

Study of Efficacious use of Blockchain in 6G Technology-Path for the Future

Ritvik Voleti

KCC-ITM, Greater Noida, Uttar Pradesh,
India

Abstract - Since the 5G does not cope with the exceedingly high IoT demands hence, the onus lies on 6G network to ensure that high throughput is experienced compared to the previous networks as we see a surge in development of new facilities and applications like multiple-gigabit communication rate, improved authenticity, low latency. A smart resource management along with proper distribution is necessary for achieving all the ambitions due to lack of spectrum resource, efficient resource management and sharing. Blockchain is the answer to all these expectations and has lately gained massive significance and is highly critical for sixth generation wireless network and beyond due to its smart adaptability and inbuilt features. With the help of technologies like IoT, network slicing, D2D and domain blockchain environments we can see an enormous future for blockchain in terms of managing the resources. This review article is based on the blockchain technology reshaping the industries that brings safe production which ensures detectability, consent, security, improved standard, and validation. We analyzed on many advantages of blockchain along with 6G and its lapses and blockchain technology addresses daunting difficulties of sixth generation wireless network with its prospective opportunities.

Keywords: 6G, Blockchain, Wireless Blockchain, IoT.

I. INTRODUCTION

Multi-use devices are being utilized tremendously as they support us in fulfilling our daily needs. We sense a great deal of simplicity that we, the humans are living in a connected world via the communication networks (like Internet, wireless and mobile networks) and finally will reach the universal ecosystem. Wi-fi communication structure is the Eureka equivalents with rapid technological developments for the past years and symmetry advancements in the IoT [1]. Till now, Vth generations of wi-fi mobile data communications systems are present. In wi-fi data communication generation develops nearly in every decade since 1980's, starting from 1981 the Ist generation had the analog frequency modulation cellular system, From 1992 the IIIrd generation at 2001, with the IVth generation which is often called as LTE on 2011 [2][3]. In the last 10 years a massive transformation took place in the wi-fi communications that led in data-demanding apps, which includes multimedia, gaming, and HD video streams to thrive. The profitable Internet technology that becomes a catalyst which enables and propagates different latest services, like shopping using mobiles and other forms of online transactions. [2][4].

Its well familiar that fifth generation is itself a cellphone network, the 5G network provides a lot of channels that focusses on enabling multi gadgets to link, as fifth generation technology depends tremendously on IoT. As we see a rise in demand for cell phones along with networks, latest Internet of Everything for users and industries has installed quickly. The arrival of SDN brings a lot of attributes which allows the network arranger and consumers to approach the network gadgets at a remote place, while grasping the international view for the these places, the usage of Software defined networking technologies presents a variety of difficulties and needs solved by IoT [5]. The quantity of wi-fi network consumers is ascending gradually because of WWW, IoT, D2D and M2M transmission, cloud- based apps and facilities. Humans consistently want ascending uplink-downlink processing costs, better standard of facilities, improved net alongside quality of experience, improved video streaming. Hence, these requests brings massively huge cellular traffic in cellphone networks. So, latest mobile approach is needed to furnish these requests. Developers and researchers prophesied that fifth generation will be an acceptable contender in response of these requirements [6]. 5G wi-fi networks introduces the IoT, that depends on improved broadband approach for machine-based transmission [7], [8]. But, for fifth generation networks since it has not been established into wider use, the aim is a long shot to be completely brought in the market. For instance, acute-frequency millimeter wave connectivity and assistance in heterogeneous IoT facilities are not accessible at the limit needed for innovative usages like pervasive virtual/amplified reality or associated autonomous approach [8]. For supporting the needs of the present and future use cases, it is a necessity to go past 5G networks as it operates in a low transmission frequency bands, towards millimeter-wave which functions at a greater carrier frequencies that is originally in the high transmission frequency window greater than twenty gigahertz, in addition to this an even greater towards optical frequencies at the detectable and undetectable electromagnetic waves spectrum [9]. Then we can witness the potential of fifth generation networks that would be moderately divulged. The succeeding years is the transformation stage in the fifth generation and NG-IoT technologies as they would trend towards forms of concurrence, wherein the usage of millimeter-wave frequency will become customary [10]. The next generation of IoT would merge technologies like Artificial Intelligence, disseminated edge computing along with end-to-end disseminated safety assisting long binary digit rates providing enhanced mobile broadband uses. Besides the evolution of wireless connectivity at the edge of the network, we anticipate major advances also on the control and management of the edge network that will be supported by the introduction of new technology approaches driven by artificial intelligence (AI) solutions, The main aim is to improve the 5G networks with the strength of intelligence provided by cognitive calculative systems which uses large quantity of accessible data

