ABSTRACT
Existing network service provisioning and lifecycle management (LCM) workflows rely on heterogeneous devices from multiple vendors and collaboration between multiple network actors, which can lead to numerous trust management and interoperability issues. Blockchain networks (BCNs) are a revolutionary way to establish trust in untrusted environments. In this complex environment, BCNs can help ensure transparency and security for network service LCM. However, BCNs are also vulnerable to quantum attacks. Advances in quantum computing will challenge the security of existing blockchain technology based on Public Key Infrastructure (PKI) technologies. In this paper, we explore how network services can be managed in a multiple administrative scenario. Our approach uses BCNs to track the operational steps of network service instantiation metrics while benefiting from the security features of post-quantum cryptography (PQC). Together with the use of N-th degree Truncated polynomial Ring Units (NTRU) as an example of a PQC algorithm that relies on the parallelization power of the Toom-Cook computation method with different security levels, we have shown that Quorum can provide a lower average time-to-write value compared to other BCNs considered (Ethereum and Hyperledger). At the end of the paper, we discuss the evaluation results and future directions regarding the coexistence of PQC algorithms and BCNs for network service orchestration and service federation between multiple administrative domains.

INDEX TERMS
Orchestration, mobile operator, post-quantum, network service, blockchain.

I. INTRODUCTION
In cybersecurity, the day when quantum computers can crack the Internet is called Q-Day [1]. Google, Microsoft, IBM, and Honeywell, as well as startups, are already advancing quantum computing and exploring its potential in a range of applications to achieve quantum supremacy. For this reason, the post-quantum era is not a distant future and will likely become a reality within the next few decades. As a defence mechanism, Post-Quantum Cryptographic (PQC) algorithms appear to be impervious to quantum attacks. The National Institute of Standards and Technology (NIST) is already working to evaluate PQC algorithms and recently announced four candidates to be standardized and the fourth round candidates for the quantum-resistant public-key encryption and digital signature algorithms in July 2023.\(^1\)

In parallel with these developments in quantum computing, there is a growing need to create a continuum for convergence between networking, computing and security ecosystems to enable faster, more secure, and better network service provisioning in the telecommunications landscape. In this context, the focus is on developing advanced solutions for network service Life Cycle Management (LCM) to provision and operate new services and applications across multiple administrative domains.
heterogeneous devices and infrastructures (e.g., edge/core clouds). As next-generation mobile networks will offer diverse applications and services, secure orchestration of network services must work even in an untrusted environment. Network service LCM may also require the involvement of multiple entities (e.g., Cloud Service Providers (CSPs), Infrastructure Provider (InP), Vertical Service Providers (SPs), Regulators, etc.) depending on the type of network service and the characteristics of the geographic location of the network service under consideration. However, this also presents significant challenges for the unified management and orchestration of networks at the network edge and cloud infrastructures that may be owned or managed by multiple administrators (e.g., different InPs operating in a federated deployment scenario). One of the biggest challenges in these environments is the lack of cooperation between entities and, in the case of collaboration, the lack of accountability, which can lead to network security issues.

In this paper, we investigate the performance of post-quantum Blockchain Network (BCN)-based mechanism in the context of network service orchestration for multi-domain scenarios in the envisioned next generation cellular networks. The goal is to provide an architecture that combines BCN and PQC to orchestrate multiple heterogeneous entities for network service LCM and provision and operate new services and infrastructure. The main contributions of the paper can be summarized as follows:

- We propose a blockchain-based network management methodology that relies on quantum-resilient security algorithms to embed an efficient trust model between network service providers for the network LCM.
- We consider a scenario for a network management and orchestration system that mainly includes different categories of entities: a) CSPs; b) InP; c) vertical SPs; d) regulation authority.
- We use the Service Orchestrator (SO) logs of the 5Growth (5Gr) project’s Management and Orchestration (MANO) stack\(^2\) to compare different BCNs and computation methods in PQC through simulations.

The remainder of the paper is organized as follows: Section II presents the related work on network service security and potential attacks from quantum computers on blockchain networks. Section III explores the proposed blockchain-based service orchestration architecture in the post-quantum era. Section IV explores the mechanism of service orchestration, the role of the Distributed Ledger Technology (DLT) and the advantages of the BCN-based MANO. Section V provides the evaluation results of the considered setup and related discussions. Finally, Section VI provides the conclusions of the paper. A list of abbreviations used in this paper can be found in Table 1.

