Emerging Directions for Blockchainized 6G

Anshuman Kalla, *MIEEE,* Chamitha de Alwis, *SMIEEE,* Sarada Prasad Gochhayat, *MIEEE,*
Gürkan Gür, *SMIEEE,* Madhusanka Liyanage, *SMIEEE,* Pawani Porambage, *MIEEE*

***Abstract*—The next generation of mobile networks, i.e., sixth-generation (6G), is expected by 2030, with already burgeoning research efforts towards this goal. Along with various other candidate technologies, blockchain is envisioned to enable and enhance numerous key functionalities of 6G. Thus, the main objective of this paper is threefold: 1) to categorize the different aspects of 6G into four emerging directions that anticipate significant advancements leveraging blockchain, 2) to discuss the potential role of blockchainized 6G under each key emerging direction, 3) to expound on the technical challenges in blockchaining 6G along with possible solutions.**

I. Introduction

The telecommunication ecosystem is going through a transformational period. On the one hand, people at large are starting to enjoy the advanced services offered by the ongoing deployment of 5G. On the other hand, the telecommunication community is engrossed in forging the vision and architecture for the next generation of mobile networks, i.e., 6G. The drive towards the 6G is shaped by the observed trends, use cases, technical requirements, and emerging new technologies [1], [2]. Some of the expected key highlights of the 6G are device and network energy efficiency, ubiquitous communication via deep-sea, space, body-area and nano-scale networking, and a new range of business applications for industry verticals to provide next-generation products and services. Numerous technologies have been identified to enable the growth of the 6G, such as THz frequency communication, Visible Light Communication (VLC), quantum networks, and Artificial Intelligence (AI)/Machine Learning (ML). Blockchain is among these technologies and envisioned to play a vital role in realizing future mobile networks [2], [3].

Blockchain, a type of Distributed Ledger Technology (DLT), is implemented as a decentralized Peer-to-Peer (P2P) network, which stores a digital ledger in a distributed and secure manner. The data structure used for building the distributed ledger is the *chain of blocks*. Every block holds a set of verified transactions, which are cryptographically sealed. As shown in figure 1, blockchains are characterized by the features such as immutability, decentralization, pseudonymity, provenance, non-repudiation, transparency, and availability [4]. *Smart contracts* extend the capabilities of the blockchain technology. They are executable codes that can softwarize all the terms and conditions of an agreement between various entities and are deployed on blockchain. Some of the advantages provided by smart contracts are automation, access control, trust-building, and elimination of third-party execution.

A. Evolution of Blockchainized Mobile Networks

Lately, the telecommunication community has witnessed significant research efforts concentrating on using blockchain, particularly for improving the 5G networks [4]. Most of these efforts are aiming to enhance the 5G technologies (e.g., network slicing, network function virtualization, edge, and cloud computing), 5G functionalities (like spectrum management, security, and privacy), and 5G applications (such as smart healthcare, smart city, and Industrial IoT). Such research efforts signifies the applicability of blockchain in the telecommunication landscape.

In the 6G era, it is envisioned that blockchains will be deployed and interconnected in a manner that they would span over different network domains (i.e., core, transport, edge, and access networks) and drive a complex 6G ecosystem providing a wide range of new and improved services and applications. Such an innate and pervasive integration of blockchains in the 6G ecosystem is conceptualized as *blockchainized 6G*. Since the vision of **blockchainized 6G** goes well beyond the 5G case, it is essential to explore what more the blockchain technology can bring to the 6G realm. For instance, blockchain

