

Exploring Blockchain Architectures for Network Sharing: Advantages, Limitations, and Suitability

Engin Zeydan, *Senior Member, IEEE*, Suayb S. Arslan, *Senior Member, IEEE*, and Yekta Turk

Abstract—The increasing demand for mobile data services has led to a need for efficient and cost-effective network sharing solutions. Blockchain technology has emerged as a promising solution for addressing the challenges associated with network sharing, such as interoperability, trust, and accountability. This paper presents a comprehensive classification and categorization of blockchain-based network sharing scenarios, highlighting their advantages and limitations. We have identified seven network sharing scenarios, ranging from centralized network sharing to fully decentralized spectrum sharing. For each scenario, the suitability of some of the selected blockchain architectures, from public, private, sidechain, and hybrid, is evaluated through extensive evaluations. We also identify gaps and opportunities of blockchain-based network sharing solution and present future research directions at the end of paper. Our analysis and results reveal that a single blockchain architecture is not suitable for all network sharing scenarios but careful analysis should be performed when selecting the suitable blockchain network in network sharing.

Index Terms—blockchain, network sharing, mobile operators.

I. INTRODUCTION

The concept of network sharing has gained significant attention in recent years in telecommunication industry, as it provides a cost-effective solution for network operators to deploy and maintain their networks [1], [2]. By sharing infrastructure, operators can reduce their capital expenditures and operational expenses, leading to a more sustainable and profitable business model. In addition to cost savings, network sharing also enables network operators to improve network coverage and capacity, particularly in areas where it is difficult to justify the deployment of a dedicated network. However, implementing network sharing can be challenging due to regulatory, technical, and operational constraints [3]. For network sharing, blockchain and Distributed Ledger Technologies (DLTs) can be used as a potential solution to address some of these challenges in network sharing scenarios [4]. By leveraging DLTs' decentralization, non-repudiation, provenance and transparency features, operators can share infrastructure resources at different layers and enforce agreements in a secure and transparent manner.

E. Zeydan is with Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, 08860 Spain e-mail: engin.zeydan@cttc.cat. S. S. Arslan is with Department of Brain and Cognitive Sciences, Massachusetts Institute of Technology, Cambridge, MA, USA, 02139. E-mail: sarslan@mit.edu. Y. Turk is an Independent Researcher based in Istanbul, Turkey, 34396. e-mail: Yektaturk@gmail.com.

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

Some challenges and considerations, as well as the importance of BCNs in specific network sharing scenarios, include: (i) **scalability and throughput**, where traditional blockchains have scalability issues due to their limited transaction throughput. Scalable blockchains can meet high throughput requirements and are therefore suitable for scenarios with numerous transactions, such as spectrum sharing; (ii) **privacy and confidentiality**, where public blockchains inherently do not provide complete privacy. However, private or consortium blockchains provide controlled access for authorized participants, making them suitable for scenarios involving user identity management and secure data exchange between known entities; (iii) **cost efficiency** if the implementation of Blockchain Networks (BCNs) is associated with infrastructure, development and maintenance costs. In scenarios where intermediary costs exceed the cost of establishing BCNs, such as cross-border roaming arrangements, BCNs can increase transparency and cost efficiency; (iv) **interoperability** where BCNs can provide protocol translation and facilitate interoperability between different networks. (v) **consensus mechanism**, where certain BCNs, such as private BCNs, may require faster consensus for efficient resource allocation; (vi) **governance and control**, where BCNs provide transparent governance through smart contracts that enable automatic compliance with agreements and minimize conflicts, making them valuable for sharing sites and spectrum; (vii) **energy efficiency**, where the use of energy-efficient blockchains or consensus mechanisms can be suitable for various sharing scenarios. Note that selecting the appropriate BCN type based on the unique characteristics of each network sharing scenario is critical to reap its benefits while overcoming challenges.

Table I gives the summary of the various topics available for network sharing with blockchain networks, highlighting some of the most relevant work for each topic and describing the contributions of the proposed work in this paper. The existing body of literature lacks a comprehensive and organized classification system for BCN architectures specifically designed for network sharing scenarios. To the best of the author's knowledge, no studies have been conducted in the realm of network sharing that explore the viability of employing blockchain networks (BCNs) for the purpose of managing networking data. In this paper, we present a comprehensive classification and categorization of blockchain-based network sharing scenarios, highlight their advantages and limitations, and evaluate the performance of some selected BCN architectures. Main contributions of the paper are as follows: (i) We first introduce the various network sharing scenarios that are grouped accordingly and the present some their challenges associated

TABLE I: A comparison of various techniques for network sharing with the proposed approach.

	Traditional Approaches		Proposed Approach	
	Characteristics	Limitations	Advantages	Differences
Radio Sharing	B-RAN framework ([5], [6]) for blockchain-based trust Provide a reliable, secure, and efficient solution for managing networking data [7]	RAN oriented approach Limited network sharing scenarios	Generalized network sharing under four main categories Large set of network sharing options	Interactions of BCN with network sharing scenarios Comparisons of BCN architectures in network sharing
Secure slice management	DLT for network slicing [8], [9] BCN-enabled slice resource leasing [10] BCN-based network slice brokering [11], [12]	Survey papers, no evaluations Missing network sharing Limited network sharing scenarios	Numerical evaluations of BCNs for network sharing Network sharing in multi-operator scenarios Fine-grained network sharing and BCN arch. categorization	Network sharing scenario validations with BCNs Extensive evaluations of BCN architectures BCN mapping for network sharing
Service Provisioning	BCN-based multi-operator service provisioning for 5G users [13] A distributed market design with the brokering mechanism [14]	Focus only on spectrum management Focus mostly on market design	High number of use cases for multi-operator network sharing Large set of network sharing options	Mapping of BCN architectures with several network sharing use cases

with each scenario. (ii) We then review the different types of blockchain architectures, including *public*, *private*, *permissioned*, *permissionless* blockchains, as well as *sidechains*, *federated blockchains*, *hybrid blockchains*. More specifically, we analyzed the suitability of *Ethereum*, *Zilliqa* and *HoloChain* for *public BCNs*, *Corda*, *HyperLedger Fabric*, *HyperLedger Sawtooth* for *private BCNs*. *DragonChain*, *Solana*, *Fantom* for *hybrid BCNs* and *KSI Blockchain*, *Polygon*, *Cosmos* for *Sidechain* implementations. (iii) We provide evaluation results of some of the most appropriate BCNs (namely *Ethereum*, *Corda*, *Solana* and *Cosmos*) and discuss the suitability of each blockchain architecture for different network sharing scenarios, highlighting the advantages and limitations of each approach. (iv) Finally, we conclude our paper with a discussion on the gaps, opportunities and potential future directions of blockchain-based network sharing solutions.

