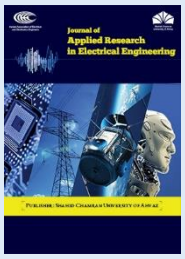
Shahid Chamran University of Ahvaz

Iranian Association of Electrical and Electronics Engineers

Journal of Applied Research in Electrical Engineering

E-ISSN: 2783-2864
P-ISSN: 2717-414X
Homepage: https://jaree.scu.ac.ir/



Review Article

Network Virtualization Utilizing Blockchain: A Review

Patikiri Arachchige Don Shehan Nilmantha Wijesekara*

Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka

** Corresponding Author: nilmantha@eie.ruh.ac.lk*

Abstract: Network Virtualization (NV) techniques enable high scalability and isolation by abstracting physical resources to provide a logical network representation that can coexist with a physical networking framework. Traditional NV is prone to security attacks and has lower privacy and trustfulness compared to blockchain-established NV. We diagnose the BC-established NV construct under 5 segments and closely appraise the literature in reference to NV technique, virtualization technology, BC-related properties, and network properties. We racked up a starting sample of 85 sources by filtering literary work for qualifying conditions searched from article retrieval platforms, engaging a rigorous and prolonged approach. Anchored from this research, in BC-established NV, we demonstrate that BC can act as a broker/manager for NV, act as a secure storage by preventing double-spending attacks, provide secure virtual network embedding with high fault tolerance, engage BC and smart contacts for resource trading in the process of NV, engage dedicated consensus approaches to reach agreement for NV among multiple parties for reducing security attacks, and establish BC-established access control for NV. Complete interpretation disseminates that from interpreted BC-established NV schemes, 45% engage BC and smart contracts for agreements and resource trading for NV, 95% engage regular BC architecture, Proof-of-Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) being the most frequently used consensus, 80% engage the overlay network concept, and it has been engaged abundantly (27.5%) in 5G networks. Finally, we deliberate the possibilities and obstacles of the framework of blockchain-established NV and then provide suggestions to suppress them.

Keywords: network virtualization; blockchain; slicing; entry coordination; cryptography; overlaying.

Article history
Received 14 February 2024; Revised 29 May 2024; Accepted 24 June 2024; Published online 30 October 2024.

How to cite this article
P. A. D. S. N. Wijesekara, "Network Virtualization Utilizing Blockchain: A Review," *J. Appl. Res. Electr. Eng.*, Vol. 3, No. 2, pp. 136-158, 2024. DOI: 10.22055/jaree.2024.46144.1110

Check for updates

1. INTRODUCTION

Network virtualization is a wide concept in networking that involves the abstraction of underlying physical resources to provide a logical network representation that can coexist with other virtual networks in the same physical network [1]. Due to network virtualization, many advantages can be realized, such as service provisioning flexibility, high manageability due to centralized management, high scalability, high isolation and fault tolerance, etc. [2]. These advantages in virtual network technologies such as virtual local area networks, virtual private networks, active and programmable networks, etc. can be evaluated by evaluating parameters, for instance, cost, revenue, throughput, bandwidth, spectrum efficiency, energy efficiency, signalling latency, and so on [3]. In network virtualization, infrastructure providers offer network resources to service providers through virtual network providers and operators, where service providers utilize them to cater services to end users [4].

In the resource sharing concept of network virtualization, resources such as spectrum, infrastructure, etc. are shared across multiple virtual networks with the aid of concepts such as dynamic spectrum sharing [5]. In comparison to resource sharing, slicing is a core function in network virtualization that slices a given spectrum, infrastructure, network, or flow into multiple sub-sets and allocates each slice to different

network service providers, which promotes independent control and isolation among virtual networks [6]. Network virtualization also involves network function virtualization, where software instances of different network functions such as routing, load balancing, and intrusion detection are typically implemented in software-defined networking, which can function in the manner of a service chain of virtualized network functions [7].

A blockchain vitally comprises a sequence of blocks intertwined in a regular or irregular sequence, conforming to the framework of distributed ledger technology [8]. Distinctly, transactions/blocks are connected to each other by means of a designated block/transaction that stores the hash digest of several antecedent transactions/blocks, making them immutable [9]. Further, they enact a universal assent methodology, such as proof-established universal assent or vote-established universal assent, for validating the blocks among the peers before combining a transaction/block on the distributed ledger technology [10]. Precisely, they apply hashing methods to secure the integrity and computer-generated signatures for securing transaction non-repudiation [11]. Similarly, they can incorporate secure cryptographic practices such as zero knowledge proofs and quantum-safe cryptography for resisting quantum attacks [12], intensifying the component of privacy safeguarding in blockchain. Nevertheless, the original blockchain itself, which dodges cryptographic practices such as key-pair cryptography for securing privacy safeguarding, is not 100% privacy safeguarding as blockchain recordings/transactions are pseudo-anonymous, expressing that recordings/transactions are identified by a confidential pseudo-identifier instead of bona fide addresses of nodes [13]. Similarly, the level of privacy protection may be tailored by following the distributed ledger category: private, consortium, or public. The public blockchain is the common permissionless blockchain, whereas private and consortium blockchains carry a designated level of centralized authority, contributing more privacy and data rights administration than the public blockchain [14].

In light of this examination, we find that blockchain-established network virtualization can be five-fold in terms of the duty of blockchain in the process of network virtualization. First, blockchain has been engaged as a broker/manager/auditor/orchestrator for different slicing in network virtualization, such as network slicing to coordinate slices and security level agreements, etc. [15], infrastructure slicing to audit and orchestrate slices [16], and spectrum slicing for spectrum management [17]. Secondly, blockchains facilitate secure storage of data, securing privacy with additional cryptographic techniques for obstructing double-spending attacks when allocating the same physical infrastructure to multiple virtual networks [18], and providing better virtual network embedding with high fault tolerance [19]. Thirdly, in spectrum slicing frameworks such as Bloc6Tel [20] and spectrum sharing frameworks such as MOSS [21], Smart Contracts (SCs) on blockchain have been engaged for providing service-level agreements and auction algorithms for resource trading. Fourthly, blockchain consensus has been specifically engaged in network virtualization processes, such as proof-of-strategy to reduce administrative expenses [22], consensus having a dynamic tip selection strategy to improve universal utility pertaining to the demand and supply of spectrum [23], Practical Byzantine Fault Tolerance (PBFT) to allocate more resources established on credibility values [24], etc. Finally, blockchain has been engaged to provide access control, making sure that only legitimate users are provided access to resources sliced or shared in network virtualization, such as devices belonging to different organizations that are provided access to a common VPN [25].

Currently, in this composition, to our present perception, no scholarly investigation has been conducted reviewing network virtualization in broad scope utilizing blockchain. Therefore, we are proud to be the primary appraisers to review in this field, which will provide a path for academicians to gain insight into current developments, discrepancies, obstacles, possibilities, and suggestions for network virtualization utilizing blockchain. However, there exist a survey that discusses the opportunities of network function virtualization in the blockchain domain [111]. In comparison to our work, the preceding work does not investigate blockchain applications in the broad scope of network virtualization.

Fig. 1 illustrates the subject catalogue of this interpretation of academic literature on network virtualization utilizing blockchain.

1.1. Contributions to Current Literature

- We classified and briefly presented a compendium of network virtualization (Section 3).
- The core concepts of network virtualization are briefly presented (Section 4).
- A compendium of blockchain technology is depicted (Section 5).
- Examine current blockchain-established network virtualization frameworks in telecommunication networks (Section 6).
- Interpret completely the examined blockchain-established network virtualization frameworks (Section 7).
- The possibilities and obstacles of blockchain-established network virtualization are deliberated (Section 8).
- Suggestions and prospective paths for engaging blockchain-established network virtualization are depicted (Section 9).

2. METHODOLOGY

This research examines the current original work on network virtualization utilizing blockchain available in print during the past years, engaging a rigorous and prolonged approach [26]. Further to that, it studies a wide spectrum of angles in network virtualization and blockchain systems. Henceforth, all unique scientific research reports and internet sites available in print on network virtualization, blockchain-established network virtualization, and blockchain inhabit the overall collection of data in this investigation. However, the whole data collection's references are impervious to inspection in the present investigation. Henceforth, engaging suitable search words and qualifying conditions, we gathered 88 references from unique scientific research reports and internet sites.

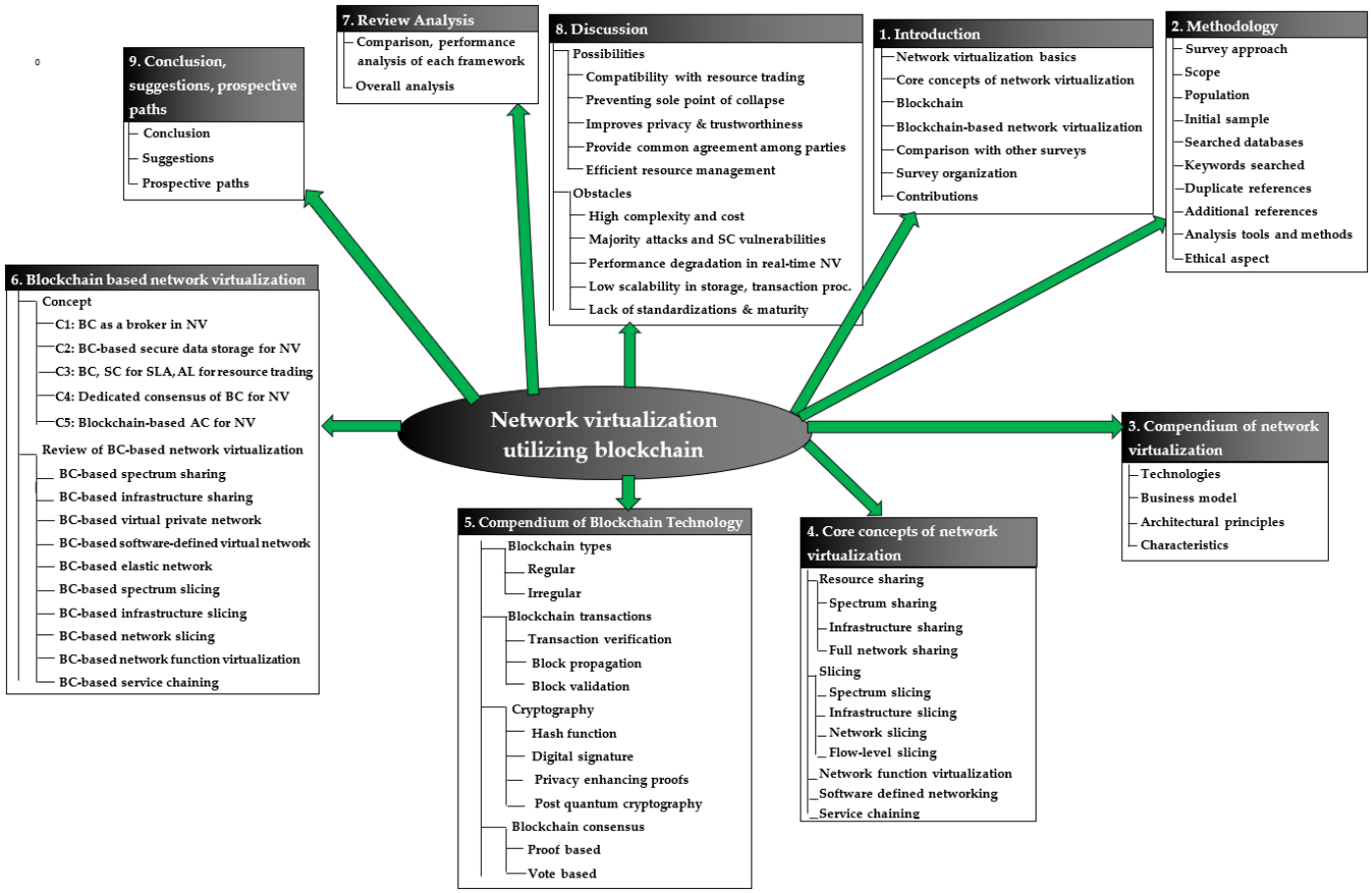


Fig. 1: Subject catalogue of this interpretation on network virtualization utilizing blockchain.

We searched IEEE Xplore technical database, Google Scholar educational content discovery platform, ACM electronic library, Wiley electronic library, ScienceDirect online scientific storage, and MDPI article retrieval platform. We commonly chose search words "Blockchain" OR "Network virtualization" OR "Blockchain-established network virtualization" OR "Blockchain-established spectrum sharing" OR "Blockchain-established infrastructure sharing" OR "Blockchain-established virtual private network" OR "Blockchain-established software-defined virtual networks" OR "blockchain-established elastic networks" OR "blockchain-established spectrum slicing" OR "Blockchain-established infrastructure slicing" OR "Blockchain-established network slicing" OR "Blockchain-established network function virtualization" OR "Blockchain-established service chaining".

A multitude of features for filtering the articles generated the qualifying conditions. The first qualifying condition dictates that the piece of writing imposes the use of English, and the second qualifying condition dictates a requirement of high pertinence to the search word. Thirdly, so as to augment the veracity of conducted research, journal articles were put in a position of prominence in contrast to meeting reports and preliminary publications. On the contrary, we didn't endorse research articles from a specific article producer in the qualifying conditions; in place of this, we treated all article producers equally. The last qualifying condition asserts that a specific piece of writing dictates public disclosure in the span of years since 1975.

The starting sample was minimized to 85 article sources; later, it was learned that 3 article sources were copies. Further to that, we adduced meanings and explanations pertaining to the heterogeneous topics presented in this research using 25 pieces of writing. To link this research with prior research, we reviewed multiple research articles; nevertheless, as only a single one examined related to blockchain-established network virtualization, we appended it to the assortment of electronic content, gaining the final summation of article sources to 111.

To evaluate the collected blockchain-established network virtualization by a multitude of features, such as blockchain characteristics, network virtualization characteristics, network factors, and effectiveness, we engaged the tabular dataset design for research qualitative assessment [27]. Further to that, we engineered visualizations engaging the Excel software to open-mindedly study research data linked with network virtualization-established and blockchain-established features.

Ethics do not apply, as this research pertains to telecommunication networks.

