

# Blockchain for Network Service Orchestration: Trust and Adoption in Multi-Domain Environments

Engin Zeydan<sup>◇</sup>, Jorge Baranda<sup>◇</sup>, Josep Mangués-Bafalluy<sup>◇</sup>, and Yekta Turk<sup>\*</sup>

<sup>◇</sup>Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Castelldefels, Barcelona, Spain, 08860.

<sup>\*</sup>Mobile Network Architect, Istanbul, Turkey, 34396.

{engin.zeydan, jorge.baranda, josep.mangués}@cttc.cat, yektaturk@gmail.com

**Abstract**—In the coming years, blockchain technologies will be used in a variety of industries, including telecommunications. In this paper, due to strict governance of telecommunication infrastructure, we propose a blockchain supported architecture (based on a permissioned distributed ledger (PDL) scheme) for a network management and orchestration platform. The main goal is to create a trusted environment for multiple-stakeholders (such as Cloud Service Providers (CSPs), a Mobile Network Operator (MNO), Vertical Service Providers (SPs), Legal and Regulation Authorities and Responsible Ministry) so that the lifecycle of automated vertical network services (e.g., instantiation, scaling, termination, migration/reallocation) can be managed securely and transparently in a multi-cloud and multi-domain environment. The proposed approach is also validated with an experimental Industry 4.0 scenario using the Quorum blockchain network (BCN) to measure various performance metrics (e.g., number of transactions and blocks, time to write) of various service orchestrator (SO)-related instantiation metrics. At the end of the paper, we present the main discussions on the evaluation results and existing standardization efforts for the convergence of BCN for Management and Orchestration (MANO) of network services for a given telecommunication infrastructure.

**Keywords**—*blockchain, verticals, services, orchestration, multi-domain.*

## I. INTRODUCTION

The rapid development of blockchain technology has the potential to change the way many industries, including telecommunication operate. Telecommunications systems need to orchestrate massive number of new services and operate with a variety of technologies and stakeholders that must work together to enable efficient service delivery and ensure security in multi-domain networks. The latter task is complicated by the fact that the underlying network services may be managed by multiple stakeholders and require collaboration among them in the network. The overall telecommunication network may therefore include a large number of network devices, multiple stakeholders (e.g., Cloud Service Providers (CSPs), vertical Service Providers (SPs), legal authority, regulators, etc.), and multiple technologies interconnected for information exchange. To ensure the security of the entire network between multiple entities involved in the provisioning of network services (e.g., instantiation, termination, scaling, migration/reallocation) across multi-domains, trust, non-repudiation, and transparency play a fundamental role.

In cases where orchestration and management of services is required, all parties (including Mobile Network Operators (MNOs), CSPs and vertical SPs) must collaborate. However, note that CSPs can also be competitors to each other. From this point of view, an environment of trust, accountability and transparency should be created between MNO and CSPs during service management and orchestration process. From accountability perspective, those who manage the services (e.g. MNOs) and those who request the service (e.g. vertical SPs) should be able to identify if a CSP does not satisfy the previously established Service Level Agreement (SLA) requirements or quality standards (e.g. the allocated compute or storage resources). Transparency between multiple entities should also be established to avoid some entities (e.g. CSPs or MNO) being unreliable and blaming others (e.g. to avoid penalties due to faulty network devices [1]).

Blockchain Networks (BCNs) are now widely used in fields such as the Internet of Things (IoT) [2], [3], [4]. The use of BCN can help to create an environment of trust in situations where different parties do not trust each other during network service provisioning especially in multiple administrative domains [5], [6]. For example, CSPs and MNO can use BCN's ledger to transparently store resource lease mapping and allocations or pre-determined SLAs and smart contracts to manage resources in a verifiable manner. After that, all of the steps for managing and orchestrating network services can be written to the blocks as transactions. In this manner, if a problem with managing network services arises, either MNO or CSPs can quickly determine which entity creates the problem. This ensures a secure, auditable, and transparent network Management and Orchestration (MANO) process.