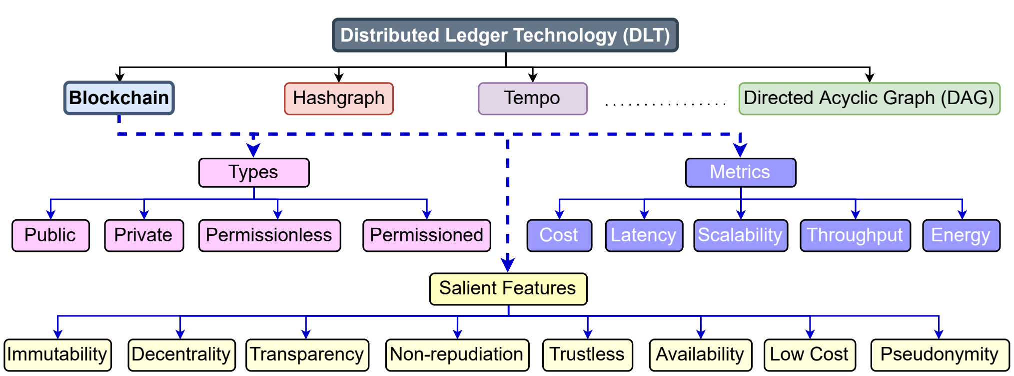

Fig. 1. DLT, Blockchain Technology, Types, Metrics and Salient Features

has immense potential to enable (or enhance) numerous *key 6G functionalities* such as automation of network management, dynamic spectrum management at THz communication, AI-powered edge computing, federated resource sharing in trustless environments, and security of ML and Federated Learning (FL) models. Furthermore, blockchainized 6G may support the realization of many new *6G applications* ranging from Connected Autonomous Vehicles (CAVs), Energy Internet (EI), Extended Reality (XR), UAV swarms, digital twin, and Industry 5.0 to Intelligent Internet of Medical Things (IIMoT) based smart healthcare.

B. Emerging Directions for 6G

In this paper we identify four emerging directions of 6G, which have a close alliance with the possible evolution of blockchainized 6G. Although, 6G is in the infancy stage, and its vision is yet to be formally and globally accepted, our categorization of the following emerging directions is an early attempt and is in accordance with the vision proposed by Hexa-X project [5].

1) **Trust-based Secure Networks (TSN)**: Enabling 6G to promise trust, security, and privacy for connected digital services.
2) **Harmonized Mobile Networks (HMN)**: Empowering 6G to emerge as a network of networks by aggregating resources such as communication, computing, sensing and intelligence at different scales, ranging from in-body environment to space.
3) **Hyper Intelligent Networks (HIN)**: Providing 6G with large-scale connected intelligence by ubiquitously integrating AI/ML in different segments of mobile networks.
4) **Resource Efficient Networks (REN)**: Realizing 6G as highly optimized communication infrastructure that largely reduces the global ICT environmental footprint.

These four directions intend to address the six challenges identified by Hexa-X project; TSN for trustworthiness, HMN for network of networks, HIN for connected intelligence and extreme experience, and REN for sustainability and global service coverage. The categorization is shown in Fig. 2, which also depicts how blockchainized 6G can help realize various 6G applications. Moreover, Table I shows the degree of association of the 6G applications with the emerging directions along with the expected performance, potential blockchain platforms, and consensus algorithms. Each category contains a list of technologies which are capable to extend the features of current 5G networks. Most of these technologies are yet to be practically implemented in future mobile networks. Specially, AI enabled hyper-intelligent networks is completely new category which is appreciable for beyond 5G network.

II. Trust-based Secure Networks (TBSNs)

The next generation of networks will thrive on having hyper-connectivity and extremely high reliability in an entirely automated manner. Thus, 6G networks are expected to emerge as distributed trust-based secure networks where security, privacy and trust are the key pillars to meet these requirements.

6G networks are foreseen to experience serious security and privacy threats due to its potentially broad ecosystem, the engagement by the governmental and other business entities, and the collection of (personal) data to train AI/ML models for pervasive intelligence. The more the data become accessible and collectible in the 6G era, the greater risk they may create on protecting user privacy and causing regulatory difficulties. Thus, in addition to ensuring the conventional security properties such as confidentiality, integrity, and authorization, it will also be challenging to overcome the novel threats that may occur due to AI/ML-based security attacks (e.g., evasion attacks, poisonous attacks, API-based attacks). Moreover, due to the expected massive number of connected devices and network tenants, the 6G ecosystem would tend to be highly prone to Distributed Denial of Service (DDoS) attacks. Such DDoS attacks are difficult to detect at an early stage because of the hidden colluding nature of the compromised network entities.

