Article:
Afraz, Nima, Wilhelmi, Francesc, Ahmadi, Hamed et al. (2023) Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. IEEE Access. pp. 95653-95666. ISSN: 2169-3536

https://doi.org/10.1109/ACCESS.2023.3309423

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 August 2023, accepted 22 August 2023, date of publication 28 August 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3309423

RESEARCH ARTICLE

Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis

NIMA AFRAZ[1], (Senior Member, IEEE), FRANCESC WILHELMI[2], (Member, IEEE), HAMED AHMADI[3], (Senior Member, IEEE), AND MARCO RUFFINI[4], (Senior Member, IEEE)

[1]CONNECT Centre, School of Computer Science, University College Dublin, Dublin 4, D04 C1P1 Ireland
[2]Radio Systems Research, Nokia Bell Labs, 70435 Stuttgart, Germany
[3]School of Physics Engineering and Technology, University of York, YO10 5DD York, U.K.
[4]CONNECT Centre, School of Computer Science and Statistics, Trinity College Dublin, Dublin 2, D02 PN40 Ireland

Corresponding author: Nima Afraz (nima.afraz@ucd.ie)

This work was supported in part by the Irish Research Council under Grant GOIPD/2020/333, in part by the Science Foundation Ireland under Grant 14/IA/252 (O'SHARE) and Grant 13/RC/2077, and in part by Google Cloud.

ABSTRACT Blockchain technology offers solutions to numerous network problems by leveraging distributed record-keeping and collaborative decision-making features. However, deployment considerations such as blockchain infrastructure cost, performance requirements, and scalability are often overlooked. This paper provides an in-depth perspective on deploying blockchain-based solutions for telecommunications networks, estimating costs, comparing infrastructure options (on-premises, IaaS, BaaS), and choosing a suitable blockchain platform. To that end, we identify the performance limitations of the proposed solution under various deployment infrastructures by studying two prominent use cases: one proposing a distributed marketplace solution for 5G slice brokering and another one on the decentralization of federated learning (FL) through blockchain. For the slice brokering use case, our experiments showed that sub-second latency could be achieved for a maximum transaction throughput in the range of 10 to 200 transactions per second (TPS), whereas use cases requiring a higher throughput (300 to 400 TPS) would need more computational resources. Meanwhile, the FL use case provided insights into the achievable accuracy of distributed learning under various blockchain settings (public, consortium, and private), which led to the understanding that private and consortium blockchains can achieve acceptable accuracy in significantly lower training times compared to public blockchains.

INDEX TERMS 5G network slicing, blockchain for telecom, blockchained federated learning, blockchain scalability, cloud-native distributed ledger, cost analysis, permissioned blockchain, smart contracts.

I. INTRODUCTION

Modern telecommunication networks have evolved from single-operator systems to heterogeneous ecosystems where many stakeholders are involved in the deployment, operation, and service provisioning. Fifth Generation (5G) wireless radio access networks have accelerated this trend by providing the means for smaller stakeholders to play a role in the telecommunications ecosystem. This is made possible thanks to the network virtualization technology that allows the dynamic (re)allocation of network resources to a small service provider to serve a wide base of customers without owning the physical infrastructure.

The shift in telecommunications ecosystems implies new power dynamics that demand new trust relationships. This trust is traditionally provided by a central trusted mediator [1]. For instance, a small smart city service provider can enter the market and start serving customers almost immediately by acquiring a virtual slice of the network from other operators (who own physical infrastructure in

The associate editor coordinating the review of this manuscript and approving it for publication was Nafees Mansoor.

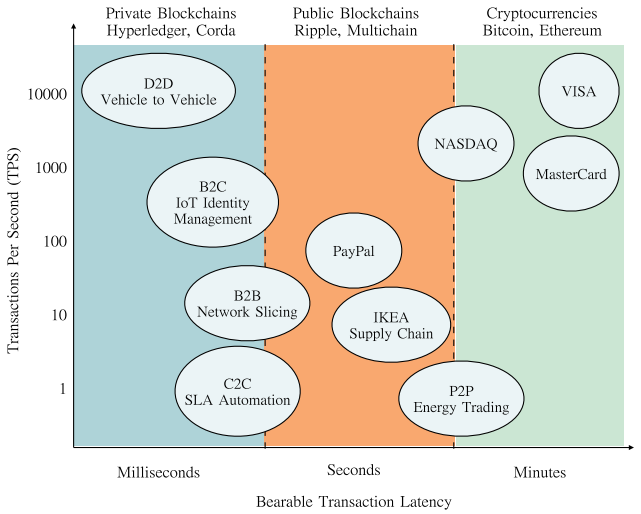

FIGURE 1. Blockchain categories and application areas.

the area). While the need for resources puts the smaller service providers (that do not own network infrastructure) in a vulnerable position, the presence of the central mediator (third party) intends to balance the power in favor of the smaller operators since it cannot be guaranteed for the larger operators to act fairly as a central decision-maker. In other words, the unequal competition between the network stakeholders poses a challenge to the conventional assumption that a central trustee could be trusted to mediate between all the parties. One example of this could be the leverage that larger operators have in influencing standards and regulations at national and international levels.

Blockchain technology, initially developed to address the issue of a single source of trust in the banking industry, is since then being studied to provide the distributed trust needed for the evolving telecoms ecosystems. For instance, the new telecommunications infrastructure ownership models are moving away from business/ownership models (where a handful of network operators governed the entire ecosystem) to a model with many small players with very little leverage to co-exist with larger players. Therefore, the single sources of trust (e.g., regulatory agencies acting as dispute settlement authority in network sharing) are becoming less relevant in the new ecosystem, and distributed alternatives for ensuring trust are required. This is due to the inherent limitations of centralized systems that allow limited scalability and expose the entire ecosystem to issues associated with the single point of failure.

Telecommunications is not the only industry exploiting the potential of blockchain technology to address trust-related issues (refer to Fig. 1 for an overview of blockchain application areas and players). Numerous industries, including pharmaceutical, consumer electronics, health care, and insurance, and their verticals like supply chains and smart cities, have already developed blockchain-based solutions. According to the analysis in [2], the blockchain market is expected to grow up to USD 39.7 billion by 2025.

However, the scalability of blockchain networks remains a major obstacle to the widespread adoption of blockchain-based solutions. Similarly to other fault-tolerant systems, blockchains achieve trust by adding redundancy to the system. For instance, in a centralized resource-sharing marketplace, one authority is in charge of recording the operators' received offers, executing the market mechanism, and recording the outcome on a single database. The equivalent solution in the blockchain would maintain multiple replicas of the records and require all of the operators (or some, depending on the consensus protocol) to execute the market logic and maintain their records of the outcome. Depending on the system's scale, this redundancy can add substantial costs to the operation. In addition to the cost aspect, such redundancy could impose extra latency and limitations on the transaction throughput, compared to a centralized system.

In a blockchain ecosystem, the participating members dedicate a particular share of resources to host the blockchain network components (nodes). These resources typically include computing capacity to execute the smart contracts and the consensus protocol, storage for recording the ever-growing chain of blocks, and the state database and networking infrastructure to allow communication between blockchain nodes belonging to different members. The infrastructure design and provisioning decisions have direct implications regarding the security, trust, and cost of the blockchain ecosystem.

A. CONTRIBUTIONS

In this article, we address two often overlooked key aspects when considering the practical viability of blockchain applications in telecommunications, namely the cost implications (i.e., in terms of capital infrastructure, operational costs, and onboarding) and performance requirements. Therefore, our contributions are as follows:

1) Categorization of various application areas and use cases of blockchain and smart contracts technology.
2) Analyzing and extracting the latency, cost, network scale, access levels, and transaction throughput requirements of the blockchain use cases in telecom.
3) A comprehensive comparison of different blockchain deployment options (e.g., BaaS, IaaS, and on-premises) in terms of monthly cost per member organization.
4) A case study of 5G slice brokering and reporting on the cost analysis of various blockchain deployment options.
5) A case study of blockchained Federated Learning (FL) and evaluation of its performance under various blockchain configurations.