There exist few works which have used both the BCN and MANO framework in telecommunication systems and there is still scope for improvement to bridge the gap between evolving BCN and MANO technologies for enterprise grade business to business platforms. BCNs have been shown to have some potentials in the decentralized fog/cloud domain [7]. Previous works for blockchain-aided network management propose various architecture solutions such as a multi-domain architecture for orchestrating network slices based on blockchain and a trusted execution environment [8], a blockchain-enabled distributed Network Function Virtualization (NFV) framework to achieve consensus among multiple MANO systems [9], a blockchain-empowered framework for spectrum and infrastructure trading between multiple MNOs in a decentralized

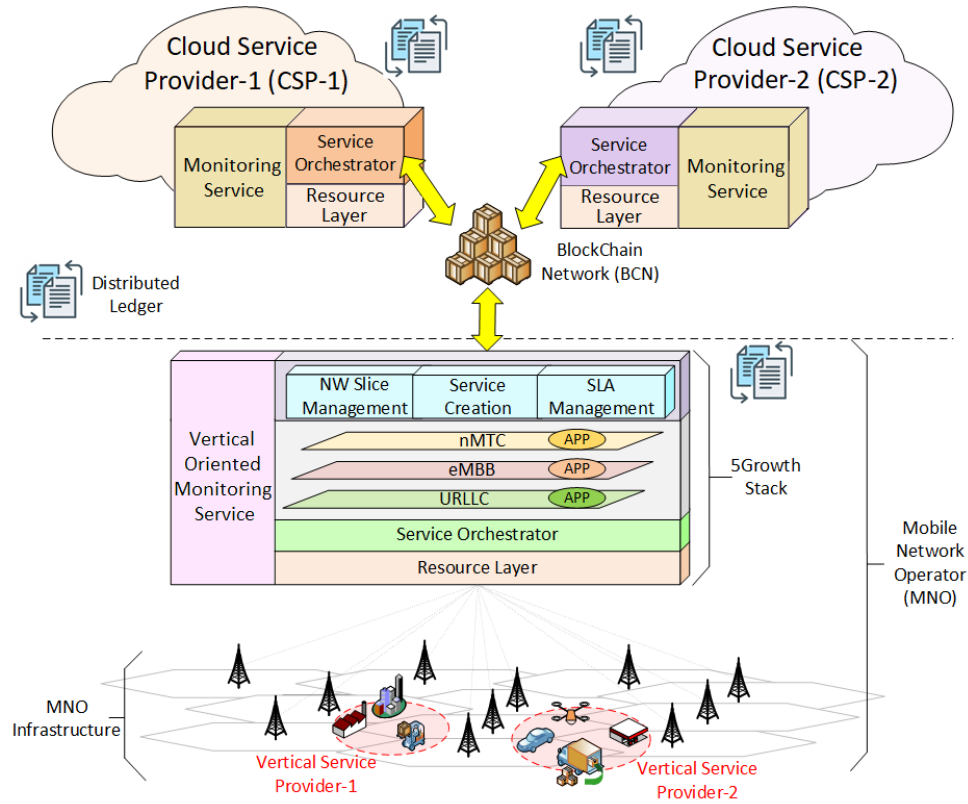


Fig. 1: High-level view of the system architecture providing network service through 5Gr-MANO stack integrated with BCNs.

6G network [10], blockchain-based decentralized applications embedded in multiple administrative domain scenarios [6] and blockchain technology for services provided by the multi-cloud (but only from the perspective of fault localization) [11]. However, embedding an efficient trust model between network service providers for network Lifecycle Management (LCM) in realistic use cases have been overlooked in the existing approaches.

Different than these studies, this paper describes how a permissioned blockchain-enabled MANO stack in particular 5Growth (5Gr)-MANO<sup>1</sup> stack, can be used to create a secure and a trusted environment for multi-cloud or multi-domain deployment scenarios especially for an Industry 4.0 use case. The main aim of the proposed architecture is to automate the network management and orchestration without going through long contractual processes and potential disputes between multiple CSPs and MNO and leverage their competitive and cooperative coexistence relationship when network service provisioning is needed in multiple domains or cloud environments. The main contributions of this paper are as follows:

- We discuss key concepts and present the integration of BCNs-enabled decentralized architecture for multi-stakeholder cloud environment with mobile network man-

agement and orchestration system via a potential Industry 4.0 use case. (Section II and III)

- We evaluate how an example BCN (Quorum Permissioned Distributed Ledger (PDL)) can be integrated with MANO stack of 5Gr via simulation analysis and discuss the evaluation results.(Section IV)
- From a standardization perspective, we describe current Standards Developing Organizations (SDOs) efforts in terms of their potential contributions to network management and orchestration as well as BCN technologies. (Section V)

## II. SYSTEM ARCHITECTURE AND WORKFLOW

### A. High-Level View of the System Design

PDL BCN allows restricted member participation with reduced delays in comparison to permissionless BCNs, since they do not need every node for validation purposes and can manage the number of users who can access and join. Fig. 1 shows a high level view of BCN-based network service LCM in a multi-cloud environment. In this figure, there are multiple stakeholders including vertical SPs (providing vertical services using enablers such as drones, Automated Guided Vehicles (AGVs), vehicles), MNO (providing connectivity) and CSPs (participating in the process of network service provisioning). This figure also shows the general diagram of the 5Gr MANO

<sup>1</sup>Europe Union (EU) H2020 5GPPP project, <https://5growth.eu/>, Accessed: Jan.-2022.

