Trusted Registry of correlation patterns and next best action for Networks

Rakesh Girija Ramesan Nair
rakesh_ramesannair@infosys.com
Senior Technology Architect
Amsterdam, Netherlands

Abstract—The paper is envisaged to explain how we can leverage blockchain based technology to create a trusted registry of frequently observed correlation patterns and their next best action across network domains. One of the key challenges across Telecom service providers is the network operations area with multi-vendor multi-cloud kind of scenarios across domains like core, access and mobile. Service Providers across the globe have been looking at AIOPs tools/modules for proactively identifying the issues, patterns and the best action that need to be performed for correcting the same. Identifying the next best action is difficult as the type of network, vendor involvement will vary across various service providers.
This article covers the possibilities to be explored with blockchain, the challenges it poses and how it can help telcos across the globe.

Keywords— **AIOPs, Blockchain, Closed Loop Assurance, Autonomous Networks, Intelligent Management**

I. Introduction

Emerging technologies are being explored by all Telcos across the globe to identify the right fit and drive potential benefits. Blockchain is one such technology that if applied appropriately in the networking space can help generate more revenue and address some of the key problem areas.

The hindsight is that the benefits of blockchain are immense & real. Most telcos are undergoing a transformation which affects the way they are run and its customer relationships. Companies have already embarked on the journey to adopt cloud computing, SDN and NFV practices to enable smart networks.
Having an efficient network operation division is key to the success of service providers in ensuring maintenance of existing customers and for creating the leeway for building new customer base. Every service provider across the globe is working on streamlining operations by embracing emerging technologies and automation is key in this journey. An effective Operational approach can deliver better customer service experience at lower cost.

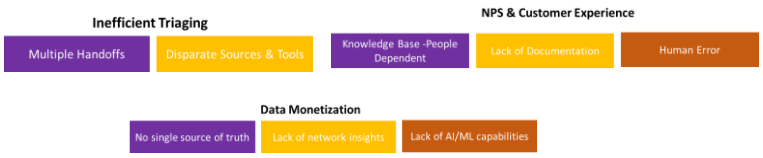

Fig. 1 Key challenges in the network operations space

II. Industry Alignment

A key focus area across Telco industry is around autonomous networks. Industry bodies like ETSI, TM Forum and MEF are working along with communication service providers and equipment manufacturers to create an architectural reference model that can be reused.

- ETSI - Generic Autonomic Networking Architecture (GANA) - Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services

- Closed Loop Anomaly Detection and Resolution Automation (CLADRA) – AI-CLA reference architecture defined by TM Forum. The architecture addresses a key area of any service provider to improve operational efficiency and resilience with faster problem detection and resolution aiding in zero- down-time.

- CAMARA a Linux Foundation initiative with close collaboration from GSMA Operator Platform Group to expose Network capabilities as API's. The focus in CAMARA for this paper would be technology-specific APIs that offers programmable access to telco infrastructure, network, service, and IT capabilities.

The proposed solution is aligned with the industry bodies reference architecture and in addition brings in blockchain technology to share the experience and learning from other telcos that can be consumed and used by closed loop assurance systems to improve their own decision making.

III. Blockchain - a Short introduction

Some of the key words that needs to be familiarized in a blockchain context is asset, ledger, participants, channel, transaction, and contract.

A basic architecture for blockchain provides participants a shared ledger which gets updated every time a transaction occurs. It is ensured via cryptography that participants in a channel see only parts that are relevant to them. These transactions are highly secure, verifiable, and authenticated. Smart contracts are programs that execute on the blockchain, that helps digitize contract management and automate manual intensive dealings that exist between multiple organizations. Shared Ledger helps maintain an immutable ledger containing all transactions involving all participants in the corresponding business network. It ensures visibility to all participants on what is happening, thereby ensuring transparency. Any kind of conflicts or issues are avoided as the transactions need to be endorsed by relevant participants, thereby adding the most important feature of trust. Equity and equality in blockchain are ensured through consensus. Variety of consensus algorithms are available to optimize computational power and time required.

The above characteristics of blockchain like immutability, trust, consensus help reduce risks, time to market and cost by providing the required quality and conviction.
Blockchain can be categorized into two mainly Permissionless and Permissioned.

