A Smart Distributed Marketplace

Evgenia Kapassa[1,2,*], Marios Touloupos[1,2], Dimosthenis Kyriazis[2],
Marinos Themistocleous[1]

[1] Institute for the Future (IFF), University of Nicosia, Nicosia, Cyprus
{kapassa.e, touloupos.m, themistocleous.m}@unic.ac.cy
[2] Department of Digital Systems, University of Piraeus, Piraeus, Greece
{ekapassa, mtouloup, dimos}@unipi.gr

Abstract. Online marketplaces are incredibly popular with customers around the globe selling products, also providing everyone as an online seller with a platform to reach a large, ready-to-buy products. Nonetheless, the issue is that it can be difficult to determine which one to trust as a seller. Especially in the world of 5G, where a marketplace is a mandatory component where developers can upload and verify their developed Network Services (NSs) or chained Virtual Network Functions (VNFs). Since those NSs are provisioned for a production environment, their consumers would need to trust the developer or the owner of that NS. To this end, in this paper we propose a smart distributed NFV Marketplace, in which we try to resolve security weaknesses related to the verification of the integrity of the developed VNFs and NSs. .

Keywords: blockchain · distribution · licensing · smart contracts · marketplace · NFV · 5G networks

1 Introduction

Undisputedly, the rapid evolution of mobile communications delivers a remarkable impact on the social and economic development. Network Function Virtualization (NFV) is expected to be the key enabler for agile network management in the upcoming 5G networks, as it will allow optimized service management through softwarization and virtualization of network components [1]. It is of no doubt that the advent of 5G will provide the support of a plethora of innovating services with improvements in system capacity and spectrum coverage. A challenge that arises, is the efficient composition of those Network Services (NSs) from heterogeneous Virtual Network Functions (VNFs). The paramount requirement of a unified framework is deemed indispensable for the exposure and the regulation of the services. Within this scope of the future Internet, an open marketplace comprises a key element in the advertisement and publication of the developed services from different vendors, introducing diversity in the context of network services [2]. The plethora of packages and diverse developers though, introduces an even more critical challenge regarding the incorporation of trust between end-users [3].

Distributed Ledger Technology (DLT) could redefine trust [4] due to the fact that spreads the idea that any type of transaction should be processed without a mediator. DLT gained notoriety by being used for the trading of cryptocurrencies, such as Bitcoins, which are issued and validated by the underlying Blockchain users rather than by a central authority. Recent Blockchain developments focused on the provisioning of trust, including also smart contracts. In the NFV context, these characteristics can be used to resolve security weaknesses related to the verification of the integrity of the developed VNFs and NSs.

The notion of such a decentralized marketplace of storing, retrieving, advertising, purchasing and comparing services is in absence in the 5G concept. To this effect, service providers and developers will be provisioned with a plethora of developed services from the various stakeholders, with seamless and expeditious deployments [5]. Consequently, the ultimate aim of the decentralized marketplace is to introduce the notion of an economic plane in the exchanges of VNFs/NS via the several stakeholders by promoting trust, anonymity and transparency.

To this end, in this paper we are proposing a design of a smart distributed NFV marketplace as a multi–faceted repository, supporting the storage, publication and proposal of the developed VNFs/NSs in a 5G infrastructure. Such component will not only provide a solution for exchanging and trading VNFs/NSs on the-fly, but also rely on the use of publicly auditable smart contracts, deployed in a blockchain that increase the transparency and trust, with respect to the provenance tracking and accountability of the provided NSs. As such, the proposed smart distributed NFV marketplace will act as a mean to commercialize new virtualized products and network-aware applications, by providing also licensing models, verified with smart contracts.

The remaining of the paper is organized as follows. Section II presents the related work and motivation of this study while in section III we introduce the overall architecture of the proposed “Smart NFV Marketplace” and its internal components. Finally, in Section IV, we conclude our work with some thoughts and ideas for future research.

