Journal of Nonlinear Analysis and Optimization
Vol. 14, Issue. 01 : 2023
ISSN : **1906-9685**

BLOCKCHAIN AND 6G: THE FUTURE OF SECURE AND UBIQUITOUS COMMUNICATION

[#1]BURLA SRINIVAS~~Dr. T. NARAYANAN~~, ***Professor,***

Department of Computer Science and Engineering

[#2]K~~ADICHERLA RAMESHISHOR KUMAR GAJULA~~, ***Assistant Professor,***

Department of Computer Science and Engineering,

MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.

ABSTRACT: The future of communication is safe and reliable. The functionality of futuristic apps depends on a few key features. This research classifies these application needs into two key groups to show how blockchain and 6G may impact future communication systems. Data rates, latency, dependability, and the ability to handle a huge connection capacity are the primary concerns of Requirement Group I (RG-I). Data integrity, non-repudiability, and auditability are the main concerns of Requirement Group II (RG-II). By decentralizing and making resource sharing easier, blockchain and 6G technology would help achieve RG-I's goals and reduce wasteful overuse of assets. The RG-II requirements can be easily met by 6G applications using appropriate blockchain and consensus technology. This research suggests that in the future, dependable and broad connectivity can be achieved through the integration of blockchain technology and 6G.

Keywords: *Blockchain, RG-I,6G Technology.*

1.INTRODUCTION

6G vision papers are being written as the commercial viability of 5G grows. The results of these studies suggest that HBC (haptic-based communication), XR (extended reality), WTech (wireless technology), LS-CAS (low-latency communication and sensing), and improved support for vertical domains are all crucial components of 6G services and applications. Large amounts of data must be sent and received reliably and on time by these apps. Someone with ties to LUMS's Electrical Engineering program. I. Hassan; U. It comes to 54792. Their email accounts, 18060048@lums.edu.pk and naveed.hassan@lums.edu.pk, can be used to reach them. A single "C" represents the user's input. Yuen is a part of a 2,000-person team as an Engineer Product Developer at SUTD. Singapore 487372 is the location of the business at 8 Somapah Road. The user's input is a single letter, "J." He lives in Singapore and works at the Nanyang Technological University School of Computer Science and Engineering. If you need to get in touch with me, my email is yuenchau@sutd.edu.sg. The address for Junzhao's email is dniyato@ntu.edu.sg. Zhang is currently working as an employee at Oslo University's Informatics Department in Oslo, Norway 0315. Feel free to email me at yanzhang@ifi.uio.no.H. V. Poor works in the 08544 area as a member of the faculty in the Department of Electrical and Computer Engineering at Princeton University. In the

United States, use Poor@princeton.edu as your email address. The LUMS Faculty Initiative Fund provided the bulk of the funding for this endeavor. The RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund - Pre Positioning from A*STAR, the Singapore Ministry of Education Tier 1 (RG16/20), and the National Science Foundation all contributed to the funding of this study. The views, observations, inferences, and recommendations presented here may not reflect those of A*STAR. For permission to use it in other ways, please email pubs-permissions@ieee.org. More stringent data security measures are required because 6G application data is becoming increasingly sensitive and vital. Block chain technology creates a chain of data blocks using cryptographic hash functions and consensus mechanisms for their integrity. Blockchain technology may be key in bringing 6G to fruition. Reconfigurable Intelligent Surfaces (RIS), TeraHertz (THz) connection, artificial intelligence (AI), and micro cell networks are all needed for these applications. When trust is low, people need to work together to make the most of these tools and reach their performance goals. Complexity in infrastructure and networking is introduced by the vast network settings needed for these technologies. The dispersion of a network calls for decentralization. Blockchain facilitates trustworthy and open distributed ledgers. Blockchain's intrinsic security features make it a viable solution for the evolving needs of secure data networks.

The necessary components of the blockchain can modify the blockchain's decentralization, security, and scalability to meet the needs of a certain application. When it comes to the status of a blockchain network, all nodes must be in complete agreement for consensus to be reached. Data on a blockchain can be verified, protected, and verified using consensus procedures. The degree to which a system can be decentralized and expanded depends on how well its information networks function. While Proof of Work (PoW) helps with power distribution and scaling to accommodate more transactions, it has no bearing on network throughput. Rapid convergence is made possible by the combination of 6G and other communication-heavy technologies, such as PBFT. We have divided the needs of 6G apps into two categories to make blockchain integration with 6G easier. Data rates, latency, reliability, and other network-related needs are all part of Requirement Group I (RG-I). These efficiency standards promote global interaction. RG-II's security guidelines prioritize the non-repudiation, auditability, and integrity of data. The most important takeaways from this research are as follows:

The 6G program's schedule is set. In terms of security, not all measures are created equal.