and ML algorithms [11] [9]. The sixth generation wireless network would bring in improved standards which would slowly develop and evolve and give a superior and increasingly solid network.

II. RESEARCH ARE PERFORMED ON 6G

In today's world, sixth generation wireless network mobile transmission technology is a demanding research area. The 6G will transform conduct, community, trade and transmission systems. It's a pivotal period to envisage the prospective applications, methods and difficulties of sixth generation wireless network technology. Significantly, sixth generation wireless network will generate tremendous research prospects and allow different types of latest technologies. Sixth generation wireless network would be a turning point in various types of fields. Hence, the envisaging of the sixth-generation wireless network technology is needed to transform the contemporary world. At present numerous nations are positioning the fifth-generation technology productively. But fifth generation and B5G could not give the absolute necessities of the IoT. Subsequently, sixth generation wireless network is quite demanding in the market. Analysts have commenced explaining the difficulties of beyond 5G cellphone communication. In coming 4-5 years, beyond 5G would develop and is extremely anticipated that sixth generation wireless network would completely run from 2030. The sixth generation wireless network would be an eminent field of research for coming 1-2 decades. The sixth generation wireless network analysis had started in Finland from 2018 and named by "6genesis flagship project" [12]. On 2019, China, USA and South Korea had propelled a 6G project [13]. Japan also started sixth generation wireless network design by 2020 [14]. NTT had issued the white paper on Jan 2020. Countless nations have commenced the sixth generation wireless network project. There is a update in mobile generation every 10 years. [15].

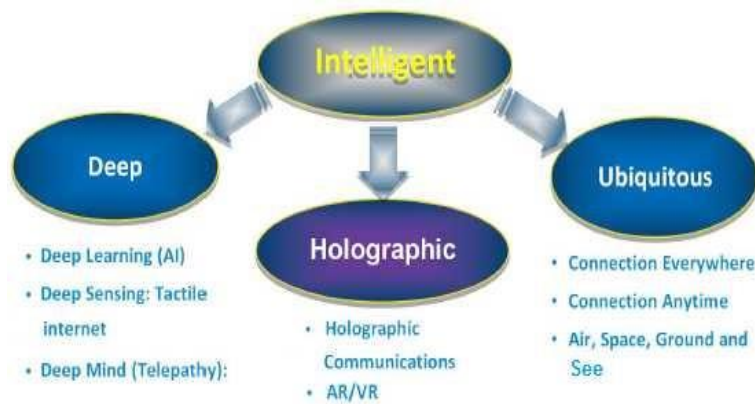


Fig.1 Benefits of 6G [16]

Sixth generation wireless technology is anticipated to initiate various features ultra-high security, lower latency, along with maximum efficiency inter-gadget synchronicity [17]. Hence, it inspired to explore on key matters and difficulties of sixth generation wireless technology. The sixth generation wireless technology will modify the clarity and approach of contemporary conduct, community, business, and transmission. It is anticipated that sixth generation network technology will cohort in transforming different fields.

Sixth generation wireless cellphone networks are contemplated to provide the prospect of ubiquitously attached data-intensive inventive society [18] enriched with total automation with consistent combination of all types of wi-fi networks on underwater, land, space and sky [19]. Sixth generation wireless technology is visualized to maintain with the massive advancement in cellphone traffic that is predicted as 607 Exabyte per month by 2025 and increased to 5016 Exabyte per month till 2030 [20]. The coming generation cellphone networks are predicted to be inherently softwarezied, virtual and cloud based systems [18], [21] for the aim to connect coherently an astounding quantity of heterogeneous gadgets including large Internet of Things gadgets, to serve the awaited large success in data interruptions at drastically-steep data rates besides the drastically-small latency [19], to make magnificent scope of modern vertical network facilities [22], [21] and to assist the growth of latest collection of real-time [19] along with data-accelerated applications.

