ACCEPTED FROM OPEN CALL

Blockchain and 6G: The Future of Secure and Ubiquitous Communication

Ali Hussain Khan, Naveed UL Hassan, Chau Yuen, Jun Zhao, Dusit Niyato, Yan Zhang, and H. Vincent Poor

Abstract

Future communication will be characterized by ubiquitous connectivity and security. These features will be essential requirements for the efficient functioning of futuristic applications. In this article, in order to highlight the impact of blockchain and 6G on future communication systems, we categorize these application requirements into two broad groups. In the first category, called Requirement Group I (RG-I), we include the performance-related needs on data rates, latency, reliability and massive connectivity, while in the second category, called Requirement Group II (RG-II), we include the security-related needs on data integrity, non-repudiability, and auditability. With blockchain and 6G, network decentralization and resource sharing would minimize resource under-utilization, thereby facilitating RG-I targets. Furthermore, through appropriate selection of blockchain type and consensus algorithms, RG-II needs of 6G applications can also be readily addressed. Through this study, the combination of blockchain and 6G emerges as an elegant solution for secure and ubiquitous future communication.

Introduction

As 5G is approaching commercial readiness, 6G vision papers have started to appear in the literature [1–5]. These papers identify some key 6G applications and services such as Human Bond Communication (HBC), Multi-sensory eXtended Reality Applications (XR), Wearable Technology based Futuristic Applications (WTech), Large-scale connected autonomous systems (LS-CAS), and greater support for several vertical domains. These applications have very stringent requirements of data rate, latency and reliability. The nature of data collected by several 6G applications will be increasingly sensitive and critical. The successful adoption of 6G applications by the users would therefore require strict data security guarantees. Blockchain is a distributed ledger technology where cryptography and hash functions are used to form a chain of data blocks, created when an event occurs and verified in a decentralized way using consensus algorithms [6]. Blockchain, initially only used in cryptocurrencies, is now being used in other application domains such as smart grid, connected vehicles, and Internet of Things. [7–10].

Blockchain is believed to be a key technology in 6G applications [1, 2, 4]. The stringent network performance requirements of these applications will require support of technologies such as Reconfigurable Intelligent Surfaces (RIS), TeraHertz (THz) communication, Artificial Intelligence (AI) and small cell networks. To enable efficient combination of these technologies for the provision of resources to achieve the performance requirements, collaboration and coordination in a transparent and trustless environment is needed. These technologies also require dense network deployments which will lead to more infrastructure and complicated network deployment. Network decentralization will be needed to simplify the network deployment. Blockchain will provide the desired transparency and trustlessness in the decentralized network. Blockchain will also provide the strict security requirements of future communication systems because of its built-in security features.

Based on the application requirements, the decentralization, security and scalability of blockchain can be fine tuned by selection of appropriate blockchain components. Consensus is an important property in blockchain systems which ensures that all the nodes agree on the network state. By a careful consideration of consensus algorithms and protocols, blockchain can attain superior and diverse security features such as data integrity, non-repudiation, and auditability [7, 11]. Appropriate selection of a communication network can have an impact on the decentralization and scalability of the system. For example, if latency is not an issue but decentralization and scalability are required, Proof-of-Work (PoW) can be used. If the system is required to converge in a very short time, 6G can be used with communication-intensive mechanisms such as Practical Byzantine Fault Tolerance (PBFT).

We divide 6G application requirements into two broad categories with the objective of making the blockchain and 6G combination easier to understand. In the first category, called Requirement Group I (RG-I), we include the performance-related needs on data rates, latency, reliability and massive connectivity. These performance requirements will help enable ubiquitous communication. In the second category, called Requirement Group II (RG-II), we include the security-related needs on data integrity, non-repudiability, and auditability. The major contributions of this article are as follows:

Ali Hussain Khan and Naveed UL Hassan are with Lahore University of Management Sciences (LUMS); Chau Yuen is with Singapore University of Technology and Design (SUTD); Jun Zhao and Dusit Niyato are with Nanyang Technological University; Yan Zhang is with the University of Oslo; H. Vincent Poor is with Princeton University.

Digital Object Identifier:
10.1109/MWC.001.2100255

1536-1284/22/$25.00 © 2022 IEEE

- We identify the requirements for optimal performance of 6G applications. We divide these requirements into two groups based on traditional and security requirements.
- We discuss the combination of blockchain and 6G for these application requirements. The decentralization and trustlessness and the security features of blockchain will cater to both types of application requirements.
- We consider the blockchain employment in an LS-CAS scenario. We derive the time required to detect malicious miners in a blockchain system. By simulation results, we show that blockchain will help detect malicious miners and 6G will help accelerate this detection.

6G Applications and Their Requirements

In this section, we discuss some futuristic 6G applications as shown in Fig. 1 and discuss their requirements.

