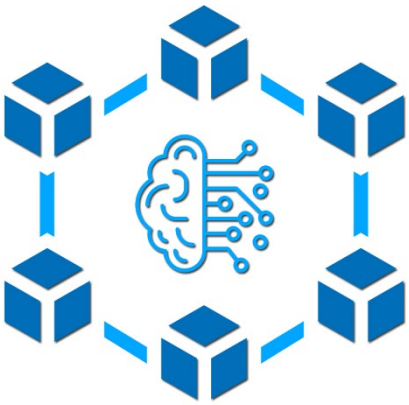

NANCY

**An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution [GA: 101096456]**

# Deliverable 2.1

# NANCY Requirements Analysis

*Programme: HORIZON-JU-SNS-2022-STREAM-A-01-06*

*Start Date: 01 January 2023*

*Duration: 36 Months*

Co-funded by the European Union

6GSNS

NANCY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096456.

## Document Control Page

| | |
|---|---|
| **Deliverable Name** | NANCY Requirements Analysis |
| **Deliverable Number** | D2.1 |
| **Work Package** | WP2 |
| **Associated Task** | Task 2.1 Use case definitions, network requirements specifications and technology enablers |
| **Dissemination Level** | Public |
| **Due Date** | 31 December 2023 (M12) |
| **Completion Date** | 28 December 2023 |
| **Submission Date** | 30 December 2023 |
| **Deliverable Lead Partner** | OTE |
| **Deliverable Author(s)** | Maria Belesioti (OTE), Antonella Clavenna (ITL), Stylianos Trevlakis (INNO), Lambrini Mitsiou (INNO), Alexandros Boulogeorgos (UOWM), Dimitrios Kavallieros (CERTH), Dimitris Manolopoulos (UBITECH), Andrea Wrona (CRAT), Emanuele De Santis (CRAT), Antonio Pietrabissa (CRAT), Martina Panfili (CRAT), Alessandro Giuseppi (CRAT), Francesco Delli Priscoli (CRAT), Danilo Menegatti (CRAT), Miguel Catalan-Cid (i2CAT), Ioannis Hadjigoergiou (SID), Christos Chaschatzis (MINDS), Andreas Maropoulos (MINDS), Stathis Mavridopoulos (MINDS), Dimitrios Asimopoulos (MINDS), Ioannis Makris (MINDS), Nikolaos Ntampakis (MINDS), Giuseppe Celozzi (TEI), Abir Yasser Barakat (TEI), Giancarlo Sacco (TEI), Marco Tambasco (TEI), Panagiotis Sarigiannidis (UOWM), Thomas Lagkas (UOWM), Dimitrios Pliatsios (UOWM), Athanasios Liatifis (UOWM), Sotirios Tegos (UOWM) |
| **Version** | 1.0 |

## Document History

| Version | Date | Change History | Author(s) | Organisation |
|---|---|---|---|---|
| 0.1 | 23/02/2023 | Initial version | Maria Belesioti | OTE |
| 0.2 | 1/04/2023 | Updated Version | Antonella Clavenna | ITL |
| 0.3 | 7/4/2023 | Updated Version | Maria Belesioti | OTE |
| 0.4 | 11/4 | New Version | Maria Belesioti, Stylianos Trevlakis, Alexandros Boulogeorgos | OTE, INNO, UoWM |
| 0.5 | 22/5 | New Version | Maria Belesioti, Stelios Trevlakis, Alexandros Boulogeorgos, Dimitrios Kavallieros | OTE, INNO, UoWM, CERTH |
| 0.6 | 01/06 | Section 4 Update | Maria Belesioti, Stylianos Trevlakis, Alexandros | OTE, INNO, UoWM, CERTH |

| | | | | |
|---|---|---|---|---|
| | | | Boulogeorgos, Dimitrios Kavallieros | |
| 0.6 | 10/06 | Section 2.3 | Christos Chaschatzis, Andreas Maropoulos, Stathis Mavridopoulos, Dimitrios Asimopoulos, Ioannis Makris, Nikolaos Ntampakis, Ioannis Hadjigoergiou | MINDS, SID |
| 0.7 | 14/06 | Section 2.3 completed<br>Section 5.1 "CoMP connectivity" Update | Dimitris Manolopoulos, Antonella Clavenna | UBI, ITL |
| 0.8 | 06/10/2023 | Sections 3.2 & 3.3 update<br>Section 5.1.2.3 update<br>Section 2 updates and various comments | Stylianos Trevlakis, Antonella Clavenna, Andrea Wrona, Emanuele De Santis, Antonio Pietrabissa, Martina Panfili, Alessandro Giuseppi, Francesco Delli Priscoli, Danilo Menegatti | INNO, ITL, CRAT |
| 0.9 | 03/11/2023 | Section 3.3 | Stylianos Trevlakis, Lambrini Mitsiou | INNO |
| 0.9 | 04/11/2023 | Section 5.2 | Dimitrios Pliatsios, Athanasios Liatifis, Sotirios Tegos | UOWM |
| 0.9 | 06/11/2023 | Sections 5.1.3.2 & 5.1.3.3 | Antonella Clavenna | ITL |
| 0.9 | 29/11/2023 | Section 5.2.3 (ad-hoc mesh) | Miguel Catalan-Cid | I2CAT |
| 0.9 | 04/12/2023 | Section 5.1.2.4 (CoMP relevant performance metrics) | Antonella Clavenna | ITL |
| 0.9 | 04/12/2023 | Section 6.1 | Giuseppe Celozzi, Abir Yasser Barakat, Giancarlo Sacco, Marco Tambasco | TEI |
| 1.0 | 28/12/2023 | Final revisions | Panagiotis Sarigiannidis, Thomas Lagkas, Dimitrios Pliatsios, Athanasios Liatifis, Sotirios Tegos | UOWM |

## Internal Review History

| Name | Organisation | Date |
|---|---|---|
| Ramon Sanchez-Iborra | UMU | 12 December 2023 |
| Alessandro Biondi, Daniel Casini, Mauro Marinoni | SSS | 18 December 2023 |

## Quality Manager Revision

| Name | Organisation | Date |
|---|---|---|
| Anna Triantafyllou, Dimitrios Pliatsios | UOWM | 27 December 2023 |

# Table of Contents

# List of Figures

# List of Tables

# List of Acronyms

| Acronym | Explanation |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 5G | Fifth generation mobile network standard |
| 6G | Sixth generation mobile network standard |
| AI | Artificial Intelligence |
| AIaaS | AI-as-a-Service |
| AMF | Access and Mobility Management Function |
| AODV | Ad hoc On-Demand Distance Vector |
| API | Application Programming Interface |
| APs | Access Points |
| AR | Augmented Reality |
| ASM | Advanced Sleep Modes |
| AUSF | Authentication Server Function |
| B5G | Beyond the fifth Generation |
| BAP | Backhaul Adaptation Protocol |
| BBU | Baseband Unit |
| BE-RAN | Blockchain-enabled Radio Access Networks |
| BF | Beamforming |
| B-RAN | Blockchain Radio Access Networks |
| BS | Base Station |
| BSC | Base-Station Controller |
| BSS | Business Support System |
| CAM | Cooperative Awareness Message |
| CAPEX | Capital Expenditures |
| CB | Coordinated Beamforming |
| CDN | Content Delivery Network |
| CoMP | Coordinated multipoint |
| CPU | Central Processing Unit |
| CS | Coordinated Scheduling |
| CSI | Channel State Information |
| CU | Central Unit |
| DE | Data efficiency |
| DL-CoMP | Downlink coordinated multi-point transmission |
| DoFs | Degrees of Freedom |
| DRL | Deep Reinforcement Learning |
| DPS | Dynamic point selection |
| DU | Distributed Unit |
| E2E | End-to-End |
| EC | Energy Consumption |
| EE | Environmental Engineering |
| EM | Electromagnetic |
| eMBB | Enhanced Mobile Broadband |
| ES | Energy Saving |
| FCC | Federal Communications Commission |
| FDD | Frequency Division Duplex |
| FML | Federated Machine Learning |

| | |
|---|---|
| GDPR | General Data Protection Regulation |
| GNSS | Global Navigation Satellite System |
| GoB | Grid of Beams |
| GSMA | Groupe Speciale Mobile Association |
| IAB | Integrated Access and Backhaul |
| IAB-MT | Integrated Access and Backhaul-Mobile Termination |
| ICI | Inter-Cell Interference |
| IoT | Internet of Things |
| ISAC | Integrated sensing and communication |
| ISP | Internet Service Provider |
| IT | Information Technology |
| JR | Joint Reception |
| JP | Joint Processing |
| JT | Joint Transmission |
| KEM | Key Encapsulation Mechanism |
| KPI | Key Performance Indicator |
| KVI | Key Value Indicator |
| KYC | Know Your Customer |
| LTE | Long Term Evolution |
| LWE | Learning With Error |
| MDAS | Management Data Analytics Service |
| MEAO | Mobile Edge Application Orchestrator |
| MEC | Multi-access Edge Computing |
| MIMO | Multiple-Input Multiple-Output |
| ML | Machine Learning |
| mMTC | Massive Machine Type Communication |
| MmW | Millimeter Wave |
| MTBF | Mean time between failures |
| MTTR | Mean time to resolution |
| NFV | Network Function Virtualization |
| NFVO | Network Functions Virtualization Orchestrator |
| MNO | Mobile Network Operator |
| M-RAT-NCP | MultiRAT Nomadic Connectivity Providers |
| NGN | Next-Generation Network |
| NIST | National Institute of Standards and Technology |
| Non-RT RIC | Non-Real Time Radio Access Network Intelligent Controller |
| NSA | Non Stand Alone |
| NTN | Non-Terrestrial Networks |
| OPEX | Operational Expenditures |
| OQS | Open Quantum Safe |
| O-RAN | Open-Radio Access Network |
| OSLR | Optimized Link State Routing |
| OT | Operational Technology |
| P2P | Point-to-Point |
| PBFT | Practical Byzantine Fault Tolerance |
| PDCP | Packet Data Convergence Protocol |
| PKI | Public Key Infrastructure |
| PPDR | Public Protection and Disaster Recovery |

| | |
|---|---|
| PRB | Physical Resource Block |
| PQC | Post-Quantum Cryptography |
| PUSCH | Physical Uplink Shared Channel |
| QKD | Quantum Key Distribution |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RF | Radio Frequency |
| RIC | Radio Aaccess Network Intelligent Controller |
| RL | Reinforcement Learning |
| RRU | Remote Radio Unit |
| RSA | Rivest–Shamir–Adleman |
| RSRP | Reference Signal Received Power |
| RSRQ | Reference Signal Received Quality |
| RU | Radio Unit |
| SA | Stand Alone |
| SDG | Sustainable Development Goals |
| SDN | Software-Defined Networking |
| SLA | Service Level Agreement |
| SLI | Service Level Indicators |
| SLO | Service Level Objectives |
| SLS | Service Level Specifications |
| SMF | Session Management Function |
| SON | Self-Organizing Network |
| SPP | Smart Pricing Policies |
| TCO | Total Cost of Ownership |
| TDD | Time Division Duplex |
| TPs | Transmission Points |
| TSN | Time-Sensitive Networking |
| TTI | Transmission Time Intervals |
| TTM | Time-To-Market |
| UAV | Unmanned Aerial Vehicle |
| UDM | User Data Management |
| UE | User Equipment |
| UL-CoMP | Uplink coordinated multi-point reception |
| UPF | User Plane Function |
| uRLLC | Ultra Reliable Low Latency Communication |
| V2V | Vehicle-to-Vehicle |
| V2X | Vehicle-to-Everything |
| V2X AS | Vehicle-to-Everything Application Server |
| VR | Virtual Reality |
| WiFi | Wireless Fidelity |
| WP | Work Package |
| XR | eXtended Reality |

# Executive summary

NANCY aims to introduce a secure and intelligent architecture for the beyond-fifth generation (B5G) wireless networks. Leveraging artificial intelligence (AI) and Blockchain, NANCY enables secure and intelligent resource management, flexible networking, and orchestration. In this direction, novel architectures, namely point-to-point (P2P) connectivity for device-to-device connectivity, mesh networking, and relay-based communications, as well as protocols for medium access, mobility management, and resource allocation will be designed and implemented.

NANCY provides a two-level contribution by developing techniques for Edge AI (e.g., federated ML-FML) and by providing an AI-based Blockchain-radio access network (B-RAN) orchestration with slicer instantiation that automates and optimizes Edge AI deployments in directions that optimize performance, security and energy efficiency. In addition, a novel AI virtualiser will be developed to exploit the network's underutilized computational and communication resources. NANCY develops novel semantic and goal-oriented communication schemes to achieve the abovementioned goals beyond Shannon excellence. Moreover, the project supports cloud management intelligence at two different levels and granularities, i.e., federated intelligence and peer-to-peer and ad hoc intelligence, towards providing decentralized and automated adaptation of cloud computing resources across the cloud/edge continuum.

NANCY will provide a novel B-RAN architecture based on the Open-radio access network (O-RAN) architecture, which is built on the ideas of component disaggregation, virtualization, and a software-based architecture. These components are interconnected via open and well-defined interfaces, ensuring compatibility across different operators. Disaggregation and virtualization enable flexible solutions based on cloud-native principles, hence enhancing the resilience and agility of the RAN. The use of open and interoperable interfaces simplifies the integration of different equipment suppliers, therefore fostering the inclusion of smaller participants in the RAN ecosystem. The integration of intelligent, data-driven closed-loop control for the RAN is achieved by using open interfaces and software-defined protocol stacks. The heart of the NANCY architecture will be a security and privacy toolbox that contains lightweight consensus mechanisms, decentralized Blockchain components, and an experimental validated B-RAN theoretical framework.

These architectures and protocols will make the most by jointly optimizing the midhaul and fronthaul. This is expected to enable genuinely distributed intelligence and transform the network into a low-power computer. Likewise, by following a holistic optimization approach and leveraging the developments in blockchain, NANCY aims to support end-to-end (E2E) personalized, multitenant, and perpetual protection.

This deliverable presents the outcome of Task 2.1, and it is focused on describing the usage scenarios, the specifications and the corresponding KPIs (Key Performance Indicators), the use cases, and the NANCY demonstrators that will be studied and demonstrated during the project's lifetime to fulfill the aforementioned goal.

To this respect, we present several use cases proposed by the literature and identify the common aspects of the demonstrations considered by NANCY. In addition, the project focuses on a wide range of usage scenarios that will be tested on lab premises and in NANCY demonstrators, which will evaluate the project's outcomes in real environments. Each of the usage scenarios includes a set of sub-scenarios that will be addressed as in-lab testbeds, evaluating the NANCY proposed technologies and innovation. Following these scenarios, the three NANCY demonstrators, mapped to the NANCY architecture, highlight which technical components will be the core ones. For each demonstrator,

besides its objectives, we define a set of preliminary targeted key performance indicators (KPIs) and key value indicators (KVIs). It should be noted here that these KPIs and KVIs might be further enhanced and refined in the upcoming deliverables. Finally, for each one of the demonstrators, we identify the actors involved, potential risks, and main challenges.

The following WP2 deliverables will be focused on the Experimental-Driven Modelling (D2.2), NANCY Network Information Framework (D2.3) and System Performance Assessment (D2.4). The detailed demonstrator definitions and requirements will act as blueprints for their implementation in WP6.

# 1 Introduction

With the deployment of 5G commercial networks, both industry and academia have started to envision sixth-generation (6G) communications towards 2030. This preliminary stage in the light of 6G is defined as B5G networks. While on the path of embracing the 6G evolution, it is necessary to expand the fundamental network design paradigm from a performance-oriented vision to a combined performance and value-oriented design to meet B5G and 6G challenges.

In B5G networks, trust in the data delivered, integrity of information, and privacy are of high importance. By integrating AI and Blockchain functions into wireless networks, they become service and resource-aware capable of adapting in a dynamic manner, optimizing the system efficiency.

A main goal of NANCY is to introduce a secure and intelligent architecture for B5G wireless networks by leveraging AI and Blockchain technology. This architecture is envisioned to successfully support dynamic and seamless services for use cases with stringent requirements steaming from 6G. Moreover, it aims to address the difficulties related to network management and resource orchestration due to the rapid complexity of wireless networks.

This report is the first deliverable of Work Package 2 (WP2) “Usage scenario and B-RAN modelling, network requirements, and performance assessment” aiming to identify the user requirements and define the NANCY KPIs and KVIs based on the user expectations and vision, and possible constraints and boundaries of B5G realms.

## 1.1 Structure and Main Objectives of Work Package 2

The purpose of WP2 is to identify the user and stakeholder requirements and define the NANCY KPIs based on the user expectations and vision, and possible constraints and boundaries of B5G realms. In addition, this WP will conduct experimental-driven B-RAN modelling.

More specifically, the objectives of WP2 are listed below:

(a) To define the use cases and user/system/network and stakeholder requirements.

(b) To synthetize all the requirements and derive integrated system functional and technical specifications.

(c) To perform experimental-driven B-RAN modelling.

(d) To identify and describe the NANCY concept technology enables and evaluate their performance bounds through respective simulations.

(e) To identify possible types of attacks and assess the security and privacy risks; and

(f) To derive analytical models for theoretically estimating the performance bounds of B-RAN.

## 1.2 Deliverable 2.1 Objective and Relation to Other WPs

The deliverable, entitled ‘NANCY Requirements Analysis’, is focused on presenting the outcomes of Task 2.1, which is related to the definition of the NANCY ‘Use cases and Demonstrators’ requirements, the specifications as well as their corresponding KVIs and KPIs. It is considered a basis deliverable,

taking input from all other technical WPs, as depicted below, and acting as a blueprint for WP6 where the NANCY architecture will be validated.

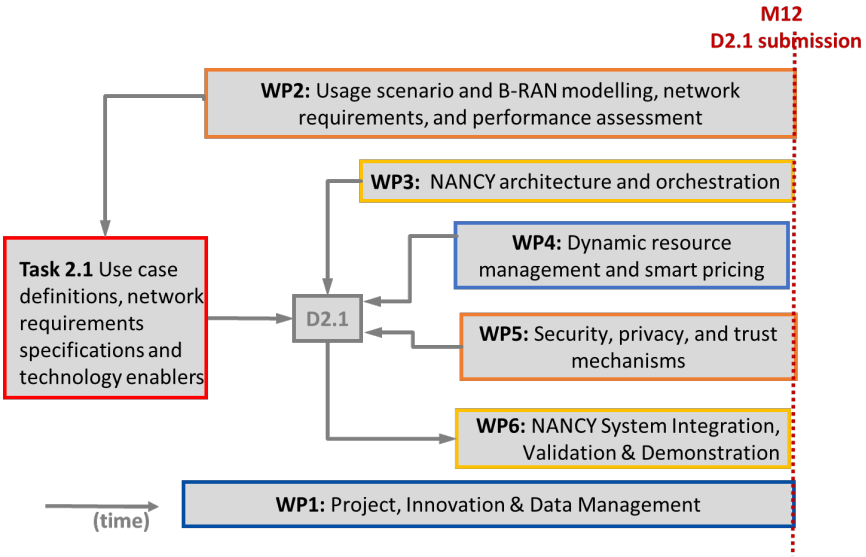


Figure 1: Relation of D2.1 to Other WPs

In this deliverable, we identify the key enablers considered by the project and we provide a synopsis of the NANCY vision, as well as a high-level overview of NANCY architecture. After a literature review on Beyond 5G/6G KPIs and KVIs, we propose preliminary targeted KPIs and KVIs that will be further enhanced and refined in WP6 deliverables, after the conclusion of the demonstrations. Moreover, we investigate a wide range of reference use cases and BRAN scenarios, so as to highlight their similarities and differences with NANCY demonstrators. Then, we describe the three NANCY demonstrators and the corresponding experimental scenarios. In particular, we provide a detailed description, we identify the main NANCY architectural elements participating in each one of the challenges addressed, we present the involved actors and their roles, and we present the testbeds that will validate each one of them. For each demonstrator, this analysis leads us to the identification of functional and non-functional requirements, hence addressing their target values. The testbeds participating in the validation process will be parameterized accordingly and will be refined to the level of detail required for conducting the demonstrations effectively. This work will be used as input for implementing the demonstrations in WP6.

## 1.3 Structure of the Deliverable

This deliverable is organised as follows:

- **Section 2 – Targeted Performance Metrics** presents a literature review on KPIs and KVIs as well as the project's targeted values acknowledging their importance for a successful outcome.
- **Section 3 – NANCY Vision and Enabling Technologies** provides a conceptual overview of the NANCY architecture and its core technological enabling technologies highlighting the project's vision. A more detailed analysis of the architecture will be presented in Deliverable D2.2.
- **Section 4 – Reference Use Cases Overview** describes the path from 5G to 6G by presenting a wide range of use cases proposed by the literature, reference 6G projects, and B-RAN Scenarios which are either related to the NANCY vision and concept or are focused on related domains.
- **Section 5 – NANCY Usage Scenarios** presents the NANCY usage scenarios namely: i) fronthaul network of fixed topology, ii) advanced coverage expansion, and iii) advanced connectivity of mobile nodes addressing the challenges considered by NANCY.

- **Section 6 – Demonstrators** is focused on the NANCY demonstrators that will be validated during the project. More specifically, we present the considered experimentation scenarios and their testbeds as well as the involved blocks of NANCY architecture. We also identify the targeted KPIs and KVIs that each one addresses, finally, and we highlight their functional and non-functional requirements.
- Finally, **Section 7 – Conclusion** concludes the deliverable.

# 2 Targeted Performance Metrics

## 2.1 Terminology

In the NANCY project, we employed the usage research data model in order to define the usage scenario and the use case. The following list provides the key definitions used throughout the deliverable:

- **Usage scenario:** A usage scenario is a description of a way (or the envisioned way) someone uses an existing product or system.
- **Use case:** A use case is a definition of a specific business objective that the system needs to accomplish. This can be achieved by describing the various external actors (or entities) that exist outside of the system, together with the specific interactions that they have with the system to accomplish the objective.
- **Demonstrator:** A demonstrator is a prototype, rough example, or an otherwise incomplete version of a conceivable product or future system, put together as a proof of concept with the primary purpose of showcasing the possible applications, feasibility, performance, and method of an idea for a new technology.
- **KPIs:** A key performance indicator is a quantifiable metric used to track progress towards a specific goal or objective. It relates a specific demonstration outcome with a targeted performance measure. It defines a set of values against which to measure network functions and/or network operations.
- **KVIs**: Key value indicators are evaluation criteria that measure sustainability, social, financial, and environmental impact as well as trustworthiness, which must be considered in the system architecture design evolution to 6G.

## 2.2 Literature on Beyond 5G/6G KPIs and KVIs

The evolution of wireless communication networks from the first to the fourth generation has witnessed remarkable advancements in terms of speed, connectivity, and capacity. However, the insatiable demand for high-speed data and the emergence of new technologies and applications have led to the exploration of Beyond 5G/6G networks. These networks aim to provide unprecedented performance, reliability, and connectivity. The development and utilization of KPIs and KVIs have become increasingly critical to assess and optimize the performance of Beyond 5G/6G networks. The evolution of wireless communication systems beyond 5G into the realm of 6G represents a transformative phase in the field. To ensure the success and efficacy of these advanced networks, it is essential to define and delineate KPIs and KVIs that encompass not only technical aspects but also broader societal, economic, and environmental factors. This literature review delves deeper into the state of research and industry perspectives on Beyond 5G/6G KPIs and KVIs, with a focus on prominent metrics and indicators proposed in recent studies.

### 2.2.1 5G and Beyond 5G/6G Evolution

5G networks have made substantial progress in meeting the demands of today's mobile communication needs [1]. However, as the number of connected devices and applications continues to surge, there are challenges that 5G and its predecessors cannot address effectively. B5G/6G networks represent the next frontier in wireless communication, designed to overcome these limitations. These networks are expected to offer significantly higher data rates, lower latency, and

enhanced reliability, enabling a wide range of innovative applications such as augmented reality, autonomous vehicles, and smart cities, among many others [2].

### 2.2.2 KPIs and KVIs in Beyond 5G/6G: Definitions and Importance

KPIs and KVIs are critical parameters used to assess and measure the performance of wireless communication systems. KPIs typically encompass metrics related to reliability, latency, throughput, coverage, energy efficiency, and more. KVIs, on the other hand, go beyond traditional KPIs by considering factors such as user experience, economic benefits, and societal impacts. They play a pivotal role in shaping the goals and objectives of Beyond 5G/6G networks. Several studies emphasize the need for a holistic approach to KPIs and KVIs that balances technical aspects with broader socio-economic and environmental considerations.

In the context of beyond 5G/6G, several KPIs are crucial for assessing and improving network capabilities:

1. **Throughput:** B5G/6G networks aim to deliver multi-gigabit-per-second data rates, making high throughput a critical KPI [3].
2. **Latency:** Ultra-low latency is essential for applications like remote surgery, autonomous vehicles, and real-time gaming. Beyond 5G/6G networks aim to achieve sub-millisecond latency, pushing the boundaries of what is currently achievable [4], thus KPIs for latency are expected to reach unprecedented levels [5].
3. **Network Capacity**: Increasing the 5G/6G network capacity is crucial when dealing with a high number of requests from multiple users, who have a certain desired quality of service/experience in terms of downlink data throughput or transmitting power.
4. **Network Coverage**: It refers to the extent to which a mobile network can provide signal reception and connectivity to its customers within a specified geographic area.
5. **Reliability:** B5G/6G networks need to ensure highly reliable connections for mission-critical applications, such as industrial automation and public safety [6].
6. **Energy Efficiency** is a key concern due to the sustainability goals of B5G/6G networks. It involves optimizing energy consumption per transmitted bit, and researchers are exploring innovative techniques like energy-efficient modulation and green communication technologies [7]. As sustainability becomes a growing concern, KPIs that are related to energy efficiency will be essential to minimize the environmental impact of these networks [8].
7. **Spectral Efficiency:** Spectral efficiency remains a foundational metric in wireless communications, measuring how effectively data can be transmitted over a given bandwidth. With Horizon Europe projects pushing the boundaries of spectral efficiency, research efforts have intensified in this area. The goal is to accommodate the soaring data requirements of emerging applications while optimizing spectral resources [9]. To make the best use of available frequency bands, spectral efficiency KPIs focus on how efficiently the network utilizes the spectrum [10].
8. **Quality of Experience (QoE):** KPIs will assess the end-user's satisfaction, abstracting factors like data rate, latency, and reliability, to provide a holistic view of the network's performance [11].
9. **Network Congestion**: Specific KPIs will represent the 5G/6G base station saturation in terms of (i) band spectrum occupancy, (ii) power allocation, (iii) downlink data throughput, and (iv) uplink data throughput.
10. **Service Availability:** KPIs will evaluate how consistently services are available, especially for critical applications, ensuring high service availability [12].
11. **Scalability:** Scalability KPIs will measure the network's ability to handle the growing number of connected devices and the increasing demand for data [13].

12. **Security:** Security KPIs will assess the network's ability to protect against cyber threats and safeguard user data and privacy [14].

KVIs go beyond traditional KPIs by considering the overall value provided to end-users and stakeholders:

1. **Societal and Economic KVIs:**
    a. **Cost-effectiveness:** KVIs will consider the economic viability of Beyond 5G/6G networks, taking into account deployment and maintenance costs [15].
    b. **Economic Growth and Innovation:** B5G/6G networks are expected to stimulate economic growth through new business models and industries. KVIs here include indicators related to job creation, gross domestic product growth, and technological innovation [16].
    c. **Social Inclusion and Digital Divide:** Ensuring that the benefits of B5G/6G are accessible to all segments of society is a critical KVI. Researchers and policymakers are exploring metrics related to digital inclusion, affordability, and bridging the digital divide [17].
2. **Environmental and Sustainability KVIs:**
    a. **Carbon Footprint:** The carbon footprint of wireless networks is a growing concern. KVIs in this context include indicators that assess the environmental impact of B5G/6G networks, such as reduced energy consumption and greenhouse gas emissions [18].
    b. **Resource Efficiency:** Evaluating the efficient use of resources, including spectrum and materials, is vital for sustainability. KVIs here encompass metrics that promote resource sharing, reuse, and recycling [11].

### 2.2.3 Literature on 6G KPIs and KVIs

This section, following the work of [19], outlines how KVIs and KPIs and related concepts have been used in other projects to provide input for future identification of the KVIs and KPIs.

#### *2.2.3.1 Open Ecosystem for OT Networks*

In the ACI20 project [20], an open ecosystem for Operational Technology (OT) networks in industrial environments is motivated. This ecosystem emphasizes openness for interoperability, compatibility with technologies like Time-Sensitive Networking (TSN), and integration with existing infrastructure. To quantify the level of openness, novel KVIs are required. The project distinguishes between local and remote use cases, addressing aspects such as isolation, data privacy, and dependability metrics to meet automation application requirements. Additionally, reliable time synchronization and integration with security frameworks are key considerations.

#### *2.2.3.2 Clustering of KVIs*

Work in [21] clusters KVIs into growth and sustainability/efficiency domains. Growth-related indicators measure economic growth, value chain expansion, and ecosystem and business models. Sustainability and efficiency objectives utilize value indicators like total cost of ownership (TCO), time-to-market (TTM), flexibility, security, privacy, and trust, energy consumption, serving the underserved, megacity impact, and Public Protection and Disaster Recovery (PPDR). Specific performance indicators with high economic impact include the number of private networks, devices, network slicing, and network automation.

#### *2.2.3.3 Vision of Ever-present Intelligent Communication*

The study in [22] envisions 6G as Ever-present Intelligent Communication driven by trustworthiness, sustainability, extreme applications, and simplified life. It highlights expanding quantitative parameters like capacity, data rates, latency, and device connectivity, as well as qualitative domains

such as security compute integration, service availability, and positioning and sensing capacities. Energy efficiency, coverage, and sustainable cost of ownership are also fundamental considerations.

#### *2.2.3.4 Cyber-Physical Fusion in 6G*

Authors of [23] focus on 6G's Cyber-Physical Fusion and its main areas, including solving social problems, human-to-thing communication, expanding the communication environment, and refining cyber-physical fusion. It emphasizes expanding 5G capabilities, such as data rate, capacity, energy efficiency, latency, reliability, and massive connectivity, along with new dimensions in security/privacy and positioning/sensing.