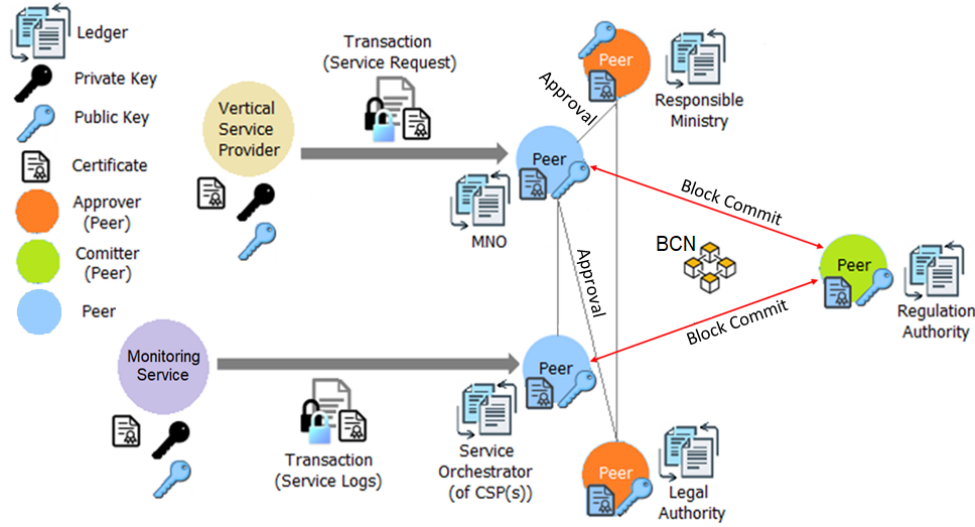


Fig. 2: Workflow of the permissioned blockchain-based service orchestration for verticals in a multi-cloud environment and all peers.

stack consisting of Service Orchestrator (SO), Resource Layer (RL) and Vertical Oriented monitoring system (VoMS) modules that are integrated with BCNs to assure trust and improve the credibility of the network operation. 5Gr-SO provides both network service orchestration and resource orchestration capabilities for instantiating network slices within and between multiple domains. 5Gr-RL manages network and infrastructure resources such as routers, switches, and servers. VoMS provides a mechanism for collecting, storing and processing information, based on metrics, received from the deployed services. For example, operational steps for network service and management are collected by VoMS by interacting with 5Gr-SO or 5Gr-RL.

The three key elements of the architectural solution of Fig. 1 are: (i) 5Gr-MANO stack for autonomous decision making on end-to-end NFV-Network Service (NS) (de)composition from multiple administrative domains so that NFV-NS requirements are met, and aggregation of virtual resources and services offered by multiple providers via federating them through their respective SOs. (ii) BCN for trust and transparency for managing multi-cloud network services, (iii) Multiple CSPs and vertical SPs (mobile and cloud infrastructure, vertical services), network service provisioning approval authorities (such as the legal authority, the responsible ministry), and the relevant regulation authority for each country.

### B. Workflow and Entities

Fig. 2 shows a BCN-based network service deployment flow and all involved peers. The role of each peers in Fig. 2 are described as follows:

- *CSPs* are mainly responsible for providing the infrastructure for network service provisioning and represented by a blue-colored peer in Fig. 2. They interact with MNO to jointly deploy network services. They are also Cloud

Native Function (CNF) software and cloud platform vendors.

- *MNO* is the vital part of our proposed BCN-enabled network service MANO scheme and is represented by a blue-coloured peer in Fig. 2. MNO is managing both 5Gr-MANO stack and BCNs. They are also interacting with regulatory authorities and vertical SPs. It is assumed that each participating entity operate as a full blockchain node to perform security related operations, transaction commitment and contribution to the consensus process.
- *Vertical SPs* interact with 5Gr-MANO stack and request a network slice customized according to their service requirements.
- *Responsible Ministry* is the local authority to endorse the given network service and ensure to obey the law requirements decided by the ministry. It is represented by a orange-coloured peer in Fig. 2.
- *Legal Authority* controls compliance with the law requirements for the requested network service as an approver. It is represented by a orange-coloured peer in Fig. 2.
- *Regulation Authority* is the national telecommunications regulatory and supervisory authority that acts as an independent administrative body (e.g., Ofcom in the U.K. and Federal Communications Commission (FCC) in the U.S.) and is represented by a green-coloured peer in Fig. 2. Its primary role is to monitor, regulate and supervise the telecommunications sector. In our scenario, the proper provision of the requested vertical network services in accordance with the legal requirements, is the responsibility of the MNO and regulated by the competent authority.

