Zoological Archives: An International Journal
https://stanfordgroup.org/
Vol 5, Issue 2, 2025

THE POTENTIAL OF 6G AND BLOCKCHAIN FOR SECURE AND SUSTAINABLE COMMUNICATION

[#1]Mr.KANDUKURI CHANDRA SENA CHARY, *Assistant Professor*
[#2]Mr.PEDDI KISHOR, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT— Future communication will be secure and consistent. Futuristic apps need certain traits to work. This research divides these application needs into two main areas to underline how blockchain and 6G will affect future communication systems. Requirement Group I (RG-I) covers data speeds, latency, reliability, and large connection, whereas RG-II covers data integrity, non-repudiability, and auditability. Blockchain and 6G would reduce resource underutilization and support RG-I goals by decentralizing and sharing resources. By selecting the correct blockchain and consensus methods, 6G apps may easily meet RG-II criteria. This study indicates that blockchain and 6G can deliver safe, pervasive connectivity in the future

Keywords:Blockchain,RG-I,6G

1.INTRODUCTION

As 5G commercializes, 6G vision papers are published. These studies list HBC, XR, WTech, LS-CAS, and enhanced vertical domain support as essential 6G services and applications. These programs must send and receive massive volumes of data fast and reliably. LUMS Electrical Engineering Department member A. U. Hassan. (54792). Contact them at 18060048@lums.edu.pk and naveed.hassan@lums.edu.pk. C. Yuen is an Engineer Product Developer at SUTD, 8 Somapah Road, Singapore 487372. Email yuenchau@sutd.edu.sg.J. Zhao, D. He works in Singapore's Nanyang Technological University School of Computer Science and Engineering, 639798. Junzhao can be reached at dniyato@ntu.edu.sg.Y. Zhang is affiliated with Oslo University's Informatics Department in Oslo, Norway 0315. Contact me at yanzhang@ifi.uio.no.H. Princeton University Electrical and Computer Engineering Department 08544 employs V. Poor. Email poor@princeton.edu.U.S. and LUMS Faculty Initiative Fund partially funded this work. This work was partially supported by funds from the National Science Foundation (CCF-1908308 and ECCS-2039716), Singapore MOE Tier 1 (RG16/20), and A*STAR's RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund – Pre Positioning. Author opinions, findings, conclusions, and suggestions may not reflect A*STAR's.Copyright © IEEE 20xx. For use elsewhere, email pubs-permissions@ieee.org. 6G app data is more private and important, requiring strict data security promises. Blockchain uses cryptography and hash functions to create a chain of data blocks, which are then checked by consensus methods Blockchain could be crucial for 6G. These apps require Reconfigurable Intelligent Surfaces (RIS), TeraHertz (THz) connectivity, AI, and micro cell networks for fast networks. People must collaborate to use these technologies to accomplish performance goals when they don't trust one other. These technologies require dense network arrangements, complicating infrastructure and networks. Network distribution requires decentralization. Blockchain makes independent networks open and trustworthy. Blockchain can fulfill future information network security standards due to its built-in security features.

The correct blockchain components can adjust the blockchain's decentralization, security, and scalability to suit an application. Blockchain consensus ensures network state agreement among nodes. Blockchain can verify, lock, and check data via consensus protocols. Information network performance affects system decentralization and scalability. PoW can be utilized for decentralization and scalability but not latency. 6G can be used with PBFT and other communication-intensive approaches for fast convergence.We divided 6G application demands into two groups to simplify blockchain-6G integration. The first group, Requirement Group I (RG-I), has data speed, latency, dependability, and several connecting specifications. These performance standards enable global communication. RG-II security criteria include data integrity, non-repudiability, and auditability. The study's main contributions are:

We determine 6G program speed. Traditional and security demands are separate.

Bitcoin and 6G are being considered for many applications. Decentralized, trustless, and safe, blockchain can be used for both.

For blockchain tasks, LS-CAS scenarios are employed. We calculate the time needed to discover bad miners in a blockchain system. Simulations demonstrate Blockchain and 6G will find bad miners.