6G Applications

Human Bond Communication: This application is concerned with data from all five human senses to allow more expressive, realistic and holistic information exchange between humans and machines. This application would require strict security guarantees because a lot of intimate data would be transmitted.

Multi-Sensory eXtended Reality Applications: By combining information from human senses, human gestures, the surrounding environment, and multiple data sources, XR applications can provide a fully-immersive user experiences. Data integrity is required for this application because any data attack by a malicious entity could change the entire user experience.

Wearable Technology Based Futuristic Applications: Another key area is wearable technology (implantable sensors, wearable clothing, brain-computer-interface (BCI)), which requires ultra-reliability for reliable data exchange. Existing 5G systems fall short in leveraging the numerous potential opportunities beyond traditional healthcare scenarios.

Large-Scale Connected Autonomous Systems: Another area where 6G can find potential applications is connected robotics and autonomous systems, which include drone-delivery systems, autonomous cars, autonomous drone swarms, vehicle platoons, and autonomous robotics [1]. These applications simultaneously demand all three 5G service classes, and network slicing in 5G may not be the ideal way to achieve the requirements of such applications.

Greater Support for Vertical Domains: For vertical industries in which similar products or services are developed, produced, and provided (e.g., manufacturing, energy, health, automation), 3GPP has defined multiple key performance indicators (KPIs) for several core and secondary quality of service (QoS) parameters. 5G massive machine type communication (mMTC) will not be able to keep up with the increasing number of connected devices in vertical industries.

6G Application Requirements

We divide 6G application requirements into two broad categories with the objective of making it easier to understand blockchain utility. In the first category, we group those requirements that have always remained a major consideration in all the previous generations of wireless communication systems. These traditional requirements include ultra-reliability, low-latency, enhanced data rates, and massive connectivity. We refer to these as "Requirement-Group-I" (RG-I). 6G applications will demand several orders of magnitude improvements in RG-I values. In the second category, we include privacy and confidentiality, data integrity, non-repudiability, and auditability requirements. We refer to these, mostly security-related requirements, as "Requirement-Group-II" (RG-II). 6G applications are envisioned to use and manipulate the large amount of data produced by human senses/organs, and autonomous agents that necessitate the inclusion of both types of requirements as inherent and necessary components/features.

In 6G vision papers, we find a lot of discussion on various technologies that can help in the further improvements in RG-I values. Some of these front-runner 6G technologies include THz communication, RIS [1, 2, 4] and AI [3, 12]. We anticipate that the advancements in these new technologies and new network architectures will enable ultra-reliable, low-latency, and enhanced broadband connectivity for a massive number of devices in 6G communication systems. On the other hand, in 6G literature, there is not much discussion about RG-II. This is due to several reasons. The exact definition and scope of security-related requirements may vary in different application scenarios due to the nature of involved entities such as operators, equipment, and machines, and assigning responsibility for the fulfillment of these requirements is also not straightforward. As the application and use-case landscape in future 6G applications becomes more and more complex, fixing RG-II values also becomes challenging.

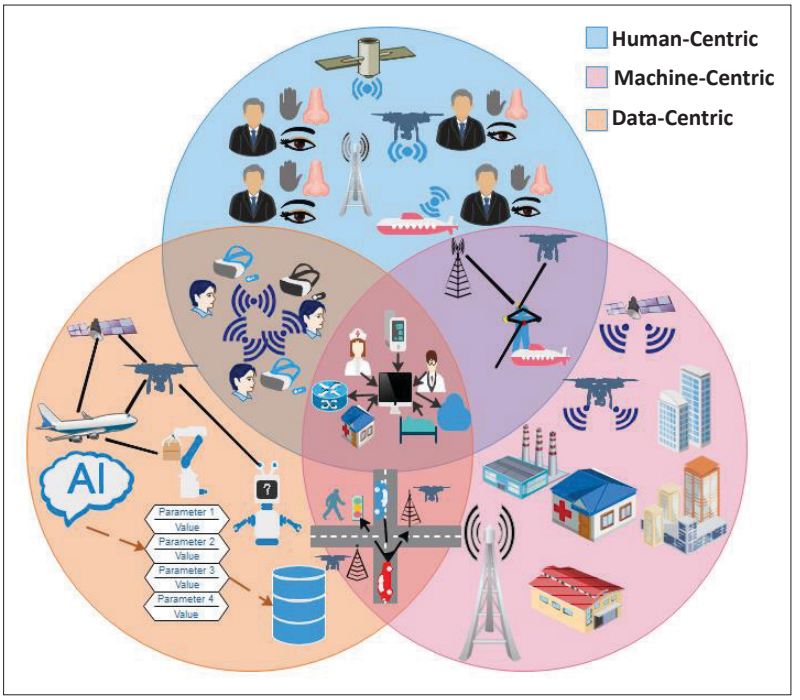

FIGURE 1. 6G Applications.

