Blockchain-enabled Private 5G Networks: A Primer

Nisita Weerasinghe*, Tharaka Hewa†, Anshuman Kalla‡, Mika Ylianttila§, Madhusanka Liyanage¶,
*†§Centre for Wireless Communications, University of Oulu, Finland
‡CGPIT, Uka Tarsadia University, India
¶School of Computer Science, University College Dublin, Ireland
Email: *†§[firstname.lastname]@oulu.fi,‡anshuman.kalla@ieee.org,¶madhusanka@ucd.ie

***Abstract*—Private 5G Networks (P5GNs) are a newly emerging paradigm that the telecommunication sector and industry verticals are about to witness. The concept of P5GN is to build a 5G network with just enough infrastructure, which is required to fulfill the specific and local needs of an industry vertical. Broadly, P5GNs offer two-fold benefits. First, it creates new business opportunities for new entrants with small investments, and second, it satisfies the specific need of industry verticals with contextual and location-aware services and content. However, there are numerous challenges like spectrum scarcity, roaming fraud, limited infrastructure, confined coverage, security vulnerabilities, and management of massive small data. Thus, this paper aims to explore various existing challenges and discuss how blockchain technology, in conjunction with smart contracts, can be leveraged to mitigate them. Further, the implementation challenges in rolling out blockchain-enabled solutions are presented with possible solutions to overcome them.**

***Index Terms*—5G mobile communication, P5GN, Blockchain, Smart Contracts**

I. Introduction

The recent advancements in P5GNs have opened doors for new business opportunities and innovative ways to meet heterogeneous industry verticals' contextual and typical requirements. In general, P5GNs are built to operate as small cell communication infrastructure to cater to industry verticals' specific needs effectively. This is to say that from the user's perspective, P5GNs offer highly context-oriented services and content locally to the serving industry verticals, thereby complementing traditional mobile broadband offerings. Moreover, location-aware applications and use cases such as smart cities, smart factories, and smart hospitals can be rolled out in a dedicated and flexible manner using P5GNs. From the business perspective, P5GNs broaden the horizons of the 5G business value chain by allowing easy and less capital-intensive entry for new players (i.e., small operators) in the market. Despite the multitude of benefits and range of applications that can be achieved with the roll-out of the P5GNs, numerous challenges are blocking the road ahead. Some of these challenges are spectrum scarcity, roaming frauds, limited infrastructure, confined coverage, and massive small data [1], [2], [3], [4]. Hence, the quest is to address these challenges to reap timely the services of P5GNs.

Blockchain, the most popular type of Distributed Ledger Technology (DLT), turns out to be a promising technology for the next generation of mobile networks [5], [6] and for the creation of open and trustless business ecosystem [7]. Blockchain is a distributed, tamper-persistent and verifiable digital ledger sustained in a decentralized manner by a network of nodes connected in a Peer-to-Peer (P2P) fashion [8]. In this paper, we aim to explore how blockchain technology, in conjunction with smart contracts, can effectively realize P5GNs by overcoming related challenges.

The outline of the paper is as follows. Section II presents numerous existing challenges for P5GNs and how blockchain-based solutions can potentially resolve them. Section III discusses implementation challenges that could be encountered with using blockchain in P5GN and briefly lists possible solutions. Section IV concludes the paper.

This work was supported in part by the Academy of Finland under 6Genesis Flagship (Grant No. 318927) and 5GEAR (Grant No. 319669) projects.

II. Existing Challenges in P5GNs and mitigating role of Blockchain

This section elaborates on various technical challenges that obstruct the wide adaptation of P5GN. It also discusses how blockchain-based solutions can potentially mitigate them. The overview of the proposed blockchain-based solution and its applications is depicted in Fig. 1.