3. A Compendium of Network Virtualization

3.1. Technologies

3.1.1. Virtual Local Area Network (VLAN)

A VLAN brings together network hosts within a singular broadcast domain logically, irrespective of physical-

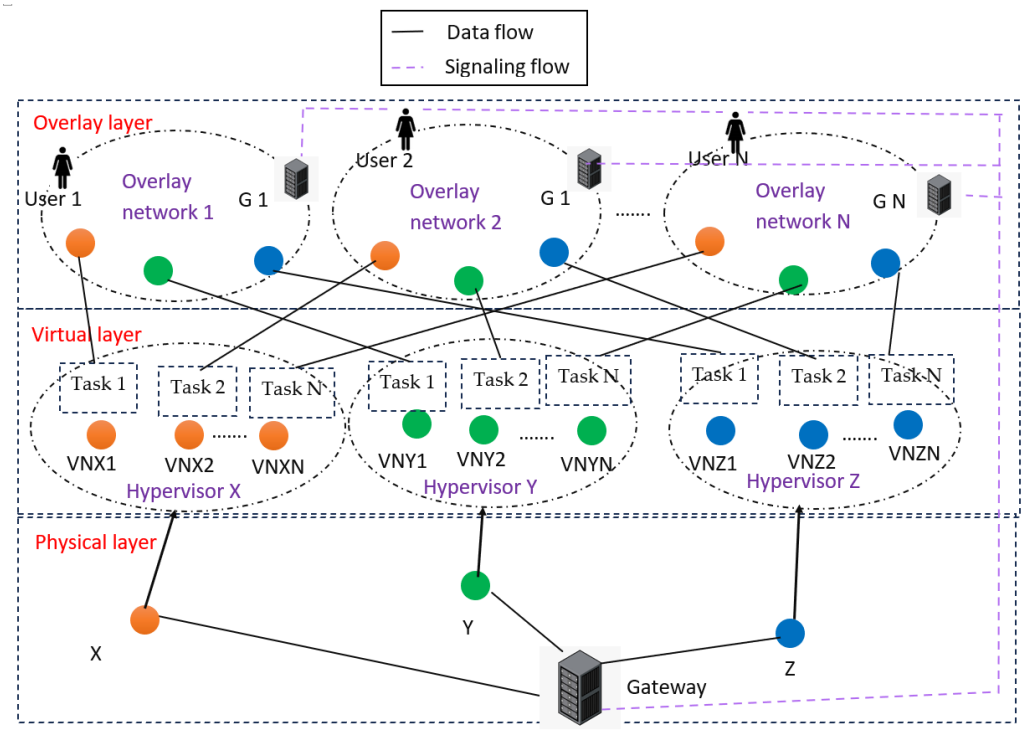


Fig. 2: Generic architecture of an Overlay network

-connectivity, where network administration and reconfiguration are simpler. These networks forward packets using the VLAN identifier and media access control address of the data link layer [28]. VLANs help in network segmentation, which allows network administrators to isolate devices in order to improve the security of the network by separating sensitive and critical resources from the rest of the network [29].

3.1.2. Virtual Private Network (VPN)

A VPN delivers secure and private encrypted tunnels for multiple sites over public communication networks that route users' traffic through a server belonging to the VPN provider, which is geographically distributed. In VPNs, customer-edge devices can be associated with provider-edge routers. They provide privacy and anonymity by hiding the real internet protocol address and are particularly useful when connecting public Wi-Fi networks to reduce potential hacking attacks [30].

VPNs can be categorized into tier 1, tier 2, and tier 3, established on the layer of the open-system interconnected model in which they operate. Tier 1 VPN is the physical layer VPN that is typically used in circuit switching networks and has the least level of application among VPN types. They use an asynchronous transfer mode for communication. Tier 2 VPN functions on the data link layer that extends the concept of VLAN over a large distance and uses multi-protocol label switching. On the other hand, tier 3 VPN operates in the network tier, which uses protocols such as internet protocol security, secure socket layer, etc. for establishing secure connections and is the most widely used VPN type [31].

3.1.3. Active and programmable Network (APN)

An APN promotes programmability, where network administrators can program high-level network policies to be engaged in the network, and network isolation, allowing multiple parties to implement conflicting codes on the same network equipment without any conflict. Network programmability promotes the logical separation of control functions from data-forwarding functions. There are two approaches for these networks: the active network approach and the open signalling approach. In the active networks approach, network services can be customized, involve implementing executable programmed code in network nodes, and are more flexible than the other approach [32]. In the open signalling approach, the exchange of control information among the network devices, known as signalling, is engaged to control the behavior of the network. NETKIT is a software-component established approach to structuring programmable networks that can accommodate multiple levels of networking systems in either of the approaches for active and programmable networks [33].

3.1.4. Overlay Network

An overlay network, typically implemented at the application layer, is a logical network implemented over a physical network in which virtual links exist among the nodes [34]. Overlay networks have been engaged to realize numerous goals, such as reducing security attacks, improving the quality of service, enabling multicasting, etc. The architecture of a generic overlay network is illustrated in Fig. 2.

For instance, SIPTVMON is a SIP protocol and cryptography-established secure multicast overlay network that is capable of optimizing network latency and bandwidth utilization through load balancing [1]. These networks promote network virtualization by abstracting the complexities of the physical network and using tunnelling techniques to transmit data among the nodes. For instance, NoEncap is a software-established optimization scheme to

reduce the overhead of packets in overlay-established virtual networks [35].

3.1.5. Elastic Network

An elastic network is a conceptual network where the infrastructure can dynamically adapt the allocation of network resources to changing demands of the network, such as traffic patterns, congestion, events, etc. [36]. In these networks, physical resources are virtualized, and they can be scaled up or down established on network demands and typically provide elastic services using optimization techniques. The virtual network embedding (mapping virtual network resources into physical network resources) in elastic networks is typically solved using optimization techniques. For instance, in [37], virtual network embedding for an elastic optical network is realized by optimizing to select light paths from a set of light paths having diverse modulation schemes, forward error correction rates, baud rates, etc.

3.2. Business model

Network virtualization involves multiple parties during its process, as in Infrastructure Providers (InPs), Service Providers (SPs), Mobile Virtual Network Providers (MVNPs), Mobile Virtual Network Operators (MVNOs), and end users.

3.2.1. Infrastructure provider

Infrastructure providers offer the network resources (such as servers, routers, and switches) owned by them to other parties using programmable interfaces. They are responsible for managing the underlying physical assets of the virtual network. Multiple infrastructure providers can allocate resources to single MVNP and also multiple MVNPs can lease resources from a single InP in network virtualization [4].

3.2.2. Mobile virtual network provider

MVNP is an organization that leases network infrastructure from InPs and creates virtual resources to be used by MVNO in the wireless mobile virtual network [38].

3.2.3. Mobile virtual network operator

The MVNO utilizes the virtual resources provided by the MVNPs and assigns them to service providers. MVNOs have more control than MVNPs over the services they provide. MVNOs can sometimes act as MVNPs and lease infrastructure from InPs as well. In such cases, matching theory and auction approaches have been utilized to allocate resources (slices) from multiple InPs to MVNOs to maximize their revenue [39].

3.2.4. Service provider

Service providers involve using virtual network resources provided by MVNOs and using them to provide services like data services, voice communication, etc. to end users in order to create virtual networks. SPs can program allocated virtual network resources to offer services. It can partition the virtual network services, creating multiple child virtual networks. Since there is competition among service providers, the expenditure of leased assets in SPs and client latency can be minimized while meeting client service level agreements under server bandwidth constraints [40].

3.2.5. End user

End users are the customers or subscribers that utilize the services bestowed by service providers. Note that in the network virtualization model, a given end user has the capability to connect to multiple virtual networks provided by multiple service providers. In network virtualization, multi-layer games have been suggested as an approach for allocating services and resources among multiple parties, such as InPs, MVNOs, end users, etc., where there exists a balancing act among the quality of service of EUs and the compensation of MVNOs and InPs, where end users attempt to find an optimal policy to obtain services from the service providers [41].

3.3. Architectural Principles

3.3.1. Abstraction

In network virtualization, underlying physical resources are abstracted and encapsulated to provide a more simplified logical network representation. This promotes simplified and easier network management, as it can be achieved without having to know about the details of complex network infrastructure. For instance, in [42], diverse types of information sources in vehicular networks are abstracted as broadcasting nodes and agents, and the controller is abstracted as a sink and a global solution optimizer for simplified data collection. Moreover, in [43], an enhanced logical view for network virtualization in distributed overlay virtual networks by achieving an advanced network abstraction in order to provide tenant contracts and provide application layer network services has been suggested.

3.3.2. Coexistence

Coexistence states the characteristic that multiple virtual networks provided by multiple service providers can exist together in the same physical network (partially or fully sharing the physical infrastructure) without having interference with each other. In the interest of achieving coexistence, there should be efficient isolation and resource allocation techniques such that one virtual network does not negatively contribute towards the performance of another virtual network. For instance, Ipv4-only networks can be virtualized over Ipv6 networks to facilitate communication among Ipv4 virtual network segments through an Ipv4-Ipv6 tunnel, allowing the coexistence of both types of networks [44].

3.3.3. Recursion/Nesting

Virtual networks can appear as a hierarchy of virtual networks where one virtual network is nested within another, in which multiple child virtual networks can be spawned from a parent virtual network. This hierarchical existence is known as recursion, and it allows scalability, as each virtual network in the hierarchy can have its own set of policies and configurations. BrFusion and Hostlo have been presented as frameworks to address the issues of network virtualization duplication and pod engagements bounded by virtual machines in nested network virtualization by shortening the packet lengths and reducing resource fragmentation [45].

3.3.4. Inheritance

In hierarchical virtual networks, inheritance refers to the property that a child virtual network automatically inherits

rules, configurations, policies, etc. from its parent virtual network. This simplifies the management of virtual networks, as network administrators need not be involved in redefining policies and configurations for virtual networks at the lower level of the hierarchy, as most of them are inherited from upper-layer virtual networks. In service-oriented hierarchical network virtualization, there exist different layers of services bestowed by different players that can be dynamically uncovered, where the lower layers inherit from the upper layers [46].

3.3.5. *Revisitation*

Revisitation refers to the ability of virtual networks to be revisited and to be dynamically reconfigured and modified during their lifecycle. They can be either automatically reconfigured, established on dynamic network conditions or manually reconfigured by network administrators with updated policies, rules, etc. Moreover, for one physical node, multiple virtual nodes of the matching virtual network can be configured and updated dynamically by revisiting to rearrange the virtual network structure. Thus, the virtual network embedding in virtual networks can be dynamically configured. In [47], virtual network embedding is dynamically configured by modelling as an integer linear programming problem considering resource fragmentation cost along with a virtual network embedding algorithm to consider resource fragmentation degree relying on the present network status and virtual network requests.

3.4. Characteristics

Virtual networks are characterized by several features that distinctly identify them, which are discussed in brief in the following subsections.

3.4.1. *Flexibility*

Flexibility refers to the freedom that exists within the service providers to adjust network topology, forwarding policies, security policies, etc. without being influenced by the underlying physical infrastructure or other virtual networks. For instance, sensors can be virtualized to provide data fusion tasks by selecting an appropriate technique to create flexible and virtual sensors in a sensor network without needing to know sensor-related details [48]. It allows customization of network environments to match applications. In [2], flexibility of a virtual network is defined as the ability to cater to new requests, such as requirement changes, and provide quantitative measures to measure the degree of flexibility in softwarized networks, such as virtual networks, while proving that these networks have a high degree of flexibility.

3.4.2. *Manageability*

Virtualized networks allow central management capabilities, allowing network administrators to manage the network centrally without having to configure hardware manually. Service providers are given full control permission for the virtual network. HYVI is a hybrid virtualization system that combines the benefits of software and hardware virtualization to seek a balance between the performance and manageability of virtualization [49]. Moreover, as InPs are separated from SPs, manageability is easier since SPs deal with virtual resources and not with physical infrastructure.

3.4.3. *Scalability*

Network virtualization allows the creation of new virtual networks or the expansion of existing ones when network demand increases without significant changes to the physical infrastructure. However, in cases where physical resources are inadequate to meet the increasing demand, InPs should provide more resources to be converted into virtual resources by MVNPs. For instance, SVLAN is a scalable VLAN that can scale to a high number of distributed systems and can provide network isolation at different granularities [50].

3.4.4. *Isolation*

When numerous virtual networks survive in a physical network, there should be isolation among them to improve fault tolerance and security in simultaneous operation. This isolation allows faults or security attacks in one virtual network to not affect other core virtual networks. For instance, FlowVisor provided network virtualization in the data plane, where the same hardware forwarding resources can be shared between numerous logical networks having distinct forwarding policies, providing isolation among the virtualized networks [51].

3.4.5. *Programmability*

Programmability refers to the ability of the virtual networks to be programmed such that service providers can engage customized protocols using application programming interfaces that allow a high degree of automation for network management. Programmability allows conveying application policies to the underlying network infrastructure. VNode has been suggested as a virtual infrastructure that can achieve high performance and programmability so that network developers can implement high level policies in network virtualization [52].

3.4.6. *Heterogeneity*

Virtual networks can be engaged on top of a combination of heterogeneous networks such as optical, cellular, vehicular, Wi-Fi, wired, etc., and each of the multiple virtual networks within the given physical infrastructures can also be heterogeneous with respect to each other. Specifically, virtualization can be realized in vehicular networks with the aid of network function virtualization, SDN, and network slicing to improve the functionality of traditional locally trained and machine learning-driven autonomous driving [53]. As network virtualization can abstract diverse network functions, virtual networks tend to have a high degree of heterogeneity. Network virtualization enables heterogeneous network platforms from different vendors having diverse programming environments, protocols, etc. to be interoperable [3].

3.4.7. *Multi-tenancy*

Virtual networks support multi-tenancy by allowing multiple users or groups to have their own secluded virtual networks; however, they share the corresponding (same) physical infrastructure. This allows logical separation of user functions, despite the fact that they use the same physical resources. Typically, software-defined networking and network function virtualization can be engaged to allow multi-tenancy by slicing the network [54].

