Managing Network Slicing Resources Using Blockchain in a Multi-Domain Software Defined Optical Network Scenario

P.Alemany(1), R.Vilalta(1), R.Muñoz(1), R.Martínez(1), R.Casellas(1)

(1) Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), pol.alemany@cttc.cat

Abstract *This paper presents an experimental validation to use a peer-to-peer network composed of network slicing managers to manage and share optical network resources using Blockchain in a network scenario with multiple domains and without the need of a central authority that validates any information exchange.*

Introduction

Nowadays, the strategy to add resources to give service to the maximum users possible is no more the best option as the resources might be under-used. A different possibility is to design a collaborative system in which the network owners collaborate and share their resources in a trustworthy and reliable way, whilst being able of offering different services across the network and keeping the privacy of each service consumer.

Network Function Virtualisation (NFV)[1] together with Network Slicing[2][3][4] allow a flexible and efficient network resources management and control. NFV defines the idea of deploying virtual devices over generic pieces of hardware allowing them to change their network role at any moment while Network Slicing aims to create virtual networks (over the physical one) called Network Slices (Slices) that are composed by virtual network devices and paths. A Network Slice Manager (Slicer) is the element in charge of the Slices life-cycle. It is placed on the top of a NFV Orchestrator (NFVO) to create the Slices composed by the interconnection of different Network Services (NSs) managed by the NFVO. In a multi-domain NFV scenario with multiple Slicers, it is necessary to have a common understanding among the different domain Slicers in order to create End-to-End (E2E) Slices. One option is the use of hierarchical architectures[5] with a single element on the top (Fig.1-A) controlling everything, the other option is a peer-to-peer (p2p) blockchain-based architecture (Fig.1-B) where all nodes are equal.

Blockchain is a database (DB) geographically distributed over a set of nodes that all together create a p2p network. In a Blockchain, there is no central authority as all the peers share the same information and rights to add or modify the data in the DB while maintaining it stable and safe using a consensus mechanism[6]. Using Blockchain, the resource information exchange between one network owner and another may be done using a procedure that follows a set of rules publicly known by all the peers. So, if one of them tries to act in a malicious way, the others will notice and block its fraudulent action. The most known examples of Blockchain are Bitcoin[7], Ethereum[8] and Hyperledger[9].

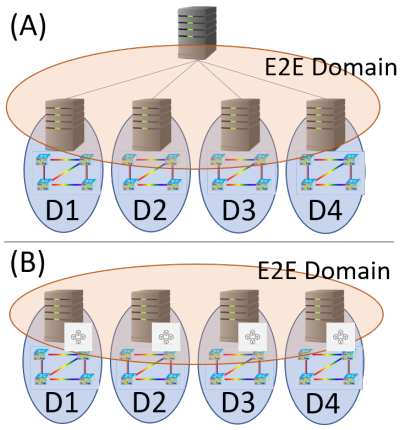

Fig. 1: Hierarchical (A) and P2P/Blockchain (B) Architectures

While the hierarchical architecture has been widely used[10], this paper aims to enforce the use of Blockchain to manage multi-domain Network Slicing resources, previously addressed in[11] only for data center resources. In this paper, we propose a distributed ledger solution for the previous described problems on top of a complete network scenario consisting of both compute and (transport) network resources. We analyze the benefits of Blockchain and Network Slicing on the services management across transport networks and finally present the results obtained using a real testbed infrastructure. Blockchain has been already used on the management of computing and optical network resources[12][13] but this is the first paper to experimentally use Blockchain on a p2p architecture for the E2E Slice management with multiple Slicers.

Integration of Blockchain in a Network Slicing multi-domain architecture.

