HORIZON-MSCA-2022-SE-01-01
(MSCA Staff Exchanges 2022)

This project has received funding from the European Union's HORIZON.1.2 - Marie Skłodowska-Curie Actions (MSCA) programme under grant agreement ID 101131481.

distributed ledger technologies and user-driven automation towards self-SOVEREIGN mobile data access in beyond 5G networks

WP2– System Architecture, Requirements and Data

Deliverable D2.1 "SOVEREIGN scenarios framework and business models"

Editor(s):	Dionysis Xenakis (UOA)
Author(s):	Dionysis Xenakis (UOA), Nikos Passas (UOA), Anastasia Tsiota (UOA), Ioannis Neokosmidis (INC), Bogdan Padeanu (IQB), Christos Xenakis (IQB), Symeon Chatzinotas (ULU), Nikolaos Pappas (LIU), Jonathan Rodriguez (IT), Claudia Barbosa (IT), Georgios Zachos (IT), Dimitris Tsolkas (FOG), Ioannis Vardakas (IQU), Theodoros Rokkas (INC)
Dissemination Level:	**Public**
Type:	**R**
Version:	1

Project Profile

Contract Number	101131481
Acronym	SOVEREIGN
Title	distributed ledger technologies and user-driven automation towards self-SOVEREIGN mobile data access in beyond 5G networks
Start Date	January 1st, 2024
Duration	48 Months

Document History

VERSIONS

Version	Date	Author	Remarks
0.1	09/09/2024	Dionysis Xenakis (UOA)	Table of Contents
0.2	02/12/2024	Anastasia Tsiota (UOA)	
1	31/12/2024	Ioannis Neokosmidis (INC)	Final version

Executive Summary

The main objective of WP2 is to i) specify the SOVEREIGN access scenarios and business models for self-sovereign mobile data access over natively disintermediated B5G infrastructures, ii) to conceptualize an end-to-end DLT-backed B5G service architecture that enables B5G stakeholders to advertise available resource pools and service capabilities on-the-fly, allowing intelligent nodes to dynamically discover, negotiate, formalize, deliver, and consume them in view of MPO1, iii) to provide a meticulous study on necessary functional upgrades to the 3GPP 5G system architecture and iv) to develop intelligent strategies enabling online service pricing and function chaining in B5G.

For this specific deliverable, the project aims to amalgamize the outputs of Task 2.1 by defining the SOVEREIGN scenarios framework and business models. In more detail, the deliverable firstly aims to collect, filter, and put together information from MNOs, service providers, etc., to define users, usage, and business requirements for self-sovereign access. Secondly, to define business models and scenarios. Thirdly, to review SotA tools for i) simulation-driven performance evaluation, ii) experimental tools for DLT-backed B5G service prototyping, iii) platforms and products for data-driven B5G network automation, iv) relevant EU-funded actions, v) relevant / target standards for contributions and vi) products for B5G identity management and anonymity.

Contents

Table of Figures

Table of Tables

1. Common practices and information for mobile data access in Beyond 5G systems

1.1. State-of-the-art models for mobile data access in Beyond 5G systems

The introduction of 5G along with the new technologies that are being developed and tested and are expected to be adopted in beyond 5G systems the next years are transforming the mobile data access moving from traditional fixed contract models to more contract-less dynamic models. With the term contract-less we refer to a new type of contracts that are not static and signed offline but to a new era of contracts that are dynamic based on blockchain technology that allows parties to consume, share and trade data in decentralized and anonymous ways. The introduction of this new type of contracts will dictate the introduction of new and more sophisticated business models for Mobile Network Operators (MNOs) that will provide greater flexibility and the ability to create more dynamic and customizable solutions for their customers. Another evolution that is fueling the change of the current business models and the adoption of more complex ones is the expansion of the customer base of MNOs introducing, apart from humans, devices that are the consumers or creators of vast amount of data. In the envisioned future where everything will be connected, most of the traffic will be the exchange of information between devices that include all types of usage like for example sensors, medical devices, robots in manufacturing, and autonomous vehicles.

The analysis that is presented in the following sections includes an analysis of the current landscape of the telecom market, explores the existing business models for mobile data access, and then provides insights about the future technologies and the associated business models of mobile data access beyond 5G. Furthermore, we assess the potential decline of contract-based mobile data access in favor of more flexible alternatives.

1.1.1. Status of telecom market

The global telecom market experiences a rapid growth driven by the widespread adoption of 5G technology all over the world. According to industry reports, 5G subscriptions are forecasted to reach over 1.5 billion globally by 2024. This expansion is assisted by the increasing demand for high-speed internet, low latency, and massive connectivity for devices such as IoT (Internet of Things), autonomous vehicles and drones, smart cities, and industrial automation. In parallel, operators explore "Beyond 5G" technologies, which aim to support even more advanced use cases such as 6G systems, satellite communication, and ultra-reliable low-latency communication (URLLC).

The key challenges that the telecom market is experiencing are the integration of edge computing, the densification of networks, and the management of spectrum. Bringing computation and data storage closer to the network edge (closer to data sources and users) to support real-time applications by reducing latency is one of the major challenges that has technical aspects but also financial consequences. The deployment of more base stations,

small cells, and distributed antenna systems improve coverage and capacity, particularly in urban areas. Network densification includes not only densification over space but also over frequency, utilizing larger portions of radio spectrum in diverse bands. Auctions of high-frequency millimeter-wavelength (mmWave) spectrum and efforts of re-auction of unlicensed spectrum for 5G are critical to provide greater data transfer rates and connectivity. The radio frequency spectrum is not an inexhaustible resource. It is a very precious resource which must be managed to ensure efficient and equitable access to the services which use it.

The ever-increasing user requirements, their diverse nature in terms of performance metrics and the use of various **novel technologies**, such as millimeter wave (mmWave) transmission, massive multiple-input multiple- output (mMIMO) configurations and non-orthogonal multiple access (NOMA), render the multi-constraint nature of the radio resource management (RRM) problem. In this context, machine learning (ML) and mobile edge computing (MEC) constitute a promising framework to provide improved quality of service (QoS) for end users, dynamic allocation of network resources based on traffic patterns, user mobility, and network conditions. Real-time adjustment of parameters (e.g., power, bandwidth) to optimize performance [INC-1]. Predictive analytics using machine learning models for traffic forecasting, resource allocation, network fault detection and biological competitive models for the growth of subscribers [INC-1], [INC-2]. Autonomous network adaptation to changes using reinforcement learning techniques for self-optimization. Deep learning and Reinforcement Learning approaches can speed up the performance of 5G and B5G networks, due to their ability to quickly learn and cooperate with all the elements of the network's environment.

The incorporation of Non-Terrestrial Networks (NTN) such us satellites [INC-3], drones (UAVs) [INC-4], and high-altitude platform systems (HAPS) aims to provide coverage in remote and underserved areas, by constructing 3D cellular networks which integrate drone base stations and drone users, with satellites and HAPS. There are hybrid models that integrate terrestrial and non-terrestrial networks to ensure a providing data access.

Integrated Access and Backhaul (IAB) allows the use of the same spectrum for both access (device-to-base station communication) and backhaul (base station-to-core network communication). IAB is an important new feature in 5G NR that enables rapid and cost-effective millimeter-wave (mmWave) deployments through self-backhauling in the same spectrum [INC-5]. Joint optimization models are used to manage the simultaneous use of spectrum for access and backhaul. Adaptive beamforming and power allocation strategies to ensure efficient use of spectrum. IAB deployments can achieve excellent cell edge coverage, uplink rates above 100 Mb/s, while significantly reducing the amount of required fiber.

The telecom industry is one of the largest contributors to global GDP, with forecasts to generate ca. **$4.8 trillion** in economic value by 2025. With 5G adoption, this figure is expected

to rise further, particularly through sectors like manufacturing, healthcare, agriculture, and entertainment that rely heavily on 5G technologies for innovation. Ericsson Mobility Report [INC-6] predicts that at the end of 2024 the usage of smartphones will increase up to 45% by consuming more than 21 GB of data per month on average (about 4 times more than the amount consumed in 2018) and generating 95% of the total mobile data traffic. In this context, satisfying all of the user requests and providing the desired Quality of Service (QoS) anytime and anywhere, even when traveling on cruises, high-speed trains, and airplanes, is one of the main challenges for future telecommunication systems.

Driven largely by video traffic, global data consumption over telecom networks will nearly triple, from 3.4 million petabytes (PB) in 2022 to **9.7 million PB** in 2027. But because providers appear to have little to no pricing power on increasingly commoditized connectivity and data services, revenues from internet access—our proxy for spending on broadband activity—will rise at only a modest 4% CAGR to US$921.6 billion through 2027. At the same time, telecommunications companies (telcos) must make heavy investments in the costly infrastructure that enables them to serve customers. As the transition to 5G continues and newer technological standards gain traction, telcos are projected to invest US$342.1 billion in their networks in 2027 alone.

These are the signal findings in PwC's inaugural Global Telecom Outlook [INC-7], which provides vital data and thinking to illuminate the strategic paths companies should consider taking in order to sustain outcomes and growth in an increasingly complex and competitive environment. As they maintain their long-standing focus on cost cutting, optimization and automation, companies can seek out pockets of growth. These include internet of things (IOT) solutions; private 5G networks for business customers; fixed wireless home broadband for households; and, in some markets, the provision of digital infrastructure, data, content and platform services tailored to the needs of sectors such as entertainment and media (E&M), healthcare, manufacturing and mobility. As they lean into these hotspots, the strategic imperative for telcos is to become more comfortable working in the broader ecosystems that are transforming this vast industry.

1.1.2. Trends

The telecommunications market is a continuous evolution triggered by the appearance of 5G and the upcoming advancements in beyond 5G (B5G) and 6G networks that come with promises of changing the current landscape by adopting new technologies and also unlocking **new business models**. These next-generation networks are designed to deliver ultra-reliable, high-speed, and low-latency communication, alongside increased capacity, large-scale device connectivity, and enhanced energy efficiency, in order to satisfy the future needs in high-speed communication and energy consumption.

Following the first commercial adoptions of 5G the telecom industry has been transforming to more decentralized and flexible models of mobile data access, driven by user demand for greater control over personal data, network services, and cost structures. **Self-sovereign mobile data access, facilitated by blockchain and Distributed Ledger Technologies (DLTs), offers an alternative to traditional subscription-based models.** This alternative and newly introduced model allows users to take control of their own mobile data without long-term contracts, enabling dynamic pricing and real-time access to network resources. Later we explore how this contract-less model fits into the market, how blockchain/DLTs are used in 5G/6G networks, and provide a detailed business model comparison.

A short overview of the main of the technological changes that 5G has introduced and has impact on the business models associated with the future mobile data access models include Massive Multiple Input, Multiple Output (MIMO) and Beamforming, Millimeter-Wave (mmWave) and Terahertz (THz) Communications, Cloud-Native and Service-Based Architecture (SBA), Multi-Access Edge Computing (MEC) and Network slicing.

Massive MIMO utilizes large numbers of antennas at base stations to improve capacity and spectral efficiency. The beamforming directs signals specifically toward the user rather than broadcasting them in all directions. By implementing these technologies, the position of the user is tracked while the dynamic adjustment of antennas can optimize aspects such as data access, minimize interference and allow simultaneous communication with multiple devices. The utilization of higher frequency bands (30–300 GHz) is an efficient way to support faster data transmission over shorter distances. To overcome the short-range limitations of this higher frequency band, mass small cell deployments will be required along with spectrum aggregation techniques that maximize bandwidth and directional antennas. 5G adopts cloud-native principles by utilizing Virtualized, distributed Network Functions (NFV) and Software-Defined Networking (SDN). Most of the network resources are transforming into softwarised solutions reducing the associated cost for MNOs but increasing the complexity of operation and maintenance. MEC brings the computations closer to the user by deploying edge servers. The result of moving resources closer to users is the reduced latency for applications that require real-time processing (e.g., autonomous driving, virtual reality). Finally, network slicing is a technique of dividing single physical networks into multiple virtual ones, each optimized for a specific service. The aim is to support different requirements of applications and users.

There are also ongoing research efforts focusing on defining what the future B5G will offer. We present here a short overview of the most promising technologies keeping an eye for the ones that can differentiate mobile data access in the future. The evolution of networks after 5G is defined as even more faster allowing the implementation of services such as holographic communications providing immersive communication experiences, distributed AI algorithms at the edge for network optimizations, integration of AI and Machine Learning (ML) at the core of the network and integration of even more radio networks such as satellite for

providing the always connected experience. One of the most promising tools to reshape telecom network services is considering blockchain technology that can have an impact on security and privacy and enhance network efficiency. The next generation of mobile networks is expected to be an open, generic, and multi-party participatory digital platform for emerging new application services.

1.1.3. Business Models for Mobile Data Access and MNOs

One of the first definitions of the business model concept developed in the technological field is the iconic definition by [INC-8] who explains a business model as "*an architecture for the product, service and information flows including a description of the various business actors and their roles, the potential benefits for the various business actors, and the sources of revenues.*"

Mobile Network Operators (MNOs) are using several business models for mobile data access satisfying user needs and capitalizing on new revenue streams. Most of these come from the past generations (4G, 3G) and are in most cases static in nature, have fixed durations and don't offer any flexibility. The most common mobile data access models include subscription-based models targeted at end users and leasing of infrastructure mainly used at wholesale products

Traditionally, MNOs use either subscription (contracts)-based models where customers pay monthly fees for getting a predefined amount of data, voice minutes, and text messages or prepaid plans in which users pay for mobile data in advance without the need for a long-term contract. The **contract-based models** can be further classified to:

- **Pay-as-you-go Plans** in which charged based on the volume usage of actual data and
- **Limited Data Plans** in which customers have the option to choose from different available data plans (e.g., 5GB, 10GB etc.) based on their usage requirements on a fixed price. After that limit has been surpassed the cost for data transfer is usually increased in terms of €/Gbyte compared to the cost within the data plan.
- **Unlimited data plans** have been introduced for covering the needs of users with large data consumption, also to overcome this shortcut. These are typically, although advertised as unlimited, come with a set of "good" usage policies that may prioritize other customers during times of network congestion or limit the speed after a size limit has been reached. Almost all operators offer unlimited data plans in their contract-based options and as the consumption of data is increasing more and more users are migrating to this type of contract.
- **Prepaid plan**: another option that was introduced during the first deployments of mobile networks and is not present in the fixed telecommunication operators is the prepaid plan. It was introduced in first 2G generations mainly because the cost of

mobile access was very high and MNOs wanted an option to increase their market share. This type of access allows users to pay for mobile data in advance without the need for a long-term contract. Users have flexibility in choosing their data plans and can switch providers easily. Prepaid models are dominant in emerging markets due to lower-income levels and users' desire for flexibility such as students. However, MNOs cannot have a predictable revenue compared to contract-based plans.

For wholesale access to their networks MNO usually provide contracts with long term leasing for accessing or using their network assets. The wholesale leasing can be in areas where other MNOs don’t have presence or to **Mobile Virtual Network Operators (MVNOs)** that is a special flavor of MNOs that don't’ own any spectrum or infrastructure. MVNOs lease network access from MNOs and offer data plans to customers. This business model focuses on customer needs usually not served by the offering of MNOs and is usually based on lower pricing offerings that can be provided avoiding the high costs of infrastructure. MNOs also collaborate with businesses that require private network solutions.

While these models are still the dominant ones, with the introduction of 5G new more dynamic pricing strategies are starting to appear. **The traditional model of long-term contracts for mobile data access is increasingly considered outdated**, as consumers demand more flexible, personalized, and adjustable options. Several key factors such as new user needs, slicing influence this trend.

With advancements in technology such as the network slicing technology, MNOs are moving towards offering more flexible, on-demand data access models. Network slicing allows operators to create virtual networks able to satisfy specific user needs, optimizing performance and resources for each of their customers. For example, businesses can request network slices that guarantee specific Quality of Service (QoS) parameters (e.g., low latency, high reliability) for mission-critical applications or any other services that are QoS depended. There are also cases in which enterprises can lease different slices and tunnel their different types of data traffic through the appropriate configured slice. This evolution makes contract-based models obsolete as the slicing might be created dynamic, modified if the requirements are changed and can include different number and type of assets. Another example of slicing that is becoming to appear is the one for supporting a high number of IoT devices that require low data rates, in that case also contract-based data consumption models are not able to cover the modified needs that machine to machine communication will bring.

With the growing prevalence of network slicing, MNOs can provide highly personalized mobile data services tailored to specific use cases, making rigid contracts unnecessary. For instance, enterprises might lease a network slice only during peak periods or for individual events, paying only for the data they need.

Future business models will rely heavily on flexible mobile data leasing, driven by developments in network slicing and programmable networks. This allows for real-time adjustments of data allocations and QoS parameters, especially in enterprise applications like smart cities, Industry 4.0, and healthcare.

As a result, new models such as "**Data as a Service" (DaaS)**” are emerging allowing users to access data on a pay-per-use basis or by dynamically adjusting bandwidth as needed. This model is designed to be more agile and responsive to fluctuating user demands, particularly for industries where data consumption varies widely.

The increased popularity of MVNOs that offer more flexible and affordable alternatives to traditional MNO contracts is another factor that can also make contract-based mobile data access obsolete. Many MVNOs provide no-contract plans or month-to-month subscriptions, which are addressed to customers who prefer independence from long-term commitments. As more users shift towards MVNOs, traditional MNOs are under social pressure to adopt similar models or risk losing market share.

Modern consumers seek greater control over their mobile data access, i.e., **self-sovereignty**, especially in terms of transparent pricing, flexibility, and user-centric features. With the rise of technologies like eSIM (a built-in digital SIM card that enables secure 5G network access without the need for a physical SIM card), which simplifies switching between providers, MNOs are increasingly motivated to re-evaluate the contract-based model.

These changes in the existing business models focus on optimizing network utilization, improving customer experience, and offering greater flexibility for both MNOs and users.

1.1.4. Take-aways

The evolution from 5G to 6G will introduce more intelligent, adaptable, and efficient models for mobile data access. Technologies like AI, edge computing, mmWave, beamforming, and blockchain will be pivotal in addressing the requirements of next-generation applications. Current research efforts are dedicated to address the challenges of ultra-dense networks, spectrum limitations, and energy optimization to deliver continuous, reliable mobile data access globally.

The contract-based mobile data model is steadily becoming outdated, as consumer demand shifts towards flexible, on-demand services. New technology efforts like 5G, network slicing, and eSIM trigger new business models designed to meet these dynamic needs. Both MNOs and MVNOs are innovative and customer-focused approaches to stay competitive in the swiftly evolving.

1.2. Information relevant to mobile data access in Beyond 5G systems

An integrated analysis of the B5G and 6G telecom market requires the collection and evaluation of proper technical and economic **Key Performance Indicators (KPIs)**. With these KPIs it will be possible to assess the market development, the user demand, the technological progress, and the financial viability of the corresponding investments. Moreover, identifying and utilizing relevant and correct datasets is essential to accurately forecast the future demand and to project future growth within the telecom sector.

To better understand the market of mobile data access in Beyond 5G systems questions related to the market size and growth, the number and type of players in the market, the status of 5G deployments, the consumption of data by users along with data related to the expenses of 5G deployment and estimation of revenues is required. The next table presents an overview of the minimum set of KPIs that are required to assess the mobile data access market along with the possible source of information and further details on what is required. The experience has shown that the collection of concrete data is a hard process, although some of the information is published by the National Regulatory Authority (NRA) of each country there are some inconsistencies in the process. Some of the reports are published only once a year from some NRAs or in different intervals from others, the definition of the KPIs is not always the same across countries and sometimes the collected KPI may change from one reporting period to another. A combination of information found in different sources (NRAs, MNO reports and industry reports) is the safest way of collecting accurate information but is time consuming.

Table 1 : KPIs for telecom market assessment

KPI name	KPI definition	Source	Comments	Open data
5G operators	*Number of 5G operators per country*	*NRAs, desk research*	*Includes both MNOs and MVNOs Is SA enabled (yes/no)*	*Yes*
5G spectrum	*Spectrum per operator*	*NRAs, desk research*	*All related frequency bands (includes price, date acquired)*	*Yes*
5G coverage	*Coverage of 5G networks in country (% of area)*	*NRAs, MNOs, desk research*	*Additional split by geotype (urban, rural)*	*Yes*

5G users	*Number of 5G users in country*	*NRAs, MNOs, desk research*	*Additional splits: prepaid, postpaid, M2M Type: private users, business users*	*Yes, maybe not all splits available. Publishing period not always consistent.*
5G private networks	*Number of 5G private networks in country*	*NRAs, MNOs, desk research*	*Vertical involved Owned (MNO, third parties)*	*No existing datasets, information is public but must be collected through search.*
5G base stations	*Number of 5G base stations in country*	*NRAs, MNOs, desk research*	*Includes all small cells*	*https://opencellid.org/ contains info based on users' data*
Peek data rate	*Maximum data rate that the network provides*	*NRAs, MNOs, desk research, reports*	*Uplink and Downlink*	*Industrial reports but now always open*
Average traffic per user	*Traffic consumed per month per user*	*NRAs, MNOs, desk research, reports*	*Additional splits: prepaid, postpaid, M2M Type: private users, business users*	*Yes (depends on NRA), maybe not all splits available. Publishing period not always consistent*
Average Revenue per User (ARPU):	*Revenue generated per user*	*MNOs, desk research*	*Additional splits: prepaid, postpaid, M2M Type: private users, business users*	*No*
Capital Expenditure (CAPEX)	*Allocated for 5G network deployment*	*Vendors, desk research*	*Unit cost for 5G equipment*	*No*
Operational Expenditure (OPEX)	*Allocated for 5G network operation*	*Desk research*	*Cost for maintenance of 5G equipment, support activities, personnel cost.*	*No*
Total Cost of Ownership (TCO):	*The cost of deploying and maintaining*	*Desk research*		*No*

	5G infrastructure			

There are some datasets available that are reliable and openly available published by governmental agencies, standards organizations, academic institutions, and telecom regulatory bodies. The most important ones are the following:

- *International Telecommunication Union (ITU)* is the UN specialized agency for information and communication technology (ICT) and is the official source of international ICT statistics. Data is released twice a year via the World Telecommunication/ICT Indicators Database and its website, and various publications, including the flagship series Facts and figures and ICT price trends.
- *OpenCellID* [INC-9] is a collaborative community project that collects GPS positions of cell towers and their corresponding location area identity.
- *National Regulatory Authorities (NRAs)* publish annual reports that contain datasets relevant to spectrum allocation and licenses, market penetration, investments in the telecom sector etc.
- *World Bank* [INC-10] provides also data regarding mobile subscriptions per country and other indicators such as telecommunications revenue and investments.
- *Organisation for Economic Co-operation and Development (OECD)* [INC-11] provides bi-annual updates of fixed and mobile broadband data to track the evolution of these technologies and compare them across OECD member countries using a common methodology. It includes indicators such as 5G subscriptions, broadband speeds in urban and rural areas, and provides access to various national broadband deployment maps.
- EUROSTAT [INC-12] publishes indices related to revenue, spending and usage across EU countries.
- GSMA Intelligence [INC-13] provides a vast number of datasets coming from operators all over the world, there are some limited datasets available while the whole dataset is available through a membership service.

2. Business Models and Scenarios for self-sovereign mobile data access

2.1. How contract-less mobile data access can fit into the market

Contract-less mobile data access allows users to purchase data, services, and resources on-demand without the need of using and paying long-term subscriptions. This new type of model is well-suited to the evolving telecom market for several reasons.

It gives users the flexibility to purchase data or services based on their actual consumption. This is especially important for cases of end users with no fixed but varying data pattern as for example seasonal workers, tourists and users that have increased needs that can be predicted.

Contract-less data models in 5G/6G are more dynamic, allowing users meet the needs for specific services (e.g., high-bandwidth access for a short period). Users don't have to check or worry if their current contract can meet the requirements of each service, the automatic negotiation and allocation of requested resources will allow users to get access to the service they require (it is assumed that there will be some constrains from the user's side regarding the max amount is willing to spent).

New innovations such as eSIM technology that started as a feature available only in high end devices is now finding is way in lower cost smartphones and wearables. It allows users to be able to subscribe simultaneously and use the one that meets their needs that specific period of time. An example is the use of eSIM for reducing the costs of roaming. It is expected that in the future more and more MNOs and MVNOs will support eSIMs.

In the new era of 5G and the new generation of services that will rely on machine-to-machine communications a simpler and dynamic way of accessing on demand mobile data, from many and different locations from many and different devices is required. The amount of data that will be demanded may vary depending on the type of device and its location. With dynamic contracts it will be easier for MNOs to design new services and offer these to customers in a form of a bundle covering all their devices making more easy and transparent charging mechanisms. In addition, MNOs will have the ability to better utilize their resources.

Different verticals like automotive, industry, smart cities, agriculture have different requirements that cannot be captured by the existing contract-based schemes. The dynamic and decentralized provisioning of services is better suited to their needs and can be adjusted to meet future demands.

2.2. How blockchains are typically used in beyond 5G/6G networks

Blockchain in B5G and networks is foreseen as a tool that can be used to enhance security,

improve data management, increase trust and transparency and help realise economic benefits. Blockchain integration helps deliver value-added advantages with unprecedented levels of higher security and privacy to B5G and 6G networks. Blockchain can help in protecting the data from unauthorized access and data breaches by decentralizing the data storage and executing cryptographic algorithms. If anything is to be take a note of, it is entered in a block and linked to the previous block making it a permanent chain. This ensures that the data is immutable and is not subject to malicious modification, making it a compelling security architecture for B5G networks. Also, by decentralising removes the current single point of failure, resulting in reduced opportunity for targeted cyber-attacks.