#### *2.2.3.5 Hyper-connected Experience with 6G*

The proposal in [24] envisions 6G as providing a hyper-connected experience, emphasizing megatrends like connected machines, AI, openness, and societal goals. It highlights new services like immersive XR, mobile holograms, and digital replicas, which require improvements in 5G KPIs and expansion into new capabilities, including communication-computing convergence and heightened security.

#### *2.2.3.6 Key Drivers and Research Challenges for 6G*

The work in [25] addresses key drivers and research challenges for 6G, categorizing KPIs into technology-driven and sustainability/society-driven domains. Technology-driven KPIs include latency, jitter, link budget, range/coverage, 3D-mapping fidelity, position accuracy, cost, and energy-related metrics. Sustainability and society-driven KPIs encompass vertical player inclusion, transparency, privacy/security/trust, global use case-oriented application programming interfaces (APIs), UN SDG-inspired indicators, open-source adoption, and ethics considerations.

#### *2.2.3.7 Thematic Areas in 6G Research*

6G Flagship [26] presents various thematic areas in 6G research, delving deeper into performance and value indicators for specific topics. It highlights the use case dependency of KPIs and KVIs, emphasizing that numerical values are context-dependent and that KPI assessment varies across verticals.

#### *2.2.3.8 Societal Requirements in 6G*

Societal requirements include energy efficiency [13], low environmental impact [27], digital inclusion [28], security [29], resilience [30], and electromagnetic field awareness [31]. These requirements are considered equally vital as performance metrics, ensuring societal relevance and acceptance in 6G development.

These insights from various projects and research initiatives provide valuable input for the identification and refinement of KVIs and KPIs in the context of B5G/6G networks, considering diverse use cases and societal needs.

### 2.2.4 Challenges and Future Directions

Challenges in defining and implementing KPIs and KVIs for B5G/6G networks include:

- Developing unified standards for KPIs and KVIs to ensure interoperability and consistency across heterogeneous network elements.
- Integrating emerging technologies such as artificial intelligence, edge computing, and quantum communication into KPI and KVI frameworks.
- Addressing ethical, security, and privacy concerns related to collecting and analyzing data for KVIs.
- Defining unified KPIs and KVIs regardless of use cases, which may vary from ultra-reliable low-latency communications for critical applications to massive machine-type communications for the Internet of Things (IoT).

B5G/6G networks represent the future of wireless communication, promising unparalleled performance and connectivity. The establishment of comprehensive KPIs and KVIs is essential to guide the development and assessment of these networks, ensuring they meet technical, societal, economic, and environmental goals. These metrics will not only gauge network performance but also assess the overall value delivered to users and stakeholders, driving innovation and progress in the field of wireless communication. As technology continues to evolve, the refinement and adaptation of KPIs and KVIs will be vital to meet the diverse needs of these advanced networks.

## 2.3 Targeted KPI's and KVI's Definition

Addressing a set of KPIs for sustainability in the context of NANCY is crucial for the assessment of its environmental, and socioeconomic impact. In other words, sustainability refers to the responsible and eco-conscious use, operation, deployment, and impact of the advancements and technologies that will be developed in the context of the project. More precisely, there are a number of principles that aim to minimize the overall environmental, social, and economic footprint, while maximizing the long-term benefits. The corresponding key aspects can be summarized as:

- **Environmental Responsibility:** Sustainable, and innovative networks should be designed and operated with the primary goal of minimization of their impact on the environment. For instance, this can include reductions in energy consumption, carbon emissions, and electronic waste, by utilizing energy-efficient equipment and renewable energy sources, leading to a greener digital eco-system.
- **Resource Efficiency**: Sustainability also entails the optimization of the use of resources that a network requires, like a network infrastructure, and computational power, among others. An efficient resource allocation can prevent resource wastage and reduce operational costs.
- **Socioeconomic Development**: Beyond connectivity and reliability in advanced networks, sustainability is, also, concerned, with socioeconomic development, involving economic growth, and enhancing the quality of life.
- **Resilience and Future-Proofing:** Novel and advanced network designs should have adaptability and resilience in mind, as they should be capable of encountering environmental challenges and, simultaneously, meet potential future communications needs.

Overall, sustainability in advanced network designs is more than just faster and more reliable communications; it is about building a digital network ecosystem that is aligned with the global goals of environmental protection, and economic development.

### 2.3.1 Trustworthiness

Trustworthiness refers to the level of reliability, security, and ethical conduct that is associated with the utilization and deployment of 5G networks and their corresponding technologies. More precisely, it involves a range of practices that aim to ensure that networks are secure and operate in a way that preserves user's privacy, regulations, and ethical standards. Some key characteristics are:

- **Reliability and Dependability:** Trustworthy 5G and B5G should be significantly reliable, and they should simultaneously be capable of ensuring continuous connectivity and solid performance.
- **Security:** Security is closely connected with trustworthiness, as most network environments should implement robust security mechanisms to protect the confidentiality, integrity, and availability of users' data. For example, encryption and authentication technologies should be core components of modern network developments.
- **Transparency:** Transparency refers to the degree of clarity of the operations conducted inside a network. This includes insights into the mechanisms that collect, or process data, and decisions that potential AI/ML models make, among others.

- **Privacy:** In order to increase the trustworthiness of a network, special attention should be paid to the privacy of data, as all users should have full control over their data, while the system is responsible for operating according to the regulations and principles in order to preserve data privacy.

As it was described, trustworthiness is extremely important and should be considered when developing and designing new 5G, and B5G networks in order to ensure that each technology is used in a responsible, secure, and ethical manner.

### 2.3.2 Digital inclusion

Digital Inclusion refers to the efforts and strategic plans that aim at ensuring that most individuals and communities can benefit from the integration and implementation of innovative networks, regardless of their socioeconomic status, geographic location, or abilities. Key aspects include:

- **Equal Access:** Digital inclusion in this domain is linked with the provision of equal access to a 5G, B5G network characterized by increased reliability, and consistent connectivity. In other words, it means that everyone should be able to have access to the corresponding digital infrastructure.
- **Affordability:** The level with which the services provided by the network are ensured is affordable regardless of the income of both individuals and communities. This is a significant aspect of digital inclusion. It encompasses strategies to reduce the costs of devices and the corresponding cost of accessing certain services.
- **Accessibility:** Digital inclusion can be extended to individuals with certain special needs. It involves strategies to design networks, devices, components, and applications to be accessible and usable by people with, for example, visual, hearing, or mobility impairments.

In general, digital inclusion is not only about providing access to certain services and technologies; it's about creating an eco-system in which all individuals and communities have equal opportunities to benefit from the advancements of 5G and B5G networks.

### 2.3.3 Technological Push

Technological Push is driven by advancements stemming from research, innovation, and development in the technological sector. In the realm of B5G/6G, several essential KPIs stand out:

- **Throughput**: Indicates the capability of a network to process large volumes of data in specific timeframes.
- **Latency**: Represents the delay time taken for a packet of data to move from the source to its destination.
- **Reliability:** Reflects the network's stability in maintaining connections and ensuring that data transmissions are error-free.
- **Energy Efficiency:** It emphasizes reducing energy wastage and optimizing power consumption.
- **Service Availability:** It underscores the importance of consistent service by minimizing downtimes and ensuring that users have constant access to the network.
- **Spectral Efficiency**: Highlights the importance of transmitting data effectively over the available bandwidth.

Equally vital in this context are the KVIs. Some indicative KVIs could be:

- **Quality of Experience:** It uses metrics like latency, throughput, and reliability to measure user satisfaction.
- **Security:** It is all about guarding against threats and safeguarding user data.
- **Scalability:** As the large number of connected devices increases the networks should evolve to accommodate the growing demand.

### 2.3.4 Societal Impact

Societal Impact delves into the effects of technology on society, which includes the economy, culture, and daily life. Within this framework, some significant KVIs are:

- **Carbon Footprint:** It quantifies the environmental impact, usually the total emissions of CO2, of network operations.
- **Resource Efficiency:** It highlights the effectiveness with which networks utilize available resources, ensuring that the wastage is minimized.

On the other hand, on the KVIs front:

- **Economic Growth and Innovation:** It looks at indicators such as job creation, gross domestic product growth, and technological leaps.
- **Social Inclusion and the Digital Divide:** It focuses on equitable access to technological advancements by bridging the gap between different societal segments.
- **Environmental and Sustainability:** It emphasizes best practices in eco-friendly operations. Encourages resource-sharing, reuse of materials, and recycling initiatives.

# 3 NANCY Vision and Enabling Technologies

In contemporary scientific debates, Blockchain technology has been acknowledged as a disruptive innovation of considerable magnitude [32],[33]. The Federal Communications Commission (FCC) has proposed the potential integration of Blockchain technology into wireless communications for the upcoming next-generation network (NGN), as presented at the Mobile World Congress 2018 [34]. Similarly, the novel notion of B-RAN was officially introduced and delineated. B-RAN is a wireless access paradigm that is both decentralized and secure. It operates on the principle of Blockchain and integrates multiple trustless networks into a larger shared network. This results in positive network effects that benefit multiple parties. B-RAN has the potential to significantly enhance network throughput by means of cross-network sharing and offloading, as stated in reference [35]. Moreover, the favorable network effect may facilitate B-RAN in the recruitment and attraction of a greater number of participants, encompassing network operators, spectral owners, infrastructure manufacturers, and service clients alike. The amplification of a collaborative network platform would enhance its worth, resulting in a constructive feedback cycle. Over time, a substantial quantity of individual access points (APs) can be systematically arranged into a B-RAN and transformed into a marketable commodity, resulting in the establishment of a widespread and extensive wireless network. This network has the potential to considerably enhance the effectiveness of both spectra and infrastructures. The implementation of B-RAN can involve the flexible codification of the rights, responsibilities, and obligations of each participant through the execution of smart contracts via Blockchain technology.

B-RAN is based on the O-RAN architecture, which provides significant benefits with regard to proprietary counterparts. O-RAN decreases capital expenditures (CAPEX) by fostering a successful ecosystem of several vendors that benefits from economies of scale, improves network efficiency and performance, and allows the integration of novel network capabilities. Specifically, the O-RAN open interfaces remove the need for a single manufacturer and enable collaborative installations with several vendors, hence fostering a more competitive and dynamic supplier ecosystem. The use of open software and hardware reference designs facilitates accelerated innovation by fostering a more extensive ecosystem. The native cloud feature of O-RAN allows for the implementation of scale-out designs, which prioritize capacity, dependability, and availability, as opposed to costly scale-up solutions. Finally, O-RAN decreases operational expenditure (OPEX) via the use of RAN automation. O-RAN incorporates embedded intelligence across the whole RAN architecture and utilizes advanced machine learning technologies to greatly automate operational network operations. This leads to a reduction in operational activities and thereby lowers OPEX.

In addition to CAPEX reduction, O-RAN enables continuous monitoring of network performance and resources, enabling real-time closed-loop control with little human interaction. O-RAN will possess the intrinsic capability to provide effective and optimal radio resource management via closed-loop control, hence improving network performance and enhancing user experience, even for very intricate networks. The interactions between Non-RT RIC and Near-RT RIC may be used to enhance and refine control algorithms, namely those pertaining to load balancing, mobility management, multi-connection control, QoS management, and network energy conservation. Lastly, O-RAN simplifies the process of incorporating new network functionality by means of easy software updates, using its inherent cloud infrastructures.

## 3.1 NANCY Rationale and Vision

To establish a durable, adaptable, and widely accessible energy-efficient network for use in B5G systems, which guarantees robust security and privacy measures, it will be necessary to monetize the

currently underutilized resources contributed by both individual and corporate entities. This will entail the implementation of innovative network technologies and models, as well as a reassessment of the information theoretical framework, traditional network design principles, and architectures. In the forthcoming era of beyond 5G, it is anticipated that 5G networks will undergo a transformation from serving as universal resource managers to becoming fully adaptive distributed computers, while simultaneously providing highly reliable and trustworthy connectivity services.

The realization of AI-assisted blockchain wireless radio access beyond 5G networks necessitates the development of a versatile, expandable, and robust machine learning-based orchestration framework, innovative blockchain and attack models, a groundbreaking network information theory approach, as well as the creation of advanced technology components. The aforementioned technologies encompass NFs that facilitate typical network functionalities, blockchain and cell-free radio access mechanisms, AI-driven resource and network orchestration, distributed and decentralized blockchain approaches that are bolstered by multi-access edge computing (MEC), and proactive self-recovery and self-healing mechanisms. Additionally, it is imperative to develop an appropriate experimental-driven performance evaluation and evaluation framework that is defined by the judicious selection of usage scenarios and relevant metrics. Furthermore, NANCY aims to identify crucial technological deficiencies and develop, refine, showcase, and evaluate the primary facilitators for the B5G RAN. The NANCY approach is founded on three distinct pillars, which have been clearly defined.

- The first pillar of NANCY proposes the implementation of a distributed and self-evolving B-RAN system that utilizes blockchain, PQC, and cell-free radio access mechanisms to enhance scalability, security, and privacy in a heterogeneous environment. This approach aims to optimize radio resource usage by introducing innovative strategies for range and service expansion, supporting new use cases and applications, and leveraging underutilized spectrum.
- The second pillar of NANCY aims to develop an AI-based wireless RAN orchestration that is Pareto-optimal, maximizing energy efficiency and trustworthiness while supporting ultra-high availability and diverse application requirements. The proposed solution also optimizes network topology and management, enables device collaboration and collaborative sensing, and allows for reproducibility and explainability of system-level and network-level AI models. Ultimately, this approach aims to transform B5G RANs into intelligent platforms, creating new service models for telecom/ISP and individual providers.
- The third pillar of NANCY involves the implementation of a distributed MEC system that aims to achieve near-zero latency and high computational capabilities at the edge of the network where data is generated. This will be achieved through the use of social-aware data and AI model caching, as well as task offloading. The ultimate goal of this approach is to transform B5G verticals into intelligent and real-time flexible and reliable platforms.

In order to achieve the three visionary pillars and corresponding objectives, NANCY will undertake a significant number of meticulously planned and coordinated research and development tasks. These tasks will involve analytical and fundamental studies, algorithm and signal processing, resource management strategy, and network modules interface design, as well as network architecture and model-based and data-driven optimization. The aforementioned objectives will be achieved through the demonstration, validation, and evaluation of key technological breakthroughs, including innovations, theoretical findings, and techniques in order to:

- Empirically verify the theoretical discoveries and technological advancements.
- Conduct a comprehensive evaluation of the practical limitations and obstacles associated with the implementation of AI-assisted B-RAN in a real-life operating environment. The assessment will be carried out through both qualitative and quantitative analyses.

- Evaluate the practicability of the suggested framework and the amalgamation of its constituent parts and features.
- Identify potential accelerators for the adoption of AI-aided B-RAN in the roadmaps of networks beyond 5G. Additionally, it explores potential limitations that may act as showstoppers and proposes ways to overcome the associated obstacles.

## 3.2 NANCY Enabling Technologies

The consortium of NANCY possesses a variety of interrelated technologies that are poised to achieve greater levels of advancement. The aforementioned objectives will be achieved through the adoption, extension, combination, and transformation of these technologies. The primary focus of these concerns is on software components, with particular emphasis on resource orchestration, virtualization, security, trust, and predictive analytics. In addition, the technologies that have been implemented encompass both hardware components, such as 5G deployments, and software solutions that ensure seamless interoperability, such as the IO Toolkit Generator. Additionally, ML tools, virtual simulation environments, and optimization algorithms have also been incorporated. All of them are employed in the implementation of the frameworks and components of the NANCY architecture layers.

### 3.2.1 Blockchain

Blockchain will be used for increasing security and traceability in the heterogeneous B5G wireless network that NANCY will propose. More specifically, blockchain will benefit NANCY with the following characteristics and functionalities:

- Security and privacy of users and devices, by means of different cryptographic schemes, and permission and identity management.
- Automated and traceable secure transactions, by means of smart contracts.
- Data integrity and security mechanisms through a Practical Byzantine Fault Tolerance (PBFT) consensus.

Task 5.2 and Task 5.3 will also produce insights towards the B-RAN scalability.

Pillar I has a major dependency on blockchain technologies. Namely, blockchain, together with PQC and cell-free radio access mechanisms must provide the basis for a distributed B-RAN for dynamic scalability, security, and privacy in a changing and heterogeneous environment. In the case of blockchain, this directly connects with some of the outcomes and results key to the project, e.g., R3 “A novel security and privacy toolbox that contains lightweight consensus mechanisms, and decentralized blockchain components” and R4 “Realistic blockchain and attacks models and an experimental validated B-RAN theoretical framework.

Blockchain, through the use of smart contracts among other mechanisms, is also a fundamental enabler for transparently and dynamically registering the multi-vendor offerings for resource management that users and stakeholders in general can request (or provide). These resources can include radio, network, edge, cloud or others and converge with the idea of an O-RAN in which catalogues can be provided – and contractually bonded when it comes to e.g. SLA and rates – by these operators, offering other participants differently priced resource “menus”. Blockchain minimizes, securely, the time needed for reaching service agreements and eliminates the need for third-party intermediaries. These must be done through lighter consensus algorithms and, when applicable, MEC.

The blockchain developments in NANCY will contribute mainly to KVIs:

- Block throughput
- Probability of attack

### 3.2.2 Multi-access Edge Computing

MEC is one of the major paradigms of current and future B5G networks. It is one of the main NANCY Pillars, which without it, performance goals in terms of latency and computation would be impossible to achieve. In particular, MEC will be used in NANCY to attain:

- Reduced latency and increased computational resources, by distributing MEC nodes in high-demand places, enabling task-offloading strategies and cache mechanisms of services close to the end-users.
- Optimized flexibility and resource allocation, using MEC nodes as valuable resources to offer to other operators and vendors and offer mobility of services among available MEC nodes supported by AI decision engines.
- Enhanced security, enabling distributed locations to gather numerous information about potential threats, which can be correlated, as well as providing infrastructure to enforce countermeasures.

MEC represents the Pilar III of NANCY. Its main objective is to aid other modules and components of the architecture to enhance their functionality by granting reduced latency and computational resources to constrained devices or to other operators, allowing the deployment of services as close to the end-user as possible. Task offloading (R14) is one of the main concerns of NANCY that implies the use of the MEC that, together with user-centric caching mechanisms (R15), focuses on granting seamless low-latency services. Also, B-RAN orchestration (R7) will leverage MEC nodes and resource optimization engines (R8) to select the best placement and mobility of services to keep latency low and to instantiate offloaded tasks in the best locations. Finally, security is also enabled by the MEC, lightweight consensus mechanisms and decentralized blockchain components (R3) will use the inherited distributed topology of MEC nodes to perform their operations. In addition, MEC nodes will serve as a perfect place to gather data, extract metrics, perform anomaly detection, and enforce countermeasures (R13).

The MEC nodes in NANCY will contribute mainly to KVIs:

- Security
- Ultra-high reliability
- Network and learning latency minimization
- Ultra-high scalability and flexibility
- Bandwidth saving and traffic reduction
- Dynamic reusability
- User-centric services

### 3.2.3 Quantum Key Distribution

Blockchain technology has been widely recognized as a highly transformative and groundbreaking innovation over the past decade. However, it is important to acknowledge the potential threat posed by quantum computing, a forthcoming technology that has the capability to compromise the security measures that blockchain offers. The potential of quantum computing technology poses a significant threat to the security of systems that depend on specific mathematical methods for safeguarding data, including the blockchain technology presently employed. The transmission of data over electronic means between two locations exposes it to the risk of interception.

Employing public key encryption to secure the data during transit does not guarantee absolute protection, since it remains susceptible to a potential assault known as "harvest now and decrypt later." This implies that an assailant methodically captures the encrypted data during its transmission, with the intention of deciphering it at their convenience in the future, when quantum computers have adequate computational capabilities to overcome cryptographic algorithms. The urgency of this issue is increasing due to the rapid advancement of quantum computing, which has the potential to significantly decrease the time required to decode data that is safeguarded using public key encryption.

The utilization of quantum key distribution (QKD) technology capitalizes on the principles of quantum physics, enabling two entities to establish mutual consensus on a secret key while also detecting any potential interception attempts by a third party during the key agreement procedure. QKD presently possesses the capability to sustain mission-critical applications within urban regions, where relevant, in conjunction with post-quantum cryptography through a hybrid methodology. The integration of QKD into a hybrid framework for achieving quantum resistance holds the potential to provide enduring security, hence thwarting any attempts to harvest and decrypt the encrypted data that relies on public key encryption.

The preservation of data security is a significant obstacle presented by the swift advancement of contemporary information technology. The storage of sensitive data on remote, cloud-based servers has witnessed a significant rise, hence elevating the importance of ensuring secure access to this data. The establishment of secure data transmission is contingent upon the utilization of encryption techniques to safeguard the integrity and confidentiality of information transmitted across public networks. The secure sharing of data using QKD has emerged as a critical commercial factor for businesses.

The processing of data is facilitated by core banking software and video conferencing tools across expansive networks. QKD represents an initial stride in the direction of eliminating the reliance on public-key assumptions within blockchain applications. The utilization of this mechanism facilitates the dissemination of confidential cryptographic keys that play a crucial role in safeguarding extremely sensitive information, which holds significant importance across several industries. Data confidentiality is a crucial aspect of safeguarding sensitive information in several areas such as banking, defense, utilities, and health. Additionally, it plays a vital role in protecting the important infrastructure that supports the functioning of smart cities and smart energy grids.

The fundamental basis of security in QKD lies in the process of encoding individual bits of the key onto single photons, which are sent via conventional optical fibers as an example. The act of reading or replicating the photons results in a modification of their encoding, so enabling the verification and assurance of the confidentiality of each key. It is neither possible to divide a solitary photon into constituent particles, nor can it be replicated without inducing modifications to the encoded information it carries. The act of cloning, as discussed in the aforementioned no-cloning theorem, is explicitly forbidden. The aforementioned feature facilitates the implementation of robust security measures inherent in QKD.

Permissioned blockchain networks frequently handle substantial volumes of sensitive data. While the intended audience for this information may consist of different entities within the network, it is imperative to ensure the preservation of data confidentiality during the transmission process. At present, the safeguarding of data secrecy relies on the implementation of conventional public-key cryptography systems. However, it is anticipated that these measures will be inadequate in mitigating the threat posed by a quantum-capable eavesdropper in the future.

By using QKD, networks can enhance the security of their communication infrastructure against the wide range of cyber threats existing now, as well as potential future threats. Currently, hackers employ methods such as data harvesting and decryption to retain data, intending to decode it in the future when they acquire the necessary computational power through advancements in supercomputing, the development of quantum computers, or the identification of novel cryptanalysis techniques. QKD ensures the security of data that necessitates long-term protection, not only in the current information technology environment but also in anticipation of the forthcoming quantum era.

### 3.2.4 Post-quantum cryptography

#### *3.2.4.1 Quantum threats*

Our connected world relies on information technologies (IT), cryptographic algorithms, and public key infrastructure (PKI) schemes for secure, confidential, and non-refutable transactions to prevent fraud, to provide trust and protect privacy. But a quantum revolution is on the horizon. Quantum computing is the most noticeable example of how the use of quantum physics can perform calculations that are far beyond what a classical supercomputer will ever be able to achieve. While this will benefit many fields and industries and lead to many welcome innovations, it will render some of today's most widely used cryptography obsolete and therefore poses a severe security risk.

Fortunately, already new cryptographic routines, so-called post-quantum cryptography (PQC) that resist the upcoming quantum threat are being developed. The transition toward quantum-resistant systems and solutions, which will require the upgrade of such a core security function as the underlying cryptographic routines, will be a very long and complex process. Therefore, there is some urgency to start with the first steps for the necessary transition and to ensure IT system resilience.

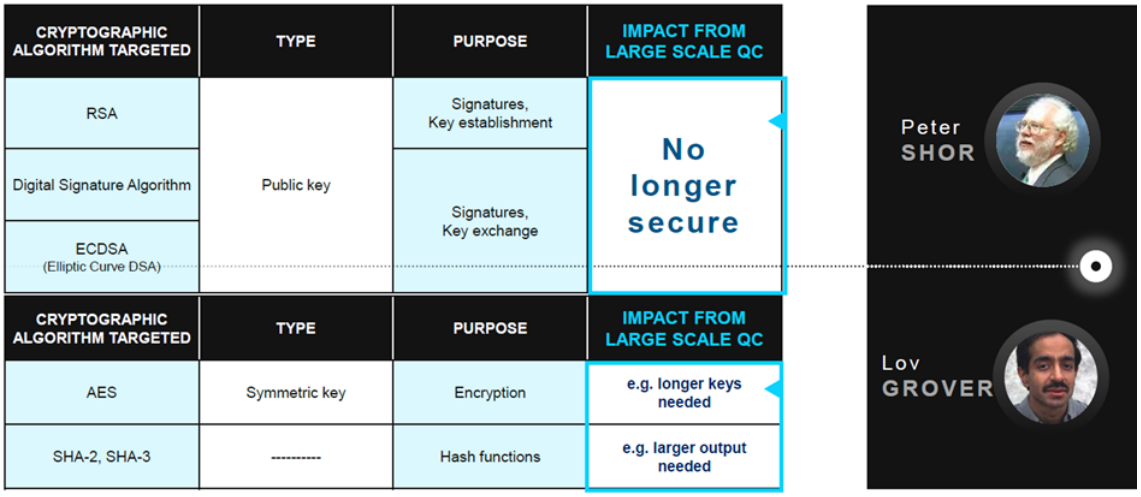


Figure 2: Cryptography algorithms and their impact from Quantum computers.

Figure 2 summarizes the different existing cryptography algorithms and their impact on Quantum computers. In the cases of symmetric cryptography (e.g., advanced encryption standard - AES) and hash functions (e.g., secure hash algorithm - SHA), the related algorithms would be quantum-safe with adapted key and digest sizes. Unfortunately, the currently used public key cryptography (Rivest–Shamir–Adleman – RSA algorithm, elliptic curve digital signature algorithm - ECDSA) will be no longer secured.

### *3.2.4.2 Post-Quantum Cryptography*

#### 3.2.4.2.1 SHOR'S ALGORITHM

Shor's algorithm [36] is a quantum computer algorithm for finding the prime factors of an integer. It was developed in 1994 by the mathematician Peter Shor and shows that a future quantum computer with a sufficient number of qubits can achieve an exponential speed-up to make it feasible to break today's typical PKI schemes based on RSA, ECC or Diffie-Hellman key exchange, which are at the heart of today's digital transactions, data security and confidentially of communications.

#### 3.2.4.2.2 NIST PQC standardization process

As we are on the brink of entering the quantum computing age, the race to find new quantum-resistant cryptography started already many years ago. Most prominent and well-advanced is the public competition launched by National Institute of Standards and Technology (NIST) to have a new PQC standard by 2024 [37]. The selected algorithms target the two use cases Key Encapsulation Mechanism (KEM) and Digital Signature.


Figure 3: NIST procedure to define PQC

In 2022, NIST announced that a total of four algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.

Table 1: NIST third round standardization candidates

| | Key Encryption / KEM | Signature |
|---|---|---|
| Primary algorithms | o CRYSTALS-KYBER | o CRYSTALS-Dilithium |
| Additional algorithms | | o FALCON<br>o SPHINCS+ |

CRYSTALS-KYBER for key-establishment and CRYSTALS-Dilithium for digital signatures are both lattice-based asymmetric crypto schemes and were selected for their strong security and excellent performance, and NIST expects them to work well in most applications.

Not part of the competition are several existing stateful hash-based signature algorithms, which are considered quantum-safe by default (same as symmetric cryptography with sufficiently long keys) and are already standardized. However, they are only suitable for specific applications and not for general use, and especially they are also not suitable for memory and performance-restrained systems, such as the microchips used in smartcards.

#### 3.2.4.2.3 Other National standardization initiatives

The need for an internationally harmonized approach is acknowledged by all national standardization institutes and organizations.

In the US, the White House mandated federal agencies to define post-quantum trajectory for critical systems by summer 2022 and NSA plans a transition for National Security Systems for 2025-2033.

BSI in Germany, the Federal Office for Information Security, is also part of an international network in the field of cryptography and closely follows the NIST standardization process.

1. As the practical implementations of the new PQC schemes have not been tested yet as extensively as the classical schemes known for decades, there remains a concern that cryptanalytic attacks or maybe also implementation flaws allowing side-channel or error attacks by classical computers could emerge.
2. BSI therefore recommends the use of hybrid protocols, i.e., a combination of classical and quantum-resistant primitives, as this combination should protect both against conventional and quantum threats. BSI also calls for 'crypto-agility', to make the cryptographic mechanisms as flexible as possible in order to react flexibly to all conceivable developments and have the options to replace algorithms in the future that no longer guarantee the desired level of security.

In France, the National IS security agency ANSSI proposes a 3-step transition period to Post Quantum Security to be concluded in 2030:

1. Phase 1 (2022-2025): hybridization to provide some additional post-quantum defence-in-depth to the pre-quantum security assurance.
2. Phase 2 (2025-2030): hybridization to provide post-quantum security assurance while avoiding any pre-quantum security regression.
   Phase 3 (2030): optional standalone post-quantum cryptography

#### 3.2.4.2.4 CRYSTALS-KYBER & CRYSTALS-Dilithium

Cryptographic Suite for Algebraic Lattices (CRYSTALS) [38] encompassed two cryptographic primitives that both were selected by NIST:

- CRYSTALS-Kyber is a key encapsulation mechanism;
- CRYSTALS-Dilithium is a digital signature scheme.

CRYSTALS is based on a structured lattice and the so-called "Learning With Error (LWE)" problem, which is mathematically hard to solve. As with RSA (prime factorization) or ECC (discrete logarithm), the related private and public keys are relatively easy to compute, but finding the fitting private key for a known public key is both for classical and any future quantum computer virtually impossible.

Concerning the resilience of blockchain wallets as discussed above, NANCY is focusing on Crystals-Dilithium PQC Signature.

### *3.2.4.3 Quantum-Safe Blockchain*

Today's Blockchain technology uses Public-key cryptography (i.e., like the ECDSA scheme) and a hash function (i.e., SHA) for signing transactions.