Multiple use cases are being considered for Bitcoin and 6G. Since it is decentralized, blockchain technology guarantees honesty and safety, which benefits both sides.

In the realm of blockchain-based work, LS-CAS scenarios are in use. A time estimate is made for finding malicious miners in a blockchain network. Computer simulations show that both Blockchain and 6G technologies may be used to track down and ban malicious miners.

2.6G APPLICATIONS AND THEIR REQUIREMENTS

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

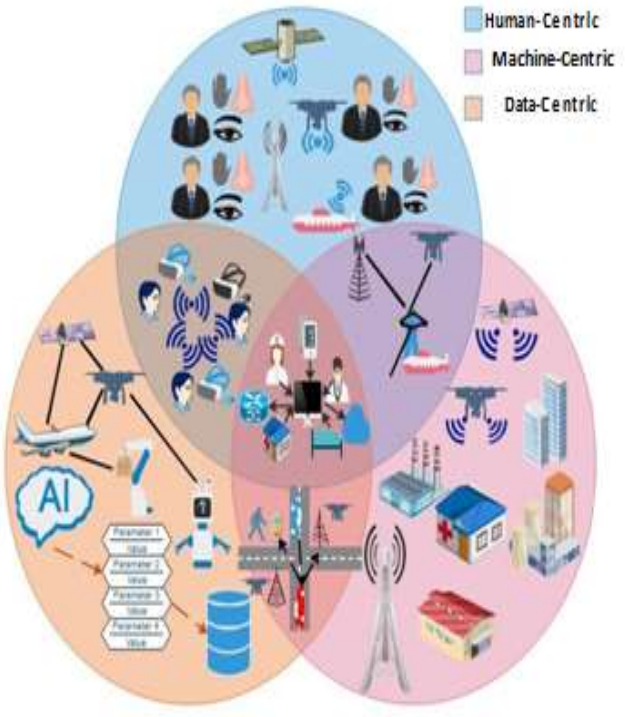

Figure1. 6GApplications.

Human Bond Communication:

This program uses all of a person's senses to make human-machine communication more nuanced, expressive, and realistic. Due to the sensitive nature of the data being transmitted, the software in question must be extremely secure.

Multi-sensory ~~eXtended~~extended Reality Applications: XR

By combining information about the user with data about their surroundings, apps create immersive experiences. This application requires data protection because of the possible impact of a catastrophic data attack on the user experience.

Large-scale connected ~~autonomous~~autonomous systems:

High reliability in data transmission and reception is essential for implantable devices, pervasive technology, and BCI technologies. Opportunities outside of healthcare cannot be completely realized with current 5G technologies.

Greater Support for Vertical Domains:

6G's capabilities can be put to use by autonomous vehicles, drone swarms, vehicle platoons, and robots that operate without human input. However, network segmentation will not be useful for all 5G applications because some of them require the use of all three types of service.

6G Application Requirements

Similar products and services are offered by businesses in the manufacturing, energy, healthcare, and technology sectors. Both primary and secondary Quality of Service (QoS) metrics are given their own unique Key Performance Indicators (KPIs) inside the 3rd Generation Partnership Project (3GPP). More device connections are needed in vertical companies than 5G m MTC can provide.

We divided the needs of 6G applications into two categories to demonstrate the value of blockchain. In the first group, we have all the specs needed for various forms of wireless communication gear. The network has many connections, high data transmission speeds, low latency, and high reliability. The "Requirement-Group-I" includes these specific stipulations. For 6G networks, RG-I values must be scaled up by several orders of magnitude. Privacy, secrecy, honesty, veracity, and the capacity to conduct an audit are all included. The criteria for safety are included in Requirement Group II. Large volumes of data generated by human senses, organs, and self-driving vehicles necessitate the use of 6G apps for collection and processing.