Tremendous research works are being carried out in 6G networks and will continue to go on in the coming future.

Gui et al. deliberated on different feasible uses of MBBLL, mBBMT, mLLMT [23].

Zhang et al. targets on FeMBB, ERLLC, umMTC, LDHMC and ELPC [24].

Dang et al. furnishes prospective opportunities of sixth generation wireless network [13]. Besides this, researchers have written some controversial works on 6G [25]. Ironically, it is highly essential to discover the difficulties to be tackled by the anticipated sixth generation technology.

B. Zong et al. have examined the principal factors and current coherent beginning of sixth generation wirele network [26].

Z. Zhang et al. have evaluated sixth generation network, elaborating a cluster of encouraging methods like THz transmission, LISs, OAM, blockchain-based spectrum distribution, quantum transmission, computing, along with molecular communications [27].

R. Heath represented 3 principal directions in sixth generation wireless network of the physical surface [28].

P. Yang et al. elaborated on many modern approach of sixth generation wireless network in the communication with network layer [29].

- K. Letaief et al. gave a developmental direction of sixth generation wireless using AI depended technologies [30].
F. Tariq et al. gave the tendency of development in sixth generation wireless in depth [31].
W. Saad et al. studies the different possible future problems arising from the sixth generation wireless networks [32].
K. David et al. 6G technology focusses on various needs of Internet of Everything [33].
B. Zong et al. explains the development of evolving trends like ubiquitous and distributed AI [34].

III. VULNERABILITIES OF 6G

The difficulties in building a reliable sixth generation wireless network are multiple ordered spanning tele-communication, rules, TEA, politics and conduct. A collection of the present rules, economic impetus and development are keeping up with the present capability of hacking, deficiency of reliability, secrecy and protection on the net. In sixth generation wireless network, it will not satisfy as the personal integrity will completely based on IT alongside the usage for transmission over the networks. Hence, we require reliable sixth generation wireless network. The part of reliability, protection and secrecy are interrelated in some way or the other, but various levels of upcoming generation of networks. Some expected difficulties in the sixth-generation network are clarified in [35]. Difficulties suitable to machine to machine transmissions are given in [36].

Flexibility: Physically coated protective methods can provide smart results for protecting the most integral and least analyzed network sections that are the joining the body sensors with a sink node or a hub. Latest Researches are based on the highly adaptable coating facilities to be utilized for safety algorithms in sixth generation wireless network that contain the maximum network flexibility, various types of gadgets and types of malignant attacks.

The commercial Internet of Things passionate predicts that uncountable number of gadgets will be linked and functioned in the coming commercial ecosystems by the development of notions like mMTC. So it is a challenge to customize the sixth generation wireless network systems during traffic need.

Integration: The integration is an important need during demanding commercial applications. The integral spine of a nation includes power sharing systems and automotive networks have to integrate at real time to sustain a precise operation.

Verification with access restriction: The stored data needs to protect with the entry control procedure to avoid illegitimate changes. In the tremendous innovative needs expected in the sixth generation wireless network, the standard validation and entry restriction techniques would get limited on the basis of flexibility. The latest Internet of Things gadgets with sixth generation wireless network would ascend 10 times from ten billion in fifth generation wireless network to hundred billion in sixth generation wireless networks. The economic dependency and Information Technology's societal impact increases due to the distribution and usage of the sixth generation wireless networks.

Real-time transmission with least latency: Real-time transmission is an integral need in the coming processing environment. The D2D and M2M transmissions need a powerful accuracy which should have nearly 0 stoppages for accurate operations. A maintained low delay transmission is needed in extensive data exchange like autonomic driving and augmented reality assistance in medical aiding systems.