#### 3.2.4.3.1 Hash function

The hash function SHA-256 is, to date, considered quantum-safe, which means that there is no efficient known algorithm, classical or quantum, that can invert it.

While there is a known quantum algorithm, namely Grover's algorithm [39], which performs "quantum search" over a black-box function, as of today, SHA-256 has proven to be secure against both collision and preimage attacks. A conservative approach would be to increase the digest size (e.g. moving from SHA-256 to SHA-384) but, as of today, this is not considered a requirement within the NANCY project.

#### 3.2.4.3.2 Public Key cryptography

Public Key cryptography, in which security is based upon the difficulty of solving the discrete logarithm, is vulnerable to quantum computing and must be replaced with a quantum-resistant scheme.

Public-key cryptography is used to establish a distributed consensus of trust, which is essential for ensuring security and privacy in Blockchain. While the chain itself is relatively secure, the “wallets” at the endpoints have already been demonstrated to be "hackable," and quantum computing techniques will further expose the network to fraudsters and criminals.

The solution to the blockchain wallet vulnerabilities problem is to create quantum-safe crypto wallets secured by a PQC algorithm approved by NIST [37].

### *3.2.4.4 Secure Communication*

PQC plays a crucial role in ensuring the security of communication in the face of potential advancements in quantum computing. The Open Quantum Safe (OQS) project is committed to advancing quantum-resistant cryptography within an open-source framework. Within the OQS initiative, the primary emphasis is on two pivotal areas: firstly, the creation of liboqs, a dedicated open-source C library tailored for cryptographic algorithms resilient to quantum computing, and secondly, the integration of prototypes into a range of protocols and applications, including the widely utilized OpenSSL library. These tools not only bolster research efforts but also contribute to the pursuits of other interested individuals or groups. The development of OQS featuring multiple releases concentrates on different aspects of quantum-safe cryptography, regularly updating to incorporate new advancements and improvements in this field.

Integrating the OQS library into the OpenSSL framework to create secure communication elements is a critical step. The challenge posed by the community’s limited focus on specific operating systems, combined with the rapid evolution of this technology, underscores the need for broader collaboration and adaptation across various platforms to ensure widespread adoption and effectiveness.

### *3.2.4.5 Cyber resilience with Crypto Agility*

As recommended by National Security Agencies (i.e., BSI, ANSSI, etc.), a pivotal property to achieve long-term security and cyber-resilience is crypto agility applied to the security equipment or devices in charge of cryptographic computation. It combines two essential features:

- OS Security update, which supports a secure update mechanism to patch OS program code and crypto libraries for devices/equipment already issued and on the field.
- Crypto versatility, which depicts the capability and agility to support different cryptographic mechanisms and standards and therefore the possibility to switch to alternative cryptography in electronic documents already issued, without causing significant disruption to the infrastructure.

### *3.2.4.6 Project Results and KPI/KVI*

Contribution to the Project Results:

- [R1] B-RAN architecture
- [R3] A novel security and privacy toolbox that contains lightweight consensus mechanisms, and decentralized blockchain components
- [R4] Realistic blockchain and attacks models and an experimental validated B-RAN theoretical framework
- [R5] Quantum safety mechanisms to boost end-user privacy

Contribution to KPIs/KVIs:

- Key generation performance duration
- Signing performance duration
- Verification performance duration

### 3.2.5 Artificial intelligence

The realization of AI-assisted Blockchain wireless radio access B5G networks necessitates the development of a versatile, adaptable, and robust ML-based orchestration framework, innovative Blockchain and attack models, a ground-breaking network information theory approach, and the creation of state-of-the-art technology components. The aforementioned features encompass NFs that facilitate the implementation of shared network functionalities, Blockchain and cell-free radio access mechanisms, AI-driven resource and network orchestration, decentralized and distributed Blockchain approaches that are reinforced by MEC, and pre-emptive self-recovery and self-healing mechanisms. Additionally, it is imperative to devise a performance evaluation and assessment framework that is experimentally driven and defined by the appropriate selection of usage scenarios and pertinent metrics. Furthermore, NANCY shall detect the essential technological deficiencies and devise, enhance, exhibit, and evaluate the principal facilitators for the B5G RAN.

NANCY aims to develop an AI-based wireless RAN orchestration that is Pareto-optimal, maximizing energy efficiency and trustworthiness, supporting ultra-high availability and applications with diverse requirements, optimizing network topology and management, enabling device collaboration, as well as collaborative sensing perspective. Additionally, the proposed system allows for the reproducibility and explainability of system-level and network-level AI models, and transforms B5G RANs into intelligent platforms, opening up new service models for telecom/ISP and individual providers. In more detail, the main challenges of NANCY with a focus on the intelligent functionalities of the network include:

- Support hyper-dense networks with dynamically changing topologies.
- Drastically increased complexity due to large-scale networks and large data volumes.
- Maximize the network's energy efficiency.
- Support ultra-high availability.
- Support applications with diverse requirements.
- Optimize network topology and management.
- Enabling device collaboration.
- Enabling anomaly detection and provisioning at the network level as well as self-healing and self-recovery mechanisms.

To overcome the aforementioned challenges, NANCY will develop a portfolio of AI-enabled components that will cooperate in order to transform B5G infrastructures into intelligent platforms capable of integrating ultra-reliable connectivity and providing high-energy efficiency. Specifically, the major intelligent results of NANCY are:

- Data-driven real-time optimization with ML to improve network deployment, management, and resource reuse [R7].
- AI-based slices instantiation to support applications with diverse requirements [R7].
- Support dynamic cells by means of joint node association/pairing and resource allocation with minimum complexity and side-information requirements [R8].
- Model-based optimization to improve known analytical models of limited accuracy [R9].

- An experimentally driven RL-based optimization framework of B-RAN [R10].
- AI-enabled semantic and goal-oriented communication schemes for beyond Shannon excellence [R11]
- An explainable AI framework that boosts trustworthiness [R12].
- Proacting mechanism for anomaly detection, self-healing and self-recovering [R13].
- Novel battery and computational-capabilities aware offloading policies that exploit the increased DoFs (Degrees of Freedom) provided by B-RAN [R14].

### 3.2.6 Virtualization

Considering the challenges posed by sophisticated applications and the increasing demands for connectivity, processing, and storage, the following NANCY pillars play crucial roles: Distributed and self-evolving B-RAN, AI-based wireless RAN orchestration, and distributed MEC. These pillars address scalability, security, privacy, energy efficiency, availability, latency, and computational capabilities, enabling networks to meet the requirements of advanced applications and effectively utilize radio resources. The use of an AI virtualizer (R8) for the exploitation of said resources is a key point in the development of NANCY, as it addresses the three main pillars of the project, providing a potential improvement in resource utilization using distributed AI techniques while providing support to the use of high computational capabilities at the edge.

In this context, the AI Virtualizer is an advanced solution designed to analyze the computational resources required for specific tasks and facilitate optimal offloading decisions. It enables the decision of whether the capacity should be offloaded totally or partially, as well as the selection of the appropriate nodes to engage in the computation process. The objective is to maximize the overall system utilization within predefined limits, considering node capabilities and energy reserves. The integration of cutting-edge technologies such as network function virtualization (NFV), software defined networking (SDN), and slicing enhances the resource manager's flexibility.

These objectives align with several KPIs. Firstly, the focus on efficiently using computational resources aligns with the KPI related to resource utilization, which measures the effectiveness of resource usage. Furthermore, the integration of virtualization technologies reflects a focus on cost efficiency, aiming to optimize resource management and potentially achieve cost savings. The consideration of appropriate node selection and their capabilities implies a concern for fairness and equitable distribution of resources among different entities. Lastly, the objectives align with performance metrics such as response time, throughput, and quality of service, aiming to provide efficient and high-quality computational services.

The AI Virtualizer demonstrates its synergy with the existing slicing architecture. As detailed in [40], the Lifecycle of a Network Slice Instance holds significant importance in managing network slicing. The utilization of an AI Virtualizer directly impacts three out of the four main phases (Commissioning, Operation, and Decommissioning). By actively suggesting recommendations to the Slice Manager, the AI Virtualizer facilitates the seamless activation, deactivation, or modification of services, enhancing operational efficiency.

It is crucial to highlight the significance of employing virtualization techniques as a foundation for sliced services. Cloud management platforms such as OpenStack play a pivotal role in the successful deployment of network slices. These platforms provide the necessary infrastructure and management capabilities that are essential for slicing operations. The streamlined deployment and configuration processes offered by OpenStack are facilitated through REST API calls. OpenStack also offers a

comprehensive set of APIs, enabling seamless integration with various components and systems. This integration allows for the coordination between slicing management and orchestration systems, ensuring efficient management of the network slice lifecycle alongside the underlying OpenStack infrastructure.

Last but not least, novel virtualization solutions will be introduced to complement the existing infrastructure. Interfacing seamlessly with OpenStack, these solutions will serve as an effective means to improve further the latency and security KPIs at the edge of the network.

The ability for flexible deployment of network functions on-top of virtual resources has facilitated the exploitation of edge resources to the greatest extent. At the same time, existing cloud approaches are not a perfect fit for edge servers' deployments, as there is an increasing demand for lightweight virtualization solutions at this network layer. In this scope, NANCY will offer a novel virtualization solution for ARM edge servers based on VOSySmonitor. This technology, relying on TrustZone, is able to provide hardware-isolated compartments ideal for running lightweight virtual machines where to offload network functions or mining workloads, thus making a valuable component in the AI Virtualizer architecture.

## 3.3 NANCY Overall Architectural Approach

The advent of the 5G systems in the wireless domain has led to a growing need for pioneering technological advancements that will serve as the foundation for B5G or 6G systems. Cisco has projected a significant surge in global mobile data-traffic, estimating an increase of over 10 times from 7.2 to 77.5 EB/month between 2017 and 2022. This trend is expected to follow an exponential pattern in the 2020s. Additionally, the number of networked devices is also anticipated to grow at a similar rate, reaching 28.5 billion by 2022 [41]. Furthermore, it is anticipated that forthcoming networks will possess an inherent capacity to accommodate an extensive and varied assortment of innovative usage scenarios and applications. These requirements will necessitate, in addition to exceedingly high data rates, the ability to be agile, flexible, available, reliable, and possess zero response time. Moreover, artificial intelligence will need to be integrated within a framework that prioritizes security and privacy. Virtual, artificial, and extended reality, as well as 3D printing, autonomous vehicles, and cyber-physical systems for intelligent transportation, smart traffic, Industry 4.0, and e-health, are among the highly anticipated use cases. 5G technology has incorporated various design principles that are transformative in nature, including the utilization of higher frequency bands such as mmW and THz, network densification, virtualization, and orchestration. These principles are intended to improve scalability, flexibility, and resource management, leading to the emergence of more heterogeneous and complex RANs. In the absence of well-crafted inter-operation, mobile network operators (MNOs) are compelled to depend on their individual infrastructures and spectra to provide data, which frequently results in duplication, redundancy, and inefficiency. A significant proportion of APs that are currently in use by businesses or individuals have not been integrated into the existing architecture of RANs and consequently are not being utilized to their full potential. Currently, UEs are restricted from accessing APs belonging to operators other than their own, despite the possibility of improved link quality and economic benefits. The current situation of increasing traffic demands, along with the inadequate utilization of available spectra and infrastructure resources, provides impetus for the creation of a new network architecture. This architecture aims to integrate various service providers and clients, thereby revolutionizing the inflexible network access paradigm that is currently prevalent.

The evolution of networks towards B5G entails the utilization of underutilized resources and the development of novel concepts that facilitate the emergence of new DoFs. This is achieved by integrating all modules into a network architecture that is both feasible and scalable, while also

providing personalized, multi-tenant, and continuous protection based on security, privacy, and trust mechanisms. These mechanisms are particularly crucial in highly virtualized software environments and must be considered from an end-to-end perspective. NANCY aims to conduct research, create a blueprint, and construct and authenticate the initial B-RAN in this context. The aim of NANCY is to fulfill the demands of the post-5G era through the presentation of an AI-driven B-RAN structure that is founded on the principles of SDN and MEC. We will identify the technologies that enable this architecture, establish a theoretical framework to accurately model and evaluate its performance, develop novel technologies and system concepts, and validate and optimize it using five testbeds.

NANCY will implement the fundamental structure of the O-RAN Alliance, which builds upon the 3GPP NR 7.2 split used in base stations. The described technique entails breaking out the functions of the base station into three separate units: the Central Unit (CU), the Distributed Unit (DU), and the Radio Unit (RU). In addition, O-RAN creates a linkage between intelligent controllers using open interfaces, easing the transfer of telemetry data from the RAN and enabling the implementation of control actions and policies. The O-RAN architecture consists of two RAN Intelligent Controllers (RICs) that perform network management and control tasks at both near-real-time and non-real-time time intervals.

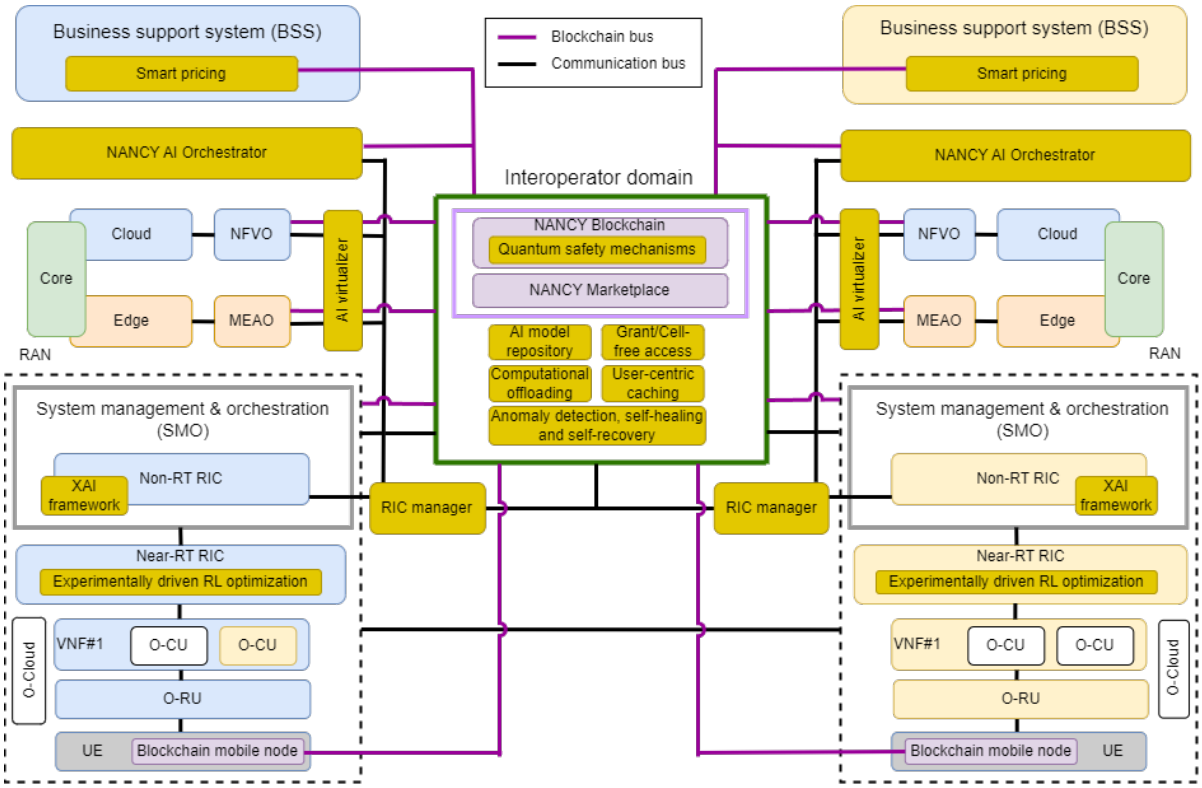


Figure 4: NANCY high-level network architecture.

Figure 4 provides a visual representation of the high-level architecture of the NANCY network. The illustration focuses on the linkages that exist between the NANCY architecture and the different components of the core, edge, cloud, and RAN. The core is deployed in the edge-to-cloud continuum, with the cloud being regulated by the network functions virtualization orchestrator (NFVO), and the edge being managed by the mobile edge application orchestrator (MEAO), respectively. In addition, the RAN component of the design, which uses the O-RAN architecture as its foundation, is shown by the black dashed line in the diagram. The NANCY components are shown in yellow and purple, with yellow representing network-oriented components and purple representing Blockchain-oriented components, accordingly. The blockchain is the most important technology that makes NANCY possible. This technology may be accessed by the many end users of the NANCY platform by way of

the marketplace that is located in the interoperator domain. The interoperator domain is the primary plane of the NANCY architecture. It is where all of the NANCY components that are deployed and shared amongst the various providers are stored. These components include the AI model repository, offloading, caching, anomaly detection, self-healing, and self-recovery methods. Other components are quantum safety and grant/cell-free access mechanisms.

In order to make use of the features described above that are made available by NANCY, every single operator has their own connection to the interoperator domain. In this course of action, some NANCY components are required to be installed on the premises of each operator, and as a result, the NANCY platform as a whole will contain numerous instances of each of these components. The NANCY AI orchestrator, the AI virtualizer, the RIC manager, the experimentally driven RL optimization mechanisms, the XAI framework, and the smart pricing policies are all examples of such components. These modules are required to provide the core capabilities of the NANCY platform and are thus essential. In particular, the AI orchestrator of each operator communicates not only with the components of the interoperator domain, such as the marketplace, computational offloading, caching, and other components, but also with the RIC manager and the AI virtualizer, in order to achieve the optimal instantiation and management of the resources of its operator. This is done in order to achieve the goal of achieving the optimal instantiation and management of the resources of its operator. In addition, the smart pricing module can be found inside the business support system (BSS), and it supplies the market with the policies that are required for the development and maintenance of smart contracts prior to their deployment on the blockchain. In conclusion, the XAI framework engages in communication with the non-RT RIC in order to provide insights that are explicable about the many components of network operations.

A detailed description of NANCY architecture is presented in D3.1 ‘NANCY Architecture Design’.

# 4 Reference Use Cases Overview

## 4.1 The Path from 5G to 6G

5G use cases are driven by the needs and requirements of Industry 4.0 verticals, acting as key enablers, and are designed to address specific challenges of these verticals. The deployment of 5G networks has already started to provide benefits in three major areas, also known as the 5G triangle:

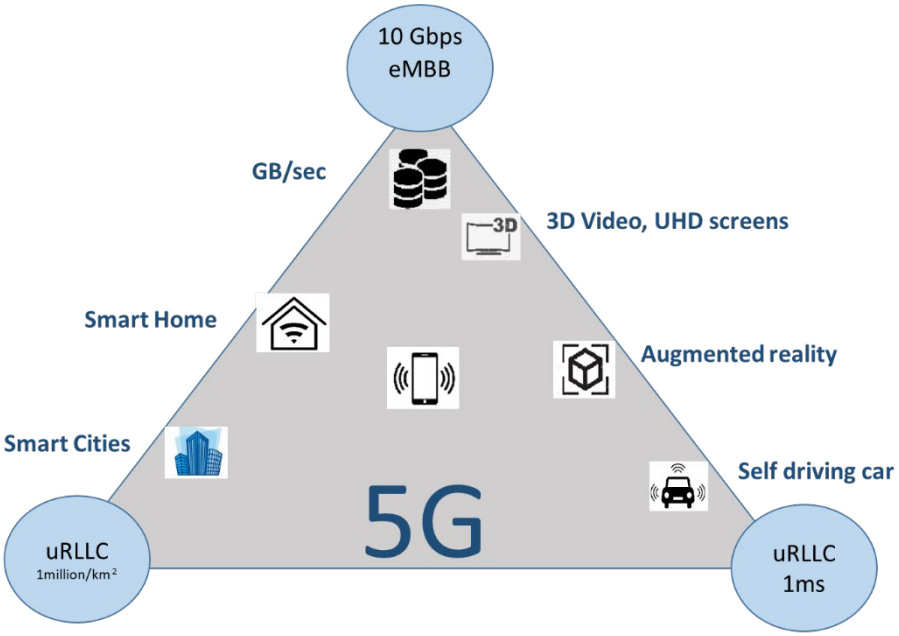


Figure 5: 5G Use Cases [42]

- uRLLC: Ultra Reliable Low Latency Communication use cases
- mMTC: Massive Machine Type Communication (IoT) use cases
- eMBB: Enhanced Mobile Broadband – high-speed use cases

The arrival of B5G technologies has enabled the emergence of a visionary approach with a vision of reshaping society's future. In this direction, the NANCY project envisions the role of B5G as a fundamental part in terms of societal evolution. Within the scope of the project, the NANCY consortium has identified a specific set of use cases that serve as a baseline for guiding the technical work that the NANCY Project supports. The first use case, **Enhanced Mobile Broadband (eMBB)**, focuses mainly on enhancing the capabilities of the previous generation wireless networks and communications by facilitating high-speed data transmission and offering a high-quality experience for the end-users. The **Ultra-Reliable Low-Latency Communications (URLLC)** use case corresponds to establishing of ultra-reliable communication networks for mission-critical applications like autonomous vehicles, which have witnessed increasing attention in recent years. Another critical use case that the NANCY project will showcase is the **Massive Machine-Type Communications (mMTC)**, which facilitates the continuous connectivity of a vast number of existing IoT devices, resulting in the growth of industrial automation and smart city infrastructure. The **mMTC-MBB** use case extends both eMBB and mMTC use cases by merging them in a single UC, thus offering effective mobile broadband services and machine-type communications. The **URLLC-MBB** use case investigates the combination of enhanced mobile broadband and ultra-reliable low-latency communications use cases, paving the way

for augmented reality and ground-breaking healthcare applications. The **URLLC-mMTC** use case, which is of particular significance in fields like smart factories and real-time infrastructure monitoring, leverages both use cases to facilitate seamless interaction among critical applications and a broad range of IoT devices. Overall, the aforementioned use cases epitomise the different prospects and challenges that B5G/6G technology holds for society.

The NANCY project will consider the following reference use cases:

- eMBB
- URLLC
- mMTC
- mMTC-MBB
- URLLC-MBB
- URLLC-mMTC

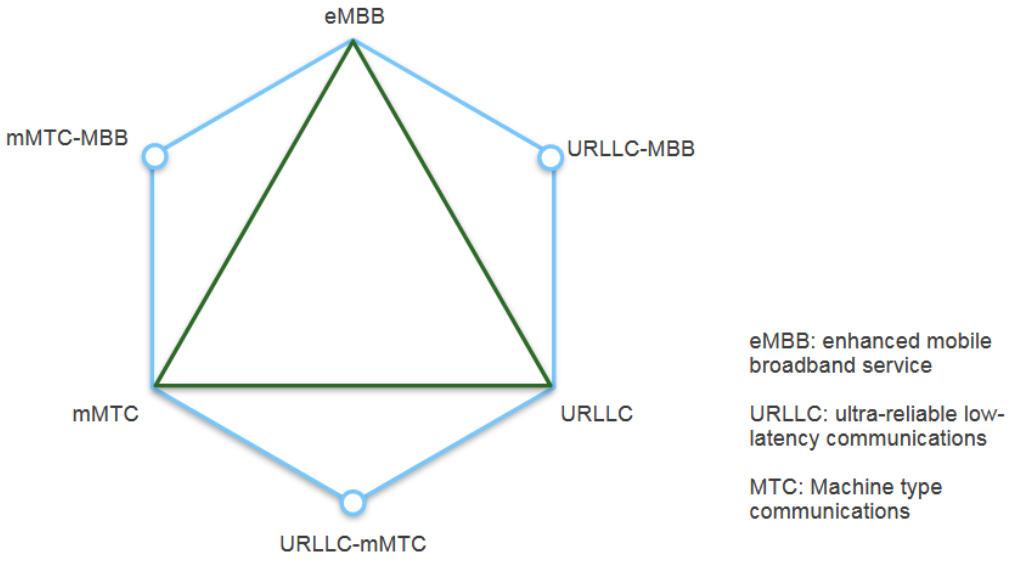


Figure 6: B5G/6G Reference Use Cases

### 4.1.1 Use Case#1: eMBB

#### 4.1.1.1 Use Case Overview

The eMBB use case (UC), derived from the Third Generation Partnership Project (3GPP), intends to surpass the limits of data throughput and enhance user experiences to unprecedented levels in contrast to the current 5G wireless networks. Endeavours in this direction, aim to meet the continuously increasing bandwidth requirements and needs of modern applications and usage scenarios. Notable examples of such situations are high-quality video streaming, virtual reality (VR), and gaming experiences since all the above aim for a significant amount of data to be transferred in parallel with almost zero latency.

#### 4.1.1.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Latency | < 5ms |
| Energy efficiency | energy consumption reduction by 20x compared to 5G |

| | |
|---|---|
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Security of wireless access for any traffic loaf/patterns | 99.99% |
| Ultra-high privacy with probability of successful attack | 10^-5 |
| Network and learning latency minimization | "almost-zero" latency |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Operation cost reduction | >30% |
| Bandwidth saving and traffic reduction | - |
| Complexity and overhead reduction | - |
| Block throughput | 10-20 operations/node/sec |
| Availability | 99.9999% |
| Signing | <10ms |
| Verification | <1ms |
| Communication chatter | -30% |
| Data efficiency (DE) improvement | >20% |

#### 4.1.1.3 Relevance to NANCY demonstrators

Italian massive-IoT testbed (Demonstrator #1): The eMBB use case is especially applicable to the massive-IoT testbed located in Italy. Specifically, it supports high-definition video streaming, IoT sensors and massive machine-type communications (MTC), guarantees stable connectivity for traffic management, strengthens security and privacy via encryption and PQC, caters to a variety of applications, and ensures continuous availability. These capabilities are vital for effectively finalizing the testbed, mitigating cyber threats, and providing real-time monitoring and responses.

Greek outdoor testbed (Demonstrator #3): The NANCY project's Greek outdoor demonstrator, which focuses on delivering interactive Augmented and Virtual Reality (AR/VR) material in an urban area, like the city of Athens, appears especially fitting to the eMBB (Enhanced Mobile Broadband) use case. The fundamental capabilities of the eMBB use case, offer a substantial number of vital features and characteristics such as extremely low latency, massive data rates, security, and privacy, preferably correspond to the demands of immersive AR/VR experiences. The efficient and seamless transmission of AR/VR content is guaranteed by eMBB's flexibility and resource allocation capabilities, providing support for CoMP scenarios. In this urban context, its capability of enabling smart pricing and optimizing connection ecosystems is essential to successful completion of performance KPIs associated with security, energy utilization, range expansion, scalability, and cost management.

### 4.1.2 Use Case#2: URLLC

#### 4.1.2.1 Use Case Overview

According to 3GPP standard the URLLC uc contributes significantly to the process of developing the 5G Wireless standard's specifications. In particular, URLLC main focus is to deliver communication services that are both fast and reliable. Mission-critical applications such as remote healthcare operations, autonomous driving, industrial automation, and public safety depend on this uc. Due to URLLC's dedication to delivering data with ultra-low latency and reliability, real-time applications benefit greatly and continue their seamless operation.

#### 4.1.2.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Security of wireless access for any traffic load/patterns | 99.99% |

| | |
|---|---|
| Ultra-high privacy with probability of successful attack | 10^-5 |
| Network and learning latency minimization | ("almost-zero" latency) |
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Operation cost reduction | >30% |
| Complexity and overhead reduction | - |
| Range expansion | Up to 100m |
| Security and privacy | High |
| Availability | 99.9999% |
| Key generation | <1ms |
| Signing | <10ms |
| Verification | <1ms |
| Data loss events | -10% |
| Data efficiency (DE) improvement | >20% |
| Latency | < 5ms |
| Reliability | 99.99999% |

#### 4.1.2.3 Relevance to NANCY demonstrators

Spain outdoor testbed (Demonstrator #2): The NANCY project's demonstrator is highly applicable to the URLLC use case as it focuses on offering ultra-low latency and high reliability in communication services. In particular, the testbed provides a URLLC network slice with guaranteed 1 ms latency, which aligns with URLLC's goal of supporting immediate and dependable communication. Featuring an emphasis on mission-critical applications the demonstrator of NANCY illustrates enhanced connectivity, energy efficiency, mobility management, and scalability. Therefore, the NANCY project's Spain outdoor testbed efficiently fulfills the URLLC use case's needs and objectives in the context of 5G specifications.

Greek outdoor testbed (Demonstrator #3): The aforementioned use case of URLLC is targeted to the fourth testbed of the NANCY project located in Greece, at the Athens city center. The demonstrator emphasizes offering innovative multimedia services in a metropolitan environment. In addition, Augmented and Virtual Reality (AR/VR) content implementation entails specialized network slices that are designed for distributing high-quality content at immense data rates in parallel with extremely low latency. To create an enjoyable AR/VR experience for end users, URLLC indicates to provide ultra-reliable connectivity with zero latency. The demonstrator addresses the objectives of URLLC by guaranteeing high data rates, near-zero latency, and the necessary flexibility to adapt to network resources, facilitating high-quality multimedia services in urban environments for users.

### 4.1.3 Use Case#3: mMTC

#### 4.1.3.1 Use Case Overview

The mMTC UC aims to highlight the connectivity requirements of multiple interconnected devices that entail low data rates regarding transmissions and can be considered energy efficient. The UC implementation can be found throughout numerous applications, including smart farming/agriculture and smart cities, thus offering new and promising concepts for their advancement. Regarding the vertical sector of digital agriculture, connected devices/sensors can monitor and respond to real-time changes in the growing conditions across wide regions. Therefore, it is feasible to make on-the-fly decisions that will prove beneficial to boost growth rates and improve digital agriculture. Additionally, multiple sectors and industries could capitalize on mMTC UC. Coordination of manufacturing

procedures and maintaining reliability are some indicative examples that mMTC can greatly contribute. The previously mentioned scenarios indicate how mMTC could impact sectors by facilitating real-time data gathering that strengthens productivity and capacity for decision-making. In conclusion, by utilizing this UC, several industries/sectors can benefit from interconnected sensors to facilitate personalized reactions, reduce time- consuming processes, and boost the overall effectiveness of their operations.