6G vision research focuses mostly on methods to increase the RG-I value. Within the 6G framework, core technologies include terahertz (THz) transmission, reconfigurable intelligent surfaces (RIS), and artificial intelligence (AI). We believe that these new technologies and network architectures will make it possible for 6G communication networks to quickly, reliably, and wirelessly link a large number of devices. The RG-II standard is rarely mentioned in 6G writing. This occurred due to a number of elements coming together. The diverse needs of workers, machines, and tools make it difficult to centrally manage their security. Challenges in modifying the value of RG-II arise from the complexity of future 6G application and usage situations.

3.BLOCKCHAINAND6G

The blockchain concept comes first, followed by the development of 6G technology. Additional blockchain-based ideas include RG-I and RG-II.

Blockchain

The blockchain stores blocks of information in a decentralized ledger. ——Blockchain is a break through in technology because it combines previously separate areas of study in network, consensus, and automation. Careful selection of these technologies is required to guarantee that the application has the required security features. As the number of applications for blockchain technology grows, so does the variety of methods for creating and implementing the technology. Public, private, and invitation-only blockchains are the three main categories of blockchain accessibility. ——The distributed ledger's open architecture makes it possible for any node to join, leave, get access to, or contribute information. Two different companies are using blockchain

technology, one in a consortium and the other in a private setting.—— Despite providing the highest level of data immutability, Proof of Work (PoW) systems present difficulties when implemented on nodes with limited resources.—— Increasing the number of network verifiers is recommended to increase the security of PoS variants like dPoS by slowing down the rate of communication and consensus. When predetermined circumstances are met, assets can be automatically transferred between peers using smart contracts that establish the respective roles and obligations of those involved.

Category	Sub-Category	Description	Blockchain Based Solution
Resource Management Solutions)	Spectrum Management	Spectrum owners can coordinate with each other to provide spectrum resource for high data rates	Spectrum usage information can be stored on blockchain
	Infrastructure & Asset Management	3D 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

Blockchain and 6G RG-I

Implementing a 3D 6G infrastructure is crucial to realizing the RG-I goals. It will be difficult to keep track of this asset and gadget. Models for sharing resources like bandwidth, storage space, and processing power will become more complex. To maximize efficiency, you need artificial intelligence. Keeping up with trained models will be harder than ever. Blockchain's trustworthiness and safety improves the management of assets and AI.

Resource Management Solutions:

Spectrum, computing power, and infrastructure are all in high demand for 6G applications.

Spectrum Management:

As bandwidth grows, so does the rate at which data may be transferred. Spectrum sharing allows 6G applications to support high data rates. Licensed and unlicensed users alike can utilize smart contracts on the blockchain to keep up with the changing terms and conditions of spectrum use so that they can maximize efficiency across all frequency bands. The idea of sharing bandwidth, which is addressed in reference , can be used to 5G networks. The chief operator (the one with access to the user's registration information) evaluates the availability of bandwidth when a user makes a request. Otherwise, it will inquire for more information.

Table 1 demonstrates how 6G apps utilize AI model parameters and RG-I resource management built on the blockchain.

The manager is responsible for providing the necessary materials. After the first operator verifies the user's information, the secondary operator offers a SLA and gives the primary operator access to the spectrum. After a validating node confirms a transaction, the ledger is updated. This consortium blockchain and consensus mechanism configuration improves 6G security. The modified system inserts a transaction into the validated network block that comprises operator and user IDs and the beginning and ending times of frequency usage. The spectrum-sharing transaction block is added to the blockchain after verification.

Infrastructure & Asset Management:

There must be a large number of operators or SASPs to launch communication drones, HAPs, and submarines in all three cardinal directions for RG-I targets. Safeguarding 6G service quality while improving network performance and SASP revenue requires optimal utilization of all available resources. The benefits of blockchain technology may be seen in the process of determining the best SASP connection nodes in order to reduce latency. In order to find the closest connection nodes, users of a blockchain-based infrastructure and asset management system will do a location search. The blockchain then initiates the connection based on the SLAs in the smart contract, after verifying the user and network registration details. The transaction is added to the blockchain once the confirmation is received via a consensus process.