\(^2\)Online: https://5growth.eu/, Accessed: April-2022

| Acronym | Full Text |
|---------|-----------|
| 5Gr     | 5Growth   |
| 5Gr-VS  | 5Growth Vertical Slicer |
| 5Gr-SO  | 5Growth Service Orchestrator |
| 5Gr-RL  | 5Growth Resource Layer |
| 5Gr-VoMS| 5Growth Vertical-oriented monitoring system |
| AOV     | Automated Guided Vehicle |
| AOVc    | AOV controller |
| AI      | Artificial Intelligence |
| API     | Application Programming Interface |
| AWS     | Amazon Web Services |
| BCN     | Blockchain Network |
| CMM     | Coordinate Measuring Machine |
| CSP     | Cloud Service Provider |
| DB      | Database |
| DLT     | Distributed Ledger Technology |
| DSAC    | Digital Signature Algorithm |
| ECC     | Elliptic Curve Cryptography |
| ECDSA   | Elliptic Curve Digital Signature Algorithm |
| IaaS    | Infrastructure as a Service |
| InP     | Infrastructure Provider |
| IoT     | Internet of Things |
| IT      | Information Technology |
| GCP     | Google Cloud Platform |
| LCM     | Lifecycle Management |
| LL      | Logical Link |
| MANO    | Management and Orchestration |
| MPI     | Message Passing Interface |
| ML      | Machine Learning |
| MVNO    | Mobile Virtual Network Operator |
| NRI     | Northbound Interface |
| NIST    | National Institute of Standards and Technology |
| NS      | Network Service |
| NSD     | Network Service Descriptor |
| NSIR    | Network Service Instantiation Resource |
| NTRU    | N-th degree Truncated polynomial Ring Units |
| ONAP    | Open Network Automation Platform |
| OSM     | Open Service MANO |
| OTT     | Over-The-Top |
| PA      | Placement Algorithm |
| PaasS   | Platform as a Service |
| PDL     | Permissioned Distributed Ledger |
| PKI     | Public Key Infrastructure |
| PoS     | Proof-of-Stake |
| PQC     | Post Quantum Cryptography |
| QRSA    | Quantum Resistant Security Algorithms |
| RL      | Resource Layer |
| ROE     | Resource Orchestration Engine |
| RSA     | Rivest–Shamir–Adleman |
| SaaS    | Software as a Service |
| SLA     | Service Level Agreement |
| SO      | Service Orchestrator |
| SOE     | Service Orchestration Engine |
| SOEc    | Service Orchestration Engine child |
| SOEp    | Service Orchestration Engine parent |
| SP      | Service Provider |
| VIM     | Virtual Infrastructure Manager |
| VNF     | Virtual Network Function |
| VL      | Virtual Link |
| VNFQ    | VNF Descriptor |
| VoMS    | Vertical Oriented monitoring system |
| VM      | Virtual Machine |

Table 1. Acronyms and their corresponding full text used throughout the paper.
II. RELATED WORKS

A. NETWORK SERVICE SECURITY AND INTEGRATION OF BLOCKCHAIN INTO SERVICE ORCHESTRATION

A secure network LCM allows multiple InPs to dynamically offer their network services to SPs, enabling better business models with optimal use of network resources (e.g., by using Artificial Intelligence (AI)-based Virtual Network Function (VNF) placement algorithms) that can offer a lower price to SPs and a higher profit to InPs and other administrative domains [2], [3]. Therefore, secure and transparent network service orchestration across multiple administrative domains is one of the most important requirements for the telecommunication infrastructure, especially in the future post-quantum era in terms of user service value and profitability of InPs.

BCNs, a type of DLT, and smart contracts are seen as a disruptive technology that can bring several benefits (e.g., trustworthiness, tamper-resistance, decentralization, possible interaction between untrusted parties) to telecommunications and networks, especially in the area of network management [4]. BCNs have immense potential to improve the operation of various aspects of network service management and orchestration, and to extend the use cases of next-generation mobile networks through enhanced security features, decentralized network management, and secure orchestration of network services [5].

The entire process of network service LCM, including instantiation, termination, scaling, and migration/reallocation of services, can be encoded in smart contracts (executable code that enable software agreements between different entities and their deployment on BCNs) to achieve transparent, decentralized, and immutable tracking of network service operations in multi-cloud and multi-domain environments [6]. For example, in the 6G era, BCNs can be deployed to interconnect multiple network domains (i.e., radio, transport, core) and multiple entities (which need to interoperate to provide network services) [7]. BCNs can facilitate collaboration between all parties involved in the orchestrating and managing services (including InPs, CSPs and vertical SPs) to realize service orchestration in multi-administration domains (e.g., with CSP, InP, or Mobile Virtual Network Operator (MVNO)). For example, if a CSP does not comply with the pre-defined Service Level Agreement (SLA) during network LCM operation, this can be easily detected by other entities (e.g., InPs) that manage the service. In this way, transparency can be easily established between multiple entities that do not necessarily need to rely on each other’s operations. However, this trust-building approach can be difficult to achieve, especially in the post-quantum era. In our previous work, we proposed a Permissioned Distributed Ledger (PDL)-based blockchain-supported architecture for a network management and orchestration platform [6]. However, that work did not investigate the impact of PQC on the performance of different BCN platforms.

B. QUANTUM COMPUTERS AND ATTACKS TO BLOCKCHAIN

Quantum computers are capable of solving problems such as the discrete logarithm, which makes cryptographic algorithms such as Diffie-Hellman key exchange, the Digital Signature Algorithm (DSA), and Elliptic Curve Cryptography (ECC) insecure. Shor’s algorithm already provides significant improvements in factorization of large numbers, opening vulnerabilities for quantum computing, while Grover’s algorithm can speed up the generation of hashes, making the linking of blocks by hashing less secure [8], [9].