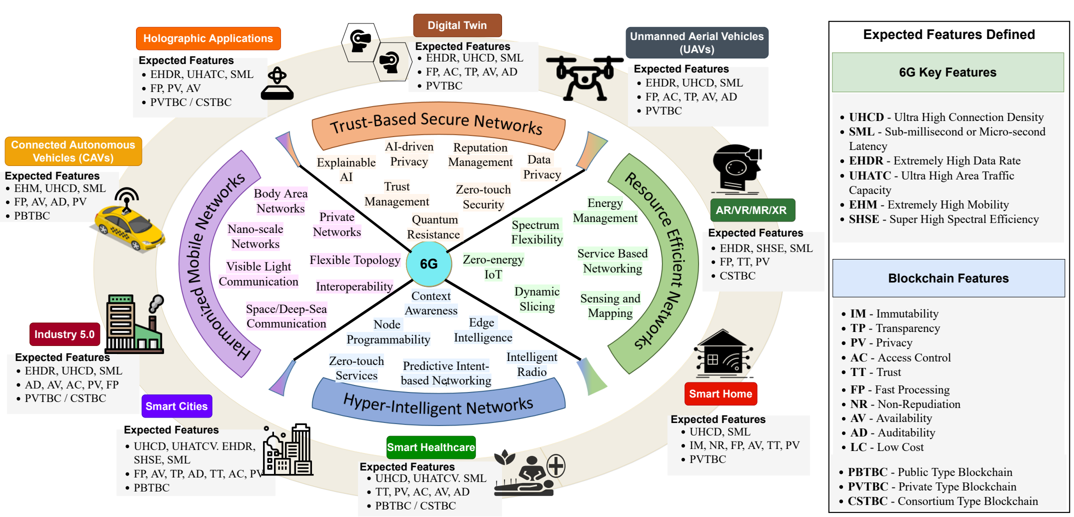

Fig. 2. Emerging directions for Blockchainized 6G ecosystem

TABLE I

MAPPING OF 6G APPLICATIONS TOWARDS THE FOUR KEY DIRECTIONS FOR BLOCKCHAINIZED 6G WITH EXPECTED REQUIREMENTS

Applications	Key Direction				Potential Technical Requirements			
	TBSN	HMN	HIN	REN	Consensus Algorithm	Throughput	Latency	Potential Platform
Industry 5.0	H	H	H	H	PoW, PoS, PoA, PBFT, Credit-based consensus	10^4 - $10^6$1 transactions per factory per day	Within seconds	Ethereum, Raiden, Plasma, Lighhning Network, Hyperledger
Smart Cities	H	H	H	H	PoS, PoW, DPoS	$> 10^6$ transactions per day	Within seconds	Ethereum, Hyperledger, Multichain, EOS.IO
Smart Healthcare	H	H	M	M	PoW, PoS, Proof-of-Interoperability, PBFT	10^3 - 10^6 transactions per minute per Hospital	Within seconds	Ethereum, Hyperledger (fabric, sawtooth, Iroha, composer, and Indy), Gcoin
Smart Home	H	L	L	M	PoS, PoA, PoW, PBFT, PoEG, PoEC	10 - 100 transactions per hour per home	Within seconds	Ethereum, Hyperledger
AR/VR/MR/XR	H	M	L	L	DPoS, DLS, BFT	10 - 100 transactions per hour per device	Less than 30 ms	Hyperledger, RevolutionVR, CryptoCarz, EOS, IOTA
UAVs	H	M	M	H	PoS, PoA, PoW, PBFT	30K- 60K transactions per minute per UAV	Within milliseconds	Ethereum, Hyperledger Fabric
Digital Twin	H	M	L	L	IBFT, Clique PoA, PoA, PoW	30K- 60K transactions per minute per digital twin	Within milliseconds	Ethereum, Hyperledger Besu
Holographic Applications	H	M	L	L	RAFT, DPoS, BFT	10 - 100 transactions per hour per device	Within milliseconds	Vibehub, Hyperledger
CAVs	H	H	H	M	PoS, PoW, DPoS	30K- 60K transactions per minute per Vehicle	Within milliseconds	Ethereum, Hyperledger, Parkchain

H - High Impact, **M** - Medium Impact, **L** - Low Impact

From the business model point-of-view, the 6G ecosystem and the associated value chain would include many players (e.g., cloud service providers, MNOs, third-party VNF providers), all working together to achieve common goals (e.g., trust-based resource sharing). Thus it will be crucial to maintain trust among these players.

