Blockchain-Based Decentralized Applications for Multiple Administrative Domain Networking

Raphael Vicente Rosa and Christian Esteve Rothenberg

Abstract

Evolving networking scenarios include multi-administrative domain network services as drivers of novel business opportunities along with emerging operational challenges. As a potential approach to tackle upcoming requirements providing basic primitives to encompass analytics, automation, and distributed orchestration, we investigate blockchain-based decentralized applications (DApps) in the context of operational phases in support of multi-administrative domain networking. We present and discuss a generalized framework for multi-domain service orchestration using blockchain-based DApps and then showcase proof-of-concept prototype experiments based on best of breed open source components that demonstrate DApp functionalities as candidate enablers of multi-domain network services. We then analyze three use case scenarios pursued by ongoing work at standards development organizations, namely MEF, 3GPP, and ETSI NFV, discussing standardization opportunities around blockchain-based DApps.

Introduction

Diverse envisioned fifth generation (5G) services (e.g., augmented reality, vehicular communications, Internet of Things [IoT]) call for advanced multi-administrative domain service deployments, with open challenges arising from vertical customers of communication service providers [1], leading to complex distributed service level agreement (SLA)-based orchestration hazards. Stakeholders at different administrative domains are looking for shared revenue models from the roaming scenario and vertical businesses [2]. For a given end-to-end network service, its realization would benefit from every per-domain segment being able to distributively contribute to the delivery and assurance of a given service supply chain (e.g., *proof-of-relay* attesting to intermediary flow attributes including throughput, latency, packet loss ratio, etc.), in addition to contractual operational workflows in the case of SLA breaches.

To attend decentralized non-trusting administrative domains in need of chained smart contracts (inter-domain transactions and billing) for consensus (composed SLAs), we advocate for the opportunities unlocked by a shared ledger of abstracted capabilities (end-to-end service slices) via blockchain-based decentralized applications (DApps) for multi-administrative domain networking. Such natively distributed and dynamic scenarios, built for robustness and fault tolerance, are hardly addressable by trusted centralized databases or intermediate marketplaces (Table 1), as recognized by pre-standardization research efforts[1] and early commercial solutions.[2]

The main contribution of this article is establishing a walk-through from background baselines, via motivating perspectives and potential candidate strategies and implementation options to incorporate blockchain-based DApps into multiple administrative domain scenarios. Our proof-of-concept prototype experiments of blockchain-based multi-domain orchestrators (MdOs), demoed in [3], showcase smart contracts for life cycle management of network services across administrative domains. Such argumentative baggage sustains our standardization outlook discussion toward feasibility prospects of incorporating blockchain-based DApps into three standards development organization (SDO) use case scenarios.

Background Concepts and Definitions

Following the Next Generation Mobile Networks (NGMN) Alliance terminology [2], "provider" refers to any entity that provides a service (e.g., infrastructure, platform, or network as a service), including an "operator" of some administrative domain. A provider may obtain benefits from offering service spare capabilities or resources to/from 3rd parties to enrich the services provided to its end customer.

Henceforth, we refer to an administrative domain as the scope of jurisdiction of a provider. An MdO stands for the entity responsible for providing network service life cycle operation/management across administrative (and technology) domains. A network asset consists of any resource (e.g., network function, virtualized environment, connectivity) available for a network service.

Beyond Traditional IP Peering

Further than Border Gateway Protocol (BGP), possible bi/multi-lateral partnership agreements among providers implementing software defined networking (SDN) and/or network functions virtualization (NFV) technologies can

The authors are with the University of Campinas (UNICAMP).

[1] Decentralized Internet Infrastructure Research Group (dinrg); https://datatracker.ietf.org/rg/dinrg/about/ and ITU Focus Group on Application of Distributed Ledger Technology (DLT) at https://www.itu.int/en/ITU-T/focusgroups/dlt/, accessed May 1, 2018.

[2] For example, Blockstack, A New Internet for Decentralized Apps; https://blockstack.org and, NKN, New Kind of Network at https://nkn.org, accessed May 1, 2018.

Digital Object Identifier: 10.1109/MCOMSTD.2018.1800015

2471-2825/18/$25.00 © 2018 IEEE

Factor	Discourse
1. The database	Internet and telecom services are global-scope ecosystems sustained without central points of failure or provider detaining higher permissions, hence the fit for transparent shared ledgers
2. Multiple writers	Distributed MdO orchestrator instances, with dynamic scaling and diverse stakeholders (e.g., providers of VNFs, infrastructure resources, platforms, services, slice tenants)
3. Absence of trust	Stakeholders (VNF vendors, infrastructure/service providers, etc.) belong to different organizations globally distributed pursuing different social, technological, political, and financial interests
4. Disintermediation	A blockchain-enabled business plane for network assets proliferates innovation and settles opportunities for newcomers allowing open, autonomous, and low-hierarchical models of governance
5. Transaction interaction	Providers must collaborate to deploy end-to-end services, upholding their SLAs through shared smart contracts addressing dependable network assets (e.g., ultra-reliable low latency) enabling revenue sharing
6. Set the rule	Each network asset detaining a certificate of provenance states the operations it might be subject to, posing boundary rules for its operational behavior inside a smart contract life cycle
7. Pick your validators	MdO providers hosting miners compose a win-win consortium demanding certification and auditing check-ups to federation-like members of a reliably designed blockchain network
8. Back your assets	Diverse stakeholders (e.g., VNF developers and vendors, infrastructure and service providers) pose themselves in a flat Internet marketplace being able to independently stand behind their own network assets

Table 1. Discourse factors on why MdO calls for blockchain approaches instead of centralized databases or marketplaces.

result in complex end-to-end service deployments covering various network assets. Next, we formalize generalized network service operational phases in a multi-administrative domain setting as follows (Fig. 1):

Discovery: Consists of perceiving provider boundaries and the interconnections that might exist with direct or remote administrative domains to provide/obtain service capabilities via so-called entry points

Exposure: Exchanges of selected information regarding network assets (e.g., capability, reachability, metering) among providers

Intent: Defines the proposal of intended network service requirements among providers aiming to realize an SLA

Negotiate: Encompasses provider's policy enforcement to attain operational business needs (e.g., cost, scalability, geographical restriction).