Permissionless blockchain technology are public networks where anyone can participate anonymously. To overcome lack of trust in this type of blockchain technology it uses an incentive cost in return for high transactional & computational powers.

Permissioned block chain works within a closed network where we have trusted participants operating under a governance model. Consensus algorithms is key to maintain the integrity of the chain ensuring that no single node or group can manipulate the network. Consensus algorithms are critical in blockchain technology enabling the below: -

- Security
- Decentralization – all nodes come into a consensus for validating a transaction.
- Transparency
- Efficiency

The consensus algorithms are applicable across both Permissionless and Permissioned blockchain categories. The focus on this paper is more around permissioned blockchain and related algorithms.
Examples of consensus algorithms used in Permissionless blockchain are Proof of Work, Proof of Stake its different variants, Proof of Authority etc. Similarly in Permissioned blockchain we see usage of Byzantine Fault Tolerance, its different variants, Proof of Elapsed Time etc. Hyper Ledger Fabric is one potential example that can be leveraged to build permissioned blockchain solution as the nodes are known and trusted.

IV. Solution – Trusted Registry using Blockchain integrating with AIOps

Fig 2 represents a complex orchestration architecture model in a Telco world: -

i. An MDSO (Multi-Domain Service Orchestrator) to break down the complex tasks, sequence them in a proper workflow including parallel execution.
ii. A Network Data Store (NDS) that has access to real-time and historical data of systems from all domains.
iii. A closed loop assurance or AIOps system that can auto correct based on real-time and historical data.
iv. Domain Controllers/Orchestrators that abstract the complexity from MDSO and executes specific tasks.

Network Operation in a service provider world is undergoing a paradigm shift. The increasing demands on network with complex networks, 5G – distributed edge with hybrid cloud environments raises the need for an intelligent /smart network operations system. AIOps adoption has been on the rise and is seen as one of the must have solutions. The journey towards intelligent networks involves moving from reactive to proactive to predictive. Machine learning and Artificial intelligence plays a crucial role in reaching the target state of being predictive.

Key to this journey is collecting network data from discrete systems like EMS, Domain Controllers, Network Devices from multiple domains into a single source of truth – Network Data Store.
Telcos across the world deploy an intricate ecosystem of network devices and systems managing the various network domains. Over a period managing these network elements and system has become more complex. Depending on the type of network domain in a Telco – the involvement of the network equipment manufacturer varies. Data from different network domains like Core, Cloud/Applications, Domain for each access network type - Mobile, DOCSIS, xPON etc all need to be collected into single source of truth -Network Data Store. It is a known industry problem that each vendor follows a different data model and do not completely align to any standard models. Network data store should have: -

- Data from the different network domains including telemetry, alarms, events, configuration, and inventory.
- Along with this knowledge models including from network equipment manufacturer is key to defining remedial actions.

As explained the overall Telco ecosystem is complicated and having a single vendor or stakeholder intelligent solution is not viable.