Potential Use of Blockchainized 6G: Blockchainized 6G can play an instrumental role in the development of trust-based secure networks. Table II provides expected degree of requirement of various blockchain features for TBSNs.

- Privacy Compliance and Access Control: In the hyper-connected 6G era, it is imperative to protect privacy and implement robust access control mechanisms to allow users and stakeholders to access network network resources, critical services, (private) data, and computational or storage resources. Blockchainized 6G with its features such as pseudonymity, computationally secure cryptographic techniques, and smart contract based access control has the potential to realize a privacy-compliant ecosystem. Moreover, consortium or private permissioned blockchains turn out to be a promising option when privacy is of significant concern.

- Data Security: 6G will be likely to face the challenge for handling a massive small data due to the expansion of IoTs and connected verticals. Blockchain can offer scalable solutions to ensure the integrity, accountability, and privacy of these small data. The distributed nature of blockchains can support the realization of secure micro data centres in the 6G era to process these data efficiently. Blockchain, with its cryptographic primitives can be used to ensure a data-level security allowing data to be served from any location. Caching of data at intermediate network nodes can act as off-chain storage. The integrity of content received from any such off-chain storage can be verified by cross-checking the digital fingerprints available on blockchain.

- Trustless Trading: In 6G, trustless resource trading will be highly essential for economic, flexible, and optimized networks. It is achieved by establishing trust on the reputation of the networking entities and stakeholders participating in a given trade. Blockchain can be used as a tool for trust management in future networks. The immutability and transparency of the execution logic embedded in smart contracts have immense potential to inculcate trust in the 6G ecosystem.

- Federated Learning (FL): Due to the proliferation of increasingly powerful mobile devices, it is very likely that distributed AI, in particular FL, will surpass the traditional AI methods in 6G. As various actors from multiple networks are involved in FL, there arise various challenges such as trust in the locally trained model and secure collection and aggregation of FL model updates. Blockchain can enable trust in the quality and integrity of the produced FL model and automate the governing terms evaluation of the alliance during computations.

III. HARMONIZED MOBILE NETWORKS (HMNS)

6G plans aggregating multiple types of resources, including communication, storage, processing, and AI, which will be used to interconnect different type of networks such as nano-scale networks, body-area networks, local private networks, visible light networks, intra-machine networks, indoor networks, deep-sea networks, space networks and IoT networks [2]. Harmonization or unification of such heterogeneous networks of different types is essential to have a highly capable, intelligent, and efficient 6G ecosystem, which would act as a single network of networks. These harmonized 6G networks could enable E2E services for different nodes, handle mass-scale deployment, improve flexibility, fulfill vastly diversified requirements, and reduce operational costs.

Potential Use of Blockchainized 6G: Blockchainized 6G is envisaged to play a critical role in realizing HMNs.

- Integration of Local Private Networks: The introduction of network softwarization in 5G enabled the possibility of creating small-scale local private 5G networks. It is expected that millions of local private networks will be deployed in 6G era. Blockchain can act as a service layer in the 6G ecosystem comprising of local private network operators and enable different services such as automated spectrum sharing, service-level monitoring, reputation management, automated payment handling, resource optimization and security management.

- Federated Slice Brokering: To offer specialized E2E services spanning multiple networks, federated slicing is required. Blockchain-based decentralized brokering can enable the selection and procurement of resources from various operators in a multi-operator environment to create a federated slice. In addition, blockchain can automate the slice deployment, service quality assurance, and security management of federated slices.

- Efficient Roaming and Offloading: In a network of networks environment like 6G, users and tenants will frequently change the attached network by performing roaming and offloading instances to obtain better network conditions. In the traditional roaming services, a clearing house is used as a third party intermediary between MNOs. It handles exchange of all the roaming related information among home and visitor networks, and enables billing settlement. Use of such a centralized entity increases security and trust concerns in addition to the cost overheads [6]. Blockchain and smart contract based decentralized roaming services can be built by a consortium of mobile operators to eliminate the use of clearing house. Such service can offer secure exchange of roaming information, transparent billing, and dynamic agreement. In addition, blockchain can create a universal identity and wallet for roaming users, preventing the roaming frauds.

