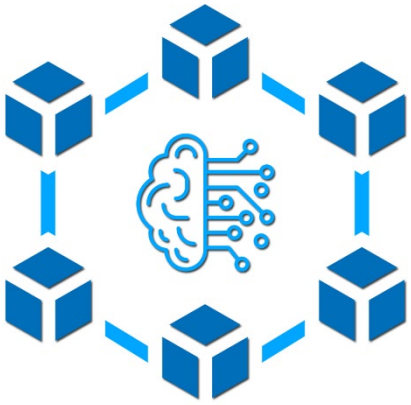



**An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution [GA: 101096456]**

# Deliverable 1.11

# Techno-economic Analysis and Commercialization Plans

*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** | Techno-economic Analysis and Commercialization Plans |
| **Deliverable Number** | D1.11 |
| **Work Package** | WP1 'Project, Innovation & Data Management' |
| **Associated Task** | T1.7 'Business Planning & Market Analysis' |
| **Dissemination Level** | Public |
| **Due Date** | 31 December 2025 (M36) |
| **Completion Date** | 29 December 2025 |
| **Submission Date** | 30 December 2025 |
| **Deliverable Lead Partner** | 8BELLS |
| **Deliverable Author(s)** | Ilias Theodoropoulos (8BELLS), Stratos Vamvourellis (8BELLS), Stylianos Trevlakis (INNO), Theodoros Tsiftsis (INNO), Eirini Gkarnetidou (INNO), Lamprini Mitsiou (INNO), Vasileios Kouvakis (INNO), Athanasios Tziouvaras (Bi2S), Maria Belesioti (OTE), Nikos Ntampakis (MINDS), Marco Tambasco (TEI), Olga Segou (INTRA), Hatim Chergui (i2CAT), Alvise Rigo (VOS), Javier de Vicente (NEC), Damien Bertonnier (TDIS) |
| **Version** | 1.0 |

### Document History

| Version | Date | Change History | Author(s) | Organisation |
|---|---|---|---|---|
| 0.1 | 01/11/2025 | Initial version & ToC | Ilias Theodoropoulos, Stratos Vamvourellis | 8BELLS |
| 0.2 | 20/11/2025 | Section 1 | Ilias Theodoropoulos, Stratos Vamvourellis | 8BELLS |
| 0.3 | 27/11/2025 | Section 2 | Ilias Theodoropoulos | 8BELLS |
| 0.4 | 28/11/2025 | Section 3 | Stratos Vamvourellis | 8BELLS |
| 0.5 | 01/12/2025 | Skeleton for Section s4, 5<br><br>Contribution concerning ER22 | Ilias Theodoropoulos | 8BELLS |
| | 04/12/2025 | Contribution concerning ER16 and ER24 | Athanasios Tziouvaras | Bi2S |
| | 05/12/2025 | Contribution concerning ER11 | Nikos Ntampakis | MINDS |
| | 08/12/2025 | Contributions concerning ER5, ER6 and ER10 | Stylianos Trevlakis, Theodoros Tsiftsis, Eirini Gkarnetidou, Lamprini Mitsiou, Vasileios Kouvakis | INNO |
| | 09/12/2025 | Contribution concerning ER28 | Olga Segou | INTRA |

| | | | | |
|---|---|---|---|---|
| | 10/12/2025 | Contribution concerning ER7 | Hatim Chergui | i2CAT |
| | | Contribution concerning ER4 and ER23 | Marco Tambasco | TEI |
| | 11/12/2025 | Contribution concerning ER13 | Alvise Rigo | VOS |
| | | Contribution concerning ER20 | Maria Belesioti | OTE |
| | | Contribution concerning ER3 | Javier de Vicente | NEC |
| | | Contribution concerning ER2 | Damien Bertonnier | TDIS |
| | | Finalization of Sections 4, 5.1 | Ilias Theodoropoulos | 8BELLS |
| 0.6 | 15/12/2025 | Section 5.2 | Ilias Theodoropoulos, Stratos Vamvourellis | 8BELLS |
| 0.7 | 17/12/2025 | Section 6 & Bibliography | Stratos Vamvourellis | 8BELLS |
| 0.8 | 19/12/2025 | Final Version for Internal Review | Ilias Theodoropoulos, Stratos Vamvourellis | 8BELLS |
| 0.9 | 24/12/2025 | Addressing Reviewer Comments | Ilias Theodoropoulos, Stratos Vamvourellis | 8BELLS |
| 1.0 | 29/12/2025 | Final version after quality revisions | Anna Triantafyllou, Dimitrios Pliatsios | UOWM |

## Internal Review History

| Name | Organisation | Date |
|---|---|---|
| Stylianos Trevlakis, Eirini Gkarnetidou, Lamprini Mitsiou | INNO | 22 December 2025 |
| Giorgos-Nektarios Panayotidis, Theofanis Xifilidis, Dimitris Kavallieros | CERTH | 23 December 2025 |

## Quality Manager Revision

| Name | Organisation | Date |
|---|---|---|
| Anna Triantafyllou, Dimitrios Pliatsios | UOWM | 29 December 2025 |

# Table of Contents

Table of Contents ..... 5
List of Figures ..... 8
List of Tables ..... 9
List of Acronyms ..... 11
Executive summary ..... 13
1. Introduction ..... 14
1.1. Relation to Other Tasks and Deliverables ..... 14
1.2. Structure of the Deliverable ..... 14
2. Methodological Approach ..... 15
2.1. Methodology for the Market Analysis ..... 15
2.2. Methodology for the Technoeconomic Analysis & Business Modelling ..... 16
2.2.1. Selection of Commercially Relevant Results ..... 16
2.2.2. SWOT Analysis ..... 16
2.2.3. Lean Canvas Modelling ..... 17
2.2.4. Complementary Use of Both Tools ..... 17
2.3. Methodology for the Commercialization Planning ..... 18
2.3.1. Characterization Table for Commercially Relevant Results ..... 18
2.3.2. Fuzzy AHP for Prioritization of Success Factors ..... 18
2.3.3. Relationship Between Both Tools ..... 23
3. Market Analysis ..... 24
3.1. Target Markets ..... 24
3.1.1. 5G / B5G Market Trends ..... 24
3.1.2. 5G / B5G Market Challenges - Entry Barriers ..... 26
3.1.3. Blockchain in Telecom Market Trends ..... 27
3.1.4. Blockchain in Telecom Market Challenges - Entry Barriers ..... 28
3.1.5. Cybersecurity & Post-Quantum Security Market Trends ..... 29
3.1.6. Cybersecurity & Post-Quantum Security Market Challenges - Entry Barriers ..... 31
3.1.7. Cloud/IoT/Edge Continuum Market Trends ..... 31
3.1.8. Cloud/IoT/Edge Continuum Market Challenges - Entry Barriers ..... 33
3.1.9. Artificial Intelligence for Networks Market Trends ..... 35
3.1.10. Artificial Intelligence for Networks Market Challenges - Entry Barriers ..... 36
3.2. Competitive Landscape ..... 37
3.2.1. Research Projects ..... 37
3.2.2. Business Solutions ..... 38

3.3. Key EU Initiatives ..... 40
3.3.1. Data Governance Act ..... 40
3.3.2. Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography ..... 41
3.3.3. NIS2 ..... 41
4. Techno-economic Analysis & Business Modelling ..... 43
4.1. Commercial Exploitable Results ..... 43
4.2. SWOT and Lean Canvas ..... 44
4.2.1. ER2: PQC Signature Solution ..... 44
4.2.2. ER3: Blockchain wallet with SSI and PQC capabilities ..... 45
4.2.3. ER4: PQC secure communication ..... 47
4.2.4. ER5: B-RAN Theoretical Framework ..... 49
4.2.5. ER6: QKD Simulation Framework ..... 52
4.2.6. ER7: A novel AI virtualiser for underutilized computational & communication resource exploitation ..... 54
4.2.7. ER10: Semantic Communications Framework ..... 56
4.2.8. ER11: An explainable AI framework ..... 58
4.2.9. ER13: Virtio-based cross-world transport layer ..... 60
4.2.10. ER16: Machine learning models for decision-making ..... 61
4.2.11. ER20: Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing ..... 63
4.2.12. ER22: Smart Pricing Policies ..... 65
4.2.13. ER23: Big Data Platform for self-healing and self-recovery ..... 67
4.2.14. ER24: A framework for data and concept drift detection in 6G networks ..... 68
4.2.15. ER28: Central Management Domain ..... 70
5. Commercialization Planning ..... 74
5.1. Characterization Table for each Commercial Exploitable Result ..... 74
5.1.1. ER2: PQC Signature Solution ..... 74
5.1.2. ER3: Blockchain Wallet with SSI and PQC Capabilities ..... 74
5.1.3. ER4: PQC Secure Communication ..... 76
5.1.4. ER5: B-RAN Theoretical Framework ..... 77
5.1.5. ER6: QKD Simulation Framework ..... 79
5.1.6. ER7: A novel AI virtualiser for underutilized computational & communication resource exploitation ..... 81
5.1.7. ER10: Semantic Communications Framework ..... 82
5.1.8. ER11: An explainable AI framework ..... 84
5.1.9. ER13: Virtio-based cross-world transport layer ..... 86

5.1.10. ER16: Machine learning models for decision-making ..... 87
5.1.11. ER20: Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing ..... 89
5.1.12. ER22: Smart Pricing Policies ..... 90
5.1.13. ER23: Big Data Platform for self-healing and self-recovery ..... 92
5.1.14. ER24: A framework for data and concept drift detection in 6G networks ..... 93
5.1.15. ER28: Central Management Domain ..... 95
5.2. Fuzzy Analytical Hierarchy Process ..... 97
5.2.1. Criteria and Sub-Criteria Selection ..... 97
5.2.2. Survey Description ..... 99
5.2.3. Derivation of Final Results ..... 105
5.2.4. Interpretation of Results ..... 109
5.3. Horizon Results ..... 115
6. Conclusion ..... 116
Bibliography ..... 117

# List of Figures

Figure 1: Accenture 5G GDP Forecast ..... 25
Figure 2: Blockchain in Telecom Market Value Forecast ..... 27
Figure 3: Global Cybersecurity Spending Forecast ..... 30
Figure 4: Edge Computing Market Size Forecast ..... 32
Figure 5: AI in Networks Market Size Forecast ..... 35
Figure 6: AHP Criteria and Sub-criteria Hierarchy ..... 99
Figure 7: AHP Questionnaire (1) ..... 101
Figure 8: AHP Questionnaire (2) ..... 102
Figure 9: AHP Questionnaire (3) ..... 103
Figure 10: AHP Questionnaire (4) ..... 104
Figure 11: Ranking of Main Criteria ..... 110
Figure 12: Ranking of Sub-Criteria under Scalability & Ecosystem Fit ..... 111
Figure 13: Ranking of Sub-Criteria under Trust & Security ..... 112
Figure 14: Ranking of Sub-Criteria under Performance & Reliability ..... 113
Figure 15: Total Ranking of Sub-Criteria ..... 115

# List of Tables

Table 1: Mapping of Linguistic Scale to Triangular Fuzzy Number ..... 20
Table 2: Crisp Mapping of Linguistic Scale ..... 21
Table 3: Commercial Exploitable Results ..... 43
Table 4: SWOT Analysis for ER2 ..... 44
Table 5: Lean Canvas for ER2 ..... 44
Table 6: SWOT Analysis for ER3 ..... 45
Table 7: Lean Canvas for ER3 ..... 46
Table 8: SWOT Analysis for ER4 ..... 47
Table 9: Lean Canvas for ER4 ..... 48
Table 10: SWOT Analysis for ER5 ..... 49
Table 11: Lean Canvas for ER5 ..... 50
Table 12: SWOT Analysis for ER6 ..... 52
Table 13: Lean Canvas for ER6 ..... 53
Table 14: SWOT Analysis for ER7 ..... 54
Table 15: Lean Canvas for ER7 ..... 55
Table 16: SWOT Analysis for ER10 ..... 56
Table 17: Lean Canvas for ER10 ..... 57
Table 18: SWOT Analysis for ER11 ..... 58
Table 19: Lean Canvas for ER11 ..... 59
Table 20: SWOT Analysis for ER13 ..... 60
Table 21: Lean Canvas for ER13 ..... 60
Table 22: SWOT Analysis for ER16 ..... 61
Table 23: Lean Canvas for ER16 ..... 62
Table 24: SWOT Analysis for ER20 ..... 63
Table 25: Lean Canvas for ER20 ..... 64
Table 26: SWOT Analysis for ER22 ..... 65
Table 27: Lean Canvas for ER22 ..... 66
Table 28: SWOT Analysis for ER23 ..... 67
Table 29: Lean Canvas for ER23 ..... 67
Table 30: SWOT Analysis for ER24 ..... 68
Table 31: Lean Canvas for ER24 ..... 69
Table 32: SWOT Analysis for ER28 ..... 70
Table 33: Lean Canvas for ER28 ..... 71
Table 34: Characterization Table for ER2 ..... 74
Table 35: Characterization Table for ER3 ..... 74
Table 36: Characterization Table for ER4 ..... 76
Table 37: Characterization Table for ER5 ..... 77
Table 38: Characterization Table for ER6 ..... 79
Table 39: Characterization Table for ER7 ..... 81
Table 40: Characterization Table for ER10 ..... 82
Table 41: Characterization Table for ER11 ..... 84
Table 42: Characterization Table for ER13 ..... 86
Table 43: Characterization Table for ER16 ..... 87
Table 44: Characterization Table for ER20 ..... 89
Table 45: Characterization Table for ER22 ..... 90
Table 46: Characterization Table for ER23 ..... 92

Table 47: Characterization Table for ER24 ..... 93
Table 48: Characterization Table for ER28 ..... 95
Table 49: Aggregated Fuzzy Pairwise Comparison Matrix for the Main Criteria ..... 105
Table 50: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Scalability & Ecosystem Fit ..... 105
Table 51: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Trust & Security ..... 106
Table 52: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Performance & Reliability ..... 106
Table 53: Fuzzy Weights for the Main Criteria ..... 107
Table 54: Fuzzy Weights for the Sub-Criteria under Scalability & Ecosystem Fit ..... 107
Table 55: Fuzzy Weights for the Sub-Criteria under Trust & Security ..... 107
Table 56: Fuzzy Weights for the Sub-Criteria under Performance & Reliability ..... 107
Table 57: Ranking of the Main Criteria ..... 108
Table 58: Ranking of the Sub-Criteria under Scalability & Ecosystem Fit ..... 108
Table 59: Ranking of the Sub-Criteria under Trust & Security ..... 108
Table 60: Ranking of the Sub-Criteria under Performance & Reliability ..... 108
Table 61: Total Ranking of Sub-Criteria ..... 114

# List of Acronyms

| Acronym | Explanation |
|---|---|
| **AI** | Artificial Intelligence |
| **AHP** | Analytical Hierarchy Process |
| **API** | Application Programming Interface |
| **AWS** | Amazon Web Services |
| **B5G** | Beyond 5G |
| **B-RAN** | Blockchain-enabled Radio Access Network (as used in NANCY) |
| **CAGR** | Compound Annual Growth Rate |
| **CBRS** | Citizens Broadband Radio Service |
| **CI/CD** | Continuous Integration / Continuous Delivery |
| **CR** | Consistency Ratio (in AHP) |
| **CU/DU/RU** | Central Unit / Distributed Unit / Radio Unit |
| **DID** | Decentralized Identity |
| **ETSI** | European Telecommunications Standards Institute |
| **3GPP** | Third Generation Partnership Project |
| **FAHP** | Fuzzy Analytical Hierarchy Process |
| **GDP** | Gross Domestic Product |
| **GDPR** | General Data Protection Regulation |
| **GPU** | Graphics Processing Unit |
| **GUI** | Graphical User Interface |
| **HRP** | Horizon Results Platform |
| **HSM** | Hardware Security Module |
| **ER** | Exploitable Result |
| **IoT** | Internet of Things |
| **KPI** | Key Performance Indicator |
| **KER** | Key Exploitable Result |
| **LLM** | Large Language Model |
| **LoRaWAN** | Long Range Wide Area Network |
| **MEC** | Multi-access Edge Computing |
| **ML** | Machine Learning |
| **O-RAN** | Open Radio Access Network |
| **OER** | Other Exploitable Result |
| **P2P** | Peer-to-Peer |
| **PKCS#11** | Public-Key Cryptography Standards #11 |
| **PKI** | Public Key Infrastructure |
| **PQC** | Post-Quantum Cryptography |
| **QKD** | Quantum Key Distribution |
| **QoE** | Quality of Experience |
| **QoS** | Quality of Service |
| **RAN** | Radio Access Network |
| **SDK** | Software Development Kit |
| **SLA** | Service Level Agreement |

| | |
|---|---|
| **SWOT** | Strengths, Weaknesses, Opportunities, Threats |
| **TFN** | Triangular Fuzzy Number |
| **TLS** | Transport Layer Security |
| **TRL** | Technology Readiness Level |
| **URLLC** | Ultra-Reliable Low-Latency Communication |
| **VPN** | Virtual Private Network |
| **XAI** | Explainable AI |
| **AR** | Augmented Reality |
| **XR** | Extended Reality |
| **VR** | Virtual Reality |
| **SDN** | Software Defined Network |
| **LPWAN** | Low-Power Wide-Area Network |
| **eMBB** | enhanced Mobile Broadband |

# Executive summary

This deliverable D1.11 “Techno-economic Analysis and Commercialization Plans” presents the final outcomes of Task 1.7 “Business Planning & Market Analysis”, encompassing the comprehensive techno-economic assessment, business modelling and commercialization planning activities carried out during the course of the NANCY project. Its objective is to evaluate the market potential of NANCY’s technological innovations and to define structured pathways for their exploitation and adoption within the Beyond 5G ecosystem and the forthcoming 6G landscape.

Building upon the earlier D1.8 “Market Analysis, Roadmap and Business Modelling Report”, this deliverable consolidates the methodologies, analytical tools and strategic frameworks that guide NANCY’s transition from research excellence to market readiness. The analysis integrates multiple perspectives, including market dynamics, competitive positioning and techno-economic feasibility, ensuring that the project’s innovations are aligned with real-world needs and industry expectations.

A robust methodological framework was established to support these objectives. The approach combines qualitative and quantitative tools, including Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis, Lean Canvas business modelling, Characterization Tables and the Fuzzy Analytical Hierarchy Process. These tools were applied across NANCY’s Exploitable Results to systematically assess their strengths, market opportunities, adoption barriers and commercialization potential. The resulting evaluations provide a consistent evidence base for prioritizing exploitation actions and identifying key success factors for future deployment.

The market analysis component explores global and European trends across the domains most relevant to NANCY’s technological innovations, namely 5G/B5G networks, blockchain for telecom, cybersecurity and post-quantum security, cloud/edge computing and Artificial Intelligence (AI) for network automation. Each domain analysis identifies growth trajectories, entry barriers and regulatory influences shaping market evolution. The findings confirm that NANCY’s modular, AI-enabled and blockchain-secured architecture directly addresses emerging industry priorities such as trustworthiness, interoperability, energy efficiency and quantum resilience.

From a techno-economic perspective, the report evaluates the commercial and operational viability of NANCY’s core results, outlining potential use cases, value propositions and business models. The commercialization planning process translates these assessments into actionable strategies for exploitation and identifying enabling conditions for sustainable market uptake.

Furthermore, the application of the Fuzzy AHP methodology introduces a structured mechanism to prioritize the most critical success factors for commercialization. By synthesizing expert judgments across multiple criteria, this analysis provides a transparent, evidence-based ranking of factors influencing market success, such as technical maturity, scalability, regulatory alignment and ecosystem readiness.

Overall, D1.11 provides a strategic and operational bridge between research outcomes and commercial implementation. It equips the consortium and stakeholders with the analytical foundations necessary to transform NANCY’s innovations into tangible market impact, supporting Europe’s leadership in secure, intelligent and sustainable Beyond 5G communications. The deliverable concludes that the project’s results exhibit alignment with current and emerging market needs and that they possess significant potential for exploitation through collaborative innovation, standardization and industrial engagement beyond the project’s lifetime.

# 1. Introduction

As part of Work Package 1, Task 1.7 "Business Planning & Market Analysis" focuses on business planning and market analysis to ensure that the project's outcomes can be effectively transferred to market contexts and deliver tangible socio-economic impact.

This deliverable is the updated final version of D1.8 "Market Analysis, Roadmap and Business Modelling Report" [1] and consolidates the results of the techno-economic analysis and commercialization planning activities. It provides partners and stakeholders with an integrated perspective on how the project's technical results can evolve into viable solutions, supporting both exploitation strategies and informed decision-making for further investment and development.

The purpose of this document is to assess and structure the commercial potential of NANCY's results. It identifies market opportunities, evaluates economic viability and defines the pathways for transitioning research outputs into deployable products or services. The document also serves as a strategic guide for the consortium's exploitation planning, supporting alignment among partners regarding market positioning, target segments and long-term business prospects.

More specifically, the deliverable aims to:

- Analyze trends, barriers and opportunities in markets relevant to NANCY's technologies.
- Evaluate each Exploitable Result's technical and commercial potential through SWOT and Lean Canvas analyses.
- Document commercialization strategies and adoption factors using Characterization Tables.
- Prioritize success factors via a structured Fuzzy AHP methodology.

## 1.1. Relation to Other Tasks and Deliverables

The deliverable is related with all the technical tasks of the project as it analyzes the exploitation potential of the project results and outlines future commercialization plans.

## 1.2. Structure of the Deliverable

The deliverable is structured as follows:

- **Section 1 – Introduction** provides serves as an introduction to the deliverable, presenting its aim, relationship with other tasks, and structure.
- **Section 2 – Methodological Approach** details the methodological approach, describing the frameworks and analytical tools applied to assess the project's results.
- **Section 3 – Market Analysis** presents a comprehensive market analysis across NANCY's technological domains, identifying trends, challenges and competitive dynamics.
- **Section 4 – Techno-economic Analysis & Business Modelling** outlines the techno-economic analysis and business modelling results for each Exploitable Result, combining SWOT and Lean Canvas analyses.
- **Section 5 – Commercialization Planning** focuses on commercialization planning, summarizing the characterization of each Exploitable Result and presenting the prioritization of success factors derived from the Fuzzy AHP model.
- **Section 6 – Conclusion** summarizes and concludes the deliverable.

# 2. Methodological Approach

This section outlines the methodological approach applied in the preparation of the market analysis, the technoeconomic and business modelling activities, and the commercialization planning presented in this deliverable. The methods used provide a structured way to collect, organize and analyze information relevant to the project's Exploitable Results (ERs) and the broader technological landscape in which they operate.

The approach is divided into three components. The first concerns the market analysis, which draws on desk research to describe market trends, competitive dynamics, and relevant economic and technological developments. The second focuses on the methods used to assess each ER from a technoeconomic and business perspective, relying on standardized analytical tools. The third component covers the tools used to document commercialization planning for each result and to structure the prioritization of factors that may influence their future uptake.

The following sections describe the methodological steps associated with each component.

## 2.1. Methodology for the Market Analysis

The market analysis presented in Section 3 employs a structured desk-research methodology aimed at collecting, organizing and interpreting publicly available information relevant to the technological domains addressed by the project mainly based on Key Exploitable Results (KERs) and/or Exploitable Results (ERs). The approach ensures consistent coverage of sectoral developments, industry actors and policy dynamics. The analysis is organized into four principal elements, each addressing a specific dimension of the external environment.

The first element consists of a review of target markets across domains such as 5G/Beyond 5G (B5G), blockchain in telecom, cybersecurity and post-quantum security, cloud/edge continuum and artificial intelligence for networks. For each domain, the method focuses particularly on documented challenges, technological gaps and recognized barriers to adoption. This enables a structured understanding of the issues that currently affect market evolution.

The second element examines the competitive landscape by identifying and characterizing companies, initiatives, research programmes and technological approaches active within the relevant domains. This component relies on publicly available documents to map the activities of industry incumbents, emerging players and collaborative ecosystems. The analysis focuses on their solution offerings and innovation directions, thereby providing insight into how competitive dynamics and industry structures influence technological development pathways.

The third element addresses EU-level economic and policy trends that affect the adoption, funding and regulation of advanced communication and digital technologies. The objective is to situate the project's technological domains within the broader institutional and policy environment that shapes market expectations, directs public investment and defines compliance requirements.

Collectively, these three methodological components form a coherent framework for describing the external environment relevant to the project. The approach organizes available evidence, contextualizes technological developments and highlights structural factors influencing market evolution, without deriving quantitative forecasts or normative judgements.

## 2.2. Methodology for the Technoeconomic Analysis & Business Modelling

The technoeconomic and business modelling activities presented in Section 4 rely on a structured methodological approach applied individually to each ER. The purpose of this section is to organize and analyze information relevant to the technological characteristics, potential value and deployment context of each result. Two complementary tools are used: the SWOT analysis and the Lean Canvas. Both tools follow established formats and allow for a systematic examination of each ER from different analytical angles.

### 2.2.1. Selection of Commercially Relevant Results

Before applying the analytical tools, the consortium identified the results that demonstrate potential for commercialization. The identification process was based on partner input and internal discussions and did not rely on predefined thresholds such as Technology Readiness Level (TRL) or revenue potential. Instead, it focused on determining which outputs could reasonably be associated with:

- a potential user or customer community,
- identifiable market needs or adoption contexts,
- or a foreseeable path toward industrial application.

Only these results were included in the modelling activities of Section 4.

### 2.2.2. SWOT Analysis

The first methodological step involves the preparation of a SWOT analysis for each ER. This tool structures information into four categories: strengths, which refer to internal attributes of the ER that may support its potential use or distinctiveness; weaknesses, which capture internal limitations or constraints that may hinder uptake; opportunities, referring to external trends, needs, or conditions that could favour the relevance or adoption of the result; and threats, reflecting external risks, competing developments, or market conditions that may pose challenges. The methodology for producing each SWOT analysis relies on inputs provided by the ER owner and is further supported by insights drawn from the market analysis presented in Section 3. The process focuses on identifying and articulating the main factors that describe the ER's internal positioning and the external environment it may encounter. This structured overview provides a qualitative foundation for understanding the contextual elements surrounding each result.

Beyond its descriptive function, SWOT is particularly valuable in technoeconomic analysis because it enables a comprehensive integration of technical characteristics with market and contextual considerations. SWOT avoids the pitfalls of premature quantification by offering a disciplined method for synthesizing expert knowledge, technological evidence and market observations into a coherent narrative of potential. It draws attention to the intrinsic qualities that may confer competitive advantage, but equally to the internal limitations that could influence future development paths or resource needs. At the same time, it situates the technology within its wider landscape by identifying external drivers of adoption, regulatory or societal enablers and sources of pressure or uncertainty that could shape market entry or scalability.

The value of this approach lies not only in the clarity it brings to each ER but also in its consistency across multiple results, allowing for comparable assessments that support prioritization and strategic planning. By systematically characterizing both internal capabilities and external conditions, SWOT helps determine where further technical refinement is required, where alignment with market

demands is strong and where risks may necessitate mitigation strategies. This makes SWOT an appropriate and effective early-stage tool for technoeconomic analysis, creating the interpretive framework upon which more detailed quantitative evaluation and exploitation planning can later be built.

### 2.2.3.Lean Canvas Modelling

A Lean Canvas was developed in parallel for each commercially relevant result, providing a structured way to organize early-stage business considerations. The approach involves articulating the problem the result aims to address, the corresponding solution it offers and the customer or user segments for whom the result may hold value. It also includes defining the unique value proposition, identifying potential differentiators or competitive advantages, outlining expected channels for outreach or distribution and capturing preliminary views on cost structures, revenue mechanisms and any key metrics that may guide future evaluation. Through this process, the Lean Canvas reflects the partners' current understanding of how each result might be positioned within a commercial landscape. It serves as a structured representation of initial assumptions, hypotheses and considerations.

This approach is particularly effective for technoeconomic analysis because it helps translate a technically oriented ER into a coherent early business model. Technoeconomic evaluation requires understanding not only how a technology performs but also how it creates and captures value within a specific ecosystem. The Lean Canvas supports this by forcing clarity on the nature of the problem being solved, the profile of intended adopters and the mechanisms through which adoption could occur. In this way, it bridges the gap between technological development and market feasibility by capturing the preliminary logic of how a result could enter, influence, or create a market.

Additionally, the Lean Canvas highlights uncertainties explicitly, making it easier to identify which components of the emerging business model require further validation, data collection, or stakeholder engagement. It promotes comparability across multiple ERs because each is summarized using the same framework, enabling more informed prioritization and strategic planning. By structuring early insights into a concise yet comprehensive format, the Lean Canvas supports the broader technoeconomic process, helping ensure that subsequent modelling, risk analysis, or exploitation planning builds on clearly articulated assumptions about value, customers and operational pathways.

### 2.2.4.Complementary Use of Both Tools

Using SWOT and Lean Canvas together provides two complementary methodological perspectives that strengthen the early-stage evaluation of each commercially relevant result. The SWOT analysis captures internal and external contextual factors, offering a qualitative understanding of the technological, organizational and environmental conditions that may influence adoption. In parallel, the Lean Canvas structures the emerging business model by articulating the problem–solution fit, identifying potential users or customers, clarifying the unique value proposition and outlining the preliminary logic of costs, revenues and operational pathways.

Combined, these tools establish a coherent foundation for the technoeconomic and business modelling presented in Section 4. They allow available information to be organized systematically and transparently, ensuring that both the contextual positioning of the technology and its potential commercial configuration are considered from the outset. They provide a structured, assumption-based framework that highlights what is known, what is uncertain and what requires further validation. This integrated perspective enhances the robustness of subsequent technoeconomic assessments by

grounding them in clearly articulated insights regarding technological potential, market relevance and preliminary business logic.

## 2.3. Methodology for the Commercialization Planning

The commercialization planning presented in Section 5 is based on a structured methodology designed to document how each commercially relevant project result may progress toward potential adoption and use. This component of the methodology supports partners in articulating intended exploitation paths and in identifying the factors that may influence the successful realization of these intentions. Two tools are used for this purpose: the **Characterization Table** and the **Fuzzy Analytical Hierarchy Process (Fuzzy AHP).**

### 2.3.1. Characterization Table for Commercially Relevant Results

For each result identified as commercially relevant, partners completed a Characterization Table in accordance with a commonly used template which was taken from the Horizon Booster Platform. This table serves as a structured planning and documentation tool rather than as an analytical input. Its primary purpose is to consolidate, in a single coherent format, the information required to articulate the potential commercialization trajectory of each result. The table captures elements typically considered in early-stage exploitation planning, including a concise description of the result; the target markets and end users it is intended for; the needs or problems those users may face; the competitive environment and available alternative solutions; the unique value proposition as currently perceived by the partners; the intended use model such as product, service, licensing, or technology transfer; potential early adopters; the expected timeline for development or deployment; and relevant aspects of the intellectual property strategy.

This structured consolidation of information is important for commercialization planning because it anchors strategic decision-making in a clear, shared understanding of each result's positioning and potential. Commercial pathways can only be meaningfully defined when technical capabilities, market contexts, user needs and competitive dynamics are explicitly mapped. By requiring partners to articulate these elements in a consistent manner, the Characterisation Table makes it easier to identify gaps in knowledge, uncertainties requiring validation and dependencies that may influence exploitation strategies. It also supports alignment among partners by ensuring that assumptions about markets, use cases, differentiation and IP considerations are recorded transparently rather than implicitly held or unevenly understood.

Furthermore, the table's standardized structure facilitates comparability across multiple results, which is essential when prioritizing resources, identifying synergies, or determining which results are most suitable for specific exploitation routes. It establishes the informational baseline upon which more detailed commercial assessments, risk analyses, or investment decisions can later be built. In this way, the Characterisation Table provides a foundational reference point for the broader commercialization planning work described in subsequent sections, ensuring that strategic discussions and modelling activities are grounded in consistent, well-organized, and partner-validated inputs.

### 2.3.2. Fuzzy AHP for Prioritization of Success Factors

The project also applies the Fuzzy Analytical Hierarchy Process (Fuzzy AHP) at the overall project level to complement the documentation of result-specific commercialization paths. This method enables the structured prioritization of factors that may influence the commercialization prospects of the project's results. The approach begins with the definition of evaluation criteria and sub-criteria that

represent aspects considered relevant for commercialization success. Domain experts then perform pairwise comparisons of these criteria, allowing them to express the relative importance of each factor. Instead of requiring exact numerical judgements, the method incorporates fuzzy logic, which captures uncertainty and variability in expert assessments. The process ultimately yields criterion weights that represent a prioritized set of commercialization-relevant factors based on the collective expert perspective under conditions of uncertainty.

This method is valuable for commercialization planning because it offers a systematic way to identify which considerations are perceived as most critical for successful exploitation. While individual results may have unique attributes and market contexts, commercialization at the project level also depends on overarching factors that influence the likelihood of uptake across different domains. By quantifying expert consensus in a way that accommodates ambiguity, Fuzzy AHP provides a more realistic representation of the decision environment surrounding innovation deployment, where complete information is rarely available and expert judgments often involve degrees of confidence rather than definitive values.

The resulting prioritization does not evaluate specific results but instead clarifies which success factors warrant emphasis in future exploitation activities. This helps guide strategic planning by highlighting where resources, attention, or risk-mitigation measures may need to be concentrated. It also promotes transparency and consistency in decision-making, ensuring that subsequent commercialization efforts are aligned with an agreed set of structured priorities rather than informal or unarticulated assumptions. In this way, Fuzzy AHP strengthens the project's overall exploitation framework by grounding high-level planning in a methodologically robust, uncertainty-aware process.

Below, we provide a detailed description of the mathematical process that was followed.