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 and 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 and 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

TABLE 1. Blockchain Based Resource and AI model parameter management for RG-I in 6G applications.

Blockchain and 6G

In this section, we first discuss blockchain followed by the combination of blockchain and 6G from the RG-I and RG-II perspectives.

Blockchain

Blockchain is a distributed ledger in which information is stored as a chain of data blocks. Blockchain is an amalgamation of several technologies for network, consensus and automation management. All these technologies have to be carefully combined and selected to attain the desired security features required for the underlying application scenario. As the use cases of blockchain are expanding, so are the number of available options to build a blockchain. With respect to administrative control, blockchain can be either public, consortium or private. Any node can join, leave, read or write on the public blockchain and it is completely decentralized. In consortium and private blockchains, the write access is owned respectively by a group of organizations and a single organization. PoW algorithms provide the greatest amount of security features in terms of data immutability but their use on resource-constrained nodes becomes challenging. PoS variants like dPoS, on the other hand, can be made more secure by engaging a large number of verifiers in the network which increases the communication overhead and the time required for reaching consensus. Automation on blockchain is managed through smart contracts which are computer programs stored on the blockchain to define the contractual obligations and enable the automatic transfer of assets between peers when the required conditions are met.

Blockchain and 6G RG-I

For RG-I targets, 6G is expected to be 3D integrated with infrastructure elements being present in all three dimensions. The management of this infrastructure and asset will be a challenging task. The spectrum, storage and computation sharing models will also become more complex. AI will be an essential part for resource optimization. The management of trained models will become complex. Blockchain will provide the essential trustless environment and security required for the resource and AI management (Table 1).

Resource Management Solutions: 6G applications would demand a large amount of spectrum, computing power, and other available resources and infrastructure.

Spectrum Management: High data rate requirements of 6G applications can be aided by spectrum sharing as data rate is directly proportional to the available bandwidth. To maximize spectrum utilization, licensed spectrum owners as well as unlicensed spectrum operators in any band can coordinate and cooperate with each other under different terms and conditions automated through smart contracts which are deployed on a blockchain. The spectrum sharing framework described in [13] for 5G can be applied. In this framework, when a user requests the desired bandwidth, the primary operator (the operator who has the registration information of the user) checks to see if it has the desired resources. If not, it requests the secondary operator regarding the resource availability. Once confirmed, the primary operator sends the user's information to the secondary operator, who sends a service level agreement (SLA) to the primary operator and provides the required permission to use the spectrum. The authorized node verifies the transaction and adds it to the blockchain. This framework can be made more secure for 6G by choosing a consortium blockchain along with appropriate consensus algorithms.

In such an improved framework, a transaction containing both the operator identities, user identity, and start and end time of spectrum usage is added to the current block which is verified by the network. Once verified, the new block containing the spectrum sharing transaction is added to the blockchain.

Infrastructure and Asset Management: Dense deployment of communication devices in all three spatial dimensions owned by multiple operators or some specialized asset service providers (SASPs) (e.g., specializing in communication drones, HAPs, submarines) in 6G would be critical for RG-I targets. At the same time, maximum utilization of all the available resources would ensure the quality of service (QoS) of 6G users and would also maximize the revenues of network operators and SASPs. We explain the utility of blockchain through an example of a user wanting to decrease the communication latency by finding the best communication relays provided by the SASPs. In a blockchain-assisted infrastructure and asset management system, an authenticated and registered user will search for the nearest communication relays. The relays check the registration information of the user and its network from the blockchain

and then provide the desired connectivity to the user according to the SLAs available in the smart contract for that network. The transaction is recorded on the blockchain after verification through an appropriate consensus algorithm.

Computing Power and Data Storage Management: Many 6G applications would require a large amount of data from a very large number of sensors and nodes. For example, to provide fully immersive XR experiences, thousands (if not millions) of extremely small sensors may be required. Processing all this data into meaningful rich information will require a huge amount of computing power. However, even with future enhancements in battery technologies, such intensive applications will severely deplete the battery and storage of mobile devices, and computing and storage resources might also be inadequate. For compute power and storage management, authenticated users could use a public blockchain. We can assume a double auction market model where some users in need of computing power or storage space would submit their asks (required resources and price) while others with spare computing power or storage space can place their bids (available resources and price). In every such market round, bids and asks are matched and a market clearing price is determined. The double auction algorithm is automated through a smart contract. The transactions are added to new blocks which are verified through consensus and added to the blockchain.