For more effective data management practices, a blockchain based concept is being investigated. Using its transparent and efficient distributed ledger technology, it enables tracking and managing data. This creates an open ledger of every transaction, every transfer of data that are transparent and verifiable, reducing the potential for error and fraud. Additionally, blockchain can facilitate data sharing between the multiple parties involved in the network and lead to stronger cooperation and better interoperability.

With blockchain technology, future networks will have higher efficiency, particularly in terms of resource allocation and latency. A smart contract can facilitate network functions, such as allocating bandwidth and routing data, without needing a third party to manage external processes. This automation reduces manual effort and can lead to faster speeds and greater stability of the network. In addition, blockchain will be able to serve as a source for running decentralized applications, which will run independently of traditional central servers, thus helping the overall efficiency of a network.

The nature of Blockchain as trusted and transparent technology are crucial to B5G networks from the state of trust maintaining during transmission of packets. Blockchain-based transactions are open and accessible to all participants in the network, that is, your working environment is maximally transparent, and any transaction action is traceable and verifiable. This transparency is vital in building trust between users, service providers, other stakeholders and is one of the key elements that will accelerate the B5G mass adaptation process.

Another application that is foreseen is for reducing operational costs that can be easily automated through the elimination of intermediates by utilizing blockchain. This cost reduction can be passed on to end-users through lower prices and enhanced services. In addition, blockchain could also support new business models such as micro-payments and decentralized marketplaces, enhancing economic growth and innovation in the envisioned future ecosystem.

2.3. Helium network business model

Known as "The People's Network," Helium Network operates a disruptive decentralized wireless infrastructure model of national and global scope for low-cost, secure and decentralized Internet of Things (IoT) coverage. Its deployment uses blockchain technology as an incentive to reward participants with rewards. The Helium business model federates actors and mechanisms for creating a shared, decentralized, peer-to-peer (P2P) wireless network, and in doing so, redefines the telecommunications business model.

The most important actors within the Helium Network include:

Hotspot Hosts: These are people or businesses that buy and set up “Hotspots” (or gateways), that wirelessly offer coverage for some specific, usually IoT devices, and joins the network by validating transactions on the Helium blockchain. In exchange for hosting hotspots and proving data transfer over the network, they are rewarded with Helium's native cryptocurrency (HNT).

IoT Device Users (Customers): IoT devices gain wireless connectivity using the Helium Network and pay for data credits (DCs) for transferring data over the network. Examples of IoT devices vary from GPS trackers to temperature sensors, utilizing the cost-effectiveness and low power consumption of the network.

Validators: the participants who confirm and validate transactions with the help of the blockchain to ensure that the records are accurate. In order to participate, validators are required to stake some HNT and earn rewards to be part of the validators that validate blocks.

Helium & Decentralized Governance (DAO): Although Helium Inc. built the majority of the network, it is now moving towards a decentralized governance model with decisions made by community participants, the (DAO).

HNT token holders: HNT is a utility token that is intrinsic to the Helium ecosystem, allowing people who help the network to be rewarded with a pragmatic token that can be staked, tradable, or used for anything in the Helium ecosystem.

Among the actors the following interaction and exchange of resources are made.

Hotspot mining and data transfer

Supply coverage and transfer associated data Hotspot Owners earn HNT supplied. This encourages expansion of the network coverage since the Hotspots are intended to provide coverage in their respective areas. Hotspots earn HNT for successfully validating each other’s Proof-of-Coverage (PoC), which confirms coverage and reliability. Data credits (DCs) are burned (in exchange for HNT) to make payment for data transfer. With increasing demand for

the network comes a decrease in HNT supply, through this “burn-and-mint” model.

Stake and Reward Model

To maintain the integrity of the network, Validators stake HNT and are rewarded for transaction processing.

The process of staking requires the holders to be incentivized to keep their tokens for as long as an uptrend in price does not move them to sell. This, in return, makes the network stronger and its service more reliable.

Tokenomics and Governance Participation

HNT holders take part in network governance and DAO decisions which includes voting on network upgrades, adjustments to reward, and resource allocation.

Market Transactions

HNT tokens are tradable on open markets providing liquidity to users and hotspot hosts who wish to monetize their contributions.

Benefits and drawbacks of Helium Business Model

Based on the need for distribution, as many hotspots as possible will need to be distributed for coverage, allowing for very rapid, scalable coverage with little central control. Helium Network does not maintain any infrastructure, it lets the public do it all and lower rent charges and maintenance costs of telecom networks.

Participants gain HNT for hosting hotspots and providing coverage, which means interests are aligned toward growing and securing the network

Helium is the only wireless network that supports a variety of IoT applications including asset tracking, environmental monitoring, and agriculture, fueled by a growing IoT market.

Apart from benefits there are also the following drawbacks. The Helium Network has no other capabilities apart from being an IoT network, which can be a limiting factor for adoption if the demand for IoT connectivity is low in any given region. As preference shrinks, it can lead to diminished token prices (and earnings) for hosts, which might disincentivize the deployment of hotspots over time. In some areas, operators cannot cover the network demand so that big users in IoT cannot rely on their service. The governance model can slow down decision-making, which can hinder agility but is also a drawback of this complex governance structure as the network moves to a DAO. There may be regulatory scrutiny on the use of blockchain technology and cryptocurrency, which may affect the operations in certain regions.

Helium Business Model Vs Traditional Business Models

Helium Network proposes a distributed ownership, while other telecoms are top-down owned, the Helium Network needs people to own and operate infrastructure. Instead of creating immediate cash flows for participants that share in these revenues through service fees, Helium rewards all participants with a cryptocurrency (HNT), closely linking participant incentives with use and growth of the network. The HNT and data credits together form a special economics where demand and supply are automatically balanced and the currency of participation is co-created at all times. Compared to the conventional hierarchy of telecoms, Helium is powered by community governance under the new DAO-led structure. Where traditional telecoms are competing for pricey slices of high-speed data for use in mobile devices, Helium focusses on low-power, long-range IoT applications where the extreme network design lowers costs and enables use cases that are likely very different from those of traditional mobile networks.

Helium Network provides a new model for building and maintaining wireless infrastructure with the property rights and governance structure hidden in its decentralized nature (unlike the telecom structure described above). Involving individual hotspot hosts and deploying a token economy, Helium created an economically sustainable network with the potential to scale massively. But its foundation remains nascent, with hurdles including dependency on IoT demand, potential revenue volatility, and regulatory barriers.

2.4. The SOVEREIGN mobile data access model

In a heterogeneous wireless network, mobile users are interested in consuming video content hosted by servers located in the far Internet. To achieve this, end users utilize different radio access technologies (RATs) to gain access to the available network tiers, having as an entry key pre-cached access credentials provided by their home network operator, e.g. subscriber ID, IMSI, social media account, network keys and passwords. Depending on the RAT and the access rights of end users, mobile data access is governed by i) the coverage provided by the accessible network tiers in the near area, ii) the status of nearby attachment points (in light of the additional load offered by other users and the backhaul connectivity available), and iii) the mobile data usage plan agreed with the home operator per user.

In contrast, the proposed mobile data access model enables end users, access points and cellular base stations to share, trade and consume their network assets (backhaul links, Internet connectivity, cached content, etc.) in real-time and without a-priori service license agreements (SLAs). In SOVEREIGN, we employ and shall extend the mobile data access model defined in previous work of the partners in [UOA-1]. Under the **proposed mobile data access model**, *end users* (termed as SOVEREIGN clients) and *service providers* (termed as SOVEREIGN servers) can set up on-the-fly service agreements and implement blockchain-backed service charging on a per delivered video chunk basis in line with their current service requirements,

coverage, available assets (including local content) and preferences.

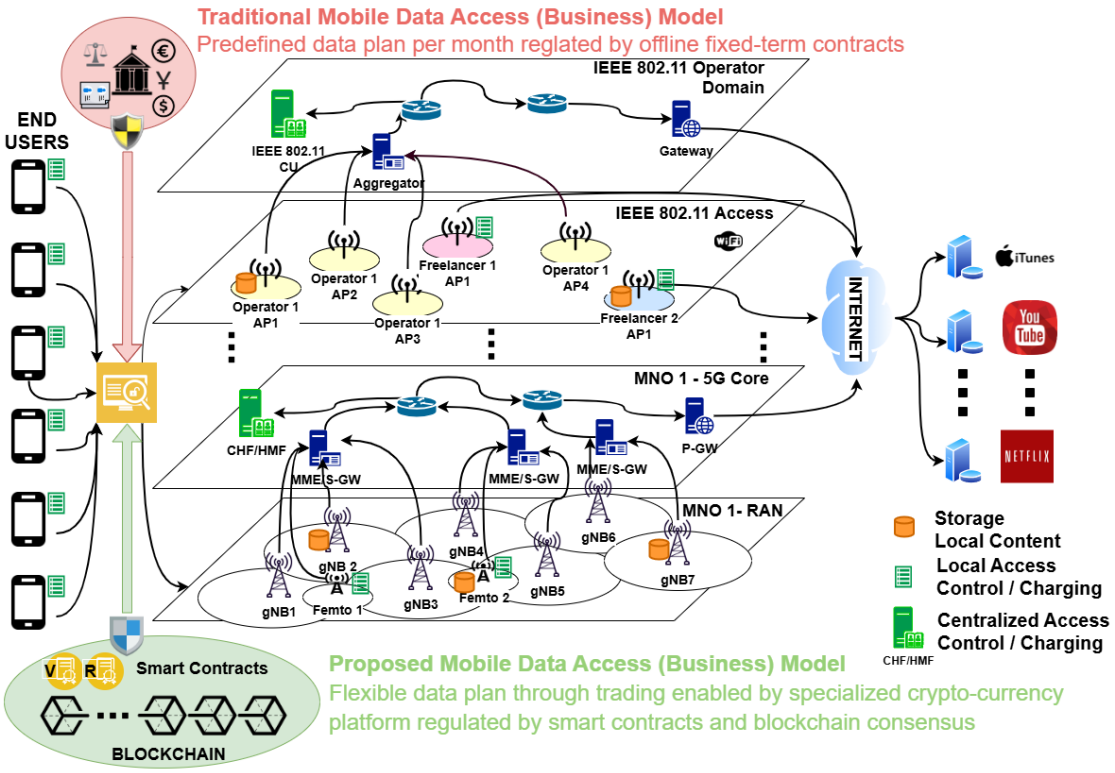

Fig. 1 The SOVEREIGN approach

At minimum, end users and service providers should hold a blockchain ID (public address) and be capable of assessing the blockchain status, e.g. by querying consensus nodes that are responsible for maintaining the SOVEREIGN blockchain (transactions propagation, block validations, consensus protocols, etc.). Depending on their operational requirements and functional capacity, SOVEREIGN nodes undertake specialized roles that we will detail in D2.2, e.g. block validators, payment relays, mixing servers, consensus nodes, witnesses. Even though existing MNOs and large-scale providers will still have a competitive advantage due to their large-scale coverage and reputation, under the SOVEREIGN model, any network asset holder is enabled to trade under-utilized network assets, complementing (or even competing with) large-scale MNOs in geographical regions with poor service coverage, or non-competitive prices.

Support of the SOVEREIGN mobile data access model, necessitates the employment of functional and operational enhancements that span both the blockchain and network domains. In the blockchain domain, the mobile data network should be built on-top of a blockchain-backed platform that enables:

i) a high degree of decentralization, by enabling different roles and levels of engagement to the Beyond 5G key,

ii) scalability by supporting a multi-million transactions throughput and
iii) security, by addressing the blockchain/network ID coupling problem.

In the network domain, fully-decentralized and personalized mobile video content consumption beyond 5G, urges the industry and academia to further delve into user-controlled network-assisted procedures, a design approach that has been within scope of large standardization bodies over the past decade, e.g. user-driven network selection and service control by IEEE, autonomous cell search by, MEC/RAN integration by ETSI.

In the sequel, we discuss network-level enhancements that are necessary for blockchain-based design for mobile video content delivery in Beyond 5G networks. To this end, we decompose the implementation of the proposed service into three phases (Fig. 2): i) service discovery and pairing 2.4.1, ii) service negotiation and parameterization 2.4.2, and iii) online service management and charging 2.4.3. The main actions performed during each phase and some key implementation issues are discussed in detail.

At this point, it is important to note that we do not consider that all network functions necessary for mobile video delivery are migrated to the SOVEREIGN blockchain. Such an approach is not scalable and would insert to the blockchain-backed mobile video delivery process enormous overheads for keeping track of all network-level interactions at a global scale. Thus, service discovery, pairing, negotiation, parameterization and management (including optimization through fine-tuning of network-level parameters) are still performed by using network-level protocols that are modified accordingly. However, the SOVEREIGN blockchain-backed platform implements credible service charging, enabling on-the-fly service setup between SOVEREIGN nodes without a-priori SLAs. Also, SCs are used only for enforcing distributed consensus and honest operation of SOVEREIGN nodes, such as block validators, payment relays and coin mixers, but not for formalizing SLAs between SOVEREIGN nodes.

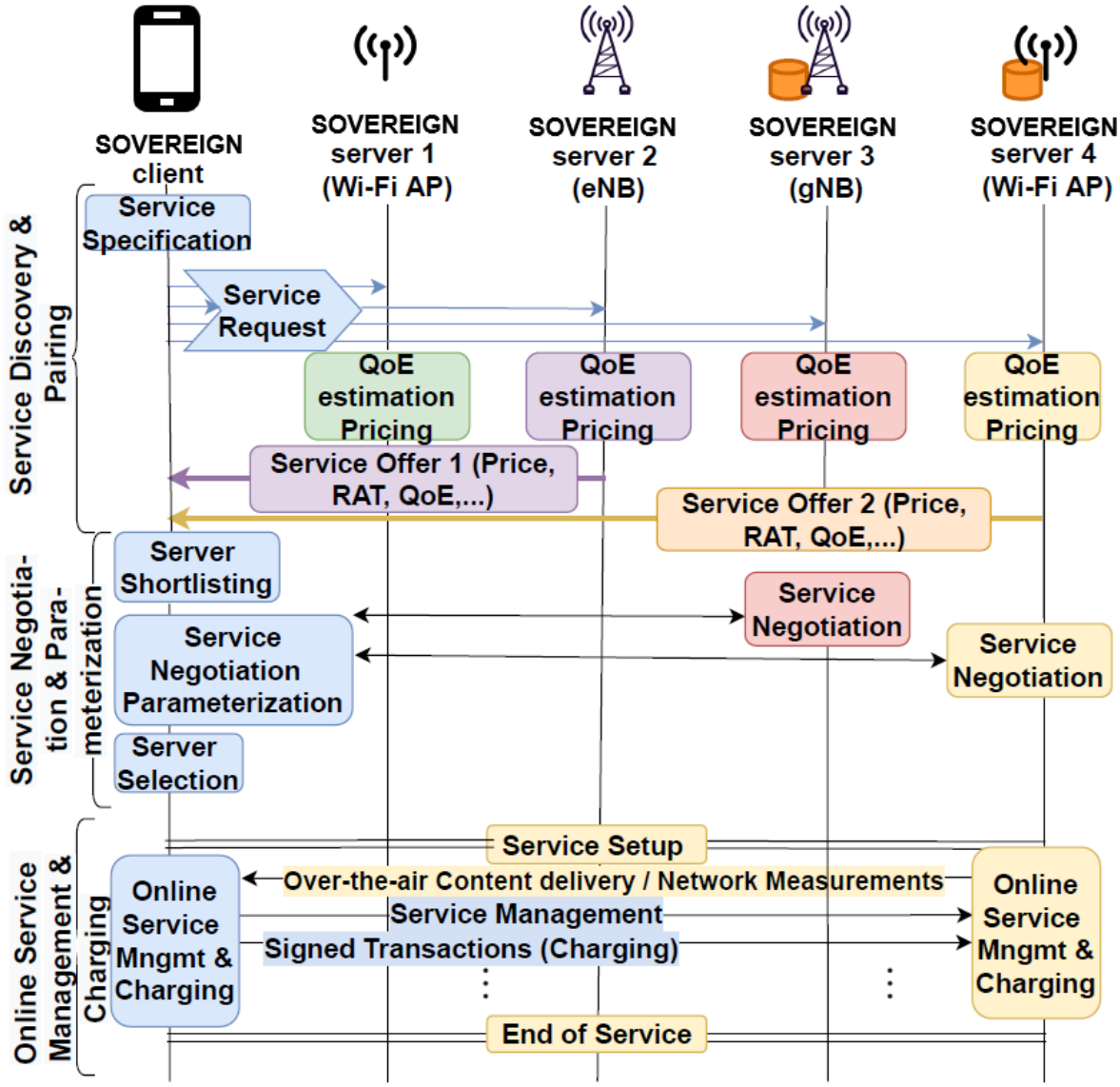

Fig. 2 The SOVEREIGN service phases

2.4.1. Service Discovery and Pairing

Service discovery and pairing is the inextricable prelude for any network-level service. During this phase, SOVEREIGN clients communicate their service requirements to SOVEREIGN servers, specifying necessary parameters regarding the target content (e.g. URL, author, keywords) and the target QoE key performance indicators KPIs (section III.B.1). SOVEREIGN servers should advertise their available network asset pools and respond to the service requests with targeted offers, also specifying necessary implementation details (e.g. RAT, resources). Service discovery and pairing can be implemented using **client-driven**, or **server-driven** approaches. Under the client-driven approach, SOVEREIGN clients shall broadcast their service requests and receive targeted service offers from SOVEREIGN servers that are interested in serving the tagged request. Under the server-driven approach, SOVEREIGN

servers shall advertise their available asset pools, including locally cached content, data rates for Internet connectivity, tariff list, etc., and SOVEREIGN clients shall filter service offers to select the most suitable server (service pairing).

Apart from the approach used to communicate service requests and offers, the medium through which this process is implemented plays a key role in the overall robustness of the blockchain-backed mobile trading platform. Service discovery and pairing can be implemented using **network-level**, or **blockchain-level** interactions. Network-level interaction enables the SOVEREIGN service peers to communicate their requests/offers off-chain, exchanging local network messages over-the-air. On the other hand, blockchain-level interaction enables the SOVEREIGN service peers to advertise their requests/offers in the public ledger, enabling on-chain service discovery and pairing. A **mixture** of both methods can take place as well: i) on-chain service requests by SOVEREIGN clients and off-chain offers by SOVEREIGN servers, or ii) on-chain advertisements by SOVEREIGN servers and off-chain service requests by SOVEREIGN clients.

Although on-chain service discovery and pairing is appealing, due to the transparency and immutability offered when the service data are recorded on-chain, it also comes with enormous on-chain costs and transactions throughput overheads. Taking into consideration i) the large volume of available network assets worldwide (e.g. billions of content), ii) the large number of service peers in a 5G ecosystem (e.g. 50B devices by 2025 [UOA-2], iii) the dynamic nature of the wireless medium and iv) the negative impact of user mobility on the 'freshness' of service requests/offers [UOA-3], keeping asset requests/offers up-to-date on a per service peer basis, updating the tariff list on a per asset/server basis, or filtering and extracting service requests/offers from the public ledger, is not scalable with current blockchain-backed systems. Since the mobile video content delivery necessitates physical proximity between the service peers, network-level service discovery and pairing is more practical, mitigating on-chain costs and transactions capacity overheads for service control over the public ledger. User-driven service discovery and pairing is also more relevant with the case study under scope, as it enables reactive service control whenever necessary and mitigates the requirement for a large number of messages for the proactive advertisement of generic service offers.

Under the SOVEREIGN mobile content trading platform, service discovery and pairing is implemented using network-level interactions between the service peers in a user-driven fashion. SOVEREIGN clients broadcast their requests over-the-air and SOVEREIGN servers reply with targeted offers using network-level protocols. The main steps of the SOVEREIGN service discovery and pairing phase are illustrated in Fig. 2. A discussion of how this process can be integrated in Rel. 18/19 of the 3GPP 5G system will provided in the next project deliverable D2.2.

2.4.1.1. QoS/QoE-estimation

SOVEREIGN clients should be able to specify all parameters of mobile video consumption (Fig. 2), e.g., min/average video bitrate, delay tolerance, packet loss rate, available buffer, target screen resolution. Similarly, the SOVEREIGN server should be able to estimate its capability to carry out a service request on the basis of the parameters specified by the SOVEREIGN client and the locally available asset pools (content, spectrum, Internet connectivity, processing and storage capacity, RAT interfaces, etc.). Current literature on QoS/QoE estimation is vast [UOA-4], including a wide range of KPIs and methodologies for QoS/QoE service provisioning at both the client and the server sides. QoS/QoE parameter values specified during this phase, are formalized and adjusted during the negotiation and parameterization phase (section III.C).

2.4.1.2. Asset Pricing

Asset pricing refers to the logic followed by the SOVEREIGN servers to conclude on the tariff they should offer to SOVEREIGN clients depending on the received service requests, availability of local network assets and the service offers provided by other servers. SOVEREIGN servers shall follow their own **asset pricing strategy** and communicate their offers using network-level protocols. Asset pricing should account for the target QoE KPI values specified in the service request message. For example, a higher video bit rate would increase the service cost, e.g. users with larger screen resolutions consume more spectrum resources. The RAT used to implement the last hop of the content delivery service also plays a key role on the pricing strategy, e.g. unlicensed spectrum typically incurs lower costs but lower QoE guarantees. The robustness (supported rates, on-time, jitter, etc.) and cost of backhaul links available for implementing the end-to-end content delivery chain should also be considered. If a costly backhaul connection is used to reach distant Internet servers, asset pricing should adapt accordingly. Service costs shall not only account for the cost of utilized spectrum, but should additionally incorporate depreciation and operation costs, e.g. purchase of equipment, energy consumption.

Asset pricing can also take into consideration the current status of the local market. SOVEREIGN servers can be part of a larger cluster of servers that aim to increase their reputation, or local market share, offering lower prices to attract new users. A higher price can be also requested if the SOVEREIGN server monopolizes the local asset trading market, or it is widely accepted as trusted. Another important pricing parameter is the availability of requested content in the near area. For example, the server can exploit its local storage resources to fetch popular content in its local cache and lower the price of popular video chunks. In this scenario, the effectiveness of the content placement strategy, which involves content popularity prediction and optimized local storage management, will be clearly a competitive advantage in light of an open Beyond 5G mobile data trading market [UOA-5]. Besides, lower prices can be attained if the server is part of a larger content caching and

delivery ecosystem that extends Information-Centric Networking (ICN) to Asset-Centric Networking (ACN), a concept that will be within the scope of the project.

2.4.2. Service Negotiation and Parameterization

During this phase, the SOVEREIGN server employs its own strategy to select the most suitable SOVEREIGN server (service offer selection in Fig. 2 and interact at the network-level towards service parameterization. Having received the offers of nearby SOVEREIGN servers, SOVEREIGN clients shall deploy their own **server selection strategies** to shortlist service offers. During this process, the SOVEREIGN client should take into consideration criteria regarding i) the price included in the offer, ii) the RAT options available by the SOVEREIGN server, iii) the QoE KPI values specified in the offer, iv) the reputation of the SOVEREIGN server (e.g. servers of large MNOs can be considered as trusted) and v) other service implementation options provided by the server (e.g. support of a given codec, use of minimum encryption). After shortlisting the offers, SOVEREIGN clients shall negotiate with shortlisted SOVEREIGN servers important service parameters spanning the entire protocol stack. Firstly, service peers shall conclude on the target QoE KPIs, having as a starting point the original service request/offer messages. Secondly, they should specify the RAT technology to be utilized, the spectrum bands through which the delivery will take place, security parameters regarding the encryption protocol, etc. Thirdly, if a payment relay (or mixing) service is to be utilized (sections IV.C and IV.D), i.e. to reduce on-chain costs necessary to implement service charging, or use micro-payments, service peers should further agree on the payment relay.

To select SOVEREIGN server(s), SOVEREIGN clients shall take into consideration network-level parameters specified during the service negotiation phase (mentioned above) as well as blockchain-level parameters, such as the on-chain balance of candidate SOVEREIGN servers (SOVEREIGN with increased stake in the system can be considered as more credible), the requested amount of coins for the target service, or other roles assigned to the public address of the server (e.g. FoC server). Multiple servers can be also utilized to meet the service requirements set by the SOVEREIGN client, e.g. using multi-source dynamic adaptive streaming over HTTP. Even though the decision context of the server selection process is enlarged with blockchain-level parameter values, SOVEREIGN server selection can be implemented using existing protocols optimization tools, e.g. dynamic programming, convex optimization, machine learning and online convex optimization. For example, SOVEREIGN clients can shortlist SOVEREIGN servers based on whether they meet the target QoE KPIs (Fig. 2 and select the SOVEREIGN server requesting the minimum amount of coins. SOVEREIGN clients that have also acted as validator (or relay) witnesses may choose to prioritize access to FoC servers. Thus, the SOVEREIGN server selection software shall be implementation-specific, enabling end users to adjust the selection according to their preferences, operational requirements and functional capabilities.

