E2.1 Use Cases and Requirements Elicitation v1.0

Publication Date: 30/06/2023

DLT for 6G: Smart Marketplace
[6GENABLERS-DLT]
TSI-063000-2021-12

6G Networks Enabled through Technology Driven Solutions
[6GENABLERS]

Programa de Universalización de Infraestructuras Digitales para la Cohesión – 6G I+D

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

Work Package (WP)	P2
WP Leader	i2CAT
Main Editor	Adriana Fernández-Fernández (i2CAT)
Contributors	i2CAT, ATOS, VICOM
Dissemination Level	PU
Type	RE

Dissemination Level	
PU	Public
PP	Restricted to other program participants
RE	Restricted to a group specified by the consortium
CO	Confidential for consortium members only

Type	
PR	Prototype
RE	Report
SP	Specification
TO	Tool
OT	Other

	Document version history			
Version	Authors	Status	Date	Comments
v0.0	Adriana Fernández-Fernández	Template	27-04-23	Document structure and ToC
v0.1	Adriana Fernández-Fernández, Mario Montagud (i2CAT)	Working Document	10-05-23	Use Case Description
v0.2	Adriana Fernández-Fernández	Working Document	31-05-23	Smart Discovery contributions
v0.3	Adriana Fernández-Fernández, Guillermo Gómez (ATOS), Ángel Martín (Vicomtech)	Full document Version ready for tech review	02-06-23	Merge partners contributions. Add general sections
v0.4	Adriana Fernández-Fernández, Guillermo Gómez (ATOS), Ángel Martín (Vicomtech)	Full document Tech review comments	22-06-23	Address tech review comments
V0.5	Adriana Fernández-Fernández, Ángel Martín (Vicomtech)	Version ready for QA review	26-06-23	Address tech review comments
v1.0	Adriana Fernández-Fernández	Version ready for submission	30-06-23	Address QA review comments

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Table of Contents

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

List of Tables

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

List of Figures

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

List of Acronyms

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
5GaaS	5G-as-a-Service
5GZORRO	Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks
6G	Sixth Generation
ACTN	Abstraction and Control of Traffic Engineered Networks
AI	Artificial Intelligence
AN	Active Network
ANM	Autonomic Network Management
API	Application Programming Interface
B2B	Business to Business
B2C	Business to Consumer
B5G	Beyond 5G
BGP	Border Gateway Protocol
BSS	Business Support Systems
CCAM	Cooperative, Connected and Automated Mobility
CN	Core Network
CNC	Customer Network Controller
CNF	Containerised Network Function
COMS	Common Operation and Management on network Slices
CPU	Central Processing Unit
CSP	Communication Service Provider
DAG	Directed Acyclic Graph
DHT	Distributed Hash Table
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
E2E	End-to-End
eIDAS	electronic IDentification, Authentication and trust Services
eMBB	Enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
EU	European Union
GPU	Graphics Processing Unit
GSMA	Global System for Mobile Communications
GST	Generic Slice Template
IBN	Intent-based Network Management
ICT	Information and Communications Technology
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISG	Industry Specification Group
ISO	International Organisation for Standardisation
IT	Information Technology
K8s	Kubernetes
KPI	Key Performance Indicator
LCM	Lifecycle Management
MANO	Management and Orchestration

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

MDSC	Multi-Domain Service Coordinator
MEC	Multi-Access Edge Computing
MEF	Metro Ethernet Forum
mIoT	Massive IoT
ML	Machine Learning
MNO	Mobile Network Operator
NaaS	Network as a Service
NFT	Non-Fungible Token
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
NGP	Next Generation Protocols
NLP	Natural Language Processing
NS	Network Service
NSC	Network Slice Customer
NSD	Network Service Descriptor
NSI	Network Slice Instance
NSP	Network Slice Provider
NSSI	Network Slice Subnet Instance
NWDAF	NetWork Data Analytics Function
OAM&P	Operations, Administration, Maintenance and Provisioning
ODA	Open Digital Architecture
ONAP	Open Network Automation Platform
OSM	Open-source MANO
OSS	Operations Support Systems
P2P	Peer-to-peer
PBNM	Policy-based Network Management
PDL	Permissioned Distributed Ledger
PNC	Provisioning Network Controller
PNF	Physical Network Function
PNFD	Physical Network Function Descriptor
PoC	Proof of Concept
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
SA	Stand Alone
SC	Smart Contract
SD	Smart Discovery
SDN	Software-defined Network
SDO	Standards Developing Organisation
SDR	Software-defined Radio
SFC	Service Functions Chains
SLA	Service Level Agreement
SLO	Service-Level Objective
SNS-JU	Smart Networks and Services Joint Undertaking
SOFIE	Secure Open Federation for Internet Everywhere
SON	Self-Organising Networks
SSE	Sum of Squared Error
SST	Standardised Slice Type
SVM	Support Vector Machine

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

TC	Technical Committee
TCO	Total Cost of Ownership
TEAS	Traffic Engineering Architecture and Signalling
TM Forum	Tele Management Forum
TN	Transport Network
TOSCA	Topology and Orchestration Specification for Cloud Applications
TR	Technical Report
TS	Technical Specification
T&Cs	Terms and Conditions
UC	Use Case
UNICO	Universalización de Infraestructuras Digitales para la Cohesión
URLLC	Ultra-Reliable Low Latency Communications
UUID	Universally Unique Identifier
VNF	Virtual Network Function
VSC	Vertical Service Consumer
VSP	Vertical Service Provider
VSV	Vertical Service Vendor
xNF	Any Network Function
XR	Extended Reality
ZTM	Zero-Touch Network Management

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Executive Summary

This document corresponds to the deliverable *E2.1 Use Cases and Requirements Elicitation*, envisaged in the framework of the project 6GENABLERS-DLT (TSI-063000-2021-12). Starting the technical work, this deliverable provides a comprehensive exploration of the 6GENABLERS-DLT project, focusing on multi-party collaboration in dynamic 6G environments. It presents the state-of-the-art technologies, including Distributed Ledger Technologies (DLTs), Smart Contracts, Smart Discovery, and Service Level Agreement (SLA) assurance, which serve as the building blocks for the DLT-anchored Smart Marketplace to be developed within the project. The document describes a Use Case (UC) centred around multi-party real-time holographic communications, showcasing the role of these technologies in enabling future 6G networks. It outlines UC scenarios, defines actors and roles, and highlights the main benefits provided by each technological pillar. The platform capabilities and requirements for the DLT, Smart Contracts, Smart Discovery, and SLA assurance systems are detailed. Key performance indicators (KPIs) and evaluation criteria are identified for each technological pillar, providing a framework for assessing their effectiveness. Overall, this document serves as a comprehensive guide to understanding the objectives, technologies, UC scenarios, and requirements of the 6GENABLERS-DLT project, paving the way for the development of innovative solutions in the 6G ecosystem.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

1 Introduction

The 6GENABLERS-DLT project is dedicated to addressing the challenges of multi-party collaboration within dynamic Sixth Generation (6G) environments, where operators and service providers frequently rely on third-party resources to fulfil their contractual obligations. The project aims to offer a comprehensive solution that enables seamless resource sharing among multiple parties, fostering collaboration and innovation.

At the core of the project is the development of a decentralised Marketplace anchored on Distributed Ledger Technologies (DLTs) (i.e., the 6GENABLERS Marketplace), which serves as a collaborative platform for operators, resource and service providers to advertise their offerings to potential consumers. This Marketplace acts as a club where participants can discover, trade, and access resources in a transparent and efficient manner. The 6GENABLERS Marketplace operates within a permissioned environment, where participants are authorised to join. This permissioned nature distinguishes it from public DLT/Blockchain solutions, addressing vulnerabilities and complexity concerns of open trading systems. By carefully controlling participant access, the 6GENABLERS Marketplace enhances security measures and reduces the risks associated with public DLTs, where anyone can join and participate in the consensus process. This permissioned approach allows for greater control, governance, and privacy within the Marketplace, making it well-suited for specific enterprise or consortium Use Cases (UCs) in the Information and Communications Technology (ICT) sector.

The range of resources available within the Marketplace is vast and encompasses various aspects of the 6G network infrastructure. These resources include virtualised mobile core components, Radio Access Network (RAN) assets, edge and cloud infrastructure, as well as vertical applications tailored to specific industry needs. This diverse array of resources caters to the evolving requirements of 6G environments, where flexibility and scalability are of paramount importance. By leveraging the Marketplace, operators and resource/service providers can seamlessly tap into the telco assets offered by different providers, enabling them to meet their operational needs and deliver enhanced services to end consumers.

The 6GENABLERS Marketplace embraces decentralisation as a core design principle to address the limitations of centralised approaches. By adopting a decentralised architecture, it mitigates the risks of a single point of failure and eliminates the need for a trusted party as the central operator. To achieve this, the system will consist of multiple interconnected nodes or instances that work together to form a distributed network, instead of relying on a single centralised instance. The decentralised nature of the Marketplace ensures transparency, trust, redundancy, fault tolerance, and resilience against single points of failure, enhancing the system's robustness.

Through the 6GENABLERS-DLT project, the vision of a highly interconnected and collaborative 6G ecosystem comes to fruition, where stakeholders can harness the collective power of resources to drive the next wave of technological advancements. This deliverable will delve deeper into the technical aspects and functionalities of the Marketplace, showcasing the transformative potential it holds for multi-party collaboration within the dynamic landscape of 6G environments.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

1.1 Document Scope and Objectives

The present document corresponds to the first technical deliverable of the 6GENABLERS-DLT project. As such, this deliverable provides the definition of the project UC, featuring a multi-party real-time holographic communications service, which will serve as a validation for the role of the 6GENABLERS Marketplace as an enabling technology for future 6G networks. Additionally, this document defines specific validation scenarios and outlines the systems' requirements, which are gathered in an agile way, taking into account that new and/or different requirements may have to be implemented as the project execution unfolds.

In correspondence with the aforementioned scope, the primary objectives of this document are as follows:

1. UC Definition: The document provides a detailed description of the selected UC, which serves as a crucial validation point for demonstrating the capabilities of the 6GENABLERS Marketplace. The UC showcases the application of the Marketplace within the context of a multi-party real-time holographic communications service, highlighting its potential in facilitating collaborative communication experiences.
2. Technology-Based UC Scenarios: The document further presents technology-based UC scenarios that are closely tied to the application of the technological pillars, namely DLTs, Smart Contracts, Smart Discovery, and Service Level Agreement (SLA) assurance. These scenarios explore how each of these building blocks contributes to the successful implementation and operation of the multi-party real-time holographic communications UC, enabling seamless collaboration and resource sharing.
3. Systems Capabilities and Requirements: In addition to the UC scenarios, the document outlines the associated functional and non-functional requirements that the envisioned systems must meet. These requirements serve as guidelines for the design, development, and implementation of the 6GENABLERS Marketplace. By defining these requirements, the document ensures that the Marketplace adequately supports the needs and expectations of the involved stakeholders.
4. Key Performance Indicators (KPIs): Lastly, the document highlights the importance of monitoring and evaluating the performance of the technological pillars through KPIs. It identifies specific KPIs related to each pillar, providing a measurable framework to assess the effectiveness and efficiency of the Marketplace in enabling multi-party real-time holographic communications. These KPIs serve as benchmarks for evaluating the success of the project and guiding future improvements.

1.2 Relation to the Project's Activities

This deliverable constitutes a key outcome of Work Package 2 (P2). This work package focuses on identifying and defining the UC specifications for future 6G networks, with a specific emphasis on utilising DLT as an enabling technology for multi-party resource and service trading. P2 aims to provide a comprehensive illustration of the DLT-anchored Marketplace platform, showcasing its potential usage through technical-oriented

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

scenarios. Additionally, P2 will design an architecture that fulfils the requirements of the enablers, ensuring flexibility for adaptation during implementation while upholding essential architectural qualities such as reliability, scalability, and maintainability. The ultimate goal is to establish a robust and efficient framework that aligns with the evolving needs of the envisioned 6G networks, leveraging the capabilities of DLT as a foundational technology.

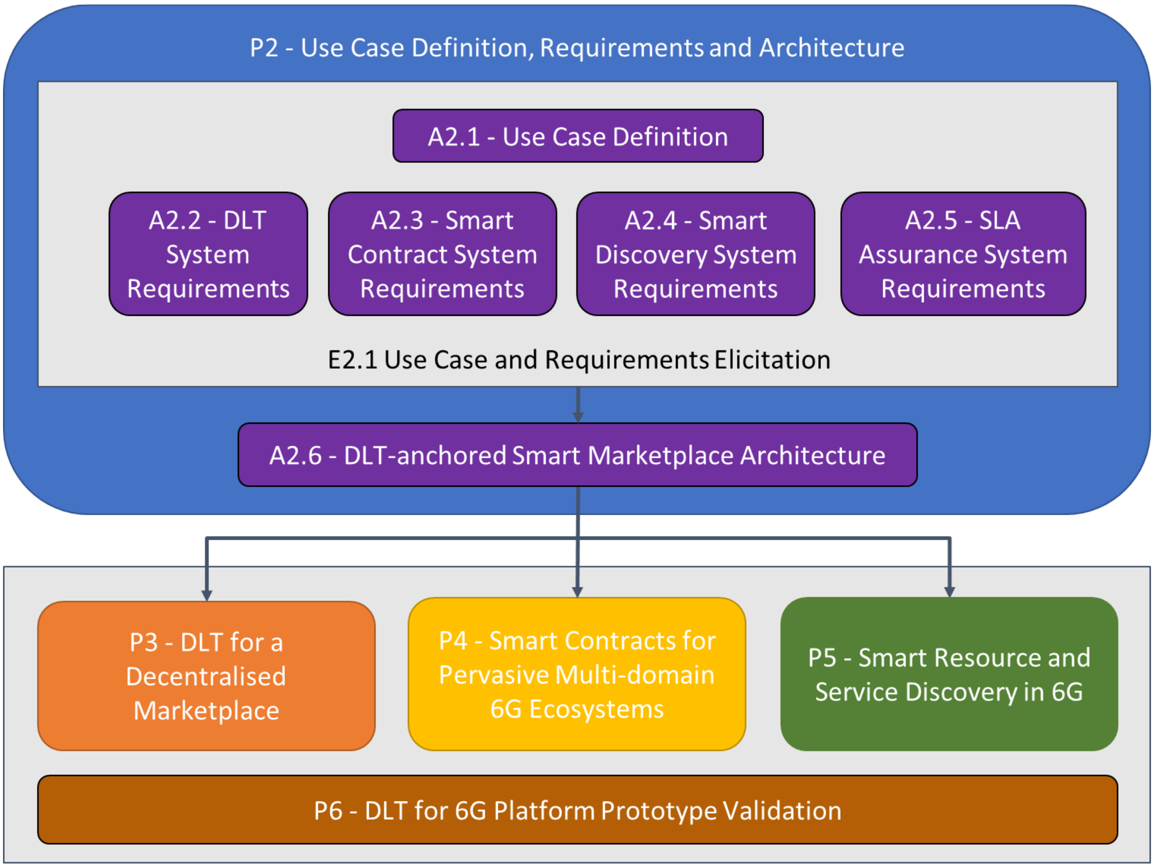

Figure 1-1. E2.1 positioning and relation to the project's activities

As depicted in Figure 1-1, deliverable E2.1 is the joint result of the work done in five tasks within P2, which are listed below:

- A2.1 – Use Case Definition: This task focuses on identifying technology-based UC scenarios for a multi-party real-time holographic communications service that aligns with the immersive environments expected in future 6G networks.
- A2.2 – DLT System Requirements: This task delves into the analysis of system functionalities related to DLT frameworks. Additionally, KPIs are identified to indicate expected capabilities and thresholds for the system.
- A2.3 – Smart Contract System Requirements: This task focuses on the requirement analysis of system functionalities related to Smart Contracts for negotiation purposes. Like A2.2, KPIs are identified to ensure the system fulfils the expected capabilities.
- A2.4 – Smart Discovery System Requirements: This task involves a detailed requirement analysis for system functionalities associated with Smart Discovery capabilities. Likewise, KPIs are established to determine the system's expected capabilities and thresholds.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

- A2.5 – SLA Assurance System Requirements: This task focuses on the requirement analysis of system functionalities related to SLA assurance capabilities. Similarly, KPIs are identified to ensure the system meets the expected capabilities and thresholds.

The insights gathered from the earlier tasks regarding the system requirements of the technological pillars will play a crucial role in shaping the functional architecture of the DLT-anchored Distributed Telco Marketplace (A2.6 – DLT-anchored Smart Marketplace Architecture). This design, along with the specified requirements and system capabilities, will serve as the foundation for the subsequent development of prototypes to be conducted in P3, P4, and P5. Furthermore, the identified KPIs will be instrumental in validating the platform's performance and effectiveness in a later phase during P6. This holistic approach ensures that the architecture and prototypes align with the project's objectives and pave the way for a robust and successful implementation of the envisioned Marketplace.

1.3 Structure of the Document

The current document is structured in several sections that set the stage for defining the capabilities of the 6GENABLERS Marketplace in the evolving landscape of 6G networks. In particular, the document is structured as follows:

- Section 1: This section provides an overview of the document, including its objectives, the relationship to the project's activities, and the structure of the document itself.
- Section 2: This section explores the current state-of-the-art and provides a detailed description of the technologies relevant to the project, namely DLT, Smart Contracts, Smart Discovery, and SLA assurance.
- Section 3: This section presents a specific UC focused on multi-party real-time holographic communications. It includes a description of the UC and scenarios particularly relevant for each one the associated technologies. It also defines the actors and roles involved in each scenario and outlines the main benefits provided by each technological pillar.
- Section 4: This section outlines the capabilities and requirements of the platform. It specifies the system capabilities, functional requirements, and non-functional requirements for DLT, Smart Contracts, Smart Discovery, and SLA assurance.
- Section 5: In this section, KPIs and evaluation criteria are identified for each technological pillar. It provides a framework to assess the performance and effectiveness of DLT, Smart Contracts, Smart Discovery, and SLA assurance in meeting the project's objectives.
- Section 6: The conclusion section summarises the main findings and highlights the key takeaways from the document.
- Section 7: This section lists the sources and references cited throughout the document, providing a comprehensive list of the materials used to support the information presented.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

2 State-of-the-Art and Technologies Description

In this section, we provide an overview of the state-of-the-art and the technologies description of the main pillars that form the foundation of the 6GENABLERS-DLT project. These technologies include DLTs, Smart Contracts, Smart Discovery, and SLA assurance. Understanding these building blocks is crucial for comprehending the advancements and innovations that our project aims to achieve.

- **DLT** is a decentralised and immutable digital ledger that records transactions across multiple nodes in a network. It eliminates the need for a central authority by employing consensus algorithms, which often have a foundation in game theory principles, and public key cryptography to validate and secure transactions. DLT provides transparency, trust, and immutability, making it an ideal technology for building secure and tamper-proof systems. Examples of DLT platforms include Blockchain and Directed Acyclic Graph (DAG) systems.

- **Smart Contracts** are self-executing contracts with the terms of the agreement directly written into code. These contracts automatically enforce the predefined rules and conditions, eliminating the need for intermediaries. By utilising Smart Contracts, parties can securely and efficiently interact with each other, ensuring trust and transparency in transactions. Smart Contracts are an integral part of DLT-based systems and play a vital role in automating business processes.

- **Smart Discovery** refers to the process of intelligently discovering and selecting resource/service offers that best meet specific requirements. It involves leveraging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) to analyse and match user intents with available offerings. Smart Discovery enables efficient resource allocation, enhances user experience, and optimises system performance. It plays a crucial role in the dynamic 6G ecosystem by facilitating the identification and selection of appropriate resources and services offered over the Marketplace.

- **SLAs** are contractual agreements between service providers and consumers that define the quality and performance metrics of a service. They establish the expectations, responsibilities, and guarantees between the parties involved. SLAs outline the agreed-upon service levels, such as availability, response time, and reliability, ensuring that the service meets the defined standards. In the context of the 6GENABLERS-DLT project, SLAs are essential for governing the relationships and interactions among stakeholders within the Marketplace.

By understanding the capabilities and implications of these technologies, we can better appreciate the transformative potential of the 6GENABLERS-DLT project. These technologies form the basis for building a secure, decentralised, and efficient ecosystem that enables multi-party collaboration, automated transactions, intelligent resource discovery, and adherence to service-level commitments. In the following subsections,

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

we will delve deeper into the utilisation and integration of these technologies within our project framework.

2.1 Distributed Ledger Technologies

Distributed ledgers consist of a secure database for tracking physical or virtualised resources, without requiring a centralised mediation. The benefit of a distributed ledger is its potential for minimising the latencies and the costs associated with data exchange. Each record in the distributed ledger is time stamped, together with an associated unique cryptographic signature ensuring the authenticity and the integrity of the data without a central trusted intermediary validating the records and transactions. The type of DLT is based on the process for establishing consensus between nodes storing data. The consensus process can be either permissioned, where just private and restricted access to individuals is allowed, or permission-less, implying public access.

DLTs provide support for Smart Contracts as a digital document to be automatically stored over a distributed infrastructure. This technology also brings some key features for contracts such as, immutability of the stored contracts, different visibility alternatives for public or private access, decentralisation avoiding the control from a central entity, transparency as all the participants can track the changes and updates, and participants cannot repudiate a stored contract. These functions open the possibility of developing solutions for the interconnection of network segments in accordance with agreed levels of Quality of Service (QoS).

DLTs have a promising future within the current Fifth Generation (5G) of mobile networks and future 6G networks where the intelligence and automation to manage different logical and virtual networks allow an efficient response to the concurrent communications needs of different applications or services. In this way, the technologies for orchestrating "network slicing" solutions across different networks can be supported by decentralised DLTs for multi-lateral agreements.

2.1.1 DLT in the Telecom Sector

5G is supported by the transformation of network functions into programmable software components, remotely controlled through Application Programming Interfaces (APIs), which are virtualised and instantiated on top of cloud technologies, enabling cost-performance trade-off control. These software and virtualisation paradigms open new possibilities for smart, dynamic and efficient network management enabling on demand scaling and efficient provisioning to satisfy application and service demands.

High-performance applications such as multi-party Extended Reality (XR) involve distant participants which can be in remote locations, which implies the use of different mobile networks local to the users. These applications need wireless setups to enhance immersivity and enforce the feeling of freedom of mobility.

Thus, some applications could need network assets devoted to their traffic to ensure the required communications performance. Network slicing is the solution from network operators to provide logical networks for specific applications, services, protocols or users. A network slice spans radio, core and edge resources inter-connected as an isolated network.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Network operators could get new money flows monetising their infrastructures and assets making them available in a marketplace, where application developers or virtual operators could ask for a network slice ready to be used. As different roles and managers meet in a single marketplace a contract to link up different participants and stakeholders is needed.

It becomes evident that in a context with distributed infrastructures and different actors, where decentralisation, transparency and no-repudiation are required by design, DLT makes the difference when compared to legacy/traditional trading systems of virtualised assets on Cloud platform vendors.

Unlike traditional communications networks, future networks are expected to be distributed, decentralised, autonomous, and self-managed. The digital transformation of networks is based on technologies such as the transformation of network functions into software services that can be programmed and remotely operated, and virtualisation that brings all the benefits of mature cloud infrastructure solutions, which allow a radical change in the management and operation of networks so that they can behave dynamically, elastically, adaptively and cooperatively.

All these features turn DLT into a perfect technology to sustain a 6G marketplace with network operators offering their infrastructures and application managers or virtual operators ordering specific assets on the available networks to achieve a target QoS by means of a declared cost.

2.1.2 DLT Enabler for 6G Marketplaces

DLT will have a salient position in the telecommunications industry as it fuels the path towards a decentralised marketplace for multi-administrative domains, where different networks have their own operators and administrators. An open and decentralised marketplace can aid 6G UCs such as inter-provider agreements, where multi-administrative domains can lease or buy resources to meet the needs of consumers. Going further, the agreements between multi-administrative domain managers can be performed using DLT, fostering trust and transparency for SLA management, penalties, or billing.

Some authors [1]-[4] have recently outlined the role of DLT for registering inter-provider agreements that allows stakeholders to transact and exchange network resources while maintaining trust. The work in [1][2] studies the 5G scenarios, the architectures, the view from multiple stakeholders and intended use, such as cognitive automation and Self-Organising Networks (SON) [3], as wells as SLA enforcement and accountability including Smart Contracts for SLA [4]. However, they lack engaging telecom providers, the assessment of multi-domain Quality of Experience (QoE) and an implementation with tests.

In such a context, the management of different actors, roles and identities in a multi-domain context is a core topic, where Decentralised Identifiers (DIDs) [5] provide verifiable and decentralised digital identities, and electronic IDentification, Authentication and trust Services (eIDAS) regulation [6] is a key enabler for secure cross-border transactions. Going deeper in the design stage, the authors in [7] propose an architecture for Smart Contracts including SLA governance. However, solutions for radio and

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

spectrum resource sharing and the identities management for multi-domain networks are not covered.

Some works [8] tested Ethereum for contracting network resources concluding that it involves high transaction costs and latencies. Specifically, for a marketplace of multiple 5G networks, authors in [9] stress the same technology to check the limitations for live auctions, stressing in this context how the latency affects to the general timing of the marketplace dynamics and ignoring the complexity of multiple actors. Whereas authors in [10] study the storage costs of Smart Contracts emulating the analysis in a testing network. Other authors [11] move to permissioned (Hyperledger Fabric and Quorum) and permissionless (Ropsten testnet) ledgers to evaluate Smart Contracts for SLAs but ignore the multi-domain operation. Furthermore, some works [12] also investigate the agreements on shared spectrum at different locations including tracking and verification for regulation authorities.

Moving from the atomic tests of DLTs and conceptual vision on its role for multi-operator network marketplaces, to a complete telecommunications marketplace, the authors in [13] propose a specific format for the Smart Contract with focus on SLA conditions. Authors in [14] design, implement and validate an identity system for multiple domains and actors in the marketplace. Authors in [1] explore how to simplify the orders to make selection from offers more accurate and intelligent lacking the production of a standard vocabulary and taxonomy. The work in [15] provides the application of configurations on slices on top of multiple networks for the realisation of zero-touch management but it does not provide an interface or the implementation to broker different orchestrators and controllers. Finally, different authors [16][17] identify DLT and AI as key technologies in 6G, beyond visible light and millimetre wave communications. These AI investigations need to move from the simulations to field experiments.

2.1.3 DLT Standardisation and Specifications

The list of 5G/6G projects in the European scope using DLT in the telecommunications industry are described in this section. The project 6G Flagship employs DLT to reach consensus for ordering concurrent spectrum use [18]. The project 5GaaS provides pre-designed contracts lo lease spectrum, hardware, software components and VNFs using DLT [19]. The project 5GZORRO uses DLT to store the SLA contracts [20]. The project Inspire-5Gplus, exploits DLT for security in Cooperative, Connected and Automated Mobility (CCAM) and Industry 4.0 verticals [21]. The project Dedicat6G employs the DLT technology to trust other systems thanks to the transparency and immutability of distributed data [22]. From this subset, 5GZORRO is the project closer to the vision and technologies involved in this project.