The rest of the paper is organized as follows. Section II discusses the network sharing categories. The system architecture is explained in Section III. The proposed mapping of BCN architecture with network sharing is discussed in Section IV. Evaluation results are provided in Section V. Gaps, opportunities, and future research directions are discussed in Section VI. Finally, Section VII concludes the paper.

II. NETWORK SHARING CATEGORIZATION

Multiple Mobile Network Operators (MNOs) can perform network sharing to complement established Multi-Operator Core Networks (MOCN), Multi Operator RAN (MORAN) and Distributed Antenna Systems (DAS) approaches. There are several options for network sharing, including (i) **Base Station (BS) sharing**: Multiple operators share the same BS, but operate their own Core Networks (CNs). Under this category, *MOCN as MORAN* and *MORAN with 2 Baseband Units (BBUs)* scenarios exist. (ii) **RAN and CNs sharing**: Multiple operators share both the RAN and CNs infrastructure. Under this category, *Gateway Core Network (GWCN) as MORAN* and *GWCN* scenarios exist. (iii) **Spectrum sharing**: Multiple operators share the same spectrum, but operate their own Radio Access Network (RAN) and CN infrastructure. Spectrum sharing can be achieved through different techniques such as time-division, frequency-division, and space-division multiplexing. Under this category, *MOCN* scenario exist. (iv) **Site/Geographical sharing**: This facilitates the sharing of passive elements and offers the possibility of selecting spectrum sharing as an option. Within this category, there are two scenarios: *Site sharing* and *Geographical split*.

Each option has its own advantages and limitations, and the choice of option depends on the specific needs and requirements of the operators involved. Fig. 1 shows a summary

of different configuration options for network sharing are described as follows:

Group Site/Geographical sharing involves two scenarios as shown in Fig. 1. In *Site Sharing* scenario both MNOs position their gNodeBs at the same location, and all the CN equipment is separate. This involves sharing passive elements of the RAN, such as towers, poles, and shelters. Site sharing is a simple and cost-effective way to reduce the overall capital and operational expenditure of network operators. All the cells and frequencies belong to the MNOs. The advantages of site sharing include sharing the energy resources and site leasing costs, no software configurations being needed for BBUs, and being the least complex sharing scenario in terms of network configuration. However, challenges include the questionable OPeX saving, two sets of operations under the same physical space, and the need for an agreement among MNOs for suitable site selection. Other scenario The second scenario named *Geographical split* involves two or more MNOs serving different geographical locations across the country. The advantages of this scenario include the option to select spectrum sharing based on implementation and regulative constraints. However, MNOs need to obey each other's site selection and deployment policies, and providing quality-of-service (QoS) and cost saving is questionable due to different MNO subscriber distributions in different regions across the country.

Group Spectrum sharing involves scenario *MOCN* as shown in Fig. 1. This scenario involves two or more MNOs sharing one gNodeB for radio access while the core network is dedicated for each operator. This scenario has no additional carries and BBU investments and relatively easy configuration compared to MORAN (scenario MOCN as MORAN and MORAN with 2 BBUs). However, the operation is difficult since the ownership of BS is questionable, and there are regulation difficulties due to traffic aggregation at the same nodes (both in BBU and carrier).

Group RAN and CN sharing involves two scenarios as shown in Fig. 1. Scenario *GWCN* involves the gNodeB and Access and Mobility Management Function (AMF) being shared by two or more MNOs, with User plane Function (UPF) potentially being shared as well. This scenario is best for OPEX and CAPEX savings due to the shared AMF, UPF, and BBU, and no additional interconnection is needed between MNOs. However, it may be more suitable for Mobile Virtual Network Operators (MVNOs) than MNOs due to the high number of virtualized nodes, and regulation license of MVNOs may be required for MNOs. In other scenario *GWCN as MORAN* involves both gNodeB and AMF are shared by two or more MNOs, and non-shared cells can be enabled by

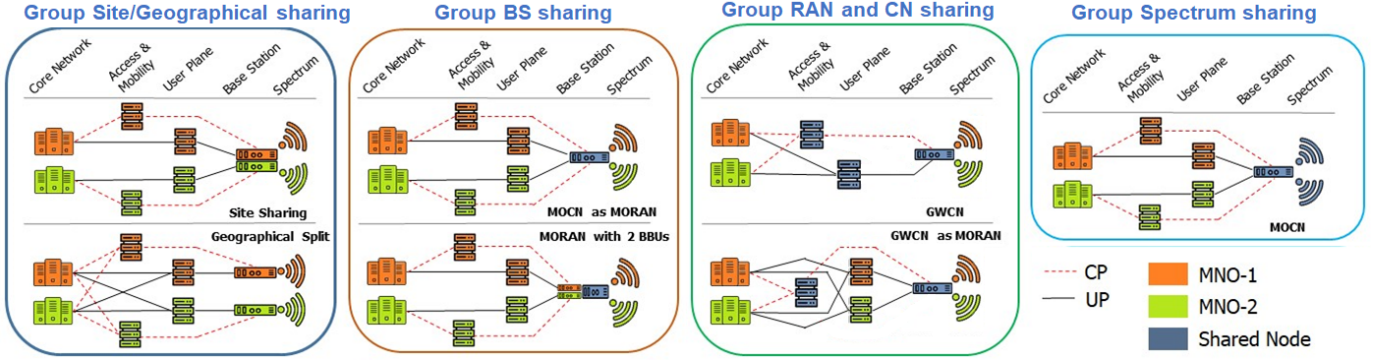


Fig. 1: Different configuration scenarios for network sharing. CP: Control Plane, UP: User Plane

network configuration (dedicated frequency for each operator). Advantages include a reduction in the number of Control Plane (CP) signalling and no additional AMF and BBU investment. Challenges include the authentication of BS done at the shared AMF (which can bring security issues) and agreement issues on parameter adjustments of CP signalling among MNOs.

Group BS sharing involves two scenarios as shown in Fig. 1. *Scenario MOCN as MORAN* where multiple operators share a common RAN infrastructure, but operate their own CN. MORAN sharing enables each operator to utilize a separate carrier to achieve more freedom and independence on the control of the radio resources. Separate carriers can be used at the RAN side, and cells are connected to the operator-owned carriers, with one shared BBU used for transport traffic aggregation. Advantages include full compliance with regulation authority rules, each MNO aggregating mobile traffic in their owned carrier frequencies, no additional BBU investment, and relatively less complex QoS configuration when compared with other MORAN scenarios. However, challenges include the need for a highly capable BBU to operate with different carriers, complexity in the management of BBU, the questionable ownership of BBU, and the need for agreements on QoS policies due to a single BBU. In other *scenario MORAN with 2BBUs* two DUs or BBU units that belong to different MNOs can share radio units and the support system. Operators have their carriers and individual configurations of all parameters. Advantages include each MNO owning and controlling their own network, a reduced impact of interference, and the ability to operate independently. However, challenges include the complexity in managing and synchronizing multiple BBUs, a higher CapEx investment required, and a need for agreement between MNOs on site selection.