2.6G APPLICATIONS AND THEIR REQUIREMENTS

This section discusses 6G application needs, as seen in Figure 1.6G applications.

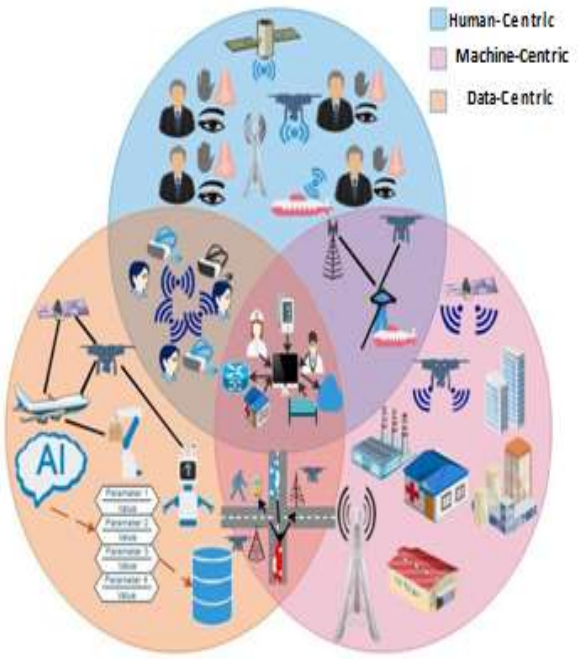

Figure 1. 6G Applications.

Human Bond Communication: This application improves human-machine dialogue by using all five senses to be more expressive, realistic, and rich. This software must be safe because it sends private data..

Multi-sensory eXtended Reality Applications: XR apps combine user, gesture, environmental, and other data to create immersive experiences. Data security is needed for this app because a disastrous data attack could harm user experience.

Large-scale connected autonomous systems: Implantable devices, wearable gear, and BCI technology must be reliable to send and receive data. Existing 5G systems can't capitalize on non-healthcare prospects.

Greater Support for Vertical Domains: Self-driving automobiles, drone swarms, vehicle platoons, and autonomous robotics can utilise 6G. 5G network separation may work for some uses, but not for those that need all three service classes.

6G Application Requirements

Manufacturing, energy, health, and technology companies develop and sell similar products. KPIs for main and secondary QoS measures vary by 3GPP. Vertical businesses will have more devices to link than 5G mMTC can manage.

To demonstrate blockchain's value, we divided 6G

application needs into two groups. The first group includes all-time wireless communication device needs. Ultra-reliability, minimal latency, fast data rates, and a large connection are typical. These are "Requirement-Group-I". For 6G networks, RG-I numbers must increase by many orders of magnitude. Privacy, secrecy, data integrity, non-lying, and auditability are included. Requirement Group II covers security standards. 6G apps must process and exploit massive amounts of data from human senses and organs and self-driving cars.

Much 6G vision research focuses on RG-I value-boosting techniques. THz transmission, RIS [1, 2, 4], and AI [3, 12] are key 6G technologies. We believe these new technologies and network architectures will allow 6G communication systems to link many devices fast, reliably, and over-the-air. RG-II is rarely mentioned in 6G publications. Many factors cause this. Operators, equipment, and tools are varied, hence their security needs vary with application, making it difficult to address them. The complex variety of applications and use scenarios for future 6G apps makes RG-II value fixing difficult.

3.BLOCKCHAIN AND 6G

First, blockchain, then RG-I and RG-II's 6G and blockchain concepts.

Blockchain

Blockchain stores data blocks in a shared list. Blockchain combines network, consensus, and automation. These technologies must be carefully selected to provide the right security characteristics for the application. The number of blockchain construction methods expands with its uses. Blockchains can be public, consortium, or administratively secret. Since the public blockchain is open, any node can join, leave, read, or write. One corporation writes to a private blockchain, whereas a coalition writes to a consortium blockchain. PoW algorithms offer the maximum data immutability, but they are difficult to employ on low-resource nodes. To make PoS variants like dPoS safer, add extra verifiers to the network to slow down communication and agreement. Smart contracts define who does what and allow peers move assets automatically under particular conditions.

