

Decentralized Identity Management for Secure Resource Sharing in O-RAN

Engin Zeydan*, Luis Blanco*, Josep Mangués*, Suayb Arslan†, Yekta Turk◊

*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, 08860.

† Massachusetts Institute of Technology, MA, USA, 02139.

◊Mobile Network Architect, Istanbul, Turkey, 34396.

Email: {engin.zeydan, luis.blanco, josep.mangués}@cttc.cat, sarslan@mit.edu, yektaturk@gmail.com

Abstract—Self-Sovereign Identity (SSI) has recently emerged as an identity and access management framework based on Distributed Ledger Technology (DLT) that enables users or organizations to control their own data. The Open RAN (O-RAN), on the other hand, provides a framework for sharing infrastructure-related data between users and mobile network operators (MNOs). By leveraging SSI, O-RAN can benefit from decentralized and secure identity management that enables a more transparent, efficient, and user-centric network ecosystem. This paper examines identity, inventory and configuration management, and authentication of users or MNOs for a resource sharing scenario in an O-RAN architecture. At the end of the paper, we explain the potential limitations and possible solutions for applying SSI to improve security, privacy, trust, and interoperability in O-RANs.

Keywords—self-sovereign identity, blockchain, resource sharing, O-RAN.

I. INTRODUCTION

In recent years, rapid advances in telecommunications technology have paved the way for open radio access networks (Open Radio Access Networks (O-RANs)). O-RANs bring a paradigm shift by disaggregating traditional monolithic radio access network components, enabling greater flexibility, interoperability and innovation in wireless communications deployment [1]. With the increasing importance of O-RANs, ensuring secure and trustworthy identity management (of various entities within the O-RAN ecosystem) also becomes a critical issue. O-RAN introduces a more open and disaggregated architecture that increases the attack surface and potential vulnerabilities. O-RAN also aims to promote interoperability between different network components and vendors. Appropriate identity management therefore ensures that the various components can communicate with each other securely and seamlessly. Decentralized Identifiers (DIDs) are unique identifiers tied to cryptographic keys, and verifiable credentials are digitally signed claims issued by trusted entities [2]. Users, Mobile Network Operators (MNOs) and device manufacturers can create their DIDs for themselves and their devices participating in the O-RAN ecosystem and obtain verifiable credentials from trusted authorities. This enables secure authentication, supports interoperability and facilitates trust between participants, and provides the foundation for building

Self-Sovereign Identity (SSI) systems in O-RAN that empower users, MNOs and device owners and improve network security and privacy. Each DID is associated with a DID document that contains relevant information about the entity, such as public keys, authentication mechanisms, service endpoints, and other metadata. The DID document is stored and distributed in a decentralized manner so that it is accessible for verification and validation by other participants in the O-RAN ecosystem. DIDs are usually represented as URIs (Uniform Resource Identifiers) and follow the DID specification defined by the World Wide Web Consortium (W3C). DIDs consists of two main components: the DID method and the DID specific identifier. The DID method specifies the rules and mechanisms for the creation and resolution of DIDs. It defines how DIDs are created, managed, and associated with cryptographic keys and other relevant data. The DID-specific identifier is a unique string or series of characters that identifies a specific entity within the selected DID method.

Enlightened by the power of blockchain technology, the authors in [3] develop decentralized, secure, and efficient mechanisms for managing network access and authentication between inherently untrusted network entities. The paper in [4] proposes a blockchain-based identity management and authentication system for mobile networks, where users' identifying information is controlled by the users themselves. [5] present an approach that allows a user to prove their right to access a particular service without revealing information about the user themselves. The authors in [6] propose a secure endogenous wireless access network architecture based on blockchain that includes a communication plane and a blockchain plane, the latter including blockchain networks and their applications. The application of Blockchain Network (BCN)-based SSI was performed in our previous work [7] and proposed in the context of vehicular networks. The paper in [8] proposes a blockchain-based identity and access management system for Internet of Things (IoT) – in particular for smart vehicles – as an example application and shows two interoperable blockchains, Ethereum and Hyperledger Indy, and a self-sovereign identity model. In the context of applying BCN in O-RAN, the authors in [9] propose the integration of blockchain technology to enable mobile operators and other actors to autonomously and dynamically exchange radio access network (RAN) resources (e.g., infrastructure) in the form of Virtual Network Functions (VNFs). A blockchain-enabled RAN and decentralized privacy-preserving Peer-to-Peer (P2P) communication system with secure identity management through mutual

This work was partially funded by “ERDF A way of making Europe” project PID2021-126431OB-I00 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55) Grant PID2021-126431OB-I00 funded by MCIN/AEI/ 10.13039/501100011033.

authentication is investigated in [10].