Regarding the open challenges, the 6GFlagship project does not produce a Smart Contract format. The 5GZORRO project does not achieve neither the acceptance from public administration nor the brokerage of different controllers and orchestrators. Furthermore, 5GaaS does not focus on SLAs. The project Inspire-5Gplus does not meet UC implementations in multi-domain environments. Then, Dedicat6G project is limited to the emulation in a testing network.

Beyond the activities and research performed by different projects, there are different Standards Developing Organisations (SDOs) which drive 5G and 6G specifications and could define UCs, interfaces to DLT frameworks from network management systems or

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Smart Contract requirements. It is important to underline, that according to Smart Networks and Services Joint Undertaking (SNS-JU) directives, Blockchain is a key technology, but it is not a core enabler in any of the phase 1 and phase 2 calls. Most relevant initiatives and outgoing specifications for DLT in mobile networks are listed below.

- International Organisation for Standardisation (ISO) is working on UCs and architectures.
  - Technical Specification (TS) 23257:2022 Blockchain and DLT, Reference architecture. This document provides a general architecture not specific for the network industry, so its relevance is limited.
  - Technical Report (TR) 3242:2022 Blockchain and DLT, Use Cases. This document focuses on UCs but with the pending focus on governance, compliance, interoperability, cross-border regulations, and scalability which are not considered.
  - Technical Committee (TC) 307 Blockchain and DLT. This document highlights the identity management and privacy topics but needs to study the business plans.
- Institute of Electrical and Electronics Engineers (IEEE) is focused on the application of DLT to abstract items.
  - Standards Association P2418.10 Blockchain-based Digital Asset Management. This document proposes solutions for digital assets without providing a baseline architectural framework.
- The UCs in the industry that utilise the blockchain have been published by the Tele Management Forum (TM Forum) including a scenario for SLA.
  - TR279 Communications Service Providers (CSPs) Use Cases Utilizing Blockchain (v4.0.0). This document analyses UCs ignoring multiple stakeholders, just focused on service providers.
- European Telecommunications Standards Institute (ETSI) groups are more focused on secured and cognitive networking.
  - ETSI Industry Specification Group (ISG) is studying Permissioned Distributed Ledger (PDL) to commercialise compliant and accountable carrier grade services ignoring technical specifications.
- Internet Engineering Task Force (IETF) is working in protocols in the communications stack.
  - IETF Network Working Group provides a specification for secured Border Gateway Protocol (BGP) and gateways with a narrow view on actors and roles, just focused on the border protocol.
- 3rd Generation Partnership Project (3GPP).
  - Study on Application Layer support for enabling Blockchain usage for 5G Verticals. This document explores extensions on the 3GPP's Release 18 but it does not include interfaces to the Management and Orchestration (MANO) stack.

2.2 Smart Contracts

The telecommunication sector has been under continuous pressure in the past decade to adapt to the rapid trends in competing markets, which are directly eroding the telco's traditional value pools, making it imperative to evolve [23]. In Spain, the 2G/3G networks

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

are expected to be shut down by the end of 2025 [24], thus telco's future is bound to pivot around the 4G/5G/6G networks and the associated technologies, where virtualisation of the infrastructure, digitalisation of assets and their commercialisation in a marketplace play a central role.

Together with DLTs, Smart Contracts (SCs) provide a powerful combination that can enable the creation of a digital, decentralised marketplace that is agile, transparent, secure, and efficient, enabling greater innovation and collaboration. By leveraging these technologies, stakeholders in the telco industry and, even new players, can transact with each other more effectively the commercialisation of virtualised services, infrastructure, and networks.

2.2.1 Smart Contracts Standardisation and Specifications

Standardisation is crucial to enable the realisation of a thriving digital marketplace for the telecommunication sector. Without standardisation, the complexity and cost of integrating different services could become prohibitive, limiting the potential benefits of the ecosystem.

Standardisation is not a one-time action, rather the result of many activities and the lessons learnt from a plethora of innovation and research projects, their continuous feedback and aggregation by several entities devoted to the creation and dissemination of standards. At the European Union (EU) level, the current Horizon Europe programme for research and innovation has increased the total budget about a 20% respect to the previous programme, with a much stronger dissemination and exploitation emphasis to promote and help to create appropriate (international) standards [25]. Two projects can serve as examples in the context of DLT and Smart Contracts due to their similarities with the 6GENABLERS-DLT project. Thus, they will be used as baseline of research and implementation performed in the context of ubiquitous and pervasive SC UCs. Additionally, both projects have had a direct impact on standardisation entities and their outcomes:

- SOFIE (Secure Open Federation for Internet Everywhere) [26]: This project implemented, and distributed as open source, the building blocks needed for other projects such a SMAUG [27] to create a decentralised marketplace based on DLT and End-to-End (E2E) delivery of SC for the rental of smart lockers.
- 5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G Networks) [20]: This project was able to showcase Proof of Concept (PoCs) on the applicability of SCs in Network Services (NSs), trust computations for SCs and federated data, DLT interoperability and Trusted Execution Environments, particularly in UCs such as NFV (Network Function Virtualisation) resource brokering, spectrum trading and service deployment and activation.

Both of the listed projects have contributed and/or used specifications from similar entities at the technical and business level. Thus, these projects are also considered as baseline for elaboration of the requirements of the SC system in this document as well as for the activities to be conducted in WP4, where the system architecture is being designed. The following set of standards, reports and specifications have been examined to drive this document and the overall work on SCs:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

- ETSI is an independent, not-for-profit, standardisation organisation in the field of information and communications [28]. Although it is very extensive, two complementary ISGs from ETSI have released a number of specifications of interest to the project.
    - ETSI ISG for PDL [29] mission is to analyse and provide the foundations for the operation of PDLs, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors.
        - ETSI GR PDL 004: Smart Contracts System Architecture and Functional Specification [30].
        - ETSI GR PDL 008: Research and Innovation Landscape [25].
        - ETSI GS PDL 011: Specification of Requirements for Smart Contracts' Architecture and Security [31].
    - ETSI ISG for NFV counts with more than 10 years of work and has created a large community that intensely works to develop the required standards for NFV transformation incorporating latest technologies, as well as sharing their experiences of NFV implementation and testing in multi-vendor environments.
        - ETSI GR NFV-EVE 010: Licensing Management; Report on License Management for NFV.
        - ETSI GS NFV-SOL 004: Protocols and Data Models; Virtual Network Functions (VNF) Package and Physical Network Function Descriptor (PNFD) Archive Specification.
        - ETSI GS NFV-SOL 007: Protocols and Data Models; Network Service Descriptor File Structure Specification.
        - ETSI GR NFV-SEC 005: Trust; Report on Certificate Management.
        - ETSI GS NFV-SEC 021: Security; VNF Package Security Specification.
- TM Forum [32] is a global industry confederation actively working on evolving current Operations/Business Support Systems (OSS/BSS), seeking solutions that facilitate their consumption by verticals and their integration into existing standards-driven architectural frameworks.
    - TMF IG1143: License Management
    - TMF IF1167: Open Digital Architecture (ODA) Functional Architecture
    - TMF 633: Service Catalog Management
    - TMF 634: Resource Catalog Management
    - TMF 638: Service Inventory Management
    - TMF 639: Resource Inventory
    - TMF 641: Service Ordering
    - TMF 909: API Suite Specification for Network as a Service (NaaS)
- Metro Ethernet Forum (MEF) [33] is a global non-profit industry association of network, cloud, and technology providers that develop standards, certifications and APIs to empower enterprise digital transformation.
    - MEF White Paper: Standardized VNF License Management Framework White Paper

All the revised literature introduced here is being used to realise the architecture of the Smart Contract System and will be reported in deliverable E4.1.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

2.2.2 Smart Contracts Definition and Composition

Traditional contracts are based on manual, time-consuming processes involving intermediaries, e.g., lawyers and brokers, which are not aligned with the agile spirit of a digital marketplace. SCs are tamper-proof thanks to their integration with DLT, which provides the required layer of security and guarantees the correctness of their execution. Thus, SCs are ideal to automate most of the processes of traditional contracts management as they enable a way to remove unnecessary intermediaries, enhance the fairness of critical tasks, guarantee the quality of data sources, etc. Given these capabilities, the idea of automating legally recognised contracts in this way is very appealing.

The work in [34] describes a DLT blockchain system as a finite state machine. Under this perspective, SCs are the state-transition functions that move the system from one state to the other. Therefore, a SC is essentially a program running on a ledger, maintaining some internal state, and updating this state through transactions exposed as an API consisting of one or more functions [35]. Overall, a SC shall be immutable, transparent, self-executable, reusable and accessible to the authorised actors [30].

In general, SCs consist of a combination of both computer code that works based on the terms of the contract, and legal prose that reflects the legal clauses of the agreement between the parties. As a global system, the computer code is therefore also part of the contractual agreement [36]. In the context of 6GENABLERS-DLT, interest is on the definition of the state of the SC, the legal prose side of the SC and the whole set of transactions required to correctly save the agreement in the DLT (see Section 2.2.3). Essentially, the elaboration of a model flexible enough so that it would then be used by a single SC Code to control all agreements in a telco marketplace.

After initialisation of the SC, its clauses are triggered by a series of events which are to be audited against what is defined in the SC state and then reflected in the DLT as an update to the state in a linked transaction. For that information to reach the SC, ETSI PDL [31] proposes a series of strategies for data input and output. Given the selected UC in the project (see Section 3), the most suitable option must allow external input data and events to reach the SC in order to verify that there is no license breach based on the corresponding agreement conditions. Oracles are used to take input from several data sources, process them and provide input to SCs. Oracles are blockchain-agnostic and typically generalised enough to access any ledger and provide the data. A problem with oracles is that they are sometimes not trustworthy [31]. In the case of 6GENABLERS-DLT, the DLT layer will evaluate how to provide a suitable solution to input data and events to the DLT from external components ensuring that the communications are secure and trustworthy.

Given all the information collected from the standards, the E2E SC reference architecture is composed of a three-legged system, depicted in Figure 2-1, which is built around the DLT layer. Next, the three SC components shown in Figure 2-1 will be presented for clarity. Further information and implementation architecture will come in E4.1.

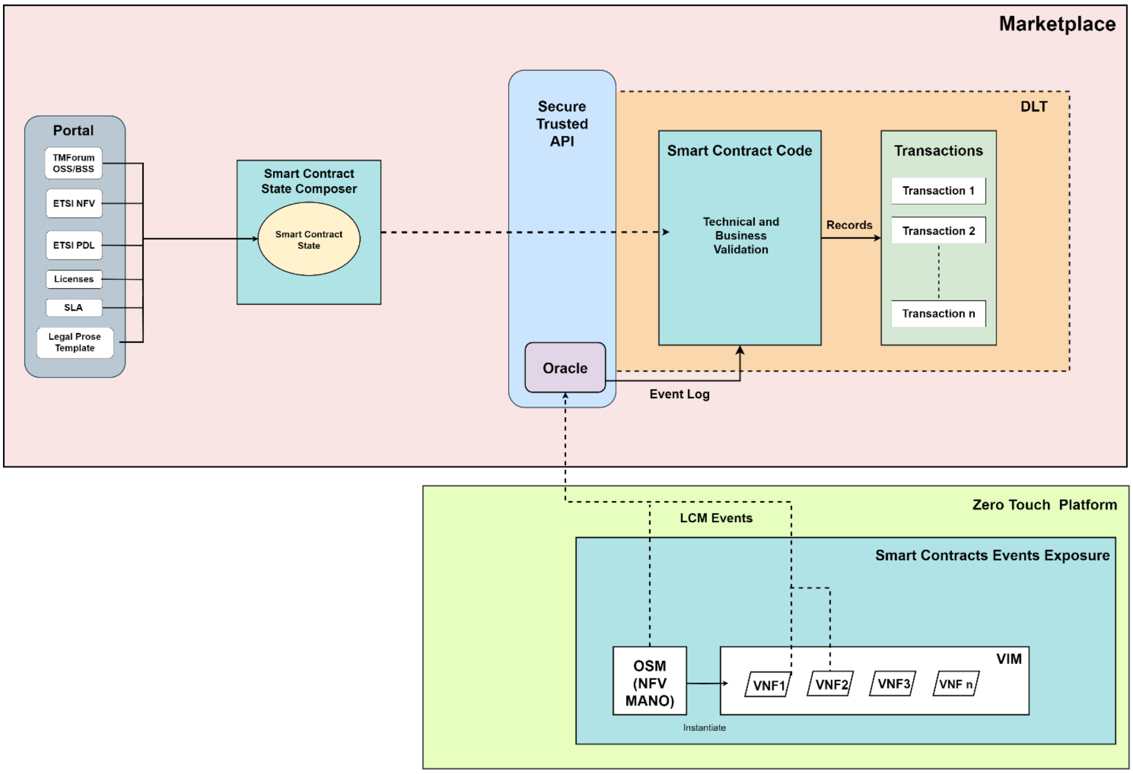

Figure 2-1. E2E Smart Contract Marketplace reference architecture

SC State Composer: The creation of the SC state is the result from the standardisation efforts from TM Forum, ETSI PDL, ETSI NFV and ETSI NFV-EVE. The objective is to best reflect the business model of the asset exchanged allowing a high level of flexibility, granularity, reusability, and particularisation. This state needs to be recorded as a transaction by the marketplace into the DLT using APIs offered by it, each time an event happens which needs to be reflected in the DLT, a new state is appended.

Therefore, a SC's state shall include the following information:

1. The description of the involved actors.
2. The description of the asset, the functionalities included, maintenance and update commitments to the asset, duration of the agreement, termination clause.
3. Manifest of the contents of the asset as a proof to the final user that there is no unilateral change of the asset and thus, the authenticity of the service consumed.
4. A Universally Unique Identifier (UUID) of the asset. This is particularly important as digital assets are difficult to map to a unique and unalterable ID. Not only it is possible to alter the name or ID of a digital asset without affecting to the manifest content, but also, digital assets are referenced based on the hosting service, which may or may not be part of the marketplace platform.
5. Associated licenses and Terms and Conditions (T&Cs) of commercialisation to ensure that all legal requirements are duly recognised and technically verified through the chain of transactions in which the asset might be involved, e.g., Business to Business (B2B) and then Business to Consumer (B2C).
6. Description of the restrictions and limits of usage. While the T&Cs may focus on the legal and business limits of usage, digital assets need an additional description of the limits from a technical perspective by including an actual

metrics that can be audited. This item necessarily involves the description of monitoring mechanisms to track such metric.
7. Pricing model. The cost of using the asset may be provided as a single value or tiered cost structure.
8. SLAs defining the committed performance and corresponding indemnification in case of breach. Modern transactions could also include predictive methods for the detection of SLA breaches and thus be able to offer a series of rules and algorithms to trigger automated actions such as scaling or migrating the asset.
9. Additional legal prose defining the rights and obligations of the involved actors in the transaction provided as a human readable report document.

Rendering techniques are being evaluated to compose the final SC report document [37][38]. This step will help define how contracts are written, how they are enforced, and how to ensure that the automated performance of a contract is faithful to the meaning of the legal documentation from a manual auditing point of view [39]. This document shall reflect the whole transaction, including the previous items listed here, but in a human-readable manner. By having the involved stakeholders confirm or sign it and then certified and notarised by the DLT, the document could fully represent the rights and obligations that accrue to the different parties, and potentially be used to referee discrepancies on the decisions taken and thus be legally enforced.

SC Code: Its development and deployment to the DLT needs to go through a series of stages prior to its delivery to a production environment. The design and implementation of a SC is a technically intense activity and, since they are immutable, careful planning and scrutiny of the code before deployment to the ledger is of utmost importance [30]. The resulting SC code shall be immutable, transparent, self-executable, reusable, and accessible to the authorised actors only. ETSI proposes a lifecycle for the development of a SC, depicted in Figure 2-2, that shall be used as reference [30].

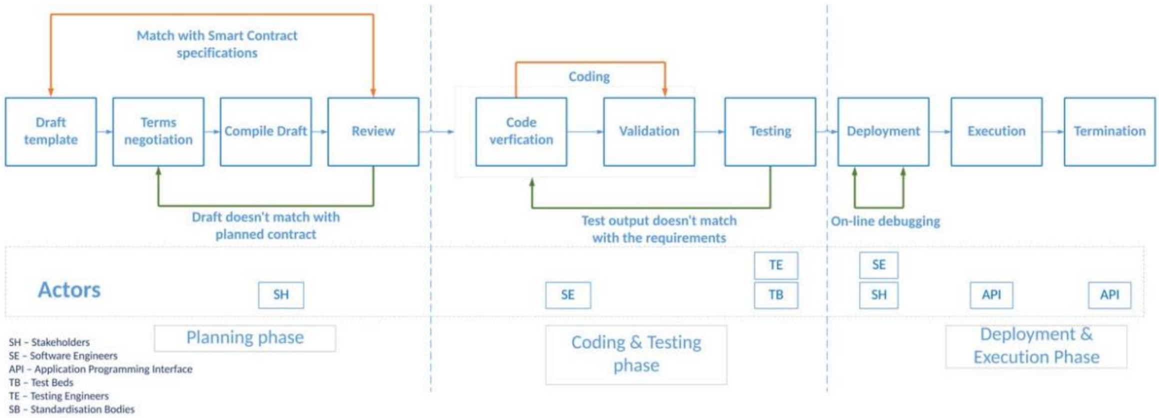

Figure 2-2. Smart Contract code development lifecycle [30]

Overall, it requires a deep understanding of the business objectives of the type of agreements that will be included, as well as of the technical capabilities of the DLT layer. Such scenarios are initially presented in Section 3.3.1.1 and will be further documented in deliverable E4.1. The trade-off for such complexity is that it simplifies the commercialisation afterwards and enables the automation of many time-consuming processes.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

The definition of the SC State has been planned to allow the reutilisation of a single SC Code component thanks to the inclusion of scripts as part of the corresponding resource in the TM Forum data models. Figure 2-2 depicts the reference implementation of the SC Code [36]. This will be further elaborated in E4.1.

SC Events Exposure: The MANO stack and the VNF instances are essential sources of information for the usage validation of an asset e.g., Lifecycle Management (LCM) events including the validation of an instantiation request and the metering and reporting of VNF usage. By interacting with the DLT via oracles or similar, these events can be used as input to the SC code to evaluate them and decide if they are or not aligned with the business and technical constrains and rules contained in the SC state.

The definition of the SC System has been planned to allow the reutilisation of a single SC Code component thanks to the inclusion of scripts as part of the corresponding resource in the TM Forum data models.

Figure 2-3 depicts the reference architecture for SCs proposed by [31], which complies with the definition given here. This will be further elaborated in E4.1. Notice that, in ETSI nomenclature, the DLT layer is referred to as PDL. Additional security aspects need to be studied by the DLT layer as to define how authentication of these APIs works.

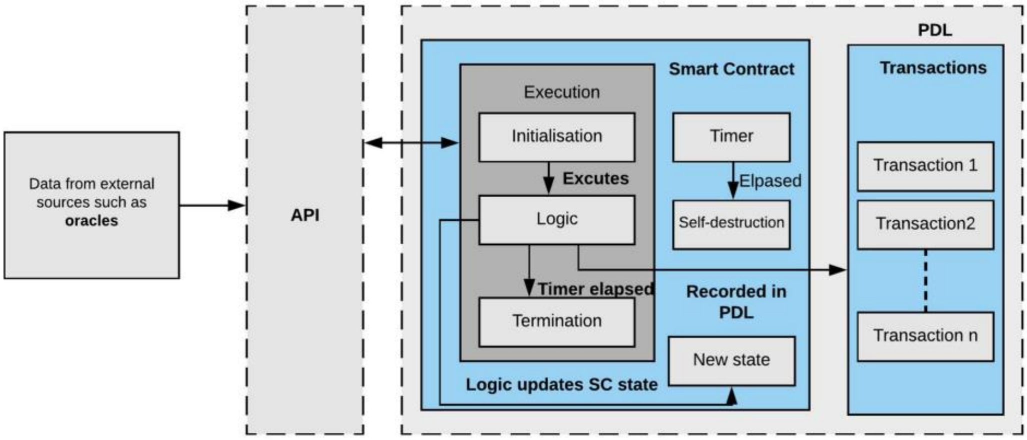

Figure 2-3. Smart Contract with external input through API [31]

2.2.3 Smart Contracts Integration with DLTs

The previous section already introduced a SC System that leverages a DLT layer as a way to ensure immutability and tamper-proof properties. In fact, the proposed definition of the SC system showcases three parts, all of which have some level of integration with the DLT.

Thus, it is recommended the creation of Hybrid Smart Contracts in 6GENABLERS-DLT, which combines code running on the blockchain (on-chain) with data and computation from outside the blockchain (off-chain) to create a feature-rich decentralised application [40]. Adaptations may come due to alignment with the DLT layer of the project.

Although it will be part of E4.1, it is envisioned that for the SC System to be realised, the DLT layer will provide a series of secured and trusted APIs for the inclusion of, at least, the types of objects below.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

- Product Offers
- Product Orders
- Smart Contract States
- Smart Contract Violations
- Service Level Agreements Violations

E4.1 will include the exact data model for each of the objects listed considering the DLT storage requirements and the DLT APIs description.

2.3 Smart Discovery

In 6GENABLERS-DLT, network resources are made available through the Marketplace, enabling operators, resource and service providers to easily discover and access the resources they need to fulfil their contractual obligations. This results in a more efficient and streamlined collaboration process, which benefits all parties involved. Such approach represents a significant advancement in the field of 6G networking, as it provides a unified platform for resource sharing and collaboration among multiple parties, while aligned with the sustainability vision of 6G. Its ability to seamlessly integrate third-party resources from different parts of the network makes it an ideal solution for dynamic and complex 6G environments.

However, considering a decentralised and highly populated Marketplace, finding the right offer can become a complex task. Therefore, a discovery service is aimed to facilitate the interactions of consumers with the offering platform. In the following subsections, we start by defining the role of the discovery service while navigating through its applicability and specifications in various fields. Next, we outline the benefits of considering a DLT-anchored system as main enabler for the automated discovery. Then, some of the major ML techniques suitable to support the discovery functionality are identified. Finally, we revisit some of the existing works regarding the use of discovery services in 6G oriented Marketplaces.

2.3.1 Discovery Service

The concept of providing a discovery service is a fundamental principle in many industries and contexts, and as such it has evolved to meet the needs of users in different settings. Broadly speaking, it involves the identification of elements that meet a particular set of requirements specified in a query. The goal of a discovery service is to help users find what they are looking for quickly and efficiently.

The concept of discovery services has been largely applied in various fields, from e-commerce to data science, and has taken on different meanings depending on the context. In e-commerce, discovery services can help customers find products that meet their needs by providing recommendations based on their previous purchases or search history. In data science, discovery services are used to find insights and patterns in large datasets, helping analysts to make informed decisions based on their findings.

The adoption of discovery services in different contexts has led to the development of various techniques and technologies that aid in the discovery process. These techniques include Natural Language Processing (NLP), ML, and semantic web technologies, among others. These techniques help to improve the accuracy and relevance of the

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

results produced by the discovery service, ensuring that users are presented with the most relevant items that match their requirements.

Another example is the case of peer-to-peer (P2P) file sharing systems, which usually are designed as decentralised and unstructured networks, because they impose few constraints on topology and data placement compared to the structured scheme. P2P file sharing systems are a type of network where users can share files directly with one another, without the need for a central server. In these systems, a discovery service is crucial in enabling users to find the files they are looking for, as they cannot rely on a central index to search for files.

Discovery services in P2P file sharing systems work by allowing users to search for files based on their name, type, or other attributes. The search query is then broadcast to all nodes in the network, and the nodes that have the requested file respond to the query. The search results are then aggregated and presented to the user, who can choose which node to download the file from. This way, users can share files more effectively, as they are not limited by the capacity of a central server. Instead, the network of nodes allows for the distribution of files across multiple users, reducing the burden on any one node. The use of discovery services in P2P file sharing systems has also led to the development of innovative technologies and techniques, such as Distributed Hash Tables (DHTs), which have further improved the efficiency of these systems.

In the cloud-native architecture, the use of discovery services has a very prominent role when designing and deploying efficient and scalable systems. In this type of architecture, applications are built and deployed as a collection of microservices, which are small, independent components that work together to provide the overall functionality of the application. These microservices can be deployed across multiple servers or cloud instances, and as such, a discovery service is essential for enabling these services to find and communicate with each other.

Discovery services in cloud-native architectures work by providing a central registry of all the microservices in the system, along with their endpoints and metadata. When a microservice needs to communicate with another microservice, it first queries the discovery service to locate the appropriate endpoint. The discovery service then returns the endpoint information, which the calling microservice can use to initiate communication with the other microservice. The use of discovery services in cloud-native architectures has enabled developers to build more complex and scalable applications, as they can easily add or remove microservices as needed without disrupting the overall system. It has also facilitated the adoption of containerisation technologies, such as Docker and Kubernetes, which rely heavily on discovery services to manage and orchestrate containers.

In the context of a decentralised DLT-anchored Marketplace, the proposed discovery service is intended to return a customised subset of offers that best satisfy the consumer's expectations. The primary goal of this component is to enable programmatic and intent-based discovery by utilising smart selection techniques based on ML, reducing the burden on the consumer and enabling them to focus on their core business objectives.

By leveraging ML algorithms, the discovery service can learn from the consumer's previous selections and preferences, as well as their current contextual data, to generate

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

a set of recommendations that are tailored to their specific needs. This enables consumers to quickly and easily discover the resources they are looking for, without the need for manual searching or analysis. The inclusion of a discovery service based on ML techniques is a significant advancement, as it ensures that the discovered offers are tailored to the consumer's specific needs and are continuously refined over time, improving the discovery process.

2.3.2 Automated Discovery Enablement

The process of registering resources and services on the Marketplace involves using a standardised data format or schema leading to the composition of offers. This standardisation is crucial to ensure that the offers registered on the Marketplace are easily searchable and understandable by consumers. The registered resources and services form a catalogue of offers available for consumers to browse and select from.

Once registered, these offers for resources and services trading become tokenised digital assets that are stored and tracked by the underlying DLT. The DLT provides a secure and transparent platform for the storage and management of these digital assets. The tokenisation of these assets allows for the creation of an immutable record of offers ownership and availability on the ledger.

This record is maintained and updated over time in accordance with an associated Smart Contract. The Smart Contract governs any state change that may occur, such as a metadata update or when a resource or service is leased to a particular consumer. The Smart Contract ensures that all transactions are recorded on the ledger and that the state of the digital asset is accurately reflected in real-time.