Blockchain and 6G RG-I

Three-dimensional 6G infrastructure will meet RG-I goals. This gear and asset will be difficult to manage. Models for shared airwaves, storage, and computation will also get more complicated. AI is essential to optimize resources. Taking care of trained models will get harder. Resource and AI management benefit from blockchain's safety and distrust.

Resource Management Solutions: 6G apps require lots of spectrum, computer power, and infrastructure.

Spectrum Management: Data rate grows with bandwidth. Sharing spectrum can help 6G apps handle high data rates. Blockchain-based smart contracts with various terms and conditions allow licensed and unlicensed spectrum users in any band to maximize spectrum utilisation. The bandwidth sharing in [13] can be exploited for 5G. A user requests bandwidth, and the principal operator (the operator with the user's registration information) examines its resources. If not, it look for extra

Table 1 : AI model parameters and blockchain-based RG-I resource management are employed in 6G apps.

Category	Sub-Category	Description	Blockchain Based Solution
Resource Management Solutions)	Spectrum Management	Spectrum owners can coordinate with each other to provide spectrum resources for high data rates	Spectrum usage information can be stored on blockchain
	Infrastructure & Asset Management	6D communication infrastructure is mobile, dense and diverse with complex ownership models. Its management is a challenging task for one entity	Infrastructure location, ownership information, usage information, maintenance requirements, and useful life data can be stored on blockchain
	Computing Power & Data Storage Management	Un-utilized computing power or storage space anywhere in the network can shared to reduce battery drainage, decrease task latency, balance resources, and improve performance	Computing power and data space shared information can be stored on blockchain
AI Model Parameter Management	AI	AI models can be trained for complex operational and environmental optimization tasks	Hard trained AI model parameters are securely stored on and retrieved from blockchain

operator regarding resource supply. The secondary operator delivers the primary operator a SLA and spectrum rights when the primary operator verifies the user's details. The blockchain is updated after an authorized node confirms the

transaction. This consortium blockchain and consensus method configuration is safer for 6G. A transaction with operator and user IDs and frequency use start and end timings is added to the network-verified block with this new framework. After verification, the spectrum sharing transaction block is put to the blockchain.

Infrastructure & Asset Management: RG-I targets require many operators or SASPs to deploy communication drones, HAPs, and submarines in all three directions. Using all resources efficiently will protect 6G users' quality of service and boost network and SASP revenue. Finding the optimal SASP communication nodes to reduce latency shows blockchain's value. Registered users will search for the nearest communication nodes in a blockchain-based infrastructure and asset management system. After the blockchain verifies user and network registration information, relays link based on smart contract SLAs. A consensus algorithm adds the transaction to the blockchain after verifying it.

Computing Power & Data Storage Management: Many 6G apps demand sensor and terminal data. For realistic XR experiences, thousands or millions of small sensors may be needed. This data requires a lot of processing power to become valuable, rich knowledge. Such heavy programs will consume mobile devices' batteries and storage, and even if battery technology advances, these features may not fulfill future needs. Verified users could use a public blockchain for compute and storage. As in a double auction, persons who need computing power or storage space submit requests (with price and resources) and those with resources submit bids. Every round, bids and offers are compared to set the market closing price. Smart contracts automate double auctions. New transaction blocks are authorized by consensus and added to the blockchain.

AI Model Parameter Management Solutions: AI makes 6G networks smarter about operations and the globe. Network densification, unique RIS-based channel models, conflicting goals, and many factors make 6G network optimization NP-hard. Deep learning will replace classical optimization for dynamic operating and environmental network resource optimization. AI models are fast and powerful, but learning is difficult. Blockchain can protect hard-to-find AI model training parameters.

4.BLOCKCHAIN AND 6G RG-II

Data security, non-repudiation, and auditability are defined. These new security features are needed for 6G applications.

