NANCY - An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution

Panagiotis Sarigiannidis (psarigiannidis@uowm.gr)
Alexandros-Apostolos A. Boulogeorgos (aboulogeorgos@uowm.gr)

This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement No 101096456.
The project is supported by the Smart Networks and Services Joint Undertaking and its members.

Agenda

NANCY

Consortium

Concept &
Objectives

Results &
Overall approach

Consortium

Consortium

Research institutes

University of Western Macedonia (Greece)

i2cat (Spain)

Consorzio Per La Ricerca Nell' Automatica E Nelle Telecomunicazioni C.R.A.T. (Italy)

Universidad de Murcia (Spain)

Tecnalia (Spain)

Josef Stefan Institute (Slovenia)

Centre for research & technology Hellas (Greece)

Scuola Superiore Di Studi Universitari E Di Perfezionamento S Anna (Italy)

9 organizations

4 countries

Consortium

Industries

NEC (Germany)

Italtel (Italy)

Netcompany-intrasoft (Luxemburg)

THALES (France)

Hellenic Telecommunications Organisation S.A. (Greece)

ERICSSON (Italy)

6 organizations

5 countries

Consortium

SMEs

MINDS Metamind innovations IKE (Greece)

Ubitech (Greece)

Eight Bells LTD (Cyprus)

Draxis (Greece)

VOS (France)

Bi2S LTD (Cyprus)

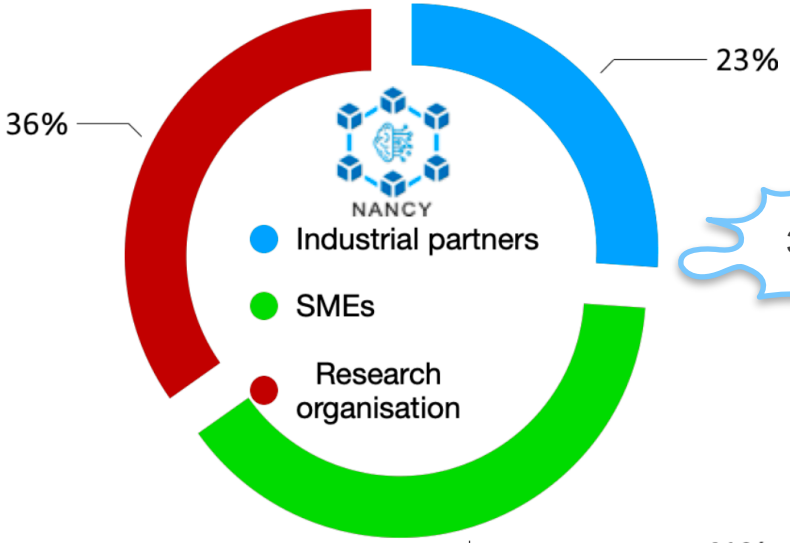
InnoCube IKE (Greece)

Sirocco holdings limited (Cyprus)