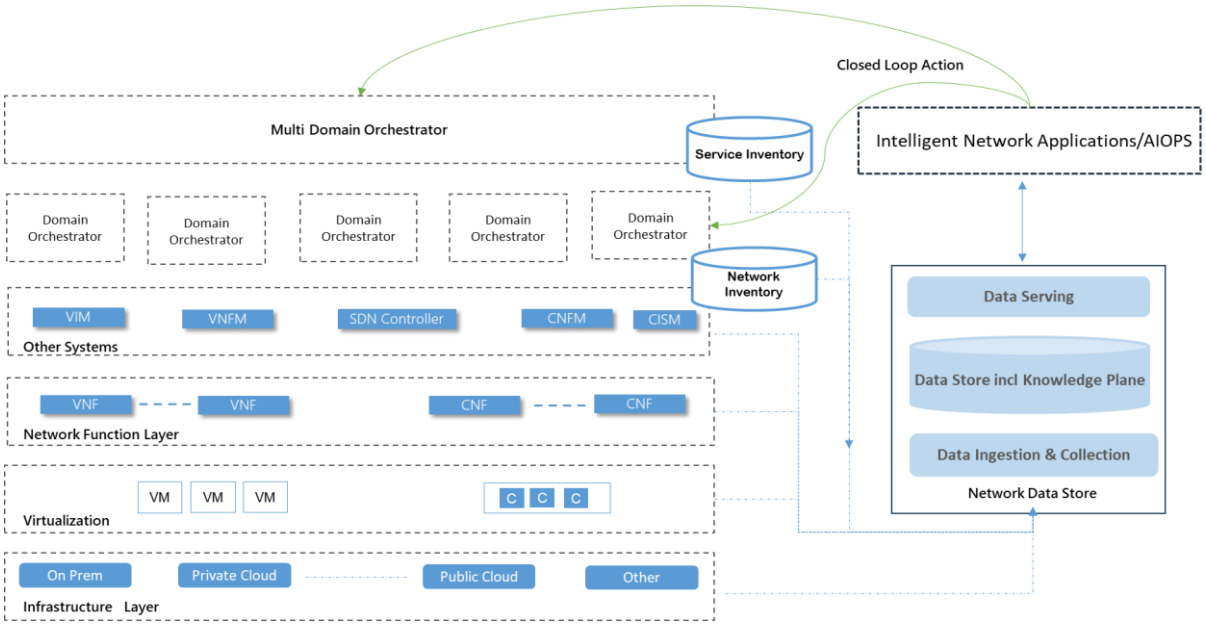

Fig. 2 Complex orchestration model in a Telco

Defining common data model across domains and having data transformation to convert available raw device data into a structured format is complicated and involves deep learning/expertise. Standardization for data consumers (like Intelligent Management Applications) via industry body defined models is very important in realizing the true potential of network data store.

Having real time and historical data collected in one place helps fast track the process as the intelligent network management applications can consume data from one single place and focus on the key capabilities like AI/ML algorithms that can be run, rather than having to work on the different integration touch points.

AIOps system run their AI/ML algorithms on historical data to unearth various patterns or correlations that results in network anomalies. With the network becoming programmable many of these abnormalities can be auto corrected via programmable interfaces exposed via the various layers of the orchestration system including the network devices (CNF, VNF, PNF). Most of the network equipment manufacturers already have an internal knowledge base system that deals with many of the common customer network failures and the next best action that need to be taken.

The proposed solution in this paper is very much aligned with the TM forum ODA Intelligence Management. There is considerable similarity in the ODA Intelligence Management functional block and ETSI - Generic Autonomic Network Architecture (GANA).

The core part of this paper is to leverage a permissioned block chain solution to store these network patterns and next best action, which will be part of the local knowledge base and if approved by the Telco moves to a centralized knowledge base which can be used by other Telcos as well.

The proposed solution architecture is agnostic of Telco organization or not constrained by the nature of implementation. The solution is applicable irrespective of the maturity of the orchestration solution in the Telco, be it legacy or the transformed modern orchestration model.

V. IMPLEMENTATION APPROACH

The proposed solution has two parts and is designed to complement a service providers existing orchestration landscape by enabling blockchain based knowledge base. One which will be deployed and maintained within all Telcos holding the localized knowledge base. Second more of a digital marketplace where commonly observed network anomalies and their next best action in localized knowledge base is published centrally. This would encourage reusability across Telcos, help standardize the data synchronization of knowledge base and enable faster cycle towards intelligent networks.

A. Localized Knowledge Base

This section of the paper covers the solution part which is deployed locally in a Telco.

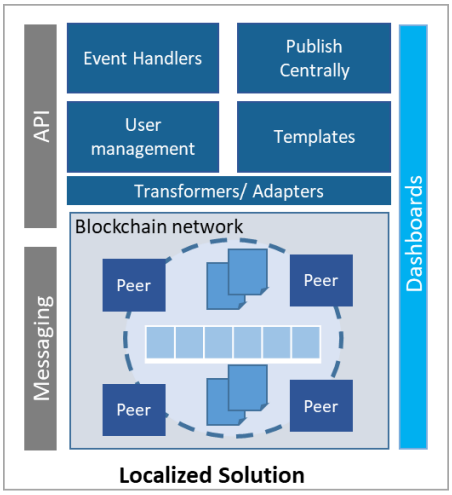

Fig. 3 Solution architecture for localized deployment

The solution provides a portal where smart contract would be defined upfront based on the service provided by the CSP and the associated SLA. Customer experience is of paramount importance and, hence maintaining the SLA.