*Definition of the criteria set*

Let

$$\mathbb{C} = \{C_1, C_2, \ldots, C_n\}$$

denote the set of commercialization-related criteria. The objective of the analysis is to derive a weight vector

$$W = \{w_1, w_2, \ldots, w_n\}$$

where $W_i$ represents the relative importance of criterion $C_i$.

All the weights should add up to one, namely:

$$\sum_{i=1}^{n} w_i = 1$$

*Elicitation of expert judgements (pairwise comparisons)*

A panel of experts provides pairwise comparisons of the criteria. For each unordered pair $(C_i, C_j)$, with $i \neq j$, experts express:

1. **Direction of preference** (which criterion is more important) and

2. **Strength of preference** using a linguistic scale.

The linguistic scale is defined as:

- Equal importance
- Slightly more important
- Moderately more important
- Extremely more important

For each pair $(C_i,\ C_j)$, each expert selects exactly one option, such as

"$C_i$is moderately more important than $C_j$" or

"$C_j$is slightly more important than $C_i$" or

"Equal importance".

*Linguistic scale and fuzzy representation*

Each linguistic term is mapped to a triangular fuzzy number (TFN) $a_{ij} = (L,\ M,\ U)$, where $L$ , $M$ and $U$ denote the lower, mid and upper bounds of the judgment, respectively. A typical mapping is shown in Table 1:

Table 1: Mapping of Linguistic Scale to Triangular Fuzzy Number

| Linguistic Scale | Mapping |
|---|---|
| **Equal Importance** | **(1,1,1)** |
| **Slightly more important** | **(1,2,3)** |
| **Moderately more important** | **(2,3,4)** |
| **Extremely more important** | **(4,5,6)** |

If for a given pair $(C_i,\ C_j)$ the expert states that "$C_i$ is $X$ more important than $C_j$" and $X$ corresponds to $(L,\ M,\ U)$, then the reciprocal judgement "$C_j$ is $X$ less important than $C_i$" is represented by the fuzzy reciprocal:

$$a_{ji} = \left(\frac{1}{U},\ \frac{1}{M},\ \frac{1}{L}\right)$$

Diagonal elements are defined as $a_{ii} = (1,\ 1,\ 1)$.

*Individual fuzzy pairwise comparison matrices*

For each expert, a fuzzy pairwise comparison matrix of size $n\ x\ n$ is constructed, where each element $a_{ij}$ is the TFN associated with the judgement of criterion $C_i$ against $C_j$.

By construction:

- $a_{ii} = (1,\ 1,\ 1)$
- $a_{ji}$ is the fuzzy reciprocal of $a_{ij}$

*Consistency analysis (crisp AHP at individual level)*

Consistency is evaluated at the **individual expert level** using the classical AHP Consistency Ratio (CR). To this end, each linguistic judgement is also mapped to a single crisp number (e.g. to the midpoint of the corresponding TFN), as shown Table 2:

Table 2: Crisp Mapping of Linguistic Scale

| Linguistic Scale | Crisp Mapping |
|---|---|
| **Equal Importance** | **1** |
| **Slightly more important** | **2** |
| **Moderately more important** | **3** |
| **Extremely more important** | **5** |

This yields a crisp comparison matrix for each expert. For each matrix:

1. The priority vector $w$ is computed.
2. The maximum eigenvalue $\lambda_{max}$ is determined.
3. The Consistency Index $CI$ is calculated as:

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

where $n$ is the number of criteria.

4. The CR is:

$$CR = \frac{CI}{RI_n}$$

where $RI_n$ is the Random Index for matrix size $n$ (e.g. $RI_3 = 0.58$, $RI_4 = 0.9$, $RI_5 = 1.12$, etc.).

Only expert matrices with acceptable consistency, namely $CR < 0.1$, are retained for the fuzzy aggregation step. This ensures that the final fuzzy analysis is based on internally coherent judgements.

*Aggregation of consistent expert judgements*

For each pair $(i, j)$, the fuzzy judgements from all consistent experts are aggregated by component-wise averaging of the corresponding TFNs:

$$a_{ij} = \left( \frac{1}{m} \sum_{k=1}^{m} L_{ij}(k), \frac{1}{m} \sum_{k=1}^{m} M_{ij}(k), \frac{1}{m} \sum_{k=1}^{m} U_{ij}(k) \right)$$

where $m$ is the number of experts whose CR met the threshold.

This yields a single aggregated fuzzy pairwise comparison matrix.

*Derivation of fuzzy criterion weights*

To derive fuzzy weights from this final matrix, a standard fuzzy AHP procedure is applied. A simple and transparent formulation is:

1. Compute the **row-wise fuzzy sums**:

$$S_i = \sum_{j=1}^{n} a_{ij}$$

2. Compute the **total fuzzy sum**:

$$S_{tot} = \sum_{j=1}^{n} S_i$$

3. Obtain the fuzzy weight for each criterion by fuzzy division:

$$w_i = \frac{S_i}{S_{tot}},\ i = 1,\ \ldots,\ n$$

where division of TFNs is performed component-wise.

This results in a fuzzy weight vector

$$W = \{w_1,\ \ldots,\ w_n\}$$

where each $w_i = (L_i,\ M_i,\ U_i)$ expresses the importance of criterion $C_i$under uncertainty.

*Defuzzification and normalization*

For practical use and reporting, each fuzzy weight is transformed into a crisp value via the centroid method:

$$w_i' = \frac{L_i + M_i + U_i}{3}$$

These preliminary crisp scores are then normalized to obtain the final weights:

$$w_i = \frac{w_i'}{\sum w_j'}$$

*Use of the resulting weights*

The final normalized weights $w_i$represent the relative importance of each commercialization success factor, as derived from consistent expert judgements under uncertainty. These weights can subsequently be used to:

- Rank the criteria in terms of perceived influence and
- Inform the design of commercialization and exploitation strategies

In this way, the mathematical formulation of Fuzzy AHP operationalizes expert knowledge into a quantitative, uncertainty-aware weighting scheme that supports transparent and reproducible decision-making.

### 2.3.3. Relationship Between Both Tools

The Characterization Tables and the Fuzzy AHP serve complementary roles within Section 5, each contributing a distinct layer of insight to the project's commercialization planning. The Characterization Tables document the commercialization intentions, assumptions, and contextual elements associated with each ER. They capture result-specific information such as target markets, competitive positioning, value propositions, and potential pathways for deployment, ensuring that each result is described with precision and consistency.

The Fuzzy AHP, by contrast, operates at the project level and identifies which categories of factors are collectively considered most influential in shaping commercialization outcomes. Through a structured, uncertainty-aware weighting process, it highlights the broader success conditions that may affect multiple results, regardless of their specific technical characteristics or intended markets.

Together, these tools form the methodological foundation for Section 5 by integrating bottom-up and top-down perspectives. The Characterization Tables provide detailed narratives of individual exploitation trajectories, while the Fuzzy AHP supplies a cross-cutting prioritization of success factors that can inform strategic focus, resource allocation, and risk awareness. This combined approach allows commercialization planning to be presented in a coherent, transparent, and systematically organized manner without attempting to generate commercial forecasts or prescriptive recommendations. Instead, it establishes a structured decision-support framework that captures partner intentions, expert judgments, and the key conditions that may influence future exploitation efforts.

# 3. Market Analysis

## 3.1. Target Markets

### 3.1.1. 5G / B5G Market Trends

The 5G and B5G landscape is undergoing a period of accelerated transformation driven by the convergence of wireless communications, AI, and edge-enabled digital services. The global 5G ecosystem, including devices, networks, and enabling materials, continues to expand rapidly, supported by large-scale deployments across industrial, urban, and consumer domains [2] [3] [4] [5].

*Massive Market Growth and Network Densification*

The 5G market is projected to reach over USD 427 billion by 2028, representing a Compound Annual Growth Rate (CAGR) exceeding 34% [6]. Supporting this trajectory, 5G materials alone are expected to grow from USD 0.2 billion (2024) to USD 2.0 billion by 2029 [2], reflecting the proliferation of high-frequency and low-loss materials essential for millimeter-wave performance. These innovations address increasing demands for enhanced mobile broadband (eMBB) and ultra-reliable low-latency communication (URLLC) services. The corresponding densification of small-cell and indoor-5G networks forecast to grow from USD 17.48 billion (2025) to USD 54.40 billion (2034) [7] is key to sustaining throughput and connectivity across smart cities, logistics hubs, and industrial environments.

For NANCY, these developments illustrate a vibrant technological base into which its distributed, intelligent, and blockchain-enhanced networking components could integrate. The system's architecture aligns with a future network topology characterized by decentralized orchestration, distributed intelligence, and resource virtualization.

*Industrial and Societal Digitalization*

Accenture forecasts that 5G could add €1 trillion to European Gross Domestic Product (GDP) between 2021 and 2025, as shown in Figure 1 [4] [8]. Growth stems from vertical-specific deployments, smart manufacturing, connected health and autonomous mobility, which require deterministic latency and resilient service assurance. The rise of private 5G networks [7] and industrial Internet of Things (IoT) clusters points to a shift from consumer-centric to enterprise-driven revenue models. McKinsey [9] and KPMG [10] both underline that 5G serves as a technological backbone for AI-native applications, distributed sensing, and data-driven sustainability monitoring.

Within this context, NANCY's focus on flexible, trust-enhanced network orchestration aligns with macro-trends toward secure, sustainable 5G infrastructures. Its design concepts, such as blockchain-based trust management and cognitive orchestration, address emerging industry priorities of transparency, energy efficiency, and multi-stakeholder interoperability.

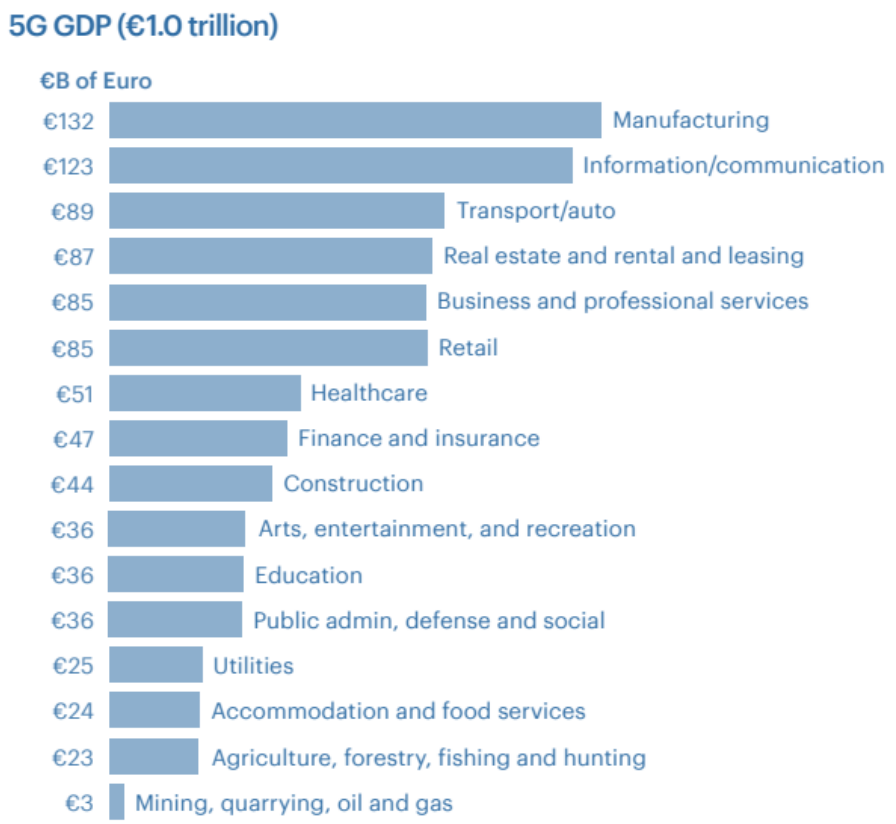



Figure 1: Accenture 5G GDP Forecast

### *AI-Native and Energy-Efficient 6G Transition*

Looking toward beyond-5G and 6G, reports from ITU-R M.2516 [11] and McKinsey [9] emphasize a convergence of communications, computing, and sensing within AI-driven architectures. Future International Mobile Telecommunications systems will feature AI-native communications, integrated sensing & computing, energy-aware radio designs, and trustworthy operation [12]. The emergence of such intelligent network fabrics will benefit from platforms capable of self-optimization and policy-driven security, concepts echoed in NANCY's modular AI-enhanced framework.

As 5G infrastructure becomes foundational for 6G experimentation, early adoption of AI-assisted orchestration, zero-trust security models, and programmable interfaces offers a competitive advantage. NANCY's approach to blockchain-secured orchestration and distributed trust fits within the anticipated move toward decentralized, machine-assisted network governance.

### *Cross-Sector Convergence and Ecosystem Partnerships*

The telecom sector is evolving into a "Techco" model [10], where connectivity providers expand into integrated digital-service ecosystems combining content delivery, cloud-edge infrastructure, and AI analytics. Strategic partnerships between equipment vendors, operators, and software platforms are essential to unlock interoperable and sustainable network solutions.

In this collaborative environment, NANCY's modular and open-source-inspired framework can serve as an enabling layer for multi-party experimentation. Its alignment with open interfaces, Open RAN (O-RAN) principles, and blockchain-based accountability supports future cross-industry federations without asserting dominance or exclusivity. Moreover, NANCY's architecture incorporates a service-driven marketplace, enabling the registration, discovery, and negotiation of network functions and capabilities, which aligns naturally with the sector's transition toward digital service ecosystems.

### 3.1.2. 5G / B5G Market Challenges - Entry Barriers

Despite substantial momentum, the 5G market faces technical, economic, and regulatory barriers that may constrain diffusion. Many of these challenges correspond to areas where NANCY's capabilities decentralization, secure orchestration, and AI-assisted automation could provide incremental improvements.

*High Deployment and Operational Costs*

Infrastructure rollout remains capital-intensive. The shift to dense networks with numerous small cells [7] [5] requires significant investment in spectrum, power management, and backhaul. According to Ericsson [5], fewer than 20% of service providers currently operate 5G standalone (SA) networks, revealing an ongoing gap between potential and deployment. Moreover, sustainability constraints highlighted by KPMG [10] add pressure to minimize energy consumption and carbon footprint.

NANCY's lightweight, software-defined components and intelligent resource management mechanisms can support operators in experimenting with cost-optimized architectures, particularly for private and localized deployments, without altering core business models.

*Spectrum Fragmentation and Regulatory Heterogeneity*

Uneven spectrum allocation and inconsistent regulatory frameworks across regions [4] [5] [11] slow global harmonization. Divergent frequency bands and licensing regimes hinder economies of scale and equipment interoperability. The EU's goal of coordinated 5G rollout faces administrative delays and divergent national policies.

By embedding flexible policy enforcement and distributed trust, NANCY's blockchain-based control plane could complement standardization efforts, offering traceable configuration management and secure inter-operator coordination. However, adoption remains dependent on compatibility with established European Telecommunications Standards Institute (ETSI) and 3GPP frameworks. In this regard, as an example, NANCY's KER3 already follows the guidance of ETSI [13].

*Security, Privacy and Trust Deficits*

As networks become more software-defined and data-centric, vulnerabilities increase. Concerns over supply-chain integrity, vendor trust, and data governance continue to shape procurement strategies [10] [11]. The introduction of AI for autonomous management introduces additional attack surfaces that require explainability and accountability.

NANCY's integration of blockchain for auditable transactions and AI for anomaly detection corresponds to industry moves toward zero-trust architectures, but widespread implementation will depend on cost, interoperability, and regulatory acceptance.

*Sustainability and Energy Consumption*

Energy usage of 5G radio access networks (RAN) and edge data centers is rising [10] [11]. As environmental policies tighten, operators are pressured to adopt energy-aware architectures and carbon-neutral operations. Materials research [2] and AI-based optimization are recognized as core enablers for energy efficiency.

Several NANCY results target energy-aware optimizations [14]. For example, KER12 introduces AI-based RAN orchestration mechanisms that enhance efficiency and reduce energy consumption in radio access operations, while KER9 applies semantic compression to lower traffic volumes, increasing both energy and data efficiency across the network. Complementary, working on efficient AI execution, such

as the data-drift detection framework, developed in OER2, further contributes to reducing the computational footprint of AI network components.

### 3.1.3. Blockchain in Telecom Market Trends

Blockchain adoption in telecommunications is progressing from exploratory pilots to progressively more structured deployments, driven by the need for secure, transparent, and automated network operations. Our findings highlight a rapidly expanding market, with estimates ranging from USD 3.21 billion in 2023 to nearly USD 20 billion in 2035 for blockchain-in-telecom applications, see Figure 2 [15] [16]. Growth is underpinned by demand for fraud reduction, decentralized trust mechanisms, automated service assurance, and integration with 5G/B5G architectures. These trends create a favorable environment for platforms such as NANCY, which integrates blockchain as part of its Blockchain Radio Access Network (B-RAN) framework.

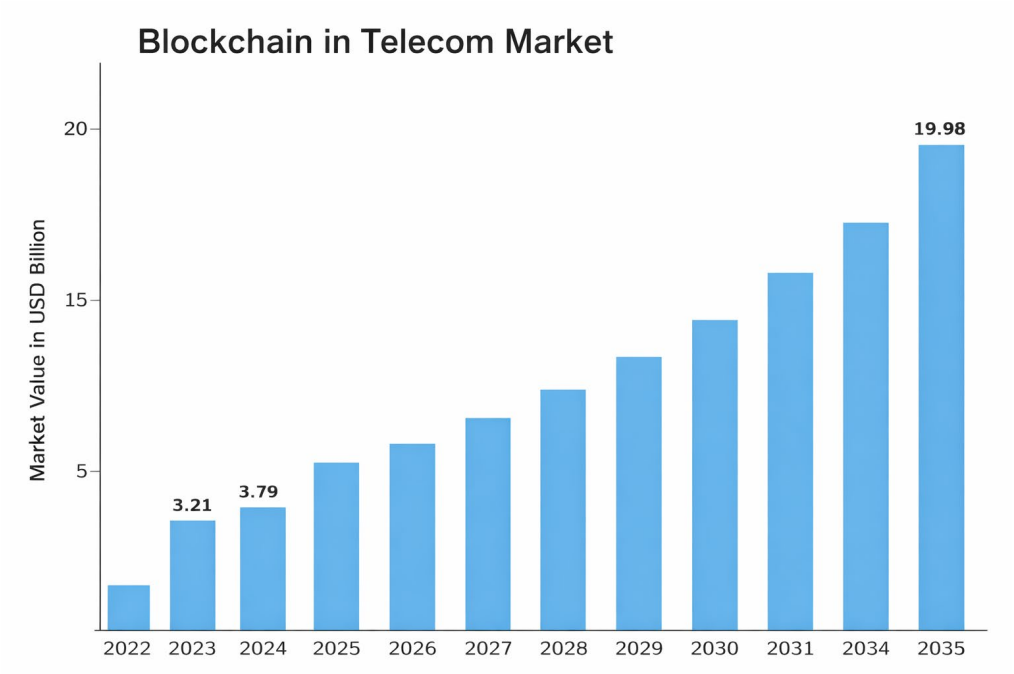



Figure 2: Blockchain in Telecom Market Value Forecast

*Rapid Market Expansion Driven by Security, Automation and Decentralization*

Across multiple sources, blockchain technology is projected to grow at high CAGRs: 18–31 % specifically for telecom [15] [16] and more than 40 % for the broader blockchain market [17] [18]. Telecom-specific adoption is dominated by fraud management, identity authentication, and smart-contract-powered automation [15]. Fraud alone accounts for annual operator losses exceeding USD 30 billion, motivating investment in tamper-resistant transaction systems and verifiable identity management [16].

These technology trajectories resonate with NANCY's approach to decentralized security assurance in the B-RAN architecture, where distributed ledger components can enhance transparency, traceability and trust among nodes without depending on a single authority.

*Emergence of Blockchain for Identity, Service Assurance and Network Resource Management*

Studies note that decentralized identity (DID) frameworks and verifiable credentials are becoming essential enablers for secure onboarding of devices and users [19] [15] [20]. Decentralized identities reduce reliance on centralized authentication databases, decrease risk from single points of failure, and enable secure interoperability across multi-provider environments. Smart contracts are also

identified as the fastest-growing segment within telecom-blockchain deployments [15], reflecting increased interest in automated billing, Service Level Agreement (SLA) enforcement, roaming agreements, and dynamic resource trading.

These directions align naturally with several NANCY functional areas, particularly the blockchain-enhanced control plane and multi-tenant B-RAN logic, which enable accountable interactions among network actors. NANCY's emphasis on lightweight distributed trust mechanisms provides an experimental testbed for evaluating how smart contracts and tamper-resistant logs may support service provisioning in B5G scenarios.

*Convergence with 5G, IoT and Edge Computing*

Blockchain is increasingly positioned as a complementary technology to 5G, capable of improving security and coordination across dense IoT ecosystems. Reports forecast that integration with 5G infrastructure will enable low-latency, high-throughput blockchain transactions and support new decentralized applications [16]. Telecom operators are particularly exploring use cases such as device lifecycle tracking, spectrum sharing, and multi-operator network slicing. Broader market studies show that blockchain adoption correlates with uptake of IoT and edge computing services, especially where trust and verifiability are essential [17] [21].

These trends connect well with NANCY's technical vision; the project already integrates blockchain-based components with distributed AI and edge processing. The interplay among these technologies illustrates realistic future deployment paths for B-RAN-style infrastructures, strengthening the European position in trustworthy 6G-era architectures.

### 3.1.4. Blockchain in Telecom Market Challenges - Entry Barriers

Even with positive momentum, blockchain adoption in telecom faces several structural challenges. Many of these issues overlap with areas that NANCY can help investigate experimentally. NANCY's blockchain-enabled B-RAN modules can provide evidence-driven insights on feasibility, overhead, and integration pathways.

*Scalability, Throughput and Latency Constraints*

A recurring concern across sources is blockchain scalability, particularly for telecom workloads that involve millions of devices and real-time operations [16] [22]. Traditional consensus mechanisms may not meet latency requirements for B5G control loops, fast handovers, or time-sensitive service assurance. Even advanced Layer-2 or sharded architectures require careful tuning to support telecom-grade performance.

NANCY's design emphasizes lightweight consensus and selective blockchain usage, avoiding heavy reliance on blockchain as a data-plane mechanism [23]. This approach reflects broader industry guidance that blockchain must be deployed judiciously to avoid introducing bottlenecks into latency-critical 5G/B5G systems.

*Integration with Legacy Systems and Multi-Vendor Environments*

Telecom networks are heterogeneous, multi-generation environments, and integrating blockchain into billing, subscriber management, or roaming systems is non-trivial. Reports note that integration complexity and interoperability limitations are major inhibitors for adoption [15] [16] [22]. Legacy platforms often rely on centralized data management schemas that are difficult to adapt to distributed ledger operations.

In this context, NANCY offers a controlled, research-grade framework where operators can test interoperability scenarios, such as using smart contracts for localized resource policies or using

decentralized logs for anomaly tracking. These demonstrations can support understanding of integration trade-offs.

*Regulatory Uncertainty and Compliance Requirements*

Blockchain deployments in telecom must comply with General Data Protection Regulation (GDPR), data-retention laws, lawful-intercept regulations, and sector-specific security policies. However, the immutability and decentralization of blockchain can complicate deletion, auditability, and jurisdictional control. Multiple reports observe that regulatory uncertainty remains one of the largest barriers to adoption, especially in Europe [17] [18] [22].

NANCY's experimentation with permissioned blockchain models provides researchers with insights into how compliance-friendly ledger configurations may support secure telecom operations, as well as a platform for experimentation.

*Energy Consumption and Sustainability Concerns*

While many telecom-blockchain deployments use energy-efficient permissioned ledgers, wider industry discourse still highlights concerns about energy usage [17] [20]. Sustainability considerations are increasingly important as operators aim to reduce their carbon footprint and align with the EU Green Deal objectives.

NANCY's architecture supports the investigation of energy-aware blockchain configurations and can contribute to studies on low-overhead consensus mechanisms suitable for edge and RAN environments [23].

### 3.1.5.Cybersecurity & Post-Quantum Security Market Trends

Cybersecurity has become a foundational pillar of digital transformation across all Information and Communications Technology (ICT) domains, and our Market Analysis highlights a sustained acceleration in both traditional and emerging security markets. The cybersecurity sector is forecast to reach USD 262.29 billion by 2030 [24], while global spending across security categories may surpass USD 1 trillion annually by 2031, in Figure 3 [25]. Within this broad landscape, new drivers, AI-powered security analytics, decentralized trust models, quantum-safe cryptography, and zero-trust architectures are reshaping expectations for 5G and beyond.

These market developments directly affect the trust, resilience, and security requirements of future B5G networks, areas that NANCY addresses through secure orchestration, blockchain-assisted verification, AI-enabled detection modules, and Post-Quantum Cryptography (PQC) experimentation.

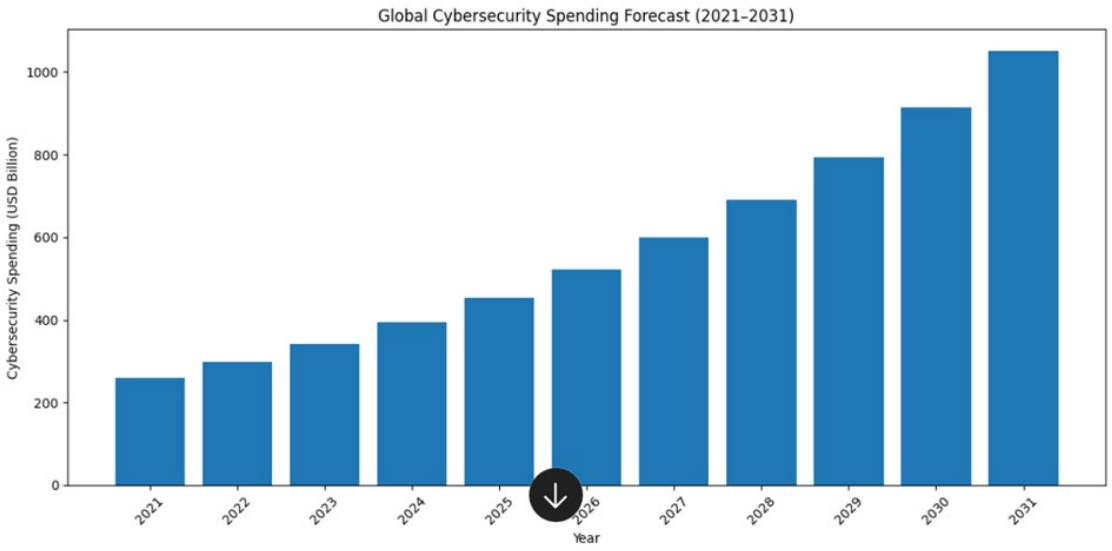



Figure 3: Global Cybersecurity Spending Forecast

### *Rising Importance of Blockchain-Enhanced Security*

The blockchain-in-security market is expected to grow from USD 3.15 billion in 2024 to USD 176.6 billion by 2035 (CAGR 44.2%) [6] [26]. Drivers include enhanced data integrity, tamper-proof logs, decentralized identity, and privacy-preserving analytics. As networks become more distributed, with multi-tenant RANs, edge nodes, and dynamic slices, blockchain provides mechanisms for trustworthy coordination and verifiable policy enforcement.

NANCY's B-RAN concept integrates blockchain to enhance trust across distributed nodes, providing a realistic test environment for exploring secure ledger-based control, decentralized identity management, and transparent policy execution in telecom settings.

### *Europe's Strategic Push Toward Zero-Trust and Regulatory Compliance*

The European cybersecurity market alone is projected to reach USD 107.5 billion by 2030, driven by regulatory pressures, growing attack sophistication, and national digital-sovereignty goals. Zero-trust architectures, identity and access management, and encryption-centric security are highlighted as priority investment areas [27].

NANCY contributes to this trend through its focus on verifiable trust mechanisms, secure onboarding, and strong identity management within the B-RAN framework. These capabilities complement market efforts toward compliance-aligned, transparent, and auditable security architectures.

### *Escalation of Quantum-Era Threats and Demand for PQC*

The Quantum Key Distribution (QKD) and broader PQC markets show significant expansion, with QKD expected to grow from USD 0.48 billion in 2024 to USD 2.63 billion by 2030 (CAGR 32.6 %) [28]. Increased concern over "harvest-now, decrypt-later" attacks and the long-term confidentiality of sensitive data is pushing operators and governments toward quantum-resistant security strategies.

NANCY's architecture actively explores quantum-safe communication mechanisms through several KERs that advance both PQC and QKD. KER3 and KER5 allow NANCY to experimentally evaluate PQC and QKD protocols within its distributed B-RAN framework, quantifying overhead, interoperability, and integration potential, thereby demonstrating practical pathways toward quantum-resilient B5G network security [14].

### 3.1.6.Cybersecurity & Post-Quantum Security Market Challenges - Entry Barriers

While market growth is strong, cybersecurity and PQC adoption face several inhibitors. These challenges correspond to areas where NANCY can support targeted technical exploration.

*Operational Complexity Across Heterogeneous and Multi-Cloud Environments*

Enterprises and telecom operators increasingly manage complex infrastructures spanning cloud, edge, and on-premises environments. This complexity makes threat detection, identity management, and policy enforcement more challenging, especially as network slices and dynamic service chains proliferate. Reports note that secure integration of AI and blockchain into existing systems remains difficult due to interoperability constraints and legacy architectures [6] [27].

NANCY's distributed orchestration model, combined with blockchain-based trust layers, provides a structured environment for evaluating these integration constraints securely. The project demonstrates how decentralized verification and AI-assisted monitoring could be integrated in future B5G settings while keeping security a priority.

*Cost, Scalability and Performance Limitations*

AI-driven cybersecurity and quantum-safe cryptography can introduce additional computational overhead. QKD and PQC deployments face cost barriers, including specialized hardware, cryptographic library updates, and re-architecting secure channels [29] [28].

NANCY provides an experimental platform to measure these overheads in telecom-specific scenarios, helping stakeholders understand performance impacts and transition pathways toward quantum-safe architectures. Moreover, KER4 helps in reducing development and deployment costs.

*Emergence of New Attack Surfaces and Adversarial AI*

The growing adoption of AI and distributed intelligence expands the attack surface. Cybersecurity Ventures forecasts security spending rising sharply due to evolving AI-enabled threats, adversarial manipulation, and increased automation in attacks [25].

NANCY's research into secure AI-based orchestration and anomaly detection contributes exploratory defenses against such emerging threats. NANCY addresses these evolving threat vectors through its work on KER12, which reinforces the project's capacity to counter these new threats.

### 3.1.7.Cloud/IoT/Edge Continuum Market Trends

The Cloud / IoT / Edge Continuum has become a central enabler of digital transformation across industries, indicating rapid acceleration in all three segments. The global cloud computing market is projected to grow from USD 912.77 billion in 2025 to USD 5.15 trillion by 2034 [30] [31], while IoT markets are forecast to surpass USD 2.7 trillion by 2030 and USD 4 trillion by 2032 depending on the source [32] [33]. Edge computing is also expanding rapidly, with estimates ranging from USD 168.40 billion in 2025 to USD 327.79 billion by 2033, as seen in Figure 4 [34] [35]. Across this continuum, new drivers including AI-enabled cloud services, low-latency edge analytics, sovereign distributed infrastructures, and large-scale IoT integration are reshaping expectations for next-generation 5G and B5G networks.

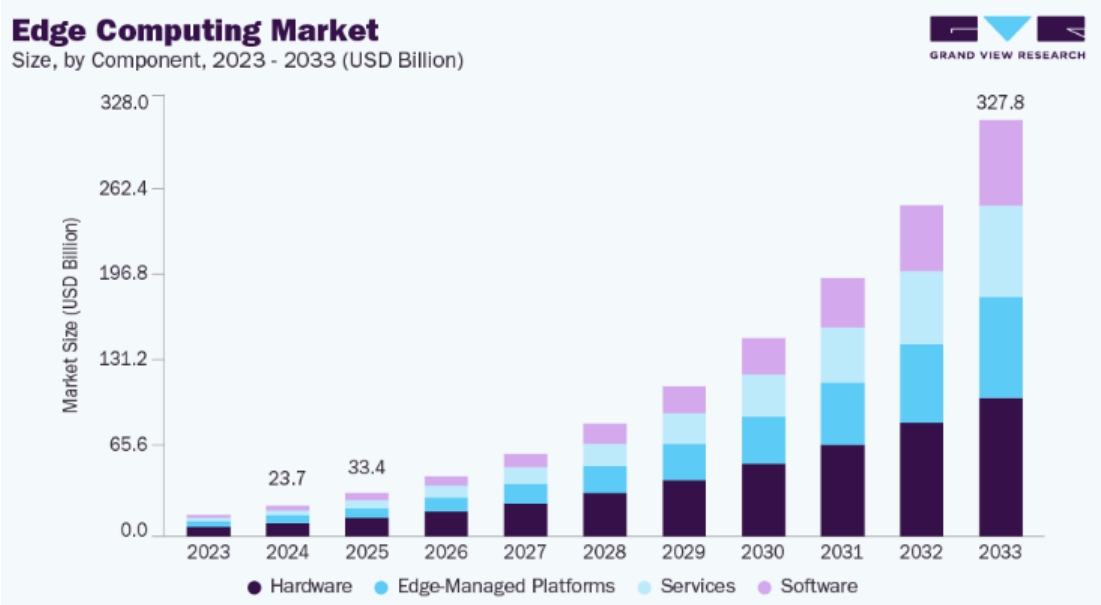



Figure 4: Edge Computing Market Size Forecast

### *Rapid Growth Across Cloud, IoT and Edge Segments*

Our Analysis shows that the Cloud/IoT/Edge continuum is expanding at an exceptional scale. Cloud computing alone is projected to grow from USD 912.77 billion in 2025 to USD 5.15 trillion by 2034, driven by widespread migration to scalable cloud infrastructures and mainstream adoption of hybrid and multi-cloud strategies [30] [31]. In parallel, IoT markets are forecast to reach between USD 864.32 billion and USD 4.06 trillion by 2032, depending on the source, supported by increased sensor deployment, Industry 4.0 automation, smart cities, and large-scale digital transformation initiatives [36] [33]. Edge computing, which underpins real-time processing and low-latency applications, is also expanding rapidly, with estimates ranging from USD 168.4 billion in 2025 to USD 327.79 billion by 2033 [34] [35].