Quantum computers are capable of attacking BCNs, particularly the Proof-of-Stake (PoS) blockchain (e.g., used by Ethereum), using both the Grover and Shor algorithms [10]. BCNs rely on one-way mathematical functions (which are easy to execute on a conventional computer but difficult to compute backwards) to generate digital signatures (to authenticate BCN users) and hash functions (to validate transaction history in the blockchain ledger) are vulnerable to quantum networks [11]. Therefore, the operating principles of BCNs are threatened when quantum computers become fully operational. Recent research shows that quantum machines with 13 million qubits are capable of cracking Bitcoin’s encryption mechanism (SHA-256), and significant advances in the next decade could produce quantum machines with such power [12]. For this reason, new quantum-safe encryption methods are needed to secure BCNs. At the same time, according to the existing knowledge in the literature so far, quantum computing does not pose major challenges to the security of hash functions [13]. Therefore, any efforts to ensure the future viability of cryptographic protocols in the presence of large-scale quantum computing must focus on public-key cryptography. For example, Google Cloud recently announced that [14] they will use one of the PQC algorithms in its internal Application Layer Transport Security (ALTS) protocol against large-scale quantum computing to fully break public-key cryptography algorithms (such as Rivest-Shamir-Adleman (RSA) and ECC) in the future.

PQC algorithms are designed to target both conventional computers and quantum computers. PQC algorithms can be divided into two main parts: (i) Key exchange, where cryptographic keys are exchanged between two entities, and (ii) Digital signature, where the authenticity of digital messages is established. Four dominant research areas on PQC were previously identified by NIST: Lattice-based, Code-based, Multivariate-based and Isogeny-based cryptography [15]. Several of these algorithms had their own advantages and disadvantages. For example, multivariate-based technique provides small signatures compared to lattice-based technique, while it provide lower security and larger public keys compared to lattice-based technique. On the other hand, code-based techniques are mature and secure, but they require too much memory for computation [16]. Therefore, there is currently no post-quantum blockchain algorithm that
offers fast and small key size, short signature size, low computational complexity, and low energy consumption.

In parallel with these developments, NIST has recently identified four algorithms that are candidates for standardization and will be implemented for most use cases: \(^3\) CRYSTALS-KYBER (for key-establishment), CRYSTALS-Dilithium (for digital signatures) and FALCON and SPHINCS+ (for signature schemes). There are various forms of implementation concepts for PQC algorithms [17], [18], [19]. For example, in [17], the authors used a PQC algorithm with the Internet of Things (IoT) system from AirBox to monitor air quality in a integration setup demo. The design of PQC-based BCNs has also been studied in detail in previous works [20], [21], [22], [23].

Previous works in the literature have addressed the convergence of BCN and network MANO framework in the telecommunication ecosystem [6], [24], [25], but there is still room for improvement to bridge the gap between the evolving BCN and MANO technologies especially in the post-quantum era. Our previous work in [26] has also proposed an architecture that combines post-quantum and BCNs, focusing on securing data sharing and minimizing the impact of latency in data transactions across different blockchain-based networks (namely Ethereum [27], Hyperledger Fabric\(^4\) and Quorum\(^5\)) in the post-quantum era. Unlike the method proposed in this paper, the previous work in [26] does not specifically focus on blockchain-enabled MANO frameworks using a realistic application scenario and relevant metrics. To tackle BCN-enabled network services in the post-quantum era, InPs may need to build the complex connectivity between multiple entities (e.g., SPs, CSPs) that relies on the security of PQC algorithms and highly diversified resources. A post-quantum BCN-based service orchestrator will be useful for the network LCM. Although BCN-based service orchestration is an evolving topic [28], its use with PQC algorithms has not yet been discovered. To the best of our knowledge, there is currently no other research showing a post-quantum BCN-enabled mechanism for network service management and orchestration.

**III. BLOCKCHAIN-BASED SERVICE ORCHESTRATION IN POST-QUANTUM ERA**

**A. SYSTEM ARCHITECTURE**

Figure 1 shows the architecture of the network service LCM, which is secured with blockchain and Quantum Resistant Security Algorithms (QRASAs) (or PQC algorithms). In this architecture, there are multiple entities (CSPs, InP, etc.), QRASAs [29] (lattice-based, code-based, etc.), different computation methods (Karatsuba [30], Toom-Cook [31], etc.), BCNs (Quorum, Ethereum, etc.), and MANO-related SOs (Open Source MANO (OSM),\(^6\) Open Network Automation Platform (ONAP),\(^7\) Kubernetes,\(^8\) etc.). Note that considering all factors, it is not easy to choose an appropriate BCN, PQC algorithm, computation methods, and SOs for various network service LCM tasks in a multi-administration environment.