2 Literature Review

In the context of a 5G infrastructure, a smart distributed marketplace can facilitate the high-availability storage of VNFs/NS, as well as a database containing the necessary meta-data of enriching the information of these entities. The ChoiceNet architecture [5] proposed a meeting ground for providing NFV advertisements and user requirements through common minimal semantics. In the ChoiceNet framework, the deployment of several open marketplaces provided their hierarchical arrangements of offering service bundling and auction services. This proposed approach was structured with the aim of the utmost importance of economic perspective of the services yet ignoring the integration with the production environment of a 5G infrastructure. On top of this marketplace template, NetEx [6] constitutes a network marketplace extending to the physical layer for a cloud datacenter. That approach provided the ground for the telecommunication service providers to deploy their services in the infrastructure and publish the relevant set prices, requirements and policies. NetEx had the aim of motivating providers to expose necessary information for offering and, correspondingly, receiving accountable services. However, it was designed without the vision of integrating it in a production environment of the 5G infrastructure. The T-NOVA project [7] introduced the realization of an NFV marketplace, targeting to the user selection of the services and the virtual appliances already published. Additionally, to this point, the T-NOVA marketplace involved multiple metrics from trading and billing policies in order to optimize the VNF combinations and selections. The diverse stakeholders interact with the several instances of the marketplace in different ways depending on the role of each stakeholder in the system. Every relationship between stakeholders involved a commercial transaction with consequent billing information and agreements.

Although there is large research and development of centralized marketplaces for VNF packages, there is a lack in distributed ledger technologies adoption, in order to promote privacy and openness. Till now, the available solutions require that the users trust completely the database integrity of the provider [8]. An initial work that tries to solve this challenge is presented by Scheid in [9], where he proposes a blockchain-based, trusted VNF package repository for securing the underlying 5G environment. Blockchain design must provide high data integrity, protection, consistency and privacy to guarantee the confidentiality of a Blockchain system [10]. Usually, information is distributed and processed throughout the participants in a blockchain. Updating this information requires the approval of most participants who validate that requested update is legitimate and permissible in compliance with the blockchain's programmed rules. The participants serve as both users and data controllers within each blockchain implementation, which effectively eliminates the data [11].

Therefore, the combination of these properties contributes towards research on the use of Distributed Ledger Technologies (DLT) in the sense of NFV. A suggested solution is also discussed in [12] where authors presented a blockchain-based NFV Management and Orchestration (MANO), named SINFONIA. SINFONIA (Secure Virtual Network Function Orchestra for Non-Repudiation, Integrity, and Auditability) is intended for network infrastructure where multiple Network Services (i.e. chained VNFs) are deployed from different customers.

Although there is an escalating interest in the delivery of a decentralized repositories in 5G environments, a major lack exists in the consolidation of an open marketplace as a secure and trustful component, which return the VNFs, NSs and their metadata control, back to the users. Thus, a challenge exists in the orientation of this component beyond the plain storage functionalities. With the evolving plethora of 5G network requirements and the DLT, the verification of VNF package’s integrity without relying on a Trusted Third Party (TTP) is deemed of paramount importance.

3 Proposed Architecture

The proposed smart distributed NFV Marketplace constitutes a vital component in the 5G environment. This section provides the architectural description of the NFV Marketplace, in terms of interacting software components and entities. Taking into consideration the inter-connection between a distributed set of users, developers and service providers, the implementation of the Marketplace aims to take advantage of a blockchain-based approach to support VNFs, NSs, packages and license transactions integrity, accountability and provenance tracking, in order to ensure trust and transparency in the 5G ecosystem. The proposed architecture is consisted of three main blocks: a) the dPortal, b) the NFV Marketplace and c) the blockchain-enabled Validation System, as depicted in Figure 1. The description of the aforementioned components is discussed in the following sub-sections. It should be pointed out, that the NFV MANO and NFV Infrastructure are not discussed in the current study, as we assume that third-party solutions are included. Although, the proposed architecture can be integrated into existing NFV solutions, such as orchestration platforms that are able to manage deployed VNFs, such as SONATA (powered by 5GTANGO) platform [13].