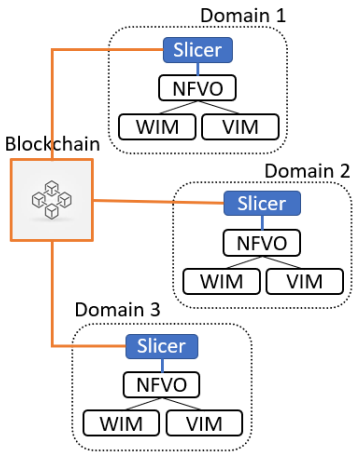

Fig. 2: Collaborative p2p Network Slice Manager architecture

Fig.2 shows the architecture used to develop the collaborative system. In common to all domains there is the Blockchain with the associated Slicers being the nodes that compose the p2p network. Each Slicer, makes the Network Slice Templates (NSTs) -i.e. the descriptor with the Slice definition- public and available to be used as a possible component (as slice-subnet) of an E2E Slice. Other than participating to the Blockchain, each Slicer is in charge of managing the resources in its domain when it receives intra-domain (local deployments) or inter-domain (through the Blockchain) requests. Then, under each Slicer, there is the NFV Infrastructure (NFVI), with the NFVO in direct contact with the Slicer. The NFVO is the responsible of managing and orchestrating the virtual elements in each domain using Virtualised Infrastructure Managers (VIMs) and managing the virtual flows over the transport paths using WAN Infrastructure Managers (WIMs). A VIM is a software able to create ad configure virtual elements -i.e. kVM or containers- in which the desired services are deployed. A WIM is a Software-Defined Networking (SDN) controller that allows to create virtual paths over the optical transport networks and interconnect the different domains of a network.

For all this architecture to work and so, to have the desired collaboration, the deployment of an E2E Slice has been designed to follow the steps presented in Fig.3. As an example, a vertical in domain 1 wants an E2E Slice composed by a set of slice-subnets -i.e. NSTs-: some owned by its local domain Slicer -i.e. Slicer D1- and others owned by other domain Slicers -i.e. Slicer DX-. First the vertical requests the E2E Slice to define the elements to compose it (1) to the Slicer D1. Then Slicer D1 creates the Network Slice Instance (NSI) object with the description of the E2E Slice and looks for the domain each slice-subnet belongs to. If the slice-subnet is one of its own, then it requests its deployment to the NFVO below (2). Whereas the slice-subnet belongs to another domain, Slicer D1 passes the requests to the Blockchain (3) which warns all of its associated Slicers (4) and informs them that the transaction was completed by the Slicer D1 (5). Meanwhile, Slicer DX keeps the instantiation of their NSTs (6) requested through the Blockchain. While all the slice-subnets are being deployed by the appropriate Slicer, the Slicer D1 controls all the slice-subnets belonging to the E2E Slice: either of the local deployments (7) or when an inter-domain slice-subnet is ready and the Blockchain is informed (10), this warns about the readiness of the slice-subnet (11) and confirms tha the transaction was correctly done (12). In both cases, if the checked slice-subnet is the last one missing to compose the E2E Slice, then the Slicer D1 finishes the whole process and updates the NSI object (8 and 13), otherwise it keeps waiting for the remaining slice-subnets (9 and 14).

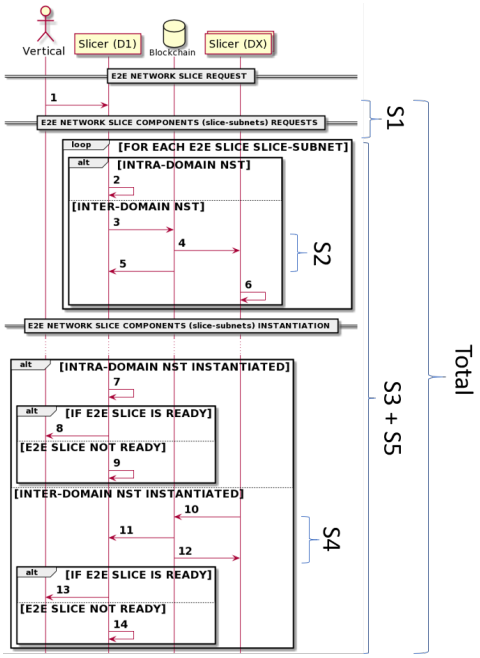

Fig. 3: Collaborative p2p Network Slice deployment workflow

Experimental validation

In order to validate the proposed architecture and workflow, a set of tests were done using the CTTC ADRENALINE Testbed. This infrastructure is composed of different transport networks (both packet and optical-based) and different domains such as four edge Data-Centers (DCs) and one core DC among other capabilities which are out of