B. BLOCKCHAIN PROS AND CONS

Blockchain technology offers significant advantages [3] in terms of security, transparency, and efficiency. However, similar to other distributed systems, they come at the cost of redundant network and computational resources. For instance, the security brought to 5G networks [4] through

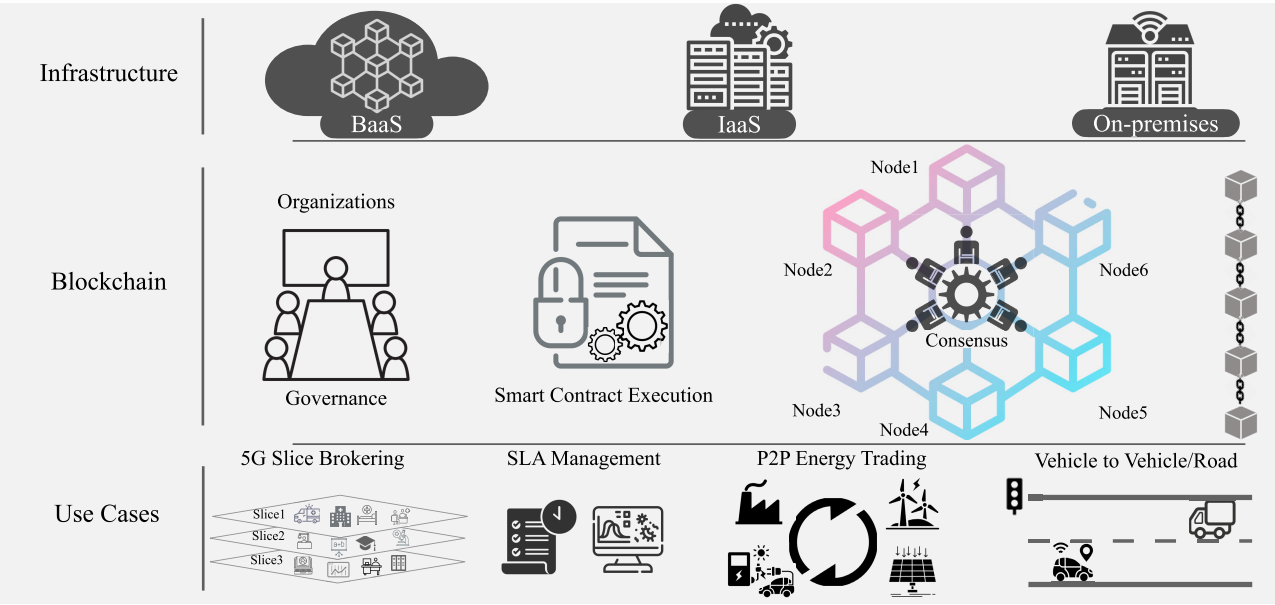

FIGURE 2. Blockchain use cases in telecommunications.

enhancement with blockchain comes at the cost of additional hardware (such as computing, storage, and network access) and operational processes (i.e., the inclusion of the blockchain in the end-to-end service management). In addition, the processing will have to be performed in parallel in many servers rather than in a central server. Similarly, the transparency provided by the immutable and distributed nature of the blockchain ledger entails a more than significant cost to store and process transactions in multiple locations at the edge of the network, rather than in a highly efficient data center. Therefore, the advantages mentioned previously should be carefully weighed against disadvantages such as additional complexity (in the design and operation of blockchains), extra energy consumption, and challenges around the scalability of blockchain-based solutions for 5G networks.

In the next section, we will focus on the main challenge of scalability, which could become a bottleneck in the widespread adoption of blockchain technology in telecommunication networks.

II. BLOCKCHAIN PLATFORMS AND SCALABILITY

Blockchain frameworks are differentiated based on their hierarchical structure, which determines the users' level of access to network governance (admitting new users, changing the consensus protocol, etc.) and the ledger content. Blockchains such as Bitcoin belong to a category called public blockchains since any user (or entity) could join the network, transact (read and write), and also operate mining and verification of the blocks merely by contributing computing resources without the need for permission to join. A second category is that of private blockchains, with a central governing entity enforcing strict limitations on the users who can read, write, and transact on the blockchain. Finally, a third category is consortium blockchains, which propose a middle ground between the public and private blockchains. Unlike a private blockchain, a consortium blockchain is governed collectively by all members but, differently from a public blockchain, such members are identified and need appropriate permissions to join the network.

Public blockchains are different from private and consortium blockchains in that the trust is achieved purely by consensus protocols, e.g., Proof of Work (PoW), that rely on extreme measures such as solving complex cryptographic puzzles. These puzzles are intentionally designed to be so complex that they delay the execution and recording of transactions by minutes. In addition, solving these complex puzzles demands substantial computational and electrical power. A blockchain like Bitcoin consumes 69.37 TWh of electricity per year [5], being a single transaction on the Bitcoin network equivalent to the power that an average U.S. household consumes over 20 days [5].

Although numerous efficient consensus protocols for public blockchain have been proposed (e.g., Proof of Stake (PoS)), none have been widely adopted. In September 2022, Ethereum switched to PoS to replace the PoW consensus protocol to reduce the processing burden of verifying transactions on the network. This is in addition to the cost of hardware infrastructure and related operational costs. Hence, public blockchains are ruled out as a sustainable solution for the majority of telecommunications use cases where latency and costs are vital. On the other hand, private blockchains are also not suitable for telecommunications, as they do not support the distributed feature that is key to removing the need for a central organizer. Consortium blockchains are instead suitable as they present the advantage of reduced

computation requirements while maintaining the support for their users' totally independent operations. Thus, in the rest of the article, we focus our attention on consortium blockchains.

Consortium blockchains achieve trust by controlling users' admissions to the ecosystem (as a collective decision) and distributed record-keeping and logic execution. Hyperledger, Enterprise Ethereum, and Corda are the major consortium blockchain platforms. What is common between them is that they rely on the accountability of the pre-vetted members (since their identity is known to others) and lightweight consensus protocols (e.g., Raft and Byzantine-Fault-Tolerant (BFT)) to achieve trust in the ecosystem. This enables consortium blockchains to overcome most scalability issues. For instance, Hyperledger Fabric can process up to 20,000 Transactions per Second (TPS) [6] while maintaining the transaction confirmation latency below 1 second. When compared to Bitcoin, which has a capacity of about 5 TPS and an average latency of 10 minutes, it becomes clear that permissioned blockchain performs better at scale. The detailed comparison of these platforms is outside the scope of this work and has been previously presented in [7].

III. BLOCKCHAIN FOR 5G AND BEYOND COMMUNICATIONS

Blockchain technology has gained increasing levels of attention in telecommunications since the introduction of smart contracts. A smart contract is an immutable computer program that is designed to automatically execute contractual commitments conditional to the endorsement of the parties involved. Although the adoption of purpose-built cryptocurrency/credits for inter-operator transactions has been largely studied [8], the majority of the blockchain use cases in telecommunications rely on smart contracts technology to solve issues involving trust, security, automation, and identity management.

In this work, we study several blockchain-enabled telecommunications use cases (see Fig. 2) and analyze their scalability requirements, such as the number of users, transaction latency, and transaction throughput (number of transactions processed per second). We choose scalability as the primary factor since, as discussed in Section II, the scale of the blockchain network drives the cost and feasibility of a blockchain application (see Fig. 3).

A. DECENTRALIZED MARKETPLACES

In addition to technological advancements in signal transmission and resource management, modern communication networks have experienced a shift in the network and infrastructure ownership models. This includes a wide variety of verticals and over-the-top service providers that participate in this ecosystem as business entities. Hence, considering such a diverse business ecosystem, traditional centralized trust mechanisms will not be able to provide the new levels of trust required in these environments.

One example of such new network ownership models relates to network slicing in 5G [9]. Network slicing allows

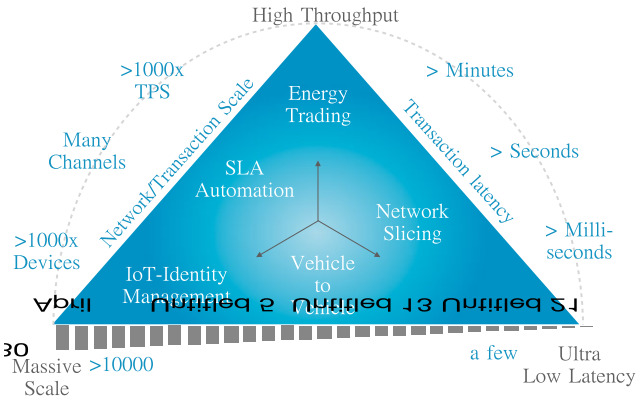

FIGURE 3. Blockchain use cases' KPIs.

the customization of network resources to tenants such as virtual network operators as well as specific services. In an open system, one could envisage a network brokering [10] where infrastructure owners and primary users of the network can trade resources to form network slices, consisting of a variety of network, computing, and storage resources. When initially proposed, such brokering relied upon a central slice broker to make all the trade decisions, including the price and allocation of the slices.