- Dynamic Agreements: Various Service Level Agreements (SLAs) and other agreements have to be established between networks to enable services such as roaming, offloading, federated slicing, and AI and security management. Since a very large number of different networks are envisioned with 6G, the existing static agreement model will not scale. Blockchain, together with smart contracts, can be used to establish dynamic agreements between different networks. Blockchain can eliminate the need for third-party entities for management, monitoring, and conflict resolution of such agreements. Added dynamicity in smart contracts allows establishing ad-hoc agreements with any networks, which helps users receive services from the best network based on both real-time and heuristic performance parameters.

- Eliminate Silos and Enable Model resiliency for better AI: As 6G would heavily rely on AI, it may require obtaining data from multiple entities, possibly from different networks. Blockchain can eliminate data silos by enabling trust between different networks. Smart contracts can be used to automate the data sharing between different networks and enforce strict access control.

IV. Hyper-Intelligent Networks (HINs)

In 6G, the concept of the hyper-intelligent networks envisions smart and autonomous networks, which intends to facilitate key operational functions such as self-configuration, self-monitoring, self-healing, and self-optimization with minimal human effort and intervention [7]. Furthermore, the digital services and applications will be hyper-flexible, customizable, and adaptive in a self-driven manner to provide the best user experience in a ubiquitous manner. The main difference in 6G from current efforts, e.g., for 5G networks, is that such cognitive networks would rely on AI/ML as a foundational element from the design phase, not a later improvement, and for all the network aspects, not just limited to some specific functions. Although intelligence is a transversal concept envisaged for different aspects in current networks (and future networks), the infusion and adoption of innate intelligence at different layers is expected to form a hyper-intelligent environment at a very large scale in 6G networks, i.e., the hyper-intelligent networks. From a practical point of view, the first step towards hyper-intelligent networks is ETSI ZSM architecture entailing closed-loop operation and AI/ML techniques with pervasive automation of network management operations [8]. Further, FL will be widely used across the network as a mechanism for distributed AI.

Potential Use of Blockchainized 6G: Blockchain can provide following vital functions to address the challenges related to the pervasive use of AI/ML in the large-scale 6G ecosystem.

- Context-awareness and Autonomicity Hyper-intelligent 6G networks have to be context-aware for network management as well as providing smart digital services. This is possible with ultra-scale sensing functions (discussed next), which will support such context-aware operation. Additionally, they need to be self-driven and autonomic to be able to meet performance KPIs. Blockchain will provide trusted execution with smart contracts to process available data for context deduction and data sharing in a trustworthy, immutable and transparent manner for context-awareness and, consequently, autonomic operation driven by AI/ML.

- Ultra-scale Sensing Integration of advanced sensor technologies with mobile networks accompanied by low-energy communication capabilities will lead to pervasive intelligent sensing and localized services. For enabling these operations, blockchain will serve as a decentralized and trustworthy data stratum (data collection, data storage, and processing) for ultra-scale sensing and big data analytics in 6G.

- Control of Massive-scale Intelligent Surfaces The use of programmable intelligent surfaces to cover man-made structures (e.g., buildings, roads, indoor walls) allows intelligent control of the transmission environment in wireless systems [9]. Such intelligent surfaces are considered to play a vital role for 6G radio environments when the signal quality degrades. In a blockchainized 6G network, blockchain provides the key capability of facilitating federated control among disparate intelligent surfaces. Moreover, intelligent surface control functions from different administrative domains (e.g., different network operators) can exchange synchronization and reconfiguration information in a trustworthy manner, thanks to blockchainized 6G.