When new offers (and offer updates) become available on the Marketplace, it is essential that all trading stakeholders are informed promptly. This dissemination of information is enabled precisely by posting the offers on the DLT. Once posted on the DLT, the offers are immediately available to all trading stakeholder Marketplace nodes. This means that anyone with access to the Marketplace can view the updates in real-time. This instantaneous availability of information is crucial in ensuring that all trading stakeholders have the most up-to-date information about offers available on the Marketplace.

The dissemination of offers information through the DLT ensures that all trading stakeholders have equal access to the updates. It provides a transparent and decentralised platform for the dissemination of offers, eliminating the need for centralised authorities to disseminate the information. Moreover, the use of a DLT provides a secure and tamper-proof platform for the storage and dissemination of information. The information posted on the DLT is stored in a decentralised manner, which means that there is no single point of failure that could result in the loss of data or a security breach.

Overall, the registration of offers for resources and services trading on the Marketplace using a standardised data format or schema, and the tokenisation of these assets on the DLT, provides a secure and transparent platform for the management and exchange of digital assets. The associated Smart Contract guarantees that all transactions are accurately recorded, providing consumers with a reliable and trustworthy platform for accessing and utilising these digital assets. In this way, the use of DLT and Smart Contracts to exchange new offers and their availability and updates in real time ensures that all trading stakeholders have equal access to the most updated information.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

2.3.3 Machine Learning Techniques

Clustering algorithms are a ML technique widely used in a variety of applications related to data analysis and pattern recognition, including customer segmentation, image recognition, anomaly detection, among others. They are particularly useful for identifying groups of data points that share similar characteristics or properties.

One of the primary advantages of clustering algorithms is their ability to identify patterns in large and complex datasets. These algorithms can automatically group data points into clusters based on similarity or distance metrics, without any prior knowledge of the data structure. This can help uncover hidden patterns in the data, which can then be used for decision making, prediction, or classification.

Another advantage of clustering algorithms is their scalability. They can be used to cluster datasets of various sizes and dimensions, making them suitable for big data applications. Moreover, a distinctive feature of this type of technique, that certainly contributes to its high degree of usability, is that they are also adaptable to different types of data, including numerical, categorical, and text data.

Abovementioned attributes position the use of clustering mechanism as a valuable tool for identifying patterns among the offers exposed on a highly populated Marketplace covering a large heterogeneity of resource categories. Essentially, the introduction of this kind of ML technique in the Marketplace enables the intelligent allocation of offers into various clusters based on their features. This means that clusters' labels are assigned to the offers, allowing for a more consistent mapping between the users' requests and the available resources.

Although clustering algorithms are a popular and effective technique for data analysis and pattern recognition, they have some limitations. For instance, they may not always produce meaningful or useful results if the data is noisy, the input of a request does not have all the features of the training data or if there are no clear boundaries between the clusters. Additionally, the choice of clustering algorithm and its parameters can significantly affect the clustering results, which requires careful consideration and evaluation.

To overcome this, clustering algorithms are often used in conjunction with other ML techniques to create more accurate and efficient data-driven engines. In particular, prior research proposes the combination of offline clustering algorithms, which identify common features and assign cluster labels, and online classification algorithms, which offer more accurate classification and faster retraining [41], [42], [43].

The aim of classification algorithms is to categorise data into distinct classes or groups based on features or characteristics. This technique is commonly used in online systems to predict the class of new data based on patterns learned from labelled training data. Decision trees, random forests, Support Vector Machines (SVM), and Naive Bayes are some of the commonly used classification algorithms.

Decision trees are hierarchical structures that recursively partition data based on the values of attributes to predict the class of an unknown sample. Random forests, on the other hand, use multiple decision trees to make a prediction based on the majority vote of the individual trees. SVM is a binary classification algorithm that finds the optimal hyperplane to separate the data into two classes.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Naive Bayes is a probabilistic classification algorithm that assumes independence between the features of the data. It calculates the probability of a new data point belonging to a particular class by estimating the probability of the features given that class.

By jointly using clustering and classification algorithms a more effective search and classification process can be achieved in the context of the Marketplace. The main benefits of using clustering and classification algorithms together include:

- Improved accuracy: Clustering algorithms can help identify patterns and assign labels to the offers, which can then be used to train the classification algorithms allowing to provide more accurate predictions.
- Faster processing: Clustering algorithms can be used offline to determine the clusters, while classification algorithms can be employed online to classify incoming offers in a more efficient and faster way.
- Enhanced scalability: Clustering algorithms can help reduce the dimensionality of the offers dataset, making it easier to process and classify with classification algorithms, which can improve the scalability of the system.
- Better decision-making: By combining clustering and classification algorithms, it is possible to make more informed decisions based on the characteristics and features of the offers, leading to better resource allocation and optimisation.

In addition to the use of clustering and classification algorithms for the intelligent processing of offers, intent-based approaches stand out as appealing mechanisms for simplifying the interaction of consumers with the Marketplace. In general, intent-based refers to the use of NLP and ML techniques to identify the intent behind a user's query. By analysing the text input, this technique can extract the meaning of the user's request and identify the specific action or information the user is seeking.

Intent-based approaches are used in various domains, such as chatbots, virtual assistants, search engines, and recommendation systems. They enable a more natural and intuitive interaction between users and systems, allowing users to express their needs and desires in their own words, rather than requiring them to learn specific commands or search for information using predefined categories or filters.

In addition to improving the user experience, intent-based approaches can also increase the efficiency and accuracy of systems by reducing the need for manual intervention or interpretation of user input. They can also enable the automation of complex tasks, such as resource allocation in dynamic environments, by identifying the user's intent and provisioning the appropriate services automatically. This can be particularly useful in complex and dynamic environments, where the availability and suitability of resources can change rapidly.

For the purpose of smart discovery, an intent-based discovery enables the automatic selection of offers based on the user's intent or requirements, rather than requiring them to search for and select offers manually. Following this approach, users can express their needs or requirements in a natural language query, which is then translated into a machine-readable format using NLP techniques. The identified user's intent is then automatically mapped to the cluster(s) of offers that best satisfy the customer expectations, based on which a subset of offered resources and services is selected and presented to the user.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

The aim of such intent-based discovery, assisted with clustering and classification techniques, is to provide a more user-friendly and efficient way of accessing resources and services offered over the Marketplace, while also reducing the burden on users to manually search and select offers, significantly enhancing the performance and user experience of the Marketplace.

2.3.4 Smart Discovery in Decentralised 6G Marketplaces

The potential of DLT-enabled Marketplaces in the telecommunication sector has spurred several industrial-driven activities, which have been materialised through the TM Forum Catalyst Projects. These initiatives seek to explore and develop innovative solutions using emerging technologies in the telecommunications industry, with the ultimate goal of advancing the industry forward.

The "Blockchain-based Telecom Infrastructure Marketplace" project focuses on creating a decentralised marketplace for telecom infrastructure assets using blockchain technology. The project aims to simplify the process of transacting assets and services between multiple stakeholders, such as telecom operators and infrastructure providers, by using programmable Smart Contracts [44].

The "Vertical Industry Telcos: a Federated DLT-based Marketplace" project explores the development of a federated digital marketplace that brings together multiple vertical industries and telecom operators. This marketplace will use DLT and Smart Contracts to automate and streamline the process of transacting assets and services, enabling stakeholders to conduct business under transparent and multilateral agreements [45].

The "Digital Business Marketplace III – Delivering end-to-end multi-partner Industry 4.0, now! – Phase III" project focuses on developing a digital marketplace for Industry 4.0 solutions that enables multiple partners to collaborate and offer E2E solutions. The project uses a federated architecture and a combination of emerging technologies such as blockchain, AI, and Internet of Things (IoT) to create a marketplace that offers a seamless and secure experience for stakeholders [46].

The "AI driven business assurance for 5G" project aims to develop an AI-driven assurance system for 5G networks that provides E2E visibility and real-time insights into network performance. The project uses AI and ML techniques to analyse network data and identify potential issues, allowing stakeholders to proactively address them before they impact service quality [47].

Also supporting the aim of a decentralised marketplace, prior research efforts have been conducted by former 5GPPP projects, such as SOFIE, 5GaaS and 5GZORRO, in order to address the need of Beyond 5G (B5G) and 6G systems for ubiquitous connectivity and pervasive computing.

SOFIE (Secure Open Federation for Internet Everywhere) is an H2020 project that focuses on enabling secure and trustworthy interoperability between heterogeneous IoT platforms [48]. As part of this project, a decentralised marketplace using Smart Contracts has been developed. This marketplace allows IoT service providers to offer and consume services in a secure and trusted environment. The marketplace leverages blockchain technology to ensure transparency, immutability, and decentralisation. It uses Smart Contracts to automate the negotiation, agreement, and execution of contracts between

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

service providers and consumers. The marketplace also includes a reputation system to enable trust between the parties.

The 5GaaS (5G-as-a-Service) project is an EU-funded initiative focused on developing a decentralised digital marketplace acting as a one-stop-shop for telecom companies. The 5GaaS marketplace provides a seamless platform for demand and supply of digital assets and services in the telecom sector. The platform relies on the trustworthiness of DLT and the programmability of Smart Contracts, to simplify the transaction process and enable transparent multilateral business agreements between stakeholders such as Mobile Network Operators (MNOs), CSPs, neutral hosts, and landlords [49]. In terms of resource discovery, the scope is limited to ensure the automatic discovery of resources in a decentralised way by leveraging on the DLT infrastructure. To simplify the retrieval and visualisation of offers the marketplace offers a user-friendly interface that masks the complex integration with the DLT.

5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks) is an H2020 project focused on providing a decentralised, trustful, and secure infrastructure for 5G networks, aiming to enable a seamless network ecosystem that can meet the demands of the emerging digital economy. As part of this effort, the project developed a decentralised marketplace that utilises DLT to provide a secure and transparent platform for buying and selling 5G network resources [50]. The marketplace is designed to be flexible and scalable, allowing service and resource providers to easily offer and monetise their resources while ensuring security, privacy, and trust. The project also integrates AI-based resource management to help maximise the efficiency of resource utilisation.

While SOFIE and 5GaaS projects provide functional marketplaces, they do not contemplate the introduction of novel smart discovery capabilities, placing the burden of selecting the most appropriate third-party resources on the customer. In addition to the impact on the customers' QoE, the lack of data-driven techniques also limits the zero-touch capabilities of the system. In contrast, in 5GZORRO the marketplace functionalities are complemented with intelligent discovery capabilities to further foster collaboration for cross-domain resource and service trading among multiple stakeholders in the B5G/6G ecosystem [1]. Therefore, for the smart discovery service of 6GENABLERS-DLT, we will build upon the work done in 5GZORRO, improving the level of decentralisation and the intent-based processing.

2.4 Service Level Agreement Assurance

In modern communication systems, there are heterogeneous connectivity requirements from the applications like mobile devices, virtual reality devices, automatic driving cars, IoT devices, among others [51]. Each type of device or application may have different QoS requirements, meaning they have varying demands and expectations for network performance and reliability. The challenge in modern communication systems lies in providing connectivity solutions that can cater to these diverse requirements simultaneously. Network technologies like 5G, B5G and 6G aim to address this challenge by providing flexible and scalable connectivity options, allowing different devices and applications to be served with the appropriate QoS based on their specific needs, in which network slicing plays a vital role [52]. Network slicing unfolds a new paradigm for the providers as well as for the users.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

The heterogeneous provisioning of QoS to services needs the monitoring of telecommunication resources to control the SLA. SLA compiles expectations about the provided service quality seen from the end-user perspective expressed as aggregated metrics. Thus, the purpose of SLAs is to formally define the delivery parameters guaranteed by the provider. After agreeing upon an SLA, the specified parameters are monitored in order to detect breaches. One of the main issues of SLA creation is to define methods of measuring certain service parameters that must be agreed upon by both sides of the contract. When an SLA breach is detected, an appropriate remedy procedure should be applied. Moreover, the client is eligible to get some compensation from the provider by means of penalties.

2.4.1 SLA Assurance in the Telecom Sector

SLAs heavily rely on KPIs. Thus, all KPIs are periodically captured to evaluate SLAs continuously [53][54]. Solutions for monitoring VNFs include tools such as Monasca for multi-tenant monitoring integrated with OpenStack, Prometheus for Kubernetes, and storage to produce data lakes including InfluxDB and Prometheus for time series. KPIs metrics and activity logs are essential to 5G. The NetWork Data Analytics Function (NWDAF) is designed to streamline the way Core Network (CN) data is produced and consumed, as well as to generate insights and take actions to enhance end-user experience. Introduced in release 15, it has been evolved in release 18 to support Operations, Administration, Maintenance and Provisioning (OAM&P) for intelligence and automation systems including: self-configuration of RAN network entities; enhancement of autonomous network levels, advanced intent driven management services for mobile networks, and AI/ML-based management [55]. For such reasons, NWDAF is the network function that provides analytical services and reporting as part of the 5G CN [56]. Cross-domain data services are also needed to provide data persistence across management domains while also allowing management systems to run on the stored data as a way to achieve E2E global optimisation.

The monitoring of QoS parameters of specific applications could imply to deploy specific agents to assess the metrics at different levels [57] and network systems [54]. The mapping of low-level system metrics to high-level QoS values in the SLA is also needed by turning KPIs into Service-Level Objectives (SLOs), which are listed in specific SLA levels [58]. Once a situation to be addressed has been identified by monitoring services, the network administrator applies policies to decide the action to be executed to mitigate, fix or prevent it [59]. The remedy can also be applied in a specific slice [58] without adding significant delays. More advanced solutions on top of ML realise SON [60].

Considering the revolution on 5G networks sustained by softwarisation and virtualisation paradigms, it is important to consider the SLA monitoring and negotiation done in cloud infrastructures. Cloud resources are on-demand charged services. There, SLAs contain negotiated and agreed QoS attributes that are used to achieve a level ground for service provision and consumption thereof. Thus, negotiations are effective means of establishing QoS attributes. Dynamic SLA negotiation and monitoring in cloud computing is still an emerging trend in public cloud deployment and efforts were and are being made for addressing SLA negotiations in service-oriented architectures. However, none of the cloud service providers has a dynamic negotiable SLA [61]. Majority of cloud service providers do not provide easily measurable QoS attributes for their services. Research works have focused on autonomic systems for monitoring SLA violations, providing tools that monitor performance and violations of cloud services. Sometimes a neutral party negotiates and monitors the SLAs between and on behalf of the service provider and the service consumer. This third party serves as a broker in this regard. Thus, the intermediary monitors relevant parameters based on its experience [62].

2.4.2 SLA Assurance Enabler for 6G Marketplaces

SLA assurance should enable the generation of multiple network slices that meet SLA requirements, guaranteeing specific performance parameters, such as low latency and high throughput, for each application. A control loop composed by several systems is needed to enable the enforcement of SLAs agreed between different providers and consumers. To achieve this, first, it is necessary to monitor the actual values from live captured metrics. Second, the constant evaluation of the conditions declared in the SLA terms and conditions to continuously assess the satisfaction and detect any infraction. Third, when necessary, an actuator on the provided infrastructure enables prevention of any potential violation or addressing of any detected breach.

SLA monitoring and violation assessment is crucial to determine whether the SLOs have been met or not. SLOs instruct penal actions to be taken in the violation of an SLA. The monitoring of metrics from the different resources provisioned is essential to capture in real time the local performance of each asset. Then, these values are aggregated into E2E metrics. The aggregated metrics can then be used to evaluate SLAs [63]. The collection of individual captured metrics, the aggregated data and the resulting E2E metrics into a data lake is fundamental for facilitating the processing of data from pipelines updated dynamically. The knowledge extraction from data located in different areas of decentralised infrastructures and within data lakes in the form of unstructured data is intricated and complex. The simplicity of a data lake model combined with reliable and efficient cloud-native computation and privacy-aware data access is the more viable option. The SLA terms and conditions usually contain formulation to ease the automated SLA composition and reasoning including penalties for violation conditions [64]. To evaluate the SLA conditions on top of data lakes there are different serverless solutions to perform stateless computations such as AWS Step Functions, Azure Durable Functions, Apache AirFlow and Apache OpenWhisk Composer [65].

Once the metrics monitoring and the aggregation of metrics is performed, the evaluation of SLAs may identify a problem. In this case, the next step is to perform a mitigation action or to trigger a countermeasure. The actuation will require to modify the provided network resources or configurations to restore functionality and performance requirements.

Network slices are deployed to continuously fulfil requirements from vertical industries. Network slicing, which requires a 5G Stand Alone (SA) CN, enables multiple virtual networks to be created within a single physical network infrastructure, where each slice is dedicated for a specific application or service. 5G SA network operators can create a slice for automated vehicles, other for IoT and another one for live video streaming. This means that a single 5G SA network can support a broad mix of UCs simultaneously, using setting tailored to the traffic demand. In terms of computing assets for virtualised infrastructures, an application processing JSON-formatted IoT messages could process all the incoming messages in a lightweight machine flavour (in terms of Central Processing Unit (CPU) and Random Access Memory (RAM)), while the same machine

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

could face bottlenecks to process image data, needing a hardware upgrade to a more muscled flavour. Thus, the management of SLAs in network slices and assets processing is fundamental. 5G aims to achieve efficiency by providing dynamic network optimisation that make a maximum use of the resources to get as much capacity and QoS as possible.

Network operators must ensure the SLA requirements for latency, bandwidth, resources availability, etc. for each network slice while utilising the limited resources efficiently, i.e., optimal resource assignment and dynamic resource scaling for each network slice. Existing resource scaling approaches can be classified into reactive and proactive types [66]. Trade-offs between assurance and efficiency are translated into operational rules managing the network slices to be scaled up and down effectively while reducing the costs of SLA violations and resource overprovisioning.

Often, the actions triggered to react or prevent SLA issues are based on allocation/release of underlying resources in order to perform scale out/in operations [66]. Authors from [67] operates experimental testbeds by automatically scaling network systems in a federated domain being able to apply changes in less than 1 minute.

The adoption of novel network automation solutions when operating networks, called zero-touch management, is a key enabler for SLA assurance. Active Networks (ANs), SON, Autonomic Network Management (ANM) and Zero-touch Network Management (ZTM) embed policies and intelligence into the network for automation and optimisation purposes [68]. These solutions can be supported by Policy-based Network Management (PBNM) applying rules, which verify conditions and apply predefined networking actions or by more advanced Intent-based Network Management (IBN) approaches, which make an abstraction of the specific and detailed setup and configurations and support the declaration of an action without specifying how to apply it.

For cross-domain management and coordination, an E2E manager is needed. To bridge local and central management systems, each network domain needs to expose and/or consume a set of endpoints including data probing/capturing services, which enable data sharing, persistence and control, which facilitates the telematic exposure of management services.

Then, to allocate and apply the configurations in the different networks' assets and network slices, the Camara Project defines APIs enabling seamless access to telco network capabilities simplifying telco network complexity. These APIs provide abstraction from network-specific interfaces, orchestration systems and controllers, as well as the availability to interact with telco networks across countries, with different distribution options, using a common and simplified service API. This abstraction layer paves the way for transforming operator networks into service enablement platforms, facilitating the application-to-network integration.

Some APIs provided by virtualised networks to manage the configuration and lifecycle of the NSs are the ones published by OSM, Cloudify and Open Network Automation Platform (ONAP) as the orchestrators to manage logically isolated networks, or the ones provided by solutions like FlexRAN and FlexRIC in order to control Software-defined Radio (SDR) assets [68]. Programmatic control of network routing can be done with OpenFlow, which provides a forwarding abstraction for packet-switched networks.

It is evident that different systems, the ones applying data processing, those identifying or forecasting an issue, the ones translating an issue into an action, and the ones

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

mapping an action into a specific modification in one or multiple network slices, would need to exchange information and status. Here, event streaming platforms like KAFKA are widely used to deliver messages to multiple systems in real time.

Once the control loop identifies situations that need an actuation to restore or enforce the SLA conditions, it is important to apply the required change in the logic or virtualised asset provided by multi-domain network infrastructures.

5G network slicing enables cellular networks to connect heterogeneous clients and services with required capacity, throughput, and latency. It opens a new marketplace opportunity for cloud providers and network operators to sell portions of their networks to address specific customer needs in 5G, B5G and 6G applications.

There are numerous open challenges for providing E2E slices in a marketplace. To provide an E2E network slice it is necessary to manage the coordination of RAN, CN, Edge Computing infrastructures and Transport Networks (TNs) operating Software-defined Network (SDN) and NFV technologies [69]. This implies the provisioning of a set of connections between a group of VNFs or/and PNFs from the RAN, the CN and the Multi-Access Edge Computing (MEC) segments. ONAP implementation of network slices employs Topology and Orchestration Specification for Cloud Applications (TOSCA) files to automate the deployment of a network slice based on VNFs [70]. Other works model E2E slices as Service Functions Chains (SFCs), in which each CN and RAN component is represented as a VNF [71]. The creation of network slices involving different network tenants is a complex operation, which requires a discovery or inventory of available assets and configurations, the mapping of logic assets and infrastructure systems, the aggregation of metrics from different networks and the augmentation service, which enables the tenant to increase or decrease allocated resources [72]. Here, some open challenges are the definition of slices' setup as a graph or a template, the normalisation of slice identifiers and the features provided, and the mapping of the topology to the different slices to allow live and soft modifications applying smooth mutations or changes. As it can be complex for network management services to adapt a specific configuration to local network setups, intent-based brokers can be used to translate actions into different administrative networks [73].

Virtualisation infrastructures, such as MEC infrastructures, offer application developers and service providers cloud-computing capabilities and an Information Technology (IT) service environment at the edge of mobile networks. Provisioning and scalability for fast resource provisioning times in multi-operator environments is crucial. A key problem in edge computing is the optimal placement of computational units (virtual machines, containers, tasks, or functions) of novel distributed applications. These components are deployed to a geographically distributed virtualised infrastructure and heterogeneous networking technologies are invoked to connect them while respecting quality requirements [74].

Often the literature covers single-operator scenarios, where resources are owned and managed by a single provider. The more complex and more challenging multi-operator setups are also studied and addressed [75]. Simulations such as [76] focus on provisioning and placement optimisation. Others [77] try to make a smart choice based on intelligent prediction, which reduces the bandwidth consumption of edge services and minimises the cost of edge service providers. In this context, the blockchain technology is key to create a framework for robust, flexible, and credible SLA enforcement [78].

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Another key aspect to address is the cost and price sharing. To determine resource pricing and allocation, the work in [79] envisions two innovative market mechanisms. First, it assumes pre-assigned fixed sharing rates of infrastructure, and it relies on a trading post mechanism to allocate the resource. This mechanism redistributes budgets in bids and customises their allocations to maximise profits. Second approach includes no bound on their sharing quota. The work provides simulations to analyse the market mechanism's economic properties and the convergence rates of the algorithms.

Kaputa brings a blockchain-enabled network slice broker and Non-Fungible Token (NFT)-enabled network slice marketplace [80]. Here, different stakeholders such as cloud providers, network operators, RAN providers, and TN providers can rent their resources. It orchestrates the network slices according to blockchain smart contracts. The orchestrated network slices are encoded as NFT tokens and published in the Kaputa NFT marketplace. Customers can purchase the network slices from the marketplace based on their 5G application requirements via paying crypto/fiat currency. The revenue is distributed among different providers. Consequently, Blockchain has become a core technology to support 5G/6G network marketplace for trading network resources [1][50].

2.4.3 Standardisation and Specification Aspects

SLA management in an environment with multiple administrative and technology domains, where different actors and stakeholders are interconnected, is essential to build a reliable 6G marketplace.

The orchestration of available resources in mobile networks is usually associated to policies and mechanisms to deliver logic and virtualised network slices over a common physical network infrastructure. Thus, network slicing is the technological solution from MNOs to provide SLA levels over customised networks to customers needing the coordination of the accumulated traffic over the idle/available resources. The intrinsic relationship between slicing and SLAs in the mobile networks drives the understanding of roles and actors in SLA management towards the documents released by standardisation and industrial bodies in terms of network slicing and SLA.

Regarding the standards, there are different SDOs which drive 5G and 6G specifications and could define UCs, interfaces to slice orchestration, SLA specifications and multi-tenant requirements. A network slice is a logically isolated network over multi-domain, multi-technology physical networks that provides resources. Network slicing is an ongoing standardisation work performed by different SDOs targeting each a specific part of the network slicing architecture. Most relevant initiatives and outgoing specifications for SLA and slicing technology in mobile networks are listed hereafter.

Concerning the network slice lifecycle, the 3GPP specification considers 4 phases: a) preparation phase, including design and pre-provisioning; b) instantiation, configuration, and activation phase; c) a run-time phase including supervision and reporting; as well as upgrade, reconfiguration and scaling, and d) a decommissioning phase.

Declaration models of network slices are not yet closed. Models describe all the network slice management entities as well as their relationships from the perspective of operators and service providers. This is even more complex when considering multiple networks needing to stitch together the different subnet models from RAN, CN and TN segments.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

In this realm, the Global System for Mobile Communications (GSMA) is investigating network slice characteristics, from vertical industries and gathering them in a template called Generic Slice Template (GST). The goal is to help both the Network Slice Customer (NSC) and Network Slice Provider (NSP) to identify a suitable network slice. The GST will be used as a reference by vendors, operators, providers, and customers in order to browse from available items. GSMA approach has several advantages over Standardised Slice Types (SSTs) as it allows operators and providers to define custom UC requirements beyond Enhanced Mobile Broadband (eMBB) (1), Ultra-Reliable Low Latency Communications (URLLC) (2) and Massive IoT (mIoT) (3) SST values.

RAN and CN slicing are still under standardisation by 3GPP. Several working groups particularly SA1 (Service Requirements), SA2 (Architecture), SA3 (Security), SA5 (Network Management) are studying different aspects. The 3GPP network slice information model has been defined by the SA5 group specifying the entities that compose a network slice and the way they interact with each other using the information model [81]. However, the entities NS, VNF and PNF are out of the scope of 3GPP working groups. Thus, their descriptions are delegated to ETSI. There, Network Slice Subnet Instances (NSSIs) are separated units associated to a Network Slice Instance (NSI). They can also be used (shared) simultaneously by another NSI if needed. Moreover, the NSInfo attribute provides real-time information of a NSI that corresponds to a NSSI. This attribute contains many information such as the reference to the flavour of the Network Service Descriptor (NSD) used to instantiate the NS and the reference to all information on NS's constituents VNFs and PNFs [82].

In terms of the network topology description this is an open area with different solutions from IETF Traffic Engineering Architecture and Signalling (TEAS) workgroup such as its Abstraction and Control of Traffic Engineered Networks (ACTN), including 3 controllers: the Customer Network Controller (CNC), the Multi-Domain Service Coordinator (MDSC) and the Provisioning Network Controller (PNC) [83], or the Common Operation and Management on network Slices (COMS) data model for technology-independent management of NSs [84].

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO
DE ESPAÑA
Plan de Recuperación,
Transformación
y Resiliencia

3 Use Case: Multi-party Real-time Holographic Communications

In this section, we present a UC that exemplifies the application and significance of the technologies employed in the 6GENABLERS-DLT project. The UC revolves around the establishment of multi-party real-time holographic communications, a compelling scenario that showcases the potential of the 6GENABLERS Marketplace.