Data Integrity: Data security detects unauthorized data alterations. By modifying data, data integrity concerns harm communication systems. Data integrity issues could compromise vertical domain and LS-CAS control systems.

Non-repudiation: Non-repudiation proves an action occurred even if network parts aren't working. We expect most 6G machine-type nodes to act like humans as AI spreads. Non-repudiation is needed for many 6G uses.

Auditability: Auditability involves reconstructing an event or action from historical records. To determine who is responsible for issues, conflicts, or business and financial interests, many LS-CAS decision-making systems must be auditable.

We examine 4G and 5G security options to learn how blockchain can help 6G RG-II application goals using these standards. Many authentication tools in older communication systems use symmetric-key cryptography, which encrypts and decrypts data with the same key. Many 4G data networks use AKA and EAP frameworks. EAP verifies identity with the eNodeB and authentication server, while AKA uses challenge-and-response authentication. In contrast, 5G communication uses more secure asymmetric PKI-based cryptography. No data security is possible in 4G communications. 5G communication devices need to protect the integrity of data at the air interface. Because it takes a lot of resources, 5G's fastest integrity-protected data rate is 64kbps. Because 4G uses symmetric key encryption, it doesn't have non-repudiation. 5G, on the other hand, uses PKI-based cryptography. 4G and 5G transmission technologies don't make it easy to check the data

they send.

Blockchain technology in 6G would help RG-II goals and keep them in check. With the right network, consensus, and automation tools, blockchain can make sure that data is correct, can't be changed, and can be checked. For better data privacy and security with blockchain, asymmetric PKI-based encryption and privacy protection systems are used. New blocks are only accepted after they have been approved by a consensus process that involves many P2P hubs. Each block is linked to its parent block (the block before it in the chain) by a cryptography hash function. This lets data be checked and audited all the way back to the genesis block. Hash trees make it easy to check the accuracy of block data. As the blockchain grows, it gets harder to change data because all of the activities are linked together. Also, 5G uses the most advanced security technology in real data networks. The 128-NIA1 5G encryption method is 128 bits strong, the same as AES 128. For data proof, blockchain uses data that has been encrypted. The number of the block is passed on to the next block to store data. To protect privacy, 5G uses ECIES. The International Mobile Subscriber Identity (IMSI) of the user is encrypted many times to make unique IDs. Because each transaction on blockchain has its own unique key pair, transactions can't be linked together, so users stay anonymous. The control plane for 5G is made up of SDN and NFV. It is clear that availability is linked to a risk. Blockchain is less controlled and easier to use.

5.CASE STUDY AND SIMULATION RESULTS

Type and consensus approaches might easily meet the RG-II requirements of 6G applications. As a result, merging blockchain and 6G has the potential to provide ubiquitous and secure communication. In this section, we present a case study to demonstrate how integrating blockchain with 6G can result in a fast and secure communication solution. We will look at an LS-CAS example, which is a machine- and data-centric application in which a considerable amount of essential data is created and transferred autonomously among autonomous nodes. Such applications have previously been examined by 4G and 5G communication technologies. However, we will demonstrate that combining blockchain with 4G or 5G would not yield the same degree of synergy as combining blockchain with 6G. This is because the heightened security features of blockchain necessitate resource-intensive consensus methods and cutting-edge communication networks. When 6G speeds are combined with blockchain security, we achieve the intended effect of genuinely rapid and secure communication.

LS-CAS Scenario

In our LS-CAS scenario, the User Equipments (UE) and Road Side Units (RSU) are autonomous autos and delivery drones. Some RSUs may be installed on drones, while others may be immobile. This program supports user equipment to user equipment, user equipment to infrastructure, and infrastructure to infrastructure communications. UEs and RSUs work together to form a large wirelessly networked distributed autonomous system. We anticipate that UEs will be equipped with a range of sensors and cutting-edge camera systems. Real-time navigational assistance, position data, infotainment, RSU reputation data, sensor readings, and any other data essential to UE safety, transit, or entertainment requirements may be produced by UEs. This data should be distributed across the network as quickly as possible while maintaining data integrity, which is critical for a variety of reasons, including safe navigation. In a scenario where our system is being attacked by hostile actors (RSUs and collaborating automobiles) inside the network who can alter data to their benefit, we need a mechanism to detect data tampering as well as identify malicious actors. Because of the blockchain and its capabilities, such data integrity issues and rogue actors can now be easily discovered.