Mapping blockchain terminologies to the solution construct: -

- Asset – would be a network pattern or anomaly detected against a service.
- Participants - Service Provider, Network equipment manufacturers involved in providing the different network functions, Cloud Provider where the infrastructure is hosted and possibly the service orchestration vendor as required.
- Smart Contract – Defining the various SLA that needs to be met as part of providing the E2E service to customer.

Every time Intelligent Management application identifies a network pattern it is send to the blockchain solution which then based on the type of network and service involved validate the transaction through smart contracts.

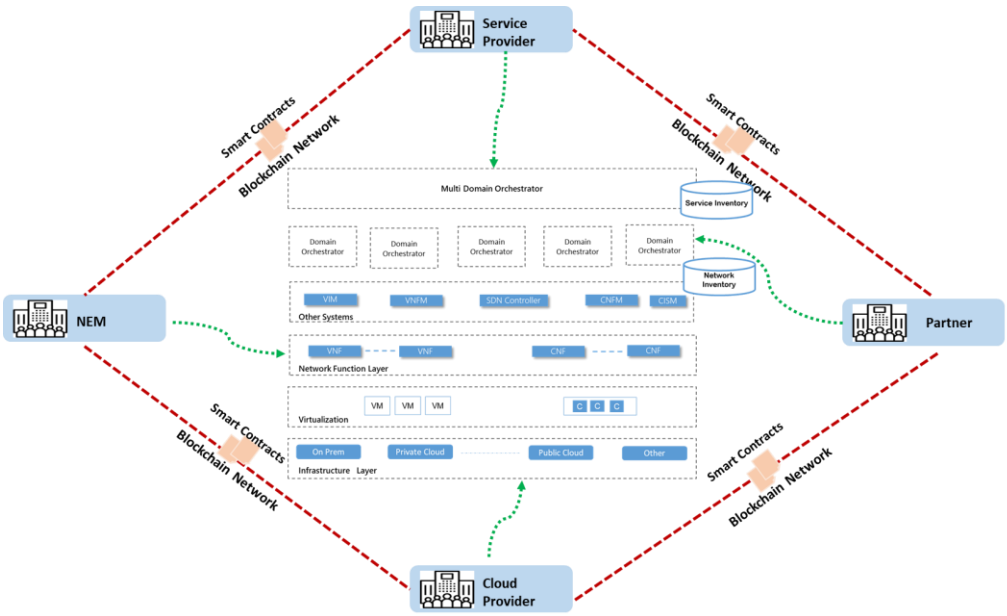

Fig. 4 Sample Smart Contract representation with possible participants

Once the business contract between the various participants is agreed, we can have them as executable programs in the blockchain network. This is more efficient than the manual process followed currently. Hyperledger Fabric based permissioned blockchain network is considered to provide solution references examples. Smart contract and chaincode are terms commonly used with Hyperledger Fabric, chaincode is the package that is deployed into the blockchain network and can contain multiple smart contracts. Smart contracts have endorsement policy associated with it and it identifies the participants/organizations that is required to make a transaction valid. The transaction validated through smart contracts (endorsed by all participants) will be added to the block chain and from then onwards is immutable. The asset ledger can then be updated whenever such patterns occur in the network and is rectified by the next best action defined.

In this context based on the type of network and customer service, the type of participants involved will vary. Hyperledger Fabric provides an option for participants to simultaneously involve in multiple blockchain networks via the concept of channels. Channels provide an efficient mechanism for participants to involve maintaining their security and data privacy. Depending on the number of participants, implementation of smart contracts in each node and their endorsement policy the time taken to commit results to the ledger will also vary.