However, the research community soon realized that, in a market of competing network operators, the expectation that all of them should trust a single entity to have full control was unrealistic. Therefore, the authors in [11] have proposed to leverage the collaborative decision-making feature offered by the blockchain smart contract technology to assure trust among the operators and other participants involved in the 5G slice brokering market. Similar proposals for distributed blockchain-based Network Function Virtualization (NFV) marketplaces have been discussed in [12]. Blockchain-based NFV marketplaces enable trust without relying on a trusted third party.

Inter-operator marketplaces will require a blockchain solution to provide strictly controlled access to prevent malicious entities from penetrating the network. In addition, the transactions between operators will need privacy protection. These two requirements are built into the permissioned blockchains (e.g., Hyperledger Fabric), which allow the creation of virtual channels between any number of organizations. As shown in Table 1, the decentralized markets' scale and performance requirements are moderate and readily achievable with common blockchain platforms.

B. SERVICE LEVEL AGREEMENT (SLA) MANAGEMENT

SLAs are contractual agreements between a service provider and parties using the service. Conventionally, an SLA describes in detail the provider's commitments in terms of service availability (e.g., 99.9%) and the corresponding compensation mechanism in case of violation. However, SLAs in inter-operator scenarios could become more sophisticated as other parameters related to Quality of Service (QoS) are

embedded into the agreements. For instance, an SLA between an optical infrastructure provider and a mobile network operator could include commitments of certain latency and jitter thresholds (e.g., $\leq$ 100μs for 95 % of the time) to assure seamless service to the end-users.

One application of blockchain-based SLAs is the neutral host small cell deployment. In this architecture, third parties such as shopping malls, coffee shops, or even private homeowners could participate in the cellular network market by installing small cells on their premises, which could then serve network subscribers on behalf of the mobile operators [13]. The small-cell providers can have contracts with multiple mobile operators or other service providers and vice versa. This means that the parties will have to monitor and comply with multiple SLAs.

Once the terms of an SLA are agreed upon between the small-cell providers and the operators, the enforcement of its terms will depend on a process in which parties to the contract will monitor the compliance of the opposite party (service availability from the provider side and financial commitment from the operator side) based on their measurements and will raise a complaint in case a violation is discovered. If all parties to the SLA verify the pending complaint, the terms defined in the contract (e.g., a penalty or termination) will be automatically enforced [14].

However, suppose a party refuses to adhere (e.g., in case of a measurement/calculation mismatch or contract ambiguity). In that case, the enforcement will depend on a third-party mediator to resolve the dispute. This mediator will introduce additional costs, bureaucracy, and delays in the process. The decentralization of SLA monitoring and enforcement could bypass this bureaucracy by assuring a transparent record-keeping of the measurements enabled by the blockchain technology and use of immutable smart contracts to implement SLAs [14]. Hence, the parties to the SLA will benefit from an automatically enforceable contract without requiring a third-party intermediary. Table 1 depicts the operational requirements of blockchain-based SLA automation.

C. PEER-TO-PEER (P2P) SMART GRID ENERGY TRADING

Internet-connected smart grids offer a sustainable alternative to conventional power grids and enable multi-fold more efficient power distribution. The smart grid uses innovative technologies to integrate green and renewable energy sources into the grid. A new business model has also been introduced to enable this vision where a consumer can also produce (and redistribute) an excess of energy. This new concept is known as the *Prosumer Economy* and relies heavily on a distributed market model to function. In addition to Peer-to-Peer (P2P) energy trading [15], blockchain could facilitate load balancing in the smart grid and enable automatic offsetting of CO_2 emissions, which is challenging to do with the current centralized platforms.

As depicted in Table 1, in the P2P energy trading use case, the scale of network deployment (in terms of the number of nodes) could become a bottleneck, assuming that each prosumer will operate as an individual organization. However, this could be alleviated if several prosumers coordinated together as a group, thus reducing the number of organizations. For instance, specific prosumer groups could be formed based on the type of energy source (wind, solar, etc.).

D. VEHICULAR COMMUNICATIONS

The rapidly emerging Intelligent Vehicle (IV) technology and, more broadly Intelligent Transport Systems (ITS), are expected to reduce road casualties, CO_2 emissions, and improve traffic flow. The IVs achieve this by efficient, fast, and uninterrupted Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. However, such a communication network requires extreme security measures in place as the variety and number of the Internet of Things (IoT) devices connected to such a network are massive. In addition, the identification, authentication, and authorization processes of a vehicle/device that wants to communicate over the network have to occur with low latency to allow immediate decision-making. To realize robust IV data sharing, several major issues remain open, including trust, data accuracy, and reliability [25]. By providing a decentralized data sharing and identity management alternative to conventional third-party reliance, blockchain technology could address these issues. Considering the massive scale of V2V networks, designing a blockchain network to meet their stringent operational requirements (see Table 1) could raise serious obstacles. For instance, in a certain geographical area, thousands of vehicles will need to exchange data with each other and with thousands of other connected road infrastructure components while adhering to strict low-latency limits.

E. IDENTITY AS A SERVICE

Blockchain-based identity management is another application to which network operators are paying attention, as it unlocks appealing use cases such as eSIM, roaming [8], Device-to-Device (D2D) authentication [23], or Identity as a Service (IDaaS) [24]. Blockchain identity ensures security and privacy properties while providing decentralization and transparency to user management operations such as authentication. In particular, the usage of advanced cryptographic techniques such as Elliptic Curve Cryptography (ECC) allows identifying devices and linking them to subscribers' identities (e.g., using eSIMs), which can be useful to replace the existing costly mechanisms whereby International Mobile Subscriber Identity (IMSI) broadcasting is required when a user visits another network. Following an edge-cloud architecture, an identity management blockchain could be deployed to facilitate the identification of users in real time. Through this approach, network operators, verticals, and vendors with heterogeneous network deployments would participate in maintaining the blockchain, registering user authentication requests, and validating and monitoring the provisioning of different services. The blockchain approach

TABLE 1. Cost/performance profile of telecommunications use cases of blockchain.

	Transaction Throughput	Latency Tolerance	Transaction Cost Budget	Network Scale	Access
Decentralized Marketplaces [11]	>10 TPS	>Minutes	High	Few-to-Few	Highly restrictive
SLA Automation [16], [17]	>100 TPS	>10 seconds	Average	Few-to-Many	Restrictive
P2P Energy Trading [18], [19]	>1000 TPS	>A few seconds	Low	Many-to-Many	Moderate
Vehicle to Vehicle [20]–[22]	$>10^5$ TPS	>Milliseconds	Very low	Massive-to-Massive	Restrictive
Identity management [8]–[24]	$>10^5$ TPS	>Seconds	Very low	Massive-to-Massive	Open/Public

would dramatically reduce the overheads associated with user authentication. Besides, thanks to eSIM authentication, the costs associated with manufacturing physical SIM cards would be removed, therefore contributing to enabling massive connectivity as in IoT or Machine-to-Machine (M2M).

The scenarios described in this section (see Fig. 3 and Table 1) represent a fraction of potential blockchain-based use cases involving telecommunications. Having discussed the various performance requirements and the operation scales, we review the available network deployment options for blockchain solutions in the following section. We study each option's pros and cons and present a cost estimation associated with each deployment option.

IV. BLOCKCHAIN DEPLOYMENT OPTIONS

Blockchain technology's strength is its distributed architecture that allows trustable functioning without reliance on a central trustee. This is achieved by enabling an ecosystem of participants, where each contributes resources to serve as blockchain nodes with various roles. This applies to all blockchain applications, independently of the blockchain framework used (Hyperledger, Ethereum, R3 Corda Quorum, etc.). The infrastructure upon which the blockchain application is deployed should provide adequate computing, storage, and network resources for the blockchain nodes to process, store, and communicate transaction information within the network. Similar to other software, there are various deployment options, each having its pros and cons. This section introduces and discusses the main blockchain deployment infrastructure options and provides cost estimation for each.

A. BLOCKCHAIN AS A SERVICE

The Blockchain as a Service (BaaS) market is expected to reach USD 24.94 billion by 2027 [26]. Therefore, many cloud providers are currently competing for a bigger market share by offering BaaS services that are easy to set up, requiring little or no expertise in blockchain implementation. BaaS providers allow blockchain participants to use a graphical interface to design their desired blockchain architecture and to initialize the components using pre-installed containers/Virtual Machines (VMs) and install smart contracts. The resources allocated to blockchain components scales up/down automatically depending on the transaction rate and other factors. Certain threshold alarms can be set to prevent bill shock. Similarly, the participants can use the Graphical User Interface (GUI) to install customized smart contracts on the blockchain.