In the multi-stakeholder environment of mobile networks implemented using blockchain-based service orchestration architecture and controls, all stakeholders are collaboratively forming a consortium blockchain where all entities are known

in advance but not necessarily trusted. The approvers (in our example responsible ministry and legal authority) are responsible for endorsing the request to instantiate the network service. Approvers do not necessarily review the general ledger for endorsements, but approve the instantiation of the network service by reviewing only its functionality.

As given in Fig. 2, there are three phases to implement the proposed workflow. First, the vertical service provider forwards the approval request to the relevant agencies (relevant ministry, legal authority) for approval in the *approval phase*. Here, the vertical SP coordinates the process of network service instantiation with the relevant authorities (e.g., with responsible ministry and legal authority). For example, suppose that a vertical service provider operates for an industrial factory. In this case, the Ministry of Labour and Employment is notified that a new Industry 4.0 network service is to be deployed. The reason for this could be that the vertical service safety requirements (e.g., minimum required latency for AGVs operating on factory floor to avoid collision or transmit advance notifications) used for the safety of the factory workers on the factory must be approved by the Ministry of Labour and Employment. Another reason could be that the new industrial equipment used by factory workers in a particular network service must be tested for safety or effectiveness before it can be used in the country.

In the *transaction phase*, the network service is instantiated by MNO with the governance of the blockchain. Then in the *block commit phase*, MNO negotiates with regulators over the BCN. In block commit phase, the approved request is converted into a transaction and forwarded to the 5Gr-MANO stack. After the blockchain-enabled MANO receives the transaction, it is transmitted to the BCN. Once the negotiations are complete, the network service can be instantiated securely.

### III. SERVICE ORCHESTRATION PLATFORM FOR VERTICALS IN MULTI-CLOUD ENVIRONMENT

#### A. A Case Study

For experimental evaluations, we consider *Connected Worker: Augmented Zero Defect Manufacturing (ZDM) Decision Support System (DSS)* use case of the 5Gr project as described in<sup>2</sup>. This use case enables collaboration between two originally isolated systems (AGV and Coordinate Measuring Machine (CMM) control systems are coordinated to share a single CMM machine across multiple production lines) by leveraging Machine to Machine (M2M) communication between the AGV and the CMM over the Edge network. The network service we use (to collect operation and management logs for instantiating the service and committing into BCN) enables an AGV device moving near the CMM (the quality control equipment).

The provision of ZDM DSS network services may require multiple CSPs, a MNO, a vertical SP, multiple approvers (e.g., a legal authority that grants permission for the use of sensitive production equipment, or a responsible ministry that oversees the use of specific types of equipment tailored to the

factory environment), as well as a regulation authority that acts as the administrative authority for monitoring, controlling and regulating service, cloud, and telecommunication providers per country. Therefore, there is a need for accountability and transparency when it comes to provisioning such a network service in multi-cloud and multi-domain environments. Hence, the use of BCN and the corresponding applications help to create a trustworthy environment between closed set of untrusted entities (e.g. MNOs, CSPs and vertical SPs) by committing all the operational steps as separate transactions in the blocks of the BCN.

#### B. Service Orchestrator Related Metrics

The 5Gr-SO-related log files can be parsed to calculate the various time difference metrics during the network service instantiation operation. In our evaluations, we use the following 5Gr-SO specific metrics for instantiation operation (more details in [12] and 5Gr project website):

- **Total instantiation time:** The time that elapses since 5Gr-SO creates the service identifier for a network service until it is fully instantiated.
- **Operation ID for Instantiation Op:** The time it takes for the Northbound Interface to generate an ID to identify the instantiation operation.
- **Hierarchical Service Orchestration Engine (SOE) dispatching:** The time the hierarchical SOE uses to select the appropriate instantiation process based on the nature of service (single NS, composite NS)
- **Retrieving descriptor from catalogue Databases (DBs):** The time to collect the descriptor from the Network Service Descriptor (NSD) catalogue
- **Resource Orchestration Engine (ROE) parsing NSDs:** The time taken by the ROE submodule to parse NSD and VNF Descriptors (VNFDs) of a network service to get the required information for the Placement Algorithm (PA).
- **ROE retrieve RL resources:** The time to recollect the information from the RL.
- **PA calculation:** The time to build the request to the PA, send it to the external PA service, and receive its answers.
- **ROE extract Virtual Links (VLs):** The time taken by the ROE to determine the request of the different VLs that require resources in the Logical Links (LLs) because connected Virtual Network Functions (VNFs) have been deployed in multiple Virtualized Infrastructure Managers (VIMs).
- **ROE created VLs:** Interaction time between ROE and RL to allocate resources in the LLs based on the ROE extract request.
- **ROE updating DBs:** Time to update DBs to declare NS as operative and the instantiation operation as successful.
- **Create monitoring jobs:** Time for the interaction between SOE and the Monitoring Manager modules of 5Gr-SO to determine the monitoring jobs (exporters) and dashboards to be configured in the 5Gr-VoMS, and the interaction to configure them and receive the associated object identifiers and update the information in the Network Service Instantiation Resource (NSIR) DB.

