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, Ireland
Email: *[firstname.lastname]@oulu.fi, †gueu@zhaw.ch, ‡anshuman.kalla@jaipur.manipal.edu,
¶an.braeken@vub.be, ‖madhusanka@ucd.ie

***Abstract*—The world transforms towards the intelligent information era by 2030. The key domains linked with human life such as healthcare, transport, entertainment, and smart cities expected to elevate the quality of service with high-end user experience. The telecommunication infrastructure has to accept the unprecedented compatibility standards to the connectivity of future systems such as extensive data rate and volume for the prominent future domains such as Augented Reality(AR), Virtual Reality (VR), Mixed Reality(MR), Machine to Machine (M2M) communication, Massive Input-Massive Output (MIMO), and massive Machine Type Communication (mMTC). There are significant challenges identifiable in the communication context in matching the future demand booms. The blockchain and distributed ledger technology is one of the most disruptive technology enabler to address most of the limitations and advance the functional standards of 6G. We explored the role of blockchain to address significant challenges in 6G, future application opportunities and research directions.**

***Index Terms*—6G Networks, Blockchain, Distributed Ledger Technology, Internet of Things (IoT), 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 integrating of all sorts of wireless networks spread over ground, underwater, air and space [2]. Moreover, 6G is also envisaged to meet-up the futuristic explosive growth in mobile traffic which is estimated to be 607 Exabyte/month by 2025 and 5016 Exabyte/month by 2030 [3]. Some of the captivating uses case of 6G are VR/AR/MR and XR (Extended Reality) applications (require data rate of minimum 10 Gbps [2]), M2M type subscription and applications [3], 3D holographic imaging and presence [4], [5], 5D communications (sight, hearing, touch, smell and taste) [4], VLC (Visible Light Communications) [6], smart clothing and wearables, fully autonomous (Level-5 [7]) vehicles, accurate indoor positioning [8], Blockchain as Service (BaaS) for massive M2M communications [9].

By and large, the next generation of mobile networks are expected to be predominantly softwarized, virtualized and cloudified networks [1], [10] which are designed *to interconnect* seamlessly staggering a number of heterogeneous devices including massive IoT/IoE devices, *to cater* anticipated

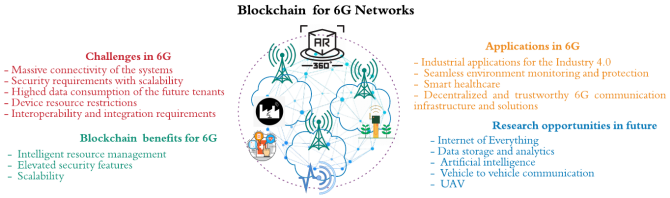

Fig. 1. The role of blockchain in 6G networks

explosive growth in data traffic at enormous high data rate along with ultra-low latency [2], *to create* wide range of incredible new vertical network services [11], [10], and *to support* the development of brand-new fleet of real-time [2] and data-intensive [9] applications.

Undoubtedly, softwarization, virtualization and cloudification of next generation mobile networks bring-in enormous advantages like micro operator based business models [12], agile and efficent management and network orchestration (MANO), on-the-fly creation of verticle services, differentiated services with network slicing [13], etc. However, they tend to exacerbate the issues like network reliability, security vulnerability, data privacy and immutability [14], soft spectrum sharing, multiple access control, authentic Virtual Network Functions (VNFs) [15], legitimate resource utilization, differential security for differentiated services offered by different virtual networks [13], etc.

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 DoS or DDoS), *(vi)* comparatively less processing delay as well as processing fee. Thus blockchain can be indispensable technology to establish trust in future networks.

Since blockchain has been envisioned as one of the key

enabling technology for 6G mobile networks [1], [10], [2], it is imperative to explore various benefits, opportunities and challenges foreseen with the use of blockchain. Figure 1 projects the role of blockchain in the 6G networks briefly.

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. [16].

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 Communication (mMTC). Thus it would be challenging to tailor the design of 6G systems for such an unprecedented traffic demands.

2) Real-time communication with minimal latency: The real-time communication is a crucial requirement in the future computing ecosystems. The device to device and machine to machine communication require a robust accuracy with near zero delays for the precise operation. The use cases such as autonomous driving and AR assisted healthcare systems may require a consistent minimal delay communication enablement in higher scaled transaction traffic.

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 realtime.

4) Synchronization: The synchronization is a significant requirement in time critical industrial applications. The power generation and distribution systems, vehicular networks require protection from faults in the communication and synchronization.

B. Security requirements in future computing ecosystems

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

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 principle requirement in the future ecosystems. Especially, the sophistication of the 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 attempts.

4) Authentication and access control: The data generated by the communicating nodes and data in-transit requires to establish access control mechanisms in order to define the scope of data access for various users. The authentication mechanisms which utilize centralized base station create a bottleneck in the massive nodes in the ecosystem. The complexity of network utilizing services incur a significant overhead on the definition of different access control mechanisms for the tenants of the 5G network.

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 the tenants of 5G ecosystem. The auditing of a massive number of tenants will be a significant challenge in 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 5G network ecosystems. The applications such as AR, VR, HD and 3D ultra video require a higher data rate and data consumption.

