Blockchain-based Decentralized Applications meet Multi-Administrative Domain Networking

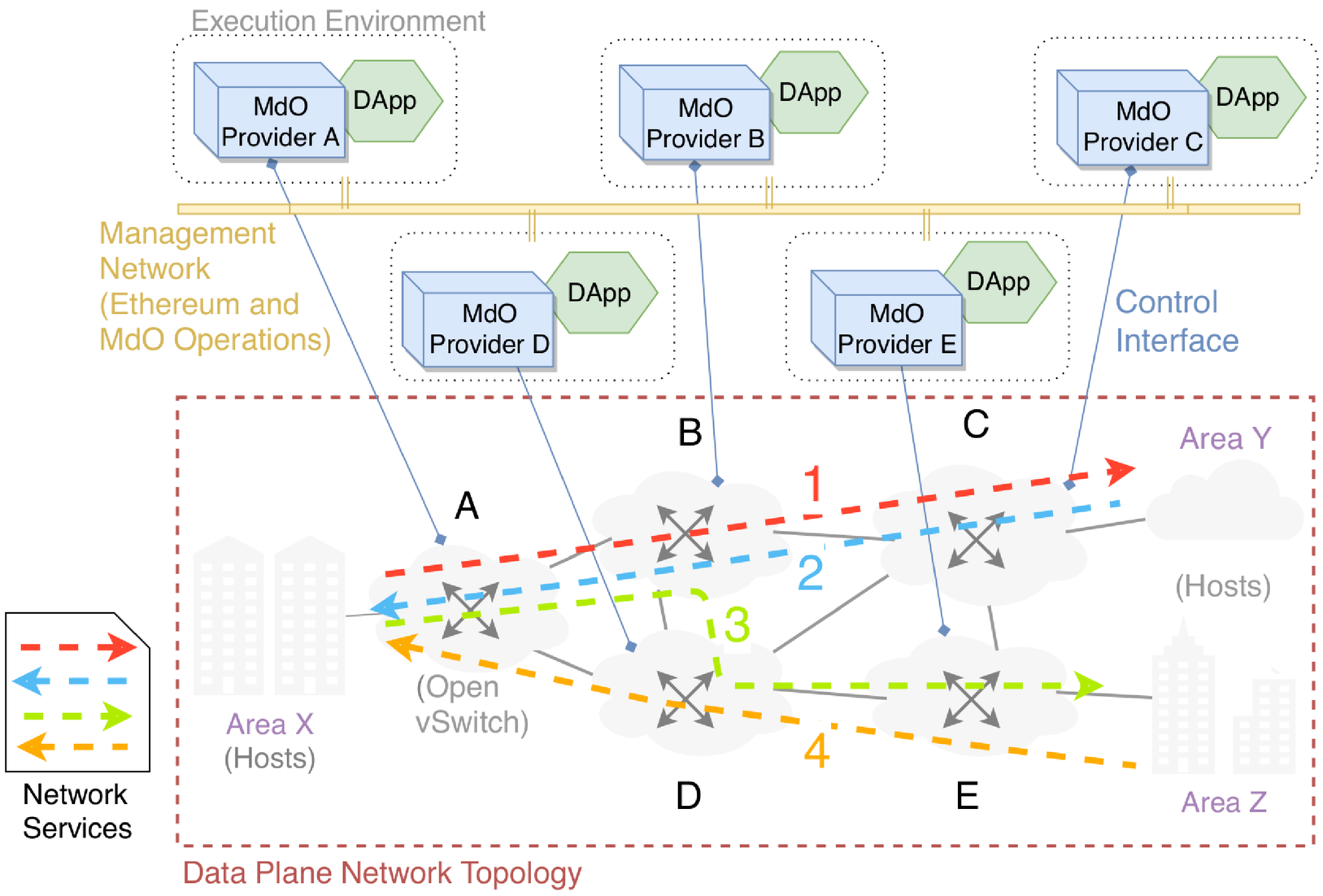
Raphael Vicente Rosa and Christian Esteve Rothenberg
School of Electrical and Computer Engineering (FEEC) - University of Campinas (UNICAMP), Brazil