Fulfill: Conceives the instantiation of a network service business agreement over providers, enforcing its life cycle operation/management workflows (e.g., deployment, monitoring, billing) by traded policies.

The proposed structured MdO phases are mainly meant to elucidate, throughout the article, potential specific mechanisms that might be associated with a particular blockchain DApp functionality. In an MdO process, it is not mandatory that such operational phases occur strictly in the presented order or are not exempt from taking place simultaneously and iterating in different orders. For instance, the discovery and exposure phases might be merged to form a single stage. An example mapping to traditional BGP peering could be as follows:

1. An administrative domain discovers reachable autonomous system numbers (ASNs).
2. A TCP connection on port 179 is established among border routers, and default routes are exchanged.
3. An operator refines routing information it intends to advertise/receive through policy maps and BGP configuration knobs.
4. Routing exchanges proceed, following each provider BGP policy, to establish effective peering/transit/customer relationships.
5. Forwarding entries in border and intra-domain routers are installed after BGP route selection while maintenance operations keep them in production.

Operational Requirements of Multi-Domain Networking

Carrier-grade MdO calls for advances in transport and value-based network services to address distributed inter-connections among cloud environments, with on-demand fulfillment of business verticals to handle the expected quality of and ever growing traffic needs from the edge, rendering perceivable aggregated value beyond just "dumb pipes" through improved operational practices.

Analytics: Measurements of network service operational metrics across domains must prevail for providers to transparently verify costs associated with the utilization of network assets for policy and SLA enforcement. Besides, cohesive analysis of network asset behavioral patterns should conceive inference methods to enable predictive and reactive actuation workflows for network services runtime optimization.

Automation: Agile networking demands automation, for instance, applied to service life cycle management/orchestration in multi-administrative networking, including self-scaling/healing of the virtual and physical infrastructure. To attain vertical business requirements (e.g., low time to market), automation must transform the current manual and monolithic network operational environments into a dynamic on-demand network services fulfillment mode of operation.

Distributed Orchestration: Jointly with compute and storage resources in heterogeneous networking environments (e.g., radio, optical, core), an MdO must concisely abstract network assets, capabilities, and requirements, ensure the fulfillment of network services, and transparently sustain (e.g., via scaling, migrating, healing) agreed SLAs, leveraging network analytics.

A Glimpse of Blockchain

In this section, we introduce the main concepts of blockchain required to understand this article. The relevant blockchain literature includes [4–6].}

Blockchain allows consensus in the storage of data structures fulfilled by non-trusting distributed entities. Entangled blocks placed in a chain contain sets of signed data structures (e.g., transactions or contracts), including transparent manners to verify their internal information. Public or private, blockchain can implement different consensus algorithms executed by miners, which validate and incorporate transactions or contracts into blocks.

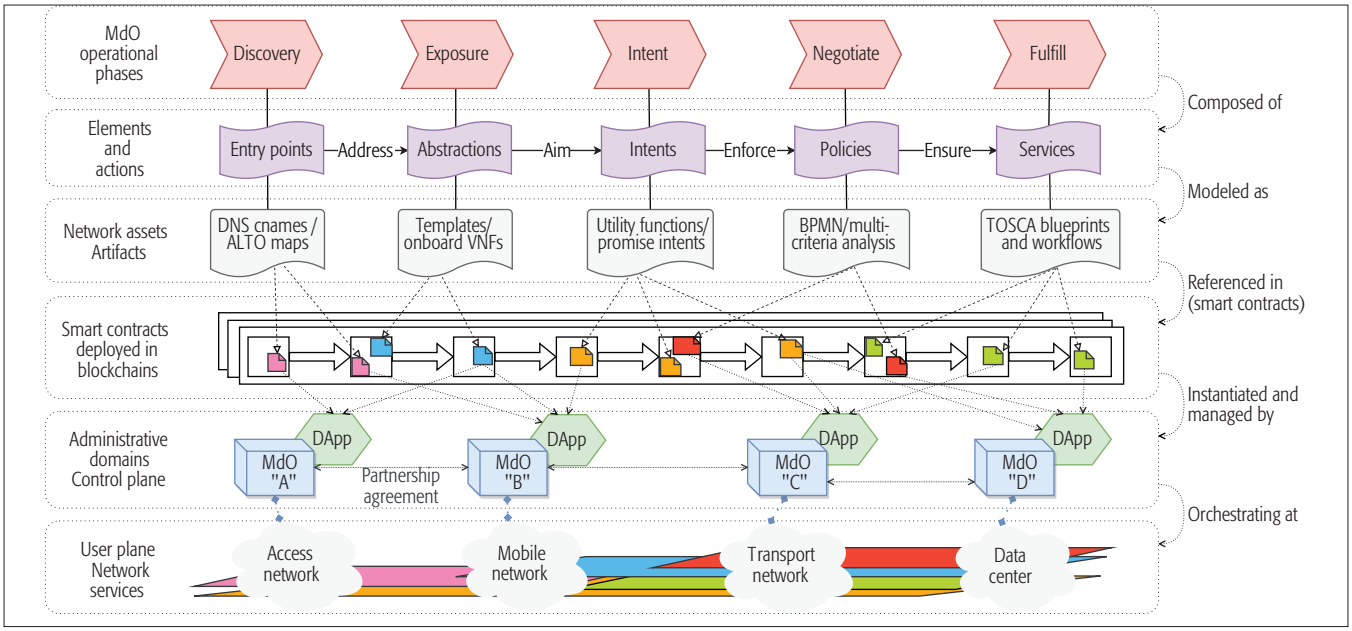

FIGURE 1. Operational phases of multi-administrative service orchestration associated with blockchain-based DApps.