A. Spectrum Sharing

Spectrum being a limited resource must be utilized as efficiently as possible. Moreover, given the growing demands of industry verticals, the effective management of the spectrum becomes even more critical. As per [1], three different spectrum management opportunities have been identified for PG5Ns. First, the Mobile Network Operator (MNO)-centric approach, where MNOs deploy P5GNs by their licensed spectrum bands. Second, a collaboration-centric model where a P5GN operator leases spare spectrum from MNOs. Third, a local operator-centric mechanism where a P5GN operator gets the license directly from the regulatory body for local use. Two types of stakeholders in the collaboration-centric model are MNOs and P5GN, whereas in local operator model are regulatory bodies and P5GN operators. Hence, a centralized management party must monitor whether the collaborating parties function based on the negotiated terms and conditions. This arrangement will provide an overhead to each stakeholder, which compels subscribers to expend additional fees on the management entity.

Possible Blockchain-based Solutions: The blockchain is an up-and-coming solution for effective and on-demand sharing of the spectrum among the stakeholders by eliminating costly centralized authority. In addition to cost reduction, a blockchain-based coordination mechanism can

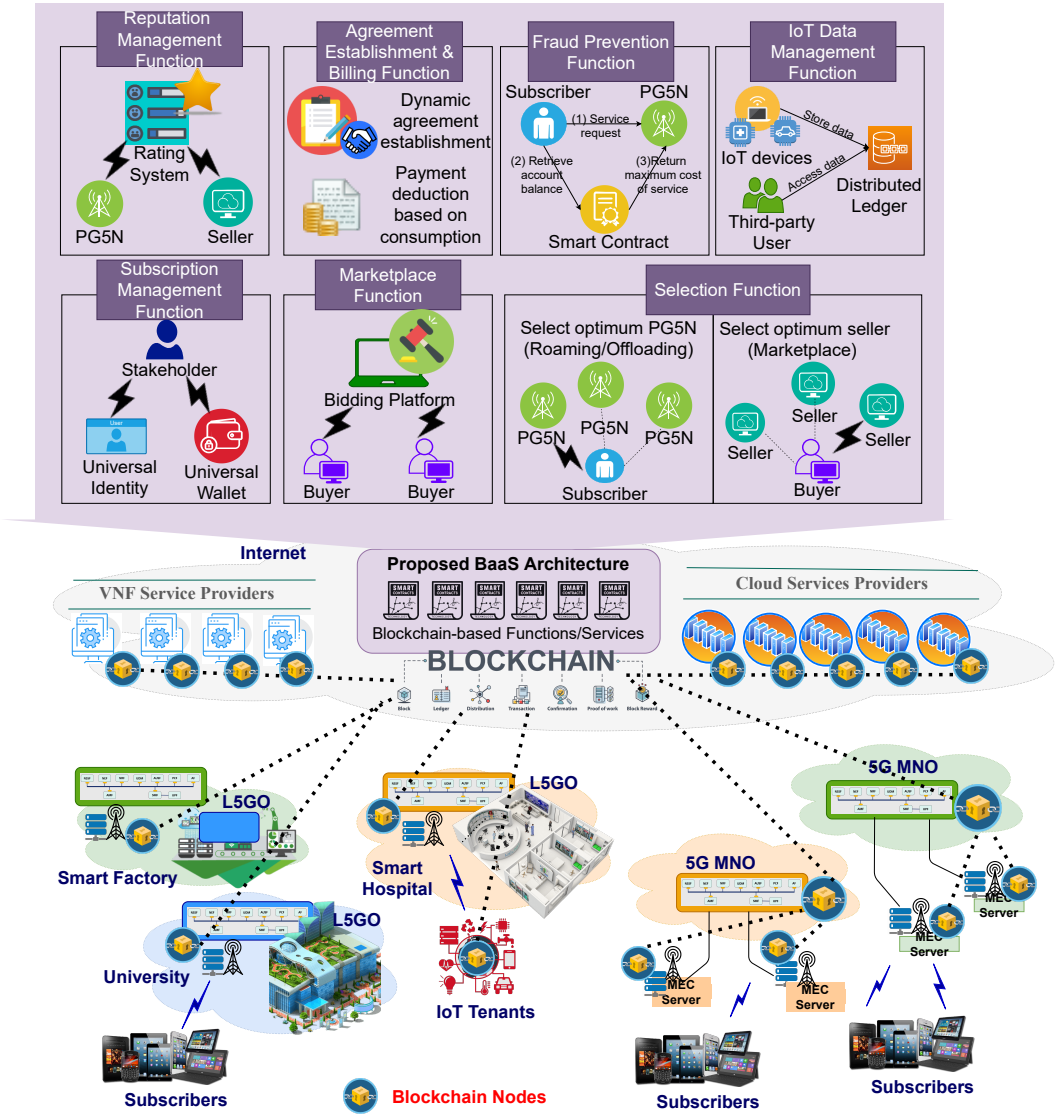

Fig. 1: Blockchain-enabled Services in P5GN Ecosystem

establish decentralized trust between the stakeholders. This is possible because of the transparency and immutability of the transaction data and the smart contracts on the blockchain. Also, using smart contracts can effectuate dynamic spectrum agreements in an agile manner. Moreover, blockchain can enable spectrum sharing in cognitive radio networks.

B. Roaming

Roaming in P5GN refers to the transfer of ongoing connection from the Home Mobile Network Operator (HMNO) to the Visitor Mobile Network Operator (VMNO), when a subscriber moves to a geographical location that HMNO does not cover. Usually, HMNO or home P5GN has pre-signed agreements with VMNO or visitor P5GN based on which services are provided. However, there are numerous issues with such kind of agreements like limited coverage by visitor network, variation in price packages by visitor network which may generate bill-shocks to customers [9], and variations in Qulaity of Service (QoS) since there is no transparency in the system. Further, the roaming frauds are estimated to cost over USD 38 billion every year to the telecommunication industry [2]. This is mainly due to the delay incurred while transferring Call Detail Records (CDR) from Visited Public Mobile Network (VPMN) to Home Public Mobile Network (HPMN). The cause of this delay is the existence of a Data Clearing House (DCH) as an intermediary.