B. Centralized Knowledge Base

The centralized knowledge base forms the second part of the solution which acts as a marketplace or as a service offering which can be regularly consumed by the localized knowledge bases. On demand basis pull from centralized to local knowledge base is also possible. Telco's who are in the journey of AIOps transformation do not have to start from scratch and can leverage the knowledge from across Telco's for the different type of networks. From data publish perspective, once there is sufficient confidence on the pattern within the localized environment this can be published to the centralized knowledge based. The decision to make it available to other Telcos can be only done after all specific regulatory security checks have been completed. This includes actions like whether the asset has been verified, audited for data governance, provenance and any GDPR enforcements considered. This solution opens a whole gamut of opportunities where data can be shared across organizations with mutual trust. This blockchain based solution allows all service providers anywhere in the world access to reliable data without being able to modify it

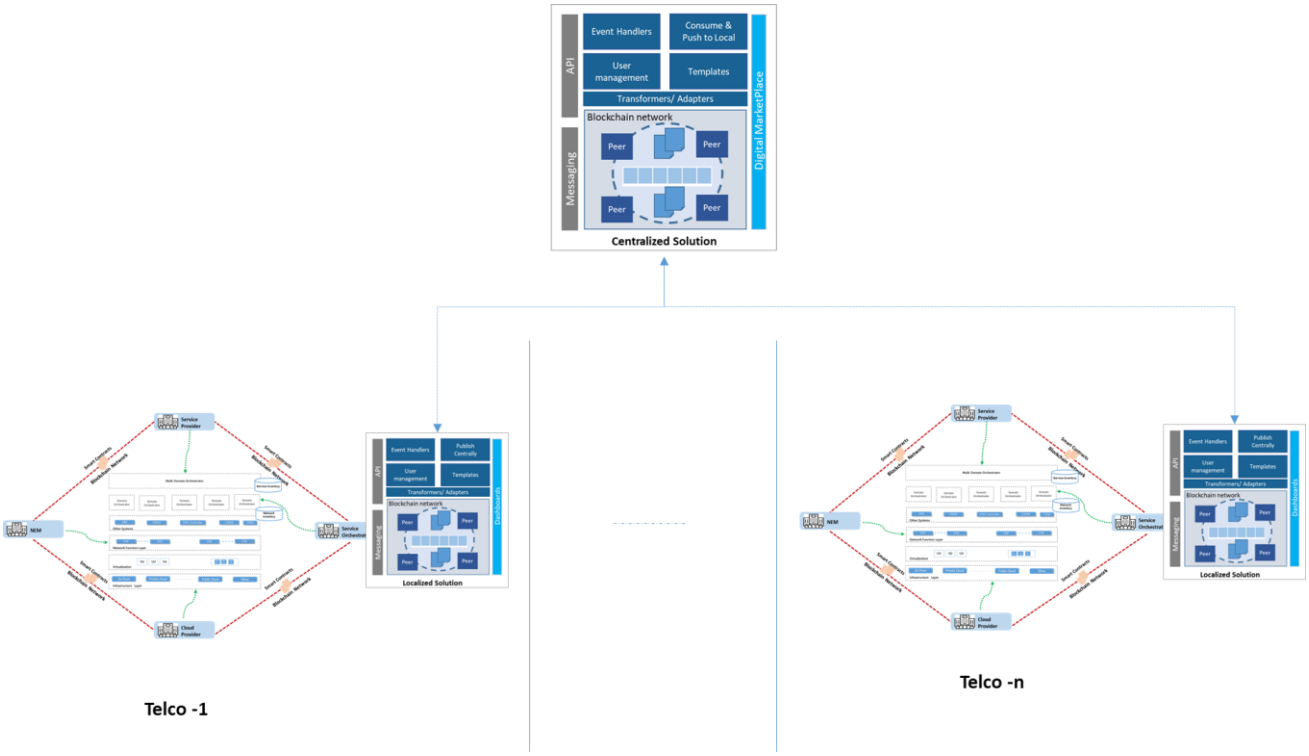

Fig. 5 Centralized knowledge base shared across Telcos.

C. *Implementation Challenges with Blockchain*

While the recommended solution leverage blockchain, implementing this has its own challenges. Having the right expertise and understanding is key to implement. Below listed are some of key challenges while using blockchain for implementing enterprise solutions: -

- Lack of data standards between various systems for seamless connectivity, read, write, and interpret data on blockchain. It will aid in interoperability and scalability of the blockchain implementation.

- Complexity in creating specific data access and protection to blockchain solutions. Since data on blockchain is immutable, hence the recommendation to use permissioned blockchain technology.

- Understanding governance in blockchain is a challenge since there are many parties involved. No standard framework currently available for the blockchain network governance. The focus has been shifting from off-chain to on-chain where all the updates are provided to participants automatically and reaching a consensus.

