# The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions

Tharaka Hewa*, Gürkan Gür†, Anshuman Kalla‡, Mika Ylianttila§, An Braeken¶, Madhusanka Liyanage‖
*§‖Centre for Wireless Communications, University of Oulu, Finland
†Zurich University of Applied Sciences, Winterthur, Switzerland
‡School of Computing and Information Technology, Manipal University Jaipur, India
¶Vrije Universiteit Brussel, Anderlecht, Belgium
‖School of Computer Science, University College Dublin, Dublin, Ireland
Email: *§‖[firstname.lastname]@oulu.fi, †gueu@zhaw.ch, ‡anshuman.kalla@jaipur.manipal.edu,
¶an.braeken@vub.be, ‖madhusanka@ucd.ie

***Abstract*—The world is going through a fundamental transformation with the emergence of the intelligent information era. The key domains linked with human life such as healthcare, transport, entertainment, and smart cities are expected to elevate the quality of service with high-end user experience. Therefore, the telecommunication infrastructure has to meet unprecedented service level requirements such as ultra high data rates and traffic volume for the prominent future applications such as Virtual Reality (VR), holographic communications, and massive Machine Type Communications (mMTC). There are significant challenges identifiable in the communication context to match the envisaged demand surge. The blockchain and distributed ledger technology is one of the most disruptive technology enablers to address most of the current limitations and facilitate the functional standards of 6G. In this work, we explore the role of blockchain to address formidable challenges in 6G, future application opportunities and potential research directions.**

***Index Terms*—6G Networks, Blockchain, Distributed Ledger Technology, massive Machine Type Communications (mMTC), Industrial Internet**

## I. Introduction

6G mobile networks are envisioned to nurture the future of ubiquitously connected data-intensive intelligent society [1] powered with complete automation by seamless integration of all sorts of wireless networks spread over ground, underwater, air and space [2]. Moreover, 6G is also envisaged to keep up with the explosive growth in mobile traffic which is estimated to be 607 Exabyte/month by 2025 and 5016 Exabyte/month by 2030 [3] for the emerging applications such as [4]–[7].

By and large, the next generation of mobile networks are expected to be innately softwarized, virtualized and cloudified systems [1], [8] with the motive *to interconnect* seamlessly a staggering number of heterogeneous devices including massive IoT/IoE devices, *to cater* anticipated explosive growth in data traffic at ultra-high data rates along with ultra-low latency [2], *to create* incredible range of new vertical network services [9], [8], and *to support* the development of brand-new set of real-time [2] and data-intensive [7] applications.

Undoubtedly, softwarization, virtualization and cloudification of next generation mobile networks lead to enormous advantages like micro operator based business models [10], agile and efficient management and network orchestration (MANO), on-the-fly creation of vertical services, differentiated services with network slicing [11], etc. However, they tend to exacerbate the issues like network reliability, security vulnerability, data privacy and immutability [12], soft spectrum sharing, multiple access control, authentic Virtual Network Functions (VNFs) [13], legitimate resource utilization, and differential security for differentiated services offered by different virtual networks [11].

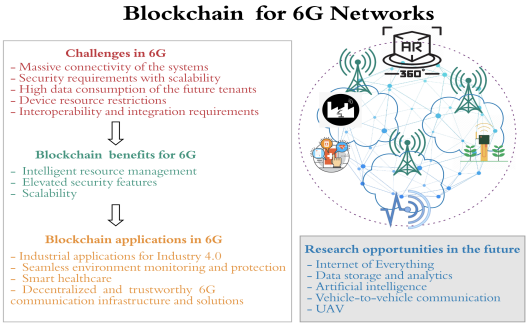


Fig. 1. The role of blockchain in 6G networks.