Possible Blockchain-based Solutions: Blockchain's features like immutability, non-repudiation, and auditability, along with smart contract-based tight access control and transparent agreements, can pave the way to deal with roaming operations and related frauds [10]. Instead of pre-agreements, dynamic agreements via smart contracts can be issued. Such kind of dynamic and softwarized agreements allow agility and Service Level Agreement (SLA) compliance. Moreover, a blockchain-powered real-time monitoring mechanism can be designed to rate the performance experienced at any visitor network. Smart contract-based pre-selection of a network operator based on the input parameters (such as signal strength and dynamic reputation of the operators) can help overcome the issues such as poor service delivery and price discrepancies. Further, the roaming fraud can be dealt with by disintermediating the entities like DCH using blockchain.

C. Offloading

In the 5G ecosystem, offloading techniques are key in improving overall network performance. Offloading allows over-utilized MNOs or P5GNs to dynamically handover their subscribers to another available under-utilized network. With the commercialization of concepts like smart cities and autonomous vehicles, the popularity of P5GNs will increase, which may reduce the overall network performance and user experience [11]. Thus, offloading techniques turn out to be a profitable solution. Nonetheless, to effectively adopt offloading for MNOs and P5GNs, many challenges need to be addressed. For instance, manual selection will not be feasible with increased offloading instances and the number of network candidates. To overcome such challenges, a real-time performance rating system is required to effectuate the selection of the best P5GN to offload.

Possible Blockchain-based Solutions: Blockchain can offer a viable solution for all the challenges related to offloading. The use of a blockchain platform for common communication and negotiation can be instrumental in dynamic offloading. It can support network operators to select the next optimal P5GN to offload dynamically based on various factors such as available capacity, bandwidth, cost scheme, and reputation. The dynamic agreement can be established between the source network (MNO or P5GN) and the hired network (selected P5GN) via smart contracts.

