Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6985492, 10 pages
https://doi.org/10.1155/2021/6985492

Research Article

Decentralized Certificate Management for Network Function Virtualisation (NFV) Implementation in Telecommunication Networks

Junzhi Yan, Na Li, Bo Yang, Min Li, Li Su, and Shen He

China Mobile Research Institute, Beijing 100053, China

Correspondence should be addressed to Junzhi Yan; j.z.yan@163.com

Received 11 August 2021; Accepted 23 September 2021; Published 18 October 2021

Academic Editor: Ximeng Liu

The certificate management complexity and cost increase when PKI technology is leveraged into Network Function Virtualisation (NFV), a significant enabling technology for 5G networks. The expected security of PKI cannot be met due to the unavailability of the certificate revocation inquiry in the telecommunication operator's core network. This paper analyses the issues and challenges during the NFV implementation and proposes a blockchain-based decentralized NFV certificate management mechanism. During instantiation, the Virtual Network Functions (VNF) instance generates certificates according to the certificate profile provided in the VNF package. The certificate management unit is responsible for the certificate enrolment, renewal, and revocation. The certificates submitted to the decentralized certificate management system by the instance will be recorded into the ledger after validation and consensus. The experiment and analysis show the transaction throughput, and the transaction delay is noncritical in practice, which could be fulfilled by the proposed mechanism. The certificate inquiry performance is critical, which can be facilitated by the decentralized deployment of inquiry nodes.

1. Introduction

Network Function Virtualisation (NFV), featured as decoupling software from hardware, flexible network function deployment, and dynamic operation, is a significant enabling technology for 5G networks. In NFV, network functions are implemented by vendors in software components known as Virtual Network Functions (VNFs), which are deployed on cloud infrastructure or massively distributed servers instead of dedicated hardware [1].

The architectural framework of NFV defined by the European Telecommunication Standardization Institute (ETSI) is depicted in Figure 1. It enabled the execution and deployment of VNF on NFV infrastructure comprising a pool of network, storage, and computing resources. The NFV infrastructure is usually a decentralized cloud infrastructure in which servers are distributed over various locations. The operation, deployment, and execution of network services and VNFs in NFV infrastructure are controlled by an orchestration and management system, whose performance is steered by NFV descriptors.

Typically, NFV is capable of overcoming certain 5G challenges, such as reducing the energy cost by maximizing the resource usage, scaling, and mobilizing VNFs from one resource to another, ensuring VNF performance operations [3]. A VNF is a virtualisation of a network function in a legacy nonvirtualised network. In 5G networks, Network Functions (NFs) defined in 3GPP TS 23.501 [4] are implemented on NFV infrastructure.

PKI public key certificates are widely used by the VNF, MANO (Management and Orchestration), and OSS/BSS/EM (Operation Support Systems, Business Support System, Element Management) in NFV. These certificates are used for authentication and secure communication. The NFs in 5G networks use TLS protocol to connect each other [5]. However, some issues and challenges arise during the NFV deployment. These issues and challenges are related with the certificate cost, across-domain trust, CRL/OCSP

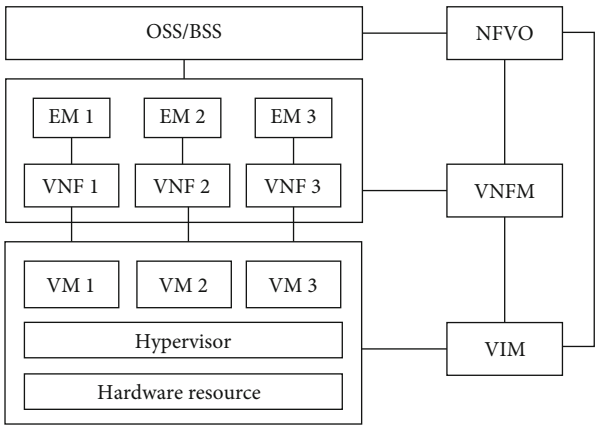

Figure 1: Architectural framework of NFV defined by ETSI [2].

(Certificate Revocation List/Online Certificate Status Protocol) services, certificate validation, and certificate maintenance. The essence of some issues is the lack of trust among the multiple participants in the NFV deployment, while others are related with the intranet structure of the operator's core network. Blockchain featured as decentralization and tamper resistance may benefit PKI technology [6]. The blockchain-based decentralized PKI is a significant trend for PKI technology, which could be used to facilitate the certificate management for NFV deployment.

The main contribution of this paper is the blockchain-based decentralized NFV certificate management mechanism, which is aimed at solving the issues during NFV implementation in telecommunication networks. Section 2 discusses the related researches. The issues and challenges aroused during the NFV implementation are presented in Section 3. Section 4 provides the framework of decentralized NFV certificate management mechanism and the certificate management method. The performance is evaluated and analyzed in Section 5. The conclusion is provided in Section 6.

2. Related Works

ETSI has published series of NFV standards, of which ETSI GS NFV 002 defines the architectural framework [2], ETSI GS NFV 001 provides a list of use cases and examples of target network functions for virtualisation [7], and ETSI GR NFV SEC 005 analyses the certificate management using traditional PKI technology [8].