<sup>2</sup>H2020 5Growth Project D4.4: Final validation and verification report, <https://bit.ly/3dDoZc6>, Accessed: August-2022

- **Create threshold-based alerts:** Time interaction between SOE-SLA Manager modules of the 5Gr-SO to determine the threshold-alerts objects (when there is no Artificial Intelligence (AI)/Machine Learning (ML) treatment) to be configured at the 5Gr-VoMS and the interaction to configure them at the 5Gr-VoMS and receive the associated object identifiers and update the information in NSIR DB.
- **Create AI/ML alerts:** Time interaction between SOE-SLA Manager to configure AI/ML workflow to drive scaling operations. Creating and configuring the data engineering pipeline consists of: i) interacting with 5Gr-VoMS to create a Kafka Topic, ii) interacting with the 5Gr-AIML platform to download the required model, iii) creating an inference job at Apache Spark, iv) updating NSIR DB.
- **SOE time:** Time spent in the SOE module (both in the SOE parent (SOEp) and SOE child (SOEc) sub-modules) during the instantiation process.
- **ROE time:** Time spent in the ROE module during the instantiation process.
- **Core MANO Wrapper time:** Time spent in the Core MANO Wrapper module during the instantiation process to create a virtual network that support the VLs, the Virtual Machines (VMs) that support the VNFs, and update the NSIR DB.

#### IV. EXPERIMENTAL EVALUATIONS

For the evaluation of the BCN result comparisons, we use the block size [bytes] of the Quorum BCN, the time to write to PDL (basically latency values including verification time and network delay) and the number of transactions as evaluation metrics. In all evaluations, one transaction is sent for each line in the 5Gr-SO log files considered. The logs are also preprocessed so that they can be provided to the BCN per SO operation. In addition, the “Total instantiation time” log includes all operations. For both the network service instantiation time results and BCN performance comparison, the experiments were performed with 10 repetitions.

##### A. Hardware & Software Specifications

Our experimental setup consists of an instance of a 5Gr-MANO stack and Quorum BCNs. The log File is collected from 5Gr-SO of Fig. 1. Later, it is transmitted to the BCN with three nodes via a JavaScript app that reads the file (file reader Application Programming Interface (API) of the BCN) and sends it as transactions depending on the selected transaction log size (chosen as 1 line in the simulations, so the number of log lines in our analysis is equal to number of transactions). Table I shows the simulation environment. Two approvers (acting as the legal authority and responsible ministry), one committer (acting as the regulation authority) and three peers (acting as two CSPs and one MNO) are involved in the evaluations. Due to single regulation authority, no consensus algorithms are used. In our simulations, all transactions are sent from the external user to Node 1. Since the other nodes only update their own databases, their memory and Central Processing Unit (CPU) consumption is less than that of Node

TABLE I  
BLOCKCHAIN NETWORK SIMULATION ENVIRONMENT

<b>Host OS</b>	Windows 10 Pro (V21H1)
<b>Guest OS</b>	Ubuntu 20.04.3 LTS on Vmware Pro (2 Cores on VM)
<b>Docker Containers (Under Full Load)</b>	Node 1 (Committer): CPU: 30% Memory Usage: 640 MB
	Nodes 2-3 (Approvers): CPU: ~ 9% Memory Usage: ~370 MB
	Nodes 4-6 (Peers): CPU: ~ 11% Memory Usage: ~ 375 MB
<b>CPU</b>	AMD Ryzen 5 Pro 3400G 3.70 Ghz (2 Cores assigned to VM)
<b>Memory</b>	16 GB 2666MHz DDR4 (6 GB assigned to VM)
<b>Blockchain state</b>	Blockchain platform: Quora Total Size (360 MB), Transaction Size (64kB), Average Block Size (25.6 MB), Average Block Time (50 ms)

1. The information contained in the transaction (the size of a single line in the log file) may vary. This may change the duration of the approval process for this transaction.