Computing Power & Data Storage Management:

Data from terminals and sensors is essential for many 6G uses. Thousands or even millions of small sensors may be required for really immersive XR experiences. It takes a lot of computing power to turn this information into useful knowledge. Batteries and storage space on mobile devices will be quickly depleted by these kinds of intensive programs. Battery technology has come a long way, but whether or not it will be able to keep up with expected demand remains to be seen. Calculations and data storage can be done on a blockchain by anyone with a valid identity. Requests for computing power or data storage space are posted by those in need and include details like cost and availability, while offers to sell said capacities are posted by those in possession. The market closes at the end of each round after bids and offers are evaluated. Auctions that are held too often are routinely automated using smart contracts. After being approved by the network as a whole, new transaction blocks are added to the ledger.

AI Model Parameter Management Solutions:

Terminal and sensor data are both essential for many 6G applications. Thousands or even millions of small sensors may be required for really immersive XR experiences. It takes a lot of computing power to turn this information into useful knowledge. Batteries and storage space on mobile devices will be quickly depleted by these kinds of intensive programs. It is unclear if present capabilities will be sufficient to fulfill future demands, even with developments in battery technology. Users with confirmed identities can perform computations and store data safely in a distributed ledger called a blockchain. Those in need of computing power or data storage space put in requests, outlining their needs along with pricing and availability information, while those with surplus capacity put in proposals. The closing price of the market is determined after each round of bidding and offering. Auctions that are held too often are routinely automated using smart contracts. Once consensus has been reached, additional transaction blocks are added to the blockchain.

4.BLOCKCHAIN AND 6GRG-II

Safekeeping of information, non-repudiation, and auditability are all well-established principles. The successful operation of 6G apps depends on the widespread adoption of these heightened security measures.

Data Integrity:

The purpose of data security is to identify instances of information tampering. Threats to the accuracy of the data transmitted via a network can disrupt those networks. Control systems in the vertical domain and the LS-CAS are vulnerable to data integrity difficulties.

Non-repudiation:

Non-repudiation guarantees that an action's occurrence can be verified, regardless of the health of the underlying network infrastructure. Most machine-type 6G terminals are expected to behave like humans due to the proliferation of AI. Nonrepudiation is crucial for many uses in the 6G era.

Auditability:

Reconstructing a past event or action from documentation is what we mean when we talk about auditability. Many LS-CAS decision-making systems require audits to determine who is responsible for problems, conflicts, or financial entanglements.

We investigate the possibility of blockchain technology using 4G and 5G network security alternatives to help realize the aims of 6G RG-II applications. Symmetric-key cryptography, in which the same key is used for both encryption and decryption, was widely used for authentication in earlier communication systems. The AKA and EAP protocols are used by a number of different 4G data networks. AKA uses challenge-and-response authentication, while EAP uses an eNodeB and an authentication server. In contrast, asymmetric PKI-based cryptography is used in 5G connections, making them extremely secure. In 4G communications, data security cannot be guaranteed. Data integrity at the air

interface is a crucial requirement for 5G communications devices. Due to its resource-intensive nature, 5G's maximum data rate with integrity protection is capped at 64 kbps. Since 4G relies on symmetric key encryption, non-repudiation is impossible. 5G, on the other hand, makes use of cryptography based on the Public Key Infrastructure (PKI). It is difficult to verify the information offered by 4G and 5G networks.

The implementation of RG-II goals would be supervised and facilitated using 6G blockchain technology. Blockchain technology has the potential to ensure the truthfulness, immutability, and verifiability of data with the help of the right network, consensus mechanism, and automation tools. Blockchain uses encryption and privacy protection methods based on asymmetric PKI to improve the security and confidentiality of stored information. Only if a large number of peer-to-peer nodes have reached a consensus is a block added to the blockchain. In cryptography, a hash function links each block to the parent block that came before it in the chain. This allows for early evaluation and validation of data. In order to verify block data, hash trees are used. Due to the interrelated structure of all activities, altering data on the blockchain is becoming more and more difficult as it grows. Moreover, 5G makes use of the cutting-edge data network security tools available now. The 128-bit key size is shared by the AES 128 and 128-NIA1 5G algorithms for security. Blockchain uses encrypted information for its verification function. The next block receives the block number and uses it to store the data. Elliptic Curve Integrated Encryption Scheme (5G) is used to keep private information just that: private. Multiple rounds of encryption are applied to the user's International Mobile Subscriber Identity (IMSI) before it is used to generate new, unique identities. Each transaction in a blockchain has its own unique key pair, making it impossible to trace back to a specific user. In the context of 5G, the control plane relies heavily on SDN (Software-Defined Networking) and NFV (Network Functions Virtualization). Availability and risk go hand in hand. Reduced governmental interference and increased utility are two hallmarks of the blockchain.