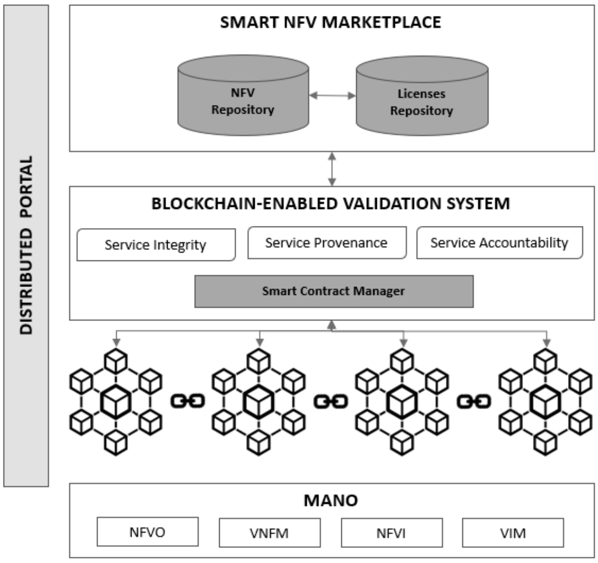

Fig. 1 Overview of the proposed smart NFV marketplace

3.2 dPortal

In this sub-section, the proposed distributed portal (aka “dPortal”) which is a dApp (i.e. decentralized application). It is worth mentioning that dApps are considered to be the fourth stage for the evolution of applications, as they are distributed, resilient and transparent [14]. The “dPortal” is a Graphical User Interface (GUI) in order to be accessible to the end-users. The “dPortal” is responsible for user interaction and presenting information, such as available and acquired VNFs and NSs, as well as licenses and prices. The proposed “dPortal” is divided into sections that include Packages, VNFs and NSs management, Licensing management, as well as an Operation section for NS instantiation management. The entities that are expected to take part in the distributed process and are identified by the “dPortal” are a) the service developers, b) the SP providers and c) the end-users. The main role of the “dPortal” is to help the developers to register their NS packages in a trustworthy NFV Marketplace, support the provider for the formulation of smart licenses for each package and finally benefit the end-users by providing an end-to-end verification system based on blockchain that verifies the integrity of the deployed NSs.

3.3 Smart NFV Marketplace

The below sub-section describes the key component of the proposed architecture, which is consisted by two components namely a) NFV Repository and b) Licenses Repository.

NFV Repository. The NFV Repository is considered to be a multi-sided catalogue, addressing different stakeholder needs in the entire lifecycle of the NSs. The inclusion of the correlated information refers to the NS enables the annotation of VNFs/NSs with metadata. The attached information contributes to the enhancement of the key functions and interfaces of the NFV Repository for storing, searching and retrieving VNFs/NS based on these metadata, as well as providing added value services.

Our approach incorporates the selection of one of the most famous databases from the family of the Documents Stores, MongoDB [15]. The aim of selecting MongoDB for our approach is the convenient management of complex data document and the developer-friendly environment for interpretable JSON/JSON–like data types.

Furthermore, MongoDB introduces considerably enhanced performance in the time complexity of the available CRUD operations, along with advanced query engine and index structures [16]. The deployment of a NoSQL MongoDB addresses the management and storage necessities of the template files of NSDs, VNFDs and packages. The stored descriptors are required for the selection, development and instantiation of the NS by the NFV Orchestrator (NFVO) as well as for data analysis in order for the added value functionalities of NFV Repository to operate properly. Thus, the following object categories are defined:

- Network Service Stored Objects: Feasibility of storage information about all the on boarded NSs, aiding the creation and management of the network service deployment templates.
- Virtual Network Function Stored Objects: Feasibility of storage information about VNFs, referring to the description template, reference to the software images (or even the software image itself) and manifest files.
- Package Stored Objects: Feasibility of storage information about packages, acting as an index to describe the files contained in the package.
- Acquired Licenses Objects: Feasibility of storage information about correlations between the end-user the corresponding licenses and the corresponding payments, resulting from the successful instantiations.
- Verification Information Objects: Feasibility of storage information about the integrity of the VNFs, NSs, packages that are stored into the repository. Additionally, this kind of objects are storing verification information regarding the anonymity of the user's wo sign smart contracts related to the licenses.