All of the above approaches offer different options for identity management, either as a stand-alone solution or in combination with other techniques. Further work of O-RAN with BCN in literature is based on BCN's capabilities as a ledger technology [11]. However, it lacks a SSI-embedded platform for reliable resource sharing (e.g. spectrum, network capacity, infrastructure components, etc.) between users and operators in the O-RAN architecture that can simultaneously provide confidentiality, integrity, and authentication. Sharing resources can enable more efficient utilization of the network infrastructure, cost savings for operators and fair competition. Note that O-RAN is a complex and evolving ecosystem for open and intelligent radio access networks, and integrating new technologies like BCN-based SSI would need to align with O-RAN's objectives. Therefore, in this paper, we propose an BCN-based SSI embedded O-RAN architecture and a design approach for the resource sharing process which according to authors knowledge is the first work introducing BCN-Based SSI in O-RAN. The rest of the paper is organized as follows: In Section II we present possible applications of Distributed Identity Management (DIM) in the Open RAN architecture. In Section III we present the general architecture and the entities involved in O-RAN and BCN. Section IV presents the steps of the authentication process. In Section V, we present an use case example of spectrum sharing. Section VI highlights some of the limitations of the proposed approach and possible solutions. Finally, Section VII presents the conclusions of the paper.

II. DIM IN OPEN RAN

DIDs are typically associated with cryptographic keys to ensure secure authentication and data integrity [12]. Participants in the O-RAN ecosystem, such as users and operators as well device owners, generate public-private key pairs. The public key is included in the DID document associated with the DID (that can be stored in BCN), while the private key is securely stored by the corresponding entity. This key pair enables cryptographic operations, such as signing and verification, to establish trust and secure interactions within the O-RAN network. The application of DIM is an open issue in O-RAN and a solution based on Distributed Ledger Technologies (DLTs) can be very powerful. A BCN-based SSI in an O-RAN architecture for equipment management or resource sharing can help overcome some of limitations. First of all, in the context of O-RAN, a specific DID method needs to be defined to support the unique requirements of the ecosystem. The DID method for O-RAN should consider aspects such as scalability, interoperability, and integration with existing identity systems. The method defines the operations and protocols for creating, updating, and resolving DIDs within the O-RAN environment.

Implementing a BCN-based SSI solution can provide robustness and security to the identity management process in O-RAN. BCNs, such as a permissioned or consortium network, can be utilized to store and validate the DID documents associated with each entity. The immutability and transparency of the BCN can enhance trust and integrity within the identity management process. Innovative approaches like sharding, sidechains, or layer 2 solutions can be employed to solve scalability issues. These techniques can help distribute the

computational and storage requirements, ensuring efficient and scalable identity management in O-RAN. To enable seamless interactions and interoperability between different O-RAN and identity systems, the standardization of DIM protocols and specifications is crucial. Collaborative efforts, industry alliances, and adherence to recognized standards, such as those proposed by W3C, can foster interoperability and facilitate the integration of diverse O-RAN. Participants in the O-RAN ecosystem, including users, operators, and device owners, should also generate and manage their cryptographic keys securely. The public keys can be included in the DID documents, while the private keys are kept confidential to ensure secure interactions and establish trust.