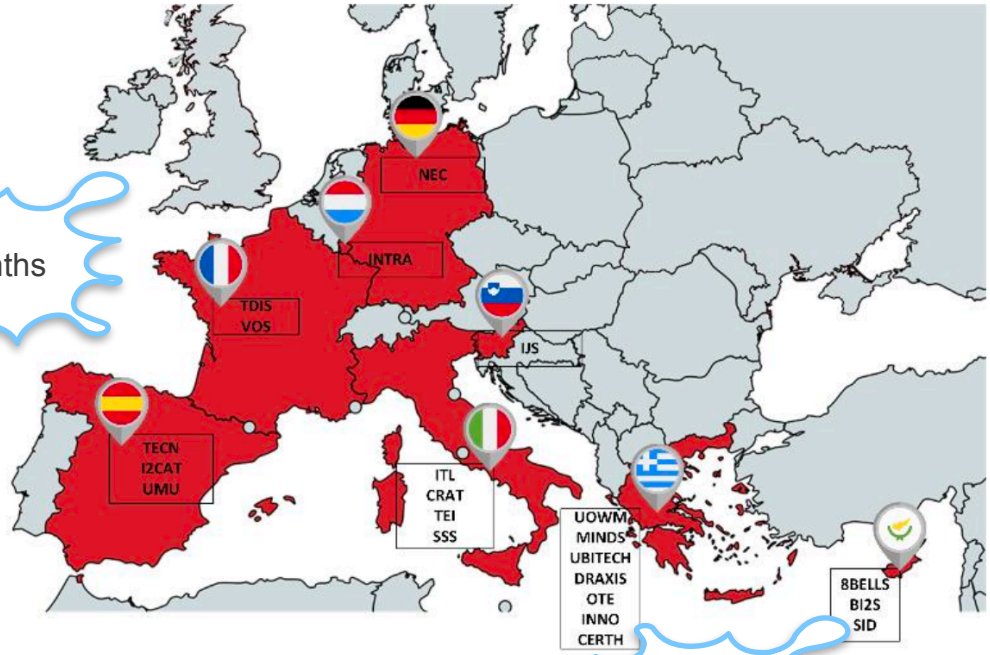
8 organizations

3 countries

Consortium



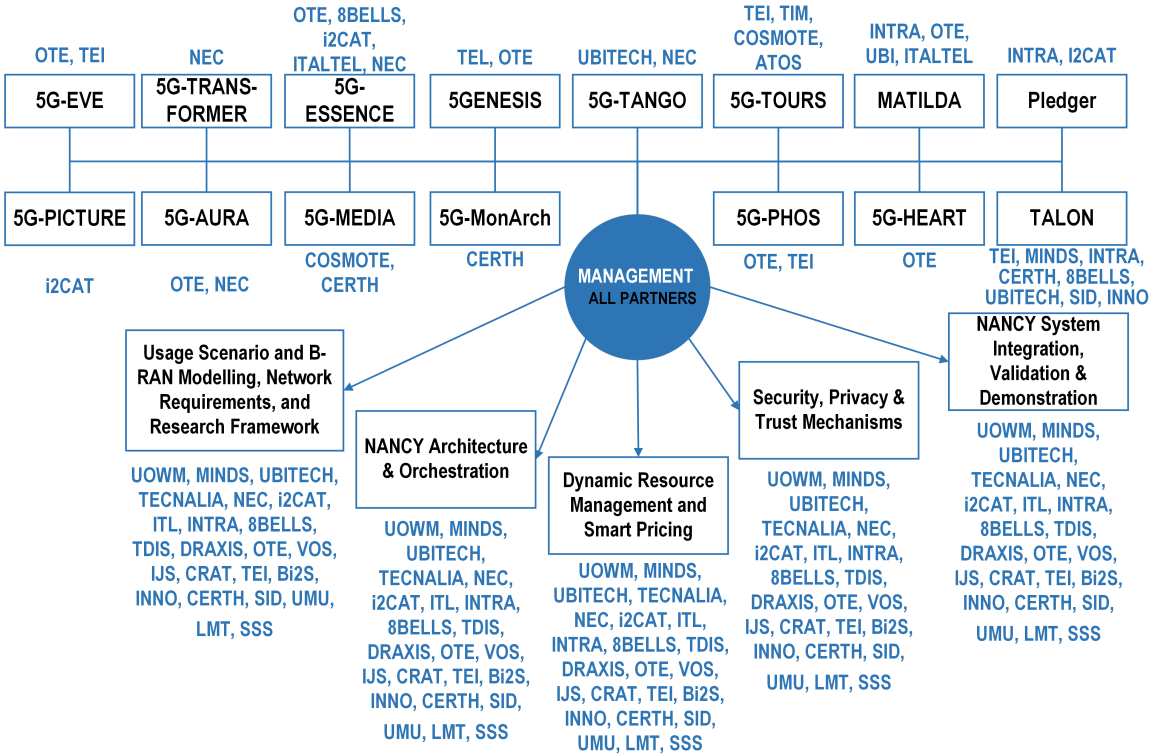
36 Months



22 organizations

8 countries

Consortium


OTE, TEI
5G-EVE
NEC
5G-TRANS-FORMER
OTE, 8BELLS, i2CAT, ITALTEL, NEC
5G-ESSENCE
TEL, OTE
5GENESIS
UBITECH, NEC
5G-TANGO
TEI, TIM, COSMOTE, ATOS
5G-TOURS
INTRA, OTE, UBI, ITALTEL
MATILDA
INTRA, I2CAT
Pledger
5G-PICTURE
i2CAT
5G-AURA
OTE, NEC
5G-MEDIA
COSMOTE, CERTH
5G-MonArch
CERTH
MANAGEMENT
ALL PARTNERS
5G-PHOS
OTE, TEI
5G-HEART
OTE
TALON
TEI, MINDS, INTRA, CERTH, 8BELLS, UBITECH, SID, INNO
Usage Scenario and B-RAN Modelling, Network Requirements, and Research Framework
UOWM, MINDS, UBITECH, TECNALIA, NEC, i2CAT, ITL, INTRA, 8BELLS, TDIS, DRAXIS, OTE, VOS, IJS, CRAT, TEI, Bi2S, INNO, CERTH, SID, UMU, LMT, SSS