5.CASE STUDYAND SIMULATION RESULTS

Type and consensus methods make it easy to meet the RG-II standards necessary for 6G applications. Secure and extensive communication is made possible by the combination of blockchain technology and 6G technology. Here, we give a case study showing how blockchain technology and 6G can work together to create a fast and secure means of communication. Let's take a look at LS-CAS, an application focused on machines and data that generates a lot of critical data and automatically distributes it over multiple nodes. Several previous studies have looked into the potential of 4G and 5G for a variety of applications. However, we will show that the synergy created by combining blockchain technology and 4G or 5G networks is not as great as that created by combining the two with 6G. Blockchain's increased security features necessitate the use of resource-intensive consensus processes and new communication networks. Fast and secure communication is achieved by combining 6G speeds with blockchain security.

LS-CAS Scenario

In our LS-CAS scenario, autonomous vehicles and delivery drones are examples of User Equipments (UE) and Road Side Units (RSU). While some Roadside Units (RSUs) are designed to be mounted on UAVs, others may be stationary. This program makes it easier for the infrastructure and user devices to talk to one another. When UEs and RSUs are combined, a massive distributed autonomous system is created across a wireless network. A plethora of sensors and cutting-edge cameras are expected to be included in UEs. For the sake of user equipment (UE) security, transportation, and entertainment, all relevant data, including real-time navigation aid, positioning data, infotainment, reputation data of Roadside Units (RSUs), sensor readings, and so on, are permitted. For many reasons, including navigational safety, it is critical that this information be transmitted quickly via the

network without compromising its integrity. It is crucial that we devise a method of detecting data tampering and identifying the malicious individuals involved if our system is to withstand attacks from adversarial entities (such as RSUs and collaborating automobiles) in the network with the potential to change data for their own profit. The blockchain's design makes it simple to identify malicious actors and problems with data integrity.

Secure_Enhanced_dPoS_Algorithm_for_LS-CAS

Check out the blockchain-based setup [8]. Multiple layers of security and a trustworthy, regularly updated delegated Proof of Stake (dPoS) algorithm keep information shared on this blockchain safe. To build and store the blockchain, RSUs must have access to the appropriate resources. To create blocks, RSUs rely on information provided by UEs and use a dPoS consensus procedure. We argue that the unreliability of RSUs is a direct outcome of their susceptibility to corruption. It's possible that some UEs will still work with the damaged RSUs. After a successful round of data exchange and record uploads to the blockchain, miners' reputations are updated. In the next sections, we'll go over how to make changes to your reputation and generate new blocks once. This procedure is shown in Figure 2 as well.

Autos and drones alike cast votes for active and inactive miners based on the reputations of the candidates. The most trustworthy miners are the active miners who take turns serving as the block administrator. As soon as the live data has been delivered to all UEs, the log of data exchange is forwarded to the next available RSU (Roadside Unit). Additionally, UEs communicate their current reputation scores to the nearest RSUs. The current round's block manager receives this data from RSUs.

Both active and inactive miners are sorted into several groups according to their reputation scores. The block manager creates an intelligent contract for each kind and releases them simultaneously. Smart contracts are designed to primarily benefit the verifier in charge of confirming that specific smart contract. The surrounding community reviews the inspection results before releasing the block to the block manager.