A transaction/contract can be created by any uniquely identifiable node, provided it is part of a blockchain network. Such operation propagates in blockchain nodes, which verify the content and eventually settle it as confirmed when added in a mined/chained block. Depending on the blockchain network parameters and the mining consensus algorithm, a transaction may take different amounts of time until confirmed.

A smart contract consists of a script that might provide access permissions to store data and execute a programmable logic (i.e., code) inside the blockchain. Nodes can join a contract and interact with it via transactions, which might trigger programmable events containing various attributes. DApps are developed using blockchain distributed consensus operations to perform transactions and smart contracts.

Why and How Blockchain DApps for Multi-Administrative Domain Networking

Similar to agile cloud environments in web-scale companies, carriers pursue fluid network infrastructures to support analytics, automation, and distributed orchestration via software-centric innovations from radio access to the core. However, current monolithic end-to-end connectivity services, slowly deployed through intra-domain manual configurations over redundant/costly infrastructure footprints, settle opaque SLAs to eventually ensure inter-domain handshake agreements.

Through concise access permissions, a blockchain smart contract turns a distributed MdO partnership agreement into a software artifact, securely programmable to compose a transparent and automated chain of custody for network assets across providers. Indulging blockchain DApps,[3] administrative domains can partner via smart contracts designed to offer, negotiate, and track network assets, their metrics and life cycle management operations, and be projected to trigger events upon the occurrence of specific transactions. Analyzing the logged events, providers can perform proper actions over their smart contracted network assets, including trading, onboarding, healing, billing, and so on. Table 1 summarizes the key rationale of MdO calling for a blockchain approach instead of traditional centralized database approaches.[4]

Incorporating DApps into MdO

Figure 1 presents an architectural integration with a high-level view of multi-domain network service orchestrators and their respective interactions with blockchain DApps. Public and private blockchains can coexist, containing sets of evolving DApps interacting at different operational phases. In each one of the previously enumerated MdO operational phases, we highlight strategies for incorporating DApps:

Discovery: Via DApps, providers can compose smart contracts to store and update information concerning maps of open-consult gateways to entry points indicating offers of evolving abstracted network assets and their capabilities.

Exposure: Composing a decentralized marketplace, providers can configure policies to express the scrutiny of abstracted views of their network assets and capabilities to be stored in smart contracts and presented by their methods via previously discovered entry points.

Intent: Comprehending a provider intent-based policy containing an SLA and capability requirements for a network service, a DApp can implement a smart contract to enforce automated strategies according to exposed abstraction views to propose the acquisition of assets from other providers.

Negotiate: DApps can define interfaces to trade network assets through smart contracts (e.g., token-valued transfers, temporal auctions, multi-signature contracts) under a particular revenue-logic that might respect programmable

[3] The closest business-ready related work in the cloud computing realm would be iExec Blockchain-Based Decentralized Cloud Computing; https://iex.ec/whitepaper/, accessed May 1, 2018.

[4] Following blockchain project guidelines by Gideon Greenspan; https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/, accessed May 1, 2018.

Group	Design pattern	MdO phase	Use case feature
Data	Identity gateway	Discovery	Keep registry of administrative domains
	Name registry	Discovery	Organize entry points for different service capabilities
	Data feed	Exposure	Maintain records of network infrastructure assets
Transaction and value	Asset token	Intent	Store set of strategies according to incentives for service capabilities
	Exchange	Negotiation	Define business trades of networking assets and monetary values
Action and control	Event log	Fulfill	Keep track of infrastructure resources consumption
	Incentivized trigger	Fulfill	React to failures or workloads to execute life cycle workflows

Table 2. DApp Design patterns associated with MdO operational phase and use case features.

thresholds as contract conditions (e.g., bids, time of day, offer vs. demand).

Fulfill: Via smart contracts, DApps can keep track of network assets deployment in remote administrative domains through logged events of transactions representing their life cycle management workflows. Besides, a coordinated feedback loop can be established among providers when such events trigger hired reactions programmed inside an agreed smart contract.

Multi-Administrative Domain DApp: A Primer

For each administrative domain, a DApp shall define at least:

- Consistency of the information provenance stored in the blockchain associated with actual abstracted network assets
- Progress when evolving their internal states and logically expressing their operational and management attributes
- Safety for completing tasks strictly in conformance with providers' goals and intended outcomes, avoiding hazards and faults

Below, we present a step-by-step DApps design guide for multi-domain network service orchestration.

Set General Goals: These define the DApp objectives to explore one or more MdO operational phases, the outline of its application programming interfaces (APIs), managed smart contracts (inputs/outputs), and access permissions for the blockchain network.

Identify the Assets: This entails the representation of network assets when stored in the blockchain, delineating properties and attributes to explicitly represent their status in different operational states.

Understand Changes in State of Accounts/Contracts: This brings the DApp interface to operations and conditions of smart contract methods, containing entries and logical functions to modify the status of network assets and reflect actions taken on (or by) them.

Define DApp and Contract Life Cycle: This settles the DApp and smart contracts operational logic, and establishes a timeline of events/conditions they might trigger/interface from instantiation until decommission, including details of possible behavior and actions altering the programmable logic.

As illustrative guiding examples, shown in Table 2, models of smart contract design patterns[5] were associated with categories of MdO use cases. Furthermore, MdO operational phases can be associated with one or more smart contract design patterns, and DApps designed for different operational phases might share information.