BaaS platforms have been subject to criticism as their centralized nature goes against the primary aim of blockchain, which is indeed decentralization and disintermediation. In other words, hosting a blockchain network on a BaaS introduces the provider as a third-party entity with considerable control over the software, data, and blockchain governance. In [27], the authors address in detail the issues of BaaS which could undermine the core principles of the blockchain and Distributed Ledger Technology (DLT). The authors raise the following question:

> "If the [BaaS] provider, with its technical security infrastructure, is considered trustworthy, is there still a need for BaaS, or indeed, DLTs more generally? [27]"

The answer is not straightforward as it depends on the level of BaaS provider's intervention in the operational/technical oversight of the blockchain's governance. For instance, typical questions that arise are *who gets to decide whether to admit/remove a member to/from the consortium?* and *whether the BaaS provider would allow members to vote for such blockchain governance concerns*.

Another problem associated with BaaS is that the BaaS providers are usually at the same time general cloud service providers and offer the managed blockchain service only on their cloud. This means that all members of the blockchain will have to use the cloud resources provided by that particular cloud provider, which leads to vendor lock-in. This could be a major obstacle for larger blockchain consortia, as an organization might not be able to migrate its services to a particular provider's cloud due to internal policies or regulatory issues. A more in-depth comparison of the available BaaS platforms has been provided in [38]. The pros/cons of BaaS platforms are depicted in Table 2.

1) MIDDLEMAN BaaS ORCHESTRATOR

The lack of flexibility of BaaS providers in allowing the members to choose their own cloud provider and the consequential interoperability issues have led to the emergence of a new third-party-based BaaS providing model. The middleman BaaS provider acts as an orchestrator and allows the deployment of the services in a broader range of cloud options rather than locking in the members with a particular cloud provider. The middleman platforms provide a

TABLE 2. Analysis and monthly cost of blockchain deployment options.

	Average annual cost (10 Nodes)	Description	Pros	Cons
BaaS	$15,403	AWS $1,408.90 [28] IBM $868.70 [29] Huawei $2,343.30 [30]	• No on-boarding cost for server admin • No on-boarding costs for BC development/deployment • Plug and Play Deployment	• No interoperability (multi-cloud/on premises) • Members are not in charge of BC governance • Limited control over the lower-level BC configuration
Middleman BaaS	$8,388	Kaleido $857.62 [31] Xooa $1,000.00 [32] Chainstack $598.60 [33] Kompitech $899.00 [34]		
IaaS	$5,799 +BC Admin Cost	AWS $453.32 [28] GCloud $533.36 [35] Azure $683.28 [36] IBM $650.00 [29]	• No onboarding cost for server admin • Allows interoperability • Members in charge of BC governance • Lowest cost for hosting BC	• On-boarding costs for BC development/deployment • Higher transaction latency if deployed in multi-cloud
On-Prem	$185,000 + HW Cost + BC Admin Cost + Server Admin Cost	Estimated on-prem cost (5 yrs) *Total Cost of Ownership [37]	• Full decentralization possible (no third-party) • No vendor lock-in • Members in charge of BC governance	• On-boarding costs for server administration and BC development/deployment • High transaction latency in hybrid deployment

*Cost estimations are based on the price calculators available on providers' websites [28]–[37] for two nodes per member (each node 8 vCPUs, 32 GB RAM, and 500 GiB of storage).

similar managed blockchain service to the BaaS. However, each participant can choose their cloud provider (and often on-premises node hosting) among a given number of options. Although middleman BaaS providers offer more flexibility to the member organizations in terms of hosting the blockchain components, the problem of centralized blockchain governance remains an issue similar to the traditional BaaS providers.

B. INFRASTRUCTURE AS A SERVICE DEPLOYMENT

Infrastructure as a Service (IaaS) platforms are another alternative for hosting the blockchain ecosystems. Hosting the blockchain on IaaS allows the member organizations to be in charge of the governance and have the liberty to customize the underlying software and take advantage of the modular architecture of the blockchain platforms. The distinction between the BaaS and IaaS is that the burden of installation, setup, and architecture design of the blockchain ecosystem is on the blockchain members. The blockchain members should put the available infrastructure solutions together, including compute, storage, and access management, to build the blockchain infrastructure. Besides, they should come to pre-production agreements on the blockchain governance guidelines.

IaaS providers offer low-cost service/application hosting to enterprises in comparison to BaaS, while providing the flexibility required for cloud infrastructure interoperability. Hosting a service on a public cloud would free the enterprise from dealing with server maintenance and staff onboarding costs related to the cloud operation. Hence, the number of big enterprises that choose to host a wide range of their services on the public cloud is rapidly growing. It is noteworthy that hosting the blockchain platform in a multi-cloud model might imply higher communication overhead compared to single-cloud BaaS as the servers are not collocated within the same premises (e.g., a data center). Therefore, higher network and consequently transaction latency should be expected. In an IaaS deployment, unlike for BaaS, members have to contribute with blockchain expertise to the ecosystem's design and deployment. The pros/cons of IaaS platforms can be found in Table 2.

C. ON-PREMISES DEPLOYMENT

Certain blockchain stakeholders, such as government agencies dealing with sensitive data, might have to follow strict guidelines regarding data storage. This also applies to private enterprises that have to follow particular regulations or company policies regarding user data. For instance, the General Data Protection Regulation (GDPR) has strict guidelines regarding the hosting and transferring of user data outside of the European Union's European Economic Area (EEA). Therefore, it is expected that some blockchain members will prefer to deploy the ecosystem on the infrastructure available on-premises (off the cloud). This decision will intuitively imply higher Capital Expenditure (CapEx) and Operating Expenditure (OpEx) compared to previously discussed deployment options. Thus, the burden of installation, server maintenance/monitoring, power, blockchain development, and regulatory compliance falls on the blockchain members. Nevertheless, if the member organizations already maintain an on-premises data center, the burden of hosting the blockchain platform might not be substantial. This is because most blockchain platforms can be deployed on general-purpose hardware and operating systems. The pros/cons of on-premises deployment are described in Table 2.

D. EDGE/FOG DEPLOYMENT

Single-board computers are becoming more powerful and at the same time more cost-efficient. These computers are finding more applications in IoT, machine-to-machine communication, and Industry 4.0 [39]. The authors in [39]

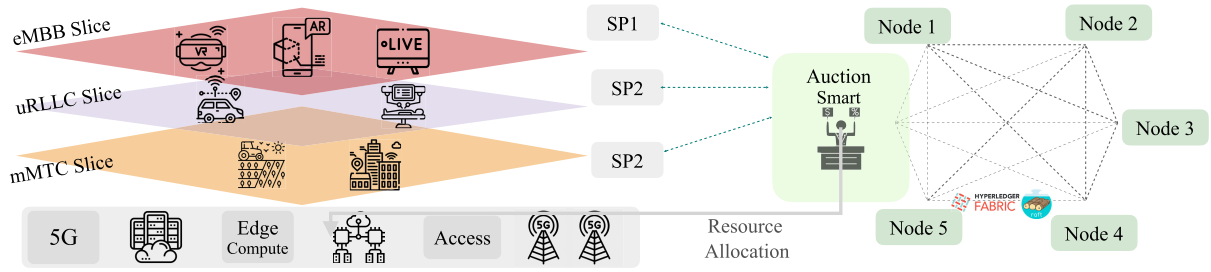

FIGURE 4. Blockchain-Based 5G Slice Brokering Usecase.

perform several experiments on integrating blockchain solutions with IoT architecture where the blockchain node runs autonomously on ARM-based single-board computers while exerting direct access control over IoT devices. While major blockchain software platforms are not ready to be deployed at the network edge, processing transactions closer to the users would offer significant improvements in terms of scalability. For instance, Hyperledger Fabric does not support ARM processors out of the box [40], but the community has been working towards porting the Hyperledger Fabric docker images to work with ARM-based low-cost computers such as Raspberry Pi. The single-board computers can be the computing element of the next-generation blockchain nodes that could reduce the cost and be strategically located to minimize latency.

V. 5G SLICE BROKERING CASE STUDY

In this section, we study 5G slice brokering as a use case that could benefit from a distributed implementation [11] based on blockchain technology. Network slicing in 5G allows the operators to divide the physical network resources and form virtual networks that are tailored to specific requirements. As a result, network operators can provision virtual slices of network resources for specific use cases depending on their requirements. Therefore customized slices of the network could be offered to verticals that do not own network infrastructure.