As depicted in Figure 2, prior to the attachment of the metadata to the stored objects, the inspection of the validity and integrity of the document structure is a critical step. Thus, a Validation System based on blockchain technology is introduced. Since the documents are specified in machine-readable formats, the review of the integrity contributes to data security into the NFV Repository.

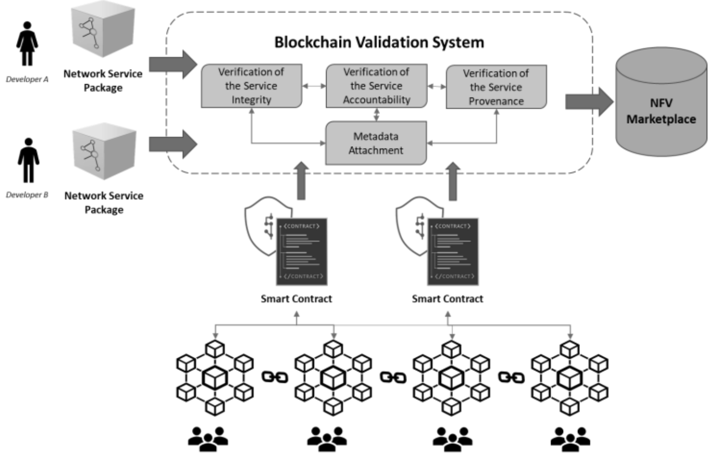

Fig. 2 Blockchain enabled validation

Licenses Repository. The Licensing Repository is responsible for handling customers requests to acquire VNFs and NSs. The License Management process that takes place in the presented work covers the license acquisition by the end-user, leaving the legal agreements to the "Smart Contract Manager" as we will describe in the sub-section III-C-2 below. Each license object stored into the Licenses Repository adopts a service-based licensing model, which links a license to a specific end-user and an instantiated NS, by specifying also the number of allowed NS instances. The licenses are being verified by creating smart contracts through the blockchain verification system of the proposed solution. The Licensing Repository stores the following licensing types:

- Public License: The Public License refers to an open source NS, which the descriptor (i.e. source code) is available to the end-users for instantiation free of charge. As previously mentioned, the Public License comes with no instantiation restrictions.

- Trial License: The Trial License refers to the NSs which end-users can try before they buy. Once the end-user in registered and selects to instantiate a NS with a Trial license he or she activates the license "silently", and can use it for the time period specified in the smart contract. Apart from the constrained period, the Trial License has a limited amount of free NS instances that the end-user can have it activated at the same time.
- Private License: In the proposed architecture, the Private License means that the customer needs to buy a license before instantiating a service. Additionally, this type of license specifies the number of allowed simultaneous instances per customer.

3.4 Blockchain Validation System

In this sub-section we are going to describe the proposed blockchain-enabled verification system which is the component that promotes trust and transparency among all the services and licenses transactions, toward the "Smart NFV Marketplace".

Blockchain Infrastructure. A blockchain involves many machines working together in a decentralized network, thus, it is a shared computer system infrastructure. This infrastructure is consisted of distributed computers which are documented in a manner that prevents their subsequent modification. Blockchain technology helps to increase security, accelerates information exchange in a manner that is more cost-effective and transparent, and also is a key technology for validation and verification of any kind of applications and services [17]. In this section we are going to describe our approach related on how we can ensure the security and provenance of the VNFs and NSs that are going to be stored into the NFV Marketplace. Additionally, the proposed approach promotes the trust and transparency of the licenses' payment transactions, between the service provider and the end-user (e.g. service customer). The verification process is based on the security policy language used by smart contracts, as introduced by the Model-based Security Toolkit (SecKit) [18].