The use of NFV technology in telecommunication networks, especially in 5G networks, has attracted much attention. An overview of enabling technologies like NFV and SDN (Software Defined Network) for 5G was provided in [9]. It highlighted challenges for ensuring an envisaged 5G networking system. The work highlighted that base station virtualisation and wireless resource sharing to formulate appropriate requirements. A flexible 5G architecture design for network slicing, built on SDN and NFV technologies, was presented in [10]. It emphasized schemes which provide effective substrate resource utilization for NS. In [11], the performance deterioration issue of virtualised access points occurring due to NFV implementation was addressed, and an overcoming approach was presented. Blockchain as an emerging technology has been leveraged to mobile networks in many researches. A blockchain-based secure key management scheme was proposed in [12] to improve the trustworthiness of the base station. The incentive mechanism combining edge computing was addressed in [13, 14]. The blockchain-based collaboration perception and privacy-preserving were studied in [15].

Some typical researches focusing on the decentralized PKI have appeared for years. A blockchain-based PKI framework in mobile networks was proposed in [16]. It focused on the problems when traditional PKI is leveraged into mobile networks. It provided some scenarios and application cases in mobile networks. The optimization for the certificate storage in blockchain-based PKI system was analyzed in [17]. The provided methods are aimed at improving the storage efficiency of specific nodes in blockchain-based PKI system. Research in [18] focused on the trust among multiple CAs (Certification Authority) using blockchain and provided some use cases in mobile networks. The implementation of blockchain-based PKI management framework in [19] used the standard X.509v3 certificate with an addition to the extension fields to indicate its location in the blockchain. The smart contract of each CA contained one list with all issued certificates and another list for revoked certificates. BlockPKI [20] required multiple CAs to perform a complete domain validation from different vantage points for an increased resilience to compromise and hijacking, scale to a high number of CAs by using an efficient multi-signature scheme, and provided a framework for paying multiple CAs automatically. SCPKI [21] worked on Ethereum blockchain and used an entity or authority in the system to verify another entity's identity. It could be used to detect rogue certificates when they are published.

Standard development organizations such as ISO/IEC and ITU-T have begun to study and standardize blockchain-based PKI and certificate management technology. These works are focusing on the profile and the mechanism of blockchain-recorded certificates. However, these normative works are still under development.

Considering that there will be lots of devices in the telecommunication networks which do not support decentralized solutions, the hybrid PKI certificate management supporting traditional and decentralized solutions will coexist in a long time. So, we will focus on the framework and methods proposed in [16, 19], which reuse the standard X.509 certificates [22] and be compatible to traditional solutions. Our innovation is to make the framework compatible to the NFV infrastructure and the certificate management in the operator's domain and make the NFV components support the decentralized PKI certificate management.

3. Issues and Challenges

There are mainly three kinds of certificates use cases in NFV, i.e., VNF certificate use case, MANO certificate use case, and OSS/BSS/EM certificate use case, which had been discussed in [8]. A VNF component instance (VNFCI) needs one or

more certificates provisioned to attest its identity to the VNFM or EM to establish a secure connection between them. During NFV implementation, the number of VNF certificates is far more than that in the other two use cases. The management of VNF certificates will be discussed in this paper. However, the certificates in the other two use cases could use the same method as VNF certificates.

By using traditional solutions, each instance of VNF could enroll certificates to CA/RA (Certification Authority/Registration Authority) directly or by a delegator such as VNFM [8]. However, the issues and challenges are as follows:

3.1. Cost of Certificates. VNFs are implemented with one or more VNF components. While a VNF component instance composed of various VNFCIs could have multiple logical identities, each of which is represented by a certificate, to communicate with different peers [8]. As a result, there will be a huge number of certificates required for the VNFs in 5G networks. It will be costly to use certificates issued by commercial CAs. The telecommunication operators prefer to use their own CA, vendor's CA or designated CAs to provide certificate service due to the cost. This may cause the problem of trust across CA domains.

3.2. Trust across CA Domains. A VNFCI may communicate with another VNFCI in another telecommunication operator's network. These two peers may be equipped with certificates issued by different CAs. The traditional methods to deal with multiple CAs include trusted root list, cross certification, and bridge CA. The trusted root list relies on the list maintained by the relying party. The list is usually preconfigured into the devices. It will be costly to update the list. Cross certification is suitable for a small amount of CAs. If there are a large amount of CAs, the cross relationship will make a complex structure. Besides, the usage of certificate policies will be limited after multiple mappings. The certificate chain of bridge CA will be much longer, and the validation will cost more computing resources.

3.3. CRL/OCSP Unavailable due to Intranet Implementation. The devices, including the network functions of 5G network, deployed in the telecommunication operator's core network cannot access the Internet. It makes CRL/OCSP unavailable for these devices and network functions. Moreover, the telecommunication operator's core network is usually divided into different security domains. These security domains are isolated physically or logically. The entity in one security domain cannot communicate with the entities in another security domain directly. In practice, the CA/RA service and CRL/OCSP services are usually deployed in a different security domain from the telecommunication operator's core network. It means the entities in the core network cannot access the CRL/OCSP services. Unless, the telecommunication operator deploys the CRL/OCSP services in each security domain, which is a complex and costly work.