NANCY operates directly within this continuum by leveraging cloud-based AI engines, edge-intelligent B-RAN nodes, and IoT-interfacing components. Its distributed architecture reflects the same structural shifts identified in the market, demonstrating how telecom systems can coordinate intelligence, trust and orchestration across heterogeneous cloud–edge–IoT environments.

### *Integration of AI, Analytics and Advanced Cloud Services*

Across cloud markets, AI-optimized infrastructure is becoming central to value creation. Gartner and related analyses highlight that cloud-native AI, Graphics Processing Unit (GPU)-accelerated compute, and real-time data processing pipelines are driving enterprise adoption of IaaS and PaaS models, with public cloud spending expected to exceed USD 723 billion by 2025 [30] [31] [37]. IoT markets similarly emphasize AI as a requirement for predictive maintenance, anomaly detection, and automated decision-making, with generative AI emerging as a complementary tool for synthetic IoT data generation [33]. Edge platforms increasingly integrate machine-learning inference engines to support Augmented Reality (AR) /VR, autonomous systems, and industrial control workloads [35].

NANCY reinforces this market trend through several exploitable results focused on distributed intelligence and cloud-native AI orchestration. As an example, KER11 is directly tied to the edge computing and IoT continuum, since it leverages Software Defined Network (SDN) enabled Multi-access Edge Computing (MEC) to perform autonomous anomaly detection and self-healing close to IoT data sources, minimizing latency and ensuring resilient operation in cloud-to-edge ecosystems.

*IoT Expansion and the Shift Toward Distributed Intelligence*

The IoT market continues to grow strongly across multiple segments. Mordor Intelligence projects IoT revenues rising from USD 1.35 trillion in 2025 to USD 2.72 trillion by 2030, driven by connected-device proliferation, declining sensor costs, and 5G/ Low-Power Wide-Area Network (LPWAN) expansion [32]. Precedence Research highlights that software and cloud-based analytics dominate IoT value creation, while cloud remains the leading IoT deployment model due to scalability and cost-efficiency [38]. Key sectors, including manufacturing, healthcare, and logistics, rely heavily on real-time insights, which increasingly depend on distributed intelligence across cloud and edge layers.

NANCY supports these industry directions by enabling secure IoT integration through the B-RAN architecture. Its decentralized trust mechanisms and AI-driven orchestration facilitate IoT-enhanced connectivity with verifiable behavior and low-latency responsiveness, attributes that resonate with the evolution of Industry 4.0 and smart-infrastructure deployments.

*Evolution of Edge Computing and Distributed Cloud Services*

Edge computing markets reflect strong demand for low-latency, real-time capabilities. According to MRFR and IMARC, edge and distributed edge cloud markets are projected to expand to USD 42.56 billion (IoT edge) and USD 114.4 billion (general edge computing) by 2035 and 2033, respectively [39] [40]. Drivers include the rise of mission-critical applications, 5G-enabled connectivity, network slicing, AR/ Extended Reality (XR) workloads, and sovereign cloud requirements. The distributed edge cloud market specifically emphasizes data security and compliance as leading application segments [41]. Key industry players are expanding their portfolios with edge-native frameworks and orchestration platforms [42] [35] [40].

NANCY follows these trends through its B-RAN edge nodes, designed to provide localized intelligence, reduced latency, and resilient connectivity for 5G/B5G. Moreover, NANCY's combination of AI orchestration and blockchain-secured coordination demonstrates lab-tested pathways toward trustworthy, distributed edge-cloud ecosystems.

### 3.1.8.Cloud/IoT/Edge Continuum Market Challenges - Entry Barriers

Despite strong momentum across cloud, IoT, and edge markets, we identified several structural and operational barriers that continue to hinder large-scale adoption. Organizations face increasing complexity in managing multi-cloud ecosystems, securing vast IoT device populations, and orchestrating distributed edge infrastructures [30] [39] [32]. Challenges related to interoperability, data sovereignty, compliance, and rising deployment costs further constrain the ability of enterprises to fully leverage continuum-based architectures [41] [35] [40]. Together, these barriers highlight the need for more efficient, trustworthy, and coordinated mechanisms capable of supporting distributed intelligence across cloud, edge, and IoT domains.

*Multi-Cloud Complexity and Operational Overhead*

Enterprises increasingly adopt multi-cloud architectures, but studies show that governance, interoperability, and opacity in cost management remain persistent obstacles. Analysts note that 75% of organizations express concern about cloud security, while hybrid architectures introduce additional integration overheads and architectural fragmentation [30] [43]. Edge computing adds further layers of complexity due to distributed nodes, heterogeneous hardware, and the need for unified orchestration frameworks [34] [35].

NANCY addresses these multi-cloud and edge orchestration challenges through its advanced management and AI-driven coordination frameworks. For example, KER11 enables distributed edge nodes to coordinate reliably under heterogeneous cloud environments with minimal human

intervention. Complementing this, OER14 provides a unified orchestration backbone to deploy, test, and manage NANCY components across geo-distributed Kubernetes clusters with secure connectivity and transparent lifecycle control. Together, these results offer a structured and extensible environment for experimenting with decentralized orchestration pipelines, demonstrating how cloud-native automation can lower operational and maintenance overhead in B5G ecosystems.

### *Security, Privacy and Data Integrity Concerns*

Security remains one of the most significant inhibitors in IoT and edge adoption. Reports highlight ongoing challenges in securing connected devices, managing data integrity, and preventing protocol fragmentation from undermining interoperability [36] [32] [33]. Edge computing also introduces decentralized data flows that must comply with strict regulatory and sovereignty requirements [41] [35].

NANCY tackles these security and integrity challenges through several dedicated KERs. For example, KER3 delivers PQC-ready signature mechanisms and advanced access-control models that enhance protection across heterogeneous IoT and edge environments. Additionally, OER6 “Exploitation of Blockchain technology powered by AI/Machine Learning (ML) algorithms in the field of 5G and Edge computing” extends these capabilities by combining blockchain consensus with intelligent analytics to secure distributed data flows and support verifiable decision pipelines at the edge. These and other results enable NANCY to support secure, interoperable, and regulation-aligned distributed systems where data integrity, accountability, and cross-domain device trust can be systematically validated.

### *Scalability, Interoperability and Standardization Gaps*

Market studies repeatedly emphasize that fragmentation in Application Programming Interfaces (API), protocols, and device ecosystems inhibits the deployment of IoT and edge systems at scale [39] [41] [42] [40]. Scalability challenges particularly affect mission-critical and latency-sensitive deployments, while interoperability gaps increase time-to-market and operational cost. Standardization of orchestration frameworks remains incomplete across edge cloud ecosystems.

NANCY’s modular and open architectural approach, built on interoperable interfaces and decentralized coordination, allows experimentation with cross-domain interoperability between cloud, edge, and IoT components. NANCY leverages established open-source and standardized interfaces across the cloud–edge continuum, notably through its integration with ONF’s SD-RAN framework, which provides cloud-native and interoperable RAN-edge control and alignment with O-RAN specifications. By integrating these ecosystems, NANCY ensures that its components operate on top of widely adopted, standards-driven cloud/edge platforms. In parallel, OER13 “System integration on different Edge platform architectures” validates NANCY’s components across diverse edge hardware platforms, demonstrating efficient integration on heterogeneous systems.

### *High Deployment Costs and Infrastructure Requirements*

Edge and IoT deployments often require significant upfront investment, particularly in hardware, secure gateways, distributed nodes, and AI-enabled processing systems [39] [42]. Additionally, energy demands and resource inefficiencies introduce ongoing operational costs, especially in large-scale distributed systems [34] [35].

NANCY provides a research-grade platform to explore lightweight, cost-efficient architectures. Through distributed AI and blockchain functions tailored for telecom environments, NANCY demonstrates how B5G networks might reduce overhead while maintaining security and performance. KER12 introduces computational offloading and resource-aware scaling mechanisms, low-overhead

policies that reduce the processing burden on edge and IoT devices while sustaining performance in constrained environments.

### 3.1.9.Artificial Intelligence for Networks Market Trends

AI has become a central enabler for next-generation telecom networks, driven by increasing network complexity, accelerated 5G rollout, and demand for automation and real-time decision-making. Across all sources, our Market Analysis consistently identifies AI as one of the fastest-growing technology categories in telecom, with specialized sub-markets emerging for network optimization, orchestration, predictive maintenance, and autonomous network management. The AI in Telecommunication market alone is expected to grow from USD 1.55 billion in 2024 to USD 37.71 billion by 2035 (33.68 % CAGR) [44]. Meanwhile, the broader AI in Networks market is projected to expand from USD 11.53 billion in 2024 to USD 192.42 billion by 2034 (32.51 % CAGR), as seen in Figure 5 [45]. These figures reflect a global shift from manual, rules-based network management toward data-driven autonomous systems, an evolution that directly aligns with NANCY's distributed AI-based orchestration and analytics components.

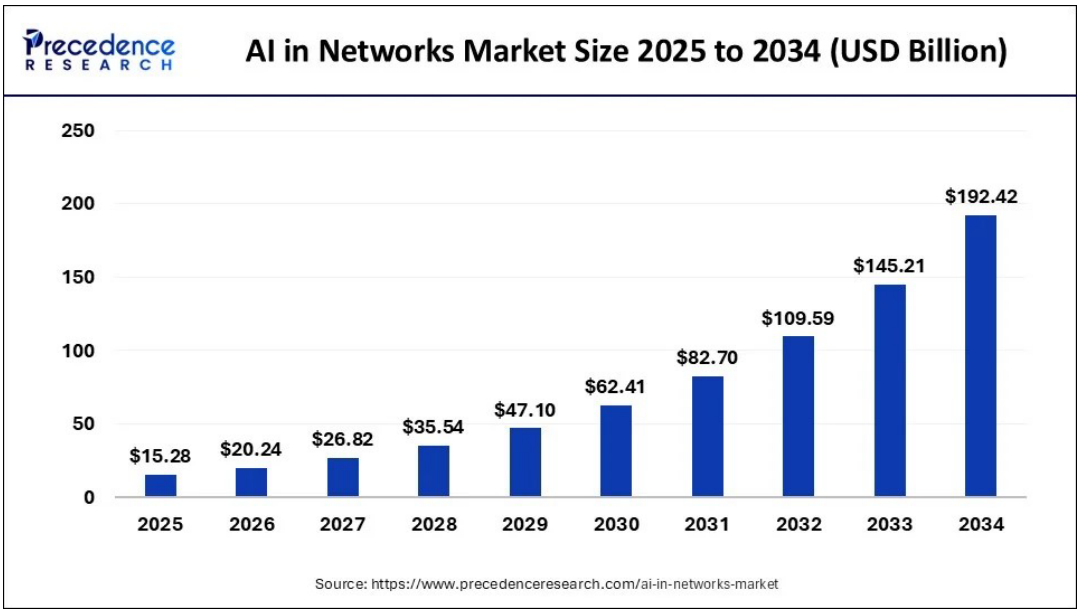



Figure 5: AI in Networks Market Size Forecast

*Growing Use of AI for Network Optimization and Predictive Management*

AI adoption is accelerating across core operational domains such as network optimization, predictive maintenance, anomaly detection, and customer-experience analytics [44] [45] [46]. Telecom networks generate massive volumes of telemetry, and AI enables operators to extract insights for performance tuning, dynamic configuration, and fault prediction. Early deployments have already demonstrated improvements in network resilience and reduced downtime [46].

These trends align closely with NANCY's AI-driven decision engines, which support resource orchestration, anomaly detection, and dynamic policy enforcement within the B-RAN architecture. OER2 "Machine learning models for decision-making" delivers advanced machine-learning models for decision-making, using deep neural networks and reinforcement learning to optimize computational offloading, anticipate performance degradation, and enhance real-time resource selection. Together with KER8's, these components demonstrate how NANCY operationalizes distributed intelligence for continuous optimization, predictive maintenance, and reduced operational overhead in emerging 5G/6G environments.

*AI Orchestration and the Move Toward End-to-End Automation*

Market reports indicate a rapid expansion in AI orchestration, projected to reach USD 17.1 billion by 2028 and USD 35.2 billion by 2031 [45]. AI orchestration supports lifecycle automation for training, inference, data preparation, and real-time optimization. Telecom operators increasingly rely on these tools to address heterogeneous 5G infrastructures, multi-vendor environments, multi-layer service assurance, and edge cloud distribution.

NANCY's architecture aligns strongly with this shift toward end-to-end automation. KER8 offers a pipeline with data and model versioning as well as automatic training and management. In parallel, OER10 "A framework for data and concept drift detection in 6G networks" provides a framework for data and concept drift detection in 6G networks, ensuring that AI models remain reliable over time by identifying when changing network conditions require model retraining or policy adaptations. These are two examples of NANCY's broader suite of results that collectively support the automation of AI model management and retraining.

*AI Combined with Edge Computing for Real-Time Decision-Making*

The combination of AI and edge computing is becoming essential for ultra-low latency and distributed intelligence [44] [47]. Edge deployments can outperform cloud processing for inference tasks, particularly in IoT, MEC, and RAN domains.

Because NANCY integrates distributed AI across both cloud and edge environments, it can concretely demonstrate how real-time decision-making and workload optimization are enabled in B5G systems. KER12 introduces computational offloading mechanisms with resource-aware scaling policies, allowing edge devices to dynamically offload. Complementing this, KER7 provides an AI virtualizer that exploits underutilized computational and communication resources, enabling more efficient execution of inference tasks at the edge. These results, together with others, illustrate how NANCY's edge-intelligent ecosystem reduces dependency on centralized processing while enabling rapid, autonomous adaptation across IoT, MEC, and RAN domains.

### 3.1.10. Artificial Intelligence for Networks Market Challenges - Entry Barriers

Despite substantial growth, AI integration into telecom networks faces structural challenges, many of which NANCY can overcome.

*Explainability, Trust and Regulatory Compliance*

With AI models influencing resource allocation, Quality of Service (QoS) decisions, and security policies, regulatory bodies increasingly emphasize the need for explainability, accountability, and transparency in automated decision-making [10] [48]. Lack of clarity in model outputs or provenance can undermine operator trust and complicate compliance with EU regulations.

NANCY addresses these emerging regulatory and trust requirements through KER10 that delivers an explainable AI framework tailored for network management, enabling operators to interpret model decisions related to resource allocation, anomaly detection, and policy enforcement for trustworthiness and transparency.

*Computational Overhead and Energy Efficiency*

Advanced AI models, especially deep learning and agentic systems, require significant computational and energy resources, which may increase operational costs if not carefully optimized. According to McKinsey, the surge in AI workloads, driven by agentic AI and specialized semiconductors, creates substantial infrastructure demands that organizations must address when scaling intelligent network functions [9]. Similarly, cloud-computing analyses indicate that the move toward ubiquitous AI and

edge intelligence increases pressure on cloud, GPU, and storage resources, requiring operators to manage rising energy consumption and hardware costs [30] [43]. These constraints highlight the need for energy-efficient orchestration and resource-aware AI execution strategies in telecom environments.

NANCY's architecture provides concrete mechanisms to mitigate the energy and computational constraints associated with advanced AI deployments. KER12 introduces computational offloading and resource-aware scaling techniques enabling lightweight inference by dynamically shifting workloads from constrained devices to suitable edge or cloud resources. In parallel, OER10 "A framework for data and concept drift detection in 6G networks" eliminates the need for unnecessary AI training computations by identifying the correct time a model needs to be retrained, contributing to lower energy consumption. These results demonstrate how NANCY supports energy-efficient AI execution across heterogeneous B5G infrastructures.

## 3.2. Competitive Landscape

The analysis presented in Deliverable D1.8 [1] remains largely valid, as the competitive landscape has not changed significantly since its publication. The research projects and business solutions identified there continue to represent the main relevant actors in the field. However, for completeness and to reflect recent developments, additional initiatives and solutions have been included in this updated section.

### 3.2.1. Research Projects

*ACROSS*

The ACROSS (Accelerating Cloud-native cross-domain Orchestration and Service management) project is part of the EU's Smart Networks & Services initiative. ACROSS is developing a secure, cloud-native service deployment and management platform that orchestrates geographically distributed edge-to-core infrastructures. It uses a distributed grid of domain-level orchestrators, supervised by a cloud-managed multi-domain orchestrator linked through a standardized integration fabric [49]. The project focuses on zero-touch operations and end-to-end telemetry, it collects detailed monitoring data from network and compute resources, and employs unsupervised artificial intelligence to turn this data into proactive orchestration decisions. Objectives include designing a future-proof orchestration framework with iterative deep infrastructure visibility, developing a highly distributed service deployment framework, implementing an ultra-sensing telemetry infrastructure, creating an "ultra-instinct" AI stratum for automated decision-making, and ensuring trusted orchestration by protecting devices and data. AI is central to ACROSS, with unsupervised AI for secure reasoning and automated decisions.

*BeGREEN*

BeGREEN is a "beyond-5G" research project focused on AI-assisted energy-efficient O-RAN [50]. The project aims to evolve radio networks, so they support growing traffic and services while treating energy consumption as a first-class design metric. BeGREEN's research spans multiple layers. At the architecture level, it evaluates massive multiple-input multiple-output RAN designs for flexible, energy-efficient connectivity. At the hardware level, it explores radio-unit control schemes and GPU-based offloading engines to reduce the power consumption. At the link level, it uses integrated sensing to balance spectral efficiency with power consumption. Finally, at the system level, it develops AI/ML procedures to adapt the energy usage of softwarized network functions based on utilization patterns, proposing an Intelligent Plane that allows data, models, and inferences to be exchanged across network functions.

*6g-sandbox*

6G-SANDBOX is a project that aims to build a comprehensive, modular experimentation facility to validate next-generation 6G technologies across Europe [51]. Its name derives from its mission: Supporting architectural and technological network evolutions through an intelligent, secure, and twinning-enabled open experimentation facility. The project introduces the concept of trial networks, fully configurable and controllable end-to-end networks that combine physical infrastructure and digital twin elements to support research across user, data, control, and management planes. Its specific objectives include defining an open and modular 6G experimentation architecture aligned with standardization efforts, developing an O-RAN-driven end-to-end connectivity infrastructure incorporating disruptive wireless, transport, and core innovations, creating a resource-management framework that treats the network as "Infrastructure as Code", and offering an automated API-based experimentation lifecycle that produces measurements for emerging 6G use cases.

*Comparison with NANCY*

NANCY differs from these projects through its emphasis on security and trust. Like ACROSS and BeGREEN, NANCY leverages AI for orchestration, but it also integrates blockchain at the RAN level to ensure secure resource management and flexible network operations. It designs Peer-to-Peer (P2P) and mesh architectures to enable distributed intelligence, while aiming for end-to-end protection through blockchain, an aspect absent from ACROSS and BeGREEN. Thus, whereas ACROSS targets cross-domain orchestration, BeGREEN focuses on energy-efficient O-RAN,, and 6G-SANDBOX provides testbeds for 6G trials, NANCY stands out by melding AI and blockchain to build a secure B-RAN architecture that prioritizes privacy, trust, energy-efficiency, and low-latency edge computing.

### 3.2.2. Business Solutions

While advancements in RAN technologies continue at a rapid pace, the telecommunications industry has not yet widely adopted blockchain-based solutions in RAN deployments, with the notable exception of the Helium Network. Although blockchain offers potential benefits in enhancing security, decentralized management, and trust mechanisms, its integration remains limited. Most telecom vendors continue to prioritize traditional innovations such as network slicing, O-RAN, and edge computing.

*Nokia and Mavenir*

Nokia and Mavenir are positioning themselves as key suppliers in the evolving RAN landscape. Nokia's anyRAN strategy frames the company as a neutral systems integrator. Its open-source-based Cloud RAN and purpose-built RAN share common software to ensure feature and performance consistency across hybrid networks. Cloud RAN vertically disaggregates the baseband, so Central Unit / Distributed Unit (CU/DU) software can run on commercial off-the-shelf servers [52], while O-RAN horizontally disaggregates the Radio Unit (RU)-DU-CU chain using standardized interfaces such as the open fronthaul. Nokia argues that its anyRAN approach gives operators "true flexibility" to mix and match vendors and to scale network capacity efficiently. It highlights benefits such as safe investment protection, faster deployment and upgrades, and simplified network operations [53]. The company is developing an L1 "In-Line" SmartNIC to achieve performance parity with purpose-built RAN, which it claims will deliver higher capacity per server and improved energy efficiency. Nokia's commitment to openness extends to partner ecosystems. The Cloud RAN roadmap notes partnerships with Dell, HPE, and hyperscalers (AWS, Google, IBM, and Microsoft) to provide server and container-as-a-service options.

In November 2023, Nokia and Mavenir demonstrated 5G peak performance by interconnecting a Mavenir Citizens Broadband Radio Service (CBRS) with Nokia's AirScale baseband using the

O-RAN-compliant 7-2x interface, activating 4CC carrier aggregation across Time Division Duplex and Frequency Division Duplex spectrum [54]. The test validates Nokia's claim that its anyRAN software can interoperate with multiple radio suppliers without compromising performance or energy efficiency. Mavenir emphasized that the trial represents "real Open RAN" where products from different vendors integrate seamlessly [55]. Collectively, these developments suggest a competitive landscape where incumbent suppliers such as Nokia invest heavily in open and cloud-native architectures to maintain market share.

### *Parallel Wireless*

Parallel Wireless positions its O-RAN solution as a flexible alternative to traditional RAN architectures. Their 5G New Radio uses flexible waveforms and multiple access techniques to improve spectral efficiency and network capacity, supporting a broad mix of services and deployment scenarios. Parallel Wireless's cloud-native O-RAN software suite can increase spectrum efficiency, traffic capacity, and reliability while reducing end-to-end latency. The solution supports fixed wireless access, eMBB, massive machine-type communications and URLLC, and the company's O-RAN hardware is software-upgradable for future-proofing [56]. Beyond the radio layer, Parallel Wireless offers an O-RAN controller and network orchestrator that automates multi-vendor RAN deployments, providing self-configuration, self-optimization, and predictive scheduling to lower deployment and maintenance costs. Its analytics suite uses big data to train and infer machine-learning models for anomaly detection and performance prediction, enabling AI-driven decisions that improve subscriber experience and network troubleshooting.

In 2025, Zain Kuwait and Parallel Wireless completed a proof-of-concept demonstrating the maturity of O-RAN for fixed wireless access [57]. The test used Parallel Wireless's GreenRAN hardware-agnostic solution and achieved download speeds exceeding 1.3 Gbps. The tests also delivered more than 35 % energy savings compared with legacy benchmarks. Together, these results highlight that Parallel Wireless not only delivers AI-enhanced network automation but also demonstrates real-world performance and sustainability benefits, strengthening its position in the competitive O-RAN landscape.

### *Helium Decentralized Network*

The Helium Network presents a radically different approach to wireless infrastructure by combining a global Long Range Wide Area Network (LoRaWAN) network for IoT sensors with a people-powered mobile network built on Wi-Fi hotspots [58]. Individuals or businesses purchase and install Helium "Hotspots", which provide local coverage and relay data across the network, earning rewards in the form of Helium Network Tokens. This decentralized architecture has expanded beyond its roots by integrating a 5G network using 5G-equipped hotspots, enabling participants to contribute to cellular coverage. The crowdsourced model flips the traditional telecom paradigm by putting network ownership in the hands of individuals rather than operators.

Helium's two networks each target distinct market segments yet share a common token economy. The IoT network, described as the world's largest contiguous LoRaWAN network, supports asset tracking, smart agriculture, smart cities, and other industrial IoT applications. Companies and developers leverage it to connect sensors and devices [59]. Helium's mobile network is marketed as "crowd-built cellular", using people-owned hotspots and existing passpoint-capable Wi-Fi access points to offload traffic for major U.S. carriers and deliver low-cost coverage to communities. Participants earn cryptocurrency by providing coverage, while users burn cryptocurrency when sending data across the network, ensuring a balance between supply and demand and giving everyone a stake in the network's success. Helium's decentralized, blockchain-enabled model positions it as an unconventional

competitor in the wireless landscape, especially for IoT and carrier offload use cases, but its competitive advantage hinges on community participation and regulatory clarity.

## 3.3. Key EU Initiatives

### 3.3.1. Data Governance Act

The Data Governance Act (DGA) is an EU regulation designed to increase the availability, accessibility, and trustworthy reuse of data across the European Union [60]. It establishes a harmonized framework that enables both personal and non-personal data held by public-sector bodies to be reused under secure and controlled conditions. By complementing existing laws such as the GDPR, the DGA introduces additional technical and organizational safeguards, such as anonymization, pseudonymization, and secure processing environments, to unlock data that cannot be released as open data.

A central element of the DGA is the creation and regulation of data intermediation services. These intermediaries are required to operate as neutral, transparent facilitators that help organizations and individuals share or pool data without exploiting the data for their own benefit. The goal is to increase trust in cross-sector and cross-border data transactions, thereby supporting the development of common European data spaces in areas such as health, mobility, energy, and manufacturing.

The DGA also introduces data altruism, enabling organizations and individuals to voluntarily provide data for projects serving the public interest. To support this, the Act defines requirements for recognized data altruism organizations and establishes the European Data Innovation Board, which promotes best practices, interoperability standards, and governance frameworks needed for a functioning EU-wide data ecosystem.

*Relevance to NANCY*

NANCY demonstrates strong alignment with the DGA through its emphasis on trustworthy data handling and secure data reuse across distributed network infrastructures. The DGA seeks to enhance confidence in cross-sector and cross-border data flows by mandating transparency, accountability, and robust technical safeguards. NANCY's Blockchain-RAN architecture directly supports this objective by introducing tamper-evident, auditable, and verifiable transaction records. By maintaining immutable logs of data access events and network decisions, the system offers a transparent foundation that reinforces trust among diverse stakeholders and mitigates the risk of information asymmetry in multi-party environments.

Furthermore, the integration of smart contracts within NANCY enables the automated enforcement of well-defined data governance rules. These programmable mechanisms ensure that data use conditions are consistently applied, traceable, and aligned with declared policies. As a result, NANCY provides a technical substrate that mirrors the DGA's ambition to create neutral, accountable intermediaries capable of supporting high-value data exchange without exerting unilateral control or exploiting shared data assets. This establishes NANCY as a technically neutral mediator in the data-sharing ecosystem, consistent with the regulatory expectations for data intermediation services under the DGA.

### 3.3.2.Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography establishes an EU-wide strategy for mitigating the systemic risks that quantum computing poses to current cryptographic foundations [61]. Recognizing that public-key schemes such as RSA and discrete-logarithm–based mechanisms will become vulnerable once large-scale quantum computers emerge, the roadmap underscores the urgency created by long data-retention periods and the "store now, decrypt later" threat model. With expert estimates indicating a meaningful probability of quantum breaks within the next decade and considering that cryptographic transitions for critical infrastructures often require more than five years, the roadmap positions immediate preparation as a strategic necessity.

The roadmap structures Member-State action into coordinated milestones. By the end of 2026, governments are expected to complete foundational tasks: establishing national coordination structures, conducting detailed cryptographic inventories, mapping dependencies, integrating quantum risk into executive risk management, engaging suppliers, and initiating pilot migrations for medium- and high-risk systems. By 2030, Member States should have implemented cryptographic agility, updated certification frameworks to incorporate post-quantum algorithms, strengthened secure update mechanisms, allocated long-term resources, and completed migration of high-risk systems—those with long confidentiality lifetimes or significant migration complexity. New long-lifecycle products entering the market before 2030 must already support PQ-ready upgrade paths.

*Relevance to NANCY*

NANCY aligns exceptionally well with the EU Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography because the project capabilities map directly onto the roadmap's requirements. KER3 provides the strongest evidence of this alignment, as it delivers multiple interoperable technological elements, namely ER2, ER3, and ER4, that collectively operationalize core principles of the EU roadmap. ER2 introduces a post-quantum signature token and Public-Key Cryptography Standards #11 (PKCS#11)–based driver, enabling hybrid (classic + PQC) digital signatures on smart cards, precisely the type of crypto-agile identity and Public Key Infrastructure (PKI) capability the roadmap calls for. ER3 extends quantum-safe protection into the emerging digital identity and blockchain ecosystem by integrating Self-Sovereign Identity, Verifiable Credentials, and PQC into a unified wallet, addressing critical concerns such as long-term credential integrity, quantum-resistant authentication, and cross-border interoperability. ER4 complements these elements by implementing PQC-protected communication in 5G massive IoT scenarios, which is an environment explicitly identified by the roadmap as high-risk due to longevity, scale, and complexity. Together, these exploitable results demonstrate how KER3 supports the initiative's objectives for cryptographic agility, secure identity infrastructures, and PQ-ready networked systems.

### 3.3.3.NIS2

The NIS2 Directive (Directive (EU) 2022/2555) is European Union legislation designed to establish a high common level of cybersecurity across the EU by enhancing the security and resilience of network and information systems [62]. It replaces the earlier NIS Directive and broadens both the scope of covered entities and the cybersecurity requirements they must meet, including risk-management measures and incident reporting obligations. NIS2 applies to a wide range of essential and important sectors, requiring organizations to implement robust cybersecurity practices, ensure continuous

protection against threats, and collaborate with national authorities to manage incidents and risks effectively.

Under NIS2, organizations are expected to strengthen their cyber risk management capabilities, increase operational resilience, and maintain consistent reporting and response processes in order to mitigate evolving cyber threats. Member States are also required to designate competent authorities and responsible national cybersecurity strategies to support the directive's implementation and to enhance cross-border cooperation and information exchange across the EU.

*Relevance to NANCY*

One of the core results of NANCY, articulated in KER11, is the development of a next-generation SDN-enabled MEC system that provides autonomous anomaly detection**,** self-healing, and self-recovery capabilities. These features are highly relevant to the goals and technical expectations of the NIS2 Directive.

First, anomaly detection is a foundational requirement for effective cybersecurity risk management under NIS2. The directive expects organizations to implement mechanisms that enable continuous monitoring of network and information systems to identify unusual behaviors, potential breaches, or system faults before they escalate into significant incidents. NANCY's architecture integrates real-time monitoring and pattern analysis at the edge of the network, enabling early detection of threats or operational anomalies without reliance on centralized systems. This real-time monitoring supports the continuous vigilance that NIS2 mandates for essential and important entities operating critical digital infrastructures. Second, NIS2 emphasizes the need for robust incident handling and recovery processes. Traditional cybersecurity frameworks often depend on manual intervention to address detected threats, which can lead to delays and increased exposure to damage. By contrast, NANCY's self-healing and self-recovery mechanisms are designed to autonomously respond to detected anomalies.

# 4. Techno-economic Analysis & Business Modelling

## 4.1. Commercial Exploitable Results

Table 3 lists the exploitable results that have been identified as commercial by their respective owners.