D. Infrastructure Sharing

P5GN is mainly designed to cater to the massive and diverse requirements of users by deploying customized services locally. Depending on the current demands and available resources and the type of deployment scenario, P5GN needs to lease various types of deficit resources from resource providers. These providers can be network infrastructure providers, content providers, and/or facility owners [12]. To establish a successful collaboration between P5GNs and resource providers as well as to ensure that both the parties function as per the agreement, the trend is to have an intervention of trusted third parties [13]. However, this costs extra service fees and additional delay, which is a burden to both parties. Moreover, in case of a successful attack, these third parties can reveal all the private information of customers as well as business secrets [14].

Possible Blockchain-based Solutions: The use of blockchain technology provides trustless, transparent, and decentralized infrastructure sharing in P5GNs. In particular, it can remove the central authority and reduce the excessive charges imposed by intermediary parties. Moreover, the dynamic agreements between P5GNs and vendors can be established using smart contracts on top of the blockchain. Also, the implementation of a real-time and transparent monitoring system to ensure compliance with service level commitments can be effectively realized with the help of blockchain.

E. Fraud Prevention

Fraudulent activities are possible in any network ecosystem. Especially when the number of tenants increases, it gets increasingly challenging to design mechanisms that ensure complete fraud prevention. Moreover, implementing robust fraud prevention techniques may affect the anticipated performance of P5GN. For instance, Machine Learning (ML) based techniques deployed in centralized stations to identify the outlier tenants will affect the service delivery performance of the network. Furthermore, at times some of the frauds committed can be unaccountable and cannot be resolved due to the lack of trust. For instance, the consumer may not accept the centralized base station logs provided by MNOs. Besides, the centralized storage of logs is also a significant overhead in terms of computation and storage.

Possible Blockchain-based Solutions: Integration of blockchain and smart contracts in P5GNs can offer multifaceted benefits. From the user's perspective, their data can be stored using blockchain in a distributed fashion, thereby overcoming the issues associated with centralized storage. Smart contracts can be utilized to provide robust access control. Moreover, transparency and immutability of the code and the self-execution capabilities of blockchain-based smart contracts build trust between involved parties. From the network's perspective, blockchain can be used to track the activities of each party by logging them on the ledger. These logs can later be used to resolve any kind of dispute. Unlike the logs stored in a centralized system, these logs are transparent, immutable, and provide non-repudiation, thus helping in identifying and preventing fraud.

F. Subscription Management

The major challenge in subscription management within the PG5N ecosystem is identity or subscription theft. A malevolent node intentionally utilizes an authentic identity credential of a user to commit fraud within P5GN by getting access permission. Another challenge is that subscribers have to go through authentication procedures every time they move to another PG5N, which negatively affects the customer experience. Additionally, capabilities required to share securely user-subscription information between other operators are inadequate in currently available systems [3].

Possible Blockchain-based Solutions: Issues related to subscription management can be resolved by integrating blockchain in the P5GN ecosystem. User profile details can be secured against forgery using encryption techniques like hashing before storing it in the distributed ledger. Also, a mechanism for assigning a universally unique identity to each subscriber can be devised via blockchain. This will be vital to recognize each subscriber distinctly and globally.

G. Virtual Network Function (VNF) Management

The collaborative model of Network Functions Virtualization (NFV) and Multi-access Edge Computing (MEC) drives the 5G network services toward the edge layer. Although there are significant benefits, the migration and management procedures open up a few security challenges. Normally, most of the operators deploy the NFV ecosystem as per their business requirements. The malicious practices of the VNF expose the entire NFV ecosystem to various types of risk, for instance, damaging the generic VNF hardware. Moreover, issues like compatibility, secure migration, consumption, and payment settlements [15], [16] will be hard to resolve with the existing ecosystems. Further, there are no methods exist to assess the reputation of VNF providers.

Possible Blockchain-based Solutions: Blockchain and smart contracts have the required potential to overcome the aforementioned issues. Illegal utilization can be prevented by registering all the organizations connected to the NFV ecosystem in the distributed ledger and assigning a unique identity. Interoperability issues can be eradicated by establishing dynamic agreements between the P5GN and VNF vendors via smart contracts. Further, developing a blockchain-powered dynamic reputation system for VNF providers can enable P5GNs to select the optimal vendor as per the requirements. Additionally, blockchain can ensure secure transfer of payment from P5GN to third-party vendors based on P5GN's consumption and agreed pricing policies.