Table 1: A compendium of current literature on diverse aspects of network virtualization.

Virtualization aspect	Sub-aspect	Stratagem	Performance
Technologies	Virtual local area network	Topology discovery using VLAN ID, MAC addresses [28]	Function in heterogeneous networks
		Network segmentation for sensitive and critical resources [29]	Simplify network management and provide improved security
	Virtual private network	Associating customer edge devices with provider routers [30]	Provide privacy and anonymity
		Layer 2 and Layer 3 VPN implementation [31]	No performance evaluation presented
	Active & program. network	Customized services, executable programmed code [32]	In capsule processing, Java network I/O is a bottleneck
		Accommodate multiple levels of networking system [33]	Able to incorporate all programmable networking levels
	Overlay network	SIP, cryptography established secure multicast overlaying [1]	Optimized network latency and bandwidth utilization
		Software-established optimization scheme [35]	Eliminate encapsulation overheads
	Elastic network	Optimization to select light paths for VNE [37]	Save 60% spectrum resources, faster solution
Business model	Infrastructure provider	Resource allocation with multiple InPs [4]	Low processing time, successful embedding, high acceptance
	MVNP	3-sided matching using size and cyclic preference [38]	Enhance user throughput, less running time
	MVNO	Allocate resources using matching theory, auctioning [39]	Maximize social welfare, stable matching
	Service provider	Leased resource cost minimization by server selection [40]	Low response time, link utilization, and jitter
	End user	Multi-layer game to allocate resources [41]	Maximize payoffs of InPs, MVNOs, offer spectrum to users
Architectural principles	Abstraction	Advanced network abstraction using overlay network [43]	Provide tenant contracts and network services
	Coexistence	Virtualizing IpV4 over Ipv6 networks using tunnelling [44]	No performance evaluation
	Recursion	Avoid NV duplication-short packets, resource fragmenting [45]	40% reduction in cloud utilization cost
	Inheritance	Layered services with inheritance [46]	Services can be dynamically discovered
	Revisitation	ILP to dynamically configure VNE [47]	Reduce fragmented resources
Characteristics	Flexibility	Quantitative measures flexibility in softwarized networks [2]	Provide a trade-off between cost and flexibility
	Manageability	Hybrid software and hardware virtualization [49]	Strike a balance in performance and manageability
	Scalability	A VLAN scaling to a high number of distributed systems [50]	Offer communication isolation with different granularities
	Isolation	FlowVisor to share hardware resources with isolation [51]	Does not require programmable hardware
	Programmability	VNode to implement high-level network policies [52]	Coexistence performance and programmability
	Heterogeneity	Heterogeneous network platforms using virtualization [3]	High interoperability and scalability
	Multi-tenancy	Using SDN and NFV [54]	Flexible and efficient resource allocation for multiple tenants

Table 1 illustrates a compendium of current literature on diverse aspects of network virtualization.

4. Core Concepts of Network Virtualization

4.1. Resource sharing

4.1.1. Spectrum sharing

Spectrum sharing essentially means that multiple MVNOs can share the same spectrum established by agreements among the operators. This considers the wireless spectrum resource as a whole and shares it among virtual networks [55]. Dynamic Spectrum Sharing (DSS) is the most widely used spectrum sharing technique that allocates spectrum dynamically, considering real-time demands, and is used in intelligent networks. In [56], a spectrum sharing framework supporting any number of radio networks engages machine learning for forecasting and clustering in order to allocate spectrum for 5G virtualized networks.

4.1.2. Infrastructure sharing

Infrastructure sharing refers to network operators sharing infrastructure resources such as passive buildings and sites, power and energy infrastructure, radio frequency antennas and eNodeBs, backhaul and backbone networks, routers, switches, etc., not being limited to network infrastructure. This reduces the cost per mobile network operator, and it can be achieved by varying technical and economic parameters, for instance, achievable throughput and pricing strategies in different infrastructure sharing strategies [5].

4.1.3. Full Network Sharing (FNS)

FNS is the combination of spectrum and infrastructure sharing, where both spectrum and infrastructure can be shared between numerous MVNOs using agreements. Full network sharing is supported in multi-operator core networks and gateway core network configurations. Virtualization is more efficient and flexible for full network sharing. In the 3GPP standard for full network sharing, multi-operator and gateway core networks coexist [57].

4.2. Slicing

4.2.1. Spectrum slicing

Spectrum slicing involves slicing (dividing) a given spectrum into multiple non-overlapping slices in a specific domain, such as time, frequency, or space, where multiple service providers can be allocated to different slices of the

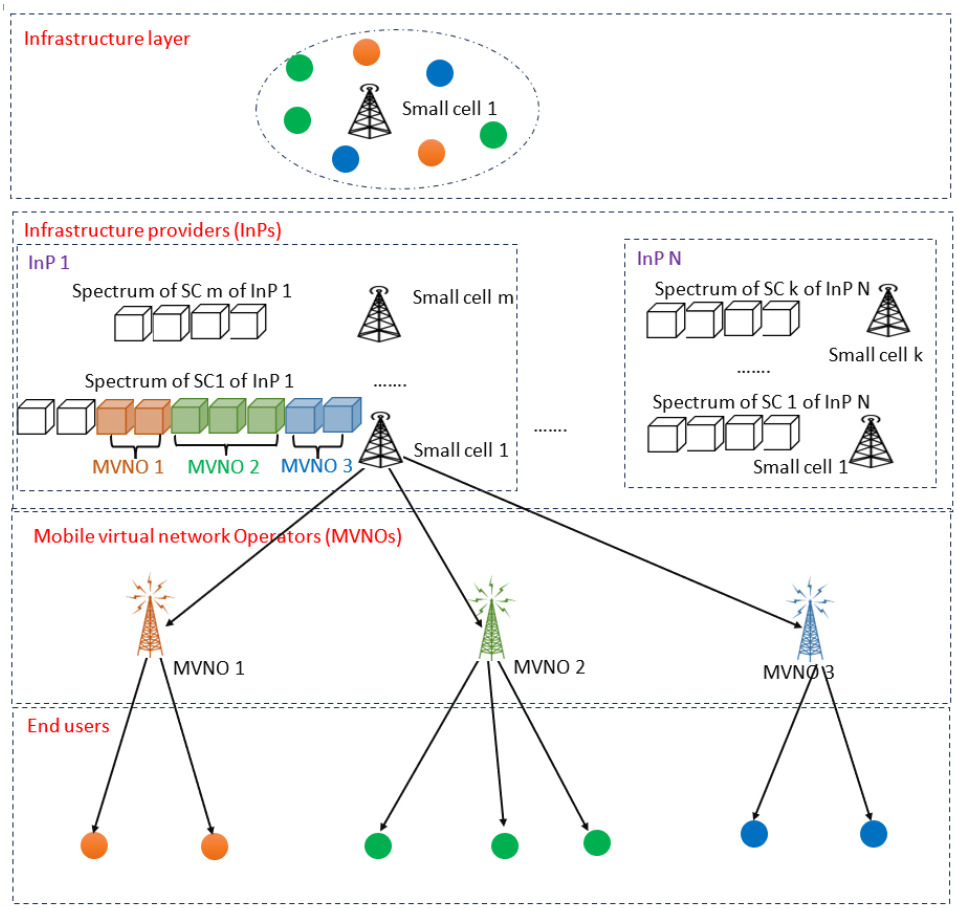


Fig. 3: Generic spectrum slicing concept within a small cell.

sliced spectrum. This allows multiple users/services to transmit simultaneously without causing interference to each other. In [6], the spectrum is sliced by minimizing the bandwidth blocking rate and the total number of slicers using mixed integer linear programming in an elastic optical network.

The generic spectrum slicing concept within a small cell in a mobile network is illustrated in Fig. 3.

4.2.2. Infrastructure slicing

Infrastructure slicing involves slicing the physical resources (creating multiple virtual instances of the same physical infrastructure) such as base stations, antennas, and other hardware resources such as computing, storage, etc. by MVNPs into virtual slices and allocating each infrastructure slice to different virtual networks (MVNOs) [58]. For instance, when a MVNO needs to lease spectrum from an InP, the MVNP has to slice and virtualize the infrastructure and allocate it to the corresponding MVNO. In [59], OpenFlow has been engaged to provide cross-layer infrastructure virtualization, allowing multiple virtual infrastructures to share a given physical infrastructure.

4.2.3. Network slicing

Network slicing involves creating logically isolated virtual networks that are implemented on a shared physical infrastructure. This can be achieved using infrastructure slicing and other concepts such as spectrum slicing and network sharing. Per each virtual network slice, different parameters, for instance, quality of service, bandwidth, latency, etc., can be defined as required, allowing the coexistence of multiple isolated virtual networks providing different services [60]. The generic network slicing concept in a mobile communication network is illustrated in Fig. 4.

For instance, a dynamic network slicing scheme for 5G networks implements a virtual network embedding task by using an algorithm to predict traffic demands and a tactic to uncover the number of virtual network functions and resources needed for each network slice [61].

4.2.4. Flow-level slicing

Flow-level slicing occurs within a network slice. For a given network slice (virtual network), slicing will occur established on the characteristics of different flows. It allows fine-grained control in a network slice. For instance, high-priority flows can allocate more resources even under high-resource usage instances, and vice versa. For instance, in a software-defined wireless virtual network, multi-flow transmissions are realized by virtual resource allocation considering quality of service requirements by modelling it as a social assistance maximization task having distance as the transaction expense along with a shadow pricing scheme [62].

4.3. Network Function Virtualization (NFV)

NFV is the process of creating virtual network functions just like routers, load balancers, intrusion detectors, etc. instead of dedicated hardware resources for achieving them. NFV uses virtual machines or containers to implement software instances of network functions, and it promotes resource sharing and efficiency as multiple network functions can be virtually implemented on the same physical device. In [63], for forward graph embedding of network function virtualization of an elastic optical network, computational

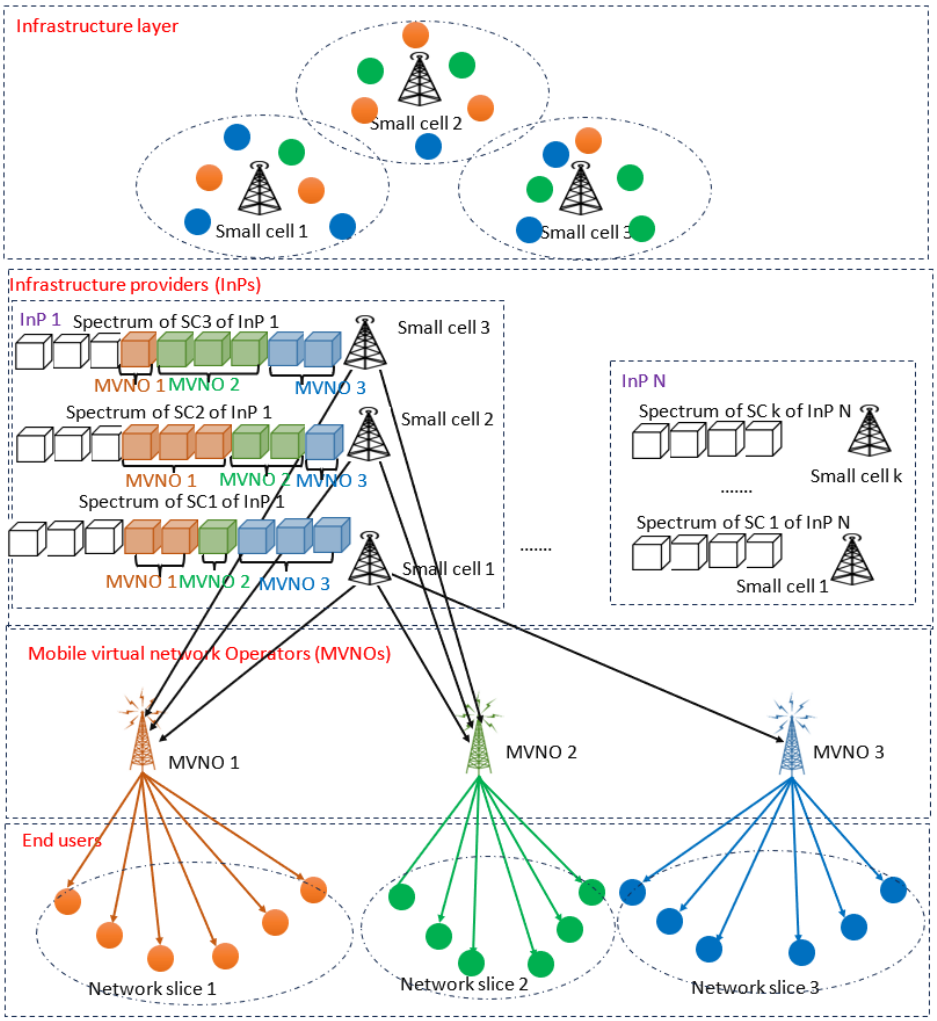


Fig. 4: Generic network slicing concept in a mobile network.

resources and optical bandwidth are allocated using an integer linear programming model for smooth operation of virtual network functions having interconnections among them.

4.4. Software-Defined Networking (SDN)

SDN embarks on logical decoupling of the control layer from the data layer, allowing centralized network control and management using a software-established controller [64]. SDN and NFV are often engaged in combination, where the SDN engages multiple instances of NFV in its network. Deep Reinforcement Learning (DRL) has been engaged to manage virtual network data flows in a programmable software-defined IoT edge network implementing NFV [65].

4.5. Service chaining

Service chaining involves creating a chain of virtualized network services through which network traffic should pass in sequence. It is a customizable service path that can be dynamically updated if required without requiring dedicated hardware. Service chaining is often engaged in combination with NFV and SDN. For instance, LASH-5G implements virtualized functions in edge clouds to provide adaptive and latency-aware service chaining of network function virtualization-established virtual functions across network domains interconnected using software-defined networking [66].

Table 2 illustrates a compendium of current literature on network virtualization concepts.

5. A Compendium of Blockchain Technology

A sequence of intertwined blocks or recordings/transactions comprises the distributed ledger called the blockchain.

