IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CLOUD - FOG - EDGE COMPUTING IN CYBER-PHYSICAL-SOCIAL SYSTEMS (CPSS)

Received March 4, 2020, accepted April 1, 2020, date of publication April 3, 2020, date of current version April 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985580

Blockchain Based Dynamic Spectrum Access of Non-Real-Time Data in Cyber-Physical-Social Systems

XIN FAN AND YAN HUO, (Senior Member, IEEE)
School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Corresponding author: Yan Huo (yhuo@bjtu.edu.cn)

This work was supported by the Fundamental Research Funds for the Central Universities under Grant 2019JBZ001.

ABSTRACT Big data sharing in Cyber-Physical-Social Systems (CPSSs) relies on wireless transmission between numerous devices, causing a serious scarcity of radio spectrum resources. Although license-free spectrum access has great potential to alleviate the growing scarcity of spectrum resources, spectrum competition is more intense due to lower access requirements. A blockchain technology may solve this competition problem by introducing a dynamic cycle of "competition-verification-synchronization-competition". In this paper, we propose a general framework for license-free spectrum resource management in CPSSs based on blockchain technologies and smart contracts. The management framework is mainly used for edge computing of non-real-time data. In particular, we divide spectrum of a local cell into multiple channels and each channel corresponds to a blockchain. Then, we propose a blockchain-KM protocol that may improve transaction processing speed without losing typical attributes of a general blockchain. For the proposed Blockchain-KM protocol, the entire private chain becomes a multi-ring blockchain and users rely on mining or leasing to access wireless spectrum. Different from the traditional mining process, the reward in our mining process is not only virtual currency but also a spectrum access license. Once a miner obtain a spectrum access license, it will exploit the license to transmit its messages over wireless links. Also, the miner may sell its license by an auction when it does not want to transmit messages. In the auction, we introduce a virtual currency, called as Xcoin, for spectrums or other trading (e.g., paid edge computing services).

INDEX TERMS Cyber-physical-social systems, edge computing, spectrum access, blockchain, smart contract.

I. INTRODUCTION

A cyber-physical-social system (CPSS) is a multi-dimensional intelligent system. After mining social relationships behind big data, it can exploit social attributes to control a traditional cyber-physical system [1], [2]. Integrated with the rapidly developing computing-communication-control technologies, CPSSs can realize real-time sensing [3], dynamic control [4], and information services [5], which can be expected to revolutionize our industrial paradigm [6] and improve the quality of human life [7]. However, extensive deployment of devices in CPSSs has made scarce spectrum resources even more worse. It is necessary to develop a new spectrum scheduling strategy to optimize available spectrum allocation and improve spectrum utilization.

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

Spectrum allocation in current wireless communications is static. The spectrum is allocated fixedly by the government (e.g. Federal Communications Commission or State Radio Regulation of China) and authorized to licensed users or licensed services. According to the static allocation strategy, spectrum resources can be divided into two categories, i.e., licensed spectrum and license-free spectrum. Although the static allocation strategy improves quality of service of licensed users, the spectrum utilization is rather low due to the fact that licensed users do not continuously utilize their assigned spectrum [8]. To make full use of spectrum resources, researchers present dynamic spectrum allocation strategies, such as the cognitive radio (CR) technology [9]. In a CR network, an unlicensed user can access spectrum holes opportunistically [10], [11]. It is considered to be the best solution to cope with the low spectrum utilization of static allocation.

However, it is not enough to simply increase the spectrum utilization of licensed spectrum. In general, service providers, enterprises, and individual users may use the license-free spectrum to deploy numerous wireless devices [12]. Spectrum of different communication systems may partially or completely overlap, resulting in co-channel interference. The interference among devices will be more serious along with the large-scale application of wireless devices, thereby reducing system availability and user experience. Also, the device deployment mode of license-free spectrum access is usually a point-like and scattered layout, causing hard to scale networks [13]. Moreover, there is no a uniform and consistent standard for wireless access. To cope with the surge in wireless services, the stability and sustainability of using license-free spectrum is a general trend. Thus, how to manage the license-free spectrum resources effectively is an urgent issue.

It is necessary to establish a fair and efficient spectrum competition access mechanism. The existing access mechanism to solve spectrum competition is listen-before-talk (LBT) [14], [15]. The core of LBT is spectrum sensing. A node can use the spectrum if it senses the spectrum is idle; otherwise it continues to sense until it finds an idle spectrum. It seems to solve the problem of spectrum contention by using LBT. Yet, there may exist errors in spectrum sensing, such as hidden terminals [16] and exposed terminals [17]. Moreover, when multiple nodes in a system simultaneously sense the same idle spectrum, there may be a persistent collision problem. The system may crash due to long-term collisions when the number of nodes is excessive.