H. Internet of Things (IoT) Data Management

IoT ecosystems are anticipated to exponentially expand across different industrial contexts in the future. Security of IoT networks and related data is becoming difficult because of the limited resources (e.g., battery life, processing, and storage capability) and various levels of heterogeneity of IoT devices, on the one hand, and the high volume of (small) data generated, on the other hand. The use of the current centralized system to manage all the IoT nodes tends to exacerbate the issues like single-point-of-failure, service unavailability, ownership of data, illegal access, higher communication delay, and many more. However, it has been concluded by many recent studies that the use of blockchain, is one of the most disruptive technologies to ensure decentralized security [17].

Possible Blockchain-based Solutions: A blockchain makes highly secure peer-to-peer networks possible with the help of multiple nodes connected together. While acting as nodes in the blockchain network, IoT devices will be able to offload major process-intensive tasks to the blockchain. Thanks to the decentralized nature, blockchain-based data management solutions will be able to be connected with billions of nodes simultaneously.

Table I summarizes all the challenges and discusses, in a nutshell, the benefits of using blockchain-based solutions to mitigate each of them. Expected performance and applications of blockchain-based services for P5GNs are given in the table II.

III. Discussion on Implementation Challenges

Despite all the benefits that blockchain can bring in the realm of P5GNs, there are crucial bottlenecks that need to be improved. This section discusses the implementation challenges and proposes various techniques to tackle them.

A. Legal Issues

As of now, there is an absence of legal frameworks for blockchain-based systems. This makes blockchain technology a double-edged sword. On the one hand, the technology offers many promising features such as disintermediation, immutability, pseudonymity, and cryptographically sealed distributed ledger. On the other hand, it has various legal issues like the absence of a legally liable entity, non-availability of rules and regulations to deal with legal disputes and ownership of damages caused due to the malfunctioning of smart contracts. The most significant legal hurdle in the blockchain-based P5GNs arises when the personal data is accessed and stored at all the participating nodes that are outside the premises of a given P5GN to which a set of users are subscribed.

Possible Solutions: Early initiatives from government and regulatory bodies can resolve such legal issues and can give a boost to the use of blockchain for P5GNs. The establishment of legal frameworks by understanding the influence of blockchain in both commercial and customer segments of P5GN can help overcome the skepticism and easy onboarding of various stakeholders for blockchain-based P5GN.

B. Scalability - Latency and Throughput

Given the increasing popularity of P5GN, the use of state-of-art blockchain technology will pose significant scalability issues. This is because P5GN is expected to give rise to an enormous number of transactions to be handled because it is characterized by a large volume of IoT data, dynamic resource trading, on-the-fly offloading, and frequent roaming instances thus there will be. Blockchain technology, in general, has low throughput due to its inherent distributed nature, transaction validation process, block mining and block verification process, and network-level replication of information. Moreover, the throughput and the overall latency depend on the type of blockchain and the underlying platform being used. For example, public permissionless blockchains like Bitcoin and Ethereum can process around 4 to 15 transactions per second (tps), whereas, ripple can process about 1500 tps [33]. Additionally, lightweight nodes anticipated to operate within P5GNs will experience scalability issues due to the existence of operational overheads involving cryptographic functions.

Possible Solutions: The above challenges can be prevented by lowering the network load within the P5GN network. This can be achieved by offloading the users connected to one P5GN to another P5GN. In addition to that, few techniques are already available to scale up the performance of blockchain. One of them is the implementation of Lightning Network technology to accelerate the transaction speed. Another solution is to execute the Sharding model, where a shard is a subclass of the blockchain network, in which data is stored in multiple shards and they handle transactions parallelly. Moreover, Segwit and Pos are other concepts introduced to tackle scalability issues.