NANCY Architecture & Orchestration
UOWM, MINDS, UBITECH, TECNALIA, NEC, i2CAT, ITL, INTRA, 8BELLS, TDIS, DRAXIS, OTE, VOS, IJS, CRAT, TEI, Bi2S, INNO, CERTH, SID, UMU, LMT, SSS
Dynamic Resource Management and Smart Pricing
UOWM, MINDS, UBITECH, TECNALIA, NEC, i2CAT, ITL, INTRA, 8BELLS, TDIS, DRAXIS, OTE, VOS, IJS, CRAT, TEI, Bi2S, INNO, CERTH, SID, UMU, LMT, SSS
Security, Privacy & Trust Mechanisms
UOWM, MINDS, UBITECH, TECNALIA, NEC, i2CAT, ITL, INTRA, 8BELLS, TDIS, DRAXIS, OTE, VOS, IJS, CRAT, TEI, Bi2S, INNO, CERTH, SID, UMU, LMT, SSS
NANCY System Integration, Validation & Demonstration
UOWM, MINDS, UBITECH, TECNALIA, NEC, i2CAT, ITL, INTRA, 8BELLS, TDIS, DRAXIS, OTE, VOS, IJS, CRAT, TEI, Bi2S, INNO, CERTH, SID, UMU, LMT, SSS