3.4. Certificate Validation. When a VNFCI issues a certificate from the CA/RA, the identity of VNFCI will be validated by RA. The subject field in the certificate may be an IP address, FQDN, or other unique identifiers, which is related with the deployment. It is impossible for the RA to validate the subject field, unless an endorsement for the identity in the subject field is provided. The endorsement needs to be provided by some designated administrators. During implementation, there will be kinds of administrators responsible for corresponding identifiers. Thus, the deep cooperation between the RA and the administrators is significant and it makes the certificate validation complicated.

3.5. Certificate Maintenance. The certificate needs to be renewed when the validation period expires. Or else, it will not be trusted by the relying party. In 5G networks, there will be more than thousands of VNF certificates. It has to be ensured each certificate be renewed before it expires and be revoked once it is insecure or the VNFCI is terminated.

The essence of the above issues is the lack of trust among the multiple participants (such as vendors, telecommunication operator, and CA/RAs) during the NFV implementation. A trusted information sharing and endorsement method is necessary to solve the issues. The blockchain is featured as decentralization and tamper resistance. The endorsement and consensus mechanisms in blockchain help to make the information submitted to the participants in the blockchain system be trusted. It provides a decentralized way to solve the issues of the NFV certificate management.

4. Decentralized NFV Certificate Management

4.1. Framework. Figure 2 shows the participants included in the NFV certificate management scenario. The vendors and service providers develop the VNF packages. The packages contain the certificates issued by the vendor. During implementation, these VNFs will be instantiated with new certificates trusted by the operators. The operators are in different trusted domains. In our new framework, we aim to support both traditional PKI solution and decentralized solution. So, CAs will be included in the decentralized framework.

We make some improvements to the blockchain-based PKI framework proposed in [16] and make it more suitable to the NFV environment. The framework consists of submission nodes, validator nodes, and inquiry nodes. The VNF has kinds of identities. The validators usually are unable to validate the consistency of the VNF's identities and identities in the certificate, unless there is an endorsement. The endorsements can be made by the administrators, and then we add endorsers in the framework. A certificate management unit is also added which acts as the submission node. The framework for VNF certificate management is shown in Figure 3.

The VNFCI is the owner of the certificate. The Certificate Management Unit (CMU) works as a client to submit certificates and related information into the blockchain-based NFV certificate management system. The CMU could be a function in NFV architecture, e.g., located in VNFM, and it also could be independent to the NFV architecture.

The endorser is the node to endorse the identity in the submitted certificates. It could be the administrator of the network or the trusted third party (e.g., CA). Only the

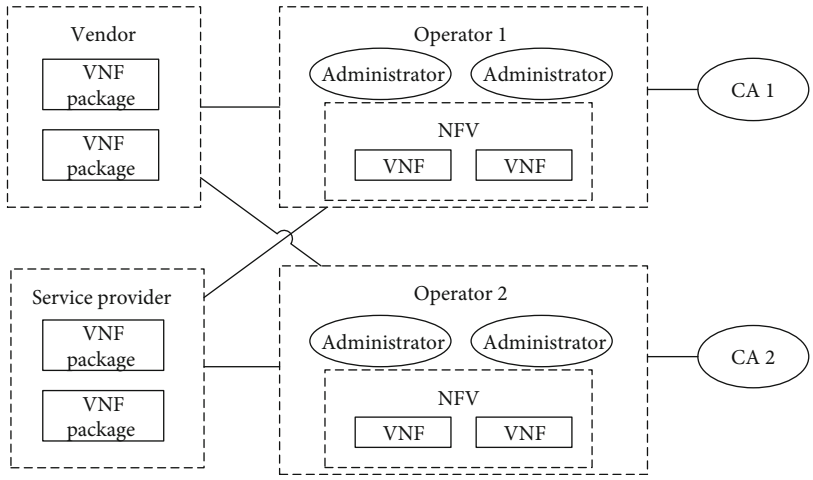

Figure 2: Participants included in the NFV certificate management scenario.

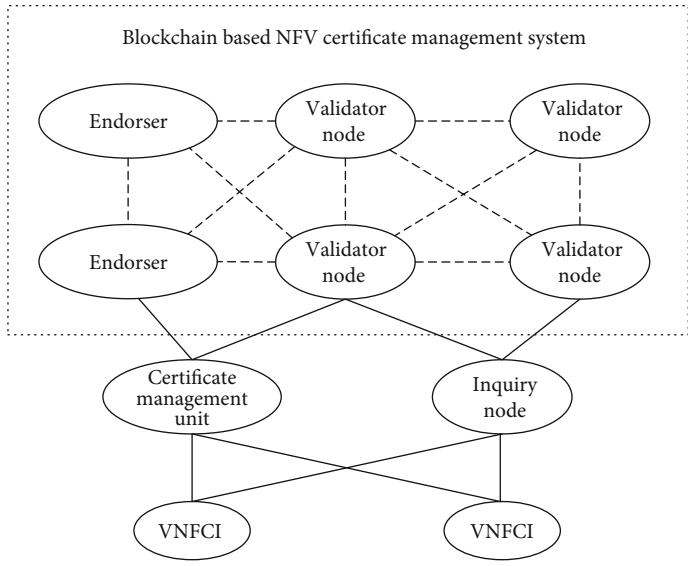

Figure 3: Framework for decentralized NFV certificate management system.

endorsed certificates and requests could be processed by the validator nodes.