Table 3: Commercial Exploitable Results

| ER# | KER/OER# | Result Title | Owner |
|---|---|---|---|
| ER2 | KER3 | PQC Signature Solution | TDIS |
| ER3 | KER3 | Blockchain Wallet with SSI and PQC Capabilities | NEC |
| ER4 | KER3 | PQC Secure Communication | TEI |
| ER5 | KER4 | B-RAN Theoretical Framework | INNO |
| ER6 | KER5 | QKD Simulation Framework | INNO |
| ER7 | KER7 | A novel AI virtualiser for underutilized computational & communication resource exploitation | i2CAT |
| ER10 | KER9 | Semantic Communications Framework | INNO |
| ER11 | KER10 | An explainable AI framework | MINDS |
| ER13 | KER12 | Virtio-based cross-world transport layer | VOS |
| ER16 | OER2 | Machine learning models for decision-making | Bi2S |
| ER20 | OER6 | Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing | OTE |
| ER22 | OER8 | Smart Pricing Policies | 8BELLS |
| ER23 | OER9 | Big Data Platform for self-healing and self-recovery | TEI |
| ER24 | OER10 | A framework for data and concept drift detection in 6G networks | Bi2S |
| ER28 | OER14 | Central Management Domain | INTRA |

## 4.2. SWOT and Lean Canvas

### 4.2.1.ER2: PQC Signature Solution

*SWOT Analysis*

Table 4: SWOT Analysis for ER2

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Secure implementation of a PQC signature and a PQC key exchange on a secure microcontroller with limited volatile and non-volatile memory<br><br>•PKCS #11–based driver, enabling hybrid (classic + PQC) digital signatures on smart cards<br><br>•Crypto agility | Current implementation still requires too many resources and limits the deployment of PQC algorithms on some low-end secure microcontrollers |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| Security agencies like NIST, BSI or ANSSI request migration to quantum-safe algorithms. | Rapid evolution of PQC standards and implementations could require frequent updates. New potential PQC algorithms are still possible. |

*Lean Canvas*

Table 5: Lean Canvas for ER2

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Secure qualified signatures and secure key exchanges against the potential threats posed by both quantum and classical computers. | Integrate PQC algorithms in token | Secure implementation expertise to integrate PQC algorithms on a microcontroller with limited resources | •First implementation done on a real product (MultiApp V5.2 premium PQC EAL6+ common criteria certified)<br><br>•Patents for secure crypto implementation and crypto protocols | •Governments<br><br>•Telecom operators<br><br>•Critical infrastructures |
| **Key Metrics** | | **Channels** | | |

| | |
|---|---|
| •Security level of the PQC algorithms<br><br>•Performance for signature generation, signature verification, and key exchange.<br><br>•Resources necessary for the implementation<br><br>•Number of keys supported by the token | •Technical whitepapers.<br><br>•Participate in EU projects, standardization efforts, and technical working groups to demonstrate the capability<br><br>•Introduction of PQC algorithms and PQC crypto protocol into the different applicable standards (ICAO, ISO, Global Platform) |
| **Cost Structure** | **Revenue Streams** |
| •Distribution costs<br><br>•People<br><br>•Marketing<br><br>•R&D costs<br><br>•Engineering and Production costs<br><br>•Security certifications | •Sales<br><br>•Licenses on patents |

### 4.2.2.ER3: Blockchain wallet with SSI and PQC capabilities

*SWOT Analysis*

Table 6: SWOT Analysis for ER3

| **Internal Factors** | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Combines Self-Sovereign Identity and Post-Quantum Cryptography in a single wallet, beyond the current state of the art<br><br>•Strong privacy, user control, and future-proof security aligned with 5G requirements<br><br>•Designed for permissioned blockchains, matching private-sector and enterprise needs<br><br>•High relevance for regulated environments (telecom, critical infrastructure) | •SSI and PQC technologies are still maturing, with limited real-world deployments<br><br>•Potential integration complexity with existing 5G and enterprise systems<br><br>•Performance and usability trade-offs due to PQC computational overhead<br><br>•Requires stakeholder education and trust in emerging standards |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •Growing demand for privacy-preserving identity and quantum-resistant security in 5G and beyond<br><br>•Early positioning for future regulatory and standardisation requirements | •Rapid evolution of standards may require frequent redesign or re-certification<br><br>•Large technology vendors could integrate SSI or PQC features into existing platforms<br><br>•Uncertainty around which PQC algorithms will become dominant |

| | |
|---|---|
| •Adoption by telecom operators, system integrators, and enterprise blockchain consortia<br><br>•Potential influence on emerging SSI, PQC, and 5G security standards | •Resistance to change from established centralized identity and security solutions |

*Lean Canvas*

Table 7: Lean Canvas for ER3

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| 1) Centralised Identity: Centralised identity providers (like Google, Facebook, banks) control user identities, often leading to privacy loss, data breaches, and a lack of user control. A blockchain wallet with SSI lets users authenticate, sign transactions, or access services without revealing more information than needed (zero-knowledge).<br><br>2) Quantum Threats: Current cryptographic algorithms (RSA, ECDSA) used in blockchain wallets and identity schemes are vulnerable to quantum computers, which could break them in the next decade. NEC's wallet combines next-gen crypto with identity—preventing attackers from forging identity credentials or stealing funds using quantum capabilities.<br><br>3) Fragmentation: users need multiple apps for identity (e.g., ID wallets) and assets (e.g., crypto wallets).<br><br>4) Legacy solutions lack portability and privacy across countries and sectors. NEC's wallet supports W3C Verifiable Credentials and Decentralised Identifiers for interoperability, while PQC | 1) A secure blockchain wallet integrating Self-Sovereign Identity (SSI) to enable user-controlled, privacy-preserving authentication for 5G services<br><br>2) PQC–based key management and transactions to ensure long-term security against quantum threats<br><br>3) Seamless operation within permissioned blockchain environments, supporting trusted enterprise and telecom use cases<br><br>4) Modular and interoperable architecture allowing integration with existing 5G provisioning, access control, and enterprise systems | PQC will shortly become one of the main cryptography standards. While quantum secure wallets and SSI wallets have seen progress, a unified, production-grade wallet combining both SSI and PQC is still emerging. So far, a fully integrated PQC-able and SSI-able blockchain wallet solution does not exist. | 1) Early integration of SSI and Post-Quantum Cryptography in a single wallet, backed by specialized expertise across identity, cryptography, and 5G systems<br><br>2) Proprietary architecture optimized for permissioned blockchains and 5G service provisioning, developed through hands-on experimentation rather than off-the-shelf components<br><br>3) First-mover advantage and know-how in adapting PQC algorithms to constrained, real-time 5G workflows | 1) Telecom operators and 5G service providers deploying secure, privacy-preserving service provisioning platforms<br><br>2) Enterprise and private-sector organizations using permissioned blockchains for identity, access, and service management<br><br>3) System integrators and technology providers building end-to-end 5G and blockchain-based solutions |

| | | | | |
|---|---|---|---|---|
| ensures long-term compliance with evolving standards (e.g., NIST). | | | | |

| Key Metrics | Channels |
|---|---|
| •Adoption & Usage: Number of active wallets, onboarded enterprises, and integrated 5G services<br><br>•Security & Privacy: Successful SSI credential verifications, zero identity breaches, and compliance with PQC security benchmarks<br><br>•Performance: Authentication latency and transaction throughput within 5G provisioning workflows<br><br>•Business Impact: Reduction in onboarding time, operational costs, or identity-management overhead for enterprise customers | •Direct B2B sales to telecom operators, enterprises, and private blockchain consortia<br><br>•Partnerships with system integrators and 5G vendors to embed the wallet into existing provisioning platforms<br><br>•Industry pilots, testbeds, and proof-of-concept deployments in telecom and enterprise environments<br><br>•Standards bodies, industry forums, and technical conferences to gain visibility and credibility among early adopters |

| Cost Structure | Revenue Streams |
|---|---|
| •Research and development costs for SSI integration, PQC implementation, and wallet security hardening<br><br>•Engineering and integration costs related to interoperability with permissioned blockchains and 5G systems<br><br>•Infrastructure and operations costs for testing environments, pilot deployments, and maintenance<br><br>•Compliance, standardisation, and certification costs associated with telecom, security, and cryptographic requirements | •Software licensing fees for enterprise and telecom deployments of the wallet<br><br>•Subscription or usage-based fees for managed wallet services, updates, and security maintenance<br><br>•Integration and customization services for adapting the solution to specific 5G or blockchain environments<br><br>•Consulting and support contracts related to SSI, PQC adoption, and compliance in enterprise systems |

### 4.2.3.ER4: PQC secure communication

*SWOT Analysis*

Table 8: SWOT Analysis for ER4

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Flexible integration across multiple communication scenarios, including 5G networks and other mobile/IoT deployments.<br><br>•Uses standards-based protocols (e.g., Transport Layer Security (TLS)), easing interoperability and adoption.<br><br>•Supports optional hardware-based signing via PKCS#11-compatible tokens, enabling higher- | •Hardware-token signing introduces higher latency and lower throughput compared with optimized software implementations, which can impact high-frequency signing use cases.<br><br>•Computational and memory demands of some PQC algorithms can limit feasibility on constrained devices (e.g., low-power IoT endpoints).<br><br>•Early-stage PQC implementations and interoperability gaps across algorithm sets and |

| | |
|---|---|
| assurance key protection and non-extractable private keys.<br><br>•Solution oriented toward both quantum and classical-threat resistance, improving long-term security posture. | libraries may increase development and testing effort. |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •Growth of 5G/B5G/6G ecosystems and massive IoT deployments increases demand for advanced cryptographic solutions.<br><br>•Regulatory and standardization momentum (NIST selections, EU guidance, critical-infrastructure requirements) is likely to accelerate PQC adoption in industry and government.<br><br>•Market demand for post-quantum assurance creates commercial differentiation for products and services that integrate PQC signing tokens and hybrid schemes.<br><br>•Ability to offer hybrid PQC/classical modes during migration can enable phased adoption and compatibility with legacy systems. | •Integration complexity at scale (key management, certificate lifecycles, hybrid-mode compatibility) may impact large-scale rollouts.<br><br>•Budget and operational constraints in target sectors may delay upgrades of legacy devices and infrastructure.<br><br>•Rapid evolution of PQC standards and implementations could require frequent updates, increasing maintenance costs. |

*Lean Canvas*

Table 9: Lean Canvas for ER4

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Secure communication against the potential threat posed by both quantum and classical computers, particularly for 5G deployments. | Integrate PQC into 5G scenarios using PQC-capable digital signature tokens and standards-based protocols with support for hybrid PQC/classical modes. | Improve communication protection by delivering a practical, standards-aligned PQC integration path that combines software and optional hardware token support to provide forward-looking cryptographic resistance. | •End-to-end PQC prototyping and benchmarking experience across 5G scenarios and IoT devices.<br><br>•PKCS#11 compatible hardware token integration for non-extractable private keys — combining PQC algorithm support with | •Telecom operators seeking future-proofed cryptography.<br><br>•IoT device manufacturers (massive IoT, industrial IoT).<br><br>•Critical infrastructure operators (energy, transportation, healthcare) with long-lived assets requiring quantum-resistant protection. |

| | | | | |
|---|---|---|---|---|
| | | | Hardware Security Module (HSM) ecosystems. | |

| Key Metrics | Channels |
|---|---|
| •Cryptographic operation latency: signature generation/verification and key-establishment times.<br><br>•Throughput and transactions/sec for signing and key exchange under realistic loads.<br><br>•Memory and CPU utilization on representative device classes. | •Pilot projects with telecom operators, IoT vendors, and critical-infrastructure providers (proofs-of-concept in live 5G testbeds).<br><br>•Technical whitepapers, benchmarks, and implementation guides targeting engineers and security architects.<br><br>•Strategic partnerships with HSM/token vendors, and system integrators to embed PQC options into product stacks.<br><br>•Developer Software Development Kits (SDK), reference implementations, and open-source examples to lower integration friction. |
| **Cost Structure** | **Revenue Streams** |
| •Distribution costs<br>•People<br>•Marketing<br>•R&D costs<br>•Engineering and Production costs<br>•Permits, authorisations, etc. | •Sales<br>•Services (consultancy / training / etc.)<br>•Maintenance |

### 4.2.4.ER5: B-RAN Theoretical Framework

*SWOT Analysis*

Table 10: SWOT Analysis for ER5

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •A solid theoretical basis, which combines queueing theory, Markov chains, AI, ML, and enables precise, explainable performance models<br><br>•Flexible framework to adapt to different B-RAN architectures, traffic profiles, and deployment scenarios (edge/cloud, private/public)<br><br>•High-impact on cost reduction, by allowing for optimized dimensioning and configuration of B-RAN networks before they go live | •Currently a theoretical and simulation framework; no ready-to-use commercial product exists<br><br>•Requires high-level technical knowledge (network engineering, stochastic modeling, AI/ML) to understand and use the results of the framework<br><br>•Validated in large-scale real-world deployments of TRL 7-8 has been limited so far and would require additional pilots |

| | |
|---|---|
| | •Additional interfaces and custom effort may be necessary to connect with the existing operators' planning and orchestration tools |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •There is growing interest in private B-RAN deployments (e.g., Industry 4.0, campus, smart cities) requiring reliable performance planning and cost optimization<br><br>•Operators require tools to de-risk CAPEX/OPEX during 5G/6G and B-RAN rollouts, especially in energy- and cost-restricted environments<br><br>•Increased regulatory and business pressure for efficient use of spectrum and infrastructure will likely support the adoption of accurate planning tools<br><br>•It may also be possible to expand the framework to include support for emerging technologies (e.g., network slicing, edge computing, blockchain-based resource management) and offer it as a premium planning service | •Existing network planning/dimensioning tools from established vendors are already embedded into many operators' toolchains<br><br>•The rapid evolution of B-RAN standards and architectures will likely require frequent updates to maintain alignment with the latest developments<br><br>•Conservative stakeholders may resist adopting new modeling frameworks unless there is significant field validation<br><br>•Low-cost open-source or free planning tools may partially commoditize basic planning capabilities, making operators less willing to pay for advanced models |

*Lean Canvas*

Table 11: Lean Canvas for ER5

| **Lean Canvas** | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Reduces development and deployment costs. | Accurately model and estimate the achievable performance of B-RAN. | •Enable end-users to evaluate and design B-RAN prior to deployment, providing confidence in designing and optimizing B-RAN deployments with realistic, model-based performance estimates.<br><br>•Provide cost-effective means to reduce development and deployment costs while maintaining or improving service quality. | •INNO generated project-specific expertise in realistic blockchain and attack models and their interaction with B-RAN scenarios.<br><br>•Combination of rigorous stochastic modeling and AI/ML-based methods within a coherent framework.<br><br>•Access to project-specific data sets, scenarios, and knowledge not easily accessible to competitors. | •Mobile network operators and neutral-host providers that deploy private or public B-RAN networks.<br><br>•Large enterprise and government entities that plan to implement private B-RAN networks (factories, campuses, ports, municipalities).<br><br>•Vendors and system integrators developing B-RAN solutions that require advanced planning |

| | | | | |
|---|---|---|---|---|
| | | •Allow for customization of the framework to fit specific needs and constraints of each customer's environment. | •Potential for inclusion with other INNO results (e.g., security, semantic communications) to provide a broader, multi-faceted planning solution. | and performance modeling.<br><br>•Research institutions and innovation laboratories that develop new B-RAN architectures and algorithms. |

| Key Metrics | Channels |
|---|---|
| •Precision of performance prediction versus actual KPIs (e.g., throughput, latency, blocking/queueing probabilities).<br><br>•Reduction in development and deployment costs (CAPEX/OPEX savings) when compared to baseline planning approaches.<br><br>•Time to decision for network design (how quickly a satisfactory configuration can be found).<br><br>•Number of deployment scenarios evaluated per unit of time (scalability of the framework).<br><br>•Increase in QoS/ Quality of Experience (QoE) indicators post-use of the framework to optimize prior to deployment. | •Collaborate directly with telecom operators, vendors, and system integrators through pilot projects and consulting.<br><br>•Participate in EU projects, standardization efforts, and technical working groups to demonstrate the capability.<br><br>•Publish scientific articles, whitepapers, and perform demonstrations in academic and industry conferences/workshops.<br><br>•Disseminate targeted information via the project website, webinars, and professional networks (industry associations, clusters). |

| Cost Structure | Revenue Streams |
|---|---|
| •Personnel (experts in modeling, AI/ML, network engineering, and software development).<br><br>•R&D Costs (model development, validation, and ongoing enhancement).<br><br>•Engineering and Production Costs (tool implementation, integration, and packaging).<br><br>•Marketing (customer acquisition costs) for dissemination, demonstrations, and participation in events.<br><br>•Licenses, permits, etc., if required for pilots or field trials (e.g., spectrum trials, test site). | •Services (consulting/training/etc.): customized performance assessments, design services, and training for operators and organizations.<br><br>•Sales: licensing of the framework as a software tool or module to operators, vendors, and integrators.<br><br>•Maintenance: contracts for ongoing support and updates to ensure the models align with evolving B-RAN technology and deployments. |

### 4.2.5.ER6: QKD Simulation Framework

*SWOT Analysis*

Table 12: SWOT Analysis for ER6

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Expertise in both quantum communications and performance modeling exists in-house<br><br>•The simulation has a high degree of fidelity when compared to experimental QKD testbeds that it is directly modeled after<br><br>•The model can simulate a variety of different QKD protocols, physical channels and network architectures<br><br>•It allows for "what if" analysis to occur in the early stages of development, thereby saving on the use of expensive hardware<br><br>•The modular, software-based architecture allows the model to be integrated into other network planning tools | •The configuration and interpretation of results requires specialized knowledge of QKD and numerical simulation<br><br>•The validity of the model relies upon the availability of experimental data from partners; this could limit the scope of certain scenarios<br><br>•Currently, it does not include the full-stack integration of key-management systems or cryptographic systems<br><br>•The model's user interface/visualization capabilities are limited (primarily a research-oriented tool); further work is required in order to develop a more user-friendly version<br><br>•Optimization of the model's scalability to large-scale quantum network topologies is also underway |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •There is growing interest among telecommunications operators, cloud providers, and government organizations regarding QKD and quantum-safe communications<br><br>•EU-level and national programs are providing funding for quantum infrastructure pilot programs and testbeds<br><br>•A need exists for techno-economic studies prior to deploying costly quantum hardware<br><br>•The model has the potential to serve as a reference tool for standardization bodies and industry consortia, creating QKD performance benchmarks<br><br>•The model can potentially be extended to create quantum-safe/cryptographically agile network planning tools | •Simulations created by large equipment vendors/operators as a part of their in-house efforts<br><br>•Changes in QKD technologies and protocols will likely result in a continued effort to maintain the model at the cutting edge of these changes<br><br>•Uncertainty exists related to regulatory issues associated with large-scale deployments of QKD infrastructures and the migration timelines for cryptographic systems<br><br>•Budgetary constraints may cause delays or cancellations of QKD deployments, resulting in a smaller-than-expected near-term market size<br><br>•Some organizations may prefer to use black-box commercial simulation tools rather than a research-driven, open-source framework |

*Lean Canvas*

Table 13: Lean Canvas for ER6

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Achieve close to real-life performance.<br>Plan and/or estimate the performance of QKD communications without the need for expensive QKD equipment. | Simulates the performance of QKD communications without the need for equipment. | Plan and/or estimate the performance of QKD communications. | •Direct access to experimental QKD setups/measurement data within the project (allows for accurate calibration/ validation).<br><br>•Combination of expertise in quantum communications/ network modeling/algorithms within a single group/team.<br><br>•A neutral research-driven tool that is not bound to a single vendor, allowing for comparisons of various QKD solutions.<br><br>•Re-use of existing modeling assets/knowledge base from previous INNO frameworks (performance/cost modeling). | •Telecommunications operators/network service providers designing/maintaining QKD-enabled backhaul/metro networks.<br><br>•Government agencies/public institutions responsible for critical infrastructure assessing quantum-safe communication options.<br><br>•Vendors/system integrators of QKD equipment utilizing an independent tool for the assessment of QKD performance.<br><br>•Universities/research organizations involved in quantum communications/quantum networks.<br><br>•Consulting firms conducting techno-economic analyses for secure communication infrastructures. |
| **Key Metrics** | | | **Channels** | |
| •Quantum bit error rate (QBER)/secret key rate as a function of distance/topology/system parameters.<br><br>•The types of QKD protocols/channels/ hardware configurations that are supported by the model.<br><br>•Gap between the simulated results and experimental measurements (i.e., a measure of accuracy; e.g., a percentage of difference).<br><br>•Speed/scaling of the simulation as it relates to number of nodes/links.<br><br>•The number of pilot studies/industrial trials/projects that utilize the model. | | | •Pilot projects/joint activities with project partners (vendors/operators/public entities) where the model is utilized to design QKD trials.<br><br>•Peer-reviewed scientific publications/conference demos/open workshops focused on the quantum communications community.<br><br>•Direct outreach to telecommunications operators/integrators/equipment vendors via individual meetings/NDA's.<br><br>•Contributions to standardization/working groups where the model can be used to develop reference scenarios.<br>•On-line presence via project website/whitepapers/technical documentation. | |

| | |
|---|---|
| •User satisfaction/reuse of the model during later design iterations. | |
| **Cost Structure** | **Revenue Streams** |
| •Personnel (researchers/software engineers/domain experts who maintain/extend the framework).<br><br>•R&D costs (development/design/ validation/integration).<br><br>•Manufacturing/engineering/ production (prototyping/ packaging/documentation/testing)<br><br>•Marketing (events/demonstrators /dissemination materials). | •Service (consulting/performance study/customized scenario evaluation for operators/government entities).<br><br>•Maintenance/support contract fees for organizations utilizing the framework for extended periods of time.<br><br>•Enhanced/customized versions (e.g., with specific modules/GUIs/integrations) of the framework sold under license.<br><br>•Dual-license strategy (open-source research version/basic features/commercial license version with advanced features/add-ons). |

### 4.2.6. ER7: A novel AI virtualiser for underutilized computational & communication resource exploitation

*SWOT Analysis*

Table 14: SWOT Analysis for ER7

| **Internal Factors** | |
|---|---|
| Strengths (+) | Weaknesses (-) |
| •The AI virtualiser addresses technical limitations of current orchestration systems, including siloed control, inefficient resource sharing, substantial telemetry requirements, and a lack of emergent communication capabilities<br><br>•The originality of the AI virtualiser lies in combining emergent communication, latent-space representation learning, and flexible observation/action models, with direct enforcement through an orchestration API. This transforms orchestration into a collaborative, adaptive, and semantic process, going beyond traditional rule-based or analytics-driven automation<br><br>•The AI Virtualiser demonstrated superior performance to a MADRL baseline in terms of number of conflicts (x6 improvement), latency (x3.5 improvement) and resource underutilization (x1.4 improvement) | •An instance of the AI virtualiser solves one unique automation/orchestration problem; the application of the technology to complex automation/orchestration problems involving several network domains requires a more complex deployment<br><br>•The dynamicity and granularity of the reallocation of resources achievable by the AI virtualiser are limited by the capabilities of the underlying infrastructure. This is especially relevant for advanced GPU resource scheduling, which is not currently supported by all GPU vendors |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |

| | |
|---|---|
| •Industry-wide trend towards autonomous networks at level 4 and beyond as defined by the TMForum. Increasingly high telco network operational costs are accelerating this trend<br><br>•Agentic AI was recently recognized in an industry whitepaper from TMForum and global telcos as one of the most promising enablers for network automation level 4 and beyond | •Potential lack of trust in connectivity providers in conversational AI technologies due to low technological maturity<br><br>•Lack of trust in AI at the wider society level may have future implications in terms of restrictive regulations around the use of AI technologies<br><br>•The development of new telco standards and specifications may limit the applicability of the AI Virtualiser to commercial networks |

*Lean Canvas*

Table 15: Lean Canvas for ER7

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Inter-slice resource conflict and underutilization. | Develop a multi-agent communication protocol, learning to establish collaboration between concurrent slices. | Efficient use of resources to maximise the return from leasing the infrastructure to multiple tenants whilst reducing operational costs. | The unfair advantage of the AI Virtualiser stems mainly from the requirement for specialized multi-disciplinary knowledge at the convergence of telecommunication technologies and novel AI techniques such as agentic AI. | Three potential customer segments have been identified: telcos, system integrators, and orchestration/automation solution providers. |
| **Key Metrics** | | | **Channels** | |
| Compared to a MADRL baseline, the AI Virtualiser achieves a x6 improvement in number of conflicts; a x3.5 improvement in latency; and a x1.4 improvement in resource underutilization. | | | Initially, a demonstration video of the technology will be prepared and used as a tool to engage with potential adopters. Regional and national potential adopters will be identified and contacted through i2CAT's technology transfer and business development teams, with the purpose of establishing a collaboration for the demonstration of the use of the AI Virtualiser in a specific use case relevant to each potential adopter. | |
| **Cost Structure** | | | **Revenue Streams** | |
| The monetization strategy of the AI Virtualiser targets the transfer or licensing of the tool to third parties. Thus, the main costs are associated with R&D and engineering refactoring, and time spent by the market transfer and business development teams on customer engagement. | | | The main revenue stream is sales, related to technology transferring or licensing, and potentially to consultancy and training, to support adopters with the integration of the AI Virtualiser with their existing technologies. | |

### 4.2.7.ER10: Semantic Communications Framework

*SWOT Analysis*

Table 16: SWOT Analysis for ER10

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Combines conventional techniques and AI to support the Semantic Communications that can outperform those using the Shannon approach<br><br>•Directly supports the urgent industry needs to make Networks Sustainable<br><br>•Has the potential to be used in numerous different network situations and by different stakeholders<br><br>•Pushes the current SoTA of networks towards making them sustainable through intelligent data reduction<br><br>•Can be applied to all of the stakeholders in the Industry and Public Sector | •Limited validation in real-world environments<br><br>•Requires specialized knowledge of AI/ML and semantic communications<br><br>•The implementation of the framework could impose changes to existing network systems |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •There is increasing demand from both regulatory bodies and corporations for energy-efficient communications<br><br>• Next-generation networks are looking at ways to improve their efficiency<br><br>•More companies are starting to look into optimizing the way they design their networks using AI/ML<br><br>•The framework can be applied to many different markets (Telecommunications, Data Centers, IoT, Edge Computing)<br><br>•There is the opportunity to develop new standards in semantic communications<br><br>• As there is interest in the framework from large network operators, there are opportunities for creating new licensing models and partnering with these companies | •There are already many solutions available for reducing the amount of energy being consumed by networks (Compression, Optimization Techniques)<br><br>•Rapid technological advancements in the network space mean the framework will have to adapt quickly<br><br>•New standards and regulations for networks can slow down the rate at which the framework is adopted<br><br>•Legacy systems and incumbent technologies can be resistant to adopting new frameworks<br><br>•Other research groups are working on similar ideas in semantic communications, and there is the risk that one or more of these research groups may obtain patents that would create barriers to entry to the market |

*Lean Canvas*

Table 17: Lean Canvas for ER10

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Increase energy and data efficiency, and pushes the current SoTA of the networks towards sustainability. | Intelligently reduce the amount of data transferred in the network. | Increase energy and data efficiency. | • Custom-trained models of semantic comprehension and knowledge of the network domain<br><br>•Hybrid method of AI and traditional techniques, which cannot easily be duplicated by competitors.<br><br>•Built upon INNO's exclusive research in semantic communications and goal-oriented communications.<br><br>•First to market with a working semantic communications framework.<br><br>•Complete end-to-end solution; not just optimizing one component of the network. | •Large telecommunications operators<br><br>•Mobile network operators<br><br>•Providers of cloud and datacenter services<br><br>•Providers of internet backbones<br><br>•Satellite communications operators<br><br>•IoT and Edge Computing Platforms<br><br>•Enterprise networks needing high levels of efficiency |
| **Key Metrics** | | | **Channels** | |
| •Energy savings: percentage of network energy used reduced<br><br>•Data efficiency: amount of data (bytes) transferred to convey a given unit of information<br><br>•Latency impact: how much time it takes to send the data<br><br>•Semantic accuracy: preservation of information that has meaning relative to the overall data that is being reduced<br><br>•Scalability: will this framework work across different sized networks? | | | •Partnerships with major telecommunications companies and network equipment suppliers<br><br>•Publications and conference presentations in leading technical conferences<br><br>•Collaboration with organizations that develop standards for technology<br>Pilot programs with early adopting industry partners<br><br>•License agreements with system integrators and telecom equipment suppliers<br><br>•Release of some of the modules developed for the project as open source software in order to encourage the creation of an ecosystem and to help promote the adoption of the new framework<br>•Expert consulting for customers who need to implement and optimize their own use of the framework | |

| | |
|---|---|
| •Throughput: how fast (in bits/sec) can you move the semantic content through the network?<br><br>•Compatibility index: will this work with the other network protocols? | |

| Cost Structure | Revenue Streams |
|---|---|
| •Costs associated with developing the framework, training AI models, and optimizing the algorithms<br><br>•Costs associated with implementing software into the network, integrating systems, and establishing test environments<br><br>•Hiring AI/ML engineers, network scientists, and systems architects<br><br>•Costs of distributing the software, creating and maintaining the infrastructure needed to deploy the software<br><br>•Presence at industry conferences, providing technical documentation, and developing proof-of-concept demonstrations<br><br>•Obtaining authorization for frequency spectrum use, and reviewing regulatory compliance | •Licensing the software to network operators and equipment manufacturers<br><br>•Providing consulting services, custom implementations, and performance optimizations<br><br>•Ongoing maintenance and support, including retraining models and updating algorithms<br><br>•Providing commercial services related to open source components<br><br>•Licensing IP for integrated network solutions<br><br>•Certification and training programs for personnel of network operators |

### 4.2.8.ER11: An explainable AI framework

*SWOT Analysis*

Table 18: SWOT Analysis for ER11

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| • Modular and scalable architecture with three specialized Explainable AI (XAI) components (Anomaly Detection, Outage Prediction, Semantic Communications)<br><br>•Integration of Large Language Model (LLM)-powered natural language explanations making technical outputs accessible to non-experts<br><br>•Real-world validation<br><br>•Integration capabilities and options | •Computational complexity may limit real-time explainability in resource-constrained environments<br><br>•Currently focused on specific use cases (network management, cybersecurity), limiting immediate generalization |
| **External Factors** | |

| Opportunities (+) | Threats (-) |
|---|---|
| •Growing regulatory pressure (EU AI Act, GDPR) mandating explainable AI in critical infrastructure<br><br>•Expanding B5G/6G market requiring trustworthy AI for network management<br><br>•Increasing demand for transparent cybersecurity solutions across industries | •Established competitors with mature XAI platforms (IBM, Google, etc.)<br><br>•Rapid technological evolution requiring continuous updates and maintenance<br><br>•Market skepticism toward "black box" AI may slow adoption despite explainability features<br><br>•Budget constraints in target industries limiting investment in explainability solutions |

*Lean Canvas*

Table 19: Lean Canvas for ER11

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| The low clarity and understandability of AI-enabled components' decisions pose significant challenges in various domains. When AI systems make decisions, especially in complex tasks or critical contexts, the lack of clarity can impede trust, comprehension, and accountability. This opacity may stem from the intricate inner workings of deep learning models, the black-box nature of certain algorithms, or the absence of transparent decision-making processes. The integration of plain language is essential for decision-making using explainability reports. | The aforementioned problem can be addressed by providing easy-to-understand visualisation of the main findings and insights of the XAI algorithms in order for non-expert personnel to be able to benefit from them, integrating plain language explanations. | Increase energy and data efficiency. | •EU Horizon-funded consortium bringing together leading research institutions and SMEs<br><br>•Integration with federated learning, preserving privacy while enabling explainability<br><br>• Domain-specific fine-tuning (cybersecurity-focused LLM) unavailable in generic XAI tools<br><br>•Real-world validation through NANCY project testbeds and use cases<br><br>•Specialized expertise in B5G/6G network management and security | •Primary: Network operators and telecom service providers managing B5G/6G infrastructure<br><br>•Secondary: Cybersecurity teams requiring explainable intrusion detection |
| **Key Metrics** | | | **Channels** | |
| •Explanation accuracy: Correlation between XAI outputs and expert assessments<br><br>•Response time: Latency for generating explanations in real-time scenarios | | | •Academic conferences and publications<br><br>•EU project consortium networks and dissemination events<br><br>•Industry workshops and webinars targeting network operators | |

| | |
|---|---|
| •Model performance: Classification accuracy maintained while providing explainability<br><br>•User satisfaction scores: Feedback ratings from dashboard users | •Direct engagement with telecom operators through pilot programs<br><br>•Professional social networks (LinkedIn etc.) |
| **Cost Structure** | **Revenue Streams** |
| •Distribution costs<br><br>•People<br><br>•Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs<br><br>•Permits, authorisations, etc. | •Open-source<br><br>•Sales<br><br>•Services (consultancy / training / etc.)<br><br>•Maintenance |

### 4.2.9.ER13: Virtio-based cross-world transport layer

*SWOT Analysis*

Table 20: SWOT Analysis for ER13

| **Internal Factors** | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| The virtio-based cross-world transport layer is an innovative solution that simplifies the implementation of a fast data plane in constrained environments, allowing the system integrator to re-use existing virtio-based devices. | This solution targets a specific system architecture and applies only to recent ARM-based architectures. |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| The increasing complexity of heterogeneous architectures and edge computing use cases increases the demand for innovative solutions like the proposed one. | Very often, major players monopolize the market because they appear to customers as more reliable suppliers with a claimed superior ability to handle liabilities. |

*Lean Canvas*

Table 21: Lean Canvas for ER13

| **Lean Canvas** | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Nowadays, there are not so many options when it comes to realizing a software stack where multiple operating systems are co-executing on the same platform, most of the time with addressing tasks of diverse criticalities. In these cases, the company, usually the system integrator, is forced to | VOS will provide development services to tailor its technologies around the specific needs of the customer, with the final objective of | This result enables the implementation of powerful software stacks for ARM systems featuring the TrustZone | Competitors usually do not reach the level of simple bottom-up integration and efficiency allowed by the | System integrators and software architects dealing with heterogeneous and integrated platforms. |

| | | | | |
|---|---|---|---|---|
| look at very expensive virtualisation solutions that come already with a variety of black-box software and tools that are effectively locking-in the system integrator. For this reason, the software stack will be designed around the purchased virtualisation solution, instead of being tailored specifically to one use case. Instead, the virtio-based technology based on the Virtual Open System (VOS) VOSySmonitor offers a more open and flexible alternative, made even more appealing by a customer needs based business model. | providing what the customer needs instead of an all-and-too-much-inclusive, black-box, solution. | extension that can rely on different operating systems to address tasks of diverse criticalities, while sharing a set of resources in an efficient way. | proposed solution. | |

| Key Metrics | Channels |
|---|---|
| The majority of the time, bandwidth and latency are the primary metrics used for evaluating network interface performance in Linux and, in general, of data planes. However, there are numerous other metrics that can provide valuable insights into the system performance. In this case, other less objective metrics should be considered, like the impact of the chosen solution on the existing software stack that must be adapted to embrace the new technology. | VOS has been disseminating this technology through its website, posters, and papers. Thanks to these channels and their established customer base, VOS is expecting to engage some potential customers. |

| Cost Structure | Revenue Streams |
|---|---|
| •Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs | •Services (consultancy / training / etc.)<br><br>•Maintenance |

### 4.2.10. ER16: Machine learning models for decision-making

*SWOT Analysis*

Table 22: SWOT Analysis for ER16

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •State-of-the-art performance and decision-making<br><br>•Applicability to very large telecommunication networks<br><br>•High-levels of automation<br><br>•The solution redistributes computational load and reduces energy consumption. | •Requires tuning to the network under consideration (e.g. fine-tuning or re-training)<br><br>•Requires prior information to function efficiently (e.g. average execution time of an application) |

| | |
|---|---|
| •Transferable to IoT, 4G, B5G | |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •EU's Green Deal will accelerate the adoption rate of solutions that lower the computational load of a network and result in reduced energy consumption<br><br>•6G and beyond networks, that will emerge in the future, will require similar products, especially in the Cloud-Edge continuum<br><br>•New standardization practices for future (and contemporary) protocols will turn towards energy-efficient computing | •Legislature that constrains the use of AI may hinder the adoption rate of similar services<br><br>•The market is currently dominated by few "big" players<br><br>•Consolidation levels of the market continue to rise |

