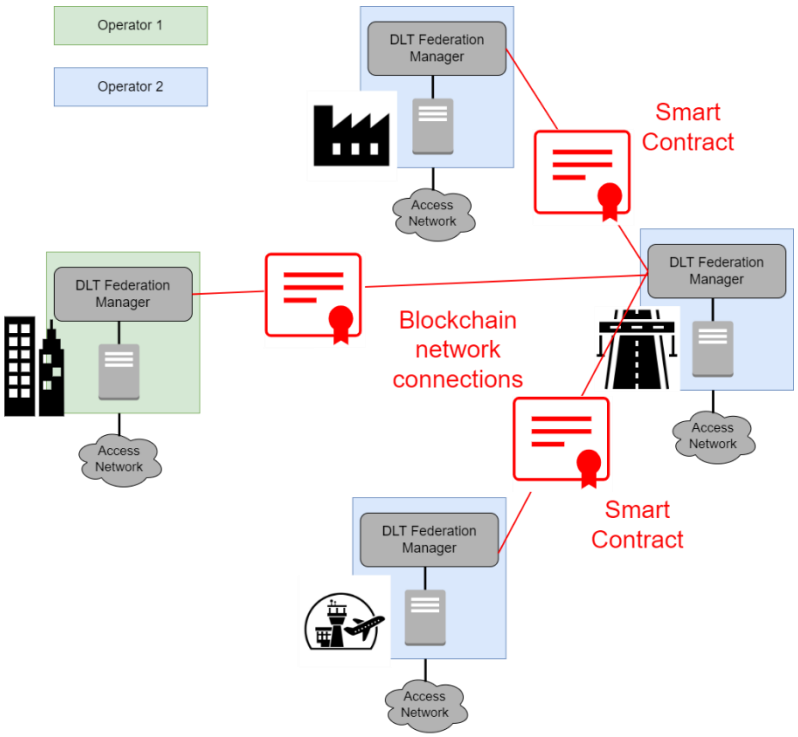

FIGURE 3: DLT FEDERATION DEPLOYMENT WITHIN MULTIPLE OPERATORS.

Extracted from GSMA OP (Association, 2021), DLT federation offers a key advantage of accessing operators systems globally across diverse regions or varied access networks, as depicted in Figure 3. This facilitates application providers in delivering their services to consumers connected to any access network linked to the federated systems dynamically and on demand. Even when consumers transition across different access networks, the application service is anticipated to seamlessly persist as they connect to visited networks. Usually the compute and networking infrastructure are not be under the ownership of the same operator, as exemplified in Figure 3. In a DLT federation deployment, Operator 1 may permit Operator 2 to utilize its system in a dynamic fashion by signing a smart contract that holds the available resources and leasing prices in that specific moment of time. This federation scenario has the potential to address technical complexities. For instance, if Operator 1 deploys a private 5G network (Local 5G), establishing a federated system between operators might pose challenges in managing interconnected networks. Sharing Operator 1's network on-the-fly could offer a workaround for this issue.

The consolidation of systems through a DLT federation can give rise to a compelling business case. A smaller operator, unable to bear the operational expenses (OPEX) associated with maintaining a complete standalone network, with the help of the DLT federation, could be invited to federate with a larger operator's networks that already supports the needed capabilities.

5. Conclusions

This document presents the initial system design for dynamic and agile mechanisms for the interconnection between non public and public networks and compute service providers (for industrial environments). The proposed system re-uses the GSMA OP architecture and extends further the concept of Federation management for dynamically extending the industrial service footprint when needed. In particular, the use of Blockchain technology has been proposed as a mechanism for interconnecting various network operators and in-network compute service providers. The Smart Contract feature of the Blockchain Technology offers unique opportunities for industrial verticals to sing on-the-fly contracts with service providers and rent compute or networking resources while preserving the privacy and security in the interactions. Additionally, some business cases and possible deployment scenarios are described motivating the applicability of DLT based solution for federation.

6. References

Association, G. (2021). *Operator Platform Telco Edge Requirements.* The GSM Association.

Bernardos, C. J. (2023). *Using RAW as Control Plane for Wireless Deterministic Networks: Challenges Ahead.* Washington, DC, USA: Association for Computing Machinery.

Carlos Barroso-Fernández, J. M.-P. (2023). *Aligning rTWT with 802.1Qbv: a Network Calculus Approach.* Washington, DC, USA: Association for Computing Machinery.

Jorge Martín-Pérez, C. J. (2022). *Initial system architecture.* Online.

Kiril Antevski, C. J. (2023). Applying Blockchain consensus mechanisms to Network Service Federation: Analysis and performance evaluation. *Computer Networks*, 109913.

Zahir, A., Groshev, M., Antevski, K., J.Bernardo, C., Ayimba, C., & Oliva, A. d. (2024). Performance evaluation of Private and Public Blockchains formulti-cloud service federation. *International Conference on Distributed Computing and Networking (ICDCN24).* Chennai, India: ACM.