Lately, blockchain technology and in general distributed ledger technology have gained momentum and have been embraced by the industry and research communities across the globe. Some of the offerings of blockchain technology are: *(i)* decentralization by eliminating the need of central trusted third parties and intermediaries, *(ii)* transparency with anonymity, *(iii)* provenance and non-repudiation of the transactions made, *(iv)* immutability and tamper-proofing of the distributed ledger's content, *(v)* elimination of single point-of-failure (improving resiliency and resistance to attacks like DDoS), *(vi)* comparatively less processing delay as well as processing fee. Thus blockchain is regarded as an indispensable technology to establish trust in future networks.

Since blockchain has been envisioned as one of the key enabling technologies for 6G mobile networks [1], [2], [8], it is imperative to explore various benefits, opportunities and challenges foreseen with its exploitation. Fig. 1 depicts the role of blockchain in the 6G networks while the following

sections elaborate on identified aspects of that integration.

## II. General Challenges in 6G

Some of the perceptible challenges in 6G are expounded by Behnaam et al. in [1]. Moreover, challenges pertinent to M2M communications are presented by Biral et al. [14].

### A. Massive connectivity in future systems

*1) Scalability:* The industrial IoT enthusiasts predict that billions of devices will be connected and operated in the future industrial ecosystems with the emergence of concepts such as massive Machine Type Communications (mMTC). Thus it would be challenging to tailor the design of 6G systems for such an unprecedented traffic demand.

*2) Real-time communication with minimal latency:* The real-time communication is a crucial requirement in future computing ecosystems. The device-to-device and machine-to-machine communications require a robust accuracy with near zero delays for precise operation. The use cases such as autonomous driving and AR assisted healthcare systems may require a consistent minimal delay communication enabled in large-scale data exchange.

*3) Higher throughput:* The mission critical systems which utilize the future 5G and beyond communication ecosystems require concurrent connectivity of billions of devices. The network infrastructure such as base stations should handle the enormous volume of transactions in real time.

*4) Synchronization:* The synchronization is a significant requirement in time critical industrial applications. The mission critical backbone systems of a country, including power distribution systems and vehicular networks must synchronize in real time for accurate operation.

### B. Security requirements in future computing ecosystems

*1) Confidentiality:* The future computing infrastructure such as IoT exposes immense threat surfaces with wireless connectivity. The encryption techniques such as symmetric key encryption algorithms require to be lightweight for the low power IoT devices. However, the lightweight cryptographic techniques may expose the data into privacy risks due to computational restrictions [15].

*2) Integrity:* The massive volume of data produced by the future systems require the data to be accessed and modified by the authorized users when the data in transit. The eavesdropping and modification of data in transit will deviate the system functionality from the expected behavior.

*3) Availability:* The service availability is a principal requirement in future networks. Especially, the sophistication of 5G ecosystems with a large volume of interconnected devices expands the risk of DDoS attacks. The speciality of the current network security tools cannot directly apply into the 5G and beyond networks to detect threats and breach attempts [16].

*4) Authentication and access control:* The data, either in transit or store requires to secure with the access control mechanisms in order to prevent unauthorized manipulations. The conventional centralized authentication and access control mechanisms will restrain in terms of scalability in the massive futuristic demands anticipated in 6G.The sophisticated access control requirements to match the diversification of future tenants in the 6G ecosystem will be resource-intensive and cause bottlenecks in the associated services.

*5) Audit:* An audit is required to evaluate the compliance of the behavior of the tenants in the network ecosystem. For the elevated security standards, deep packet level audit may require to identify and flag the behavior of those tenants. The auditing of a massive number of tenants will be challenging from the perspective of enforcing security.

### C. Higher data consumption in sophisticated solutions

The higher data rate is one of the most significant expectation in the future network ecosystems. The applications such as VR, holographic communications, 16K video and 3D ultra video require a higher data rate and data consumption.

### D. Device resource restrictions

The computational and storage restrictions are anticipated to limit the capabilities of cryptographic algorithms and eventually lead to deviation from the standard mechanisms. The standard adoption of the security is harder with such device resource constraints.