III. BCN ARCHITECTURES

A. Classification

There are various classifications for BCNs [15]. Below, we have summarized the four most common ways of categorizing it: (i) **Public blockchains** (permissionless or permissioned) have high consensus building cost which increases robustness against data being falsified by a particular participant. These types of blockchains are typically used in situations where the network is open to the public but still requires permission to participate in the consensus process.

TABLE II
EXAMINED BLOCKCHAIN SYSTEMS.

BCN Class	Studied BCNs.		
Public	Ethereum	Zilliqa	HoloChain
Private	Corda	HyperLedger Fabric	HyperLedger Sawtooth
Hybrid	Solana	DragonChain	Fantom
Sidechains	Cosmos	KSI Blockchain	Polygon

(ii) **Private chains (permissioned)** provide greater control and privacy compared to public blockchains, making them a more suitable option in scenarios where sensitive data is involved and strict access control is required. Some permissioned blockchain platform examples are Corda, Hyperledger Sawtooth, and Hyperledger Fabric. (iii) **Hybrid blockchains** are a combination of public and private blockchains and can also be used for a blockchain that uses a combination of different types of consensus mechanisms. Some relevant hybrid blockchains are Fantom [16] and Dragonchain [17]. (iv) **Sidechains** are separate blockchains that are attached to an existing blockchain, allowing for the creation of new applications or use cases without affecting the existing blockchain. Some examples are the Cosmos, KSI Blockchain and Polygon.

B. Metrics and BCN Comparisons

The strengths and weaknesses of different BCN architectures can be measured using a variety of indicators. In Table II, the list of the studied blockchain systems for network sharing scenarios is also presented. In this table, *Ethereum, Zilliqa and HoloChain* are public BCNs, *Corda, HyperLedger Fabric, HyperLedger Sawtooth* are private BCNs. *DragonChain, Solana, Fantom* are hybrid BCNs. Some platforms listed may also support sidechain implementations *KSI Blockchain, Polygon, Cosmos*. We can classify the metrics into two main categories based on their focus. *Operational and Functional Metrics* (scalability, security, privacy, cost-effectiveness, interoperability and performance) and *Incentive Layer Metrics* (decentralization, governance, consensus mechanism, sustainability and adoption). While the incentive layer metrics focus on contributing to participants' motivations, decision-making, and the BCN's long-term viability, the operation and functional properties metrics provide insights into the overall performance and usability of the blockchain network ensuring the BCN's effective performance and alignment with network goals and the incentive layer metrics. In network sharing

scenarios, above metrics collectively provide a comprehensive framework for assessing the suitability of different BCN architectures. These metrics collectively contribute to understanding the network's strengths and weaknesses and its potential to meet the requirements of different applications. By evaluating each metric's relevance and impact in the context of specific sharing scenarios, it becomes possible to make informed decisions about the most appropriate BCN type to implement. Let's delve into how the metrics are relevant in this paper's scenarios:

Incentive Layer Metrics: **Decentralization** is the degree to which the BCN is decentralized, meaning the power and control is distributed among network participants. In Ethereum network, decentralization is one of the core principles and goals. **Governance** is the mechanisms and processes used to make decisions about the operation and development of the BCN. Corda stands out for its strong emphasis on governance which is specifically designed for enterprise use cases that require strict governance and privacy. **Consensus mechanism** is the method used to achieve consensus among nodes in the BCN. They vary widely between different blockchain architectures. Ethereum provides a robust and efficient consensus mechanism called Ethash, which is a Proof-of-Work (PoW) algorithm [18]. **Sustainability** refers to the capacity of a BCN to function in a manner that is environmentally responsible and minimizes energy consumption. Solana can be considered a sustainable hybrid blockchain architecture. Its architecture and efficient algorithms contribute to a relatively low energy consumption per transaction [19]. **Adoption** is the level of adoption and use of the BCN, including the number of active users and the number of applications built on top of it. Cosmos BCN has built a strong community of developers.

Operational and Functional Property Metrics: **Scalability** is the ability of the BCN to handle a large number of transactions per second. From Table II, Solana is considered to be highly scalable, achieving scalability through its unique architecture [20]. **Security** is related to the level of security provided by the BCN, including resistance to attacks and protection against data tampering. From Table II, Ethereum stands out in terms of security, with established security mechanisms and active communities working on improvements [21]. **Privacy** is the degree to which user data is protected and kept confidential. From Table II, private blockchains like Corda prioritize privacy and offer strong security features suitable for enterprise use cases [22]. **Cost-effectiveness** is the cost of using the BCN, including fees for transactions and maintenance. It can be difficult to measure, but it is generally less expensive to use permissioned blockchain than permissionless ones. **Interoperability** is the ability of the BCN to communicate and interact with other systems. Hyperledger Fabric has been designed to be more interoperable than some other blockchain architectures, due to its modular architecture and support for plug-and-play consensus algorithms. Cosmos is also known for its focus on interoperability. **Performance** typically refers to the rate of transaction confirmations. Among the investigated BCNs, (Ethereum, Corda, Solana, and Cosmos), Corda stands out for its high performance and scalability capable of handling a large number of Transactions Per Second

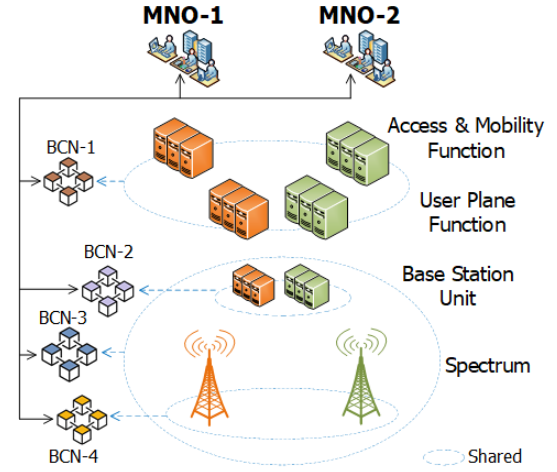


Fig. 2: Interactions of different network sharing scenarios with blockchain.

(TPS) with low latency.

IV. MAPPING OF BCNs WITH NETWORK SHARING

Blockchain technology can provide a secure and transparent platform for the sharing of network resources among MNOs, while ensuring the integrity and privacy of the shared data. BCN can be used in combination with the above network sharing scenarios to address certain challenges and enable certain advantages. Some possible ways to combine blockchain architectural options with the network sharing scenarios is shown in Fig. 2. A summary of the relationship between key performance indicators (KPIs), different network sharing categories and BCN architecture is presented in Fig. 3 which is detailed in the subsections below.