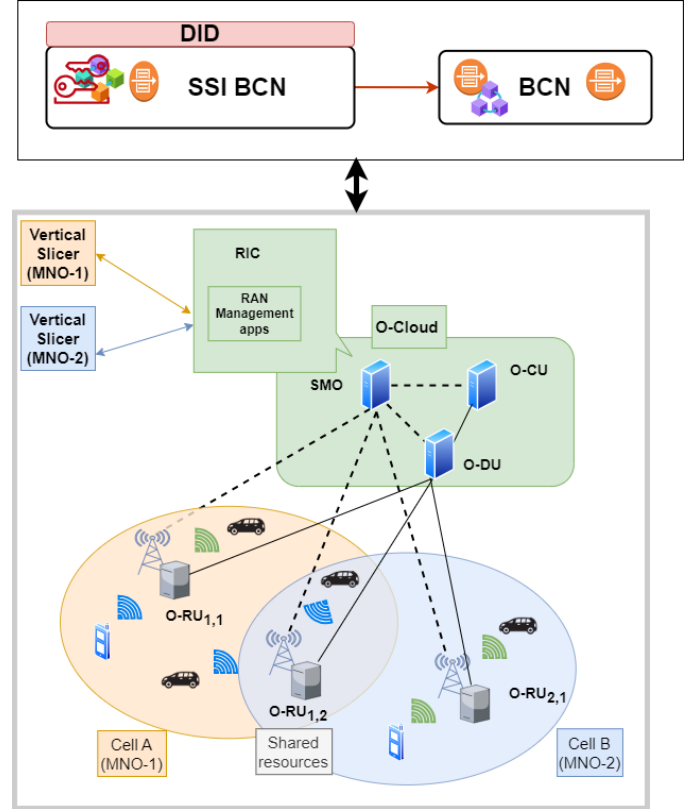


Fig. 1: BCN-based SSI and BCN enabled RAN sharing.

III. THE ROLE OF BCN IN O-RAN

A. General architecture

A promising approach to ensure identity management and trust for network management operations during resource sharing (e.g., Radio Units (RUs), Distributed Units (DUs), or Central Units (CUs) in O-RAN) and data exchange between entities (e.g., users, MNOs, or regulators) in an O-RAN architecture is the use of DLTs such as BCN and SSI. Fig. 1 shows BCN-based SSI and BCN enabled system for RAN sharing scenario for multiple operator scenario. In this architecture, RAN resources (in O-RU) are shared by two operators (namely MNO-1 and MNO-2), and requests to Radio Intelligence Controller (RIC) are executed by vertical slicers of each operator. Inside O-Cloud, there exists O-RAN control, management and orchestration entities, namely vertical slicers (that request network slice service management tasks done by verticals), Service Management and Orchestration (SMO) (that includes RIC), O-DU and O-CU.

For resource sharing among multiple MNOs (or users) in O-RANs while relying on SSI, BCNs can play a critical role in providing the underlying infrastructure for secure and decentralized operations (e.g. see its usage in [13], [14] for cellular networks). The BCN serves as a decentralized ledger where SSIs of users and MNOs (as well as logs related to the resource sharing process in a separate BCN) are stored. Each user/MNO is assigned a unique identity by an issuer in the form of a cryptographic key pair so that they can control and manage their identity information. In such a configuration, the BCN-based SSI ensures the integrity and immutability of the identity data and prevents tampering or unauthorized changes. The BCN provides enhanced security and privacy for the SSIs and sensitive information exchanged between MNOs. The use of cryptographic techniques ensures the confidentiality and integrity of data, preventing unauthorized access or tampering. The decentralized nature of the BCN also reduces the risk of a single point of failure or control, making it resilient to attack or breach.

Resource sharing logs in BCN: As MNOs negotiate and interact with each other during resource sharing process (e.g. for spectrum sharing), the BCN also records all transactions and agreements in a transparent and immutable manner (e.g. in a separate chain in this paper as given in Fig. 2). Each interaction between users and MNOs can be recorded on the blockchain or a distributed ledger. These records can include details such as the type of resource accessed, the duration of usage, and the identities of the involved parties. This provides an auditable history of resource sharing activities, ensuring trust and accountability among the participating operators. By having an immutable and transparent audit trail, it becomes easier to detect any anomalies or suspicious behavior during the resource sharing process. The immutable records also help resolve disputes or conflicts, if any. The BCN employs a consensus mechanism, such as proof-of-work or proof-of-stake, to validate and agree upon the state of the shared ledger. Consensus ensures that all network participants reach a consensus on the order and validity of transactions, preventing fraudulent or malicious activities. This consensus mechanism enhances the overall security and trustworthiness of the resource sharing process. In the context of resource sharing, smart contracts, which are self-executing and programmable agreements, can define the rules and conditions of resource sharing agreements between MNOs. These contracts can automatically enforce access control policies, manage allocation and utilization of resources, and facilitate settlement between MNOs. Smart contracts enable automation, transparency, and enforceability of the agreed-upon terms.