V. Resource Efficient Networks (RENs)

Another exciting direction where 6G networks are considered to make significant advancements is the ultra-efficient utilization of different types of resources. Three basic types of resources are network resources (e.g., radio spectrum,

TABLE II

PROMINENCE AND LIMITATIONS OF BLOCKCHAIN TOWARDS FOUR KEY DIRECTIONS OF BLOCKCHAINIZED 6G [10], [11]

Key Direction	Key Blockchain Features								Prominence of Blockchain	Limitations of Blockchain
	Immutability	Transparency	Privacy	Automation	Trust	Non-Repudiation	Availability	Auditability		
TBSN	H	H	H	M	H	H	M	H	These key features make blockchain a prominent technology towards TBSN compared to complementary solutions based on quantum computing, physical layer security, and distributable and scalable AI/ML.	Blockchain-related security and privacy issues (e.g., 51% attacks, double spending attacks, reentrency attacks, and Sybil attacks), interoperability issues, and decentralization requirements.
HMN	M	M	L	H	H	L	H	M	Blockchain can facilitate HMN in supporting cross-layer technologies, network programmability, AI-powered automation, multi-tenant networks, and cell-free communication.	Blockchain scalability, privacy issues, longer consensus time, and lower degree of decentrality with less active nodes.
HIN	L	M	H	H	M	L	H	M	Blockchain and smart contracts provide privacy, automation, fast processing, and high availability to facilitate FL, edge AI, and ZSM towards HIN.	Scalability limitations for network-wide automation, longer consensus time, and interoperability issues for smooth ZSM.
REN	M	M	M	H	M	L	H	M	Blockchain and smart contracts based platform can eliminate third parties and support dynamic spectrum access, energy transfer and harvesting for RENs.	Computational and communication overheads, high storage demands, DDoS attacks, and interoperability are the limitations for RENs.

H - High Impact, **M** - Medium Impact, **L** - Low Impact

hardware infrastructure, Physical Network Functions (PNFs), and Virtual Network Functions (VNFs)), computing resources (e.g., edge computing, core computing, and cloud computing), and storage resources (e.g., in-network caching, edge data centres, core storage, and cloud storage). In general, RENs call for secure and dynamic virtualization of physical resources, agile yet optimized scheduling and allocation of available resources, and AI-based proactive management of overall resources. In particular, efficient spectrum (sensing, sharing, and) management, on-demand network infrastructure sharing, and optimized ultra-dense heterogeneous (logical) networks are considered important steps towards resource-efficient 6G networks.

Potential Use of Blockchainized 6G: Blockchainized 6G can pave the way for the emergence of RENs.

- Dynamic Network Slicing: The paradigm permits a network operator to create and support dedicated virtual networks. Such networks are customized to the specific needs of diverse users and multiple tenants (e.g., industry verticals, and local operators). Blockchain has already been identified as an enabler to build decentralized network slice brokering service. Blockchain-based slice broker can securely coordinate with the network tenants, on the one hand, and slice managers of network operators, on the other hand. Moreover, based on the dynamic demands, virtualized resources can be either added or removed from an existing slice, and the corresponding logs are immutably recorded on the blockchain.

- Spectrum and Interference Management: Efficient management of the 6G spectra is essential in light of issues such as high cost of administration for centralized spectrum management, high interference with decreasing cell size and increasing mobility handovers, and the rapid emergence of local private networks. Hence advance spectrum-sharing and management techniques are required to mitigate these issues. The use of blockchain can improve spectrum efficiency by recording real-time spectrum utilization, dynamically allocating spectrum bands based on devices' dynamic demands, and enabling incentive mechanisms for spectrum sharing between devices. Interestingly, information like spectrum sensing, spectrum auction results, spectrum lease mappings, and idle spectrum availability, can be stored on blockchain to harness maximum spectrum utilization. Furthermore, blockchain-based tokenization model for management of spectrum has been shown to be economical in terms of operations as well as light in terms of overheads [3].

- Data Storage: Extremely high data traffic in 6G era would demand network-wide data caching or caching at network edges. Thus, mechanisms are required to incentive nodes for the storage services they provide. Blockchain with smart contracts turns out to be a promising candidate to give life to such automated incentive mechanisms that are transparent, trustless and dispute-free.

VI. TECHNICAL CHALLENGES AND POSSIBLE SOLUTIONS

This section discusses the technical challenges along with possible solutions for building blockchainized 6G networks. Table III shows the importance of these technical challenges for the four key directions.