Concept & objectives

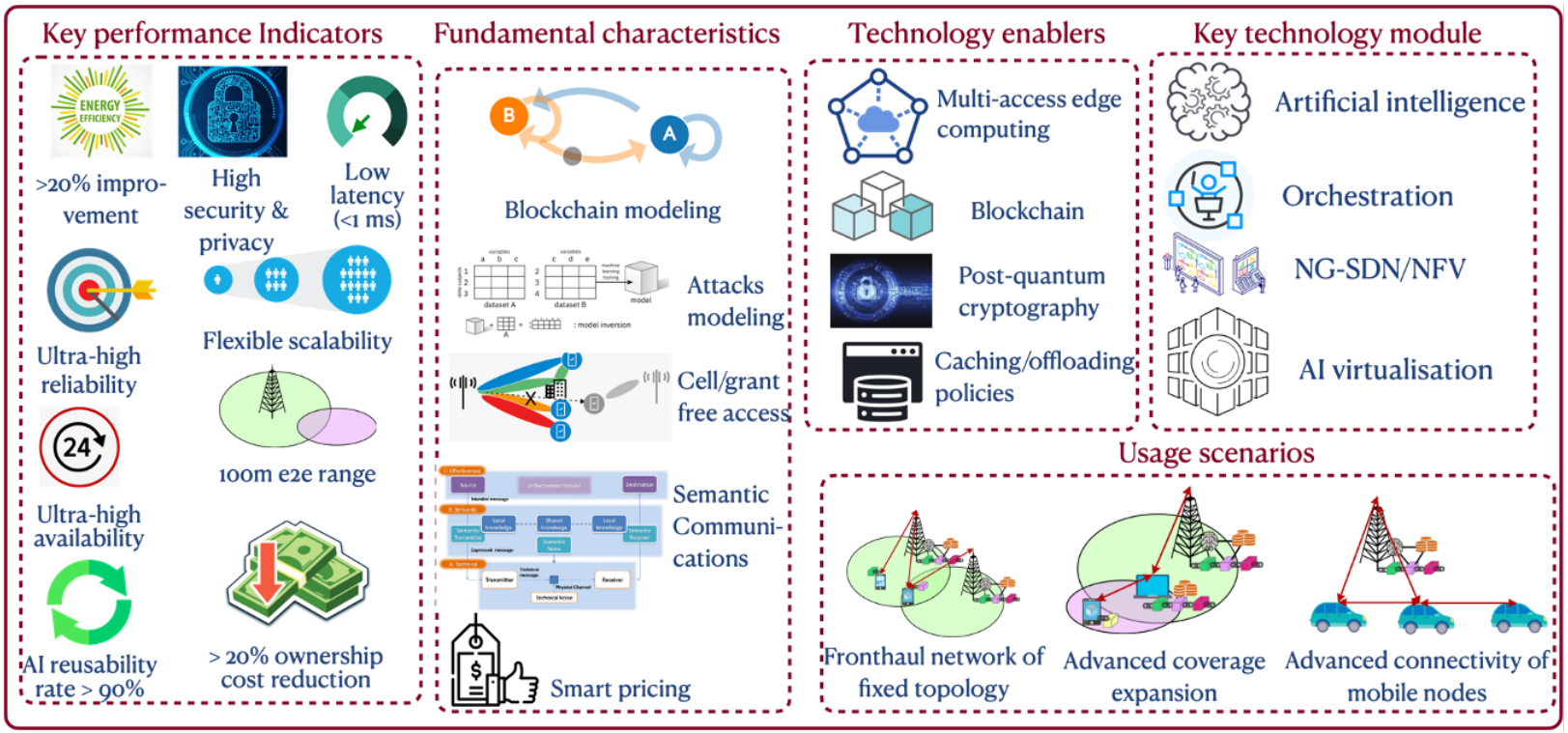
Overall objective

NANCY

The overall aim of NANCY is to introduce a secure and intelligent architecture for the beyond the fifth generation (B5G) wireless network. Leveraging AI and blockchain, NANCY enables secure and intelligent resource management, flexible networking, and orchestration. In this direction, novel architectures, namely point-to-point (P2P) connectivity for device-to-device connectivity, mesh networking, and relay-based communications, as well as protocols for medium access, mobility management, and resource allocation are designed. These architectures and protocols will make the most by jointly optimizing the midhaul, and fronthaul. This is expected to enable truly distributed intelligence and transform the network to a low-power computer. Likewise, by following a holistic optimization approach and leveraging the developments in blockchain, NANCY aims at supporting end-to-end (E2E) personalized, multi-tenant and perpetual protection. Finally, in order to accommodate the particularities of the new RAN that are generated due to the use of novel building blocks, such as blockchain, multi-access edge computing, and AI, a new experimentally-verified network information theoretic framework will be presented.