#### 4.1.3.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Security of wireless access for any traffic load/patterns | 99.99% |
| Ultra-high privacy with probability of successful attack | 10^-5 |
| Ultra-high reliability for a massive number of nodes with a probability of availability | in the order of 99.9999% |
| Network and learning latency minimization | "almost-zero" latency |
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Operation cost reduction | >30% |
| Availability | 99.9999% |
| Key generation | <1ms |
| Signing | <10ms |
| Verification | <1ms |
| Latency | < 5ms |
| EE improvement | 37-41% (AI service orchestration) |

#### 4.1.3.3 Relevance to NANCY demonstrators

Spain outdoor testbed (Demonstrator #2): The Spanish demonstrator is highly applicable to the mMTC use case in the context of 5G standards due to the way it supports the objective of enabling connectivity for a significant number of interconnected devices with reasonable data rate needs while emphasizing energy efficiency by showcasing the skills necessary for quickly connecting and monitoring a large number of devices. It can be significant in applications like smart cities and smart farming/agriculture, where interconnected equipment and sensors monitor real-time conditions and facilitate instantaneous decision-making, accelerating growth and production rates. By offering real-time data gathering and decision-making capability, the demonstrator illustrates how the aforementioned UC can drastically benefit industries and enhance overall efficiency through interconnected sensors and devices.

### 4.1.4 Use Case#4: mMTC-MBB

#### 4.1.4.1 Use Case Overview

The mMTC-MBB UC combines two different UCs and aims to provide both extensive connection and enhanced broadband services. The main goal of this UC is to enable high-bandwidth applications like enriched multimedia experiences and video streaming while also delivering dependable connectivity services for a wide variety of IoT devices.

#### 4.1.4.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Security of wireless access for any traffic load/patterns | 99.99% |
| Ultra-high privacy with probability of successful attack | 10^-5 |

| | |
|---|---|
| Ultra-high reliability for a massive number of nodes with a probability of availability | in the order of 99.9999% |
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Operation cost reduction | >30% |
| Bandwidth saving and traffic reduction | - |
| Availability | 99.9999% |
| Key generation | <1ms |
| Signing | <10ms |
| Verification | <1ms |
| Data efficiency (DE) improvement | >20% |
| Latency | < 5ms |
| EE improvement | 37-41% (AI service orchestration) |

#### 4.1.4.3 Relevance to NANCY demonstrators

Spain outdoor testbed (Demonstrator #2): The mMTC-MBB use case, which combines the mMTC and MBB use cases, shows great relevance to the second demonstrator of the NANCY project (Spanish outdoor testbed). Particularly, the Spanish testbed is a key component of the project's validation efforts considering it delivers a suitable environment for evaluating complex communication characteristics. The proposed setup of the demonstrator facilitates the evaluation and validation of network capabilities intended for delivering broad connections and optimized broadband services. The testbed's capabilities, which consist of a single AP/BS and vehicles outfitted with portable 5G modems, enable the exploration of scenarios that cater to applications with high bandwidth such as optimized multimedia experiences and video streaming while also ensuring steadfast connectivity services for multiple IoT devices.

### 4.1.5 Use Case#5: URLCC – mMTC

#### 4.1.5.1 Use Case Overview

The URLLC-mMTC UC integrates two independent use cases, namely URLLC and mMTC. Both UCs combined can provide ultra-reliable, low-latency communication requirements and massive connectivity needs. In this direction, the particular UC aims at applications that depend highly on a significant level of reliability and connectivity across multiple devices. Power grids, healthcare, and IoT are a few indicative domains. Concerning the IoT environments, URLLC-mMTC UC increases their primary operation offering reliability, optimized procedures, and significant enhancement in their overall performance. Additionally, regarding the management of the power grid, enables real-time monitoring, as well as an efficient resource allocation policy. Finally, as for the healthcare sector, remote monitoring systems allow for continuous data collecting, improving treatments for patients.

#### 4.1.5.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Security of wireless access for any traffic load/patterns | 99.99% |
| Ultra-high privacy with probability of successful attack | 10^-5 |
| Ultra-high reliability for a massive number of nodes with a probability of availability | in the order of 99.9999% |
| Network and learning latency minimization | ("almost-zero" latency) |
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |

| | |
|---|---|
| Dynamic reusability | estimated reusability rate >90% |
| Operation cost reduction | >30% |
| Bandwidth saving and traffic reduction | - |
| Complexity and overhead reduction | - |
| Range expansion | Up to 100m |
| Availability | 99.9999% |
| Key generation | <1ms |
| Signing | <10ms |
| Verification | <1ms |
| Data loss events | -10% |
| Data efficiency (DE) improvement | >20% |
| Latency | < 5 ms |
| Resource utilization rate | >99.99% |
| EE improvement | 37-41% (AI service orchestration) |
| Reliability | 99.99999% |
| E2C EE improvement | 37-41% (AI service orchestration) |

#### 4.1.5.3 Relevance to NANCY demonstrators

Italian massive-IoT testbed (Demonstrator #1) The URLLC-mMTC use case has a lot of relevance to the Italian Massive IoT demonstrator. In particular, the use case is relevant for a wide range of industries sectors including logistics, healthcare, and the Internet of Things, and combines the essential components of ultra-reliable low-latency communication and immense connection. The demonstrator serves as an excellent example of the need for high availability, security, and support for a broad service diversity across the seaport it highlights how novel approaches like quantum coding and centralized B-RAN (CB-RAN) are currently used to effectively tackle these challenges. The objectives of this use case are perfectly aligned with the Italian demonstrator's capabilities, making it the most suitable platform to validate and indicate the NANCY project's capabilities in these areas of high-quality connectivity, durability toward cyber threats, and support for a multitude of applications.

Spain outdoor testbed (Demonstrator #2): The Spanish outdoor demonstration encompasses many points of relevance to the URLLC-mMTC use case. The URLLC-mMTC integrates the requirements of extensive connectivity and ultra-reliable, low-latency communication, which are essential for a wide range of applications, notably the IoT, healthcare, and power grid administration. Through an accurate assessment and confirmation of these crucial requirements employing the Spanish outdoor testbed, reliable, standardized communication protocols can be stipulated, resulting in increased performance in IoT contexts. This corresponds to the testbed's capabilities, giving it the perfect setting to demonstrate how the NANCY project could offer real-time monitoring, effective resource management, and continuous data collection for improved treatments—all essential parts of the URLLC-mMTC use case previously described.

### 4.1.6 Use Case#6: URLCC - MBB

#### 4.1.6.1 Use Case Overview

The **URLLC-MBB** UC combines two highly vital UCs, namely the URLLC and eMBB, to provide highly reliable and near-zero latency communications as well as improved broadband services. It enables applications spanning from real-time cloud, to AR situations, and remote monitoring of robotic devices that demand both high reliability and large data rates.

#### 4.1.6.2 Key UC Requirements and KPIs Addressed

| KPIs | Metrics |
|---|---|
| Scalability | flexible |
| Energy Efficiency | (20% higher compared to its Predecessor) |
| Security of wireless access for any traffic load/patterns | 99.99% |
| Ultra-high privacy with probability of successful attack | 10^-5 |
| Network and learning latency minimization | ("almost-zero" latency) |
| E2E coverage | 100m outdoor |
| Ultra-high scalability and flexibility | resource availability ~99.999% |
| Operation cost reduction | >30% |
| Complexity and overhead reduction | - |
| Availability | 99.9999% |
| Key generation | <1ms |
| Verification | <1ms |
| Data efficiency (DE) improvement | >20% |
| Latency | < 5ms |
| Resource utilization rate | >99.99% |
| Reliability | 99.99999% |
| E2C EE improvement | 37-41% (AI service orchestration) |

#### 4.1.6.3 Relevance to NANCY demonstrators

Italian massive-IoT testbed (Demonstrator #1): The outdoor testbed, located in Italy, that is addressed in the NANCY Project encompasses many characteristics in common with the URLLC-MBB use case. In particular, the aforementioned testbed demonstrates the development of a centralized B-RAN (CB-RAN) architecture with an emphasis on enhanced safety, reliability, and support for a broad range of applications, rendering it an adequate testing ground for the amalgamation of URLLC and eMBB technologies. The Italian massive-IoT testbed offers an ideal setting to assess the efficacy of such technologies in the context of URLLC-MBB UC, where ultra-reliable and low-latency communication is vital for real-time cloud services, augmented reality experiences, and remote monitoring of devices that require high reliability and large data rates simultaneously. This testbed serves as a valuable showcase for the URLLC-MBB use case by implementing these cutting-edge communication solutions within a seaport's critical infrastructure. Overall, this testbed shows the potential to ensure the continuous operation of mission-critical applications while enhancing broadband services.

Greek outdoor testbed (Demonstrator #3): The previously described URLLC-MBB use case is extremely applicable to the Greek outdoor testbed, located in the Athens urban centre. The objective of this testbed is to deliver interactive AR/VR material to end users, resulting in the need for high data rates, minimal latency, and robust security. The testbed's setup consists of mobile network equipment adjustments to higher layer software, MEC and central cloud servers, and multimedia devices. It aims to test the NANCY project's capacity to cope with CoMP scenarios and advanced coverage expansion under the demanding conditions of future applications. Smart pricing, AI-based B-RAN orchestration, computational offloading, and socially conscious caching represent a few of the features that require to be investigated in order to provide low-latency and high-data-rate connectivity.

## 4.2 6G Reference Projects

### 4.2.1 Hexa –X families of Use Cases

The Hexa-X project [43] employs a novel perspective on the crucial role of 6G technology in societal growth and advancement. A preliminary set of use cases has been established by the Hexa-X consortium as the basis for all technological efforts made during the project. These use cases cover a wide range of activities, from ones that have been based on 5G's capabilities to more revolutionary ones bringing novel opportunities and innovative benefits for society in general. In this direction, the use cases families presented by Hexa-X are listed in the following table. These use case families include a plethora of use cases that have been thoroughly analysed throughout the duration of the Hexa-X project.

Table 2: Hexa-X families of Use Cases

| Use cases | Explanation |
|---|---|
| Sustainable development | This use case family describes how sixth generation wireless networks (6G) can contribute in terms of society transformation, targeting UN sustainable development goals and the EU Green Deal. |
| Massive twinning | This use case family involves the use of digital twins in order to represent the physical world. |
| The Telepresence | This use case family covers telepresence for enhanced interactions providing highly immersive experience. |
| Robots to cobots | This particular use case family involves various use cases such as interacting robots at home or business in order to improve everyday life. |
| Local trust zones (for human and machine) | This use case family covers diverse UCs, starting from nanoscale in-body networks to wide area deployment of sensors networks. |
| Enabling services harnessing new capabilities | Includes a set of novel UCs that will lead to a merging of communication, computing, data and sensing, including Artificial Intelligence. |

### 4.2.2 one 6G

The one6G project [44] highlights a significant collection of use cases far exceeding any other similar project. These use cases are grouped into different verticals, each displaying a specific domain. Based on the breakdown of use cases, we can highlight the most important requirements for sixth-generation wireless communications in each industry. Some of these industries include various sectors such as manufacturing, automotive, telecommunications, healthcare, etc. In the table below, we have collected all the proposed use cases that have been presented in the one6G project.

Table 3: one6G project reference Use Cases

| Use case families | Explanation |
|---|---|
| Remote software update for vehicles in underserved areas | This use case addresses the gap caused by sporadic mobile network coverage by utilizing a secondary communication route through satellite to provide software upgrades for automobiles in remote areas. |

| | |
|---|---|
| Tele-operated driving in the presence of mobile network coverage gaps | This use case makes use of additional wireless channels (i.e., satellite communication) in order to maintain a constant connection between the vehicle and the ToD server amid gaps in mobile network coverage. |
| Simplified mobile network for indoor mobile Traffic | This use case illustrates how to effectively address the unique requirements of indoor-generated mobile traffic. The MNO can minimize resources and expenses while still offering dependable mobile multimedia communication services to subscribers by optimizing the network design and removing mobility support. |
| Secure delegation of trust for mobile connectivity | With the help of this use case, a novel trust model is introduced that permits secure delegation of trust across devices without the need for cryptographic hardware chips. In order to ensure smooth connectivity, it overcomes the issues of identity management in a scenario with high levels of connectivity and enables authorized subscribers the capability to allocate trust to other devices. |
| Integrated sensing and communication for V2X in ultra-dense networks | By enabling base stations to change their configuration proactively in response to the presence of active and passive devices within their coverage area, this use case guarantees the effective operation of extremely dense networks. The base stations can improve their performance and match the rigorous demands of connected vehicles by monitoring while taking into account the environment's constant motion. |
| Integrated sensing and communication for V2V communication | The present use case aims to make it feasible for automated vehicles to connect directly with desired vehicles that are nearby. Autonomous vehicles may adjust their communication modes based on changes and obstacles by sensing and detecting the environment around them, ensuring continuous and effective exchange of information. |
| Ultra-high reliability support with tighter integration between mobile communication network and application layer | To achieve ultra-high reliability, this use case emphasizes the necessity for closer integration between the mobile communication network and the application layer. The network can effortlessly transfer traffic to alternative servers in the event of application server failures, ensuring ongoing connectivity. |
| Integrated sensing and communication (ISAC) for motion control in dynamic factory environments | In dynamic production environments, this use case emphasizes the importance of integrating sensing and communication for motion control. |
| Integrated sensing and communication for cooperative carrying of unknown objects by mobile robots | The advantages of integrated sensing and communication for cooperative carrying of ambiguous objects by mobile robots in industrial settings are illustrated by this use case. The mobile robots can recognize object features, coordinate their operations, and guarantee effective and secure transportation within the factory by utilizing ISAC capabilities, including sensing and communication. |
| Geographical positioning and location sensing as mobile network service | This use case demonstrates how 6G networks could offer extremely precise positioning and location-based services to both connected and non-connected items. By utilizing novel technologies and integrating them with current systems like |

| | |
|---|---|
| | GNSS (Global Navigation Satellite System), 6G can support a variety of applications. |
| RF or Optical Wireless Communication Enhanced by Optical Sensing | In this use case, it is proposed to utilize the optical image sensor's high-resolution sensing capabilities to improve the RF and optical high throughput wireless communication network. This will significantly enhance the accuracy and speed of beam searching and tracking, which will further enhance the wireless communication network's reliability, capacity, and mobility. |
| Intelligent, deterministic and time synchronization network for haptic and future factories | The need for an intelligent, innovative network to support IVR communication and future manufacturing is shown by this use case. |
| Advanced and sustainable massive MIMO wireless transmission technologies for ultra-high data rate applications | This use case showcases how the 6G network is implementing novel and massive MIMO wireless transmission technologies. The MNO provides ultra-high data rate connectivity for visual applications by utilizing massive MIMO and access points installed on city lampposts. As a consequence of the network's faultless transition between access points, smartphone users can take advantage of stable, high-speed wireless connectivity while simultaneously saving energy. |
| AI-as-a-service for V2X | The deployment of AI-as-a-Service (AIaaS) for Vehicle-to-Everything (V2X) applications, mainly in the context of environmental perception, is the main focus of this use case. This enables users to access, implement, and manage AI capabilities for their applications. |
| Factory Automation and Predictive Maintenance by Remote Control of Cyber-Physical Systems in Future Factories | The use case presented here focuses on the usage of 6G technology in future corporations for factory automation and preventive maintenance. The objective is to enable remote control of cyber-physical systems and develop an environment that is fully automated. |
| Mixed tactile and VR content in robotic control | This use case aims to provide eXtended Reality (XR) across mobile networks to enable intuitive and transparent operation of robots in remote situations. |
| Monitoring of cross-level passages in railroads | This use case illustrates the significance of mobile communications and network slicing in facilitating effective and economical railroad crossing monitoring while satisfying the unique needs of security, isolation, and reliability in the railway sector. |
| Livestock Health and Behavior Monitoring | This use case seeks to enhance livestock management by keeping an eye on the general health and behaviour of animals when they are grazing in open fields, with the use of sensor technologies and data analysis. |
| UAV Remote Controlling for Precise Agriculture | Benefits of this use case include enhanced agricultural output, less environmental contamination, and improved pesticide and fertilizer application accuracy by incorporating innovative technologies and robust network access. |
| Agricultural Machinery Remote Monitoring and Controlling | This use case offers advantages including cost reduction through preventative maintenance, increased productivity overall, and increased efficiency in agricultural activities. Farmers may optimize the productivity of their machines, |

| | |
|---|---|
| | resulting in more sustainable and lucrative farming methods, through the use of cutting-edge technologies and reliable network connectivity |
| AI-as-a-service for industrial robots: Learning to be collaborative | Through the use of AI/ML techniques, this use case enables collaborative robots to learn and adapt to varied tasks and surroundings |
| AI-as-a-service for industrial robots: Collaborative to learn | This use case highlights the use of FL and collaborative learning in the IIoT sector, utilizing wireless networks and AI/ML services to improve production procedures as well as the learning capabilities of industrial robots. |
| Scalable resource control for high-demand localized services | In order to meet the localized high demand for services, this use case highlights the significance of scalable resource control and dynamic adaptation. |
| THz communication enabled data kiosks | This use case illustrates how high-speed data transfer in locations, such as factories, can be enabled using THz communications and data kiosks, enabling rapid software updates or updates of autonomous robot systems. With the aid of this technology, autonomous robots can function more efficiently and adapt to changing industrial environments. |

## 4.3 O-RAN Use Cases

This Section investigates the use cases that showcase the extensive capabilities of the O-RAN architecture [45]. Some of these use cases involve using intelligent technologies to create and implement models based on long-term data and policies to regulate the real-time behavior of RAN. Other use cases concentrate on optimizing RAN through configurations and policies, while some combine both approaches to facilitate closed-loop optimizations and ensure SLA compliance.

Table 4: O-RAN reference Use Cases

| Use cases | Explanation |
|---|---|
| Context-Based Dynamic HO Management for V2X | V2X communication offers a multitude of advantages, including enhancing road safety, minimizing emissions, and saving time. The V2X architecture includes the V2X UE, which consists of a SIM card and a device connected to a vehicle, and it connects with the V2X Application Server (V2X AS). The information transferred includes Cooperative Awareness Messages (CAMs) from User Equipment (UE) to Vehicle-to-Everything Application Server (V2X AS), radio cell IDs, connection IDs, and basic radio measures such as Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ). |
| Flight Path-Based Dynamic UAV Radio Resource Allocation | This use case outlines the rationale, motivation, and specifications for supporting the use case of flight path-based dynamic UAV Radio Resource Allocation. It enables operators to modify radio resource allocation policies using the O-RAN architecture, thereby minimizing unnecessary handovers and enhancing the utilization of radio resources. |
| Radio Resource Allocation for UAV Application Scenario | This use case considers a UAV with cameras, sensors, and other equipment flying at low height and speed. The Operation Terminal remotely controls the UAV for border/forest inspection, high voltage/base station inspection, field mapping, pollution sampling, and HD live transmission. To maintain low-altitude safety in particular locations, the UAV control mobile station and UAV anti-weapon combination offer UAV control, combat illegal UAVs, and other services. The UAV |

| | |
|---|---|
| | Control Vehicle is linked to the UAV Operation terminal, anti-UAV weapon, and UAV control mobile station. To deliver dependable network services across 5G networks, UAV Control Vehicle uses O-CU, O-DU, Non-RT RIC, Near RT RIC function modules, and Application Server (in this instance, an Edge computing Service Platform). |
| QoE Optimization | Cloud VR and industrial automation are bandwidth- and latency-intensive 5G native applications. Current 4G and 5G applications like online multiplayer gaming and linked cars are generally handled with the best effort and little application-specific optimization. Current semi-static QoS frameworks cannot effectively meet diverse QoE needs for these traffic-intensive and highly dynamic apps. These requirements may change over time, particularly for applications with dynamic performance needs and radio transmission capacity fluctuations. QoE estimation/prediction from the application level may assist in coping with such uncertainty, enhance radio resource efficiency, and perhaps improve user experience and RAN resource efficiency. If semi-static profiles are “preloaded” onto RAN nodes without a more automated closed-loop solution, more mobile apps with different QoE needs will become unmanageable. Improving user experience via RAN performance exposure to an external application is also expected. |
| Traffic Steering | 5G systems will support LTE, NR, NR-U, and Wi-Fi. Multiple multi-access deployment options are conceivable with 5GC, supporting diverse applications and meeting the spectrum needs of various service providers:<br>- Licensed band NR and NR-U carrier aggregation<br>- Dual licensed band NR/NR-U connection from Primary Cell to Secondary Cell<br>- Dual connection between licensed bands LTE and NR-U, and licensed band NR and Wi-Fi.<br>Traffic steering uses the A1 interface to dynamically specify optimization strategies and employ performance criteria to proactively manage user traffic across access technologies. The A1 interface may also give enrichment information like radio fingerprints based on past RAN data analytics. |
| Massive MIMO Beamforming Optimization | Multi-antenna transmission and reception can provide diversity and capacity by targeting high-gain antenna beams at one or more subscribers, improving receive power levels and spatially filtering interference from neighbouring subscribers and transmission points. By spatially reusing restricted time/frequency resource blocks to send multiple data streams to/from one or more users, spatial multiplexing operations may increase network capacity. Controlling electromagnetic (EM) emissions or using sophisticated network management technologies like beam shaping, beam-based load balancing, optimal beam mobility, and adaptive cell coverage regions are also benefits, particularly in dense urban 3D settings with mobile users. Fully digital beamforming (BF) approaches should be used for sub-6 GHz wireless telecommunications to improve networks, such as spectral efficiency, coverage, and cell capacity. Grid of Beams (GoB) is a BF approach that selectively covers areas of interest using a subset of radio beams from a dictionary. BF's Beam-based Mobility Robustness Optimization improves beam-specific mobility performance by adding offsets. |
| RAN Sharing | Network operators must launch several services while meeting diverse QoS criteria and maintaining a sustainable network investment. Network sharing is envisioned as a sustainable solution to speed 5G implementation by pooling physical infrastructure and resources between two or more partner operators.<br>In addition, regulatory constraints typically oblige operators to cover unprofitable regions, reducing profitability. RAN sharing is a potential option that may save |

| | |
|---|---|
| | network costs, enhance capacity and coverage, and improve customer happiness. The open and multivendor O-RAN architecture may speed the introduction and development of RAN-sharing solutions by improving the deployment of virtual network functions (VNF) on commodity-shared hardware while meeting different QoS criteria. |
| QoS Based Resource Optimization | When the network provides preferred QoS for some users, QoS-based resource optimization may be applied. A network setup to handle e2e slices is one example. In this example, the network isolates resources between slices and monitors slice Service Level Specifications (SLS). The scheduler in RAN isolates Physical Resource Block (PRB) resources between slices and optimizes their utilization to meet SLS for various slices. Slices' default RAN behavior is set via O1. At slice instantiation, the ratio of physical resources (PRBs) reserved for a slice is specified via O1. QoS may also instruct the RAN scheduler to assign PRB resources to users in real time to meet a slice's SLS. The resource partition property in the NR NRM describes this. |
| RAN Slice SLA Assurance | The 3GPP standards created a sliceable 5G infrastructure that enables the design and administration of customizable networks to satisfy future application, service, and business sector needs. A flexible architecture requires distinct functionality, performance, and user requirements for each service, which might vary substantially. The 5G standardization initiative defined application/service-type-specific slices and SLAs. Since network slicing is an end-to-end feature that comprises the core network, transport network, and RAN, these criteria should be addressed at every slice subnet throughout its lifetime, notably the RAN side. In SDOs like 3GPP and Groupe Speciale Mobile Association (GSMA), slice performance criteria are high in throughput, energy efficiency, latency, and dependability. These criteria are used to establish SLA/contractual agreements for each slice that NG-RAN must handle properly. |
| Multi-vendor Slices | This use case allows for the creation of several slices that include functionalities offered by various suppliers. For example, slice #1 consists of DUs and CUs given by vendor A, whereas slice #2 consists of DUs and CUs provided by vendor B. |
| NSSI Resource Allocation Optimization | The complexity of 5G networks is growing due to the increased deployment of millimetre wave small cells and the introduction of new services like eMBB, URLLC, and mMTC. These services are characterized by high-speed, high-data volume, low-speed, ultra-low latency, and infrequent, low-data volume transmission from a large number of emerging smart devices. Allocating resources dynamically and effectively across different network nodes to provide diverse services is a significant challenge for 5G networks. |
| Local Indoor Positioning in RAN | Cellular network-based positioning is a crucial technology for 5G vertical sectors, people, and operators, particularly in small interior environments. For example, a mall may provide additional services that enhance its value, such as providing real-time indoor positioning for local interior navigation and store recommendations. The industrial manufacturing sector should implement a system that sends immediate safety alerts to advise operators to stay clear of hazardous areas. This system should also include real-time indoor location technology. |
| Massive MIMO SU/MU-MIMO Grouping Optimization | This technology utilizes multi-antenna transmission and reception to naturally offer diversity and enhance capacity. It achieves this by directing high gain antenna beams towards one or multiple subscribers, resulting in improved receive power levels and spatial filtering of interference from neighbouring subscribers and transmission points. The scenario when a specific physical resource block of a massive MIMO cell serves just one subscriber during a |

| | |
|---|---|
| | transmission interval is referred to as single-user MIMO. Multi-user MIMO refers to the scenario when a single physical resource block of a massive MIMO cell serves numerous subscribers during a transmission interval. |
| O-RAN Signalling Storm Protection | The reliance of society on network connection is growing, with a rising variety of device kinds, ranging from advanced smartphones to basic and affordable IoT devices, connecting to the network. The extensive proliferation of interconnected devices, along with the diverse array of device categories, renders the mobility network susceptible to inadvertent or deliberate assaults that have the potential to disrupt the normal functioning of the network. As life-critical applications transition to wireless networks, any interruptions to these networks might not only be inconvenient but also have significant implications for the well-being and safety of persons. The O-RAN architecture provides a chance to tackle security concerns in flexible and innovative manners by using the near-real-time RIC xApps and non-real-time RIC rApps. |
| Industrial IoT Optimization | The 3GPP Industrial Internet of Things item considers novel situations with high dependability in the industrial automation and transport industries. Industrial IoT in 5G systems supports data duplication and multi-connectivity enhancement, time-sensitive networking, and different prioritized transmission multiplexing to meet these scenarios. Some of these procedures may be optimized using O-RAN architecture. PDCP (Packet Data Convergence Protocol*)* duplication supports 4 RLC entities/legs. Initial setups employ RRC signalling. MAC CE controls dynamically. PDCP duplication is only allowed for NR, per 3GPP. DRB-associated PDCP entities may be set by RRC for EHC. Each PDCP entity containing user plane data may utilize EHC. No more than one EHC compressor and decompressor per PDCP entity. In multiplexed communications, higher-priority transmissions may cancel lower-priority broadcasts. Related setups employ RRC signalling. |
| BBU Pooling to achieve RAN Elasticity | Cloudification aims to reduce costs by increasing workload flexibility. This use case offers BBU pooling for RAN flexibility. O-RAN CADS presents numerous deployment methods for cloudified NFs, allowing varying edge and regional cloud centralizations. Cloudified BBUs may be installed on a cloud-centralized hardware pool. This centralization allows O-RUs to be dynamically mapped to BBUs, allowing RAN flexibility and possibly saving costs. |
| Integrated SON Function | Self-Organizing Network (SON) functionalities for 5G reduce mobile network costs by automating configuration, optimization, protection, and healing functions from deployment to operation. SON improves network performance, customer experience, OPEX-to-revenue ratio, and unnecessary CAPEX. SON automates network setup and resource and configuration management for maximum performance. SON algorithms perform SON functions singly or in groups. SON algorithms take management data, including MDAS (Management Data Analytics Service) data, and evaluate it to find network faults and solutions. |
| Shared O-RU | The current fronthaul standards have role-based access control features to limit rights to certain areas of an O-RU's configuration depending on privileges. Additionally, they enable parallel administration interfaces to facilitate hybrid fronthaul installations. Nevertheless, the existing bottom layer split design is limited by the need for an O-RU node to function with just one O-DU node. The use of fronthaul systems to enable advanced use cases, which include the utilization of numerous O-DU nodes to increase the capabilities provided by O-RAN's open fronthaul standards, is restricted by this limitation. |
| Energy Saving | The energy consumption (EC) of the Radio Access Network is a significant concern for network operators, particularly in the context of 5G networks. The |

| | |
|---|---|
| | effectiveness of RAN energy saving (ES) relies on meticulous design and setup. The optimization of EC in the RAN is a challenging task due to the fluctuating traffic load and user mobility. It may be applied to various network levels and time scales. There is a potential for RAN equipment to use a significant amount of energy while operating with little or no traffic.<br>Various ES characteristics are being examined in the industry, with some ones being implemented in operational networks. Examples include entering deep sleep mode, disabling the carrier, and toggling the on/off state of RF channels. Recently, there have been proposals for mechanisms called Advanced Sleep Modes (ASM) that operate at symbol-, subframe-, and frame-levels, targeting small time scales. |
| MU-MIMO Optimization | Multi-User-MIMO is a crucial technology that may enhance the capabilities of UE and cells by using the current time and frequency resources. By using multiple antennas, it becomes possible to direct beams towards various UEs, with each beam effectively reducing interference from the other beams by spatial filtering. When there are eNB/gNB antennas, this has the potential to increase the overall cell capacity. During a commercial deployment, subscribers may be categorized into three groups: stationary, pedestrian moving slowly, and moving at fast speed. Conventional MU-MIMO systems are very susceptible to changes in subscriber mobility, which restricts the extent of capacity improvements gained via the use of multiple antennas.<br>Emerging beamforming methods are being developed to accommodate Multi-User-MIMO technology with reduced time sensitivity, enabling their use in the near-RT RIC. These systems may be used for both downlink and uplink data channels, as well as for both TDD and FDD. They are capable of delivering great performance for both users and cells, even when subscribers are traveling at various speeds. |
| Sharing Non-RT RIC Data with the Core | With the increasing complexity of networks, there is a growing need for advanced analytics that can be accessed almost instantly. This is necessary to enable automated network management loops via entities like the Non-RT RIC and the Near-RT RIC. However, the need for such analytics is not limited to the RAN alone but also extends to the 5G Core. Therefore, the NWDAF function has been specified by 3GPP in the 3GPP 5GC architecture.<br>The NWDAF employs standardized interfaces to provide analytics to other 5G Core network functions, which use these insights to enhance their network operations. This trend is similar to the one seen with the non-RT RIC. The non-RT RIC uses a standardized interface (ie.e., A1-EI) to provide analytics to 5G RAN network functions, namely the Near-RT RIC instances. These analytics are then utilized by the Near-RT RIC instances to enhance network processing. |
| Non-Public Network (NPN) RAN-Sharing via Midhaul for Multi-Operator Coverage | This use case guarantees the security and privacy of NPN-Network traffic by maintaining a clear separation between private and public traffic, ensuring that private communication remains confidential. This use-case facilitates the implementation of NPN-RAN sharing, allowing various MNOs to expand their network coverage. It addresses the MNOs' security concerns by providing a solution for connecting to an untrusted NPN-network. |

## 4.4 Literature Review on B-RAN Scenarios

5G and beyond networks have been designed to meet the diverse requirements such as URLLC, mMTC, and eMBB, such as SDN, NFV, ML, and cloud computing, are being integrated into the 5G to address specific challenges such as decentralization, interoperability, and security. In this respect, Blockchain

has emerged as a potential solution due to its capabilities such as transparency, data, encryption, auditability, immutability, and distributed architecture [46].