Smart Contracts Manager. In this sub-section we are going to describe the proposed Smart Contract Manager which is responsible for handling end users' requests to store and/or retrieve VNF and NS packages, in a trustful way. The proposed Smart Contract Manger helps to extend the underlying Blockchain Infrastructure by including pieces of code that are the "smart contracts". These small programs are stored in the blockchain and programmed to autonomously behave in a given manner when some conditions are met [19]. We could define the smart contracts as digital contracts which "allow terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution" [20]. The aim of smart contracts is to evaluate the conformity that is defined as the fact that a service, method, license or even an individual (e.g. developer) meets stated requirements and can boost business interests, transparency and trust between all the stakeholders, with respect to the verification process.

The proposed Verification System is a framework for building privacy preserving smart contracts in order to a) verify the network services' integrity, b) verify the network services' accountability, c) verify the network services' origin and d) provide trust to licenses payment transactions between the service provider and the customer. The creation and execution of the smart contracts are facilitated by a specific entity, namely "Smart Contract Manager". The "Smart Contract Manager" can see the developer's inputs to the system (i.e. VNFs, NSs, packages) and is trusted not to disclose developer's private data. At this point we should mention that the manager needs also to be a trusted entity, and that's why it is distributed and at the same time verified among each blockchain user. For instance, if multiple contract instances are running concurrently, each smart contract may specify an individual manager, distributed among the infrastructure [21].

Moving forward, when a service developer enters the system and requests the storage or retrieval of a NS package, automatically subscribes to a specific Smart Contract Manager. The manager then is responsible to create a policy-based data usage contract specifying constraints on the usage and redistribution of any service obtained explicitly or implicitly by the system. The manager in this approach functions as a data provenance monitor, policy validation entity and event logger, allowing the system to easily verify all network service transfers and license transactions, ensuring that only transactions in compliance with the smart contract policy are allowed and recorded in the blockchain [22,23]. Once the Smart Contract Manager verify and validate the integrity, accountability and provenance of all the actions related to the services and licenses, the information is forwarded into the NFV Marketplace for further usage.

4 Summary and Future Work

Security and trust in the 5G environment are still a central concern for users and enterprises, which are increasingly relying on NFV infrastructures to support their business models and deliver their services. In this paper, we introduced a novel prototyping distributed NFV marketplace that goes beyond the plain NFV data repository. The proposed architecture is based in a blockchain infrastructure, taking advantage of the advantages of smart contracts in order to validate all the marketplace-oriented transactions of the VNFs, NSs, packages and license integrity, accountability and provenance tracking, towards trust and transparency in the 5G ecosystem.

It is doubtless that there is a lot of work ahead of us, till this work is ready to be adopted in a production environment. Therefore, we are planning to use business blockchain approaches, such as Hyperledger, as the implementation solution toward this direction. Moreover, we are planning to enhance the capabilities of the proposed smart contract manager, to automatically generate contracts from specified policies.

Acknowledgements. This work has been partially supported by the PARITY project, funded by the European Commission under Grant Agreement Number 864319 through the Horizon 2020. Moreover, this scientific work has been performed in the framework of the 5GTANGO project, funded by the European Commission under Grant number H2020ICT-2016-2761493 through the Horizon 2020 and 5G-PPP programs (http://5gtango.eu).