Integration aspects: The integration of O-RAN with BCN can be achieved by a module or layer that interacts with the BCN to store and retrieve O-RAN infrastructure data in a secure and transparent manner. A secure data exchange between O-RAN entities and BCN can be achieved with a secure communication protocol which ensures only the desired data can be stored in the BCN, excluding all private data. Smart contract-based trust verification provides proof of trust through the BCN by verifying the authenticity and integrity of the data exchanged between entities. On the other hand, permissioned BCN can also be utilized to ensure privacy by selecting only authorized entities to access the BCN. Access control mechanisms and encryption techniques can be implemented to

protect the data in the BCN to achieve this. In a permissioned system, only authorized entities are allowed to participate in the consensus process and update the ledger. This can help reduce the computational overhead and ensure that only trusted entities are involved inside O-RAN architecture. Note that the specific roles and types of nodes within the BCN (full, light, mining, validator and end-user nodes) would depend on the blockchain technology used and the design choices. The BCN itself can be hosted on appropriate infrastructure, such as cloud services or on-premises servers, depending on the project's requirements and resources.

B. MNOs in O-RAN

BCN-based SSI can also be applied to facilitate network resource sharing between multiple MNO in O-RAN. By leveraging SSI in resource sharing, multiple MNOs in O-RAN can establish a secure and transparent ecosystem for collaboration. SSI ensures that MNOs retain control over their resources while enabling efficient and trusted sharing among authorized entities. This promotes resource optimization, cost reduction, and increased flexibility in managing and utilizing shared resources in O-RANs. BCN-based SSI can help to support resource sharing among multiple MNOs in multiple ways: *Identity-Based Resource Allocation:* SSI enables MNOs to establish unique and verifiable identities for their resources, such as network infrastructure, spectrum, or computing resources. By assigning SSIs to these resources, MNOs can securely track and manage their availability, capabilities, and usage. *Secure Negotiation and Agreements:* SSI provides a secure framework for MNOs to negotiate and establish resource-sharing agreements. Each operator can present their self-sovereign identity along with their resource capabilities and requirements, facilitating transparent and trusted negotiations. Smart contracts can be used to enforce the terms and conditions of resource sharing. *Access Control and Authorization:* SSI allows MNOs to control access to their shared resources based on verifiable identities. MNOs can define access policies and permissions tied to SSIs, ensuring that only authorized entities can utilize the shared resources. This helps maintain security and prevent unauthorized usage. *Auditing and Accountability:* SSI enables transparent auditing and accountability in resource sharing. Each MNO can maintain a tamper-proof record of resource usage and transactions associated with their self-sovereign identity. This promotes trust among MNOs and allows for efficient tracking and settlement of resource usage. *Interoperability and Interconnection:* SSI supports interoperability and interconnection between MNOs by providing a decentralized and standardized identity framework. Operators can securely recognize and authenticate each other's identities, enabling seamless sharing of resources across different networks and deployments.

IV. AUTHENTICATION PROCESS

Fig. 2 provides an overview of the key entities involved in BCN-based SSI. These entities include the SSI BCN, the issuer, the holder, and the verifier. The issuer, such as a regulatory authority responsible for O-RAN services in each country, possesses the authority to create and issue digital credentials, also known as verifiable credentials, to individuals or entities. These credentials contain relevant claims or attributes about the