*Lean Canvas*

Table 23: Lean Canvas for ER16

| **Lean Canvas** | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Telecommunication service providers: NANCY's "Machine learning models for decision-making" solve the issues of computational offloading in Edge ecosystems. The main problem is the optimal use of Edge computational resources that maximise the QoS and reduce the computational complexity for each end user.<br>Telecommunication Infrastructure providers: The main problem that NANCY's "Machine learning models for decision-making" solve is the reduction of computational resources required for AI model training and inference operations." | The proposed "Machine learning models for decision-making" adopts novel approaches to optimise the computational resource utilisation of the Edge with respect to the QoS of the network. To achieve this, NANCY employs an AI approach that makes on-the-fly decisions on what type of services to offload to the Edge of the network. This decision-making process is conducted while considering several network parameters. A novel reinforcement learning framework guarantees the minimisation of computational requirements of the models, during the AI training and inference processes. | Increased QoS within the network, increased computational distribution between Cloud and Edge, Real-time adaptation, computational offloading provisioning under diverse operating scenarios. | •The core Reinforcement learning mechanism is hard to replicate since it was created by experts within the consortium, using state-of-the-art methods.<br><br>•The capability of efficient scaling (with the number of network nodes) is also hard to replicate. | •Telecommunication operators<br><br>•Infrastructure provideps (E.g. Cloud providers)<br><br>•Network operators<br><br>•Consultancies |

| Key Metrics | Channels |
|---|---|
| From the conducted experiments, the following KPIs illustrate the performance of our solution:<br><br>•Average energy consumption reduction in "low and medium loads": ≥ 20% reduction<br><br>•Average energy consumption reduction in "high loads": ≥ 30% reduction<br><br>•Edge resource utilization (due to task re-distribution): ≥ 85% on average reduction<br><br>•Estimated cost reduction for infrastructure operators: ≥ 15%<br><br>•Increased overall QoS: ≥ 25% | •Social media and web campaigns<br><br>•Presentations and demonstrations at events and exhibitions<br><br>•Later, direct sales through partnerships |
| **Cost Structure** | **Revenue Streams** |
| •Distribution costs<br><br>•Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs | •Sales<br><br>•Services (consultancy / training / etc.) |

### 4.2.11. ER20: Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing

*SWOT Analysis*

Table 24: SWOT Analysis for ER20

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Blockchain provides enhanced transparency and trust without performance degradation<br><br>•User experience with advanced security and privacy<br><br>•Improved resource allocation through AI/ML models real time prediction | •Computational overhead of Blockchain that may affect network latency and cause service degradation<br><br>•Complexity in Blockchain integration with 5G network components<br><br>•Implementation Costs |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |

| | |
|---|---|
| •AI/ML assisted blockchain could support efficient real-time decision making<br><br>•Early adoption of the technologies could lead to market advantage against competitors | •Increased cost of investment<br><br>•Regulatory constraints<br><br>•Possible interoperability issues |

*Lean Canvas*

Table 25: Lean Canvas for ER20

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| By leveraging blockchain, network decentralisation is enhanced in parallel with trust and security. Moreover, AI/ML algorithms enable intelligent, real-time orchestration optimising resource allocation and improving energy efficiency. | Enhancing security and trust, protecting data and resources. | OTE aims to exploit the outcomes of the NANCY project by integrating blockchain powered by AI/ML algorithms into 5G and edge computing environments, with a focus on evaluating their efficiency and testing overall network performance. | System-level integration of AI/ML models with blockchain-based trust mechanisms specifically optimized for 5G and Edge Computing environments. | •Regulatory Bodies:<br><br>Regulatory bodies establish and enforce data protection laws such as GDPR, ensuring that data privacy solutions comply with EU legislation and protect individuals' rights. Regulatory bodies benefit from technologies aiming to offer an extra layer of data protection as they enable operators to meet compliance requirements more effectively.<br><br>•End-Users: individuals or corporate/business clients, especially those dealing with sensitive data such as health data, could benefit from enhanced data privacy and security, as they experience an extra level of authentication while utilizing personalized and on-demand services. |
| **Key Metrics** | | | **Channels** | |
| The trust gained and the advanced protection of end users can only be evaluated through KVIs, which are not quantifiable, but they have a direct impact on the user experience and the brand name of an organization. | | | OTE Group of Companies owns the largest 5G network in Greece, with population coverage now exceeding 99% and currently covering approximately 60% of the population with over seven (7) million subscribers. Having that as a starting point, marketing and sales campaigns can identify target markets and develop strategies to promote the usability of the feature; inform users about its benefits and onboard new customers. | |
| **Cost Structure** | | | **Revenue Streams** | |
| •Marketing<br><br>•R&D costs | | | •Services | |

| | |
|---|---|
| •Engineering costs | |

### 4.2.12. ER22: Smart Pricing Policies

*SWOT Analysis*

Table 26: SWOT Analysis for ER22

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Advanced auction-based mechanism that promotes fairness, efficiency, and transparency in competitive environments<br><br>•Innovative AI-driven pricing intelligence that adapts to dynamic demand, making the Smart Pricing Module (SPM) more responsive than static pricing systems<br><br>•Modular architecture allowing integration into diverse network ecosystems without redesigning the whole infrastructure<br><br>•Built-in incentive alignment that can nudge providers toward efficient and cooperative resource participation. | •Dependence on high-quality telemetry and clean data, which may not be consistently available across all operators<br><br>•High technical complexity, requiring sophisticated tuning, monitoring, and expertise to operate effectively<br><br>•Limited transparency for non-technical stakeholders, which may reduce trust or hinder adoption<br><br>•Potential fragility in algorithmic parameters, where small errors can lead to unstable or unfair pricing outcomes |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •Emergence of multi-provider marketplaces where real-time pricing can unlock new business models<br><br>•Growing industry push toward autonomous 6G networks that require dynamic, market-based resource management<br><br>•Regulatory interest in fair, auditable allocation mechanisms, which the SPM can support<br><br>•Demand for cost-efficient operations | •Market resistance from operators hesitant to rely on automated pricing systems, affecting revenue control<br><br>•Regulatory pushback if dynamic pricing is perceived as unfair or too complex for users to understand<br><br>•Risk of strategic manipulation by sophisticated providers exploiting loopholes in auction or ranking mechanisms<br><br>•Public perception risks, especially if dynamic pricing spikes during emergencies or peak demand events |

*Lean Canvas*

Table 27: Lean Canvas for ER22

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| The shift toward decentralized B5G/6G networks creates environments where multiple providers must share resources dynamically, but existing pricing models cannot keep up with rapid fluctuations in demand. Static or centrally controlled pricing leads to inefficiencies, unfairness, and bottlenecks, especially when many independent actors are competing to offer similar services. | The problem is addressed by implementing smart pricing schemes that introduce financial incentives for UEs and providers. These mechanisms promote dynamic cooperation and resource sharing across different network operators. | The determined price is tailored to the specific service, aiming to maximise revenue while minimising potential profit loss. | • The SPM's main strength comes from combining AI-based learning with multi-round auctions, a concept being introduced for the first time.<br><br>• Its ability to work in decentralized networks gives it an early lead in new B5G/6G markets.<br><br>• This positions the SPM to become a reference model for both commercial products and academic research in the future. | • Telecom operators, cloud providers, and enterprise network owners gain more dynamic, competitive, and efficient pricing models for resource sharing.<br>• Technology vendors and solution integrators benefit from value-added capabilities that enhance the attractiveness of their platforms in the 5G/6G market.<br>• Researchers in AI, networking, and economics gain a rich experimental framework for studying multi-agent learning, auctions, and decentralized market design, enabling novel academic contributions and advanced prototypes. |
| **Key Metrics** | | | **Channels** | |
| •Improved efficiency in allocating network resources and setting dynamic prices across multiple providers.<br><br>•Faster and more accurate decision-making during high-demand or congested conditions.<br><br>•Minimized operational overhead by automating pricing, negotiation, and provider selection processes. | | | Private-sector engagement is driven through pilot deployments, industry showcases, technical partnerships, and integration into vendor ecosystems, enabling companies to test and adopt the SPM with low onboarding friction. Research dissemination focuses on peer-reviewed publications, open-source components, academic workshops, and collaborative testbeds, making the system visible and accessible to the scientific community. | |
| **Cost Structure** | | | **Revenue Streams** | |
| •R&D costs<br><br>•Engineering and Production costs | | | •Sales<br><br>•Maintenance | |

### 4.2.13. ER23: Big Data Platform for self-healing and self-recovery

*SWOT Analysis*

Table 28: SWOT Analysis for ER23

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •Modular, scalable architecture designed specifically for self-healing and self-recovery workflows, enabling easier integration and deployment<br><br>•Multi-broker approach that supports distributed processing and reduces data movement<br><br>•Real-world validation on a commercial 5G testbed, demonstrating functional performance and operational feasibility | •Current solution scope targets a limited set of use cases; additional generalization is needed to address broader verticals and workflows<br><br>•Integration complexity: multi-broker components may require sophisticated orchestration and operational expertise |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •Growing B5G/6G and edge markets demand higher availability, low latency, and autonomous network operation, strong market pull for self-healing platforms<br><br>•Rising adoption of industrial IoT, smart cities, and critical communications where reliability guarantees and automated recovery are required<br><br>•Regulatory and enterprise emphasis on data locality and privacy favors distributed architectures that avoid sensitive data centralization | •Established competitors and commercial vendors with mature solutions and larger ecosystems may capture market share, especially for cloud-only deployments<br><br>•Open-source platforms and alternative distributed frameworks could be adapted quickly to offer similar capabilities |

*Lean Canvas*

Table 29: Lean Canvas for ER23

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| 5G/B5G networks frequently suffer service degradation and outages caused by faults, misconfigurations, and rapid traffic shifts across distributed sites. Current monitoring and automation tools cannot efficiently | A modular, scalable Big Data platform that ingests, stores, and serves extreme volumes of data to power timely self-healing and self-recovery workflows. It | Enable autonomous, data-driven self-healing of 5G/B5G networks at extreme scale by combining distributed data management, multi-broker architecture, and | •Multi-broker architecture specifically designed for telecom edge topologies.<br><br>•Demonstrated real-world validation on a | •Large mobile network operators seeking to improve network availability and automate operations across core and edge.<br><br>•Enterprise/private network operators in industrial IoT, |

| | | | | |
|---|---|---|---|---|
| handle the extreme, high-velocity data from many edge locations, centralizing data is costly or infeasible. The result is delayed or inaccurate detection and slow recovery, leaving operators unable to meet stringent availability and latency targets. A lightweight, distributed data-and-analytics approach is needed to detect, diagnose, and remediate quickly while preserving bandwidth and data locality. | uses a multi-broker data management approach to perform distributed analytics, preserving data locality while providing low latency inference and automated remediation. | validated edge operation. | commercial 5G testbed. | smart manufacturing, logistics, and critical communications requiring high availability and low latency. |

| Key Metrics | Channels |
|---|---|
| •Recovery success rate: percentage of issues resolved automatically without human intervention.<br><br>•Self-healing and recovery algorithms performance. | •Strategic partnerships with network operators, private network integrators for pilot projects, and validation.<br><br>•Collaboration and commercial offerings via edge infrastructure providers to reach distributed deployments. |

| Cost Structure | Revenue Streams |
|---|---|
| •Distribution costs<br><br>•People<br><br>•Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs<br><br>•Permits, authorisations, etc. | •Sales<br><br>•Services (consultancy / training / etc.)<br><br>•Maintenance |

### 4.2.14. ER24: A framework for data and concept drift detection in 6G networks

*SWOT Analysis*

Table 30: SWOT Analysis for ER24

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| •State-of-the-art performance compared to existing algorithms, methods, and solutions<br><br>•Reliable and robust methods with short execution time<br><br>•Low energy consumption | •There is no “one size fits all” in data drift problems. As a result, the method may require some fine-tuning, according to the task at hand<br><br>•Requires a fully trained AI model to function<br><br>•Does not support image data, for the time being |

| | |
|---|---|
| •Interoperability: Can be used with any AI model, without limitations<br><br>•Saves a significant amount of energy and increases the target model performance<br><br>•Supports time series and numerical data | |
| **External Factors** | |
| **Opportunities (+)** | **Threats (-)** |
| •EU's Green Deal will accelerate the adoption rate of solutions that optimise energy efficiency<br><br>•This type of method/product will become indispensable for 6G and beyond networks<br><br>•New standardization practices for future (and contemporary) protocols will turn towards energy-efficient computing<br><br>•New, more complex AI models will require the support of similar products, since their re-training operations will be costly<br><br>•The market is segmented with low levels of consolidation | •Legislature that constrains the use of AI<br><br>•Brute force solutions (i.e. product that do not utilise a sophisticated decision-making mechanism) are currently used in the industry. Some inertia exists when adopting new solutions for these types of problems |

*Lean Canvas*

Table 31: Lean Canvas for ER24

| **Lean Canvas** | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Telecommunication service providers: NANCY's "A framework for data and concept drift detection in 6G networks " solves the issues of AI model re-training. The product indicates "when" to re-train an AI model in optimal periods of time thus, saving time, energy and costs while also maintaining high model quality.<br>Telecommunication Infrastructure providers: The main problem that NANCY's " A framework for data and concept drift | The proposed data/drift detection models introduce two unsupervised methods, that use model-agnostic batch concept drift detectors. Both methods compute an expected-utility score to decide when concept drift occurred and if model retraining is warranted, without requiring ground-truth labels after deployment. We validated our | Increased QoS within the network, high energy-efficiency when AI models are retrained, real-time adaptation, increased AI model quality, framework generalisability to other verticals. | •The core AI methods are hard to replicate since it was created by experts within the consortium, using state-of-the-art methods.<br><br>•The model-agnostic approach (i.e., the product is interoperable with any AI model) is hard to replicate.<br><br>•The real-world testing scenarios and the results we obtained from NANCY's Use | •Telecom operators<br>•Infrastructure providers (e.g., Cloud providers)<br><br>•Network operators<br><br>•Consultancies<br><br>•Vertical industries with high AI adoption rate (such as manufacturing industry)<br><br>•Cybersecurity companies |

| | | | | |
|---|---|---|---|---|
| detection in 6G networks " alleviates is the issue of large power consumption, used for model training operations | approach using real-world datasets, stemming from NANCY's data repositories. | | Cases are difficult to find and to evaluate models with. | |

| Key Metrics | Channels |
|---|---|
| From the conducted experiments, the following KPIs illustrate the performance of our solution:<br><br>•Drift detection accuracy: ≥ 95%<br><br>•False positive rate: ≤ 8%<br><br>•Energy savings due to well-chosen re-training operations: ≥ 35%<br><br>•Increased model quality to well-chosen re-training operations: ≥ 40% | •Social media and web campaigns<br><br>•Presentations and demonstrations in events and exhibitions<br><br>•Later, direct sales through partnerships<br><br>•Direct relationships with the existing network of collaborators. |
| **Cost Structure** | **Revenue Streams** |
| •Distribution costs<br><br>•Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs | •Open-source licensing<br><br>•Sales<br><br>•Services (consultancy / training / etc.) |

### 4.2.15. ER28: Central Management Domain

*SWOT Analysis*

Table 32: SWOT Analysis for ER28

| Internal Factors | |
|---|---|
| **Strengths (+)** | **Weaknesses (-)** |
| The NANCY Central Management Domain couples a state-of-the-art Continuous Integration/Continuous Delivery system (provided by INTRA) with advanced orchestration (provided by UBI) and creates the capacity to excel in automating testing and deployment pipelines across virtualized network segments, enabling rapid provisioning of resources for diverse use cases. Specifically, the MAESTRO orchestrator supports multi-domain end-to-end service orchestration, managing full-service lifecycles across geo-distributed, multi-stakeholder environments. Multi-vendor compatibility and model-driven architecture further enhance flexibility, allowing dynamic instantiation based on QoS parameters. | Orchestration complexity poses significant challenges, requiring advanced multi-domain and multi-vendor integration that can lead to high initial setup costs. Security vulnerabilities in dynamic slicing and Continuous Integration / Continuous Delivery (CI/CD) pipelines may expose isolated networks to risks if not robustly managed. |
| **External Factors** | |

| Opportunities (+) | Threats (-) |
|---|---|
| Integration with 5G/6G ecosystems lowers the barriers for service providers to deliver their services, while at the same time opens avenues for network providers to monetize tailored slices, supporting enterprise self-provisioning and SLA-driven services. CI/CD advancements enable faster software release through continuous automation, positioning the system as a cornerstone for 5G/6G ecosystems by accelerating innovation in cloud-native functions. Expansion into private networks and edge computing could capture growing demand. | Competition from established companies like Ericsson (Ericsson SMO) or VMWare (VMware Telco Cloud Automation) could erode market share without strong differentiation in cross-domain capabilities. |

*Lean Canvas*

Table 33: Lean Canvas for ER28

| Lean Canvas | | | | |
|---|---|---|---|---|
| **Problem** | **Solution** | **Unique Value Proposition** | **Unfair Advantage** | **Customer Segments** |
| Telco operators and enterprises face siloed and fragmented CI/CD pipelines that hinder multi-domain deployments, leading to slow service rollouts, manual orchestration errors, and scalability issues in 5G/6G networks with network slicing. Existing tools lack unified intent-based management across vendors and clouds, increasing operational costs and latency mismatches. | CI/CD automates testing, makes it easier to manage code versions, and in general streamlines code delivery to be faster, more efficient and less error prone. By coupling these services with a multi-domain orchestrator like MAESTRO we ensure that the Kubernetes /Helm-integrated pipeline can deliver end-to-end automation for complex telco environments, enabling seamless deployment across RAN, core, transport, and slicing domains while minimizing manual errors and accelerating service rollouts. Tighter integration among these components makes the combined solution more than the sum of its parts. The integrated Central Management Domain Deployment and Orchestration platform is better equipped for | The INTRA CI/CD pipeline is used to help organisations consistently deliver code that meets high quality standards. UBI's Maestro service orchestrator deals with the deployment and orchestration of services. The Orchestration and CI/CD system services are hosted in the central NANCY Kubernetes cluster, which serves a dual purpose: (a)To establish a common development and testing environment for containerized NANCY components, aiming to verify their functionalities and ensure integration among various components and services prior to deployment in operational settings (separate Kubernetes clusters at NANCY testbeds/ demonstrators), (b) To host NANCY Management domain services, which include as mentioned above orchestration services that are accessible across different operational environments via secure VPN tunnels. The CI/CD | INTRA and UBITECH designed their solutions and integrated them tightly together based on their expertise and deep knowledge of the telco ecosystem. This means that the solution was designed with specific challenges of this sector in mind and is better positioned to address them. | Telco providers (MNOs), private network operators, and service providers adopting 5G slicing. |

| | | | | |
|---|---|---|---|---|
| | multi-domain environments while also being able to fully take advantage of the automation offered by an enterprise-grade CI/CD solution. | Platform provides DevOps automation capabilities through the configuration of software build, testing and deployment pipelines for the different NANCY components and services. The NANCY CI/CD system is connected to the central NANCY Kubernetes cluster, supporting the development and testing of NANCY components. The CI/CD system services are also securely connected to the Kubernetes environments of the different NANCY testbeds and demonstrators to control the deployments of NANCY containerized components and services either directly through the CI server or through the Maestro service orchestrator. Maestro is a cloud-native service orchestrator designed to manage the lifecycle of end-to-end services across geo-distributed infrastructures. It facilitates automated deployment, scaling, and lifecycle management of microservices-based applications. Maestro integrates with Kubernetes and OpenStack environments to deploy services via containers or virtual machines. Maestro operates in environments involving Kubernetes clusters and integrates with edge and core infrastructures. It uses Kubernetes-as-a-Service (K8s-aaS) for resource orchestration. Container images and Helm charts are managed in the NANCY Harbor container registry, ensuring smooth retrieval of artifacts during deployment. Service providers onboard containerized services, which are subsequently deployed via Kubernetes. | | |

| Key Metrics | Channels |
|---|---|
| Unified pipelines support multi-vendor interoperability, fostering collaboration for enterprises and MNOs. The setup created for the NANCY Central Management Domain is designed to lower Mean-time-to-Production and Mean-time-to-Repair metrics (MTTP/MTTR), boost code quality via continuous feedback, and unlock monetization through rapid, SLA-compliant service delivery. The most important measurable KPIs therefore include deployment time reduction (%), MTTP, as well as MTTR in case of failures. | The channels that may be engaged are:<br><br>•Direct through existing partnerships in the 5G/6G domain;<br><br>•Online demos and showcases through NANCY and other related projects that can verify the performance and efficiency of the proposed solution;<br><br>•Proof-of-concept demonstrators at client premises; and,<br><br>•Industry and scientific events that engage the related stakeholders (such as EuCNC, Infocom World, Mobile World Congress etc). |
| **Cost Structure** | **Revenue Streams** |
| •People<br><br>•Marketing (Customer Acquisition costs)<br><br>•R&D costs<br><br>•Engineering and Production costs | •Sales<br><br>•Services (consultancy / training / etc.)<br><br>•Maintenance |

# 5. Commercialization Planning

## 5.1. Characterization Table for each Commercial Exploitable Result

### 5.1.1.ER2: PQC Signature Solution

Table 34: Characterization Table for ER2

| Result: PQC Signature Solution | |
|---|---|
| | Input from Beneficiary |
| **Description** | This solution offers PQC algorithms to allow to generate, verify signatures and exchange keys securely against the threat crated by the future quantum computers. |
| **Target market/end users** | Governments, Telecom operators, critical infrastructure operators, industry |
| **End-users needs / problems** | •Protect key exchange and signature against future quantum-enabled attacks.<br>•Maintain interoperability with deployed software solution while migrating to PQC.<br>•Regulatory and compliance pressure to demonstrate preparedness for post-quantum transition. |
| **Competitive advantages** | First secure implementation of PQC algorithms common criteria certified. |
| **Use model** | Deliver the product |
| **Early Adopters** | Governments and critical entities that want to be prepared against the quantum computer threats. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | No alternative solution against future quantum attacks. |
| **Unique Value Proposition** | First provider of a common criteria product with PQC algorithms. |
| **Competitors** | Classical smartcard operating system providers. |
| **Timing** | First common criteria product already available. |
| **IP Strategy** | A proprietary IP strategy will be followed. |

### 5.1.2.ER3: Blockchain Wallet with SSI and PQC Capabilities

Table 35: Characterization Table for ER3

| Result: Blockchain Wallet with SSI and PQC Capabilities | |
|---|---|
| | Input from Beneficiary |
| **Description** | A blockchain wallet with Self-Sovereign Identity (SSI) and PQC aimed at enhancing privacy and security in 5G service provisioning, targeted at the private sector and permissioned blockchains |
| **Target market/end users** | Operators, service providers and end-users |
| **End-users needs / problems** | Potential end-users in the private sector face increasing challenges in protecting user identities and sensitive data during 5G service provisioning. Current wallet and identity solutions rely on centralized trust models and cryptographic schemes that are vulnerable to data breaches and future quantum attacks. There is also a lack of user-controlled identity mechanisms that preserve privacy while enabling secure authentication across multiple services. End-users need a secure, privacy-preserving, and future-proof |

| | |
|---|---|
| | wallet solution that can operate reliably within permissioned blockchain environments. |
| **Competitive advantages** | The proposed wallet addresses these challenges by integrating Self-Sovereign Identity, allowing end-users to maintain full control over their identities and selectively disclose credentials without relying on centralized identity providers. By incorporating Post-Quantum Cryptography, the solution ensures long-term security against quantum-enabled attacks, surpassing the protection offered by current blockchain wallets that rely on classical cryptographic schemes. Unlike existing solutions, which typically address either identity management or cryptographic resilience in isolation, this wallet combines both capabilities within a single, interoperable platform. Its design for permissioned blockchain environments makes it particularly well-suited for private-sector 5G service provisioning, where trust, compliance, and high security are critical. |
| **Use model** | The result can be made available as a commercial blockchain wallet product tailored for private-sector 5G ecosystems. It may be deployed as a licensed software solution or offered as a managed service integrated into existing permissioned blockchain infrastructures. Technology transfer to telecom operators, service providers, or system integrators can support large-scale adoption. In parallel, selected components may contribute to standardisation efforts or be released through technical publications to encourage interoperability and industry uptake. |
| **Early Adopters** | Early adopters are expected to be telecom operators, 5G service providers, and enterprise network operators experimenting with permissioned blockchains and advanced security solutions. Research-driven enterprises and technology integrators focusing on privacy-preserving and quantum-resistant systems are also likely to adopt the solution early. |
| **Adopters' problems/needs** | Please refer to End-users needs/problems. |
| **Alternative Solution** | Alternative solutions include conventional blockchain wallets that rely on classical public-key cryptography and centralized identity management systems, which offer limited privacy and are not resilient to quantum threats. Some platforms provide SSI-based identity wallets, but they typically lack integration with blockchain-based service provisioning and do not support post-quantum algorithms. Other approaches focus on PQC at the network or protocol level without addressing user identity control. |
| **Unique Value Proposition** | A future-proof blockchain wallet that unifies self-sovereign identity and post-quantum cryptography to deliver privacy-preserving, quantum-resilient authentication for 5G service provisioning in permissioned environments. |
| **Competitors** | Enterprise blockchain wallets and platforms such as IBM (Hyperledger Fabric) and R3 Corda, which support permissioned blockchains but rely on classical cryptography and limited identity self-sovereignty.<br><br>SSI-focused companies like Evernym, SpruceID, and Sovrin, which provide decentralized identity solutions but do not integrate post-quantum cryptography or 5G service provisioning.<br><br>Blockchain wallet providers such as ConsenSys (MetaMask), which focus on blockchain access but are not designed for permissioned enterprise or telecom environments. |

| | |
|---|---|
| | Centralized IAM and security providers like Microsoft Entra (Azure AD) and Okta, which are widely used in enterprise and telecom settings but lack SSI principles and quantum-resistant security |
| **Timing** | To be defined |
| **IP Strategy** | To be defined |

### 5.1.3.ER4: PQC Secure Communication

Table 36: Characterization Table for ER4

| **Result: PQC Secure Communication** | |
|---|---|
| | Input from Beneficiary |
| **Description** | This solution delivers PQC for secure communications particularly suited for 5G scenarios by combining standards-aligned protocols with support for PQC digital-signature tokens and hybrid PQC/classical modes. Its objective is to provide robust post-quantum assurance for device-to-network and device-to-device communications across different environments (e.g., mobile and IoT deployments), enabling assets to remain protected as quantum-capable adversaries emerge. The solution's primary advantage is its resilience against both quantum and classical threats, preserving confidentiality and integrity where legacy cryptography may eventually fail. It is based on an end-to-end prototype including integration with PKCS#11 compatible hardware signature tokens. This capability is important because it strengthens long-term communications security for operators and device manufacturers and offers a reputational and regulatory edge for organizations that proactively adopt quantum-resistant measures. |
| **Target market/end users** | Telecom operators, critical infrastructure operators, industry. |
| **End-users needs / problems** | •Need to protect communications against future quantum-enabled attacks.<br>•Requirement to maintain interoperability with existing PKI/TLS ecosystems while migrating to PQC.<br>•Desire for hardware-backed key protection (non-extractable keys) to meet high-assurance use cases.<br>•Regulatory and compliance pressure to demonstrate preparedness for post-quantum transition. |
| **Competitive advantages** | •Combined software and hardware approach: supports both software PQC paths and PKCS#11 compatible hardware tokens for higher assurance.<br>•Standards-aligned integration facilitating interoperability and phased migration from classical cryptography.<br>•Demonstrated prototyping experience in live 5G contexts, reducing integration risk for early adopters. |
| **Use model** | •Delivered as a combination of reference implementations, SDKs, and integration guides for operators.<br>•Pilot deployments and proof-of-concept integrations with telecom testbeds to validate performance and interoperability.<br>•Collaboration with HSM/token vendors to commercialize turnkey options. |
| **Early Adopters** | •Telecom operators running B5G/6G testbed willing to pilot hybrid PQC to gain operational experience.<br>•Massive IoT and industrial IoT with high-value devices or long update cycles who prioritize long-term cryptographic assurance.<br>•Security-conscious enterprises in healthcare, transportation, and utilities that can invest in pilots and have regulatory impetus. |

| | |
|---|---|
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | •Classical public-key cryptography (RSA, ECC) over TLS, widely deployed but vulnerable to future quantum attacks.<br>•Software-only PQC libraries provide post-quantum algorithms but may lack hardware-backed key protection and can be resource-heavy for constrained devices.<br>•Hardware Security Modules (HSMs) and Secure Elements using classical algorithms, offer key protection but not PQC resistance unless re-engineered. |
| **Unique Value Proposition** | Improve communication protection by delivering a practical, standards-aligned PQC integration path that combines software and optional hardware token support to provide forward-looking cryptographic resistance. |
| **Competitors** | •Classical cryptography vendors (HSM/secure element providers): mature ecosystems and high performance, but lack inherent PQC resistance without redesign.<br>•Pure software PQC libraries (open-source and commercial): offer algorithm support but may lack hardware-backed key. |
| **Timing** | Expected time to market: First adoption depends on customer readiness (24–48 months).<br><br>Current readiness: Prototype/Testbed stage.<br><br>Adoption feasibility: Growing regulatory and standards momentum (NIST selections, EU guidance) makes the current context favorable for pilots and phased migrations. |
| **IP Strategy** | None |

### 5.1.4.ER5: B-RAN Theoretical Framework

Table 37: Characterization Table for ER5

| **Result: B-RAN Theoretical Framework** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Models the performance of the B-RAN in various scenarios<br><br>Objectives: Accurately model and estimate the achievable performance of B-RAN.<br><br>Advantages: Customised development of B-RAN based on the client's needs.<br><br>What is new: Novel framework.<br><br>Why is it important: Reduces development and deployment costs. |
| **Target market/end users** | Industry & Public sector (Interesting technology for any stakeholder trying to deploy private or public B-RAN) |
| **End-users needs / problems** | • Must design and dimension B-RAN networks that meet strict QoS/QoE demands, without excessive CAPEX/OPEX.<br>• Limited insight into how different configurations and traffic profiles influence performance before deploying.<br>• Reduced investment risk in designs by testing numerous virtual design alternatives, instead of relying solely on physical pilots. |

| | |
|---|---|
| | • Require tools capable of capturing B-RAN-specific features and integrating with emerging technologies (e.g., blockchain, edge, slicing). |
| **Competitive advantages** | • Specifically designed for B-RAN, employing advanced queueing, Markov and AI/ML-based models instead of generic heuristic-based planning.<br>• Ability to rapidly examine a wide variety of design and configuration options, to allow for more informed decisions on the final design.<br>• Customizable to fit specific needs and constraints of each stakeholder's environment, KPIs and constraints.<br>• Possible integration with other INNO frameworks (security and semantic communications) for richer, multi-faceted evaluations. |
| **Use model** | • Delivered as a specialized modeling and planning service, wherein INNO experts execute studies and produce reports/recommendations.<br>• Licensing as a specialized modeling and planning software framework/toolkit, that can be incorporated into existing planning processes or operator toolchains.<br>• Joint R&D or innovation collaborations with operators, vendors and public authorities.<br>• Future possibility for packaging as a user-friendly application (with dashboards and configuration interfaces for scenario selection) for non-expert users. |
| **Early Adopters** | Researchers |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | • Generic radio network planning tools, not tailored to B-RAN characteristics, often rely on oversimplified assumptions.<br>• Manual engineering based on experience and rule-of-thumb dimensioning, potentially leading to either over-provisioning or performance problems.<br>• Proprietary planning tools offered by vendors, potentially locking customers into one vendor's ecosystem and lacking transparency regarding the underlying models.<br>• Empirical trial-and-error pilots, which are expensive and time-consuming, before arriving at an optimal configuration. |
| **Unique Value Proposition** | • Enable end-users to evaluate and design B-RAN prior to deployment, providing confidence in designing and optimizing B-RAN deployments with realistic, model-based performance estimates.<br>• Provide a cost-effective means to reduce development and deployment costs while maintaining or improving service quality.<br>• Allow for customization of the framework to fit specific needs and constraints of each customer's environment. |
| **Competitors** | • Well-established radio network planning and optimization tools provided by major telecom vendors.<br>• Independent, commercially available planning software focusing on 5G/6G and private networks.<br>• Internal planning tools developed by large operators or vendors.<br>• Advantages of competitors: market presence, integration into existing ecosystems, and maturity of Graphical User Interface (GUI).<br>• Limitations of competitor products: lack of specificity to B-RAN, limited transparency of models, risk of vendor-lock-in, less flexibility to integrate novel frameworks (e.g., realistic blockchain-related aspects). |

| | |
|---|---|
| **Timing** | Short-to mid-term (within 1–3 years) for initial commercial interactions with the first operators and organizations to deploy private/public B-RAN networks.<br><br>Given the increased momentum around private 5G/6G and B-RAN deployments, it is currently an ideal time to launch advanced planning and modeling tools.<br><br>As B-RAN deployments grow, the anticipated demand for optimization and cost reduction tools will support both short-term and longer-term utilization. |
| **IP Strategy** | None |

