Blockchain-over-Optical Networks: A Trusted Virtual Network Function (VNF) Management Proposition for 5G Optical Networks

Avishek Nag[1], **Anshuman Kalla**[2], **Madusanka Liyanage**[1]

[1] *University College Dublin, Ireland,* [2] *Manipal University Jaipur, India*

avishek.nag@ucd.ie, anshuman.kalla@jaipur.manipal.edu, madhusanka@ucd.ie

Abstract: In this paper, we discuss the security issues revolving around the management of VNFs in 5G optical networks; and present a high-level view of work-in-progress by leveraging a Blockchain-over-optical network to mitigate these issues.

OCIS codes: 060.4250, 060.4256.

1. Introduction

Optical networks or generally the telecom networks are constantly evolving with newer technological driving factors. In future telecom networks, where most of the control and management is envisioned to be software-defined [1], the network functionalities such as firewall, deep packet inspection, encryption, intrusion detection system, etc. are expected to be deployed as software entities running as virtual machines in some cloud data centres [2] (as opposed to traditional hardware middleboxes). This paradigm is termed as Network Function Virtualization (NFV) and the soft network functions are called Virtual Network Functions (VNF). Thus the software-defined network control and orchestration along with NFV form the major building blocks for next-generation agile and automated networks that would enable high degree of flexibility, fine-tuned manageability, ubiquitous and large-scale connectivity for evolving 5G networks, Internet of Things (IoT), Cyber Physical System (CPS), etc. Especially for 5G and beyond networks, where some applications such as autonomous ground vehicles and UAVs require highly reliable connectivity and a service set-up time of the order of milliseconds, may demand the deployment of VNFs at edge nodes which are closer to the users [3]. Usually, VNFs are implemented in the core network data center or clouds. Figure 1 shows an instance of 5G network configured with cloud data centres which would run the orchestration software that handles migration of the VNFs to the edge nodes (as and when needed) in a distributed fashion to support 5G IoT use cases. Such orchestration software are generally realized by an open source Management And Network Orchestration (MANO) framework.

The migration and overall management of VNF are vulnerable to various security issues. During the VNF migration, MitM (Man-in-the-Middle) attacker can modify arbitrary VNF or application states [4]. Moreover, a malicious VNF can misuse the privileges of hypervisor to install pernicious kernel root kit in edge nodes' Operating System, and manipulate the other VNFs and the edge node [5]. Moreover, an attacker can migrate a compromised VNF to an edge node which has less security or privacy policies to gain additional access to the system [5]. Even after the deployments of VNFs at edge nodes, malicious VNF applications can consume high CPU, hard disk, and memory resources at the edge node so that, they can exhaust the hypervisor resources to other VNFs [5]. Therefore, it is necessary to have a proper auditing and verification platform to enable the trust between the VNFs, the edge nodes, and the centralized cloud. Moreover, the network softwarization in 5G offers the flexibility to use VNFs which are provided by the different VNF suppliers. Different suppliers can offer the VNF with similar service features. Then, it is the job of the MANO to select the best VNF for the particular instance. In order to take this decision, the MANO has to know the price of the VNF instances and also the quality of VNFs. Some kind of historical performance metric or rating system will be helpful to take such informed decisions.

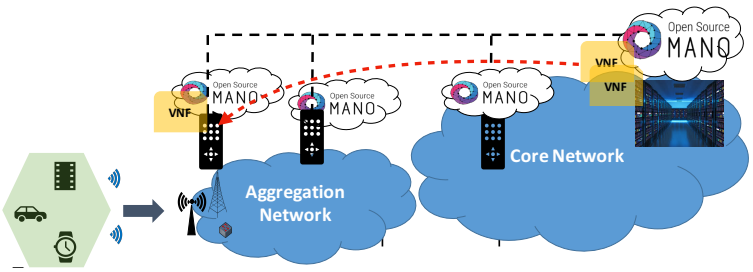

Fig. 1. VNF Migration in edge nodes.

To solve these inevitable issues Blockchain technology, featured with decentralization, cryptographic techniques, consensus-driven mechanism, etc., can offer an intriguing alternative. Blockchain technology has received all-around attention from the industry as well as academia. It has been viewed as one of the most important innovations since the inception of the Internet as far as immutability, non-repudiation, proof of provenance, integrity,

privacy, etc., are concerned. In this paper, we propose a fully decentralized control plane empowered with trust and verification mechanism, with all its computing distributed across the optical network nodes, by leveraging the principles of Blockchain. Further, we identify some of the associated problems related to such implementation. This is a unique proposition as it will implement a fully decentralised orchestration framework for a telecom network, where the nodes collectively collaborate towards autonomy and cognition.

2. Proposed Blockchain-based Trusted VNF Management Platform

We propose a Blockchain-based trusted VNF management platform (Fig. 2). The decentralised implementation would enable availability of VNFs for latency-sensitive applications together with enhanced privacy and security of the VNFs. The Blockchain is a powerful technology that facilitates distributed and decentralised computing with a certain guaranteed level of security and privacy [6].