- Scalability including management of growing users & data pruning is another major challenge while implementing blockchain. As the number of transactions increases the block containing them in the chain also grows resulting in lengthier transaction times. We would need to prune the blockchain for data efficiency as it grows year on year. Most blockchain solutions currently don't support pruning.

VI. POTENTIAL BENEFITS

There is a compelling need to apply AI/ML based algorithms on past and real time data/Knowledge to identify “unknown “network anomalies due the complexity of networks and services that are being provided today. AIOps system designed today work more on a localized environment with limited reusability or cross-learning. The next best action defined are predefined workflows in the automated system with very limited trust.

The solution described above address the various challenges and brings a more collaborative way of working through standardization across Telcos.

A. *Better Agility*

Looking at the rapidly evolving network space and customer demands having flexibility and agility is key to success. Leverage AI knowledge base with trust that the proposed solution offers to meet the increasing & changing demands.

B. *Improved Collaboration & reusability*

Lack of a collaboration platform where data can be exchanged with trust resulting in siloed use of solutions and data. The blockchain based trust registry will help achieve better collaboration and reusability across Telco organizations.

D. *Smart Operations*

The solution helps provide access to a rich set of information that helps the service providers operate in a dynamic way. Intelligence sharing across Telcos help fast-track the journey towards autonomous networks.

E. *Less Error Prone*

Complex operational management using humans is error prone and risky. Improved visibility of anomalies leading to network issues through the Trusted registry solution. Moreover, less error prone since asset history would provide the much-needed confidence in the identified pattern and the next best action defined.

F. *Productivity Improvement with reduced Cost* -

It takes a lot of time and high cost/skilled expertise of different technology to identify these anomalies and next best action. Leveraging the centralized trusted knowledge base solution helps jumpstart and provide the much-required operational efficiency.

VII. CONCLUSIONS

Industry bodies have defined reference architecture for Intelligent Management and Knowledge base models. No defined implementation approach or solution has been prescribed. The paper covers a solution with an implementation approach defined leveraging emerging technologies like blockchain to build the much-required trust across Telcos.

ACKNOWLEDGMENT

I would like to acknowledge my organization, Infosys whose policies towards continuous learning and improvement fosters the much-needed inquisitiveness to innovate and look for new ideas. I would like to thank my seniors, mentors in the organization who have guided me throughout. I would also like to thank my family (wife and son) without whose understanding and support, I would never have been able to find those extra hours after my work to pursue the ideas that help us to innovate and succeed.

.

REFERENCES

[1] IG1167_ODA_Functional_Architecture_Exploratory_Report_v6.0.0
[2] IG1219A_AI_Closed_Loop_Automation_Management_v1.3.0.
[3] GB998_Open_Digital_Architecture_ODA_Concepts_Principles_v2.1.0.
[4] IG1318_TMF_and_Camara_APIs_for_Telco_standardized_service_exposure_v1.1.0
[5] https://hyperledger-fabric.readthedocs.io/en/release-2.5/
[6] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
[7] https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/HL_Whitepaper_IntroductiontoHyperledger.pdf
[8] https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf
[9] https://www.sciencedirect.com/science/article/pii/S2405959521001041
[10] https://escholarship.org/uc/item/5jt327gh

Definitions/Abbreviations

ETSI	European Telecommunications Standards Institute
MEF	Metro Ethernet Forum
SDN	Software Defined Networking
NFV	Network Function Virtualiztaion
AIOPS	Artificial Intelligence for Operations
CSP	Communication Service Provider
NEM	Network Equipment Manufacturer
SLA	Service Level Agreement
DOCSIS	Data Over Cable Service Interface Specification
xPON	any type of Passive Optical Network
ODA	Open Digital Architecture
E2E	End to End
API	Application Programming Interface
GANA	Generic Autonomic Networking Architecture
CLADRA	Closed Loop Anomaly Detection and Resolution Automation
TM Forum	TeleManagement Forum
AI	Artificial Intelligence
CLA	Closed Loop Assurance
GDPR	General Data Protection Regulation
ML	Machine Learning
CNF	Cloud-native Network Function
VNF	Virtual Network Function
PNF	Physical Network Function
MDSO	Multi Domain Service Orchestrator
NDS	Network Data Store