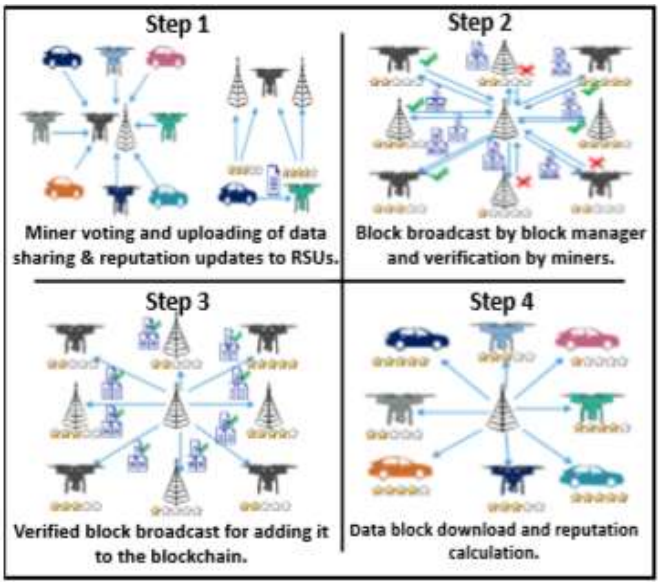

Figure 2 depicts how LS-CAS uses a blockchain to implement delegated Proof of Stake (dPoS) and reputation.

Once the block manager has received all of the verification reports, a new data block is built using a 2/3 majority consensus. Once agreement is obtained, the block manager sends a new block to the RSUs, which add it to their own personal blockchains.

The newest data block is obtained by the UEs from the RSU that is geographically nearest to them. After ensuring that their previous trades were legitimate, they update the RSU's reputation score for the next iteration.

Many methods for identifying bad actors and stopping collusion attempts are included into the dPoS architecture. However, it is clear that the capacity to identify fraud is significantly impacted by the time it takes to accomplish various activities in each cycle. Each iteration has multiple steps, and their respective latencies can be broken down into three broad classes: transmission latency, processing latency, and information dissemination delay. Since reasonably fast CPUs are already present in

vehicles and RSUs, the duration of this phase will be determined by the speed and scale of the network.

The role of Communication Network

The capabilities of 4G, 5G, and 6G networks are demonstrated through a series of simulations. The goals of these simulations were achieved using a 150 sq. km. region. RSUs are spread out evenly across the network, and UE placement is determined at random. The density of network deployments determines the optimal placement and coverage area for RSUs. Both positive and negative interactions are given equal importance, each with a weight of 0.40. There is a 70% chance that your message will reach its intended recipient. This is where certain traits were first developed. A value of 0.75 has been applied as the flights adjustment factor. Reputation scores are determined using the multi-weight subjective logic (MWSL) method [8]. We take into account networks of all sizes, from the smallest to the largest possible. Several simulation-related elements, such as the typical number of hops to the block manager, verifier categories, and the total number of RSUs transmitting UE data, are affected by network scalability. We examine a situation in which a miner engages in a potentially dangerous activity within these simulations after twenty iterations. In order to boost their reputation, the malicious miner uses 25%, 33%, and 50% of the UEs. The potential for a blockchain-based system to detect malicious miners in next-generation wireless networks is now under investigation. Figure 3 depicts the time required to detect a rogue miner across multiple network sizes (4G/5G/6G) and attack situations, while Table II provides essential simulation variables. The time needed to locate malicious miners grows proportionally with the size of the network. The time it takes to identify a malicious miner in a network of a given size grows proportionally with the number of UEs that are part of the network. With a 50% collusion rate, the 4G network is only effective enough for use in small to medium-sized networks. It takes only 15 and 340 seconds, respectively, to detect illegal miners in these networks. Within 681 ms in typical networks and 1826 ms in massive ones, a 5G network can detect a malicious miner participating in 50% collusion. A fraudulent miner who is in cahoots with 50 percent of the network can be exposed in 25 seconds in a 6G network. The same detection may be accomplished in as little as 53 seconds in extremely large networks.

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

In this research, we examine the actions of an adversary who starts off as honorable for 20 interactions, then acts dishonorably for 15 interactions, and finally reverts back to being honorable for 5 interactions. The goal is to learn more about the function and significance of blockchain technology in this setting. We use blockchains that implement a wide variety of reputation models, including MWSL, beta, and sigmoid.

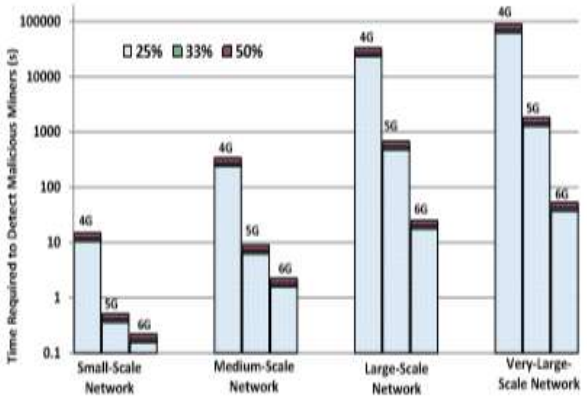

Figure 3.Time required to detect a malicious miner at various collusion rates and network sizes.