AI Model Parameter Management Solutions: Operational and environmental intelligence may be achieved in 6G networks with the help of AI. With network densification, novel RIS-based channel models, multiple conflicting objectives, and an extremely large number of variables, optimization problems in 6G networks would become NP-hard. Instead of applying traditional optimization, deep learning techniques will mostly be used for efficient optimization of network resources in rapidly changing operational and environmental conditions. AI models are difficult to train but very efficient to use and produce results in no time. In this context, blockchain may be used to safely store the hard-found AI model training parameters.

Blockchain and 6G RG-II

In the following, we provide definitions of data integrity, non-repudiation and auditability. These are essential security features for 6G applications and have not been clearly defined previously in that context.

Data Integrity: Data integrity refers to the detection of unauthorized changes in data. Data integrity attacks deliberately modify the original information to corrupt a communication system for some malicious gains. Data integrity breaches may create safety issues in several control applications in vertical domains and LS-CAS applications.

Non-Repudiation: Non-repudiation refers to the availability of irrefutable proof of who performed a certain action even if the nodes in the network are not cooperating. As AI is becoming commonplace, we anticipate a very large number of machine-type nodes in 6G applications to mimic some form of human intelligence. In this context, non-repudiation will become an important requirement in several 6G applications.

Auditability: Auditability is concerned with the ability to reconstruct a complete history of a certain event or action from the historical records. In many LS-CAS applications where critical decision making is involved, auditability would be required to fix liability in case of malfunctions, conflicts, or to safeguard commercial and financial interests.

With these definitions and in order to better understand the advantages provided by blockchain for RG-II targets of 6G applications, we present a brief discussion of security related options available in 4G and 5G systems. The legacy authentication mechanisms in previous generations of communication systems mostly employ symmetric-key cryptography where the same key is used for encryption and decryption of data [14]. Up to 4G communication systems, the Authenticated key agreement protocol (AKA) and Extensible Authentication Protocols (EAP) frameworks are largely used. AKA is a challenge-and-response based authentication protocol, while in EAP, the user provides an identity to the eNodeB which is then authenticated by the authentication server. On the other hand, in 5G communication systems, asymmetric public-key-infrastructure (PKI) based cryptography, which provides stronger security properties than symmetric key cryptography, is used [15]. There is no protection in 4G communication systems for user data integrity. In 5G communication systems, protection of user data integrity is mandatory over the air interface. Integrity protection is resource demanding, therefore, the maximum data rate for integrity protected data traffic in 5G is limited to 64kb/s. 4G communication systems have no provision for non-repudiation because of symmetric key cryptography, while non-repudiation protection is provided by 5G due to PKI based cryptography. In both 4G and 5G communication systems, there is no defined mechanism for auditability of data.

Integration of blockchain in 6G would not only help but also control RG-II targets. Through the appropriate selection of network, consensus, and automation management algorithms, blockchain can provide desired levels of data integrity, non-repudiation and auditability. Blockchain allows asymmetric PKI based cryptography and the inclusion of privacy preservation frameworks for greater data *privacy and confidentiality*. Blockchain accepts new blocks only after verification through a consensus mechanism among multiple P2P nodes. Every block is linked to its parent block (previous block in the chain) by a cryptographic hash function. This allows *auditability* and makes it possible to verify data all the way back to the genesis block. *Data integrity* in any block can be easily verified simply by checking the hash-trees. Moreover, as the blockchain size increases, data tampering becomes even more difficult because of the linkage between all the chained blocks.

In addition to that, some state-of-the-art security technologies in practical communication systems are used in 5G. The encryption system used in 5G is 128-NIA1 which provides a 128 bit security level, that is, equivalent to that of AES 128. Blockchain utilizes two different levels of security where, for data verification, the data is encrypted. For data storage, the hash of the block is cascaded into the next block. For privacy, 5G uses the Elliptic Curve Integrated Encryption System (ECIES). Here the International Mobile Subscriber Identity (IMSI) of

Integration of blockchain in 6G would not only help but also control RG-II targets. Through the appropriate selection of network, consensus, and automation management algorithms, blockchain can provide desired levels of data integrity, non-repudiation and auditability. Blockchain allows asymmetric PKI based cryptography and the inclusion of privacy preservation frameworks for greater data privacy and confidentiality.