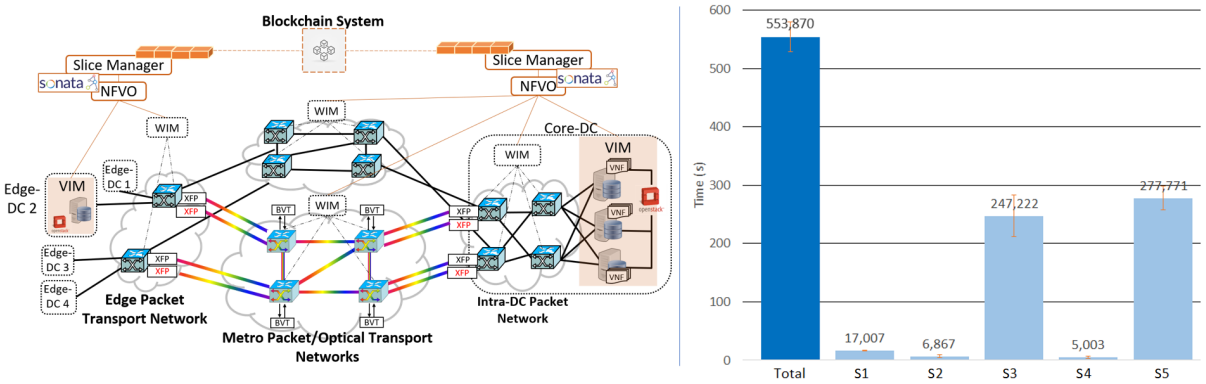

Fig. 4: Experimental Architecture (left) and measured setup delay (right)

the scope of this paper such as a vehicle domain. Regarding the management of the computing resources across the architecture, there are two different technologies available: Kernel-Virtual Machines (kVM) and containers. In order to interconnect all these domains, the architecture has different transport networks that make use of both packet and optical technologies. Each domain follows the architecture presented in Fig.2: on the top of each domain, there is a SONATA Service Platform (SP) software instance that has both Network Slicing and NFVO functionalities and in parallel they also act as a peer of the created Ethereum Blockchain. Each SONATA SP has a set of associated VIMs and WIMs to control the domain resources.

Following the same procedure done in previous work[11], an E2E Slice composed by 2 NSTs distributed in the Edge-DC2 and Core-DC in Fig.4(left) was deployed 10 times. Based on the amount of resources available in each DC, the NSTs were composed of a single NS with 2 VNFs (3 VMs in total) in the Edge-DC2 and 3 NSs using the same NS (9 VMs in total) in the Core-DC. So the E2E Slice was composed of 12 VMs in total distributed across the two used DCs.

Together with the workflow in Fig.3, there are the different time samples we used to verify the influence of Blockchain over the total time of an E2E Slice deployment. Fig.4 (right) presents the mean set up time values to deploy the E2E Slice (from the moment it is requested until it is completely deployed) and Tab.1 contains the corresponding standard deviation values. The first column shows the total time which is then divided in five time steps: (S1) since the requests arrive to the Slicer until the E2E Slice instance data object is created, (S2) the time to pass the inter-domain slice-subnet request to the Blockchain and for this to be accepted by the appropriate Slicer, (S3) instantiation time, (S4) when the inter-domain slice-subnet is ready and the Blockchain is updated, (S5) the rest of the E2E Slice instantiation time.