Experimenting with a MdO DApp Prototype

Going after proof-of-concept perspectives, we present a DApp implementation (further details about the demo are available in [3]) through an experiment aimed at showcasing the *Fulfill* operational phase along the registration of life cycle management events of network services deployed across multiple domains.[6]

Figure 2a illustrates our experimental setup based on a Mininet[7] emulated topology where each Open vSwitch instance represents a single administrative domain network infrastructure, shown as clouds `A`, `B`, `C`, `D`, `E`, and hosts represented by areas `X`, `Y`, and `Z`. In addition, administrative domain MdOs running Docker containers are interconnected via a management network and interface a common private blockchain network implemented with Ethereum.[8] Each MdO instance is built on the following components.

Exchange: This interconnects internal elements through event-oriented APIs. *Peering* handles the interaction between administrative domains. *Slicing* uses the Aria-TOSCA[9] engine jointly with blueprints to exercise an SDN plugin interfacing SDN applications and to realize life cycle service orchestration intra/inter-administrative domains. *Notary* represents the DApp that manages and operates smart contracts.

SDN App: Based on the Ryu[10] controller, this receives REST commands from the *Slicing* component for southbound programming of traffic forwarding rules in the OVS instances through flow entries (OpenFlow v1.3) and queue configuration (OF-Config).

Graph App: This interfaces *Notary* blockchain DApps where MdO smart contracts reside, enabling their information to be periodically pulled and pushed into the Neo4j[11] graph database model for network services auditing. Therefore, queries can be made into specific chained occurrences of particular contracts and events.

The experiment features a customer of provider `A` realizing multi-administrative service deployments (shown in Fig. 2a as dashed lines 1 to 4) from instantiation to decommission, using assets from providers `A`, `B`, `C`, `D`, and `E`. Accordingly, the customer issues a smart contract to log life cycle management events of services in each domain, wherein provider `A` deploys the smart contract in the blockchain network, requesting other domains to join it, and registers each of them along their associated roles for the upcoming service deployments. When the customer instantiates the smart contract, in the Exchange platform of each administrative domain a programmable

[5] https://www.youtube.com/watch?v\=XkJ8mg-R7C0, accessed May 1, 2018.

[6] A 3-minute video illustrating the experimental setup is available at https://drive.google.com/file/d/14gsJuzS4PgOt_X5o1Lh0SOpwYRBcHrmB, accessed July 3, 2018.

[7] https://github.com/mininet/mininet, accessed May 1, 2018.

[8] https://www.ethereum.org/, accessed May 1, 2018.

[9] http://ariatosca.incubator.apache.org/, accessed May 1, 2018.

[10] https://github.com/osrg/ryu/, accessed May 1, 2018.

[11] https://neo4j.com/, accessed May 1, 2018.