1) Scalability (Throughput and Storage) and Energy Overhead: 6G is envisioned to operate at Tbps, provide extremely high connection density and tailored services to numerous network tenants. Accordingly, as the number of participating stakeholders and the rate of accessing a blockchainized 6G increase, the scalability issues, both in terms of throughput and storage, will become a significant concern. Especially, low throughput turns out to be a bottleneck for latency-sensitive applications such as UAVs, CAVs, smart healthcare (remote surgery) and DTs. Another challenge is the large energy consumption due to the high computation involved in block mining. Blockchains that require large energy to operate (for e.g., public permissionless) may impair the performance of resource-constraint applications such as wearable devices and massive sensor networks.

Possible Solutions: Throughput depends on various factors such as hardware capacity, network latency, size of distributed ledger, size of the blockchain P2P network, the consensus protocol employed, and complexity of both the cryptographic techniques and the smart contracts used. Thus, different kinds of solutions are applicable, for instance, sharding and DAG. Solutions to deal with storage scalability are off-chain storage, sidechain, data compression, and hierarchical blockchain. To resolve the high energy consumption challenge, less computational intensive consensus algorithms and private permissioned or consortium type of blockchains can be used.

2) Security and Privacy: In general, blockchainized systems are equipped with strong security and privacy measures. Nevertheless, such systems are still prone to blockchain-based attacks (e.g., 51% majority attack and DDoS attack) and smart contract based attacks (e.g., Parity Multi-Sig wallet attack and Integer underflow). Thus, blockchainized 6G needs careful considerations in terms of security and privacy aspects.

Possible Solutions: Use of blockchain-based common communication channel may enable the identification of network users by pseudo names instead of direct personal identities. In order to assure the liability of each party in a Blockchainized 6G, smart contracts can be used to define Trust Level Agreements (TLAs) and Security Service Level Agreements (SSLAs). Moreover, privacy protection of sensitive information can be achieved by customizing the structure of block header.

3) Consensus Algorithm: A variety of consensus algorithms exists in blockchains, however, most of the consensus algorithms are not suitable for the mobile networks and the associated services. For instance, PoW like algorithms will be computationally intensive, incur large synchronization overheads, and is costly as it needs a huge source of energy that gets wasted if a node fails to mine a new block. Moreover, most of the existing contemporary cryptographic mechanisms used in consensus algorithms (e.g., PoW currently utilizes hash schemes like SHA256 or KECCAK256) will also become vulnerable to the attacks in the post-quantum era.

Possible Solutions: A quantum-safe consensus algorithm can be designed by focusing on randomness rather than computational difficulty [12]. 6G networks consist of various random data sources such as channel information, traffic patterns, and noise level, which can potentially be used to design consensus algorithms. Moreover, it is possible to design 6G specific consensus algorithms where miners have to focus on useful tasks such as spectrum sensing, abnormality detection, and traffic pattern analysis rather than meaningless hash value calculations [13].

4) Interoperability: The present blockchain landscape is heavily scattered with multiple platforms that are incompatible with each other. Therefore, several issues may arise when establishing interoperability among multiple blockchain platforms in 6G networks. For instance, performing functions such as sending tokens, executing smart contracts, and guaranteeing the validity of stored data among multiple blockchain platforms is not possible at present [11].

Possible Solutions: Several solutions are being investigated to resolve the interoperability issues in blockchains. For instance, inter-blockchain communication protocols are also being developed to facilitate cross-blockchain smart contract interactions. Furthermore, by the use of blockchain gates, interoperability issues across blockchain systems can be solved by defining parameters including perimeters for blockchain autonomous systems, interdomain transactions, and interdomain trust establishment [11].

TABLE III
IMPORTANCE OF TECHNICAL CHALLENGES FOR FOUR KEY DIRECTIONS

Challenge	Key Direction				Remarks
	TBSN	HMN	HIN	REN	
Scalability (Throughput and Storage)	M	H	H	H	As per the Ethereum organization, sharding and layer-2 solutions have the potential to enhance scalability by handling transactions off the main Ethereum chain.
Security and Privacy	H	H	M	L	ETSI provides a layered model for Permissioned Distributed Ledgers (PDL) to assess security, safety and privacy of blockchain platforms [14].
Consensus Algorithm	M	H	H	M	ETSI specifies 'double-safety' mechanism for PDL due to consensus mechanism and the mutual responsibility of the permitted validating nodes [14].
Inter-operability	H	H	H	H	ETSI is in the process of developing interoperability guidelines for PDLs [14].
Measure of Decentrality	H	H	M	M	Ethereum 2.0 upgrade will use staking to make the platform more decentralized.