Secure Enhanced dPoS Algorithm for LS-CAS

We consider a blockchain-based configuration such as [8]. A multitude of precautions and a secure and upgraded dPoS algorithm protect the

shared data on this blockchain. The resources required to create and store the blockchain are assumed to be contained in RSUs. The RSUs mine blocks utilizing a dPoS consensus process and data supplied by the UEs. We think that RSUs can be tainted and are hence untrustworthy. Some UEs may also collaborate with the harmed RSUs. As a result, miner reputations are updated following a successful round of data exchange and the uploading of the record to the blockchain. In the next paragraphs, we will go over one cycle of block creation and reputation modifications. This process is also depicted in Figure 2.

The stakeholders (vehicles/drones) first vote to determine active and standby miners based on reputation scores. Active miners are a set number of miners with the highest reputation among all miners who take turns acting as block managers for the subsequent rounds. Real-time data is distributed across UEs, and the data sharing record is delivered to the nearest accessible RSU. Furthermore, UEs report their most recent reputation scores to the nearest RSU. RSUs send this information to the block manager for that round.

Active and standby miners are classified into numerous categories according on their reputation rankings. The block manager produces a smart contract for each kind and broadcasts it together with the other smart contracts. Smart contracts are designed to be beneficial just to the verifier who tries the specific smart contract. Before returning the block to the block manager, the neighborhood in the area examines the results of the check.

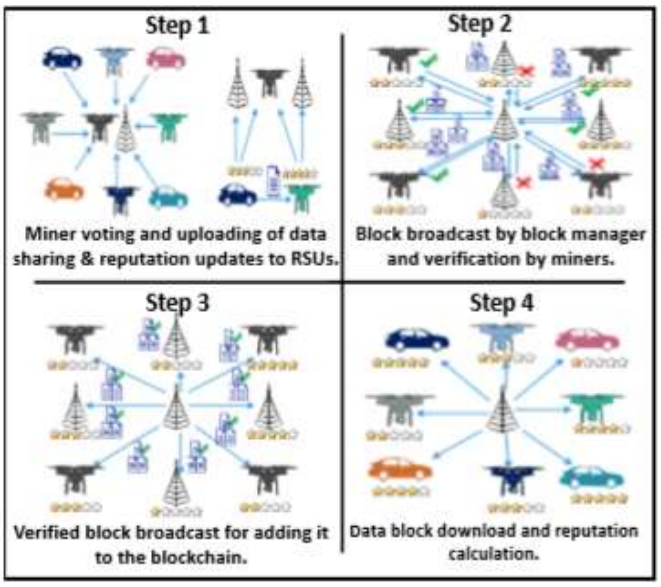

Figure 2. For the LS-CAS application, dPoS and reputation on a blockchain are being implemented.

The block manager constructs a new data block using a 2/3 majority consensus after receiving the verification reports. Once consensus is reached, the block manager broadcasts a new block, which the RSUs incorporate into their local blockchain copy.

The UEs download the most recent data block from the nearest RSU, verify the legitimacy of their previous transactions, and accordingly update the RSU's reputation score for the future round.

This dPoS system has a number of safeguards that allow for the detection of malicious actors and collusion attacks. However, it is evident that the time required to complete numerous tasks in each round has a major impact on whether or not malicious activity can be identified. The latency of multiple phases in each round can be classified using transmission latency, processing latency, and information diffusion delay. Because of the availability of reasonably fast processors in vehicles and RSUs, the time required for one round of this step will depend on network speeds and network scale.

The role of Communication Network

We run several simulations to show how 4G, 5G, and 6G communication networks work. We chose a 150 km2 area for the purposes of these simulations. RSUs are dispersed evenly over the network, and UE places are assigned at random.