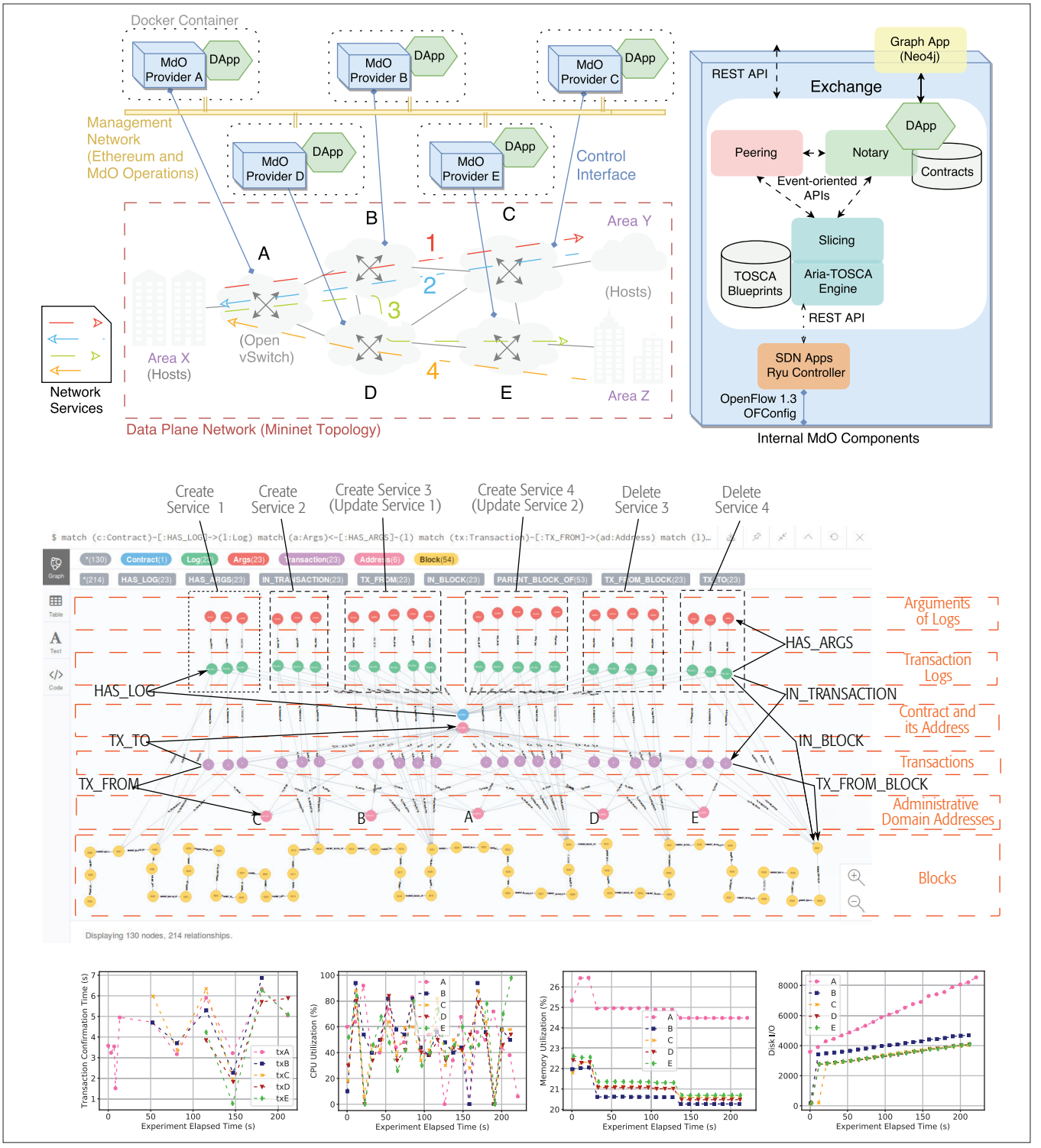

FIGURE 2. Experimental setup and overall results: a) left, experimental testbed consisting of a Mininet-based topology, multi-domain orchestrators (MdO) running the DApp, and right, component details of the MdO/DApp prototype implementation; b) modeled Neo4j graph of network service life cycle events extracted from blockchain in multi-domain orchestration experiments; c) transactions confirmation time; (d) CPU % measurements; e) memory % measurements; (f) disk I/O write measurements.

logic takes place, establishing a semantic association of the smart contract with workflow events from the TOSCA service blueprint deployment; that is, in each *Slicing* operation, an event, containing information about the workflow call and its respective output, will be triggered to *Notary* to create a transaction into the agreed smart contract, logging the requested life cycle management operation with reference to the customer network service status.

While the dynamics of the experiment occur to demonstrate the feasibility of an MdO auditable ledger, in the Neo4j application, the customer can oversee an abstracted graph model of the blockchain and the smart contract, presenting the chronological storyline of logged life cycle

Use case scenario	Challenges	Approach	Benefits	Prospects
MEF SD-WAN	Secure on-demand tailored paths across non-trusting providers	Discovery and exposure of certified providers' assets by DApps	Transparency for signed network assets and their providers	MEF LSO Soonata and Interlude interfaces intercommunicating with DApps
ETSI NFVIaaS	Access permission to resources between providers' NFV-MANO components	Smart contracts store access permission and assets information for MANO components	Secure access permissions of assets between MANO components	Scalability and performance requirements from DApps to realize MANO-to-MANO bridge
3GPP network slicing	Network slice instances across mobile/transport operators	Smart contracts record roaming NSIs and their QoS requirements	Agile and transparent business agreements among operators	Intercommunication of multi-operator management systems through DApps

TABLE 3. Analysis of use case scenarios in different standardization bodies.

management events of each MdO service deployment.

Figure 2 shows an annotated print screen of the organized graph abstraction extracted from the smart contracted services agreement. In the graph model, nodes are classified into dashed rectangles with their corresponding category name on the right (e.g., Blocks, Transactions, Arguments of Logs). Relationships among nodes are represented as solid arrows annotated with capital letters (e.g., `IN_BLOCK`, `IN_TRANSACTION`, `HAS_LOG`). On the top of Fig. 2, squared areas represent all logged events per administrative domain MdO participating in the life cycle management workflows of Services *1*, *2*, *3*, and *4*.

Bottom-up, Fig. 2 shows blocks, sequentially mined in the blockchain from left to right. Some of these blocks contain `TX_FROM_BLOCK` transactions, referencing administrative domain addresses (`A`, `B`, `C`, `D`, `E`), from (`TX_FROM`) where they were called and also the destination (`TX_TO`) contract address. `IN_TRANSACTION` events are represented by *Transaction Logs*, which reference every life cycle management call that the *Slicing* component (from each provider) triggered when deploying the requested service. Logs also contain `HAS_ARGS` arguments with attributes of each logged event's properties and outputs, which can be searched by refined graph queries to inspect their content and debug/attest outcomes of each provider life cycle management workflow.

An analysis of performance profiling metrics extracted from each MdO execution environment (Figs. 2c–2f), from the contract registration until the services decommission, shows average transaction confirmation times of less than 7 s, in line with the expected timing of MdO operational phases (tens of seconds to minutes) in our scope. The utilization of CPU presents peaks in each MdO due to blockchain consensus through proof of work, positively correlating with the increased disk writes (mined blocks), whereas the utilization of memory stays stable in all domains.

Scenarios under Standardization Lenses

From ideas to realistic networking scenarios, the definition of standard information models and interfaces are mandatory to integrate blockchain DApps with providers' functional entities realizing orchestration/management capabilities and business support systems. Through the analysis of three use case scenarios, namely SD-WAN, NFV infrastructure as a service (NFVIaaS), and network slicing in the context of architectural work at the Metro Ethernet Forum (MEF), European Telecommunications Standards Institute (ETSI) Network Functions Virtualization (NFV), and Third Generation Partnership Project (3GPP), respectively, we illustrate blockchain DApp functionalities, discuss potential approaches and benefits to address challenges of multi-domain network services, and elaborate standardization prospects summarized in Table 3.

MEF: SD-WAN

Context: MEF Third Network Vision proposes a Life Cycle Service Orchestration (LSO) reference architecture and framework to address agile, ensured, and orchestrated connectivity services. Those include end-to-end deployments where LSO interacts with potentially several providers through Sonata and Interlude reference interfaces interconnecting cross-domain business applications and service orchestration functionalities, respectively. Mapped to LSO, ongoing work at MEF aims to standardize software-defined WAN (SD-WAN) (e.g., terminology, components, architecture).

Challenges: An initial proposal [7] defines SD-WAN as the means to flexibly achieve programmable micro-segmented paths — based on Quality of Service (QoS), security, and business policies — across sites (public or private clouds), using overlay tunnels over varied underlay technologies, such as broadband Internet and multiprotocol label switching (MPLS). Potentially spanning multiple provider sites, an SD-WAN operator must tailor and scale paths on demand to ensure application policies (e.g., performance profiles, geographical boundaries, data privacy policies) by interfacing SD-WAN routers through non-trusting administrative domains in heterogeneous wired/wireless underlay networks with varying performance metrics.