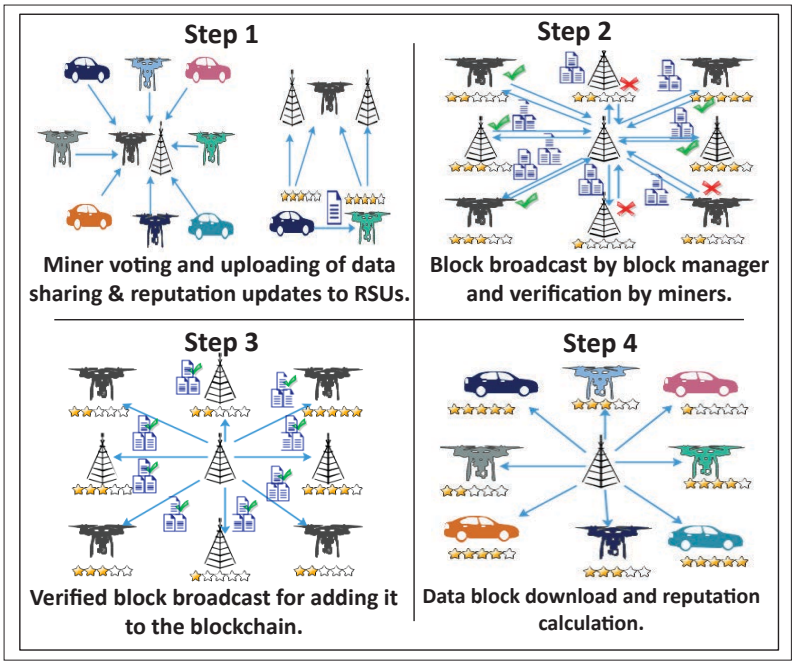

FIGURE 2. Blockchain-based reputation and dPoS Implementation for LS-CAS application.

the user is encrypted multiple times to generate different identities every time. In blockchain, privacy is ensured by generating a different key pair for every transaction to avoid linking of transactions. The control plane of 5G is logically centralized using SDN and NFV. This highlights an obvious vulnerability related to availability. Blockchain, being a decentralized network, provides better availability.

Case Study and Simulation Results

In this section, we present a case study to show how blockchain and 6G combined can provide a fast and secure communication system. We consider an LS-CAS example which is a data-centric and machine-centric application and a large amount of critical data is automatically generated and shared between autonomous nodes. Such applications have already been discussed in 4G and 5G communication systems. However, we will demonstrate that combining blockchain and 4G or blockchain and 5G cannot achieve the same level of synergy that we can obtain with blockchain and 6G, because the superior security features of blockchain require resource-intensive consensus algorithms and superior communication networks. Therefore, when 6G speeds are combined with blockhain security, we achieve the desired goal of truly fast and secure communication.

LS-CAS Scenario

Our LS-CAS scenario consists of autonomous vehicles and delivery drones (collectively referred to as User Equipments (UE)) and Road Side Units (RSU). We assume that some RSUs are fixed while others are drone-mounted. In this application, we have U2U (user equipment to user equipment), U2I (user equipment to infrastructure) and I2I (infrastructure to infrastructure) communications. UEs and RSUs together form a large-scale wireless-connected distributed autonomous system. We assume UEs are equipped with several sensors and state-of-the art camera systems. The data generated by UEs might represent real-time road maps, location information, infotainment, RSU reputation information, sensor readings, or any other information related to UE safety, transportation or entertainment needs. This data should be shared in the network with low latency while ensuring data integrity which is important for safe navigation and other reasons. In a scenario where this system is under attack from some malicious actors (RSUs and colluding vehicles) inside the network who can tamper data for their advantage, we need a mechanism to detect data tampering and also to recognize malicious actors. With the introduction of blockchain and its features, such data integrity attacks and bad actors can be easily recognized.

Secure Enhanced dPoS Algorithm for LS-CAS

We consider a blockchain-based setup similar to [8]. This blockchain uses a secure and enhanced dPoS algorithm and there are numerous safeguards for the protection of shared data. We assume RSUs have the necessary resources to implement and store the blockchain. The data shared among the UEs is sent to the RSUs, which run a dPoS consensus algorithm for block mining. We assume that RSUs are not fully trusted and can get compromised. Additionally, some UEs can also collude with the compromised RSUs. Therefore, miner reputations are updated after a complete round of data exchange and the record is uploaded to the blockchain. In the following, we explain one round of block creation and reputation updates. This process is also depicted in Fig. 2.

First, the stakeholders (vehicles/drones) participate in a voting process to determine active and standby miners according to the reputation scores. Active miners are a pre-defined number of higher reputation miners from all the miners, and they act as block managers in a round-robin fashion for the following rounds. Real-time data is shared among UEs and the data sharing record is shared with the nearest available RSU. UEs also upload recently calculated reputation scores to the nearest RSU. RSUs route this data to the block manager of that round.

Active and standby miners are split into different types based on their reputation scores. The block manager designs a smart contract for each type and broadcasts the unverified data block along with the different smart contracts. Smart contracts are designed such that a verifier gets maximum utility only if it attempts the respective smart contract. The block is verified and the verification results are audited by the local neighborhood, after which the block is sent back to the block manager.