Concept

NANCY



Pillars & objectives

Pillars	Objectives	Actions	Results
B-RAN	Support dynamic scalability, high-security and privacy	• B-RAN and attacks modeling • Grant-/cell-free access • Consensus mechanisms • Distributed and decentralized blockchain • Smart pricing	[R1] [R2] [R3] [R4] [R5] [R6]
AI-based wireless RAN orchestration	Ultra reliable connectivity and high energy efficiency	• ML-based joint node association and resource allocation • Model-based and data-driven ML-based optimization • ML-based slices instantiation • FL-based anomaly detection, self-healing, and self-recovery	[R7] [R8] [R9] [R10] [R11] [R12]
MEC	Almost-zero latency and high computational capabilities at the edge	• Adjuctable to MEC resources B-RAN functions • Trade-off between B-RAN performance and resource usage • Resource aware/provisioning mechanisms • Offloading policies • Social-aware caching	[R13] [R14] [R15]

Testbeds

- Greek in-lab testbed
- Italy in-lab testbed
- Italy out-of-lab testbed
- Spain out-of-lab testbed
- Greek out-of-lab testbed

KPIs

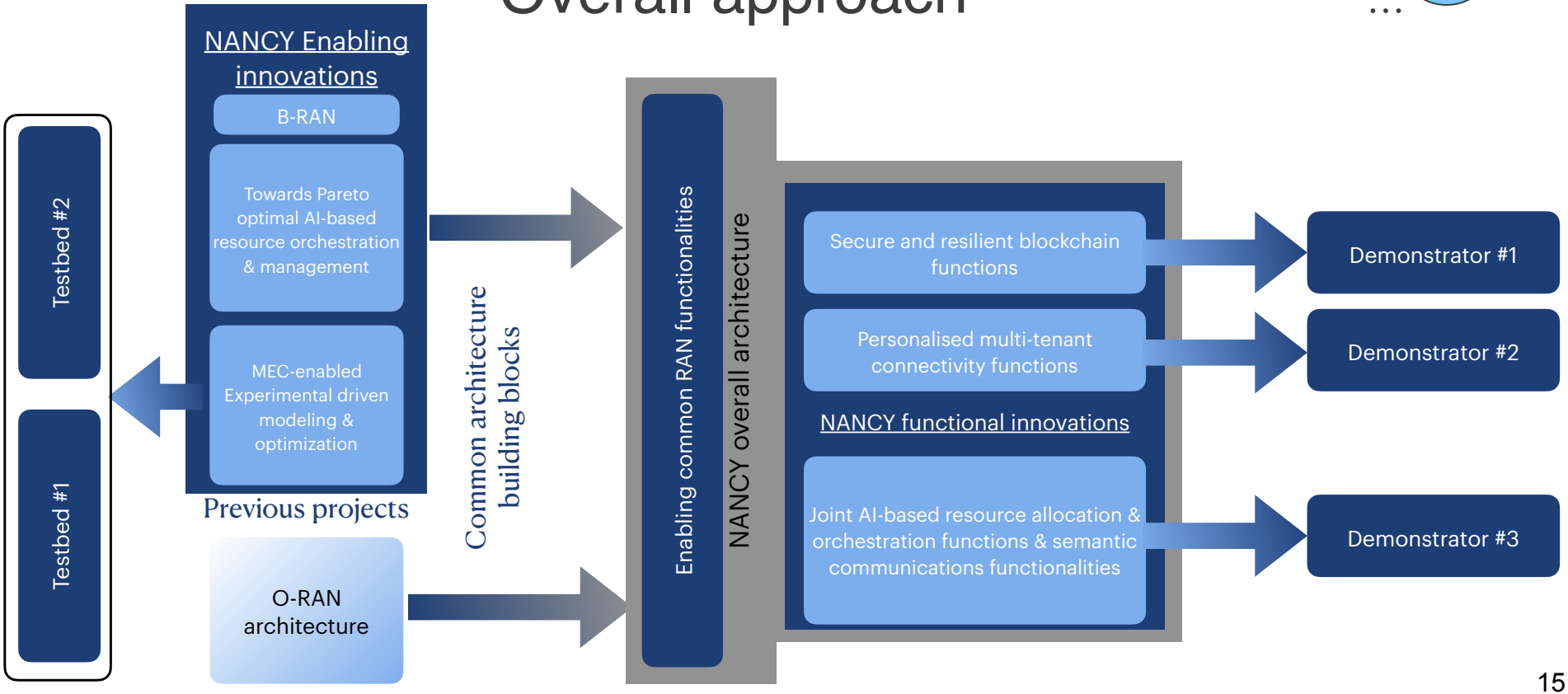
- Extremely high security and privacy
- >20% reduction of the cost ownership
- >20% energy efficiency improvement
- Ultra-high reliability and availability
- Flexible scalability to support masive number of devices
- >1ms latency
- 100 m range expantion