Figure 4 depicts the idea of network slicing in the context of 5G where applications such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine Type Communications (mMTC) can access network resources from various providers to form their customized slices of the network. In addition, this flexibility will enable new business models. For instance, a vertical that requires network connectivity to serve a wide range of smart IoT devices can source its required network resources across various operators or vendors. Therefore, a new marketplace is formed where verticals and operators can trade *slices* of their network resources. Such marketplaces have been previously proposed in the literature where a broker [41] will mediate this market and match providers of the slice resources to the buyers.

The slice broker [42] uses admission mechanisms or in the case of multi-tenant networks an auction model [43] to decide the allocation of resources to the users. However, these methods are implemented in a centralized manner, where the final decision is made by the central broker (e.g., one of the operators). This centralized decision-making process poses concerns regarding a single point of failure and centralization of power, which will then lead to a lack of trust among the participants of this slicing marketplace. To address the challenges associated with the centralized implementation of the slice brokering mechanism, distributed mechanisms have been introduced in [11], [44], and [45], where the parts or all the decision-making related to the brokering process is taken by a collective of the participants.

The authors in [45] have designed a brokerage mechanism dividing slices to subslice components including computing resources (e.g., CPU, I/O), storage, radio, and transport (e.g., VLAN, VPN) and verified the results using a Python-based simulation. They have performed stress tests on the blockchain scaling up to 20 parallel slice requests submitted by 20 verticals to 50 resource providers. The consensus protocol used in this work is Hashcash, which is similar to Bitcoin's PoW. In [44], the authors have designed a simple one-sided auction mechanism (implemented as a smart contract) in which the highest bidder wins the network slice. The authors then studied the impact of Consortium size (number of network tenants), the consensus protocol (Solo, Raft, and Kafka), and the chain size on the throughput and the latency of the mechanism. However, since the auction algorithm is one-sided, it cannot accommodate scenarios where multiple sellers and multiple buyers are trading.

In this work, we introduce an approach where the auction market mechanism is implemented as a smart contract (chaincode) on a permissioned blockchain (Hyperledger Fabric). This smart contract implements a double-sided auction mechanism that allows multiple tenants to bid for the network slice units (consisting of computing, storage, and RAN resources) provided by multiple resource providers. The matching of sellers and buyers happens in a more sophisticated manner than the mechanism in [44] as our mechanism does not simply sell the slice to the highest bidder. We use the second highest bid (a variant of Vickrey auctions [46]) as the winning bid, therefore, the sellers/buyers do not have the incentive

to represent an untruthful value for the slice. As shown in Fig. 4, each node in the blockchain is associated with a particular service provider and executes a containerized instance of the smart contract. This means that every round of the auction which determines the real-time allocation of resources to slices will be executed and endorsed by all the service providers or other market participants. Hence, the market does not rely on a central broker to execute and verify allocations. The brokering smart contract implements a sealed-bid multi-item double auction [47] which allows sellers and buyers of resources to trade at a fair and transparent market while maximizing the global utility of the market.

The steps of the auction mechanism implemented on the brokering smart contract are as follows:

1) The auction smart contract receives the bids/asks;
2) Sellers and buyers are sorted based on their values (ascending and descending, respectively);
3) Each node calculates the Walrasian equilibrium quantity (the point at which the supply equals the demand at a price affordable for the buyers and agreeable to the sellers);
4) The price is determined by a trade reduction mechanism that will assure truthful price reporting;
5) Finally, the quantity of the items won by each buyer and the price is sent as transactions to get endorsed by all the nodes and be written on the blockchain ledger as blocks.

The bid/ask prices are submitted for a unit of network slice as the auction mechanism only allows for a single type of commodity. Future research could address trading different resources at every round of auction using the Combinatorial auction mechanism [48].

A. EXPERIMENT RESULTS

We perform a set of experiments to identify the infrastructure requirements, performance limitations, and cost of operating the network slice brokering process over the Hyperledger Fabric blockchain platform. The experimental blockchain network is deployed on a public IaaS provider's infrastructure. We run a series of experiments where multiple operators participate in a network slice marketplace equipped with a smart contract (a double auction mechanism) that allows the exchange of network slices without a central broker. We then repeat the same experiments on SUTs with a varying number of organizations (therefore the network size) and network and computing resources available to the blockchain. Each organization is represented by a node on the Hypreldeger Fabric blockchain and is implemented on a separate VM.

The Hyperledger Fabric (version 1.4.1) framework is used to implement the blockchain application. The SUTs consists of one VM instance that hosts Hyperledger Caliper, a benchmark tool designed to measure the performance of blockchains. The blockchain network consists of multiple organizations (operators), each hosting one peer, orderer, chaincode, and certificate authority in their dedicated VM (in a fully containerized environment). Table 3 contains the specifications of each SUT along with their estimated cost of operation. The experiment consists of multiple rounds of benchmarks with varying transaction send rates (from 10 to 400 TPS). For each benchmark, we generate 100,000 transactions (i.e., each transaction performs one round of double auction) and submit them to the blockchain to measure the average transaction latency and transaction throughput.

TABLE 3. System Under Test (SUT) Specifications.

SUT	# Orgs	Nodes' Config	*est.* Annual Cost (USD)
SUT1	2	2 × 32 vCPUs, 28 GB Mem	13,931.04
SUT2	2	2 × 8 vCPUs, 7.2 GB Mem	3,504.36
SUT3	5	5 × 32 vCPUs, 28 GB Mem	34,784.28
SUT4	5	5 × 16 vCPUs, 14.4 GB Mem	17,406.6
SUT5	5	5 × 8 vCPUs, 7.2 GB Mem	8,717.64

*Estimations are based on Google Cloud platform's pricing [35].

Figure 5 illustrates the maximum achievable transaction throughput and the corresponding average transaction latency for the SUTs considered. As expected, SUT1 and 2 (with two organizations) achieve higher throughput (of 400 TPS) compared to SUT 3-5 (with five organizations), which achieve up to 300 TPS. Indeed, the smaller number of organizations means less inter-organization communication as well as fewer nodes that will have to endorse/validate each transaction/block. This also affects the average latency, which remains under one second for SUTs with two organizations. In contrast, for SUT3, the average latency goes above one second at 300 TPS. While authors in [49] recommend that the time-scale envisioned for a 5G network slice provisioning is in the order of minutes, sub-second transaction latency will enable the distributed slice broker to carry out operations in real time.

B. DISCUSSION

It is noteworthy that our case study results should not be generalized to infer the highest possible performance of the Hyperledger Fabric, as they are specific to our smart contract, network/blockchain configuration, and resources available to the SUTs. The performance achieved by our experiments implies that a wide range of previously discussed telecommunications use cases for blockchain, including 5G network slicing, can meet their required performance while taking into account the associated cost. However, utilizing blockchains for more demanding use cases with considerably higher transaction throughput and lower latency tolerance will require further investigation. This also applies to use cases where the per-transaction cost budget is more constrained. Various methods are being studied to improve the performance of blockchains. These include efforts to develop more efficient consensus protocols, Field-Programmable Gate Array (FPGA)-based acceleration, off-chain storage, and sharding.

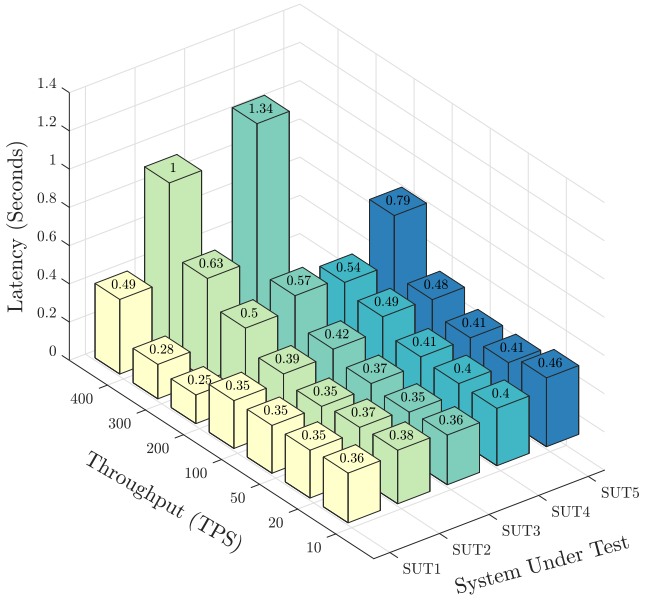

FIGURE 5. Latency and throughput in various SUTs.

