Resource-Efficient DAG Blockchain with Sharding for 6G Networks

Jin Xie, Ke Zhang, YunLong Lu, and Yan Zhang

Abstract

The sixth-generation (6G) system is widely envisioned as a global network consisting of pervasive devices that interact with each other. Besides exchanging information, these peer entities also share heterogeneous and distributed edge resources. Blockchain is a promising technology to secure resource sharing in a peer-to-peer way. However, constrained by limited transaction throughput, existing blockchain systems (e.g., Bitcoin) cannot process numerous resource transactions concurrently produced in large-scale 6G networks. To cope with this issue, we propose a blockchain scaling scheme that combines Directed Acyclic Graph (DAG) with sharding. Our sharding method divides blockchain transactions into multiple mutually disjoint subsets maintained by different committees, which enables high-volume resource transactions to be processed and recorded concurrently. Additionally, all committees maintain a global DAG of blocks to resolve the security degradation raised by the sharding method. Moreover, we put forth a computation efficient consensus algorithm by leveraging miners' computing power to improve resource utilization efficiency. Numerical results show that the proposed scheme achieves good performance in resource utilization efficiency.

Introduction

As a new paradigm of wireless communication, the sixth generation(6G) system is expected to provide ubiquitous wireless coverage and enable powerful mobile applications, such as fully autonomous vehicles, holographic telepresence and telemedicine [1]. In order to realize these 6G-empowered applications, mobile nodes need to consume massive heterogeneous edge resources, including computing power, wireless spectrum and cache capacity. The nodes with limited resources always resort to resource sharing from edge infrastructures or the other nodes empowered with sufficient capabilities.

Resource sharing can be taken as a kind of transaction that involves the interests of the supply and demand sides. Driven by the interests, there may occur some attacks, forgery and tampering of the transaction information from malicious nodes. Thus, a transaction security protection mechanism against malicious behaviors is imperatively required. Blockchain, which holds batches of immutable and tamper-proof transactions in distributed digital ledgers, is a promising technology to address the security problem [2]. The distributed transaction recording mode of the blockchain well matches the distributed mode of edge resources sharing among multiple nodes. Moreover, blockchain's multi-point consensus avoids system failure caused by single ledger node corruption.

Although blockchain brings great benefits for securing the edge resource sharing process, some critical challenges have emerged in its efficient application in 6G networks. In the 6G era, pervasive connectivity is achieved between smart devices, which enables resource sharing to occur at any place and at any time in a variety of transaction forms and under diverse management strategies. Moreover, some interactive and real-time applications depend on the delay-constrained resource sharing process. These huge numbers of time-sensitive resource sharing transactions significantly challenge the scalability and efficiency of the blockchain system.

Catering to this challenge, we take sharding technology to boost blockchain's scalability and increase transactional throughput. In blockchain sharding, the whole blockchain network is divided into multiple committees that are comprised of subsets of recorded transactions. Each chain node only maintains transaction information related to its own committee. In such a way, the blockchain can flexibly match the highly distributed recording requirements of massive transactions in 6G networks, while maintaining low-complexity operation and fast block generation.

Along with the improved efficiency, some security issues have arisen in the sharding enabled block system. Since sharding splits the whole blockchain into smaller pieces, the number of chain nodes is reduced and the complexity of the consensus gets lower. This splitting allows an attacker to consume less computing power to complete a 51 percent attack and successfully tamper with the recorded transaction data in the block sharing system than in a traditional blockchain. A graph theoretic approach named directed acyclic graph (DAG) is a potential way to address this security problem. DAG is defined as a kind of data structure that assembles the relations of data units as tree logic. Applying DAG into the blockchain system, blocks from different sharding committees could be assembled into a DAG, and make multiple committees mutually secure each other and verify the updated chain data. However, this mutual verification in the DAG blockchain incurs some extra costs in terms

Jin Xie and Ke Zhang (corresponding author) are with the University of Electronic Science and Technology of China; YunLong Lu is with Beijing Jiaotong University; Yan Zhang is with the University of Oslo.