The above LBT based access mechanism is an opportunistic access mechanism that means competition. In the process of competition, collisions are inevitable. This collision phenomenon is actually because there is no consensus. Competition and consensus are precisely the key research content of blockchain technology that is oriented to distributed systems. Therefore, it is reasonable for us to use the blockchain technology to solve the issue of dynamic spectrum access. At the same time, users of the spectrum are recorded in the blockchain, which is also conducive to the secure management of spectrum resources. In this paper, we propose a blockchain based spectrum framework in a edge computing system that is a semi-distributed network.[1] To the best of our knowledge, we are the first to use blockchain to achieve wireless spectrum access. Our main contributions are as follows.

- We present a semi-distributed wireless network consisting of servers (including a cloud center and fog servers) and edge nodes. In such a network, servers only provide storage, forwarding and synchronization services while edge nodes can communicate with each other in peer-to-peer (P2P) mode.
- We propose a Blockchain-KM protocol to improve transaction processing speed without losing general attributes of blockchain. The spectrum is divided into multiple channels. Each channel corresponds to a blockchain, resulting in the private chain as a multi-chain structure. Each chain consists of two kinds of blocks: key blocks and micro blocks. Key blocks are used to elect the corresponding spectrum license holder and micro blocks are used to record transactions.
- We propose a blockchain-based spectrum access mechanism. Once a node successfully finds a key block, it gets a spectrum license until the next key block is found. If the node does not want to use the spectrum during this time, it can lease the spectrum to other nodes.

The remainder of this paper is organized as follows. Recent studies (including spectrum access and blockchain) related to our work is summarized in Section II, where we highlighted the innovations of our work. In Section III, we introduce the semi-decentralized wireless network and present the blockchain based spectrum management framework. In this framework, we define two spectrum access methods (mining and auction) and two communication methods (P2P and cooperative communication), which require blockchain and smart contracts to provide support services. Meanwhile, in this section, we introduce the virtual currency required for transactions: Xcoin. Next, we specify the design of spectrum access based on blockchain in Section IV. We propose a Blockchain-KM protocol to support a dynamic cognitive radio system, where a proposed PoS-after-PoW mechanism to generate key blocks for determining primary users and a lower-PoW mechanism to generate micro block for recording transactions. These two types of blocks form a multi-chain structure. In Section V, we evaluate the performance of proposed spectrum access mechanism through theoretical analysis and simulation experiments. Finally, we conclude our work and present future studies in Section VI.

II. RELATED WORK

A. SPECTRUM ACCESS

Recently, there is no standard for unlicensed spectrum. LBT is the most common mechanism in wireless communications for unlicensed spectrum access, such as IEEE 802.11 medium access control protocols used in WiFi systems. The carrier sense multiple access and collision avoidance (CSMA/CA) principle in WiFi is an opportunistic access mechanism based on contention. In CSMA/CS, nodes need to monitor before accessing a channel. A user can access to a channel only if the channel is probed to be idle. CSMA/CA has been widely used and studied due to its simple architecture [18]. However, it is defective in spectrum utilization and vulnerable to collision, which may degrade system performance [19].

The above LBT mechanism is equivalent to a distributed spectrum access. To solve the collision problem, centralized spectrum access mechanisms are proposed to remove channel contention and monitoring errors [20], [21]. This mechanism means that there is a control center to be responsible for spectrum allocation and access of the entire network. Due to the existence of the control center,

[1] Cloud and fog nodes are regarded as semi-centralized nodes.

market-based spectrum access mechanisms have been extensively studied, especially auction-based [22], [23] and pricing-based [24], [25] spectrum access mechanisms. These auction-based works are characterized by fairer price competition and lower reliance on global information. Compared with auction-based spectrum access mechanisms, pricing-based spectrum access mechanisms more focus on how to price spectrum and require more information of users who compete in bidding.

Different from the LBT mechanisms, a central spectrum access mechanism may be more efficient. Yet, the central mechanism is not suitable for centerless networks (also called as distributed wireless networks). Currently, license-free spectrum is more suitable for distributed networks. Since license-free spectrum is free to the public, market-based spectrum access mechanisms are obviously no longer applicable unless unlicensed spectrum is publicly sold by the government.