In the beta reputation paradigm, the beta probability density function is used to aggregate comments and calculate standing. A sigmoid model is used to calculate an individual's reputation, which factors in both positive and negative deeds. Based on the presented criteria and assuming a 33% network collaboration factor, it is clear that some blockchains can detect malicious miners while others cannot (Figure). There will be times when 6G proves ineffective. When combined with the right blockchain model, 6G's low latency makes it possible to quickly identify malicious miners. This research shows that careful selection of blockchain structure is necessary for LS-CAS to detect dangerous actions and improve security. 6G and blockchain are the best technology for enabling fast detection. In this regard, both systems will function admirably in an LS-CAS setting.

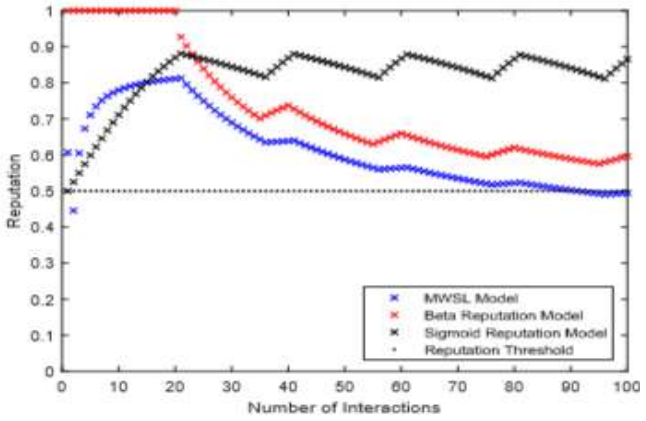

Figure4.Several reputation schemes' sensitivity has been upgraded.

These simulation results are very encouraging,

These simulation results show that more secure blockchain systems can be integrated with 6G networks. Safe consensus procedures improve the safety of these applications, while faster installation times make them easier to set up. With the advent of a trustless environment in 6G, the underutilization of valuable resources that are subject to complex ownership and sharing structures can be avoided by implementing more secure blockchain systems. The problems caused by the rapid expansion of blockchain implementations in 6G necessitate additional study in the following areas:

Convergence times in extremely large blockchain networks can be further decreased by employing sharding and sub-blockchain techniques.

In order to reduce the amount of time it takes to establish consensus and the overall size of each block, effective methods for optimizing smart contracts are required. The potential for harm linked with smart contracts must be carefully considered during their development.

When the capacity of a network increases, more storage space is required. It's obvious the need for safe consensus algorithms that consume fewer resources without compromising on security. The block signature can be stored on the blockchain, and data can also be stored off-chain.

6.CONCLUSION

In this article, we connected the dots between the future of blockchain technology and 6G wireless technology. To better understand the interplay, we classified the requirements for 6G applications into two categories: those concerned with performance (RG-I) and those concerned with security (RG-II). We showed how the trustless nature of blockchain makes it easy to manage and audit AI model parameters and 3D network resources in 6G networks with convoluted ownership structures. With blockchain, it will be much easier to harness the growing size and complexity of 6G networks to further RG-I goals. In addition, by selectively utilizing blockchain

REFERENCES

1. W. Saad, M. Bennis, and M. Chen, “A vision of 6G wireless systems:Applications, trends, technologies, and open research problems,” IEEENetwork,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 CommunicationsMagazine,vol.58,no.3,pp.55–61,2020.
4. S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, “What should 6Gbe? ”NatureElectronics,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
6. shifts,”Science China Information Sciences ,vol.64,no.1,pp.1–74,2021.
7. M.SadekFerdous, M.JabedMorshed Chowdhury, M.A.Hoque, and A. Colman, “Blockchain consensus algorithms: A survey,” arXivpreprintarXiv:2001.07091,2020.
8. N. U. Hassan, C. Yuen, and D. Niyato, “Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions,” IEEEIndustrialElectronicsMagazine,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: Asurvey,” IEEE Internet of Things Journal, vol.6 ,no.5,pp.8076–8094,2019.