## III. What Blockchain Can Bring to 6G

The blockchain is one of the most prominent technologies to unleash the potential of 6G systems. The capabilities and strengths of the blockchain technology to eliminate the potential challenges discussed in Section II are explored in this section.

### A. Intelligent resource management

The network resource management is challenging in the envisaged massive connectivity demands in the future telecommunication ecosystems. The resource management operations such as spectrum sharing, orchestration and decentralized computation requires to be compatible with massively-large infrastructure. Zhang et al. [17] presented an edge intelligence and IIoT framework with secured and flexible service management in Beyond 5G. Maksymyuk et al. [18] proposed an intelligent network architecture which utilizes blockchain technology by handling the relationship between operators and users applying smart contracts. The authors developed an unlicensed spectrum sharing algorithm based on game theory. Dai et al. [19] presented the application of blockchain and deep reinforcement learning for efficient resource management services including spectrum sharing and energy management. Mafakheri1 et al. [20] applied blockchain for resource sharing and demonstrated the utilization of smart contracts to provide self-organizing network features.

### B. Elevated security features

*1) Privacy:* The privacy is a significant consideration in the perspective of security. Application of data privacy is diverse in the complex security requirements in the future 6G network ecosystem. In that regard, Fan et al. [21] proposed a privacy preservation scheme based on blockchain for content-centric 5G networks.

*2) Authentication and access control:* The access control of centralized systems suffer scalability limitations. Therefore, access control with centralization is a significant challenge in the design of future networks. Yang et al. [22] presented blockchain based authentication and access control mechanisms for cloud radio over fiber network in 5G.

*3) Integrity:* The data integrity of massive data volume generated in the future computing ecosystems is a principal concern. Adat et al. [23] presented a blockchain based solution to prevent pollution attacks which violate the integrity of data. Ortega et al. [24] proposed a blockchain based framework to ensure the integrity of information exchanged over the network.

*4) Availability:* The service availability is a significant requirement in the future communication ecosystems. Especially, with the broader threat surface and massive connectivity in the 5G ecosystem, the risk for DDoS attacks is comparably higher. Rodrigues et al. [25] presented a DDoS prevention mechanism with the support of blockchain. Sharma et al. [26] proposed the applicability of blockchain and SDN for the enforcement of significant security services including DDoS attack prevention, data protection, and access control.

*5) Accountability:* The accountability of the 5G and beyond network ecosystem is a key requirement. The security, surveillance, and governance of the network can be implemented through the blockchain and distributed ledger technology in general. The distributed ledger remains as an immutable and transparent log for each event which can be utilized in the auditing of events.

### C. Scalability

The scalability is a major requirement in 5G and beyond systems. The scalability limitations of centralized systems can be eradicated by the blockchain and smart contracts to face the envisaged massive connectivity demand in future. The decentralized nature and the integration convenience of edge and fog computing nodes will improve the service strengths in those networks.

## IV. Application and Service Opportunities via Blockchains in 6G Systems

As listed in Section I, 6G vision entails a multitude of applications which can be enabled or improved via utilization of blockchains. The premise of blockchains for providing/improving such applications in 6G stem from the capabilities listed in Section III which are enabled by its core attributes, i.e., decentralization, transparency, immutability, availability and security.

### A. Industrial Applications for Beyond Industry 4.0

In 6G, the industrial applications will be important drivers for exploiting the envisaged 6G capabilities. The key attributes of blockchains and the challenges discussed in Section II are especially applicable to industrial environments. For example, holographic communications for industrial use-cases such as remote maintenance or massive connectivity of industrial manufacturing equipment requires decentralized architectures which are trustworthy at the same time [9]. Blockchains can provide these capabilities when they are integrated into these applications or use-cases. However, there are also important research challenges regarding blockchain-based solutions, namely latency and scalability. They are formidable due to stringent performance requirements in industrial applications and valid for industrial networks and IoT [8].