The description of the entities involved in the PDL process is as follows:

- **InP** provides compute, storage, and network resources and also manages the BCN. It is also responsible for creating new services based on SP requirements.
- **Vertical SP** can be a vertical industry or an Over-The-Top (OTT) SP. They may deploy IoT devices, sensors, smartphones, cameras for monitoring or smart grid infrastructures and require InP support to provide network connectivity.
- **CSP** offers a cloud-based platform, either Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). In addition to InPs, major cloud providers (Amazon Web Services (AWS), Azure and Google Cloud Platform (GCP)) are also aiming to automate network services. For example, RIFT SO is used to manage end-to-end 5G networks on AWS [32].
- **Regulation authority** is the government-approved regulatory and competition authority for telecommunications. During the network service lifecycle, approval occurs during block commitment between the MANO platform and the regulator.

The transactions in BCN refer to the request for resources of the vertical SP from CSPs and InP (bandwidth, storage), the overall allocation of resources, and the operational steps of the network service LCM as described within the blocks of Figure 1. Note that depending on the use case, many decisions need to be made based on the BCN platform and its performance, node hardware, available resources, computation methods, SO type and required security levels.

**B. MITIGATING VULNERABILITIES AGAINST QUANTUM ATTACKS**

To ensure secure information exchange between entities, BCN relies on a Public Key Infrastructure (PKI) via digital signatures (e.g., Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) signatures). As mentioned earlier, quantum computing could make today’s public key cryptography obsolete. Figure 2 describes the scenario in which a quantum attack occurs on a BCN-based service orchestration architecture. In Figure 2a, Eve can use a quantum computer to attack the transaction, and in Figure 2b, PQC algorithms have been developed to prevent Eve’s quantum attack. The system can be divided into the following three phases:

---

1. Online: [https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4](https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4), Accessed: October-2022
2. Online: [https://www.hyperledger.org](https://www.hyperledger.org), Accessed: October-2022
3. Online: [https://consensys.net/quorum/](https://consensys.net/quorum/), Accessed: October-2022
4. Online: [https://kubernetes.io/](https://kubernetes.io/), Accessed: October-2022
5. Online: [https://osm.etsi.org/](https://osm.etsi.org/), Accessed: October-2022
6. Online: [https://onap.org/](https://onap.org/), Accessed: October-2022
7. Online: [https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4](https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4), Accessed: October-2022
8. Online: [https://consensys.net/quorum/](https://consensys.net/quorum/), Accessed: October-2022
1) In the approval phase, each validator on PDL is responsible for approving the network service request of the vertical SP by committing certain resources required to establish the network service. This phase is vulnerable to quantum attacks due to the use of modern public key cryptosystems.

2) In the transaction phase, a candidate block representing transactions is generated. However, validation of these transactions is not yet complete. The network service LCM data is transferred between SP and the MANO stack, which is owned by InP. This transaction data in the candidate block is also vulnerable to
quantum attacks as both entities use asymmetric encryption methods such as RSA, ECC, etc. along with their private/public keys.

3) During the block commit phase between InP and the regulation authority, hashing is used to authenticate the signatures and append the new blocks to each participant’s BCN. Note that, hash functions here are less vulnerable to quantum attacks [13], [33]. Moreover, quantum resilient signature schemes can also help mitigate the impact [16]. For this reason, the security risk in this phase is minimal compared to the previous phases.

Considering the above phases, securing all phases of BCN is crucial and their cryptographic security level should be improved by developing PQC algorithms against quantum attacks to replace modern PKI. The PQC algorithms in the NIST competition use high-order polynomial multiplications. Various multiplication methods such as Karatsuba [30], Toom-Cook [31] can help reduce the computational load when using PQC algorithms. These methods allow efficient multiplication operations to reduce the time complexity as the degree of polynomials increases [5] which are also used in this paper.

IV. POST-QUANTUM BLOCKCHAIN SERVICE ORCHESTRATION MECHANISM

A. NETWORK SERVICE MANAGEMENT AND ORCHESTRATION OPERATIONS

The network service LCM deals with operations such as onboarding a network service (registering it in the catalogue), instantiating, scaling, updating or terminating network services. In this paper, we are interested in the process of instantiating network services. These processes require interaction between all layers of the MANO architecture (we use the three-layer 5Gr-MANO platform in this paper). Inside 5Gr-MANO platform, there are mainly four components: The 5Growth Vertical Slicer (5Gr-VS) acts as entry point for verticals to request a custom network slice. The 5Growth Service Orchestrator (5Gr-SO) provides both network service and resource orchestration capabilities in order to instantiate network slices within and across multiple domains. The 5Gr-SO hosts all the compute, storage and networking physical and virtual resources where network slices and end-to-end services are executed. The 5Growth Vertical-oriented monitoring system (5Gr-VoMS) allows monitoring of vertical services. A schematic diagram of those components is also given in Figure 3. The functionalities of each service instantiation metric are explained below.