C. Security and Privacy

Though blockchain is known for its strong security features, nevertheless, it is not completely immune to attacks like 51% attack, selfish mining, and DoS/DDoS attacks. From P5GN's viewpoint, a compromised IoT node (or group of compromised nodes) under the control of an attacker can launch DoS (or DDoS) attack to slow down or make the services unavailable. Moreover, due to the distributed nature of blockchain, all the full nodes have a complete and exact replica of the ledger with them. Thus, the distributed nature of the ledger opens the door to privacy issues.

Possible Solutions: Numerous types of solutions are possible ranging from stronger encryption techniques like the homomorphic signature, Trusted Execution Environment (TEE) for secure smart contracts, and techniques like mixing, Attribute-Based Encryption (ABE), and Privacy

TABLE I: Potential challenges in P5GNs and blockchain-based solutions

Challenges	Brief Description	Benefit of Blockchain-based solutions
Spectrum Sharing [18], [19], [6]	Absence of transparency in the current spectrum sharing approaches due to its subjective involvements [20]	Validating the transparency of the spectrum marketplace publicly by the decentralized network of blockchain nodes
	Only static agreements can be established	Enforcement of dynamic agreements using smart contracts
	Breach of pre-established static agreements by network operators	
Roaming [21]	Generation of additional cost to the roaming subscribers, with the transfer of their billing records from VPMN to their respective HPMN, via DCH	Removal of third-party entities such as DCH by transferring its duties to the blockchain, which relaxes the cost burden of roaming customers
	Subscribers experiencing bill-shocks [9] with the change of package prices time-to-time. Further, the cause of roaming fraud when MNOs try to alter transaction logs	Assurance of transparency in every transaction record motivates the provider to act fairly. Enablement of fast dispute resolution by storing verified transactions in the distributed ledger
	Possibility for roaming subscribers to exploit the resources of VPMN, owing to the existence of CDR exchange delay from VPMN to HPMN [2]	Permitting VPMN to offer roaming service with reference to the available credits on the subscriber's wallet
	Because of the network congestion that could occur with the increasing demand of PG5Ns, the user experience of subscribers will be negatively affected	Enforcement of network load sharing techniques between P5GNs by executing a smart contract to find and offload the subscriber with the least connectivity to the optimal P5GN. Further, the selection of the optimal P5GN to offload can be enabled using smart contracts
	Stakeholders are paying unnecessary charges for the mediators to manage agreements between them	Replacement of intermediary organizations with the blockchain by allowing it to offer the services delivered by them.
Offloading [11]	Inconvenience in selecting a suitable P5GN to offload manually due to the increasing number of P5GNs	Execution of a dynamic selection system via smart contracts to find the next appropriate P5GN to offload
Infrastructure Sharing [22], [23]	Infrastructure providers tend to deliver second-rate services	Record and analyze the behavior of vendors by storing each of their performance information during every session in the ledger
Subscription Management [3]	Stealing subscription ID	Assignment of a unique identifier for every user and store it in the ledger. Whenever a subscriber connects to the network, P5GN can look up the database to authenticate the onboarded users
VNF Management [24]	Third-party VNF providers may not deliver services as they have agreed at the period of advertisement	Enforcement of penalty scheme via smart contracts if the vendors have not met the standards as they promised by analyzing the recorded performance information of vendors
	Possibility to vandalize the VNF by a malicious party during the VNF's migration process	Use of smart contracts to state the authorized callers who are responsible to call certain transactions, which can be realized by examining the transaction's digital signature
	Payment settlement process requires to track the usage of VNFs and to transfer the payment from network operator to VNF providers securely	Record of usage details and payment transfer via smart contracts
	Non-existence of a monitoring and reputation system to evaluate the performance of VNF providers	Execution of dynamic reputation system via smart contracts
IoT data Management [25], [26] [27]	Modifying transaction records stored in IoT devices	Enforcement of immutable decentralized transaction logs
	IoT nodes consist of limited storage capabilities	Utilization of distributed ledger for storage purposes
	IoT nodes lack processing competences to handle data sharing activities	Offloading processor-intensive tasks to blockchain
	IoT end-devices are vulnerable to Distributed Denial of Service (DDoS) attacks [28]	Prevention of DDoS attacks with the exploitation of cryptographic nature of blockchain, which guarantees the security of transactions

Enhancing Technologies (PETs) can be used for preserving privacy.