The block manager receives the verification reports and creates a new data block based on a 2/3 majority consensus basis. After consensus, the block manager broadcasts the new block and the RSUs add this block to their local blockchain copies. UEs download the latest data block from their nearest RSU, check the accuracy of their previous transactions, and accordingly update the reputation score of the RSU for the next round.

There are numerous safeguards in this dPoS scheme to allow for the detection of malicious actors and collusion attacks. However, it is also obvious that the detection of any malicious activity largely depends on the amount of time required to complete different tasks in each

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	10Mb/s(4G), 500Mb/s(5G), 100Gb/s(6G)	10Mb/s(4G), 500Mb/s(5G), 100Gb/s(6G)	10Mb/s(4G), 500Mb/s(5G), 100Gb/s(6G)	10Mb/s(4G), 500Mb/s(5G), 100Gb/s(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

TABLE 2. Parameters and their values.

round. We can divide the latency of different steps in each round into transmission latency, computational latency and information diffusion latency. Due to the availability of relatively fast processors in vehicles and RSUs, we neglect the computational latency and thus the time for one round of this step will depend on the network speeds and network scale.

The Role of Communication Networks

To show the role of communication networks (4G/5G/6G) we perform some simulations. In these simulations, we assume a total area of 150km^2. UE positions are randomly initialized and RSUs are uniformly deployed across the network. The positions and the range of RSUs are set according to the density of network deployment. The weight of positive and negative interactions is set as 0.4 and 0.6, respectively. The probability of successful message transmission is 0.7. These parameters are derived from [8]. The adjustment factor for the number of hops is set to be 0.75. The reputation scores are computed using a multi-weight subjective logic (MWSL) model [8]. We consider four different network scales, that is, small-scale, medium scale, large-scale, and very-large-scale. Different parameters required in the simulation (e.g., average number of hops to block manager, types of verifiers, number of RSUs with UE records) are adjusted according to the network scale. In these simulations, we consider an attack scenario where a miner starts to behave maliciously after 20 rounds. The malicious miner also colludes with 25 percent, 33 percent and 50 percent of UEs in order to get high reputation scores. We consider the ability of the blockchain-based scheme to detect the malicious miner in 4G, 5G and 6G networks. Important simulation parameters are given in Table 2.

In Fig. 3, we plot the amount of time required to detect a malicious miner for different network sizes in 4G/5G/6G for different attack scenarios. As we increase the network size, the amount of time required for the detection of malicious miners increases. Similarly, for the same network size,

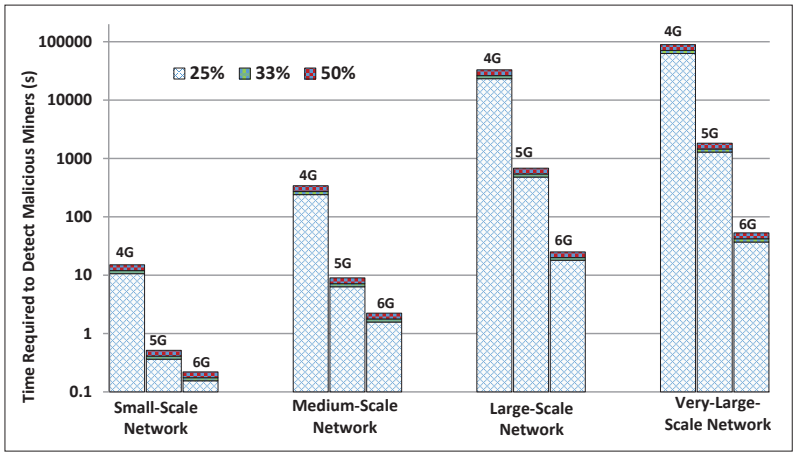

FIGURE 3. Time required to detect malicious miner for different collusion rates in different sized networks.

as we increase the percentage of colluding UEs, the amount of time required to detect a malicious miner also increases. The performance of a 4G network is only adequate in a small and medium-scale network where at 50 percent collusion it is able to detect the malicious miner in 15s and 340s, respectively. In large and very-large-scale networks, at 50 percent collusion, a 5G network requires 681s and 1826s, respectively to detect a malicious miner. On the other hand, a 6G network only requires 25s and 53s, respectively, in large and very-large-scale networks to detect a malicious miner at 50 percent collusion.