Multi-party real-time holographic communications refers to a collaborative communication environment where multiple participants engage in interactive and immersive holographic interactions in real-time. This UC involves the seamless integration of advanced technologies, such as holography, high-speed networks, and intelligent systems, to enable lifelike communication experiences that transcend physical boundaries.

In the context of multi-party real-time holographic communications, **DLT** can play a crucial role in establishing trust, security, and accountability among the involved parties. By utilising DLT, the communication sessions, metadata, and transaction records can be securely stored and immutably recorded.

Smart Contracts can automate and enforce the predefined rules and conditions governing multi-party real-time holographic communications. In this context, Smart Contracts act as digital agreements that ensure seamless and reliable interaction among participants.

Smart Discovery mechanisms contribute to the efficient and intelligent selection of resources and services offered within the marketplace to further boost multi-party real-time holographic communications. This solution aims an accurate matching of participants' requirements with available offers, enhancing the user experience through intelligent service recommendations.

SLA plays a vital role in ensuring the quality, reliability, and performance of multi-party real-time holographic communications. In addition to the clear definition of service levels and performance metrics, the introduction of an SLA assurance system will allow the enforcement of agreed-upon quality standards.

This section will first provide an overall description of the global UC, and then define UC scenarios particularly relevant for each one the associated technologies (i.e., DLT, Smart Contracts, Smart Discovery, and SLA assurance) as building blocks of the 6GENABLERS-DLT project. By considering these UC scenarios and their associated technologies, we can appreciate the value and impact of the 6GENABLERS-DLT project in revolutionising multi-party real-time holographic communications.

The subsequent subsections will delve deeper into the potential of these technologies for the implementation of the 6GENABLERS Marketplace to foster multi-party real-time holographic communications, outlining their specific roles and interactions within the project framework. For each technology-driven scenario, we will identify the actors and roles and the main benefits provided by the corresponding technology.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

3.1 Use Case Description

XR services need to ensure ethics, privacy, security and safety to achieve a broader adoption and gain the trust of users, while providing satisfactory SLAs, to avoid social, economic and legal implications. In this context, Metaverse-like services, including multi-party holographic communications, will potentially become a powerful medium to hold realistic, natural, and trustworthy meetings between remote users in a variety of entertainment and professional scopes [85].

In 6GENABLERS-DLT, a worldwide pioneering modular platform to enable multi-party real-time holographic communications between remote users, called HoloMIT [86][87] will be adopted as a key UC. This is a disruptive technology to enable human-cyber-physical services, which will very likely become the next-generation social interaction and collaboration medium, with high impact in a variety of verticals (entertainment, culture, training, virtual tourism, meetings, eHealth…).

Unlike most of the existing multi-user XR platforms that rely on the use of synthetic avatars, HoloMIT provides realistic volumetric user self and others' representations, captured in real-time, which contributes to the trustworthiness of the communications and a robust identity management. Likewise, unlike the few available volumetric video capture systems, HoloMIT makes use of lightweight and low-cost off-the-shelf capture sensors and has been built based on standard-compliant technologies and formats, which contributes to interoperability and reliability.

Figure 3-1 shows examples of scenarios and applications supported by HoloMIT, like four users within a shared XR environment, with some of them having full 3D Point Cloud (i.e., holographic) representations and other having more limited (2D-video avatar) representations, two holographic user tele-ported into a virtual museum, and two holographic users having a virtual meeting.

Figure 3-1. Envisioned Metaverse-like services with holographic comms [86][87]

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

On the one hand, XR and Metaverse-like services still encounter many barriers and challenges regarding security, privacy, ethics and trustworthiness. On the other hand, next-generation XR services, like HoloMIT, are subject to evolve toward modularisation, virtualisation and exploiting the capabilities of smart network and orchestration strategies, including the virtualisation and instantiation of virtualised network/media functions over the Cloud Continuum (see envisioned architecture in Figure 3-2). This is meant to improve the adaptability, scalability, and interoperability of the targeted services, but also brings extra challenges in terms of trustworthiness, security, privacy and reliability, especially when considering open, ubiquitous and cross-domain deployments.

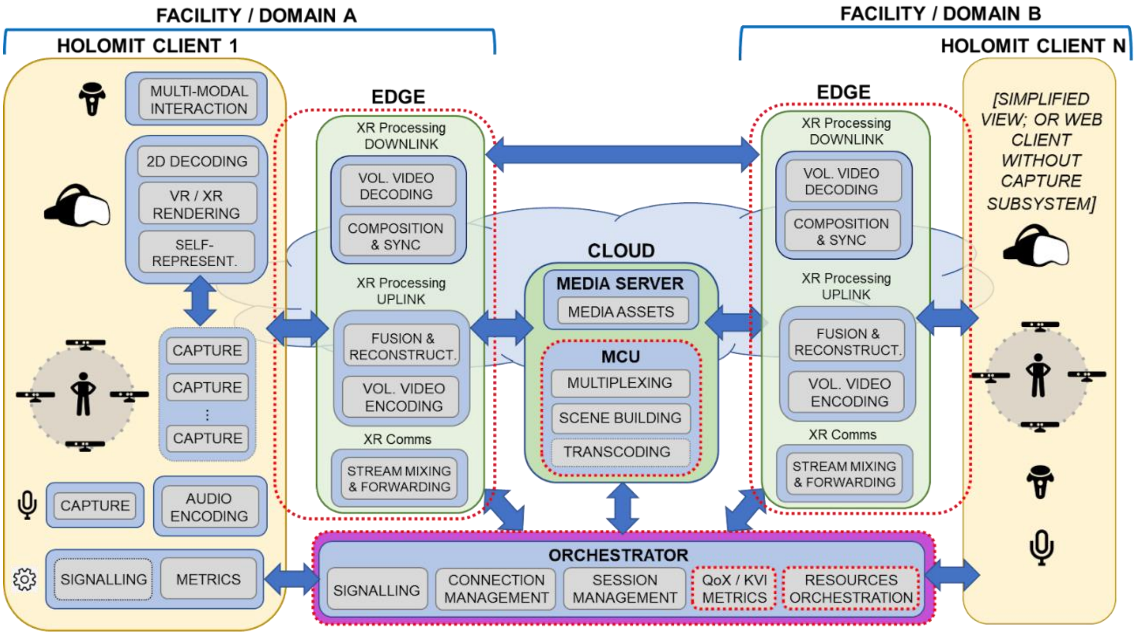

Figure 3-2. Evolution roadmap of HoloMIT and its relevance to 6GENABLERS-DLT

Under this umbrella, 6GENABLERS-DLT aims to assess potential requirements and associated solutions to overcome the identified barriers. Examples include reliable and trustworthy distribution of application artifacts and service slots, as well as network and Cloud Continuum resources; registration of users and service slots, interfacing cloud-based servers; requesting the use of trusted Edge processing resources, etc.

Through a DLT-anchored Smart Marketplace, distributed and heterogeneous resources can be offered, reserved, and consumed in order to deploy cross-domain holographic comm services, instantiating the required XR, network and infrastructure resources. Unleashed by a secure collaboration between multiple network operators and infrastructure providers, trusted edge resources closer to the final users could become available on-demand to the service provider in an automated and transparent way via the introduction of Smart Contracts, expediting the negotiation process, while also providing satisfactory SLAs levels (e.g., in terms of latency), without impacting the Total Cost of Ownership (TCO). Likewise, a variety of related VNFs (such as client and edge processing apps, stream forwarding entities, etc.) can be exposed, discovered, and traded over the Marketplace in order to further enable interoperability and foster novel business models between VNF vendors and service providers. Additionally, performed transactions are subject to SLA terms, which are tracked and monitored allowing resource and service providers to promptly react to potential degradations while ensuring the shareholders' access and verification of immutable records. These are all potential UC scenarios and requirements to be addressed in 6GENABLERS-DLT.

3.2 Definition of Actors and Roles

In the context of the multi-party real-time holographic communications UC, various actors and roles play essential parts in enabling immersive communication experiences, while contributing to the seamless integration and efficient management of resources and services exposed over the Marketplace. Understanding the responsibilities and contributions of each actor is crucial for effectively implementing and orchestrating this innovative communication scenario.

Let's examine the key actors and their roles. Each actor below has one or more roles based on their contribution and interest in the overall system.

1. **Vertical Service Providers (VSPs):** This actor serves as the central entity responsible for delivering the holo-comm services, corresponding to the service provider in a B2C transaction. Their role extends to leveraging the 6GENABLERS Marketplace to acquire and utilise distributed resources and services (such as computing resources, network connectivity, storage capabilities, and VNFs) that are essential for the establishment of ubiquitous and sustainable real-time holographic communication sessions. Given its crucial role in the UC, sample interactions with other actors follow:
    a. VSP may have agreements with the Network Operators for the deployment of holo-comm services inside the operators' domain.
    b. VSP may have agreements with the Infrastructure Providers to acquire available edge computing resources and storage capabilities.
    c. VSP may acquire VNFs from application vendors or create their own to compose NSs that can be then offered on the Marketplace.
2. **Network operators**: This actor corresponds to the MNO, and also can be referred to as CSPs. Network operators play a crucial role in ensuring reliable and high-quality connectivity for multi-party holographic communications. They provide the underlying network infrastructure, including 5G or future-generation networks (B5G and 6G), where vertical services are installed and exposed (although parts of it may be additionally provided by third-party infrastructure providers). Their responsibilities include managing network resources, optimising network performance, and ensuring reliable communication links. With the integration of the 6GENABLERS Marketplace, they may engage in the marketplace as participants, offering their network infrastructure resources and services. This enables VSPs to access and leverage their networks to ensure low-latency and high-bandwidth holographic communication experiences.
3. **Infrastructure Providers**: Infrastructure providers are responsible for offering infrastructure resources (additional to the ones offered by the Network Operators) to facilitate real-time data transmission with low latency and high bandwidth. This includes providing edge computing resources, network connectivity, and storage capabilities required for processing and transmitting holographic data in real-time. These actors contribute to the Marketplace by offering for instance their edge computing resources, with Graphics Processing Unit (GPU), CPU, and storage capabilities, for utilisation in holographic communication scenarios.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

4. **Vertical Service Vendors (VSVs):** This actor corresponds to the application provider in a B2B transaction. Application vendors play a vital role in creating VNFs that leverage the capabilities of multi-party holographic communications. They may design and develop user interfaces, collaboration tools, and content sharing applications specifically tailored for holographic communication environments. Through the 6GENABLERS Marketplace, VSVs engage in transactions with VSPs, unleashing new business models around the trading of developed VNFs.
5. **Vertical Service Consumers (VSCs):** This actor represents entities who participate in the multi-party real-time holo-comm sessions, acting as final customers of the application provided by the VSPs. They engage in interactive and immersive communication experiences through holographic displays and interfaces. Their role involves initiating and participating in holographic calls, collaborating with other participants, and leveraging the capabilities of the holographic communication platform. Within the marketplace, they engage in B2C transactions with the VSP, being the beneficiary of such contract.
6. **Governance Board**: Team conformed by admin stakeholders and regulators, which shall oversee the operation and management of the 6GENABLERS Marketplace. They ensure the marketplace's stability, integrity, and functionality, including maintaining the blockchain network, voting on the onboarding of new members, validating transactions, resolving disputes, and enforcing Marketplace policies. The Marketplace Governance Board facilitates the smooth functioning of the Marketplace ecosystem and support the interactions among the various actors. The Governance Board is formed by at least one Marketplace Admin. Note that any actor can also have the role of Marketplace Admin, which has rights to take decisions on the Governance Board, like for example, to approve or reject new members into the Marketplace.

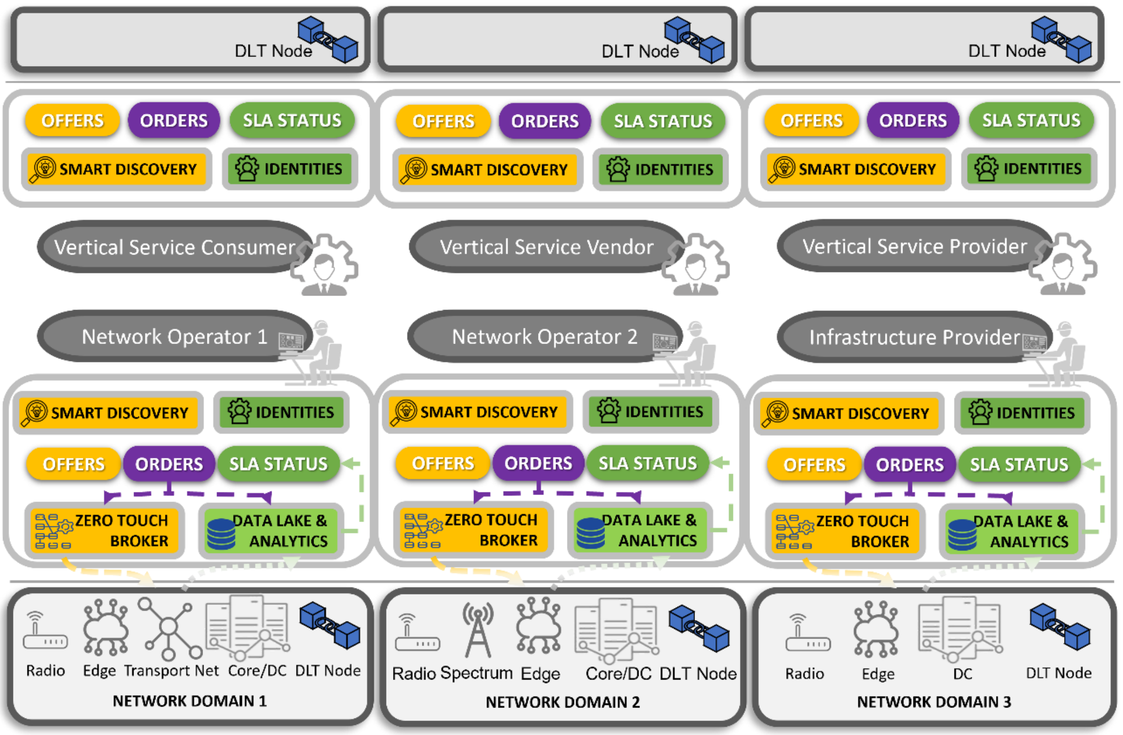

Figure 3-3. Actors in the 6GENABLERS Marketplace

All the aforementioned actors must be registered in the DLT network to participate in the different transactions and to be able to see and audit them. Each one shall be assigned unique identities and access control rights. The Marketplace governance is responsible to ensure that all the actors are allocated unique access rights that match their needs. The different actors considered in this project are illustrated in Figure 3-3.

In Figure 3-3, we can see at the bottom the Network Operators and Infrastructure Providers owning the network assets and operating them. Overall, each stakeholder needs to deploy an instance of the decentralised Marketplace platform and a DLT node in order to join the 6GENABLERS Marketplace. This setup can be deployed over private virtualised resources of the owned infrastructure or on top of a public cloud. In any case, this decentralised platform hosts the Marketplace elements including offers from Network Operators, Infrastructure Providers, VSPs and VSV; orders from VSP and VSC; and a register of the SLAs for active orders. Stakeholders managing the network and infrastructure resources and owning VNFs and NSs advertise their available telco assets through offers of the Marketplace, deciding the price and declaring the QoS. Then, stakeholders acting as consumers are performing orders convenient to their traffic needs, users' location, and acceptable costs.

Additionally, the network infrastructure needs to provide access to the endpoints of the local monitoring and control systems, which are made accessible to the Marketplace analytics and brokerage systems. To this end, network operators need to make required configurations to inter-connect network domains and controllers. When a new order, an update or a termination is triggered, the local broker performs individual requests to the corresponding network controllers in order to provision the contracted E2E network slice and agreed SLA. The platform features proactive monitoring that track the SLAs associated with the active orders requested by consumers. In this regard, a data lake captures individual metrics of the deployed network slices and aggregates metrics related to the SLA terms. When a violation is identified from the conditions declared in the SLA, involved providers and consumers are notified and further actions can be taken as defined in the contract.

In addition to the previously mentioned stakeholders, which are particularly relevant to the considered UC, additional actors and roles can be illustrated in the Marketplace ecosystem. Let's explore the expanded list of actors and their roles:

1. Regulator Authority: As the entity responsible for ensuring compliance with regulatory requirements, this actor holds the authority to oversee transactions involving licensed radio spectrum within the Marketplace. As a member of the Governance Board, the Regulator Authority actively monitors and regulates the use of communication resources associated with licensed spectrum, to ensure fair and lawful operations.
2. Device Manufacturers: Device manufacturers design and produce the hardware components, devices, and peripherals that enable end-users to participate in holographic communication sessions. They design and manufacture holographic displays, cameras, sensors, and other essential equipment needed to capture, render, and display holographic content. With the integration of the 6GENABLERS Marketplace, device manufacturers can collaborate and integrate their devices with the Marketplace ecosystem. This would allow for seamless

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

interoperability and compatibility between manufacturers and VSPs, ensuring VSCs can access and utilise holographic communication services using their preferred devices.

3. Smart Contract Developers: Smart contract developers are responsible for designing and implementing the smart contracts that govern the interactions and transactions within the 6GENABLERS Marketplace. They define the rules, conditions, and processes that regulate resource discovery, negotiation, and consumption. Smart Contracts enable automated and secure execution of agreements between VSPs, network operators, infrastructure providers, and other marketplace participants.
4. Blockchain/DLT Providers: The appearance of the 6GENABLERS Marketplace could introduce the role of blockchain/DLT providers. These providers offer the underlying blockchain infrastructure, ensuring the security, transparency, and immutability of transactions and interactions within the marketplace. They contribute to the development and maintenance of the blockchain/DLT network that powers the marketplace, facilitating trust, and enabling efficient resource allocation and service provisioning.

Once, the actors and roles have been described, it is important to design how money flows run to understand the established relations and commitments supporting the Marketplace. Table 3-1 summarises an initial vision on the business relations among the actors including their role.

Table 3-1. Summary of roles, actors and general business flows

Actor	Role	Business Flow
Vertical Service Providers	• Order different network assets from one or several network operators to provide connectivity to their services. • Order different infrastructure resources from one or several Infrastructure Providers to host their services. • Order different VNF resources from one or several VSVs to conform their NS offers. • Offer NS to VSCs.	• Establish price for offered assets. • Get money from consumers (VSC). • Pay applicable price as agreed in the ordered asset. • Pay-as-it-goes for selected assets.
Network Operators	• Own and operate network resources that they make available on the Marketplace. • Order different infrastructure resources from one or several Infrastructure Providers to extend their network footprint.	• Establish price for offered assets. • Get money from consumers (VSP). • Pay applicable price as agreed in the ordered asset. • Pay-as-it-goes for selected assets.
Infrastructure Providers	• Own infrastructure resources that they make available on the Marketplace.	• Establish price for offered assets. • Get money from consumers (VSP, Network Operator).
Vertical Service Vendors	• Own VNF resources that they make available on the Marketplace.	• Establish price for offered assets. • Get money from consumers (VSP).
Vertical Service Consumers	• Order different NSs from one or several VSPs to consume offered services.	• Pay applicable price as agreed in the ordered asset. • Pay-as-it-goes for selected assets.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Similarly, Table 3-2 summarises an initial vision on the relations among the actors in terms of SLA and monitoring of deployed services.

Table 3-2. Summary of roles, actors and general SLA assurance flows

Actor	Role	SLA assurance flow
Vertical Service Providers	• Order different network assets from one or several network operators to provide connectivity to their services. • Order different infrastructure resources from one or several Infrastructure Providers to host their services. • Order different VNF resources from one or several VSVs to conform their NS offers. • Offer NS to VSCs.	• Establish SLA for offered services. • Reputation penalty for SLA violations. • Negotiate and sign SLA contract. • Negotiate reactions to SLA breaches and receive compensations. • Subscribe to notifications on related SLA violations.
Network Operators	• Own and operate network resources that they make available on the Marketplace. • Order different infrastructure resources from one or several Infrastructure Providers to extend their network footprint.	• Establish SLA for offered assets. • Allocate, manage, and release network slices on demand. • Interconnect local monitoring and controllers with platform's analytics and zero-touch broker systems. • Proactively monitor active SLAs. • Produce monitoring metrics and publish them to the data lake. • Aggregates network slices metrics into E2E KPIs to assess the SLA. • Broadcast SLA violations to involved parties. • Reputation penalty for SLA violations.
Infrastructure Providers	• Own infrastructure resources that they make available on the Marketplace.	• Establish SLA for offered assets. • Allocate, manage, and release infrastructure assets on demand. • Interconnect local monitoring and controllers with platform's analytics and zero-touch broker systems. • Proactively monitor active SLAs. • Produce monitoring metrics and publish them to the data lake. • Broadcast SLA violations to involved parties. • Reputation penalty for SLA violations.
Vertical Service Vendors	• Own VNF resources that they make available on the Marketplace.	• Establish SLA for offered assets. • Reputation penalty for SLA violations.
Vertical Service Consumers	• Order different NSs from one or several VSPs to consume offered services.	• Negotiate and sign SLA contract. • Negotiate reactions to SLA breaches and receive compensations. • Subscribe to notifications on related SLA violations.

3.3 Use Case Scenarios

In the context of the considered UC, oriented towards multi-party real-time holographic communications, different scenarios are defined to showcase the potentialities of the

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

6GENABLERS Marketplace to further enable the adoption and spread of such innovative applications as envisioned by 6G.

The selected UC contains a wide range of components and services required to realise the application. Even more challenging, the platform is modular and distributed across the continuum in at least 3 target infrastructures according to their compute and network requirements among other criteria: client, edge and cloud. Thanks to the privilege location of the telco infrastructure, which offers the closest possible communication path to the client when connected through the mobile network, the edge side of the HoloMIT platform is a suitable UC to participate in the decentralised 6GENABLERS Marketplace. Potential extensions of the telco support could apply to components from the client side if extreme edge infrastructure was made available to the telco domain and even parts of the cloud side could be further separated between central public cloud applications and per-CSP private telco cloud applications.

Additional benefits that could be part of a UC such as this one, could be the purchase of specific network slices tailored to the HoloMIT services. Slices have been introduced in 5G to provide service flexibility and ability to deliver communications faster with high security, isolation, and applicable characteristics to meet the contracted SLAs within the telco domain [88].

3.3.1 Distributed Ledger Technologies

Figure 3-4 shows an XR Holoportation (i.e., holographic tele-transportation) service requiring for connectivity assets in two network domains and including a contracted SLA. In the case of infraction, it is registered, including the IDs of all the involved participants and items. This is possible thanks to a distributed interconnection setup. As a decentralised Marketplace each network operator has their own instance of the full platform as well as the customer willing to make an order, which makes it able to use any of the supported Marketplace services.

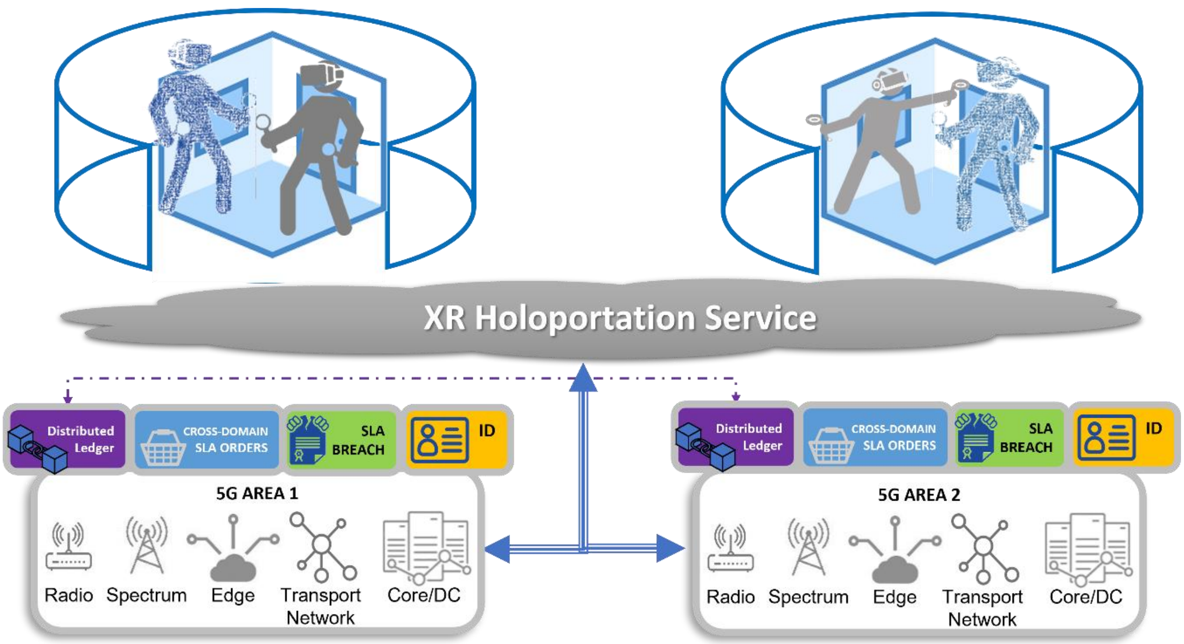

Figure 3-4. 6GENABLERS Marketplace scenario

Being a fundamental system of the 6GENABLERS Marketplace, the scenario covered in this section sets the ground for the functioning of the Marketplace in terms of required capabilities for the exposure, trading and tracking of advertised telco assets. In particular, this scenario contemplates from the onboarding of a new trader member, the creation of offers and orders, till the notification of an SLA breach. Given its broad scope, this scenario is further divided into the following five main operations, which are further detailed next:

1. Get an identification from the marketplace interface with associated permissions.
2. Use the marketplace interface to create, store and publish an offer.
3. Use the marketplace interface to declare requirements, select assets, locations, negotiate SLAs and agree on a price to register, store and share an order, which could comprise one or several networks and administrative domains.
4. Report to the marketplace interface an SLA violation of an active order including the network origin of the violation when several networks are involved in the order.
5. Use the marketplace interface to get awareness of violated order and the affected network.

Accordingly, next tables compile the details of each operation and what they imply for the scenario setup where the UC is executed.