5.1. Arrangements

Every block within the regular blockchain, which comprises a header section and record section, is related to its precursive block (excluding the origin block), putting to use the precursive block's hash digest, and the recordings/transactions within the record section are structured as a Merkle tree structure [9].

Irregular blockchain comprises an assortment of intertwined recordings/transactions where one recording/transaction might validate various other recordings/transactions that originated prior to it. These recordings/transactions are deficient in header sections and record sections; due to this, Merkle trees are absent [8].

Fig. 5 illustrates the architecture of regular and irregular blockchains.

Table 2: A compendium of current literature on network virtualization concepts.

Virtualization concept	Specific concept	Stratagem	Performance
Resource sharing	Spectrum sharing	Machine learning for forecasting and clustering [56]	Allow arbitrary network slices to share resources
	Infrastructure sharing	IS by varying technical and economic parameters [5]	Sharing configurations affected by number of paying users
	Spectrum sharing	Coexistence of multi-operator and gateway core networks [57]	No performance evaluation
Slicing	Spectrum slicing	Integer linear programming-Min. BW blocking rate [6]	68% increment in bandwidth blocking rate
	Infrastructure slicing	OpenFlow for cross-layer infrastructure virtualization [59]	Capability of manipulating virtualization behavior independently
	Network slicing	Strategy to find VNF, resources for slicing [61]	No performance evaluation
	Flow-level slicing	Social welfare maximization problem [62]	Energy efficient slicing
Network function virtualization	Forward graph embedding	Allocate resources using integer linear programming [63]	Feasible VNF despite its complexity
Software defined networking	Network function virtual.	Deep RL to manage virtual network data flows [65]	Goal is met on average in 183 episodes
Service chaining	Network function virtual.	Virtual functions across network domains using SDN [66]	Low latency and self-adaptive

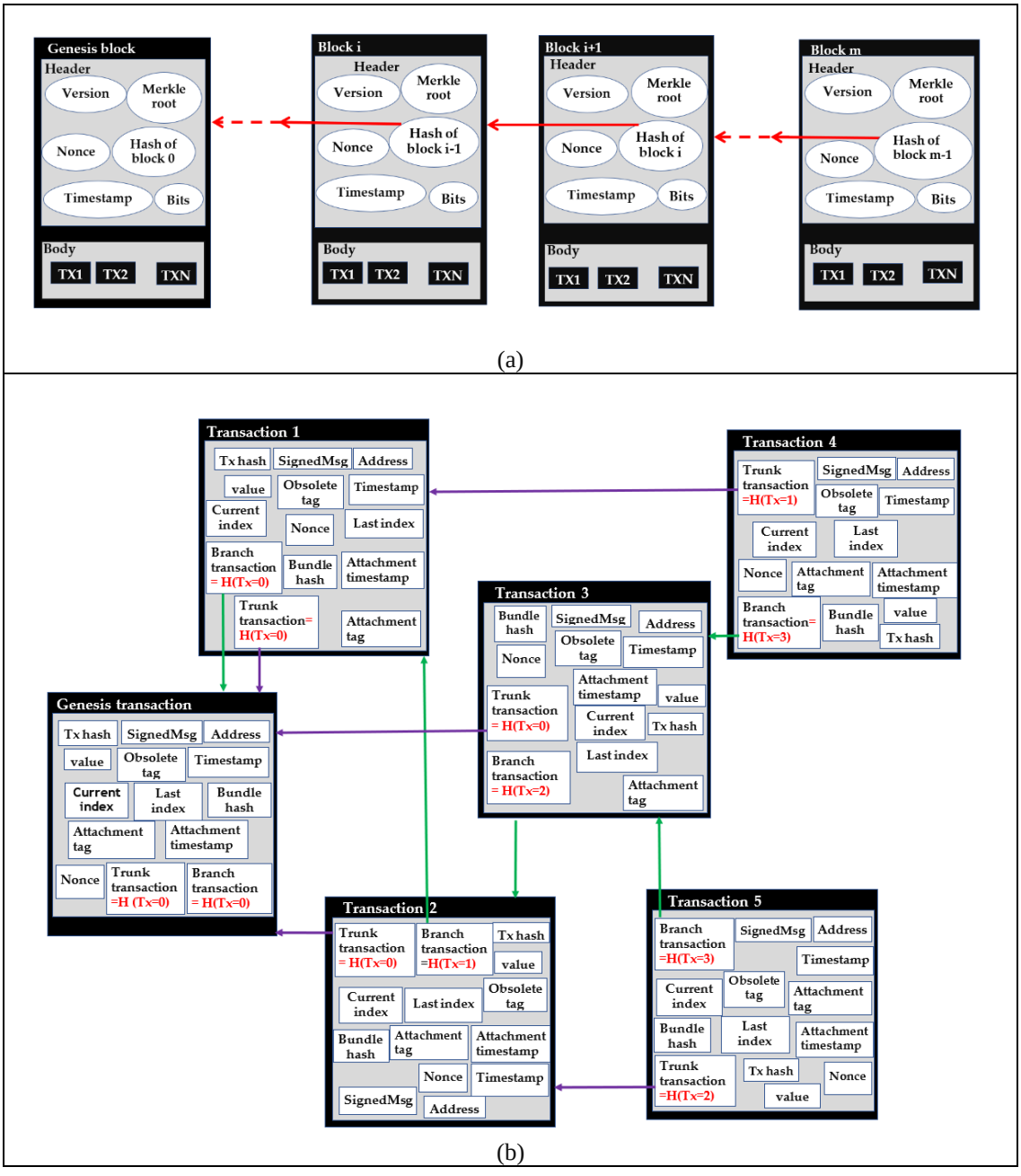


Fig. 5: Blockchain architectures. (a) Regular. (b) Irregular (IOTA).

5.2. Transactions

A given peer node can commence a blockchain transaction/recording, which is subsequently sent to all network peers and secured by putting to use the sender's secret key. A consensus strategy will commence once each peer puts to use the non-secret key to validate the transaction/recording. Block generators should embroil in consensus/assent by combining the transaction/recording within a block, which is subsequently sent to the distributed ledger network and pitched in by each peer node in the distributed ledger network posterior to block validation [67].

5.3. Blockchain cryptography

To secure the integrity of recordings/transactions in the blockchain, a hashing method is put into use to dispense constant-size hash digests with lesser collisions [11].

Putting into use a computer-generated signature, key pair cryptography incorporating an asymmetric cryptographic key duet is put into use to validate recordings/transactions. For the purpose of intensifying the isolation of data, it's equally feasible to put it into use to encode blockchain recordings/transactions [10].

In the interest of validating recordings'/transactions' accuracy, zero-knowledge proofs are put into use, concealing the identity-related data of recordings/transactions, intensifying isolation, and hindering the sending of confidential data [68].

Quantum-safe cryptography puts into use competent cryptographic techniques that are buffered from attacks from quantum machines, such as SIKE, Kyber, and so on [12].

5.4. Consensus/Universal assent

Blockchain consensus puts widespread universal assent into use to generate and validate fresh blocks, securing the integrity of the distributed ledger.

In vote-established universal assent, data is sent out and brought in within the network peers as they collaborate closely to validate blocks. The beloved choice vote-established universal assent technique put into use, PBFT, in the course of which a chief combines recordings/transactions within a block, sends it, and peer nodes resend it to validate the block brought in through the agency of the parent, is the same [13]. If every given peer got the same reproduction of a fresh block through the agency of going past the two-thirds majority of the network's peers, the block would become combined with the distributed ledger.

Proof-established universal assent requires peers to dispense compelling support because they are vitally compensated for combining a fresh block into the distributed ledger. The most widespread proof-established universal assent technique is named proof-of-work, which demands a peer execute tasks by tackling a complex problem for the purpose of securing its faithfulness [69]. However, this approach is more energy-consuming.

6. BLOCKCHAIN-ESTABLISHED NETWORK VIRTUALIZATION

6.1. Construct

Grounded in this documentary analysis, the blockchain-established network virtualization construct can be segmented into the succeeding 5 segments.

- C1 --Act as a broker/manager for slicing, NFV, etc. Ex: Blockchain and SCs can act as auditors or orchestrators in network/infrastructure/spectrum slicing, NFV, etc.
- C2 -- Secure storage of data, preserving privacy by engaging cryptographic techniques, and improving loyalty by preventing security attacks such as double spending attacks, etc. Ex: Virtual network embedding, allocating resources established on high credibility, etc.
- C3 -- Providing service level agreements, auction algorithms for resource trading, mechanisms to deal with own transactions, etc., engaging blockchain and SCs.
- C4 -- Dedicated distributed consensus to reach agreement for network virtualization among multiple parties, reducing security attacks. Ex: proof-of-strategy reducing administrative expenses, consensus with dynamic tip selection, learning algorithms for resource sharing, etc.
- C5 -- Blockchain-established access control for network virtualization.

Fig. 6 illustrates the construct of network virtualization utilizing blockchain.

6.2. Review on Existing Frameworks for network virtualization utilizing blockchain

6.2.1. Blockchain established Spectrum sharing

An incentive-provider, privacy-preserving blockchain has been engaged for efficient spectrum sharing in 5G mobile networks, which has two stages: in the first stage, human-to-human users enter into a contract in conjunction with the base station to receive payments considering the contribution, and in the second stage, spectrum is allocated to machine-to-machine users [70]. Preventing the spectrum allocation process from singular vulnerability, work in [22] proposes a distributed citizens broadband radio service for 6G mobile networks established on blockchain, engaging a ring signature technique for privacy protection and a new proof-of-strategy consensus that is able to allocate spectrum, reducing administrative expenses. In cognitive radio-established internet of battlefield things networks, ProBLeSS is a blockchain-established framework for secure sharing of spectrum sensing information amidst secondary user equipment in order to make collaborative spectrum sharing judgments. It engages a protocol known as proactive blockchain-established spectrum sharing (ProBLeSS) in order to engage blockchain to counter-attack SSDF attacks using a novel consensus algorithm and SCs to validate

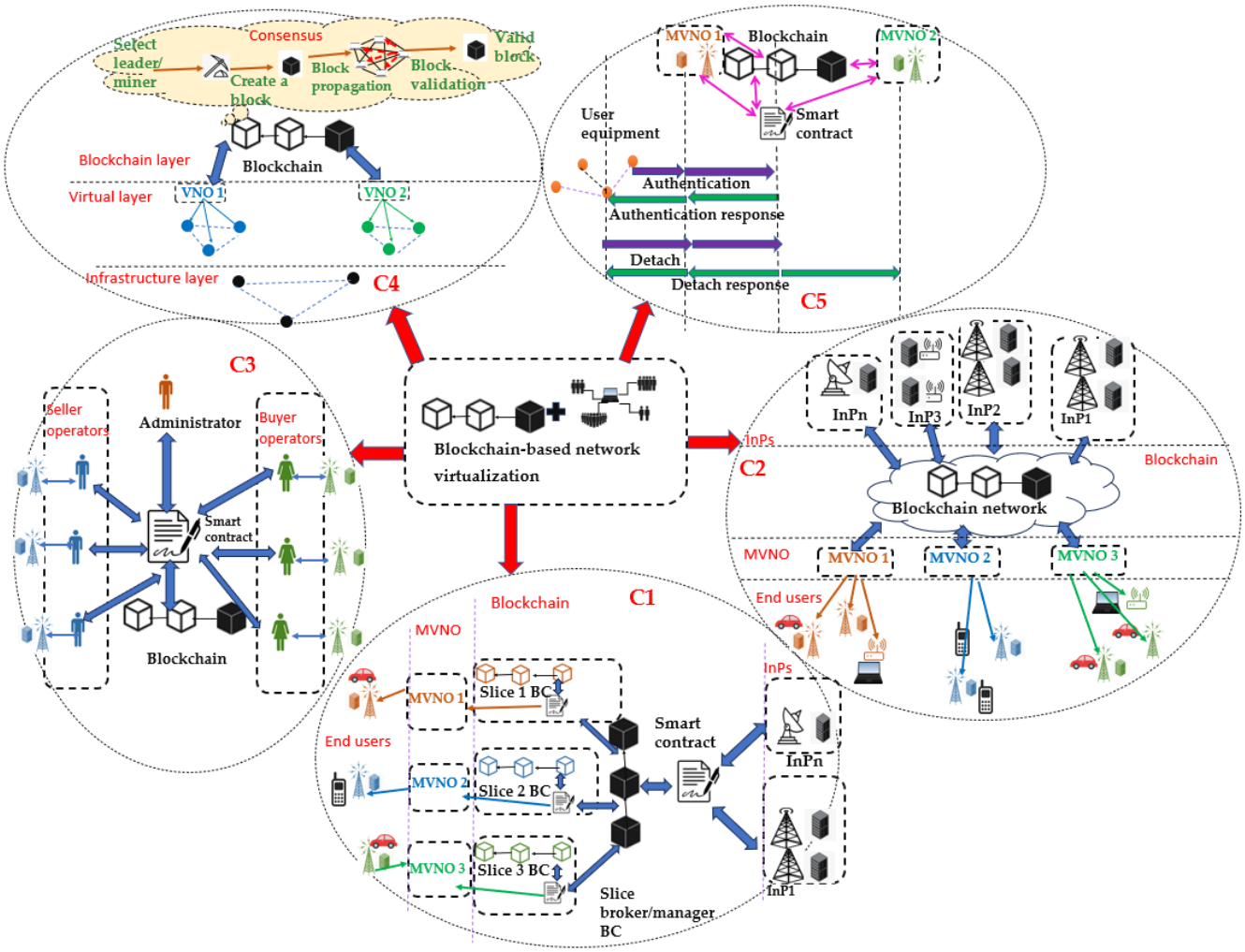


Fig. 6: Construct of network virtualization utilizing blockchain.

spectrum data [71]. In large-scale 6G-enabled IoT networks, a directed acyclic graph blockchain has been engaged for user autonomy spectrum sharing, providing a scalable solution where the swarm intelligence of users achieves convergence in blockchain consensus and a dynamic tip selection strategy to improve universal utility pertaining to the demand and supply of spectrum where the ring signature is integrated to improve the privacy of the spectrum sharing process [23]. In a blockchain-established spectrum sharing system engaged in a 5G-enabled IoT dense network where users can efficiently share spectrum using SCs, a game theoretic approach along with a tit-for-tat technique has been engaged to obtain corporation from non-cooperating users [72]. Alternatively, a blockchain-established dynamic spectrum sharing scheme for IoT considers privacy and transaction dynamical behavior by using a SC-implemented double auction technique considering differential privacy to remunerate spectrum sharing and considering time-varying valuations where a DRL technique is engaged to determine the winner of the auction game [73]. In a multiple mobile network operator wireless communication environment, Hyperledger fabric blockchain is utilized for recording spectrum allocation using SCs, where a multi-chief multi-disciple Stackelberg game is engaged to solve optimal spectrum pricing and buying strategies for spectrum sharing [74]. Similarly, MOSS is another multi-operator spectrum sharing platform that uses SCs engaged on permissioned blockchain to implement spectrum trading among multiple operators, enabling trustful spectrum sharing with a punishment technique for malicious operators [21].