Approach: Embracing the discovery and exposure blockchain-based MdO operational phases, through the LSO Sonata interface a smart contract can be programmed to contain signatures of accredited SD-WAN providers to fill in such contract information regarding certified network connectivity assets (e.g., MPLS tunnels) and associated QoS capabilities (e.g., throughput, latency, frame loss ratio) (Fig. 3a).

Benefits: Securely discovering exposed and certified SD-WAN assets that match an application traffic operational policy, a customer can automate an SD-WAN service deployment via a smart contract, which guarantees transparency

in the analysis of signed network assets and their respective providers.

Prospects: Focused on the interaction of Sonata and Interlude reference interfaces, the investigations of LSO engineering aspects involving the blockchain guiding designs of this article can outline information models, business process flows, and APIs to enable and enhance the positioned operational threads for LSO concerning multi-administrative networking, such as partners/providers onboarding. As the SD-WAN standardization proposal references LSO, benefits directly apply.

ETSI NFV: NFVIaaS

Context: Referencing the use case "virtual network function (VNF) composition across multiple administrative domains" at ETSI NFV ISG, the Interfaces and Architecture (IFA) Working Group has proposed NFV management and orchestration (MANO) services across administrative domains [8].

Through use cases, the document identifies responsibilities of the NFVIaaS consumer and provider, and proposes potential extensions of interfaces and functional blocks in the NFV MANO architectural framework.

Challenges: Associated with the operation and management of NFV MANO resources, the main differences of potential NFVIaaS architectural options proposed in [8] consist of role-based access control to grant proper permissions for the relationship of NFV MANO functional blocks between administrative domains.

Approach: As shown in Fig. 3b, a DApp managed by each administrative domain MANO can issue smart contracts programmed to allow access permission for NFVIaaS counterparts signatures and store abstracted views of traded NFV assets, mappings of the structure of quotas, access grants, and capacity, available to NFVIaaS consumers.

Benefits: DApps for multi-administrative NFVIaaS enable security for enhanced intercommunication among NFV MANO functional components, transparency on identity/permission management for NFVIaaS providers and consumers, and certified information for policy enforcement concerning the utilization of NFV MANO resources.

Prospects: Reference [8] proposes changes in reference points to attend recommendations of NFV MANO interfaces among administrative domains. Similar investigations can coexist to understand scalability and performance of MANO-to-MANO operations required from blockchain DApps realizing NFVIaaS, proposing potential architecture options with explicit operational flows and interface adaptations/proposals among MANO components and DApps, including the security implications.

3GPP: Network Slicing

Context: 3GPP establishes multi-network connectivity and service delivery across operators as a 5G requirement motivated by subscribers' access to different services via multiple networks (providers) for better user experience. In [9] 3GPP SA WG5 proposed use cases, potential requirements, and candidate solutions for the management and orchestration of next-generation network slices, included "Solution Options for Network Slice Instance (NSI) Creation across Multiple Operators."

Challenges: 3GPP defines an NSI containing a set of interconnected functions in radio access and core networks. A single NSI can be rolled out through multiple administrative domains, in accordance with specific requirements (e.g., ultra-