- **Total instantiation time**: The time elapsed since the 5Gr-SO created the service identifier for a network service until it is fully instantiated.
- **Operation ID for Instantiation Op**: The time taken for the Northbound Interface (NBI) to generate an ID to identify the instantiation operation.
- **Hierarchical Service Orchestration Engine (SOE) dispatching**: The time used by the hierarchical SOE to select the appropriate instantiation process based on the type of service (single Network Service (NS), composite NS)
- **Retrieving descriptor from catalogue Database (DB)**: The time to collect the descriptor from the Network Service Descriptor (NSD) catalogue
- **Resource Orchestration Engine (ROE) parsing NSD**: 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 Resource Layer (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 response.
- **ROE extract Virtual Link (VL)**: The time taken by ROE to determine the request of the various VLs requiring resources in the Logical Links (LLs) because connected VNFs were deployed in multiple Virtual Infrastructure Managers (VIMs).
- **ROE created VLs**: Time in interaction between ROE and RL to allocate resources in the LLs based on the ROE extract request.
- **ROE updating DB**: Time to update the DBs to declare the NS as operational and the instantiation operation as successful.
- **Create monitoring jobs**: Time 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-Vertical Oriented monitoring system (VoMS), and the interaction to configure them and obtain the associated object identifiers and update the information in the Network Service Instantiation Resource (NSIR) DB.
- **Create threshold based alerts**: Time interaction between the SOE-SLA Manager modules of the 5Gr-SO to determine threshold-alert objects (when there is no AI/Machine Learning (ML) treatment) to be configured at the 5Gr-VoMS, and interact to configure them at the 5Gr-VoMS and obtain the associated object identifiers and update the information in NSIR DB.
- **Create AIml alerts**: Time interaction between SOE-SLA Manager to configure AI/ML workflow to control scaling operations. Data engineering pipeline creation and configuration consists of: i) interaction with 5Gr-VoMS to create a Kafka Topic, ii) interaction with the 5Gr-AIml platform to download the required model, iii) creation of an inference job at Apache Spark, iv) updating NSIR DB.
- **SOE time**: The time spent in the SOE module (both at the SOE parent (SOEp), 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 supports the VLs, the Virtual Machines (VMs) that support the VNFs, and to update the NSIR DB.

Network service provisioning can be a very large and complex process and involves a lot of effort and cost for a single InP. The network service federation mechanism, on the other hand, can be used to transfer some of these tasks from an InP to CSPs. For example, InPs may prefer to move some service provisioning tasks to the cloud infrastructure (that meets compute and storage requirements) owned by CSPs. After the entities are registered in the system, they perform transactions through the BCN related to the operational steps. Note that these steps can now be observed or verified by all participating entities, which adds transparency to the system.

B. THE ROLE OF PERMISSIONED DISTRIBUTED LEDGER

In public PDLs, all entities involved in the process of providing network services can read the logs, but only a few are authorized to add or modify them. However, in our scenario, we assume a private PDL designed for network service LCM operation logs that require read and write permissions. Therefore, read-only or read and write permissions are strictly regulated by the network governance and privacy compliance can be enforced with strict access management.

To ensure traceability and prevent collusion between CSPs, the PDL scheme ensures that network service LCM operation updates are agreed upon by each participating entity and conform to a set of rules (i.e., SLAs) that have been previously established. This type of PDL is appropriate for the use case considered in this paper as access rules can be fine-grained and tailored to the requirements of each entity involved in the network service provisioning process. Furthermore, the visibility of service provisioning logs can be restricted to a predefined group of participants. For example, mutual coordination between InPs can be performed with a private PDL without scaling restrictions.

C. POST-QUANTUM BCN-BASED MANO BENEFITS

The goal of the proposed post-quantum BCN-based network service MANO platform is to enable optimized network service deployment in a secure and controlled manner (i.e., based on providing access to network services depending on the established agreements between multiple entities). This can provide significant benefits to both InPs and SPs. First of all, the interaction between cross services on multiple domains is improved since all necessary operational steps are defined in PDL. This makes it easier to track progress on services such as building mission-critical networks.

Second, SPs and InPs will be able to securely extend their services through federated service offerings from other providers. SPs will also benefit from lower costs as they will need to purchase less network equipment for federated services. This will be critical for futuristic beyond 5G and 6G services with stringent and diverse network requirements.

Third, the flow of operational steps during network service provisioning between different entities will be traceable to meet network service operation auditing requirements. Therefore, all this information generated by each CSP and InP can be added to the BCN for operational information verification.

V. EVALUATIONS

We consider the Connected Worker: Augmented Zero Defect Manufacturing (ZDM) Decision Support System (DSS) use case that was studied in the 5Gr project. The operational logs used for the analysis in PQC-based BCN are from the 5Gr project and are based on the interaction of the 5Gr architecture. Note that the considered use case is based on a network service that allows Automated Guided Vehicle (AGV) to operate in a factory environment. The goal is to semi-automate the measurement process through communication between the AGV controller and the Coordinate Measuring Machine (CMM) (or 3D-scanner machine).