Blockchain is expected to enable services and applications that will lead to business models. By building trust and carrying out transactions in a distributed manner multiple parties related to the mobile industry can work together without friction. Integrating Blockchain will result in cost reductions and new services. In addition, ever-growing demands for data and streaming services have created a need for an efficient content delivery network (CDN) that will help reduce such bottlenecks and meet the QoS/QoE of end-users.

The potential and benefits of Blockchain in 5G networks motivated network operators to integrate Blockchain technologies into their networks. For instance, IBM and Telefonica collaborated to use Blockchain technology to streamline core business processes in the operator's network [47]. South Korea's largest telecommunication provider has launched a Blockchain-powered 5G network GiGA chain that aims to secure IoT devices [48] while China Mobile, China Unicom, and China Telecom used the Blockchain platform pilot project to share information on Know Your Customer (KYC) procedures for quick customer identification [49]. In the figure below, a Taxonomy of Blockchain Application in 5G is depicted.

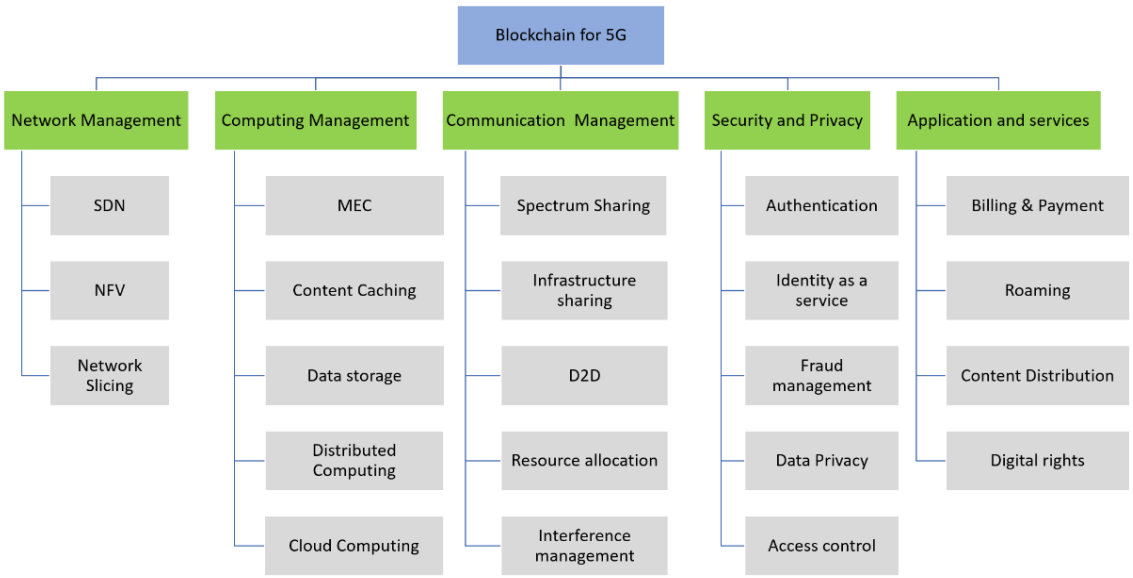


Figure 7: Taxonomy of Blockchain Application in 5G [46]

According to [50] when it comes to B-RAN architecture, it adds the Blockchain layer based on the well–known C-RAN architecture, which records the messages/transactions in the form of blocks in the mobile communication network, especially sensitive information like identity exchange, asset trades, etc.

In another study [51], B-RAN is proposed as a novel decentralized RAN architecture to facilitate enhanced security and privacy on identification and authentication. Also, a potential operating model with thorough decentralization of RAN is envisioned. A distributed privacy-preserving P2P communication approach, as one of the core use cases for future mobile networks, as an essential complement to the existing core network-based security and privacy management is also proposed. The resulting B-RAN significantly improves communication and computation overheads compared to the existing communication authentication protocols.

Heider-Aviet et al. [52] in their work proposed a generic solution for the inter-MNO RAN data exchange and management, considering this cross-carrier collaboration essential for the provision of seamless coverage and connectivity across national borders. Leveraging distributed ledger technology for data governance enables a secure, trusted, and transparent system for all MNOs, where public data can be shared in parallel to dynamic individual private alignments. The main mechanism of permissioned Blockchain facilitates access management since each MNO is protected by a CA assuring the overall integrity and consistency by cooperatively maintaining the blocks and transactions. In this respect, they proposed a scenario considering geographical cross-border areas in which two or more MNOs in different countries operate at least one network cell.

Nguyen et al. in [53] investigated the recent advances in the Blockchain applications in 5G Internet of Things in a variety of use-case domains, such as smart healthcare, smart city, smart transportation, smart grid, and UAVs as shown in the following figure.

| 5G IoT application | Ref. | Use case | Main contributions | Limitations |
|---|---|---|---|---|
| Smart healthcare | Li et al. (2019c) | Blockchain for healthcare | A blockchain solution for healthcare networks. | Implementation to investigate the system efficiency is lacked. |
| | Feng et al. (2018b) | Blockchain for D2D-based mobile networks | A blockchain scheme for secure D2D in large scale feature extraction in mobile networks. | Only conceptual analysis is provided and simulation to evaluate the proposal is lacked. |
| | Lin et al. (2019) | Blockchain for MEC-based healthcare | A blockchain model for mobile edge computing (MEC)-empowered healthcare applications. | The performance of the proposed framework has not been simulated. |
| | Wang et al. (2019c) | Blockchain for cloud-based healthcare | A blockchain scheme for cloud-based healthcare networks. | Privacy issues in blockchain transactions has not been taken into consideration. |
| Smart city | Liu et al. (2018e) | Blockchain for secure vehicular data storage | A peer-to-peer transaction and decentralized storage model for secure records of transaction data of EVs. | Data privacy has not been investigated. |
| | Zhou et al. (2019) | Blockchain for energy trading in V2G | A V2G energy trading model with a combination of blockchain and edge computing. | The feasibility of the proposed model has not been investigated on real world energy platforms. |
| | Zhang et al. (2019c) | Blockchain for controlled vehicular networks | A blockchain network for building secured and controlled vehicular ad hoc networks. | The performance of the proposed framework has not been investigated. |
| Smart grid | Guan et al. (2018) | Blockchain for private smart grid | A blockchain model for privacy-preserving and efficient data aggregation network. | Data privacy should be taken into consideration. |
| | Gao et al. (2018b) | Blockchain for traced power delivery | A blockchain scheme for traceability of power delivery in smart grid. | Implementation to investigate the system efficiency is lacked. |
| | Singh and Choube (2018) | Blockchain for detecting cyber-attacks | A model with blockchain to mitigate cyber-attacks on a smart grid. | The effectiveness of the proposed framework has not been simulated. |
| Unmanned Aerial Vehicles | Qiu et al. (2019a) | Blockchain for UAV spectrum sharing | A blockchain model for secure spectrum sharing platform between the aerial and terrestrial communication. | Only conceptual analysis is provided and simulation to evaluate the proposal is lacked. |
| | Lei et al. (2019) | Blockchain for secure UAV data services | A blockchain model for decentralized content storage services and detect internal attackers in UAV. | The feasibility of the proposed model has not been evaluated on real world IoT platforms. |
| | Kapitonov et al. (2017) | Blockchain for economic model in UAV | A blockchain scheme for an autonomous economic system with UAVs. | Data privacy has not been investigated. |

Figure 8: Blockchain applications use-case domains

According to their research [53] the integration of Blockchain into 5G, is mainly implemented via simulations and experiments. They conclude that Blockchain is very promising in many practical 5G areas, ranging from 5G technological enhancement (i.e., Blockchain- cloud combination, Blockchain-SDN adoption) to 5G services (e.g., Blockchain-based data offloading, Blockchain-empowered spectrum sharing) and 5G IoT (e.g., Blockchain-based smart city).

In addition, Ling et al. [54] proposed a large self-organized Blockchain radio access network architecture with decentralized, secure, and efficient mechanisms to manage network access and authentication among inherently trustless network entities, demonstrating the benefits of B-RAN architecture.

In [55] a performance assessment of B-RAN using a unique in-house prototype through three representative case studies is presented. This research through the development of a hierarchical architecture consisting of six layers as a general framework of B-RAN investigated key enabling technologies, illustrated network pooling effects, latency-security trade-off, and Rogue's Dilemma aiming to showcase how B-RAN can improve efficacy and productivity.

# 5 NANCY Usage Scenarios

Novel requirements arise from challenging verticals, jointly using secure software engineering and operational procedures to manage risks across multiple stakeholders including quantification of security attributes and communication of associated risk for stakeholders. In this respect the consortium mapped the vertical usage scenarios into three distinctive usage scenarios, namely: i) fronthaul network of fixed topology, ii) advanced coverage expansion, and iii) advanced connectivity of mobile nodes.

These usage scenarios have been widely recognized as the cornerstone of almost all the 6G SNS-described verticals. Moreover, NANCY envisions freeing the role of the network nodes and allowing them to interchangeably be connectivity/service consumers and providers.

Thus, NANCY enables multi-tenancy and collaboration between different providers in a secure, private, and trusted manner. This is achieved by combining the highly virtualised features with blockchain, MEC, and AI functionalities. Additionally, to further enhance network security, proactive federal learning self-healing, and recovery mechanisms are developed.

In the following, the NANCY's usage scenarios are described.

## 5.1 Fronthaul network of fixed topology Usage Scenario

In this scenario, each UE performs a computation-intensive and delay-sensitive task, such as navigation, video streaming, VR, etc. considering that BS/APs belonging to the same or different providers are equipped with MEC capabilities; thus, they have high availability of computation resources and can execute AI functions.

Resource-limited mobile devices can offload their tasks to the heterogeneous edge infrastructures (BS/APs), which utilize fine-grained computational resource allocation policies to process the offloaded tasks. Moreover, since the UE is within the range of at least two BS/APs, CoMP connectivity can be utilized in order to boost the system's reliability and energy efficiency.

Finally, spectrum aggregation can be performed to increase the achievable data rate at the UE. The need to utilise B-RAN is identified since the interactions between UE and BS/APs are not trust-based. In such scenarios, apart from the high reliability, security, and privacy, the critical system parameters are the aggregated data rate achieved by the end-UEs, which is expected to exceed 100 Gbps, the energy efficiency, and the network latency. Therefore, the use of the AI-based orchestrator is required to jointly optimize the infrastructure selection and the resource and NF allocation.

### 5.1.1 Direct connectivity

Section 5.1.1 explores the concept of direct connectivity, highlighting its fundamental role in wireless communications. Emphasis is placed on understanding the increasing need for direct, uninterrupted connections in the rapidly evolving digital era. The importance of these links in enabling instantaneous data exchange and supporting real-time interactions is examined, reflecting their critical importance in today's networked world. Attention is given to the mechanisms that facilitate these rapid connections, as well as the challenges of ensuring their security and cost-effectiveness. Throughout this section, the intricacies of direct connectivity are revealed, demonstrating its vital contribution to improving the efficiency and reliability of wireless communication networks.

#### 5.1.1.1 Motivation and Objectives

In the domain of wireless communication, there is a growing emphasis on achieving swift and direct connections. As we navigate into an era characterized by immediate data exchanges and real-time

interactions, achieving uninterrupted links is of outmost importance [59]. Direct connectivity facilitates an efficient communication pathway from the source to the destination without intermediary delays.

This methodology ensures rapid data transfers, vital for real-time video streaming and for the seamless operation of IoT devices [56]. However, challenges arise, particularly in ensuring the security and cost-effectiveness of these connections. In the context of the B-RAN era, our primary focus is to ascertain that these direct connections are both rapid and secure while also being cost-efficient [56].

#### 5.1.1.2 Relevant Technologies

Several pivotal technologies enhance the efficacy of direct connectivity, namely Blockchain, smart pricing strategies, MEC, semantic communications, and cell-free access mechanisms.

Blockchain, in the context of direct connectivity, provides a secure and decentralized mechanism to authenticate and log data transactions. With the robustness of blockchain ledgers, we can confidently ensure the verification and secure recording of every data transaction. Its decentralized nature negates the necessity for a central governing body, fostering a more transparent communication ecosystem.

Cost considerations are paramount. While direct connections are inherently efficient, they might be associated with elevated costs due to resource consumption. Smart pricing strategies address this by dynamically adjusting costs based on parameters like data volume, urgency, and network demand. Such strategies ensure that users derive maximum value, making direct connectivity a more viable choice.

In scenarios dominated by direct connectivity, there is often a substantial data transfer, especially from IoT devices. MEC assists by processing this data closer to its origin, minimizing transmission distances, and ensuring expedited processing. This not only accelerates data processing but also alleviates the strain on primary servers, enhancing the overall efficiency of direct connections.

Semantic communications add a novel dimension to direct connectivity. This technology shifts the focus from simply transmitting data to transmitting meaningful information. By prioritizing the context and relevance of the message, semantic communication ensures that the essence of the communication is preserved and understood, even under less-than-ideal transmission conditions. This approach is particularly beneficial for optimizing network resources and improving the clarity and efficiency of communications in complex scenarios.

Cell-free access mechanisms represent another significant advancement in improving direct connectivity. Moving away from traditional cell-based network structures, this approach uses a distributed array of access points to provide service. This method significantly improves network coverage and capacity, particularly in densely populated or geographically challenging areas. By ensuring a more consistent and higher quality connection across locations, cell-free access mechanisms are instrumental in improving the user experience and overall network performance.

Summarising, with the support of technologies such as blockchain, intelligent pricing, edge computing, semantic communications, and cell-free access mechanisms, direct connectivity is poised to be a cornerstone in the future of wireless communications, ensuring speed, security, and cost-effectiveness.

### 5.1.2 Coordinated multi-point connectivity

Coordinated multi-point (CoMP) transmission and reception refer to a wide range of techniques that enable dynamic coordination or transmission and reception with multiple geographically separated antennas. Its aim is to enhance the overall system performance, utilize the resources more effectively, and improve the end-user service quality. The fundamental principle of CoMP is to utilize multiple

transmit and receive antennas from multiple antenna site locations, which may or may not belong to the same physical cell, to enhance the received signal quality as well as to reduce interference, improve spectrum efficiency, and enhance effective coverage area by exploiting the co-channel interferences. CoMP transmission and reception were first introduced in 3GPP Rel-11 and enhanced during the following releases. It has been used as an effective technology to enhance cell edge coverage and overall system performance in traditional cellular networks.

CoMP mainly has been targeted to improve cell-edge UE experience, but regardless of the location, it is also used to enhance system throughput to UEs that experience strong signals of different BSs/cells. As a matter of fact, CoMP can allow cell edge users to communicate with multiple BSs (forming a CoMP cooperating set) and hence improve the throughput of cell edge users and the overall network.

A CoMP (cooperating) set generally is defined as the group of BSs within a geographic area that are directly or indirectly participating in data transmission/reception to/from a UE. The UE may or may not know about this set. The direct participation BSs are those actually transmitting/receiving data. Based on the neighboring BS's signal and planning consideration, BSs are in fact grouped in clusters at the network level. Each cluster is called a CoMP cooperating set, in terms of network point of view, and is defined for all UEs under the BSs of that cluster. In this approach, a portion of BSs belonging to the cluster takes part in transmission/scheduling/reception decisions for individual UE. According to different deployment scenarios, CoMP cooperating set is defined as network-centric, UE-specific, and network-centric UE-assisted.

CoMP may be further categorized into downlink coordinated multi-point transmission (DL-CoMP) and uplink coordinated multi-point reception (UL-CoMP); both imply dynamic coordination among multiple geographically separated points.

Figure 9 below shows the different CoMP categories and schemes based on downlink (DL) and uplink (UL) transmission:

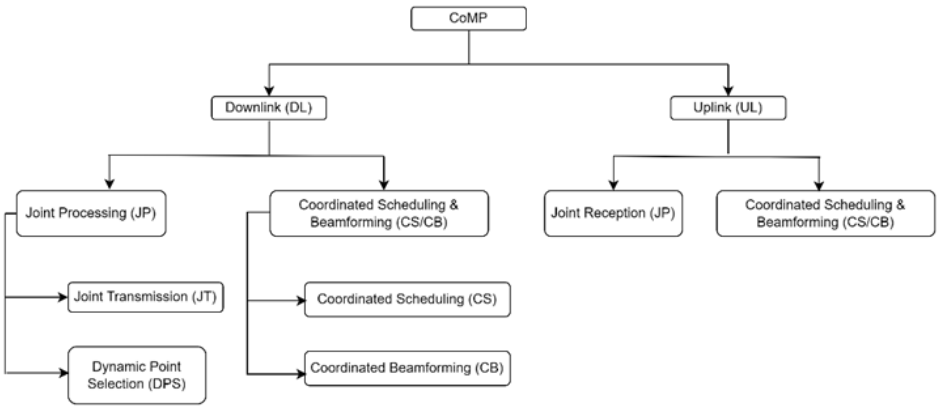


Figure 9: Different CoMP categories and schemes

The DL-CoMP scheme may be, in turn, further categorized into different categories. The main are:

1. Joint Processing (JP): Data for a UE is available at more than one point in the CoMP cooperating set for a time-frequency resource. These are the different applicable techniques:
   - Joint Transmission (JT): Simultaneous data transmission from multiple points (part of or entire CoMP cooperating set) to a single UE or multiple UEs in a time-frequency resource.

- Dynamic point selection (DPS)/muting: Data transmission from one point (within the CoMP cooperating set) in a time-frequency resource. This includes Dynamic cell selection (DCS).
- DPS combined with JT in which case multiple points can be selected for data transmission in the time-frequency resource.

2. Coordinated Scheduling/Beamforming (CS/CB): Data for a UE is only available at and transmitted from one point in the CoMP cooperating set (DL data transmission is done from that point) for a time-frequency resource, but user scheduling/beamforming decisions are made with coordination among points corresponding to the CoMP cooperating set.

Considering the DL-CoMP JP scheme, although data are indeed transmitted from several sites, the JT scheme fulfills data transmission simultaneously, while the DPS scheme uses a fast cell selection approach and only one of them transmits data at a time. This advanced pair of techniques is particularly beneficial for cell-edge throughput and is anticipated to be the dominant application of CoMP. Figure 10 and Figure 11 show a simplified scheme of the two techniques. In both cases, JP CoMP schemes jointly process and exchange user data and channel state information (CSI). Joint signal processing is implemented in a base-station controller (BSC), and thus it is necessary to exchange channel state information and data for the target user to the BSC. JP CoMP schemes thus require tight time and frequency synchronization and highly reliable backhaul. Indeed, user data needs to be shared among base stations so a very fast link interconnecting them is required, although the complexity of the signal processing is higher in the joint transmission scheme. Due to the significant feedback overhead, the performance of JT is directly dictated by the backhaul network among coordinated BSs.

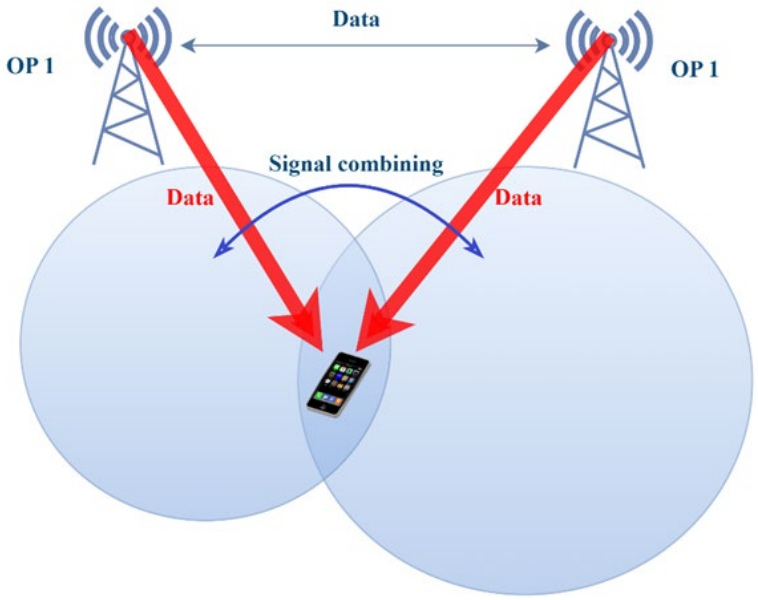


Figure 10: Joint Transmission JP DL-CoMP


Figure 11: Fast (dynamic) Point (Cell) Selection (FCS) JP DL-CoMP

UL-CoMP reception can involve joint reception (JR) of the transmitted signal at multiple reception points and/or CS decisions among points to control interference and improve coverage; the UL-CoMP scheme may be further categorized into different categories too. The main categories are:

1. Joint Reception (JR): Physical Uplink Shared CHannel (PUSCH) transmitted by the UE is received jointly at multiple points (part of or entire CoMP cooperating set) at a time, e.g., to improve the received signal quality.
2. Coordinated Scheduling and Beamforming (CS/CB): user scheduling and precoding selection decisions are made with coordination among points corresponding to the CoMP cooperating set. Data is intended for one point only.

#### 5.1.2.1 Motivation and Objectives

Here the UE is within the range of at least two Base Stations/Access Points (BS/APs). CoMP connectivity can be utilized in order to boost the system's reliability and energy efficiency; the interactions between UE and BS/APs are not trust-based. So, two different configurations are considered:

- Usage scenario 1.1: both BSs belong to the same operator. Therefore, a simple CoMP scheme can be implemented.
- Usage scenario 1.2: BS1 belongs to operator 1 (OP1) and BS2 belongs to OP2. Therefore, the CoMP scheme requires establishing a deal between the two operators and it is of special interest to NANCY.

The sharing of RAN infrastructure by multiple actors can help build 6G networks at a reduced cost, as well as create new business models; however, "sharing" faces challenges, in terms of transparency, reliability, protection of user privacy, and efficient maintenance. A fair and transparent way that is able to track the cost and usage of the shared infrastructure and resources could encourage it. It is envisioned that the 5G and 6G services will comprise a set of chained virtual network functions, which will be dynamically instantiated and deployed in a shared and distributed cloud-edge infrastructure. Consequently, models for sharing the RAN network infrastructure may represent another key element of 5G and 6G networks. Blockchain radio access network has emerged as a decentralized, trustworthy radio access paradigm. B-RAN is a decentralized and secure wireless access paradigm that leverages

the principle of blockchain to multiple trustless networks into a larger shared network and benefits multiple parties from positive network effects. B-RAN represents one promising approach to enable the sharing of RAN infrastructure and resources.

Currently deployed access points, business or individual, have not been coordinated in the existing architecture of RANs, and sometimes it happens that their resources are under-utilized. Meanwhile, UE have not granted access to APs of operators other than their own, even though they are under their coverage. In this context, the CoMP connectivity scheme together with the concept of B-RAN is described, considering it particularly interesting for NANCY.

As summarized in the scenario's introduction, CoMP is a technique in which two or more BSs coordinate dynamically, supporting joint scheduling and transmission of the signals as well as the joint processing of received signals by the receiver through multiple transmission points (TPs). In the beginning, it was used to mitigate inter-cell interference (ICI), especially at the cell boundaries. Using this technique, not only the reception and transmission of the signals are improved but cell-edge throughput also increases. Most of the CoMP approaches share the requirement of needing some scheduling information regarding the users at the different base stations that must be shared among them. This means that very-low-latency links are required so that information can be exchanged between coordinated nodes.

In the CoMP connectivity scenario described here, a UE is within the range of at least two Base Stations/Access Points (BS/APs) and the interactions between UE and BSs/APs are not trust-based. Two different CoMP connectivity configurations are considered:

1. Usage scenario 1.1, where both BSs/APs belong to the same operator
2. Usage scenario 1.2, where BS1/AP1 belongs to operator 1 (OP1) and BS2/AP2 belongs to OP2

Usage scenario 1.2, in which the CoMP connectivity scheme can be utilized in order to boost the system's reliability and energy efficiency, is of special interest to NANCY since it requires establishing a deal between the two operators. In this case, the two APs can be organized into B-RAN, considered as a commodity, to form a sizable and ubiquitous wireless network, which can significantly improve the utility of spectral resources and infrastructures. In practice, the rights, responsibilities, and obligations of each participant in this B-RAN can be flexibly codified as smart contracts executed by the Blockchain.

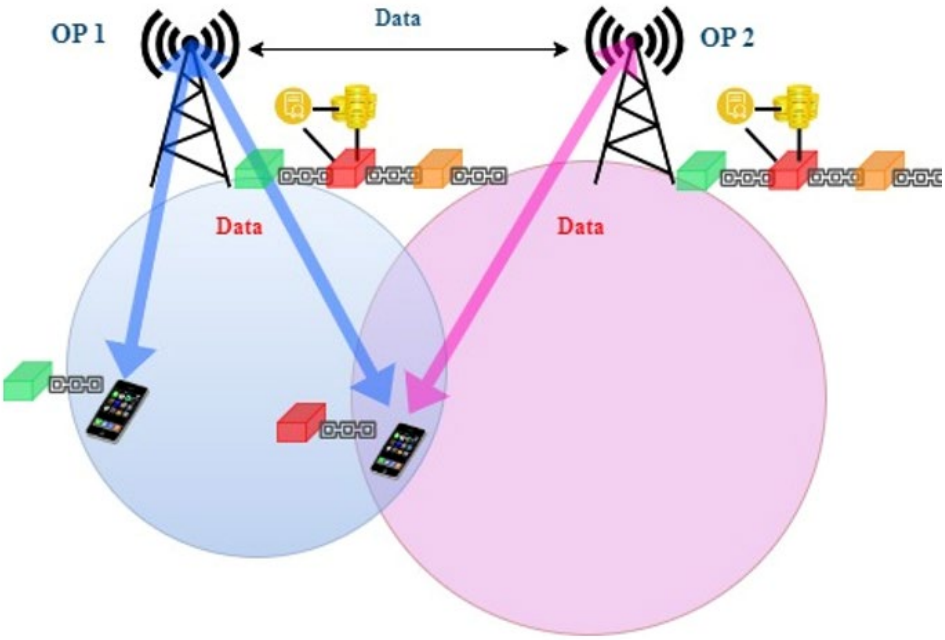


Figure 12: CoMP Usage scenario 1.2

#### 5.1.2.2 Relevant Technologies

The concept of Blockchain radio access network was formally proposed and defined in [54]. Leveraging the principle of Blockchain, it is feasible to multiple trustless networks into a larger shared network and to benefit multiple parties from positive network effects. As revealed in [54], B-RAN can improve network throughput via cross-network sharing and offloading, and recruit and attract more players, including network operators, spectral owners, infrastructure manufacturers, and service clients.

Leveraging Blockchain technology in the CoMP scenario, two or more APs can be organized to form a B-RAN and, furthermore, the adoption of smart contracts enables to achieve service level agreement (SLA) for accessing the resources.

These two or more APs, belonging to different SPs, are organized in a confederacy to provide wireless access under shared control and, at the same time, can receive payment or credit for these services.

#### 5.1.2.3 Proposed Innovation

Compared with their 5G counterparts, 6G networks are expected to achieve extreme connectivity performance, which requires hundreds of MHz to tens of GHz of spectrum resources to cater to capacity-hungry applications.

One critical bottleneck for 6G is to realize secure, efficient, and fine-grained spectrum resource management. The variant network traffic loads cause a strong imbalance in spectrum demands, where the static spectrum management diagram alone cannot meet the dynamic spectrum requests of different operators considering spatial and temporal variance.

Sustainability is a big issue with respect to the deployment of costly RAN hardware. With 6G networks, telecom operators are under higher pressure from the cost of continued traffic growth and static price expectations.

By sharing network resources and infrastructure with other MNOs or businesses, MNOs can reduce their capital expenditure significantly. Furthermore, resource sharing promotes energy efficiency by minimizing the number of operational devices and contributes to environmental sustainability by

reducing infrastructure footprint. However, establishing trust and reaching agreements among the sharing parties is essential.

CoMP may be a technique for sharing network resources and infrastructures, and it can provide high reliability as well as increased capacity. This, however, requires coordination and cooperation between the participating entities, such as base station and end nodes, to allocate resources optimally. The cooperation may be achieved easily among the homogeneous network belonging to the same operator. But in a diverse network, where the network operators have to coordinate among various network elements belonging to other operators, it is challenging. Furthermore, developing a cooperation strategy that rewards and punishes in a dynamic environment securely and transparently is highly challenging.

Utilizing Blockchain-based solutions in the CoMP scenario may offer several advantages. As a distributed ledger technology, blockchain establishes a distributed peer-to-peer trusted network with cryptography and a consensus mechanism, and thus secure spectrum resource auctioning/trading. Therefore, spectrum access and regulation can be conducted without a trusted third party. Smart contracts enable the automated handling of complex sharing arrangements and the establishment of regulations.

With a smart contract deployed on the chain, spectrum trading/sharing transactions can be automatically executed with predefined rules, which greatly facilitates efficiency. Smart contracts enable the automated handling of complex sharing arrangements and the establishment of regulations, remove the need for costly intermediaries and third parties, and enable automation of management and operation. Furthermore, this represents an incentive for cellular RAN operators to coordinate services and coverages. With the help of blockchain, it is possible to form an expansive cooperative network of different operators that is capable of delivering high-quality service at high spectrum efficiency while protecting the interests of all legal participants.