Digital Object Identifier: 10.1109/MNET.211.2100345

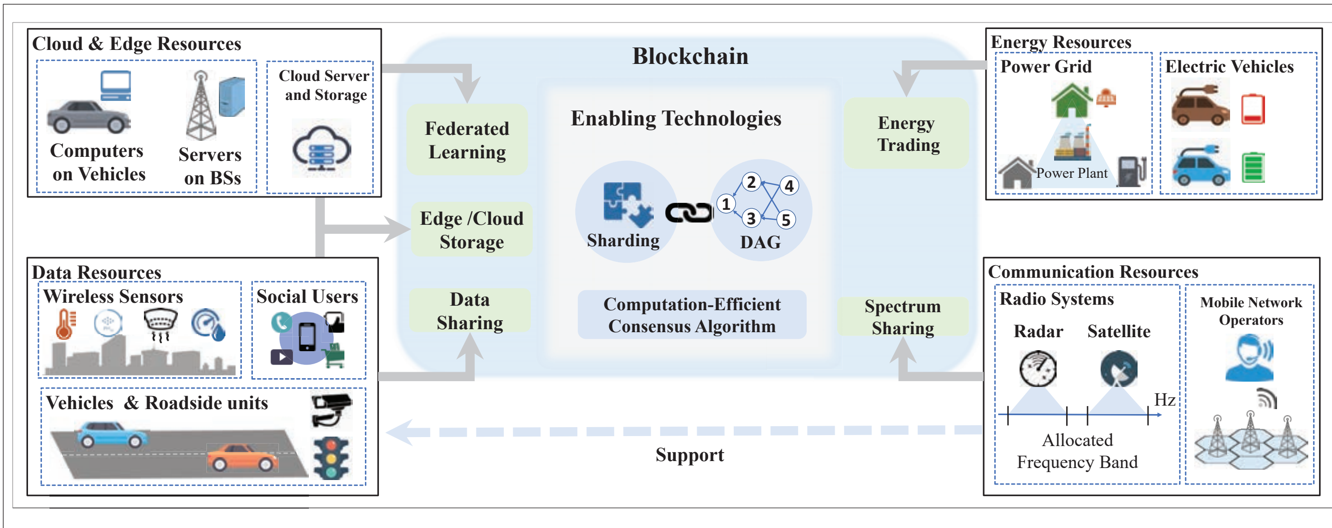

FIGURE 1. Blockchain applications in 6G networks.

of communication bandwidth and computing power. However, the way to achieve both data security and cost efficiency in DAG blockchains is still an unexplored problem.

To fill this gap, we propose a DAG-based blockchain SHarding (DASH) scheme that combines the efficient data recording of sharding and the secure blockchain updating of DAG. Unlike the traditional blockchain that all the blockchain nodes maintain complete blockchain data, our sharding method divides the blockchain network into multiple committees, and blockchain nodes only process and store the historical transactions generated locally. However, the separation of committees might cause security issues. To cope with this problem, our scheme reunites the computing power of different committees by maintaining a global DAG. Moreover, the DAG in our scheme consists of the block headers instead of the entire block. In this way, block headers are broadcasted across the network rather than the block with full transaction data, so the communication overhead could be largely reduced. To the best of our knowledge, this is the first work that investigates the joint optimization of blockchain's scalability and security in edge resource sharing. In addition, we design a resource-efficient consensus mechanism, which saves the computational cost of the consensus process and improves spectrum efficiency.

Resource-Efficient DAG Blockchain and Sharding for 6G Networks

This section introduces the emerging blockchain applications in 6G networks, which are identified by the kind of related resources.Then we present the necessity and feasibility of exploiting DASH and a computation-efficient consensus algorithm in our blockchain-enabled resource sharing mechanism.

Blockchain Empowered Distributed Applications in 6G Networks

Figure 1 shows five different distributed resource sharing applications in 6G networks, and this section briefly introduces the characters blockchain plays in these applications. Furthermore, we focus on the scenario of blockchain-enabled spectrum sharing, and present an analysis and comparison of several existing works with a table.

Data Sharing: In data sharing, blockchain is utilized to record the digests of sharing data, which can be used by receivers to verify the received data's authenticity and reliability [3]. For instance, wireless sensors collect the environmental variables in the smart city, and these variables are shared in an untrust environment. On-road vehicles and roadside units collect real-time traffic information and share them with each other [4]. Social network users upload popular content to the edge of the network, which eliminates the transmission latency in center-to-end type.

Edge/Cloud Storage: In edge and cloud storage, blockchain is utilized to build a decentralized access control system. The access rights are recorded transparently on the blockchain and updated by the peer nodes instead of a central server.

Energy Trading: Figure 1 shows the situations of energy trading among peer entities. Smart buildings with solar panels are able to harvest ambient energy and trade energy with each other. In the load peak of the power grid, vehicles with redundant power can feed their energy back to the grid or sell energy to other vehicles. During this process, blockchain works as a secure trading platform to enable P2P energy trading without a trusted intermediary [5].

Federated Learning: By leveraging blockchain in federated learning, the local models are aggregated into a global model by multiple miners in the blockchain instead of a vulnerable central sever [9]. To better utilize the computation resources residing on the edge of the network, blockchain implements an incentive mechanism to motivate local computers on vehicles or base stations for updating high-quality local models.

Spectrum Sharing: Spectrum sharing is the basis of other kinds of resource sharing, which could help task offloading through wireless communication and also the transmitting of signaling messages in energy sharing.