Figure 3 shows the schematic diagram of the proposed blockchain-based network management methodology applied to Connected Worker: Augmented ZDM DSS scenario in the post-quantum era where PQC-based BCN is interacting with 5Gr-MANO stack. In this use case, both the AGV controller and the CMM controller VMs are deployed in the cloud-edge using the 5Gr MANO platform. The AGV is connected to a separate 5G Customer Premise(s) Equipment (CPE), which enables full mobility of the device. The AGV controller (AGVc) application runs on the datacenter servers. The AGV sends information to the AGVc VM and the application controls the movement of the AGV.

In the use case under consideration, an AGV brings the pieces to the scan area, which is placed in the same room as the CMM. A CMM system can be remotely controlled and perform the metrological data processing and analysis using 5G network and 5G core functions. Loading the inspection program for the CMM is automated while an AGV transports the piece to be measured from the production line to the measuring station. There is communication between the AGVc and the robot link. When the AGV moves the part to the desired position for scanning, the AGVc sends a command to report this to the CMM controller VM. Then the robot link commands the CMM to begin scanning. When scanning is complete, the robot link communicates this to the AGVc, which instructs the AGV to move again and take the part to another location. More details on the implementations can also be found in [34]. In addition, the corresponding document of [35] provides further details about the network service.

A. IMPLEMENTATION SETUP

BCNs are implemented using Hyperledger Fabric (an open-source permissioned blockchain), Ethereum, and Quorum.

9Online: https://github.com/ethereum, Accessed: November-2022
10Online: https://consensys.net/quorum/, Accessed: November-2022
The BCNs and nodes run in Docker containers. The simulations are run over a blockchain network with a size of five nodes (three nodes for the approval process) each with five central processing unit (CPU) cores. The block size is identical for Hyperledger and Ethereum. In the Quorum network, the block size is not configured and the block creation time is set to 50 ms, which means that after 50 ms, a block is created with the current number of transactions. Since we set all BCN platforms to similar configurations, the size of metadata in a transaction is set to 1 KB for all three blockchain platforms. 5Gr-SO is used to provide both network services and resource orchestration capabilities (e.g., instantiation of network slices within and across multiple domains).

We used the Toom-Cook computation method with parallel programming (Message Passing Interface (MPI) for Python) over five CPU cores as a post-quantum computation method. We did not use Karatsuba’s method due to the availability of resources in the cloud environment, as Karatsuba’s method works better without parallelization and with only one CPU core. The PQC computation applications are implemented in Docker containers on the nodes and in another container. The running QRSAs in the NIST competition generally use polynomials whose degree varies between 256 and 512. For this reason, we evaluated the product of two polynomials of degree 512 (security level three) and 821 (security level five). The reason for this choice is that using the Toom-Cook computation method for N-th degree Truncated polynomial Ring Units (NTRU) (a lattice-based public key encryption algorithm whose keys consist of polynomials with integer coefficients), the highest-order polynomial multiplication is of degree 821. Note that the performance of post-quantum computation methods may also depend on the implemented and optimized hardware.

Each experiment consists of ten trials and each metric is calculated as an average over all trials. Instantiation time represents the 5Gr-SO related metrics for instantiation operations as given in Section IV. Time to write is the sum of approval time, transaction time, and block commit time. To obtain performances of BCNs, we used offline 5Gr-SO data logs without loss of generality. A file reader Application Programming Interface (API) is used to transfer data to the BCNs, selecting each line per log until the end.

The details of BCNs state are as follows: Average block size is 25.6 MB and the average block time 50 ms. The blockchain size is about 360 MB for all the tests we performed. Quorum transaction size is 64 Kb. Since we are using PDL, there is no miner and since we do not have mining, we do not have hashrate or reward per block values. We assumed there is no consensus algorithm or reward mechanism during the block commit stage, since there is only one regulator available, whereas multiple regulators are possible in the context of this study. For both the network service instantiation time results and the comparisons of BCNs with Toom-Cook computation method, the experiments were conducted with 10 repetitions.

B. RESULTS

Figure 4 shows the number of log lines and average instantiation time for various SO metrics. The results in this figure show that there is no direct correlation between the number of lines in the log files and the SO instantiation time.
For example, the ROE retrieve logs have a low instantiation time (about 0.031 s) but a large number of log lines (about 1060). On the other hand, the Core MANO Wrapper operation log has a large instantiation time (about 107.48 s) and a small number of log lines (about 323). Figure 4b shows the average time to write for the Toom-Cook computation method on five CPU cores under multiplication of two polynomials with degree 512 for different BCNs and SO metrics. We can see that the distributions are the same for all considered BCNs and correlate with the number of log lines in each log as given in Figure 4. However, among all the considered BCNs, Quorum has lower average time to write values (e.g., approximately 27.23 s for total instantiation time) and Ethereum has the highest values for time to write (e.g., approximately 95.29 s for total instantiation time) among the various SO metrics for instantiation. The performance of Hyperledger BCN is between Quorum and Ethereum.