In order to clarify the importance of blockchain in this scenario, we consider an adversary, which behaves honestly for 20 interactions and then switches between malicious and honest behavior for 15 and 5 interactions alternatively. We use blockchain with the MWSL model as well as blockchain with the beta and sigmoid reputation models. In the beta reputation model, the beta probability density function is used to combine feedback and derive reputation. In the sigmoid model, reputation is calculated as a sigmoid function of an overall impact of honest and

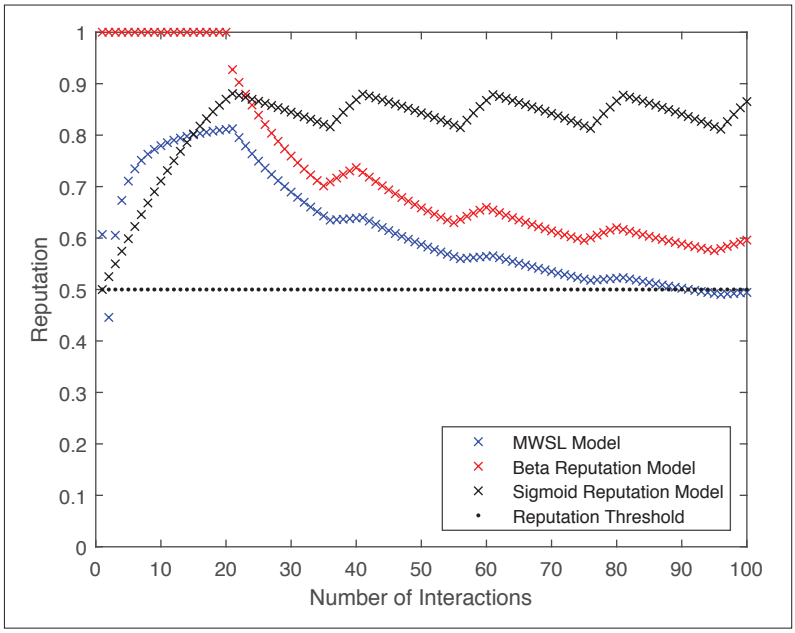

FIGURE 4. Update sensitivity of different reputation schemes.

malicious behavior. Using appropriate parameters and considering 33 percent network collusion, we observe that some blockchains are able to detect malicious miners, while others are not, as shown in Fig. 4. Even using 6G will not help in those cases. Using the latency results of 6G, we will see that malicious miners are detected the earliest when using 6G with an appropriate blockchain model. This result shows that in LS-CAS, the appropriate selection of blockchain structure is necessary for detecting malicious activity, and therefore improving the system integrity. Along with blockchain, 6G is the most appropriate technology that will facilitate timely detection. In that sense, blockchain and 6G will form an ideal combination for the application used, that is, LS-CAS.

These simulation results are very promising and suggest the use of more secure blockchain implementations in 6G are possible as both complement each other. Secure consensus algorithms enhance security of 6G applications while 6G enables their implementation through its faster speeds. At the same time, the creation of a trustless environment in 6G by more secure blockchain implementations would benefit RG-I by eliminating under-utilization of critical resources deployed under complex ownership and sharing models. Some challenges for wider blockchain implementations in 6G would require further research in the following directions:

- Sharding and sub-blockchain techniques could be utilized for further reduction in convergence times in very large blockchain networks.
- Smart contracts optimization techniques are necessary for decreasing block size and consensus latency. Smart contracts should also be written extremely carefully to make them less vulnerable to hackers.
- Larger network sizes translate into larger storage requirements. Off-chain storage can be used and a signature associated with the block can be stored on the chain.
- Without compromising the security features, there is a clear need for less resource intensive consensus algorithms.

Conclusion

In this article, we have discussed the potential of blockchain and 6G for future communication and highlighted a synergy between them. We have divided 6G application requirements into performance related (RG-I) and security related (RG-II) groups with the objective of making the synergy more understandable. We have shown that the trustless nature of blockchain would make it easier to manage and audit 3D network resources and AI model parameters in 6G networks with complex ownership models. This flexible use of increasingly large and complex network resources in 6G with the help of blockchain would significantly facilitate RG-I targets. Furthermore, through the appropriate selection of blockchain type and consensus algorithms, the RG-II needs of 6G applications could also be readily addressed. Therefore, blockchain and 6G combined can provide secure and ubiquitous communication.

Acknowledgments

This work was supported in part by the LUMS Faculty Initiative Fund (FIF); in part by the U.S. National Science Foundation under Grants CCF-1908308 and ECCS-2039716; in part by WASP/NTU grant M4082187 (4080) and Singapore Ministry of Education (MOE) Tier 1 (RG16/20); and in part by A*STAR under its RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund – Pre Positioning (IAF-PP) (Grant No. A19D6a0053). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of A*STAR.