D. Device resource restrictions

The computational and storage restrictions are anticipated in the future computing ecosystems. The restrictions limit the capabilities of cryptographic algorithms and eventually deviate from the standard mechanisms. The standard adoption of the security is harder with the device resource restrictions.

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 based smart contracts in order to address the challenges discussed previously are mentioned in this section.

A. Intelligent resource management

The network resource management and sharing is a significant in the 6G. Especially, with the exponential expansion of the tenants future, the resource management operations such as spectrum sharing, orchestration and decentralized computation requires to be compatible with massive infrastructure volumes. 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 the unlicensed spectrum sharing algorithm based on game theory. Dai et al. [19] presented the application of blockchain and deep reinforcement learning for the efficient resource management services including spectrum sharing and energy management. Mafakheri1 et al. [20] applied blockchain for resource sharing to utilize 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. Especially, the massive data volume in the future 5G networks require to enforce privacy in different milestones including data in storage as well as data in transit. 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 owe scalability limitations. The access control with the centralization is a significant challenge in the design of future 5G associated systems. 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 the DDoS attack 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 distributed ledger technology. 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 eliminated in the blockchain and smart contracts to enable the massive connectivity in future. The peer to peer operational capability and the integration of edge and fog computing nodes will improve the service strengths in the future network ecosystems.

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 [11]. 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 challenges due to stringent performance requirements in industrial applications. These are also valid for industrial networks and IoT [10].

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 in 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 [14].
- *"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. Research Opportunities in Future

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

A. Internet of Everything (IoE)

The IoE is more general than IoT and has the purpose to seamlessly connect in an intelligent way people, processes, data and things [27]. It is expected that the IoE will reinvent 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. For instance, Nike is now also entering the market of healthcare via the introduction of its smart cloths and shoes.

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, which is also called by Gartner as the business moment. Moreover, the impact of adding blockchain based technologies for the purpose of e.g. billing, to enable interoperability among different businesses requires further research.

B. Data storage and analytics

By implementing this 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 in it. However, it is not yet clear how to distribute, combine these technologies at different levels (edge, fog, 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 bunch of data to be used in 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 taken 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 Communication: 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 a multi-junction road network.

2) Unmanned aerial vehicle (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 the 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.

There are several blockchain based application for drones. First of all, the blockchain technology can help to arrange identity management. Next, also air traffic management can be arranged in a secure, accurate and efficient way. Finally, insurance companies can use the stored records in case of events or disputes.

VI. Conclusion

An exponential growth of demand anticipated for the 6G telecommunication in the information era, by 2030. The role of blockchain to eliminate limitations foreseen with the future massive demands and the the contribution to escalate the service values in telecommunication identified in the paper. The future research directions also presented in the paper.

References

[1] B. Aazhang, P. Ahokangas, H. Alves, M.-S. Alouini, J. Beek, H. Benn, M. Bennis, J. Belfiore, E. Strinati, F. Chen, K. Chang, F. Clazzer, S. Dizit, K. DongSeung, M. Giordiani, W. Haselmayr, J. Haapola, E. Hardouin, E. Harjula, and P. Zhu, *Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper)*, 09 2019.

[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] I. Union, "Imt traffic estimates for the years 2020 to 2030," *Report ITU-R M. 2370–0, ITU-R Radiocommunication Sector of ITU*, 2015.

[4] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Kténas, N. Cassiau, and C. Dehos, "6g: The next frontier," *arXiv preprint arXiv:1901.03239*, 2019.

[5] M. Piran, D. Y. Suh *et al.*, "Learning-driven wireless communications, towards 6g," *arXiv preprint arXiv:1908.07335*, 2019.

[6] 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.

[7] J. Fleetwood, "Public health, ethics, and autonomous vehicles," *American journal of public health*, vol. 107, no. 4, pp. 532–537, 2017.

[8] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "From a human-centric perspective: What might 6g be?" *arXiv preprint arXiv:1906.00741*, 2019.

[9] 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.

[10] 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.

[11] 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.

[12] S. Yrjölä, "Decentralized 6g business models."

[13] 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.

[14] 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.

[15] 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*. Optical Society of America, 2019, pp. M4A–222.

[16] 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.

[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 International Conference on Advanced Information and Communications Technologies (AICT)*. IEEE, 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)*. IEEE, 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] O. A. https://ioe.org/, "Internet of everything. (2019). internet of everything (ioe)."

[28] A. W. R. Sattiraju and H. D. Schotten, "Performance analysis of deep learning based on recurrent neural networks for channel coding," in *Proceedings of 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2018.

[29] J. K. R. Sattiraju and H. D. Schotten, "Machine learning based obstacle detection for automatic train pairing," in *IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2017, pp. 1–4.

[30] J. L. a. H. S. A. Weinand, M. Karrenbauer, "Physical layer authentication for mission critical machine type communication using gaussian mixture model based clustering," in *IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[31] Y. J. S. T. A.S. Khan, K. Balan and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in vanet," *Sensors*, vol. 19, no. 4954, 2019.

[32] M. K. S. R. P. B. B. T. Rana, A. Shankar, "An intelligent approach for uav and drone privacy security using blockchain methodology," in *9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019.

[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.