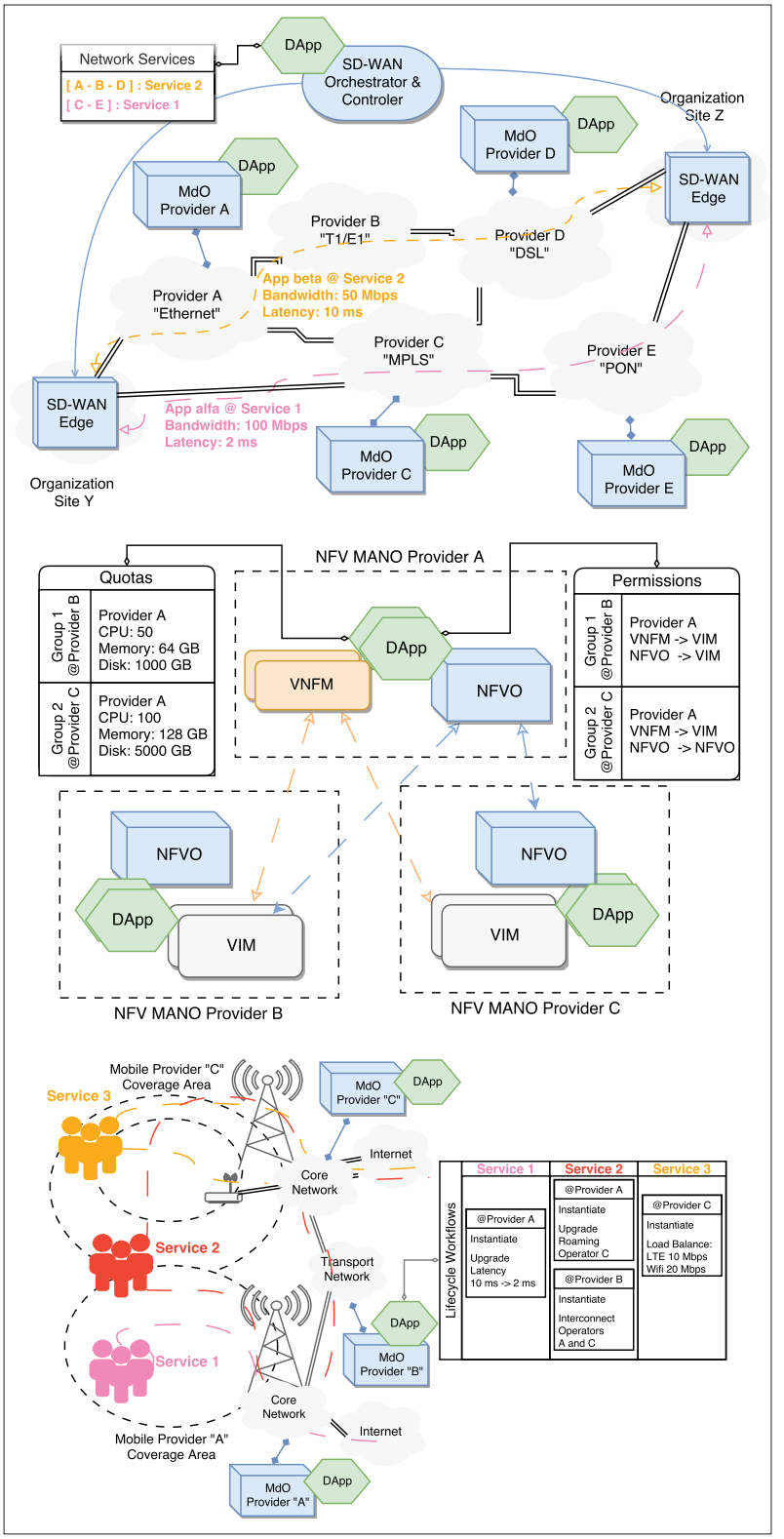

Figure 3. Potential scenarios: top: SD-WAN DApps; middle: NFVIaaS DApps; bottom: mobile network slicing DApps.

When applying DApp functionalities for network slicing, the main advantages of smart contracts include well-formatted decentralized specifications of NSI QoS requirements among mobile operators, establishment of a traffic supply chain for user equipment across NSIs in different administrative domains, and a consistent auditable registry for NSI life cycle management workflows.

low latency, ultra-reliability, isolation), addressing mobile setups, such as coverage area, distribution of users, mobility, and traffic demand. Orchestrating network slices across administrative domains requires coordinating user equipment roaming between NSIs in different coverage areas, instantiation of end-to-end NSIs across operators, and management and isolation of shared functions in access and core networks. As mentioned in [9], such requirements involve the establishment of mutual trust relationships, roaming agreements, and multiple NSIs among operators.

Approach: A DApp managed by an operator can instantiate smart contracts that record roaming NSIs, establish signed QoS agreements along with an end-to-end shared NSI across mobile operators and transport providers, and store the status of NSI life cycle management workflows (Fig. 3, bottom).

Benefits: When applying DApp functionalities for network slicing, the main advantages of smart contracts include well-formatted decentralized specifications of NSI QoS requirements among mobile operators, establishment of a traffic supply chain for user equipment across NSIs in different administrative domains, and a consistent auditable registry for NSI life cycle management workflows.

Prospects: A clear definition of the dynamics of operator management systems (OMSs) interfacing blockchain DApps can compose a way for business agreements between operators via smart contracts, which can be designed to perform the transparent storage of NSI QoS records demanded by user equipment in roaming networks while in control of the home operator. Likewise, blockchain DApps can be investigated to realize a communication channel of OMSs between operators.

Challenges Ahead

As tempting as it might be to claim and uphold the proposed prospects for the shown SDO use cases, currently we identify clear argumentative pros and cons emerging according to the fast-paced evolution of blockchain platforms, gradual real-life utility examples of solid designed blockchain use cases, and mature research efforts focused on the topics listed below, which will unveil advantages and pitfalls of incorporating blockchain DApps into multi-administrative domain networking:

- Performance: Bounded guarantees of transaction confirmation time must be well defined while realizing MdO operational phases by blockchain DApps (e.g., our experimental results depict such need).
- Scalability: There must be well defined operational metrics (e.g., storage overhead) to represent the scaling dimensions of a blockchain network across providers.
- Security: The design of an MdO blockchain network must define an architecture that guarantees its progress and safety (e.g., avoiding 51 percent of attacks) while sustaining the policy regulations of network assets in administrative domains.

In particular, certification and reputation[12] schemes must be designed by administrative domains to ensure semantic association of the provided information in a smart contract with an actual network asset, as blockchain does not impose guarantees of provenance. Hence, we believe the proper representation and interpretation of smart contract events across providers is an open field for the research of future protocols to standardize public and private MdO-DApp interfaces.

Related Work

Based on the analysis of BGP and Domain Name System (DNS), the work in [10] shows how blockchain could enhance security, among other benefits. Concerning the Internet of Things (IoT), [4, 11] investigate the use of blockchains to securely facilitate the sharing of services and resources, possibly automating time-consuming workflows and improving operational metrics.

Similar to DNS, Blockstack [12] defines the design and implementation of a distributed blockchain naming and storage system on top of the Namecoin blockchain along a series of production design trade-offs. From an early commercial view, Open Crypto Trust[13] proposes blockchain as a transport (BTaaS) applied to virtual extensible LAN (VXLAN) tunnels across sites resulting in a blockchain defined WAN (BD-WAN), in the spirit of a flexible security-enhanced software-defined WAN.

Current research efforts investigate undeniable blockchain-related issues regarding performance [13], scalability [14], and security [15], which may hinder broad deployments of blockchain platforms for different business cases. In the scope of the Internet Research Task Force (IRTF), the Decentralized Internet Infrastructure Research Group (dinrg) proposal[14] pursues a series of challenges inspired by blockchain-like approaches. In addition, the International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) Focus Group on Application of Distributed Ledger Technology (DLT) aims to develop a standardization roadmap for interoperable DLT-based services.[15]

Conclusion and Future Work

Multi-domain networking is considered a promising approach for the delivery of upcoming 5G innovative services involving new wholesale offerings and verticals with varied business needs: a landscape demanding advances from the current monolithic inter-domain connectivity model into agile and transparent SLAs for intricate end-to-end network services.