In spectrum sharing, users can acquire additional spectra frequency from other radio systems called incumbents [10], such as the radar

Paper	Blockchain type and consensus algorithm	Scalability	Computation consumption	Storage	Allocation scheme
[6]	Consortium/PBFT	Unable to scale	Low	Full	Opportunistic Access
[7]	Consortium/PBFT	Unable to scale	Low	Full	Matching-based
[8]	Permissionless/PoW	Able to scale with limits	High	Full	Auction-based

TABLE 1. Existing works of blockchain-empowered spectrum sharing.

and satellite systems. The deployment of blockchain to spectrum management systems enables incumbents to sell their frequency bands to users without a spectrum management center, thus reducing the transaction fees of spectrum sharing [11]. The authorizations of spectrum access are recorded as transactions in the blockchain, and all the participates reach an agreement on the authorizations of spectrum access through the blockchain consensus mechanism [12].

Table 1 lists several works of blockchain-enabled spectrum sharing. There are three types of allocation schemes. Opportunistic access is adopted in work [6], where the spectrum sharing transactions are randomly picked by miners and attached to the blockchain. Auction-based and matching-based schemes are both deterministic allocation schemes, where the specific spectrum resource is allocated to the highest bidder or the best matching user. Work [8] is different from others because it uses the PoW consensus algorithm, which brings better scalability. However, the blockchain in work [8] can only scale-out with the number of users rather than the network's geographical coverage because the same frequency band cannot be reused at different places even if they are distant from each other. It can be seen through the comparison that there are still some problems inherent in blockchain when dealing with a large-scale network, such as scalability issues, excessive storage overhead, and consuming too much computation resources on the consensus process. To cope with these problems, we present our solutions in the next subsection.

Sharding and DAG for Blockchain-Enabled 6G Networks

In essence, blockchain applications enable the sharing of energy, data, computation, and spectrum resources among peer entities. Therefore, the transaction processing capacity of blockchain directly determines the efficiency of resource sharing. Some scaling technologies such as Lightning network and Sidechain could increase the blockchain's throughput, but they are not feasible for resource sharing due to the fixed membership of blockchain participants. To this end, we attempt to utilize a public DAG-based blockchain to solve the scalability issue. However, deploying DAG-based blockchain over the resource sharing system in a fully distributed manner brings new challenges that have not been investigated. The first challenge is that conflicting and duplicated transactions might be appended to the DAG-based blockchain simultaneously by non-cooperative miners. Another challenge is that more blocks are created concurrently in the DAG approach, which results in more communication and storage overhead to maintain the consistency of the blockchain.

To cope with these challenges, we utilize the sharding method to partition the blockchain network into multiple committees, where resource transactions are processed and recorded locally. The rationale behind this approach is that specific information of resource sharing is unnecessary to be broadcasted and stored across the network. For example, in spectrum sharing, different users can access the same frequency band without the concern of interference as long as they are distant from each other. Thus, users only care about the channel state information in proximity to their locations. Moreover, conflict management is easier to be realized within the committee. However, unlike other existing blockchain sharding schemes such as Rapidchain [13], the committee in DASH has a double identity. In the blockchain, a committee is a group of nodes maintaining the same subsets of blockchain data. In the physical network, committees are geographic areas that divide the resources of the network into individual parts. Moreover, the resources that belong to a committee can only be shared within the committee.

Figure 2a is an instance of existing blockchain sharding (e.g., Rapidchain), where committees maintain their chain of blocks individually. The cross-committee transaction enables nodes to transfer value between different committees. However, the cross-committee transaction will not be triggered if all transactions are invoked within the committee. On the one hand, sharding enables the storage devices to store partial data of blockchain. On the other hand, it also partitions the computing power of the whole network, which is not expected. Miners in different committees construct candidate blocks separately. Therefore, the malicious nodes only need 51 percent computing power of the committee to launch a double-spend attack, which is obviously easier than aggregating more than half of the computing power of the whole network. In order to utilize sharding in DAG-based blockchain without degeneration of security, our DASH scheme is proposed.

Our solution DASH is illustrated in Fig. 2b. For the sake of simplicity, there are three committees. Committees generate blocks stamped with their ID, and the intact data of the block (transactions) is stored locally, which is similar to the traditional blockchain sharding. However, more importantly, committees keep a global DAG recording the existence of all the blocks. Moreover, any node can reconstruct the DAG as long as it has headers of all blocks because the hash references between the blocks are contained in the header. New blocks containing transactions are broadcasted through the gossip protocol. However, when blockchain nodes at the border of the committee receive valid blocks from other committees, they will discard the transactions of these blocks and forward the block headers to other