#### 5.1.2.4 Relevant performance metrics

Considering the CoMP connectivity scenario in the NANCY project, the relevant performance metrics are first of all those related to the system's reliability and energy efficiency.

Reliability relies on stable and non-stop service to fulfill the customers' ever-rising demands for high-quality communication services. Four metrics are commonly used to measure reliability: uptime, SLAs, mean time between failures (MTBF), and mean time to resolution (MTTR).

Uptime is the amount of time that a system is available for use. It is typically measured as the percentage of time that a system is accessible by users over a given period or the percentage of user requests that the system successfully fulfilled over a given period. 100% uptime is ideal but isn't realistic due to the unpredictability of complex distributed systems. Instead, NANCY aims for high availability, which sets a high minimum uptime target that the project strives for (e.g., 99.99% availability allows for less than five minutes of downtime per month).

Service Level Agreements, or SLAs, are contracts between an organization and its customers that promise a minimum quality of service. They typically describe service quality in terms of uptime/availability, response time, error rate, performance, and other measurements. At the foundation of SLAs are Service Level Indicators (SLIs), the specific metrics to monitor to track their adherence to an SLA. An SLA comprises one or more Service Level Objectives (SLOs), which are the ranges that SLIs must fall within to satisfy the SLA requirements.

The mean time between failures is the average time between system failures. This metric directly impacts uptime. A low MTBF means the systems often fail, which implies deploying problematic code or not addressing the underlying causes of failure. It also means customers are more frequently impacted by incidents, and the operations teams are likely spending a lot of time managing these issues.

The mean time to resolution is the average time to detect and fix problems. A low MTTR means that problems are addressed quickly; a high MTTR means systems are down for a long time, and it is difficult to troubleshoot and resolve issues.

Additionally, in line with the European Commission's 2030 climate and energy framework, there is a pressing need for a higher energy efficiency of 5G/B5G networks to reduce global greenhouse gas (GHG) emissions. A typical network experiences large variations in traffic demand in a day. Moreover, since networks are designed to cater to peak demands, large variations could lead to the under-utilization of base station resources and higher energy consumption during off-peak hours. As one of the main targets of 5G/B5G networks to enhance energy efficiency is to adapt the system capacity and the associated power consumption to the network load, to this end CoMP scenario can contribute to an optimized use of resources and, in turn, optimize energy consumption. To this aim, load-aware metrics can be useful to quantify related energy savings. In this context, ETSI has defined the mobile network data energy efficiency metric, EEDV [bit/J] [57], which is the ratio between the data volume, DV, delivered in the network and the network energy consumption, EC, observed during the time period required to deliver such data, i.e., EEDV = DV/EC. In this specific case, the data volume to be considered is the aggregated data rate achievable through CoMP connectivity in NANCY.

Moreover, performance metrics related to security and privacy are also relevant to the CoMP scenario. Since a B-RAN architecture together with PQC is envisioned, to define the security level of the NANCY B-RAN concept in the CoMP scenario, the probability of a successful attack may be taken into consideration.

## 5.2 Advanced coverage expansion

The concept of advanced coverage expansion is a key development that addresses the ever-increasing demand for reliable, high-speed connectivity in diverse environments. This approach leverages innovative techniques such as using infrastructure as relay nodes, dynamic node topologies, and efficient connectivity models to enhance network performance. These strategies not only ensure a broader and more robust network reach but also significantly reduce latency and improve energy efficiency. They also incorporate advanced security measures, such as the use of blockchain technology, to enhance privacy and trust in communications. The integration of these elements reflects a forward-thinking approach to meeting the complex and evolving needs of modern connectivity, emphasizing the importance of adaptability, security, and efficiency in network expansion.

### 5.2.1 Multi- Hop Connectivity

As we transition into a world dominated by the IoT and an ever-increasing number of connected devices, the traditional single-hop communication paradigm is proving inadequate. This is where multi-hop connectivity comes into play [59]. In the era of 5G networks and beyond, demands for higher data rates, lower latency, and more efficient resource utilization in wireless communication systems are escalating [60]. With the advent of 5G technology, accommodating a diverse array of devices and applications, from smartphones and IoT sensors to autonomous vehicles and augmented reality devices, becomes crucial [56]. These applications necessitate not only faster data rates but also reliable

and low-latency connections. To address these challenges, future networks are expected to tap into higher frequency bands, including millimeter and Terahertz waves [59]. However, the broader spectrum might compromise the energy efficiency of 6G networks due to high path loss. Multi-hop networks, by enabling devices to communicate through intermediate nodes, present a promising solution [60]. This approach can mitigate congestion and interference issues prevalent in traditional single-hop networks while also counteracting the effects of path loss in higher frequency bands, thus enhancing overall network performance [62].

#### 5.2.1.1 Motivation and Objectives

Multi-hop connectivity involves multiple intermediary nodes, often referred to as "hops", that relay information from the source to the destination [61]. These nodes can range from routers and relays to base stations and even mobile devices. This approach is particularly beneficial in scenarios where direct communication between the source and destination is hindered by constraints such as physical barriers, signal interference, or vast geographical distances [62]. By leveraging intermediary nodes, multi-hop connectivity ensures that data packets navigate their way to the intended recipient, even in challenging environments [63].

Looking beyond 5G to future generations of wireless networks, such as 6G, the motivation for multi-hop networks becomes even more pronounced [60]. These networks promise not only higher data rates but also groundbreaking use cases like holographic communication, global-scale IoT, and ultra-reliable low-latency communication [56]. Multi-hop networking can be instrumental in realizing these ambitious goals by allowing efficient and flexible routing of data packets across a dynamic and densely interconnected network [61]. By enabling devices to relay data to one another, multi-hop networks can reduce the burden on central base stations, enhancing the network's scalability, resilience, and energy efficiency [58]. However, the significance of multi-hop connectivity extends beyond these immediate advantages. This paradigm introduces a new level of adaptability and resilience into wireless communication networks, facilitating efficient data transmission even amidst network disruptions or environmental challenges [62]. Moreover, multi-hop connectivity can optimize resource utilization, reduce latency, and enhance energy efficiency, making it a key player in the ongoing evolution of modern communication [63]. A significant challenge in this paradigm is trust. Given that data traverses multiple nodes, ensuring the integrity and confidentiality of the transmitted information becomes paramount. This challenge is of utmost importance for our objectives in this section, where we aim to explore solutions that facilitate multi-hop communication while instilling trust and security [58].

#### 5.2.1.2 Relevant Technologies

To address the challenges posed by multi-hop connectivity, several technologies come to the forefront. Integrating Blockchain into our multi-hop connectivity scenario serves several critical purposes [59]. First and foremost, it allows for the provision of significant economic incentives while eliminating redundant overhead [58] costs associated with centralized systems. In addition, Blockchain integration establishes critical trust among participating users, such as the UE, midhaul node, and BS/AP, which is a key element in promoting secure and efficient network collaboration [58]. Compared to the existing trend of spectrum trading for network cooperation, B-RAN participants, acting as both access users and access providers, have the ability to self-organize into a robust network by eliminating intermediate brokers and their associated security risks [59]. This self-organization eliminates intermediate brokers and the inherent security risks they pose. Through Blockchain, B-RAN facilitates seamless roaming data exchange across different parties and networks, resulting in rapid identification of visiting subscribers [60]. Operating as a virtual public network, B-RAN embodies intrinsic security and self-organization features, creating an open market environment. Within this framework, healthy

competition and cooperation among participants naturally drive down the cost of large-scale data access services, eliminating the need to deploy additional wireless infrastructure [56].

Furthermore, smart pricing in B-RAN represents a paradigm shift in the way network resources are allocated and managed [58] . By integrating Blockchain technology, B-RAN introduces an innovative approach to pricing strategies, enabling dynamic and intelligent resource allocation [59]. Smart pricing in B-RAN leverages the decentralized and transparent nature of Blockchain to enable real-time monitoring of network supply and demand [60]. Through smart contracts and automated algorithms, B-RAN can adjust pricing based on network congestion, user demand, and quality of service requirements [56]. This dynamic pricing mechanism ensures that network resources are allocated efficiently, optimizing user experience and network performance [58]. In addition, smart pricing fosters a competitive environment that encourages network participants to offer competitive rates and services, ultimately benefiting both users and service providers [59]. By incorporating smart pricing into our multi-hop connectivity paradigm, the network achieves a balance between supply and demand, resulting in improved resource utilization and overall network efficiency [60].

#### 5.2.1.3 Proposed Innovation

The utilization of multi-hop connectivity toward reducing the energy consumption of the radio links will be investigated. Specifically, a UE, such as a laptop, will be used as an intermediate node between the BS and another UE. As a result, the distance radio link distance will be reduced, leading to reduced energy consumption at both the BS and the UE. Additionally, Blockchain will be integrated in order to ensure the security and privacy of the data that will be forwarded through the intermediate node. Finally, to provide incentives for a UE to act as intermediate, smart pricing policies will be integrated.

#### 5.2.1.4 Relevant performance metrics

In the aforementioned usage scenario, various metrics will be considered for assessing the performance, focusing on security, privacy, reliability, availability, and energy efficiency, as described in Section 2.

### 5.2.2 Ad-Hoc Mesh

#### 5.2.2.1 Motivation and Objectives

Coverage extension through ad-hoc and mesh networks is a well-known approach to expand the range of a network without relying on a wired and fixed infrastructure. Traditionally this approach has been implemented through Wi-Fi networks, which enable ad-hoc and mesh connectivity through layer-3 (i.e., using routing protocols such as AODV or OSLR) [64] and layer-2 (i.e., IEEE 802.11s) [65] approaches. Essentially, mesh networks imply the presence of fixed nodes devoted to providing multi-hop connectivity, while ad-hoc networks allow the spontaneous interconnection of users forming dynamic and mobile topologies. In any case, both paradigms face similar challenges, mainly related to the proper routing and allocation of traffic flows through the multi-hop links [66].

Recently, wireless mesh topologies have gained attention from 3GPP to extend the coverage of 5G networks without the need for wired links and by reusing access infrastructure. To this end, 3GPP introduced the Integrated Access and Backhaul (IAB) technology in Release 16 [67]. The main focus of IAB is to enable the massive deployment of outdoor small cells without requiring the associated massive deployment of dedicated fibre lines. Figure 13 depicts an example of IAB architecture, where the node with wired connectivity takes the role of the IAB-donor, implementing the CU, while the other access IAB-nodes only need to implement DU functionalities to provide radio access to the UEs or to allow other IAB-nodes to reach the IAB-donor, acting as relays. Note that IAB-nodes implement IAB Mobile Termination (IAB-MT) to connect to the access network of its parent IAB-node or of the IAB-donor.

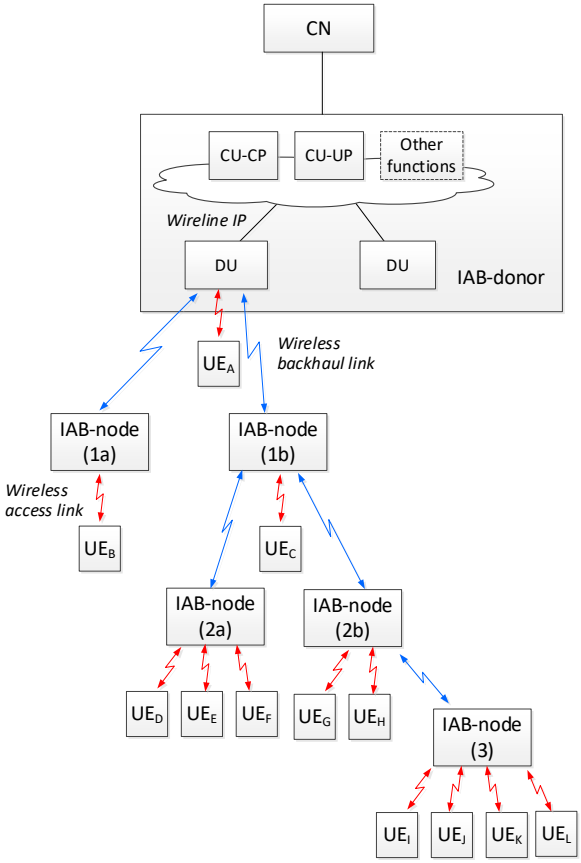


Figure 13: IAB architecture with 3 hops and 12 UEs [68]

The routing of flows in IAB networks is implemented through the Backhaul Adaptation Protocol (BAP), which is based on source routing: a set of paths between each IAB-node and its IAB-donor is precomputed and the next hop for each path is programmed into the forwarding logic of each IAB-node. Mesh topologies are allowed by having an IAB node connected to different parent IAB nodes. This opens the door to the implementation of differentiated routing/forwarding strategies with the objective of balancing the load, prioritizing specific traffic flows, or coping with temporary link blockages. For instance, Figure 14 shows an example of route modification due to a link blockage.

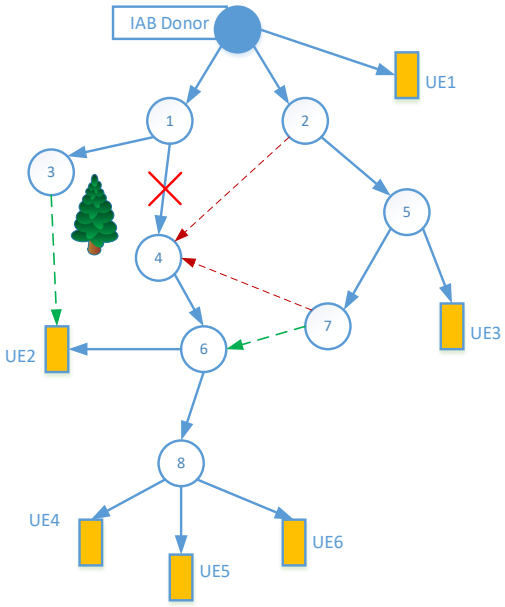


Figure 14: Example of a route recovery in an IAB network

It is worth noting that IAB architecture fits more into mesh networks than into ad-hoc, due to the presence of a fixed infrastructure. Nevertheless, in some application scenarios, such as vehicular (V2X) or non-terrestrial networks (NTN), mobility may cause some IAB-nodes to dynamically join and leave the IAB network [69]. Additionally, RAN sharing agreements in multi-tenant scenarios may have an impact on the availability or the resource allocation of the IAB links. This latter case may open the door to the integration of B-RAN approaches to influence the decision-making in the routing of traffic flows in IAB networks.

Within the NANCY project, we will focus on routing strategies to intelligently allocate flows to IAB paths. Moreover, we will aim at the application of AI/ML-based approaches to rule the selection of paths, particularly through Deep Reinforcement Learning (DRL).

#### 5.2.2.2 Relevant Technologies

As stated in the previous section, IAB and BAP-based routing are the main technologies to be considered in this scenario. In addition, AI/ML-based approaches are of special interest due to the large computational costs of applying optimal routing strategies that make them impractical in wireless scenarios with variable topology or traffic demands. Therefore, to reduce execution times, contemporary research field has delved into the utilization of Machine Learning techniques. The majority of these studies employ a Reinforcement Learning (RL) framework. In this framework, a routing agent is considered, which functions by choosing a path or next-hop as an action. The agent models the environment by utilizing counters present in the routing nodes and establishes a reward system that encapsulates a specific routing objective.

To this end, authors in [70] propose a DRL framework to solve the resource allocation and routing problem based on the local information of each agent (one per IAB node), aiming at minimizing the latency while satisfying the reliability requirements of URLLC flows. Another ML-based approach is presented in [71], which describes a genetic algorithm to assist the planning stage of IAB networks, and a routing heuristic to cope with temporary link blockages.

The integration of IAB and O-RAN architecture is also a relevant topic to be considered within the scope of NANCY. Authors in [72] discuss the main challenges of such an integration, focusing on the required

extensions of components and interfaces. Following the introduced approach regarding the application of AI/ML to enhance routing decision-making in IAB networks, a logical integration with O-RAN would rely on the implementation of such algorithms and agents as rApps and xApps within the non-RT and near-RT RICs frameworks.

#### 5.2.2.3 Proposed Innovation

The proposed innovation relies on the following two main contributions:

- Design of a novel IAB architecture that combines Sub6 and mm-wave multi-hop links. Although the baseline IAB solution only considered mm-wave frequencies, in urban environments these frequencies are often subject to blocking issues, and to non-line of sight performance degradation. In addition, the resources devoted to backhaul connectivity will remove capacity from the access network. Therefore, combining sub-6 GHz spectrum together with mm-wave frequencies in the backhaul segment will be a good approach to address both coverage and capacity requirements in dense urban deployments of small cells.
- Design and implementation of an IAB forwarding engine based on an online DRL agent. The envisioned solution will support flexible traffic engineering criteria to perform path allocations in Sub6 enhanced IAB networks, dynamically updating the flow to path mappings according to varying traffic demands.

#### 5.2.2.4 Relevant performance metrics

The relevant performance metrics will be mainly related to the capability of the proposed solution to meet the traffic engineering criteria compared to other alternatives. For instance, we are considering a throughput efficiency metric to capture the portion of offered load being carried by the network according to the allocated paths, and a fairness metric that characterizes the level of fairness among the routed flows. Nevertheless, additional criteria may be considered during the realization of the project.

Additionally, the adaptability of the solution to network dynamics will also be evaluated. First, the required period to infer a solution will determine the reaction time to load variations. Secondly, a proper performance under untrained topologies will be needed to consider scenarios where links or flows vary due to node mobility or RAN sharing agreements.

### 5.2.3 Point –to- Multipoint Connectivity

#### 5.2.3.1 Motivation and Objectives

Wireless communications are rapidly advancing, and within this landscape, point-to-multipoint (PMP) connectivity stands out as a key communication model. PMP communication, which enables one source to interact with multiple end-users at once, is gaining attention, especially in the 5G era and beyond. The increasing number and variety of connected devices call for more streamlined communication methods [60].

Point-to-multipoint (PMP) communication is a unique one-to-many connection model, providing multiple pathways from a central node to several end nodes [73]. In essence, PMP involves a base station communicating with multiple subscribers using shared network resources. Setting up a PMP network is relatively straightforward, especially when compared to point-to-point networks, as new equipment is only required at the subscriber's location [74]. The primary requirement is that all remote sites should be within the range and visibility of the base station. As sectors like industry, healthcare, and natural ecosystems increasingly digitize, the sheer number of devices seeking access to central resources highlights the limitations of traditional one-to-one communication, particularly its

bandwidth constraints [56]. PMP connectivity emerges as a solution, enabling efficient communication with multiple users without the need for individual connections, thereby optimizing bandwidth usage.

Such connectivity is particularly beneficial in broadcasting and multicasting scenarios where a base station transmits data to multiple receivers simultaneously [75]. In urban settings, where numerous devices might require access to a single data source, PMP ensures efficient data distribution. However, the increased connectivity that PMP offers also brings challenges, especially given the sheer number of devices it serves. Key concerns include maintaining quality of service, ensuring security, and distributing resources fairly among all endpoints. The primary goal of this section is to ensure consistent and high-quality connections for all connected devices.

#### 5.2.3.2 Relevant Technologies

Addressing PMP connectivity challenges requires innovative technological solutions. As multiple devices access a single data source, the integrity and authenticity of the data become crucial. It becomes challenging to identify or prevent unauthorized users from accessing the network. Blockchain, with its decentralized and unchangeable ledger system, provides a solution for authenticating edge users. Every data transaction recorded on the blockchain undergoes network verification, ensuring data integrity. Additionally, the transparency of blockchain allows all connected devices to view data transactions, fostering trust within the network.

Different end users in a PMP setup often have varied data consumption levels. Smart pricing policies can adjust costs based on data usage, ensuring fair charges for users. As data usage correlates with the resources a node uses to serve each user, smart pricing can also help balance resource distribution among users. By taking into account factors like data volume, connection duration, and network demand, these policies promote fair pricing and resource allocation for all connected devices.

In PMP configurations, the central source frequently faces a high volume of data requests. MEC can help by processing data closer to its source, offering intelligent functionalities near the end users. This decentralized approach to data processing ensures faster response times and lightens the load on the central source. Additionally, since edge computing is closer to end users, it can reduce access delays, enhancing the quality of service by improving network computing capabilities and reducing data transmission delays.

In conclusion, with the support of technologies like blockchain, smart pricing, and edge computing, PMP transmission can bolster the connectivity of wireless networks. This ensures security, quality of service, and fairness for all users.

## 5.3 Advanced connectivity of mobile nodes

This scenario supports vehicle-to-AP and vehicle-to-vehicle communication. Content is shared between vehicles and one vehicle acts as a relay to forward traffic to an access point or base station. Since vehicles may not trust each other, they need to use pseudonyms when sharing data to increase security and privacy protection. To this end, the project's Blockchain-based outcomes will be deployed on the edge and the vehicles. Moreover, to minimize connectivity gaps and increase the range of the cell-free vehicle network, NANCY enables multi-hop communications between vehicles.

### 5.3.1 Vehicle- to-AP

#### 5.3.1.1 Motivation and Objectives

The vehicle-to-AP communication requires a wireless technology with high coverage and low power consumption to support the mobility of the vehicles in outdoor scenarios. The 5G technology is suitable for this purpose as it provides wide area coverage, good performance in terms of latency/throughput and it is energy-efficient as well. The goal is to deploy a 5G network that interconnects the vehicle-to-vehicle ad-hoc network with the rest of the remote elements deployed in the context of the project.

#### 5.3.1.2 Relevant Technologies

The basis of vehicle-to-AP communication is provided by a 5G System, which is comprised of a 5G New Radio component and a 5G Core component as well as the vehicles equipped with a 5G UE module. This scenario adopts network slicing technology, where vehicles can connect to a slice that provides them with the computing and networking resources according to their communication requirements. This slice primarily provides URLLC capabilities, to minimize the latency of the communications between the vehicle and the base station.

MEC and task offloading along with intelligent orchestration capabilities are also crucial components of this scenario. MEC provides computational capabilities close to the vehicles generating the data, which are significantly lightweight in order to afford much processing power themselves. AI-based orchestration and task offloading algorithms contribute to the efficiency of the scenario by making cognitive decisions, ensuring the latency of the communications, and the placement of the computational tasks between the vehicles and the eligible MEC nodes.

Blockchain technology is used to guarantee the security and privacy of vehicles, through blockchain-based authentication using PQC signatures on the vehicles. This scenario adopts the B-RAN architecture developed in NANCY, built upon the O-RAN paradigm for the 5G RAN.

#### 5.3.1.3 Proposed Innovation

One of the vehicles in the fleet acts as a relay node and provides connectivity to the AP. This vehicle will have interfaces to both cellular and ad-hoc networks, which might require two different communication modules. This forwarding between interfaces requires novel strategies to manage the exchange of messages at a certain layer, e.g., network layer, application level, etc.

#### 5.3.1.4 Relevant performance metrics

The most relevant performance metrics for vehicle-to-AP communication are throughput and latency. Each metric has its own threshold, as it is shown in Table 5.

Table 5: Performance metrics and thresholds for vehicle-to-AP

| Performance metric | Threshold |
|---|---|
| Latency | < 50 ms (carrier-grade networks) |
| Throughput | Depends on the app |

### 5.3.2 Vehicle- to-vehicle

#### 5.3.2.1 Motivation and Objectives

Traditionally, vehicular communications have relied on ground infrastructure for the vehicle-to-vehicle (V2V) communication. However, the emerging vehicular services demand ever more stringent requirements that these approaches cannot satisfy, For instance, the vehicles can move far from the base station, so low latency cannot be guaranteed for applications that require real-time synchronization between vehicles, in case the communication needs to traverse the base station. In this case, V2V communications allow a direct exchange of data without the intervention of any

infrastructure (i.e., a base station or an access point). Dispensing with infrastructure also has drawbacks, such as the lack of a centralized entity that manages the network security. The goal is to deploy a secure and efficient V2V communication network that validates the feasibility of V2X scenarios in the context of the project.

#### 5.3.2.2 Relevant Technologies

The relevant technologies to this use case expand on the ones from the vehicle-to-AP, as this scenario complements it by providing an extension to the network by allowing communication between vehicles.

The technology to enable this type of vehicle-to-vehicle communication is C-V2X, the cellular V2X technology applicable to LTE and 5G. C-V2X uses the PC5 interface of the 5G architecture for the communication between vehicles, also known as the sidelink interface, as opposed to the Uu interface between the UE and the base station used in regular 5G communications.

However, sidelink relying to enable communication across several vehicles (i.e. multi-hop communication between vehicles) only began standardization in Release 17 of 3GPP. Therefore, to realize multi-hop communications, an additional software layer is required to be developed in order to program the routing logic across individual PC5 interfaces between each pair of vehicles.

#### 5.3.2.3 Proposed Innovation

The vehicles will be part of a V2X communication network in which the data is sent directly without the intervention of a centralized access point or base station. This limits the range of connectivity and requires strict coordination amongst the vehicles. The V2X modules must be lightweight to be onboarded into the vehicles. Attention must be paid to the noise and interference in the V2V communication because it can drastically reduce the quality of the signal. Therefore, this usage scenario might require the implementation of specific communication protocols that provide additional redundancy to minimize packet loss. In addition, the vehicles will have computing resources to perform data preprocessing and reduce the amount of traffic exchanged or implement security-related functionalities (blockchain). Moreover, multi-hop communication is also envisaged as part of this usage scenario. Some V2X standards already define the communication between two non-consecutive nodes, using a third node that acts as a relay. As in the case of vehicle-to-AP relay, such communication can be implemented at different layers.

#### 5.3.2.4 Relevant performance metrics

The most relevant performance metrics in V2V communication are latency and packet loss. Each metric has its own threshold, as it is shown in Table 6.

Table 6: Performance metrics and thresholds for vehicle-to-vehicle

| Performance metric | Threshold |
|---|---|
| Latency | < 50 ms (carrier-grade networks) |
| Packet loss | (Depends on the app) |

# 6 NANCY Demonstrators

The first step towards describing the NANCY use cases is to acknowledge the technical and business framework that has already started to revolve around 5G/6G technologies. The identification of the NANCY use cases reflects the developing 5G/6G ecosystem novelties and advancements when combined with Blockchain technology and AI algorithms. Considering this, the 5G and beyond technical aspects should be highlighted, mapped to the three proposed scenarios, and associated with proposed KVIs and KPIs as defined by the relevant standardization bodies.

The main objective of the proposed demonstrators is to evaluate the NANCY architecture in real and in two cases outdoor environments during the demonstrations that will take place in the context of WP6.

## 6.1 Demonstrator 1 Description

#### 6.1.1.1 Demonstrator Objective

To validate the efficiency of the CB-RAN architecture, the following applications will be implemented in this testbed:

1. Traffic management (critical machine type communications-MTC): the testbed will connect IoT devices that simulated traffic lights through 5G indoor links with the following requirements: (i) reliable and resilience connectivity; (ii) the IoT devices (simulated traffic lights) can be added/removed over time (ad-hoc connectivity); and (iii) data privacy and security are of high importance due to regulations. Traffic management is implemented using the connectivity part, and PQC functionalities will be foreseen to improve end-to-end data communication security. Crypto-agile libraries shall be integrated to generate E2E encryption using new PQC libraries which are being standardized by NIST.
2. IoT sensors measurements (massive MTC): sensor measurements are based on a traffic simulator able to yield a massive IoT scenario that needs to support high-uplink traffic and mobility management. An IoT simulator will generate a large number of messages with the same format as the IoT sensors. Large volume connection client/server application will demonstrate crypto agility and will collect performances of new PQC algorithms to compare with the ones currently in use (e.g., RSA, DSA, etc.)

The PQC Encrypt/decrypt modules will be able to deploy PQC cryptography. A PQC library is needed in both IoT device and edge IoT application. The PQC algorithm should be selected based on the computational capacity of the IoT devices, while the provider of the IoT devices should identify the libraries that support PQC in the device and in the edge application that is receiving the data from the sensors.

The demonstrator architecture is represented in the Figure 15

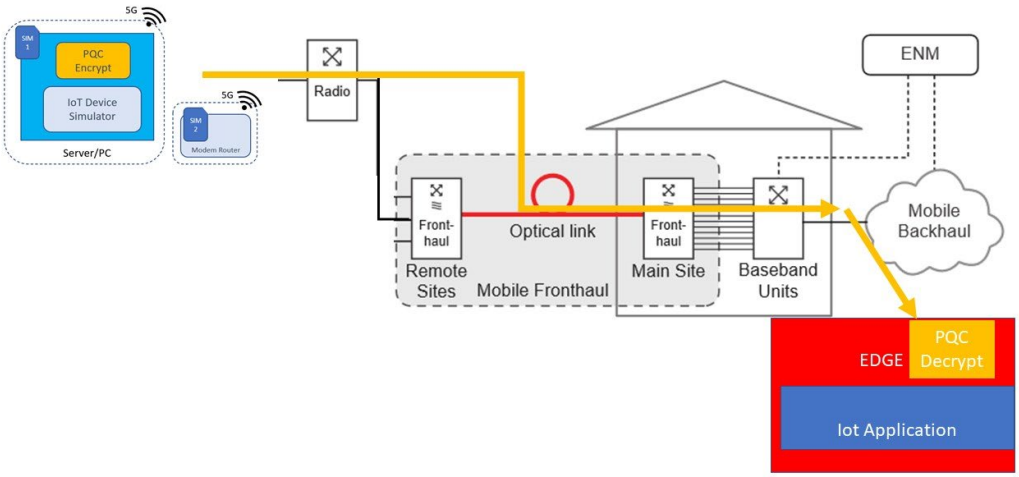


Figure 15: TEI's testbed topology for NANCY Use Case

#### 6.1.1.2 Actors, Risks, Challenges, Assumptions

Several actors are involved in the NANCY value chain such as Network Operator, Application Developers, Infrastructure Providers, Datacenter Service Providers, and Virtualization Infrastructure Service Providers.

Introducing new encryption algorithms to deliver secure traffic can impact performance and therefore transmission delay and increase power consumption which can impact particular IoT devices that have limited battery power available.

New actors may be added depending on the services and/or network applications.

#### 6.1.1.3 Main Blocks of NANCY architecture

The following architectural components will be showcased by the demonstrator:

- 5G technology
- Edge Computing
- Self-healing and self-recovery mechanisms @Edge
- Task offloading
- PQC secure communication

#### 6.1.1.4 Relevant requirements for demonstrator nr.1 (Italian massive-IoT testbed)

The Italian Massive IoT testbed aims to demonstrate a fixed topology fronthaul 5G network with direct connectivity. This setup could showcase specific aspects and applications related to IoT Technology.