The validator node is the node to verify the received requests and generate new blocks. It validates the certificates and request according to the policies. The validator nodes are held by vendors, service providers, operators, and CAs. One node could act as both an endorser and a validator.

The inquiry node provides certificate inquiry services. It needs to receive new blocks, but do not need to participate into the generation of new blocks. The inquiry nodes are held and deployed by any party which is capable to access the blockchain-based certificate management system. To support traditional solution, the inquiry node supports OCSP protocol and acts as a proxy. It transmits the OCSP request from the relying party to the corresponding destination and transmits the OCSP respond from the OCSP server to the relying party.

4.2. Certificate Enrolment. During instantiation, VNFCI needs to enroll certificates to communicate with other VNFCI or MANO/OSS/BSS/EM. The certificate could be a certificate issued by CA/RA as descripted in [8]. It could also be a self-signed certificate generated by the VNFCI. Both of these two kinds of certificates will be discussed in this paper.

The VNF configuration is based on parameterization captured at the design time, included in the VNF package, and complemented during the VNF instantiation. Before a VNF is installed, the VNF package will be on-boarded by NFVO. The VNF package includes a component of VNFD (Virtualised Network Function Descriptor), which is a deployment template describing a VNF in terms of deployment and operational behaviour requirements [23]. The VNFD is a static description file. The metadata in the VNFD is not changed during the whole VNF lifecycle. However, some parameters in the VNFD could be declared to be

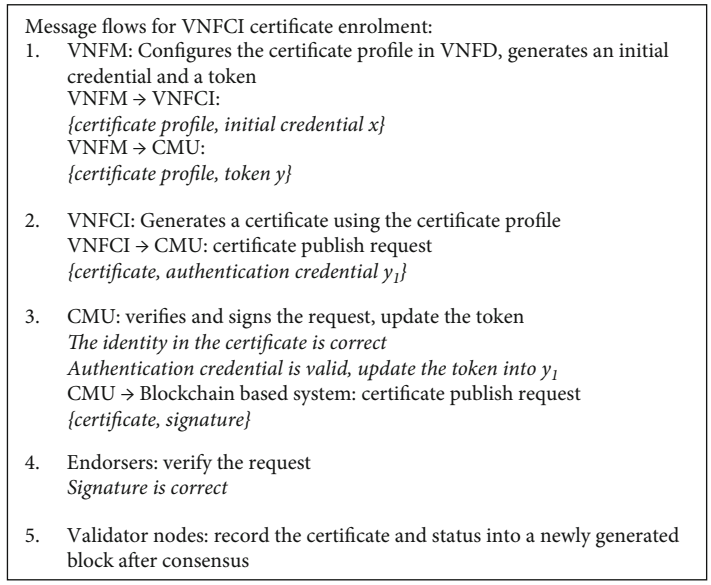

Figure 4: Message flows for VNFCI certificate enrolment

configurable during the VNF design phase [24]. We add the certificate profile into VNFD and make it be configurable. During the VNF instantiation, the VNFM accesses to the VNFD and configures the certificate profile. The parameters used to configure the certificate profile could be defined by the administrator. The VNFCI enrolls a certificate as follows, and the message flow is shown in Figure 4.

(1) The VNFM configures the certificate profile and initial credential for each VNFCI which are included in the VNFD and sends the certificate profile and token for each VNFCI to the CMU

The VNF parameters describing the certificate profile in the VNFD are declared to be configurable during the VNF design phase and be configured by the VNFM during or after the VNF instantiation [24]. The certificate profile declares the information used to generate the certificate, such as the subject, key usage, and basic constraint [25].

The subject field identifies the entity associated with the public key stored in the subject public key field and contains a distinguished name. The distinguished name may be an FQDN, a serial number, or other kinds of names, according to the operator's policy. It is suggested to include the operator's information in the distinguished name field, so as to identify the HPLMN (Home Public Land Mobile Network) in roaming scenarios. Multiple names could be addressed in the SAN (Subject Alternative Name) field [25]. The address of the inquiry node could be included in the extension field of the certificate.

The VNFM sends the certificate profile and a token to CMU. The token and information in the certificate profile will be used to validate the submitted VNFCI certificates. For the sake of simplicity, we use a token which is the value of multiple hash operations on the initial credential. The initial credential is kept as a secret by the VNFCI. Denote the initial credential by x, the token by y. Then, we have

$$H(H(\cdots H(x))) = y. \quad (1)$$

y is the value of multiple times (e.g., n times) hash operations of x.

(2) The VNFCI generates a self-signed certificate and submits the certificate publish request to the CMU

The public-private key pair used to generate a self-signed certificate is generated using the methods addressed in [8]. The VNFCI generates the certificate using the information and certificate profile provided in the VNFD and then generates the authentication credential based on the initial credential. The authentication credential is the value (denoted by y_1) of multiple hash operations (e.g., $n-1$ times) on the initial credential (x), of which the hash value equals the token (y). The VNFCI submits certificate publish request to the CMU, while the request consists of the certificate and the authentication credential.

To support the traditional solution, the VNFCI can enroll the certificate via CMU or from RA/CA directly by using protocols such as CMP (Certificate Management Protocol). Then, VNFCI submits the CA-issued certificate in the certificate publish request to the CMU.