### 5.1.5.ER6: QKD Simulation Framework

Table 38: Characterization Table for ER6

| **Result: QKD Simulation Framework** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Simulates the performance of QKD communications without the need for equipment.<br><br>Objectives: Achieve close to real-life performance.<br><br>Advantages: No need for expensive QKD equipment.<br><br>What is new: The component will be compared to actual experiments in the duration of the project.<br><br>Why is it important: Highly reduced costs compared to the actual equipment. |
| **Target market/end users** | Industry & Public sector (Interesting technology for any stakeholder trying to deploy QKD solutions). |
| **End-users needs / problems** | • Before spending money on expensive hardware, there is a need to determine whether QKD can meet the necessary performance/reliability expectations.<br>• Currently, there are no tools available to simultaneously model quantum-level effects/network behavior/realistic operating conditions.<br>• Difficulties exist in comparing various QKD technologies/vendors/deployment scenarios based on comparable criteria.<br>• Trade-offs need to be quantified between cost/distance/topology/achievable key rates.<br>• Need to provide justification for investment decisions/roadmaps to internal decision-makers/regulators. |
| **Competitive advantages** | • Allows for realistic/experiment-calibrated predictions of QKD performance without the need for physical QKD equipment.<br>• Permits comparative analysis of different protocols/hardware parameters/network designs within a single framework.<br>• Reduces time-to-decision/time-to-deploy for QKD projects by replacing multiple costly test cycles with simulations.<br>• Has a vendor-neutral/extensible architecture that enables the inclusion of new protocols/components as the technology evolves.<br>• Supports both technical/techno-economic studies that enable effective communication between engineers/managers/policymakers. |

| | |
|---|---|
| **Use model** | • Software tool provided to INNO for delivery of consultancy/performance assessment studies.<br>• Installed locally/on-premises/cloud environment for operators/public authorities under license/service agreement.<br>• Collaborative research projects/pilots that use the model as the reference simulation framework for QKD scenarios.<br>• Potential future release of a research-oriented version (with reduced functionality) for general community use to encourage adoption/use. |
| **Early Adopters** | Researchers |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | Performance assessment of QKD is currently done using:<br><br>• Laboratory experiments/testbeds using actual QKD equipment.<br>• Simplistic analytical models that cannot accurately represent realistic impairments/network effects.<br>• Vendor-specific planning tools that are opaque/transparency-limited and optimized for one technology stack.<br>• Tools that plan classical security/optical networks that do not account for quantum-specific phenomena/key-rate behavior. |
| **Unique Value Proposition** | Plan and/or estimate the performance of QKD communications. |
| **Competitors** | Proprietary QKD simulation/planning tools provided by major equipment vendors.<br><br>Academic simulation frameworks focused on specific protocols/limited network topologies.<br><br>General optical-network planning tools provide only rough estimates of QKD performance.<br><br>Compared to the above, the QKD Simulation Framework is more transparent/configurable than vendor black-box tools. Also, it is capable of modeling a greater range of scenarios than most single-protocol academic simulators. Finally, it provides quantum-aware modeling that general classical network planners cannot. |
| **Timing** | Short to medium term (0-3 years): Use in pilots/R&D projects/early feasibility studies where QKD deployments are being evaluated.<br><br>Medium to long term (3-7 years): Commercial rollout support as QKD infrastructure matures and standardization advances.<br><br>Given the current focus of increased attention to quantum-safe communications/EU-level initiatives, forward-thinking organizations have the ability to implement the model today. |
| **IP Strategy** | None |

### 5.1.6. ER7: A novel AI virtualiser for underutilized computational & communication resource exploitation

Table 39: Characterization Table for ER7

| Result: A novel AI virtualiser for underutilized computational & communication resource exploitation | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Inter-slice conflict and underutilization mitigation<br><br>Objectives: Efficient resource exploitation in the RAN-Edge-Cloud continuum<br><br>What is new: protocol learning as a basis |
| **Target market/end users** | The target market for the AI Virtualiser includes orchestration/automation solution providers. The end users are the telcos and communication service providers that adopt such orchestration/automation solutions in their networks. |
| **End-users needs / problems** | The inefficient use of network resources results in prohibitive OPEX costs for telcos. Current low automation solutions result in poor efficiency in terms of resource utilization, especially in rapidly changing scenarios. In addition, low automation solutions typically require substantial manual configurations, which further increases OPEX and potentially leads to human errors that can disrupt services. |
| **Competitive advantages** | The AI Virtualiser provides a fully-automated solution for inter-slice resource management that can be mapped to TMForum's automation level 4. It reduces operational costs related to poor resource utilization and heavy manual interventions, and provides better quality of user experience by providing a faster recovery from congestion. |
| **Use model** | A technology transfer or licensing model will be followed. Scientific publications will also be pursued. |
| **Early Adopters** | Orchestration/automation solution providers have been identified as potential early adopters, as the AI Virtualiser has the potential to improve the technological capabilities of their solution and therefore provide enhanced added value to their customers. This customer segment will be prioritized over the others. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | The most mature solutions for intra and inter- network slice resource allocation rely on existing cloud-native resource scaling capabilities (e.g., those provided by Kubernetes). Algorithms based on DRL, MADRL and transfer learning have been proposed, but these are mainly at a theoretical level and lack working implementations. |
| **Unique Value Proposition** | Efficient use of resources to maximise the return from leasing the infrastructure to multiple tenants whilst reducing operational costs. |
| **Competitors** | Big vendors (Ericsson, Nokia, Symphonica) provide cloud-native, AI-driven OSS/BSS solutions. System integrators such as Indra and Minsait provide AI-driven orchestration solutions. All of the above products have wide acceptance from major communication service providers, as they have a deep knowledge of the industry and their products are certified to the highest standards, but they also have a high pricing point for both technological and support offerings. The AI Virtualiser offers a better |

| | |
|---|---|
| | alternative in terms of the Key Performance Indicator (KPI) gains it potentially achieves, and it can also offer a more competent alternative in terms of pricing if integrated with alternative network orchestration/automation solutions. In addition, the AI Virtualiser is highly customizable and can be adapted to specific customer needs. |
| **Timing** | The expected time to market is 2 to 3 years. During this time, it is expected that a higher maturity will be achieved through integration with relevant use cases. In addition, the maturity and acceptance of agentic AI solutions will increase in the market if their benefits continue to be demonstrated. |
| **IP Strategy** | A proprietary IP strategy will be followed to enable the transfer or licensing of the AI Virtualiser to potential adopters. |

### 5.1.7.ER10: Semantic Communications Framework

Table 40: Characterization Table for ER10

| **Result: Semantic Communications Framework** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Next-gen energy and data-efficient communications.<br><br>Objectives: Intelligently reduce the amount of data transferred in the network.<br><br>Advantages: Increase energy and data efficiency.<br><br>What is new: Novel framework based on AI and conventional techniques.<br><br>Why is it important: Pushes the current SoTA of the networks towards sustainability. |
| **Target market/end users** | Industry & Public sector (Interesting technology for any stakeholder trying to reduce network traffic and/or improve energy efficiency in communication/networking tasks.) |
| **End-users needs / problems** | Key problems being solved:<br><br>• Energy Consumption – The world's network infrastructure consumes between 4-5 percent of the total amount of electricity used globally; telecom companies are being pushed to cut their energy expenses and carbon footprints.<br>• Data Explosion – As data is transmitted at an exponential rate, it is causing operational difficulties and expenses for the telecommunications company.<br>• Regulatory Compliance – The EU Green Deal and other new regulations regarding energy efficiency and sustainability are pushing companies toward a green approach and increasing the cost of non-compliance through carbon pricing.<br>• Capital Expenses – New network expansions will require large amounts of capital investments by telecom companies, and efficiencies realized from using this technology will also decrease both the Capex and Opex.<br>• Climate Pledges – Companies are making corporate-wide climate pledges, which include a significant reduction in the energy consumed.<br><br>Examples of specific use cases:<br><br>• Optimizing traffic on backbone networks |

| | |
|---|---|
| | • Reducing energy consumption from mobile networks during both peak and off-peak times<br>• Supporting sustainable data center operations• Providing efficient satellite communications<br>• Supporting the deployment of IoT and edge computing applications |
| **Competitive advantages** | • Semantic awareness, based on understanding the semantic meaning and goal orientation of communications, enables us to be more efficient than blind compression.<br>• Hybrid approach combines the benefits of ML (adaptable, recognizes patterns) with the reliability and interpretability of signal processing theory, thus we have the robustness that is missing in either pure AI or pure conventional approaches.<br>• Comprehensive end-to-end solution for optimizing multiple network layers rather than offering point solutions that incrementally optimize only one layer.<br>• Extension beyond traditional limits of communication theory to improve performance through semantic comprehension.<br>• Application to different types of network architectures and network implementations, whereas many competing solutions are limited to a few specific scenarios. |
| **Use model** | Software License Model: License the framework as a standalone software package for network operators to install into their existing networks. Integrate our framework into existing network management systems. Offer subscription models or perpetual license options.<br><br>Service Based Model: Offer hosted optimization service to network operators. Provide API-based integration with network infrastructure. Develop performance monitoring and analytics dashboards for customers.<br><br>Technology Transfer Model: License to network equipment manufacturers for integration into products. Jointly develop frameworks for specific use cases. Offer consulting services for implementing the framework customized to each customer's needs.<br><br>Standardization Path: Submit our framework to international standards organizations for consideration to become part of standardized protocols. Contribute to developing industry standards for semantic communications.<br><br>Open Source Components: Release selected components of our framework as open source. Create an ecosystem and accelerate adoption. Offer premium versions of our commercial products with enterprise features and support. |
| **Early Adopters** | Researchers |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | • Traditional data compression methods (lossless/lossy codec)<br>• Network optimization and traffic management<br>• Hardware that is more efficient (lower power usage devices)<br>• Shannon-based communication theory methods<br>• QOS and load balancing<br>• Routing algorithms that are aware of the cost of energy |

| | |
|---|---|
| **Unique Value Proposition** | Increase energy and data efficiency. |
| **Competitors** | • Other academic and industrial research groups focused on semantic communications<br>• Vendors of network optimization software packages<br>• Telecom equipment manufacturers with their own initiatives to increase efficiency<br>• Traditional vendors of network compression tools<br>• Hardware efficiency manufacturers<br>• Network slicing and virtualization solutions |
| **Timing** | 0 – 3 years: Identify major stakeholders and early adopters, initiate pilot programs, clarify regulatory path forward<br><br>Year 4: Finalize market study, finalize commercial partnerships, plan for product release<br><br>5 – 7 years: Anticipate market entry with commercial products and/or services<br><br>The current state of the markets is very favorable for the adoption of semantic communications solutions:<br><br>• Industry-wide immediate demand for energy efficiency solutions for telecommunications infrastructure<br>• Regulatory drivers such as the EU Green Deal and carbon pricing are forcing the industry to move towards greener solutions<br>• Opportunities exist for integrating semantic communications into emerging 5G/6G standardizations<br>• Available funding for post COVID-19 improvements in telecommunications infrastructure optimization. |
| **IP Strategy** | None |

### 5.1.8.ER11: An explainable AI framework

Table 41: Characterization Table for ER11

| **Result: R11 - An explainable AI Framework** | |
|---|---|
| | Input from Beneficiary |
| **Description** | "NANCY Explainable AI Toolbox" presents the overall architecture, functionalities, and components of the XAI Toolbox. It provides an overview of the methodologies and tools that support transparency and interpretability for decision-making B5G network functions. The main components of the NANCY XAI Toolbox are (i) the anomaly detection XAI Component, (ii) the outage prediction XAI Component, and (iii) the semantic communications XAI Component. Furthermore, the deliverable presents the implementation of the centralised XAI dashboard, which provides access to global and local model explanations through visual and interactive interfaces. The integration of an LLM-Powered Analysis Component is introduced as a Dashboard's sub-component, which facilitates the transformation of technical outputs into natural language for better usability by non-experts. Additionally, the deliverable provides a comprehensive description of the optimisation strategies that support stability and scalability. Overall, this |

| | |
|---|---|
| | deliverable contributes towards a trustworthy and understandable AI, addressing the needs of end-users in network management. |
| **Target market/end users** | Industry |
| **End-users needs / problems** | • Trust deficit: Inability to trust AI-driven network decisions due to lack of transparency<br>• Regulatory compliance: Difficulty meeting EU AI Act explainability requirements<br>• Operational efficiency: Slow incident resolution due to opaque AI alerts requiring extensive investigation<br>• Knowledge gap: Technical AI outputs inaccessible to non-expert network operators<br>• Risk management: Inability to validate AI predictions before acting on critical decisions |
| **Competitive advantages** | • Domain specialization: Purpose-built for B5G/6G network management vs. generic XAI tools<br>• Integrated solution: Complete toolbox (components + dashboard + LLM) vs. fragmented offerings requiring assembly<br>• Natural language explanations: LLM integration providing beginner-friendly insights vs. technical visualizations only<br>• Multi-level explainability: Both global and local explanations supporting different user needs- Real-world validation: Tested in NANCY testbeds vs. theoretical or lab-only solutions |
| **Use model** | • Service-based: Consultancy for implementation, customization and integration<br>• Technology transfer: Licensing to equipment manufacturers for integration into products<br>• Training programs: Certification courses for network operators and AI engineers<br>• Maintenance contracts: Ongoing support, updates and SLA guarantees for enterprise users |
| **Early Adopters** | No established early adopters have been identified yet. Potential candidates include:<br>• NANCY project consortium partners for internal validation<br>• Telecom operators participating in testbed demonstrations<br>• European network operators engaged through SNS initiatives |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | Currently, this problem is addressed through:<br>• Manual inspection of network logs and traffic patterns by expert analysts<br>• Rule-based alerting systems without explanation capabilities<br>• Standalone XAI libraries (LIME, SHAP) requiring integration effort and ML expertise<br>• Solutions with limited customization and interoperability<br>• Traditional monitoring dashboards provide metrics without interpretation |

| | |
|---|---|
| **Unique Value Proposition** | Increase energy and data efficiency. |
| **Competitors** | • IBM OpenScale o Strengths: Mature platform, enterprise support, multi-cloud deployment o Weaknesses: Generic (not telecom-specific), expensive, complex setup<br>• Google What-If Tool o Strengths: TensorFlow integration, interactive visualizations o Weaknesses: Requires significant ML expertise, no domain-specific features |
| **Timing** | • Expected time to market: 8-14 months post-project completion (Q4 2026 – Q1 2027)<br>• Current readiness: Prototype stage, undergoing validation in testbeds<br>• Adoption feasibility: Feasible now for early adopters willing to participate in early- stage validation |
| **IP Strategy** | None |

### 5.1.9.ER13: Virtio-based cross-world transport layer

Table 42: Characterization Table for ER13

| **Result: Virtio-based cross-world transport layer** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Virtio transport layer that allows configuring virtio backend and frontend in different worlds of a TrustZone-enabled ARM system. For instance, this result would enable running the backend of a virtio device in the secure world while the frontend is in the non-secure world.<br><br>Objectives: Provide extreme flexibility when the execution of multiple operating systems on the same platform is required. In these cases, the multiplexing of physical resources must be performed in an extremely efficient way, and this result is a key component to achieving that.<br><br>Advantages: This virtio-based transport layer does not rely on a type-1 or type-2 hypervisor, thus involving less virtualisation overhead, making it suitable for embedded use-cases where careful handling of the available resources is needed. Additionally, this technology can have a great impact on all those systems that do not have multiple independent video/graphic pipelines. With the virtio-based cross-world transport layer, it is possible to allow the two worlds to render to the same screen, keeping the contact surface as narrow as possible.<br><br>What is new: The specific way in which virtio is used in a non-virtualised environment.<br><br>Why is it important: Paired with VOS' VOSySmonitor partitioning technology, it can constitute the foundation for software stacks in various embedded market segments as an alternative to highly priced and locked-in commercial solutions. |
| **Target market/end users** | Industrial (Industrial stakeholders can benefit from this exploitable result to realize commercial software stacks), on-premises cloud. |

| | |
|---|---|
| **End-users needs / problems** | In an heterogeneous platform where a complex software stack is deployed, engineers often face challenges related to inter-OS data exchange and the multiplexing of hardware capabilities. |
| **Competitive advantages** | The proposed solution allows to have virtio devices in an OS running inside an isolated hardware partition, allowing to achieve any form of data exchange between two OSes. Specifically, this technology enables the decoupling of the virtio frontend and backend, allowing them to run on separate operating systems. This facilitates the multiplexing of hardware capabilities, which is a difficult task when using more traditional technologies. Thanks to this technology, someone can design a system with multiple constrained OSes that address crucial, possibly safety-related, tasks. These operating systems, despite being limited to a small number of hardware devices due to safety and hardware constraints, can still utilize virtio devices whose backends reside on more feature-rich operating systems. |
| **Use model** | VOS expects to make this technology available to the interested customers mainly through development services that target the realization of PoCs, prior to the support activity to bring the solution to the production level. |
| **Early Adopters** | In the second half of 2025, the pool of possible stakeholders has increased due to some new developments on VOS' virtio-based transport layer. Specifically, VOS was successful in running virtio-gpu on top of virtio-loopback, unlocking interesting new possibilities and stakeholders for the virtio-based transport layer. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | Nowadays, big companies are providing all-inclusive "black-box" solutions that are supposed to meet all the customer needs. These solutions, however, most of the time include unnecessary functionalities that the customers still pay for in full. In these cases, the communication between heterogeneous OSes happens with closed-source solution that requires adaptations of the customer's software stack with custom network interfaces similar to Linux's TAP devices. |
| **Unique Value Proposition** | This result enables the implementation of powerful software stacks for ARM systems featuring the TrustZone extension that can rely on different operating systems to address tasks of diverse criticalities, while sharing a set of resources in an efficient way. |
| **Competitors** | The market, especially in other market segments such as the automotive, offers various hypervisors/virtualization kits that provide technologies able to implement similar architectures. |
| **Timing** | The current status of the technology already allows the realization of a PoC for the interested organizations. |
| **IP Strategy** | Disseminating by publishing papers in order to make the solution visible, while considering open sourcing. |

### 5.1.10. ER16: Machine learning models for decision-making

Table 43: Characterization Table for ER16

| **Result: Machine learning models for decision-making** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: AI training framework, novel AI model architecture, Deep Neural Network models, ML algorithms, innovative reinforcement learning approach. |

| | |
|---|---|
| | Objectives: To improve the State-of-the-art in the corresponding domains, to increase the efficiency of ML models, to achieve near-optimal performance in computational offloading tasks in next generation 5G/6G networks.<br><br>Advantages: Real-time service migration. Beyond SotA policy selection for computational offloading tasks. Consideration of multiple factors for the decision-making process. Reduced AI model training time.<br><br>What is new: Existing AI models/methodologies consider only a few factors to perform policy optimisation for computation offloading. NANCY's ML models consider a significant number of parameters to do so and thus, they manage to properly select the optimal policies. To accomplish this, SotA reinforcement learning AI techniques are leveraged and novel AI training methods are employed.<br><br>Why is it important: This exploitable result not only advances the state-of-the-art of the AI models for computational offloading, but also provides a real solution for next generation 5G/6G networks. The algorithms are designed to achieve near-optimal performance in real-world scenarios with real-world data. |
| **Target market/end users** | Industry |
| **End-users needs / problems** | • Increase in energy consumption of modern telecommunication networks, due to computationally heavy workloads. This increases operational costs and negatively influences the environment.<br>• Reduced QoS due to complex and computationally demanding applications. Emerging applications in 5G, 6G, and beyond require seamless connectivity and ultra-low latency to uphold high standards of QoS. Computation offloading will help in this direction.<br>• Task allocation/scheduling to maximise computational resource utilization. Contemporary networks try to maximise the utilization of computational, storage, and memory resources in an efficient way. The proposed solution excels in this domain. |
| **Competitive advantages** | • Based on open-source software, and thus, no additional costs are implied during the deployment phase.<br>• Multi-parameter optimisation. Most of the existing solutions try to optimise either computation, storage, or memory constraints. The proposed solution considers all three elements, resulting in a more holistic resource optimisation approach.<br>• Cost. The proposed solution will offer competitive price advantages compared to the<br>(pretty) expensive alternatives that exist in the market. |
| **Use model** | • Standalone usage. The product can be used in a standalone way over an existing network infrastructure.<br>• Integration into a scheduling suite. The product can be integrated into an existing task scheduler for large-scale networks and improve its efficiency. |
| **Early Adopters** | Bi2S has initiated contact with partners from the industry (telecommunications and Cloud providers) in order to formulate the requirements for the ML models. Through this process (bilateral online calls and email exchange), Bi2S has gathered information on what type of data |

| | |
|---|---|
| | should the components use, how much resources should utilise, how fast should the decision-making process be conducted, what is an acceptable ML accuracy score in commercial applications, what are the specific needs for these sectors and what type of solutions/algorithms are being used to address those needs at the moment. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | This issue is currently addressed by commercial service orchestrators that redistribute the load of the network to the available nodes/devices. Examples of such products are Kubernetes, HPE Edge Orchestrator, and Intel's Open Edge Platform. Such products utilise mixed-processing elements as they employ both numerical and AI methods to optimise the load distribution and offload tasks to the Edge. |
| **Unique Value Proposition** | Increased QoS within the network, increased computational distribution between Cloud and Edge, Real-time adaptation, computational offloading provisioning under diverse operating scenarios. |
| **Competitors** | Main competitors are:<br><br>• Cloud Native Computing Foundation. Product: Kubernetes.<br>• Hewlett Packard. Product: HPE Edge Orchestrator<br>• Intel. Product: Open Edge Platform<br>• Amazon. Product: AWS step functions<br>• Arm. Product: Edge AI Platform. |
| **Timing** | • Within 1 year: Seek out investment opportunities to increase TRL to 9<br>• Within 2 years: Set up a network of collaborations and connections for promotion activities<br>• Within 3 years: Re-evaluate the business plan and go-to market |
| **IP Strategy** | Background (Reinforcement learning AI models and AI training framework) |

### 5.1.11. ER20: Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing

Table 44: Characterization Table for ER20

| **Result: Exploitation of Blockchain technology powered by AI/ML algorithms in the field of 5G and Edge Computing** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: Artificial Intelligence, Machine Learning, Blockchain<br><br>Objectives: Integration of blockchain and AI/ML algorithms in 5G networks and beyond.<br><br>Advantages: The integration of these technologies will support the development of new services and business models, positioning OTE at the forefront of next-generation network transformation.<br><br>What is new: B-RAN.<br><br>Why is it important: OTE's exploitation goal aims to demonstrate how blockchain and B-RAN architecture have the ability to drive innovation in B5G mobile networks by enabling dynamic network scalability, while simultaneously enhancing trust, security, and privacy. |

| | |
|---|---|
| **Target market/end users** | OTE, as a telecom operator and service provider, offers a wide range of services to end users and corporate clients, such as ICT services, cloud storage and accessm and network connectivity. |
| **End-users needs / problems** | End users perceive the terms of security and privacy when it comes to ICT services. They overestimate their ability to detect hazards and threatsm and they usually have low awareness of privacy concerns, since they are invisible. In this context, it is a matter of trust for the service provider /operator to safeguard their privacy and security. |
| **Competitive advantages** | Integrating Blockchain into B5G network as an extra layer of authentication will provide advanced security and privacy to end users and will enhance OTE's position and strategic competitiveness in the evolving telecommunication market. |
| **Use model** | The solution will be integrated into the already available telecom infrastructure. It could be used as an extra feature on top of the already provided services or as part of consultancy services. Also, possible publications and presentations in high–end conferences and workshops could be made available for the promotion of the above mentioned technology. |
| **Early Adopters** | IT, Integration and Testing Engineers will be responsible for integrating AI/ML algorithms and Blockchain into existing 5G networks. They should ensure seamless deployment and interoperability within existing mobile systems and databases, with minimal service disruption. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | In the competitive landscape of security and privacy, several commercial solutions aim to ensure enhanced trust, privacy, and security without degradations in the overall user experience, such as firewalls and PQ Security technologies. |
| **Unique Value Proposition** | OTE aims to exploit the outcomes of the NANCY project by integrating blockchain powered by AI/ML algorithms into 5G and edge computing environments, with a focus on evaluating their efficiency and testing overall network performance. |
| **Competitors** | • Other service providers<br>• Telecom Operators |
| **Timing** | This information cannot be available. The timing for a new service or a new feature launch depends on several parameters such as technical maturity of the proposed solution, market needs, upper management strategic planning and decisions, competitors, etc. |
| **IP Strategy** | None |

### 5.1.12. ER22: Smart Pricing Policies

Table 45: Characterization Table for ER22

| **Result: Smart Pricing Policies** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: A smart pricing module integrated into NANCY's architecture.<br><br>Objectives: To dynamically determine optimal pricing for provided services. |

| | |
|---|---|
| | Advantages: Optimised and dynamic pricing.<br><br>What is new: Integrating auction and game theoretic methods into the pricing model.<br><br>Why is it important: Creation of new monetary incentives for providers and users. |
| **Target market/end users** | Private sector and Researchers |
| **End-users needs / problems** | Needs:<br>• Efficient allocation of network resources to cope with fluctuating demand.<br>• Dynamic and fair pricing mechanisms that reflect real-time conditions and reduce the need for manual tariff adjustments.<br>• Automated optimisation of resource-sharing stakeholders, reducing operational overhead.<br>• Increased resilience and adaptability, ensuring networks can adjust pricing and allocation during unexpected demand spikes or special events.<br><br>Problems:<br>• Inability to efficiently handle volatile or unpredictable traffic patterns under static pricing models, leading to congestion or wasted capacity.<br>• Complexity of manually managing resource allocation, especially in multi-operator or multi-service deployments.<br>• Limited visibility into network demand drivers, making it difficult to set prices that are both competitive and sustainable.<br>• Risk of unfair or inefficient outcomes when traditional pricing fails to reflect actual usage or real-time network conditions.<br>• Difficulty balancing competing objectives such as fairness, efficiency, revenue optimization, and QoS guarantees. |
| **Competitive advantages** | Gain creators:<br><br>• Transforms static networks into dynamic marketplaces, enabling real-time pricing that better reflects demand and resource availability than traditional policy-based or fixed-tariff approaches.<br>• Supports multi-tenant environments natively, giving both operators and tenants clearer control, transparency, and customisation compared with standard slicing orchestrators.<br>• Reduces dependence on manual configuration, offering automated optimisation that adapts as the ecosystem evolves.<br><br>Pain relievers:<br>• Addresses volatility more effectively than competitors' static or semi-dynamic pricing, preventing congestion or underuse during sudden demand shifts.<br>• Reduces operational complexity by automating decisions typically requiring manual tuning or multi-team coordination.<br>• Mitigates integration friction through a modular architecture that plugs into existing telemetry, identity, QoS, and settlement systems more easily than monolithic vendor solutions.<br>• Protects smaller players and new entrants, offering mechanisms that prevent marketplace domination. |

| | |
|---|---|
| **Use model** | As the SPM introduces a dynamic, data-driven approach to allocating and monetizing network resources, its primary use model is to integrate it as an add-on service to existing network management and orchestration platforms. Operators can deploy it as a modular component that enhances their ability to price, auction, and govern capacity in multi-tenant or high-variability environments. Moreover, SPM can be offered through technology transfer or licensing agreements to vendors building next-generation 5G/6G resource controllers. |
| **Early Adopters** | • Mobile Network Operators<br>• Private Network Operators<br>• Research Testbeds<br>• Researchers |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | •Static or rule-based pricing models used by operators to predefine service costs, offering predictable but inflexible pricing that does not adapt to real-time network conditions.<br>•Centralized orchestration platforms are employed in current telecom environments to allocate resources based on fixed policies or thresholds, limiting scalability in multi-provider ecosystems. |
| **Unique Value Proposition** | The determined price is tailored to the specific service, aiming to maximise revenue while minimising potential profit loss. |
| **Competitors** | Big technology vendors and network solution providers are exploring mechanisms that partially overlap with SPM, mainly through policy-driven network slicing, automated orchestration, or cloud-style resource pricing. Their main strength is the maturity of their platforms and their large integration ecosystems. However, these solutions typically rely on static or semi-dynamic pricing models, which limit their ability to capture real-time demand or operate as true marketplaces. |
| **Timing** | The core concepts behind SPM, namely dynamic auctions, AI-assisted pricing, and multi-tenant resource markets, are technically feasible today, but widespread adoption still depends on ecosystem readiness. Many operators are currently undergoing cloud-native transformations, which creates a favorable context for early experimentation. A first functional prototype of SPM could realistically be demonstrated within 12–18 months, assuming access to testbed infrastructure. Market-ready integration with commercial networks is expected to take longer (approximately 3-5 years), as it requires alignment with operational processes, regulatory considerations, and marketplace governance models. |
| **IP Strategy** | None |

### 5.1.13. ER23: Big Data Platform for self-healing and self-recovery

Table 46: Characterization Table for ER23

| **Result: Big Data Platform for self-healing and self-recovery** | |
|---|---|
| | Input from Beneficiary |
| **Description** | The Big Data Platform provides end-to-end management of data required by self-healing and self-recovery algorithms. Its core features include high-throughput ingestion of extreme-volume telemetry, low-latency, and inference at the edge, and support for a multi-broker architecture. The primary objective is to implement scalable data management mechanisms that maintain performance as volumes grow, while preserving data locality. |

| | |
|---|---|
| | By enabling automated detection, diagnosis, and remediation workflows, the platform improves the reliability and availability of 5G and B5G networks and helps operators meet Service Level Objectives. |
| **Target market/end users** | Industry / Telecom Operators |
| **End-users needs / problems** | •Rapid, accurate detection of faults and performance degradations across distributed 5G/B5G and private network sites.<br>•Fast, automated recovery to meet stringent SLOs. |
| **Competitive advantages** | •Multi-broker architecture enabling distributed processing while keeping data local.<br>•Low-latency decisions at the edge reduce decision latency compared with cloud-only platforms. |
| **Use model** | •Available as a managed service for operators seeking low-friction adoption.<br>•On-premises software package for private networks and sensitive industrial deployments. |
| **Early Adopters** | •Operator willing to run pilots in selected markets or slices to improve availability.<br>•Industrial and private 5G adopters with strict uptime and latency requirements. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | •Vendor-native network management systems with rule-based automation (often cloud-centric).<br>•Centralized big data/observability platforms that consolidate data in the cloud but face privacy, latency, and bandwidth limits for edge scenarios.<br>•Ad-hoc or vertical-specific monitoring stacks (Prometheus, ELK, Grafana) combined with manual incident response and human-in-the-loop remediation. |
| **Unique Value Proposition** | Enable autonomous, data-driven self-healing of 5G/B5G networks at extreme scale by combining distributed data management, multi-broker architecture, and validated edge operation. |
| **Competitors** | •Centralized observability platforms (commercial cloud observability providers) with scalable cloud analytics.<br>•Open-source monitoring stacks and processing (e.g., Prometheus/ELK). |
| **Timing** | Expected timing: Pilot deployments within 12–24 months depending on integration scope. |
| **IP Strategy** | None |

### 5.1.14. ER24: A framework for data and concept drift detection in 6G networks

Table 47: Characterization Table for ER24

| **Result: A framework for data and concept drift detection in 6G networks** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: End-to-end ML pipeline, data processing components, ML algorithms, data drift detection framework, and decision-making model.<br><br>Objectives: To improve the State-of-the-art in the corresponding domains, to increase the efficiency of ML models, to achieve near-optimal performance in data/concept drift detection tasks, in next-generation 6G networks.<br><br>Advantages: Real-time decision-making on whether an AI model should be retrained or not. Beyond SotA performance. Consideration of multiple |

| | |
|---|---|
| | factors for the decision-making process. Increase the efficiency of maintaining AI models.<br><br>What is new: Existing methodologies consider only a few factors to assess whether an AI model should be retrained or not, given new input data. NANCY's data drift and concept drift detectors employ a complex yet highly computationally efficient mechanism to integrate several parameters into the mix. This highly increases the assessment accuracy and perfectly situates the result under investigation to be used in production environments.<br><br>Why is it important: This exploitable result not only advances the state-of-the-art of the AI models for data drift and concept drift detection, but also provides a real solution for next generation 5G/6G networks. The algorithms are designed to achieve near-optimal performance in real-world scenarios with real-world data. The ultimate gains translate to direct energy consumption (from unnecessary model re-training operations) and to increased model quality. |
| **Target market/end users** | Industry |
| **End-users needs / problems** | • Increase in energy consumption of modern AI models due to increased size and complexity. This increases the model re-training costs in terms of time, computational resources, and energy and thus negatively influences the environment.<br>• Reduced model quality due to new data. Newly collected data may come from different data distributions (compared with the model's training dataset) and negatively influence the model quality. The question "when should the model be retrained" is imperative to be answered to maintain modern AI models. |
| **Competitive advantages** | • Based on open-source software, and thus, no additional costs are implied during the deployment phase.<br>• Cost. The proposed solution will offer competitive price advantages compared to the alternatives that exist in the market.<br>• Performance. The proposed solution achieves high-end performance (in terms of detection accuracy) that situates it at the top of the list.<br>• Interoperability. The proposed solution is compatible with any type of Deep Learning model. |
| **Use model** | • Standalone usage. The product can be used in a standalone way over an existing network infrastructure.<br>• Integration into an AI management or MLOps platform. The product can be integrated into an existing solution to improve its efficiency. |
| **Early Adopters** | Bi2S has initiated contact with partners from the Industry (telecommunications and Cloud providers) in order to formulate the requirements for the ML models. Through this process (bilateral online calls and email exchange), Bi2S has gathered information on what type of data should the components use, how much resources should utilise, how fast should the decision-making process be conducted, what is an acceptable ML accuracy score in commercial applications, what are the specific needs for these sectors and what type of solutions/algorithms are being used to address those needs at the moment. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |

| | |
|---|---|
| **Alternative Solution** | Main alternative solutions (as commercial products) include Evidently AI, Alibi Detect, WhyLabs, and Fiddler AI. |
| **Unique Value Proposition** | Increased QoS within the network, high energy-efficiency when AI models are retrained, real-time adaptation, increased AI model quality, and framework generalisability to other verticals. |
| **Competitors** | Main competitors are:<br><br>• Evidently AI. Product: ML monitoring service<br>• WhyLabs (acquired by Apple). Product: N/A<br>• Fiddler AI. Product: AI observability |
| **Timing** | • Within 1 year: Seek out investment opportunities to increase TRL to 9, or to integrate the solution into an existing platform<br>• Within 2 years: Set up a network of collaborations and connections for promotion activities<br>• Within 3 year: Re-evaluate the business plan and go-to market |
| **IP Strategy** | Background (Reinforcement learning AI models and AI training framework) |