D. Synchronization Network Overheads

Continuous synchronization is required among the nodes in the blockchain. All nodes require to be consistent and should have a replica of the ledger. A newly mined (deem-to-be valid) block is disseminated in the P2P blockchain network and is eventually stored after verification. This broadcast type of traffic in blockchain leads to significant network overheads which tend to increase, with the increase in the number of nodes.

Possible Solutions: One of the possible solutions to reduce the synchronization network overheads is the customization of consensus algorithm towards data optimal synchronization. In addition, network overheads can be decreased by removing redundant data and restructuring the transaction data objects in a way to decrease their size.

IV. Conclusion

P5GNs are the latest trend that is going to flourish with the full-fledged deployment of 5G. It will allow easy entry to new entrants in the telecommunication market and has the potential to offer dedicated services to industry verticals. In this work, numerous challenges pertaining to the deployment of P5GNs are presented, and blockchain technology has been identified as the key enabler to mitigate these challenges. Nevertheless, there are challenges associated with the implementation of blockchain-based solutions in P5GN. Thus, the possible ways to overcome these implementation challenges are also discussed.

Acknowledgement

This work was supported in part by the Academy of Finland under 6Genesis Flagship (Grant No. 318927) project and by Science Foundation Ireland under CONNECT phase 2 (Grant no. 13/RC/2077_P2) project.

References

[1] M. Matinmikko-Blue, S. Yrjölä, V. Seppänen, P. Ahokangas, H. Hämmäinen, and M. Latva-aho, "Analysis of Spectrum Valuation Approaches: The Viewpoint of Local 5G Networks in Shared Spectrum Bands," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2018, pp. 1–9.

[2] G. Macia-Fernandez, P. Garcia-Teodoro, and J. Diaz-Verdejo, "Fraud in Roaming Scenarios: an Overview," *IEEE Wireless Communications*, vol. 16, no. 6, pp. 88–94, 2009.

[3] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 108–127, 2019.

[4] N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere, and M. Ylianttila, "A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 575–601, 2021.

[5] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, p. 102693, 2020.

[6] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based Secure Spectrum Trading for Unmanned-erial-vehicle-assisted Cellular Networks: An Operator's Perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2019.

TABLE II: Expected Performance for Blockchain-based Services in P5GNs

Blockchain based Service	Application	Expected Capacity	Expected Latency	Expected Scalability	Other Requirements
Auctioning [29]	Spectrum and infrastructure sharing	100 - 1000 Mbps	<10s	10-1000 transactions per day	Report generation from the ledger, and end-to-end data security
Network Selection [30]	Roaming	1 Mbps per session	<15ms per selection	> 1 million transactions per network	Lower data operation, and lower computational overhead
	Offloading: Selecting best network to offload	50 kbps per session	<15ms per selection	> 0.5 million transactions per region	Optimal offloading decision
Offload User Selection [11]	Offloading: Selecting optimum user to offload	20 kbps per selection	< 10 ms	> 10,000 transactions per day	Proper service authentication
Fraud Prevention [2]	Roaming Fraud	> 10 - 100 Mbps per request	< 5ms	10,000 transactions per region	Broad array of fraud rules, and upgrading capability dynamic fraud rules
Infrastructure Provider Selection [22], [31]	Infrastructure sharing	5 Mbps per selection	< 1min per transaction	> 50 - 100 transactions per ecosystem	Compatibility with existing infrastructure services
	VNF management	> 10 Mbps per operation	< 30s per transaction	>100 per factory	Adaptability to future NFV techniques
User Verification [32]	Authentication	50 kpbs	1ms per authentication request	>1 million transactions per network	Authentic service availability for higher transactions simultaneously, optimal data exchange, and replay attack prevention for the data in transit.
IoT [25]	IoT management	30 Gbps	<1ms	>1 billion transactions per region	Computationally optimal operations for the lightweight nodes, and extensibility towards massive future demands of the network nodes

[7] S. Yrjölä, "How could Blockchain transform 6G towards open ecosystemic business models?" in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2020, pp. 1–6.