Looking at the contribution of each time-phase, it is quite clear that Blockchain has no big influence on the deployment time. Steps S2 and S4 are the two periods of time in which Blockchain is involved: when the local Slicer sends an inter-domain request to the Blockchain, so it can warn the other Slicers about the necessity of deploying a slice-subnet -i.e. S2 = 6,867s- and when a slice-subnet is ready and its information has to reach the Slicer that has requested it -i.e. S4 = 5,003s-. These two values compared to the others are the lowest values and so, they are the time values that least affect the overall instantiation process. Adding the times of these two steps -i.e. S2+S4 = 11,87s- and comparing it to the total instantiation time (553,87s), the percentage of influence is equal to a 2,14% of the total time.

Tab. 1: Time steps standard deviation

σ (s)					
Total	S1	S2	S3	S4	S5
24,7	0,3	2,8	35,8	2,1	20,7

Conclusions

This paper has presented a new possible architecture to manage network resources through the use of Blockchain and Network Slicing. In addition, it presented the possible influence that the added Blockchain layer might have on the deployment of an E2E Network Slice across different domains using a real testbed infrastructure with multiple domains interconnected through optical/packet transport networks. Finally, its results demonstrated the low influence of Blockchain over the whole process.

Acknowledgements

Work partially funded by the EC through the 5GPPP INSPIRE-5GPlus (871808) and MINECO AURORAS (RTI2018-099178-B-I00) projects.

References

[1] NFV-ETSI-ISG, *Network functions virtualisation (nfv);management and orchestration*, 1st ed., ETSI, 650 Route des Lucioles - Sophia Antipolis (FRANCE), Dec. 2014.

[2] 3GPP, *Study on management and orchestration of network slicing for next generation network*, 15th ed., 3GPP, 650 Route des Lucioles - Sophia Antipolis (FRANCE), Jan. 2018.

[3] T. Soenen, R. Banerjee, W. Tavernier, D. Colle, and M. Pickavet, "Demystifying network slicing: From theory to practice", in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 1115–1120.

[4] P. Alemany, J. L. de la Cruz, A. Pol, A. Roman, P. Trakadas, P. Karkazis, M. Touloupou, E. Kapassa, D. Kyriazis, T. Soenen, C. Parada, J. Bonnet, R. Casellas, R. MartÃnez, R. Vilalta, and R. Muñoz, "Network slicing over a packet/optical network for vertical applications applied to multimedia real-time communications", in *2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, IEEE, 2019, pp. 1–2.

[5] R. Muñoz, R. Vilalta, R. Casellas, R. MartÃnez, F. Vicens, J. Martrat, V. LÃ^3pez, and D. LÃ^3pez, "Hierarchical and recursive nfv service platform for end-to-end network service orchestration across multiple nfvi domains", in *2018 20th International Conference on Transparent Optical Networks (ICTON)*, IEEE, 2018, pp. 1–5.

[6] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks", *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *Cryptography Mailing list at https://metzdowd.com*, Mar. 2009.

[8] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[9] The Linux Foundation. (2020). Hyperledger official website, [Online]. Available: `https://www.hyperledger.org/` (visited on 08/26/2020).

[10] D. Gkounis, N. Uniyal, A. S. Muqaddas, R. Nejabati, and D. Simeonidou, "Demonstration of the 5GUK exchange: A lightweight platform for dynamic end-to-end orchestration of softwarized 5g networks", in *2018 European Conference on Optical Communication (ECOC)*, 2018, pp. 1–3.

[11] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas, and R. MartÃnez, "Peer-to-peer nfv service platform for end-to-end network slice orchestration across multiple nfvi domains", Accepted in the Workshop on 5G Security: Current Trends, Challenges and New Enablers belonging to the IEEE 5G World Forum (5G-WF) Conference, Jul. 2020.

[12] S. Kou, H. Yang, H. Zheng, W. Bai, J. Zhang, and Y. Wu, "Blockchain mechanism based on enhancing consensus for trusted optical networks", in *2017 Asia Communications and Photonics Conference (ACP)*, 2017, pp. 1–3.

[13] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5g", in *2017 16th International Conference on Optical Communications and Networks (ICOCN)*, 2017, pp. 1–3.