A. Group Site/Geographical Sharing

Hybrid blockchain for site sharing - Blockchain can be used to automate and manage the agreement among MNOs for suitable site selection, and to track and enforce the terms of the agreement. A hybrid BCN can allow multiple parties to share and access data securely and transparently, while still maintaining control over their data. Smart contracts can be used to specify the terms of the agreement, such as how the energy resources and site leasing costs are shared, and to automatically execute payments and penalties based on the performance of each MNO. The contract could be transparently managed by both MNOs and enforced automatically through the blockchain, reducing the need for trust between the parties. In this scenario, cost efficiency (to reduce administrative costs), decentralization (to collaborate among MNOs without intermediaries), and governance (to define and enforce agreements) are of great importance. Solana, which is a hybrid blockchain architecture, can be a suitable option because it provides granular control over network access and data visibility, ensuring data privacy and confidentiality. Solana also offers a modular architecture that allows for easy integration with existing systems. This can be useful in the site-sharing scenario, as MNOs may have their own legacy systems. Additionally, Solana's support for smart contracts and

its ability to provide a tamper-proof audit trail ensures data integrity, automation, and transparency among the participating mobile network operators.

Hybrid blockchain for Geographical split: In this scenario, multiple MNOs are serving different geographical locations across the country. *Hybrid blockchains* could be useful in this scenario where different MNOs have different requirements and preferences for the type of blockchain architecture used. Since multiple MNOs are serving different geographical locations, a hybrid blockchain could allow each MNO to choose the type of blockchain architecture that works best for their specific region, while still maintaining some level of interoperability and shared infrastructure. They can be used to manage access control and coordination between the different MNOs. For example, the blockchain can be used to ensure that each MNO obeys the site selection and deployment policies of the others, and to verify that QoS requirements are being met. The blockchain can also be used to facilitate spectrum sharing between the different MNOs, with smart contracts governing the allocation and usage of shared resources. In the case of geographical split, blockchain can be used to create a shared ledger of network resources, including spectrum, cells, and equipment. This ledger can be distributed among all the participating MNOs and used to track the utilization and availability of resources. In this scenario, cost efficiency (to reduce infrastructure costs), decentralization (to allow collaborative decisions), governance (to enforce adherence to site selection policies) and consensus mechanisms (to handle resource allocation decisions) are of great importance. A hybrid BCN could enable MNOs to reach agreements on site selection and deployment policies, as well as QoS and cost-sharing arrangements and automate the allocation of resources based on pre-defined rules and conditions. Additionally, such blockchain-based solution could enable the transparent and secure sharing of network usage data, which could be used to inform decisions around resource allocation and network optimization.

B. Group Spectrum Sharing

Sidechain blockchain for MOCN scenario has two or more MNOs share one gNodeB while the core network is dedicated for each operator. A sidechain blockchain can be a suitable solution for managing access control and coordination between different MNOs in a shared network scenario. Since multiple MNOs are sharing the same gNodeB, there is an increased risk of security breaches and unauthorized access. By implementing a sidechain blockchain, a controlled environment can be created where only authorized parties have access to the network, ensuring secure information and data sharing. Smart contracts can be utilized to enforce agreements between the MNOs regarding ownership of the shared gNodeB, fair distribution of costs, and facilitate inter-MNO transactions and settlements. The sidechain blockchain can establish a shared ledger of network ownership, including ownership of the gNodeB/BS, creating a transparent and clear ownership structure for shared network resources. This helps reduce the risk of disputes and regulatory difficulties. Smart contracts

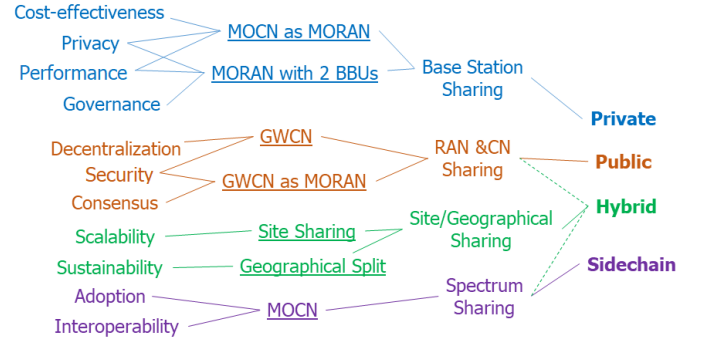


Fig. 3: A summary of mapping strategy with attributes, network sharing options, categories and blockchain architectures.

play a vital role in automating resource sharing and ensuring equitable allocation among participating MNOs. In this scenario, a hybrid blockchain architecture, combining elements of public and private blockchains, could also be employed to manage ownership and access rights to the shared equipment, ensuring appropriate access and control for each MNO. In this scenario, governance (to enforce resource sharing agreements), cost efficiency (for fair cost sharing mechanisms), and consensus mechanisms (to manage resource access) are of great importance.

In the context of this scenario, the Cosmos architecture can be leveraged to create an interconnected ecosystem where each MNO maintains its own independent blockchain while enabling seamless communication and collaboration. Each MNO can deploy its own blockchain within the Cosmos network. This blockchain would represent the MNO's specific network infrastructure, including gNodeBs, authentication mechanisms, and other relevant components. The Cosmos architecture allows these individual blockchains to operate independently, maintaining their own consensus mechanisms and governance models. Interoperability is a key advantage of the Cosmos architecture. Through the use of inter-blockchain communication (IBC) protocols, different MNO blockchains within the Cosmos network can securely and efficiently exchange data and assets. This enables coordination, sharing of resources, and seamless communication between the MNOs. The Cosmos Hub [23], which acts as a central connecting point within the Cosmos network, facilitates the secure exchange of data and transactions between MNO blockchains. Furthermore, Cosmos provides flexibility in terms of consensus mechanisms, allowing MNOs to select the most suitable consensus protocol for their specific requirements. This ensures that the network sharing arrangement can accommodate the diverse needs and preferences of the participating MNOs.

C. Group RAN and CN sharing

Public blockchain for GWCN scenario involves the gNodeB and the AMF are shared by two or more MNOs. Each MNO can have dedicated cells and frequencies assigned to them, allowing them to maintain some level of autonomy over their network resources. Public BCN in the GWCN scenario, can facilitate various aspects of network operations, such as authentication, billing, and QoS management. A public

blockchain can provide a shared ledger that records and verifies transactions related to these services. It can ensure transparency, immutability, and decentralization in inter-operator communication and data management. Smart contracts on the public blockchain can automate and enforce payment terms, ensuring that each MNO receives its fair share of revenue generated by the shared network. In this scenario, security (to ensure secure billing and QoS management), privacy (to safeguard subscriber data), governance (to enforce transparent inter-MNO transactions) and adoption (thanks to secure and transparent cross-operator service encouraging MNO participation) are of great importance.