6.2.2. *Blockchain established Infrastructure sharing*

A blockchain network is engaged in 5G small cell networks where blockchain provides a distributed home subscriber server in which core networks of different operators can utilize HSS in a secure approach and SCs are engaged to provide self-organizing network features in order to cope with own-transactions among mobile operators as a tribute for sharing small cell infrastructure [75]. BEAT is a permissioned blockchain-established trustworthy and honest infrastructure sharing framework for 6G and surpassing 6G mobile networks, providing accountability and transparency parameters where infrastructure is shared among providers having device-level accountability and SCs initializing service-level agreements [76].

6.2.3. *Blockchain established Virtual Private Network*

In a blockchain-established framework for access control in large-scale inter-organizational IoT networks, IoT devices attached to various organizations but corporate with each other are included in the same VPN for optimizing time and resources for access control using the blockchain in a per-VPN approach [25].

6.2.4. Blockchain established Software-defined virtual Networks

Virtual Network Embedding (VNE): efficient allocation and implementation of virtual network requests using a blockchain-established VNE algorithm has shown high fault tolerance performance in software-defined virtual networks [19]. A three-layered consortium blockchain with a joint proof-of-stake and a modified version of PBFT consensus along with a vehicle trust value prediction approach is engaged to allocate more resources to high-credibility vehicles of a software-defined virtual network, where the multipath mapping task of the virtual network is converted to a flow problem involving multiple commodities in order to improve resource allocation efficiency [24]. A framework integrating SDN, edge computing, and blockchain technology for achieving efficient and secure wireless network virtualization where SDN enables network programming, edge computing enables user signal processing at base stations with low delay, and blockchain allows to halt the double-spending attack of reserving the same physical wireless resource to multiple virtual networks [18]. Software-defined IoT management virtual resources that support multi-tenancy can be hosted on edge devices where permissioned blockchain is engaged to securely distribute code and act as storage, which has resulted in low delay performance [77].

6.2.5. Blockchain established Elastic network

Blockchain has been engaged to receive and process device-to-device vehicular transactions, where a categorized and chiefless consensus approach is engaged to decrease communication burden and improve scalability, and Lyapunov optimization is engaged for elastic resource allocation of the vehicular network in order to achieve high throughput [78].

6.2.6. Blockchain established spectrum slicing

In cyber-physical social systems engaging wireless communication, SCs on blockchain have been used for spectrum management, where the spectrum of a local cell is sliced into multiple channels and each channel is allocated a blockchain, and then using a KM protocol for transaction processing, where users mine or lease to access spectrum [17]. Bloc6Tel is a blockchain-integrated, secure, and trusted 6G spectrum allocation framework among telecom providers, where a blockchain-established auction algorithm engaged using SCs allocates the sliced spectrums, while telecom providers act as bidders and government authorities as auctioneers [20]. STBC is a spectrum trading platform for trading multiple sliced spectra among virtual networks in an efficient and secure manner using blockchain, which has a consensus mechanism to tolerate up to 33% of malicious nodes and sharding to improve the blockchain efficiency, which can prevent DDoS attacks using anonymous transactions [79]. Similarly, another blockchain-supported spectrum trading platform for elastic virtual optical networks, which trades different sliced spectrums established on the capacity requirements of virtual networks, where a virtual network with unutilized spectra can trade away the unused spectra and be rewarded with credits, while blockchain ensures the trustworthiness of the trading records, has been studied in [80]. For a wireless network operated by multiple virtual network operators, a decentralized blockchain-enabled spectrum acquisition system to dynamically acquire the downlink spectrum by minimizing the total transmit power while fulfilling the average transmission rate thresholds has been effective by automatically achieving spectrum acquisition, charging, and authorization with the aid of SCs [81].

6.2.7. Blockchain established Infrastructure slicing

An infrastructure slicing framework for providing virtual network functions by creating network slices and engaging blockchain to provide auditability and orchestration operations of sliced infrastructure while guaranteeing privacy and isolation of slices has been suggested in [16]. In [82], SCs on consortium blockchain are engaged for safe resource slicing and trading amidst mobile virtual network operators in a 5G radio access network, where the incentive mechanism is formulated as a two-stage Stackelberg game and its equilibrium is achieved through a duelling deep Q network.

6.2.8. Blockchain established Network slicing

DBNS is a scheme that enables distributed network slicing, which provides the opportunity for service and resource suppliers to lease resources dynamically to provide good performance for the services. It has a global service positioning component to provide admission control and dynamic resource assignment using a bidding system founded on blockchain [83]. In [15], blockchain is engaged as a secure network slice broker to provide a factory as a service that allows coordination of slice and security service level agreement managers to provide distributed network services for allocating resources using a federated slice selection algorithm with a Stackelberg game approach, where optimal prices are computed using DRL. Similarly, NSBchain is another blockchain-established network slicing brokerage framework that addresses new business models' requirements by defining an intermediate broker, allowing infrastructure suppliers to assign network assets to intermediate brokers with the aid of SCs and intermediate brokers to assign and distribute resources between tenants [84]. A hierarchical framework engages a consortium blockchain for spectrum trading amidst infrastructure suppliers acting as providers and mobile virtual network operators acting as buyers to create network slices and subsequent slice adjustment by considering underloaded and overloaded mobile virtual network operators, where incentive maximization by demand and pricing prediction is achieved using a 3-stage Stackelberg game whose equilibrium is realized using DRL [85]. BENS is a network slicing scheme using blockchain consensus that implements a leaning established algorithm that deals with the allocation of spectrum with proper primary user and secondary user interactions, minimizing 5G service provider costs, and providing the opportunity for resource providers to contract resources dynamically [86]. For service guarantee in inter-domain network slicing, SCs on blockchain are engaged to manage the lifecycle of service level agreements from service negotiation to decommissioning, using an artificial intelligence-driven closed loop to monitor exchanged services and predict service level agreement violations to activate mitigation actions [87]. A latency aware and user equipment state-established network slice allocation is realized in a transparent and secure manner for 5G mobile network slicing using blockchain in order to improve resource handling operation efficiency [88]. Blockchain is engaged to store service parameters securely using an encryption algorithm (trapdoor order-revealing) to preserve privacy, where SCs are engaged to audit the network slicing-service

Table 3: Interpretation of Blockchain-established network virtualization frameworks.

Virtualization technique	Stratagem	BC construct	Blockchain arrangement	Blockchain consensus	Blockchain division	Virtual technology	Network division	Performance
Spectrum sharing	B-ESSS [70]	C2	Regular	PoW	Consortium	Overlay	5G	Secure, efficient spectrum sharing, high throughput
	BEDSS [22]	C4	Regular	PoStrategy	Generic	Overlay	6G	Prevent SPoF, good system utility
	ProBLeSS [71]	C3, C4	Regular	PCA	Generic	Overlay	IoBT	Reduced CU-2.74%, Increased BR:8.3%, SD:5.5%
	DAG-EUA [23]	C4	Irregular	DTS	Generic	Overlay	6G-IoT	10% enhancement in global utility
	GTAB-BSS [72]	C3	Regular	Generic	Generic	Overlay	5G-IoT	Improve spectrum sharing by 55.1%
	WDP-DRL [73]	C3	Regular	PoW	Consortium	Overlay	IoT	Satisfy differential privacy, rationality, truthfulness
	MODSS [74]	C3	Regular	PBFT, RAFT, Kafka	Consortium	Overlay	Wireless	Average latency increases with participants
	MOSS [21]	C3	Regular	PBFT	Permissioned	Overlay	Wireless	High privacy, openness, and fairness
Infrastructure sharing	B-IS [75]	C5	Regular	dBFT	Consortium	Overlay	5G-SC	No performance evaluation
	BEAT [76]	C3	Regular	PoAuthority	Permissioned	Overlay	6G	Low overhead processing time
Virtual private network	VPNB-DAC [25]	C5	Regular	Generic	Generic	VPN	IoT	Secure, decentralized, scalable access control
Software-defined networking	B-BVNE [19]	C2	Regular	Generic	Generic	APN, overlay, elastic	SDVN	High fault-tolerant performance
	CB-BSSDN [24]	C4	Regular	PoS + PBFT	Consortium	APN, overlay, elastic	SDVN	Better safety, LB, low consensus time
	SDN-EC-BC [18]	C2	Regular	Generic	Generic	APN, overlay, elastic	Wireless	Increased trust, throughput, transparency
	V-IoT-EH [77]	C2	Regular	PBFT	Permissioned	APN, overlay, elastic	SD-IoT	Permissioned BC can store virtual resource state data
Elastic network	ERA-D2D [78]	C2	Regular	Grouped and leaderless	Generic	Elastic	Vehicular	Low communication overhead
Spectrum slicing	BBDSA-CPSS [17]	C3	Regular	PoS + PoW	Private	Elastic	Cyber-physical	High security, prevent SPF
	Bloc6Tel [20]	C3	Regular	Generic	Generic	Elastic	6G	Better resource utilization, request overhead, fairness
	STBC [79]	C4	Regular	Custom	Generic	Elastic	5G-IoT	Prevent double spending, DDoS, 30% better spectrum utilization
	B-AST [80]	C4	Regular	PoContribution	Generic	Elastic	Optical	Improves network capacity utilization, QoS
	DB-BDSA [81]	C3	Regular	PBFT, Raft	Permissioned	Elastic	Wireless	Similar minimum sum power for spectrum allocation
Infrastructure slicing	ISIVF-B [16]	C1	Regular	BFT	Consortium	Overlay	Generic	Secure, but consensus is challenging
	B-RTDRL [82]	C3	Regular	PBFT	Consortium	Overlay	5G	Reduce double spending attack by 12%
Network slicing	DBNS [83]	C3	Regular	Generic	Private	Overlay	5G	Improved throughput, acceptable average delay
	SNSB [15]	C1	Regular	PBFT	Public/ consortium	Overlay	5G	High success rate, low mean federated slice cost
	NSBchain [84]	C1	Regular	Kafka/Raft	Consortium	Overlay	5G	Good throughput, SR collision increases with variance
	CB-STNS [85]	C3	Regular	Generic	Consortium	Overlay	5G	Utility is maximized, fair, secure
	BENS [86]	C4	Regular	Custom	Private	Overlay	5G	High energy efficiency, overall system throughput
	B-ZTSA [87]	C1	Regular	Default Corda	Permissioned	Overlay	5G	Predict dynamics in service demand accurately
	NS-5G [88]	C3	Regular	PoAuthority	Generic	Overlay	5G	Improved transparency and efficiency of resource handling
	B-SLAAS [89]	C3	Regular	PoW	Public	Overlay	5G	Low encryption time, gas consumption
	SliceBlock [90]	C2	Irregular	PoSpace	Generic	Overlay	6G	Secure and scalable network slicing
Network function virtualization	NFV-MANO [91]	C4	Regular	Custom	Generic	Overlay	IoV	Lower loss and high reward
	BE-SLA [92]	C3	Regular	PoW	Private	Overlay	Edge	Less time required for SLA, validation time increases with transactions, nodes
	B-NFV-MEC [93]	C4	Regular	Custom	Generic	Overlay	Mobile edge cloud	Low latency and operational cost in resource allocation
	B-NFV-ASC [94]	C3	Regular	Generic	Public	Overlay	Cloud	Throughput up to 20%
	BRAIN [95]	C3	Regular	PoW	Public	Overlay	Generic	Feasible, consume additional fees, time

	NFV-B5G [96]	C2	Regular	Generic	Generic	Overlay	5G	Latency increases with nodes, arrival rate
	CMM-NFV [97]	C1	Regular	PBFT	Generic	Overlay	Generic	Total data, consensus time increase with BC modules
Service chaining	SCS-B [98]	C3	Regular	PoW	Private	Overlay, APN, elastic	SDN	28.7% saving in retrieval time

level agreements and activate punishments automatically when violating such agreements [89]. SliceBlock utilizes generative adversarial networks for network slicing, considering slice capacity, QoS demands, etc., where an irregular blockchain with proof-of-space consensus is engaged per slice in 6G network function virtualization environments for ensuring the security and privacy of transactions in each slice [90].

6.2.9. Blockchain established Network function virtualization

Blockchain has been engaged in reaching distributed consensus between various administration and orchestration systems for network function virtualization, in which mobile edge computing is engaged to handle blockchain computations where node, administration and orchestration system, and edge server selection are formulated as a problem and solved using DRL [91]. In edge-established network function virtualization, in order to provide trusted service level agreements among the infrastructure provider and edge device owner, SCs engaged on a private blockchain have been engaged, replacing trustless centralized authority [92]. Similarly, for the mobile edge cloud paradigm for distributed network function virtualization under multiple management and orchestration systems, blockchain has been engaged to reach consensus among such systems along with an optimization approach to resource allocation considering service latency and operational cost [93]. Alternatively, network function virtualization has been engaged to virtualize the work of the blockchain using the autonomous operation of SCs among virtual nodes established on cloud computing, where transactions among the virtual nodes occur smoothly through the blockchain [94]. BRAIN is a blockchain established reverse auction mechanism where infrastructure providers compete to supply network function virtualization considering the demands of specific end users, which enables the monetization of network function virtualization and reduces the costs associated with it [95]. Blockchain has been engaged to dynamically share spectrum resources among industry applications that use network function virtualization gadgets while reaching extremely reliable low-latency communication requirements in 5G and beyond mobile networks [96]. Blockchain has been effective in secure administration, setup, and migration of virtual network functions by providing a robust framework for storing configuration updates in an immutable manner and providing anonymity for virtual network functions and tenants [97].