Accessibility: The utility accessibility is a main need in prospective networks. The fear of Distributed Denial of Service attack is increased due to the sophisticated sixth generation wireless network environment with a giant number of interrelated gadgets. Besides this the 6G cannot find the breaches and dangerous attempts as the uniqueness of the present network protective tools because it cannot directly apply into the 6G networks [37].

Confidentiality: The evolution with cloud framework is assumed to advance in sixth generation wireless networks. The move towards a secure cryptography after the quantum age as wide ranged computing is not a task to be fulfilled easily in the coming future. Current symmetric cryptography is still the most secure since quantum computing. The prospective computing framework like Internet of Things shows a large menacing behavior with wi-fi connection. Being light is an integral part of encryption methods such as symmetric key encryption algorithms especially in the case of less powered Internet of Things gadgets. But this method will reveal a high privacy threat because of computational limitations [38].

Improved throughput: The main system which would use the 6G transmission environment will need synchronous connection of uncountable gadgets. The network framework like base stations would manage the large quantity of businesses at real time.

Integrity: The large quantity of data made by the prospective systems would need accessibility and modification in data provided by the legitimate consumers when data is in transition. Eavesdropping along with transformation in transit data would diverge the system functionality from expectation.

IV. PROSPECTS REGARDING 6G USING BLOCKCHAIN TECHNOLOGY

Blockchain is like a clear, include-only and sequential sections of data which is supervised by many candidates that avoid distortion. Before any addition in the blockchain verification and acceptance of the new section of data is needed by most of the candidates. During the period of verifying the participants need an observer of preceding data. Hence, blockchain is largely accepted like the advanced trusted mechanism for validating the 6G networks [39], [40]. Blockchain mechanism favors fragmented uses and propagation of reliability, as observed by production chains and cryptocurrency along with trusted systems. Blockchains are designed like disseminated chains that prevent one-point collapse. Till now, sixth generation wireless network facilities could utilize blockchain guaranteeing reliability and safety for instance in access restrictions, verification, shared key administration and evaluative deposition [41]. Hence, the predicted facilities and maximum execution of sixth generation wireless networks improves the development with the use of blockchain and the usage of blockchain for the facilities is predicted to enhance their rise that leads in an improved feedback loop. The blockchain propagation of reliability and safety and

Cloud computing provides assistance to the sixth generation wireless network use conditions (facilities and developments). Blockchain can contribute with a distributed structure for confederated learning removing the necessity for rationalizing command on studying and analysis in edge-based administered ML [42]. A smart, administered cellphone network framework that is depended at open-source wi-fi networks [43], needs an open retail in which consumers, spectrum and ISP owners may openly involve to transfer their reserve using blockchain [44].

Blockchain is a key developmental technology to show the true capability of sixth generation wireless network systems. For the prospective automation environment the reserve regulation over network is a difficulty due to the predicted immense connectedness requirement. The regulation in the reserve functions like spectrum distribution, distributed calculation/analysis required adaptability with large-scale framework.

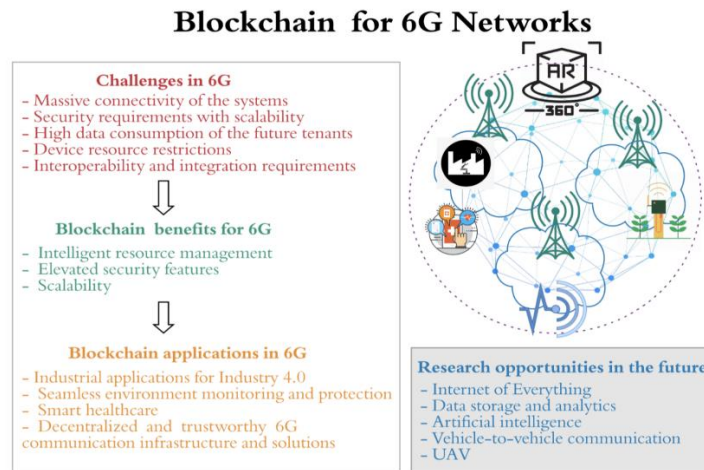


Fig.2 Blockchain with 6G network [45]

V. STUDIES PERFORMED ON 6G NETWORK WITH BLOCKCHAIN TECHNOLOGY

Various studies have been carried out and are still continuing for this ever trending subject which is the need of the hour. Few of the key researchers on this subject are as follows:

Zhang et al. [46] conferred on edge intelligence with Industrial Internet of Things structure having a reliable and adaptable service managing in post fifth generation wireless network.