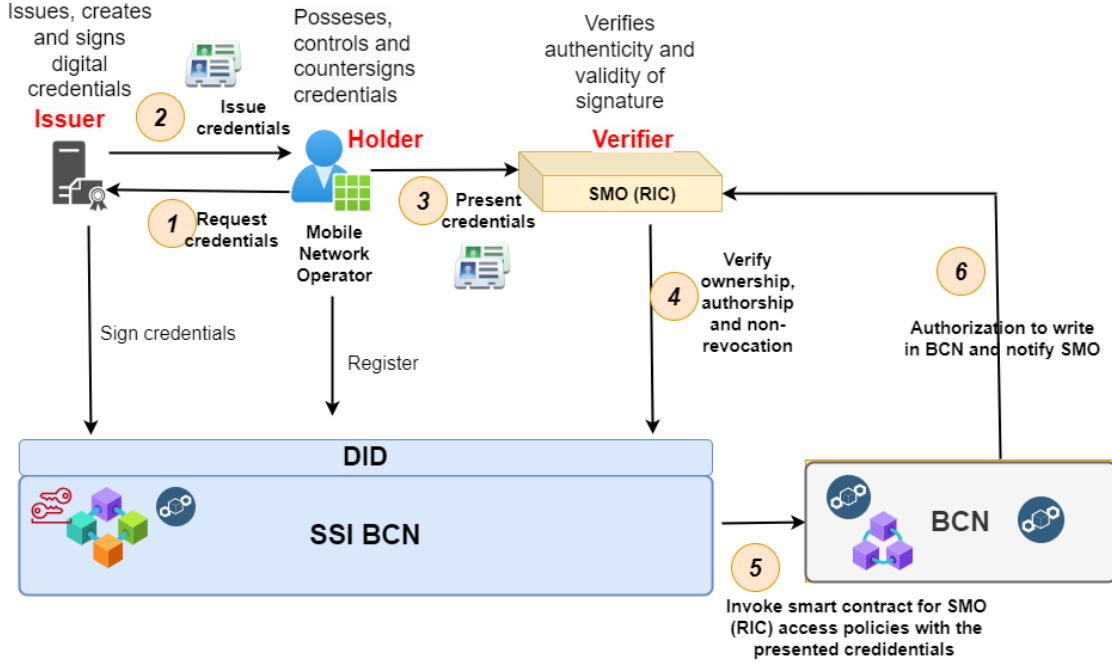


Fig. 2: Authentication with BCN-based SSI enabled O-RAN design.

holder and are digitally signed by the issuer using their private key to ensure their authenticity and integrity. The holder, such as a MNOs, receives and possesses the digital credentials issued by the issuer. The holder has complete control over their own credentials and can decide when and how to present them to verifiers. The credentials are securely stored in the holder's digital wallet or enterprise data store, protected by cryptography and the holder's private key. The holder has the ability to selectively share specific credentials or attributes with verifiers based on their specific needs or requirements by using cryptography and zero-knowledge proofs, if necessary, enabling them to maintain control over their own data.

In the context of our case, the verifier (specifically the RIC in SMO) plays the role of an entity responsible for verifying specific claims or attributes about another entity. When the verifier needs to verify the authenticity or validity of a claim made by the holder, they can request the presentation of relevant credentials or attributes for verification purposes. To establish trust in the credentials, the verifier relies on the cryptographic signatures and integrity of the credentials. By validating the digital signatures and ensuring the integrity of the credentials using the issuer's public key, the verifier can ascertain that the credentials were issued by a trusted issuer and have not been tampered with. In the context of our system, the RIC in SMO plays a crucial role in the authorization process. In **step 1**, when a holder (such as an MNOs) wishes to access the RAN service, they establish an authenticated channel with the issuer through BCN-based SSI. In **step 2**, the issuer issues a verifiable credential to the holder, including specific terms for the smart contract and the RIC in SMO to refine access policies. These terms may specify authorized time slots, specific parts of RIC in SMO, and more. In **step 3**, the holder presents the credentials to the RIC in SMO (verifier), which is then forwarded to BCN-based SSI. In **step 4**, the RIC in SMO verifies the ownership, authorship, and non-revocation of the credential. Additionally, the verifier checks the credential against a list of access policies set by

the issuer. Notably, the smart contract on BCN-based SSI has exclusive invocation properties restricted to the issuer and the RIC in SMO controlled by that smart contract. If authentication fails, the RIC in SMO denies RAN service requests from unauthenticated MNOs or refuses to collaborate with them. In **step 5**, the BCN-based SSI invokes the smart contract on the online BCN to check the RIC in SMO access policies using the presented credentials. The smart contract informs the RIC in SMO about the authorization to write in the BCN. Upon successful authentication, the RIC in SMO initiates RAN services in collaboration with authenticated MNOs, and relevant logs are recorded in the BCN.