A hybrid blockchain can also be a suitable option for the GWCN scenario, considering the need to balance transparency and privacy. A hybrid blockchain could enable secure and transparent sharing of the gNodeB and AMF resources between the operators while ensuring that each operator maintains control over their own UPF and BBU. It can provide features such as data privacy, transparency and interoperability, governance and control and scalability and performance in GWCN scenario. The public blockchain component of the hybrid blockchain could be used to enable secure and transparent sharing of the gNodeB and AMF resources, while the private blockchain component could be used to enable each operator to maintain control over their own UPF and BBU. However, it is crucial to design the hybrid blockchain architecture carefully, considering factors such as network scalability, interoperability, and consensus mechanisms. Additionally, appropriate security measures and access controls must be implemented to protect sensitive data and prevent unauthorized access. Ethereum could be a suitable blockchain architecture for Scenario GWCN, where gNodeB and AMF are shared by multiple MNOs. Ethereum provides privacy and confidentiality by allowing for private channels and endorsing peer policies. It also allows for fine-grained access control and flexible consensus mechanisms. These features are important for ensuring secure and efficient sharing of resources between MNOs. Moreover, Ethereum's modular architecture allows for customization and scalability, making it suitable for GWCN scenario with multiple virtualized nodes.

In *Public blockchain GWCN as MORAN* scenario, BCN can be used to improve security and privacy in the authentication of BS at the shared AMF and manage authentication and authorization of BSs at the shared AMF securely, ensuring that only authorized devices are allowed to connect to the network. By using a blockchain-based identity and access management system, each MNO can have control over their own user authentication and authorization, while still being able to share the AMF. This can reduce the risk of unauthorized access and data breaches. The public blockchain can also be used to create a transparent ledger of parameter adjustments made by each MNO, enabling all parties to monitor and verify changes made to the network. In this scenario, security (to ensure secure authentication), privacy (to safeguard subscriber data), governance (to protect user authorization data) and consensus mechanism (to handle authentication decision) and decentralization (to eliminate central authentication) are of great importance. Ethereum blockchain architecture that can

handle multi-party authentication and agreement on network configuration parameters would be suitable for this scenario when a public implementation is used. Ethereum supports configurable endorsement policies and allows multiple organizations to participate in the consensus process. This allows for the definition of specific rules and requirements for endorsing transactions, enabling consensus among multiple parties in determining network configuration parameters. Moreover, the use of smart contracts in Ethereum can help automate the configuration process and ensure that all parties follow the agreed-upon parameters, reducing the chances of errors and disagreements.

D. Group BS Sharing

Private blockchain for MOCN as MORAN scenario can be used to establish ownership of the shared BBU and to manage QoS policies among the MNOs. BCN can be used to create an immutable record of network performance data, such as latency and throughput, that all MNOs can access and use to monitor the network's health. By using a blockchain-based ownership registry, each MNO can have a verifiable and immutable record of their ownership share in the BBU. The blockchain can also be used to create a decentralized ledger of QoS policies agreed upon by all MNOs, reducing the need for a single point of control and the risk of conflicts between the operators. Smart contracts can be used to specify and enforce QoS policies, such as how bandwidth is allocated among the MNOs. In this scenario, governance (to enforce ownership and QoS policies), consensus mechanisms (to ensure data consistency) and security (to secure ownership and performance records) are of great importance. BCN architectures that support interoperability and cross-chain communication, such as Corda may be suitable for this scenario. These architectures provide features such as smart contract support, permissioned access, and privacy, which can help in managing the complexities involved in cross-network resource integration and sharing, and can provide a trustworthy and secure environment for network operators. Additionally, these architectures also support modular designs, which can help in managing the complexities involved in managing a highly capable BBU to operate with different carriers.

In *MORAN with 2 BBUs scenario*, private blockchain can be used to enable more efficient and secure synchronization of multiple BBUs and create a decentralized and secure record of network synchronization data, such as timing and frequency adjustments, ensuring that all MNOs are synchronized and interference is minimized. Consortium blockchain provides a controlled and secure environment that allows multiple MNOs to join the network and share data while maintaining their autonomy. In this scenario, governance (to enforce BBU ownership and sharing), scalability (to efficiently synchronize multiple BBUs, consensus mechanism (to manage BBU agreement), decentralization (to ensure autonomous BBUs) and sustainability (to reduce energy usage with efficient BBU synchronization) are of great importance. By using a consortium blockchain-based consensus algorithm, the BBUs can reach agreement on the state of the network and synchronize their

TABLE III
SUMMARY FOR MAPPING OF THE DIFFERENT NETWORK SHARING DEPLOYMENTS
SCENARIOS WITH SUITABLE BCN ARCHITECTURES.

Group	Scenario	Characteristics	Suitable BCN Architecture	Relevant Metrics
Site/Geographic Sharing	Site Sharing	<ul style="list-style-type: none"> Both MNOs position their gNodeBs at same location All the CN equipment are separate All cells and frequencies belong to MNOs 	<ul style="list-style-type: none"> Hybrid BCN to automate and manage agreement among MNOs Smart contracts to specify terms of agreement To automate payments and penalties 	<ul style="list-style-type: none"> Cost-effectiveness to reduce administrative costs Decentralization to collaborate among MNOs without intermediaries Governance to define and enforce agreements
	Geographical Split	<ul style="list-style-type: none"> Two or more MNOs are serving to the different geographical locations across the country Collaborative large scale network deployment among MNOs 	<ul style="list-style-type: none"> Hybrid BCN to manage access control and coordination among MNOs To ensure each MNO obeys the site selection and deployment policies and to verify QoS requirements. To facilitate spectrum sharing. Create a shared ledger of network resources, including spectrum, cells, and equipment To automate the allocation of resources 	<ul style="list-style-type: none"> Cost-effectiveness to reduce infrastructure costs Decentralization to allow collaborative decisions Governance to enforce adherence to site selection policies Consensus mechanisms to handle allocation decisions
Spectrum Sharing	MOCN	<ul style="list-style-type: none"> Two or more MNOs share one gNodeB while the core network is dedicated for each operator. 	<ul style="list-style-type: none"> Sidechain BCN to manage access control and coordination To ensure that each MNO is paying its fair share of the costs To establish a clear and transparent ownership for shared network resources To automate the sharing of resources 	<ul style="list-style-type: none"> Governance to enforce resource-sharing agreements Cost-effectiveness for fair cost-sharing mechanisms Consensus mechanism to manage resource access.
BS Sharing	MOCN as MORAN	<ul style="list-style-type: none"> Separate carriers at the RAN side Cells connected to the operator owned carriers and one shared BBU is used for transport traffic aggregation 	<ul style="list-style-type: none"> Private BCN to establish ownership of the shared BBU To create an immutable record of network performance data and QoS policies To specify and enforce QoS policies 	<ul style="list-style-type: none"> Governance to enforce ownership and QoS policies Consensus mechanism to ensure data consistency. Security to secure ownership and performance records.
	MORAN with 2BBUs	<ul style="list-style-type: none"> Two DUs or BBU units that belong to different MNOs can share radio units and the support system Operators have their own carriers and individual configuration of all parameters 	<ul style="list-style-type: none"> Private blockchain to enable more efficient and secure synchronization of multiple BBUs BBUs can reach agreement on network state To create a transparent ledger of site selection agreements and ownership of network components. 	<ul style="list-style-type: none"> Governance to enforce BBU ownership and sharing. Scalability to efficiently synchronize multiple BBUs. Consensus mechanism to manage BBU agreement. Decentralization to ensure autonomous BBUs. Reduce energy usage with efficient BBU synchronization.
RAN and CN Sharing	GWCN as MORAN	<ul style="list-style-type: none"> Both gNodeB and AMF are shared by two or more MNOs By network configuration non-shared cells can be enabled (dedicated frequency for each operator.) 	<ul style="list-style-type: none"> Public BCN to improve security and privacy in the authentication of BS Each MNO to have control over their own user authentication and authorization. To enable all parties to monitor and verify changes made to the network 	<ul style="list-style-type: none"> Security to ensure secure authentication. Privacy to protect user authorization data. Consensus mechanism to handle authentication decisions. Decentralization to eliminate central authentication.
	GWCN	<ul style="list-style-type: none"> The gNodeB and the AMF are shared by two or more MNOs UPF can also be shared based on deployment All the cells and frequencies are shared 	<ul style="list-style-type: none"> Public BCN for authentication, billing, and QoS management To facilitate secure and transparent inter-operator communication To ensure the integrity and confidentiality of subscriber data To facilitate inter-MNO transactions and settlements To ensure security and integrity of the shared network 	<ul style="list-style-type: none"> Security to ensure secure billing and QoS management. Privacy to safeguard subscriber data. Governance to enforce transparent inter-MNO transactions. Adoption thanks to secure and transparent cross-operator services encouraging MNO participation.