In this paper, we pioneer the use of blockchain technology to achieve spectrum allocation in distributed wireless networks. Note that there are some recent researches [26], [27] using blockchains for spectrum access. But they only use blockchains as a way for trading. The authors used a blockchain as a decentralized database to verify and secure spectrum trading between primary users and second users in cognitive radio networks. Unlike these, we make full use of the mining mechanism of the blockchain to solve the problem of spectrum contention. A node that successfully finds a key block will become a temporary control center with the right to govern the spectrum, including occupy to use or auction. In this way, nodes in networks are all profitable and easier to reach consensus.

B. BLOCKCHAIN

Recently, a blockchain has only attracted much attention due to the emergence of bitcoin [28]. With the great success of bitcoin, the blockchain technology has been rapidly applied to many other fields, such as smart contract [29], human resource management [30], crowdsourcing [31], reputation systems [32], security services [33], [34], privacy preserving [35], supply chain [36], data verification [37], and Internet-of-Things [38]. In essence, it is a decentralized database used to record transactions and data in a trustless scenario. In a blockchain, a new block containing numbers of transactions can be linked to its previous block by the hash value of the previous block, as long as it is approved by the public. Due to this structural feature, once the data of a specific block in the blockchain is changed, it will cause the entire chain to collapse.

Different blockchain systems have different schemes to generate a new block. In a bitcoin system, proof of work (PoW) is used to find a new block. In PoW, users need to solve a hash mathematical problem, called as mining, to generate blocks for many years. However, its mining process requires a lot of computing ability due to the high complexity of solving the hash problem. Moreover, since transactions require storage and verification processes and there is an inherent time interval for generating a new block, the delay of transactions is very high. In general, the bitcoin system can only process 7 transactions per second [39].

Furthermore, some studies proposed the proof of Stake (PoS). It determines generators based on the quantity and time of holding virtual currency. Despite reduce the computational energy consumption, PoS introduces new problems [40], [41]. The mechanism that a user with the highest amount of stake has the right to generate a new block makes the blockchain easier to be centralized. Since the mining process is almost zero consumption, there exists a problem called nothing at stake in PoS systems. It means that bad behaviors do not bring losses, which may make it easier to do evil.

To reduce the delay of transaction processing, the authors proposed a Bitcoin-NG (Next Generation) protocol in [42]. They introduced two different types of blocks, named key blocks and micro blocks. The key block is generated by PoW and used for leader election. The elected leader can generate micro blocks that require no PoW to record transactions. Because micro blocks do not require PoW, the delay of transaction processing can be greatly reduced. However, Bitcoin-NG may pose a security risk for malicious miners releasing large amounts of micro blocks in a short time. In addition to the above general methods, there are several other well-established methods applied into different systems [41].

In this paper, we use the above-mentioned blockchain technologies to solve the issues of spectrum access. We design an framework based on blockchain to build a dynamic cognitive radio system. Since the existing consensus algorithms cannot be used directly in our spectrum access mechanism, we changed them to fit our mechanism.

First, we design a PoS-after-PoW mechanism to generate the key block so as to select a primary user (PU). Note that the hybrid mechanism of PoW and PoS is usually PoW-plus-PoS, which means that half of the generated blocks are generated by PoW, and half are generated by PoS. Therefore, in a PoW-plus-PoS system, e.g., Ethereum [43], both PoW miners and PoS miners can participate in the system consensus. Different from PoW-plus-PoS, our proposed PoS-after-PoW means that if multiple key blocks are generated simultaneously by different miners through the process of PoW, the miner with more Coin-age is elected as the PU. Here, PoS becomes a tool to eliminate forks.

Second, PUs may not always use spectrum, and the spectrum they get can be leased to users who need it. The results of spectrum transactions need to be recorded in the blockchain to ensure security. But if the transactions are recorded in key blocks generated by PoS-after-PoW, the transaction speed is too slow. To increase transaction speed, we design another type of block, micro block, to record transactions. Micro blocks can only be generated by PUs with a lower-level PoW, which not only guarantees transaction speed, but also saves energy.