(3) The CMU verifies the certificate publish request, signs the request, and transmits it to the blockchain-based certificate management system

The CMU verifies the certificate in the request to ensure it is consistent with the certificate profile, and the information contained in the certificate is correct (e.g., the information in the subject field is valid). The authentication

credential is verified to ensure it is consistent with the token. Then, the CMU signs the request and submits it to the blockchain-based certificate management system. The token could only be used once so as to protect against replay attacks. Thus, CMU updates the token from y into y_1. The one-time token makes it possible for the VNFCI to enroll multiple certificates.

If it is a CA issued certificate in the request, the CMU verifies and signs the request and transmits it to the blockchain-based system.

(4) The endorsers in the blockchain-based system verify the request and endorse the verified request

The endorsers verify the signature of the certificate publish request. After verification, the endorsers sign the request with their own private keys. The endorsement methods are the same to the self-signed certificates and CA-issued certificates. However, the endorsement policy is made and can be configured by the participants. The endorsers can even verify the identity of each VNFCI if necessary.

(5) The validator nodes record the certificates in the endorsed requests and their statuses into the ledger after consensus

The two kinds of certificates are recorded into the ledger. The inquiry node can inquiry these certificates and their statuses and provide inquiry service to the relying party.

During implementation, the certificates submitted to the blockchain system can be replaced by the certificate hashes. The CMU needs to use certificates hashes in the certificate publish request before it signs the request and submits the request to the blockchain-based system. Then, the size of the transactions will be smaller, and the storage resource requirement will be less, which was discussed in [16].

4.3. Certificate Revocation. A VNFCI certificate needs to be revoked, when it is insecure or the VNFCI is terminated. The VNFCI generates and submits a certificate revocation request to the CMU. The certificate revocation request can be generated by the CMU according to the policy. The certificate revocation request contains the certificate or its identifier, and then it is signed by the CMU.

The CMU submits the certificate revocation request to the blockchain-based certificate management system. The endorsers and validator nodes verify the request and then update the status of the certificate as "revoked" in the ledger. If it is a CA-issued certificate, the CMU will transmit the revocation request to the corresponding RA and forward the response to the VNFCI.

4.4. Certificate Renewal. The certificate to be expired needs to be renewed. The certificate renewal request is initiated by the VNFCI. The CMU could indicate the VNFCI to initiate a certificate renewal process.

The VNFCI generates the certificate renewal request and submits it to the CMU. The request contains the certificate to be renewed or its identifier, the new certificate, and the signature signed by the private key corresponding to the certificate to be renewed. The CMU submits the certificate renewal request to the blockchain-based certificate management system. The endorsers and validator nodes verify the request and then record the new certificate into the ledger and update the status of the former certificate as "revoked" in the ledger. If it is a CA-issued certificate, the CMU will transmit the certificate renewal request to the corresponding RA and forward the response to the VNFCI.

4.5. Certificate Inquiry. Ideally, the NFV infrastructure of all the telecommunication operators utilize the blockchain-based certificate management solution. However, in practice, some operators may use blockchain-based solution while others use traditional PKI solution. The certificate inquiry is discussed as follows in nonroaming scenario and roaming scenario, in which the VPLMN (Visited Public Land Mobile Network) uses the blockchain-based solution.

(1) Nonroaming scenario

When a VNFCI receives a certificate from another VNFCI, it inquires the certificate and its status from the inquiry node of the blockchain-based certificate management system. The inquiry node finds the inquired certificate and its status and feedbacks them to the relying party. The relying party verifies the certificate and its status to ensure the certificate is valid. Both the CA-issued certificates and the self-signed certificates can use the same inquiry method. If some VNFCI uses a CA-issued certificate, the OCSP service can be achieved by the inquiry node. The relying party needs to send the OCSP request and receive OCSP response via the inquiry node.

(2) Roaming scenario

Figure 5 depicts a simplified certificate inquiry architecture in the case of local break out scenario which was defined in [4]. It shows an example of local break out scenario. Usually, each operator only trusts its own system, including the NFV certificate management system. In this case, the VPLMN uses the blockchain-based solution, HPLMN 1 uses the traditional PKI solution, and HPLMN 2 uses the blockchain-based solution which is independent to the VPLMN.

The inquiry node of the VPLMN connects the CRL/OCSP servers used by HPLMN 1 and the inquiry node in NFV certificate management system of HPLMN 2. When a VNFCI in the VPLMN receives a certificate from the VNFCI of another PLMN, it connects the inquiry node in VPLMN for the certificate status. The certificate of this blockchain-based solution contains the operator's information in the distinguished name filed. The traditional CA-issued certificate contains the CRL/OCSP server's address. As a result, the inquiry node in the VPLMN connects the CRL/OCSP server of HPLMN 1 and the inquiry node of HPLMN 2, according to the information included in the certificate. The inquiry node of the VPLMN inquiries the certificate status and then feedbacks the status to the VNFCI in the VPLMN.