Ortega et al. [47] gave a system using blockchain ensuring the coherence as internet functions like a medium for transfer of information.

Dai et al. [48] conferred the uses of blockchain along with deep augmented learning to efficiently manage the facilities taking spectrum distribution and managing energy into consideration.

Mafakheri et al. [49] enforced on blockchain as a resource distributor and showed that the usage of intelligent contracts would provide self-organization in networking.

Yang et al. [50] provided verification using blockchain technology and coordinated procedures to provide cloud radio utilizing the fiber network technology.

Fan et al. [51] gave a safety protection scheme that was using blockchain in the content-significant networks.

Adat et al. [52] conferred an explanation on blockchain for avoiding polluting charge that harm the coherence of data.

Maksymyuk et al. [53] gave a smart network framework that uses blockchain mechanism by managing the relation between providers and consumers providing intelligent contracts. This was a without licensed spectrum distributive algorithm that dependent in the game theory.

Rodrigues et al. [54] conferred a Distributed Denial-of-Service prevention structure by the assistance of blockchain.

Sharma et al. [55] suggested that the blockchain usability and Software-defined-network to enforce compelling security facilities like Distributed Denial-of-Service attack avoidance, data security and access restraint.

VI. VULNERABILITIES/THREATS OF USING BLOCKCHAIN TECHNOLOGY IN 6G

Safety risks using Blockchain as a integral part of our technology would introduces us to numerous threats [56], that are passed on to sixth generation wireless network. The types of core attacks for which blockchain becomes susceptible are as follows:

Susceptibilities: Blockchain functions on providing safety and privacy with no sort of involvement of the mediators with a mandatory agreement of most of the members. But the attackers are able to get power of the complete system by gaining the control of more than fifty percent of members. Using Bitcoin an attacker needs fifty one percent of the computation capability of the network to manage on Bitcoin network [56]. Double-spending tries to forge the righteousness surrounding the blockchain's supplied ledger.

Expandability because of its dissolute nature and since bitcoin requires a large bandwidth, computation and repository to maintain the righteousness surrounding the ledger. Blockchain regulations needs mandatory blockages and a large quantity of transferred messages and broadcasting by the members. The throughput of any blockchain-built application on the basis of

latency along with expandability could hence be prohibitive [57]. For instance Bitcoin's highest throughput is 7 transactions per second and has a latency of 10 minutes for each verified block.

Underlying Networking: Enabling an acceptable method in the blockchain becomes a costly affair and there is a substantial need for bandwidth sources. Sources are scarce in upcoming networks hence the resource regulation for big transaction performance is paramount as the resources needs would be tough to meet up with the present system in place.

Exchange in security exploits: Blockchain is based on transparency of exchange in information. Therefore the consumer security is threatened in system which are blockchain dependent. In addition, several attacks versus blockchain contain selfish mining [58] along with sybil attacks [59]. The prior mining is a method to access more profit and misuse the sources of honest miners using the PoW mechanism, on the contrary in the latter attack the consumer builds a collection of blockchain accounts for manipulation. So, intelligent contracts that are dependent on blockchain are increasingly broaden blockchain feasibility by enabling contracts by definition typically software-based between members like exchanges [60].

Repository: Every duplicate node in the traditional blockchain network have to compute and keep a duplicate of the finished exchanged data. This could increase the repository and calculation load on Internet of Things gadgets, that are mostly limited to the resource thereby hindering their involvement in blockchain network.

There are many obstacles surrounding the perfect functioning of block chain technology while there vulnerabilities in it there are still many reasons to be optimistic in this potentially secure technology.