Table 3-3. Onboarding of a new stakeholder that joins the platform

Name	**Get onboarded to the platform as trader (provider or consumer)**
Description	Get ID to access the platform, get permissions to add/update offers and orders from the DLT-based distributed ID service.
Actors	Network Operator willing to become a new stakeholder of the marketplace, Marketplace Admins (Governance Board)
Pre-conditions	• The marketplace has been initialised and Governance administrators' peers exist with ability to grant all permissions to new parties joining the network. • The Network Operator knows the marketplace APIs endpoint to obtain the ID and credentials according to the requested permissions. • The Network Operator gets the instructions and automation scripts to deploy an instance of the Marketplace platform, a DLT node and VPN agents to interconnect network infrastructure with other peers of the decentralised Marketplace. • The Network Operator deploys a cluster in the private/public cloud virtualisation infrastructure to install an instance of the Marketplace platform using the provided instructions. • The Network Operator deploys a container in the private/public cloud virtualisation infrastructure to install a DLT node client using the provided instructions. • The Network Operator deploys a container in the private/public cloud virtualisation infrastructure to install a VPN client using the provided instructions. • The Network Operator knows the local endpoints and credentials to access and connect to the monitoring and controller systems.
Sequence Workflow	1. The Network Operator submits a request to join the network. 2. The Governance Board (Marketplace Admins) handles the onboarding request based on an approval mechanism, resulting in its approval/rejection. 3. If approved, the Marketplace Admins answer to the network operator with the ID and credentials to be used in all the operations on the decentralised Marketplace.
Post-conditions	• The Network Operator can begin advertising/consuming telco assets based on their assigned roles & permissions.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Alternatives	Some other stakeholders, according to their roles, will not need to perform the inter-connection of the monitoring and controller systems.
DLT enabler	The DLT technology provides a Distributed ID including the permissions to interact with the Marketplace services.

Table 3-4. Network offer creation

Name	**Create a network offer**
Description	Make network assets available on the Marketplace
Actors	Network Operator
Pre-conditions	• A network operator manages idle network resources including radio/base station, core and edge resources. • The network operator identifies the idle resources and locations. • The network operator assesses the nominal QoS metrics for different set of assets and configuration profiles. • The network operator gets the prices for the different assets, individual/grouped, and based on QoS levels and configuration profiles. • The network operator knows the marketplace APIs endpoint of its local instance and has an ID and permissions for trading, obtained from the marketplace governance.
Sequence Workflow	1. The network operator asks to the local marketplace APIs to register different network offers using its network operator ID and providing assets, possible configurations, location areas, the QoS metrics building an SLA for each offer and the applicable price. 2. The marketplace answers to the network operator the success message and an offer ID for the network offer in the case it has been properly registered, or an error if something fails. 3. The offers get disseminated to all the parties of the Marketplace.
Post-conditions	• The local discovery service instance of the decentralised marketplace parses the generated offers and classifies them based on pre-computed clusters.
Alternatives	Update available assets, if not allocated in an order, referring to the original ID provided to an offer.
DLT enabler	• Storage of information, offers in this case, automatically and instantly synchronised in all actors in the marketplace according to the permissions associated to their DID.

Table 3-5. Network order creation

Name	**Create a network order**
Description	Acquire telco assets (network or infrastructure resources, VNFs, NSs) from the marketplace
Actors	VSP, Network Operators
Scenarios	• A VSP needs a temporal or permanent network deployment for users/subscribers in a specific area and requesting a certain QoS.
Pre-conditions	• The VSP identifies locations areas where to deploy a network infrastructure to provide connectivity to its users/subscribers. • The VSP decides the required QoS to provide to its subscribers. • The VSP assesses the suitable cost to provide connectivity to its subscribers. • The VSP knows the marketplace APIs endpoint of its local instance and has an ID and permissions for trading, obtained from the marketplace governance.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Sequence Workflow	1. The VSP asks to the marketplace API for high-level and technical required offers criteria including locations, computing capacity and QoS. 2. The marketplace answers to the VSP the available possibilities and the applicable prices. 3. The VSP asks to the marketplace API to register a network order potentially covering different offers including the configurations, location areas, SLA in terms of QoS metrics and the price. 4. The marketplace answers to the VSP, with an ID for the network order, in the case it has been properly registered, or an error if something fails.
Post-conditions	• The network operators involved in the VSP order, deploy and interconnect the associated telco assets, resulting in a functional network slice to provide connectivity to users/subscribers. • The marketplace provides to VSP the detailed configuration of the deployed slice in order to proceed with the deployment of the VSP's NS in the allocated compute resources.
Alternatives	Not applicable
DLT enabler	• Storage of information, order in this case, implying different actors in the marketplace, which are notified and can explicitly agree updating it according to the permissions associated to their DID.

Table 3-6. SLA violation registration

Name	**Register an SLA violation**
Description	Disclosure of the SLA breach violating an active contract.
Actors	Network Operators, subscribed systems of the Marketplace
Pre-conditions	• The traffic delivered by a network slice in a network infrastructure or different networks involved in an order does not achieve the SLA metrics contracted in the SLA and accordingly it is registered to provide awareness to all the actors involved. • At the Network Operator domain, the local proactive SLA monitor system is parsing all the active orders in which assets from the local network are involved and retrieving associated monitoring metrics. • From the captured metrics, the local proactive SLA monitor identifies underperforming conditions in a specific network slice ID linked to an active smart contract of an order applicable to the local network. • The issue is raised to the data bus using a specific message format in a specific topic. • The marketplace system controlling the lifecycle of orders at the Network Operator domain is subscribed to the data bus topics regarding SLA issues.
Sequence Workflow	1. The local marketplace system controlling the lifecycle of orders receives a message declaring an SLA breach to an active order ID. 2. This system performs the registration of a ledger record indicating the SLA breach associated to the Smart Contract of an order.
Post-conditions	• The local marketplace system controlling the lifecycle of orders actively listens any update on the SLA breach regarding its resolution, but the SLA breach history will be kept.
Alternatives	Not applicable
DLT enabler	• Register of information, infraction of an SLA of an active order in this case, visible to the involved actors in the marketplace according to the permissions associated to their DIDs which cannot repudiate the recorded issue.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Table 3-7. SLA violation notification

Name	Notifying an SLA violation
Description	Notification of the SLA breach violating an active contract to Smart Contract participants.
Actors	VSP, Network Operators
Pre-conditions	• The traffic delivered by a network slice in a network infrastructure or different networks involved in an order does not achieve the QoS contracted in the SLA and accordingly it is registered to provide awareness to all the actors involved. • The SLA breach has been committed to the ledger from the Network Operator domain.
Sequence Workflow	1. The local marketplace system controlling the lifecycle of orders at the VSP domain gets aware of the SLA breach, which has been disseminated through the DLT to all the involved parties.
Post-conditions	• The Network Operator performs required actions to restore the expected QoS as agreed in the SLA, which can turn into new potential transactions. • The VSP keeps actively monitoring any update on the SLA breach to detect whether it is solved, but the SLA breach history will be kept in the ledger.
Alternatives	According to the terms reflected in the SLA, the violation of the contract can lead to different consequences, including a grace period for the restoration of the agreed QoS or the compensation to the contract beneficiary, the VSP in this case.
DLT enabler	• Register of information, restored SLA of an order in this case, visible to all actors in the marketplace according to the permissions associated to their DID which cannot repudiate the recorded issue

3.3.1.1 Main benefits provided by DLTs

The benefits of using this technology in conjunction with communication networks are evident to store intelligent contracts in a distributed, synchronised, and integral way between different actors involved in a way that links:

- the sharing of mobile communication infrastructures such as the CN functions, distributing installation and maintenance costs while isolating the different flows of each operator in slices,
- the commitment to offer the QoS in a transparent way, connecting different networks with a minimum performance,
- migration between networks (“Roaming”) allowed for network users enabling access to a network in conditions of loss of coverage,
- the radioelectric spectrum quotas allocated to different operators that share infrastructures such as antennas and base stations, encouraging their sharing, either punctually or permanently, and opening the door to new players that operate the infrastructures and lease their use to radio operators.

3.3.2 Smart Contracts

In the context of SCs, the proposed scenario will focus on the HoloMIT media services running in the edge, as they will serve as example to be later expanded to the aforementioned future opportunities without any major practical difference. In fact, media services are common UCs in the telco domain [89] as they rely heavily on good and predictable network performance and often requires of similar chains of services to boost the user’s perceived quality, particularly when real-time transmission and intense traffic

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

is added to the picture. Thus, it is reasonable to assume that a 6G marketplace for telcos will already have available reusable and reliable media services virtualised in the form of Any Network Functions (xNFs) for VSPs to leverage.

The telecom sector continues to transition from the standard purchase of NSs packaged in a service-specific hardware to a model based on the acquisition of the software of the NS and then its delivery in a general-purpose virtualised hardware. Interoperability workshops and testing events such as the ETSI Plugtest denote a growing industry with interest in this digital ecosystem, forty-nine companies coming from a variety of ETSI NFV market segments participated in 2020 [90]. The remaining content of this section is particularised to the typical business plans for the VSV, VSP and VSC actors of the UC scenario proposed for 6GENABLERS-DLT (see Section 3.2).

It is expected that the delivery strategy of the selected service will be based on the ETSI NFV-MANO framework. Aligned with the trends in the continuum, the offered virtualised infrastructure by the telcos will be based on a cloud-native environment. For simplicity, the application is expected to be delivered as a single Containerised Network Function (CNF) although everything will be designed keeping in mind the scalability and a variety of more complex scenarios.

From the Marketplace and the SC perspective, two sequential transactions are envisioned to take place for the application to be accessible to the final VSC. Figure 3-5 shows an initial transaction between the VSV and the VSP in a B2B model, which will enable its exposure to the VSCs. In this transaction, the VSV is the SC owner towards the VSP and shall act as license data usage supplier for its validation, whereas the VSP is the beneficiary of the contract with the VSV.

Then, once purchased by the VSP and gained the right to use it under certain terms, the VSP will create its own offerings to the VSCs with conditions and pricing suitable for a B2C transaction. In order to customise the selected VNF to the VSC needs and to expose it correctly to the rest of the vertical application, the VSP will compose a NS that is instantiable in the telco domain. In this transaction, the VSP is the SC owner towards the VSC and shall act as license data usage supplier for its validation, whereas the VSC is the beneficiary of the contract with the VSP.

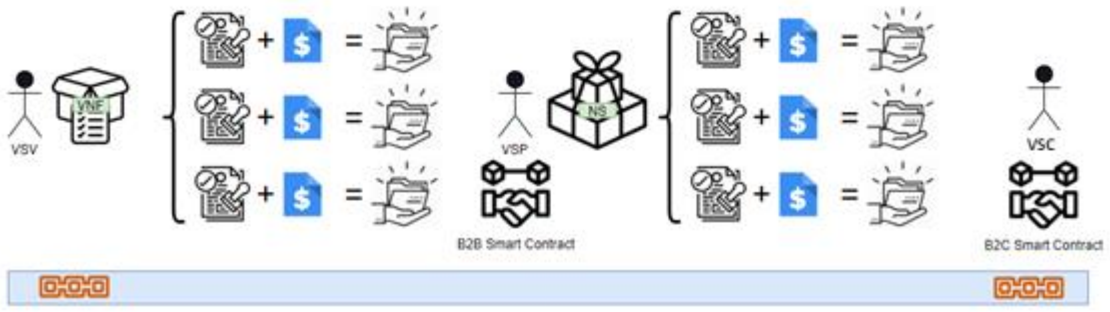

Figure 3-5. Smart Contract transactions for UC

Figure 3-5 shows a scenario in which a telco service (VNF or NS) is attached to multiple offers that the buyer can choose from. As software services, their customisation and control over used functionalities is not only feasible but a common practice. Consequently, it is possible for sellers to tailor a pricing mechanism for different types of

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

buyers and thus increase their chances of being selected when competing in the marketplace.

Next, a series of software licensing and pricing models are presented in Table 3-8 and Table 3-9, respectively, which will be used to describe the final SC states for the B2B and B2C transactions during the implementation phase.

Table 3-8. Software license models [91][92]

Name	Acquisition Type	Description	Target Transaction
Perpetual	In full	It is the most traditional model in which the buyers pay upfront for the right to use it for ever and is responsible to install and host it. It is usually bought together with a maintenance service.	B2B
Open-Source (OS)	In full	It is common to acquire OS software in a wide range of license models depending on the permissions, conditions, and limitations. The buyer is responsible to install and host it. Seller does not receive payment but does not provide liability nor warranty and often requires exposing its trademark to the final product.	B2B
Recurring	Rental	The software is purchased in full for a period of time. The buyer is responsible to install and host it.	B2B
As a Service	Rental	The buyer buys the right to use the software for a period of time, but it is maintained and hosted by the seller.	B2C

Table 3-9. Pricing models [93][94]

Pricing model	Description	Target transaction
Flat	The buyer pays the fixed amount regardless of the use of the software. Cost is usually associated to a limited number of instances of the software.	B2B
Tiered	The buyer gets better deals as they acquire more quantity of the software. The cost decreases when a tier is completely filled, and the buyer is moved to the next tier. Cost is usually associated to a metric, e.g., number of instances.	B2B
Subscription	The buyer pays a fixed amount that is usually structured in tiers depending on the functionalities that are enabled to be consumed. Cost is usually associated to a limited number of instances of the software.	B2B and B2C
Pay-As-You-Grow (PAYG)	The buyer pays only for the actual consumption of the service. Cost is usually associated to a metric e.g., calls to an endpoint, compute or network consumption, elapsed time, etc.	B2C

Depending on the final VNF selected from the HoloMIT application to be used as reference implementation for the Smart Contract system UC scenario, it will be possible to create an E2E example of the required inputs to the Smart Contract. Covering from the OSS/BSS layer (from TM Forum) to the technical requirements at the VNF level (from ETSI NFV and NFV-EVE), including the business logic as well for the B2B and B2C scenarios which will require different licenses and pricing models (from Table 3-8 and

Table 3-9).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

3.3.2.1 Main benefits provided by Smart Contracts

There are several reasons why SCs are an ideal technology for a decentralised digital Marketplace such as the one being developed in the project, which aims to prepare the grounds for a production-grade telco Marketplace where transactions are expected to be legally binding and auditable.

- Efficiency and cost-effective: Smart Contracts can help automate many of the complex and time-consuming processes that heavily impact on the time-to-market of services. It has the potential to replace intermediaries (mobile settlements, lawyers) by establishing trust between parties without the need for a trusted third party [95].
- Security and transparency: The code in a SC is immutable and tamper-proof thanks to its integration with the DLT layer, thus providing a much higher level of security against attempts of fraud. As the aim is to create a global legal prose unalterable document which contains all the information related to the contract, this can help build trust between parties and reduce the likelihood of disputes.
- Flexibility: As a fully customizable computer program, once created and deployed, a SC code can be reused indefinitely for many agreements based on the configuration and availability of data.

In 6GENABLERS-DLT, the proposed solution for the SC state will satisfy the requirements from all stakeholders defined here as it will accurately map the technical and business side of what is exchanged at the Marketplace.

3.3.3 Smart Discovery

We consider the scenario of discovering available edge resource offers that meet the holo-service expectations in terms of multiple attributes, such as location, technical specifications (e.g., GPU availability) and price.

Within the Marketplace, numerous offers for edge resources are provided by Infrastructure Providers. These offers contain essential information, such as price, location, category, and technical specifications encompassing CPU, RAM, storage, and GPU availability, among other relevant details. To ensure efficient classification and discovery of these offers, the Smart Discovery system leverages offline-computed clusters. As each offer is submitted, the system determines the most suitable cluster to associate it with, based on the similarities of its features with those already present in the clusters.

When the VSPs, acting as consumer in the Marketplace, submit an intent to the Smart Discovery system, they specify their requirements for an edge offer within a particular geographical location (e.g., a city) and with sufficient resource capabilities (e.g., specific amounts of CPU, RAM, storage, and GPU availability) to accommodate the intended application.

The Smart Discovery system then processes the received intent and translates it into the internal cluster(s) that contain the offers most aligned with the requested attributes. These offers are further ranked based on their level of similarity to the specified values. Additionally, the ranking of offers can take into consideration other factors included in

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

the consumer's intent, such as price preferences. This comprehensive sorting enables the VSP to make an informed final selection from the sorted list of offers, ensuring the best fit for their requirements within the Marketplace.

The Smart Discovery workflow is depicted in Figure 3-6. As illustrated, the interaction with the system begins with the publishing of new offers. This request triggers the classification of the incoming offer into one of the pre-computed clusters. Then, classified offers become available for discovery though the use of intents from any domain. In this scenario, Stakeholder A represents an Infrastructure Provider, whereas Stakeholder B corresponds to a VSP. We can see in the figure how the Stakeholder B acting as the VSP submits an intent to discover the edge offers that are exposed on the Marketplace with some specific requirements (in this case specifying the number of cores and the amount of memory).

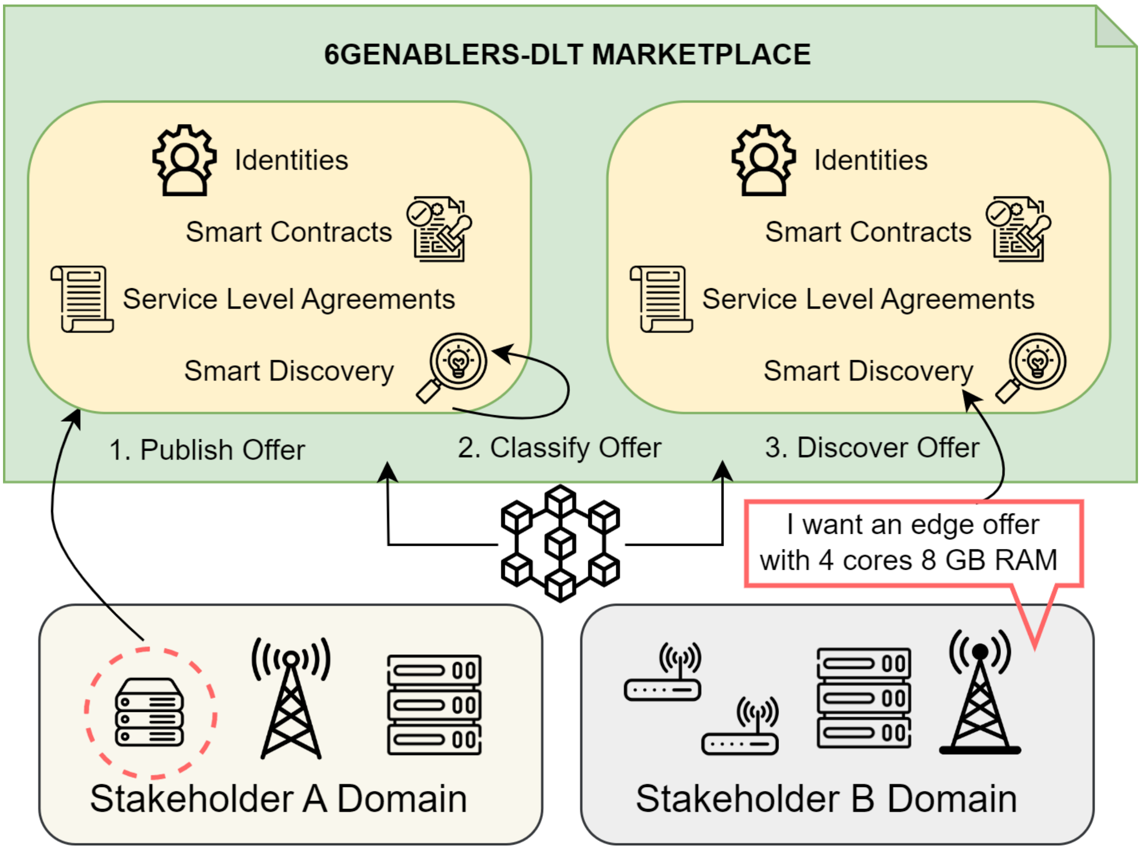

Figure 3-6. Smart Discovery workflow in the 6GENABLERS Marketplace

3.3.3.1 Main benefits provided by Smart Discovery

Considering the introduction of smart techniques to facilitate the discovery of offers over the Marketplace, holo-service providers could more easily find and select the most suitable infrastructure resources to deploy their services.

By employing the Smart Discovery system's capabilities, the process of discovering and selecting edge resource offers becomes streamlined and efficient. The integration of multiple attributes, the translation of consumer intents into relevant clusters, and the ranking of offers based on similarity and other indications empower the VSPs to make

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

well-informed decisions and acquire the most suitable edge offer to meet their holo-service expectations within the dynamic Marketplace environment.

The Smart Discovery service of the 6GENABLERS Marketplace provides several key benefits to the multi-party real-time holographic communications UC. Some of the main benefits include:

1. Efficient resource discovery: The Smart Discovery service utilises advanced algorithms and data analytics to enable efficient discovery of available resources and services offers that meet the specific requirements of multi-party real-time holographic communications. It considers attributes such as location, technical specifications, and price to identify for instance the most suitable resources for hosting the corresponding applications. This capability saves time and effort for the VSPs by providing them with a curated list of offered resources that match their needs.
2. Enhanced resource selection: The Smart Discovery service ranks the discovered resources based on their level of similarity with the requested attributes and other indications included in the consumer intent. This ranking allows VSPs to make informed decisions and select the best offer from the Marketplace. By considering factors like price, performance, and proximity, the service enables VSPs to choose resources that optimise cost-effectiveness and provide the desired QoS for real-time holographic communications.
3. Improved service quality: With the Smart Discovery service, VSPs can access resources with the necessary capabilities to ensure high-quality holographic communication sessions. The service considers technical specifications (such as CPU, RAM, storage, and GPU availability in the case of edge resources), allowing VSPs to identify resources that meet the demanding requirements of real-time rendering and processing. This ensures a smooth and immersive experience for all participants involved in multi-party real-time holographic communications.
4. Transparent and trustworthy Marketplace: The DLT-anchored nature of the marketplace ensures transparency and trust in the resource discovery process. The Smart Discovery service leverages the decentralised and immutable properties of the DLT to provide reliable information about the available resources. VSPs can verify the authenticity and integrity of the resource listings, pricing, and other relevant details. This transparency builds confidence among marketplace participants, fostering a trustworthy environment for conducting business transactions.
5. Scalability and flexibility: The Smart Discovery service, integrated in the 6GENABLERS Marketplace, offers scalability and flexibility in offers discovery. As the Marketplace grows and more edge resources become available, the service can efficiently handle the increasing volume of resource offers and adapt to evolving requirements. VSPs can easily explore and discover a diverse range of resources to support their multi-party real-time holographic communications, enabling scalability and flexibility in resource selection and allocation.

Overall, the Smart Discovery service of the 6GENABLERS Marketplace empowers VSPs in the multi-party real-time holographic communications UC by providing efficient, reliable, and transparent resource discovery capabilities. It facilitates the selection of suitable resources offered on the Marketplace, enhances service quality, and promotes

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

collaboration and innovation within the ecosystem, ultimately delivering immersive and seamless holographic communication experiences.

3.3.4 Service Level Agreement Assurance

Figure 3-7 shows the deployment of the network resources ordered by an XR service (launched by the VSP) including two networks. The metrics which compose the SLA are captured, aggregated, and stored in the local data lake. When a potential infraction is registered affecting an order provisioned by a local network, the local message bus is used to share any event or insight with other local marketplace systems.

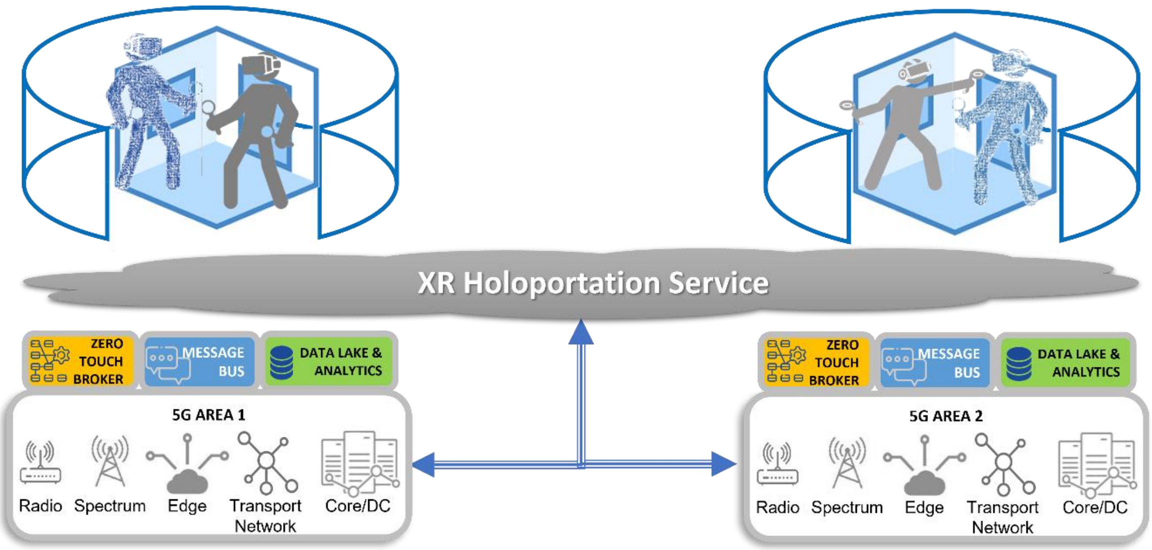

Figure 3-7. SLA assurance scenario

In particular, the scenario considered in the section contemplates from the monitoring of provisioned network assets, till the reaction implemented after the detection of an SLA breach. Given its broad scope, this scenario is further divided into the following four main operations, which are further detailed next:

1. Capture metrics of the local network (administrative) domains involved in the considered active orders, store them into a local data lake using a naming syntax, which facilitate their aggregation around a common order and store also the aggregated result in the data lake.
2. Load all the conditions declared in the order as clauses of the SLA provided, map them to metrics in the data lake and actively perform evaluations of the conditions.
3. Report to a message bus an SLA violation affecting an active order implying items on the local network, including, when possible, the network origin of the violation when several networks are involved in the order, by exploring the ingredients of the aggregation.
4. Forward the request to deploy, update or retire a network slice in the local administrative domain mapping the setup requested to the local controller and orchestrator which performs local allocation, deployment, and configurations in the network infrastructure. It also listens the status of requests and asks for updates in the orders, when applicable.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Accordingly, next tables compile the details of each operation and what they imply for the scenario setup where the UC is executed.