RSU locations and range are determined based on network deployment density. Weights of 0.4 and 0.6 are assigned to positive and negative interactions, respectively. The probability of successfully transmitting a message is 0.7. This is the source of these parameters. The adjustment factor for the number of hops is set to 0.75. The reputation ratings are calculated using the multi-weight subjective logic (MWSL) approach [8]. Small-scale, medium-scale, large-scale, and very-large-scale networks are all considered. Many simulation-related factors (such as the average number of hops to the block manager, the types of verifiers, and the number of RSUs holding UE data) are adjusted depending on the network scale. In these simulations, we consider a scenario in which a miner engages in hazardous activity after 20 rounds. To achieve high reputation scores, the malicious miner collaborates with 25%, 33%, and 50% of the UEs. We consider the blockchain-based system's ability to detect malicious miners in 4G, 5G, and 6G networks. Table II lists the key simulation parameters. Figure 3 depicts the time required to identify a rogue miner for various network sizes (4G/5G/6G) and attack scenarios. As the network grows in size, the time required to discover malicious miners grows. When we increase the fraction of collaborating UEs for the same network size, the time required to discover a rogue miner increases as well. At 50% collusion, the performance of the 4G network is only adequate in small and medium-scale networks, where it can identify the rogue miner in 15 and 340 seconds, respectively. At 50% collusion, it takes a 5G network 681s and 1826s to find a rogue miner in large and very large scale networks, respectively. In large and very-large scale networks, a 6G network can detect a rogue miner at 50% collusion in approximately 25 and 53 seconds, respectively.

Table 2 THE PARAMETERS' VALUES

Parameter	Small-Scale Network	Medium-Scale Network	Large-Scale Network	Very-Large-Scale Network
Total number of active and standby miners	100	1000	10000	20000
Total number of vehicular and drone users	100	1000	10000	20000
Vote Size	1KB	10KB	100KB	200KB
UEs and RSUs download and upload speeds	10Mbps(4G), 500Mbps(5G), 100Gbps(6G)	10Mbps(4G), 500Mbps(5G), 100Gbps(6G)	10Mbps(4G), 500Mbps(5G), 100Gbps(6G)	10Mbps(4G), 500Mbps(5G), 100Gbps(6G)
Data block size before verification	10KB	100KB	5MB	10MB
Reputation block size before verification	1.5KB	15KB	150KB	300KB
Size of smart contract	2KB	15KB	150KB	200KB
Types of Verifiers	10	10	10	10
Number of active miners	15	41	199	255
Number of RSUs with UE data record	[10, 40]	[100, 400]	[1000, 4000]	[1500, 6000]
Maximum end to end number of hops	8	23	71	100

We investigate an adversary who behaves honorably for 20 contacts before engaging in malevolent and honorable behavior for 15 and 5 encounters, respectively, to better understand the role of blockchain in this scenario. We use blockchains with the MWSL model in addition to blockchains with beta and sigmoid reputation models.

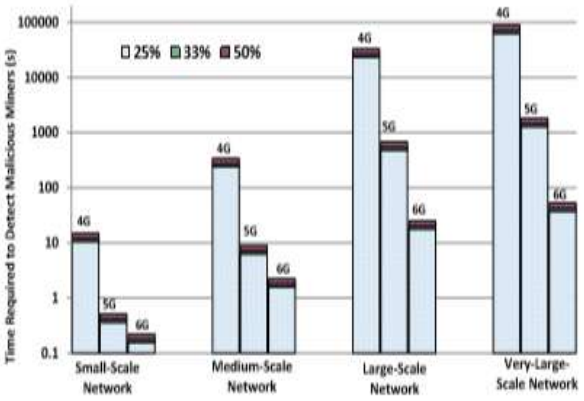

Figure 3. Time required to detect a malicious miner at various collusion rates and network sizes.