Figure 5 shows the average time to write comparisons of different BCNs for the Toom-Cook computation method running on five CPU cores under two multiplications of two polynomials of degree 512 and 821, and the corresponding 95% confidence intervals of each experiment. The results are obtained from the logs of the total instantiation time. The average time to write for the Toom-Cook computation method with degree 821 is 19%, 67%, and 33% higher than the Toom-Cook computation method with degree 512 in Ethereum, Quorum, and Hyperledger BCNs, respectively.

C. DISCUSSIONS

The transition to the post-quantum era will be slow, given existing systems, infrastructure, and cybersecurity considerations. Moreover, it will take years to formalise, develop and standardise the most appropriate PQC algorithms for practical next-generation communications and related applications. For this reason, it is expected that post-quantum and existing encryption algorithms will be deployed together before the new algorithms are widely used. Currently, most PQC solutions require more CPU cycles, runtime memory, and a larger key size compared to existing cryptographic algorithms. This, of course, has implications for the communication protocols used in the telecommunications infrastructure. However, as PQC standardization matures, a clear roadmap for the telecommunications sector will also emerge [8].

In our experiments, the time to write values for the total instantiation logs using Toom-Cook’s computation method under different security levels has shown that the time-overhead introduced by BCN can increase significantly when a higher security level is planned (e.g., a 67% increase is observed in Quorum when switching from multiplication by degree 512 (security level 3) to 821 (security level 5)). However, given the instantiation times observed in our use case in Figure 4b, this increase may not be significant for some operations, depending on the considered network LCM use case (e.g., mission-critical services). Therefore, a good trade-off between the use case requirements and the security levels for BCNs must be found.
Moreover, a higher number of log lines and hence a higher time to write values, does not necessarily lead to a higher instantiation time. These results indicate that some logs (e.g., the ROE retrieve log) arrive very quickly and generate a high transaction load, while others (e.g., the core MANO wrapper log) arrive in a longer period of time and generate a small amount of transactions, which must be taken into account when selecting appropriate PQC computation methods.

In the scenario we consider, there is only one regulator to which CSPs and InPs are bound. However, in the approval part of the block commit phase, there may be more than one institution/organization acting as a committer. For example, CSPs may actually be subject to the Information Technology (IT) regulatory authority, while InPs may be subject to telecommunications regulations. In addition, a third audit may be conducted by another entity such as the Department of Justice. In this case, there is more than one committer. The decision to add the transaction in the BCN must be made by consensus. The entire system solution can be complicated if the commit decisions are obtained from each of these institutions individually. In this case, these institutions can form a separate BCN among themselves. This new aggregated BCN will be established to approve requests from MANO (e.g., by consensus). Hence, from the perspective of MANO, a single view of PDL may appear during the block commit phase.

VI. CONCLUSION
Advances in quantum computing and its potential threat (based on Grover’s and Shor’s algorithms) to cryptosystems of BCNs have increased the importance of developing PQCs algorithms in many fields, including the telecommunications world. In this paper, we have made a detailed analysis of the use of post-quantum BCNs for orchestrating network services in the post-quantum world. For reliability and transparency reasons, the network service provisioning logs are published to various PDL BCNs where collaboration between multiple administrative domains is required in a trustless environment.

Together with the proposed post-quantum BCN-based network management and orchestration architecture, InPs can securely manage the life-cycle of the network service provisioning process in multiple administrative or federated domains. To evaluate the performance of the proposed system, we used 5Gr-SO logs and compared different BCNs and computation methods in PQC. Simulation results show that the delay caused by post-quantum BCN varies and that Quorum can be more effective than Ethereum and Hyperledger. In addition, increasing the security levels may increase the time overhead, but this increase can be tolerated when the observed values of the network service instantiation time for different SO-related metrics. On the other hand, these values may need to be reevaluated for certain other use cases (e.g., mission-critical services) that require less time to instantiate the network service.