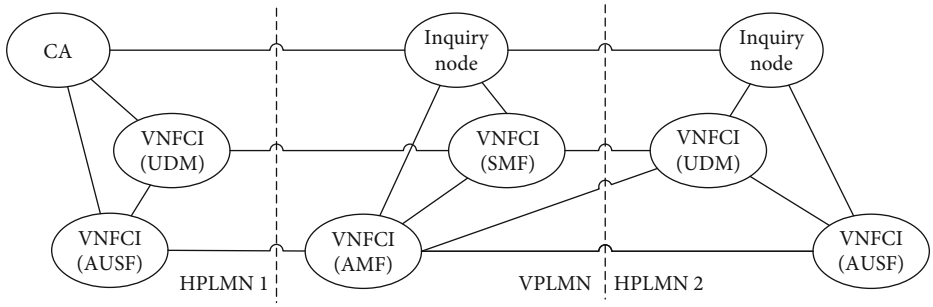

Figure 5: Certificate inquiry architecture for roaming 5G system.

5. Performance Evaluation

In this section, we perform experimental measurements to evaluate the performance of our decentralized certificate management framework. And then we make some analysis about the influence to the VNF performance.

5.1. Experimental Setup. We used Hyperledger Fabric to build a blockchain system including 2 organizations and 2 peers per organization. There is one orderer node to provide ordering service. We use the Solo consensus mechanism in these experiments. The peer nodes and orderer node run on dependent physical servers. The Apache JMeter is used to test the performance, which also runs on a physical server. Each physical server has 4 CPUs (Intel Xeon 2.3 GHz) with 16 GB RAM. All physical servers are connected with 1 Gbps network. We used the native Fabric V1.4.6 with no optimization to evaluate the performance. At least 50 times of experiments were made under each circumstance, and the average results were used in the evaluation.

5.2. Transaction Efficiency of Certificate Management. Transaction throughput, which is the number of transactions could be processed in a given time period, determines the efficiency of a blockchain-based system. Figure 6 shows the overall transaction throughput of the decentralized NFV certificate management framework. We set the block interval to 2 s and 0.25 s, respectively, and record the transaction throughput under different block sizes. We found the maximum transaction throughput is around 500 tps, and it changes little when the block size is more than 50. It performs better, however, not significantly, when the block interval is set to 0.25 s. When the block size is more than 1000, the transaction throughput reaches 550 tps.

The certificates can be replaced by their hashes when recorded into the ledger. Figure 7 shows the performance when the certificates hashes are used. In Figure 7(a), the block interval is set to 0.25 s, and we found the transaction throughput exceeds 600 tps when the block size is more than 1000. Then, we set the block size to 3000 and record the transaction throughput under different block intervals, as shown in Figure 7(b). We found it performs better when the block interval is 0.25 s. Generally, the transaction throughput achieves more than 600 tps when the certificates hashes are used.

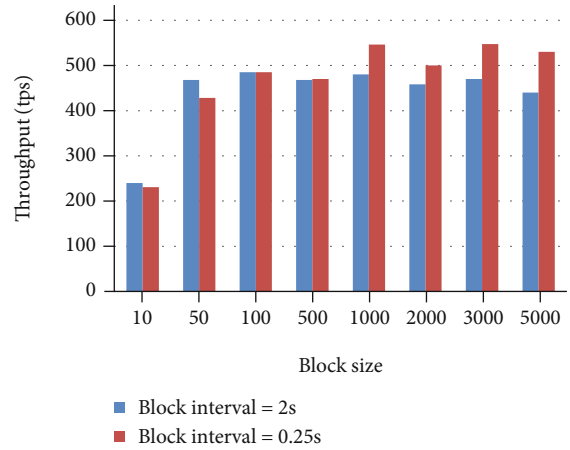

Figure 6: Transaction throughput of the decentralized certificate management framework.

5.3. Transaction Efficiency Evaluation. When we evaluate the transaction efficiency of certificate management in NFV environment, we first need to recall the performance benchmark about NFV. The certificate management such as enrolment happens during the initiation of a VNF, and we have to focus on the metrics related to the deployment of VNFs.

The ETSI GS NFV TST 009 [26] specifies vendor agnostic definitions of performance metrics and the associated methods of measurement for benchmarking networks supported in the NFVI. The key metrics are network related such as latency, throughput, delay variation, and loss. In IETF RFC 8172 [27], the metric of time to deploy VNFs is defined. It is the time taken to create 100 s of virtual machines and VNFs and make them work properly, in case the general purpose hardware is already deployed. In the work of [28], a similar KPI called deployment process delay is considered. In the process, a service instance is instantiated within the booted virtual machines and setup an operational network services.