##### B. Simulation Results

Fig. 3 shows the average distribution of BCN performance values across various SO-related metrics. Fig. 3a shows the number of lines and instantiation time values for different SO-related metrics. The highest number of lines is observed for the total instantiation time logs (since they include all logs), followed by the ROE Retrieve and Core MANO Wrapper logs. Core MANO Wrapper and Total instantiation time logs are practically giving the same instantiation time, which means that the operations performed by the Core MANO Wrapper interacting with the associated Cloudify Core MANO platform are the most time-consuming operation in the overall instantiation process on the 5Gr-SO. These operations are the creation of the required virtual networks in the corresponding edge data centre, the attachment of VMs that implement the VNF, and the creation of these VMs. Among the SOE module operations, the most time-consuming are those that prepare and coordinate the operations of the instantiation process (e.g., Operation ID, Hierarchical SOE dispatching (SOEp-SOEc), Retrieving descriptor from Catalogue DBs). The most time consuming operations in the ROE module are ROE Retrieve RL resources and PA calculation. These operations are part of the process required to select appropriate resources for network service deployment and are performed immediately before Core MANO wrapper operation. From Fig. 3a, we can observe that the number of lines and the corresponding values for the average instantiation time evolve differently. For example, ROE retrieve log generated 1060 log lines (or transactions) during its 40 ms (average) instantiation time interval. In contrast, the core MANO wrapper log generated 323 log lines (transactions) during its 100 s (average) instantiation time

interval. Therefore, if the number of lines is high (e.g., ROE retrieve logs), the corresponding instantiation time could be low. On the other hand, if the number of log lines is lower (e.g., Core MANO Wrapper logs), the corresponding instantiation time could be high.

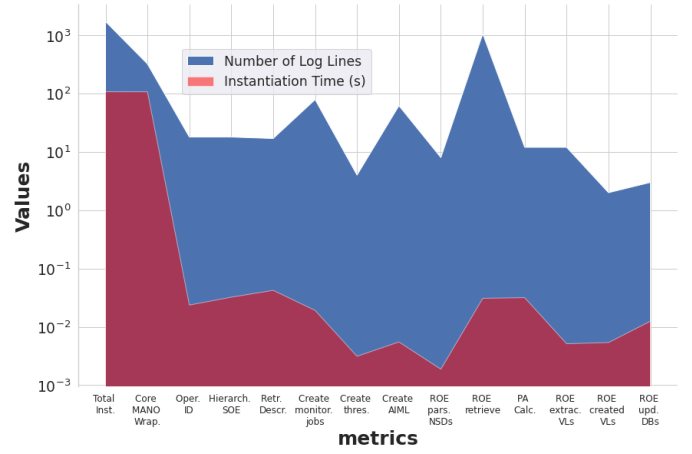
Fig. 3b shows the average number of transactions, the average time to write to the ledger, and the average number of blocks created for the SO-related metrics considered. We see that the values for the average time to write to the ledger and average number of blocks created are consistent with the changes in the number of transactions for all metrics. Thus, compared to the total instantiation values, we can again see that a higher instantiation time (e.g., for Core MANO wrapper logs) does not necessarily lead to a high number of blocks or a high time to write to the ledger because the logs contain fewer lines (e.g., compared to ROE retrieve logs).

### C. Discussions and Evaluations of Results

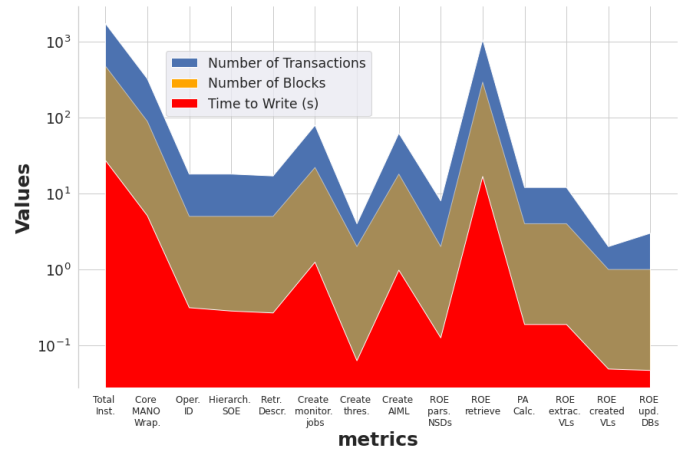
Several conclusions can be drawn from the above evaluation results on service instantiation time and BCN metrics. First, the evaluation results show that certain logs (such as the ROE retrieve log) arrive rapidly and generate a large number of transactions, while others (such as the core MANO wrapper log) arrive slowly and generate a small number of transactions. As a result, some of the logs may be lost if the file reader API of BCN does not handle them appropriately when they arrive quickly. The generation of the logs and the time it takes to write them to the BCN may depend on the speed at which the log is created as service instantiation is ongoing. As a result, there would be a difference between online and offline working modes of log processing by the BCN.