SOVEREIGN service peers should a-priori specify a **payment timeplan** that will allow progressive charging and delivery of the content delivery service, emulating fair-exchange of assets and payments while enforcing a certain level of trust among the service peers. The payment timeplan should specify both the timing and amount of intermediate payments throughout the entire service lifespan, using a pay-per-video-chunk model. An a-priori agreed payment timeplan guarantees that the client will issue the rightful amount of payments for every video chunk it receives from the server, and vice versa. If the client fails to deliver intermediate payments to the server, the video service delivery shall be interrupted. On the contrary, if the server fails to deliver a video chunk within the agreed time interval, the client can abort the protocol.

Service setup can be formalized by posting the outcome of service negotiation and parameterization on-chain, e.g. using SCs [UOA-6]. SCs can be subsequently triggered to resolve potential disputes between the service peers, allowing also other SOVEREIGN clients to infer on the credibility of SOVEREIGN servers. Nonetheless, the deployment of a SC on a per session/service peer basis is not scalable, as it will generate an excessive amount of on-chain costs and transactions capacity overheads only for service control, hindering the implementation of the actual service itself. Besides, the SOVEREIGN peers may choose to abort the service (e.g. YouTube clients typically watch a small part of YouTube videos), or even re-negotiate service parameters on-the-go (e.g. to lower the bitrate and adapt it to the status of the wireless medium), questioning the practical benefits of posting on-chain P2P SLAs. Furthermore, dispute resolution mechanisms that validate the network service status in an on-chain fashion are not easy to implement as they should employ RAT-specific protocols and mechanisms, greatly increasing the complexity of the SC logic and on-chain execution cost.

In our platform, we consider that an a-priori agreement on the key service parameters at the network-level provides sufficient formalization, mitigating unnecessary increase of the transactions throughput towards on-chain service control. However, we also note that the timing and amount of payments agreed in the payment timeplan will play a key role in preserving the credibility and sustainability of the SOVEREIGN blockchain-backed mobile video service.

2.4.3. Online Service Management and Charging

During this phase, the client and the server should take all necessary actions to establish, maintain and terminate the mobile video service at the network-level. At the blockchain-level, the service peers should follow the payment timeplan agreed during the service negotiation and parameterization phase to implement blockchain-backed charging by employing either direct on-chain P2P payments, or off-chain through SC-certified payment relays. The agreed payment timeplan can be tight in case of video service delivery among untrusted peers, or can be implemented by a single transaction when full trust can be assumed. When using

payment relays, the relay server shall follow the agreed payment timeplan and act on behalf of the client to issue legitimate payments to the SOVEREIGN server. Depending on the SC logic, the relay server can update the balance of the server in the public ledger within a prescribed time period that is acceptable by the server (relay delay). If the client/server have an established payment channel with the relay, the respective amount of payments can be aggregated to further reduce the amount and cost of on-chain payments. Network-level interactions are also necessary to attain service continuity, handle mobility management and deploy QoE-driven service provisioning. Under the SOVEREIGN mobile data access model, the service management logic is shifted to the client side assuming *user-driven network-assisted service provisioning*. The client is fully responsible for predicting potential service discontinuity (e.g. either due to unreliable SOVEREIGN server selection, or due to user mobility), taking mitigation measures whenever necessary and encompassing network measurements provided by the server (Fig. 2).

The employment of user-driven QoE provisioning is also assumed under the SOVEREIGN mobile data access model. Existing QoE estimation methodologies can be used to this end, whereas HTTP adaptive video streaming (HAS) for end-to-end video playback management is another relevant technology that enables end users to adapt video quality based on the availability of network assets at the server side or the channel status [UOA-4]. To this end, novel QoE management mechanisms can be utilized to enable sufficient network exposure from MNOs to the SOVEREIGN clients and video content providers, enabling network-aware video segment selection and caching in the context of HAS. Since service discovery and pairing is implemented using network-level protocols, we consider that an adjustment of the QoE parameters specified in the service negotiation and parameterization phase is handled at the network-level, i.e. by taking necessary corrective measures at the network level, or by allowing the SOVEREIGN client to abort the service without a blockchain-level penalty. Additional interactions at both the blockchain and network levels might be necessary to implement the logic of the mixing service and mitigate the network/blockchain ID coupling problem. SOVEREIGN servers can further create a virtual common pool of network assets that are organized in such a way that allows asset-centric networking (ACN), including service placement, discovery and delivery, moving forward from the host-centric networking model that has dominated IP-based systems over the past decades. ACN shall extend ICN architectures that leverage in-network storage for caching, multiparty communication through replication, and interaction models decoupling senders and receivers.

3. State-of-the-art tools and platforms relevant to SOVEREIGN

3.1. Tools and platforms for supporting mobile connectivity in Beyond 5G systems

3.1.1. Commercial-grade 5G infrastructure available by IT

IT has the following equipment: i) an EG5120 Industrial Edge Computing Gateway, and ii) a set of Tmote Sky sensors.

3.1.1.1 EG5120 Industrial Edge Computing Gateway

To implement the connection between the different networks, we utilize a gateway that performs the necessary computing functions to establish these connections between networks. The equipment we intend to use is the EG5120 Industrial Edge Computing Gateway, as shown in Fig. 3.

Fig. 3 EG5120 Industrial Edge Computing Gateway

Robustel's EG5120 is a new generation of industrial edge computing gateway, supporting global 5G/4G/3G/2G cellular networks. It features a fully-fledged Debian 11 (bullseye) operating system, enabling the support of thousands of existing or new ARMv8-based applications, making it compatible with Raspberry Pi. This gateway supports Docker to deploy applications easily from “RobustOS Pro”, the Robustel’s latest router OS [IT-1]. The EG5120 is equipped with a quad core 1.6 GHz Cortex A53 CPU and an integrated neural processing unit (NPU) capable of 2.3 TOPS, significantly accelerating machine learning inference. This makes it ideal for edge computing and edge AI applications, and it can also function as a combination of a cellular router and an embedded PC across various industrial fields [IT-1].

The key features of the EG5120, as provided by the manufacturer, are as follows [IT-1]:

- Highly stable 5G/4G/3G/2G cellular connectivity with global band coverage
- High performance compute engine with 1.6 GHz CPU + 16 GB eMMC Flash for running complex applications
- ‘Docker’ containerization supported
- Cutting-edge (Release 16) 5G interface
- Microsoft Azure IoT and AWS IoT Greengrass qualified
- 802.11ac Wi-Fi (optional) supporting AP and Client modes
- Bluetooth (optional), Bluetooth 5.2 compliant
- 2 x RS232/RS485 (software configurable) ports for connection to industrial/legacy devices
- 2 x DI & 2 x DO for simple monitoring and control
- Dual SIM card slots for redundant communications
- Wide Operating Temperature range for industrial applications
- Full Modbus TCP and Modbus RTU support including MQTT transfer to mainstream cloud platforms
- Supports C, C++, Java, Python, Node.js etc. for users to develop their own applications
- More than 50,000 applications from Debian repository are currently available
- Wireguard/IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN + more VPN options
- Supports RCMS – Robustel’s router/gateway management platform for effective management of large estates of devices

3.1.1.2 Tmote Sky sensors

The Tmote Sky is a wireless module, shown in Fig. 4, designed for use in sensor networks, monitoring applications, and rapid application prototyping. This ultra-low power device can seamlessly interoperate with other devices through the industry standards such USB and IEEE 802.15.4. Tmote Sky enables a wide range of mesh network applications by providing flexible interconnections with various peripherals. It is compatible with ContikiOS, an open-source operating system tailored for the Internet of Things (IoT), which facilitates the rapid development of IoT applications [IT-2].

Fig. 4 The Tmote Sky hardware platform

Tmote Sky offers many features, including:

- 250kbps 2.4GHz IEEE 802.15.4 Chipcon Wireless Transceiver
- Interoperability with other IEEE 802.15.4 devices
- 8MHz Texas Instruments MSP430 microcontroller (10k RAM, 48k Flash)
- Integrated ADC, DAC, Supply Voltage Supervisor, and DMA Controller
- Integrated onboard antenna with 50m range indoors / 125m range outdoors
- Integrated Humidity, Temperature, and Light sensors
- Ultra-low current consumption
- Fast wakeup from sleep (<6μs)
- Hardware link-layer encryption and authentication
- Programming and data collection via USB
- 16-pin expansion support and optional SMA antenna connector
- TinyOS support: mesh networking and communication implementation
- Complies with FCC Part 15 and Industry Canada regulations
- Environmentally friendly – complies with RoHS regulations

Module Description

The Tmote Sky module is a low power "mote" that integrates sensors, a radio, an antenna, a microcontroller, and programming capabilities among others. Fig. 5 presents the front and back views of the Tmote Sky module, highlighting its various components.

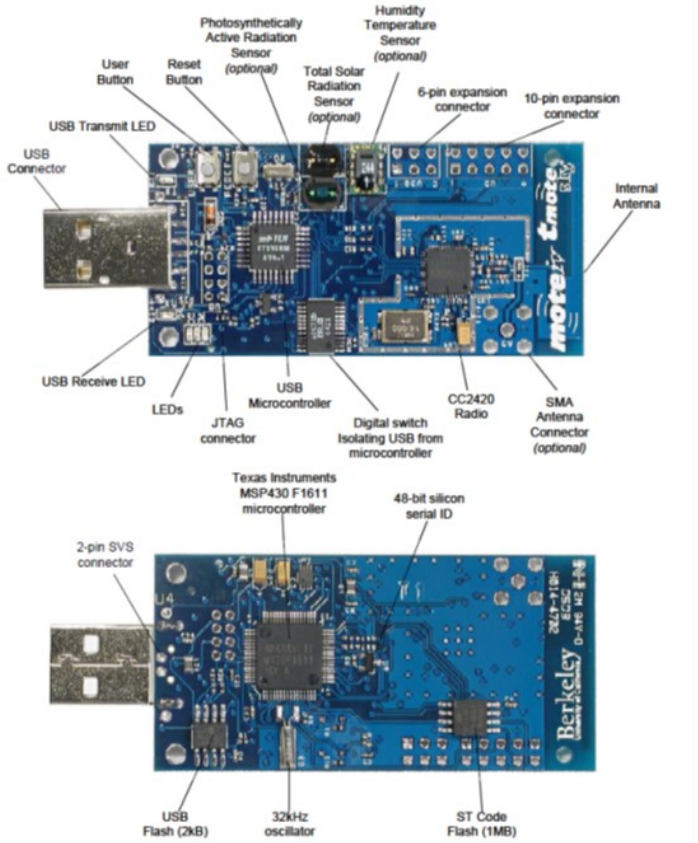

Fig. 5 Front and Back of the Tmote Sky module

Power

The Tmote Sky module can be powered by two AA batteries or through its USB port. Although it operates within a voltage range of 2.1 V to 3.6 V DC, it needs a minimum voltage of 2.7 V when programming the microcontroller flash or external flash. When connected to USB for programming or communication, it draws power from the host, and the operating voltage is set to 3 V. It is crucial that the voltage does not exceed 3.6 V, as doing so may damage the microcontroller, radio, or other components.

Microprocessor

The Tmote Sky is equipped with an ultra-low power Texas Instruments MSP430 F1611 microcontroller, featuring 10 kB of RAM, 48 kB of flash memory, and 128 B of information storage. The 16-bit RISC processor exhibits extremely low current consumption that permits the Tmote Sky to operate for years on a single pair of AA batteries. The MSP430 can run at speeds up to 8MHz, utilizing an internal Digitally Controlled Oscillator (DCO) that can be turned on from sleep mode in 6µs. However, the typical wake-up time is around 292 ns at room temperature. When DCO is off, the MSP430 operates using a 32,768 kHz external clock crystal. In addition to its processing capabilities, the MSP430 provides 8 external and 8 internal ADC ports. Furthermore, a variety of peripherals are available, including SPI, UART,

digital I/O ports, a watchdog timer, and timers with capture and compare functionality.

PC Communication

The Tmote Sky uses an FTDI USB controller to communicate with the host computer. To establish communication with the Tmote, the host computer must have the appropriate drivers installed. The Contiki software package already includes these necessary drivers. When connecting multiple Tmote Sky modules to a single host, each mote is assigned a different COM port identifier, allowing for easy differentiation and management of devices.

Programming

To program the Tmote Sky, it connects through the onboard USB connector and programmes the microcontroller flash using a modified version of the MSP430 Bootstrap Loader, called msp430-bsl. The Tmote Sky features a unique hardware circuit that generates a special sequence sent to the module during programming, preventing the mote from inadvertently resetting.

Radio

The Tmote Sky is equipped with a wireless communications radio, the Chipcon CC2420, which complies with the IEEE 802.15.4 standard, providing both physical (PHY) and some medium access control (MAC) functionalities. This radio ensures reliable wireless communication while maintaining low power consumption, and its sensitivity exceeds the requirements set by the IEEE 802.15.4 specifications. The CC2420 is controlled through an SPI port, along with several digital I/O lines and interrupts. Besides, the CC2420 includes a digital received signal strength indicator (RSSI) for enhanced performance monitoring.

Antenna

Tmote Sky features an Inverted-F microstrip antenna located at the end of the board, away from the battery pack. This internal antenna is a wire monopole with a less-than-perfect omnidirectional pattern, providing an indoor range of up to 50 meters and an outdoor range over 125 meters.

Humidity and Temperature Sensor

The humidity and temperature sensor is directly integrated into the Tmote. The SHT11 and SHT15 models are factory-calibrated, with the calibration coefficients stored in the sensor’s onboard EEPROM. The CMOS sensor is coupled with a 14-bit A/D converter, which produces a digital output. Its compact size and low power consumption make it suitable for various

environmental monitoring applications.

Light Sensors

Tmote Sky can utilize a variety of light sensors. It is equipped with two photodiodes that are capable of sensing the entire visible spectrum, including infrared light. These sensors enable the Tmote Sky to effectively monitor light conditions in various environments, making it suitable for diverse applications such as environmental monitoring and smart agriculture.

Expansion Connector

The Tmote Sky module can control additional peripherals devices, including analogue sensors, LCD displays, and digital peripherals, through its two expansion connectors and a pair of configurable onboard jumpers. These features allow for flexible integration with various components, enabling users to customize their applications according to specific needs.

3.1.2. Advanced Mobile Wireless Network playground available by IT

3.1.2.1 IoT Network Playground

IT has available an IoT network that includes various IoT devices such as Tmote Sky sensors, which monitor environmental parameters. This network also includes a 5G-enabled gateway, specifically the EG5120 Industrial Edge Computing Gateway, which facilitates the transmission of collected sensing data to a central system for analysis. This IoT network, also shown in Fig. 6, comprises the perception domain of an IoT-based monitoring system and enables real-time monitoring and data collection. This capability allows stakeholders to make informed decisions based on accurate and timely information.

In particular, the environmental Tmote Sky sensors measure critical factors including temperature, humidity, and light levels. These measurements are essential for understanding environmental conditions and can inform various applications, from agriculture to urban planning. On the other hand, the 5G-enabled gateway (i.e., EG5120 Industrial Edge Computing Gateway) plays a crucial role in enabling seamless communication between these sensors and cloud-based platforms. By leveraging high-speed connectivity, the gateway allows for rapid data transmission, which is vital for applications requiring immediate insights. This integration enhances the overall efficiency of the monitoring system, enabling organizations to respond proactively to any changes or anomalies detected in the monitored parameters [IT-3, IT-4].

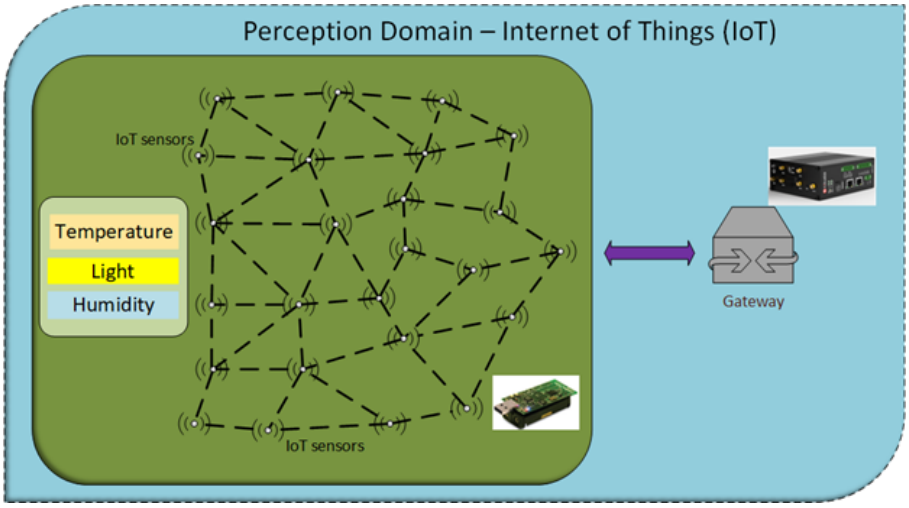

Fig. 6 IoT edge network architecture and key components

In principle, by utilizing this technology, organizations can significantly enhance their environmental management practices. For instance, real-time data from Tmote Sky sensors can help farmers optimize irrigation schedules based on current soil moisture levels, leading to more efficient water usage. Similarly, urban planners can utilize environmental data to improve air quality monitoring and implement measures to address pollution. Furthermore, the architecture of this IoT network is designed for scalability and adaptability. It can seamlessly integrate additional sensors and devices as needed, ensuring its continued effectiveness as monitoring requirements change. The incorporation of advanced analytics capabilities enables predictive maintenance and anomaly detection, allowing organizations to reduce downtime and improve operational efficiency [IT-3, IT-4].

In conclusion, this IoT network not only enables comprehensive environmental monitoring but also empowers stakeholders with the necessary tools for data-driven decision-making. By harnessing the capabilities of Tmote Sky sensors and a 5G-enabled gateway, such as EG5120 Industrial Edge Computing Gateway, organizations can effectively manage their environmental impact and quickly respond to emerging challenges [IT-3, IT-4].

3.1.2.2 Contiki OS and Cooja Simulator

Tmote Sky sensors [IT-5] operate using the Contiki operating system, a lightweight OS designed for the Internet of Things (IoT). Contiki provides a flexible platform for developing applications on resource-constrained devices, such as the Tmote Sky. It is an open-source and highly portable system written in C programming language that employs a hybrid model based on an event-driven kernel and preemptive multithreading implemented as a library on a per-process basis. A typical configuration of Contiki requires approximately 2kB of RAM and 40kB of ROM, making it suitable for devices with limited resources.

The Contiki programming model is based on protothreads, which provide a memory-efficient programming abstraction that combines features of both multithreading and event-driven programming, resulting in low memory overhead for each protothread [IT-6]. In addition, Contiki OS supports a range of networking protocols, enabling efficient communication between devices and facilitating data transmission to cloud services for analysis. This flexibility allows developers to create robust IoT applications that can operate effectively in resource-constrained environments.

The standard Contiki installation includes a multitasking kernel, optional preemptive multithreading, protothreads, TCP/IP networking, IPv6, a web browser, a web server, a simple telnet client, and virtual network computing [IT-6]. Also, it offers a network simulator called Cooja, which allows users to create network simulations using the same firmware as the actual devices. This capability enables the connection of simulated networks to real devices and to the Internet, facilitating comprehensive testing and development of IoT applications.

The Cooja simulator is the companion network simulator for the open-source Contiki Operating System, specifically designed for Wireless Sensor Networks and built in Java. The nodes simulated in Cooja are compiled and executed as if they were part of a real Contiki system. Cooja includes tools that allow users to control and analyze the system by compiling Contiki as a shared library and loading it into Java. The Cooja simulator can load different libraries within the same simulation, enabling the simulation of various types of sensors. Cooja employs several functions to control and analyze the Contiki system [IT-7]. A Cooja simulation can connect to the Internet through a gateway commonly referred to as a border router. The border router is an IoT device programmed to use the Contiki tool “tunslip6” (located in “tools/tunslip6”) over the serial port, creating an interface between IoT devices and the Internet [IT-7].

3.1.3. 6G-SpaceLab available by ULU

At the 6GSPACE Lab situated within the Interdisciplinary Centre for Security, Reliability and Trust SnT-University of Luxembourg, we conduct innovative research in the field of **6G communication systems and space technology.** ULU’s main goal is to promote innovation, foster collaboration, and contribute significantly to the development of 6G technology and space science. We intend to establish a seamless combination of terrestrial, satellite, and space-based networks that will revolutionize how we connect, communicate, and explore the universe.

Research Area

Satellite communication allows a vast coverage area beyond terrestrial systems, connects far-off sites without existing infrastructure, and has the capacity to transmit signals to thousands

of users simultaneously. To develop a future communication system that bridges the gap between Earth and space, 6GSpaceLab conducts cutting-edge research in several areas.

- **6G Research**: We are pioneers in 6G communication systems, exploring the next generation of wireless technology. Our research spans areas such as satellite communications, non-terrestrial networks, edge computing, integrated sensing and communications, hybrid communications and positioning, and AI and machine learning integration in 6G networks.
- **Space Technology**: We are actively involved in space technology research, focusing on developing advanced deep-space communication systems, interplanetary internet, lunar telerobotics, and energy-efficient signal processing.
- **Interdisciplinary Collaboration**: We believe that breakthroughs happen at the intersection of disciplines. Our lab promotes cross-disciplinary collaboration between telecommunications, electronics, robotics, space systems experts, and more. The 6GSPACE lab is physically interconnected with other interdisciplinary SnT facilities.

ULU's lab stands as a symbol of transformative scientific collaboration. Here, quantum physics intertwines with sixth-generation wireless communication, lunar research, and the enigmas of zero gravity. Enabled by our dedicated optical fiber network, these fusion promises to reshape our cosmic understanding and technological horizons.

Projects

The 6GSpaceLab collaborates with industry partners, academic institutions, and international organizations to lead groundbreaking research in space-terrestrial communication networks.

The following presents a selection of key projects realized at the 6GSPACElab, each designed to explore innovative solutions for the integration of terrestrial and non-terrestrial networks. The following is a list of projects that have been realized in our lab, along with some that are still ongoing:

- COSMIC: Direct-to-Device Communications in Mobile Satellite Systems Using C-band
- JuliaSatSim: Satellite Simulator in JULIA language
- 5G-EMERGE: Satellite-enhanced edge delivery
- TANNDEM: DEMODULATOR SUPPORTED BY ARTIFICIAL NEURAL NETWORKS
- 5G-Nanosatellite
- 5G-LEON: RADIO POSITIONING TECHNOLOGIES FOR 5G SATELLITE NETWORKS
- SATNEXT V. WI Y3.3 LEO-PNT
- TRANTOR: 5G+ Evolution to Multiorbital Multiband Networks
- ESA NGSO-Sense: Prototype for Measuring NGSO Satellite Network Interference and Radiofrequency Characteristics

- PROSPECT: High data rate, adaptive, internetworked proximity communications for Space
- 5G-LEO: OpenAirInterface™ Extension for 5G Satellite Links
- SPAICE - Satellite Signal Processing Techniques using a Commercial Off-The-Shelf AI Chipset
- SAT-SPIN - Satellite communication via space-based internet service providers
- SAFER: Demonstration of SAFE electromagnetic Radiation emitted by 5G active antennas systems
- SAFER: Demonstration of SAFE electromagnetic Radiation emitted by 5G active antennas systems
- 5G-GOA - 5G-Enabled Ground Segment Technologies Over-The-Air Demonstrator
- Micro5G: Mobile Edge Computing for 5G DROne Systems
- IRANATA - Interference and RAdiation in Network PlAnning of 5G AcTive Antenna Systems
- 5G-SpaceLab: 5G Space Communications Laboratory
- 5G-Sky: Interconnecting the Sky in Beyond 5G – A Joint Communication and Control Approach

Facilities and Equipment

The 6GSpaceLab (Fig. 7) has very advanced equipment and technologies supporting our research. The list of our publications is a direct outcome of the possibilities offered by these materials and technology. Every piece of equipment is critical to allowing our innovative ideas, from cutting-edge communication systems to complex analytical instruments.

Fig. 7 6GSPACELab

Our lab is equipped with the advanced Universal Software Radio Peripherals (USRPs) that enable rapid prototyping and deployment of wireless communication, Signal Intelligence,

Radar, and Embedded Systems. As shown in Fig. 8, in 6GSPACELab, we have different USRP models varied from Networked, Bus, Embedded, and X Series such as X310, N310, and many.

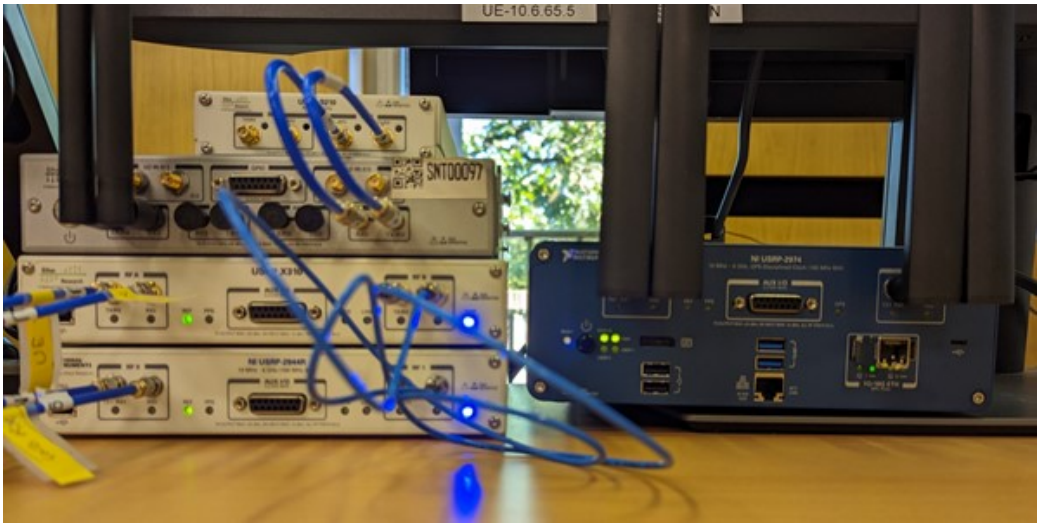

Fig. 8 Software Defined Radios

Additionally, the 6GSPACElab is equipped with Zynq UltraScale and RFSoCs that integrate cutting-edge technology using them for 5G and LTE wireless applications, Remote-PHY for cable access and satellite communications. And for running our application we use various workstations, computers, laptop, and Mini PC presented in Fig. 9. Finally, for research in artificial intelligence and digital signal processing, 6GSpaceLab has very powerful AI-Capable Chips.

Fig. 9 Processing Units

We efficiently handle the network devices in our lab by using the NetBox program. By streamlining inventory management, monitoring device configurations, and improving

network organization overall, this robust platform helps us guarantee optimal performance and dependability in our research operations. We use the NetBox tool to manage the network devices in the 6GSPACElab efficiently. Netbox allows us to optimize inventory management, track device configurations, and improve network structure, resulting in optimal performance and reliability in our research operations.

Demo

In the following, we will showcase practical applications showing efficiency and adaptability of the already mentioned resources.

- **NTN Over-The-Satellite:** The main objective of this project is to test the feasibility and performance of 5G connectivity over GEO satellites. So, we use a software-defined radio (SDR) platform and an open-source 5G software stack to establish the 5G radio access network (RAN) over the satellite GEO channel. We measure the key performance indicators (KPIs) of 5G over GEO. As a result, we achieved the MCS 17 in the downlink, which corresponds to 64-QAM modulation and rate 3/4 convolutional coding. This means that we can transmit 6 bits per symbol and have a coding rate of 0.75, which results in a high spectral efficiency and error performance. Fig. 10 presents a demo of the project.

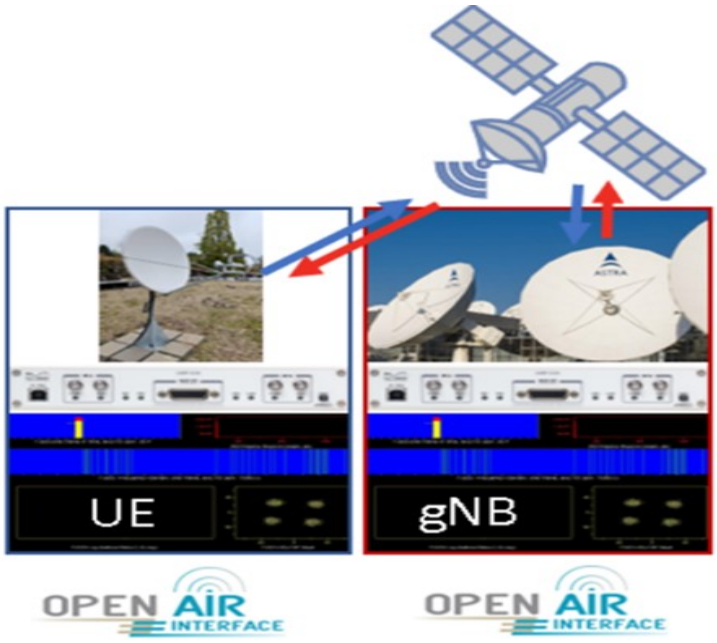

Fig. 10 NTN Over-The-Satellite demo

- **NTN Emulation:** For this project, 6GSPACElab joint project of the CDF, CubeSatLab, LunaLab and SatComLab to create a unique integrated and interdisciplinary space communications and control emulation platform for the next-generation of space

applications. We were allowed to test, validate and demonstrate space operations for many different scenarios that include Earth-orbiting satellite communications, Earth-Moon communications among many. Fig. 11 presents the experimental setup.

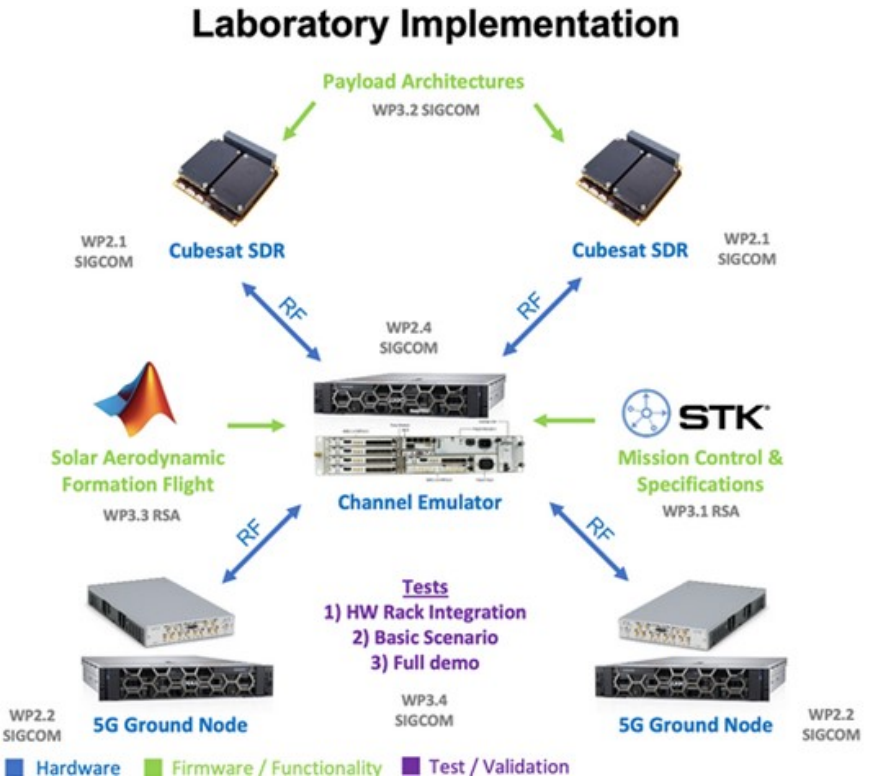

Fig. 11 The experiment setup of NTN-Emulation

- **NTN Spectrum Sensing:** The main purpose of this project is to develop a ground terminal able to identify and quantify sources of NGSO interference. The ground terminal comprises a system for measurement and characterization of the NGSO/GSO interference. As shown in Fig. 12, the system considers two antenna dishes, one for Ku-band and one for Ka-band, mounted on a metallic structure whose orientation is controlled with a 3-axis rotor system. The input signal is down converted by the Low Noise Blocks (LNBs) into several output bands. Each band can be directed to the following blocks via the Switching Matrix. The whole band can then be inspected by the Spectrum Analyzer, whereas the SDR can focus on specific areas.

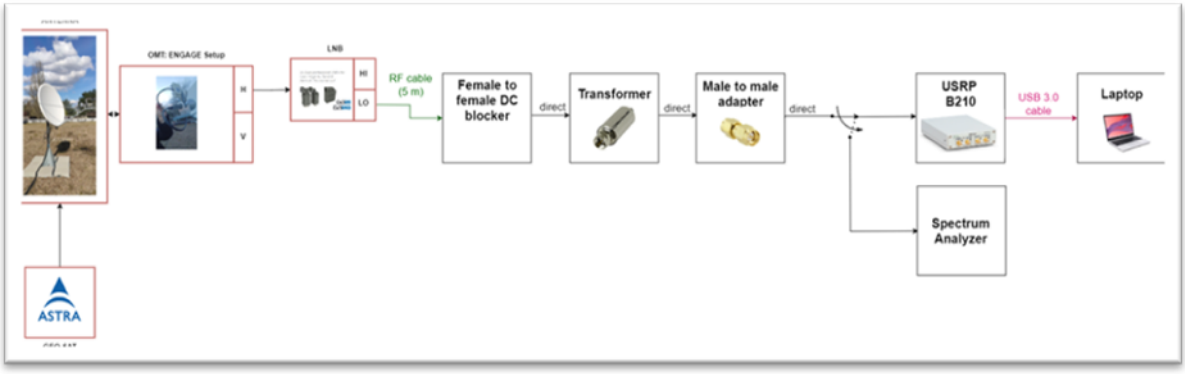

Fig. 12 The experiment setup of NTN-Spectrum Sensing

- **NTN AI-Acceleration:** in this project, we used AI-based signal processing techniques to enhance satellite communication. We did implement the architecture shown in Fig. 13. We developed methods for signal identification, spectrum monitoring, sharing, and demodulation using an off-the-shelf AI chipset. The laboratory testbed validates these techniques in both on-ground and on-board scenarios.

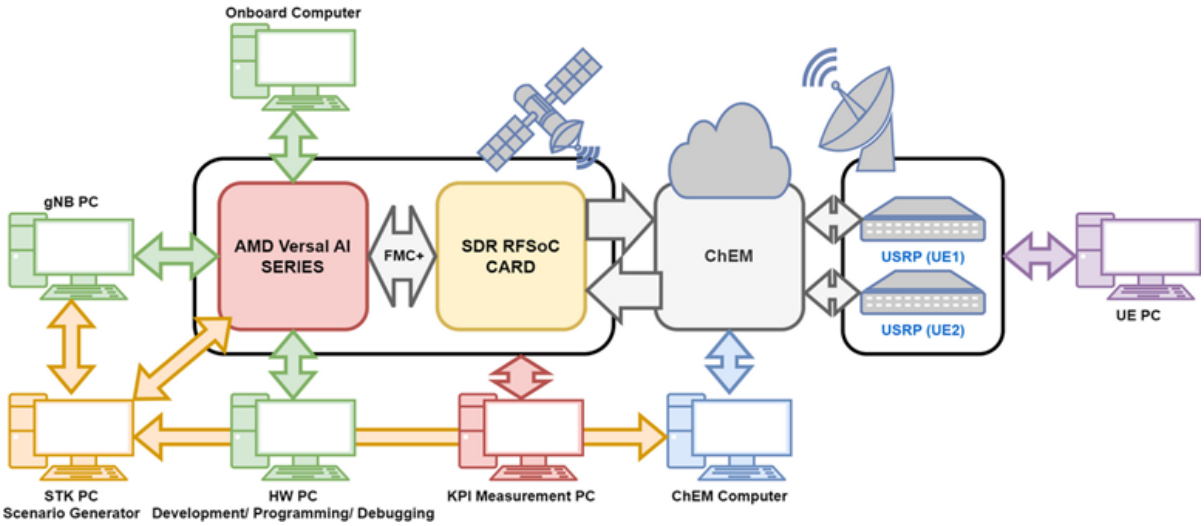

Fig. 13 The implemented architecture of NTN AI-Acceleration

3.1.4. CommLab available by ULU

The 5G NTN testbed developed at the University of Luxembourg is composed of a satellite channel emulator, spectrum analyzer, and several SDR-based end-to-end transceivers compliant with different terrestrial and satellite communication standards (e.g. DVB and 3GPP). The SDR nodes and satellite channel emulator combinedly emulate the effects of NTN scenarios, e.g., large delay, high Doppler, low SNR etc on all the layers of 3GPP 4G LTE/5G NR, i.e., **L-1, L-2 and L-3**.

The testbed is implemented using OpenAirInterface5G (OAI) and AGI STK. The 5G NTN testbed has three main parts:

- Radio Frequency (RF) Front Ends: RF front-end consists of Ettus Research SDRs: USRP B210 and USRP N310 capable of generating 4G LTE and 5G NR OFDM waveforms with the desired sampling rates.
- General Purpose Processor (GPP): For the processing of L1, L2 and L3 protocols, the testbed uses Xeon 6254 and Intel i9-10900k based high end GPP.
- Spectrum Analyzer: The testbed also consists of R & S®FSVA Signal and Spectrum Analyzer FSV3013, 10Hz-13.6GHz enabling the real time monitoring and decoding of 4G LTE/5G channels.
- Channel Emulator: The in-house developed channel emulator is implemented using a Zynq UltraScale+ RFSoC with up to eight direct RF sampling ADCs and DACs. The channel emulator can reproduce dynamically the channel conditions of the LEO/MEO/GEO scenario considering not just the static geometry, but also the antenna pattern and the attitude of the satellites, the operating frequency band and SNR of the targeted application, or the dynamic effects of the scenario such as differential propagation delay and Doppler effect. This is achieved by using the AGI STK software, which has been integrated into the channel emulator architecture. A consolidated diagram of the testbed is shown in Fig. 14 below.

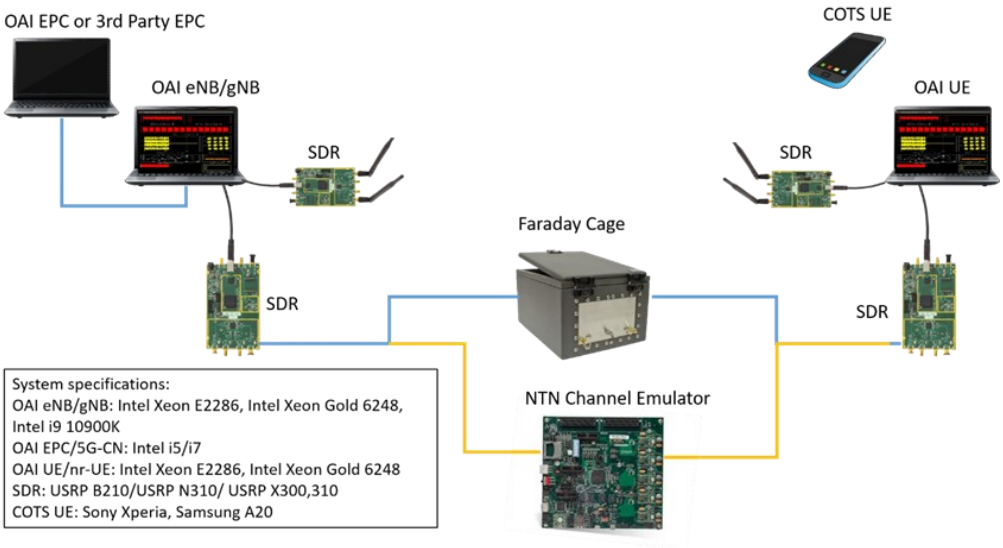

Fig. 14 Architecture of the 5G NTN testbed at SnT, University of Luxembourg

3.1.5. Beyond 5G experimental platform by IQU

Iquadrat offers a testbed that combines 5G, IoT, edge, and cloud application deployment capabilities. The testbed consists of the IoT, edge, and cloud resources, as illustrated in Fig. 15.

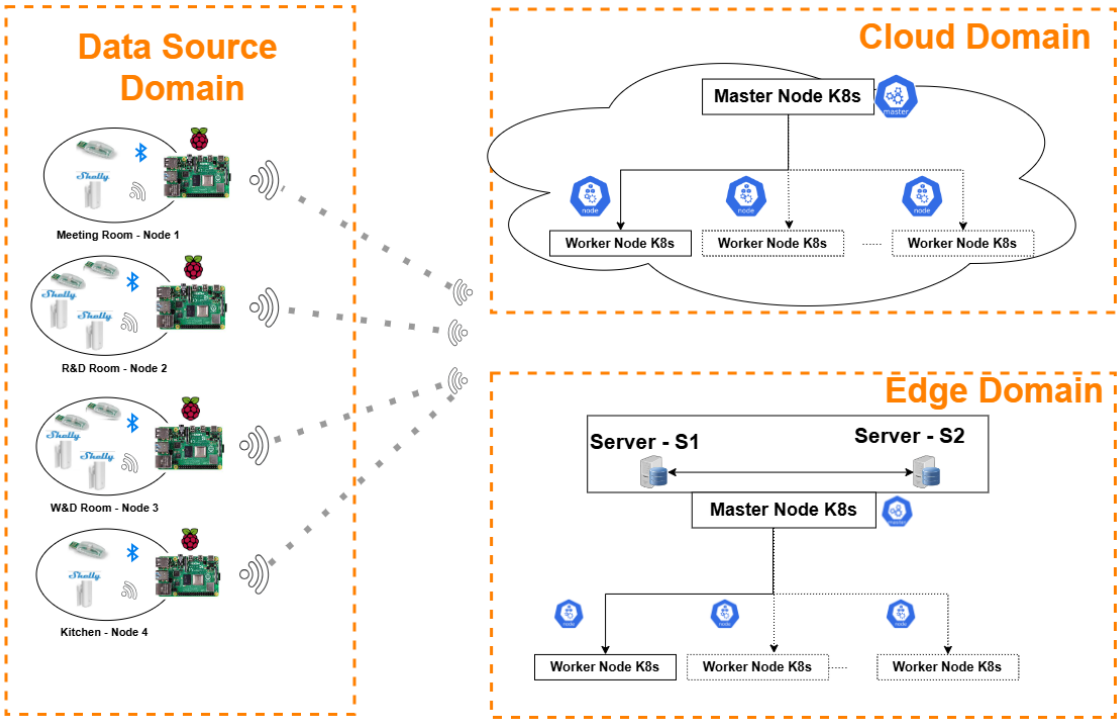

Fig. 15 IQU 5G / IoT testbed with Deep Edge deployment and local analytics.

Specifically, the testbed considers the following domains:

- **Edge Domain**: Bare metal servers S1 and S2 are utilized to create virtual machines that form a Kubernetes cluster. This setup improves resource management and scalability by enabling Kubernetes to orchestrate the containerized application of the project, across multiple virtual machines. The edge domain acts as location, where the analysis of the IoT data is as close to their source as possible, reducing communication costs and processing latency. The processing capabilities of this location is limited though and in cases of excessive traffic generated by the infrastructure processing times would increase beyond the needed SLAs.
- **Cloud Domain**: Cloud services offer access to *unlimited* resources, which would be capable of handling any data volume originating from the IoT domain. Under circumstances where the IoT infrastructures generate overwhelming data from the Edge domain, processing can be migrated to the cloud, increasing communication costs but ensuring that all data is processed respecting the SLAs of the defined. Additionally, specific services that are used for performance data collection and visualization of the data consumed by the use cases’ application will be hosted in this cloud domain. These tools enable monitoring and visualization of our local infrastructure's performance metrics. Prometheus collects data regarding the operation of our applications component’s performance, and Grafana provides interactive dashboards for data visualization, analysis and alerting.

- **Data Source Domain**: Deployed primarily for sensing, collecting, and transmitting environmental data in real-time. This domain utilizes:
    - Raspberry Pi4 & Pi5 devices: These devices are the leading platforms used in the Far Edge Domain. They are compact and cost-effective single-board computers capable of running software to manage sensor data. They are equipped with SIM8200EA-M2 5G HATs, providing 5G connectivity. However, Wi-Fi can also be used as an alternative.
    - IoT Sensors: The monitoring system uses Sensirion SCD1 CO2 sensors, and Shell Motion 2 that have been deployed as the IoT monitoring infrastructure.

The testbed, as described above, supports the following features:

- Orchestration capabilities: materialized through OpenStack and Opensource MANO (OSM) deployed in a virtualized environment.
- Monitoring System: deployment of multiple instances of the Monitoring System (MS) for data gathering and for deployment of the different enablers.
- Cloud-native Support: this is necessary to allow the flexible deployment of the enablers and to provide a federation of resources across the 5G Core Cloud and the 5G Edge Cloud Domain. A Kubernetes cluster is deployed to provide for this functionality.
- Deep Edge deployment of services, which are leveraged for performing analytics on the received sensor values, and detecting anomalies, while avoiding latencies inherent with cloud deployments.

3.2. Tools and platforms for distributed ledger technologies in Beyond 5G systems

The purpose of this section is twofold. First, it presents widely used and supported blockchain technologies. Second, it describes solutions proposed in the literature that involve the use of blockchain platforms in the context of 5G networks.

3.2.1. Blockchain/DLT platforms relevant to 5G/B5G

There are five blockchain/DLT platforms that are highly relevant to the application context of the SOVEREIGN project.

Hyperledger Fabric [IQB-1] is a blockchain platform that is open-source, allowing organizations to create and manage their own distributed ledger systems. It offers essential tools and frameworks for developing blockchain-based applications in the insurance sector, featuring capabilities like smart contracts, privacy controls, and controlled access. One of Hyperledger Fabric's key strengths lies in its ability to execute smart contracts, which can automate processes such as billing based on usage data collected in real-time across the 5G network, quick settlements, and transparency between service providers and customers. Moreover, it supports the creation of private channels, restricting data access to a designated group of participants. This can enhance a 5G network's privacy and enable secure sharing of data among authorized parties. This is particularly useful in scenarios that involve IoT networks, where multiple devices may need to share sensitive information. Additionally, Hyperledger Fabric's support for pluggable consensus mechanisms allows organizations to choose the most suitable consensus algorithm tailored to their specific needs for tasks such as policy updates, claim resolutions, and other significant network decisions. Lastly, Hyperledger Fabric can facilitate the management of network slices, enabling operators to create isolated virtual networks tailor made for specific applications and services. Smart contracts can enable the automation of provisioning and management of these slices.

uPort [IQB-2], is a decentralized identity platform built on the Ethereum blockchain and created by ConsenSys. It empowers users to establish Self-Sovereign Identities and manage their digital credentials effectively. Insurance companies can utilize uPort to verify the identities of stakeholders, thereby minimizing the risk of identity fraud and fostering trust between involved parties. 5G and B5G networks can benefit from the usage of uPort. In particular, service providers can use uPort to issue verifiable credentials related to service usage, subscriptions, or compliance with service level agreements (SLAs). This can enhance transparency and trust in the services offered over a 5G network. Another advantage of uPort is that it can simplify onboarding of new devices and users in a 5G network by providing a decentralized way to verify identities and credentials. This can lead to faster and more efficient service activation. Furthermore, uPort can help organizations comply with regulatory requirements regarding data protection and privacy by allowing users to control their personal information and how it is shared within the 5G ecosystem.

Veramo [IQB-3, IQB-4] is the evolution of uPort, offering open-source libraries that provide a flexible API for SSI and verifiable data. It enables the creation and management of interoperable DIDs and VCs without dependence on third-party providers or centralized systems. Veramo is compatible with a range of platforms, including Node, web browsers, and React Native. It can offer the functionalities the uPort framework can offer to 5G and B5G networks.

Hyperledger Aries [IQB-5] is an open-source project within the Hyperledger framework of the Linux Foundation. It serves as a foundation for developing decentralized identity (DID) solutions and interoperable identity systems, providing a suite of tools, libraries, and reusable components that support the exchange of Verifiable Credentials (VCs) and the creation of Self-Sovereign Identity (SSI) applications. Concerning 5G related Cyber Insurance incidents, insurance companies can leverage Hyperledger Aries to establish and verify the digital identities of stakeholders within the cyber insurance ecosystem, thereby enhancing the integrity and security of the cyber insurance process.

VCs can be securely stored in a stakeholder's designated storage solution known as the Hyperledger Aries wallet. In addition to authenticating digital identities, the content of these credentials can include information related to the policyholder's cyber incidents, such as incident reports or forensic data. This information can be shared selectively with other parties involved in the claims process through Hyperledger Aries's Selective Disclosure feature, facilitating the secure exchange of claims-related information and minimizing paperwork. Furthermore, Hyperledger Aries employs secure messaging protocols and cryptographic techniques, as it is built on Hyperledger Ursa, to ensure the confidentiality and integrity of communications. Similarly to uPort, Hyperledger Aries can help organizations comply with data protection regulations by allowing users to control their personal information and manage consent for data sharing.

Hyperledger Aries provides secure messaging protocols and its native cryptographic mechanisms can safeguard communications between devices and services in Beyond 5G networks, ensuring confidentiality and integrity in data exchanges. Furthermore, Hyperledger Aries can provide secure identity solutions for IoT devices operating in 5G networks, mitigating risks associated with device impersonation and unauthorized access. A unique identity corresponds to each device enhancing the system's overall security.

Ethereum [IQB-6] is an open-source, decentralized blockchain that enables developers to build and deploy smart contracts and decentralized applications. It was launched in 2015 by Vitalik Buterin, and the platform provides a framework for executing self-contracts without intermediaries. Ethereum offers significant potential when integrated with 5G networks, creating new paradigms for applications and services. Ethereum can enhance Internet of Things (IoT) applications by providing decentralized data management and secure,

autonomous communication between devices. Since 5G can connect billions of devices with higher bandwidth, Ethereum's blockchain can serve as a secure layer for verifying transactions between machines without centralized oversight. Another application of Ethereum in 5G networks is edge computing. With 5G, data processing is often done closer to the devices (at the edge), reducing latency. Ethereum can be leveraged for decentralized edge computing, allowing distributed ledger technology to enable peer-to-peer processing and storage, which improves security, reduces reliance on central servers, and lowers latency. Ethereum can also automate Service Level Agreements in Beyond 5G networks. Specifically, in 5G networks, network slicing facilitates dedicated virtual networks various applications and Ethereum's smart contracts can enforce SLAs within each slice by triggering actions based on agreed metrics, providing transparency and accountability. Of course, Ethereum in Beyond 5G networks comes with a set of disadvantages with respect to latency and scalability. Latency can be caused by its consensus algorithms execution time which can delay the inclusion of a transaction to a block. Regarding scalability restrictions there are many issues that have to be considered. The most important thing is that 5G networks generate vast amounts of data and require rapid processing for tasks like resource allocation, data validation, and device authentication. However, Ethereum's mainnet currently supports around 15–20 Transactions Per Second (TPS), which is prohibitively insufficient for high-demand 5G environments. Moreover, the high volume of data generated in 5G networks and the gas involved in submitting transactions to Ethereum render the usage of the latter prohibitively expensive.

3.2.2.1 Research works related to blockchain technology 5G/B5G

There are a variety of research works that propose using blockchain technology in the context of Beyond 5G networks. This subsection serves to present the most relevant to the context of the SOVEREIGN project.

The work presented in [IQB-7] is highly relevant to the SOVEREIGN project. This paper explores the integration of blockchain, Federated Learning (FL), and 5G edge networks to create a secure, decentralized, and intelligent framework. Specifically, this work addresses the challenges posed by privacy concerns and centralized data handling in 5G networks, proposing a novel system that leverages blockchain technology for transparency and immutability while enhancing privacy through FL. Key aspects of this work include an exploration of how Edge Networks in 5G can be combined with FL to allow User Equipment (UE) to train AI models locally, to protect their data privacy. Furthermore, it proposes using blockchain to store FL data exchanges to make them immutable. Smart contracts on Ethereum are used to incentivize the users to dedicate their computational resources. Additionally, the authors propose a dynamic pairing-based cryptographic authentication scheme to secure interactions among UE across different network layers. This system ensures secure and continuous communication across various providers without intermediaries. The framework ultimately aims to enhance efficiency, privacy, and security of 5G edge networks

and beyond by integrating blockchain and federated learning.

The architecture of the solution proposed in the paper consists of three main planes. The first is the user plane that involves the UE, which participates in FL activities by locally training AI models on private data. The trained models are updated and exchanged without exposing raw data. The user plane interacts with the edge and cloud planes for secure data exchanges. The second is the Edge Plane which hosts Mobile Edge Computing (MEC) servers with strong computational capabilities. These servers facilitate the offloading of intensive tasks from UEs, reducing their computational burden and latency. The edge plane also includes various base stations (macro and small base stations) and roadside units (RSUs). This plane is programmable and flexible, using virtualization to manage resources and deploy functions quickly. Blockchain technology is integrated here to secure and manage transactions, utilizing Ethereum smart contracts to ensure trust and accountability in FL activities. Lastly, there is the cloud plane which houses the central servers with massive computational power, responsible for aggregating the FL model updates from multiple UEs. While decentralization is emphasized, some centralized elements (like the cloud's role in model aggregation) are retained to manage large-scale data processing. The architecture offers a secure, decentralized, and efficient system for enabling AI-driven applications on 5G edge networks, combining blockchain for security and accountability with federated learning for privacy-preserving intelligence

Another relevant work from literature, especially in the sector of cyber insurance in 5G Networks, is INCHAIN [IQB-8]. INCHAIN introduces an innovative architecture designed to address several challenges facing the cyber insurance industry, such as data scarcity, fraudulent claims, identity theft, and lack of automation. The architecture leverages blockchain technology to ensure transparency and traceability of data, while integrating smart contracts and SSI for automating processes and enhancing identification mechanisms in the cyber insurance market to address challenges like Fraudulent Claims, Identity Thefts and Manual Processes.

INCHAIN addresses these challenges with a blockchain-based architecture that comprises a set of technologies and modules. These are the Blockchain Backbone, the SSI Blockchain, the Insurance Blockchain, the Smart Contracts and SSI. The Blockchain Backbone ensures secure, immutable, and transparent records of insurance transactions and cybersecurity data. Two blockchains are employed: The first is SSI Blockchain that handles identity verification through VCs and the second is the Insurance Blockchain which stores smart contracts and facilitates claim handling and payments. The Smart Contracts automate key processes, such as claim validation, policy enforcement, and premium calculations, reducing the need for human intervention. Lastly the SSI allows policy holders to manage their digital identity independently, providing verified credentials without sharing sensitive personal information directly with insurers. This enhances privacy and security while streamlining identity

verification during claim processes.

INCHAIN introduces the automation of operations for key insurance processes which are related to Incident Reporting and Reimbursement. The policy holders can report cybersecurity incidents through the blockchain, triggering automated investigation and reimbursement processes. The system checks for fraudulent claims by referencing stored claims and ensures that claims are handled without delays.

INCHAIN’s architecture provides a transparent, efficient, and secure solution for managing cyber insurance. By combining blockchain, smart contracts, and SSI, it addresses critical challenges in the sector, improving the accuracy of risk assessments, reducing fraud, and automating labor-intensive tasks, offering a solid foundation for the future of cyber insurance.

3.3. Tools and platforms for service anonymity in Beyond 5G systems

3.3.1. State-of-the-art on anonymity services

There are a variety of existing widely used technologies and novel solutions presented in conferences and journals that can be utilized in the context of 5G and B5G networks to provide anonymity to users and User Equipment.

One widely used technology that can provide anonymity in 5G and B5G networks is Idemix. **Idemix** [IQB-9] is an anonymous credential system for the selective disclosure of attributes to minimize the revelation of personal in digital communications. It provides privacy-preserving features such as anonymity, the ability to transact without revealing the identity of the transactor, and unlikability, a subject's ability to perform multiple actions without revealing that these actions were completed by the same subject.

The entities that participate in Idemix are the user, an issuer, and a verifier while the protocol itself consists of two functionalities. The first functionality is the issuance of credentials, where the user obtains credentials by the issuer. The credential consists of a set of attribute values, and cryptographic information that allows the credential's owner to create proof of possession.

Every credential is linked to a pseudonym created by the user. The user can generate multiple pseudonyms using a private key known as the Idemix master secret. These pseudonyms are untraceable, meaning it is impossible for an external party to determine if two pseudonyms stem from the same master secret. Additionally, disclosing a pseudonym does not expose any details about the master secret.

The generation of pseudonyms from a secret key is similar to traditional public key cryptography, where the public key represents the user's identity (as seen in Bitcoin). However, unlike public key cryptography, Idemix allows the user to create an unlimited number of public keys (or pseudonyms) from their private key, referred to as the master secret. The second feature of Idemix is credential proving, where a user, acting as the prover, must demonstrate possession of specific attributes to a verifier without revealing the actual attribute values, using Zero-Knowledge Proofs. When presenting a credential, the user can decide which attributes to disclose and which to keep hidden. Additionally, the user generates a pseudonym (distinct from the one used during credential issuance) that the verifier will use as a reference. This ensures that both issuers and verifiers recognize users solely by their pseudonyms, which remain unlinkable.

An extended feature of Idemix is a cryptographic mechanism known as verifiable encryption. This allows the owner of an Idemix credential to prove that their credential contains a specific attribute, which is essentially an encrypted value, using the public key of an entity, such as a trusted third party or the credential issuer. This functionality is particularly useful in scenarios

where a verifier grants access to a service only if the credential contains the user's encrypted ID card. While the verifier cannot decrypt the ID card, they can confirm that the encrypted value is present in the credential, hence the term 'verifiable encryption.' In cases where de-anonymization is needed, the verifier can send the encrypted ID card to the public key holder (either the trusted third party or the issuer), who can decrypt it with the associated private key to reveal the user's true identity.

In conferences and journals, some conceptual solutions have been designed, implemented, and evaluated for enhancing the security of Beyond 5G networks. In this section, the most representative of these 5G security architectures that provide anonymity are discussed.

In [IQB-10] a protocol is proposed that enables extended authorization for Multi-access Edge Computing (MEC)-hosted applications. Besides granting a user permission to an application, it utilizes a new functionality supported by the MEC enabler which is a protocol for anonymous authorization. The MEC enabler protocol comprises the following components:

- The Administration Module supports all MEC enabler management-related operations and the configuration of the other functional modules.
- Slice MANO is responsible for the management of the slice life cycle in the MEC area, reserving resources for specific slices and marking them according to their type of service, network identification, or by other classifications.
- Attribute-Based Access Control stores all policy data regarding services, slices, available connections, and other MEC information.
- Service Management is the MEC enabler module that manages all services. It checks services availability, their utilization, and the dedicated resources to them.
- Credentials Management generates tokens that can be used in the MEC resources’ authorization process and for service communication path protection.
- The billing module is used for billing and storing information regarding the usage of MEC.
- UPF MEC Configuration matches and properly configures UPF MEC and links appropriate network slices with dedicated MEC resources.
- AAA is in charge for the authentication, authorization, and accounting of all requests to MEC services. Once there is positive verification, the AAA module initiates the MEC access procedure beginning from the UPF MEC Configuration module and ending with the Credentials Management module. The UPF MEC Configuration module prepares the new network configuration that enables the creation of a connection with the chosen service while the Credential Management module generates a token for service authorization.

In short, the MEC enabler has three functions in the 5G MEC network security architecture model. First, it manages the application providers located in edge servers and end users.

Second, it generates service access tokens for authenticated users, guaranteeing the use of the service with the permissions indicated by the token parameters. Third, it ensures anonymous authorization of the access path to the service during its implementation.

The proposed protocol uses a JWT-based method of authorization in its access control system called JSON MEC Access Token (JMAT). A JMAT indicates that the user has successfully authenticated and has granted access to resources. More importantly, a secret is generated based on the token, which plays a role in anonymizing network traffic. Specifically, the JMAT token is used to generate secrets which are the basis of the rules the MEC Enabler supplies UPF MEC and UPF core. These rules facilitate the obfuscation of the original traffic and protect access to the service from spoofing attempts.

The anonymization method this work presents replaces the proper parameters identifying a MEC service connection, with respect to both source and destination, with random values. These random values are generated based on mathematical operations on a secret bitstring, and they are actually a group of sub-secrets. To ascertain the expected level of anonymity provided by this solution, one must count the number of all possible combinations of pairs. With the term pairs the authors refer to the parameters of the connection source and its destination addresses. An essential parameter in evaluating the anonymization level is to determine if the connections are made via the IPv4 or IPv6 protocol.

The paper presented in [IQB-11] proposes a **decentralized authentication protocol for 5G networks**, aimed at addressing security issues in the standardized 5G-AKA protocol. The authors while recognizing that 5G-AKA offers mutual authentication between User Equipment (UE), base stations, and the core network, it remains vulnerable to attacks, such as Denial of Service (DoS), Distributed DoS (DDoS), and linkability tracing.

To address these attacks, this paper proposes a solution that utilizes blockchain technology to decentralize the authentication process. This prevents the occurrence of single points of failure, which is a common issue in centralized systems such as 5G-AKA and enhances security against DDoS attacks by distributing authentication tasks across all base stations.

The proposed work protects device anonymity through encryption with Subscription Concealed Identifiers (SUCI) to conceal the identity of User Equipment (UE). Moreover, the proposed protocol mandates the Subscription Permanent Identifier (SUPI) to be encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES) to generate a SUCI. This encryption prevents adversaries from identifying or tracing devices by intercepting authentication messages. Additionally, the protocol replaces sequence numbers, commonly used in traditional 5G-AKA schemes, with Elliptic Curve Diffie Hellman (ECDH) keys to prevent linkability attacks. By eliminating sequence numbers, the protocol ensures that no synchronization failure or MAC failure messages can be used to trace specific devices thus mitigating linkability attacks.

3.3.2. Self-sovereign platforms by IQB

The purpose of this subsection is to give an overview of the Self Sovereign Identity paradigm and present its components along with its functionalities, operations and procedures. The Self-Sovereign Identity (SSI) paradigm is a model for managing digital identities that emphasizes user control, privacy, and security. The key characteristics the SSI paradigm offers are [IQB-12] [IQB-13]:

- User Control: SSI allows individuals to own and manage their own identity without relying on centralized authorities. Users can decide what information to share, with whom, and under what circumstances.
- Decentralization: Unlike traditional identity systems, which often depend on central databases, SSI leverages decentralized technologies like blockchain. This reduces the risk of data breaches and gives users greater autonomy over their identities.
- Verifiable Credentials: Users can receive digital credentials from trusted issuers (e.g., governments, educational institutions) that are cryptographically verifiable. This ensures the authenticity of the credentials without requiring direct access to the issuer's database.
- Privacy: SSI prioritizes user privacy by minimizing data sharing. Users can authenticate themselves without revealing unnecessary personal information, using selective disclosure methods.
- Interoperability: SSI systems aim to be compatible with various platforms and services, allowing users to manage their identities across different contexts and domains seamlessly.
- Security: By enabling users to store their credentials in secure wallets, SSI reduces the risks associated with centralized identity theft and fraud.

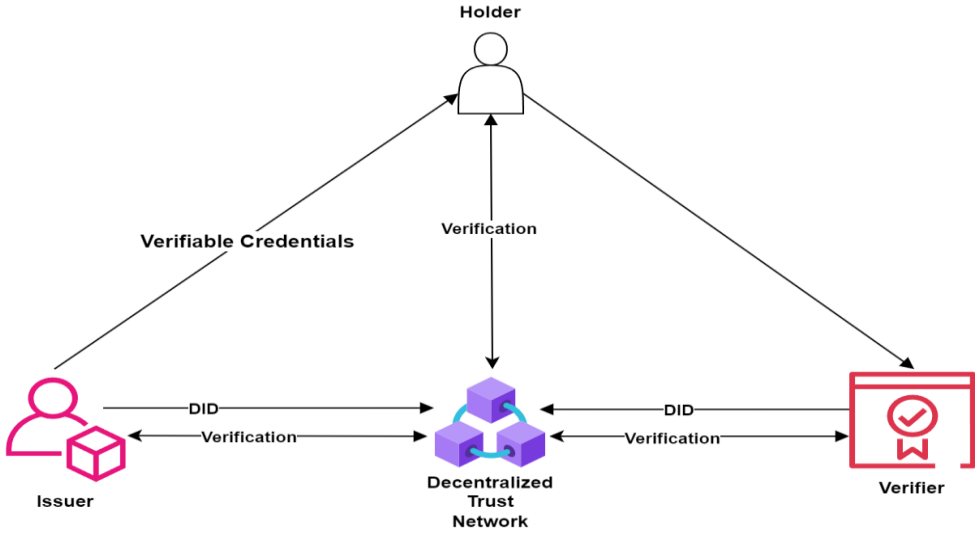

Fig. 16 High level overview of an SSI's scheme entities and interactions

Overall, SSI promotes a more secure and user-centric approach to digital identity management, aligning with the increasing demand for privacy and autonomy in the digital age. Fig. 16 provides a high-level overview of the parties involved in an SSI scheme and the interactions between them.+

3.3.2.1. Components of Self Sovereign Identity Platform

In the context of the SOVEREIGN project, the Self Sovereign Identity (SSI) framework will facilitate Authentication, Authorization, and support Accounting of actions in 5G and B5G networks. Moreover, it will enable cross-domain identity management to empower intelligent end points to perform selective attribute disclosure. SOVEREIGN's SSI framework is envisioned to comprise the following components:

- **SSI controller:** manages and controls the Decentralized Identifier (DID) of User Equipment and edge services while it also holds Verifiable Credentials (VCs) issued by trusted entities. By using identity wallets, which are apps designed for secure storage and management of these identifiers and credentials, the SSI controller decides when and with whom to share the DID related information of an entity. This approach provides individual entities with more privacy and security, as they manage their own identity without relying on central authority. When necessary, these entities can present their VCs to others who can then verify their authenticity without contacting a central provider.
- **Wallet:** The wallet resides on the SSI controller and conceptually resembles a digital safe in which entities keep their digital credentials and identity information safe and organized. These credentials may include data like serial number, manufacturer information, MAC address, and other information unique to a specific entity. The wallet employs a variety of security mechanisms, like cryptography, to ensure that only the owner entity can access and manage these details. One of its basic features is the ability to selectively share specific details with other entities, like when it is necessary to prove the identity. SSI wallets are compatible with different systems and services, thanks to standardized protocols, allowing the entity to interact securely across various platforms.
- **SSI Agents** are an integral part of SSI systems for managing VCs, including issuing, storing, and verifying them securely. They enable User Equipment/Edge Services to selectively share credentials with verifiers, thus protecting privacy by minimizing the disclosure of information. An agent is deployed on an SSI Controller and serves as a digital assistant responsible for securely managing verifiable credentials and interactions with other entities. This software component plays a critical role throughout the credential lifecycle, overseeing tasks such as credential creation, storage, updating, and presentation. By employing cryptographic methods, agents ensure that credentials remain confidential and untampered with, protecting them

from unauthorized access. Acting as intermediaries between the credential holder's device and verifiers, agents facilitate smooth interactions, following standardized protocols like DIDs and Verifiable Credentials VCs by W3C [IQB-14]. A key feature of agents is the ability to enable selective disclosure, allowing entities to share specific credentials or attributes with verifiers while keeping other sensitive information private. This approach enhances privacy. Additionally, agents may integrate with user interfaces in SSI Controller applications, offering a user-friendly way to manage credentials and engage with the digital identity ecosystem.

- **Hyperledger Aries:** The Distributed Ledger Technology best suited to support the SSI framework for 5G and B5G networks is Hyperledger Aries [IQB-5], which enables peer-to-peer interactions through blockchains. Moreover, it supports the exchange of blockchain-based data across various DLTs and enables secure exchange of messages. Hyperledger Aries’s functionalities include message encryption, blockchain interfaces for transaction handling, and secure data storage via a cryptographic wallet. Additionally, Hyperledger Aries supports VCs with advanced privacy features such as Zero-Knowledge Proofs, thus enhancing security and privacy in decentralized systems. Hyperledger Aries is recognized as a technology tailored for SSI frameworks. In short, Aries can support decentralized identity management with DIDs and VCs, integrate privacy features, ensure interoperability, and leverage blockchain for secure data management and smart contracts.
- **Distributed Ledgers** are a form of database distributed across multiple nodes, in contrast to traditional centralized databases managed by a single entity. In the context of SSI, a distributed ledger plays a crucial role in managing digital identities. Specifically, blockchain is used to register Decentralized Identifiers (DIDs), unique identifiers individuals or entities create and control. This registry ensures DIDs are unique and tamper-proof, securing identity associations with public keys since DLTs keep immutable records of all transactions. As soon as a DID or credential is recorded, it can’t be altered, guaranteeing identity related data integrity. The SSI paradigm utilizes DLT to decentralize the process of identity verification, removing the necessity for a central authority. Instead, nodes within the network validate transactions, ensuring fraud prevention and maintaining consensus. The ledger integrates with Public Key Infrastructure (PKI) by storing public keys, which are used to securely verify the authenticity of credentials and communications. Verifiers can check credentials directly using these public keys without needing to rely on a central authority. Moreover, the distributed ledger also manages credential revocation transparently, recording revocation details so that verifiers can easily confirm the status of invalidated credentials.
- **Verifiers:** The verifier plays a vital role in building trust and ensuring authenticity in digital exchanges through the verification of credential attributes or credentials. Verification starts by requesting proof from a holder, specifying the types of

credentials or attributes required for verification. The holder then provides the requested proof, typically in the form of a digitally signed assertion about their attributes, created using cryptographic techniques to guarantee integrity and authenticity. The verifier reviews the proof to ensure it meets the required standards, verifies the validity of the digital signatures, confirms that the proof has not been altered, and checks if the credentials adhere to established schemas and definitions. Furthermore, the verifier ensures that none of the presented credentials have been revoked. Through this process, the verifier confirms the holder's claims, allowing decisions or access to be granted based on the outcome. The verifier's function is key to upholding trust and security in the SSI ecosystem, fostering interoperability between various systems and organizations, and improving user privacy by requesting only essential information and allowing individuals to manage their own data.

- **Issuers:** In the context of SSI, Issuers act as Identity Providers, responsible for issuing VCs. These credentials enable devices to securely present their identities during various interactions. The process of issuing VCs involves collecting device-specific attributes and metadata, which the identity provider then cryptographically signs. For instance, a VC might verify information such as the manufacturer, model, and firmware version of a device, along with additional details like its location and operational status. These VCs are securely stored and allow devices to demonstrate their identity and capabilities within the SOVEREIGN ecosystem, enabling smooth authentication and trust in a decentralized and dynamic environment.

3.3.2.2. Processes of Self Sovereign Identity Platforms

This subsection describes the processes and operations of an SSI framework as well as the software tools that enable and support them. A Self-Sovereign Identity solution has several processes which are integral to its operation and nature. These processes are:

a) Onboarding
b) DID generation
c) Connection establishment
d) VC issuance
e) Proof presentation
f) Proof verification

a) Onboarding

Onboarding is an entity into a Self-Sovereign Identity (SSI) framework using Hyperledger Aries involves several key steps to establish a secure and verifiable identity management system. The first step is setting up the Hyperledger Aries framework, which offers essential libraries

and tools for building SSI solutions. This involves configuring the required infrastructure, such as the distributed ledger (usually Hyperledger Indy), to store decentralized identifiers (DIDs) and VCs. The process begins with device registration, where each IoT or edge device creates a unique DID along with a corresponding public/private key pair. These DIDs are then registered on the ledger, providing each device with a decentralized identity. Once registered, devices are issued VCs that serve as proof of identity and functionality. These credentials are managed through Aries agents, which ensure secure communication and interactions between devices and the network. Devices authenticate by presenting signed proofs of their credentials, facilitating secure and verified transactions. By integrating Hyperledger Aries, identity-related tasks such as credential issuance, verification, and revocation are handled efficiently, providing a decentralized, secure identity management system for IoT and edge devices. This enhances security, privacy, and trust within IoT ecosystems.

b) DID generation

Generating DIDs with Hyperledger Aries in an SSI framework involves a number of steps. Initially, the appropriate environment is set up on the User Equipment or Edge endpoint by installing the necessary Hyperledger Aries components and configuring a blockchain network to ensure proper communication between them. The next step is to create a cryptographic key pair, consisting of a public key and a private key, which are essential for securing identity. Using this key pair, the device generates a DID and a corresponding DID document. The DID document includes important details such as the device’s public keys and service endpoints, allowing others to verify the device’s identity and locate its VCs.

The DID document is then registered on the blockchain, similar to a public notice that can be independently verified. Once registered, the device gains full control over managing and updating the DID document. In case changes are necessary, such as adding a new public key or modifying a service endpoint, the device can update the DID document and submit the changes to the blockchain, ensuring that the updates are securely recorded. This process offers a decentralized and secure method for managing digital identities, allowing the device to control and update its identity without the need for a central authority.

c) Connection establishment

Establishing a secure connection using the Self-Sovereign Identity (SSI) framework in the context of Hyperledger Aries involves several steps designed to ensure decentralized and verifiable identity management. The first step is setting up the necessary environment, including installing the Aries Agent and configuring an Indy blockchain network, which serves as the underlying ledger. An agent, which represents an entity like an organization, creates a connection invitation. This invitation includes details such as endpoint and key information and is shared with another agent. The receiving agent accepts the invitation, establishing a

secure, encrypted connection between the two parties. Once the connection is established, the agents can exchange credentials. For example, an agent can issue a credential, such as a digital ID card, to the other party. This involves creating a credential schema and definition on the blockchain, sending a credential offer, and having it accepted and stored by the recipient. Additionally, agents can request proof of certain information. This process ensures that all identity interactions are secure, private, and verifiable without relying on a central authority, empowering users to control their identity data.

d) VC issuance

The issuance of Verifiable Credentials using the Hyperledger Aries framework works as follows. Initially, the device needs to set up an environment by installing Docker and cloning the Aries Cloud Agent repository. Once the Docker is up and running, the device can start an agent using Docker commands. The next step involves creating a wallet and a DID for the specific agent using API requests. Afterwards, a schema has to be created, which defines the structure of the credential, like a certificate with fields for the identity. As soon as the schema is prepared, a credential definition is created to establish how the credentials will be issued based on this schema. Finally, the user may issue credentials by sending a credential offer to a recipient and once accepted, should send the actual credential. The entire process involves the making of multiple API calls, each one building on the previous steps, to set up the agent, define the specific credential, and then issue it.

e) Proof presentation

In the Hyperledger Aries SSI framework, the presentation of proof process starts when a verifier sends a request to a holder for specific credentials or attributes. The holder, using their digital wallet, selects the necessary credentials and generates a verifiable presentation. This presentation encompasses cryptographic proofs that validate the authenticity and integrity of the data while ensuring privacy through techniques like Zero-Knowledge Proofs. The holder hen submits the Verifiable Presentation to the verifier. The verifier’s agent, utilizing the Hyperledger Aries infrastructure, verifies the proofs by cross-referencing the credential definitions and schemas on a distributed ledger, such as Hyperledger Indy. The agent ensures the digital signatures are valid and the credentials are issued by a trusted entity, thus facilitating a secure, privacy-preserving verification of the holder’s credentials in a decentralized fashion.

f) Proof verification

The proof verification process starts when a verifier requests specific credentials or attributes from a holder. The holder users their digital wallet to select the relevant credentials and generates a Verifiable Presentation that includes cryptographic proofs ensuring the authenticity and integrity of the data without revealing sensitive information by utilizing Zero-

Knowledge Proofs. This Verifiable Presentation is then sent to the verifier. The verifier’s agent, which operates with the Hyperledger Aries framework, checks the proofs against the credential definitions and schemas stored on a distributed ledger, such as Hyperledger Indy. The agent verifies the digital signatures to confirm that the credentials were indeed issued by a trusted source and have not been altered. This process ensures a secure, decentralized, and privacy preserving verification of the holder’s credentials.

3.4. Tools and platforms for user-driven access and network automation in Beyond 5G systems

3.4.1. State-of-the-art on network automation platforms

SOVEREIGN will consider IQU's platform for network automation. Specifically, the platform architecture is shown in Fig. 17 and consists of the following elements:

- **Backend Cloud Domain**: Two high-performance servers are deployed running Apache Kafka and Zookeeper services, as well as Open5GS, which is an open source 5G Mobile Core. The first server (S1) has an Intel Xeon Gold processor, with 26/52 cores running at 2.10GHz with 192GB of RAM memory and an ASUS ATX motherboard. While the second server (S2) has an Intel I9-10900L processor with 10/20 processor cores. The storage devices in S1 are: 1) one SATA SSD with 2TB of storage, and 2) a NVMe (Non-Volatile Memory Express) SSD disk with also 2TB of storage. The former is used to host the Ubuntu 20.04 filesystem and user-level data in two separate partitions. The latter is managed by ZFS, and it is used by LXD as a storage pool to allocate storage for all the VMs and containers that the server handles. S2, on the other hand, only has one NVMe SSD.
- **An Edge Domain with Multi-Edge Computing (MEC) nodes**: the Edge Domain consists of a 5G-compliant gNB and Shuttle PCs, each with a mobile Core i7 processor and 16 GB of RAM, acting as MEC nodes. The gNB currently in use is an Amarisoft Callbox Mini, which is suitable for experimental and testing environments.
- **A Deep Edge domain**, that consists of Raspberry Pi RPI4s enabled with SIM8200EA-M2 5G HATs providing 5G connectivity; WiFi can also be used as an alternative.

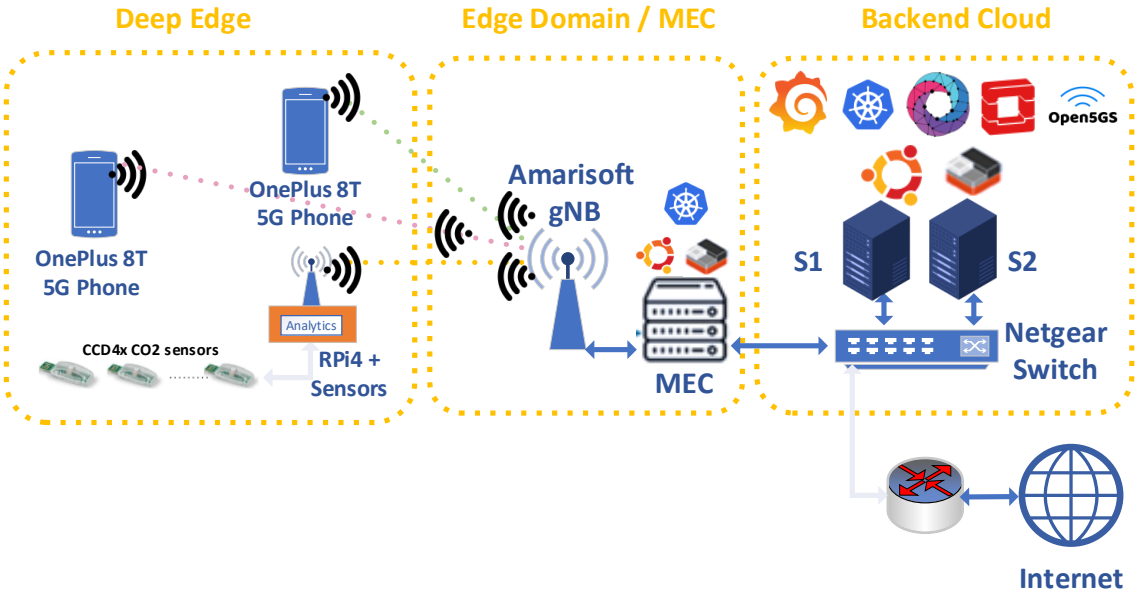

Fig. 17 Architecture of IQU 5G / IoT testbed with Deep Edge deployment and local analytics

The testbed, as described above, supports the following features:

- Orchestration capabilities: materialized through OpenStack and Opensource MANO (OSM) deployed in a virtualized environment.
- Monitoring System: deployment of multiple instances of the Monitoring System (MS) for data gathering and for deployment of the different enablers.
- Cloud-native Support: this is necessary to allow the flexible deployment of the enablers and to provide a federation of resources across the 5G Core Cloud and the 5G Edge Cloud Domain. A Kubernetes cluster is deployed to provide this functionality.
- Deep Edge deployment of services; in the context of UC1 these are leveraged for performing analytics on the received sensor values, and detecting anomalies (e.g., CO2 spikes) while avoiding latencies inherent with cloud deployments.

3.4.2. HybridNet Lab by ULU

As the world becomes increasingly connected, the challenge of orchestrating large and heterogeneous networks has become more complex than ever before. This is especially true for networks that involve technologies such as 6G, satellite, and quantum key distribution (QKD). Research paves the way to more efficient and reliable networks relying on cornerstone disciplines like Machine Learning (ML).

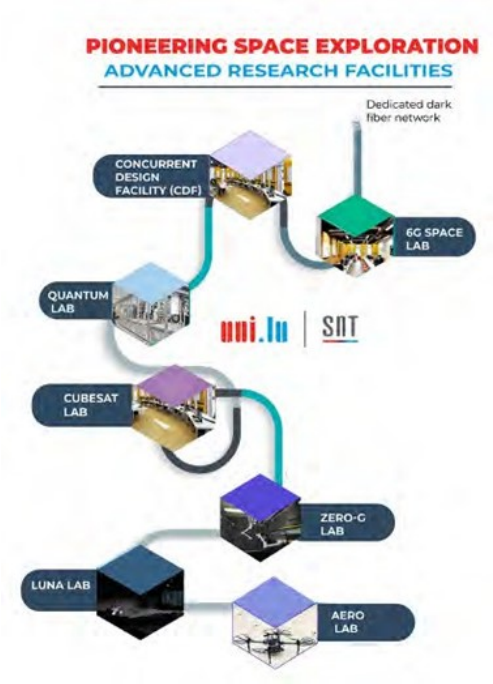

Fig. 18 SnT Lab Infrastructures

The HybridNet Lab is dedicated to in-lab validation of the advent orchestration of large-scale autonomous and heterogeneous network systems. It is empowered by a dedicated range of

hardware and software to help validate novel approaches and solve the difficult task of network orchestration in real network environments. To extend its capabilities, effectively bring research solutions to higher TRL, and fit within industrial needs, HybridNet is interconnected to other labs using a dedicated optical fiber network.

3.4.2.1. Research Area

HybridNet Labs leads the orchestrating of heterogeneous networks, integrating diverse technologies like SDN, NFV, and QKD to create a seamless research environment. Our interdisciplinary team explores synergies between traditional and emerging networks, enhancing performance and security through advanced orchestration and automation. Our state-of-the-art optical fiber network supports high-speed data transmission and robust connectivity, enabling the practical implementation of innovative solutions. To develop a seamless orchestration system, we conduct cutting-edge research in several areas:

- Software-Defined Networking (SDN): At HybridNet Labs, we revolutionize network management with SDN, centralizing control for unparalleled efficiency and security. Our research delves into cutting-edge algorithms for dynamic optimization and robust security enhancements. We tackle scalability and interoperability challenges, ensuring our solutions are ready for the networks of tomorrow.
- Network Functions Virtualization (NFV): HybridNet Labs leads the way in NFV, transforming network services with virtualization on standard hardware. Our innovative research focuses on optimizing service chaining, resource allocation, and VNF performance. We address the complexities of integration and strive for high availability and fault tolerance, pushing the boundaries of what's possible in virtualized networks.
- Network Orchestration: Our lab excels in automating network service deployment and management. We pioneer multi-domain orchestration frameworks and enhance policy management and service assurance. We ensure seamless and efficient network operations by overcoming interoperability challenges and simplifying automated provisioning.
- Network Automation: At HybridNet Labs, we harness the power of AI and ML to automate network operations, providing proactive monitoring and analytics. Our research aims to develop advanced fault management and workflow automation solutions. We focus on integrating these tools securely and reliably into existing infrastructures, paving the way for smarter networks.
- Quantum Key Distribution (QKD) Orchestration: We are at the forefront of secure communication with QKD orchestration, integrating quantum key distribution with classical networks. Our research enhances the efficiency and scalability of QKD systems and develops robust security protocols. We tackle the challenges of seamless

integration and technical limitations, ensuring our solutions are ready for widespread adoption.

Our lab stands as a symbol of transformative scientific collaboration. Here, quantum physics intertwines with sixth-generation wireless communication, lunar research, and the enigmas of zero gravity. Enabled by our dedicated optical fiber network, this fusion promises to reshape our cosmic understanding and technological horizons.

3.4.2.2. Projects

HybridNet Lab collaborates with industry partners, academic institutions, and international organizations to lead groundbreaking network orchestration and management research. The following presents a selection of key projects realized at the HybridNet Lab, each designed to explore innovative solutions for integrating heterogeneous networks. The following is a list of projects that have been realized in our lab, along with some that are still ongoing:

- 5G-EMERGE: Satellite-enhanced edge delivery
- XTRUST-6G
- LUQCIA: Luxembourg Quantum Communication Infrastructure Laboratory
- Lux4QCI: Luxembourg Experimental Network for Quantum Communication Infrastructure
- TRANTOR: 5G+ Evolution to Multiorbital Multiband Networks
- Micro5G: Mobile Edge Computing for 5G DROne Systems
- 5G-SpaceLab: 5G Space Communications Laboratory

3.4.2.3. Facilities and Equipment

HybridNet Labs has state-of-the-art infrastructure to support cutting-edge research and innovation. Our facilities are meticulously crafted to provide the optimal environment for advanced scientific exploration and technological development.

(a) ORCHID Super-Computer **(b)** Network Interconnection and Storage devices

Fig. 19 Compute, Storage and Network Facility

Hardware

Our lab’s hardware setup is composed of high-performance components that ensure robust and efficient operations:

- High-End Servers: Our lab features high-end servers, including a super-computer with 1000 CPUs and 1 TB of RAM. This immense computational power allows us to efficiently perform complex simulations, data processing, and intensive computational tasks.
- SDN Optical Switches: We utilize Software-Defined Networking (SDN) optical switches to enable high-speed data transfer across our network. These switches are designed to minimize latency, with tested performance showing latency of less than 100ms, ensuring efficient and reliable network performance.
- Monomodal Fibers: Our infrastructure includes over 80 km of monomodal fibers that interconnect all our labs. Each fiber can support data transfer rates of up to 100 Gbps, facilitating seamless communication and data exchange across our network.

Software Management

To manage and orchestrate our diverse network environment, we rely on a suite of advanced software tools:

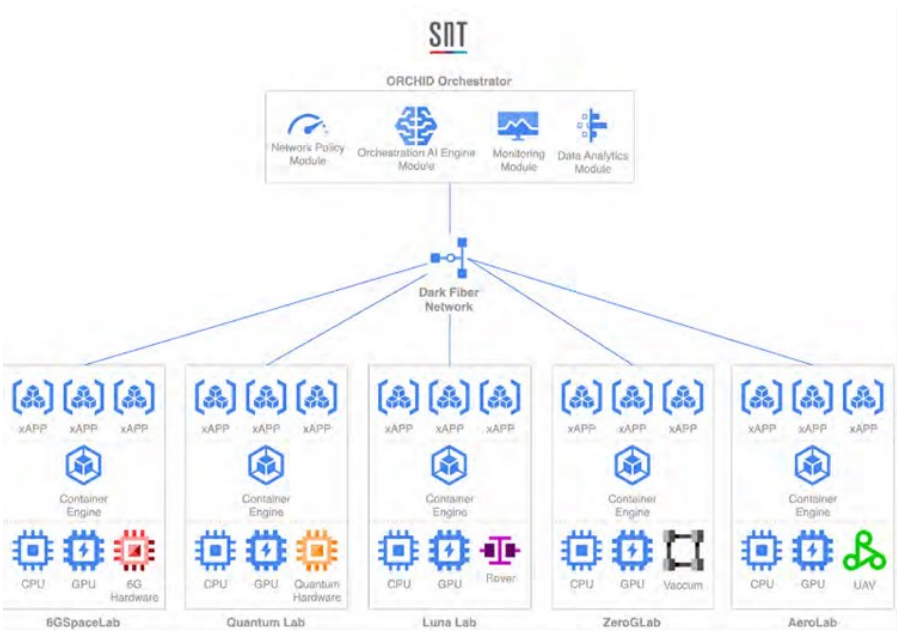

Fig. 20 ORCHID Orchestration System

- ORCHID: ORCHID, our proprietary orchestrator, is at the heart of HybridNet Labs. ORCHID is designed to deploy and manage various network configurations across all interconnected labs, ensuring seamless integration and optimal performance. It comprises several key modules: the Network Policy Module, which allows for the creation and enforcement of network policies, ensuring that all network activities adhere to predefined rules and standards; the Orchestration AI Engine, which automates the orchestration of network resources, optimizing performance and efficiency through intelligent decision-making; the Monitoring Module, which provides real-time monitoring of network performance, identifying and addressing issues promptly to maintain optimal network health; and the Data Analytics Module, which analyzes network data to offer insights into network usage patterns, performance metrics, and potential areas for improvement, driving informed decision-making and continuous optimization. ORCHID is the cornerstone of our lab, enabling us to conduct complex experiments and simulations with ease and ensuring that our network infrastructure operates at peak efficiency.
- Docker and Podman: These containerization platforms allow us to deploy and manage applications efficiently. Using Docker and Podman ensures

consistency and scalability across our infrastructure, enabling us to handle various research and development tasks.

- Open vSwitch: Open vSwitch is a multilayer virtual switch that provides robust network automation and management capabilities. It enhances our SDN environment by enabling flexible and dynamic network configurations.

Network Emulation Capabilities

HybridNet Labs excels in network emulation, providing a versatile platform for testing and validating network protocols and configurations in a controlled environment. Our emulation capabilities include:

- Realistic Network Scenarios: We create realistic network scenarios that mimic real-world conditions, allowing researchers to test the performance and reliability of their solutions under various conditions.
- Scalability Testing: Our emulation platform supports scalability testing, enabling network performance evaluation as the number of devices and traffic load increases.
- Protocol Development and Testing: We facilitate developing and testing new network protocols, ensuring they meet the required standards and perform optimally in diverse environments.
- Interoperability Testing: Our emulation capabilities allow for comprehensive interoperability testing, ensuring that different network components and systems work seamlessly together.

By combining high-performance hardware with advanced software management tools and robust network emulation capabilities, HybridNet Labs creates a comprehensive and flexible research environment. This infrastructure supports our mission to innovate and push the boundaries of network technology, enabling groundbreaking research and development. Our commitment to excellence in hardware and software management excellence ensures that we remain at the forefront of scientific discovery and technological advancement.

4. Relevant standards and international fora to the SOVEREIGN key areas

4.1. Overview of 3GPP standards relevant to Non-Terrestrial Networks in B5G

3GPP TR 38.912 v.14.0.0 Release 14: **Study on New Radio (NR) access technology**

This TN provides all technical outcome of the study item "Next Generation New Radio (NR) Access Technology" and involves the Radio Access work area of the 3GPP studies and has impacts both on the Mobile Equipment and Access Network of the 3GPP systems. There is particular focus on the precoding design in NTN scenarios, in which three transmission modes (TMs) in the 3GPP standard designated for multi-user precoding:

- **TM 5**: is specifically designed for multi-user precoding using the codebook. This TM supports up to 2 users and does not require CSI feedback. Instead, the users calculate the precoding matrix index (PMI) based on the estimated channel gain and feedback the PMI to the base station (BS), from which the BS selects the corresponding precoding vector from the codebook.
- **TM 8**: is designed for both single user (multi data streams) and 2 users. This mode allows high-resolution CSI feedback, hence both codebook-based and non-codebook-based precoding designs are possible.
- **TM 9**: supports up to 4 users (single data stream) or 2 users (two data stream). Like TM 8, this mode has high-resolution CSI feedback and allows both codebook- and non-codebook-based precoding designs.

3GPP TR 38.811 v15.2.0: “Study on New Radio (NR) to support Non-Terrestrial Networks (Release 15),” Sept. 2019.

This TR focuses on the long propagation delay, large Doppler effect, and base station movement. The required functions of the 5G-NR NTN have been studied and included in different Releases. The beam management procedure is illustrated in Fig. 21.

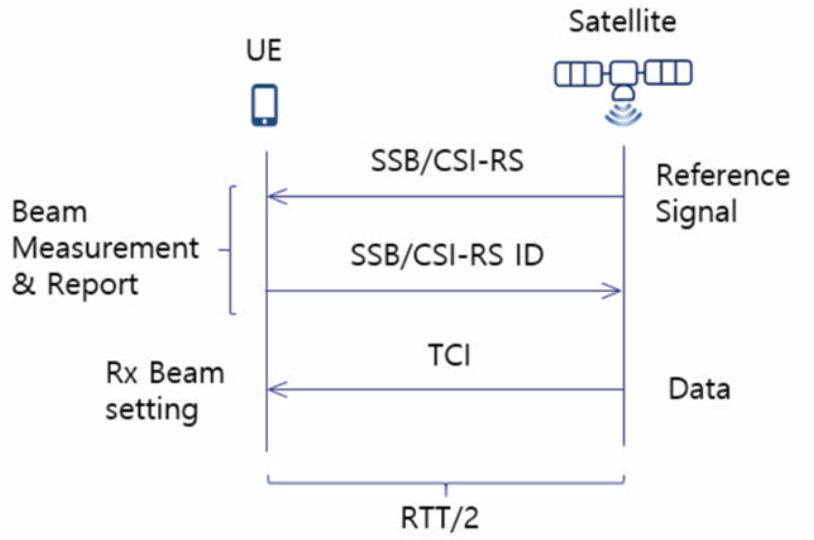

Fig. 21 Beam Management from 3GPP TR 38.811 v15.2.0

Release 16 introduces enhanced beam handling and channel-state information (CSI) feedback and support for transmission to a single UE from multiple transmission points (multi-TRP).

Although Rel.15 supports flexible beam management (BM) functionality to accommodate various implementation and usage scenarios, Rel.15 BM signaling framework could require a large amount of signaling for updating beam RS and pathloss reference RS for respective DL and UL signals when the best DL-UL beam pair is changed frequently due to UE mobility, rotation, or beam blockage.

In Rel.16, five features were introduced for BM signaling overhead and latency reduction. Additionally, in Rel.15, L1-RSRP-based beam measurement and reporting are supported. To facilitate interference-aware beam selection, L1-SINR-based beam measurement and reporting were introduced. Finally, in Rel.15, beam failure recovery (BFR) is supported only for spCell. To improve performance and reliability for SCell, BFR for SCell was introduced.

3GPP TR 38.802, “Study on new radio access technology Physical layer aspects”, V14.2.0.

3GPP TR 38.802 Section 6.1.6.1 defines beam-management as three procedures. (P1) SSB based beam sweeping (P2) CSI-RS based transmit-end beam refinement (P3) CSI-RS based receive-end beam refinement as shown in

Table 2.

Table 2 : Beam-management procedures in 5G NR in TR 38.802

Process	Functionality	Description
P1	Beam selection	gNB performs beam sweeping, UE selects the best beam and reports it to gNB
P2	Beam refinement at transmitter	gNB performs narrow beam sweeping and the UE detects and reports the best one to gNB
P3	Beam refinement at receiver	UE narrows its beam while gNB beam is fixed

4.2. Overview of 3GPP/ETSI standards for Network Automation in B5G

The ETSI Zero Touch Network and Service Management (ZSM) ISG aims to define a new, flexible, and fully operable end-to-end framework to support the agile, efficient, and high-quality management and automation of next-generation networks and services. ZSM envisions a network and service management architecture where all operational tasks—such as delivery, deployment, configuration, assurance, and optimization—are carried out automatically, ideally achieving full automation in multi-vendor environments.

While ETSI NFV has made progress in addressing specific aspects of network and service management by defining capabilities for managing virtualized network functions and services, its scope remains domain-specific. Building on this foundation, ETSI ZSM introduces a comprehensive service management concept that integrates NFV and edge computing management requirements with other critical components like data collection, analytics, and intelligence. However, NFV-based architectures still rely on monolithic control and orchestration approaches, which limit agility in the service lifecycle and operations. This poses significant challenges, especially when addressing the diverse constraints of Beyond 5G services.

ZSM aims to overcome these limitations by introducing a reference architecture composed of modular building blocks that collectively enable the creation of advanced management services and functions. It emphasizes the clear identification and separation of management domains to isolate responsibilities across varied technologies while respecting boundaries—whether technological, administrative, or geographical. Each management domain delivers a set of ZSM management services through functions that either provide or consume specific endpoints. An end-to-end service management domain plays a crucial role in cross-domain coordination, acting as the glue that integrates management services, functions, and endpoints across all domains.

The core of the ZSM architecture is built on domain integration fabrics and cross-domain integration fabric, which ensure seamless service provision and access through the defined endpoints across domains. These integration fabrics also support communication between management functions by enabling the exchange of management data with consumers. Additionally, specialized domain data services allow the storage and retrieval of data, further facilitated by these integration fabrics. According to ZSM principles, management services can be logically grouped according to the functionality offered (such as data collection, analytics, intelligence, orchestration, control). Fig. 22 depicts the ZSM framework reference architecture. The possibility to flexibly compose management services, together with the exchange of management data provide the foundation of an innovative agile service management that makes easier the integration of the various management aspects (from data collection to orchestration and analysis) enabling the closure of the control loop through network and service optimization processes.

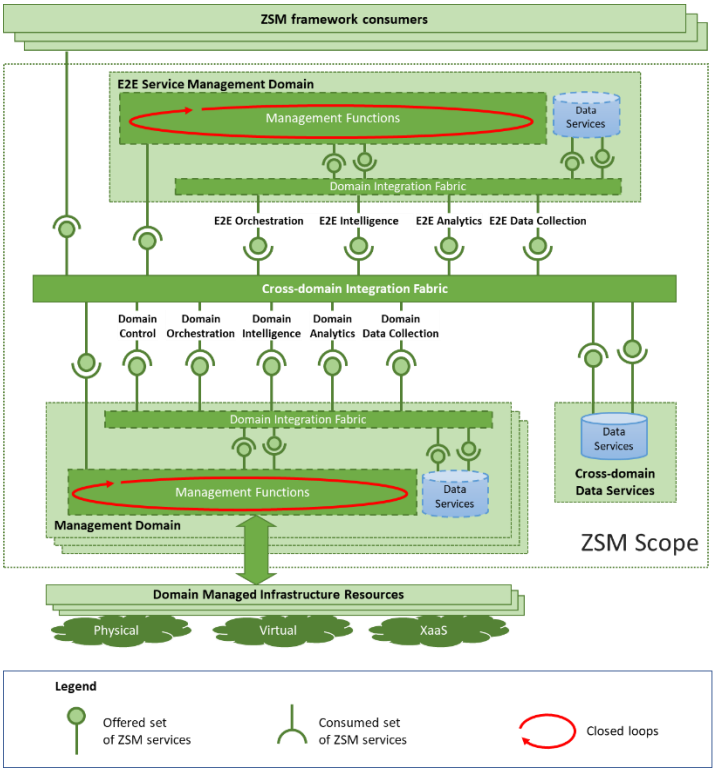

Fig. 22 ETSI ZSM reference architecture

The ETSI ZSM approach and principles align closely with the requirements of the project architecture, particularly in providing an agile framework for integrating AI-enabled vertical and network services within a unified, flexible structure. This framework supports the collaboration of orchestration, data collection and storage, analytics, and AI/ML (intelligence) functions, all operating as decoupled yet cohesive services and components. ETSI ZSM enhances existing management and orchestration capabilities, which are typically focused on the lifecycle management of standalone vertical and network services, by introducing a holistic approach. This approach integrates real-time service operations with data analytics and AI/ML functionalities, offered as value-added services. Such integration is crucial for implementing data-driven, AI-enabled management solutions tailored to the complex and varied demands of 6G networks and their use cases.

Additionally, ETSI ZSM outlines an architecture and enablers aimed at achieving full automation in network and service management. This is designed to enhance the ability of network operators and service providers to deliver, manage, and operate services at scale while minimizing operational costs. ETSI ZSM 005, in particular, introduces solutions to automate a range of functions, operational processes, and tasks related to network and service management. The overarching goal is to create autonomous systems with a high degree of automation, leveraging adaptive technologies and cognitive management systems enabled by closed-loop processes.

Automation mechanisms detailed in ETSI ZSM 005—such as policy-driven automation, intent-based service orchestration, network governance, and network stability—rely on purpose-built zero-touch closed-loop solutions. These closed-loop systems are integral to addressing specific automation challenges, ensuring seamless, intelligent operation across network and service management functions.

4.3. Overview of standards for Semantics in B5G communications

Beyond 5G (B5G) communications, often considered part of the development towards 6G, are expected to incorporate advanced semantic communication standards. Semantic communications focus not only on transmitting data accurately but on delivering contextually relevant and important information, reducing redundant and useless transmission. Below we provide an outline of the emerging standards and frameworks that are currently consider semantics in B5G communications and they are at an initial stage.

Overview of Semantic Communication in B5G

Unlike traditional communications, semantic communication emphasizes the relevance and importance of the transmitted information rather than just its accuracy. For example, rather than sending raw data, the system might extract and transmit only the data that affects the decision-making process. The key challenges include defining and encoding semantics, ensuring robustness against noise, and achieving low latency. Addressing these challenges in a standardized manner remains critical for enabling interoperable and scalable solutions.

ITU and 3GPP Standards

ITU-T Focus Groups: The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) has launched the Focus Group on Artificial Intelligence Native for Telecommunication Networks (FG AINN), which include aspects of semantic processing. Key areas include defining semantic models and metrics for evaluating semantic fidelity.

3GPP's Role in 5G and B5G: The 3rd Generation Partnership Project (3GPP) is expected to include semantic communication principles in upcoming releases (beyond 5G). The focus will likely be on defining frameworks that support semantic-aware applications, such as AR/VR and automated vehicles, which require highly efficient and contextual data transfer. Currently to the best of our knowledge there is no standard.

IEEE P1918.1: Tactile Internet Standard [LIU-1]

Purpose: IEEE P1918.1 provides foundational work for semantics in B5G by defining standards for the Tactile Internet, emphasizing ultra-low latency and high-reliability communication. LIU is part of this standard. Even though in its current draft the semantics are not clearly identified, the standard assumes some prioritization that assists for the reduction of the redundant data by ensuring that only important information is transmitted.

Performance Metrics and Evaluation Standards

Semantic Fidelity Metrics: Traditional metrics (like SNR and BER) focus on bit accuracy, but

semantic communication requires novel metrics to measure semantic fidelity. ITU-T has been exploring ways to assess “semantic accuracy” by evaluating how effectively transmitted data conveys intended meanings and context.

Energy Efficiency and Latency Standards: Standards are also being designed to ensure that semantic transmission can achieve high energy efficiency and minimal latency. This is especially crucial for real-time applications, such as autonomous driving and remote surgery, where only the most contextually relevant information should be transmitted.

Cross-domain Interoperability and Compatibility

Cross-layer: Semantic communication requires a cross-layer approach, with standards that enable cooperation between network layers to manage context-sensitive data. This approach includes dynamic adjustments in protocol layers to prioritize semantics without compromising quality.

Interoperability with IoT Standards [LIU-2]: To accommodate a broad range of devices, standards for semantic communication must interoperate with existing IoT protocols (such as MQTT and CoAP), facilitating compatibility across different domains.

The current report from ITU regarding the requirements and the KPIs titled “Technical Report ITU-T TR.Reqts-SAN - Requirements of semantic-aware networking for future networks” can be found in [LIU-3].

4.4. Overview of 5G/6G standards for B5G access

The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” providing their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. 3GPP specifications cover cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with non-3GPP networks. The figure below provides the official roadmap towards the next Releases of the 5G/6G system by 2025 according to 3GPP.

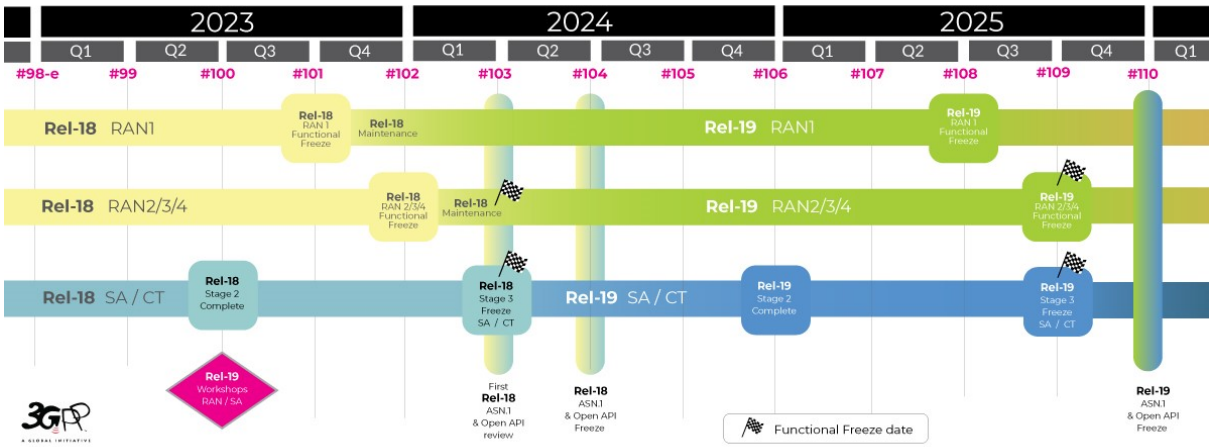

Fig. 23 3GPP specifications roadmap [https://www.3gpp.org/specifications-technologies/releases]

In the sequel we briefly overview the key items and technologies incorporated in the most recent releases of **3GPP** towards the 5G, 5G-Advanced and 6G system. The discussion below is based on the Networld Europe white paper #1 (Technologies & Standards to Enable Vertical Ecosystem Transformation in 6G) released mid 2023.

Release 17

The new standard concerns enhancements of existing functional blocks of the 5G System Architecture along with some additional technologies and verticals. MIMO enhancements like the multiple transmission and reception point (mTRP) that wil benefit eMBB and URLLC service types. Small data transmissions to facilitate 5G IoT related verticals using massive Machine Type Communication (mMTC). UEs with reduced capacity/functionality that is relevant to industrial IoT and wearables with lower computational capabilities and power resources. Also the utilization of new bands to increase throughput for eMBB services (52.6

GHz to 71 GHz). The use of Non-Terrestrial Networks (NTNs) to enhance coverage in remote areas allowing integration of satellite enabled sensors and machine type communications. Enhancements towards private networks with special focus on industrial IoT. Fine-grained accuracy in the order of <30cm positioning for remote control applications (e.g., automotive, IIoT). Extended reality considerations for eMBB services requiring low latency and high bandwidth. Enhancements towards vehicular communications considering vehicle-to-everything (V2X) for the first time.

Release 18

This standard shapes the first version of the 5G-Advanced system, paving the way towards the 6G releases (target is for Rel 21 close to 2028). This standard includes new features introducing for the first time AI/ML support for new and optimized 5G services, vehicle mounted relays, security considerations (e.g., data integrity), time-sensitive/reslieitn services, personal IoT and residential networks. Additional enhancements are proposed targeting to emerging verticals that include smart energy infrastructure, low-power high accuracy positioning for IIoT scenarios, service exposure interfaces for IIoT scenarios, mission critical services enhancements, satellite access to support control and video surveillance.

In parallel with 3PP specifications, the **Smart Networks and Services Joint Undertaking (JU)** became a financially autonomous EU body with continued commitment to deliver on Europe’s ambitions with regard to technological advancement and leadership anchored on collaboration and partnership between the European Commission, the 6G Industry Association as well as national governments, international partners and a broad base of other key stakeholders [SNS Journal 2024] .

]. The SNS JU has seen the kickstart of 28 new Research and Innovation (R&I) projects in January 2024 as part of Phase 2 of SNS JU, complementing the 35 Phase 1 projects (operational since 2023) and bringing the total to 63 running projects. With the standardisation framework designed in November 2023, workshops are being organised by ETSI leveraging the agreement signed in January 2023 with the 6G-IA.

Also, in November 2023, **the International Telecommunication Union (ITU)** published the framework for the development of standards and radio interface technologies for the sixth generation of mobile systems, commonly referred to as 6G. The IMT-2030 Framework Recommendation outlines six “usage scenarios”, three evolving from IMT-2020 and three introducing new capabilities. It has also identified 15 capabilities for 6G technology, nine of which are derived from existing 5G systems. The International Telecommunication Union Radiocommunication Sector (ITU-R) and initiatives such as Hexa-X-II are contributing significantly to this process by defining use case categories and scenarios that envision the transformative capabilities of 6G technology.

ETSI Software Development Group OpenCAPIF (SDG OCF) is developing an open source Common API Framework, as defined by 3GPP, allowing to expose and consume APIs in a secure and consistent way. The group liaises with relevant standards bodies and projects working on network transformation such as the 3GPP, TM Forum, ETSI ZSM, ETSI NFV, ETSI MEC, OpenSourceMANO, TeraFlowSDN and OpenSlice. ETSI OCF realizes a standards-aligned API manager for exposure and consumption of API services in a secure and vendor-agnostic fashion. As such, ETSI OCF is key enabler for mobile network openness to third party software providers, playing a key role as a gateway in any open architecture.

The project targets contributions in the above standards.

4.5. Overview of standards for DLTs and Blockchain

This subsection presents standards for Blockchain and Distributed Ledger Technologies architectures that have been put forward by three different standardization organizations. These organizations are the National Institute of Standards and Technology (NIST), the International Standards Organization (ISO) and European Telecommunications Standards Institute (ETSI) who have published NISTIR 8202, ISO 23257:2022, ETSI GR PDL 008 V1.1.1 (2021-09) respectively.

The standard **NISTIR 8202** [IQB-15], "Blockchain Technology Overview", offers an in-depth introduction to blockchain, outlining its fundamental components, operations, and potential use cases. Published by the NIST, the standard explains how blockchain technology creates a secure and decentralized system for recording transactions. It covers key concepts such as: a) Consensus Mechanisms which are methods, such as Proof of Work (PoW) and Proof of Stake (PoS), that ensure all participants in the network agree on the validity of transactions, b) Cryptographic Hashing, a process that guarantees data integrity by linking blocks of information in a chain, making the data immutable, and, c) Smart Contracts which are code that automates agreements between parties without the need for intermediaries. The standard also distinguishes between different types of blockchains:

- Public: Open and permissionless systems like Bitcoin and Ethereum, where anyone can participate.
- Private: Restricted blockchains, usually operated by a single organization, with controlled access.
- Permissioned: Blockchains where participants need approval to join, balancing openness with control.

Moreover, NISTIR 8202 highlights the technology's advantages, including improved security, transparency, and resilience against tampering. It also discusses potential challenges, including Scalability, Energy Consumption, and Legal and Regulatory Issues. Lastly, this standard serves as a foundational resource for both technical and non-technical audiences, offering insights into blockchain's broad applicability across industries like finance, supply chain, healthcare, and government services. It provides guidance for understanding the technology’s capabilities and limitations as well as its future impact.

ISO 23257:2022 [IQB-16], titled "Blockchain and distributed ledger technologies – Reference architecture", provides a standard framework for implementing blockchain and Distributed Ledger. It offers comprehensive reference architecture to guide the design and development of blockchain systems, ensuring interoperability, security, and scalability across various applications.

The standard also provides details on the components, processes and specifications of a typical blockchain system by describing the following:

- System Architecture: Describes how blockchain systems should be structured, including nodes, consensus mechanisms, and data management.
- Functional Components: Covers functions such as identity management, transaction processing, and smart contract execution.
- Security and Privacy: Addresses how to secure blockchain systems, maintain data privacy, and handle compliance with regulatory requirements.
- Interoperability: Provides guidelines to ensure blockchain networks can interact with each other and with other technologies.
- Governance: Outlines mechanisms for overseeing the operation and evolution of blockchain networks.

ISO 23257:2022 aims to standardize how blockchain and DLT systems are designed, making it easier for organizations to adopt these technologies with consistency and reliability.

The standard **ETSI GR PDL 008 V1.1.1** (2021-09) [IQB-17], "Permissioned Distributed Ledger (PDL); Service and Capability Layer; Report on Interoperability of Permissioned Distributed Ledgers", provides a detailed analysis of how different Permissioned Distributed Ledger (PDL) systems can achieve interoperability. Published by the ETSI, the report focuses on ensuring that PDL platforms can seamlessly interact and exchange data.

The points that the standard addresses are the following:

- Interoperability Framework: The standard outlines frameworks and protocols that allow different PDL systems to communicate and operate together while maintaining their security and operational integrity.
- Challenges: The standard identifies challenges to PDL interoperability, such as varying consensus mechanisms, governance models, and data formats.
- Solutions: The standard suggests possible solutions to these challenges, including standardized interfaces, cross-chain transactions, and common data standards.
- Use Cases: The standard provides examples of how interoperable PDL systems can benefit industries like finance, supply chain, and healthcare, where secure, multi-party collaboration is essential.

Closing, the standard aims to guide organizations in developing interoperable PDL systems, facilitating wider adoption and integration of blockchain technologies in enterprise environments.

5. Relevant EU-funded actions to the SOVEREIGN key areas

5.1. Overview of EU-funded actions towards Non-Terrestrial Networks in B5G

ETHER (SElf-evolving terrestrial/non-Terrestrial Hybrid nEtwoRks: https://www.ether-project.eu/), 2022-STREAM-B-01-03, seeks integrated terrestrial-NTNs, including a unique 3D multi-layered architecture. The ETHER architecture consists of a unified Radio Area Network (RAN) based on 5G standards provided by satellite, high-altitude, and terrestrial network resources, which enables autonomous integrated 3D mesh network management and performance optimization, and handover algorithm. ETHER aims to provide a holistic approach for integrated terrestrial-non-terrestrial networks targeting at 100% network coverage, 99.99999% service continuity and 99.99999% reliability, with 3 times higher energy efficiency and 95% Total Cost of Ownership reduction compared to current terrestrial only deployments. To achieve these goals, ETHER develops solutions for a Unified Radio Access Network (RAN) and for the energy-efficient, AI-enabled resource management across the terrestrial, aerial and space domains, while creating the business plans driving future investments in the area. ETHER relies on a multi-layered and unified space-aerial-terrestrial architecture, leveraging the benefits of Artificial Intelligence/ Machine Learning (AI/ML) for the optimization of the highly complex and heterogeneous "network of networks":

- Provide solutions for a unified and sustainable RAN for the integrated terrestrial and non-terrestrial network.
- Provide an AI-based framework for the self-evolving network slicing management and orchestration of the integrated network.
- Architect a viable, highly energy- and cost-efficient, flexible integrated terrestrial and non-terrestrial 6G network offering seamless and continuous connectivity.
- Demonstrate the effectiveness of ETHER solutions by experimentation activities that target practical applications.
- Identify the key benefits that will drive the investment in the integration of non-terrestrial with terrestrial networks.

TALON (Autonomous and Self-organized Artificial Intelligent Orchestrator for a Greener Industry 4.0, https://talon-project.eu/) introduces an AI orchestrator that envisions transforming the I5.0 into an automated intelligent platform by exploiting advances in edge networks and bringing intelligence near sensors. TALON's use of AI technologies for effectively and securely coordinating the available computing resources in multilayer architecture of NTNs. These can be realized via i) enabling zero-touch deployment and operation; ii) reducing the energy footprint of the whole AI network; iii) guaranteeing high-level security and privacy in heterogeneous application environments; iv) enabling reusability

of datasets, algorithms, metrics and models, as well as boosting the explainability and transparency of the AI approaches.

6G-NTN (6G Non Terrestrial Networks, https://6g-ntn.eu/) project aims at researching and developing innovative technical, business, regulatory, and standardization enablers to achieve full and seamless integration of the NTN component into the 6G system and establish the European leadership in this domain. The vision is to extend coverage, resilience, and sustainability of next generation mobile networks, meeting needs and expectations of both vertical and consumer market segments, while unleashing new value chains and creating broad societal impact.

6G-NTN project target full-fledged integration of the NTN component into 6G leverages multiple key project outcomes that will pave the way for a service roll-out in the 2030-2035 time frame:

- Sustainable and resilient 3D multi-layered (GSO, NGSO, HAPS, drones) network architecture.
- Software defined payload adapted to all flying platforms and all frequency bands
- Very low Earth orbiting space segment
- Flexible waveform supporting terrestrial and non-terrestrial deployments.
- Support of smartphones and vehicle/drone mounted terminals
- The use of new spectrum (i.e. C and Q/V bands) in coexistence with the terrestrial network component and high accuracy and reliable positioning solutions.

The newly designed NTN component will deliver: i.e. uRLLC (latency < 10 ms) and advanced eMBB (data rate up to several hundred of Mbps) services to vehicle, drone mounted ultra-small size devices, and battery activated nomadic terminals; ii. improved eMBB services to smartphones; iii. short emergency messaging services to smartphones in light indoor/in-vehicle environments; and iv. high accuracy (<10 cm) and reliable location service to both devices categories.

5.2. Overview of EU-funded actions towards Network Automation in B5G

The following EU-funded actions are working towards network automation in B5G and 6G networks.

- **ADROIT6G** [IQU-1]: ADROIT6G is working towards the development of a set of groundbreaking innovations with a specific vision for establishing a 6G-based network architecture designed to meet the specific requirements of next-generation applications and achieve the ambitious KPIs defined for 6G networks. Specifically, the key advancements identified by ADROIT6G as crucial for 6G network evolution include: i) AI/ML-driven optimizations throughout the network by utilizing solutions in the "Distributed Artificial Intelligence (DAI)" space to enhance performance and enable network automation; ii) transitioning to a fully cloud-native network software architecture, which can be deployed across diverse edge-cloud platforms with built-in security embedded within the network's user layer; and, iii) software-driven solutions, zero-touch operations, with the ultimate goal of fully automating all aspects of network functionality and service delivery.
- **CENTRIC** [IQU-2]: CENTRIC utilizes AI techniques through a top-down, modular approach to wireless connectivity that puts the users' communication needs and environmental constraints at the centre of the network stack design. CETRIC considers the users' objectives and application-specific requirements, in order to apply AI techniques targeting to create and customize tailor-made waveforms, transceivers, signalling, protocols and RRM procedures to support these requirements. This is the user-centric AI Air Interface (AI-AI) that CENTRIC will enable.
  CENTRIC focuses on providing the desired quality of experience (QoE) to a given user, or type of users, while optimizing spectrum usage, minimizing energy consumption and guaranteeing EMF compliance.
- **DESIRE6G** [IQU-3]: DESIRE6G is working towards network automation through the development of the Service and Management Orchestrator (SMO) layer, where services and applications are instantiated based on descriptors defined in the SMO. DESIRE6G is also working towards the employment of AI/ML algorithms in multi-agent systems targeting network automation. The DESIRE6G's SMO considers available frameworks that provide an open-source solution for managing telecom workloads, including service and network function orchestration. Examples of such frameworks include Open Source MANO (OSM) from ETSI and Open Network Automation Platform (ONAP) from the Linux Foundation.
- **DETERMINISTIC6G** [IQU-4]: The main goal of the DETERMINISTIC6G project is to define essential architectural principles and describe new conceptual solutions as enablers towards the E2E dependable time-critical communication to be provided by the 6G

ecosystem. DETERMINISTIC6G attempts the management of the entire end-to-end interaction loop (e.g. the control loop) with the underlying stochastic characteristics, especially embracing the integration of compute elements, while also aligned with the 3GPP Zero-touch Services Management (ZSM) model.

- **ACROSS** [IQU-5]: ACROSS is working towards the design and implementation of an end-to-end service deployment and management platform for next generation networks and services, aiming at unprecedented levels of automation, performance, scalability, and energy efficiency. In particular, ACROSS develops unsupervised AI solutions for automated decision-making based on telemetry data to empower control loops. Based on these solutions, ACROSS targets to be the first of a new breed of AI-driven zero-touch service deployment and management platforms and has a concrete roadmap for proof-of-concept demonstrations to selected standards.
- **6G-CLOUD** [IQU-6]: 6G-CLOUD focuses on the development and validation of key technologies to realize an AI-native and cloud-friendly system architecture atop the cloud continuum. The project also works to cloud resources offered by multiple stakeholders and allow network functions from different 6G network segments to be composed flexibly and dynamically based on service needs in hybrid cloud environments using automated orchestration.
- **6G-INTENSE** [IQU-7]: 6G-INTENSE proposes a new System Architecture for 6G targeting to deliver "6G as a Smart Service Execution platform", fully in line with the vision of sustainable infrastructure sharing to reduce space and energy costs and encouraging collaboration among all members of the value chain under a unified Network-Compute fabric. A key contribution is a novel automation architecture with a Native AI toolkit facilitating intent declaration, negotiation, and decision automation across autonomous domains, termed Distributed Intent-driven Management and Orchestration (DIMO). Moreover, sensing is adopted as a key enabler, helping to navigate the complexities and lack of reliability of the Deep Edge.
- **ORIGAMI** [IQU-8]: The key objective of ORIGAMI is the development of a novel cross-plane architecture for 6G networks that supports original exposure and compute layers, which jointly (a) remove practical barriers towards 6G, (b) enable sustainable, energy-efficient, and affordable 6G systems, and (c) promote new and disruptive 6G business models. To this end, ORIGAMI designs a Global Service-Based Architecture model that fosters inter-operability across data, control, management, orchestration and NI planes. Moreover, ORIGAMI designs an innovative exposure layer that empowers third parties and virtual operators to customize their networks on top of shared infrastructure well beyond today's network slicing technologies. This approach shall eliminate the need for trust or central coordination, as required today by 5G, offering unprecedented flexibility and autonomy in network management.

5.3. Overview of EU-funded actions towards Semantics in B5G communications

6G-GOALS (6G Goal-Oriented AI-enabled Learning and Semantic Communication Networks): This project approaches the problem by moving towards semantic and goal-oriented communications, integrating new theoretical frameworks with AI-enabled architectures and protocols, essential to distilling the data that are strictly relevant to conveying the semantic meaning or to fulfilling a goal. Moreover, it develops data-efficient protocols adaptable to network dynamics and communication objectives. With advances in semantic data representation, distributed reasoning and green wireless technologies, 6G-GOALS aims to achieve a significant transformation in mobile communications.

ROBUST- 6G (SmaRt, AutOmated, and ReliaBle SecUrity Service PlaTform for 6G): This project aims to address the cybersecurity risks that appear with the necessity for full automation in 6G systems by developing several artificial intelligence (AI) and machine learning (ML)-based solutions. These solutions will focus on advancing AI/ML cybersecurity, implementing zero-touch security management, ensuring privacy and security, promoting energy efficiency and sustainability, and safeguarding AI/ML systems from security breaches.

ETHER (sElf-evolving terrestrial/non-Terrestrial Hybrid nEtwoRks): The project will provide a comprehensive approach for integrated terrestrial-non-terrestrial networks targeting 100 % network coverage, 99.99999 % service continuity and 99.99999 % reliability, with three times higher energy efficiency and 95 % total cost of ownership reduction compared to existing terrestrial deployments. The project will develop solutions for a unified radio access network and energy-efficient, AI-enabled resource management across the terrestrial, aerial and space domains. ETHER will introduce and combine critical technologies under a unique 3D multi-layered architectural proposition. Semantics-aware data analytics solutions are developed and utilized towards energy-efficiency.

TeraWireless (Wireless Networks at Optical Speed with Deterministic Performance) aims to harness THz technology to meet these demands. It focuses on developing ultra-MIMO technology to enhance data rates and link reliability, integrating advanced electromagnetic and communication models, and leveraging semantic communication concepts. Additionally, it will provide an open-access simulation environment for optimising THz networks. TeraWireless will 1) put forth the innovative ultra-MIMO (multiple-input multiple-output) technology for increasing the data rate and link reliability through spatial multiplexing and superdirective beamforming, and will pioneer the development of electromagnetic and communication models for evaluating its performance in low-scattering THz channels, where multipath propagation cannot be exploited, by integrating sensing, localization, communication capabilities; 2) leverage the emerging concept of semantic and goal-oriented communications by folding message semantics and goals of communication within communication layers; 3) develop innovative physics-based ML solutions for energy-efficient, robust, reliable, and explainable-by-design implementations; 4) make available to the

research community the EU's and world's first open-access and open-source simulation environment - integrating ray tracing, link-level, and system-level features - for evaluating and optimizing THz large-scale deterministic networks at optical speed.

Semantic V2X communications: a paradigm shift towards scalable V2X networks:

This project, inspired from the human language to redesign V2X communications by proposing a paradigm shift that makes the semantics of the information the foundation of the V2X communication process. It will develop a novel set of analytical and numerical semantic models that determine the relevance of the information for the intended receivers considering the target application(s) and leveraging a knowledge-driven representation of the communication context. SemanticV2X will leverage the semantic models to develop a novel semantic and goal-oriented V2X communication paradigm where CAVs curate the transmitted information based on its relevance for the intended receivers. The impact of semantic V2X communications on the scalability of V2X networks, as well as on connected and autonomous driving, will be assessed using a unique and advanced CAM simulator, system-level V2X simulations, and novel semantic KPIs. Semantic V2X communications can potentially triple the capacity of V2X networks, effectively addressing the massive connectivity demands of CAM and contributing to the realization of its economic and societal benefits.

MINERVA aims at developing a framework for real-time control, estimation, and localisation in environments where autonomous systems and humans interact. This project will build on timely distributed channel estimation and goal-oriented communications and will fundamentally reassess the way Cooperative autonomous systems (CASs) interconnect and work together to determine the basic principles of real-time control, estimation and communication. This will constitute the foundations for a new framework designed to exploit greater benefits from CASs in a world increasingly reliant on automation.

SONATA (Semantics-empowered Wireless Connectivity: Theoretical and Algorithmic Foundations) project envisions a new communication paradigm that accounts for the significance and usefulness (semantics) of information being generated, processed and transmitted. The project's key scientific challenge is to pursue the mathematical convergence between signal processing and goal-oriented information transmission by exploiting source/signal properties, process variability and semantic information attributes. This will result in a reduction of unnecessary data traffic and the associated required communication, processing and energy resources.