In NFV scenario, the certificate enrolment happens during instantiation. It happens once or no more than several times for each VNFCI. Usually, the validity period of a certificate is 1-year long. However, it could be configured according to the operator's policy. The longer is the validity, and the less certificate renewal is needed. Each certificate can only be revoked once. As a result, the certificate for each VNFCI needs no more than two transactions (certificate enrolment/renewal

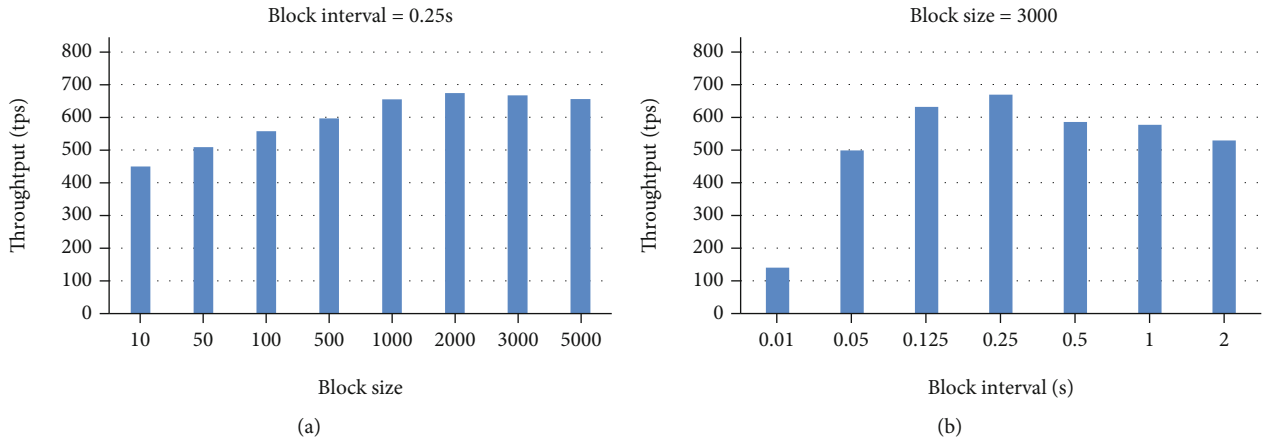

Figure 7: Transaction throughput when the certificate hashes are used.

and certificate revocation) per year on average. Even if there are millions of VNFCIs in the operator's network (more than 100 s of the VNFs defined in [27]), about 10 s of transactions happen per minute. Theoretically, the transaction efficiency is noncritical in this decentralized system. The result of the experiment shows the decentralized framework supports more than 500 transactions per second, which fulfils the requirement defined in [27].

5.4. Transaction Delay. Each certificate management request may result in a new record in the ledger. Transaction delay means the time from the certificate management request submitted to the blockchain-based system to the time that the request be processed and recorded into a new block or be rejected.

We focused on the deployment delay of VNFs defined in [27, 28]. The research in [28] compares the deployment process delay for the two platforms of OSM-4 and ONAP-B. The experiment contains an aggregate of 5 VNFCIs. The result shows the deployment process delay of aggregation level is 134 s. While the deployment process delay of each VNFCI varies from 20 s to 36 s. According to the result of our experiment in Figure 6, we observe the average delay of certificate management is less than 1 s (when the block interval is set to 2 s). It will increase 2%-5% of the deployment process delay of a VNFCI in [28]. And it will increase less than 1% of the aggregate deployment process delay of a VNF.

During the deployment of VNFs in the operator's network, each VNF may contain numeral VNFCIs. It usually takes minutes to instantiate a VNF. So, the delay of seconds is acceptable, even there are several VNFCIs which need to enroll certificates.

5.5. Performance of Certificate Inquiry. In the traditional PKI system, the certificate status is inquired by using CRL or OCSP service, which is a centralized service provided by the trusted third party. In the blockchain-based certificate management system, each node capable to access the ledger could provide certificate status inquiry service. This makes the inquiry service be decentralized. The inquiry performance of each inquiry node depends on the service and the hardware, which is not related to blockchain. More than one inquiry node can be deployed to enhance the inquiry performance, if necessary. When the inquiry node is deployed on the edge of the operator's core network and Internet, it could provide local certificate inquiry service for the entities in the core network. This may greatly enhance the availability and efficiency of certificate status inquiry service.

5.6. Other Considerations. There are some considerations to address the issues and challenges in clause 3.

(i) *Cost of Certificates*. There is no need for the operators and vendors to deploy and maintain the PKI infrastructure for the NFV implementation, so the cost is reduced

(ii) *Trust across CA Domains*. The nodes in the decentralized system consist of operators, vendors, service providers, and traditional CAs, which are in different trusted CA domains. The endorsement and consensus mechanisms make all the records in the ledger be trusted by the multiple participants from different CA domains according to the policy. It makes the trust between different trusted domains be available

(iii) *CRL/OCSP Service of Intranet Implementation*. The inquiry node can be deployed on the edge between the intranet and the Internet. It provides certificate inquiry service for the devices in the operator's core network

(iv) *Certificate Validation*. The CMU submits certificates and related information into the blockchain. The endorser, which could be the administrator of the network or the trusted third party, will endorse the identity in the submitted certificates. The CMU and the endorsers work together to endorse the identity and validate the certificate

(v) *Certificate Maintenance*. The CMU could be used to maintain the certificates. It can be used to indicate

the VNFCI to initiate a certificate renewal process and can be used to revoke certificates

6. Conclusion

Decentralized PKI is a significant direction for PKI technology. This paper analyses the issues and challenges related to the certificate management aroused during the NFV implementation in the telecommunication networks and proposes a blockchain-based decentralized NFV certificate management mechanism. The mechanism could establish the trust among the participants in the NFV implementation, such as vendors, service providers, operators, and even traditional CAs. It could ease the work load of the certificate management, reduce the cost to deploy and maintain the CA, and make certificate status inquiry available in the operator's core network. The experiment and analysis show the performance of transaction efficiency is noncritical and fulfils the requirement in practice. The high performance of the certificate inquiry could be facilitated by the decentralized deployment of inquiry nodes. This work could also facilitate the certificate usage in other scenarios in the telecommunication networks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

This research was performed as part of the employment of the authors in China Mobile Research Institute. Part of this work has been presented in EAI Mobimedia 2021.