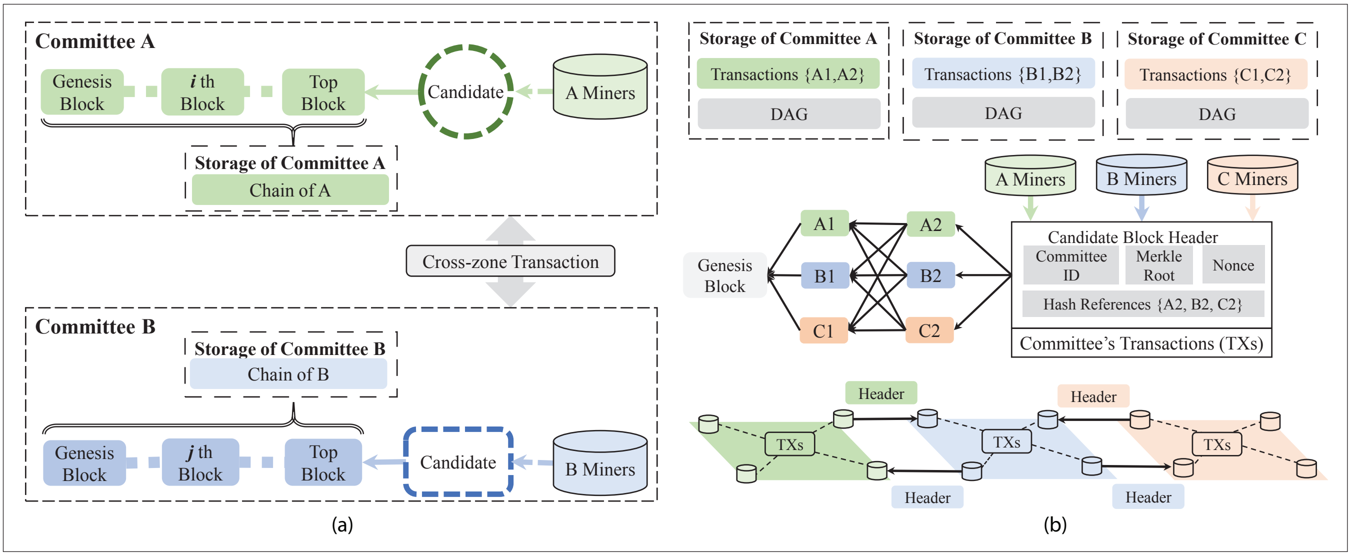

FIGURE 2. Blockchain for 6G networks: a) blockchain sharding; b) DASH.

nodes. Therefore, transactions are disseminated within the committee, but the block headers are transmitted across the network.

Once the miner receives the block headers from other committees, it will construct the candidate blocks referring to these extraneous blocks. In Fig. 2b, all the miners share the same view of blockchain, and they work on the candidate block referring to A2, B2 and C2 concurrently. Miners spend their computing power to find a valid nonce as the proof of work, and the Merkle root ensures that the block's transactions cannot be modified. In this circumstance, different committees' computing power secures each other mutually because the malicious nodes have to change all the consequent blocks if they attempt to manipulate data in A2, B2 or C2.

DASH defines the data structure of the blockchain. As another vital part of the blockchain, the consensus algorithm defines the rule and method of updating the blockchain. We exploit the permissionless blockchain to ensure that resources are managed by the public rather than a set of known and identifiable participants, which remains the fairness and decentralization of blockchain technology. Two common permissionless blockchains are Proof-of-Stake(PoS)-based and PoW-based. However, in a PoS-based blockchain, a small group of miners with the highest stake are prone to a monopoly on the generation of new blocks. It is undesired that a minority of nodes always take charge of allocating resources, which induces the unfair allocation of resources. Therefore, we stick to the PoW-based approach that introduces more randomness and fairness when considering the right of updating blockchain.

To design a computation-efficient consensus algorithm, miners' computing power would better be used to solve some practical problems instead of merely solving the hash puzzle. The answer to the problem should be verified easily, but solving the problem is quite difficult. For example, in spectrum sharing, miners compete with each other to publish a new block by solving a spectrum allocation problem. In energy trading, miners match the recharge and discharge requests from electric vehicles. If the miner's solution satisfies more vehicles, it is more likely to generate a new block. Through leveraging these enabling technologies, the benefits of blockchain technology can be better harvested.

DAG Blockchain and Sharding for Resource Sharing

In this section, we will present how DAG blockchain and sharding are deployed in the spectrum sharing system. At the inception phase, a genesis block is generated to annunciate the public keys of every incumbent and their licensed bands. After creating the genesis block, the smart contract is utilized to configure the blockchain network and implement functions for resource sharing. The main functions of the proposed sharing system are as follows.

Sharding: The network needs to be partitioned into multiple committees. The smart contract, which is included in a block after the genesis block, establishes a committee by designating its coverage area and specifying its geographical boundaries. Committees are prohibited from covering the same area, and then each base station is assigned to a specific committee according to its location. Inside the committee, blocks are created chronologically as a single chain. Therefore, only transactions in the same block share the spectrum resources concurrently. Conflicting spectrum sharing transactions could be prevented as the miner is prohibited from allocating the same frequency bands to multiple users in proximity.

Protection of Incumbents: Incumbents have the highest priority to use their licensed spectrum, so they need to announce their protection area where other users cannot use the protected frequency band. When a smart contract is created, there will be an initial version of the protected areas approved by the digital signature of incumbents.