### B. Seamless Environmental Monitoring and Protection

Blockchains allow decentralized cooperative environmental sensing applications which can be realized in global scale with 6G. Such capabilities can serve use-cases such as smart cities or transportation as well as environmental protection for green economy. Blockchains also facilitate secure data sharing among parties (ranging from IoT devices to organizations). Such massive scale trusted sensing and data sharing solutions enabled by blockchains are crucial for environmental monitoring [2]. Moreover, federated and shared learning implemented via blockchains support the data analytics and inference processes for environmental protection in a decentralized manner.

### C. Smart Healthcare

Smart healthcare in 6G will need to take one step further to solve incumbent issues in 5G networks. The deeper and ubiquitous integration of blockchains in future networks can advance current healthcare systems and improve performance in terms of better decentralization, security, and privacy. The forthcoming among these technical challenges is the privacy issue. Moreover, integrity of healthcare data is possible due to the immutability capability provided by blockchains. Specifically, user controlled privacy and secure data storage can be enabled with blockchains without a centralized trusted third-party [2]. In Europe, GDPR directives are important drivers which will become more stringent in the coming years. Better decentralization will enable higher security especially in terms of availability for this critical domain.

### D. Decentralized and Trustworthy 6G Communications Infrastructure and Solutions

There is a plethora of application opportunities for exploiting blockchains in 6G infrastructure itself for performance gains or enabling new services/use-cases. Namely,

- *Decentralized network management structures*: The decentralized blockchain-based network management will provide better resource management and more efficient system management [18].
- *Pricing, charging and billing of network services*: Blockchains can enable charging and billing without a centralized infrastructure which is a more flexible and efficient architecture compared to conventional systems.
- *Authentication, Authorization and Accounting (AAA)*: When massive scale connectivity with heterogeneous and fragmented network elements are in place in 6G networks, AAA functions need to be decentralized and much more robust for service continuity [22]. For instance, (group) key management and access control mechanisms

can be offloaded to blockchain platforms for better scalability (especially for resource-constrained end points) and transparency.
- *Service Level Agreement (SLA) management*: 6G networks will build on virtualized and sliced network architecture similar to 5G networks but yet implement that at a extremely large scale. Moreover, these networks are expected to serve a very wide spectrum of use-cases with diverse service level guarantees. Therefore, SLA management is an important system requirement. Blockchains will enable decentralized and secure SLA management in this complex setting.
- *Spectrum sharing*: Capacity expansion and spectrum agility for 6G radio access (for bands ranging from MHz to THz bands) is not evident with centralized management structures and uncoordinated sharing schemes. Blockchains and smart contracts can alleviate the spectrum sharing related cooperation and tranparency issues [12].
- *"Extreme edge"*: 6G networks need to facilitate the spatial translation of many core services from the cloud to the edge networks for achieving extremely low latency communications and instant networks. The trustworthy coordination and transparent resource bookkeeping can be attained with blockchains in these systems [20].

## V. Future Research Opportunities

The research scope of 6G is immense with diverse combinations of the computer science and telecommunication research avenues. The most prominent research opportunities for 6G with blockchain technology are discussed in this section.

### A. Internet of Everything (IoE)

The IoE is more general than IoT and has the purpose to seamlessly connect people, processes, data and things in an intelligent way [15]. The distinguishing role of IoE discussed in [27] It is expected that the IoE will re-invent business processes and business models. First, processes are optimized and automatized thanks to digital technology. Second, due to the usage of digital technology, new business models in different industries become possible.

It will be interesting to investigate from a business point of view the consequences of the numerous possibilities when introducing IoE. In particular, there will be a high need to compete with unprecedented business velocity and agility. Moreover, the impact of adding blockchain based technologies for the purpose of interoperability among different businesses, e.g. billing, requires further research.