### 5.1.15. ER28: Central Management Domain

Table 48: Characterization Table for ER28

| **Result: Central Management Domain** | |
|---|---|
| | Input from Beneficiary |
| **Description** | Main features: A suite of technical tools to automate and simplify integration, testing, deployment, and orchestration among NANCY components.<br><br>Objectives: The NANCY Central Management Domain Deployment and Orchestration incorporates Continuous Integration and Continuous Delivery, coupled with a service Orchestrator to support the efficient central management of NANCY component deployments.<br><br>Advantages: The main advantages are a reduction in development time, simplified code management, automated testing, improved orchestration, and deployment. In cases of bugs and failures, the use of a CI/CD pipeline can lead to shorter time to repair (MTTR) and allow easier tracking of bugs. Tightly integrated multi-domain orchestration (MAESTRO) enables seamless deployment across RAN, core, transport, and slicing domains while minimizing manual errors and accelerating service roll-out.<br><br>What is new: Improved cloud service and microservice development, integration, and orchestration.<br><br>Why is it important: CI/CD allows an organization to achieve better performance, faster and more cost-efficient operations, and security by design. CI/CD has been directly linked with reductions in an organization's operational expenditures (OPEX). Furthermore, by integrating CI/CD with a novel solution such as MAESTRO, we create the NANCY Central Management Domain deployment and orchestration platform that allows seamless multi-domain deployment, while minimizing manual errors and accelerating service roll-out. |
| **Target market/end users** | The tools are geared towards organisations that develop, maintain, and deploy code in their (or their clients') operations. It lowers the barriers for service providers to monetise their services, enables MNOs to capitalize on |

| | |
|---|---|
| | slice offerings, as well as simplify infrastructure/resource sharing. It can also be a low-cost alternative to large vendor solutions that help avoid customer lock-in. This makes it particularly attractive for smaller deployments (such as privately operated networks) and early adopters. |
| **End-users needs / problems** | While domain-specific solutions exist and can offer deep optimization per domain, these tend to create silo conditions that complicate the coordination of end-to-end (E2E) services. The NANCY Management Domain solution for deployment and orchestration does not suffer from limited visibility across domains, and as such, it can be a more comprehensive, holistic solution. |
| **Competitive advantages** | By combining cross-domain orchestration with enterprise-level CI/CD automation, the NANCY Central Management domain reaps the benefits of both high automation with cloud-native scalability and cross-domain visibility. |
| **Use model** | The main components of the NANCY Central Management Domain deployment and orchestration platform may be marketed as standalone services or as a single integrated platform. Service contracts may include deployment, maintenance, and/or consulting services. |
| **Early Adopters** | Enterprises deploying private networks, telco providers that deploy any mode of infrastructure sharing (for example, MVNOs, etc.), system integrators (such as Netcompany, which already deploys such systems), and cloud-native DevOps teams in multi-stakeholder environments. |
| **Adopters' problems/needs** | Same with the problems/needs of end users. |
| **Alternative Solution** | While alternative solutions exist from large vendors (such as VMWare, ZTE, Ericsson, etc.), these also tend to create lock-in conditions for their clients, often requiring them to purchase and operate full stacks of their software, and making migration difficult. The NANCY Central Management Domain components may also be marketed as standalone solutions, in order to combat this problem. The selection of solutions can be more flexible and depends on the customer's integration needs and solution maturity. We expect that this flexibility can be a strength that differentiates our offering from those of large vendors. |
| **Unique Value Proposition** | The INTRA CI/CD pipeline is used to help organisations consistently deliver code that meets high-quality standards. UBI's Maestro service orchestrator deals with the deployment and orchestration of services. The Orchestration and CI/CD system services are hosted in the central NANCY Kubernetes cluster, which serves a dual purpose: (a)To establish a common development and testing environment for containerized NANCY components, aiming to verify their functionalities and ensure integration among various components and services prior to deployment in operational settings (separate Kubernetes clusters at NANCY testbeds/demonstrators), (b) To host NANCY Management domain services, which include as mentioned above orchestration services that are accessible across different operational environments via secure VPN tunnels. The CI/CD Platform provides DevOps automation capabilities through the configuration of software build, testing, and deployment pipelines for the different NANCY components and services. The NANCY CI/CD system is connected to the central NANCY Kubernetes cluster, supporting the development and testing of NANCY components. The CI/CD system services are also securely connected to the Kubernetes environments of the different NANCY testbeds and demonstrators to control the deployments of NANCY containerized components and services either |

| | |
|---|---|
| | directly through the CI server or through the Maestro service orchestrator. Maestro is a cloud-native service orchestrator designed to manage the lifecycle of end-to-end services across geo-distributed infrastructures. It facilitates automated deployment, scaling, and lifecycle management of microservices-based applications. Maestro integrates with Kubernetes and OpenStack environments to deploy services via containers or virtual machines. Maestro operates in environments involving Kubernetes clusters and integrates with edge and core infrastructures. It uses Kubernetes-as-a-Service (K8s-aaS) for resource orchestration. Container images and Helm charts are managed in the NANCY Harbor container registry, ensuring smooth retrieval of artifacts during deployment. Service providers onboard containerized services, which are subsequently deployed via Kubernetes. |
| **Competitors** | The main competitors are large vendors with their own solutions for cross-domain or domain-specific deployment and orchestration. While there are advantages to the "one-stop-shop" approach, the solutions marketed by large vendors can also be costly and lock-in their customers by creating dependencies within their software and hardware product lines (i.e., bundling them with cloud platforms, cloud hardware, custom APIs, etc.). Open alternatives, such as the NANCY Management Domain components, mitigate this through using open standards, providing flexibility both as an alternative and as an argument against vendor dominance in the 5G/6G sector. |
| **Timing** | The main challenge in cross-domain operations is the high starting effort to set up the toolchain. Other open, cross-domain orchestration solutions such as Itential, report a period of 3-6 months upfront for initial setup, with significant later gains (in the case of Telecom Italia deployment). While the NANCY CI/CD can vastly automate the process, there can be further improvement that can set apart the NANCY Central Management Domain from its competitors. The introduction of new Artificial Intelligence powered improvements by INTRA within its pipeline can further reduce delivery and is expected to reach full maturity in 18-24 months. Once the initial setup is performed, the platform as a whole is expected to drastically accelerate enterprise services in 5G/6G. |
| **IP Strategy** | Background: Maestro is IP-protected under copyright but will become open source in the future.<br><br>Foreground: In terms of the CI/CD platform, INTRA utilizes copyright and, in some cases, trade secrets agreements. |

## 5.2. Fuzzy Analytical Hierarchy Process

### 5.2.1. Criteria and Sub-Criteria Selection

The initial set of criteria influencing the technological evolution and market potential of NANCY was identified through workshops and expert consultations among project partners. Three main criteria and their corresponding sub-criteria were defined as follows:

**Criterion 1: Scalability & Ecosystem Fit** focuses on NANCY's ability to operate efficiently at scale and integrate with broader B5G ecosystems. It is divided into three sub-criteria:

1. **AI Reusability & Self-Evolution:** The ability of AI models and data to be reused, scaled, and continuously improved through self-evolving mechanisms or distributed learning workflows.

2. **Interoperability & Deployment Flexibility:** Integration with existing 5G/B5G/RAN architectures, cloud-native platforms, open interfaces, and multi-RAT systems, enabling diverse deployments.
3. **Scalability & Low-Maintenance Operation:** Technologies that scale with demand while minimizing manual intervention, ensuring cost-efficient operation at large network scales.

**Criterion 2: Trust & Security** addresses the foundational mechanisms ensuring trust, privacy, and resilience in NANCY's intelligent network operations. This criterion includes four sub-criteria:

1. **Blockchain-Based Trust & Verifiability:** Decentralized trust mechanisms and tamper-resistant logging using blockchain.
2. **Quantum-Safe Security & Privacy:** Protection of communications and identities through quantum-resistant cryptography and advanced privacy techniques.
3. **Explainable & Transparent AI Decisions:** Ensures AI-based orchestration and decision-making processes are interpretable and transparent to users and operators.
4. **Threat Detection & Attack Resilience:** Advanced anomaly detection and resilience mechanisms that maintain secure operation under adversarial or fault conditions.

**Criterion 3: Performance & Reliability** captures NANCY's ability to deliver high performance and dependable operation in dynamic environments. Criterion 3 is composed of four sub-criteria:

1. **Edge Offloading & Low-Latency Execution:** Efficient computation offloading to edge nodes to minimize latency and improve responsiveness.
2. **Service Continuity & Resilience:** Reliable operation under dynamic network conditions, supported by self-healing and continuity mechanisms.
3. **Network Efficiency & Latency Reduction:** Optimized data flows and RAN performance improvements to enhance efficiency and responsiveness.
4. **Resource & Energy Optimization:** Intelligent management of computational and radio resources to enable sustainable, energy-efficient operation.

The full hierarchical model for NANCY's Fuzzy AHP is presented in Figure 6. At the top level lies the overall objective, to identify the key technological factors driving NANCY's market adoption. The second level represents the main criteria (Scalability & Ecosystem Fit, Trust & Security, Performance & Reliability), and the third level represents their associated sub-criteria.

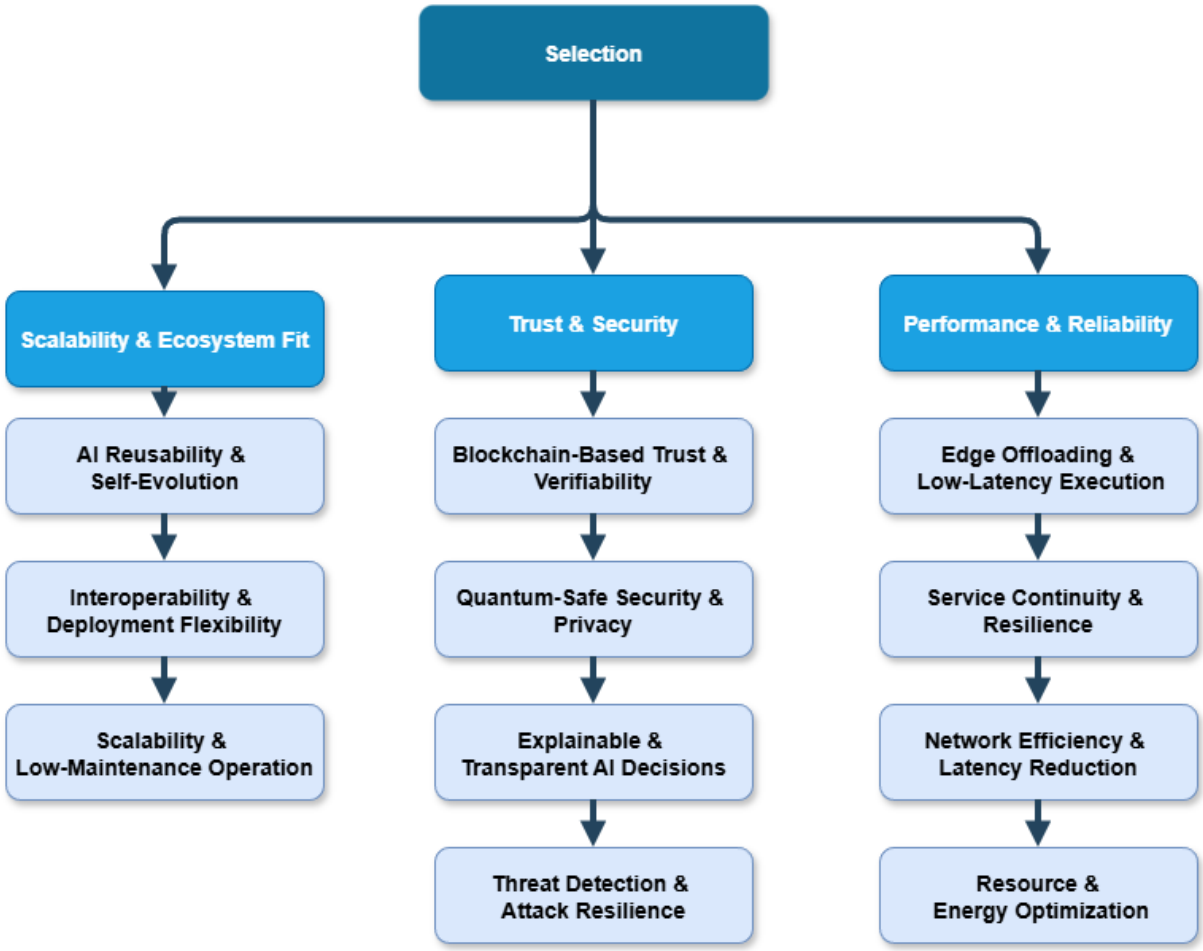



Figure 6: AHP Criteria and Sub-criteria Hierarchy

### 5.2.2.Survey Description

To conduct the Fuzzy AHP, a dedicated web-based questionnaire was developed and distributed among experts from the NANCY consortium as well as external specialists in the fields of B5G, AI, edge computing, blockchain, and network security.

The purpose of the survey was to capture expert judgments regarding the relative importance of the defined criteria and sub-criteria that influence the market attractiveness and technological evolution of NANCY.

A total of 35 valid responses were collected. Respondents represented a diverse mix of expertise, including network operators, research institutions, and technology providers, ensuring a balanced view of the market and technological perspectives relevant to B5G systems.

The questionnaire followed the principles of the Fuzzy AHP and was structured in two main parts:

1. **Pairwise Comparison of Main Criteria**:
   Participants were first asked to compare the three main criteria, Scalability & Ecosystem Fit, Trust & Security, and Performance & Reliability, in pairs, indicating which one they considered more important for driving NANCY's market adoption.
2. **Pairwise Comparison of Sub-Criteria**:
   After completing the main criteria comparison, participants evaluated the sub-criteria within each category (e.g., under Trust & Security, they compared Blockchain-Based Trust & Verifiability with Quantum-Safe Security & Privacy, and so on).

For each pair, participants expressed their preferences using qualitative terms that reflected the strength of importance based on their professional judgment and experience. The available linguistic options were: Equally important, Slightly more important, Moderately more important, Extremely more important.

These qualitative judgments were automatically converted into triangular fuzzy numbers according to predefined fuzzy scales. This allowed participants to provide nuanced opinions without requiring numerical input, while still enabling mathematical aggregation and analysis.

To ensure consistency and comprehension across all participants, the survey included a brief introductory section explaining:

- The overall objective of the exercise.
- The meaning of each linguistic term used in pairwise comparisons.
- The principle that only the relative importance between two factors should be assessed, not their absolute performance.
- The recommendation is to rely on professional judgment, prior experience, and perception of future technological and market trends.

Each participant completed the survey individually and electronically, completely anonymously.

Figure 7, Figure 8, Figure 9, and Figure 10 depict the questionnaire that was distributed.

## NANCY Driving Technology Factors

This questionnaire is part of the **NANCY project**, a Horizon Europe and SNS JU research initiative developing intelligent, secure, and scalable network technologies for Beyond 5G systems. The purpose of this survey is to **identify and prioritize the technological factors** that are expected to influence NANCY's evolution and its eventual market adoption.

You are invited to contribute **your expert judgment** to evaluate how different technical capabilities relate to **market attractiveness**. You do not need to be familiar with the specific NANCY solutions, only with the broader technology domains in which the project operates, such as Beyond 5G and Radio Access Networks, Artificial Intelligence, edge computing, blockchain, and advanced security / quantum-safe communications. Your insights on these domains and their market potential will help us guide future **NANCY development and exploitation priorities**.

You will be asked to **compare pairs of factors** and indicate which one you believe is more important and to what degree based on your professional judgment and experience. Your responses will be expressed using **qualitative terms** that reflect the strength of your preference: **'Extremely more important'**, **'Moderately more important'**, **'Slightly more important'**, and **'Equally important'**.

The **example answer below** translates to: Performance & Reliability is Moderately more important than Trust & Security based on the current trends in the market and technologies.

| | Extremely more important | Moderately more important | Slightly more important | Equally important | Slightly more important | Moderately more important | Extremely more important | |
|---|---|---|---|---|---|---|---|---|
| **Performance & Reliability** | ○ | ◉ | ○ | ○ | ○ | ○ | ○ | **Trust & Security** |

*Example answer*

Below you can find the main criteria and their respective sub-criteria, each accompanied by a short explanation. The **main criteria** represent the **broad dimensions** that influence the market attractiveness of NANCY's technologies, while the **sub-criteria** describe **more specific factors** within each dimension.

**Scalability & Ecosystem Fit**

| Sub-criterion | Explanation |
|---|---|
| AI Reusability & Self-Evolution | The ability of AI models and data to be reused, scaled and continuously improved through self-evolving mechanisms or distributed learning workflows. |
| Interoperability & Deployment Flexibility | The ability of the system to integrate with existing 5G/B5G/RAN architectures, cloud-native platforms, open interfaces and multi-RAT systems, supporting diverse deployments. |
| Scalability & Low-Maintenance Operation | Technology that scales with demand while minimizing the need for manual intervention, enabling efficient operation and lower maintenance cost at larger network scales. |

Figure 7: AHP Questionnaire (1)

**Trust & Security**

| Sub-criterion | Explanation |
|---|---|
| Blockchain-Based Trust & Verifiability | Covers decentralized trust mechanisms, verifiable interactions, and tamper-resistant logging enabled through blockchain components. |
| Quantum-Safe Security & Privacy | The ability to protect communications and identities using quantum-resistant cryptography and enhanced privacy mechanisms. |
| Explainable & Transparent AI Decisions | Understandable, interpretable and transparent to operators AI models and orchestration decisions, enhancing trust in automated control loops. |
| Threat Detection & Attack Resilience | Capabilities for detecting anomalies, preventing attacks and maintaining secure operation under adversarial conditions. |

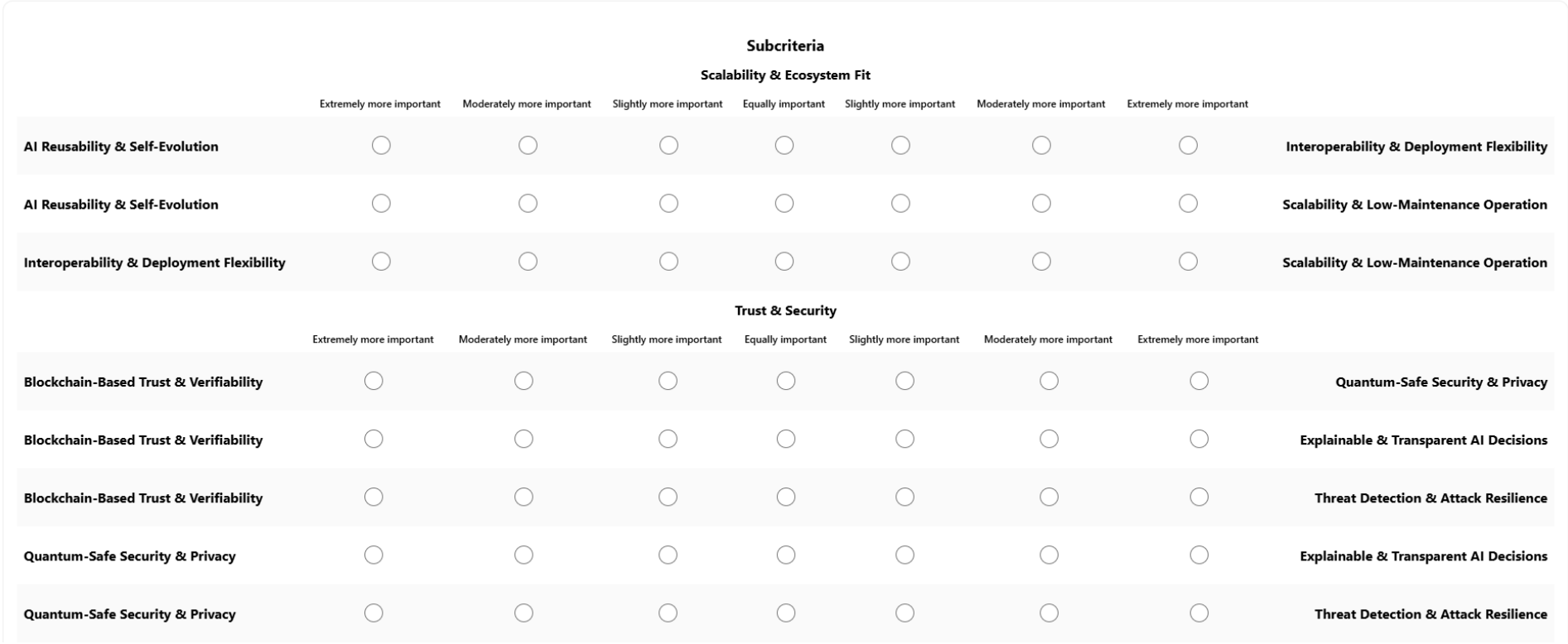
**Performance & Reliability**

| Sub-criterion | Explanation |
|---|---|
| Edge Offloading & Low-Latency Execution | Efficiently offload computation to edge nodes to reduce latency and improve responsiveness. |
| Service Continuity & Resilience | The system's ability to maintain reliable operation under dynamic conditions, faults, or network changes. Includes robustness, self-healing, and continuity mechanisms. |
| Network Efficiency & Latency Reduction | Improved network performance through optimized data flows, semantic communications, or optimized RAN behavior. |
| Resource & Energy Optimization | Efficiently use computational, radio and energy resources, contributing to sustainable and cost-effective network operation. |

**Main Criteria**

| | Extremely more important | Moderately more important | Slightly more important | Equally important | Slightly more important | Moderately more important | Extremely more important | |
|---|---|---|---|---|---|---|---|---|
| **Performance & Reliability** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Trust & Security** |
| **Performance & Reliability** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Scalability & Ecosystem Fit** |
| **Trust & Security** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Scalability & Ecosystem Fit** |

Figure 8: AHP Questionnaire (2)



**Subcriteria**

**Scalability & Ecosystem Fit**

| | Extremely more important | Moderately more important | Slightly more important | Equally important | Slightly more important | Moderately more important | Extremely more important | |
|---|---|---|---|---|---|---|---|---|
| **AI Reusability & Self-Evolution** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Interoperability & Deployment Flexibility** |
| **AI Reusability & Self-Evolution** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Scalability & Low-Maintenance Operation** |
| **Interoperability & Deployment Flexibility** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Scalability & Low-Maintenance Operation** |

**Trust & Security**

| | Extremely more important | Moderately more important | Slightly more important | Equally important | Slightly more important | Moderately more important | Extremely more important | |
|---|---|---|---|---|---|---|---|---|
| **Blockchain-Based Trust & Verifiability** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Quantum-Safe Security & Privacy** |
| **Blockchain-Based Trust & Verifiability** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Explainable & Transparent AI Decisions** |
| **Blockchain-Based Trust & Verifiability** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Threat Detection & Attack Resilience** |
| **Quantum-Safe Security & Privacy** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Explainable & Transparent AI Decisions** |
| **Quantum-Safe Security & Privacy** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | **Threat Detection & Attack Resilience** |

Figure 9: AHP Questionnaire (3)

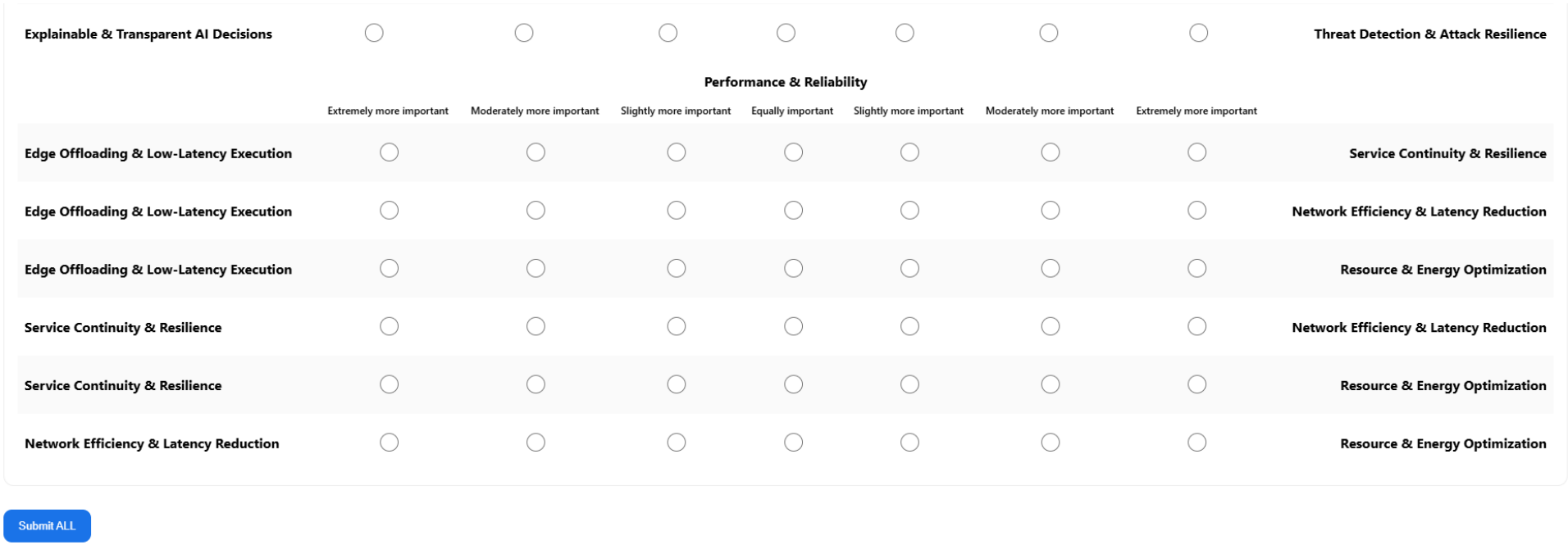



Figure 10: AHP Questionnaire (4)

### 5.2.3.Derivation of Final Results

After the collection of all expert survey responses, the methodology outlined in Section 2 was systematically applied. As a preliminary step, all individual expert responses with a consistency ratio exceeding 0.1 were discarded to ensure the reliability of the judgments; a total of four responses were excluded at this stage. Subsequently, the remaining individual pairwise comparison matrices provided by the experts were aggregated for each criterion using fuzzy triangular numbers, in accordance with the Fuzzy Analytic Hierarchy Process.

Table 49, Table 50, Table 51, and Table 52 present the aggregated fuzzy comparison values for each criteria category, reflecting the collective judgment of all participating experts. These aggregated matrices represent the consolidated importance of each criterion while accounting for uncertainty and subjectivity inherent in human evaluations.

Subsequently, the fuzzy weights of the criteria were computed using the FAHP weighting procedure described in Section 2. Table 53, Table 54, Table 55, and Table 56 show the fuzzy weights for each criterion. The resulting fuzzy weights were then transformed into crisp values through the defuzzification process, enabling direct comparison among criteria.

Table 57, Table 58, Table 59, and Table 60 summarize the final ranking of the criteria based on their defuzzified weights. This ranking reflects the relative importance of each criterion as perceived by the expert group and serves as the basis for subsequent analysis and decision-making.

*Aggregated fuzzy pairwise comparison matrices (component-wise mean)*

Table 49: Aggregated Fuzzy Pairwise Comparison Matrix for the Main Criteria

| Main Criterion | Performance & Reliability | Trust & Security | Scalability & Ecosystem Fit |
|---|---|---|---|
| Performance & Reliability | (1.0000, 1.0000, 1.0000) | (0.7690, 0.9533, 1.2024) | (1.5076, 2.2381, 3.0000) |
| Trust & Security | (1.2338, 1.6348, 2.0714) | (1.0000, 1.0000, 1.0000) | (1.7457, 2.5714, 3.4286) |
| Scalability & Ecosystem Fit | (0.4790, 0.6510, 0.9405) | (0.4029, 0.5829, 0.8929) | (1.0000, 1.0000, 1.0000) |

Table 50: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Scalability & Ecosystem Fit

| Criterion | AI Reusability & Self-Evolution | Interoperability & Deployment Flexibility | Scalability & Low-Maintenance Operation |
|---|---|---|---|
| AI Reusability & Self-Evolution | (1.000, 1.000, 1.000) | (0.665, 0.925, 1.288) | (0.806, 1.187, 1.702) |
| Interoperability & Deployment Flexibility | (1.400, 2.038, 2.712) | (1.000, 1.000, 1.000) | (1.282, 2.038, 2.846) |
| Scalability & Low-Maintenance Operation | (0.974, 1.512, 2.115) | (0.482, 0.731, 1.144) | (1.000, 1.000, 1.000) |

Table 51: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Trust & Security

| Criterion | Performance & Reliability | Trust & Security | Scalability & Ecosystem Fit | Threat Detection & Attack Resilience |
|---|---|---|---|---|
| Blockchain-Based Trust & Verifiability | (1.0000, 1.0000, 1.0000) | (0.8624, 1.2276, 1.6700) | (0.8924, 1.3872, 1.9700) | (0.5256, 0.6280, 0.8200) |
| Quantum-Safe Security & Privacy | (1.0160, 1.4196, 1.9000) | (1.0000, 1.0000, 1.0000) | (0.8588, 1.3264, 1.9200) | (0.7456, 1.0688, 1.4600) |
| Explainable & Transparent AI Decisions | (1.0488, 1.5876, 2.2300) | (0.7992, 1.2928, 1.8800) | (1.0000, 1.0000, 1.0000) | (0.8020, 1.0956, 1.4800) |
| Threat Detection & Attack Resilience | (1.6132, 2.2600, 2.9200) | (1.2092, 1.6532, 2.1800) | (1.1896, 1.6596, 2.1800) | (1.0000, 1.0000, 1.0000) |

Table 52: Aggregated Fuzzy Pairwise Comparison Matrix for the Sub-Criteria under Performance & Reliability

| Criterion | Edge Offloading & Low-Latency Execution | Service Continuity & Resilience | Network Efficiency & Latency Reduction | Resource & Energy Optimization |
|---|---|---|---|---|
| Edge Offloading & Low-Latency Execution | (1.0000, 1.0000, 1.0000) | (0.7865, 1.2995, 1.9250) | (0.8950, 1.1915, 1.5750) | (0.6570, 0.8830, 1.2500) |
| Service Continuity & Resilience | (0.8405, 1.3580, 2.0000) | (1.0000, 1.0000, 1.0000) | (1.0410, 1.5830, 2.2000) | (0.9865, 1.4265, 1.9375) |
| Network Efficiency & Latency Reduction | (0.8745, 1.2080, 1.6000) | (0.7485, 1.1180, 1.6125) | (1.0000, 1.0000, 1.0000) | (0.7445, 1.0665, 1.5250) |
| Resource & Energy Optimization | (0.9995, 1.5250, 2.1000) | (0.9195, 1.2765, 1.7375) | (0.8785, 1.3665, 1.9250) | (1.0000, 1.0000, 1.0000) |

*Fuzzy weights*

Table 53: Fuzzy Weights for the Main Criteria

| Criterion | Fuzzy Weight (TFN) |
|---|---|
| Performance & Reliability | (0.3586, 0.3604, 0.3579) |
| Trust & Security | (0.4355, 0.4476, 0.4472) |
| Scalability & Ecosystem Fit | (0.2059, 0.1920, 0.1949) |

Table 54: Fuzzy Weights for the Sub-Criteria under Scalability & Ecosystem Fit

| Criterion | Fuzzy Weight (TFN) |
|---|---|
| AI Reusability & Self-Evolution | (0.287, 0.272, 0.269) |
| Interoperability & Deployment Flexibility | (0.428, 0.444, 0.443) |
| Scalability & Low-Maintenance Operation | (0.285, 0.284, 0.288) |

Table 55: Fuzzy Weights for the Sub-Criteria under Trust & Security

| Criterion | Fuzzy Weight (TFN) |
|---|---|
| Blockchain-Based Trust & Verifiability | (0.2108, 0.2059, 0.2052) |
| Quantum-Safe Security & Privacy | (0.2326, 0.2337, 0.2360) |
| Explainable & Transparent AI Decisions | (0.2345, 0.2415, 0.2477) |
| Threat Detection & Attack Resilience | (0.3221, 0.3190, 0.3112) |

Table 56: Fuzzy Weights for the Sub-Criteria under Performance & Reliability

| Criterion | Fuzzy Weight (TFN) |
|---|---|
| Edge Offloading & Low-Latency Execution | (0.2323, 0.2266, 0.2265) |
| Service Continuity & Resilience | (0.2691, 0.2781, 0.2811) |
| Network Efficiency & Latency Reduction | (0.2343, 0.2276, 0.2260) |
| Resource & Energy Optimization | (0.2642, 0.2677, 0.2664) |

*Ranking after defuzzification*

Table 57: Ranking of the Main Criteria

| Criterion | Defuzzified Weight | Ranking |
|---|---|---|
| **Performance & Reliability** | 0.358943 | **#2** |
| **Trust & Security** | 0.443420 | **#1** |
| **Scalability & Ecosystem Fit** | 0.197637 | **#3** |

Table 58: Ranking of the Sub-Criteria under Scalability & Ecosystem Fit

| Criterion | Defuzzified Weight | Ranking |
|---|---|---|
| **AI Reusability & Self-Evolution** | 0.276246 | **#3** |
| **Interoperability & Deployment Flexibility** | 0.438197 | **#1** |
| **Scalability & Low-Maintenance Operation** | 0.285557 | **#2** |

Table 59: Ranking of the Sub-Criteria under Trust & Security

| Criterion | Defuzzified Weight | Ranking |
|---|---|---|
| **Blockchain-Based Trust & Verifiability** | 0.207289 | **#4** |
| **Quantum-Safe Security & Privacy** | 0.234096 | **#3** |
| **Explainable & Transparent AI Decisions** | 0.241221 | **#2** |
| **Threat Detection & Attack Resilience** | 0.317393 | **#1** |

Table 60: Ranking of the Sub-Criteria under Performance & Reliability

| Criterion | Defuzzified Weight | Ranking |
|---|---|---|
| **Edge Offloading & Low-Latency Execution** | 0.22846603 | **#4** |
| **Service Continuity & Resilience** | 0.27612203 | **#1** |
| **Network Efficiency & Latency Reduction** | 0.22929402 | **#3** |
| **Resource & Energy Optimization** | 0.26611792 | **#2** |

### 5.2.4.Interpretation of Results

*Ranking of the Main Criteria*

**Trust & Security — Defuzzified Weight: 0.443420 (Rank #1)**

Trust & Security emerges as the most influential criterion affecting both the technological trajectory and the market acceptance of NANCY. This result indicates that project partners perceive **trustworthiness, robustness against attacks, and assurance mechanisms** as fundamental enablers for adoption. From a market perspective, insufficient trust or security would significantly hinder deployment in real-world environments, particularly in regulated or mission-critical domains. Consequently, technological evolution efforts for NANCY are expected to prioritize secure-by-design architectures and strong trust guarantees.