In the beta reputation model, the beta probability density function is used to aggregate feedback and derive reputation. The overall influence of both honest and malicious activities is used to calculate reputation as a sigmoid function in a sigmoid model. Using the relevant criteria and accounting for 33% network cooperation, we determine that some blockchains can detect rogue miners while others cannot, as illustrated in Figure. Using 6G will not help in certain situations. According to

the 6G delay data, employing 6G in conjunction with the appropriate blockchain model provides for the quickest detection of rogue miners. This study shows that in LS-CAS, careful blockchain structure selection is necessary for detecting dangerous behavior and, as a result, improving system integrity. Along with blockchain, 6G is the best technology for enabling quick detection. In this aspect, the two technologies will be a perfect match for the LS-CAS application.

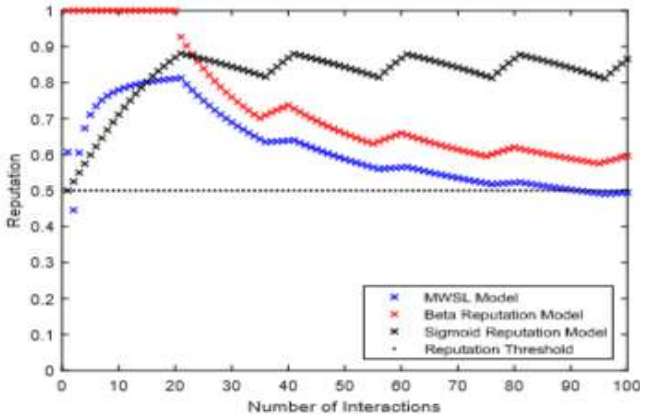

Figure 4. Several reputation schemes' sensitivity has been upgraded.

These simulation results are very encouraging, indicating that integrating more secure blockchain systems in 6G is achievable since they complement one another. While 6G enables the implementation of these applications because to its faster speeds, secure consensus mechanisms improve the security of 6G apps. RG-More secure blockchain implementations would benefit me by preventing essential resources deployed under intricate ownership and sharing models from being underutilized as a result of the advent of a trustless environment in 6G. Additional research in the following areas would be required to overcome some difficulties with expanded blockchain deployments in 6G:

In highly large blockchain networks, sharding and sub-blockchain techniques may be employed to reduce convergence times even further.

To lower consensus latency and block size, smart contract optimization techniques are required. Smart contracts should be built with care to make them less vulnerable to hacking.

Larger network sizes necessitate more storage. There is an evident need for consensus algorithms that use fewer resources while maintaining security. Off-chain storage is an option, and the block's signature can be stored on the chain.

6.CONCLUSION

In this post, we discussed the possibilities of blockchain and 6G for future communication and discovered a link between them. We divided 6G application demands into performance-related (RG-I) and security-related (RG-II) groups to make the synergy more opaque. We proved that the trustless feature of blockchain would make it easier to manage and audit 3D network resources and AI model parameters in 6G networks with complex ownership structures. The flexible use of increasingly enormous and sophisticated network resources in 6G with the use of blockchain will considerably benefit RG-I goals. Furthermore, by carefully selecting blockchain

REFERENCES

1. W. Saad, M. Bennis, and M. Chen, “A vision of 6G wireless systems: Applications, trends, technologies, and open research problems,” IEEE Network, vol. 34, no. 3, pp. 134–142, 2019.
2. F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, “A speculative study on 6G,” IEEE Wireless Communica- tions, vol. 27, no. 4, pp. 118–125, 2020.
3. M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, “To- ward 6G networks: Use cases and technologies,” IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, 2020.
4. S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, “What should 6G be?” Nature Electronics, vol. 3, no. 1, pp. 20–29, 2020.
5. X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang,
6. C. Zhang, Y. Jiang, J. Wang et al., “Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts,” Science China Information Sciences, vol. 64, no. 1, pp. 1–74, 2021.
7. M. Sadek Ferdous, M. Jabed Morshed

Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," arXiv preprint arXiv:2001.07091, 2020.

8. N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," IEEE Industrial Electronics Magazine, vol. 13, no. 4, pp. 106–118, 2019.
9. J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906–2920, 2019.
10. H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.