operations more effectively. This can reduce the risk of interference and improve network performance. Smart contracts can also be used to create a transparent ledger of site selection agreements and ownership of network components, reducing the risk of conflicts and disputes between the MNOs. In the context of the BS sharing scenario, Corda could be used to manage the coordination and agreements between the participating MNOs. It can provide a controlled environment where only authorized parties have access to the shared network and can securely share information and data. Smart contracts in Corda can automate and enforce agreements between the MNOs regarding ownership of BS, traffic aggregation, and revenue sharing. Corda's focus on privacy, permissioning, and fine-grained access control makes it suitable for scenarios where multiple entities need to collaborate and transact while maintaining confidentiality and security.

Finally, Table III provides a summary of mapping of different scenarios for network sharing deployments with suitable BCN architectures and relevant metrics.

V. EXPERIMENTAL VALIDATIONS

A. Setup and Metrics

For experiments, we implemented different BCN on Virtual Machines (VMs) that are running on OpenStack¹. Each VM is assigned with 16 central processing unit (CPU) cores, 64 GB Random Access Memory (RAM) and 500 GB storage space. Four dedicated nodes were created for each BCN in the VM. There is also a separate VM that is running a REST server to send requests to BCNs. The REST server acts as an interface

¹Online: <https://www.openstack.org/>, Available: May 2023.

or gateway for external interactions with the blockchain networks. Smart contracts for considered BCN architectures are developed using the corresponding SDK frameworks of the compared BCNs. The logic and rules defined for transactions and interactions within a blockchain network in smart contract are written in Javascript. The evaluation's use of four nodes could represent a simplified version of scenarios considered above. For example, in the RAN and CN Sharing (GWCN) scenario each node corresponds to a different MNOs' shared resources. The four nodes could be associated with different RAN and CN components, mimicking the participation of multiple operators in a shared network environment. It's important to note that the real-world GWCN scenario could involve more operators, more complex interactions, and a larger number of network elements. However, such a four-node setup can serve as an initial step in understanding how BCN-based solutions might function in such shared RAN and CN environments. Within the scope of our paper, we primarily focused on performance aspects rather than other relevant metrics such as security, decentralization, consensus mechanisms, governance, and privacy to accommodate user growth, ensure system responsiveness and process transactions swiftly and reliably.

The average transaction latency (denoted as ATL) for T transactions is calculated as the sum of the differences between the generation time $G(\{g_i\})$ and confirmation time $C(\{c_i\})$ for each transaction [24], given by

$$ATL = \mathbb{E}[|G - C|] = \frac{1}{T} \sum_i |g_i - c_i|. \quad (1)$$

By calculating the average transaction latency, blockchain network operators and participants can gain insights into the efficiency and speed of transaction processing. Lower latency indicates faster transaction confirmations, while higher latency implies longer delays in transaction finalization. TPS (TPS) is used to measure the processing speed and scalability of a blockchain network. It represents the number of transactions that can be processed and confirmed by the blockchain system within a one-second time frame. we can use the following relationship to compute TPS,

$$TPS = \frac{\alpha}{\beta} \quad (2)$$

where α represents total number of transactions processed and β represents the time taken to process the transactions. To determine the TPS value, the total number of transactions processed during a specific period and the time it took to process those transactions need to be accurately measured. Finally, CPU consumption in BCN refers to the amount of computational resources utilized by the BCN or specific blockchain-related processes (mining, validation, etc.). It measures the extent of CPU utilization or load imposed on the system by performing various tasks related to blockchain.

B. Evaluation Results

We have provided the average delay (ATL), TPS and CPU consumption (%) for various experimental BCN implementations based on 1000 transactions in Fig. 4a, Fig. 4b and Fig.

4c, respectively. From Fig. 4a, we can observe the following comparisons: Corda has the lowest average delay among the listed BCN systems, indicating faster transaction processing. Ethereum has a slightly higher average delay compared to Corda, implying slower processing time than that of Corda. Solana has a significantly higher average delay compared to both Ethereum, Corda and Cosmos, suggesting slower transaction processing. Cosmos has a higher average delay than Ethereum and Corda but is faster than Solana. Nestled in the middle ground, Cosmos boasts an average delay surpassing that of Ethereum and Corda; however, its quicker pace, in terms of reduced average delay, remains faster than Solana.