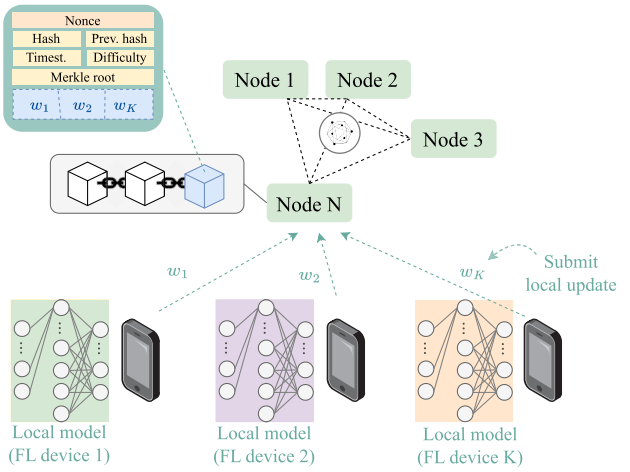

FIGURE 6. Blockchained FL operation.

While such efforts have been proven to substantially increase the reachable throughput of the blockchain (up to 20,000 TPS [6]), the transaction latency remains bounded by inter-node latency/capacity of the blockchain network (some work has been carried out to allow higher transaction throughput in the presence of network delay and network errors [50]). Hence, deploying blockchain on mono-cloud BaaS and IaaS will intuitively outperform the other infrastructure models as the network communication remains inside a data center vicinity. Therefore, a trade-off is formed where the extent of distribution of the blockchain nodes will determine the viability of the use cases with strict ultra-low latency requirements.

While public blockchains might have some application in user-facing use cases such as applications where the mobile operators will use blockchain as their main method of communicating with users or storing user data [51], the majority of the telecommunications industry applications are a better fit for permissioned (consortium) blockchains. This is due to the access control provided by these blockchains. We argue that permissioned blockchains are also a better fit to allow scalability while meeting other requirements of the telecom use cases such as privacy, access control, latency, and flexible deployment.

VI. BLOCKCHAINED FEDERATED LEARNING CASE STUDY

Another appealing domain where blockchain may bring prominent benefits is decentralized Machine Learning (ML). In particular, blockchain can unlock a wide set of next-generation communications applications (e.g., federated cellular traffic prediction [52]) that are based on collaborative intelligence. Through blockchain, several untrusted parties can securely exchange assets (e.g., training and validation data, ML models) and build accurate and trustworthy collaborative models through programmable trust.

In this use case, we focus on FL [53] and its serverless realization through blockchain, i.e., blockchained FL [54]. Under this setting, FL devices exchange ML models through the blockchain, thus eliminating the need for a central orchestrating server. Blockchained FL, compared to traditional FL, boosts decentralization and democratization by offloading the control to FL devices themselves, improves robustness and scalability by removing the single point of failure, and provides rewarding mechanisms for better incentivizing ML model training. The blockchained FL operation is depicted in Fig. 6, where a set of FL devices use a blockchain to exchange ML model updates, which are stored in a distributed, immutable, and transparent manner.

Next, we present a set of experiments that showcase the realization of blockchained FL under different blockchain settings (e.g., public blockchains) and configurations (e.g., block interval), which must be tailored to the needs of the FL use case. For that purpose, we focus on the hand-written digit recognition problem through the EMNIST dataset [55], which has become a standard benchmark for ML. The EMNIST *Digits* dataset consists of 10 balanced classes (written digits from 0 to 9) distributed over 280,000 data samples, of which 240,000 are for training and 40,000 are for validation. For evaluation purposes, we further split the validation dataset into validation (70%, 28,000 samples) and test (30%, 12,000 samples), following a hold-out cross-validation approach.

When it comes to the ML model, we define a Convolutional Neural Network (CNN) with two convolutional and two fully connected linear layers (further details of the model are provided in Table 4). The model has a total of 36,258 parameters and a size of 0.145032 Mbits and is trained across multiple FL devices collaboratively. In particular, federated averaging (FedAvg) [56] is applied as the FL approach for training and aggregating model updates. Furthermore, for the sake of simplicity, every client uses the same training strategy (e.g., Adam optimizer with the same learning rate).

TABLE 4. ML model architecture and parameters per layer.

Layer	Shape
Conv2D	$1 \times 16 \times (5\times5)$
MaxPool2D	(2×2)
Conv2D	$16 \times 12 \times (5\times5)$
MaxPool2D	(2×2)
Linear	192×60
Linear	60×10
Activation (hidden layers)	ReLU
Activation (output)	Softmax

TABLE 5. FL scenario and simulation parameters.

Parameter	Description	Value
N	Total number of FL clients	500
N_m	Number of FL clients per miner	10
R	Total number of sim. blocks	100
E	Number of local epochs	3
B	Batch size	20
o	Optimizer	Adam [60]
η	Learning rate (fixed)	0.01
S^B	Max. block size	{1, 5, 10, 15, 20, 25, 30} TX
T_l	Transaction length	0.145 Mbps
T_h	Block header length	20 Kbits
BI	Block interval per setting	{1, 10, 60} s
M	Number of miners per setting	{1, 10, 50}
C_{p2p}	P2P links' capacity	100 Mbps

In more realistic settings, typical FL scenarios involve heterogeneous deployments where clients have different and varying computation and communication characteristics [57], thus affecting the learning operation. Nevertheless, the focus of the presented experiments is on the blockchain setting, rather than on the optimization of the FL application itself.

For the simulations (the scenario and simulation parameters are collected in Table 5), we have used the open-source tool Block*FL*sim [58], an extension of BlockSim [59] developed to study blockchained FL in detail. In particular, we consider the three following blockchain settings enabling the decentralized federated task:

- **Blockchain setting 1 (BC#1):** A blockchain with an average inter-block time of $BI = 60$ s, maintained by $M = 50$ miners (notice that each miner gathers data from $N_m = 10$ FL devices). This setting characterizes a public blockchain.
- **Blockchain setting 2 (BC#2):** A blockchain with an average inter-block time of $BI = 10$ s, maintained by $M = 10$ miners. This setting characterizes a consortium blockchain.
- **Blockchain setting 3 (BC#3):** A blockchain with an average inter-block time of $BI = 1$ s, maintained by $M = 1$ miner. This setting characterizes a private blockchain.

Figure 7 summarizes the main simulation results obtained in all the different considered settings. In particular, both the FL test accuracy and the number of TPS are displayed in each case. As shown, depending on the blockchain setting and configuration, the performance of the FL model differs. In all the cases, increasing the block size has a positive impact

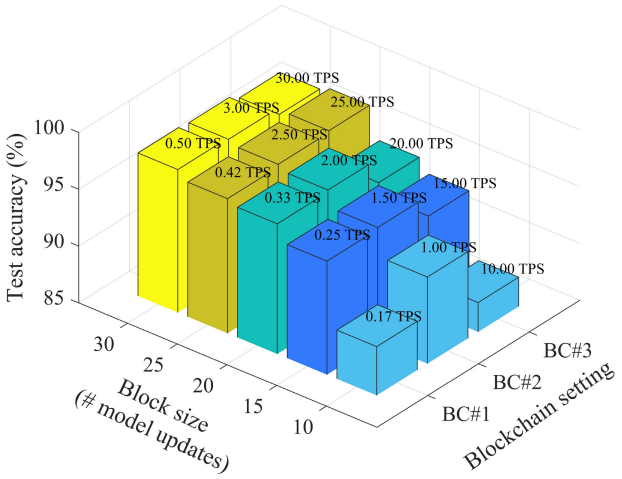

FIGURE 7. Test accuracy achieved by the FL digit recognition application running over different blockchain instances.

on the total achieved accuracy since increasing the block size allows including a higher number of model updates, which is expected to contribute to speeding up the training of the model. Nevertheless, the block size is a critical blockchain parameter to be optimized, as it is closely related to forking [61]. Moreover, for heavy models (e.g., VGG-19 has 39,316,644 parameters, equivalent to 78.63 MB [62]) and massive FL scenarios with thousands of users, using a big block size may lead to performance degradation. When it comes to the blockchain setting, the consortium blockchain (BC#2) is shown to properly address the trade-off between decentralization and performance. In particular, setting BC#2 allows involving a significant enough number of players without leading to severe scalability issues as in BC#1. In such a setting, ledger inconsistencies are notorious (∼10-15% fork probability is observed in the different scenarios) and that has an impact on the number of performed FL rounds as only ML model updates from the main chain are considered.

Finally, to further illustrate the performance of blockchained FL in each setting, Figure 8 shows the validation accuracy observed along the training process, which is monitored from each of the blocks in the main chain. Notice that a total of $R = 100$ blocks is simulated in each case, so the number of blocks in the main chain may vary depending on the approach as a result of the ledger inconsistencies (forks) experienced during the simulations.