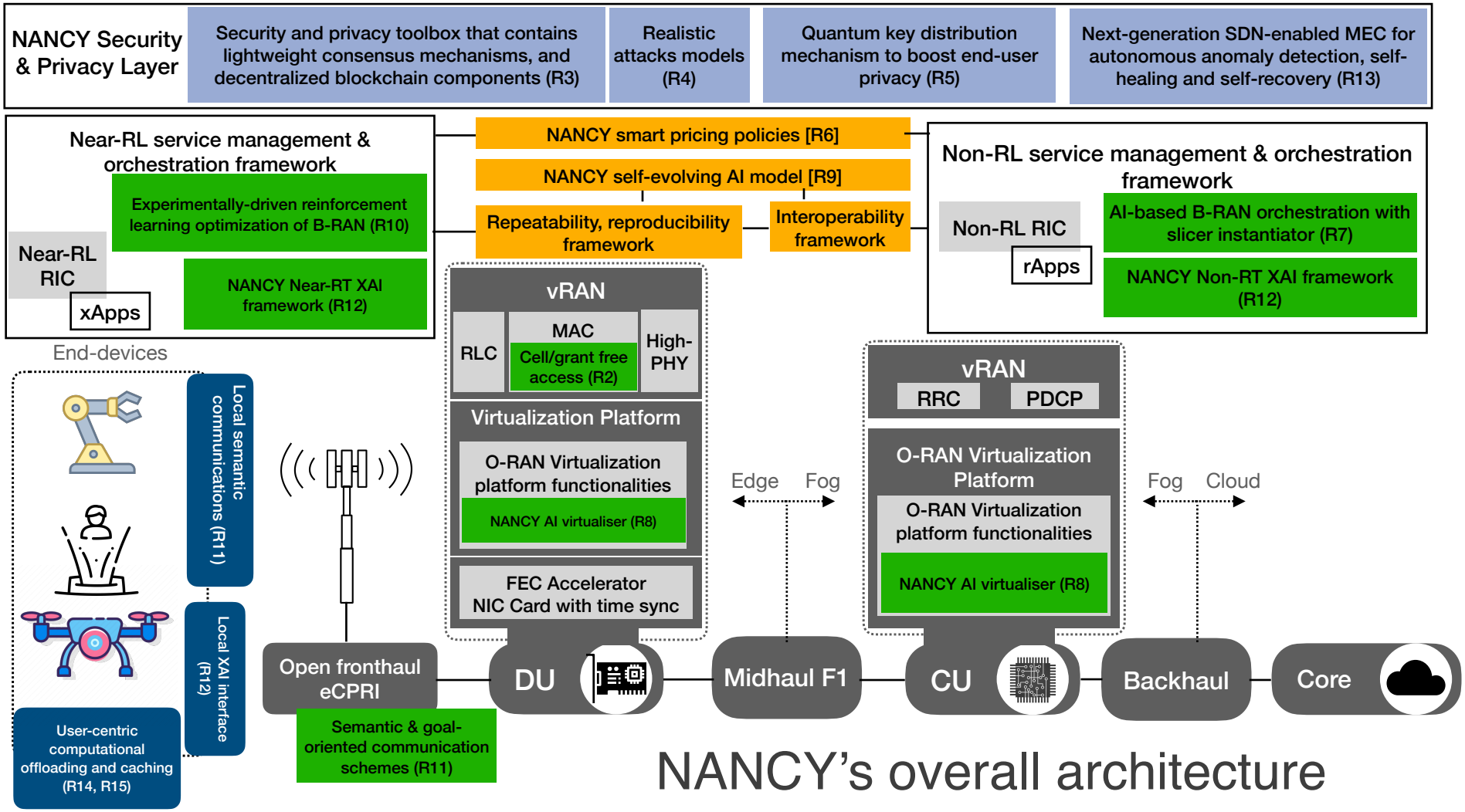
Results and overall approach

Results

ID	NANCY Technical Advances and Innovations	NANCY Pillars		
		I	II	III
R1	B-RAN architecture	✓	✓	✓
R2	Novel trustworthy grant/cell-free cooperative access mechanisms	✓	✓	✓
R3	A novel security and privacy toolbox that contains lightweight consensus mechanisms, and decentralized blockchain components	✓		✓
R4	Realistic blockchain and attacks models and an experimental validated B-RAN theoretical framework	✓		
R5	A novel quantum key distribution mechanism to boost end-user privacy	✓		
R6	Smart-pricing policies	✓	✓	
R7	AI-based B-RAN orchestration with slicer instantiator	✓	✓	✓
R8	A novel AI Virtualiser for underutilized computational and communication resource exploitation	✓	✓	✓
R9	Novel self-evolving AI model repository	✓	✓	✓
R10	Experimentally-driven reinforcement learning optimization of B-RAN		✓	✓
R11	Semantic & goal-oriented communications	✓	✓	✓
R12	An explainable AI framework			
R13	Next-generation SDN-enabled MEC for autonomous anomaly detection, self-healing and self-recovery		✓	✓
R14	A computational offloading mechanism with novel resource-aware/provision scaling mechanisms and novel battery as well as computational-capabilities aware offloading policies	✓	✓	✓
R15	User-centric caching mechanisms		✓	✓

Overall approach




NANCY Security & Privacy Layer
Security and privacy toolbox that contains lightweight consensus mechanisms, and decentralized blockchain components (R3)