6.2.10. Blockchain established Service chaining

Blockchain has been engaged to ensure the reliability and traceability of service chaining data in software-defined networking, where bloom filters and SCs are engaged to improve the retrieval efficiency from blockchain [98].

7. Review Interpretation

7.1. Interpretation of each system

Table 3 illustrates the complete interpretation of each blockchain-established network virtualization framework in relation to blockchain-related parameters, network virtualization parameters, techniques, network-related parameters, etc.

7.2. Overall Interpretation

Fig. 7 chart-wise illustrates the overall allocation of BC-established network virtualization frameworks deliberated within this work.

As illustrated in Figure 7a, the most prevalent blockchain-established network virtualization concept is held by C3 (45%), followed by C4 (22.5%), C2 (17.5%), C1 (12.5%), and C5 (5%). Thus, operating blockchain and SCs for providing service level agreements, auction algorithms for resource trading, and similar items in network virtualization are most prominent in existing literature, while blockchain-established access control for network virtualization is scarce. Moreover, as illustrated in Fig. 7b, 95% of blockchain-established network virtualization frameworks engage regular blockchain architecture, while only 5% use irregular blockchain. As illustrated in Fig. 7c, 22.5% of BC-established network virtualization frameworks do not emphasize a definitive universal assent technique apart from the remaining frameworks, where PoW (15%) is the most prevalent universal assent approach, followed by PBFT (12.5%), customized universal assent, PoAuthority, PoSpace, and so on. Furthermore, as illustrated in Fig. 7d, overlay networks are the most prevalent network virtualization technology (80%) used in the blockchain-established network virtualization frameworks reviewed, followed by elastic networks (27.5%), APN (12.5%), and VPN (2.5%). Additionally, as illustrated in Fig. 7e, BC-established network virtualization has been applied mostly to 5G networks (27.5%), followed by generic wireless networks, 6G, generic networks, IoT, 5G-IoT, SDVN, and so on. Finally, by looking at Fig. 7f, it is evident that the BC-established network virtualization concept was kickstarted in 2016 and eventually reached the highest level of concept proposals in 2020, then gradually contracted in publication volume afterwards.

As per the review, advantages such as enhanced privacy [70], reduced administrative expenses [22], prevention of SSDF attacks [71], high openness and fairness [21], high fault tolerance [19], prevention of SPF [17], better resource utilization [20], prevention of double spending and DDoS attacks [79], etc. exist in blockchain-established NV compared to traditional NV.

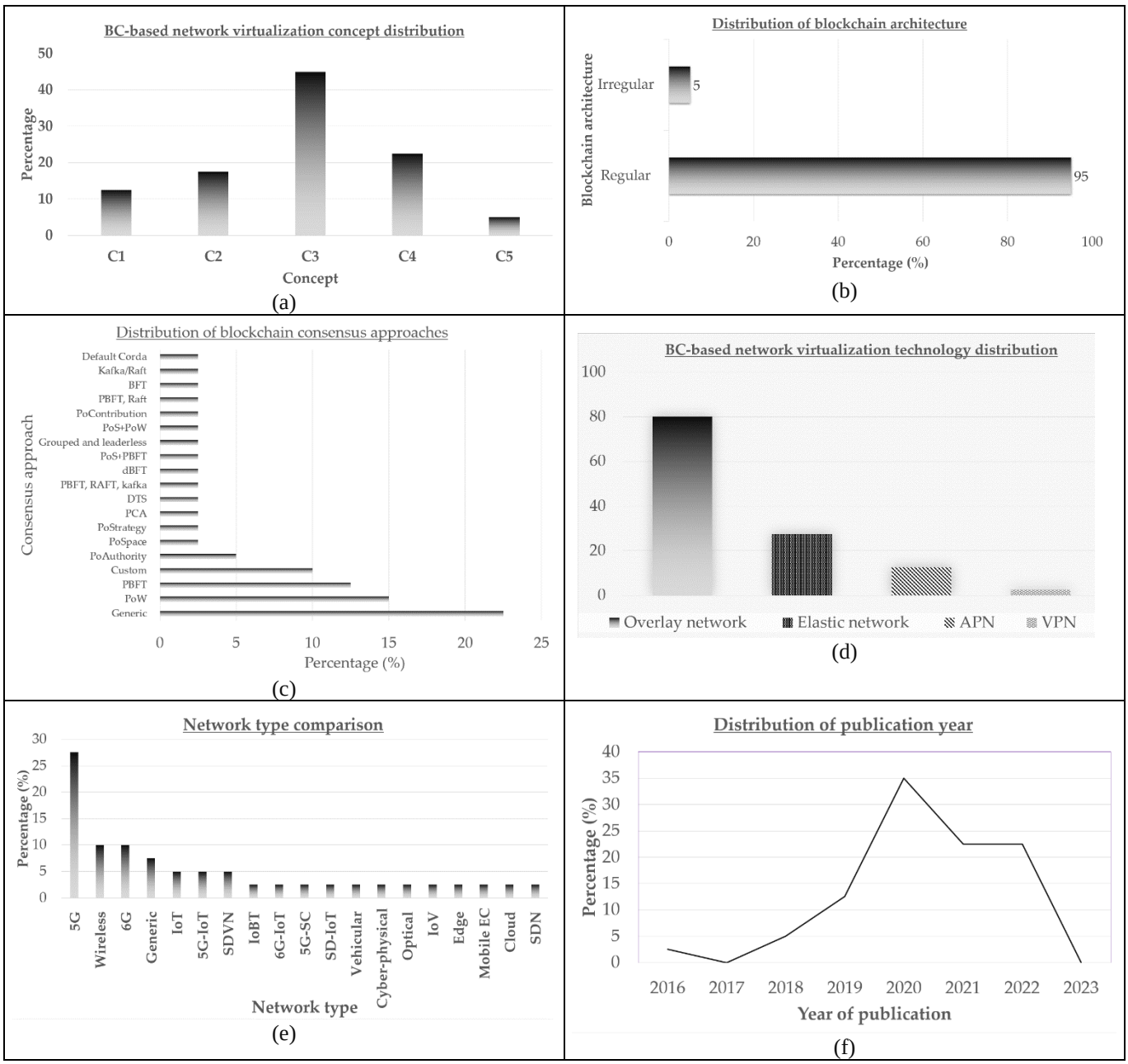


Fig. 7: Overall interpretation (a)BC-established virtualization construct (b) BC form (c) BC universal assent (d) NV technology (e) Network form (f) Instance of publication

However, from the review, we can also highlight drawbacks like latency increment with participants [74], challenging consensus [16], consuming additional fees [95], latency increment with arrival rate [96], consensus time increment [97], etc. Some possibilities and obstacles are discussed in the following subsection.

As a summary, we can specify incentive-based spectrum sharing [70], ring signature technique and a new proof-of-strategy consensus [22], blockchain-established spectrum sharing (ProBLeSS) protocol [71], dynamic tip selection strategy [23], a game theoretic approach along with a tit-for-tat technique [72], DRL and double auction technique [73], Stackelberg game [74, 82, 15, 85], punishment technique [21], HSS [75], service level agreements [76, 87, 89, 92], access control [25], VNE [19], joint consensus and trust prediction [24], SDN and edge computing [18, 77], Lyapunov optimization [78], KM-protocol [17], auction algorithm [20], spectrum trading [79, 80], spectrum acquisition [81], BC-based infrastructure slicing [16], bidding system [83], slicing brokerage [84], slice allocation [88], leaning established algorithm [86], generative adversarial networks [90], DRL [15, 73, 85, 91], consensus and optimization [93], smart contracts [94], reverse auctioning [95], NFV [96, 97], and SDN and bloom filter [98], as algorithms, protocols, or technologies utilized for BC-established NV discussed in this interpretation.

8. Discussion

8.1. Possibilities

8.1.1. Compatibility with resource trading platforms

Slicing and sharing operations in network virtualization can involve resources such as infrastructure and spectrum trading, where these resources are traded established on a pricing scheme. Blockchain is readily integrable with such platforms

to trade resources among InPs and MVNOs as buyers, considering the load of the operators. In these systems, game theory is utilized for modelling interactions and deciding the optimum incentive scheme. Blockchains go hand in hand with resource trading frameworks, as blockchains support securely performing resource trading transactions automatically using SCs and consensus approaches with punishment techniques for malicious users using incentives decided using game theory for trading transactions.

8.1.2. Preventing central node of collapse

In a centralized architecture of networking, typically a centralized authority is responsible for making decisions related to network virtualization, such as spectrum allocation, such that these systems are vulnerable to the central node collapsing. However, in blockchain-integrated network virtualization, it is free from the central node of collapse, as the approach of blockchain is decentralized and collaborative network virtualization involving multiple parties, such as InPs and MVNOs, in decision-making. Thus, even if the activity of one party is broken due to failure, the network virtualization system can perform normally as it is not relying on a centralized authority. For instance, if blockchain is applied to traditionally centralized networks such as software-defined, NFV-driven underwater networks [99], it has the capability to reduce the drawbacks of central node collapse.

8.1.3. Improves the privacy and trustfulness

One of the main purposes of engaging blockchains for network virtualization is to improve the privacy and trustfulness of the process. In particular, blockchains use pseudonymous cryptographic addresses, making transactions partially private, whose privacy can be further improved by using cryptographic algorithms and privacy-aware SCs [100]. Moreover, blockchains provide a trustful environment for virtualizing the network due to the immutable nature of blockchain transactions, and untrusted devices can be identified using consensus approaches to remove them from network operation. For instance, in an NFV instance of data collection in SDN, blockchain can be effectively utilized to improve data collection security and privacy [101]. Furthermore, it can monitor the network devices to provide a trust value for each node to facilitate trust-value established resource allocation in network virtualization. Additionally, SCs can be engaged to provide trusted service level agreements among the infrastructure providers and device owners to implement a trust-established resource allocation scheme.

8.1.4. Provides opportunity for common agreement among multiple parties

Network virtualization involves network slicing and sharing operations with the involvement of multiple resource providers and resource requestors [102]. In conventional network virtualization, it is challenging to come to a common agreement during network virtualization-related decisions. However, blockchain provides a handy framework to come to a common agreement thanks to its distributed consensus approach. These consensus approaches can additionally consider factors such as reducing administrative expenses, improving the global utility of demand and supply, reducing communication overhead, etc. while reaching agreement among multiple parties and being tolerated to a certain degree of malicious devices as decided by the consensus algorithm.

8.1.5. Efficient resource management

Blockchain-established network virtualization techniques bestow a platform for efficient resource allocation. For instance, in knowledge-defined networks, NFV can be utilized with the aid of machine learning techniques to manage network resources efficiently while achieving the desired network functions [103]. In these virtual networks, blockchains can improve the security of resource management. In these scenarios, efficiency is yielded as a result of sharing or slicing the same physical infrastructure among multiple virtual networks. The performance impact of engaging blockchain for security can be reduced by using energy-efficient blockchain implementations [104] such that the efficiency achieved for resource utilization by network virtualization is not degraded by blockchain. It includes using sharding techniques for blockchains [105], getting the support of edge computing to lower latency [106], etc. to improve the efficiency of blockchains.

8.2. Obstacles

8.2.1. High complexity and cost

When a new transaction is appended to the blockchain, it is only validated by the peers after several sessions of peer-to-peer broadcasts of the transaction and upon majority validation using a consensus approach [107]. Thus, when network virtualization is established on a blockchain network, the distributed approach for network virtualization transactions such as resource allocation data, virtual network embedding, etc., can cause additional complexity in the system compared to traditional network virtualization. Moreover, in order to engage blockchain, additional computation, memory, and communication resources will be required, which will elevate the total cost of the network virtualization process. Furthermore, as data analysis and decision-making are core processes in virtual networks, knowledge generation models like machine learning [108] can further make the system even more complex.

8.2.2. Majority attacks and SC vulnerabilities

Even though blockchain is secure under a smaller fraction of malicious devices, it can be vulnerable under a majority of malicious devices. This attack is known as the 51% vulnerability of the blockchain, where a majority of malicious devices can validate a malicious transaction in the blockchain [109]. In such a scenario, the security of the blockchain-established network virtualization process is compromised, and virtualization operations such as network slicing can be unfair and biased to the malicious users of the network. Moreover, SCs can be vulnerable if their code is not verified under all conditions. If SC code is not written without errors, attackers may gain control over the blockchain upon execution of the SCs, putting the total process of network virtualization in danger.

8.2.3. Performance degradation in real-time network virtualization

Spectrum, infrastructure, and network slicing and sharing operations in network virtualization typically require making decisions in real-time relying on different types of data, such as spectrum allocation data, service provider availability and load, network latency, user equipment state,

etc. [110]. However, blockchain networks may introduce an additional delay because of the distributed consensus process, and this delay will elevate with the rise in network extent. Therefore, the engagement of blockchain in securing the process of network virtualization will be challenging, as it may reduce the capability of making timely network virtualization decisions because of additional delays introduced in the blockchain network.

8.2.4. Low scalability in storage and transaction processing

When the network extent related to the network virtualization task is large, blockchains may struggle to perform efficiently, as in a low-size network, the storage requirements and transactions required to process them elevates rapidly with the network extent. So, the total throughput and efficiency of blockchain transactions will degrade with the rise of network extent, making it challenging to perform network virtualization operations such as slicing and resource allocation in real-time.

8.2.5. Lack of standardizations and maturity

Blockchain-established network virtualization is an emerging concept that has not yet been standardized to the best of our knowledge. This field is still evolving, so different researchers have recommended different realizations of blockchain-established solutions for achieving different network virtualization tasks. This lack of maturity can be stated as a challenge in the industrial implementation of blockchain-established network virtualization techniques, as it can be hard to find the best blockchain platform suitable for a given problem of network virtualization.