### B. Data storage and analytics

By implementing the IoE, millions of things and objects will continuously generate real-time streams of new data. As a consequence, in the first place sufficient and efficient centralized and decentralized data storage technologies are required. It is clear that blockchain enabled technologies can play a major role there. However, it is not yet clear how to distribute and combine these technologies in different domains (edge, fog, and cloud).

Second, research on methods for data analytics will be highly needed in order to analyze and extract the essential elements out of this large heap of data for efficient and accurate decision processing. The four main categories of methods are descriptive analytics, diagnostic analytics, predictive analytics, and prescriptive analytics, and mainly depend on the type of application. Again, it will be interesting to investigate the possibilities to combine these data analytics methods with a distributed blockchain based data storage, where advantage of the smart contracts can be exploited to automate the processes.

### C. Artificial Intelligence (AI)

In 4G, AI was not yet applied, while in 5G there is already a limited partial use. We expect a much deeper integration of AI on all levels of the 6G network communications with the ultimate goal to make our society super smart, super efficient and more green.

First, at the physical layer, AI and machine learning techniques have been shown to improve channel coding [28], ranging and obstacle detection [29], and physical layer security [30]. Research in each of these domains is still in a preliminary stage and requires further investigations. Next, at the network layer, the currently applied 5G technologies like SDN, NFV, and network slicing will need to be further improved in order to obtain a more flexible and self-learning adaptive architecture able to support the more complex and heterogeneous networks, which are often also dynamically changing.

The role of the blockchain in this domain will mainly be to make the decision process of the machine learning methods more understandable and coherent as all the underlying elements on which the decisions are made can be traced back.

### D. Dedicated applications

*1) Vehicle to Vehicle Communications:* Intelligent Transport Systems (ITS) are certainly one of the important applications that will break through in the next decade and will require the technical capabilities offered by a 6G network. A blockchain based approach to define the trust management of vehicles has been demonstrated and evaluated through simulation in [31]. The main shortcoming of their approach was the limitation to ad hoc networks, and thus further investigation is required to ensure also the deployment in an autonomous way, including challenging mobility settings such as a multi-junction road network.

*2) Unmanned Aerial Vehicles (UAV):* UAVs or drones will also present an important part in 6G as high-data-rate wireless connectivity will be required. Here, blockchain can play a major role to contribute to the protection of the security and privacy of the drones and thereby collected information [32]. Li et al. [33] also illustrate the significance of 5G in UAV context. IBM has even filed a blockchain patent to address drone fleet security [34]. There are several blockchain based application for drones. First of all, the blockchain technology can help to arrange identity management. Next, air traffic management can be arranged in a secure, accurate and efficient

way. Finally, insurance companies can use trusted records for dispute resolution.

## VI. Conclusion

The design of 6G wireless networks, driven by the enormous and heterogeneous demands of hyper-connected existence of everything, will indeed give rise to new business avenues. Accordingly, this paper highlights the new intriguing challenges and canvassed the key role of blockchain to mitigate some of them. Moreover, plausible future research directions are also discussed.

## Acknowledgement

This work is partly supported by European Union in RESPONSE 5G (Grant No: 789658), Academy of Finland in 6Genesis (grant no. 318927) and Secure Connect projects.

The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

## References

[1] B. Aazhang and et al, *Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence (white paper)*, 09 2019. [Online]. Available: http://jultika.oulu.fi/files/isbn9789526223544.pdf

[2] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, Requirements, Technologies, Challenges, and Research Directions," *arXiv preprint arXiv:1909.11315*, 2019.

[3] ITU, "IMT Traffic Estimates for the Years 2020 to 2030," *Report ITU-R M. 2370–0, ITU-R Radiocommunication Sector of ITU*, 2015.

[4] M. Piran, D. Y. Suh *et al.*, "Learning-Driven Wireless Communications, towards 6G," *arXiv preprint arXiv:1908.07335*, 2019.