Realistic attacks models (R4)
Quantum key distribution mechanism to boost end-user privacy (R5)
Next-generation SDN-enabled MEC for autonomous anomaly detection, self-healing and self-recovery (R13)
Near-RL service management & orchestration framework
Experimentally-driven reinforcement learning optimization of B-RAN (R10)
Near-RL RIC
xApps
NANCY Near-RT XAI framework (R12)
NANCY smart pricing policies [R6]
NANCY self-evolving AI model [R9]
Repeatability, reproducibility framework
Interoperability framework
Non-RL service management & orchestration framework
Non-RL RIC
rApps
AI-based B-RAN orchestration with slicer instantiator (R7)
NANCY Non-RT XAI framework (R12)
End-devices
Local semantic communications (R11)
Local XAI interface (R12)
User-centric computational offloading and caching (R14, R15)
vRAN
RLC
MAC
Cell/grant free access (R2)
High-PHY
Virtualization Platform
O-RAN Virtualization platform functionalities
NANCY AI virtualiser (R8)
FEC Accelerator NIC Card with time sync
vRAN
RRC
PDCP
O-RAN Virtualization Platform
O-RAN Virtualization platform functionalities
NANCY AI virtualiser (R8)
Edge
Fog
Fog
Cloud
Open fronthaul eCPRI
Semantic & goal-oriented communication schemes (R11)
DU
Midhaul F1
CU
Backhaul
Core
NANCY's overall architecture

Thank you for your attention!

Questions?

This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement No 101096456.
The project is supported by the Smart Networks and Services Joint Undertaking and its members.