[8] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[9] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and Efficiency in Roaming Services for Wireless Networks: Challenges, Approaches, and Prospects," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 142–150, 2013.

[10] N. Weerasinghe, T. Hewa, M. Dissanayake, M. Ylianttila, and M. Liyanage, "Blockchain-based roaming and offload service platform for local 5g operators," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2021, pp. 1–6.

[11] G. Liu and H. Zhao, "Power Allocation and Channel Selection in Small Cell Networks Based on Traffic-Offloading," in *2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS)*. IEEE, 2017, pp. 1–4.

[12] M. Matinmikko, M. Latva-Aho, P. Ahokangas, S. Yrjölä, and T. Koivumäki, "Micro Operators to Boost Local Service Delivery in 5G," *Wireless Personal Communications*, vol. 95, no. 1, pp. 69–82, 2017.

[13] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5g: opportunities and challenges," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.

[14] Y.-W. Chang, K.-P. Lin, and C.-Y. Shen, "Blockchain Technology for e-Marketplace," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2019, pp. 429–430.

[15] H. Jeon and B. Lee, "Network Service Chaining Challenges for VNF Outsourcing in Network Function Virtualization," in *2015 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2015, pp. 819–821.

[16] R. A. Mishra, A. Kalla, K. Shukla, A. Nag, and M. Liyanage, "B-vnf: Blockchain-enhanced architecture for vnf orchestration in mec-5g networks," in *2020 IEEE 3rd 5G World Forum (5GWF)*. IEEE, 2020, pp. 229–234.

[17] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: a Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," *IEEE Access*, vol. 8, pp. 23 022–23 040, 2020.

[18] S. Han and X. Zhu, "Blockchain based Spectrum Sharing Algorithm," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. IEEE, 2019, pp. 936–940.

[19] S. Yrjölä, "Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept," in *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer, 2017, pp. 128–139.

[20] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An Overview of Dynamic Spectrum Sharing: Ongoing Initiatives, Challenges, and a Roadmap for Future Research," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, 2016.

[21] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 142–150, 2013.

[22] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5g small cell networks," in *2018 14th International Conference on Network and Service Management (CNSM)*. IEEE, 2018, pp. 313–317.

[23] I. Badmus, M. Matinmikko-Blue, and J. S. Walia, "Network Slicing Management Technique for Local 5G micro-operator Deployments ," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2019, pp. 697–702.

[24] I. Sarrigiannis, K. Ramantas, E. Kartsakli, P.-V. Mekikis, A. Antonopoulos, and C. Verikoukis, "Online VNF Lifecycle Management in an MEC-enabled 5G IoT Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4183–4194, 2019.

[25] M. Ma, P. Wang, and C.-H. Chu, "Data Management for Internet of Things: Challenges, Approaches and Opportunities," in *2013 IEEE International conference on green computing and communications and IEEE Internet of Things and IEEE cyber, physical and social computing*. IEEE, 2013, pp. 1144–1151.

[26] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios," *Ieee Access*, vol. 8, pp. 23 022–23 040, 2020.

[27] N. Zou, S. Liang, and D. He, "Issues and Challenges of User and Data Interaction in Healthcare-related IoT," *Library Hi Tech*, 2020.

[28] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[29] H. Desai, M. Kantarcioglu, and L. Kagal, "A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 34–43.

[30] N. Nguyen, M. Arifuzzaman, and T. Sato, "A novel wlan roaming decision and selection scheme for mobile data offloading," *Journal of Electrical and Computer Engineering*, vol. 2015, 2015.

[31] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand Computing Resource Trading in IoV-assisted Smart City," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[32] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based Authentication for 5G Networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 189–194.

[33] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT express*, vol. 6, no. 2, pp. 93–97, 2020.