Conflicts of Interest

The authors declare that there is no conflict of interest.

References

[1] S. Sridharan, "A literature review of network function virtualization (NFV) in 5G networks," *International Journal of Computer Trends and Technology*, vol. 68, no. 10, pp. 49–55, 2020.

[2] ETSI GS NFV 002, "Network functions virtualisation (NFV); architectural framework," 2014, https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

[3] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.

[4] 3GPP TS 23 501, "3rd generation partnership project; technical specification group services and system aspects; system architecture for the 5G system," 2020, https://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-g70.zip.

[5] 3GPP TS 33 501, "3rd generation partnership project; technical specification group services and system aspects; security architecture and procedures for 5G system," 2020, https://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-g50.zip.

[6] T. Hepp, F. Spaeh, A. Schoenhals, P. Ehret, and B. Gipp, "Exploring potentials and challenges of blockchain-based public key infrastructures," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 847–852, Paris, France, 2019.

[7] ETSI GS NFV 001, "Network functions virtualisation (NFV); use cases," 2013, https://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf.

[8] ETSI GR NFV-SEC 005, "Network functions virtualisation (NFV); trust; report on certificate management," 2019, https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/005/01.01.01_60/gr_NFV-SEC005v010101p.pdf.

[9] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN-key technology enablers for 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, 2017.

[10] F. Z. Yousaf, M. Gramaglia, V. Friderikos et al., "Network slicing with flexible mobility and QoS/QoE support for 5G networks," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1195–1201, Paris, France, 2017.

[11] X. Wang, C. Xu, G. Zhao, and S. Yu, "Tuna: an efficient and practical scheme for wireless access point in 5G networks virtualization," *IEEE Communications Letters*, vol. 22, no. 4, pp. 748–751, 2018.

[12] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.

[13] J. Xiong, X. Chen, Q. Yang, L. Chen, and Z. Yao, "A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2347–2360, 2020.

[14] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Transactions on Industrial Informatics.*, 2021.

[15] J. Xiong, R. Bi, Y. Tian, X. Liu, and D. Wu, "Towards lightweight, privacy-preserving cooperative object classification for connected autonomous vehicles," *IEEE Internet of Things Journal*, 2021.

[16] J. Yan, X. Hang, B. Yang, L. Su, and S. He, "Blockchain based PKI and certificates management in mobile networks," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1764–1770, Guangzhou, China, 2020.

[17] J. Yan, B. Yang, L. Su, and S. He, "Storage optimization for certificates in blockchain based PKI system," in *Blockchain Technology and Application (CBCC 2020)*, vol. 1305 of Communications in Computer and Information Science, , pp. 116–125, Springer, 2021.

[18] J. Yan, J. Peng, M. Zuo, and K. Wang, "Blockchain based PKI certificate system," *Telecom Engineering Technics and Standardization*, vol. 2017, no. 11, pp. 16–20, 2017.

[19] A. Yakubov, W. Shbair, A. Wallbom, and D. Sanda, "A blockchain-based PKI management framework," in *2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*, pp. 1–6, Taipei, Taiwan, 2018.

[20] L. Dykcik, L. Chuat, P. Szalachowski, and A. Perrig, "BlockPKI: an automated, resilient, and transparent public-key infrastructure," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 105–114, Singapore, 2018.

[21] M. Al-Bassam, "SCPKI: a smart contract based PKI and identity system," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 35–40, Abu Dhabi, United Arab Emirates, 2017.

[22] ITU-T X 509, "The directory: public-key and attribute certificate frameworks," 2019, https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14033.

[23] ETSI GS NFV-IFA 011, "Network functions virtualisation (NFV) release 4; management and orchestration; VNF descriptor and packaging specification," 2020, https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/011/04.01.01_60/gs_NFV-IFA011v040101p.pdf.

[24] ETSI GS NFV-IFA 008, "Network functions virtualisation (NFV); management and orchestration; Ve-Vnfm reference point - interface and information model specification," 2019, https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/008/02.07.01_60/gs_NFV-IFA008v020701p.pdf.

[25] IETF RFC 5280, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," 2008, https://datatracker.ietf.org/doc/rfc5280/.

[26] ETSI GS NFV-TST 009, "Network functions virtualisation (NFV) release 3; testing; specification of networkixng benchmarks and measurement methods for NFVI," 2020, 2020, https://www.etsi.org/deliver/etsi_gs/NFV-TST/001_099/009/03.04.01_60/gs_NFV-TST009v030401p.pdf.

[27] IETF RFC 8172, "Considerations for benchmarking virtual network functions and their infrastructure," 2017, https://datatracker.ietf.org/doc/rfc8172/.

[28] G. Yilma, Z. Yousaf, V. Sciancalepore, and X. Costa-Perez, "Benchmarking open source NFV MANO systems: OSM and ONAP," *Computer Communications*, vol. 161, pp. 86–98, 2020.