As a solution, a suitable message bus (e.g. Apache Kafka, RabbitMQ, etc.) could be integrated into the BCN to ensure reliability, scalability, and high throughput. Note also that in our analysis, to avoid the memory limitations of BCNs, only the transaction data is stored in the BCN, not the raw data itself. Alternatively, recent solutions such as the InterPlanetary File System (IPFS) (an open-source, content-addressable peer-to-peer network) can be embedded in BCNs to store relatively large data on demand. In addition, the scalability of the BCN-based MANO solution can be improved by parallelizing as many steps as possible (including endorsement policy validation), caching transaction data, designing a hierarchical BCN structure so that multiple autonomous subnets can be accommodated, sharding BCNs to distribute the workload across different nodes, off-chain scaling or allowing aggregated interactions to be stored rather than redundant trust information that could overload the network in the long run [13].

Second, the granularity of log reading can be critical in a multi-cloud environment. To limit the number of transactions, not all logs need to be sent to PDL, but in some cases only the most important ones. The reason for this is that each transaction has to be confirmed within the BCN (e.g. by a digital signature), which adds overhead. With a larger number of transactions, it takes longer to write to PDL, resulting in a higher latency value that must be carefully considered when providing latency-sensitive network services. However,



(a)



(b)

Fig. 3: Line plots for different SO metrics showing the distribution of (a) Number of lines and average instantiation time (b) Average number of transactions, average time to write and average number of blocks generated.

depending on requirements, the time to write to the ledger can be reduced at the expense of a lower level of security if no transaction validation is required before putting into PDL.

The third conclusion is that it is crucial to follow network service provisioning procedures in the exact order to achieve synchronization between CSPs and SPs. For example, when instantiating a service, one CSP may perform a step after another CSP has completed a corresponding step. Hence, to successfully adhere to the instantiation schedule, it is critical to write the logs to the blocks in the correct order.

## V. STANDARDIZATION ROADMAP

There are several efforts around the world aimed at defining both network service management/orchestration and



BCN technologies. However, they are being worked on separately. European Telecommunications Standards Institute (ETSI) NFV-MANO is one of the major standardization bodies for network service management and orchestration. ETSI NFV ((IFA028 and IFA030) for multi-domain and IFA007/8) has already defined various MANO procedures for VNF LCM operations defined (e.g., for instantiation, termination, scaling, migration/reallocation). Several architectural options are also provided to support collaborations between multiple federation domains.

On the other hand, research on BCNs has been going on for decades. However, standardization work dealing with them, is more recent. The EU has already begun consolidating efforts to standardize blockchain for various use cases. A forum and working group have been established to accelerate blockchain innovation and the development of the blockchain ecosystem in the EU. A recent report highlights the applicability of smart contracts for 5G and beyond.<sup>3</sup> Some SDOs working on or recommending the adaption of distributed ledger/blockchain technologies are: the International Telecommunication Union (ITU) (ITU-T Focus Group on Application of Distributed Ledger Technologies (FG DLT) [14]), the National Institute of Standards and Technology (NIST) (NISTIR 8202 document<sup>4</sup>), ANSI Accredited Standards Committee X9, International Organization for Standardization (ISO) (ISO TC 307's work on ISO/TR 23455 document), IEEE Blockchain initiative<sup>5</sup>, The EU Agency for Cybersecurity (ENISA), ETSI on PDL Landscape of Standards and Technologies and the European Committee for Electrotechnical Standardization (CENELEC).

At the same time, application of BCN technologies in mobile networks and services, especially in multi-domain networking is still new, and standard BCN interfaces, detailed use cases, and operational requirements for interaction with network MANO systems have yet to be defined. However, the open source software ecosystems of both MANO (e.g., OSM, Cloudify) and BCN technologies (e.g., Quorum, Ethereum, Corda, Ripple and Hyper ledger) are, however, in favor of accelerating the convergence of these technologies in future standardization releases. Additionally, post-quantum cryptography measures should be considered as part of standardization to replace existing security standards in BCNs and ensure security and reliability [15].