8.2.6 Implementation difficulties

As reviewed in this interpretation, blockchain-established NV has difficulties in scalability where there can be performance bottlenecks like latency being increased beyond an acceptable level when the number of nodes or blockchain modules increases [96], [97]. Moreover, as blockchain-established NV is still a less matured research domain, there exists a deficiency in industry standards to implement the system. Different networks may implement different blockchain systems from diverse vendors and diverse networking elements, which can act as a barrier for these systems to be compatible with each other and become interoperable. Moreover, as regulations for blockchains are still in the process of formulation, when practically implementing a blockchain-established NV instance, there can be regulatory challenges as well.

9. Conclusion, Suggestions, and Prospective Paths

In this interpretation, we first denoted a compendium of network virtualization, denoting technologies, the business model, architectural principles, and characteristics. Next, the core concepts of network virtualization were briefly introduced. Following a concise prelude to the distributed ledger framework, we interpreted current frameworks of blockchain-established network virtualization under different virtualization techniques and concepts. Grounded in this documentary analysis, we identified 5 segments of the blockchain-established network virtualization construct: blockchain as a broker/manager for slicing, secure storage of data for network virtualization, SCs-established service level agreements, auction algorithms, etc., consensus approaches for network virtualization, and blockchain-established access control for network virtualization. Thereafter, we completely interpreted these frameworks in relation to network virtualization, blockchain features, and the blockchain-established network virtualization concept to examine directions and chasms. Finally, we deliberated the possibilities and obstacles of blockchain-established network virtualization.

This piece of work provides beneficial knowledge for current literature by providing state-of-the art blockchain-established frameworks for network virtualization along with a complete interpretation. Applying this examination, someone can instantly examine directions and chasms in blockchain-established network virtualization and also formulate anticipated time research, established on suggestions provided for the examined obstacles. Thus, forthcoming academicians can benefit from the complete interpretation and deliberation by getting insight into current works and examining where improvements are required.

Based on the detected obstacles, succeeding suggestions can be offered to mitigate them.

- Even though the infrastructure cost of transitioning from conventional network virtualization to blockchain-established virtualization is unavoidable, the operational cost and complexity can be reduced in several ways. First, SCs can be optimized for minimizing computations. In cases where blockchain-established authentication is engaged, lightweight authentication approaches using low computationally intensive cryptographic algorithms can be engaged for authentication during network virtualization. Moreover, administrative cost-reducing consensus approaches, for instance, proof-of-strategy, can be engaged.
- The 51% vulnerability of blockchain can be resisted by using a consensus approach such as delegated proof-of-stake instead of proof-of-work. Moreover, in the case of a 51% attack, an emergency response plan can help minimize the impact of such an attack. Before engaging SCs, they must be thoroughly verified formally to prove that they are mathematically and functionally correct. Moreover, regular auditing must be carried out to check whether the SCs perform in the manner specified once they are engaged in the blockchain.
- In the interest of satisfying the low latency and high throughput requirements of network slicing and sharing operations, blockchains can engage several techniques. First, sharding can be engaged to partition the blockchain into a set of subsets, where each subset can execute transactions separately, enhancing the throughput. A major source of delay in blockchain networks is the consensus process; thus, a low-delay consensus approach such as proof-of-stake is more suitable for network virtualization than proof-of-work. Moreover, if possible, the resources of the communication network infrastructure can be upgraded, such as by increasing the bandwidth of the links to complete the consensus process in a short amount of time.
- In the interest of overcoming the issues with scalability for transaction processing, network managers can engage an irregular blockchain that has a higher scalability because of its parallel processing capacity. As a solution to the scalability issue of storage, off-chain storage can be

supplemented with the blockchain, where less critical network virtualization data can be recorded off-chain. Alternatively, data can be recorded off-chain, which has the hash digest of the data recorded in blockchain to verify its validity, providing a scalable solution for secure data storage.

- In the interest of overcoming the lack of maturity for blockchain-established network virtualization, when selecting a blockchain framework for a given network virtualization task, one will have to refer to existing research work to select the type of blockchain, consensus approach, incentive mechanism, etc. because of the unavailability of industry standardizations. In the case that the existing literature does not provide satisfactory knowledge on the performance of combinations of the blockchain platform and network virtualization approach for a given network scenario, one can do a performance evaluation and select the best combination after inspecting the evaluation results.

Blockchains can be engaged to secure the integrity, privacy, authenticity, and trustfulness of different network virtualization processes, such as spectrum/infrastructure/network slicing/sharing. Forthcoming research amidst blockchain-established network virtualization may entangle developing standardizations for blockchain and network virtualization approach combinations. Furthermore, forthcoming work can probe the impact of quantum computing for authentication related to blockchain-established network virtualization.

CRediT Authorship Contribution Statement

Patikiri Arachchige Don Shehan Nilmantha Wijesekara: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Validation, Visualization, Roles/Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The ethical issues; including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, redundancy has been completely observed by the authors.

References

[1] C.H. Wang, Y.H. Chu, and T.T. Wei, "SIPTVMON: a secure multicast overlay network for load-balancing and stable IPTV service using SIP," in *2011 IEEE INFOCOM WKSHPS*, 2011, pp. 97-102.

[2] W. Kellerer, A. Basta, P. Babarczi, A. Blenk, M. He, M. Klugel, and A.M. Alba, "How to measure network flexibility? A proposal for evaluating softwarized networks," *IEEE Communications Magazine*, Vol. 56, No. 10, pp.186-192, 2018

[3] H.B. Lim, M. Iqbal, and T.J. Ng, "A virtualization framework for heterogeneous sensor network platforms," in *7th ACM Conference on Embedded Networked Sensor Systems*, 2009, pp. 319-320.

[4] M.M. Hasan, H. Amarasinghe, and A. Karmouch, "Network virtualization: Dealing with multiple infrastructure providers," in *2012 IEEE ICC*, 2012, pp. 5890-5895.

[5] L. Cano, A. Capone, G. Carello, M. Cesana, and M. Passacantando, "On optimal infrastructure sharing strategies in mobile radio networks," *IEEE Transactions on Wireless Communications*, Vol. 16, No. 5, pp.3003-3016, 2017

[6] N. Kitsuwan, K. Akaki, P. Pavarangkoon, and A. Nag, "Spectrum allocation scheme considering spectrum slicing in elastic optical networks," *Journal of Optical Communications and Networking*, Vol. 13, No. 7, pp.169-181, 2021

[7] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks," *Telecom*, Vol. 4, No. 3, pp. 393-458, 2023.

[8] M. Bhandary, M. Parmar, and D. Ambawade, "A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle," in *2020 5th ICCES*, 2020, pp. 827-832.

[9] P.A.D.S.N. Wijesekara, "A Literature Review on Access Control in Networking Employing Blockchain," *Indonesian Journal of Computer Science*, Vol. 13, No. 1, pp. 734-768, 2024.

[10] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Network*, Vol. 34, No. 6, pp.133-139, 2020

[11] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pp. 47-55, 2018.

[12] P.A.D.S.N. Wijesekara, "A Review of Blockchain-Rooted Energy Administration in Networking," *Indonesian Journal of Computer Science*, Vol. 13, No. 2, pp. 1607-1642, 2024.

[13] Z.M. Khalid, and S. Askar, "Resistant Blockchain cryptography to quantum computing attacks," *International Journal of Science and Business*, Vol. *5*, No. 3, pp.116-125, 2021.

[14] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges," *Network*, Vol. 3, No. 3, pp. 343-421, 2023.

[15] T. Hewa, P. Porambage, I. Kovacevic, N. Weerasinghe, E. Harjula, M. Liyanage, and M. Ylianttila, "Blockchain-based network slice broker to facilitate factory-as-a-service," *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 1, pp.519-530, 2022

[16] G.A.F. Rebello, G.F. Camilo, L.G. Silva, L.C. Guimarães, L.A.C. de Souza, I.D. Alvarenga, and O.C.M. Duarte, "Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology," in *2019 IEEE 20th International Conference on HPSR*, 2019, pp. 1-6.

[17] X. Fan, and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," *IEEE Access*, Vol. 8, pp.64486-64498, 2020.

[18] D.B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Communications Magazine*, Vol. 57, No. 10, pp.50-55, 2019.

[19] H. Cao, Y. Hu, Q. Wang, S. Wu, and L. Yang, "A blockchain-based virtual network embedding algorithm for secure software defined networking," in *IEEE INFOCOM 2020*, 2020, pp.1057-1062.

[20] F. Patel, P. Bhattacharya, S. Tanwar, R. Gupta, N. Kumar, and M. Guizani, "Block6Tel: Blockchain-based spectrum allocation scheme in 6G-envisioned communications," in *2021 IWCMC*, 2021, pp. 1823-1828.

[21] S. Zheng, T. Han, Y. Jiang, and X. Ge, "Smart contract-based spectrum sharing transactions for multi-operators wireless communication networks," *IEEE Access*, Vol. 8, pp.88547-88557, 2020.

[22] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *IEEE ICC 2020*, 2020, pp. 1-6.

[23] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT," *IEEE Internet of Things Journal*, Vol. 9, No. 11, pp.8012-8023, 2021.

[24] N. Zhao, H. Wu, and X. Zhao, "Consortium blockchain-based secure software defined vehicular network," *Mobile Networks and Applications*, Vol. 25, pp.314-327, 2020.

[25] R. Trabelsi, G. Fersi, and M. Jmaiel, "Virtual Private Network Blockchain-based Dynamic Access Control Solution for Inter-organisational Large Scale IoT Networks," in *International Conference on Risks and Security of Internet and Systems*, 2022, pp. 207-222.

[26] P.A.D.S.N. Wijesekara, "A study in University of Ruhuna for investigating prevalence, risk factors and remedies for psychiatric illnesses among students," *Scientific Reports*, Vol. 12, No. 1, pp. 12763, 2022.

[27] P.A.D.S.N. Wijesekara, and Y.K. Wang, "A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka," *COVID*, Vol. 2, No. 6, pp. 793-826, 2022.

[28] L. Zichao, H. Ziwei, Z. Geng, and M. Yan, "Ethernet topology discovery for virtual local area networks with incomplete information," in *2014 4th IEEE International Conference on Network Infrastructure and Digital Content*, 2014, pp. 252-256.

[29] A. Mehdizadeha, K. Suinggia, M. Mohammadpoorb, and H. Haruna, "Virtual Local Area Network (VLAN): Segmentation and Security," in *third ICCTIM2017*, 2017, Vol. 78, p. 89.

[30] E. Ramadhani, "Anonymity communication VPN and Tor: a comparative study," *Journal of Physics: Conference Series*, Vol. 983, No. 1, p. 012060, 2018

[31] P. Knight, and C. Lewis, "Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts," *IEEE Communications Magazine*, Vol. 42, No. 6, pp.124-131, 2004.

[32] T. Lavian, and P.Y. Wang, "Active networking on a programmable networking platform," in *2001 IEEE OPENARCH*, 2001, pp. 95-103.

[33] G. Coulson, G. Blair, D. Hutchison, A. Joolia, K. Lee, J. Ueyama, A. Gomes, and Y. Ye, "NETKIT: a software component-based approach to programmable networking," *ACM SIGCOMM Computer Communication Review*, Vol. 33, No. 5, pp.55-66, 2003.

[34] M. Nkomo, G.P. Hancke, A.M. Abu-Mahfouz, S. Sinha, and A.J. Onumanyi, "Overlay virtualized wireless sensor networks for application in industrial internet of things: A review," *Sensors*, Vol. 18, No. 10, p.3215, 2018.

[35] S. Guenender, K. Barabash, Y. Ben-Itzhak, A. Levin, E. Raichstein, and L. Schour, "NoEncap: overlay network virtualization with no encapsulation overheads," in *1st ACM SIGCOMM Symposium on Software Defined Networking Research*, 2015, pp. 1-7.

[36] M. Alaluna, N. Neves, and F.M. Ramos, "Elastic network virtualization," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pp. 814-823, 2020.

[37] N. Shahriar, S. Taeb, S.R. Chowdhury, M. Tornatore, R. Boutaba, J. Mitra, and M. Hemmati, "Achieving a fully-flexible virtual network embedding in elastic optical networks," in *IEEE INFOCOM 2019*, 2019, pp. 1756-1764.

[38] N. Raveendran, Y. Gu, C. Jiang, N.H. Tran, M. Pan, L. Song, and Z. Han, "Cyclic three-sided matching game inspired wireless network virtualization," *IEEE Transactions on Mobile Computing*, Vol. 20, No. 2, pp.416-428, 2019.

[39] S.A. Kazmi, A. Ndikumana, A. Manzoor, W. Saad, and C.S. Hong, "Distributed radio slice allocation in wireless network virtualization: Matching theory meets auctions," *IEEE Access*, Vol. 8, pp.73494-73507, 2020.

[40] A. El Amri, and A. Meddeb, "Optimal server selection for competitive service providers in network virtualization context," *Telecommunication Systems*, Vol. 77, pp. 451-467, 2021.

[41] D.B. Rawat, A. Alshaikhi, A. Alshammari, C. Bajracharya, and M. Song, "Payoff optimization through wireless network virtualization for IoT applications: A three layer game approach," *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.2797-2805, 2018.

[42] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "An Optimization Framework for Data Collection in Software Defined Vehicular Networks," *Sensors*, Vol. 23, No. 3, pp. 1600, 2023.

[43] L. Lewin-Eytan, K. Barabash, R. Cohen, V. Jain, and A. Levin, "Designing modular overlay solutions for network virtualization," IBM Technical Paper, IBM Research Division, Haifa Research Laboratory, Mt. Carmel 31905, Haifa, Israel, 2012.

[44] Y. Cui, P. Wu, M. Xu, J. Wu, Y.L. Lee, A. Durand, and C. Metz, "4over6: network layer virtualization for IPv4-IPv6 coexistence," *IEEE Network*, Vol. 26, No. 5, pp.44-48, 2012.

[45] M. Bacou, G. Todeschi, D. Hagimont, and A. Tchana, "Nested virtualization without the nest," in *48th International Conference on Parallel Processing*, 2019, pp. 1-10.

[46] M. El Barachi, N. Kara, and R. Dssouli, "Towards a service-oriented network virtualization architecture," in *2010 ITU-T Kaleidoscope: Beyond the Internet?-Innovations for Future Networks and Services*, 2010, pp. 1-7.