Fronthaul networks can indeed be deployed in both point-to-point and point-to-multipoint topologies, offering different advantages based on the specific needs of the network and the applications it supports.

The demonstrator will be deployed and assessed in TEI's testbed located in Genoa (Italy). This testbed is part of the Italian Ericsson Research and Development organization, and it is a private Network in a controlled environment.

The Ericsson Mobile Network used for the tests will evolve throughout the project: it allows to collect results, during the applications integration facilitating the comparison of the performances in the two architectures.

In the first phase, a non-stand-alone (NSA) architecture is implemented. From RAN's perspective, the Ericsson Radio 4422 and the Baseband 6648 will be used. In this scenario, the server for the application will be connected to the EPG and reachable by the client side through a dedicated 5G device. The fronthaul connection is implemented by the optical Ericsson FH6000 family nodes, allowing a fully flexible optical transport solution.

The second phase foresees the usage of a stand-alone (SA) architecture with the advantage of delivering the full potential of 5G mobile networks. From hardware perspective, the baseband will be the same (BB6648), the fronthaul solution will be based on the same FH6000 family nodes scaling the fronthaul rate at 25Gb (eCPRI), while the radio solution will be evaluated, depending on the phase 1 test results, between a wide range of available nodes.

Nowadays AIR6419 and AIR1281 are the two considered solutions: they are already integrated in the laboratory, and they could be the most interesting implementation for the project scope.

Table 7: Functional Requirements for Demonstrator 1

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D1_FUNCT-1** | 5G Core & RAN Deployment | Mandatory | The deployment of 5G Radio with NSA and SA allows for the advantages of a full 5G architecture. | Infrastructure Requirement |
| **D1_FUNCT-2** | Mode of Operation | Mandatory | The testbed will be capable of supporting both 5G NSA and SA mode. | Infrastructure Requirement |
| **D1_FUNCT-3** | Edge computational capabilities | Mandatory | To ensure processing capabilities near the end user, edge servers need to be deployed. | Infrastructure Requirement |
| **D1_FUNCT-4** | Integration of measurement tools | Mandatory | Measurement tools should be deployed to gather relevant metrics necessary to validate the corresponding KPIS of the demonstrator. | Infrastructure Management |
| **D1_FUNCT-5** | Monitoring | Mandatory | Monitoring information derived from the execution shall be collected. | Resource Management |

Table 8: Non- Functional Requirements for Demonstrator 1

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D1_NFUNCT-1** | KPI & KVI Validation | Mandatory | It will be possible to perform relevant measurements for assessing and validating the targeted KPIs and KVIs | |

| | | | | |
|---|---|---|---|---|
| | | | within the 5G massive IoT demonstrator. | |
| **D1_NFUNCT-2** | Security & Privacy | Mandatory | The demonstrator aims to enforce robust security measures, preventing unauthorized access, and reducing potential threats. Compliance with General Data Protection Regulation (GDPR) requirements is considered mandatory. | |
| **D1_NFUNCT-3** | Low latency | Mandatory | Maximum end-to-end latency shall be guaranteed in the testbed. | |
| **D1_NFUNCT-4** | Availability and Reliability | Mandatory | Availability and reliability must be taken into account in terms of the maximum allowed downtime. | |
| **D1_NFUNCT-5** | Authentication & authorization | Mandatory | Authentication and authorization mechanisms must be ensured. | |

#### 6.1.1.5 Targeted Demonstrator 1 KPIs & KVIs

An overview of the measurement capabilities from the NANCY Demonstrator - 1 with respect to the KPIs defined is summarized in Table 9.

The purpose of KVIs is twofold: the first is to identify the expected value benefits from technology usage, and the second is to provide a basis for a value-driven design of technology. In the following tables, the demonstrator-specific KPIs and KVIs are identified.

Table 9: Demonstrator 1 Targeted KPIs

| KPI ID | Name | Description | Targeted Value (KPI) |
|---|---|---|---|
| **D1-KP1** | Latency | Low latency should be achievable for this UC, for the efficient delivery of the service. | Network Latency: < 15- 20 ms |
| **D1-KP2** | High Availability | Ensuring 'Five nines' availability is crucial, particularly in healthcare applications and emergency services, as any brief downtime can result in significant consequences. | 99.999% |
| **D1-KP3** | High Bandwidth | High Bandwidth is required to satisfy the cumulative capacity needs of massive IoT device throughput. | up to 1Gbps |

Table 10: Demonstrator 1 Targeted KVIs

| KVI ID | Name | Description | Assessment |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **D1-KV1** | Environmental sustainability | KV related to SDGs #6, 13, 14, 15 | Objective evaluation by experts |
| **D1-KV2** | Societal sustainability | KV related to SDGs #1, 2, 3, 4, 5, 7, 11, 16 | Objective evaluation by experts and representatives |
| **D1-KV3** | Digital inclusion | KV reflecting partly UN SDG #6,15, in people being part of the digital world | Objective evaluation by experts, and subjective evaluation by representatives |
| **D1-KV4** | Trust | Ensure security in the communication between remote and application | Objective evaluation by security experts and/or tests |
| **D1-KV5** | Economical sustainability and innovation | KV related to SDGs # 9, 10, 11 | Objective evaluation by experts |

## 6.2 Demonstrator 2 Description

#### 6.2.1.1 Scope of the Demonstrator

This demonstrator aims to validate the NANCY architecture regarding its support of vehicle networks involving communication scenarios between vehicles. Based on the architecture developed in WP3, the demonstrator will employ MEC capabilities to validate the AI-based B-RAN orchestration mechanisms developed in WP3 and WP4 to optimize the vehicular network topology (including direct and multi-hop communications). One of the vehicles has some computational capabilities, enabling the demonstrator to employ the novel resource-aware policies and scaling mechanisms developed in NANCY for computational offloading. The demonstrator will also validate the NANCY mechanisms for efficient and trustworthy resource allocation and resource management through network slicing developed in WP4, employing a URLLC network slice that guarantees a latency of a few milliseconds. Overall, this demonstrator aims to validate how the different policies and mechanisms developed in NANCY can maximize energy efficiency and system scalability, whilst ensuring the latency and data rate requirements.

#### 6.2.1.2 Actors, Risks, Challenges, Assumptions

Several actors are involved in the NANCY value chain. For the specific demonstrator, it should be noticed that the actors mentioned below represent the core actors participating in this demonstrator. New actors may be added depending on the services and/or network applications.

- Block chain providers
- Application Developers
- V2X equipment vendor/developer (the team who supplies the equipment and provides the technical assistance for troubleshooting purposes).
- Vehicle driving assistant (a person who is in charge of or who gives the necessary tips to drive the specific vehicle in which the testbed will be deployed).

#### 6.2.1.3 Targeted Demonstrator 2 KPIs & KVIs

According to the description provided in Section 5.3, latency and throughout are the most relevant performance metrics for vehicle-to-AP and vehicle-to-vehicle communications. Therefore, Table 10 describes the KPIs addressed in this demonstrator.

The purpose of KVIs is twofold: the first is to identify the expected value benefits from technology usage, and the second is to provide a basis for a value-driven design of technology. In the following tables, the demonstrator-specific KPIs and KVIs are identified.

Table 11: Demonstrator 2 Targeted KPIs

| KPI ID | Name | Description | Targeted Value (KPI) |
|---|---|---|---|
| **D2-KP1** | E2E Service Latency | The round-trip delay between two services/applications. Ideally, one should be running in the vehicular node and the other one in the ground (MEC or any other location). | < 25 ms |
| **D2-KP2** | V2V Latency | The round-trip delay between 2 mobile nodes using direct V2V communication. | < 20-100 ms (ETSI TS 122 185 V16.0.0) |
| **D2-KP3** | V2I Latency | The round-trip delay between a mobile node and its corresponding base station. | < 15 ms |
| **D2-KP4** | Network Availability | Network Availability is measured as the total time of network accessibility and delivery of data traffic between network components to the total monitored period. Although the target is 100%, the most commonly referenced goal is known as “five nines,” or 99.999% availability. $Availability = \frac{T_{available}}{T_{total}} * 100\%$ | 99.999% |
| **D2-KP5** | Network Reliability | Reliability is the total time the network is delivering data packets with a latency of less than 5 msec compared to the total monitored period. $Reliability = \frac{T_{reliable}}{T_{total}} * 100\%$ | 99.999% |
| **D2-KP6** | V2V data rate | | |
| **D2-KP7** | V2I data rate | | |
| **D2-KP8** | Enhanced Security (data and access security) | It is required at the distributed computing resources in order to ensure that the application components are not compromised. | |
| **D2-KP9** | Network Coverage | | 100% |

| | | | |
|---|---|---|---|
| **D2-KP10** | Energy efficiency improvement | Energy efficiency improvement compared to SOTA mechanisms. | 20% |

Table 12: Demonstrator 2 Targeted KVIs

| KVI ID | Name | Description | Assessment |
|---|---|---|---|
| **D2-KV1** | Environmental sustainability | KV related to SDGs #6, 13, 14, 15 | Objective evaluation by experts |
| **D2-KV2** | Societal sustainability | KV related to SDGs #1, 2, 3, 4, 5, 7, 11, 16 | Objective evaluation by experts and representatives |
| **D2-KV3** | Digital inclusion | KV reflecting partly UN SDG #10, in people being part of the digital world [6][15] | Objective evaluation by experts, and subjective evaluation by representatives |
| **D2-KV4** | Trust | The sense of confidence, faith and explainability in the way that advanced systems (e.g., AI-driven decision-making) may impact humans | Objective evaluation by experts, and subjective evaluation by representatives |
| **D2-KV5** | Economical sustainability and innovation | KV related to SDGs #8, 9, 10, 12 | Objective evaluation by experts |

#### 6.2.1.4 Main Blocks of NANCY architecture

**Vehicle-to-Everything (V2X)**

The added value of the NANCY V2X for this scenario focuses on the following:

- Performance

V2X technology allows vehicles to directly exchange their information by one-hop transmission. In this mode, the transmitter sends the information to one or more receivers directly. Since this mode operates in a broadcast manner, the same data can be transmitted efficiently to multiple nodes in a common resource. In this mode, the latency mainly occurs while establishing the uplink connection and resource allocation. Furthermore, the cellular version of V2X (C-V2X) can implement additional mechanisms at the PHY layer, such as shortened transmission time intervals (TTI) [76] and self-contained subframes, to reduce the latency of the transmission.

V2X also reduces the infrastructure-dependency as it allows the deployment of ad-hoc communication networks that can be self-contained. This means that the network can be fully controlled and operated by the same organization, reducing the dependency on external network managers, and enabling the adaptation to custom scenarios.

- Extended coverage

The ad-hoc nature of V2X technology is suitable for extending the coverage of cellular networks. In this way, a node inside the V2X network can act as a relay node and forward traffic from the ad-hoc network to the infrastructure and vice versa. This functionality requires the implementation of a multi-hop transmission system that allows forwarding the traffic between two nodes using an intermediate relay node. In this sense, existing V2X technologies already provide efficient mechanisms, such as

intelligent multi-hop relay selection and route searching, to extend the communication over a large area without degrading the performance of the ad-hoc network (e.g., minimizing the throughput) [77].

- Functional redundancy and resilience

Direct communication between vehicles can be used as a backup interface for the traditional Uu interface in cellular networks. The duplication of messages via relatively independent channels can reliably support very critical safety use cases. In addition, V2X communications show a better performance in high-mobility scenarios with complex movements, which also increases the reliability compared to only infrastructure-based cellular networks.

**5G technology**
The added value of the NANCY 5G technology for this scenario focuses on the following:

- Reduce latency (within URLLC slice)

**AI-based orchestration**
The added value of the NANCY AI-based orchestration for this scenario focuses on the following:

Orchestration stands as the center in the realization of the transformative potential promised by 5G networks. 5G technology brings unprecedented speeds, ultra-low latency, and unparalleled connectivity, along with a spectrum of applications from smart cities to the Internet of Things (IoT) and autonomous vehicles. However, the complexity inherent in 5G's architecture, with its diverse network slices, dynamic service requirements, and heterogeneity, poses formidable challenges to effective orchestration. Coordinating and managing this multifaceted ecosystem in real-time demands sophisticated orchestration mechanisms, facing hurdles of scalability, interoperability, resource optimization, and adaptability within a dynamic network landscape.

Integration of AI-based methodologies presents an option to overcome the challenges inherent in orchestrating 5G networks, using as a base the proposed NANCY architecture. Leveraging machine learning algorithms, predictive analytics, and intelligent decision-making capabilities, AI offers the potential to alleviate the complexities of orchestration. By harnessing AI's prowess, orchestration systems can dynamically adapt, predict network demands, optimize resource allocation, automate decision-making, and ensure agile responsiveness to varying network conditions. Through AI-driven insights, orchestration stands to evolve into a proactive, self-optimizing framework capable of preemptively addressing network intricacies, thereby enhancing efficiency, scalability, and the overall performance of 5G networks.

An additional part of the AI-based orchestration lies in the role of a slice manager. Tasked with dynamically provisioning and managing network slices tailored to diverse service requirements, the slice manager serves as the backbone of orchestrating the complex 5G ecosystem. Its ability to allocate resources, balance network loads, and accommodate varied slice demands is crucial. Integrating AI-based techniques within the realm of slice management holds immense promise. AI empowers the slice manager with predictive analytics, learning capabilities, and adaptive decision-making, enabling it to efficiently optimize slice configurations, anticipate service needs, and autonomously adjust network resources in real-time. The amalgamation of AI-driven intelligence with the slice manager's functionalities not only streamlines orchestration complexities but also paves the way for an agile, responsive, and future-proofed network architecture capable of catering to a diverse array of service scenarios.

**Blockchain**

The added value of the NANCY Blockchain for this scenario focuses on the following:

- Overall Security

The NANCY Blockchain will be a permissioned blockchain. This means that it will run based on a known consortium, and nodes can be legally linked to each other. Also, since misbehavior is not anonymous, abuse can be easily connected to one or more identifiable nodes. Overall, a permissioned blockchain allows access to only the consortium members and can limit certain rights for certain nodes in the chain. Malicious or fraudulent nodes can be excluded from the system. This is important in an outdoor scenario, which lacks the level of control that the in-lab test-beds will have.

It is most likely that an implementation like Hyperledger Fabric is eventually used. In this case, the NANCY Blockchain would have an additional layer of control called channels.

A Hyperledger Fabric channel is a private "subnet" of communication between two or more specific network nodes, for the purpose of conducting private and confidential transactions. The channel policies, members and anchor peers can be configured as needed. Although any one anchor peer can belong to multiple channels, and therefore maintain multiple ledgers, no ledger data can pass from one channel to another. When adding a new member to an existing channel, either a genesis block or if applicable, a more recent reconfiguration block, is shared with the new member. Each peer that joins a channel is authenticated by its organisation's certificate.

- Enhanced Security at crypto level (PQC)

Quantum computing [78] threatens blockchain protocols and networks because they utilize non-quantum-resistant cryptographic algorithms. When quantum computers become robust enough to run Shor's algorithm on a large scale, the most used asymmetric algorithms, utilized for digital signatures and message encryption, such as RSA, (EC)DSA, and (EC)DH, will be no longer secure. Post-quantum cryptography (PQC) refers to a new generation of asymmetric algorithms that cannot be broken by Shor's algorithm and therefore are considered quantum-resistant. Unlike QKD, PQC does not rely on any underlying quantum processes for the exchange of symmetric key pairs but rather on leveraging mathematical problems more complex than the existing ones for the generation of asymmetric keys. The User Equipment in the scenario will be equipped with smart cards that will enable the use of PQC within the Blockchain.

- Trusted database

Blockchain will be used not only for registering users in the scenario, but also for maintaining traceability and auditability of SLAs among them. In this sense, the NANCY Blockchain will be similar to other examples in the supply chain and logistics industries

- Marketplace

Blockchain will be also used for the marketplace implementation to create a secure and transparent ecosystem where providers and consumers engage in the exchange of 5G services and resources. Furthermore, smart pricing policies are securely applied over Blockchain for fair incentives to users in terms of tokens and reputation.

- Task offloading

In this demonstrator task offloading is a main enabling mechanism for vehicular scenarios, focusing on two main objectives: (i) latency must be constrained to allow critical v2x scenarios, (ii) on-device computation should be complemented to manage large computation loads. In this regard, the

developed task-offloading-related mechanisms will be integrated with the orchestration engine, to deploy and migrate services whose behavior will be policy-driven. Task offloading decisions will be inferred by AI-engines which will select the best node and policy to manage the request according to the specified user and service requirements as well as the status of the eligible computation nodes.

- Caching mechanisms

Closely related to task offloading, the envisioned caching mechanisms streamline the start-up time of services and procedures. Predictions made about needed data, UE movement, memory and load needs, or even available instances are used to prepare the infrastructure to accomplish policy requirements. In this sense, Task offloading leverages the developed caching mechanisms to perform seamless service handover, not just of network functions but also of its associated state and data.

- Cell-free access mechanisms

Envisioned cell-free access mechanisms incorporate the use of M-RAT Nomadic Connectivity Providers (MultiRAT-NCP) to provide advanced connectivity to 5G and non-5G subscribers. D2D and ad-hoc radio connections are used as the fronthaul to provide flexible radio links which channel will be encapsulated by the MultiRAT-NCP as a uu link towards the 5G backhaul, establishing a direct connection between the user device and the core network, avoiding unnecessary intermediate nodes. The designed solution is also mobile, therefore given the nature of this device, it will allow dynamic connections enriched by the use of the novel NANCY Identity Management from which authentication an authorization is derived.

- Identity Management

Blockchain-based authentication enables non-5G subscribers to access NANCY services and external data networks through a 5G backhaul. The NANCY Identity Management is based on a privacy-preserving certificate-based approach in which capabilities associated with the user are retrieved to determine which services can be used as well as the associated QoS levels. The NANCY Identity Management leverages the nature of blockchain to obtain trustful acknowledgment of the presented identity. EAP-PSK related to 5G authentication is used to issue trustful certificates. Pseudonyms will be used to keep the privacy of the user from 3rd parties.

#### 6.2.1.5 Relevant requirements for demonstrator nr.2 (Spain Outdoor)

The 5G testbed that is going to be used in this NANCY demonstrator is a 5G deployment in a sports center located near the premises of the University of the Basque Country. This testbed will include a portable 5G RAN with O-RAN support (including RRU, DU, and CU) that will accommodate the developments of the NANCY project regarding the B-RAN architecture. The UPF and core network will be located on the premises of the University of the Basque Country, where the developments of the NANCY project in regards to intelligent orchestration mechanisms will also be hosted. The 5G network will be SA and also support network slicing.

The testbed will include three mobile vehicle units with each a 5G module and each a V2X module. V2V communications will be used between vehicles, which will also communicate to the 5G base station thanks to their 5G module. A multi-hop algorithm will be developed using the SDK tools provided by the V2X module vendor and will be included in each vehicle unit. Additionally, some computational capabilities are included in one of the vehicles to enable the efficient computational offloading capabilities developed in NANCY.

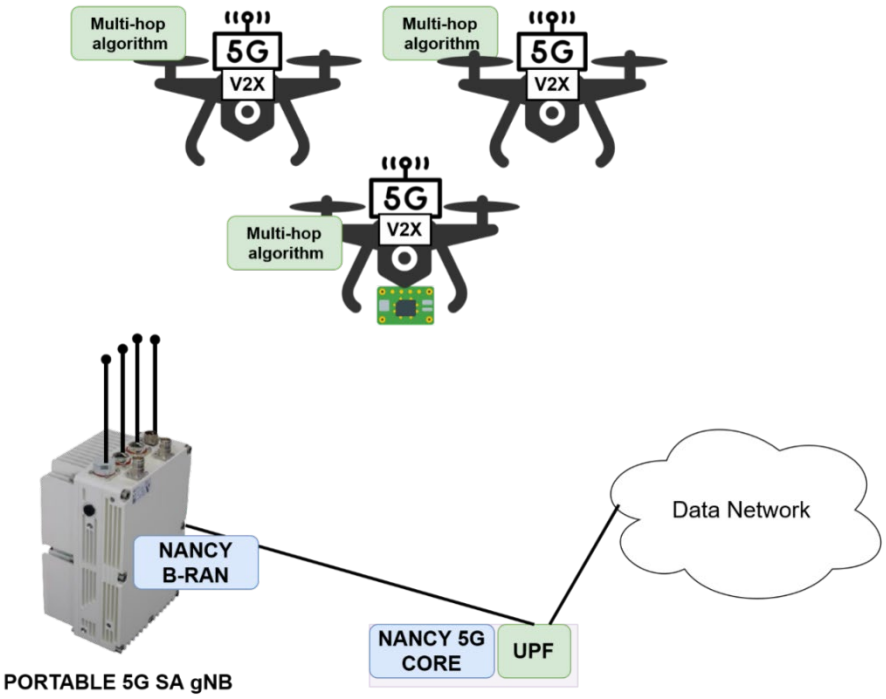


Figure 16: Testbed topology for NANCY Spanish demonstrator

Table 13: Functional Requirements for Demonstrator 2

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D2_FUNCT-1** | 5G Core & RAN Deployment | Mandatory | 5G SA RAN and core components will be available for s demonstration involving aggregation of technologies and other interworking capabilities | Infrastructure Requirement |
| **D2_FUNCT-2** | Mode of Operation | Mandatory | The testbed (core network, RAN, and UEs) shall support 5G SA mode of operation and support V2V mode of operation and multi-hop communications between UEs | Infrastructure Requirement |
| **D2_FUNCT-3** | MEC computational capabilities | Mandatory | One of the vehicles of the testbed shall contain some computational capabilities | Infrastructure Requirement |
| **D2_FUNCT-4** | Integration of measurement tools | Mandatory | The infrastructure layer shall deploy measurement tools. It shall also embrace | Infrastructure Management |

| | | | | |
|---|---|---|---|---|
| | | | the gathering of relevant metrics required for the validation of the corresponding demonstrator KPIs. | |
| **D2_FUNCT-5** | Monitoring | Mandatory | The system shall provide monitoring information derived from the demonstration execution. | Resource Management |

Table 14: Non- Functional Requirements for Demonstrator 2

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D2_NFUNCT-1** | KPI & KVI Validation | Mandatory | The 5G testbed along with all NANCY demonstrator components shall be able to measure and validate the targeted KPIs & KVIs | |
| **D2_NFUNCT-2** | Security & Privacy | Mandatory | The 5G testbed along with all NANCY demonstrators shall implement robust security measures to prevent unauthorized access and mitigate potential threads. Compliance with General Data Protection Regulation (GDPR) requirements is considered mandatory. | |
| **D2_NFUNCT-3** | Network Slicing | Mandatory | The testbed should support network slicing, allowing the creation of customized virtual networks to meet the specific requirements of the demonstrator. | |
| **D2_NFUNCT-4** | Low latency | Mandatory | The NANCY ecosystem should support maximum end-to-end latency of 5ms | |
| **D2_NFUNCT-5** | Availability and Reliability | Mandatory | The NANCY ecosystem shall provide continuous, uninterruptable operation during demonstrations. | |
| **D2_NFUNCT-6** | Authentication & authorization | Mandatory | The NANCY ecosystem shall provide means for authentication and authorization for accessing. | |

## 6.3 Demonstrator 3 Description

#### 6.3.1.1 Scope of the Demonstrator

NANCY Demonstrator 3 aims to deliver high-performance services with low latency and several 5G/6G network capabilities as described in the literature. In his respect, this demonstrator has two specific objectives that are linked directly to the concept of B5G /6G.

To validate and demonstrate the proposed B5G/6G technologies and algorithms that will be developed by NANCY partners. In this respect, technologies such as task offloading, and policies related to smart pricing will be integrated into the NANCY architecture and evaluated for their maturity. Moreover, the demonstrator will utilize the overall NANCY architecture and several of the NFs and policies developed in WP3-WP5, with a focus on orchestration, computational and storage offloading, social-aware caching, as well as security and privacy in order to demonstrate their effectiveness in supporting latency-critical broadband applications.

For this purpose, 5G AR/VR applications will be considered, exploiting the capabilities of the B5G integrated NANCY ecosystem, consisting of NANCY partners' algorithms and technologies. These applications will be developed by NANCY partners and are expected to have a direct pact on several vertical industries indicating surveillance and /or physical security service.

In the context of this use case, 5G AR/VR services will be considered, exploiting the capabilities of the NANCY architecture aiming to deliver high-performance services along with a number of 5G network capabilities. For this reason, a multi-domain deployment consisting of distinct Edge and Cloud compute domains providing:

- Advanced Security at Edge Cloud deployment, also enhanced by Blockchain algorithms.
- High availability and resilience through mesh architectures
- High capacity and low latency

The orchestration layer will be capable of collecting and processing the topology, the capabilities and characteristics of the multiple compute domains to higher Network Operation / Digital Service provisioning layers. Specific QoS characteristics for the consideration of the proposed applications will be considered.

The NANCY network deployment that will support the above-mentioned Use Case is shown Figure 18.

#### 6.3.1.2 Actors, Risks, Challenges, Assumptions

Several actors are involved in the NANCY value chain. For the specific demonstrator, it should be noticed that the actors mentioned below represent the core actors participating in this demonstrator. New actors may be added depending on the services and/or network applications.

- Mobile Network Operator: provides 5G connectivity and access to end-users,
- Service Provider: An entity whose business is to provide telecom and other services to the end-user (corporate, residential or other).
- Blockchain provider.
- Application Developers.
- Virtualization Infrastructure Service Providers.

#### 6.3.1.3 Targeted Demonstrator 3 KPIs & KVIs

An overview of the measurement capabilities from the NANCY Demonstrator - 3 with respect to the KPIs defined in Section 2.3 is summarized in Table 15. As can be seen from the table, a great number of KPI's will be covered in this demonstration, verifying the scope of the projects.

The purpose of the KVIs is twofold: the first is to identify the expected value benefits from technology usage, and the second is to provide a basis for a value-driven design of the technology. In the following tables, the demonstrator-specific KPIs and KVIs are identified.

Table 15: Demonstrator 3 Targeted KPIs

| KPI ID | Name | Description | Targeted Value (KPI) |
|---|---|---|---|
| **D3-KP1** | Network Latency - E2E Service Latency | Network Latency is the time it takes for data packet to pass from source to destination. Low latency should be achievable for this UC, for the efficient delivery of the service. | Network Latency: < 5ms. |
| **D3-KP2** | Network Offloading Latency | | 0.1-0.3sec/GB |
| **D3-KP3** | Network Availability | Network Availability is measured as the total time of network accessibility and delivery data traffic between network components to the total monitored period. Although target is 100% the most commonly referenced goal is known as "five nines," or 99.999% availability. $Availability = \frac{T_{available}}{T_{total}} * 100\%$ | High Availability: 99.999% |
| **D3-KP4** | Network Reliability | Reliability is the total time the network is delivering data packets with latency less than 5msec compared to the total monitored period. $Reliability \frac{T_{reliable}}{T_{total}} * 100\%$ | High Reliability : 99.9999% |
| **D3-KP5** | Bandwidth | High Bandwidth is required to satisfy the cumulative capacity needs of AR/VR services | up to >1Gbps |
| **D3-KP6** | Range Expansion | | 100m |
| **D3-KP7** | Ownership Cost Reduction | | -20% |
| **D3-KP8** | Data and Access Security | It is required at the distributed computing resources in order to ensure that the application components are not compromised. | 99.99% |
| **D3-KP9** | Network Coverage | | 100% |
| **D3-KP10** | Detection Rate | | 80-90% |

| | | | |
|---|---|---|---|
| **D3-KP11** | Verification | | 1ms |
| **D3-KP12** | Block throughput | | 10-20 operations /node/sec |
| **D3-KP13** | Key generation | | 1ms |
| **D3-KP14** | Signing | | 10ms |

Table 16: Demonstrator 3 Targeted KVIs

| KVI ID | Name | Description | Assessment |
|---|---|---|---|
| **D3-KV1** | Environmental sustainability | KV related to SDGs #6, 13, 14, 15 | Objective evaluation by experts |
| **D3-KV2** | Societal sustainability | KV related to SDGs #1, 2, 3, 4, 5, 7, 11, 16 | Objective evaluation by experts and representatives |
| **D3-KV3** | Digital inclusion | KV reflecting partly UN SDG #10, in people being part of the digital world [6], [15] | Objective evaluation by experts, and subjective evaluation by representatives |
| **D3-KV4** | Trust | The sense of confidence, faith and explainability in the way that advanced systems (e.g., AI-driven decision-making) may impact humans | Objective evaluation by experts, and subjective evaluation by representatives |
| **D3-KV5** | Economical sustainability and innovation | KV related to SDGs #8, 9, 10, 12 | Objective evaluation by experts |

#### 6.3.1.4 Main Blocks of NANCY architecture

**Blockchain**
The added value of the NANCY Blockchain for this scenario focuses on the following:

- Performance

Hyperledger Fabric is one of the blockchain frameworks most frequently used by industry consortia, even transnationally. Fabric can offer very good performance if properly configured. Fabric, for instance, scales exceedingly well [79] with CPU-heavy transactions but struggles with transaction payloads larger than 100 kB. Many considerations [79] [80] can help optimize performance for a Hyperledger Fabric network.

Maximum throughput depends largely on the type of transaction and the type of hardware. For homogeneous hardware, there is a clear correlation between maximum throughput and CPU use across highly heterogeneous deployments. The kind of database, the visibility of transactions (private

transactions achieve lower throughput), and network size (large Fabric networks have lower throughput) also impact maximum throughput and CPU (Figure 17). Therefore, these parameters should be considered with particular attention to detail when conceptualizing the network architecture for a use case with high-performance requirements.