In this article, we discuss how blockchain-based DApps offer an opportune approach to streamline potential solutions and standardization opportunities for multi-domain services in SDOs' use case scenarios. According to the state of affairs, activities associated with multi-administrative networking and blockchain are still in an early stage, constructing detailed requirements and mature operational evidence. Hence, we suggest essential research challenges must be tackled toward the ability necessary for incorporating blockchain DApps into multi-administrative domain networking. Furthermore, our experiments based on a proof-of-concept implementation contribute to the feasibility claims as well as a word in favor of the maturity of the enabling open source software ecosystem.

[12] For example., http://certificates.media.mit.edu/ — accessed May 1, 2018.

[13] https://www.openct.io/, accessed May 1, 2018.

[14] https://datatracker.ietf.org/rg/dinrg/about/. sccessed May 1, 2018.

[5] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx, accessed May 1, 2018.

Meanwhile, from the standardization prospects pointed out in this article, we expect detailed requirements to be established by SDOs' use case scenarios, demonstrating a clear picture of standard interfaces and operational needs from blockchain platforms. In upcoming efforts, we intend to focus on the consistency issues when integrating DApps into administrative domains realizing multi-signature smart contracts approaching shared network assets.

Acknowledgments

This research was partially supported by the Innovation Center, Ericsson S.A., Brazil, grant UNI.64, and by the European Union's Horizon 2020 grant agreement no. 777067 (NECOS — Novel Enablers for Cloud Slicing), as well as from the Brazilian Ministry of Science, Technology, Innovation, and Communication through RNP and CTIC.

References

[1] L. M. Contreras and D. R. Lopez, "A Network Service Provider Perspective on Network Slicing," Jan. 2018; https://sdn.ieee.org/newsletter/january-2018/anetwork-service-provider-perspective-on-network-slicing.

[2] NGMN Alliance, "5G Network and Service Management including Orchestration," Mar. 2017; https://www.ngmn.org/uploads/media/170307_5G_Network_and_Service_Management__including_Orchestration_2.12.7.pdf.

[3] R. V. Rosa and C. E. Rothenberg, "Blockchain-Based Decentralized Applications Meet Multi-Administrative Domain Networking," *Proc. ACM SIGCOMM Posters and Demos, ser. SIGCOMM Posters and Demos '18*, 2018; http://doi.acm.org/10.1145/3234200.3234217.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, 2016, pp. 2292–2303.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008; http://bitcoin.org/bitcoin.pdf, accessed Dec. 1, 2017.

[6] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," 2012; http://gavwood.com/paper.pdf, accessed Dec. 1, 2017.

[7] MEF, (2017, July) "Understanding SD-WAN Managed Services, July 2017; https://www.mef.net/resources/download?id=45&fileid=file1, accessed May 1, 2018.

[8] ETSI ISG NFV, "ETSI GR NFV-IFA 028 V3.1.1 — Report on Architecture Options to Support Multiple Administrative Domains," 2018; https://docbox.etsi.org/ISG/NFV/Open/Publications_pdf/Specs-Reports/NFV-IFA 028v3.1.1 — GR — Multi admin domain support-report.pdf, accessed May 1, 2018.

[9] 3GPP (2018) TR 28.801 v15.1.0, "Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)"; http://www.3gpp.org/ftp/Specs/html-info/28801.htm, accessed May 1, 2018.

[10] A. Hari and T. V. Lakshman, "The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet," *Proc. 15th ACM Wksp. Hot Topics in Networks*, ser. HotNets '16, 2016, pp. 204–10; http://doi.acm.org/10.1145/3005745.3005771.

[11] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, 2018, pp. 115–24.

[12] M. Ali *et al.*, "Blockstack: A Global Naming and Storage System Secured by Blockchains," *2016 USENIX Annual Technical Conf.*, Denver, CO, 2016, pp. 181–94; https://www.usenix.org/conference/atc16/technicalsessions/presentation/ali.

[13] T. T. A. Dinh *et al.*, "Blockbench: A Framework for Analyzing Private Blockchains," *Proc. 2017 ACM Int'l. Conf. Management of Data*, ser. SIGMOD '17, 2017, pp. 1085–100; http://doi.acm.org/10.1145/3035918.3064033.

[14] M. Selimi *et al.*, "Towards Blockchain-Enabled Wireless Mesh Networks," CoRR, vol. abs/1804.00561, 2018; http://arxiv.org/abs/1804.00561.

[15] P. K. Sharma *et al.*, "Distblocknet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun. Mag.*, vol. 55, no. 9, Sept. 2017, pp. 78–85.

Biographies

Raphael Vicente Rosa (rvrosa@dca.fee.unicamp.br) is currently working on his thesis on multi-domain distributed NFV as a Ph.D. student at the University of Campinas (UNICAMP), Brazil. During the last two years, he worked as a visiting researcher at Ericsson Research Hungary, where he contributed to the EU-FP7 Unify project and developed activities within the H2020 5G Exchange project. His main interests are in state-of-the-art SDN and NFV research topics entangled with disruptive technologies, aiming to open source his pet projects.

Christian Esteve Rothenberg (chesteve@dca.fee.unicamp.br) is an assistant professor in the Faculty of Electrical and Computer Engineering at UNICAMP, where he received his Ph.D. and currently leads the Information & Networking Technologies Research & Innovation Group (INTRIG). His research activities span all layers of distributed systems and network architectures, and are often carried out in collaboration with industry, resulting in multiple open source projects in SDN and NFV, among other scientific results.

We suggest essential research challenges must be tackled toward the ability necessary for incorporating blockchain DApps into multi-administrative domain networking. Furthermore, our experiments based on a proof of concept implementation contribute to the feasibility claims as well as a word in favor of the maturity of the enabling open source software ecosystem.