V. AN EXAMPLE USE CASE: SPECTRUM SHARING

In an O-RAN architecture, multiple MNOs can collaborate to efficiently share spectrum resources. In such situations, BCN-based SSI can play a critical role in enabling secure and trusted spectrum sharing by MNOs. By leveraging BCN-based SSI, MNOs can effectively share spectrum resources, optimize network capacity, and provide better services to their customers in O-RANs. Suppose there are three MNOs, MNO A, MNO B, and MNO C, who want to share their unused spectrum resources to improve network capacity and coverage in a specific geographical area. To accomplish this, several steps need to be followed: *First step* is to establish BCN-based SSI for each MNOs. Here, each MNO creates their SSI using BCN, which includes verifiable credentials and attributes related to their network infrastructure and available spectrum resources. These identities are stored on a decentralized and immutable ledger, ensuring data integrity and privacy. *Second step* is to negotiate spectrum sharing agreements. Here, MNOs engage in negotiation using their SSIs. They present their available spectrum resources, quality-of-service (QoS) requirements, and desired terms for sharing. During this process, BCN-based SSI allows for transparent and trusted negotiations, ensuring that all parties can verify the identities and claims of each MNO. *Third step* is to verify and grant access. Here,

TABLE I
COMPARISON BETWEEN SSI AND REGULAR BLOCKCHAIN-BASED AUTHENTICATION IN O-RAN ADOPTION

Category	SSI	BCN-based Authentication	BCN-based SSI
Characteristics	<ul style="list-style-type: none"> — Users have full control over their digital identity and personal data. — They can selectively share information as needed. — SSI is inherently decentralized, with no single authority controlling identities or personal data. 	<ul style="list-style-type: none"> — Authentication relies on public-private key pairs stored on the blockchain, but users may not have direct control over their identity and personal data. 	<ul style="list-style-type: none"> — Authentication and identity management rely on BCN, which provides a decentralized and tamper-resistant infrastructure for storing and managing identities and credentials.
Advantages	<ul style="list-style-type: none"> — In O-RAN, network participants empowerment, privacy control, enhanced security, and interoperability across platforms and services. — SSI provides strong privacy as users have control over their personal data and can choose when and with whom to share it important especially in O-RAN scenarios where sensitive data is involved. — SSI promotes interoperability by allowing users to manage and share their identity across different platforms and services. This can facilitate smooth integration of various O-RAN components and devices. — SSI offers enhanced security by leveraging cryptographic algorithms, zero-knowledge proofs, and user-controlled data sharing. 	<ul style="list-style-type: none"> — Enhanced security, transparency, immutability, and potential for decentralized governance. Only authorized devices or entities can access the O-RAN network, reducing the risk of unauthorized access or attacks. — In O-RAN, transparency can help network operators and regulators monitor network activities and ensure compliance with regulations — Regular BCN-based authentication provides strong security through the use of cryptographic mechanisms and the immutability of transactions recorded on the BCN. — Immutability ensures the integrity and auditability of authentication processes within O-RAN. — Depending on the BCN's governance model, O-RAN networks may benefit from decentralized decision-making, reducing reliance on centralized authorities. 	<ul style="list-style-type: none"> — All the advantages of SSI apply, as BCN-based SSI is a specific implementation of SSI using BCN. — BCN adds the benefits of transparency, immutability, and auditability to the SSI framework, all of which are valuable in O-RAN adoption. — The use of distributed consensus mechanisms ensures trust and integrity of the identity data stored on the BCN. This trust is essential in O-RAN networks, where secure communications and data exchange are paramount. O-RAN networks emphasize open interfaces and interoperability. — BCN-based SSI aligns with these principles by providing a secure and interoperable identity management solution. — Users in O-RAN can benefit from the privacy protection and control when and with whom they share their identity information, addressing privacy concerns in network interactions.
Limitations	<ul style="list-style-type: none"> — Potential scalability issues, complex implementation, and the need for widespread adoption for maximum effectiveness. — SSI may face challenges in scalability due to the need for decentralized identity verification and selective data sharing. — As O-RAN networks grow in complexity and size, managing decentralized identities for all network participants can become challenging. — Implementing SSI in O-RAN can be complex, requiring the development of secure identity management systems and integration with existing network infrastructure. — This complexity may increase deployment costs and resource requirements. — SSI's effectiveness relies on widespread adoption across the O-RAN ecosystem. — Achieving this level of adoption can be challenging, as it requires the buy-in of multiple stakeholders and network participants. 	<ul style="list-style-type: none"> — Exposure of certain transaction details on the public ledger, potential privacy concerns, and dependency on BCN and network consensus. — In O-RAN, this exposure could potentially reveal sensitive information about network interactions, which may not be desirable in some scenarios. — Regular BCN-based authentication may expose certain transaction details on the public ledger, potentially impacting privacy in O-RAN. — Additional measures are required to protect sensitive information. — Regular blockchain-based authentication may also face scalability challenges in O-RAN adoption, especially in public BCNs with high transaction volumes. 	<ul style="list-style-type: none"> — BCN-based SSI inherits the limitations of blockchain technology, such as scalability constraints and energy consumption. — In O-RAN, this can lead to challenges in managing a growing number of decentralized identities and credentials. O-RAN networks aiming to be energy-efficient may need to consider the environmental impact of BCN-based solutions. — Complex consensus mechanisms and governance models may require coordination and agreement among participants. Achieving consensus on identity-related matters in O-RAN can be time-consuming and challenging. — Adoption of BCN-based SSI may depend on the availability and performance of the underlying blockchain infrastructure. — Variability in BCN platforms and their capabilities can impact O-RAN deployment.