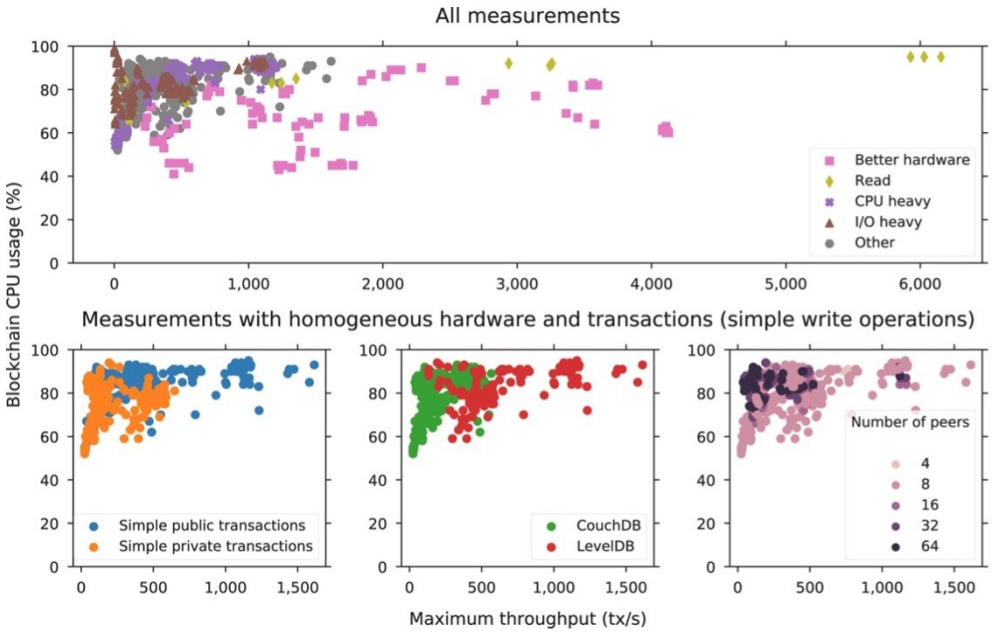


Figure 17: Measurements and the most important design parameters

Lighter consensus mechanisms, in close connection with the block time parameter, will be studied as well.

- Overall Security

The NANCY Blockchain will be a permissioned blockchain. This means that it will run based on a known consortium, and nodes can be legally linked to each other. Also, since misbehavior is not anonymous, abuse can be easily connected to one or more identifiable nodes. Overall, a permissioned blockchain allows access to only the consortium members and can limit certain rights for certain nodes in the chain. Malicious or fraudulent nodes can be excluded from the system. This is important in an outdoor scenario, which lacks the level of control that the in-lab testbeds will have.

It is most likely that an implementation like Hyperledger Fabric will eventually used. In this case, the NANCY Blockchain would have an additional layer of control called channels. A Hyperledger Fabric channel is a private "subnet" of communication between two or more specific network nodes, for the purpose of conducting private and confidential transactions. The channel policies, members and anchor peers can be configured as needed. Although any one anchor peer can belong to multiple channels, and therefore maintain multiple ledgers, no ledger data can pass from one channel to another. When adding a new member to an existing channel, either a genesis block or if applicable, a more recent reconfiguration block, is shared with the new member. Each peer that joins a channel is authenticated by its organisation's certificate.

- Enhanced Security at crypto level (PQC)

Quantum computing [78] threatens blockchain protocols and networks because they utilize non-quantum-resistant cryptographic algorithms. When quantum computers become robust enough to run Shor's algorithm on a large scale, the most used asymmetric algorithms, utilized for digital

signatures and message encryption, such as RSA, (EC)DSA, and (EC)DH, will be no longer secure. Post-quantum cryptography (PQC) refers to a new generation of asymmetric algorithms that cannot be broken by Shor's algorithm and therefore are considered quantum-resistant. Unlike QKD, PQC does not rely on any underlying quantum processes for the exchange of symmetric key pairs but rather on leveraging mathematical problems more complex than the existing ones for the generation of asymmetric keys. The User Equipment in the scenario will be equipped with smart cards that will enable the use of PQC within the Blockchain.

- Trusted database

Blockchain will be used not only for registering users in the scenario but also for maintaining traceability and auditability of SLAs among them. In this sense, the NANCY Blockchain will be similar to other examples in the supply chain and logistics industries

- Task offloading

Task offloading is one of the primary enabling technologies for resource-demanding services, e.g., AR and VR, as controlled response times are crucial to achieving the desired quality of experience. In this regard, task offloading mechanisms will be used to move computational load from constrained devices and far compute nodes to the most adequate edge node, considering the demanded computational resources and its latency with the UE. Therefore, it will be selected the edge node where enough resources to process the workloads are provided and latency is constrained to provide high-quality services.

- User-centric cache

Closely related to task offloading, cache mechanisms enhance service delivery by streamlining the movement of correlated user data. Cache brings the potential requested data close to the compute node where the computational load will take place. The selection of the data depends on the type of service requested and their characterization. For services highly related to UE's location, e.g., AR or VR, assets that belong to the same area and direction of movement could be prepared for later use.

- Smart pricing policies

The concept of Smart Pricing Policies (SPP) encompasses a comprehensive framework in which the conventional role of UE undergoes a revolutionary change, transitioning from a passive consumer of communication services to an active producer. This paradigm is predicated upon sophisticated artificial intelligence tools and game theory principles in order to offer financial incentives for users. The framework seeks to maximize the equilibrium between expanding the potential for value creation for consumers and ensuring profitability for MNOs by utilizing these technologies. Smart pricing policies leverage auction theory tools to enable the development of novel pricing models. Auctions offer distinct benefits by serving as an effective way for users to achieve greater revenue in comparison to static pricing models. In addition, game-theoretic techniques are utilized to develop resource allocation strategies, effectively representing the dynamics of conflicts and cooperation among users within the framework of Beyond Radio Access Network. The comprehensive strategy outlined in this study not only takes into account economic factors but also promotes the effective allocation of resources and collaboration within the constantly changing field of wireless communication.

Aiming at B5G and 6G, NANCY will deploy novel smart pricing policies between users to overcome the current limitations of RAN networks. The implementation of smart pricing policies will be made possible thanks to the integration of blockchain in the RAN architecture. The goal is to balance high revenues for data sellers and cost-effective solutions for buyers. Additionally, NANCY plans to offer

computational offloading incentives, such as discounted access fees and token rewards for users contributing to the B-RAN. Reputation-based rewards and tiered pricing based on resource contributions will be explored, creating a flexible and user-centric ecosystem within NANCY.

#### 6.3.1.5 Relevant requirements for demonstrator nr.3 (Greek Outdoor)

The 5G testbed that is going to be used in this NANCY Demonstrator 2 is an advanced large-scale 5G SA experimental facility, which is spread across two different locations within the metropolitan region of Athens, which are interconnected with a dedicated 10G dark fiber.

The OTE 5G SA network is based on ATHONET 5G SA Core and ERICSSON Baseband Unit (BBU) /Remote Radio Unit (RRU)/RAN. More specifically, the ATHONET 5G Core is located in OTE Academy premises and is used to drive two ERICSSON BBU units, one deployed at OTE campus and one deployed at a distant campus. Each of these two BBUs is controlling three ERICSSON RRU/RAN units at each domain, therefore realizing a large-scale 5G network with six indoor/outdoor cells/RAN units in total for both sites.

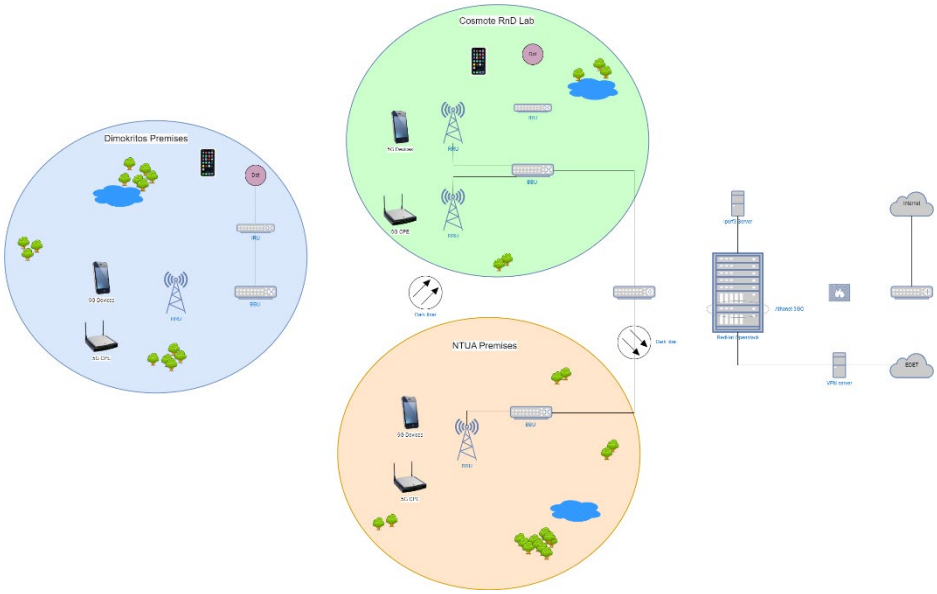


Figure 18: OTE's testbed topology for NANCY Use Case

As far as the Core Network is concerned, the option that could be utilized is the Athonet 5G SA Core. ATHONET 5G SA core network includes two User Plane Functions (UPFs) to emulate the edge and core 5G network data plane. The network also features 3GPP (3rd Generation Partnership Project) Control Plane Network Functions, including the Access and Mobility Management Function (AMF), Session Management Function (SMF), Authentication Server Function (AUSF), and User Data Management (UDM) Function. These functions enable the management and control of the network. Additionally, the network supports 3GPP interfaces, including N1, N2, N3, N4, and N6, which enable communication between network functions.

This setup is hosted at OTE Cloud facilities in Athens, providing a secure and reliable infrastructure

Table 17: Functional Requirements for Demonstrator 3

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D3_FUNCT-1** | 5G Core & RAN Deployment | Mandatory | 5G RAN and core components will be available for | Infrastructure Requirement |

| | | | | |
|---|---|---|---|---|
| | | | demonstration involving aggregation of technologies, both SA and NSA mode, and other interworking capabilities | |
| **D3_FUNCT-2** | Mode of Operation | Mandatory | The 5G testbed (core network, RAN, and UE) shall support both SA and NSA modes of operation | Infrastructure Requirement |
| **D3_FUNCT-3** | Integration of measurement tools | Mandatory | The infrastructure layer shall deploy measurement tools. It shall also embrace the gathering of relevant metrics required for the validation of the corresponding demonstrator KPIs. | Infrastructure Requirement |
| **D3_FUNCT-4** | Spectrum Allocation | Mandatory | Relevant constraints springing from regulatory authorities related to 5G-spectrum allocation must be considered. | Resource Management |
| **D3_FUNCT-5** | Monitoring | Mandatory | The system shall provide monitoring information derived from the demonstration execution. | Resource Management |

Table 18: Non-Functional Requirements for Demonstrator 3

| Req ID | Name | Priority | Description | Type |
|---|---|---|---|---|
| **D3_NFUNCT-1** | KPI & KVI Validation | Mandatory | The 5G testbed along with all NANCY demonstrator components shall be able to measure and validate the targeted KPIs & KVIs | |
| **D3_NFUNCT-2** | Security & Privacy | Mandatory | The 5G testbed along with all NANCY demonstrators shall implement robust security measures to prevent unauthorised access and mitigate potential threads. Compliance with General Data Protection Regulation (GDPR) requirements is considered mandatory. | |
| **D3_NFUNCT-3** | Network Slicing | Mandatory | The testbed should support network slicing, allowing the creation of customized virtual networks to meet the specific requirements of the demonstrator. | |

| | | | | |
|---|---|---|---|---|
| **D3_NFUNCT-4** | Low latency | Mandatory | The NANCY ecosystem should support maximum end-to-end latency of 5s | |
| **D3_NFUNCT-5** | Availability and Reliability | Mandatory | The NANCY ecosystem shall provide continuous, uninterruptable operation during demonstrations. | |
| **D3_NFUNCT-6** | Authentication & authorization | Mandatory | The NANCY ecosystem shall provide means for authentication and authorization for accessing. | |

# 7 Conclusion

The evolution of today's B5G mobile networks will soon be available to provide advanced services to a massive number of users. To enable such a vision in this rapidly changing network ecosystem, the NANCY project proposes a secure and intelligent B-RAN architecture enhanced by mechanisms that manage network access and authentication among trustless network entities. These mechanisms will identify advanced network functions, making the adoption of blockchain and AI technologies for RANs possible. End-to-end performance analysis and targeted KPIs and KVIs will be the key features to optimize intelligent resource management, flexible networking, and orchestration effectively.

In the network design domain, NANCY targets the development of novel architectures such as point-to-point connectivity for device-to-device connectivity, mesh networking, and relay-based communications, as well as protocols for medium access, mobility management, and resource allocation.

As has been extensively described in the previous sections, we focused on a wide range of usage scenarios and demonstrations in NANCY. Having as a starting point the reference use cases that led to the evolution and an overview of the relevant projected use cases, this deliverable includes a set of NANCY Usage Scenarios that are considered the cornerstone of almost all the 6G SNS-described verticals. In particular, the Usage Scenarios and their Use cases analysed are the following:

**Fronthaul network of fixed topology Usage Scenario**
- Direct connectivity
- CoMP connectivity

**Advanced coverage expansion**
- Multi-Hop Connectivity
- Ad-Hoc Mesh
- Point –to- Multipoint Connectivity

**Advanced connectivity of mobile nodes**
- Vehicle-to-AP
- Vehicle-to-vehicle

Finally, in addition to the Usage scenarios, three distinct demonstrators, one in Italy, one in Spain, and one in Greece, that will validate the NANCY architecture, are described.

- Demonstrator 1**:** Italian massive-IoT testbed
  - Traffic management (critical machine type communications-MTC)
  - IoT sensors' measurements (mMTC)
- Demonstrator 2: Validation of the AI-based B-RAN orchestration mechanisms developed in WP3 and WP4 to optimize the vehicular network topology (including direct and multi-hop communications).
- Demonstrator 3: It focuses on orchestration, computational and storage offloading, social-aware caching, as well as security and privacy to demonstrate their effectiveness in supporting latency-critical broadband applications.

More detailed definitions and requirements will be presented in WP6, where the aforementioned demonstrators will be implemented.

# Bibliography


[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?," IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, Jun. 2014..

[2] K. Samdanis and T. Taleb, "The Road beyond 5G: A Vision and Insight of the Key Technologies," in IEEE Network, vol. 34, no. 2, pp. 135-141, Mar./Apr. 2020.

[3] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," IEEE Journal on Selected Areas in Communications, vol. 35, no. 6, pp. 1201-1221, June 2017.

[4] A. Slalmi, H. Chaibi, A. Chehri, R. Saadane, G. Jeon, and N. Hakem, "On the Ultra-Reliable and Low-Latency Communications for Tactile Internet in 5G Era," Procedia Computer Science, vol. 176. Elsevier BV, pp. 3853–3862, Oct. 2020.

[5] M. Bennis, M. Debbah and H. V. Poor, "Ultrareliable and Low-Latency Wireless Communication: Tail, Risk, and Scale," Proceedings of the IEEE, vol. 106, no. 10, pp. 1834-1853, Oct. 2018.

[6] A. Salh, L. Audah, N. S. M. Shah, A. Alhammadi, Q. Abdullah, Y. H. Kim, S. A. Al-Gailani, S. A. Hamzah, B. A. F. Esmail, and A. A. Almohammedi, "A Survey on Deep Learning for Ultra-Reliable and Low-Latency Communications Challenges on 6G Wireless Systems," in IEEE Access, vol. 9, pp. 55098-55131, Mar. 2021.

[7] A. Zappone and E. Jorswieck, "Energy Efficiency in Wireless Networks via Fractional Programming Theory", Foundations and Trends in Communications and Information Theory, vol. 11, no. 3-4, pp. 185-396, June 2015.

[8] D. López-Pérez, A. De Domenico, N. Piovesan, G. Xinli, H. Bao, S. Qitao, and M. Debbah, "A Survey on 5G Radio Access Network Energy Efficiency: Massive MIMO, Lean Carrier Design, Sleep Modes, and Machine Learning," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 653-697, Firstquarter 2022.

[9] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," in IEEE Communications Magazine, vol. 58, no. 3, pp. 55-61, Mar. 2020.

[10] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jäntti and Z. Han, "Spectral Efficiency Optimization for Next Generation NOMA-Enabled IoT Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15284-15297, Dec. 2020

[11] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta and P. Popovski, "Five disruptive technology directions for 5G," in IEEE Communications Magazine, vol. 52, no. 2, pp. 74-80, Feb. 2014.

[12] P. Roy, A. Tahsin, S. Sarker, T. Adhikary, Md. A. Razzaque, and M. M. Hassan, "User mobility and Quality-of-Experience aware placement of Virtual Network Functions in 5G," Computer Communications, vol. 150. Elsevier BV, pp. 367–377, Jan. 2020.

[13] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," in IEEE Access, vol. 7, pp. 78729-78757, Jun. 2019.

[14] C. Benzaïd, T. Taleb and M. Z. Farooqi, "Trust in 5G and Beyond Networks," in IEEE Network, vol. 35, no. 3, pp. 212-222, May/Jun. 2021.

[15]S. Koratagere Anantha Kumar and E. J. Oughton, “Techno-economic assessment of 5G infrastructure sharing business models in rural areas,” Frontiers in Computer Science, vol. 5. Frontiers Media SA, Oct. 2023.

[16]A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, “6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap,” Sensors, vol. 21, no. 5. MDPI AG, p. 1709, Mar. 2021.

[17]S. Lythreatis, S. K. Singh, and A.-N. El-Kassar, “The digital divide: A review and future research agenda,” Technological Forecasting and Social Change, vol. 175. Elsevier BV, p. 121359, Feb. 2022.

[18]G. P. Fettweis, "The Tactile Internet: Applications and Challenges," in IEEE Vehicular Technology Magazine, vol. 9, no. 1, pp. 64-70, Mar. 2014.

[19]HEXA-X, “D1.2 Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum, 2021,” [Online]. Available: https://hexa-x.eu/deliverables/

[20]5G ACIA, “Key 5G Use Cases and Requirements”, 2020, https://www.5gacia.org/publications/key-5g-use-cases-and-requirements/.

[21]V. Ziegler and S. Yrjola, “6G Indicators of Value and Performance,” 2nd 6G Wireless Summit (6G SUMMIT), Mar. 2020, pp. 1-5

[22]Ericsson, "Ever-present intelligent communication: A research outlook towards 6G," Nov 2020. [Online]. Available: https://www.ericsson.com/4ab9e4/assets/local/reports-papers/white-papers/ericsson-white-paper-research-outlook-towards-6g.pdf

[23]NTT DOCOM INC., "5G Evolution and 6G," Jan 2022. [Online]. Available: https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf

[24]Samsung Research, "6G The Next Hyper-Connected Experience for All," [Online]. Available: https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf

[25]M. Latva-aho and K. Leppänen, “Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence,” 6G Research Visions 1, 6G Flagship, University of Oulu, Finland, ISBN 978-952-62-2353-7, ISSN 2669-9621, Sep. 2019.

[26]6G Flagship - University of Oulu, "Strategic research areas," [Online]. Available: https://www.6gflagship.com/6g-research/strategic-research-areas/

[27]M. Masoudi, M. G. Khafagy, A. Conte, A. El-Amine, B. Françoise, C. Nadjahi, F. E. Salem, W. Labidi, A. Sural, A. Gati, D. Bodéré, E. Arikan, F. Aklamanu, H. Louahlia-Gualous, J. Lallet, K. Pareek, L. Nuaymi, L. Meunier, P. Silva, N. T. Almeida, T. Chahed, T. Sjölund, and C. Cavdar, "Green Mobile Networks for 5G and Beyond," in IEEE Access, vol. 7, pp. 107270-107299, Aug. 2019.

[28]A. Chaoub, M. Giordani, B. Lall, V. Bhatia, A. Kliks, L. Mendes, K. Rabie, H. Saarnisaari, A. Singhal, N. Zhang, S. Dixit, and M. Zorzi, "6G for Bridging the Digital Divide: Wireless Connectivity to Remote Areas," in IEEE Wireless Communications, vol. 29, no. 1, pp. 160-168, Feb. 2022.

[29]P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage and M. Ylianttila, "6G Security Challenges and Potential Solutions," Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Jul. 2021, pp. 622-627.

[30]A. Masaracchia, V. Sharma, M. Fahim, O. A. Dobre and T. Q. Duong, "Digital Twin for Open RAN: Toward Intelligent and Resilient 6G Radio Access Networks," in IEEE Communications Magazine, vol. 61, no. 11, pp. 112-118, Nov. 2023.

[31]International Commission on Non-Ionizing Radiation Protection, "ICNIRP Guidelines for Limiting Exposure to Electromagnetic Fields (100 KHz to 300 GHz)," [Online]. Available: https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf

[32]F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Commun. Surv. Tutorials, vol. 18, no. 3, p. 2084–2123, Thirdquarter 2016

[33]Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," IEEE Network, vol. 33, no. 3, p. 10–17, May 2019

[34]Cisco Visual Networking Index, Cisco visual networking index: Global mobile data traffic forecast update, 2016-2021, Cisco, White Paper, Feb. 2017

[35]X. Ling, J. Wang, T. Bouchoucha, B. C. Levy and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," IEEE Access, vol. 7, p. 9714–9723, Jan. 2019.

[36]Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[37] National Institute of Standards and Technology, "Post-Quantum Cryptography | CSRC," [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[38]CRYSTALS Team, "Cryptographic Suite for Algebraic Lattices," [Online]. Available: https://pq-crystals.org/

[39]GE. M. Stoudenmire and X. Waintal, "Grover's Algorithm Offers No Quantum Advantage." arXiv, 2023. doi: 10.48550/ARXIV.2303.11317

[40]ETSI Technical Report "5G, Management and orchestration, Concepts, use cases and requirements, 3GPP TS 28.530 version 17.4.0 Release 17," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.04.00_60/ts_128530v170400p.pdf

[41]Cisco Visual Networking Index, Forecast and Trends, 2017-2022, White Paper, Cisco, Feb. 2019

[42]M. Belesioti, K. Tsagkaris, A. Margaris, and I. P. Chochliouros, "A 5G-Based Architecture for Localization Accuracy," IFIP Advances in Information and Communication Technology. Springer International Publishing, pp. 23–33, 2022.

[43]"Hexa-X," [Online]. Available: https://hexa-x.eu/

[44]"one6G – Taking communications to the next level," [Online]. Available: https://one6g.org/

[45]O-RAN, Alliance White Paper "O-RAN Use Cases and Deployment Scenarios, Towards Open and Smart RAN," Feb. 2020, [Online]. Available: https://assets-global.website-files.com/60b1962ffda0a42f779c765b/60d335c6d3fed506ae1dce58_O-RAN%2BUse%2BCases%2Band%2BDeployment%2BScenarios%2BWhitepaper%2BFebruary%2B2020.pdf

[46]M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, 'A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities', IEEE Access, vol. 8, pp. 115876–115904, 2020.

[47]Telefonica, "Telefonica and IBM Collaborate to Apply Blockchain to Streamline Telco Processes," Jun. 2023, [Online]. Available: https://www.telefonica.com/en/communication-room/press-room/telefonica-and-ibm-collaborate-to-apply-blockchain-to-streamline-telco-processes/

[48]H. Partz, "South Korea's Telecom Giant KT Launches DLT-Powered 5G Brand to Prevent Hacks," Apr. 2019, [Online]. Available: https://cointelegraph.com/news/south-koreas-telecom-giant-kt-launches-dlt-powered-5g-brand-to-prevent-hacks

[49]Forkast, "China Telecom Introduces its Blockchain SIM Card Project," Sep. 2019, [Online]. Available: https://forkast.news/video-audio/watch-china-telecom-introduces-its-blockchain-sim-card-project/

[50]W. Tong, X. Dong, Y. Shen, and J. Zheng, 'BC-RAN: Cloud radio access network enabled by blockchain for 5G', Computer Communications, vol. 162, pp. 179–186, Oct. 2020.

[51]H. Xu, L. Zhang, Y. Sun, and C.-L. I, 'BE-RAN: Blockchain-enabled Open RAN with Decentralized Identity Management and Privacy-Preserving Communication'. arXiv, May 29, 2021.

[52]A. Heider-Aviet et al., 'Blockchain Based RAN Data Sharing', in 2021 IEEE International Conference on Smart Data Services (SMDS), Sep. 2021, pp. 152–161.

[53]D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, 'Blockchain for 5G and beyond networks: A state of the art survey', Journal of Network and Computer Applications, vol. 166, p. 102693, Sep. 2020.

[54]X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, 'Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm', IEEE Access, vol. 7, pp. 9714–9723, 2019.

[55]X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, 'Blockchain Radio Access Network Beyond 5G', IEEE Wireless Communications, vol. 27, no. 6, pp. 160–168, Dec. 2020.

[56]H. He, X. Yu, J. Zhang, S. Song, and K. Letaief, "Cell-Free Massive MIMO for 6G Wireless Communication Networks," in IEEE Journal on Selected Areas in Communications, 2021

[57]ETSI TC EE, "ES 203 228, Environmental Engineering (EE); Assessment of mobile network energy efficiency," V1.3.1, Oct. 2020

[58]H. L. Gururaj, R. Natarajan, N. A. Almujally, F. Flammini, S. Krishna and S. K. Gupta, "Collaborative Energy-Efficient Routing Protocol for Sustainable Communication in 5G/6G Wireless Sensor Networks," IEEE Open Journal of the Communications Society, vol. 4, pp. 2050-2061, Sep. 2023.

[59]W. Hong et al., "The Role of Millimeter-Wave Technologies in 5G/6G Wireless Communications," in IEEE Journal of Microwaves, vol. 1, no. 1, pp. 101-122, Jan. 2021.

[60]X. You et al., "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts," Science China Information Sciences, vol. 64, no. 1. Springer Science and Business Media LLC, Nov. 2020.

[61] E. Longman, M. El-Hajjar, and G. V. Merrett, "Multihop networking for intermittent devices," 20th ACM Conference on Embedded Networked Sensor Systems (SenSys), Nov. 2022, pp. 878-884.

[62]J. P. Astudillo León, L. J. de la Cruz Llopis, and F. J. Rico-Novella, "A machine learning based Distributed Congestion Control Protocol for multi-hop wireless networks," Computer Networks, vol. 231. Elsevier BV, p. 109813, Jul. 2023.

[63]S. Iqbal, K. N. Qureshi, N. Kanwal, and G. Jeon, "Collaborative energy efficient zone-based routing protocol for multihop Internet of Things," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 2. Wiley, Feb. 2020.

[64]E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks," Computer Networks, vol. 56, no. 2. Elsevier BV, pp. 940–965, Feb. 2012.

[65]R. C. Carrano, L. C. S. Magalhães, D. C. M. Saade and C. V. N. Albuquerque, "IEEE 802.11s Multihop MAC: A Tutorial," IEEE Communications Surveys & Tutorials, vol. 13, no. 1, pp. 52-67, First Quarter 2011.

[66]M. Catalan-Cid, J. Paradells and C. Gómez, "Contributions to the Routing of Traffic Flows in Multi-hop IEEE 802.11 Wireless Networks", Ph.D. Thesis, Universitat Politènica de Catalunya, 2016

[67]TS 38.300 V16.8.0, NR and NG-RAN Overall Description; Stage 2 (Release 16)," December 2021

[68]3GPP TR 38.874, Study on Integrated Access and Backhaul (Release 16),” December 2018
[69]V. F. Monteiro, F. R. M. Lima, D. C. Moreira, D. A. Sousa, T. F. Maciel, B. Makki, H. Hannu, "Paving the Way Toward Mobile IAB: Problems, Solutions and Challenges," IEEE Open Journal of the Communications Society, vol. 3, pp. 2347-2379, Nov. 2022.
[70]H. Yin, S. Roy and L. Cao, "Routing and Resource Allocation for IAB Multi-Hop Network in 5G Advanced," in IEEE Transactions on Communications, vol. 70, no. 10, pp. 6704-6717, Oct. 2022.
[71]C. Madapatha, B. Makki, A. Muhammad, E. Dahlman, M.-S. Alouini and T. Svensson, "On Topology Optimization and Routing in Integrated Access and Backhaul Networks: A Genetic Algorithm-Based Approach," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2273-2291, Sep. 2021.
[72]E. Moro, G. Gemmi, M. Polese, L. Maccari, A. Capone and T. Melodia, "Toward Open Integrated Access and Backhaul with O-RAN," 21st Mediterranean Communication and Computer Networking Conference (MedComNet), Jul. 2023, pp. 61-69.
[73]H. Zuo, Y. Sun, C. Lin, S. Li, H. Xu, Z. Tan, and Y. Wang, "A Three-way Handshaking Access Mechanism for Point to Multipoint In-band Full-duplex Wireless Networks," KSII Transactions on Internet and Information Systems, vol. 10, no. 7, pp. 3131-3149, Jul. 2016.
[74]C.-H. Hsu and K.-T. Feng, "Adaptive point-to-point communication approach for subscriber stations in broadband wireless networks," Wireless Networks, vol. 17, pp. 69–86, Jul. 2010.
[75]W. Hong et al., "The Role of Millimeter-Wave Technologies in 5G/6G Wireless Communications," in IEEE Journal of Microwaves, vol. 1, no. 1, pp. 101-122, Jan. 2021.
[76]Z. Zhang, Y. Gao, Y. Liu and Z. Li, "Performance evaluation of shortened transmission time interval in LTE networks," IEEE Wireless Communications and Networking Conference (WCNC), Jun. 2018, pp. 1-5.
[77]M. E. Morocho-Cayamcela, H. Lee and W. Lim, "Machine Learning to Improve Multi-Hop Searching and Extended Wireless Reachability in V2X," in IEEE Communications Letters, vol. 24, no. 7, pp. 1477-1481, Jul. 2020.
[78]M. Allende et al., “Quantum-resistance in blockchain networks,” Scientific Reports, vol. 13, no. 1. Springer Science and Business Media LLC, Apr. 2023.
[79]T. Guggenberger, J. Sedlmeir, G. Fridgen, and A. Luckow, “An in-depth investigation of the performance characteristics of Hyperledger Fabric,” Computers & Industrial Engineering, vol. 173. Elsevier BV, p. 108716, Nov. 2022.
[80]Hyperledger Foundation, "Hyperledger Fabric - Performance considerations," [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/performance.html