Spectrum Sharing Policies: In the distributed spectrum sharing system, the peer nodes usually lack mutual trust. To secure the spectrum trading process, we use the smart contract as a public

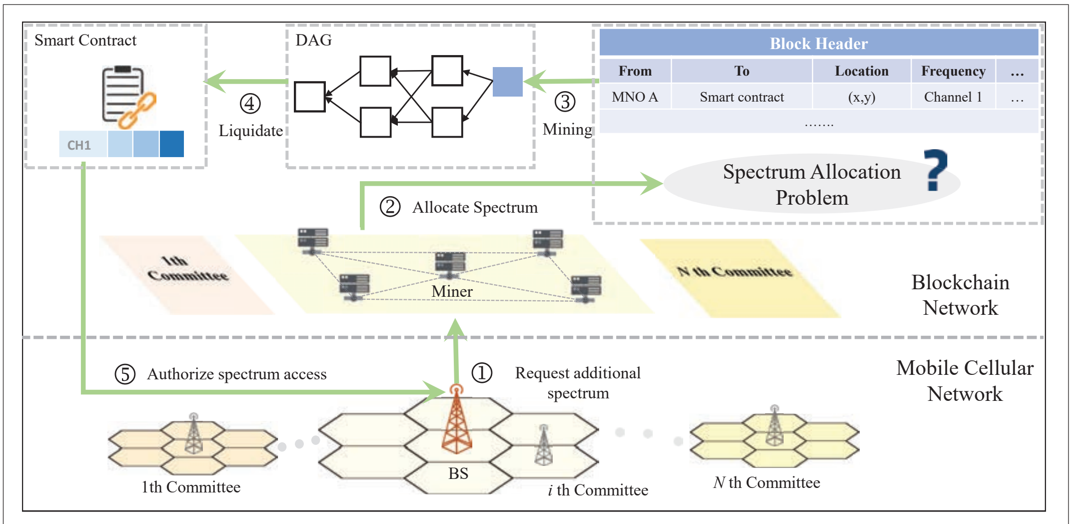

FIGURE 3. DAG blockchain sharding for spectrum allocation.

agreement to prevent users from directly dealing with the incumbents. The price for using incumbents' licensed bands is indicated in the contract. The smart contract keeps an account for each incumbent. During trading, the user who accepts the price will invoke a transaction to send value to the smart contract address. When the incumbent successfully shares its licensed bands with other users, the smart contract will increase the value of the incumbent's account.

After introducing the base functions of our spectrum sharing system, we now demonstrate how to complete a successful spectrum sharing. As shown in Fig. 3, A successful spectrum sharing process involves the following five steps.

Step 1: The base station launches the spectrum sharing process by constructing a request transaction. The transaction depicts two important attributes of the base station: its service radius and its geographical location.

Step 2: Miners of the committee collect all the request transactions from base stations. Miners then allocate frequency bands to base stations by appending the messages of allocated spectrum resources to the request transactions. Afterward, the spectrum sharing transactions will be packaged into the body of a block.

Step 3: Miners compete with each other to find a valid block through an improved PoW algorithm. Once the valid block is found, it will be broadcasted inside the committee. Other miners in the same committee will verify the block and concatenate their digital signatures to the block header. The verified block header will eventually be transmitted to all the committees.

Step 4: The smart contract is triggered by the spectrum sharing transactions. The balance of incumbents recorded in the smart contract will be updated.

Step 5: The base station gets authorization to access the specified frequency bands.

The spectrum sharing transactions are recorded in the blockchain by the steps mentioned above. The next section will present how a miner allocates the spectrum resources to base stations and the rationale behind the improved PoW-based consensus algorithm.

Resource-Efficient Consensus for Blockchain in Spectrum Sharing

In this section, we demonstrate the process of an honest miner to find a valid block according to the improved PoW-based consensus algorithm. Like the original PoW algorithm, miners still need to put a right nounce into the block header. The hash result of a valid Block header is numerically less than a target. In our proposed consensus algorithm, miners are rewarded by lowering the mining difficulty for proposing a spectrum allocation scheme with higher performance.

The set of spectrum sharing transactions in a block denotes the allocation schemes proposed by the miner for the committee. To measure the efficiency of these spectrum allocation schemes, we propose two important criteria. The first one is the fairness of spectrum sharing. Miners are expected to meet more access requests from different base stations. The second criterion is the utilization efficiency of spectrum sharing. The utilization efficiency of shared spectrum resources is evaluated according to their coverage area. A high utilization efficiency means that the frequency bands are widely reused outside the incumbents' protection area. The method relieves the blockchain network from consuming too much computing power on a conventional hash algorithm. Moreover, it also brings more fairness and efficiency to the blockchain empowered spectrum sharing system.