As shown in Figure 8, the time that it takes for each approach to reach the 100 blocks diverges significantly, being the public blockchain (BC#1, with $BI = 60$ s) the slowest one and the private one (BC#3, with $BI = 1$ s) the fastest. As for the accuracy observed in each setting, blockchains BC#2 and BC#3 provide the highest performance. In these two settings, a higher control is provided to the entire FL training process thanks to the governance mode of the blockchain, thus allowing it to converge faster. Of course, decentralization and security are paid at the expense of the transaction and

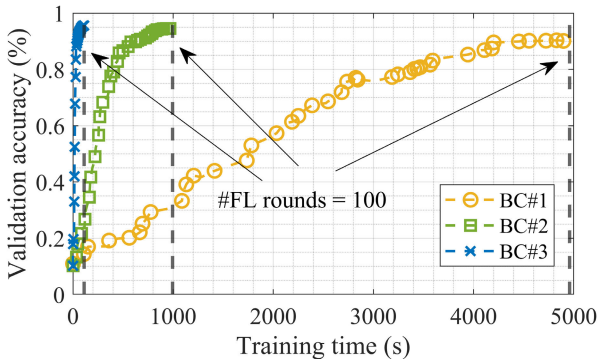

FIGURE 8. Validation accuracy achieved in each blockchain setting throughout the blocks in the main chain, for $S^B = 20$ transactions.

block validation time, but the consortium setting (BC#2) is well balanced.

VII. OPTIMIZATION OF BLOCKCHAIN SOLUTIONS

An optimization framework can be a valuable asset for system designers when architecting blockchain-based solutions for telecommunications use cases. Such a tool can assist in making purpose-fit optimized blockchain solutions that take into account various trade-offs. This includes assessing factors like transaction throughput, latency, scalability, and computing and network resource utilization. In addition, the cost implication of the deployment options (IaaS, BaaS, On-Premises) and Blockchain flavors (Public, Consortium, Private) should be included in the optimization model. Another factor would be the trade-off between security (that determines the consensus mechanism of choice and encryption methods) and performance, which should be a factor in the optimization. However, complexities such as the heterogeneity of telecom use cases, the evolving landscape of the industry, diverse requirements of the various applications, and other constraints make designing a one-size-fits-all optimization framework challenging. Future research work can concentrate on designing a comprehensive framework that encompasses a wide range of parameters and trade-offs for blockchain-based solutions. This framework should identify and catalog various parameters and incorporate trade-off analysis, enabling quantitative modeling to optimize decision-making. This framework should be adaptable to different contexts, accommodating the specific requirements and objectives of telecom operators, vendors, and the guidelines from the regulators. Therefore, designing such a framework is outside the scope of this paper. However, in this paper, we studied two use cases with various requirements using different experimental approaches including prototyping and simulation to exhibit tools and methods to perform such performance-driven cost/benefit analysis.

VIII. CONCLUSION AND FUTURE DIRECTIONS

In this article, we have thoroughly examined the challenges that hinder the wide adoption of blockchain technology in the telecommunication industry, specifically focusing on cost and scalability. Our study has introduced five notable use case areas where blockchain technology can be effectively applied in the telecommunications sector. In addition, we have conducted an in-depth investigation of the functional requirements associated with each use case area, encompassing crucial aspects such as network scalability (e.g., transaction throughput and latency), cost budget, and blockchain access rights.

Furthermore, we have provided valuable insights into the main deployment options available for blockchain solutions, including BaaS, IaaS, and on-premises deployment. Each deployment option has been thoroughly discussed, highlighting their respective advantages and disadvantages. Moreover, we have conducted a detailed inquiry into the realistic cost implications associated with each deployment option, taking into account compliance with relevant regulations that can significantly impact the choice of deployment.

To further enhance our understanding of blockchain application performance and to gain insights into expected performance, we have performed experiments targeting two prominent blockchain use cases discussed in this article: distributed 5G slice brokering and federated learning. These experiments were meticulously designed to simulate realistic production environments, providing valuable information on achievable performance levels with varying network sizes, transaction loads, and computational resources. Throughout these experiments, we have measured transaction throughput and latency, leading to the conclusion that the performance requirements of the slice brokering use case (including an average latency of under 1 second and a throughput of 200 TPS) can be met with reasonable costs. The FL use case provided valuable insights into an additional layer of trade-offs involved in the design and optimization of blockchain-based solutions in the telecommunications industry. Specifically, this use case has highlighted the importance of fine-grained parameter tuning to understand the trade-offs associated with parameters such as block size, batch size, and inter-block times. Initial findings from our research indicate that larger block sizes have a positive impact on the accuracy of trained FL models. However, it remains uncertain whether larger block sizes can be sustained in FL networks with a large number of nodes or ultra-high update frequency of the models. These factors introduce complexities and potential challenges that need to be carefully considered when implementing blockchain solutions for federated learning in telecoms.

The discussions presented in this article lay the foundation for analyzing the cost of deploying and operating blockchain solutions in the telecommunications industry. We have taken into account functional performance requirements as well as regulatory limitations, particularly regarding data privacy. However, it is important to note that further research is necessary to address other challenges, including the development of novel blockchain deployment and optimization frameworks accommodating use cases with massive scales, such as V2V and Internet of Things IoT, while still maintaining a reasonable cost.

REFERENCES

[1] S. Wong, "The fifth generation (5G) trust model," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–5.

[2] *Blockchain Market Size, Growth, Trends and Forecast to 2025 | MarketsandMarkets*. Accessed: Aug. 24, 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

[3] M. Kaur, M. Z. Khan, S. Gupta, and A. Alsaeedi, "Adoption of blockchain with 5G networks for industrial IoT: Recent advances, challenges, and potential solutions," *IEEE Access*, vol. 10, pp. 981–997, 2022.

[4] I. R. Fedorov, A. V. Pimenov, G. A. Panin, and S. V. Bezzateev, "Blockchain in 5G networks: Perfomance evaluation of private blockchain," in *Proc. Wave Electron. Appl. Inf. Telecommun. Syst. (WECONF)*, May 2021, pp. 1–4.

[5] *Bitcoin Energy Consumption Index*. Accessed: Aug. 24, 2023. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption/

[6] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "FastFabric: Scaling hyperledger fabric to 20,000 transactions per second," *Int. J. Netw. Manage.*, vol. 30, no. 5, p. e2099, Sep. 2020.

[7] M. Belotti, N. Božic, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart., 2019.

[8] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A blockchain policy and charging control framework for roaming in cellular networks," *IEEE Netw.*, vol. 34, no. 3, pp. 170–177, May 2020.

[9] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.

[10] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 32–39, Jul. 2016.

[11] N. Afraz and M. Ruffini, "5G network slice brokering: A distributed blockchain-based market," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Dubrovnik, Croatia, Jun. 2020, pp. 23–27.

[12] M. F. Franco, E. J. Scheid, L. Z. Granville, and B. Stiller, "BRAIN: Blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service," in *Proc. IFIP Netw. Conf.*, May 2019, pp. 1–9.

[13] E. D. Pascale, H. Ahmadi, L. Doyle, and I. Macaluso, "Toward scalable user-deployed ultra-dense networks: Blockchain-enabled small cells as a service," *IEEE Commun. Mag.*, vol. 58, no. 8, pp. 82–88, Aug. 2020.

[14] E. J. Scheid, B. B. Rodrigues, L. Z. Granville, and B. Stiller, "Enabling dynamic SLA compensation using blockchain-based smart contracts," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Apr. 2019, pp. 53–61.

[15] F. S. Ali, M. Aloqaily, O. Alfandi, and O. Ozkasap, "Cyberphysical blockchain-enabled peer-to-peer energy trading," *Computer*, vol. 53, no. 9, pp. 56–65, Sep. 2020.

[16] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1021–1037, Feb. 2021.

[17] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115876–115904, 2020.

[18] O. Jogunola, A. Ikpehai, K. Anoh, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Harris, "Comparative analysis of P2P architectures for energy trading and sharing," *Energies*, vol. 11, no. 1, p. 62, Dec. 2017. [Online]. Available: https://www.mdpi.com/1996-1073/11/1/62

[19] F. Jamil, N. Iqbal, S. Ahmad, and D. Kim, "Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid," *IEEE Access*, vol. 9, pp. 39193–39217, 2021.

[20] M. I. Ashraf, C.-F. Liu, M. Bennis, and W. Saad, "Towards low-latency and ultra-reliable vehicle-to-vehicle communication," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2017, pp. 1–5.