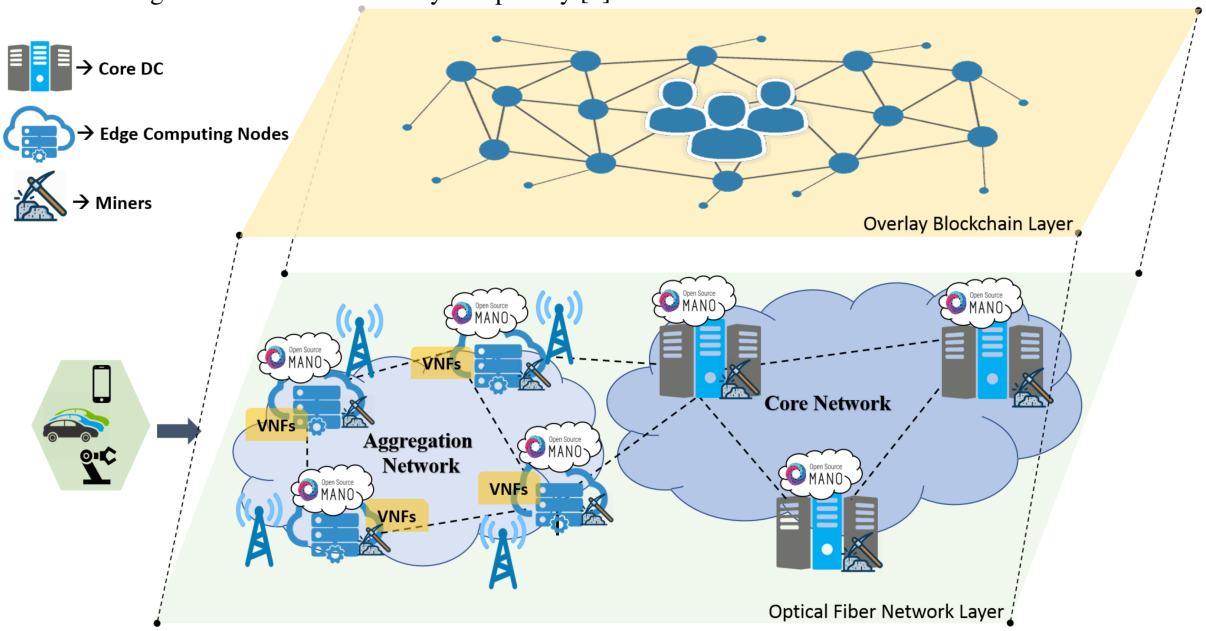

Fig. 2. A Blockchain-based implementation of the MEC example shown in Fig. 1

An instance of VNF is created and destroyed in a particular node, as and when needed, based on the network's requirements. Thus instantiation and destruction of VNF, malfunctioning of VNF, introduction of new VNF, upgradation of existing VNF, retrieval of non-functional or obsolete VNF, etc. can all be thought of as "transactions" in the Blockchain that can be verified and stored immutably in a distributed digital ledger maintained by P2P network of the participating nodes of the optical network. This will create a powerful, autonomous, decentralised, and trusted orchestration framework over a P2P network composed of the optical network's nodes [7]- [11]. Such a framework is expected to have numerous offerings, e.g.: (a) Proof of provenance of existing VNFs, (b) Logging of VNF usage that helps in optimized resource allocation and network provisioning, (c) Validity verification before instantiating a VNF, (d) Monitoring and authentic reporting of malfunctioning or defunct VNFs, (e) Smart contract based early detection of security breaches in VNFs, (f) Versioning and tracking of valid VNFs, (g) Authorized retraction of VNFs, etc. Note that, the underlying physical network/IT infrastructure can be heterogeneous in nature but the network nodes will logically form an overlay orchestration network enabling secure and trusted communication of the VNFs.

Blockchain-based implementation also suits well in the proposed scenario, as there will be multiple stakeholders owning the software and hardware entities hosted by the edge nodes. Precise use of smart contracts, deployed on the Blockchain, can automate clean and secure agreements between different stakeholders without the need of a third party. Blockchain can also be used to establish a marketplace for different VNF suppliers to sell their VNFs to the network service providers. With the added feature of Blockchain technology to solve security, safety, and transparency issues of traditional online marketplaces, it is able to offer a trusted environment for both service providers and VNF suppliers. Moreover, Blockchain-based reputation system [12] can be deployed over the same market place then, both the service providers and VNF suppliers can identify the reputed stakeholders.

3. Challenges

(a) Transaction Throughput: On one hand, to validate transactions and to create a block of valid transactions, the miners in the Blockchain network run a consensus algorithm that takes noticeable time. However, on the other hand, the low latency commitment of 5G and Beyond-5G networks requires VNFs set-up and tear-down to be very quick. Thus the use of Blockchain to enhance trust, veracity, and ease of VNF management in 5G optical network

without incurring visible delay is the central challenge to be addressed. There are some initial endeavours to deconstruct the Blockchain architecture and propose new methods to reduce the time for the consensus algorithm for Blockchain [13] but further scalable speed-up is still an open and difficult problem to be solved.