once the spectrum sharing agreements are reached, MNOs can authenticate and authorize each other based on their SSIs. This ensures that only authorized MNOs gain access to shared spectrum resources. Access control policies and permissions tied to SSIs enable seamless and secure resource utilization. *The fourth step* is for monitoring and auditing using BCN. Here, MNOs continuously monitor and track the usage of shared spectrum resources. They maintain tamper-proof records of resource allocation, utilization, and transactions associated with their SSIs. This provides transparency, accountability, and facilitates accurate settlement of resource usage among

MNOs. *The fifth step* is dynamic resource allocation. With BCN-based SSI, MNOs can dynamically allocate and release spectrum resources based on demand and availability. As needs of MNOs change, they can securely update their SSIs with revised resource offerings to ensure efficient use of shared spectrum.

Some of the advantages of using BCN-based SSI in an O-RAN architecture in the spectrum sharing use case are as follows: *Improved Spectrum Utilization:* BCN-based SSI enables efficient use of spectrum resources by facilitating transparent and trusted sharing between MNOs. *Secure and*

Trusted Collaboration: The BCN-based SSI creates a secure and trusted environment for MNOs to negotiate, authenticate, and authorize resource sharing to foster collaboration and cooperation. *Reduced Administrative Overhead:* BCN-based SSI automates identity verification and access control, reducing administrative burdens associated with resource sharing agreements. *Enhanced Accountability:* The transparent and auditable nature of BCN-based SSI ensures accountability among MNOs, promoting fair resource allocation and settlement.

VI. LIMITATIONS AND POSSIBLE SOLUTIONS

While BCN-based SSI technology offers numerous benefits for resource sharing in O-RAN, there are also some limitations that should be considered. Here are a few limitations and possible solutions: **(i) Malicious Users/Operators:** The above process assumes that the SSI registration mechanism would deter malicious users/MNOs from participating in the resource sharing process. However, it is still possible for malicious entities to join the system and disrupt the resource sharing. A reputation system can be introduced to assign reputation scores based on behavior, accuracy of models, contribution, and adherence to the protocol. Users/MNOs with low reputation scores can be excluded or given limited access, mitigating the risk of malicious behavior. **(ii) Privacy and Security:** The usage of BCN makes it challenging to double-check calculations and detect malicious clients. Solutions like resource sharing with differential privacy [15], adversarial robustness, secure multi-party computation, homomorphic encryption, and secure enclaves can enhance privacy, integrity, and confidentiality of the resource sharing process. These techniques protect against attacks, ensure secure aggregation, and prevent manipulation of the resource sharing process. **(iii) Scalability:** The use of BCN in resource sharing can introduce scalability issues due to the consensus requirement before each iteration. Consensus algorithms designed for scalability, such as Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT), can be employed to optimize the consensus process, reduce computational overhead, and minimize message exchange. These approaches improve scalability and mitigate potential bottlenecks. **(iv) Storage and Performance:** Storing large-scale resource sharing data directly on the BCN ledger can impact scalability and performance. Storing only one file validator (CRC) on the BCN while transferring log information directly between clients/MNOs and the BCN can reduce storage requirements and improve scalability. Evaluating the trade-offs between security, scalability, performance, and storage is crucial to determine the most suitable approach for the specific BCN and use case.