[5] F. Tariq, M. Khandaker, K.-K. Wong, M. Imran, M. Bennis, and M. Debbah, "A Speculative Study on 6G," *arXiv preprint arXiv:1902.06700*, 2019.

[6] J. Fleetwood, "Public Health, Ethics, and Autonomous Vehicles," *American Journal of Public Health*, vol. 107, no. 4, pp. 532–537, 2017.

[7] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *arXiv preprint arXiv:1902.10265*, 2019.

[8] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[9] N. H. Mahmood, H. Alves, O. A. López, M. Shehab, D. P. M. Osorio, and M. Latva-aho, "Six Key Enablers for Machine Type Communication in 6G," *arXiv preprint arXiv:1903.05406*, 2019.

[10] S. Yrjölä, "Decentralized 6G Business Models," in *2019 6G Wireless Summit*, 2019.

[11] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain, "Network Slicing for 5G: Challenges and Opportunities," *IEEE Internet Computing*, vol. 21, no. 5, pp. 20–27, 2017.

[12] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and Beyond Networks: A State of the Art Survey," *arXiv preprint arXiv:1912.05062*, 2019.

[13] A. Nag, A. Kalla, and M. Liyanage, "Blockchain-over-Optical Networks: A Trusted Virtual Network Function (VNF) Management Proposition for 5G Optical Networks," in *Asia Communications and Photonics Conference*, 2019, pp. M4A–222.

[14] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The Challenges of M2M Massive Access in Wireless Cellular Networks," *Digital Communications and Networks*, vol. 1, no. 1, pp. 1–19, 2015.

[15] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, *IoT Security: Advances in Authentication*. John Wiley & Sons, 2020.

[16] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[17] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things," *IEEE Network*, vol. 33, no. 5, pp. 12–19, 2019.

[18] T. Maksymyuk, J. Gazda, L. Han, and M. Jo, "Blockchain-Based Intelligent Network Management for 5G and Beyond," in *2019 3rd Int. Conf. on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 36–39.

[19] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, 2019.

[20] 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.

[21] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based Efficient Privacy Preserving and Data Sharing Scheme of Content-centric Network in 5G," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2017.

[22] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G," in *2017 16th International Conference on Optical Communications and Networks (ICOCN)*. IEEE, 2017, pp. 1–3.

[23] V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "Blockchain Enhanced SECRET Small Cells for the 5G Environment," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[24] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G Vehicular networks: Blockchains and Content-centric Networking," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 121–127, 2018.

[25] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, Cham, 2017, pp. 16–29.

[26] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: A Distributed Blockchains-based Secure SDN Architecture for IoT Networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[27] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont)," in *2015 Internet Technologies and Applications (ITA)*. IEEE, 2015, pp. 219–224.

[28] A. W. R. Sattiraju and H. D. Schotten, "Performance Analysis of Deep Learning Based on Recurrent Neural Networks for Channel Coding," in *2018 IEEE Int. Conf. on Advanced Networks and Telecommunications Systems (ANTS)*, 2018.

[29] J. K. R. Sattiraju and H. D. Schotten, "Machine Learning Based Obstacle Detection for Automatic Train Pairing," in *IEEE 13th Int. Workshop on Factory Communication Systems (WFCS)*, 2017, pp. 1–4.

[30] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, "Physical Layer Authentication for Mission Critical Machine Type Communication Using Gaussian Mixture Model Based Clustering," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–5.

[31] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET," *Sensors*, vol. 19, no. 22, p. 4954, 2019.

[32] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, "An Intelligent Approach for UAV and Drone Privacy Security Using Blockchain Methodology," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019, pp. 162–167.

[33] B. Li, Z. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241–2263, 2018.

[34] A. Douglas, *IBM applies for blockchain patent to address drone fleet security*, 2018 (accessed February 3, 2020). [Online]. Available: https://www.commercialdroneprofessional.com/ibm-applies-for-blockchain-to-address-drone-fleet-security/