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, 2019, pp. 134–42.
[2] F. Tariq *et al.*, "A Speculative Study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, 2020, pp. 118–25.
[3] M. Giordani *et al.*, "Toward 6G Networks: Use Cases and Technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, 2020, pp. 55–61.
[4] S. Dang *et al.*, "What Should 6G Be?" *Nature Electronics*, vol. 3, no. 1, 2020, pp. 20–29.
[5] X. You *et al.*, "Towards 6G Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts," *Science China Information Sciences*, vol. 64, no. 1, 2021, pp. 1–74.
[6] M. Sadek Ferdous *et al.*, "Blockchain Consensus Algorithms: A Survey," arXiv preprint arXiv:2001.07091, 2020.
[7] N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions," *IEEE Industrial Electronics Mag.*, vol. 13, no. 4, 2019, pp. 106–18.
[8] J. Kang *et al.*, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," *IEEE Trans. Vehicular Technology*, vol. 68, no. 3, 2019, pp. 2906–20.
[9] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things J.*, vol. 6, no. 5, 2019, pp. 8076–94.
[10] D. Gabay, K. Akkaya, and M. Cebe, "A Privacy Framework for Charging Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," *2019 Proc. IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium)*, 2019, pp. 66–73.
[11] Z. Zheng *et al.*, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 Proc. IEEE Int'l. Congress on Big Data (BigData Congress)*, 2017, pp. 557–64.
[12] K. B. Letaief *et al.*, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Commun. Mag.*, vol. 57, no. 8, 2019, pp. 84–90.
[13] P. Gorla *et al.*, "Blockchain Based Framework for Modeling

and Evaluating 5G Spectrum Sharing," *IEEE Network*, vol. 35, no. 2, Mar./Apr. 2021, pp. 229–235.
[14] P. Schneider and G. Horn, "Towards 5G Security," *2015 Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1165–70.
[15] J. Cao *et al.*, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Commun. Surveys & Tutorials*, vol. 22, no. 1, 2019, pp. 170–95.

Biographies

Ali Hussain Khan is currently working as a research associate in the Department of Electrical Engineering at Lahore University of Management Sciences (LUMS), Lahore, Pakistan. He received the B.S. degree in electrical and computer engineering from Texas A&M University at Qatar (TAMUQ), Doha, Qatar in 2017, and the M.S. degree in electrical engineering from LUMS in 2020. His research interests are wireless communications, 5G/6G and blockchain technology.

Naveed Ul Hassan [M08, SM15] is currently an associate professor in the Department of Electrical Engineering, Lahore University of Management Sciences (LUMS), Pakistan. He received a B.E. degree from the College of Aeronautical Engineering, Risalpur, Pakistan, in 2002, and M.S. and Ph.D. degrees from Ecole Superieure d'Electricite, Gif-sur-Yvette, France, in 2006 and 2010, respectively. His research interests are in the areas of wireless communications, 5G/6G, smart energy systems, blockchain technology, and indoor positioning systems.

Chau Yuen [S02, M06, SM12, F21] received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. From 2006 to 2010, he was with the Institute for Infocomm Research. Since 2010, he has been with the Singapore University of Technology and Design. He received the IEEE Marconi Prize Paper Award in Wireless Communications 2021, IEEE Asia Pacific Outstanding Young Researcher Award 2012, and IEEE VTS Singapore Chapter Outstanding Service Award 2019. Dr Yuen serves as an editor for *IEEE Transaction on Communications* and *IEEE Transactions on Vehicular Technology*. He is an IEEE Fellow and a Distinguished Lecturer of IEEE VTS.

Jun Zhao [S10, M15] is currently an assistant professor in the School of Computer Science and Engineering (SCSE) at Nanyang Technological University (NTU) in Singapore. He received a Ph.D. degree in May 2015 in electrical and computer engineering from Carnegie Mellon University (CMU) in the USA, affiliating with CMU's renowned CyLab Security & Privacy Institute, and a bachelor's degree in July 2010 from Shanghai Jiao Tong University in China. Before joining NTU first as a postdoc and then as a faculty member, he was a postdoc at Arizona State University as an Arizona Computing PostDoc Best Practices Fellow.

Dusit Niyato [M09, SM15, F17] is currently a professor in the School of Computer Science and Engineering at Nanyang Technological University, Singapore. He received the B.Eng. degree from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.

Yan Zhang [F20] received the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is currently a full professor with the Department of Informatics, University of Oslo, Oslo, Norway. His research interests include next generation wireless networks leading to 5G beyond/6G, green and secure cyber-physical systems (e.g., smart grid and transport). He is an editor for several IEEE publications. He was an IEEE Vehicular Technology Society Distinguished Lecturer for the term 2016–2020. He was a recipient of the global Highly Cited Researcher Award (Web of Science top one percent most cited worldwide).

H. Vincent Poor [S72, M77, SM82, F87] is the Michael Henry Strater University Professor of Electrical Engineering at Princeton University. His interests include information theory, machine learning and networks science, and their applications in wireless networks, energy systems, and related fields. He is a Member of the National Academy of Engineering and the National Academy of Sciences, and a Foreign Member of the Chinese Academy of Sciences and the Royal Society. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively, and the IEEE Alexander Graham Bell Medal in 2017.