REFERENCES
[1] D. Castelvecchi, “Preparing for Q-day,” Nature, vol. 602, no. 7869, pp. 198–201, 2022.
[2] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, “QoS and resource-aware security orchestration and life cycle management,” IEEE Trans. Mobile Comput., vol. 21, no. 8, pp. 2978–2993, Aug. 2022.
[3] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, “On multi-domain network slicing orchestration architecture and federated resource control,” IEEE Netw., vol. 33, no. 5, pp. 242–252, Sep. 2019.
[4] T. Matsymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, “Blockchain-empowered framework for decentralized network management in 6G,” IEEE Commun. Mag., vol. 58, no. 9, pp. 86–92, Sep. 2020.
[5] E. Zeydan, Y. Turk, B. Aksoy, and Y. Y. Tasbag, “Post-quantum era in V2X security: Convergence of orchestration and parallel computation,” IEEE Commun. Standards Mag., vol. 6, no. 1, pp. 76–82, Mar. 2022.
[6] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, Y. Turk, and S. B. Ozturk, “Blockchain-based service orchestration for 5G vertical industries in multi-cloud environment,” IEEE Trans. Netw. Service Manage., early access, Jul. 26, 2022, doi: 10.1109/TNSM.2022.3194078.
[7] T. M. Fernandez-Carames and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum attacks,” Springer, 2021, pp. 431–448.
[8] J. Park, N. N. Anandakumar, D. Saha, D. Mehta, N. Pundir, F. Rahman, “Threats Google Cloud, Posted in Identity and Security. [Online]. Available: https://bit.ly/3U2ANUD
[9] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A.-O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, “Post-quantum era privacy protection for intelligent infrastructures,” IEEE Access, vol. 9, pp. 36038–36077, 2021.
[10] A. M. Khalifa, A. M. Baha-Eldin, and M. A. Sobhi, “Quantum attacks and defenses for proof-of-stake,” in Proc. 14th Int. Conf. Comput. Eng. Syst. (ICCES), Dec. 2019, pp. 112–117.
[11] A. K. Fedorov, E. O. Kiktenko, and A. L. Lvovsky, “Quantum computers put blockchain security at risk,” Nature, vol. 563, pp. 465–467, Nov. 2018.
[12] M. Webber, V. Elfving, S. Weidt, and W. K. Hensinger, “The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime,” AVS Quantum Sci., vol. 4, no. 1, 2022, art. no. 013801.
[13] J. Partala, “Post-quantum cryptography in 6G,” in 6G Mobile Wireless Networks (Computer Communications and Networks), Cham, Switzerland: Springer, 2021, pp. 431–448.
[14] ISE Crypto PQC working group. (2022). Securing Tomorrow Today: Why Google Now Protects Its Internal Communications From Quantum Threats Google Cloud, Posted in Identity and Security. [Online]. Available: https://bit.ly/3U2ANUD
[15] G. Alagic, “Status report on the second round of the NIST post-quantum cryptography standardization process,” Nat. Inst. Standards Technol. Interagency Internal, Gaithersburg, MD USA, Tech. Rep., 8309, pp. 1–39, 2020.
[16] T. M. Fernandez-Carames and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” IEEE Access, vol. 8, pp. 21091–21116, 2020.
[17] C.-C. Chung, C.-C. Pai, F.-S. Ching, C. Wang, and L.-J. Chen, “When post-quantum cryptography meets the Internet of Things: An empirical study,” in Proc. 20th Annu. Int. Conf. Mobile Syst., Appl. Services, Jun. 2022, pp. 525–526.
[18] J. Park, N. N. Anandakumar, D. Saha, D. Mehta, N. Pundir, F. Rahman, P. Farahmandi, and M. M. Mehranipoor, “PQC-SEP: Power side-channel evaluation platform for post-quantum cryptography algorithms,” IACR Cryptol. ePrint Arch., vol. 2022, p. 527, Jan. 2022.
[19] J. L. Imana, P. He, T. Bao, Y. Tu, and J. Xie, “Efficient hardware arithmetic for inverted binary ring-LWE based post-quantum cryptography,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 69, no. 8, pp. 3297–3307, Aug. 2022.
[20] H. Yi, “Secure social Internet of Things based on post-quantum blockchain,” IEEE Trans. Netw. Sci. Eng., vol. 9, no. 3, pp. 950–957, May 2022.
[21] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, “A new lattice-based signature scheme in post-quantum blockchain network,” IEEE Access, vol. 7, pp. 2026–2033, 2019.
[22] P. Zhang, L. Wang, W. Wang, K. Fu, and J. Wang, “A blockchain system based on quantum-resistant digital signature,” Secure Commun. Netw., vol. 2021, pp. 1–13, Mar. 2021.
ENGIN ZEYDAN (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from the Department of Electrical and Electronics Engineering, Middle East Technical University, Ankara, Turkey, in 2004 and 2006, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA, in February 2011. He was a part-time Instructor at the Electrical and Electronics Engineering Department, Ozyegin University, from 2015 to 2018. He is currently with the Communication Networks Division, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), working as a Senior Researcher. He is also the Project Coordinator of the H2020 MonB5G European Project. His research interests include the areas of telecommunications and data engineering.

JORGE BARANDA (Senior Member, IEEE) 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 de Catalunya (CTTC), Barcelona. At CTTC, he has participated in several European, national, and industrial projects related to management and orchestration of SDN/NFV mobile networks, efficient routing strategies for mobile network backhauling, and novel wireless communication systems. He has coauthored over 30 different peer-reviewed journals and conference papers. His current research interests include management and orchestration of SDN/NFV mobile networks, wireless communications, wireless backhaul, network routing protocols, and network optimization.

JOSEP MANGUES-BAFALLUY received the Graduate and Ph.D. degrees in telecommunication 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 de Catalunya (CTTC), Barcelona. He has participated in various roles (including leadership) in several public funded and industrial research projects, such as 5GPPP 5Growth, 5G-Transformer, or Spanish 5G-REFINE. He was the Vice-Chair of the IEEE WCNC, Barcelona, in 2018. Previously, he was also a Researcher and an Assistant Professor with UPC. His research interests include NFV applied to mobile networks and autonomous network management.