Finally, Table I provides a comparative analysis between SSI-based and regular BCN-based authentication methods for O-RAN adoption.

VII. CONCLUSION

The BCN serves as a base layer that enables secure, decentralized, and transparent resource sharing among MNOs in an O-RAN architecture. It builds trust, facilitates secure transactions, and ensures the integrity of identity and transaction data, thereby increasing overall efficiency and effectiveness. DIM and resource sharing in O-RAN can provide multiple ways to maintain control over the use of shared and

non-shared resource data with third parties. In this paper, we provided authentication, integrity and confidentiality to resource sharing process between multiple MNOs relying on both BCN and BCN-based SSI solutions. By implementing an BCN-based SSI solution in O-RAN with multiple MNOs and users, the system benefits from enhanced identity management, secure authentication, access control, auditing, and data privacy. Finally, we have given limitations, possible solutions, and comparisons of the proposed approach with other potential authentication solutions.

REFERENCES

- [1] 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.
- [2] C. Brunner, U. Gellersdörfer, F. Knirsch, D. Engel, and F. Matthes, "Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust," in *Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications*, pp. 61–66, 2020.
- [3] 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.
- [4] J. Xu, K. Xue, H. Tian, J. Hong, D. S. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6688–6698, 2020.
- [5] X. Salleras and V. Daza, "Sans: Self-sovereign authentication for network slices," *Security and Communication Networks*, vol. 2020, pp. 1–8, 2020.
- [6] M. Chen, C. Tan, X. Zhu, and X. Zhang, "A blockchain-based authentication and service provision scheme for internet of things," in *2020 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, 2020.
- [7] E. Zeydan, J. Mangués, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity solution for vehicular networks," in *2023 19th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 1–7, IEEE, 2023.
- [8] M. Naghmouchi, H. K. B. Ayed, and M. Laurent, "An automatized identity and access management system for iot combining self-sovereign identity and smart contracts," in *Foundations and Practice of Security: 14th International Symposium, FPS 2021, Paris, France, December 7–10, 2021, Revised Selected Papers*, pp. 208–217, Springer, 2022.
- [9] L. Giupponi and F. Wilhelm, "Blockchain-enabled network sharing for o-ran in 5g and beyond," *IEEE Network*, vol. 36, no. 4, pp. 218–225, 2022.
- [10] 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.
- [11] N. Aryal, F. Ghaffari, E. Bertin, and N. Crespi, "Moving towards open radio access networks with blockchain technologies," in *5th Conference on Blockchain Research & Applications for Innovative Networks and Services-BRAINS 2023*, 2023.
- [12] S. R. Garzon, H. Yildiz, and A. Küpper, "Decentralized identifiers and self-sovereign identity in 6g," *IEEE Network*, vol. 36, no. 4, pp. 142–148, 2022.
- [13] M. Moussaoui, N. Aryal, E. Bertin, and N. Crespi, "Distributed ledger technologies for cellular networks and beyond 5g: a survey," in *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 37–44, IEEE, 2022.
- [14] S. B. M. Baskaran, T. Faisal, C. Wang, D. R. Lopez, J. Ordóñez-Lucena, and I. Arribas, "The role of dlt for beyond 5g systems and services: A vision," *IEEE Communications Standards Magazine*, vol. 7, no. 1, pp. 32–38, 2023.
- [15] U. Karaca, S. I. Birbil, S. Yildirim, N. Aydin, and G. Mullaoglu, "Differential privacy in multi-party resource sharing," *arXiv preprint arXiv:2110.10498*, 2021.