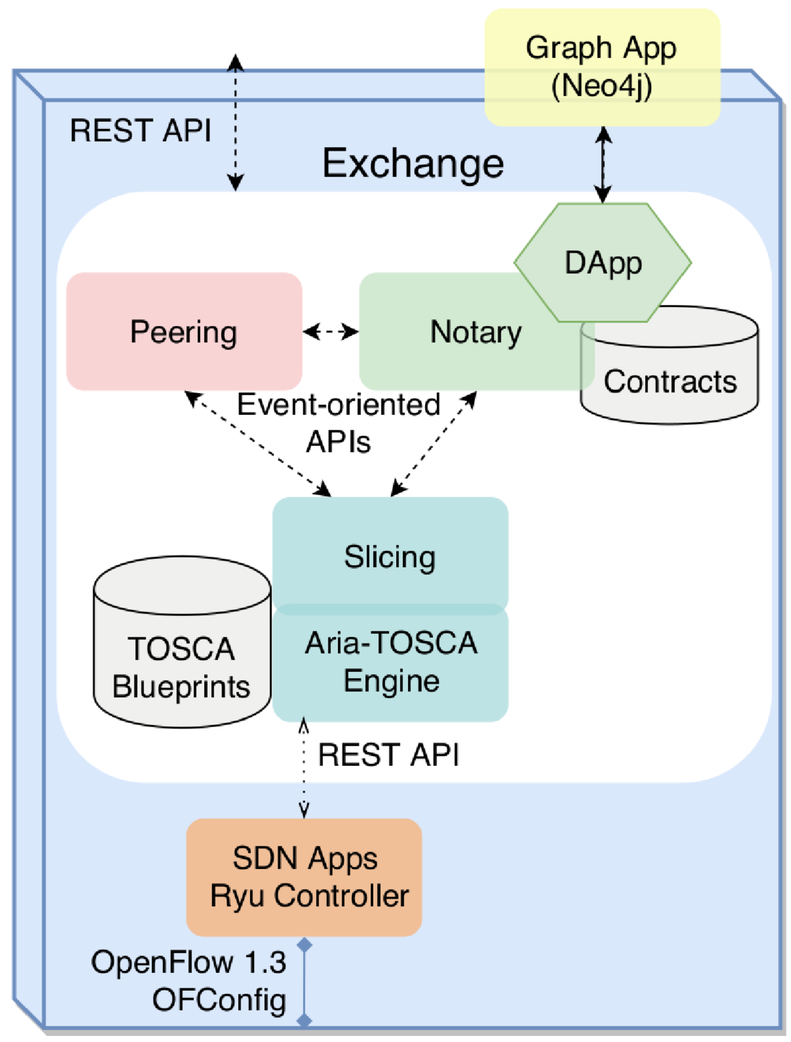
Motivation

- Administrative domains are non-trusting counterparts
- End-to-end network services increasingly complex (a.k.a. slices)
- Need for agility and transparency in multi-administrative networking (inter-domain SLAs)
- Blockchain provides on-demand consensus for distributed transactions
- Blockchain-based DApp (Decentralized Application) can realize smart contracts for lifecycle management workflows in multi-administrative domain networking

Why not Blockchain?

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 Rules	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





Demo Scenario

Demo Outlook

- Semantic relationship among smart contract and TOSCA Blueprint
  - Defines what/how/when events are being registered
- Performance measurements (cpu, memory, disk)
- Graph Model of chronological life cycle management events in multi-administrative domains
- Architecture mappings to different scenarios under standardization lenses
- Activities associated with multi-administrative networking and blockchain sit still in an early stage, respectively constructing detailed requirements and mature operational evidence

Challenges Ahead

- Performance: Bounded guarantees of transaction confirmation time must be well defined while realizing MdO operational phases by blockchain DApps
- Scalability: There must exist well defined operational metrics (e.g., storage overhead) to represent the scaling dimensions of a blockchain network across providers.
- Security: The design of a MdO blockchain network must define an architecture that guarantees its progress and safety (e.g., avoiding 51% attacks) while sustaining the policy regulations of network assets in administrative domains.
- Provenance: Certification and reputation schemes must be designed by administrative domains to assure semantical association of the provided information in a smart contract with an actual network asset, as blockchain does not impose guarantees of provenance

Reference - Raphael Rosa and Christian Esteve Rothenberg. "Blockchain-based Decentralized Applications for Multiple Administrative Domain Networking". In IEEE Communications Standards Magazine, Sep, 2018.
Acknowledgements - This research was partially supported by the Innovation Center, Ericsson S.A., Brazil, grant UNI.62, 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 (MCTIC) through RNP and CTIC..