**Performance & Reliability — Defuzzified Weight: 0.358943 (Rank #2)**

Performance & Reliability ranks second, underscoring the importance of **stable, predictable, and efficient system behavior** in sustaining NANCY's competitiveness. While high performance is essential for user satisfaction and operational feasibility, the ranking suggests that performance improvements are meaningful only insofar as they do not compromise security and trust. Reliability-related attributes such as continuity of service and fault tolerance are therefore key contributors to NANCY's perceived value in the market.

**Scalability & Ecosystem Fit — Defuzzified Weight: 0.197637 (Rank #3)**

Although ranked third, Scalability & Ecosystem Fit remains a critical dimension for long-term market potential. The lower weight reflects expert consensus that ecosystem alignment and scalability considerations become decisive **after** baseline requirements for trust, security, and reliability are met. In other words, scalability acts as an accelerator of market penetration rather than a primary gatekeeper for adoption.

A visual representation of the above rankings is provided in Figure 11.

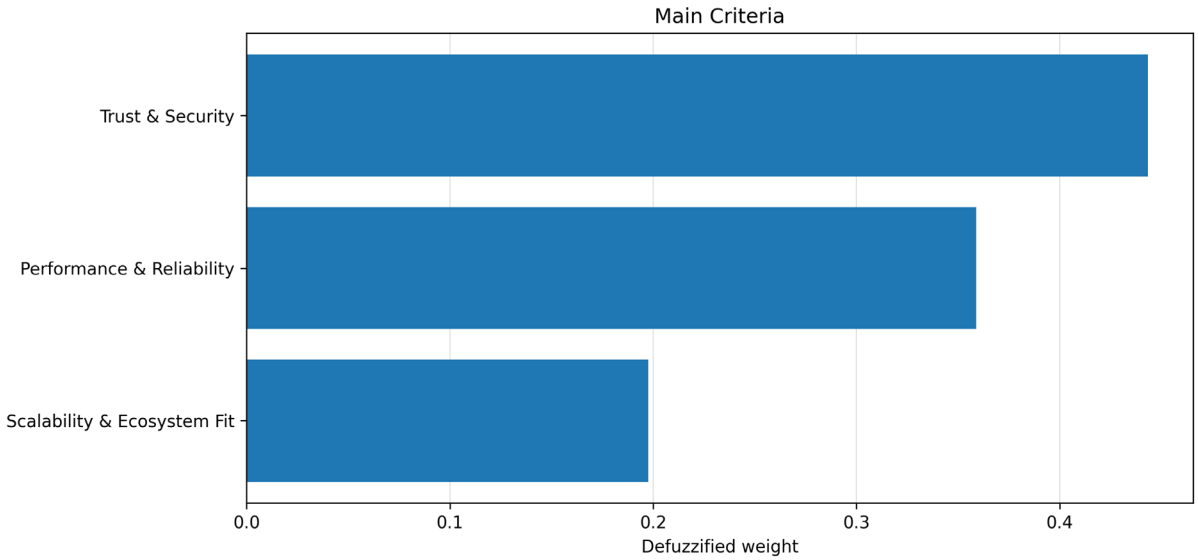



Figure 11: Ranking of Main Criteria

### *Sub-Criteria under Scalability & Ecosystem Fit*

**Interoperability & Deployment Flexibility — 0.438197 (Rank #1)**

This sub-criterion dominates the scalability dimension, highlighting that NANCY's market potential depends strongly on its ability to **integrate seamlessly into heterogeneous environments**. Support for multiple deployment models and compatibility with existing infrastructures are viewed as essential for lowering adoption barriers and facilitating cross-domain uptake.

**Scalability & Low-Maintenance Operation — 0.285557 (Rank #2)**

Operational scalability and reduced maintenance overhead are the second most important factors, reflecting partner expectations that NANCY should scale without imposing excessive operational complexity. This supports sustainable growth and cost-effective long-term operation.

**AI Reusability & Self-Evolution — 0.276246 (Rank #3)**

While still relevant, AI reusability and self-evolution rank slightly lower, suggesting that advanced adaptive capabilities are considered **value-enhancing rather than adoption-critical**. Experts appear to prioritize robustness and deployability over autonomous evolution when assessing ecosystem readiness.

A visual representation of the above rankings is provided in Figure 12.

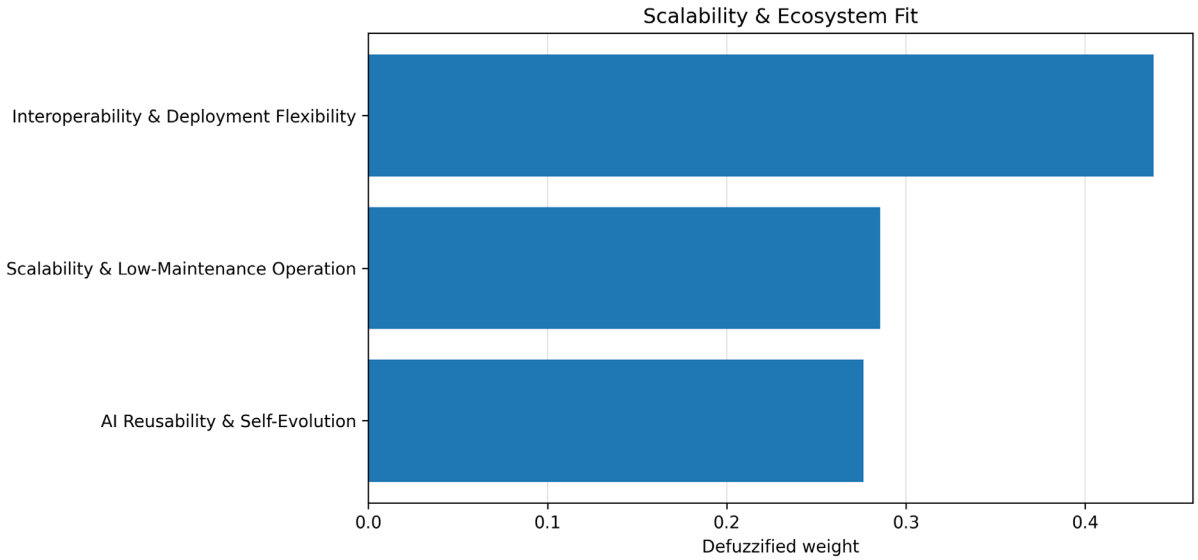



Figure 12: Ranking of Sub-Criteria under Scalability & Ecosystem Fit

### *Sub-Criteria under Trust & Security*

**Threat Detection & Attack Resilience — 0.317393 (Rank #1)**

This sub-criterion is the most influential within Trust & Security, indicating that **active defense and resilience under adversarial conditions** are central to NANCY's trust proposition. From both a technological and market standpoint, the ability to detect, withstand, and recover from attacks is seen as a prerequisite for real-world deployment.

**Explainable & Transparent AI Decisions — 0.241221 (Rank #2)**

Explainability and transparency are ranked second, reflecting their importance for **user confidence, regulatory compliance, and stakeholder acceptance**. This result suggests that trust in NANCY is not only technical but also socio-technical, requiring interpretable and auditable decision-making processes.

**Quantum-Safe Security & Privacy — 0.234096 (Rank #3)**

Quantum-safe mechanisms and privacy protection are recognized as strategically important for future-proofing NANCY. However, their slightly lower ranking indicates that experts place greater emphasis on addressing current and near-term security challenges over long-horizon cryptographic threats.

**Blockchain-Based Trust & Verifiability — 0.207289 (Rank #4)**

Blockchain-based trust mechanisms rank lowest within this group, suggesting that while verifiability and provenance are valuable, they are perceived as **context-dependent enhancements** rather than universally required features for NANCY's market success.

A visual representation of the above rankings is provided in Figure 13.

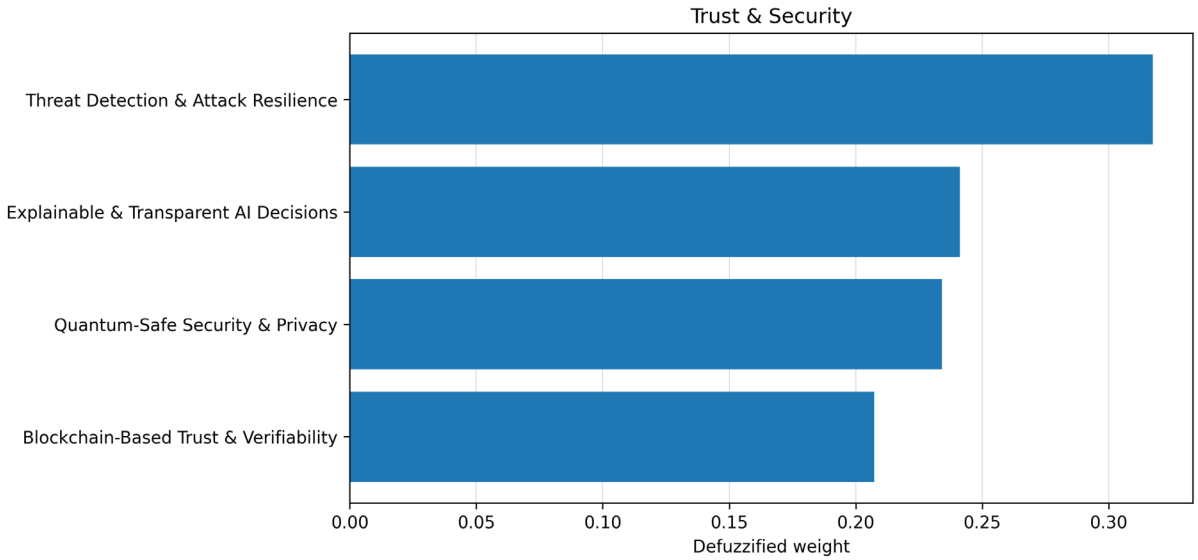



Figure 13: Ranking of Sub-Criteria under Trust & Security

*Sub-Criteria under Performance & Reliability*

**Service Continuity & Resilience — 0.276122 (Rank #1)**

Service continuity is the leading sub-criterion, emphasizing that uninterrupted operation and graceful degradation are critical for NANCY's perceived reliability. This aligns with market expectations for dependable AI-enabled systems in production environments.

**Resource & Energy Optimization — 0.266118 (Rank #2)**

Efficient use of computational and energy resources is ranked second, reflecting concerns related to **operational cost, sustainability, and deployment feasibility**, particularly in resource-constrained settings.

**Network Efficiency & Latency Reduction — 0.229294 (Rank #3)**

Network-level efficiency and latency improvements are considered important but secondary, suggesting that modest latency trade-offs are acceptable if they enable higher robustness and efficiency.

**Edge Offloading & Low-Latency Execution — 0.228466 (Rank #4)**

This sub-criterion ranks last, indicating that extremely low-latency execution and edge-centric designs are viewed as **use-case-specific optimizations** rather than core requirements for NANCY's general technological evolution.

A visual representation of the above rankings is provided in Figure 14.

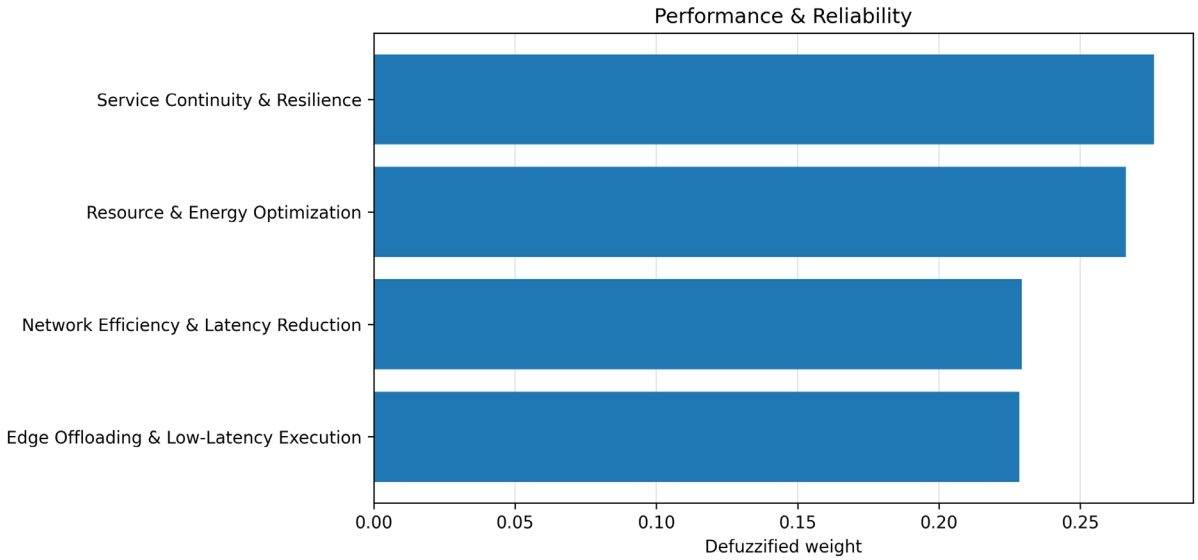



Figure 14: Ranking of Sub-Criteria under Performance & Reliability

### *Total Ranking of Sub-Criteria*

To derive a single, unified ranking across *all* sub-criteria (3 + 4 + 4 = 11), we convert the **local** sub-criteria priorities (computed within each main criterion) into **global** priorities that are comparable across the entire hierarchy.

**1. Start from the hierarchical structure.**

The evaluation model is two-level:

a. Level 1: **Main criteria** (e.g., Trust & Security) with defuzzified weights that reflect their overall contribution to NANCY's technological evolution and market potential.
b. Level 2: **Sub-criteria** under each main criterion, each with a defuzzified (local) weight reflecting its importance *relative to its parent criterion*.

**2. Compute each sub-criterion's global weight.**

Because a sub-criterion contributes to the overall goal only through its parent, its overall importance is obtained by multiplying:

$$w_{global}(s_i) = w_{main}(c_j) \cdot w_{local}(s_i \mid c_j)$$

where:

- $w_{main}(c_j)$ is the defuzzified weight of main criterion $c_j$
- $w_{local}(s_i \mid c_j)$ is the defuzzified weight of sub-criterion $s_i$ under $c_j$

This yields a **global, hierarchy-consistent priority** for every sub-criterion on the same scale.

**3. Create the total ranking.**

Once global weights are computed for all 11 sub-criteria, they are pooled into a single list and **sorted in descending order**. The resulting order constitutes the **Total Ranking of Sub-Criteria**, indicating

which detailed drivers most strongly influence NANCY's technological evolution and market potential when the full hierarchy is considered. Table 61 and Figure 15 show the final results.

Table 61: Total Ranking of Sub-Criteria

| Total Rank | Main Criterion | Sub-Criterion | Main Weight | Local Weight | Global Weight |
|---|---|---|---|---|---|
| **1** | Trust & Security | Threat Detection & Attack Resilience | 0.443420 | 0.317393 | 0.140738 |
| **2** | Trust & Security | Explainable & Transparent AI Decisions | 0.443420 | 0.241221 | 0.106962 |
| **3** | Trust & Security | Quantum-Safe Security & Privacy | 0.443420 | 0.234096 | 0.103803 |
| **4** | Performance & Reliability | Service Continuity & Resilience | 0.358943 | 0.276122 | 0.099112 |
| **5** | Performance & Reliability | Resource & Energy Optimization | 0.358943 | 0.266118 | 0.095521 |
| **6** | Trust & Security | Blockchain-Based Trust & Verifiability | 0.443420 | 0.207289 | 0.091916 |
| **7** | Scalability & Ecosystem Fit | Interoperability & Deployment Flexibility | 0.197637 | 0.438197 | 0.086604 |
| **8** | Performance & Reliability | Network Efficiency & Latency Reduction | 0.358943 | 0.229294 | 0.082303 |
| **9** | Performance & Reliability | Edge Offloading & Low-Latency Execution | 0.358943 | 0.228466 | 0.082006 |
| **10** | Scalability & Ecosystem Fit | Scalability & Low-Maintenance Operation | 0.197637 | 0.285557 | 0.056437 |
| **11** | Scalability & Ecosystem Fit | AI Reusability & Self-Evolution | 0.197637 | 0.276246 | 0.054596 |

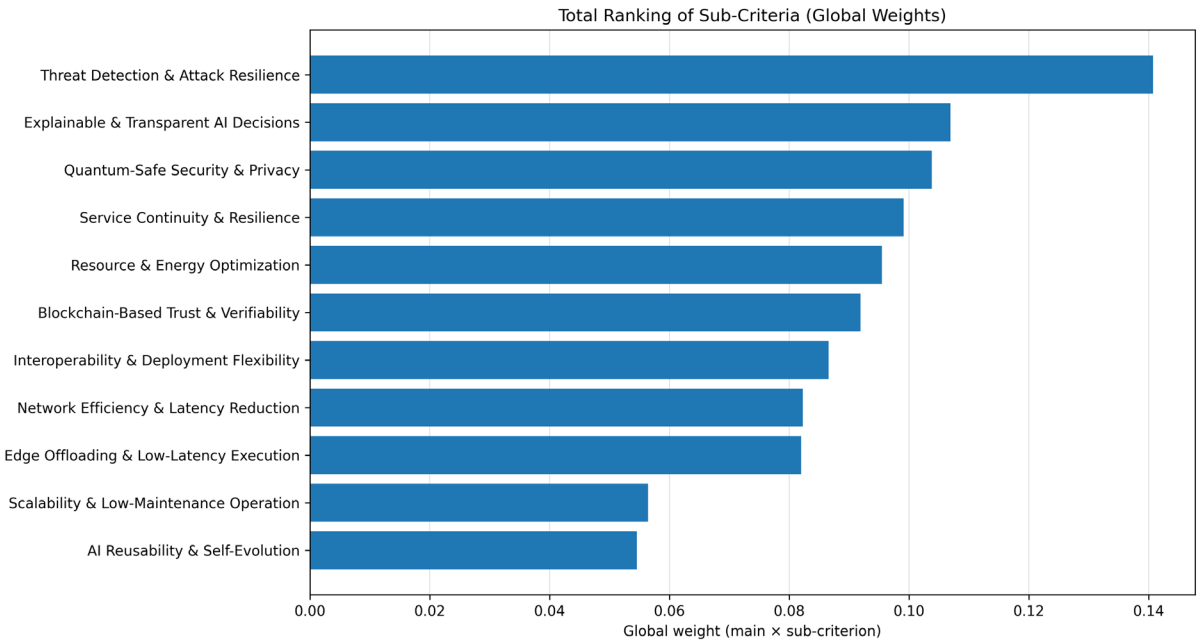



Figure 15: Total Ranking of Sub-Criteria

The total ranking table aggregates all sub-criteria into a single, hierarchy-consistent ordering by combining their local importance with the weight of their parent main criterion, thereby revealing their true overall influence on NANCY's technological evolution and market potential. As expected, sub-criteria under Trust & Security dominate the top of the ranking, since this main criterion carries the highest weight and reflects a strong expert emphasis on trustworthiness as a prerequisite for adoption; in particular, *Threat Detection & Attack Resilience* emerges first, aligning with the need for robust, attack-tolerant systems in real-world deployments. High-ranking positions for *Service Continuity & Resilience* and *Resource & Energy Optimization* further confirm that reliability and operational efficiency are viewed as critical enablers of sustainable performance. Conversely, sub-criteria under *Scalability & Ecosystem Fit* appear lower in the table, not because they lack importance, but because they are perceived as secondary, value-amplifying factors that become decisive only after foundational requirements in security and reliability have been satisfied.

## 5.3. Horizon Results

To maximize long-term visibility and potential market uptake, the consortium has leveraged the Horizon Results Platform (HRP), publishing both commercial and non-commercial results. A total of 27 out of the 28 identified exploitable results have been successfully published, ensuring NANCY's innovations are accessible to a broad ecosystem of investors, policymakers and industrial partners. This action is crucial for supporting sustained exploitation and market access, with further information available in D1.9 "Final Impact Creation Report" [14].

# 6. Conclusion

This deliverable presented a comprehensive techno-economic analysis and commercialization planning framework for the NANCY project, with the objective of assessing the market relevance, commercialization potential, and strategic positioning of its key technological results within B5G. Building upon earlier market and business analyses, the work consolidated a coherent and structured assessment that bridges research outcomes with potential pathways toward real-world adoption.

The market analysis confirmed that NANCY's technological focus areas, including AI-native network automation, blockchain-enabled trust mechanisms, post-quantum security, and cloud-edge-IoT integration, are strongly aligned with current and forecasted industry trends. Growth in 5G/B5G infrastructures, increasing reliance on distributed intelligence, rising cybersecurity and quantum-resilience requirements, and the expansion of edge computing all create a favorable context for the exploitation of NANCY results. At the same time, the analysis highlighted persistent entry barriers related to cost, complexity, interoperability, regulatory compliance, and sustainability, underlining the importance of flexible, modular, and standards-aware solutions.

From a techno-economic perspective, the combined application of SWOT analysis and Lean Canvas modelling enabled a systematic evaluation of each commercially relevant Exploitable Result. This approach provided a balanced view of internal capabilities and limitations, external opportunities and threats, and early-stage business logic. The results demonstrate that several NANCY outputs possess clear value propositions and identifiable target markets, particularly in scenarios requiring secure, automated, and trustworthy network management. While most results remain at a pre-commercial or early validation stage, the analysis identified credible pathways for further maturation through piloting, standardization alignment, ecosystem partnerships, and incremental integration with existing telecom and digital infrastructures.

The commercialization planning activities translated these assessments into exploitation narratives through the use of Characterization Tables. These tables consolidated partner perspectives on target users, use cases, differentiation, intellectual property considerations, and potential deployment models, providing a shared reference point for future exploitation efforts. Complementing this bottom-up view, the application of the Fuzzy Analytical Hierarchy Process introduced a transparent and uncertainty-aware mechanism to prioritize the success factors that most strongly influence commercialization outcomes. The final AHP ranking shows that Trust & Security is the dominant factor shaping the long-term prospects of NANCY's results, with Performance & Reliability as a close second, while Scalability & Ecosystem Fit plays a complementary role that supports market uptake once core security and reliability expectations are satisfied.

Overall, this deliverable demonstrates that NANCY has established a solid analytical and strategic foundation for transforming research innovations into exploitable assets. While further validation, investment, and stakeholder engagement will be required to achieve large-scale deployment, the project's results exhibit strong coherence with market needs and policy priorities at the European level. By combining secure-by-design architectures, AI-driven automation, and decentralized trust mechanisms, NANCY contributes to Europe's ambition to lead the development of secure, intelligent, and sustainable communication networks. The findings of this deliverable can therefore support informed decision-making by consortium partners and external stakeholders as they pursue commercialization and industrial collaboration activities beyond the duration of the project.

# Bibliography

[1] NANCY Consortium, "D1.8 NANCY Market Analysis, Roadmap and Business Modelling Report." [Online]. Available: https://nancy-project.eu/wp-content/uploads/2024/09/NANCY_D1.8_Market_Analysis_Roadmap_and_Business_Modelling_Report_v1.0.pdf

[2] MarketsandMarkets, “5G Materials Market, Industry Size Forecast Report." [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/5g-materials-market-100609646.html

[3] MarketsandMarkets, “Cellular Modem Market Size, Share, Industry Report, Trends and Growth Drivers 2033,” 2025. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cellular-modem-market-135102534.html

[4] Accenture Strategy, “The Impact of 5G on the European Economy,” 2021. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/pdf-144/Accenture-5G-WP-EU-Feb26.pdf

[5] Ericsson, “Ericsson Mobility Report,” 2025. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report

[6] M. R. Future, "Blockchain in Security Market Size, Trends," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/blockchain-in-security-market-7198

[7] “Global Indoor 5G Market Size, Trends, Share 2025-2034,” 2025. [Online]. Available: https://www.custommarketinsights.com/report/indoor-5g-market/

[8] Accenture, “Accelerating the 5G Future of Business,” 2020. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/accenture-accelerating-5g-future.pdf

[9] McKinsey & Company, “Technology Trends Outlook 2025: The Top Trends in Tech,” 2025. [Online]. Available: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-top-trends-in-tech/

[10] KPMG LLP, “Technology and Telecoms Sector Overview,” 2025. [Online]. Available: https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2025/11/cee-uk-2025-sector-overviews-technology.pdf

[11] International Telecommunication Union (ITU), “Report ITU-R M.2516-0: Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond,” 2022. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2516-2022-PDF-E.pdf

[12] GSMA, “The Mobile Economy 2025,” 2025. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/

[13] NANCY Consortium, “D1.10 Final Standardisation Activities Report.” [Online]. Available: https://nancy-project.eu/results/deliverables/.

[14] NANCY Consortium, “D1.9 Final Impact Creation Report.“ [Online]. Available: https://nancy-project.eu/results/deliverables/.

[15] G. Vyas, "Blockchain in Telecom Market size and future scope," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/blockchain-in-telecom-market-42787

[16] “Blockchain in Telecom Market - Share & Size,” 2025. [Online]. Available: https://www.mordorintelligence.com/industry-reports/blockchain-in-telecom-market

[17] MarketsandMarkets, “Blockchain Market Size, Share, Trends, Revenue Forecast & Opportunities.” [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

[18] Z. Precedence Research, "Blockchain Technology Market Size, Share and Trends,” 2025. [Online]. Available: https://www.precedenceresearch.com/blockchain-technology-market

[19] A. Gupta, "Web 3.0 Blockchain Market Size and future scope," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/web-3-0-blockchain-market-10746

[20] Fortune Business Insights, “Blockchain Technology Market Size, Share, Value Growth Report.” [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072

[21] Grand View Research, "Blockchain Technology Market (2025 - 2030)," 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

[22] GlobalData, “Blockchain Market Trends and Analysis by Region, Application, Vertical and Segment Forecast to 2030.” [Online]. Available: https://www.globaldata.com/store/report/blockchain-market-analysis/

[23] NANCY Consortium, “D5.2 NANCY Security and Privacy Distributed Blockchain-based Mechanisms.” [Online]. Available: https://nancy-project.eu/wp-content/uploads/2025/03/D5.2_NANCY_Security_and_Privacy_Distributed_Blockchain-based_Mechanisms_v1.0.pdf

[24] Statista, “Cybersecurity - Worldwide | Statista Market Forecast.” [Online]. Available: https://www.statista.com/outlook/tmo/cybersecurity/worldwide

[25] Cybersecurity Ventures, “Cybersecurity Market Report 2025–2031,” 2025. [Online]. Available: https://cybersecurityventures.com/wp-content/uploads/2023/11/CybersecuritySpending2025-2031.pdf

[26] Market Research Future, "AI in Cybersecurity Market Size, Share and Analysis," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/ai-in-cybersecurity-market-11797

[27] Grand View. Research, "Europe Cyber Security Market Size & Outlook, 2025-2030," 2025. [Online]. Available: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/europe

[28] MarketsandMarkets, “Quantum Key Distribution Market Size, share and Global Forecast.” [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/quantum-key-distribution-qkd-market-80654677.html?utm_source=prnewswire.com&utm_medium=paidpr&utm_campaign=relatedreport

[29] Business Research Insights,” Quantum Key Distribution Market Forecast & Trends 2025.” [Online]. Available: https://www.businessresearchinsights.com/market-reports/quantum-key-distribution-qkd-market-106645

[30] MarketsandMarkets, “Cloud Computing Market Size, share, Forecast to 2030.” [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

[31] Cloud Zero, “Cloud Computing Market Size and Trends,” 2025. [Online]. Available: https://www.cloudzero.com/blog/cloud-computing-market-size/

[32] Mordor Intelligence, “Internet of Things (IoT) Market Size, Share & Outlook 2030,“ 2025. [Online]. Available: https://www.mordorintelligence.com/industry-reports/internet-of-things-iot-market

[33] Fortune Business Insights, “Internet of Things [IoT] Market Size, Share, Growth, Trends, 2032.” [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

[34] MarketsandMarkets, “Edge Computing Market Size Share | Industry Trends Forecast to 2033.” [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/edge-computing-market-133384090.html

[35] Grand View Research, Edge Computing Market (2025 - 2033),” 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/edge-computing-market

[36] MarketsandMarkets, “IoT Market by Hardware, by Connectivity, by Services, by Focus Area, By Region - Forecast to 2030,” 2025. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html

[37] Statista, “Infrastructure as a Service (IAAS),” 2025. [Online]. Available: https://www.statista.com/topics/2739/cloud-infrastructure-as-a-service/

[38] Precedence Research, Internet of Things (IoT) Market Advancements Driving Smart Connectivity Solutions, 2025. Available: https://www.precedenceresearch.com/internet-of-things-market.

[39] Market Research Future, "Edge Computing in IOT Market Size, Share and Forecast | 2035 MRFR," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/edge-computing-in-iot-market-41168

[40] I. M. A. R. C. Group, Edge Computing Market Report by Component (Hardware, Software, Services), Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprises), Vertical (Manufacturing, Energy and Utilities, Government and Defense, BFSI, Telecommunications, Media and Entertainment, Retail and Consumer Goods, Transportation and Logistics, Healthcare and Life Sciences, and Others), and Region 2025-2033. [Online]. Available: https://www.imarcgroup.com/edge-computing-market

[41] Market Research Future, "Distributed Edge Cloud Market Size, Trends | Drivers 2035," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/distributed-edge-cloud-market-21867

[42] Market Research Future, "5G Edge Cloud Network and Service Market Size, Share, forecast to 2035," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/5g-edge-cloud-network-service-market-34473

[43] Gartner, “2025 Cloud Computing market size and Trends,” 2024. [Online]. Available: https://www.cloudzero.com/blog/cloud-computing-market-size/

[44] Market Research Future, "AI in Telecommunication Market Size, Trends Report - 2035," 2025. [Online]. Available: https://www.marketresearchfuture.com/reports/ai-in-telecommunication-market-6803

[45] Precedence Research, “AI in Networks Market Driving Smarter Connectivity Through Automation and Advanced Technologies,” 2025. [Online]. Available: https://www.precedenceresearch.com/ai-in-networks-market

[46] I. C. Weissberger, “IDC Report: Telecom Operators turn to AI to boost EBITDA margins – IEEE CoMSOC Technology Blog,” 2025. [Online]. Available: https://techblog.comsoc.org/2025/11/08/idc-report-telecom-operators-turn-to-ai-to-boost-ebitda-margins/

[47] GSMA Intelligence, "Telco AI: State of the Market,” 2025. [Online]. Available: https://www.gsmaintelligence.com/research/telco-ai-state-of-the-market-q3-2025

[48] Mordor Intelligence, “Agentic AI in Telecommunications and Network Management Market Size, Share & 2030 Growth Trends Report,” 2025. [Online]. Available: https://www.mordorintelligence.com/industry-reports/agentic-artificial-intelligence-in-telecommunications-and-network-management-market

[49] “Across Horizon Europe Project - Next Generation Networks.” [Online]. Available: https://across-he.eu/

[50] “BeGREEN HE :Project.” [Online]. Available: https://www.sns-begreen.com/

[51] “6G-SANDBOX SNS HE PROJECT.” [Online]. Available: https://6g-sandbox.eu/

[52] Nokia, “Nokia Cloud RAN and Open RAN Solution Roadmap.” [Online]. Available: https://onestore.nokia.com/asset/213602

[53] Nokia, C”loud RAN and Open RAN: NTT Docomo and Nokia build next-gen networks.” [Online]. Available: https://www.nokia.com/mobile-networks/ran/anyran/

[54] Nokia, “Nokia partners with Mavenir to prove Open RAN system performance,” 2023. [Online]. Available: https://www.nokia.com/newsroom/nokia-partners-with-mavenir-to-prove-open-ran-system-performance/

[55] Mavenir, Inc. and Mobile Experts, Inc., “OpenRAN: Good and Getting Better,” 2020. [Online]. Available: https://www.mavenir.com/wp-content/uploads/2022/11/Mavenir_WP_MobileExperts_Open_RAN_Good_and_Getting_Better.pdf

[56] Parallel Wireless, “5G OpenRAN,” 2021. [Online]. Available: https://www.parallelwireless.com/products/5g-openran/

[57] V. O'Grady, “Zain Kuwait and Parallel Wireless Claim Open-RAN Breakthrough,” 2025. [Online]. Available: https://developingtelecoms.com/telecom-technology/wireless-networks/17980-zain-kuwait-and-parallel-wireless-claim-open-ran-breakthrough.html

[58] “Helium Network,” [Online]. Available: https://github.com/helium/

[59] “Helium - Own the Air.” [Online]. Available: https://www.helium.com/

[60] European Comission, “Data Governance Act.” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

[61] European Comission, “A Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography.” [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[62] “NIS2 Directive: securing network and information systems.” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive