Moving towards open radio access networks with blockchain technologies

Nischal Aryal, Fariba Ghaffari, Emmanuel Bertin, Noel Crespi

Moving Towards Open Radio Access Networks with Blockchain Technologies

[1, 2] Nischal Aryal, [1, 3] Fariba Ghaffari, [1, 2] Emmanuel Bertin, [2] Noel Crespi
[1] *Orange Innovation, 14000 Caen, France*
[2] *SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France*
[3] *Institute of Research and Technology b-com, 35510 Cesson-Sévigné, France*
{nischal.aryal, emmanuel.bertin}@orange.com, fariba.ghaffari@b-com.com, and noel.crespi@it-sudparis.eu

***Abstract*—The Open Radio Access Network (O-RAN) introduces openness and intelligence into the existing, tightly-coupled RAN ecosystem. Openness promotes collaboration among various vendors to provide diverse components (hardware, software, or both) for the RAN ecosystem, while intelligence handles complex network activities using Artificial Intelligence (AI). Although O-RAN design addresses many issues in traditional RANs, such as vendor lock-in, lack of flexibility, and limited innovation, it raises several management and security concerns related to collaboration, access management, privacy, trust, and availability. Distributed Ledger Technologies (DLTs) offer a viable method of establishing trust among entities, managing resources efficiently, and automating complex network tasks. Several DLT properties, such as distributed architecture, high automation through smart contracts, immutability, and transparency, could position DLT-based ideas as game changers in a multi-vendor O-RAN ecosystem. Furthermore, this technology has the potential to introduce new business models and establish secure and trusted micro-payments among vendors and network participants. In this paper, we first present a taxonomy for discussing existing O-RAN challenges. Based on the taxonomy, we then examine the possibility of incorporating DLT-based solutions in O-RAN architecture to address these challenges.**

***Index Terms*—O-RAN, Multi-vendor, Openness, Intelligence, DLT, Blockchain, Smart contract**

I. Introduction

The rapid increase in cellular network traffic has led mobile network operators to adopt a software-driven, intelligent, and energy-efficient strategy for various network activities [1]. Next-generation cellular networks (NGNs) will not only serve users but also a wide range of smart devices (e.g., IoT) and business domains. To accomplish this, many technologies (e.g., artificial intelligence, cloud/edge computing) will need to be integrated with the existing mobile network, resulting in higher system complexity. The challenge is particularly significant in the Radio Access Network (RAN), the entity that manages the connection between the user and the mobile core network. Currently, RAN components are monolithic units produced by a small number of manufacturers, and the tight coupling between their software and hardware makes it very difficult to incorporate new technologies into the ecosystem.

To solve these limitations, multiple solutions have been offered, with Open Radio Access Network (O-RAN) being one potential option for next-generation mobile networks [1], [2]. The two main principle of O-RAN are openness and intelligence. Openness allows RAN to be disaggregated into numerous components and virtualized into commercial off-the-shelf hardware. Communication among these disaggregated entities is enabled by open and standardized interfaces, promoting a multi-vendor environment. Intelligence enables the incorporation of novel AI/ML models capable of automating and optimizing the network's complex operations. Although O-RAN addresses numerous existing concerns, such as tight hardware-software coupling, vendor lock-in, and handling sophisticated network operations, it introduces new challenges to the RAN ecosystem, such as orchestration, performance, security, deployment and operation, and business [3].

The use of DLT has grown in popularity, with Blockchain serving as its most well-known use along with its idea of smart contracts. DLTs have been examined as a possible solution to address the concerns with NGNs, thanks to their features, such as immutability, distributed nature, non-repudiation, intrinsic security, permanence, and traceability. These technologies provide a novel approach to validate data transactions and ensure traceability in a variety of contexts. The number of prominent businesses researching DLT in the telecommunications sector is constantly growing, with studies being conducted for multi-vendor design, access control and authentication, identity management, mobility management, resource/service delivery, new business models, fast technology integration, system fault tolerance improvement, increasing automation, and cost savings [1], [4]–[6].

In this paper, we will look at the O-RAN architecture and how openness and intelligence are fundamental components of it. We then provide an updated taxonomy of O-RAN challenges derived from our previous work [3], and discuss these distinct challenges in detail. Based on the existing issues and by surveying the state of the arts, we examine the viability of Blockchain-based solutions to address these challenges.

Related Works: Considering the significance of O-RAN and its prominent role in ongoing research works, several studies have emerged that concentrate on the existing challenges within this domain. For example, in a comprehensive investigation by [2], the authors thoroughly analyze the challenges prevalent in the O-RAN ecosystem and propose potential solutions to tackle these concerns. Similar concepts are explored in the works of [6] and [7]. Furthermore, our previous study [3] surveys the existing challenges of the O-RAN ecosystem and categorizes them into four key areas:

Orchestration, Performance, Security, and *Deployment and Operations*. In our current work, we expand upon this classification and address additional problems related to *Security, Deployment and Operations,* and *Business* aspects. However, it is important to note that these studies solely focus on the issues within the O-RAN system. To the best of our knowledge, our research is the first to investigate the feasibility of employing Blockchain technology to address the existing challenges in O-RAN design.

Paper organization: Section II provides a brief overview of O-RAN and outlines the significance of openness and intelligence in this architecture. Section III describes the existing O-RAN system challenges and IV investigates the possibility of Blockchain-based solutions for addressing O-RAN issues in Section. Finally, Section V presents some potential future directions and concludes the work.

II. Background of O-RAN

The main goal of O-RAN design is to bring innovation to the RAN ecosystem while lowering the cost of setting up and operating the overall mobile network [1]. The O-RAN Alliance [8] is a consortium of operators, industries, and academic institutions that work on defining standards for implementing the concepts of cloud-based economics and agility in the O-RAN ecosystem.

They are working on two main goals to achieve these objectives: openness and intelligence.

O-RAN can have multiple definitions of **openness** in terms of hardware, software, open interfaces, and the involvement of many participants in the RAN ecosystem. In terms of hardware, it refers to using commercially available off-the-shelf hardware, instead of expensive and RAN-specific hardware. Regarding software, O-RAN refers to using open-source software from various software communities, instead of hardware-specific software. The open interfaces establish standards and guidelines for connecting different services to the RAN ecosystem. This strategy aims to eliminate vendor lock-in (a small number of vendors providing RAN services) by allowing small vendors and operators to introduce their services enabling faster, more flexible, and democratic innovations.

The goal of **intelligence** in O-RAN is to develop a self-driving network capable of automating network functions by leveraging new learning-based technologies. This strategy is critical for next-generation networks, as they will be able to meet the needs of diverse users, services, and applications with varying network demands. As a network's services expand, the complexity of the network increases, making traditional management methods ineffective. Thus, integrating automated services related to resource allocation and optimization by applying deep learning techniques to multiple layers in RAN architecture could help to mitigate the complexity issue.

Figure 1 represents the general architecture of the O-RAN system. It consists of RAN functions and interfaces specified by the O-RAN Software Community (O-RAN-SC) [9]. The architecture contains two groups: the radio group and the management group. The radio group consists of Near-Real Time RIC (Near-RT RIC), Next Generation RAN (NG-RAN) – which consists of radio units (O-RU), distributed units (O-DU), and central units (O-CU) –, and O-RAN eNodeB (O-eNB) and are responsible for radio communications. The management group consists of Service Management and Orchestration (SMO) framework and Non-Real Time RIC (Non-RT RIC) and is responsible for system performance and management. O-RAN Cloud (O-Cloud) is a cloud computing platform that hosts the O-RAN functions and software.

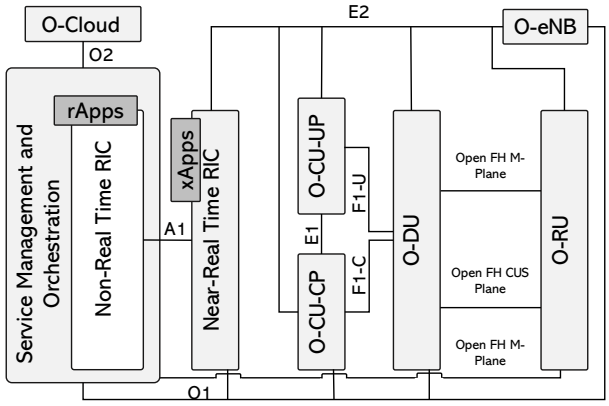

Fig. 1. General architecture of O-RAN system showing key functions and open interfaces defined by O-RAN Alliance [3].

III. Challenges in O-RAN

This section highlights the existing challenges in the O-RAN system. As shown in Figure 2, the challenges are categorized into five groups: orchestration, performance, security, development and operations, and business.

A. Orchestration

Managing the operation of different functionalities within O-RAN to make the system fully operational is referred to as *Orchestration*. Orchestration challenges can be categorized into *service management* which is related to O-RAN functions' administration/placement, and *intelligence management* concerning AI/ML function placement in this ecosystem.

1) Service Management: Due to the multi-vendor ecosystem, proper deployment and administration of diverse hardware and software are the primary concerns for O-RAN [10] [11] [3], [12]. Although O-RAN Software Community (O-RAN-SC) has defined standard interfaces for interoperability between different vendors, there are still concerns regarding operations, administration, maintenance [13] [14], and optimization of RAN module placement [15].

2) Intelligence Management: Regarding intelligence management, orchestrating AI/ML models [10], determining the right AI/ML model, choosing an appropriate deployment location and resource requirement, and considering the time scale to make input available [16] [11] [17] [18], handling fault prediction (i.e., drifting) of AI/ML results, and integrity and

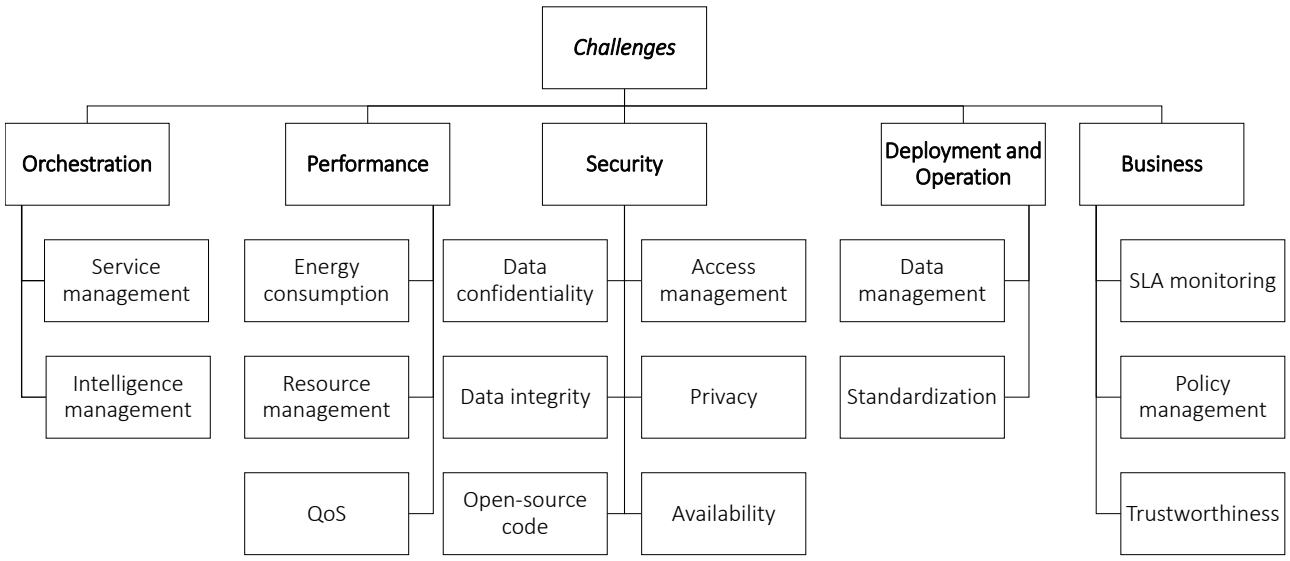

Fig. 2. Taxonomy to categorize current challenges in O-RAN system.

validity of AI/ML models in xApps and rApps [2] are some of the existing challenges for the O-RAN system [3].

B. Performance

One of the primary goals of O-RAN is to improve performance in terms of energy consumption, latency, and scalability which helps to provide better quality of services. To achieve this goal, there are several challenges that need to be addressed first. In this section, we categorize these challenges based on energy consumption, resource management, and quality of service, all of which are closely tied to O-RAN performance requirements.

1) Energy Consumption: The goal of cellular network design has always been to provide high network performance while ignoring energy conservation [19]. As a result, RANs in cellular networks consume more than half of their total energy [20]. According to [19] [21], disaggregation of network functionalities of O-RAN into various hardware, and the operation of these hardware results in increased energy consumption. Energy efficiency has become a big concern for network providers because the amount of energy utilized is proportionally tied to the operational costs of the network [22] [19] [17].

2) Resource Management: The effective allocation and utilization of network resources will be one of the main challenges for the O-RAN system. In the current cellular network, proper management of heterogeneous traffic flow concerning network capacity is still an open issue [23]. O-RAN networks should adapt to the dynamic resource requirement of the network services and users (e.g., network slicing). The growing network traffic also emphasizes the need for an intelligent and automated solution.

3) Quality of Service: The quality of service (QoS) will be a vital element in the O-RAN system, determining the system's performance and throughput. QoS enables the analysis of user satisfaction with services, which may help improve the services and reach profit growth. Network operations management, proper hardware-software selection, and continuous monitoring of application-level services are some of the fundamental decisions that contribute to improved QoS [24]. One of the challenges in the O-RAN system is identifying front-haul open interface (the connection between O-DU and O-RU as shown in Figure 1) requirements to achieve ultra-low latency [25]. Another challenge is the placement of functionalities in the network ecosystem [15] [10] and scalability [5] to achieve better performance.

C. Security

As the mobile network industry moves toward RAN virtualization, O-RAN systems must adopt a risk-based approach to their security challenges [26]. The disaggregation of the O-RAN and the introduction of new functionalities and open interfaces have increased the overall system's security risk, which needs proper identification, assessment, and security protocol implementation before deployment [27]. This section discusses the existing challenges of O-RAN regarding security in two sub-categories: data confidentiality and availability.

1) Data confidentiality: The introduction of RICs enables intelligent solutions in the form of xApps and rApps to handle complex network activities. These solutions require substantial information from the lower network level, such as DUs, for training and accurate prediction. The information generated at DU contains user-sensitive information which could get

exposed when shared with RICs [15]. Moreover, the multi-vendor ecosystem of O-RAN might also create confidentiality challenges when handling such user-sensitive data [26] [28].

2) Access management: As previously stated, various modules and functionalities in O-RAN (for example, xApps and rApps from multiple vendors) require user-sensitive data. Aside from user data, the O-RAN system also relies on machine learning datasets. These data are kept on SMO and are critical for effectively training different ML models [6], [29]. However, due to the involvement of multiple suppliers, enabling proper access to these data is a significant challenge for the O-RAN system [6]. Another challenge is the vulnerabilities of these functionalities, such as misconfiguration and program bugs, which could result in unauthorized access to the system [2]. Thus, proper planning is required to set up access control procedures in an O-RAN system because failure to do so can result in additional security issues such as denial of service and man-in-the-middle attack [2].

3) Availability: Although disaggregation could provide numerous technological and performance benefits, system availability remains a critical challenge that must be addressed [30]. The introduction of open markets and interfaces, as well as the virtualization of RAN functions, raises security concerns about the hardware and software [31]. The location of RAN functionalities has a significant impact on availability in an O-RAN system. The RIC applications may also affect availability. Because xApps and rApps handle critical control loops, these applications must be resistant to outages [32]. The O-RAN system must be highly available to operate the services of the cellular network. Moreover, unauthorized access to the infrastructure and user's sensitive data can result in denial of service in infrastructures [2], due to the complexity of access control regulation in an open and multi-vendor environment [6].

4) Privacy: Because the functionality of O-RAN is dependent on the processing of users' sensitive and personally identifiable information (PII), ensuring end-user privacy is critical in this setting. In this environment, policy rule violations are possible due to the collaboration of various stakeholders in O-RAN. It means that the O-RAN system requires precise privacy rules for transferring data, storing data in different locations, and dealing with new interfaces. Another challenge with collaboration and privacy regulation in this context is that there is no clear policy rule prohibiting transmitting user data between stakeholders and third parties such as security agencies in the existing O-RAN. As a result, there are possibilities of privacy violations between stakeholders and third parties [6].

5) Open-source code: Since O-RAN relies on open-source hardware and software, this technology inherits several well-known challenges such as malicious code injection by the distrustful entity [29], [33] and utilizing the libraries that are not under the control of the O-RAN alliance or the involved stakeholders [2]. In terms of intelligence, inserting malicious code in different parts of the O-RAN system can negatively affect the efficiency of AI/ML algorithms, security of the system, privacy, and availability.

D. Deployment and Operations

This section highlights the challenges during the deployment and operation phases of the O-RAN system. The existing challenges of O-RAN regarding deployment and operations are discussed in two sub-categories: data management and standardization.

1) Data Management: Since O-RAN will rely on AI/ML solutions to handle complex activities in RAN [1], data management will be essential. Although RAN generates a large amount of data, a key challenge lies in storing, categorizing, and selecting the data according to the use-case requirement. Another challenge lies in data access because most of the data generated by RAN base stations is proprietary to the base station owners, which is difficult to share due to privacy and competition concerns [18], [34]. Furthermore, there is also a lack of open-source data for research purposes. Because of this, academics and practitioners often rely on datasets generated through laboratory setups, which hardly represent the diversity and scope of actual cellular deployments.

2) Standardization: Standardization is essential for the O-RAN system to help ensure the safety, quality, and reliability of each functionality in the system. As O-RAN introduces the concept of openness, an operator can have different equipment from different vendors who might have different naming conventions for counters and KPIs [35]. Thus, it is necessary to set up proper standards for each functionality that will be used in the O-RAN system. However, there are no standards currently established for this functionality integration as mentioned in Section III-C5, [6], [29]. Moreover, due to the collaboration of stakeholders from different locations with different common standards for interfaces, privacy management, etc., the lack of a standard process can result in several issues such as privacy violations, non-secure interfaces, unauthorized access, etc.

E. Business

This section provides an overview of the existing challenges regarding the O-RAN's businesses concerning service level agreements and the trustworthiness among the entities as a basic concern in a multi-vendor environment.

1) Service Level Agreement (SLA) monitoring: A service level agreement (SLA) is a contract between a service provider (SP) and a service user that specifies the service standards and requirements that the provider must fulfill. The challenges regarding SLA management in O-RAN can negatively affect the performance and reliability of different functionalities such as intelligence management, collaboration among stakeholders, and service provisioning.

Malicious xApps in RIC might affect the priority levels of current SLAs, resulting in malfunctioning or wrong decision-making in service provisioning [6], [36]. Furthermore, changes to ML algorithms can result in incorrect decisions regarding dynamic resource allocation in slicing, leading to an SLA violation [37]. Furthermore, because the O-RAN market is an open market with an infinite number of users and stakeholders,

centralizing and manually administering SLA contracts in this context is inefficient. This means that when the number of entities in this environment grows, the traceability of SLAs, their integrity and authenticity, and verification would become a highly complicated IT operation [38].

2) Trustworthiness: Since O-RAN relies on collaboration among entities in a multi-vendor environment, providing trust in this distrustful environment is inevitable. Trust challenges in O-RAN can be categorized into different groups 1) trust between stakeholders regarding their provided services and payments, each stakeholder, vendor, or entity needs to be sure that the provided services are based on the predefined policies, SLAs, and agreements, and the payments (if it is required) are according to these agreements. Moreover, the stakeholders need to be trustful regarding the security of provided codes, services, etc. [29], [6]. 2) copyright and patent management for open-source software [6] that is mostly linked to the political and financial interests of competing organizations.

IV. Blockchain as a solution

In the preceding section, we discussed the existing challenges faced by the O-RAN system. As with the adoption of any new concept, there is a potential for the introduction of new issues into the system. The highlighted challenges have arisen because of O-RAN's efforts to integrate openness and intelligence into the RAN ecosystem. In this section, we will delve into various aspects of the O-RAN system where solutions based on Blockchain can be utilized to address the challenges. It is crucial to recognize that while Blockchain technology cannot resolve all the problems outlined earlier, it does offer robust solutions in specific cases such as business and collaborations, resource sharing, data management, and security.

A. Business and collaborations

Establishing coordination among the numerous providers in the O-RAN ecosystem is crucial. Given the interdependence of services and the continuous exchange of sensitive information, a significant level of trust must exist between these companies and the services they offer [39]. Additionally, to minimize complexity, enhance performance, and ensure traceability, collaborative management in this context should be highly automated, minimizing the need for manual intervention.

Blockchain technology presents numerous opportunities for managing collaboration among diverse entities within the O-RAN ecosystem [40]. For example, utilizing smart contracts to define service-level agreements not only enables high levels of automation in managing agreements but also enhances contract traceability, immutability, and non-repudiation [41], [42]. These characteristics foster transparency and trust within a distributed and potentially untrusted environment. Additionally, Blockchain can facilitate the creation of a digital marketplace where suppliers can advertise their services, and customers can utilize an interface to find the most suitable service based on their requirements [4]. Suppliers can encode all necessary requirements and rules into a smart contract, and users only need to accept these terms, while also being able to input their own specifications. The inclusion of penalties can help ensure compliance from both parties, facilitating the automated management of complex procedures [5].

When implementing Blockchain-based solutions, it is crucial to consider the specific type of Blockchain suitable for a given business context [43]. According to [39], a permissioned Blockchain is often the preferred choice as it allows for the establishment of trust among multiple parties within a system using smart contracts. This enables direct communication channels and ensures transparency in their actions. However, depending on specific requirements, other types of Blockchain can be selected. Operators can utilize Blockchain to track the performance of infrastructure provided by various vendors, enabling them to assess whether the services are providing the required performance.

B. Resource Sharing

As mentioned earlier, resource management is a critical concern for mobile network operators aiming to cater to diverse businesses. Given the limitations of resources and the associated increase in energy consumption and capital expenditure, finding a solution becomes imperative. Resource sharing emerges as a viable approach to tackle these challenges. By sharing network resources and infrastructure with other mobile network operators (MNOs) or businesses, MNOs can reduce their capital expenditure significantly. Furthermore, resource sharing promotes energy efficiency by minimizing the number of operational devices and contributes to environmental sustainability by reducing infrastructure footprint. However, establishing trust and reaching agreements among the sharing parties is essential.

Blockchain-based solutions offer several advantages in the context of resource sharing. They introduce transparent ledgers that facilitate auditing and resource management in a multi-vendor environment. Smart contracts enable the automated handling of complex sharing arrangements and the establishment of regulations [4]. Blockchain technology has been applied in various use cases of resource sharing, including cellular networks and content delivery networks. For instance, [5] propose an ecosystem that enables MNOs to share the Radio Access Network (RAN) in the form of virtual network functions (VNFs), allowing resource/infrastructure trading as a service. The use of Blockchain technology enhances trustworthiness and automation in resource sharing [44]–[47]. Other studies, such as [44]–[47] propose a Blockchain-based RAN architecture (B-RAN). Using this system, different trustless network entities can authenticate each other to provide dynamic and secure connections. This solution implements self-organized access for users and providers, along with enabling mobility management. In this method, the user equipment and host access points agree on price and digitized spectrum assets via a smart contract. In [48], the authors propose a Blockchain-based medium access control method. In [49], the authors propose BE-RAN, as a Blockchain-based RAN to provide user-centric identity management, as well as mutual

authentication possibility for all network entities. The authors in [50] propose a Blockchain-enabled wireless communication by providing a unified Blockchain-based radio access network (B-RAN) framework for 6G. In this method, the connection between UEs and RAN is done by smart contracts to provide trustworthiness for communication and payment.

C. Data management

Data management will grow in significance for network operators as intelligence becomes integrated into the O-RAN ecosystem. Handling confidential user data, including sensitive information like user location, poses a challenge within the multi-vendor environment of O-RAN. Two key categories for addressing data management challenges in O-RAN are user-related data management and AI/ML-related data management. Blockchain-based solutions offer a promising approach to tackling these issues by establishing a secure, transparent, and trusted system [51].

User related data management: In this scenario, [51] propose a Blockchain-based solution for dynamic and secure data exchange and management between multiple mobile network operators (MNOs). By utilizing a permissioned Blockchain, the solution facilitates secure access to RAN data and allows for the sharing of public data alongside dynamic private alignments. The primary objective is to enable seamless connectivity between the RANs of different MNOs while enabling internal management of their respective RAN data. In a similar vein, [52] propose a Blockchain-based Proximity Radio Access Network (P-RAN) solution for 5G and 6G. This approach utilizes the inherent capabilities of Blockchain, such as authentication and asymmetric key pairs, to manage user equipment (UE) and network usage information. Additionally, connection summaries are immutably recorded on the Blockchain for traceability and future purposes.

AI/ML related data management: In this scenario, we consider two different approaches: 1) how Blockchain can improve the existing AI/ML procedure in O-RAN, and 2) how AI/ML can positively influence the Blockchain usage in a networking application, more specifically O-RAN use cases.

- **Blockchain for AI/ML:** Based on [53], [54], shared ledger, immutability, secure peer-to-peer communication, consensus-based updating, and having timestamps for all transactions can be effective in providing *secure data and model sharing, privacy-preserving, trust in decision making and decentralized intelligence*. In this regard, [55] propose "ADVOCATE" in which they aim to gather and analyze the policy data for making decisions using machine learning. They use Blockchain technology to manage the ML data in a transparent and traceable manner, in which the non-repudiation of the participants is also guaranteed. In this method, the authors propose to send the hashed version of the data to Blockchain to validate its integrity, non-repudiation, and correctness. To preserve the privacy of the AI/ML model/data producer in the networking environment, [56] propose ModelChain on top of Blockchain. Moreover, the Ocean Protocol [57] proposes a decentralized system on top of Blockchain to share AI/ML data and models using a three-layer architecture. In this method, the data providers upload their data securely and in a private manner to sell them to customers who can discover the required data and buy them. Another Blockchain-based AI/ML-based system is proposed by [58], in which the AI/ML system is benefiting from the immutability of Blockchain to store the models to predict incidents in smart vehicles.
- **AI/ML for Blockchain**: If we view the ML and Blockchain integration from the other perspective, Blockchain also can benefit from AI/ML algorithms to improve the resource efficiency regarding the processing power and storage, improve scalability, and enhance security and privacy. Moreover, the integration of AI/ML-based systems with smart contracts brings many unprecedented opportunities regarding smart, automated, distributed, and trusted processing [53].

D. Security

Undeniably, preserving network security in a variety of aspects is an inevitable requirement for O-RAN functionality. Following are some possible playgrounds for Blockchain technology to be applied in an O-RAN use case:

- **Identity management:** Providing distributed identity management in the O-RAN use case can provide many unprecedented opportunities regarding data ownership, higher fault tolerance and availability, secure data sharing, and higher privacy due to the elimination of third parties [6]. Moreover, self-sovereign identity management systems are identity management systems that give full data and digital identity ownership and control to individuals without relying on a third party. This paradigm was implemented for the first time in 2015 by applying Blockchain technology to identity management. In other words, self-sovereign identity has three pillars: 1) Blockchain, as a decentralized database to record information in an immutable manner; 2) Decentralized Identifiers (DIDs), which are authentication and identification solutions without the need for any third party in the network. This can be achieved by immutable codes stored in Blockchain, and 3) Verifiable Credentials (VCs), which are digital cryptographically secure versions of an individual's identity. Based on its definition, this method can provide more robust, fault-tolerant, scalable, distributed, and secure identity management with better privacy [59], [60], [61].
- **Privacy:** Managing the user's identity in a distributed environment without relying on third parties, certificate authorities, or public key infrastructure can preserve the privacy of the entities in the network [6]. Note that anonymity (i.e., metadata or identity privacy) is an intrinsic Blockchain feature. Moreover, the self-sovereign identity management system enabled by Blockchain is proposed for this purpose. Regarding the policies, the definition of privacy rules in Blockchain can improve

their traceability as well as immutability in the distributed environment. For privacy-preserving solutions using Blockchain technology, in [49], the authors propose a distributed privacy-preserving solution for RAN data in P2P communication in BE-RAN. PrivacyGuard [62] provides a privacy-preserving solution for data sharing in a cloud environment. In this system, the owner's encrypted data is stored in a cloud storage with defined access policies in smart contracts. The consumer (user), anonymously asks for access permission using the smart contract, by depositing payment.

- **Authentication and Access Control:** Intrinsically distributed certificate management provided by Blockchain, along with a distributed identity management solution, can introduce Blockchain as a game-changer for authentication in O-RAN. In the O-RAN ecosystem as a disaggregated RAN, Blockchain-based solutions for identity management and authentication can help reduce overall operational costs while providing safe and user-centric services [4], [49]. Moreover, the definition of access policies and rules in Blockchain (more specifically in smart contracts) and policy enforcement using smart contracts can not only improve the immutability of rules and policies but also provide higher automation, traceability, non-repudiation, and decentralization in access control systems. Providing point-to-point communication in a cellular network without the involvement of a core network can raise many security concerns. Based on [49], a Blockchain-based RAN can address privacy concerns, as well as set up a distributed user-centric identity management system in the RAN, allowing devices from various MNOs connected to the same base station to communicate and exchange data. In [63], the authors propose a B2B cooperation solution in which sensitive information about device performance is first encrypted using a secure comparison protocol and then transmitted between parties utilizing Blockchain technology. These data are then used to fine-tune the services to prevent performance degradation.
- **Availability and fault tolerance:** Moreover, due to the nature of cellular networks, system availability is another important challenge to address. The possibility of outsourcing different O-RAN functionalities to a distributed system results in increasing the overall availability and fault tolerance of the system. For instance, instead of executing different functionalities with one or several limited numbers of servers in the network, if the functionalities are able to be executed in smart contracts on top of Blockchain, all or the majority of nodes will run the predefined functions. So, system availability is expected to be higher than in a centralized architecture.

V. Discussion and conclusion

In this research, we explored the applications of Blockchain technology in the telecommunications field, particularly in O-RAN. Our initial focus was on identifying the current challenges in O-RAN design, which encompassed areas such as orchestration, performance, security, deployment and operation, and business. Building upon these identified challenges, we investigated how Blockchain technology could offer solutions to address these issues. Our findings indicate that Blockchain has the capability to enhance access control to AI/ML data, ensuring its security and integrity while facilitating the sharing of data and models. Additionally, Blockchain offers notable advantages in secure identity management, provisioning of security measures, automated collaboration, and the introduction of innovative business models. Figure 3 provides a concise overview of the benefits of Blockchain in relation to the various existing challenges encountered in O-RAN design.

While Blockchain technology offers numerous potential benefits for O-RAN, it also faces certain challenges related to interoperability with existing business models, standardization, content privacy, consensus convergence delay, and scalability without compromising performance. However, efforts are being made to address these limitations, and ongoing research in this field is focused on finding solutions. As a result, several potential directions can be suggested.

From a *business perspective*, a comprehensive evaluation is needed to assess the interoperability of Blockchain technology with the O-RAN industry. This analysis will contribute to a better understanding of market requirements and facilitate the gradual integration of Blockchain into the existing market, avoiding sudden shifts and disruptive changes.

From a *technical standpoint*, there are several intriguing targets to address privacy and data leakage concerns. These include the development of lightweight and secure encryption solutions, establishing secure connections with off-chain distributed databases, and designing mechanisms to ensure the trustworthy handling of user data.

Furthermore, considering the impact of storage complexity and system latency on different implementation scenarios, proposing efficient methods for storage/latency optimization and security enhancements would be a valuable area for future study.

Lastly, a generic proposition for the DLT community is to build an O-RAN use-case-specific consensus model and DLT solution. This proposal could be a significant step toward meeting various system requirements such as low energy consumption, scalability, minimal delay, user privacy, and efficient resource utilization.

References

[1] O-RAN Alliance, "O-RAN towards an open and smart RAN," 2018.

[2] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, 2023.

[3] N. Aryal, E. Bertin, and N. Crespi, "Open radio access network challenges for next generation mobile network," in *2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2023, pp. 90–94.

[4] M. K. Luka, O. U. Okereke, E. E. Omizegba, and E. C. Anene, "Blockchains for spectrum management in wireless networks: A survey," *arXiv preprint arXiv:2107.01005*, 2021.

[5] L. Giupponi and F. Wilhelmi, "Blockchain-enabled network sharing for o-ran in 5g and beyond," *IEEE Network*, 2022.

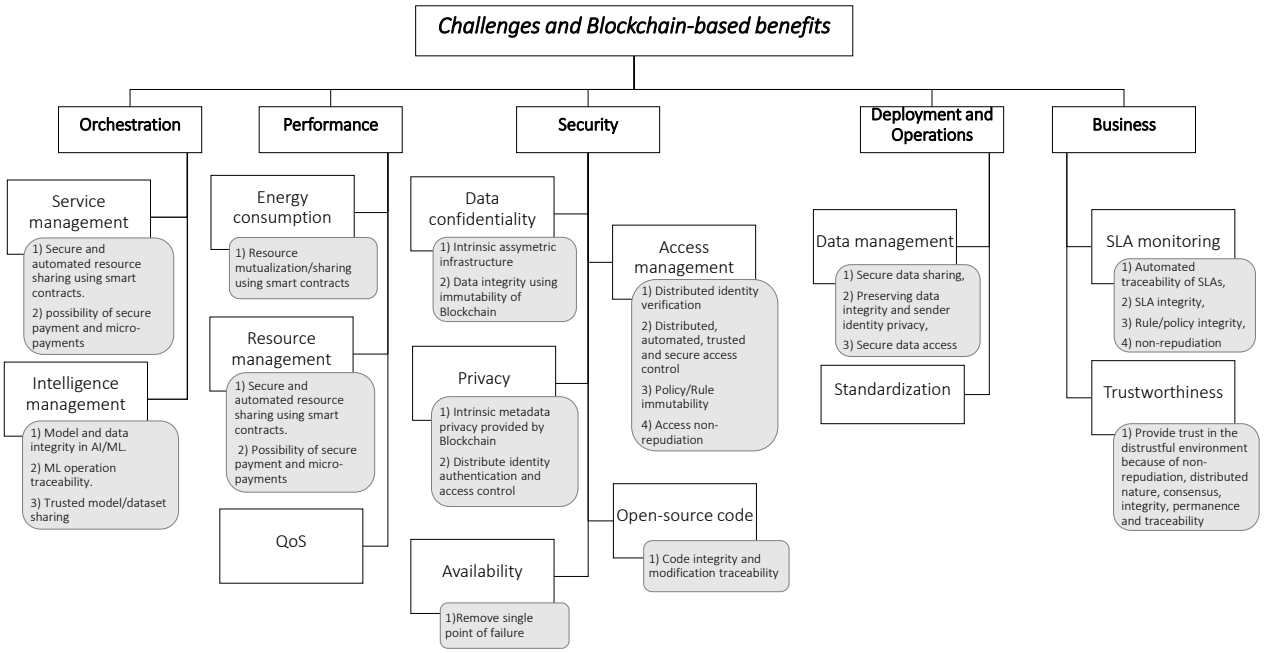

Fig. 3. O-RAN challenges and the possible benefits of Blockchain technology to address them. The gray boxes indicate Blockchain-based solutions for respective challenges. Note that, to the best of our knowledge, there is a lack of sufficient resources regarding the usage of Blockchain in QoS and Standardization areas.

[6] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open ran security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, 2023.

[7] S. K. Singh, R. Singh, and B. Kumbhani, "The evolution of radio access network towards open-ran: Challenges and opportunities," in *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2020, pp. 1–6.

[8] O-RAN Working Group 1, "O-RAN architecture description," May 2022.

[9] O-RAN Alliance, May 2022. [Online]. Available: https://www.o-ran.org/

[10] S. D'Oro, L. Bonati, M. Polese, and T. Melodia, "Orchestran: Network automation through orchestrated intelligence in the open ran," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 270–279.

[11] M. Dryjański, Ł. Kułacz, and A. Kliks, "Toward modular and flexible open ran implementations in 6g networks: Traffic steering use case and o-ran xapps," *Sensors*, vol. 21, no. 24, p. 8173, 2021.

[12] V. Ranjbar, A. Girycki, M. A. Rahman, S. Pollin, M. Moonen, and E. Vinogradov, "Cell-free mmimo support in the o-ran architecture: A phy layer perspective for 5g and beyond networks," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 28–34, 2022.

[13] T.-H. Wang, Y.-C. Chen, S.-J. Huang, K.-S. Hsu, and C.-H. Hu, "Design of a network management system for 5g open ran," in *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2021, pp. 138–141.

[14] H. Kumar, V. Sapru, and S. K. Jaisawal, "O-ran based proactive anr optimization," in *2020 IEEE Globecom Workshops (GC Wkshps*. IEEE, 2020, pp. 1–4.

[15] S. D'Oro, M. Polese, L. Bonati, H. Cheng, and T. Melodia, "dapps: Distributed applications for real-time inference and control in o-ran," *arXiv preprint arXiv:2203.02370*, 2022.

[16] H. Lee, J. Cha, D. Kwon, M. Jeong, and I. Park, "Hosting ai/ml workflows on o-ran ric platform," in *2020 IEEE Globecom Workshops (GC Wkshps*. IEEE, 2020, pp. 1–6.

[17] S. Mollahasani, M. Erol-Kantarci, and R. Wilson, "Dynamic cu-du selection for resource allocation in o-ran using actor-critic learning," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6.

[18] L. Bonati, S. D'Oro, M. Polese, S. Basagni, and T. Melodia, "Intelligence and learning in o-ran for data-driven nextg cellular networks," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 21–27, 2021.

[19] J. Wu, Y. Zhang, M. Zukerman, and E. K.-N. Yung, "Energy-efficient base-stations sleep-mode techniques in green cellular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 2, pp. 803–826, 2015.

[20] B. Brik, K. Boutiba, and A. Ksentini, "Deep learning for b5g open radio access network: Evolution, survey, case studies, and challenges," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 228–250, 2022.

[21] S. Mollahasani, T. Pamuklu, R. Wilson, and M. Erol-Kantarci, "Energy-aware dynamic du selection and nf relocation in o-ran using actor–critic learning," *Sensors*, vol. 22, no. 13, p. 5029, 2022.

[22] T. Pamuklu, S. Mollahasani, and M. Erol-Kantarci, "Energy-efficient and delay-guaranteed joint resource allocation and du selection in o-ran," in *2021 IEEE 4th 5G World Forum (5GWF)*. IEEE, 2021, pp. 99–104.

[23] A. Perveen, R. Abozariba, M. Patwary, and A. Aneiba, "Dynamic traffic forecasting and fuzzy-based optimized admission control in federated 5g-open ran networks," *Neural Computing and Applications*, pp. 1–19, 2021.

[24] G. Kougioumtzidis, V. Poulkov, Z. D. Zaharis, and P. I. Lazaridis, "Intelligent and qoe-aware open radio access networks," in *2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC)*. IEEE, 2022, pp. 1–4.

[25] J. Mongay Batalla, M. Moshin, C. X. Mavromoustakis, K. Wesołowski, G. Mastorakis, and K. Krzykowska-Piotrowska, "On deploying the internet of energy with 5g open ran technology including beamforming mechanism," *Energies*, vol. 15, no. 7, p. 2429, 2022.

[26] O-RAN Security Focus Group, "O-RAN Security threat modeling and remediation analysis," May 2022.

[27] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Evaluating the security of open radio access networks," *arXiv preprint arXiv:2201.06080*, 2022.

[28] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5g/6g tactical networks: Principles, challenges, and the role of machine learning," *arXiv preprint arXiv:2105.01478*, 2021.

[29] "Oran policy coalition," 2021. [Online]. Available: https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

[30] I. Tamim, A. Saci, M. Jammal, and A. Shami, "Downtime-aware o-ran vnf deployment strategy for optimized self-healing in the o-cloud," in

2021 IEEE Global Communications Conference (GLOBECOM). IEEE, 2021, pp. 1–6.

[31] Q. H. Duong, I. Tamim, B. Jaumard, and A. Shami, "A column generation algorithm for dedicated-protection o-ran vnf deployment," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2022, pp. 1206–1211.

[32] A. Huff, M. Hiltunen, and E. P. Duarte, "Rft: Scalable and fault-tolerant microservices for the o-ran control plane," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021, pp. 402–409.

[33] Y. Li, Y. Jiang, Z. Li, and S.-T. Xia, "Backdoor learning: A survey," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–18, 2022.

[34] Ł. Kułacz and A. Kliks, "Dynamic spectrum allocation using multi-source context information in openran networks," *Sensors*, vol. 22, no. 9, p. 3515, 2022.

[35] S. Niknam, A. Roy, H. S. Dhillon, S. Singh, R. Banerji, J. H. Reed, N. Saxena, and S. Yoon, "Intelligent o-ran for beyond 5g and 6g wireless networks," *arXiv preprint arXiv:2005.08374*, 2020.

[36] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What o-ran can and cannot do!" *IEEE Network*, vol. 36, no. 6, pp. 206–213, 2022.

[37] J. Thaliath, S. Niknam, S. Singh, R. Banerji, N. Saxena, H. S. Dhillon, J. H. Reed, A. K. Bashir, A. Bhat, and A. Roy, "Predictive closed-loop service automation in o-ran based network slicing," *arXiv preprint arXiv:2202.01966*, 2022.

[38] Z. Luo, S. Fu, M. Theis, S. Hasan, S. Ratnasamy, and S. Shenker, "Democratizing cellular access with cellbricks," in *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, 2021, pp. 626–640.

[39] A. R. Bedin, M. Capretz, and S. Mir, "Blockchain for collaborative businesses," *Mobile Networks and Applications*, vol. 26, pp. 277–284, 2021.

[40] Y. Chen, J. Gu, S. Chen, S. Huang, and X. S. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in *2019 IEEE International Conference on Web Services (ICWS)*. IEEE, 2019, pp. 219–223.

[41] R. Hull, "Blockchain: distributed event-based processing in a data-centric world," in *Proceedings of the 11th acm international conference on distributed and event-based systems*, 2017, pp. 2–4.

[42] O. López-Pintado, M. Dumas, L. García-Bañuelos, and I. Weber, "Controlled flexibility in blockchain-based collaborative business processes," *Information Systems*, vol. 104, p. 101622, 2022.

[43] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Business Horizons*, vol. 62, no. 3, pp. 295–306, 2019.

[44] 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.

[45] Y. Le, X. Ling, J. Wang, and Z. Ding, "Prototype design and test of blockchain radio access network," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[46] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Transactions on Communications*, 2020.

[47] Y. Le, X. Ling, J. Wang, R. Guo, Y. Huang, C.-X. Wang, and X. You, "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[48] X. Ling, Y. Le, J. Wang, and Z. Ding, "Hash access: Trustworthy grant-free iot access enabled by blockchain radio access networks," *IEEE Network*, vol. 34, no. 1, pp. 54–61, 2020.

[49] H. Xu, L. Zhang, Y. Sun *et al.*, "Be-ran: Blockchain-enabled open ran with decentralized identity management and privacy-preserving communication," *arXiv preprint arXiv:2101.10856*, 2021.

[50] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6g," *National science review*, vol. 8, no. 9, p. nwab069, 2021.

[51] A. Heider-Aviet, D. R. Ollik, S. Berlato, S. Ranise, R. Carbone, N. El Ioini, C. Pahl, H. R. Barzegar *et al.*, "Blockchain based ran data sharing," in *2021 IEEE International Conference on Smart Data Services (SMDS)*. IEEE, 2021, pp. 152–161.

[52] X. Liu, X. Chen, Q. Bi, W. Liang, J. Li, and Z. Zhang, "Blockchain-based distributed operation and incentive solution for p-ran," *Computer Communications*, vol. 198, pp. 77–84, 2023.

[53] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[54] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Computing*, vol. 26, no. 1, pp. 197–221, 2023.

[55] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain-based consents management for personal data processing in the iot ecosystem." *ICETE (2)*, vol. 298, pp. 572–577, 2018.

[56] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," *arXiv preprint arXiv:1802.01746*, 2018.

[57] "Ocean Protocol: Tools for the Web3 Data Economy," 2019. [Online]. Available: https://oceanprotocol.com/tech-whitepaper.pdf

[58] A. O. Philip and R. K. Saravanaguru, "Secure incident & evidence management framework (siemf) for internet of vehicles using deep learning and blockchain," *Open Computer Science*, vol. 10, no. 1, pp. 408–421, 2020.

[59] U. Der, S. Jähnichen, and J. Sürmeli, "Self-sovereign identity – opportunities and challenges for the digital revolution," *arXiv preprint arXiv:1712.01767*, 2017.

[60] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: The necessity of blockchain technology," *arXiv preprint arXiv:1904.12816*, 2019.

[61] M. Dieye, P. Valiorgue, J.-P. Gelas, E.-H. Diallo, P. Ghodous, F. Biennier, and É. Peyrol, "A self-sovereign identity based on zero-knowledge proof and blockchain," *IEEE Access*, 2023.

[62] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Privacyguard: Enforcing private data usage control with blockchain and attested off-chain contract execution," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 610–629.

[63] H. Nasu, Y. Kodera, and Y. Nogami, "A business-to-business collaboration system that promotes data utilization while encrypting information on the blockchain," *Sensors*, vol. 22, no. 13, p. 4909, 2022.