5) Measure of Decentrality: Blockchain provides decentralized means of trust among untrusted users by withstanding a large number of fake identities in a P2P network-based system and prohibiting them from gaining higher influence. Basically, decentralization refers to the system property which assures that user(s) cannot control a system's assets or enforce changes without accompanying consent from other users. Hence, measurement of decentrality requires appropriate metrics in different layers. Particularly, metrics such as Gini coefficient, entropy, Euclidean distance, and Minkowski distance are used to measure decentrality in the governance layer. Similarly, degree centrality, closeness centrality and betweenness centrality metrics are used to measure decentrality in the network layer. For security in 6G, this property needs to be maintained for any blockchain-based solution.

Possible Solutions: In [15], an entropy method from information theory is proposed to quantify the decentralization of blockchains. Using this technique, the discrete degrees of mined blocks and address balances are calculated to measure the decentralization degree for Bitcoin and Ethereum systems. In blockchainized 6G, such a decentrality measurement and monitoring system should be a part of the general security architecture to ensure the proper operation of network functions.

VII. CONCLUSION

This paper discusses how blockchainized 6G acts as an enabler of four emerging directions of 6G, namely, TBSN, HMN, HIN, and REN. In line with the vision of 6G, these four directions include many new technologies which are yet to be implemented in future 6G networks. Furthermore, HIN powered by AI/ML is a completely new category that will see developments far beyond 5G since 6G is AI-native by design. The paper also highlights some of the key technical challenges and possible solutions for blockchainized 6G towards realizing 6G networks.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

[2] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147 029–147 044, 2020.

[3] T. Maksymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.

[4] 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.

[5] M. A. Uusitalo, M. Ericson, B. Richerzhagen *et al.*, "Hexa-X The European 6G flagship project," in *2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2021, pp. 580–585.

[6] B. Mafakheri, A. Heider-Aviet, R. Riggio, and L. Goratti, "Smart contracts in the 5g roaming architecture: the fusion of blockchain with 5g networks," *IEEE Communications Magazine*, vol. 59, no. 3, pp. 77–83, 2021.

[7] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities," *Computer Networks*, vol. 183, p. 107556, 2020.

[8] ETSI, *ETSI Zero-touch Network and Service Management (ZSM): Reference Architecture*, ETSI Std., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/007/01.01.01_60/gs_zsm007v010101p.pdf

[9] M. Di Renzo, A. Zappone, M. Debbah, M. S. Alouini, C. Yuen, J. de Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[10] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet of Things Journal*, 2020.

[11] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in *International Conference on Business Process Management*. Springer, 2019, pp. 3–10.

[12] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[13] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[14] ETSI, "Permissioned distributed ledgers (PDL)," Available at https://www.etsi.org/technologies/permissioned-distributed-ledgers, accessed on 26.09.2021.

[15] K. Wu, B. Peng, H. Xie, and Z. Huang, "An information entropy method to quantify the degrees of decentralization for blockchain systems," in *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, July 2019, pp. 1–6.

Anshuman Kalla is Postdoctoral Visiting Researcher at the Centre for Wireless Communications (CWC), University of Oulu, Finland. Email: anshuman.kalla@ieee.org and anshuman.kalla@oulu.fi

Chamitha de Alwis is Senior Lecturer in the Department of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Sri Lanka. Email: chamitha@sjp.ac.lk

Sarada Prasad Gochhayat is a PostDoc fellow and an adjunct faculty at Old Dominion University, Norfolk, USA. Email: sgochhay@odu.edu

Gürkan Gür is a senior lecturer at Zurich University of Applied Sciences (ZHAW), Switzerland. Email: gueu@zhaw.ch

Madhusanka Liyanage (S07, M16, SM20) is working as Assistant Professor at School of Computer Science, University College Dublin, Ireland. Email: adhusanka@ucd.ie

Pawani Porambage is a Postdoctoral Researcher at the Centre for Wireless Communications, University of Oulu, Finland. Email: pawani.porambage@oulu.fi