Table 3-10. Capture metrics from the network slices associated with an order

Name	Capture metrics from network domains serving an order
Description	Capture and store metrics from individual networks associated with E2E network slices serving specific orders in the marketplace. Storage structure is done in a way that facilitates indexing, querying and aggregation for a specific order in the data lake.
Actors	Network Operator
Pre-conditions	• The network operator gets from the local marketplace APIs endpoint the ID and credentials according to the requested permissions. • The network operator has the endpoints and credentials to locally access to the monitoring systems and the controller systems.
Sequence Workflow	1. The local data collector reloads (periodically) active orders, parses involved networks operators and metrics involved in the applicable SLAs, identifying if a local network asset is involved in the order. 2. The data collector gets endpoints of the local monitoring services at the network operator and map the relevant metrics. 3. The data collector pulls metrics from the individual monitoring services at the local network domain. 4. The data collector stores metrics at the data lake with the namespace and structure, which enables Smart Contract-based query. 5. The local data aggregator takes the map with parsed SLAs to pull from the data lake individual metrics to calculate aggregated metrics and store them in the data lake as aggregated metrics.
Post-conditions	• Local analysis and processing services at marketplace systems access the data lake to consume metrics.
Alternatives	Not applicable

Table 3-11. Evaluate SLA conditions associated with an order

Name	Evaluate SLA conditions associated with an order
Description	Reassess periodically the conditions declared at the SLA according to logical and statistical operators of KPIs captured from the individual or aggregated metrics of the involved network slices in the order.
Actors	Network Operator
Pre-conditions	• The network operator enables the monitoring systems to parse the active orders to identify key individual and aggregated metrics to be evaluated. • The local marketplace systems actively monitor data stored in the data lake to find any issue with the agreements established in the orders involving the local network.
Sequence Workflow	1. The local proactive SLA monitor at the network operator domain reloads (periodically) active orders, parses involved networks operators and the applicable SLAs, identifying if a local network asset is involved in the order. 2. The proactive SLA monitor translates declared SLA conditions into logical and statistical formulas to be assessed. 3. The proactive SLA monitor gets the mapping of relevant metrics involved to assess the SLA conditions. 4. The proactive SLA monitor pulls the metrics from the data lake. 5. The proactive SLA monitor evaluates all the formulas with the appropriate metric values included.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Post-conditions	• The result, when negative, is reported to the message bus including the affected order and the root metric and the network operator originating the breach, when local fail is applicable.
Alternatives	Not applicable

Table 3-12. SLA violation notified associated with an order

Name	**Notifying an SLA violation to the Marketplace systems**
Description	Sending a message to notify to any management systems subscribed to the SLA breach topic as the ones managing network slices to trigger a remedy or suggest a change to address the conflicting situation.
Actors	Network Operator, subscribed systems of the Marketplace
Pre-conditions	• The traffic delivered by a network slice in a network domain or over different networks involved in an order does not achieve the QoS contracted in the SLA and accordingly it is notified to provide awareness to all involved management systems and marketplace parties. • The local proactive SLA monitor identifies underperforming conditions in a specific network slice ID linked to an active smart contract of an order.
Sequence Workflow	1. The local proactive SLA monitor at the network operator domain builds a message using a specific message format. 2. The proactive SLA monitor produces the message in the message bus in a specific topic. 3. All the systems subscribed to this topic receives a message declaring an SLA breach to an active slice ID associated to the Smart Contract of an order.
Post-conditions	• The marketplace systems are subscribed to the message bus topics regarding SLA breaches. • The marketplace systems actively monitor any update on the SLA breach to detect whether it is solved, but the SLA breach history will be kept in the ledger. • The management systems analyse the discovered resources and available offers and make recommendation for addressing the situation.
Alternatives	If no breach is detected this messaging is not performed, as it just happens when issues arise

Table 3-13. Application of an E2E network setup associated with an order

Name	**Brokerage of network setups**
Description	Request the deployment, update or removal of a network slice involving one or several network domains as a connected E2E slice.
Actors	Network Operator, VSP
Scenarios	• The VSP asks for the application of a network setup for a new or existing network slice involving one or more network operators resulting in an order. • A supporting management marketplace system asks for the application of a network setup for a new or existing network slice involving one or more network operators resulting in an order. • The VSP asks to retire a network setup for an existing network slice involving one or more network operators resulting in an order termination. • A supporting management marketplace system asks to retire a network setup for an existing network slice involving one or more network operators resulting in an order termination.
Pre-conditions	• The VSP and the involved network operators agree in an order, the creation of a new one, its update or finalisation.
Sequence Workflow	1. The order service API of the marketplace produces a new or updated Smart Contract of an order or marks a pre-existing one as terminated.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

	2. The order service requests the zero-touch broker to apply the network setup as network slices in different network operators. 3. The local zero-touch broker gets the map of controllers of the local network operator. 4. The zero-touch broker breaks down the request to a sequence of individual requests to the different involved controllers of the local network (administrative) domain getting slice IDs. 5. The local zero-touch broker synchronously or asynchronously, depending on the controller possibilities, gets the status of the individual requests to report any update to the message bus, including success or fail to manage or debug any issue.
Post-conditions	• The marketplace actively monitors any update on the SLA breach.
Alternatives	Not applicable

3.3.4.1 Main benefits provided by SLAs

The benefits of using monitoring technologies in conjunction with brokers to communication networks controllers are evident to identify underperforming situations in distributed networks and actuate on provisioned network slices in a local or coordinated manner in an integral way among different actors involved. The main innovations and benefits rely on:

- the monitoring of sharing of mobile communication infrastructures isolating the different flows of each operator in slices,
- the storage of metrics according to each service order connecting metrics form different infrastructures as a transparent segment of a whole,
- unified brokerage of controllers connecting different networks with a minimum assured performance bringing the commitment to offer the QoS in a transparent way.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

4 Platform Capabilities and Requirements

In overall terms, the 6GENABLERS Marketplace must support the following capabilities:

1. **Decentralised Architecture**: The Marketplace adopts a decentralised architecture by consisting of multiple interconnected platform instances. This distributed network approach eliminates the reliance on a single centralised instance, mitigating the risks of a single point of failure. The decentralised nature of the Marketplace ensures redundancy, fault tolerance, and resilience against failures, enhancing the overall robustness of the system.
2. **Permissioned Environment**: The Marketplace is conceived to operate within a permissioned environment, where participant access is controlled. By carefully managing participant access, the system reduces the risks associated with public DLTs, where anyone can join and participate in the consensus process. This controlled access ensures a higher level of security and reduces the potential for malicious activities. The system can define and enforce rules, access permissions, and compliance requirements, ensuring adherence to specific enterprise or consortium UCs in the ICT sector.
3. **Automated Governance**: Smart Contracts can facilitate the automation and enforcement of governance rules in the Marketplace. Smart Contracts can define the conditions, roles, and responsibilities of each participant, ensuring that the onboarding process adheres to predefined rules and agreements. This automation minimises manual intervention, reduces disputes, and increases the efficiency of collaboration.
4. **Transparency and Trust**: The immutable and transparent nature of the ledger ensures that all transactions and interactions within the Marketplace are recorded and can be audited, fostering trust and accountability. Offers information must be propagated equally to all the participants, without any centralised entity controlling or manipulating the data. A meshed network in DLT ensures that information is distributed across multiple nodes, making it difficult for any single node or malicious actor to tamper with the data.
5. **Privacy and Confidentiality**: In contrast to offer dissemination to all the nodes, transactions are to be shared amongst network participants on a need-to-know basis, while still maintaining the integrity of the ledger. This privacy-preserving approach must ensure that only the involved parties have access to the specific transaction data they are authorised to see, offering the level of privacy required to support agreements between stakeholders in the Marketplace.

Complementing these overarching capabilities, this section further details the capabilities and requirements of each one of the building blocks of 6GENABLERS-DLT. These elements will serve as a guiding principle throughout the development lifecycle, ensuring that the final solution aligns with the intended goals and objectives of the project.

In terms of requirements, the following two types are considered:

- Functional requirements (F): outline the necessary features that must be accomplished by the system. These requirements define the expected functionalities that the system should exhibit.
- Non-functional requirements (NF): focus on specifying criteria that can be used to evaluate the system's operation. These criteria may include performance,

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

reliability, security, usability, and other aspects that are crucial for assessing the overall effectiveness and quality of the system.

To adopt an incremental approach during the systems' design and development, a prioritisation mechanism based on the MoSCoW method [96] has been employed. This technique categorises requirements into four priority groups: MUST have, SHOULD have, COULD have, and WON'T have, each representing a different level of importance.

- MUST: These requirements are mandatory and essential for the system's functionality and success. They must be implemented to meet the project's objectives and deliver a functioning system.
- SHOULD: Requirements in this category are of high priority and significantly contribute to the system's effectiveness and user satisfaction. While not mandatory, they are strongly recommended for inclusion in the system.
- COULD: These requirements are desirable and preferred, but not necessary for the core functionality of the system. They can enhance the user experience or provide additional features, but their absence would not hinder the system's basic operation.
- WON'T: These requirements are deemed less critical and can be deferred or excluded from the current implementation. They are suggestions for future consideration and execution, allowing for flexibility in the system's development roadmap.

In order to ensure a clear and organised approach to requirement management, an identifier convention and relevant fields have been adopted. These elements aim to effectively categorise, describe, and track requirements. The key fields utilised are as follows:

- ID: Each requirement is assigned a unique ID. The ID is generated based on the corresponding system (DLT, SC, SD, or SLA), the type (F or NF), and an iterative number, starting from 1 and incremented by 1 for each subsequent requirement. It serves as identifier for easy reference and indexing purposes.
- Unique Name: This field specifies a unique and descriptive name for the requirement. It is intended to provide a concise indication of the feature or performance criteria targeted by the requirement.
- Priority: The priority field reflects the importance of the requirement and is determined using the MoSCoW methodology.
- Description: This field contains a comprehensive and accurate textual description of the requirement. It aims to provide a clear and more detailed understanding of the desired functionality or performance criteria.
- Rationale: This field refers to the underlying motivation or reasoning behind the requirement. It justifies why the requirement is necessary or important for the successful operation of the system.
- Outcome / KPIs: Each requirement includes the outcomes (i.e., verifiable results) and/or KPIs (i.e., measurable results) that will ensure that the requirement is correctly implemented. This field establishes a clear connection between the requirement and the specific results or performance indicators that will be used to assess their success. In the case of KPIs, each requirement may have one or more associated indicators that are relevant for evaluating its performance, which are further elaborated in Section 5.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

4.1 Distributed Ledger Technologies

Coming from the described UC scenarios, the DLT system supporting the decentralised 6GENABLERS Marketplace needs to provide some functional and non-functional features and requirements. In this subsection, we identify the envisioned system capabilities and requirements in terms of DLT functionalities.

4.1.1 System Capabilities

The DLT system supporting the Marketplace needs to provide a concise set of capabilities:

1. Provide identities to actors with associated permissions.
2. Allow to create, store, and publish Smart Contracts.
3. Get subscribed to topics of the event streaming platform about SLA.
4. Report awareness of violated order and the affected network.
5. Distributed storage in different nodes.
6. Interfaced through REST Open APIs
7. Inter-connecting different administrative networks through VPN.
8. Automate deployment of DLT nodes and interconnecting agents and configurations.

4.1.2 Functional Requirements

The functional requirements of the DLT system are listed in Table 4-1.

Table 4-1. Functional requirements of the DLT system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
DLT-F-1	Visibility	MUST	Permissioned for affiliated operators and the services they contract.	Required to provide the required access to involved stakeholders.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-F-2	Consensus model	SHOULD	Type of consensus required by the nodes to validate an agreement.	Required to avoid force on unauthorised modifications.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-F-3	Smart Contract expressiveness	SHOULD	Versatility and expressiveness of the language supported for Smart Contract.	Required to create multi-clause contracts, such as domains, items, SLAs and SLOs.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-F-4	APIs	MUST	The APIs and parameters will be documented in the generated repositories.	Required to allow role-based access to add, update, or remove data from the ledger.	APIs for the interactions with the ledger (DLT-KPI-3, DLT-KPI-13)
DLT-F-5	Identities solution	MUST	Compatible solution for management of Distributed Identities.	Required to provide IDs to actors and systems.	Access control (DLT-KPI-4)
DLT-F-6	Offer senders	MUST	Different entities providing offers.	Required to create a marketplace with several supply actors.	Number of offers and offered domains (DLT-KPI-5, DLT-KPI-9)

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

DLT-F-7	Order senders	MUST	Different entities requesting for orders.	Required to create a marketplace with several demand actors.	Number of orders, domains, and consumers (DLT-KPI-6, DLT-KPI-7, DLT-KPI-10)
DLT-F-8	Event streaming	MUST	Specific topics and messages to get subscribed to updates from active contracts.	Required to facilitate the communication across systems.	Notification and record of SLA breaches (DLT-KPI-8)
DLT-F-9	Identities management	MUST	ID solution supporting business logic IDs.	Required to produce and assign credentials to traders of the Marketplace.	ID Management (DLT-KPI-4, DLT-KPI-12, DLT-KPI-14)
DLT-F-10	Decentralisation scale	MUST	ID solution supporting permission form different actors.	Required to avoid central management of storage.	ID Management (DLT-KPI-9, DLT-KPI-11, DLT-KPI-14)
DLT-F-11	Trust management	MUST	ID solution supporting trust from systems.	Required to grant access across different systems in the Marketplace platform including DLT nodes, monitoring platforms, orchestrators, and controllers.	Interdomain connection (DLT-KPI-15)
DLT-F-12	Multiple administrative networks	MUST	Ability to interconnect in an automated manner the services hosted in different networks.	Required to keep security perimeters in the different networks while connecting just the necessary marketplace, monitoring and control systems.	Interdomain connection (DLT-KPI-15, DLT-KPI-21)

4.1.3 Non-Functional Requirements

The non-functional requirements of the DLT system are listed in Table 4-2.

Table 4-2. Non-Functional requirements of the DLT system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
DLT-NF-1	Community size of DLT solution	SHOULD	Size of the developer community and lobbies related to 3GPP.	Required to ensure compatibility, evolvability, updates and maintenance.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-NF-2	Programming language of DLT solution	SHOULD	Supported programming language for performing registry checking operations.	Required to get flexibility.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

DLT-NF-3	Wide comparison for DLT solution selection	SHOULD	Selection of most capable, evolvable, and performant technology.	Required to use a base technology in a long-term.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-NF-4	Update frequency of DLT solution	SHOULD	Frequency of updates in the repositories.	Required to ensure reliability on the solution.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-NF-5	Sustainability of DLT solution	SHOULD	Soft update when upgrading technologies.	Required to avoid interruption times of the service for maintenance.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-NF-6	Administration acceptance	SHOULD	A public administration in the EU domain accepts the ID system or the DLT ledger.	Required to engage public administration to offer spectrum permissions.	DLT solution selection (DLT-KPI-1, DLT-KPI-2)
DLT-NF-7	Deployment of node	MUST	Time to instantiate and add a new node to the distributed infrastructure.	Required to join new nodes in the different network infrastructures.	Time to instantiate (DLT-KPI-22)
DLT-NF-8	Efficiency	MUST	Performance and computing resources needed by the different nodes.	Required to keep lightweight processing and infrastructure demands.	Capacity in terms of stakeholders and offers (DLT-KPI-16, DLT-KPI-17)
DLT-NF-9	Consistency latency	MUST	Response time for processing a transaction (validated, confirmed, and added to the ledger).	Required to avoid inconsistencies and incoherent data in all the distributed ledgers.	Transaction Latency (DLT-KPI-18)
DLT-NF-10	Learning curve of DLT solution	SHOULD	Documentation and learning curve necessary for its deployment and configuration.	Required to ensure quick deployment and configuration and supported debugging.	Solution documentation (DLT-KPI-19)
DLT-NF-11	Containerisation	MUST	All modules developed will be containerised through Dockers or Ansible Playbooks, trying to keep as far as possible the official technologies used to improve their maintenance and updating.	Required to migrate the marketplace to any virtualisation environment and ready to scale.	Deployment documentation (DLT-KPI-19)
DLT-NF-12	Automation	MUST	The containers will be provided with as many variables as are necessary to accommodate their instantiation and deployment in new infrastructures without the need to regenerate the container.	Required to provide data inputs that require human interaction or cannot be autonomously discovered.	Deployment documentation and versatility (DLT-KPI-19, DLT-KPI-20)

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

4.2 Smart Contracts

The elicitation of the requirements for the proposed implementation included in this document serves to showcase the role of SCs for a multi-party real-time holo-conference service and how this novel application could be benefited by a rich Marketplace of telco virtualised services that are part of trusted and secured transactions containing all the information required to best reflect the terms, rights and conditions of the desired business model. In this subsection, we identify the envisioned system capabilities and requirements in terms of SC functionalities.

4.2.1 System Capabilities

6GENABLERS-DLT will be able to create the tools for the creation of the SC state, its negotiation, validation, and integration into the DLT layer. Figure 4-1 depicts an initial high-level diagram of the Smart Contract State Composer system (in orange) and the inner functional blocks that will implement its capabilities. As per the interaction with the DLT, it will also cover the consensus mechanisms, proper identification, and authorisation, etc. Thus, it is expected that a REST API will be made available as part of the DLT developments and will only require to be correctly authorised to use the exposed functionalities. This is covered by the DLT layer of the project.

For context, Figure 4-1 also shows in grey the marketplace portal which should be in charge of communicating the required inputs to the Smart Contract State Composer, e.g., Legal Prose templates, T&C, pricing models, constrains and limits, etc.

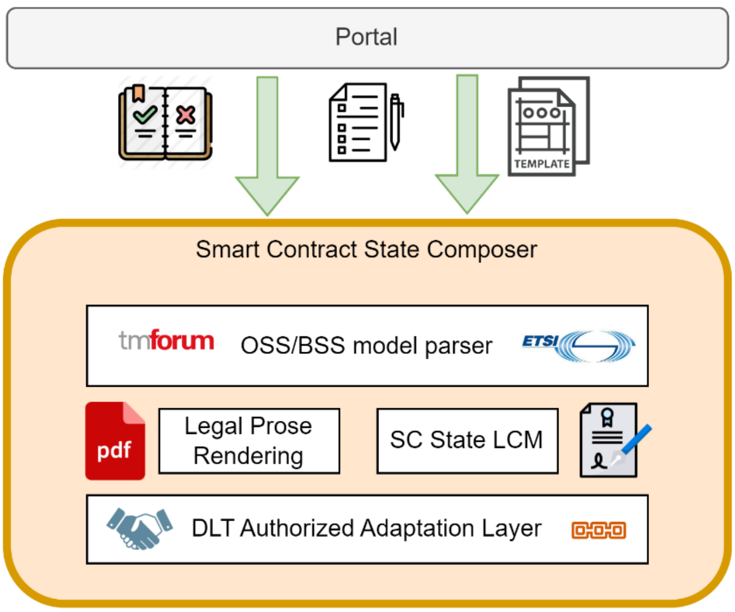

Figure 4-1. Smart Contract state composer capabilities

The task of compiling and documenting which specifications are needed to fully define the transaction of a virtualised service in B2B or B2C mode, and how to fill it out to best reflect the UC scenario presented, is of paramount importance for the project and for the SC system. This component will then interact with the DLT layer using its APIs to insert the SC state as a record of a transaction. This SC state will be standardised and aligned with the needs of the remaining components shown in Figure 2-1, starting from the work carried out in 5GZORRO.

The developed component will be able to handle templated documents containing legal prose, which defines the generic terms of use of the Marketplace and the telco infrastructure and will be then particularised with all the information specified in Section 2.2.2.

By rendering all the information to a human-readable document, it will ease the auditing of active and previous SCs as well as will provide a legally binding document that could, for example, be digitally signed and certified prior to its inclusion to the DLT. This digitally signed document would be used to verify the authenticity of configuration parameters and automations created. This mechanism ensures that all parties have agreed to the terms and cannot be modified without the consent of all parties.

In summary, the Smart Contract State Composer will provide the following capabilities:

- OSS/BSS model representation of telco assets including technical and business terms, limits, and monitoring of usage as well as the associated pricing strategies.
- Legal Prose templates describing B2B and B2C transactions in a telco environment.
- SC state standardisation, composition, and integration into DLT.
- Rendering all involved information into a human readable document.

4.2.2 Functional Requirements

In the Table 4-3, it can be found the functional system requirements that have been identified and the KPIs related to them. Each requirement has a priority associated with it. In addition, the Description field contains an explanation of the requirement, and in Rationale some extra comment to consider about it.

Table 4-3. Functional requirements of the Smart Contracts system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SC-F-1	Marketplace E2E modelling for telco assets	MUST	Create the E2E chain of TM Forum specifications that describe the OSS/BSS representation of a telco asset, with special focus on an ETSI NFV compliant xNF.	The SC State Composer defines the API that a marketplace UI needs to comply and the inputs that need to be generated to create a SC state.	Marketplace catalogue (SC-KPI-1)
SC-F-2	B2B agreement transaction	MUST	Create an E2E buyable B2B offer for 1 or more VNFs.	The UC scenario requires of a B2B SC state.	SC state (SC-KPI-2)
SC-F-3	B2C agreement transaction	MUST	Create an E2E buyable B2C offer for 1 NS composed of 1 or more VNFs.	The UC scenario requires of a B2C SC state.	SC state (SC-KPI-2)
SC-F-4	VNF OSS/BSS model for technical details	SHOULD	Unequivocally map an ETSI NFV compliant VNF to a TM Forum model including trust	Needed for the proposed B2B transaction which relates to reusability of	Multiple offers publication in marketplace for

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

			and license details.	offers in the Marketplace.	VNFs and NSs (SC-KPI-3)
SC-F-5	NS OSS/BSS model for technical details	SHOULD	Unequivocally map an ETSI NFV compliant NS to a TM Forum model including trust and license details.	Needed for the proposed B2C transaction which relates to reusability of offers in the marketplace.	Multiple offers publication in marketplace for VNFs and NSs (SC-KPI-3)
SC-F-6	VNF and NS OSS/BSS model for business	SHOULD	Include pricing description to a TM Forum model for at least 3 pricing models in B2B and B2C scenarios.	Marketplace competitivity and presence can be improved by offering the same xNF following different pricing models (flat, subscription …).	Multiple offers publication in marketplace for VNFs and NSs (SC-KPI-3)
SC-F-7	VNF and NS SC event publication scripts	COULD	Include configuration for a metric associated to a pricing description to a TM Forum model.	VNF instances are responsible for publishing the related metric about the pricing mechanism selected.	Multiple offers publication in marketplace for VNFs and NSs (SC-KPI-3)

4.2.3 Non-Functional Requirements

In turn, as in Table 4-3, Table 4-4 maintains the same structure but this time emphasising on non-functional requirements. These requirements refer to performance and run-time features of the system.

Table 4-4. Non-Functional requirements of the Smart Contracts system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SC-NF-1	Total rendering time	MUST	The final document shall be created programmatically which involves the execution of several tools.	The document could potentially be shown dynamically to the involved actors in a UI.	Rendering time (SC-KPI-4)
SC-NF-2	Smart Contract scalability	SHOULD	The system needs to be able to adapt in case of high demands.	As a backend component, it needs to be able to handle multiple requests in parallel and, potentially, scale behind a load balancer.	Deployment technology (SC-KPI-5)
SC-NF-3	Idempotence	MUST	The system needs to respond to external and internal errors in a controlled way.	Repeating the same request cannot affect the result returned.	Recovery technology (SC-KPI-6)

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

SC-NF-4	Expose functions	MUST	Expose SC capabilities via REST API aligned with the Open API specification.	The system needs to be prepared to be consumed by a marketplace portal.	NBI technology (SC-KPI-7)
SC-NF-5	Consumed functions	SHOULD	The SC state generated is stored in the DLT as a transaction.	This will prove the DLT integration of the SC State Composer and thus its alignment with the overall system envisioned.	SBI technology (SC-KPI-8)
SC-NF-6	SC state publication time	MUST	The SC state needs to be generated and then saved into the DLT.	The SC state transaction saved when the agreement is finally completed has to reach the DLT in a reasonable time.	DLT interaction time (SC-KPI-9)

4.3 Smart Discovery

The Smart Discovery service is an integral system of the 6GENABLERS Marketplace that allows telecom stakeholders to discover and select available offers based on their customer intent. In this subsection, we identify the envisioned system capabilities in terms of smart discovery functionalities. Likewise, the different requirements that the system should meet are outlined.

4.3.1 System Capabilities

The Smart Discovery system is expected to assist the Marketplace consumers when looking for an offer. Unlike traditional approaches, based on predefined filters and category pages, the proposed mechanism allows the discovery and selection of available offers on the Marketplace through the declaration of customer intents.

This functional block is built on the principles of automation and leverages ML/AI techniques to provide advanced query capabilities beyond basic lookup filters. It allows for intelligent definition of relationships between offers in the marketplace, enabling translation of high-level discovery intents to better attend to the users' requests. This functionality helps to streamline the process of obtaining access to third-party resources and enhances the overall efficiency of the Marketplace.

To make decisions about the most appropriate resources to use in each specific case, the Smart Discovery relies on different models and data sources from the offer's definition. Criteria such as price, location or technical characteristics are used to allocate offers to specific clusters. Considering the heterogeneity of the Marketplace, multiple offers categories are to be supported with distinct features. The Smart Discovery conceives this to create, train, and validate models for each specific offers type.

In addition to consumer requests, this discovery capability can also be consumed by other functional blocks. Specifically, the SLA assurance system can invoke the Smart

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Discovery to select the offers that match the needed intent with the highest score. Through the ability to invoke the Smart Discovery functionality, the SLA assurance system can retrieve available offers, enabling efficient selection of the best available resources to meet the service needs. In summary, the Smart Discovery provides an efficient way to navigate through the Marketplace more easily, being able to find the most suitable resources and services that better fit specific needs. This functionality is achieved through the main following capabilities:

- Offline computation of clusters, based on historical offers data.
- Online classification of incoming offers. based on pre-computed clusters.
- Discovery of available offers, based on consumer's intent.
- Scoring of discovered offers, based on ranking algorithms.

4.3.2 Functional Requirements

As explained before, the Smart Discovery functional block plays a crucial role in enabling efficient discovery and selection of available offers from the Marketplace. This is achieved by allowing customers to declare their intents and leveraging ML/AI techniques to discover offers that best meet their needs. To achieve this, Smart Discovery system functional requirements are listed in Table 4-5.

Table 4-5. Functional requirements of the Smart Discovery system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SD-F-1	Discovery service	MUST	Stakeholders acting as consumers must be able to discover published offers.	Required to assist consumers when looking for offers to be acquired.	Consumers are able to search for advertised offers.
SD-F-2	Automated discovery	SHOULD	Information about published offers must be obtained from the underlying ledger at every domain.	Required to support that published offers are discoverable at every domain.	Parameterised queries are run against the ledger to obtain subset of available offers.
SD-F-3	Offers' heterogeneity	MUST	Multiple offers categories must be supported with distinct features.	Required to support the trading of different types of resources and services.	Minimum number of supported offer categories (SD-KPI-1)
SD-F-4	Access to the discovery service	MUST	The discovery service must be accessible from every domain.	Required to allow stakeholders and other platform components to consume the service.	Service must be exposed and allow access from every domain.
SD-F-5	Decentralised operation	SHOULD	The service will operate following the decentralisation design principle of the Marketplace.	Required to avoid dependence and related risks of a centralised module.	An instance of the discovery service is deployed in each domain.
SD-F-6	Training datasets	SHOULD	A sufficient large dataset must be generated for models training, aligned with the defined offers data model.	Required to train the ML models, generated with realistic values according to real-world data.	Minimum number of offers in the training dataset (SD-KPI-2).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

SD-F-7	Offline clustering	MUST	To exploit clustering techniques for pattern identification across offers of a certain class/category.	Required to learn similarities between offers' properties within each offer category.	Clustering model trained offline able to generate a set of artificial clusters.
SD-F-8	Online classification	MUST	To employ supervised learning, taking the resulting clustered offers as labelled dataset for training.	Required to resolve at runtime, for every incoming offer, the cluster it belongs to.	Cluster label determined for every new offer.
SD-F-9	Offers update	MUST	Interaction with the ledger for updating offers with the determined cluster.	Required to add the determined cluster to the offer information stored in the ledger.	Cluster label added to every new offer record.
SD-F-10	Retraining	SHOULD	Training procedure should be repeated periodically (e.g., after receiving a certain set of offers or during system maintenance).	Required to ensure the model's accuracy over time.	Models retraining is performed using as training dataset incoming offers accumulated since previous training.
SD-F-11	Discovery intent	MUST	Consumers must indicate their needs in the form of an intent containing multiple attributes (e.g., price, location, technical characteristics).	Required to facilitate the interaction of consumers with the Marketplace, making it more users driven.	Support for an intent-based API that follows the open API specification.
SD-F-12	Intent recognition	MUST	Using intelligent NLP techniques, received intents must be translated into the corresponding cluster(s).	Required to recognise the offers' retrieval requests in natural language.	Returned set of offers corresponds to the customer expectations reflected in the intent.
SD-F-13	Ranking of returned offers	SHOULD	The returned offers should be sorted based on some criteria that could also be specified in the intent.	Required to present the identified offers to the consumers in an ordered way.	The resulting offers from the identified clusters are ranked in the service response.