In our proposed system, the bandwidth of incumbents is divided into M channels indexed by $j = 1, ..., M$. There are N_j unusable areas of the j-th channel consisting of the incumbents' protected areas and service areas of previous unexpired spectrum sharing transactions, which is indexed by $k = 1, ..., N_j$. Therefore, the unusable area of the j-th channel is described by a geographic coordinate and a radius, that is, $(x_{j,k}, y_{j,k})$ and $R_{j,k}$. A miner receives N request transactions from base stations indexed $i = 1, ..., N$. Each transaction denotes a request of spectrum sharing, including a location, a service area and an upper limit bandwidth. Let (x_i, y_i) denote the location of a requesting base station. The

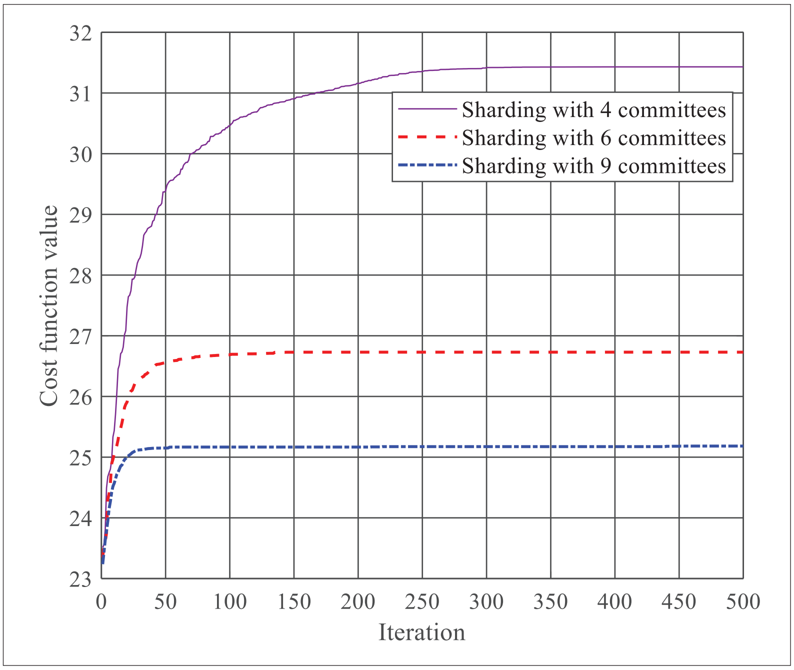

FIGURE 4. Comparsion of convergence of different number of committees.

demand of the service area is lower bounded by the minimum radius $r_i^{\min}$ and upper bounded by the maximum radius $r_i^{\max}$. The bandwidth B_i describes the maximum number of channels required by a base station. Thus the spectrum allocation scheme is a $M \times N$ matrix composed of service area radius, where $r_{j,i} = 0$ if the j-th channel is not assigned to the i-th base station. A binary variable α_i is introduced to indicate whether the i-th base station is allocated with spectra frequency, and $\alpha_i = 1$ if $\sum_j r_{j,i} \neq 0$.

In order to reuse the spectrum resources efficiently and satisfy more base stations, we formulate an optimization problem with the objective U as

$$
\begin{aligned}
&\max_{r_{j,i}} U = \lambda_1 \frac{\sum_{i,j} \pi r_{j,i}^2}{A} + \lambda_2 \sum_i \alpha_i \\
&\text{s.t.} \quad C1: r_i^{\min} \le r_{j,i} \le r_i^{\max}, \qquad \forall r_{j,i}, r_{j,i} \neq 0 \\
&\qquad\; C2: r_{j,i} + R_{j,k} \le \left| x_i - x_{j,k}, y_i - y_{j,k} \right|, \quad \forall r_{j,i}, r_{j,i} \neq 0 \\
&\qquad\; C3: \sum_j \frac{r_{j,i}}{r_{j,i}} \le B_i, \qquad \forall r_{j,i}, r_{j,i} \neq 0
\end{aligned}
$$

where A is the total area of the network, and both λ_1, λ_2 are normalization coefficients. Thus, the first term of the objective represents the spatial spectrum utilization efficiency. The second term is proportional to the number of base stations that are allocated at least one channel. Constraint C1 ensures that the requirements of base stations are satisfied in terms of working range of the shared spectrum. Constraint C2 promises that the corresponding channels are not reallocated in the incumbents' protected areas and service areas of previous unexpired spectrum sharing transactions. Constraint C3 states that the number of channels allocated to base stations shall not exceed their required number. This spectrum allocation problem is a combinational optimization problem, which cannot be solved in deterministic polynomial time. Therefore, we adopt the artificial bee colony algorithm, which uses swarm intelligence to search for the optimal solution to the allocation problem. After solving the allocation problem, miners will mine the block with the revised mining difficulty according to U of their allocation schemes.

In our proposed system, the miners still need to solve a hash puzzle after finding the optimal allocation scheme, mainly for two reasons. For the first reason, proof-of-work protects honest miners from malicious plagiarism. Because the allocation scheme is transparent to any node, plagiarists can acquire it and build their own blocks with the copied allocation scheme. However, the plagiarists still need to find a solution for its hash puzzle. During this period, the original block will be broadcasted to the majority of honest nodes. The second reason is that proof-of-work avoids the unexpected forks of blockchain induced by the sparse spectrum sharing requests in a committee. When there are only a few base stations requesting additional spectrum, the allocation problem will be quite simple for the miners to find a solution. In this case, if we disable proof-of-work, it only costs miners a very short time to find a valid block, and there will be multiple valid blocks referring to the same previous block in the committee. Consequently, blockchain forks will frequently occur, even if there are no malicious miners. Therefore, the computation consumption of solving the hash puzzle is a dispensable part of securing the blockchain.