[21] J. Lianghai, M. Liu, A. Weinand, and H. D. Schotten, "Direct vehicle-to-vehicle communication with infrastructure assistance in 5G network," in *Proc. 16th Annu. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, Jun. 2017, pp. 1–5.

[22] METIS. (Apr. 2013). *Deliverable D1.1 Scenarios, Requirements and KPIs for 5G Mobile and Wireless System*. [Online]. Available: https://cordis.europa.eu/docs/projects/cnect/9/317669/080/deliverables/001-METISD11v1pdf.pdf

[23] H. Xu, L. Zhang, and Y. Sun, "BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication," 2021, *arXiv:2101.10856*.

[24] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[25] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, *arXiv:1708.09721*.

[26] Fortune Business Insights. *Blockchain-as-a-Service (BaaS) Market to Hit USD 24.94 Bn by 2027; Rising Demand for Decentralized Software Services to Boost Market Growth: Fortune Business Insights*. Accessed: Aug. 24, 2023. [Online]. Available: https://prn.to/35TtLw5

[27] J. Singh and J. D. Michels, "Blockchain as a service (BaaS): Providers and trust," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Apr. 2018, pp. 67–74.

[28] *AWS Pricing Calculators*. Accessed: Aug. 24, 2023. [Online]. Available: https://calculator.aws

[29] IBM. *IBM Cloud Cost Estimator*. Accessed: Aug. 24, 2023. [Online]. Available: https://www.ibm.com/cloud/cloud-calculator

[30] Huawei. *Price Calculator Huawei Cloud*. Accessed: Aug. 24, 2023. [Online]. Available: https://www.huaweicloud.com/intl/en-us/pricing/index.html#/ecs

[31] Kaleido Inc. *Pricing: Blockchain SaaS & Business Cloud Services*. Accessed: Aug. 24, 2023. [Online]. Available: https://www.kaleido.io/pricing

[32] Xooa Inc. *Blockchain & Low Code Platform Pricing*. Accessed: Aug. 24, 2023. [Online]. Available: https://xooa.com/pricing.html

[33] Chainstack. *Compare Plans Chainstack*. Accessed: Aug. 24, 2023. [Online]. Available: https://chainstack.com/pricing

[34] KompiTech. *Find the Right Plan for Your Business*. Accessed: Aug. 24, 2023. [Online]. Available: https://blockchain.kompitech.com/pricing

[35] Google LLC. *Cloud Pricing Calculator*. Accessed: Aug. 24, 2023. [Online]. Available: https://cloud.google.com/products/calculator

[36] Microsoft. *Pricing Calculator Microsoft Azure*. Accessed: Aug. 24, 2023. [Online]. Available: https://azure.microsoft.com/en-us/pricing/calculator/?cdn=disable

[37] *Total Cost of Ownership (TCO) Calculator—Microsoft Azure*. Accessed: Aug. 24, 2023. [Online]. Available: https://azure.microsoft.com/en-us/pricing/tco/calculator

[38] M. M. H. Onik and M. H. Miraz, "Performance analytical comparison of blockchain-as-a-service (BaaS) platforms," in *Emerging Technologies in Computing*, M. H. Miraz, P. S. Excell, A. Ware, S. Soomro, and M. Ali, Eds. Cham, Switzerland: Springer, 2019, pp. 3–18.

[39] A. Iftekhar and X. Cui, "Anti-tamper protection for Internet of Things system using hyperledger fabric blockchain technology," 2021, *arXiv:2109.07074*.

[40] A. Goranovic, M. Meisel, S. Wilker, and T. Sauter, "Hyperledger fabric smart grid communication testbed on raspberry PI ARM architecture," in *Proc. 15th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, May 2019, pp. 1–4.

[41] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–8.

[42] V. Sciancalepore, L. Zanzi, X. Costa-Pérez, and A. Capone, "ONETS: Online network slice broker from theory to practice," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 121–134, Jan. 2022.

[43] Q. Qin and L. Tassiulas, "Auction-based network slicing architecture and experimentation on SD-RANs," in *Proc. 1st Int. Workshop Open Softw. Defined Wireless Netw.* New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–6, doi: 10.1145/3396865.3398690.

[44] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Oct. 2020, pp. 1–7.

[45] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.

[46] Z. Xu, "Auctions and application of Vickrey auction," in *Proc. Int. Conf. Econ. Manag. Corporate Governance (EMCG)*. Clausius Scientific Press (CSP), 2021.

[47] N. Afraz and M. Ruffini, "A sharing platform for multi-tenant PONs," *J. Lightw. Technol.*, vol. 36, no. 23, pp. 5413–5423, Jul. 15, 2018.
[48] X. Liu, Q. Qiu, and L. Lv, "An online combinatorial auction based resource allocation and pricing mechanism for network slicing in 5G," in *Proc. IEEE 19th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2019, pp. 908–913.
[49] L. Valcarenghi, A. Giorgetti, B. Martini, K. Kondepu, M. Gharbaoui, and P. Castoldi, "Reliable slicing in 5G networks," in *Proc. 5G Italy Conf.*, 2019, pp. 1–12.
[50] R. H. Kim, H. Noh, H. Song, and G. S. Park, "Quick block transport system for scalable hyperledger fabric blockchain over D2D-assisted 5G networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1176–1190, Jun. 2022.
[51] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.
[52] C. Zhang, S. Dang, B. Shihada, and M.-S. Alouini, "Dual attention-based federated learning for wireless traffic prediction," in *Proc. IEEE Conf. Comput. Commun.*, May 2021, pp. 1–10.
[53] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016, *arXiv:1610.05492*.
[54] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, Jun. 2020.
[55] G. Cohen, S. Afshar, J. Tapson, and A. Van Schaik, "EMNIST: Extending MNIST to handwritten letters," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Mar. 2017, pp. 2921–2926.
[56] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, vol. 54. Fort Lauderdale, FL, USA: JMLR, W&CP, 2017, pp. 1273–1282.
[57] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–7.
[58] F. Wilhelmi, E. Guerra, and P. Dini. (2022). *BlockFLsim: Blockchain Federated Learning Simulator*. Accessed: Aug. 24, 2023. [Online]. Available: https://gitlab.cttc.es/supercom/blockFLsim/-/tree/BlockFLsim
[59] M. Alharby and A. van Moorsel, "BlockSim: An extensible simulation tool for blockchain systems," *Frontiers Blockchain*, vol. 3, p. 28, Jun. 2020.
[60] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.
[61] F. Wilhelmi, S. Barrachina-Muñoz, and P. Dini, "End-to-end latency analysis and optimal block size of proof-of-work blockchain applications," *IEEE Commun. Lett.*, vol. 26, no. 10, pp. 2332–2335, Oct. 2022.
[62] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.

NIMA AFRAZ (Senior Member, IEEE) received the Ph.D. degree in computer science from Trinity College Dublin, Ireland, in 2020. He was a Postdoctoral Fellow to address the challenges in the adoption of blockchain technology in telecommunications. He is currently an Assistant Professor with the School of Computer Science, University College Dublin. He is also a Funded Investigator with the CONNECT Research Centre. His research interests include blockchain applications in telecoms, the economics of networks, and network virtualization. He was a recipient of the Government of Ireland Postdoctoral Fellowship. He is the Vice-Chair of the Linux Foundation's Hyperledger Telecom Special Interest Group.

FRANCESC WILHELMI (Member, IEEE) received the M.Sc. degree in intelligent and interactive systems and the Ph.D. degree in information and communication technologies from Universitat Pompeu Fabra (UPF), in 2016 and 2020, respectively. He is currently a Research Engineer with Nokia Bell Labs. His main research interests include Wi-Fi technologies and their evolution, network simulators and network digital twinning, machine learning, and distributed ledger technologies.

HAMED AHMADI (Senior Member, IEEE) received the Ph.D. degree from the National University of Singapore, in 2012. Since 2012, he has been with different academic and industrial positions in Ireland and the U.K. He is currently a Reader in digital engineering with the School of Physics Engineering and Technology, University of York, U.K. His research interests include the design, analysis, and optimization of wireless communications networks, the application of machine learning, and blockchain in wireless networks.

MARCO RUFFINI (Senior Member, IEEE) is currently an Associate Professor and a fellow of Trinity College Dublin. He also leads the Optical Network Architecture Group. He is also a Principal Investigator in several research projects in the area of B5G and optical networks, including OpenIreland a new research infrastructure to build open networking, beyond 5G testbed in Dublin. He has authored over 170 international publications, over ten patents, standards contribution, and has raised research funding in excess of €8M.