## VI. CONCLUSIONS

In this paper, we developed a BCN-based multi-stakeholder network management and orchestration framework for LCM of network services (e.g., instantiation, scaling, termination, migration/reallocation). The proposed solution can provide secure and transparent network services for vertical SPs using the 5Gr-SO platform. The proposed methodology covers a use case for providing ZDM DSS network services that mainly includes different categories of entities including CSPs, MNO,

vertical SPs, responsible ministry, legal authority and regulation authority.

Our evaluation results for network service instantiation have shown that the number of transactions or blocks generated in the used Quorum BCN is not directly related to the achieved service instantiation times for different metrics, and that appropriate adjustments need to be made before BCNs are integrated into the 5Gr-MANO stack of telecommunication systems. At the end of the paper, we also provide some discussion points and recommendations on the evaluation results and standardization roadmap for BCN convergence with MANO stack of telecommunication infrastructure.

## VII. ACKNOWLEDGMENT

This work has been partially funded by EC H2020 MonB5G project (Grant 871780), Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55) and Grant PID2021-126431OB-I00 funded by Spanish MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe".

## REFERENCES

- [1] P. K. Vairam *et al.*, "Towards measuring quality of service in untrusted multi-vendor service function chains: Balancing security and resource consumption," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 163–171.
- [2] HN. Dai *et al.*, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.
- [3] M. A. Ferrag *et al.*, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17 236–17 260, 2021.
- [4] K. Peng *et al.*, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 004–12 020, 2021.
- [5] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1202–1213, 2021.
- [6] R. V. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 29–37, 2018.
- [7] R. B. Uriarte and R. DeNicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 22–28, 2018.
- [8] G. He *et al.*, "Netchain: A blockchain-enabled privacy-preserving multi-domain network slice orchestration architecture," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2021.
- [9] X. Fu, F. R. Yu, J. Wang, Q. Qi, and J. Liao, "Performance optimization for blockchain-enabled distributed network function virtualization management and orchestration," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6670–6679, 2020.
- [10] T. Maksymuk *et al.*, "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.
- [11] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE Transactions on Cloud Computing*, pp. 1–1, 2021.
- [12] J. Mangues *et al.*, "5G-TRANSFORMER service orchestrator: Design, implementation, and evaluation," in *2019 European Conference on Networks and Communications (EuCNC)*. IEEE, 2019, pp. 31–36.

<sup>3</sup>EU Blockchain Observatory & Forum, "Blockchain and smart contracts," <https://bit.ly/3e9WjaD>, Accessed: August-2022.

<sup>4</sup>NISTIR 8202 Blockchain Technology Overview, <https://doi.org/10.6028/NIST.IR.8202>, Accessed: August-2022.

<sup>5</sup><https://blockchain.ieee.org/>, Accessed: Jan.-2022.

- [13] D. G. Putra *et al.*, “Towards blockchain-based trust and reputation management for trustworthy 6G networks,” *accepted for publication in the IEEE Network Magazine*, 2022.
- [14] ITU, “Focus group on application on distributed ledger—d1.3, distributed ledger technology standardization landscape,” *Technical Report, Geneva, Switzerland*, 2019.
- [15] E. Zeydan *et al.*, “Recent advances in post-quantum cryptography for networks: A survey,” in *Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, 2022, pp. 1–8.



**Josep Mangues-Bafalluy** received the degree and Ph.D. degrees in telecommunications engineering from UPC, in 1996 and 2003, respectively. He is currently a Senior Researcher and the Head of the Communication Networks Division, Centre Tecnològic de Telecomunicacions Catalunya (CTTC), Barcelona. His research interests include NFV applied to mobile networks and autonomous network management.



**Engin Zeydan** received his Ph.D. degree in Electrical Engineering from Stevens Institute of Technology, Hoboken, NJ, USA, in 2011. He is currently a Senior Researcher at Centre Tecnològic de Telecomunicacions de Catalunya (CTTC). His research interests are in the areas of telecommunications and data engineering.



**Yekta Turk** received his Ph.D. degree in Computer Engineering from Maltepe University, Istanbul, Turkey, in 2018. He is a Mobile Network Architect based in Istanbul, Turkey. His research interests are in the areas of computer networks and security.



**Jorge Baranda** received the M.S. degree in electrical engineering from the Technical University of Catalonia, in 2008. He is currently a Senior Researcher with the Department of Mobile Networks, Centre Tecnològic de Telecomunicacions Catalunya (CTTC), Barcelona. His current research interests include management and orchestration of SDN/NFV mobile networks, wireless communications, wireless backhaul, network routing protocols, and network optimization.