Illustrative Results

In this section, we show the illustrative results to demonstrate the performance of our proposed DAG blockchain sharding deployment over a spectrum sharing system. We consider a square area of 100 km^2, and two incumbents share their licensed spectrum as two channels. The radius of base stations' service area is randomly taken from [200 ,1200] m, and the spatial distribution of base stations follows the Poisson Point Process (PPP).

Figure 4 shows the cost function value with different sharding size. The network is divided into multiple committees of the same size. In each committee, the allocation problem is solved individually. The cost function value in Fig. 4 is an average of all the committees in a sharding scheme. When we divide the network into four committees, the cost function converges to the highest value, because the size of the committee is the largest, and there will be more base stations in the committee. However, the spectrum allocation problem is more complicated when dealing with a larger size committee, which can be seen through these three sharding schemes' convergence points. The number of iterations shows the computation resources the miner has used to solve the allocation problem. As a rational miner, it will not spend too much time solving the spectrum allocation problem. For instance, the miner in the sharding scheme with four committees may turn to mine a new block at 150 times of iteration after which the increase of cost function becomes quite slow.

Figure 5 compares the performance of the improved PoW algorithm and the vanilla version in terms of the utility of spectrum allocation. The overall utility consists of the spatial spectrum utilization efficiency and fairness of spectrum allocation. To be specific, fairness is described as the rate of base stations that are allocated with additional spectrum resources, and the spatial spectrum utilization efficiency is the coverage rate of the shared spectra frequency. With the increasing average number of base stations, both the schemes reach a higher utility because they raise coverage areas. However, the improved PoW algorithm always outperforms the original PoW. In the original PoW algorithm, the difficulty of mining blocks has nothing to do with the allocation scheme. The miners always put as many non-conflicting transactions into blocks as possible without considering the coverage of the shared spectrum. Thus, adopting the improved PoW algorithm can improve the spectrum utilization efficiency because miners are encouraged to propose spectrum-efficient allocation schemes.

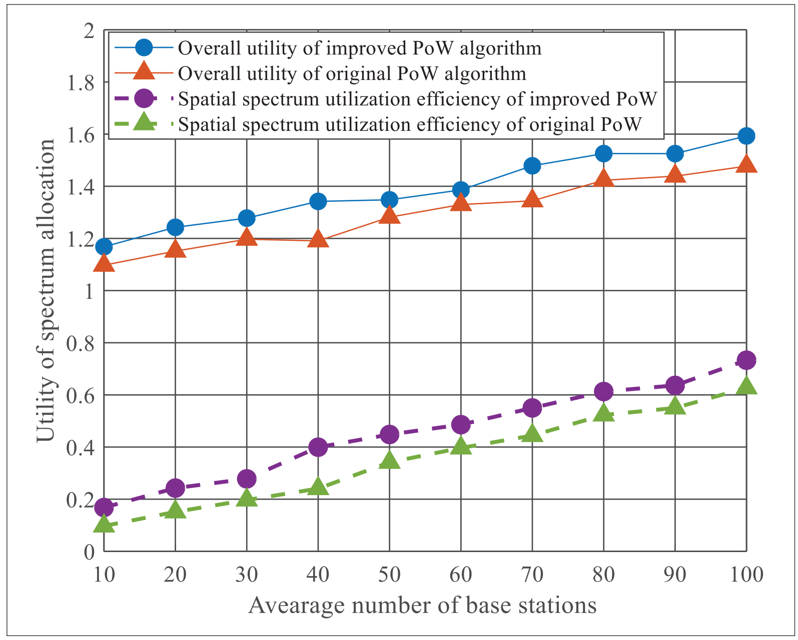

FIGURE 5. Comparsion of utility of our approach and PoW.

Conclusion and Future Work

In this article, we presented a resource-efficient DAG blockchain with a sharding scheme in 6G networks. We leverage sharding to improve the blockchain throughput and reduce the maintenance cost of the chain system. Moreover, we incorporate DAG technology into blockchain operation, which effectively overcomes the security degeneration induced by the sharding method. Then, the proposed DAG blockchain scheme was applied to spectrum sharing management to verify its application effect. Numerical results demonstrated that our scheme achieves higher spectrum efficiency and lower computation consumption compared with traditional PoW-based blockchain schemes.

Although DAG blockchain has great potential in fully-decentralized transaction management and tamper-resistant data recording, the coming 6G era will bring some unprecedented challenges such as scalability optimization and heterogeneous resource adaptation of the blockchain system.