References

1. Karl, Holger, et al. "DevOps for network function virtualisation: an architectural approach." Transactions on Emerging Telecommunications Technologies 27.9 (2016): 1206-1215.
2. Kim, Jin Baek, and Arie Segev. "A web services-enabled marketplace architecture for negotiation process management." Decision Support Systems 40.1 (2005): 71-87.
3. Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG): ETSI GS NFV-MAN 001 - V1.1.1 - Network Functions Virtualisation (NFV); Management and Orchestration, 2014, http://tiny.cc/NFVMANO Last access April 1, 2019
4. “The Difference Between Blockchain & Distributed Ledger Technology”, Available at: https://tradeix.com/distributed-ledger-technology/, Accessed in 2019.
5. Wolf, Tilman, et al. "ChoiceNet: toward an economy plane for the Internet." ACM SIGCOMM Computer Communication Review 44.3 (2014): 58-65.
6. Yu, Da, et al. "Towards a network marketplace in a cloud." 8th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 16). 2016.
7. Xilouris, Georgios, et al. "T-NOVA: A marketplace for virtualized network functions." 2014 European Conference on Networks and Communications (EuCNC). IEEE, 2014.
8. Bozic, Nikola, Guy Pujolle, and Stefano Secci. "Securing virtual machine orchestration with blockchains." 2017 1st Cyber Security in Networking Conference (CSNet). IEEE,

2017.

9. Eder J. Scheid, Manuel Keller, Muriel F. Franco, and Burkhard Stiller, "BUNKER: a Blockchain-based trUsted VNF pacKagE Repository", in press
10. Porru, Simone, et al. "Blockchain-oriented software engineering: challenges and new directions." 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). IEEE, 2017.
11. “Blockchain Solves For Trust, Not Data Management”, Available at: https://www.forbes.com/sites/forbestechcouncil/2018/11/02/blockchain-solves-for-trust-not-data-management/#88c4e55132a1 , Accessed in 2019.
12. Rebello, Gabriel Antonio Fontes, Igor Drummond Alvarenga, and Grupo de Teleinformática. "SINFONIA: Gerenciamento Seguro de Funções Virtualizadas de Rede através de Corrente de Blocos." Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain-SBRC 2018). Vol. 1. No. 1/2018. SBC, 2018.
13. 5GTANGO Project Consortium, “5GTANGO: 5G Development and Validation Platform for global Industry-specific Network Services and Apps”, Online: https://5gtango.eu, Accesed in 2019.
14. “What Are Dapps? The New Decentralized Future”, Available at: https://blockgeeks.com/guides/dapps/, Accesed in 2019.
15. Zhang, Yin, et al. "Big Data Storage Technology suitable for the Operation and Maintenance of New Generation Power Grid Dispatching Control System Operation." IOP Conference Series: Earth and Environmental Science. Vol. 300. No. 4. IOP Publishing, 2019.
16. Ali, Wajid, et al. "Comparison between SQL and NoSQL Databases and Their Relationship with Big Data Analytics." Asian Journal of Research in Computer Science (2019): 1-10.
17. Themistocleous, Marinos, Vincenzo Morabito, and Paulo Rupino da Cunha. "Introduction to the Minitrack on Blockchain and Fintech." (2018).
18. R. Neisse, G. Steri, I. Nai Fovino, and G. Baldini. 2015. “SecKit: A Model-based Security Toolkit for the Internet of Things”, Computers & Security 54, (2015),60–76.
19. Gatteschi, Valentina, et al. "Blockchain and smart contracts for insurance: Is the technology mature enough?" Future Internet 10.2 (2018): 20.
20. Cong, Lin William, and Zhiguo He. "Blockchain disruption and smart contracts." The Review of Financial Studies 32.5 (2019): 1754-1797.
21. A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, (2016, pp. 839-858.
22. Ricardo Neisse, Gary Steri, and Igor Nai-Fovino, “A Blockchain-based Approach for Data Accountability and Provenance Tracking”, In Proceedings of the 12th International Conference on Availability, Reliability and Security, 1 (2017), 1-10.
23. Tosh, Deepak, et al. "Data Provenance in the Cloud: A Blockchain-Based Approach." IEEE Consumer Electronics Magazine 8.4 (2019): 38-44