ELIXIRION (rEaLIzing healthcare 4.0 eXploIting the 6G networRk evolutION) will create the first fully-integrated, inter- and multi-disciplinary, highly-innovative training and research network that will set the foundations of the emerging Healthcare 4.0 paradigm by leveraging 6G technologies targeting to: i) provide all citizens/patients with a wide range of services of different requirements, such as ultra-low latency for latency-critical applications, high speed

for data hungry services and ubiquitous secure access to healthcare resources, anytime, anywhere, respecting all privacy aspects, and ii) ensure a secure, efficient, and profitable healthcare ecosystem to all involved stakeholders, while creating a sustainable open market easing access to new players. To achieve the aforementioned objective, ELIXIRION will: 1) leverage a gamut of 6G technologies towards a powerful interconnected network for ultra-high performance access to the healthcare ecosystem targeting up to 99,99999% reliability, 100% coverage, down to sub-ms E2E latency, up to 1 Tbps capacity, high energy- and cost-efficiency, while supporting a massive number of connections, 2) design edge-aware algorithms leveraging diverse computing capabilities offering ultra-fast task execution through parallelization, serverless and distributed computing by intra- and inter- edge node orchestration techniques for real-time mission critical healthcare applications, 3) provide an E2E slicing and zero-touch orchestration framework for optimized 6G network performance across the healthcare ecosystem, targeting at full network automation and secure information handling especially when a massive number of medical devices is considered, by leveraging AI/ML, while considering all different network parts and data analytics to derive useful information helping in the decision-making process, and 4) create a sustainable healthcare ecosystem and new business models leveraging blockchain-based incentive engineering for secure incentivized collaboration among the involved stakeholders.

5.4. Overview of EU-funded actions towards Service Anonymity for B5G access

The European Union (EU) has recognized the vital importance of preserving user privacy and data security as it navigates the complexities introduced by Beyond 5G (B5G) networks. As these advanced networks evolve, they introduce new challenges related to service anonymity, particularly given the enhanced data collection capabilities and the growing number of connected devices. This evolution necessitates a robust framework to safeguard user privacy while ensuring that data is utilized responsibly. To tackle these emerging challenges, several EU-funded initiatives have been launched, focusing on enhancing service anonymity and privacy-preserving mechanisms. These initiatives are designed to address the intricate balance between leveraging data for innovation and protecting individual rights. Key EU-funded projects focused on service anonymity for B5G include the following:

IMAGINE-B5G (01.01.2023 – 31.12.2025, https://cordis.europa.eu/project/id/101096452): It is a project under the Horizon Europe Smart Networks and Services Joint Undertaking, designed to create an advanced, secure, and programmable end-to-end (E2E) 5G platform for large-scale trials across various sectors. IMAGINE-B5G brings together four state-of-the-art 5G experimental facilities located in Norway, Spain, Portugal, and France. These facilities will leverage the existing infrastructure from previous 5G-PPP projects and vertical trial initiative, aiming to maximize the reuse and enhancement of platform components. By drawing on lessons learned from earlier projects, IMAGINE-B5G seeks to build a more robust and effective framework for conducting large-scale trials and pilots in the realm of Beyond 5G applications [IT-8].

IMAGINE-B5G aims to enhance service anonymity through the development of innovative applications that prioritize user privacy while leveraging B5G features. Recognizing the diverse needs across various sectors, the project has identified seven key verticals for targeted advancements: (i) eHealth, (ii) Smart Agriculture, (iii) Transportation, (iv) Smart Cities, (v) Industry 4.0, (vi) Energy Management, and (vii) Entertainment, where these advancements will be tested. Through these targeted advancements across diverse verticals, IMAGINE-B5G not only seeks to enhance service anonymity but also aims to foster innovation in B5G applications that respect user privacy. By prioritizing these principles, the project is paving the way for a future where advanced connectivity can coexist with robust privacy protections, ultimately benefiting users across various sectors.

The focus on service anonymity is essential as B5G networks bring forth unprecedented capabilities for data collection and processing. With the rapid expansion of connected devices and the increasing sophistication of data analytics, the risk of user privacy breaches has significantly increased. To address these challenges, the project is focused on developing applications that integrate advanced privacy-preserving technologies, including

anonymization, pseudonymization, and encryption. This proactive approach ensures that even as data is transmitted more freely and rapidly, individual identities remain protected.

CONFIDENTIAL6G (01.01.2023 – 31.12.2025, https://cordis.europa.eu/project/id/101096435): It is a project under the Horizon Europe Smart Networks and Services Joint Undertaking, focused on enhancing the security and privacy of data in the upcoming 6G networks. It aims to address the growing concerns regarding data protection in an increasingly interconnected world, where the number of devices and the complexity of networks are rapidly expanding. First of all, CONFIDENTIAL6G aims to develop cryptographic protocols that are resistant to potential threats posed by future quantum computing advancements. The project aims to create a comprehensive suite of libraries, tools, and architectural blueprints that ensure confidentiality within 6G environments. Besides, by utilizing advanced techniques such as Fully Homomorphic Encryption (FHE) and Secure Multi-Party Computation (SMPC), CONFIDENTIAL6G will facilitate the secure processing of sensitive data without exposing it, even during computation. This is particularly important for applications that require collaboration across multiple entities while ensuring the privacy of data involved. These methods enable computations to be performed on encrypted data, ensuring that sensitive information remains confidential throughout its lifecycle, thereby enabling trust and cooperation in environments where privacy is of utmost importance. Finally, the project will enhance communication security by implementing advanced protocols, including post-quantum secure networking solutions and blockchain technologies. This approach ensures that data remains protected both during transmission and while stored.

PRIVATEER (01.01.2023 – 31.12.2025, https://cordis.europa.eu/project/id/101096110): It is a project under the Horizon Europe Smart Networks and Services Joint Undertaking, focused on the study, design and development of innovative security enablers for 6G networks, adopting a privacy-by-design approach. This methodology prioritizes user privacy from the very beginning, ensuring that security measures are integrated into the network architecture rather than added as an afterthought. The enablers will complement and be compatible with standard 5G/6G security controls to achieve a holistic, privacy-friendly security solution for future networks.

PRIVATEER represents a significant step toward establishing a secure and privacy-respecting environment for future 6G networks. By emphasizing user privacy within its security frameworks and adhering to regulatory standards, the project aims to build trust among users while enabling innovative applications across various sectors. As telecommunications technology continues to advance, initiatives such as PRIVATEER are essential for ensuring that security measures keep pace with emerging threats and evolving user expectations.

5.5. Overview of EU-funded actions towards the use of DLTs and Blockchain in 5G/6G networks

The **SECRET** project (GA No 722424) utilizes blockchain to address the increasing complexity and demands of 5G networks. Blockchain ensures secure integration of broadband and mobile networking standards, supporting the transition toward highly connected, high-speed services. It provides the foundation for efficient and secure data management, fostering innovation in mobile communications while maintaining robust infrastructure capabilities.

The **SealedGRID** project (GA No 777996) applies blockchain to secure the Smart Grid against emerging ICT-based threats. Distributed ledgers, combined with other technologies, enhance node management, prevent malicious hardware or software modifications, and ensure interoperability. This security platform addresses critical vulnerabilities, safeguarding grids from cascading failures. By integrating blockchain with trusted execution environments and identity protocols, SealedGRID provides a scalable and trusted solution for sustainable energy management.

The **MonB5G** project (GA No 871780) harnesses blockchain to achieve automated, zero-touch management and orchestration of network slices in Beyond 5G. Blockchain underpins the hierarchical and fault-tolerant data-driven system, ensuring secure and efficient operation across technical and administrative domains. By trialing use cases in 5G testbeds, MonB5G demonstrates blockchain's role in scaling slice management while minimizing human intervention, focusing on both energy efficiency and reliability.

The **INSPIRE-5Gplus** project (GA No 871808) utilizes blockchain to enhance security in Beyond 5G networks. By integrating blockchain with AI and machine learning, the project achieves intelligent and trusted multi-tenancy. Blockchain reduces vulnerabilities, improves system control, and secures infrastructure across tenants, ensuring robust and scalable network operations.

The **TESTBED2** project (GA No 872172) leverages blockchain technology to enhance smart grid scalability and functionality in response to evolving energy demands. Blockchain ensures secure and efficient management of data and processes across interconnected grids. It enables seamless coordination among 12 universities and five enterprises, promoting the development and testing of scalable strategies. By addressing infrastructure challenges, the project fosters innovation in electricity delivery and resource optimization.

The **TeraFlow** project (GA No 101015857) employs blockchain to redefine software-defined networking (SDN) for Beyond 5G networks. Blockchain supports secure flow management and enables forensic evidence handling for multi-tenancy. It integrates seamlessly with existing network virtualization and edge computing structures, ensuring secure, automated operations. With blockchain-enhanced zero-touch automation, TeraFlow enables dynamic,

agile, and secure network services for telecom operators and cloud providers, revolutionizing cloud-native SDN controllers.

The **DEDICAT 6G** project (GA No 101016499) leverages blockchain to achieve dynamic intelligence distribution for efficient task execution and reduced latency. It ensures security, privacy, and trust in 6G applications, enabling novel human-digital system interactions. Blockchain enhances techniques for extending coverage with robots and drones, promoting a secure and adaptive platform for hyperconnected societies.

The **SPATIAL** project (GA No 101021808) uses blockchain to tackle the challenges of black-box AI in cybersecurity. By combining blockchain with privacy-preserving methods and resilient metrics, the project ensures accountability and transparency in AI-driven security systems. Blockchain's role in verification and data integrity underpins the development of trustworthy AI solutions, addressing societal and technical challenges in cybersecurity and enhancing trust in AI applications.

The **NANCY** project (GA No 101096456) integrates blockchain to enhance security in Beyond 5G networks by providing robust mechanisms for safe and intelligent architectures. Blockchain supports efficient data management, enabling better resource allocation and network communication. Together with AI, it creates a secure framework to address vulnerabilities in Beyond 5G transitions. By combining these technologies, NANCY ensures seamless and secure interactions among thousands of devices, mitigating risks posed by the evolving network landscape.

The **RIGOUROUS** project (GA No 101095933) leverages blockchain to enhance security and trust in 6G and advanced computing technologies. Blockchain supports the framework's compliance with security requirements, enabling proactive detection and mitigation of breaches. It also facilitates efficient automation of security management, ensuring privacy and robust operations. By integrating blockchain into software and AI systems, RIGOUROUS advances secure computing in next-generation networks.

The **DESIRE6G** project (GA No 101096466) integrates blockchain into its zero-touch management and orchestration platform for ultra-reliable, low-latency 6G applications. Blockchain underpins secure real-time networking and multi-tenancy management, ensuring precision and scalability. Its applications in extended reality and digital twins demonstrate blockchain's potential in enhancing reliability and operational efficiency for mission-critical tasks.

The **VERGE** project (GA No 101096034) employs blockchain within its modular edge platform to secure distributed AI applications. Blockchain supports trust, privacy, and security across diverse edge computing elements. Use cases in industrial Beyond 5G applications and autonomous operations highlight blockchain's role in ensuring data integrity and system resilience. The platform fosters collaboration between academia, industry, and stakeholders.

The **Hexa-X-II** project (GA No 101095759) incorporates blockchain in its blueprint for 6G platforms, ensuring secure connectivity and intelligent integration of human, physical, and digital worlds. Blockchain supports enhanced validation mechanisms for advanced use cases, aligning with the vision of "networks beyond communication." Its integration fosters innovation and ensures societal value in next-generation networks.

The **ELIXIRION** project (GA No 101120135) uses blockchain to support secure, efficient healthcare applications in Healthcare 4.0. Blockchain facilitates ultra-low latency, high-speed connectivity, and privacy in medical data exchange. Its integration ensures secure resource access and scalable healthcare services, fostering a patient-centered and innovative healthcare ecosystem.

The **SCION** project (GA No 101072375) integrates blockchain with AI and digital twins to realize intelligent network orchestration for 6G. Blockchain ensures secure machine-to-machine communications while addressing challenges like energy efficiency and massive access. It supports seamless wireless access, advancing the performance and security of next-generation networks and fostering a highly trained 6G workforce.

5.6. Overview of EU-funded actions towards the use of Self-Sovereign Identities

This section serves to present projects that use SSI and how this identity management mechanism is used in the context of each project.

The **ERATOSTHENES project (Grant Agreement: 101020416)** builds on recent challenges of Internet of Things (IoT) networks, including lack of security visibility, lack of effective information sharing between organizations and availability of tools for CERTs/CSIRTs, heterogeneity of IoT devices, lack of a common trust enforcement mechanism and relevant standards, lack of a transparent identity and privacy frameworks and lacking security training and security protocols' adoption for persons and devices. ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and the Cybersecurity Act. In the ERATOSTHENES project, the goal of Self-Sovereign Identity (SSI) is to provide identity management for the domain with advanced privacy features grounded in SSI principles. This is achieved through device authentication and credential issuance, particularly during the IoT device enrollment process. The system allows for the use of privacy-preserving credentials and disposable IDs, while also interacting with the ERATOSTHENES DLT infrastructure to publish public cryptographic information in an accessible and auditable manner. The SSI-based identity management solution is reinforced by Physical Unclonable Function (PUF) authentication, adding an extra layer of security for device identification and cryptographic fingerprinting. Moreover, this identity mechanism is supported by Distributed Ledger Technologies (DLTs) as verifiable data registries, enabling cross-domain interactions via inter-DLTs.

Another EU-funded project that employs SSI is **TRUSTEE (Grant Agreement: 101070214)** which aims to deliver a green, secure, trustworthy, and privacy-aware framework that aggregates multiple interdisciplinary data repositories (including but not limited to healthcare, education, and automotive) while also takes into account other European data federation spaces and transnational initiatives such as Gaia-X and EOSC. The Trustee project focuses on three areas: serverless computing, edge computing and secure clouds, to deliver an open-source, scalable, efficient and trusted solution, able to seamlessly operate on core and edge cloud infrastructures for time-critical, self-hosted applications. The project aims to deliver a completely encrypted solution that enables researchers to search for and utilize encrypted data. In the context of TRUSTEE, SSI will be enhanced with the use of Blockchain for the decentralized identifiers and Homomorphic Encryption for the cross-discipline federation of data. This will enable data consumers to utilize a framework that will not know anything about their identity, or their equipment and allow them to perform complex search queries across the federated TRUSTEE data repositories and communicate through robust authentication and authorization mechanisms. Hence, the system will only reveal the necessary data for any transaction or interaction

The **OASEES project (Grant Agreement: 101092702)** is funded by the EU and its purpose is to create an open, decentralized, intelligent, programmable edge framework for swarm architectures and applications. The framework will leverage the decentralized autonomous organization paradigm and integrate human-in-the-loop processes for efficient decision-making. The OASEES platform aims to establish a secure and trustworthy edge ecosystem via a decentralized approach which primarily utilizes Self-Sovereign Identity technologies for a portable digital identity without depending on central authorities. In the context of OASEES the SSI solution supports to SSI approaches. One approach focuses on the needs of IoT devices and the other on those of human users. This approach allows the proposed SSI framework to cater to the unique requirements of IoT and edge devices as well as human actors. Furthermore, it ensures a resilient and interoperable, identity infrastructure, facilitating decentralized interactions across the ecosystem. Through the integration of SSI, DIDs and VCs, OASEES aims to build a robust and scalable edge swarm ecosystem capable id securely managing a growing number of IoT devices, thereby addressing the key requirements of authenticity, privacy and integrity.

6. Conclusion

This document provides a comprehensive analysis of mobile data access in Beyond 5G systems, with a focus on emerging trends, technologies, and business models. It begins with an overview of state-of-the-art models and practices for mobile data access, examining telecom market status, key trends, and relevant information for future systems. The document then delves into business models and scenarios for self-sovereign mobile data access, followed by an exploration of state-of-the-art tools and platforms supporting mobile connectivity, distributed ledger technologies, anonymity services, and network automation. Most of the platforms are available within the consortium. Accordingly, a significant portion is dedicated to relevant standards and international fora, highlighting 3GPP, ETSI, and other standards essential for Non-Terrestrial Networks, network automation, semantics, and DLTs in 5G/6G. The final sections cover EU-funded actions in these domains, addressing initiatives for Non-Terrestrial Networks, network automation, service anonymity, and self-sovereign identities, among others. This document serves as a key resource for understanding the technical, business, and policy landscape of mobile data access scenarios and business models in Beyond 5G systems, also targeting to relevant standards and R&I functions.

7. References

[INC-1] Ioannis A. Bartsiokas; Panagiotis K. Gkonis; Dimitra I. Kaklamani; Iakovos S. Venieris, ML-Based Radio Resource Management in Beyond 5G Networks: A Survey, IEEE Access, Volume: 10, 2022.

[INC-2] Loukas Kyriakidis, Michail Kyriakidis. Self-consistent Estimation of Ordinary Differential Equation Parameters Describing Dynamical Systems: A Case Study of COVID-19 in Germany. WSEAS Transactions on Biology and Biomedicine. 2025; 22: 53-66.

[INC-3] Federic Rinaldi, Helka-Liina Määttänen, Johan Torsener, Sara Pizzi, Sergey Andreev, Antonio Iera, Yevgeni Koucheryavy, and Giuseppe Araniti, Non-Terrestrial Networks in 5G & Beyond: A Survey IEEE Access, Volume: 8, 2020.

[INC-4] Mohammad Mozaffari; Ali Taleb Zadeh Kasgari; Walid Saad; Mehdi Bennis; Mérouane Debbah, Beyond 5G With UAVs: Foundations of a 3D Wireless Cellular Network. IEEE Transactions on Wireless Communications, Volume: 18, 2019.

[INC-5] Mark Cudak; Amitabha Ghosh; Arunabha Ghosh; Jeffrey Andrews, Integrated Access and Backhaul: A Key Enabler for 5G Millimeter-Wave Deployments IEEE Communications Magazine Volume: 59, Issue: 4, 2021.

[INC-6] Ericsson. (2023). *5G and the Next Generation of Mobile Services*. / Streaming Video—From Megabits to Gigabytes, Ericsson, Stockholm, Sweden,.

[INC-7] Perspectives from the Global Telecom Outlook 2023–2027 www.pwc.com/telecom-outlook.

[INC-8] Petri Ahokangas, Annabeth Aagaard, Irina Atkova, Seppo Yrjölä, and Marja Matinmikko-Blue, The Changing World of Mobile Communications 5G, 6G and the Future of Digital Services, Edited by Petri Ahokangas and Annabeth Aagaard 2024.

[INC-9] https://opencellid.org/

[INC-10] https://databank.worldbank.org/

[INC-11] https://www.oecd.org/en/topics/sub-issues/broadband-statistics.html

[INC-12] https://ec.europa.eu/eurostat/web/main/data/database

[INC-13] https://www.gsmaintelligence.com/

[IT-1] https://www.robustel.com/product/eg5120-industrial-edge-computing-gateway/

[IT-2] http://www.crew-project.eu/sites/default/files/tmote-sky-datasheet.pdf

[IT-3] Dedeoglu, Volkan & Jurdak, Raja & Dorri, Ali & Lunardi, Roben & Michelin, Regio & Zorzo, Avelino & Kanhere, Salil. (2019). Blockchain Technologies for IoT. 10.1007/978-981-13-8775-3_3.

[IT-4] Sonia Kotel, Fatma Sbiaa, Raouda Maraoui Kamoun, Lazhar Hamel, A Blockchain-based approach for secure IoT, Procedia Computer Science, Volume 225, 2023, Pages 3876-3886, ISSN 1877-0509.

[IT-5] http://www.crew-project.eu/sites/default/files/tmote-sky-datasheet.pdf

[IT-6] Dunkels, Adam & Grönvall, Björn & Voigt, Thiemo. (2004). Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors. Proceedings - Conference on Local Computer Networks, LCN. 455-462. 10.1109/LCN.2004.38

[IT-7] https://github.com/contiki-os/contiki/wiki/An-Introduction-to-COOJA

[IT-8] https://imagineb5g.eu/

[IQB-1] Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/release-2.5/, Online, Accessed on 18-10-2024

[IQB-2] uPort, https://github.com/uport-project, Accessed on 18-10-2024

[IQB-3] Veramo, Introduction, https://veramo.io/docs/basics/introduction/, Accessed on 01-11-2024

[IQB-4] Veramo, Performant and modular APIs for Verifiable Data and SSI, https://veramo.io/, Accessed on 01-11-2024

[IQB-5] Hyperledger Aries, https://github.com/hyperledger/aries, Accessed on 18-10-2024

[IQB-6] Ethereum, "What is Ethereum", https://ethereum.org/en/what-is-ethereum/, Accessed on 01-11-2024

[IQB-7] Rahmadika, Sandi, Firdaus, Muhammad, Jang, Seolah, Rhee, Kyung-Hyune, Blockchain-Enabled 5G Edge Networks and Beyond: An Intelligent Cross-Silo Federated Learning Approach, Security and Communication Networks, 2021, 5550153, 14 pages, 2021. https://doi.org/10.1155/2021/5550153

[IQB-8] Aristeidis Farao, Georgios Paparis, Sakshyam Panda, Emmanouil Panaousis, Apostolis Zarras, and Christos Xenakis. 2023. INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. Int. J. Inf. Secur. 23, 1 (Feb 2024), 347–371. https://doi.org/10.1007/s10207-023-00741-8

[IQB-9] Camenisch, J.; Van Herreweghen, E. Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02), Washington, DC, USA, 18–22 November 2002; pp. 21–30.

[IQB-10] Wojciech Niewolski, Tomasz W. Nowak, Mariusz Sepczuk, Zbigniew Kotulski, Security architecture for authorized anonymous communication in 5G MEC, Journal of Network and Computer Applications, Volume 218, 2023, 103713, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2023.103713. (https://www.sciencedirect.com/science/article/pii/S1084804523001327)

[IQB-11] Chow, Man Chun, and Maode Ma. 2022. "A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks" Sensors 22, no. 12: 4525. https://doi.org/10.3390/s22124525

[IQB-12] Decentralized Identifiers (DIDs) v1.0, W3C, https://www.w3.org/TR/did-core/, online, Last accessed on 13-12-2024

[IQB-13] Verifiable Credentials Data Model v1.1, W3C, https://www.w3.org/TR/vc-data-model/, online, Last accessed on 13-12-2024

[IQB-14] W3C, Decentralized Identifiers (DID) v1.0, https://www.w3.org/TR/did-core/ , Accessed on 20-10-2024

[IQB-15] Dylan Yaga (NIST), Peter Mell (NIST), Nik Roby (G2), Karen Scarfone (Scarfone Cybersecurity), NIST IR 8202 Blockchain Technology Overview, National Institute of Standards and Technology, Accessed online on 20-10-2024

[IQB-16] ISO 23257:2022, Blockchain and distributed ledger technologies — Reference architecture, 2022, International Standards Organization, Accessed online on 20-10-2024

[IQB-17] European Telecommunications and Standards Institute, ETSI GR PDL 008 Permissioned Distributed Ledger (PDL); Research and Innovation Landscape, 2021, Accessed online on 20-10-2024

[UOA-1] D. Xenakis, A. Tsiota, C. -T. Koulis, C. Xenakis and N. Passas, "Contract-Less Mobile Data Access Beyond 5G: Fully-Decentralized, High-Throughput and Anonymous Asset Trading Over the Blockchain," in IEEE Access, vol. 9, pp. 73963-74016, 2021, doi: 10.1109/ACCESS.2021.3079625.

[UOA-2] Ericsson Mobility Report 2024, Nov. 2024.

[UOA-3] Z. Chen et al., "Timeliness of Status Update System: The Effect of Parallel Transmission Using Heterogeneous Updating Devices," in IEEE Transactions on Communications, vol. 72, no. 11, pp. 7093-7107, Nov. 2024, doi: 10.1109/TCOMM.2024.3409194.

[UOA-4] D. Xenakis, "To DASH, or Not to DASH? Optimal Video Bitrate Selection and Edge Network Caching in MEC-Empowered Slice-Enabled Networks," in *IEEE*

Transactions on Vehicular Technology, vol. 73, no. 4, pp. 5556-5571, April 2024, 10.1109/TVT.2023.3329662, vol. 73, no. 4, pp. 5556-5571, April 2024.

[UOA-5] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks", *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585-4600, Jun. 2019.

[UOA-6] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm", *IEEE Access*, vol. 7, pp. 9714-9723, 2019.

[IQU-1] https://adroit6g.eu/

[IQU-2] https://centric-sns.eu/

[IQU-3] https://desire6g.eu/

[IQU-4] https://deterministic6g.eu/

[IQU-5] https://across-he.eu/

[IQU-6] https://www.6g-cloud.eu/

[IQU-7] https://6g-intense.eu/

[IQU-8] https://sns-origami.eu/

[LIU-1] “IEEE Approved Draft Standard for Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture, Functions, and Technical Assumptions”, in IEEE P1918.1/D4, June 2024, vol., no., pp.1-67, 3 Oct. 2024.

[LIU-2] European Research Cluster on the Internet of Things, IoT Semantic Interoperability: Research Challenges, Best Practices, Solutions and Next Steps, IERC AC4 Manifesto "Present and Future".

[LIU-3] http://handle.itu.int/11.1002/pub/8217d06f-en