Scalability: When the blockchain is used as a ledger to manage resource sharing, the efficiency of resource transactions is constrained by the progress of block generation and consensus. Moreover, as resource sharing management becomes more refined and complex in 6G networks, the number of concurrent resource transactions grows exponentially. Increasing the number of committees could be a possible solution, but it also brings the challenge of maintaining the consistency of blockchain since more new blocks are created and broadcasted in the network. This problem is still unexplored, and needs to be further studied.

Heterogeneous Resource Adaption: In 6G networks, heterogeneous edge resources may be shared concurrently between the user nodes. Transactions of different types of resources have diverse characteristics, which requires the blockchain system to provide differentiated transaction data recording services. For instance, when performing spectrum resource sharing, taking into account the time-varying instability of the wireless environment, fast block chaining is required to support agile spectrum transactions. In contrast, energy transactions are not so strictly time-sensitive. The blockchain system can make full use of the time cost of the energy exchange process to achieve the consensus. To cope with this problem, delay-sensitive resource sharing transactions could be packaged in blocks referring to fewer historical blocks in the DAG, which avoids waiting for blocks propagation from distant committees. However, this method might introduce security issues due to the lower connection between new blocks and historical blocks in DAG, so the tradeoff between the security and performance needs to be further investigated.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grants 61941102 and 62071092.

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, 2020, pp. 134–42.

[2] H. Xu *et al.*, "Blockchain-Enabled Resource Management and Sharing for 6G Communications," *Digital Commun. and Networks*, vol. 6, no. 3, 2020, pp. 261–69.

[3] K. Zhang *et al.*, "Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things," *IEEE Network*, vol. 33, no. 5, 2019, pp. 12–19.

[4] Y. Lu *et al.*, "Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles," *IEEE Trans. Vehic. Tech.*, vol. 69, no. 4, 2020, pp. 4298–4311.

[5] Z. Li *et al.*, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. industrial Informatics*, vol. 14, no. 8, 2017, pp. 3690–700.

[6] Y. Lu *et al.*, "Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks," *IEEE Trans. Industrial Informatics*, vol. 17, no. 7, 2021, pp. 5098–5107.

[7] A. B. Flores *et al.*, "IEEE 802.11af: A Standard for TV White Space Spectrum Sharing," *IEEE Commun. Mag.*, vol. 51, no. 10, 2013, pp. 92–100.

[8] J. Eggerton, "FCC's Rosenworcel Talks Up 6G," Sept. 2018; available: https://www.nexttv.com/news/fccs-rosenworcel-talks-up-6g.

[9] T. Maksymyuk *et al.*, "Blockchain-Empowered Framework for Decentralized Network Management in 6G," *IEEE Commun. Mag.*, vol. 58, no. 9, 2020, pp. 86–92.

[10] Y. Dai *et al.*, "Blockchain and Deep Reinforcement Learn-

ing Empowered Intelligent 5G Beyond," *IEEE Network*, vol. 33, no. 3, 2019, pp. 10–17.
[11] Z. Zhou *et al.*, "Blockchain-Empowered Secure Spectrum Sharing for 5G Heterogeneous Networks," *IEEE Network*, vol. 34, no. 1, 2020, pp. 24–31.
[12] K. Kotobi and S. G. Bilén, "Blockchain-Enabled Spectrum Access in Cognitive Radio Networks," *Proc. 2017 Wireless Telecommunications Symposium (WTS)*, 2017, pp. 1–6.
[13] M. Zamani *et al.*, "Rapidchain: Scaling Blockchain via Full Sharding," *Proc. 2018 ACM SIGSAC Conf. Computer and Commun. Security*, 2018, pp. 931–48.

Biographies

Jin Xie [S'21] (JinXie@ieee.org) received his B.S. degree from Southwest Jiaotong University, Chengdu, China, in 2018. He is currently pursuing a Ph.D. degree with the School of Information and Communication Engineering at the University of Electronic Science and Technology of China. His research interests include Internet of Things security, blockchain and mobile edge computing.

Ke Zhang [M'20] (zhangke@uestc.edu.cn) received his Ph.D. degree from the University of Electronic Science and Technology of China, 2017. He is currently an associate professor in the School of Information and Communication Engineering, University of Electronic Science and Technology of China. His research interests include scheduling of mobile edge computing, design and optimization of next-generation wireless networks, and the Internet of Things.

Yunlong Lu [M'20] (yunlong.lu@ieee.org) received the M.S. and Ph.D. degrees in computer science from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2015 and 2020, respectively. He is currently an associate professor in the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University. His current research interests include blockchain, edge intelligence, and Internet of Things security.

Yan Zhang [F'19] (yanzhang@ieee.org) is a full professor with the University of Oslo, Norway. He is a Fellow of IEEE, a Fellow of IET, an Elected Member of Academia Europaea (MAE), the Royal Norwegian Society of Sciences and Letters (DKNVS), and the Norwegian Academy of Technological Sciences (NTVA). His current research interests include next-generation wireless networks leading to 6G and green and secure cyber-physical systems (e.g., smart grid and transport).