VII. CONCLUSION

Sixth generation wireless network is an integral part of technological transmission which would provide lots of modern technologies like holographic transmission. Nevertheless, the fifth generation wireless network and sixth generation wireless network are significantly different. Hence, there are many difficulties of sixth generation wireless network to maintain the necessary parameters and fulfill the prospects of this network. All controversies and difficulties surrounding the sixth generation wireless network have been revealed from each perspective. Sixth generation wireless network would modernize large fields and would prove a game changer in diversified fields. To ensure the proper resource management of 6G using blockchain we have to tackle some challenges like execution of blockchain rules through the wi-fi channel and examining the basic restrictions based on the execution and safety, enriching environment on the basis of blockchain by taking into protection and different privacy matters, development of light blockchain technology for economical Internet of Things gadgets; large-performance blockchain along with disseminating the industry and prospective networks.

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. Integrated blockchain in sixth generation wireless network would supply the network to supervise and sustain with resource usage and distributing adequately. The blockchain technology provides transparency and shared information transformation that would assist various industries. Blockchain gets a massive support by cryptocurrency along with the ledger keeping business because of the strength of the society [61], this technology has got increased interest by cellphone promoters decisionmakers [62].

REFERENCES

- [1] Mohammed H. Alsharif , Anabi Hilary Kelechi, Mahmoud A. Albreem, Shehzad Ashraf Chaudhry, M. Sultan Zia and Sunghwan Kim, "Sixth Generation (6G) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions" .
- [2] M.H. Alsharif, R. Nordin, Evolution towards fifth generation (5G) wireless networks: Current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. *Telecommun. Syst.* 2017, 64, 617–637.
- [3] M.A. Albreem, M.H. Alsharif, Kim, S . A Robust Hybrid Iterative Linear Detector for Massive MIMO Uplink Systems. *Symmetry* 2020, 12, 306.
- [4] S.L. Mohammed, M.H. Alsharif, S.K. Gharghan, I.Khan, M. Albreem, Robust Hybrid Beamforming Scheme for Millimeter-Wave Massive-MIMO 5G Wireless Networks. *Symmetry* 2019, 11, 1424.
- [5] Samaresh, B., Sudip, M. & Athanasios, V.V. (2017). Software-Defined Networking for Internet of Things: A Survey, *IEEE Internet of Things Journal*, 4(6), 1994- 2008.
- [6] Cengiz, K. (2018). Next-Generation Infrastructure and Technology Issues in 5G Systems, *Journal of Communications Software And Systems*, 14(1), 33-39.
- [7] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [8] 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.
- [9] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [10] 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.
- [11] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [12] 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.
- [13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [14] 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.
- [15] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