Regarding TPS from Fig. 4b, we can observe the following comparisons: Surprisingly, Ethereum has the highest TPS value among the listed BCN systems. Corda has a slightly lower TPS compared to Ethereum but still demonstrates high transaction throughput. Solana has a considerably lower TPS compared to both Ethereum and Corda, whereas, Cosmos has the lowest TPS among the listed BCN systems, indicating the lowest transaction throughput. There could be a few reasons why Ethereum has a higher TPS than Solana, despite Solana being a more centralized blockchain. Solana achieves this performance due to its rapid block time, large block size, and rapid consensus mechanism. Nonetheless, this augmentation also entails heightened demands on communication bandwidth and storage space for Solana network. It's worth highlighting that TPS is influenced beyond aforementioned factors including network congestion and the scale, all of which play pivotal roles. From Fig. 4c, we can observe that Ethereum has the highest CPU usage among the listed BCN systems, followed by Cosmos, Corda, and Solana. This indicates that Ethereum requires more CPU resources compared to the other systems to process the same number of transactions. On the other hand, Solana exhibits the lowest CPU usage among the four systems, implying it is relatively more efficient in terms of CPU resource utilization.

These comparisons suggest that Ethereum provides the highest practical transaction throughput and relatively low average delay, making it the most efficient in terms of TPS. However, it requires higher CPU which corresponds to a greater demand for computational resources. Corda follows closely in terms of both TPS and average delay. Solana and Cosmos have lower TPS, CPU and comparatively higher average delays, suggesting slower transaction processing compared to Ethereum and Corda and requires less CPU usage.

C. Discussions

A mapping to network scenarios based on the average delay, CPU and TPS values can be performed as follows:

Group Site/Geographic Sharing: Scenario *site sharing* can utilize any of the blockchain systems listed in Fig. 4a, Fig. 4b and Fig. 4c to enable efficient sharing of site-related resources and facilitate agreements between MNOs. *Geographical Split* scenario does not have a direct mapping in the provided table, as it focuses on geographical distribution rather than specific blockchain characteristics.

Group Spectrum Sharing: Similar to *Geographical Split* scenario, *MOCN* scenario does not have a direct mapping

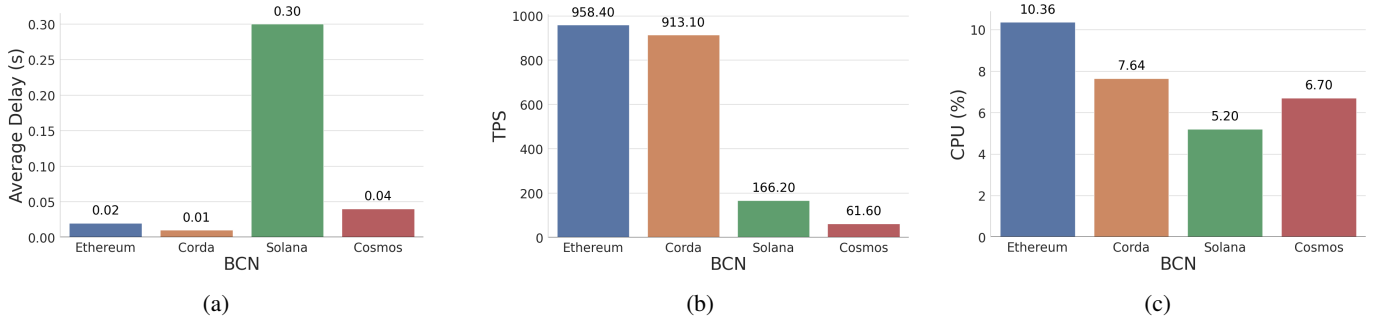


Fig. 4: (a) Average Delay (s) versus BCN. (b) TPS versus BCN (c) CPU (%) versus BCN.

in the provided table, as it involves shared gNodeB and dedicated core networks. However, blockchain systems with appropriate performance metrics could be selected based on the specific implementation requirements and challenges, such as ownership and regulation difficulties.

Group BS Sharing: Scenario *MOCN as MORAN* could potentially benefit from blockchain systems such as Ethereum or Corda, which offer low average delay and high TPS capabilities, enabling seamless sharing of resources and configuration agreements between MNOs. In scenario *MORAN with 2 BBUs* blockchain systems like Solana or Corda could be suitable, as they offer a balance between average delay and TPS, enabling efficient management and synchronization of multiple BBUs while allowing individual configurations for each MNO.

Group RAN and CN sharing Scenarios *GWCN* and *GWCN as MORAN* may benefit from blockchain systems such as Ethereum or Corda, which provide low average delay and high TPS, facilitating authentication and parameter adjustments among MNOs for CP signaling in *GWCN as MORAN* and OPEX and CAPEX savings through shared resources, including gNodeB, AMF, and potentially UPF in scenario *GWCN*.

VI. GAPS, OPPORTUNITIES AND FUTURE DIRECTION

The environmental impact of blockchain solutions in network sharing scenarios needs to be considered. For each of the network sharing architectures, BCN-based solutions can play a role in managing environmental impacts. The key is to develop or adapt BCN systems that optimize resource sharing, reduce energy consumption, and are consistent with sustainability goals specific to each scenario. Future research can focus on developing sustainable BCN solutions that minimize the energy consumption and carbon footprint of network sharing scenarios.

The economic models for blockchain in network sharing scenarios need to be carefully designed to ensure that all stakeholders can benefit from the use of blockchain. For each network sharing architecture, it's crucial to design economic models that align incentives for all stakeholders. These models should encourage collaboration, fair resource utilization, and ensure that all parties involved derive benefits from the shared infrastructure. By developing effective economic models, blockchain solutions can become more attractive and sustainable in network sharing scenarios. Future research can focus on developing economic models that incentivize

operators and users to adopt blockchain solutions in network sharing scenarios.

Interoperability and lack of regulations and standardization: There is a need for interoperability and standardization among different MNOs' networks and blockchain platforms. Ensuring seamless integration and compatibility between diverse systems is crucial for effective utilization of BCNs in network sharing scenarios. Lack of clear regulations and standards around blockchain technology in telecom networks can create legal and regulatory challenges. This can lead to difficulty in establishing partnerships and collaborations between different operators. For example in spectrum sharing, lack of standardized protocols can make it difficult for group spectrum resources to be easily shared and traded among operators. Future research can focus on developing standardized protocols and frameworks for implementing blockchain in network sharing scenarios.

Security in Post-Quantum Era is a critical concern in network sharing scenarios when BCNs are used. All network sharing scenarios can be supported by implementing post-quantum cryptography within the blockchain architecture to ensure the confidentiality and integrity of network communications, resource allocations and transactions in a quantum threat landscape. Future research can focus on developing secure blockchain solutions against quantum computer attacks that can protect the privacy and security of users and operators.

Unified identification and authorization: In the context of network sharing scenarios, Self Sovereign Identity (SSI) can be used for user identity management, allowing for a secure and decentralized way of identifying users across multiple networks and service providers. This can enable seamless roaming across different networks while ensuring the privacy and security of user data. For example, in group BS sharing, SSI can be used to securely manage user identities across multiple operator networks. In site and geographical sharing, SSI can help ensure consistent identification and authorization for shared passive elements and spectrum. Challenges related to implementing SSI in network sharing scenarios, such as interoperability issues between different blockchain platforms and the need for standardization are also available. Further research is needed to address these challenges and explore the full potential of SSI in network sharing scenarios.