To put a bit of context, let us examine the expected transaction latency equation reported in [13] which is given by: $E[\tau] = \max\{a_1(\beta)D, (a_2(\beta)/C)\log(1/\varepsilon)\}$ seconds. Where D is the propagation delay, C is the capacity of the network, ε is the probability that there are more adversarial blocks in the Blockchain network than honest blocks (usually this parameter should be very small for a practical Blockchain network). $a_1(\beta)$ and $2(\beta)$ are functions of β which is the fraction of hashing power an adversary can control without compromising system security and usually for Bitcoin, $\beta < 0.5$. According to [13], $a_1(\beta) = [5400(1-\beta)/((1-2\beta)^3\log(1/\beta-1))]\log(50/(1-2\beta))$ and $a_2(\beta) = [5400/(1-2\beta)^3]\log(50/(1-2\beta))$. Now in a typical fiber optic network $D = 5\mu$S/km of fiber. Considering C being of the orders of Gbitss for each optical channel, and considering $\varepsilon = 0.01$ and say $\beta = 0.3$, the expected transaction latency would be given by: $E[\tau] = \max\{a_1(\beta)D, (a_2(\beta)/C)\log(1/\varepsilon)\} = \max\{0.31, 5\times10^{-6}\} = 0.31$ seconds for each km separation between the closest mining node and a transaction block. Therefore, we can see even with the novel speed-up reported in [13], not only the transaction latency is a bit higher if we envisage a distributed Blockchain for 5G optical networks but also there is a limit on how far the mining nodes can be from a transaction block. Therefore, there is a scope for improving this latency for 5G applications over optical networks.

(b) Resource Constraints of the Physical Nodes: Any form of distributed computing on top of distributed communication infrastructure is resource intensive, and requires new and improved optimisation frameworks [14]. Therefore, the distributed but intense computing to support a Blockchain over edge nodes will pose difficult research problems in resource provisioning which we intend to investigate in future.

(c) Extent of Penetration of VNFs in the Edge: Besides, power and computational resource constraints, deploying the number of instances of VNFs in an edge node is governed by other factors such as the users demands and the strict latency requirements of Beyond-5G services. The edge nodes hosting the VNFs have to be close to the users to meet Beyond-5G latency requirements. They have to be also closer to other neighbouring edge nodes forming the Blockchain network to meet the requirements of the fast consensus algorithm as discussed above in point (a). Hence there is a combination of complex trade-offs that need to be addressed.

4. Conclusion and Future Scope

In this paper, we envisage a distributed blockchain platform implemented by the nodes of an optical network and have mentioned some implementation challenges of it. We have also specifically highlighted how VNF migration from core data centers to the edge-computing nodes can be secured and trusted through this distributed Blockchain over optical networks. We believe a distributed Blockchain network over a telecom network as proposed here would generate lot of food for thought for the telecom network research community.

References

1. D. Kreutz et al., "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015.
2. R. Mijumbi et al., "Network Function Virtualization: State-of-the-Art and Research Challenges," IEEE Commun. Surveys & Tutorials, vol. 18, no. 1, pp. 236-262, First quarter 2016.
3. R. A. Addad et al., "Towards a Fast Service Migration in 5G," in Proc. 2018 IEEE CSCN.
4. X. He et al., "A Trusted VM Live Migration Protocol in IaaS, in Chinese Conference on Trusted Computing and Information Security. Springer, 2017, pp. 41-52.
5. S. Lal et al., "NFV: Security Threats and Best Practices," IEEE Commun. Mag., vol. 55, no. 8, 2017.
6. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf
7. I. D. Alvarenga et al., "Securing configuration management and migration of virtual network functions using Blockchain," in proc. IEEE NOMS 2018, Taipei, 2018, pp. 1-9.
8. P. K. Sharma et al., "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115-124, 2018.
9. U. Guin et al., "Ensuring Proof-of-Authenticityof IoT Edge Devices using Blockchain Technology, in Proc. The 2018 IEEE Intnl. Conf. on Blockchain, Jul. 30 Aug. 3, 2018.
10. M. S. Ali et al., "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," IEEE Commun. Surveys & Tutorials.
11. M. A. Ferrag et al., "Blockchain Technologies for the Internet of Things: Research Issues and Challenges, arXive:1806.09099.
12. R. Dennis et al., "Rep on the block: A next generation reputation system based on the Blockchain". In Proc. IEEE ICITST (pp. 131-138).
13. V. Bagaria et al., "Deconstructing the Blockchain to Approach Physical Limits, arXiv: 1810.08092.
14. E. Di Pascale et al.,"The Network as a Computer: a Framework for Distributed Computing over IoT Mesh Networks, IEEE IoT Journal, April 2018.