- [16] 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.
- [17] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.
- [18] 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.
- [19] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.
- [20] 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.
- [21] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," IEEE Access, vol. 7, pp. 78 729–78 757, 2019.
- [22] M. H. Mazaheri, S. Ameli, A. Abedi, and O. Abari, "A millimeter wave network for billions of things." In Proc. ACM Special Interest Group Data Commun., 2019.
- [23] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, "Wireless network intelligence at the edge," 2018, arXiv:1812.02858.
- [24] M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, "6genesis flagship program: Building the bridges towards 6g-enabled wireless smart society and ecosystem," in 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM). Guadalajara, Mexico: IEEE, Nov 2018, pp. 1–9.
- [25] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" Nature Electronics, vol. 3, no. 1, pp. 2520–1131, 2020.
- [26] N. DOCOMO, "White paper 5g evolution and 6g," Accessed on 1 March 2020 from https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_20200124.pdf, 2020.
- [27] S. Chen, Y. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6g: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," IEEE Wireless Communications, pp. 1–11, 2020.
- [28] <https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-6G-Wireless-Technology.html>.
- [29] Z. Zhang et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Veh. Technol. Mag., vol. 14, no. 3, 2019, pp. 28–41.
- [30] 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>.
- [31] 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.
- [32] ITU, "IMT Traffic Estimates for the Years 2020 to 2030," Report ITU-R M. 2370–0, ITU-R Radio communication Sector of ITU, 2015.
- [33] 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.
- [34] N. H. Mahmood, H. Alves, O. A. L'opez, 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.
- [35] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6g: Opening new horizons for integration of comfort, security and intelligence," IEEE Wireless Communications, pp. 1–7, 2020.
- [36] 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, Sep. 2019.
- [37] Y. Al-Eryani and E. Hossain, "The d-oma method for massive multiple access in 6g: Performance, security, and challenges," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 92–99, 2019.
- [38] B. Zong et al., "6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies," IEEE Veh. Technol. Mag., vol. 14, no. 3, 2019, pp. 18–27.
- [39] Z. Zhang et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Veh. Technol. Mag., vol. 14, no. 3, 2019, pp. 28–41.
- [40] R. W. Heath, "Going Toward 6G," IEEE Signal Process. Mag., vol. 36, no. 3, 2019, pp. 3–4.
- [41] P. Yang et al., "6G Wireless Communications: Vision and Potential Techniques," IEEE Netw., vol. 33, no. 4, 2019, pp. 70–75.
- [42] K. B. Letaief et al., "The Roadmap to 6G – AI Empowered Wireless Networks," IEEE Commun. Mag., vol. 57, no. 8, 2019, pp. 84–90.
- [43] F. Tariq et al., "A Speculative Study on 6G," available online: <https://arxiv.org/abs/1902.06700>.
- [44] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," IEEE Netw., to be published, doi: 10.1109/MNET.001.1900287.
- [45] K. David and H. Berndt, "6G Vision and Requirements," IEEE Veh. Technol. Mag., vol. 13, no. 9, 2018, pp. 72–80.
- [46] B. Zong et al., "6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies," IEEE Veh. Technol. Mag., vol. 14, no. 3, 2019, pp. 18–27.
- [47] 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>.
- [48] 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.
- [49] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A Comprehensive Guide to 5G Security. John Wiley & Sons, 2018.
- [50] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, IoT Security: Advances in Authentication. John Wiley & Sons, 2020.
- [51] B. Aazhang, P. Ahokangas, L. Lov'en, et al., Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper). Oulu, Finland: 6G Flagship, University of Oulu, 1 ed., 2019.
- [52] 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.
- [53] 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.
- [54] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," IEEE Communications Letters, 2019.
- [55] J. Haavisto, M. Arif, L. Lov'en, T. Lepp'anen, and J. Riekk'i, "Opensource rans in practice: an over-the-air deployment for 5g mec," arXiv preprint arXiv:1905.03883, 2019.
- [56] 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), pp. 36–39, IEEE, 2019.
- [57] Tharaka Hewa*, G'urkan G'ur'ut', Anshuman Kalla†, Mika Ylianttila§, An Braeken¶, Madhusanka Liyanage‡ "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions" published in 6G Wireless Summit (6G SUMMIT), 2020 2nd.
- [58] 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.

- [59] 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.
- [60] 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.
- [61] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchainbased Infrastructure Sharing in 5G Small Cell Networks," in *2018 14th International Conference on Network and Service Management (CNSM)*. IEEE, 2018, pp. 313–317.
- [62] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchainbased Trusted Authentication in Cloud Radio over Fiber Network for 5G," in *2017 16th International Conference on Optical Communications and Networks (ICOON)*. IEEE, 2017, pp. 1–3.
- [63] 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.
- [64] 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.
- [65] 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.
- [66] 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.
- [67] 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.
- [68] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.
- [69] Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.
- [70] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (b-ran): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.
- [71] J. R. Douceur, "The sybil attack," in *International workshop on peerto-peer systems*, pp. 251–260, Springer, 2002.
- [72] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.
- [73] HaoXu, PauloValente Klain, Oluwakayode Onireti, BinCao, Muhammad Imran, LeiZhang "Blockchain-enabled Resource Management and Sharing for 6G Communications" *Digital Communications and Networks(DCN)* journal homepage: www.elsevier.com/locate/dcan.
- [74] H. Liu, Y. Zhang, T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network* 32 (3) (2018) 78–83. doi:10.1109/MNET.2018.1700344.