4.3.3 Non-Functional Requirements

In addition to the features to be supported by the Smart Discovery system, presented in the previous subsection, hereafter the expected performance attributes to assess the operation of this building block are further specified. In this regard, the non-functional requirements of the Smart Discovery system are listed in Table 4-6.

Table 4-6. Non-Functional requirements of the Smart Discovery system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SD-NF-1	Discovery modularity	MUST	The system must be modular, allowing for the upgrade and future addition or removal of individual components	Facilitate independent upgrades of components and improve the	Modular system implementation by breaking down the system into

			as needed without impacting the overall system.	scalability and flexibility of the system.	modular components.
SD-NF-2	Discovery accuracy	MUST	Accuracy of the service in matching consumer intents with the appropriate offers. Considering the multiple ML techniques used by this system, this requirement involves several KPIs.	Determines the precision of the system to accurately discover the right offers. Higher accuracy signifies a more effective selection process.	Precision errors for the different models (SD-KPI-3, SD-KPI-4, SD-KPI-5, SD-KPI-6).
SD-NF-3	Training time	SHOULD	The time taken to train the ML models, as well as the time dedicated to data pre-processing. Considering the multiple ML techniques used by this system, this requirement involves several KPIs.	Indicates the execution time required for training the models offline.	Time for the training phase of the different models (SD-KPI-7, SD-KPI-8, SD-KPI-9).
SD-NF-4	Inference time	MUST	The time taken to determine the output of trained ML models. Considering the multiple ML techniques used by this system, this requirement involves several KPIs.	Indicates the execution time required for running the models online.	Time for the inference phase of the different models (SD-KPI-10, SD-KPI-11).
SD-NF-5	Discovery time	MUST	The overall time taken to identify and present the available offers that meet the consumer expectations. It includes the intent recognition and the interaction with the ledger to retrieve the corresponding offers.	Indicates the response time of the discovery system. A shorter discovery time indicates a more efficient and responsive discovery process.	Average discovery time (SD-KPI-12).
SD-NF-6	Discovery scalability	SHOULD	The scalability and adaptability of the service as the number of offers grows. It considers factors such as the ability to handle an evolving and increasing offers base.	Assesses the limits related to offers variation under which the system performance remains acceptable.	Impact to be assumed in time and accuracy (SD-KPI-13, SD-KPI-14).

4.4 Service Level Agreement Assurance

Coming from the described UC scenarios, the SLA assurance system supporting the decentralised 6GENABLERS Marketplace needs to provide some functional and non-functional features and requirements. In this subsection, we identify the envisioned system capabilities and requirements in terms of SLA assurance functionalities.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

4.4.1 System Capabilities

The SLA assurance system which supports the validity of contracts established through the Marketplace needs to provide a concise number of capabilities:

1. Connect monitoring services to a data lake.
2. Aggregate metrics with a structure designed to facilitate SLA breaches detection and identify origin even when multiple networks are involved.
3. Proactively parse active orders and evaluate SLA conditions.
4. Send messages, over the defined topics of the event streaming platform, about any detected issue regarding SLA, including the information required to design the corresponding actuation and to report awareness of the violated order and the affected network.
5. Map the available controllers from the different networks providing offers.
6. Interface through APIs the controllers to allocate, deploy, update, or retire any network setup in different networks providing status messages to event streaming topics.

4.4.2 Functional Requirements

The functional requirements of the SLA assurance system are listed in Table 4-7.

Table 4-7. Functional requirements of the SLA assurance system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SLA-F-1	Pull relevant metrics	MUST	Ability to retrieve metrics from networks with active orders.	Required to capture performance of individual segments connected in the slices contracted.	Metrics diversity (SLA-KPI-1)
SLA-F-2	Structured granularity	SHOULD	Ability to store metrics keeping links to slice ids and orders.	Required to allow management systems to recommend an action.	Data structures (SLA-KPI-2)
SLA-F-3	Time series storage	MUST	Ability to produce a data lake with all the metrics from past or current orders stored.	Required to allow AI systems to analyse data from a mid-term perspective and forecast faults.	Query modes (SLA-KPI-4, SLA-KPI-6)
SLA-F-4	Process active orders at DLT	MUST	Ability to parse active orders.	Required to alleviate processing to just the items in action.	Number of instance and actors (SLA-KPI-5, SLA-KPI-15)
SLA-F-5	Get active SLA inputs	MUST	Map SLA conditions to aggregated metrics from slices IDs.	Required to introduce just the required ingredients.	Filtering attributes (SLA-KPI-6)
SLA-F-6	Produce numerical	MUST	Generate arithmetic and statistical formulas	Required to automate assessment.	Types of resources (SLA-KPI-7)

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

	evaluation of active SLAs		on top of mapped metrics.		
SLA-F-7	Identify SLA breaches	MUST	Generate logical comparisons for SLA conditions.	Required to trigger SLA assurance.	SLA breach (SLA-KPI-3, SLA-KPI-13, SLA-KPI-14)
SLA-F-8	Produce events	MUST	Generate SLA breaches as events at known topics.	Required to notify all stakeholders, including actors and systems.	Message channels (SLA-KPI-8)
SLA-F-9	Debuggable events	SHOULD	Include in the streamed events detailed information of involved SLA metrics and slices IDs.	Required to provide all information to management systems supporting SLA assurance.	Events message (SLA-KPI-9)
SLA-F-10	API to unique network order	MUST	Expose Open API to provide in a single request all the configurations to one or multiple networks.	Required to enable operation at once from other management systems.	Wide control (SLA-KPI-10)
SLA-F-11	API to multiple network actions	MUST	Provide Open API to allocate, configure, update, or retire individual slices from other management systems.	Required to enable different operations at different phases of the SLA assurance.	Wide control (SLA-KPI-10)
SLA-F-12	Brokerage of local controllers	MUST	Map different controllers of multiple networks to intermediate on the network setup requests.	Required to forward the operation to the appropriate controller of a specific network.	Wide control (SLA-KPI-10, SLA-KPI-11, SLA-KPI-12)
SLA-F-13	Provide status on configurations	MUST	Generate deployment status as event messages at known topics.	Required to check the status on asynchronous operations and enable debugging.	Deployment status (SLA-KPI-11, SLA-KPI-17)
SLA-F-14	Universal monitoring	SHOULD	Ability to capture metrics from RAN, Core and MEC infrastructures of the slice.	Required to identify the segment where the bottleneck or issue is originated.	Networks capacity (SLA-KPI-16, SLA-KPI-17, SLA-KPI-19)

4.4.3 Non-Functional Requirements

The non-functional requirements of the SLA assurance system are listed in Table 4-8.

Table 4-8. Non-Functional requirements of the SLA assurance system

ID	Unique name	Priority	Description	Rationale	Outcome / KPI
SLA-NF-1	Learning curve of SLA assurance solution	SHOULD	Documentation and learning curve necessary for its	Required to ensure quick deployment and	Solution documentation (SLA-KPI-18)

			deployment and configuration.	configuration and supported debugging.	
SLA-NF-2	Community size of SLA assurance solution	SHOULD	Size of the developer community and lobbies related to 3GPP.	Required to ensure compatibility, evolvability, updates and maintenance.	Versatility (SLA-KPI-17)
SLA-NF-3	Programming language of SLA assurance solution	SHOULD	Supported programming language for performing registry checking operations.	Required to get flexibility.	Versatility (SLA-KPI-17)
SLA-NF-4	Wide comparison of SLA assurance solutions	SHOULD	Selection of most capable, evolvable, and performant technology.	Required to use a base technology in a long-term.	Versatility (SLA-KPI-17)
SLA-NF-5	Update frequency of SLA assurance solution	SHOULD	Frequency of updates in the repositories.	Required to ensure reliability on the solution.	Versatility (SLA-KPI-17)
SLA-NF-6	Sustainability of SLA assurance solution	SHOULD	Soft update when upgrading technologies.	Required to avoid interruption times of the service for maintenance.	Solution documentation (SLA-KPI-18)
SLA-NF-7	Multi-purpose	COULD	Provide structured data to third-party AI management systems.	Required to provide enough data to AI systems.	Data structures (SLA-KPI-2)

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

5 KPIs and Evaluation Criteria

In order to ensure the successful achievement of the requirements previously reported in Section 4, it is essential to establish appropriate metrics and thresholds to assess the effectiveness and performance of the system. These metrics, commonly known as KPIs, will serve as measurable benchmarks to assess the performance and effectiveness of the developed Marketplace. By tracking these KPIs, it becomes possible to monitor the systems' progress and make informed decisions regarding its optimisation and improvement. Considering the building blocks of 6GENABLERS-DLT, this section documents the KPIs and evaluation criteria of each system.

Defined KPIs provide a tangible way to measure and track the performance of the system in meeting the specified requirements. The elicitation of KPIs enhances the clarity and traceability of the requirements, enabling a more structured and measurable approach to requirements management and evaluation. Regular assessment and improvement based on these metrics contribute to the continuous enhancement and optimisation of the system.

In order to ensure a clear and organised approach to KPI management, an identifier convention and relevant fields have been adopted. These elements aim to effectively categorise, describe, and track KPIs. The key fields utilised are as follows:

- ID: Each KPI is assigned a unique ID. The ID is generated based on the corresponding system (DLT, SC, SD, or SLA), the acronym KPI, and an iterative number, starting from 1 and incremented by 1 for each subsequent indicator. It serves as identifier for easy reference and indexing purposes.
- Unique Name: This field specifies a unique and descriptive name for the KPI. It is intended to provide a concise indication of the metric targeted by the KPI.
- Description: This field contains a comprehensive and accurate textual description of the KPI. It aims to provide a clear and more detailed understanding of the considered metric.

For each identified KPI, evaluation criteria are also reported in this section. Evaluation criteria are specific measures used to assess the performance of the solution. These criteria provide a structured framework for evaluating and comparing solutions' attributes based on predetermined thresholds. Evaluation criteria should be well-defined, objective, measurable, and relevant to the specific requirement under evaluation. By defining clear and relevant evaluation criteria, the performance of the developed systems can be effectively measured and evaluated, enabling the identification of strengths and weaknesses to make data-driven decisions and drive continuous improvement. Like with the KPIs, evaluation criteria are outlined following the nomenclature listed below:

- ID: This field contains the identifier of the corresponding KPI.
- Evaluation Criteria: This field specifies the criteria used to verify the fulfilment of the KPI. It provides a measurable target for the evaluation of the KPI.
- Verification Description: This field outlines the means by which the KPI's achievement can be corroborated. It details the methods and considerations to be taken into account for the measuring or computation of the KPI.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

The evaluation procedure will be driven by activities such as the execution of demos, tests, and integration workshops. Measurement will be obtained when needed and the assessment result will be reported as achieved, partially achieved, or not achieved. Based on the priority selected for each requirement, Table 5-1 shows the compliance matrix for the results analysis.

Table 5-1. Requirements compliance matrix

Priority\Result	Achieved	Partially achieved	Not achieved
MUST	PASS	FAIL	FAIL
SHOULD	PASS	PASS	FAIL
COULD	PASS	PASS	PASS
WON'T	PASS	PASS	PASS

5.1 Distributed Ledger Technologies

In order to corroborate the achievement of the quantifiable indicators and verifiable outcomes related to the DLT system, the following subsection details the KPIs and evaluation criteria to be considered for this system.

5.1.1 Key Performance Indicators

Table 5-2 summarises all the metrics around different categories present in the solution based on DLT for the decentralised Marketplace.

Table 5-2. KPIs of the DLT system

ID	Unique name	Description
DLT-KPI-1	DLT alternatives	Alternatives of DLT technologies tested and evaluated.
DLT-KPI-2	Multiple parameter criteria	Criteria considered in the evaluation and selection.
DLT-KPI-3	APIs	Interfaces provided to operate the Marketplace on top of a DLT infrastructure.
DLT-KPI-4	Access control	System to control the access based on identities.
DLT-KPI-5	Available offers	Registered offers submitted by networks.
DLT-KPI-6	Active orders	Orders requested and simultaneously active.
DLT-KPI-7	Contracted networks	Number of networks with assets involved in active smart contract orders.
DLT-KPI-8	SLA breaches	SLA breaches registered in the Marketplace requiring notification and mediation.
DLT-KPI-9	Operated networks	Number of networks providing offers, managing orders and hosting a DLT node.
DLT-KPI-10	Consuming services	Number of consumers requesting for assets in the networks and ordering smart contracts.
DLT-KPI-11	Platform administrators	Administrators of the Marketplace performing administration and governance operations.
DLT-KPI-12	Actors	Number of actors present in the DLT-based Marketplace.
DLT-KPI-13	Access to systems APIs	Number of systems interacting with common API answering to different needs through the same API.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

DLT-KPI-14	ID management	System administrating credentials and identifiers.
DLT-KPI-15	Interdomain connection	Interconnection of infrastructures and domains.
DLT-KPI-16	Actors capacity of the DLT solution	Scalable in concurrency of actors.
DLT-KPI-17	Networks capacity of the DLT solution	Scalable in offered networks concurrently.
DLT-KPI-18	Transaction latency	Registration time in the DLT system.
DLT-KPI-19	Documentation of the DLT solution	Document all repositories including deployment procedure and runtime use.
DLT-KPI-20	Versatility of the DLT solution	Supported network configurations.
DLT-KPI-21	Operating costs of the DLT solution	Estimate CAPEX and OPEX to support the definition of the business model.
DLT-KPI-22	Time to instantiate	Installation and configuration of SW pieces to adhere a new infrastructure.

5.1.2 Evaluation Criteria

Table 5-3 summarises the evaluation criteria for all the metrics present in the solution based on DLT for the decentralised Marketplace.

Table 5-3. Evaluation criteria of the DLT system

ID	Evaluation Criteria	Verification Description
DLT-KPI-1	At least 3 Open-Source solutions.	The many representative alternatives for DLT the better.
DLT-KPI-2	At least 9 criteria including private visibility, associated consensus type, supported programming language, expressiveness of the supported language, necessary computing resources, available documentation, size of its community and activity in its repositories.	Consider functional and non-functional parameters.
DLT-KPI-3	At least 3 Open-APIs for mediation between governance systems (offers and orders) or subproject (SLA violations) and DLT nodes.	Provide different APIs on different data to be stored.
DLT-KPI-4	Telematic access to the APIs controlled by a mechanism of tokens or DIDs and credentials.	Enable remote operation of all the features provided.
DLT-KPI-5	At least 1 declared offer for each operated network.	All the joined networks make some assets available.
DLT-KPI-6	At least 1 order requested for 1 XR Holoportation service consuming network and virtualisation resources.	An XR service looks for networking in an area or processing.
DLT-KPI-7	At least 2 networks connected in an order providing an XR Holoportation service to at least 1 user per network connected through a "network slice".	Involving a multi-domain environment for a same order.
DLT-KPI-8	At least 2 violations producing 2 new immediate registrations. 1 local in 1 of the networks and 1 global in 2 networks.	Check that the violations are adequately propagated.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

DLT-KPI-9	At least 2 networks offering resources.	Different options to select the most suitable flavour.
DLT-KPI-10	At least 1 XR Holoportation service consuming network and virtualisation resources.	Type of service demanding processing and connectivity resources aligned with SNS priorities.
DLT-KPI-11	At least 1 operator initiating the Marketplace platform.	Administrative domain for the platform with governance capabilities.
DLT-KPI-12	At least 5 types of actors (VSPs, Network Operators, Infrastructure Providers, VSVs and VSCs).	Different actors, permissions and identities provided and managed.
DLT-KPI-13	At least 2 systems accessing system APIs, violation detection AI systems, and governance systems that register, cancel, or update new offers and orders.	Ability of an API to respond to different system requests.
DLT-KPI-14	1 Identifier technology for different actors based on DID technologies supported by DLT.	System integrated to provide all required IDs for users and systems.
DLT-KPI-15	1 VPN system to interconnect DLT nodes according to the IDs provided to each Operator.	Ready to deploy solution for inter-connection of multiple domains through agents collocated to the DLT node to be installed when joining the platform.
DLT-KPI-16	1, 2 and 4 actors are possible without any manual intervention and without the need to scale the solution.	The SW solution will not present limits to the number of consumers and the orders generated, being limited by ceilings of the available HW.
DLT-KPI-17	A guide including the installation of the DLT node and the tests to check it is properly connected is provided.	The SW solution will provide the mechanism to instantiate a DLT node in each new network operated.
DLT-KPI-18	Less than 1 second.	Time to distribute data in all the nodes.
DLT-KPI-19	Repository for each block developed including the automatic deployment scripts and guided configuration.	Facilitate the transfer and replicability.
DLT-KPI-20	At least tested in 2 different environments operating 2 different networks or deployed on one of them.	Ensure different orders can be performed including virtualisation hosting and connectivity.
DLT-KPI-21	Report required processing for all the systems along the tests.	Support in the estimation of computing resources and volumes of data consumed during the tests that serves as the basis for the business model.
DLT-KPI-22	Less than 10 minutes over the time to download online repositories.	Time to instantiate a new Marketplace node from containers and connect with the other nodes.

5.2 Smart Contracts

In order to corroborate the achievement of the quantifiable indicators and verifiable outcomes related to the SC system, the following subsection details the KPIs and evaluation criteria to be considered for this system.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

5.2.1 Key Performance Indicators

For each of the requirements elicited in this document, a representative KPI has been identified. Table 5-4 describes those KPIs and describes how they will be measured.

Table 5-4. KPIs of the Smart Contract system

ID	Unique Name	Description
SC-KPI-1	Marketplace catalogue	SC State Composer will be deployed with a local marketplace catalogue containing the required models and specifications to execute the filling out of the templates and is rendering.
SC-KPI-2	SC state	The output of the SC State Composer shall be a json payload containing all the information presented here.
SC-KPI-3	Multiple offers publication in the Marketplace for VNFs and NSs	As part of the Marketplace catalogue, a single VNF is expected to be offered using different business models in a B2B transaction. Then, it will be reused as part of a NS offer which is also expected to be offered using different business models in a B2C transaction.
SC-KPI-4	Rendering time	The E2E time that the SC State Composer takes to generate the final rendered document. It should be kept small so that it would be possible to be shown to the Marketplace user without giving the impression of being stuck.
SC-KPI-5	Deployment technology	The SC State Composer will be deployed as a containerised application in K8s using Helm.
SC-KPI-6	Recovery technology	The SC State Composer will be a stateless application.
SC-KPI-7	NBI technology	SC State Composer will be exposed using a REST API consumed over HTTP(s).
SC-KPI-8	SBI technology	SC State Composer will consume the DLT functionalities using a REST API consumed over HTTP(s).
SC-KPI-9	DLT interaction time	The E2E time that it takes for the SC state to be published in the DLT.

5.2.2 Evaluation Criteria

For each of the selected KPIs from Table 5-4, Table 5-5 provides additional information regarding what the evaluation criteria will be, and the process that will be carried out to verify it.

Table 5-5. Evaluation criteria of the Smart Contract system

ID	Evaluation Criteria	Verification Description
SC-KPI-1	Success to execute an E2E experiment.	Verified during integration workshops.
SC-KPI-2	Compliance with the schema of the Smart Contract state that will be defined.	Verified as a unit test delivered as part of the codebase.
SC-KPI-3	Multiple offers publication in marketplace for VNFs and NSs.	Examples will be created and verified as a functional test as part of the codebase.
SC-KPI-4	Rendering Time <=2 seconds	Verified as an E2E functional test delivered as part of the codebase. Also, during integration workshops.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

SC-KPI-5	Helm chart syntax verification.	The use of chart linting will be included as a unit test delivered as part of the codebase.
SC-KPI-6	No data volumes will be used.	Verified during integration workshops.
SC-KPI-7	Compliance with the Open API specification.	Verified as a unit test delivered as part of the codebase.
SC-KPI-8	Success to communicate with the DLT layer of the project.	Verified during Integration workshops.
SC-KPI-9	DLT Interaction Time <= 5 seconds	Verified during Integration workshops.

5.3 Smart Discovery

In order to verify the achievement of the quantifiable requirements of the Smart Discovery system, different performance metrics have been identified. In this regard, the following subsection details the KPIs and evaluation criteria to be considered for the Smart Discovery system.

5.3.1 Key Performance Indicators

Table 5-6 presents a comprehensive list of KPIs for the Smart Discovery system. These KPIs are carefully selected to align with the specific requirements and functionalities of the system, enabling a thorough assessment of its performance. Each KPI is described detailing its meaning in the considered context and relevance to the system performance.

Table 5-6. KPIs of the Smart Discovery system

ID	Unique name	Description
SD-KPI-1	Minimum number of supported offer categories	This KPI determines the lower bound threshold for the number of categories (i.e., edge, VNF) to be supported by the Smart Discovery models, in order to meet the expected offers heterogeneity in the Marketplace. All the categories have a set of common features (e.g., location, price) and a group of distinct features according to the offer type.
SD-KPI-2	Minimum number of offers in the training dataset	This KPI determines the lower bound threshold for the number of offers to be included in the training dataset, per offer category. Such dataset will be generated following the data models defined for offer specifications and using reference values from Infrastructure as a Service products on several providers and worldwide portfolios.
SD-KPI-3	Sum of Squared Errors (SSE) (clustering)	This KPI evaluates the performance of the clustering model. The SSE represents the sum of the squared distances between each data point and its corresponding cluster centroid. It quantifies how well the data points are clustered around their respective centroids within a certain cluster. A lower SSE indicates that the data points within each cluster are closer to their centroid and are more tightly grouped together. Notice that SSE should not be zero since an SSE equals to zero indicates that all the instances in the cluster have exactly the same values.
SD-KPI-4	Log loss (classification)	This KPI assesses the accuracy of the classification model by calculating the logarithm of the predicted probabilities for each class and comparing them to the true class labels. This metric depends on the number of classes (in this case, the number of clusters) defined for each offer

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

		category. The log loss value ranges from 0 to infinity. A lower log loss indicates better model performance, with 0 indicating perfect predictions and higher values indicating poorer predictions.
SD-KPI-5	Translation error (NLP)	The translation (comprehension) error KPI represents the accuracy of the NLP model. It indicates the level of misinterpretation incurred by the solution compared to the actual meaning of every intent.
SD-KPI-6	Total error (NLP)	This KPI represents the divergence between the requirements set in the intent and the returned offers. It directly depends on the translation error and is also impacted by the previously conducted classification of offers. It can serve as an overall indication of the system's ability to accurately match and recommend relevant offers based on the specified criteria.
SD-KPI-7	Average data pre-processing time	This KPI measures the time consumed by tasks related to the pre-processing of the data, mostly dedicated to clean and format the entries before being used by the ML models. This metric depends (in a directly proportional way) on the size of the training dataset.
SD-KPI-8	Average training time (clustering)	This KPI measures the time consumed by training the clustering model. This metric depends on the size of the training dataset.
SD-KPI-9	Average training time (classification)	This KPI measures the time consumed by training the classification model. This metric depends on the size of the training dataset.
SD-KPI-10	Average inference time (classification)	This KPI measures the time consumed by classifying an incoming offer, i.e., to determine the class of the corresponding offer category (i.e., the cluster defined for that offer category) to which it corresponds.
SD-KPI-11	Average inference time (NLP)	This KPI measures the time consumed by processing an intent request, i.e., to translate the intent into the appropriate cluster(s) that best reflect the customer expectations shown in the intent.
SD-KPI-12	Average discovery time	This KPI measures the speed at which the Smart Discovery system processes user intents and provides the corresponding list of offers. It reflects the system's efficiency in delivering timely results to users. It involves the NLP inference time and the interaction with the ledger to retrieve the offers labelled with the identified clusters.
SD-KPI-13	Increase in the training time	This KPI establishes the admissible increase in the training time to be assumed, considering an increase in the training dataset, in order to meet the expected scalability.
SD-KPI-14	Reduction in the accuracy	This KPI establishes the admissible reduction in the accuracy to be assumed, considering a reduction in the number of pre-computed clusters per offer category, in order to meet the expected scalability.

5.3.2 Evaluation Criteria

Table 5-7 extends the information related to the KPIs outlined for the Smart Discovery system. Each KPI is associated with a corresponding evaluation criteria and verification description that provides insights into different aspects of the measurement procedure to be followed during the evaluation of the KPI.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Table 5-7. Evaluation criteria of the Smart Discovery system

ID	Evaluation Criteria	Verification Description
SD-KPI-1	Minimum number of supported categories = 5	To be verified by counting the number of categories (i.e., edge, VNF, etc.) supported by the system.
SD-KPI-2	Minimum number of offers in the training dataset = 2k	To be verified by counting the number of offers per category included in the training dataset.
SD-KPI-3	SSE (clustering) converges to a value close to zero	To be measured per offer category and considering a varying number of clusters in each case.
SD-KPI-4	Log loss (classification) <= 1	To be measured per offer category. Performed evaluation is expected to consider the optimal number of clusters per offer type, in which even if the loss is slightly higher, this is still negligible for the model's accuracy, and there is not overfitting.
SD-KPI-5	Translation error (NLP) <= 10%	To be measured per offer category and considering intents with a gradually increased complexity.
SD-KPI-6	Total error (NLP) <= 30%	
SD-KPI-7	Average data pre-processing time <= 5 mins	To be measured over several repetitions (e.g., 10 times) to ensure that no significant deviations are obtained and computed as the average of those multiple executions with appropriate confidence intervals (e.g., 95%).
SD-KPI-8	Average training time (clustering) <= 100 segs	
SD-KPI-9	Average training time (classification) <= 50 segs	
SD-KPI-10	Average inference time (classification) <= 5 segs	
SD-KPI-11	Average inference time (NLP) <= 2 segs	
SD-KPI-12	Average discovery time <= 5 segs	
SD-KPI-13	Increase in the training time <= 10%	To be measured by increasing the number of offers in the training dataset and computing the training time KPIs. Performed evaluation is expected to derive the maximum number of offers to be included in the training dataset by which an improvement in the model precision is observed, but the indicated increase in the training time is not exceeded.
SD-KPI-14	Reduction in the accuracy <= 5%	To be measured by reducing the number of pre-computed clusters and computing the accuracy KPIs. Performed evaluation is expected to derive the minimum number of clusters to be considered per offer category by which an improvement in the training time is observed, but the indicated reduction in the accuracy is not exceeded.