Cost: Implementing BCNs requires significant investments in infrastructure, hardware, and software. This can create financial challenges for operators, especially in developing countries. For example in the context of group BS sharing, cost-

effective hardware and software solutions for implementing blockchain networks are needed. In group spectrum sharing, optimizing the allocation of shared spectrum resources while considering regulatory considerations and economic models for equitable cost sharing is required. Future research could focus on cost optimization, scalability, efficiency, economic models, incentive mechanisms and regulatory considerations reduce the financial barriers and enhance the cost-effectiveness of implementing blockchain networks.

VII. CONCLUSIONS

The deployment of network sharing represents a promising solution for reducing capital and operational expenditures for mobile network operators. However, there are several challenges associated with its deployment, such as the difficulty of ensuring accountability and trust between different operators, and the lack of standardization in protocols and technologies used in the shared network. In this paper, we have undertaken a comprehensive investigation of BCN-based network sharing scenarios, with the goal of providing a structured classification, analysis, and evaluation of their suitability for secure and transparent network resource sharing among multi-operators. We have introduced a systematic categorization of network sharing scenarios and shed light on their unique challenges and intricacies to understand the diverse landscape of network sharing. We have carefully analyzed the applicability of certain blockchain platforms in the context of network sharing. We presented performance evaluation results for selected blockchain architectures, namely Ethereum, Corda, Solana, and Cosmos. This empirical analysis provides valuable insights into the practical feasibility and efficiency of these BCNs in the network sharing domain. At the end of the paper, we also discussed the different benefits and limitations of each BCN architecture to help network operators and researchers make decisions when considering BCN-based network sharing solutions.

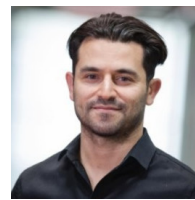
REFERENCES

- [1] Y. Turk and E. Zeydan, "On performance analysis of multioperator RAN sharing for mobile network operators," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 29, no. 2, pp. 816–830, 2021.
- [2] 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.
- [3] S. K. A. Kumar and E. J. Oughton, "Infrastructure sharing strategies for wireless broadband," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 46–52, 2023.
- [4] A. Chaer *et al.*, "Blockchain for 5G: Opportunities and challenges," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, 2019.
- [5] X. Ling *et al.*, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.
- [6] X. Ling *et al.*, "Blockchain radio access network beyond 5G," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 160–168, 2020.
- [7] T. Faisal *et al.*, "Beat: Blockchain-enabled accountable and transparent network sharing in 6G," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 52–56, 2022.
- [8] F. Javed *et al.*, "Distributed ledger technologies for network slicing: A survey," *IEEE Access*, vol. 10, pp. 19412–19442, 2022.
- [9] S. Muntaha *et al.*, "Blockchain for Dynamic Spectrum Access and Network Slicing: A Review," *IEEE Access*, vol. 11, pp. 17922–17944, 2023.
- [10] M. A. Togou *et al.*, "Dbns: A distributed blockchain-enabled network slicing framework for 5G networks," *IEEE Communications Magazine*, vol. 58, no. 11, pp. 90–96, 2020.

- [11] L. Zanzi *et al.*, "Nsbchain: A secure blockchain framework for network slicing brokerage," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2020.
- [12] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Mounsla, "A blockchain-based network slice broker for 5G services," *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, 2019.
- [13] P. Gorla, V. Chamola, V. Hassija, and N. Ansari, "Blockchain based framework for modeling and evaluating 5G spectrum sharing," *IEEE Network*, vol. 35, no. 2, pp. 229–235, 2021.
- [14] N. Afraz and M. Ruffini, "5g network slice brokering: A distributed blockchain-based market," in *2020 European Conference on Networks and Communications (EuCNC)*, pp. 23–27, 2020.
- [15] Tasca, Paolo and Tessone, Claudio J., "Taxonomy of blockchain technologies. Principles of identification and classification," *arXiv preprint arXiv:1708.04872*, 2017.
- [16] Choi, Sang-Min and Park, Jiho and Nguyen, Quan and Cronje, Andre, "Fantom: A scalable framework for asynchronous distributed systems," *arXiv preprint arXiv:1810.10360*, 2018.
- [17] Dragonchain Commercial Platform Version 6, "Dragonchain," 2017. Online : <https://bit.ly/45I3FHZ>, Available: 25August2023, White Paper.
- [18] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, "Hyperledger, ethereum and blockchain technology: a short overview," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–6, IEEE, 2021.
- [19] J. I. Ibañez and F. Rua, "The energy consumption of proof-of-stake systems: A replication and expansion," *arXiv preprint arXiv:2302.00627*, 2023.
- [20] Pierro, Giuseppe Antonio and Tonelli, Roberto, "Can solana be the solution to the blockchain scalability problem?," in *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 1219–1226, IEEE, 2022.
- [21] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.
- [22] M. Iqbal and R. Matulevičius, "Corda security ontology: example of post-trade matching and confirmation," *Baltic Journal of Modern Computing*, vol. 8, no. 4, pp. 638–674, 2020.
- [23] J. Kwon and E. Buchman, "A network of distributed ledgers," *Technical Report. Cosmos Foundation*, p. 27, 2019. [Online], Available: <https://v1.cosmos.network/resources/whitepaper>, September2023.
- [24] N. u. Sehar *et al.*, "Blockchain enabled data security in vehicular networks," *Scientific Reports*, vol. 13, no. 1, p. 4412, 2023.



Engin Zeydan received his Ph.D. degree in February 2011 from the Department of Electrical and Computer Engineering at Stevens Institute of Technology, Hoboken, NJ, USA. He is currently a Senior Researcher at Services as Networks (SaS) Research Unit in CTTC, Barcelona, Spain. He is the Project Coordinator of the European H2020 5GPP MonB5G Project. His research interests are in the areas of telecommunications and data engineering.



Suayb S. Arslan received the M.Sc. and Ph.D. degrees in Electrical and Computer Engineering from the University of California, San Diego, CA, USA, in 2009 and 2012, respectively. He is currently visiting Massachusetts Institute of Technology, Boston, MA, USA as a faculty member. His research interests include information theory, neuroscience, digital communication and storage, cloud and Quantum computing, reliability/system theory and image/video processing.



Yekta Turk received his Ph.D. degree in Computer Engineering from Maltepe University, Istanbul, Turkey, in 2018. He received the M.Sc. degree in Telecommunications & Computer Networks from The George Washington University, DC, USA, in 2007. He is an Independent Researcher based in Istanbul, Turkey. His research interests are in the areas of networking and security.