[47] H. Lu, and F. Zhang, "Resource fragmentation-aware embedding in dynamic network virtualization environments," *IEEE Transactions on Network and Service Management*, Vol. 19, No. 2, pp.936-948, 2022.

[48] C. Seneviratne, P.A.D.S.N. Wijesekara, and H. Leung, "Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks," *Sensors*, Vol. 20, No. 2, pp. 567, 2020.

[49] Y. Dong, X. Zhang, J. Dai, and H. Guan, "HYVI: a hybrid virtualization solution balancing performance and manageability," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 9, pp.2332-2341, 2013.

[50] J. Kwon, T. Lee, C. Hähni, and A. Perrig, "SVLAN: Secure & scalable network virtualization," in *NDSS 2020*, 2020, Vol. 1, 2020, pp. 498-512.

[51] R. Sherwood, G. Gibb, K.K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, "Flowvisor: A network virtualization layer," *OpenFlow Switch Consortium*, Tech. Rep, 1, p.132, 2009.

[52] K. Yamada, Y. Kanada, K. Amemiya, A. Nakao, and Y. Saida, "VNode infrastucture enhancement—Deeply programmable network virtualization," in *2015 21st APCC*, 2015, pp. 244-249.

[53] P.A.D.S.N. Wijesekara, "Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving," *Open Transportation Journal*, Vol. 16, No. 1, pp. e187444782208191, 2022.

[54] X. Li, R. Casellas, G. Landi, A. de la Oliva, X. Costa-Perez, A. Garcia-Saavedra, T. Deiss, L. Cominardi, and R. Vilalta, "5G-crosshaul network slicing: Enabling multi-tenancy in mobile transport networks," *IEEE Communications Magazine*, Vol. 55, No. 8, pp.128-137, 2017.

[55] Ahmadi, H., Macaluso, I., Gomez, I., DaSilva, L. and Doyle, L., 2016, December. Virtualization of spatial streams for enhanced spectrum sharing. In *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

[56] A.J. Morgado, F.B. Saghezchi, S. Mumtaz, V. Frascolla, J. Rodriguez, and I. Otung, "A novel machine learning-based scheme for spectrum sharing in virtualized 5g networks," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 10, pp.19691-19703, 2022.

[57] C. Liang, and F.R. Yu, "Wireless virtualization for next generation mobile cellular networks," *IEEE wireless communications*, Vol. 22, No. 1, pp.61-69, 2015.

[58] A. Cárdenas, D. Fernández, C.M. Lentisco, R.F. Moyano, and L. Bellido, "Enhancing a 5G network slicing management model to improve the support of mobile virtual network operators," *IEEE Access*, Vol. 9, pp.131382-131399, 2021.

[59] R. Nejbati, S. Azodolmolky, and D. Simeonidou, "Role of network virtualization in future Internet innovation," in *2012 17th European Conference on Networks and Optical Communications*, 2012, pp. 1-4.

[60] J. Navarro-Ortiz, O. Sallent, and J. Pérez-Romero, "Radio access network slicing strategies at spectrum planning level in 5G and beyond," *IEEE access*, Vol. 8, pp.79604-79618, 2020.

[61] J.V. Ramrao, and A. Jain, "Dynamic 5G network slicing," *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 10, No. 2, pp. 1006-1010, 2021.

[62] D. Zhang, Z. Chang, T. Hämäläinen, and F.R. Yu, "Double auction based multi-flow transmission in software-defined and virtualized wireless networks," *IEEE Transactions on Wireless Communications*, Vol. 16, No. 12, pp.8390-8404, 2017.

[63] Y. Wang, L. Nguyen, and Q. Hu, "Network Function Virtualization in Elastic Optical Networks," *Journal of Lightwave Technology*, Vol. 41, No. 16, pp.5183-5192, 2023.

[64] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks," in *20th Academic Sessions*, p.60, 2023.

[65] R.S. Alonso, I. Sittón-Candanedo, R. Casado-Vara, J. Prieto, and J.M. Corchado, "Deep reinforcement learning for the management of software-defined networks and network function virtualization in an edge-IoT architecture," *Sustainability*, Vol. 12, No. 14, p.5706, 2020.

[66] M. Gharbaoui, et al., "An experimental study on latency-aware and self-adaptive service chaining orchestration in distributed NFV and SDN infrastructures," *Computer Networks*, Vol. 208, p.108880, 2022.

[67] P.A.D.S.N. Wijesekara, "A Review on Deploying Blockchain Technology for Network Mobility Management," *International Transactions on Electrical Engineering and Computer Science*, Vol. 3, No. 1, pp. 1-33, 2024.

[68] W. Li, H. Guo, M. Nejad, and C.C. Shen, "Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach," *IEEE access*, Vol. *8*, pp.181733-181743, 2020.

[69] P.A.D.S.N. Wijesekara, "Ethical Knowledge Sharing Leveraging Blockchain: An Overview," *Science, Engineering, and Technology*, Vol. 4, No. 1, pp.112-136, 2024.

[70] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Network*, Vol. 34, No. 1, pp.24-31, 2020.

[71] M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, and K. Veezhinathan, "ProBLeSS: A proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks," *IEEE Networking Letters*, Vol. 2, No. 2, pp.67-70, 2020.

[72] Y. Choi, and I.G. Lee, "Game theoretical approach of blockchain-based spectrum sharing for 5G-enabled IoTs in dense networks," in *2019 IEEE 90th VTC2019-Fall*, 2019, pp. 1-6.

[73] K. Zhu, L. Huang, J. Nie, Y. Zhang, Z. Xiong, H.N. Dai, and J. Jin, "Privacy-aware double auction with time-dependent valuation for blockchain-based dynamic spectrum sharing in IoT systems," *IEEE Internet of Things Journal*, Vol. 10, No. 8, pp. 6756-6768, 2022.

[74] Z. Li, W. Wang, Q. Wu, and X. Wang, "Multi-operator dynamic spectrum sharing for wireless communications: a consortium blockchain enabled framework," *IEEE*

Transactions on Cognitive Communications and Networking, Vol. 9, No. 1, pp.3-15, 2022.

[75] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5G small cell networks," in *2018 14th International CNSM*, 2018, pp.313-317.

[76] T. Faisal, M. Dohler, S. Mangiante, and D.R. Lopez, "BEAT: Blockchain-Enabled Accountable and Transparent Infrastructure Sharing in 6G and Beyond," *IEEE Access*, Vol. 10, pp.48660-48672, 2022.

[77] M. Samaniego, and R. Deters, "Hosting virtual iot resources on edge-hosts with blockchain," in *2016 IEEE International conference on CIT*, 2016, pp.116-119. IEEE.

[78] Y. Lin, J. Kang, D. Niyato, Z. Gao, and Q. Wang, "Efficient Consensus and Elastic Resource Allocation Empowered Blockchain for Vehicular Networks," *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 4, pp.5513-5517, 2022.

[79] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Transactions on Cognitive Communications and Networking*, Vol. 8, No. 1, pp.13-30, 2021.

[80] S. Ding, G. Shen, K.X. Pan, S.K. Bose, Q. Zhang, and B. Mukherjee, "Blockchain-assisted spectrum trading between elastic virtual optical networks," *IEEE Network*, Vol. 34, No. 6, pp.205-211, 2020.

[81] M. Jiang, Y. Li, Q. Zhang, G. Zhang, and J. Qin, "Decentralized blockchain-based dynamic spectrum acquisition for wireless downlink communications," *IEEE Transactions on Signal Processing*, Vol. 69, pp.986-997, 2021.

[82] G.O. Boateng, D. Ayepah-Mensah, D.M. Doe, A. Mohammed, G. Sun, and G. Liu, "Blockchain-enabled resource trading and deep reinforcement learning-based autonomous RAN slicing in 5G," *IEEE Transactions on Network and Service Management*, Vol. 19, No. 1, pp.216-227, 2021.

[83] M.A. Togou et al., "DBNS: A distributed blockchain-enabled network slicing framework for 5G networks," *IEEE Communications Magazine*, Vol. 58, No. 11, pp.90-96, 2020.

[84] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *IEEE ICC 2020*, 2020, pp.1-7.

[85] G.O. Boateng, G. Sun, D.A. Mensah, D.M. Doe, R. Ou, and G. Liu, "Consortium blockchain-based spectrum trading for network slicing in 5G RAN: A multi-agent deep reinforcement learning approach," *IEEE Transactions on Mobile Computing*, Vol. 22, No. 10, pp.5801 – 5815, 2022.

[86] S. Singh, C.R. Babu, K. Ramana, I.H. Ra, and B. Yoon, "BENS− B5G: blockchain-enabled network slicing in 5G and beyond-5G (B5G) networks," *Sensors*, Vol. 22, No. 16, p.6068, 2022.

[87] V. Theodorou et al., "Blockchain-based zero touch service assurance in cross-domain network slicing," in *2021 Joint EuCNC/6G Summit*, 2021, pp.395-400.

[88] P. Gorla, V. Chamola, V. Hassija, and D. Niyato, "Network slicing for 5G with UE state based allocation and blockchain approach," *IEEE Network*, Vol. 35, No. 3, pp.184-190, 2020.

[89] K. Xiao, Z. Geng, Y. He, G. Xu, C. Wang, and Y. Tian, "A blockchain-based privacy-preserving 5G network slicing service level agreement audit scheme," *EURASIP Journal on Wireless Communications and Networking*, Vol. 2021, No. 1, p.165, 2021.

[90] I.H. Abdulqadder, and S. Zhou, "SliceBlock: context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment," *IEEE Internet of Things Journal*, Vol. 9, No. 18, pp.18079-18097, 2022.

[91] X. Fu, F.R. Yu, J. Wang, Q. Qi, and J. Liao, "Performance optimization for blockchain-enabled distributed network function virtualization management and orchestration," *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 6, pp.6670-6679, 2020.

[92] M.S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-enabled SLA compliance for crowdsourced edge-based network function virtualization," *IEEE Network*, Vol. 35, No. 5, pp.58-65, 2021.

[93] X. Fu, F.R. Yu, J. Wang, Q. Qi, and J. Liao, "Resource allocation for blockchain-enabled distributed network function virtualization (NFV) with mobile edge cloud (MEC)," in *IEEE INFOCOM 2019*, 2019, pp. 1-6.

[94] H.A. Jawdhari, and A.A. Abdullah, "A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts," *Periodicals of Engineering and Natural Sciences*, Vol. 9, No. 4, pp.834-844, 2021.

[95] M.F. Franco, E.J. Scheid, L.Z. Granville, and B. Stiller, "BRAIN: Blockchain-based reverse auction for infrastructure supply in virtual network functions-as-a-service," in *2019 IFIP Networking Conference*, 2019, pp. 1-9.

[96] H. Huang, W. Miao, G. Min, J. Tian, and A. Alamri, "NFV and blockchain enabled 5G for ultra-reliable and low-latency communications in industry: Architecture and performance evaluation," *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 8, pp.5595-5604, 2020.

[97] I.D. Alvarenga, G.A. Rebello, and O.C.M. Duarte, "Securing configuration management and migration of virtual network functions using blockchain," in *NOMS 2018*, 2018, pp. 1-9.

[98] L. Sun, "Service Chaining Security Based on Blockchain," in *Journal of Physics: Conference Series*, Vol. 1634, No. 1, p. 012031, 2020.

[99] P.A.D.S.N. Wijesekara, W.M.A.K. Sangeeth, H.S.C. Perera, and N.D. Jayasundere, "Underwater Acoustic Digital Communication Channel for an UROV," in *5th Annual Research Symposium (ARS2018)*, p. E17, 2018.

[100] M.U. Hassan, M.H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, Vol. *97*, pp.512-529, 2019.

[101] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Data Gathering Optimization in Hybrid Software Defined Vehicular Networks," in *20th Academic Sessions*, p. 59, 2023.

[102] I. Afolabi, M. Bagaa, T. Taleb, and H. Flinck, "End-to-end network slicing enabled through network function

virtualization, in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 30-35, 2017.

[103] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Comprehensive Survey on Knowledge-Defined Networking," *Telecom*, Vol. 4, No. 3, pp. 477-596, 2023.

[104] P. Chithaluru, F. Al-Turjman, T. Stephan, M. Kumar, and L. Mostarda, "Energy-efficient blockchain implementation for cognitive wireless communication networks (CWCNs)," *Energy Reports*, Vol. *7*, pp.8277-8286, 2021.

[105] J. Xie, K. Zhang, Y. Lu, and Y. Zhang, "Resource-efficient DAG blockchain with sharding for 6G networks," *Ieee Network*, Vol. *36*, No. 1, pp.189-196, 2021.

[106] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, and M. Xu, "EEDTO: An energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing," *IEEE Internet of Things Journal*, Vol. *8*, No. 4, pp.2163-2176, 2020.

[107] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *CEUR workshop proceedings*, Vol. 2058, 2018.

[108] H.M.D.P.M. Herath, W.A.S.A. Weraniyagoda, R.T.M. Rajapaksha, P.A.D.S.N. Wijesekara, K.L.K. Sudheera, and P.H.J. Chong, "Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies," *Sensors*, Vol. 22, No. 18, pp. 6966, 2022.

[109] F.A. Aponte-Novoa, A.L.S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE access*, Vol. *9*, pp.140549-140564, 2021.

[110] Y. Li, L.T.X. Phan, and B.T. Loo, "Network functions virtualization with soft real-time guarantees," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pp. 1-9, 2016.

[111] H.A. Jawdhari, and A.A. Abdullah, "The application of network functions virtualization on different networks, and its new applications in blockchain: A survey," *Management*, Vol. 18, pp. 1007-1044, 2021.

Biography

Patikiri Arachchige Don Shehan Nilmantha Wijesekara obtained his first-class hons. B.Sc. Engineering degree specialized in Electrical and Information Engineering in 2017 from University of Ruhuna. He has received 6 academic awards for his bachelor's degree including 2 gold medals and 1 scholarship. He has published his research works in reputed journals and holds and H-index of 12. He is currently pursuing Ph.D. degree from the same university in computer networking. He has been recruited as a lecturer in university of Ruhuna since 2018. His research interests include networking, machine learning, and blockchain.