5.4 Service Level Agreement Assurance

In order to corroborate the achievement of the quantifiable indicators and verifiable outcomes related to the SLA assurance system, the following subsection details the KPIs and evaluation criteria to be considered for this system.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

5.4.1 Key Performance Indicators

Table 5-8 summarises all the metrics around different categories present in the SLA assurance solution for the decentralised Marketplace.

Table 5-8. KPIs of the SLA assurance system

ID	Unique name	Description
SLA-KPI-1	Metrics diversity	Different metrics from different network segments.
SLA-KPI-2	Data structures	Namespace structure to facilitate local and global performance analysis.
SLA-KPI-3	Monitored networks	Number of networks producing data to the monitoring system.
SLA-KPI-4	Query modes	Different consumption modes for processing data.
SLA-KPI-5	Instances	Number of installations of the SLA assurance system.
SLA-KPI-6	Filtering attributes	Different filters supported to enable granular focus on local slices and global focus on E2E slices.
SLA-KPI-7	Types of resources	Number of asset types able to control.
SLA-KPI-8	Message channels	Number of topics and message types able to produce.
SLA-KPI-9	Universal support for basic features	Support to produce and consume event streaming messages.
SLA-KPI-10	Wide control	Control for all segments in a network slice.
SLA-KPI-11	Deployment status	Report on network slice deployment feedback.
SLA-KPI-12	Deployment time	Time to deliver all the requests to local controllers.
SLA-KPI-13	Administrative networks	Interconnection of multiple infrastructures and domains.
SLA-KPI-14	XR Use Case	Testing providing network assets for XR Holoportation services.
SLA-KPI-15	Actors capacity of the SLA assurance solution	Scalable in concurrency of actors.
SLA-KPI-16	Networks capacity of the SLA assurance solution	Scalable in offered networks concurrently.
SLA-KPI-17	Versatility of the SLA assurance solution	Supported network configurations.
SLA-KPI-18	Documentation of the SLA assurance solution	Document all repositories including deployment procedure and runtime use.
SLA-KPI-19	Operating costs of the SLA assurance solution	Estimate CAPEX and OPEX to support the definition of the business model.

5.4.2 Evaluation Criteria

Table 5-9 summarises the evaluation criteria for all the metrics present in the SLA assurance solution for the decentralised Marketplace.

Table 5-9. Evaluation criteria of the SLA assurance system

ID	Evaluation Criteria	Verification Description
SLA-KPI-1	At least 10 metrics being captured and aggregated from different segments and networks.	Metrics representative on conditions declared in SLAs.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

SLA-KPI-2	At least 3 structures to differentiate radio, core and MEC resources in a network slice.	The namespace should be structured to ease the data aggregation for SLAs and the identification of local issues that support minor updates.
SLA-KPI-3	At least 2 networks involved in an order and providing metrics.	Involving a multi-domain environment for a same order.
SLA-KPI-4	Compatible with batch and live data consumption.	Compatible with training and testing stages of an AI management system.
SLA-KPI-5	At least 1 operator of the SLA assurance system.	Administrative domain for the platform hosting the SLA assurance system.
SLA-KPI-6	At least 4 filters to select an E2E slice, the individual metrics before being aggregated from a local slice, a segment in a slice and a specific metric.	Different options to select the most suitable filter.
SLA-KPI-7	Mapping RAN, Core and MEC controllers from different networks.	Able to control all segments in a slice.
SLA-KPI-8	At least 2 topics for SLA breach and for network slice deployment including the order and the status.	Topics designed to share information to the management systems as message consumers.
SLA-KPI-9	At least 3 message types for SLA breach information and for network slice deployment including the order and the status parameters.	Messages designed to include all necessary parameters to the management systems as message consumers.
SLA-KPI-10	At least 3 mapped API interfaced controllers of RAN, Core and MEC controllers.	Controllers for all segments in a network slice.
SLA-KPI-11	At least an update every 30 secs.	Visibility of the deployment status.
SLA-KPI-12	Complete a deployment in less than 10 minutes.	Limit the time to get completed deployment through local controllers.
SLA-KPI-13	At least 2 networks.	Different options to select the most suitable flavour.
SLA-KPI-14	At least 2 holoportation users each on 1 operated network. A maximum of 4 holoportation users on a maximum of 3 networks.	Check the ability to share resources of the network from 2 concurrent slices.
SLA-KPI-15	1, 2 and 4 actors are possible without any manual intervention and without the need to scale the solution.	The SW solution will not present limits to the number of consumers and the orders generated, being limited by ceilings of the available HW.
SLA-KPI-16	A guide including the installation of the SLA assurance system and the tests to check it is properly connected is provided.	The SW solution will provide the mechanism to instantiate the SLA assurance system in each new network operated.
SLA-KPI-17	At least tested in 2 different environments operating 2 different networks or deployed on one of them.	Ensure different orders can be performed including virtualisation hosting and connectivity.
SLA-KPI-18	Repository for each block developed including the automatic deployment scripts and guided configuration.	Facilitate the transfer and replicability.
SLA-KPI-19	Report required processing for all the systems along the tests.	Support in the estimation of computing resources and volumes of data consumed during the tests that serves as the basis for the business model.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

6 Conclusion

The document provides a comprehensive exploration of the 6GENABLERS-DLT project, which focuses on supporting multi-party collaboration in dynamic 6G environments through the development of a DLT-anchored Smart Marketplace. To achieve this, the project aims to leverage DLTs, Smart Contracts, Smart Discovery, and SLA assurance as enabling technologies for future 6G networks.

This report covers the efforts related to several activities within P2, related to the definition of the UC (A2.1) and the elicitation of technologies' requirements (A2.2-A2.5). This information will serve as baseline for the design and implementation of the 6GENABLERS Marketplace in subsequent work packages.

The document begins with an introduction that outlines the objectives, the relation to the project's activities, and the structure of the document. It then delves into a detailed examination of the state-of-the-art and technologies and revision of a set of relevant standards, providing in-depth descriptions of the associated building blocks.

A significant portion of the document is dedicated to a specific UC about multi-party real-time holographic communications. The UC is thoroughly described, and UC scenarios are presented for each one of the involved technologies. Actors, roles and the main benefits provided by each technological pillar are identified, showcasing their relevance and potential in the context of the UC.

The document further explores the platform capabilities and requirements for DLTs, Smart Contracts, Smart Discovery, and SLA assurance, outlining system capabilities, functional requirements, and non-functional requirements for each technology. KPIs and evaluation criteria are defined to assess the effectiveness and performance of the considered systems. These KPIs provide a framework for evaluating the success of the project and its technological pillars.

Overall, this document serves as a valuable resource for understanding the objectives, technologies, UC scenarios, platform capabilities, and evaluation criteria of the 6GENABLERS-DLT project, contributing to the advancement and development of 6G systems.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

7 References

[1] A. Fernández-Fernández, E. Coronado, A. Erspamer, G. Samaras, V. Theodorou and S. Siddiqui, "Unlocking the Path toward Intelligent Telecom Marketplaces for Beyond 5G and 6G Networks," in IEEE Communications Magazine, vol. 61, no. 3, pp. 28-34, March 2023, doi: 10.1109/MCOM.002.2200266.

[2] S. B. M. Baskaran, T. Faisal, C. Wang, D. R. Lopez, J. Ordonez-Lucena and I. Arribas, "The Role of DLT for Beyond 5G Systems and Services: A Vision," in IEEE Communications Standards Magazine, vol. 7, no. 1, pp. 32-38, March 2023, doi: 10.1109/MCOMSTD.0004.2200053.

[3] G. Carrozzo et al., "AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture," 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 2020, pp. 254-258, doi: 10.1109/EuCNC48522.2020.9200928.

[4] T. Faisal, J. A. O. Lucena, D. R. Lopez, C. Wang and M. Dohler, "How to Design Autonomous Service Level Agreements for 6G," in IEEE Communications Magazine, vol. 61, no. 3, pp. 80-85, March 2023, doi: 10.1109/MCOM.001.2200131.

[5] Decentralized Identifiers (DIDs) v1.0 Core Architecture Data Model and Representations, [online] Available: https://www.w3.org/TR/did-core/

[6] eIDAS Supported Self-Sovereign Identity, [online] Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[7] T. Faisal, M. Dohler, S. Mangiante and D. R. Lopez, "BEAT: Blockchain-Enabled Accountable and Transparent Network Sharing in 6G," in IEEE Communications Magazine, vol. 60, no. 4, pp. 52-56, April 2022, doi: 10.1109/MCOM.001.2100603.

[8] F. Javed and J. Mangues-Bafalluy, "Demo: Blockchain-based Inter-Provider Agreements for 6G Networks," 2022 18th International Conference on Network and Service Management (CNSM), Thessaloniki, Greece, 2022, pp. 364-366, doi: 10.23919/CNSM55787.2022.9965033.

[9] F. Javed and J. Mangues-Bafalluy, "Blockchain-based 6G Inter-Provider Agreements: Auction vs. Marketplace," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 1271-1277, doi: 10.1109/GLOBECOM48099.2022.10001130.

[10] F. Javed and J. Mangues-Bafalluy, "Blockchain and 6G Networks: A Use Case for Cost-Efficient Inter-Provider Smart Contracts," 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 2022, pp. 602-608, doi: 10.1109/PIMRC54779.2022.9978121.

[11] T. Faisal, D. D. Francesco Maesa, N. Sastry and S. Mangiante, "How to Request Network Resources Just-in-Time using Smart Contracts," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 2021, pp. 1-5, doi: 10.1109/ICBC51069.2021.9461108.

[12] D. Krummacker, B. Veith, D. Lindenschmitt and H. D. Schotten, "Radio Resource Sharing in 6G Private Networks: Trustworthy Spectrum Allocation for Coexistence through DLT as Core Function," 2022 1st International Conference on 6G Networking (6GNet), Paris, France, 2022, pp. 1-8, doi: 10.1109/6GNet54646.2022.9830407.

[13] V. Theodorou et al., "Blockchain-based Zero Touch Service Assurance in Cross-domain Network Slicing," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 395-400, doi: 10.1109/EuCNC/6GSummit51104.2021.9482602.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia

[14] Jorquera Valero, J.M., Sánchez Sánchez, P.M., Lekidis, A. et al. Design of a Security and Trust Framework for 5G Multi-domain Scenarios. J Netw Syst Manage 30, 7 (2022). https://doi.org/10.1007/s10922-021-09623-7
[15] D. Breitgand et al., "Dynamic Slice Scaling Mechanisms for 5G Multi-domain Environments," 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 2021, pp. 56-62, doi: 10.1109/NetSoft51509.2021.9492716.
[16] W. Ye, X. Ant, X. Yan, M. Hamad and S. Steinhorst, "FLaaS6G: Federated Learning as a Service in 6G Using Distributed Data Management Architecture," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 1247-1252, doi: 10.1109/GLOBECOM48099.2022.10001307.
[17] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.
[18] 6G Flagship Project Website, https://www.6gflagship.com/.
[19] 5GaaS Project Website, https://5gaas.eu/.
[20] H2020 5GZORRO Project Website, https://www.5gzorro.eu.
[21] Inspire-5Gplus Project Website, https://5g-ppp.eu/inspire-5gplus/.
[22] Dedicat6G Project Website, https://dedicat6g.eu/.
[23] "A blueprint for telecom's critical reinvention", 2021, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/a-blueprint-for-telecoms-critical-reinvention.
[24] "Spain Telecommunication Market Report (2020-2025)", 2020, https://www.globalmonitor.us/product/spain-telecommunication-market-report.
[25] "Permissioned Distributed Ledger (PDL); Research and Innovation Landscape", ETSI GR PDL 008 V1.1.1, 2021, https://www.etsi.org/deliver/etsi_gr/PDL/001_099/008/01.01.01_60/gr_PDL008v010101p.pdf.
[26] H2020 SOFIE Project Website, https://www.sofie-iot.eu.
[27] "SMAUG: A decentralized marketplace for smart lockers built with SOFIE", H2020 SOFIE Project, Blog Post, 2020, https://www.sofie-iot.eu/news/smaug-a-decentralized-marketplace-for-smart-lockers-built-with-sofie.html.
[28] European Telecommunications Standards Institute (ETSI), https://www.etsi.org.
[29] ETSI Industry Specification Group (ISG) for Permissioned Distributed Ledgers (PDL), https://www.etsi.org/committee/1467-pdl.
[30] "Permissioned Distributed Ledger (PDL); Smart Contracts: System Architecture and Functional Specification", ETSI GR PDL 004 V1.1.1, Feb. 2021, https://www.etsi.org/deliver/etsi_gr/PDL/001_099/004/01.01.01_60/gr_PDL004v010101p.pdf.
[31] "Permissioned Distributed Ledger (PDL); Specification of Requirements for Smart Contracts' Architecture and Security", ETSI GS PDL 011 V1.1.1, Dec. 2021, https://www.etsi.org/deliver/etsi_gs/PDL/001_099/011/01.01.01_60/gs_PDL011v010101p.pdf.
[32] TM Forum Website, https://www.tmforum.org.
[33] Metro Ethernet Forum (MEF) Website, https://www.mef.net/about-mef.
[34] V. Capocasale and G. Perboli, "Standardizing Smart Contracts," in IEEE Access, vol. 10, pp. 91203-91212, 2022, doi: 10.1109/ACCESS.2022.3202550.
[35] H2020 SOFIE Project Consortium, "Deliverable D2.1: State of the Art Report", 2018, https://media.voog.com/0000/0042/0957/files/SOFIE_D2.1-State_of_the_Art_Report.pdf.
[36] H2020 5GZORRO Project Consortium, "Deliverable 2.1: Use Cases and Requirements Definition", May 2020, https://www.5gzorro.eu/wp-content/uploads/2021/08/5GZORRO_D2.1_v1.5.pdf.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

[37] Gonja tool repository, https://github.com/noirbizarre/gonja.
[38] Markdown to PDF tool repository, https://github.com/mandolyte/mdtopdf.
[39] Clack, Christopher; Bakshi, Vikram and Braine, Lee, “Smart Contract Templates: foundations, design landscape and research directions”, 2016, arxiv:1608.00771.2016.
[40] “Hybrid Smart Contracts”, Chainlink, 2023, https://chain.link/education-hub/hybrid-smart-contracts.
[41] J. E. Preciado-Velasco et al., "5G/B5G Service Classification Using Supervised Learning", Applied Sciences, vol. 11, no. 11, 2021.
[42] R. B. Uriarte, S. Tsaftaris and F. Tiezzi, "Service Clustering for Autonomic Clouds Using Random Forest", Proc. IEEE/ ACM CCGrid, 2015.
[43] M. Mullins and R. Taynann, "Cognitive Network Management for 5G", 5GPPP Work Group on Network Management and QoS, vol. 1.02, Mar. 2017.
[44] "Blockchain-based Telecom Infrastructure Marketplace", TM Forum Catalyst Project,https://www.tmforum.org/blockchain-based-telecom-infrastructure-marketplace/.
[45] "Vertical Industry Telcos: a Federated DLT-based Marketplace", TM Forum Catalyst Project, https://www.tmforum.org/vertical-industry-telcos-federated-dlt-based-marketplace/.
[46] "Digital Business Marketplace III – Delivering end-to-end multi-partner Industry 4.0, now! – Phase III", TM Forum Catalyst Project, https://www.tmforum.org/catalysts/digital-business-marketplace/.
[47] "AI driven business assurance for 5G", TM Forum Catalyst Project, https://www.tmforum.org/ai-driven-business-assurance-5g/.
[48] “Decentralized marketplace using smart contracts”, H2020 SOFIE Project Blog Post, https://www.sofie-iot.eu/news/decentralized-marketplace-using-smart-contracts.html
[49] “A Decentralised Marketplace for Telcos”, H2020 5GaaS Project, White Paper, https://5gaas.eu/wp-content/uploads/2023/05/5gaas_whitepaper-2.pdf
[50] A. Fernández-Fernández et al., "Multi-Party Collaboration in 5G Networks via DLT-Enabled Marketplaces: A Pragmatic Approach," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 550-555, doi: 10.1109/EuCNC/6GSummit51104.2021.9482487.
[51] D. Kulkarni, M. Venkatesan and A. V. Kulkarni, "Traffic Prediction with Network Slicing in 5G: A Survey," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), India, 2023, pp. 1360-1365, doi: 10.1109/ICAIS56108.2023.10073876.
[52] A. Papageorgiou, A. Fernández-Fernández, S. Siddiqui and G. Carrozzo, "On 5G network slice modelling: Service-, resource-, or deployment-driven?," Computer Communications, vol. 149, pp. 232-240, 2020, doi: 10.1016/j.comcom.2019.10.024
[53] J. Kosinski et al., "SLA Monitoring and Management Framework for Telecommunication Services," Fourth International Conference on Networking and Services (icns 2008), Gosier, France, 2008, pp. 170-175, doi: 10.1109/ICNS.2008.31.
[54] C. Di Martino and A. Walid, "Continuous Testing and SLA Management of 5G Networks for Industrial Automation," 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Wuhan, China, 2021, pp. 378-386, doi: 10.1109/ISSREW53611.2021.00105.
[55] Y. Niu, S. Zhao, X. She and P. Chen, "A Survey of 3GPP Release 18 on Network Data Analytics Function Management," 2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Sanshui, Foshan, China, 2022, pp. 146-151, doi: 10.1109/ICCCWorkshops55477.2022.9896472.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

[56] "5G System; Network Data Analytics Services; Stage 3", 3rd Generation Partnership Project (3GPP) Technical Specification (TS) 29.520, V15.11.0 (2023-04).
[57] S. Noureddine and B. Meriem, "ML-SLA-IoT: an SLA Specification and Monitoring Framework for IoT applications," 2021 International Conference on Information Systems and Advanced Technologies (ICISAT), Tebessa, Algeria, 2021, pp. 1-12, doi: 10.1109/ICISAT54145.2021.9678460.
[58] A. Papageorgiou, A. Fernández-Fernández, L. Ochoa-Aday, M. S. Peláez and M. Shuaib Siddiqui, "SLA Management Procedures in 5G Slicing-based Systems," 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 2020, pp. 7-11, doi: 10.1109/EuCNC48522.2020.9200904.
[59] E. Kapassa, M. Touloupou, A. Mavrogiorgou and D. Kyriazis, "5G & SLAs: Automated proposition and management of agreements towards QoS enforcement," 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2018, pp. 1-5, doi: 10.1109/ICIN.2018.8401587.
[60] P. V. Klaine, M. A. Imran, O. Onireti and R. D. Souza, "A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2392-2431, Fourthquarter 2017, doi: 10.1109/COMST.2017.2727878.
[61] X. Liu and F. Xu, "Cloud Service Monitoring System Based on SLA," 2013 12th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, Kingston upon Thames, UK, 2013, pp. 137-141, doi: 10.1109/DCABES.2013.32.
[62] C. -N. Nhu and M. Park, "Dynamic Network Slice Scaling Assisted by Attention-Based Prediction in 5G Core Network," in IEEE Access, vol. 10, pp. 72955-72972, 2022, doi: 10.1109/ACCESS.2022.3190640.
[63] Yow-Jian Lin and Mun Choon Chan, "A scalable monitoring approach based on aggregation and refinement," in IEEE Journal on Selected Areas in Communications, vol. 20, no. 4, pp. 677-690, May 2002, doi: 10.1109/JSAC.2002.1003035.
[64] A. Maarouf, A. Marzouk and A. Haqiq, "A review of SLA specification languages in the cloud computing," 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, Morocco, 2015, pp. 1-6, doi: 10.1109/SITA.2015.7358406.
[65] García L.P., Sánchez-Artigas M., París G., Barcelona P.D., Ruiz O.A., Pinto D.A. Comparison of FaaS orchestration systems; Proceedings of the IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion); Zurich, Switzerland. 17–20 December 2018; pp. 148–153
[66] A. Martin et al., "Network Resource Allocation System for QoE-Aware Delivery of Media Services in 5G Networks," in IEEE Transactions on Broadcasting, vol. 64, no. 2, pp. 561-574, June 2018, doi: 10.1109/TBC.2018.2828608.
[67] J. Baranda, J. Mangues-Bafalluy, L. Vettori, R. Martínez and E. Zeydan, "Enabling the SLA Management of Federated Network Services through Scaling Operations," 2022 IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, 2022, pp. 1-6, doi: 10.1109/ISCC55528.2022.9912996.
[68] E. Coronado et al., "Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2535-2578, Fourthquarter 2022, doi: 10.1109/COMST.2022.3212586.
[69] A. A. Khan, M. Abolhasan, W. Ni, J. Lipman and A. Jamalipour, "An End-to-End (E2E) Network Slicing Framework for 5G Vehicular Ad-Hoc Networks," in IEEE

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Transactions on Vehicular Technology, vol. 70, no. 7, pp. 7103-7112, July 2021, doi: 10.1109/TVT.2021.3084735.
[70] V. Q. Rodriguez, F. Guillemin and A. Boubendir, "5G E2E Network Slicing Management with ONAP," 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2020, pp. 87-94, doi: 10.1109/ICIN48450.2020.9059507.
[71] D. Harutyunyan, R. Fedrizzi, N. Shahriar, R. Boutaba and R. Riggio, "Orchestrating End-to-end Slices in 5G Networks," 2019 15th International Conference on Network and Service Management (CNSM), Halifax, NS, Canada, 2019, pp. 1-9, doi: 10.23919/CNSM46954.2019.9012732.
[72] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin and K. Ghoumid, "A Comprehensive Survey on the E2E 5G Network Slicing Model," in IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 49-62, March 2021, doi: 10.1109/TNSM.2020.3044626.
[73] E. Chirivella-Perez, P. Salva-Garcia, R. Ricart-Sanchez, J. A. Calero and Q. Wang, "Intent-Based E2E Network Slice Management for Industry 4.0," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Portugal, 2021, pp. 353-358, doi: 10.1109/EuCNC/6GSummit51104.2021.9482575
[74] B. Sonkoly, J. Czentye, M. Szalay, B. Németh and L. Toka, "Survey on Placement Methods in the Edge and Beyond," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2590-2629, Fourthquarter 2021, doi: 10.1109/COMST.2021.3101460.
[75] B. Sonkoly et al., "5G Applications From Vision to Reality: Multi-Operator Orchestration," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1401-1416, July 2020, doi: 10.1109/JSAC.2020.2999684.
[76] K. Katsalis, T. G. Papaioannou, N. Nikaein and L. Tassiulas, "SLA-Driven VM Scheduling in Mobile Edge Computing," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2016, pp. 750-757, doi: 10.1109/CLOUD.2016.0104.
[77] Y. Wang, X. Wan, X. Du, X. Chen and Z. Lu, "A Resource Allocation Strategy for Edge Services Based on Intelligent Prediction," 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud), Newark, NJ, USA, 2021, pp. 78-83, doi: 10.1109/SmartCloud52277.2021.00021.
[78] Ramneek and S. Pack, "A Credible Service Level Agreement Enforcement Framework for 5G Edge," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2021, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484429.
[79] M. Datar, E. Altman and H. L. Cadre, "Strategic Resource Pricing and Allocation in a 5G Network Slicing Stackelberg Game," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 502-520, 2023, doi: 10.1109/TNSM.2022.3216588.
[80] E. Bandara et al., "Kaputa - Blockchain, Non-Fungible Token and Model Card Integrated 5G/6G Network Slice Broker and Marketplace," MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 2022, pp. 559-564, doi: 10.1109/MILCOM55135.2022.10017900.
[81] Management and Orchestration; 5G Network Resource Model (NRM); Stage 2 and Stage 3, Version 15.5.0 Release 15, 3GPP Standard TS 28.541, 2020
[82] Network Functions Virtualisation (NFV); Management and Orchestration; OS-MA-NFVO Reference Point-interface and Information Model Specification, Version 2.1.1, ETSI Standard GS NFV IFA 013, 2016

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

[83] “Framework for abstraction and control of TE networks (ACTN),” IETF, RFC 8453, 2018.
[84] “COMS architecture,” IETF, Fremont, CA, USA, draft-geng-comsarchitecture-02, 2018.
[85] Montagud, M. et al. Social VR and multi-party holographic communications: Opportunities, Challenges and Impact in the Education and Training Sectors. arXiv:2210.00330.2022.
[86] Fernández, S., Montagud, M., Cernigliaro, G., Rincón, D. Toward hyper-realistic and interactive social VR experiences in live TV scenarios. IEEE Transactions on Broadcasting, 68(1), pp. 13-32. 2022.
[87] Fernández, S., Montagud, M., Cernigliaro, G., Rincón, D. Multiparty Holomeetings: Toward a New Era of Low-Cost Volumetric Holographic Meetings in Virtual Reality. IEEE Access, vol. 10, pp. 81856-81876, 2022.
[88] Ericsson, Network Slicing, 2023, https://www.ericsson.com/en/network-slicing.
[89] Roberto Viola, Ángel Martín, Mikel Zorrilla, Jon Montalbán, Pablo Angueira, and Gabriel-Miro Muntean. “A Survey on Virtual Network Functions for Media Streaming: Solutions and Future Challenges”, ACM Comput. Surv. 55, 11, Article 221, Nov. 2023, https://doi.org/10.1145/3567826.
[90] ETSI NFV&MEC Plugtests, ETSI Plugtests Report V1.0.0, June 2020, https://portal.etsi.org/Portals/0/TBpages/CTI/Docs/ETSI_NFV&MEC_2020_Plugtests_Report_v1_0_0.pdf.
[91] THALES, Software License Models, https://cpl.thalesgroup.com/software-monetization/software-license-models.
[92] ChooseALicense, https://choosealicense.com/licenses/.
[93] “What is tiered pricing model?”, ChargeBee, https://www.chargebee.com/resources/glossaries/tiered-pricing-model-strategy/.
[94] “Pricing of Digital Products and Services in the Manufacturing Ecosystem”, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/energy-resources/IPC_Pricing%20of%20digital%20products_final.pdf.
[95] “Permissioned Distributed Ledger (PDL); Application Scenarios”, ETSI GR PDL 003 V1.1.1, Dec. 2020, https://www.etsi.org/deliver/etsi_gr/PDL/001_099/003/01.01.01_60/gr_PDL003v010101p.pdf
[96] MoSCoW method, https://en.wikipedia.org/wiki/MoSCoW_method.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA

Plan de Recuperación, Transformación y Resiliencia