Third, the key blocks and micro blocks must be on the same chain, so as to ensure that the blockchain cannot be tampered

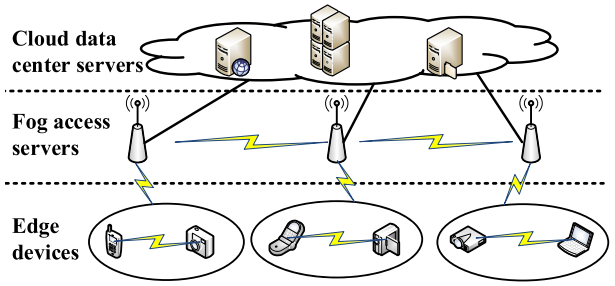


FIGURE 1. A semi-decentralized wireless system.

with and traceable. We design a multi-ring chain structure, using different hash value calculation methods to make them connected in series. The key to concatenation is the design of the first micro block (can be considered as the third type block) after a key block. Once a PU generates the key block, it needs to generate the first micro block immediately by non-PoW to play a connection role. Section IV details instructions on this.

In short, we use three consensus mechanisms (i.e., PoS-after-PoW, lower-level PoW and non-PoW) to design three different types of blocks, and use the hash value of the blocks to connect them into a multi-ring structure, which is different from any existing literature.

III. OVERVIEW

A. SYSTEM MODEL

We consider a wireless system including a cloud data center server, fog access servers and some edge devices, as shown in Fig. 1. The cloud data center server and fog access servers only provides data storage, forwarding and synchronization services.[2] They do not interfere with edge computing communications between edge devices. Edge devices can transmit messages with each other directly using unlicensed frequency bands or forward messages by a fog access server for communications without directly reachable. Obviously, the system is semi-decentralized because the servers, regarded as semi-centralized nodes, provide cooperative services instead of limiting node behaviors. In the system, all nodes may occupy spectrum resources so as to cause serious co-frequency interference. It is difficult to manage spectrums for the semi-decentralized wireless network due to the characteristics of distribution, openness, dynamic, and large-scale.

B. A BLOCKCHAIN BASED SPECTRUM MANAGEMENT FRAMEWORK

To solve the collision of spectrum utilization, we propose a blockchain based spectrum management framework in Fig. 2. The framework consists of the service plane, the access plane, and the transport plane. The details of each plane are as follows.

[2]Note that the cloud data center server and fog access servers can be connected wirelessly or wired.

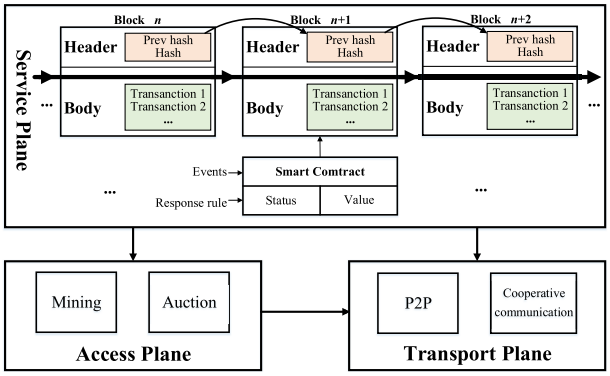


FIGURE 2. A blockchain based spectrum management framework.

1) THE SERVICE PLANE

This plane sends request information to the access plane and the transport plane. It contains three units.

- **A blockchain unit** is used to store the block information, transaction information, and spectrum access information. We utilize the non-tamperable and traceable features of a blockchain to protect privacy and data authenticity.
- **A smart contract unit** allows for credible transactions without the third party, which can be tracked and irreversible. One of the parties of the transaction applies to establish a smart contract, and the miner who generated the block attaches it to the block [44], [45]. The contract is executed automatically by the preset instruction that cannot be changed by the third party. The way that does not require mutual trust between the two transaction parties is suitable for distributed networks.
- **A payment unit** is responsible for managing users' virtual wallets. A user can pay for transaction fees by Xcoin in their wallets. Xcoin, e.g., the access spectrum, means a virtual currency, just like Bitcoin or Ethereum. It can be obtained by mining or bought by real currency. Note that Xcoin can be exchanged with various virtual currencies of other platforms.

2) THE ACCESS PLANE

This plane is used to issue spectrum access licenses. In our wireless system, an edge node does not own a spectrum access license continuously. Each license corresponds to an available wireless channel within a certain period. The license is valid only for a period and will be withdrawn afterwards. Two ways to obtain a spectrum access license are mining and auction.

In the system, a node can be as a miner to mine for a spectrum access license. Once the node mines a spectrum access license, it can use the license to transmit its messages via the corresponding channel. If the node does not want to transmit any messages, it can auction its spectrum access license to redeem Xcoin. In this case, other users may bid the spectrum access license. This spectrum access mechanism

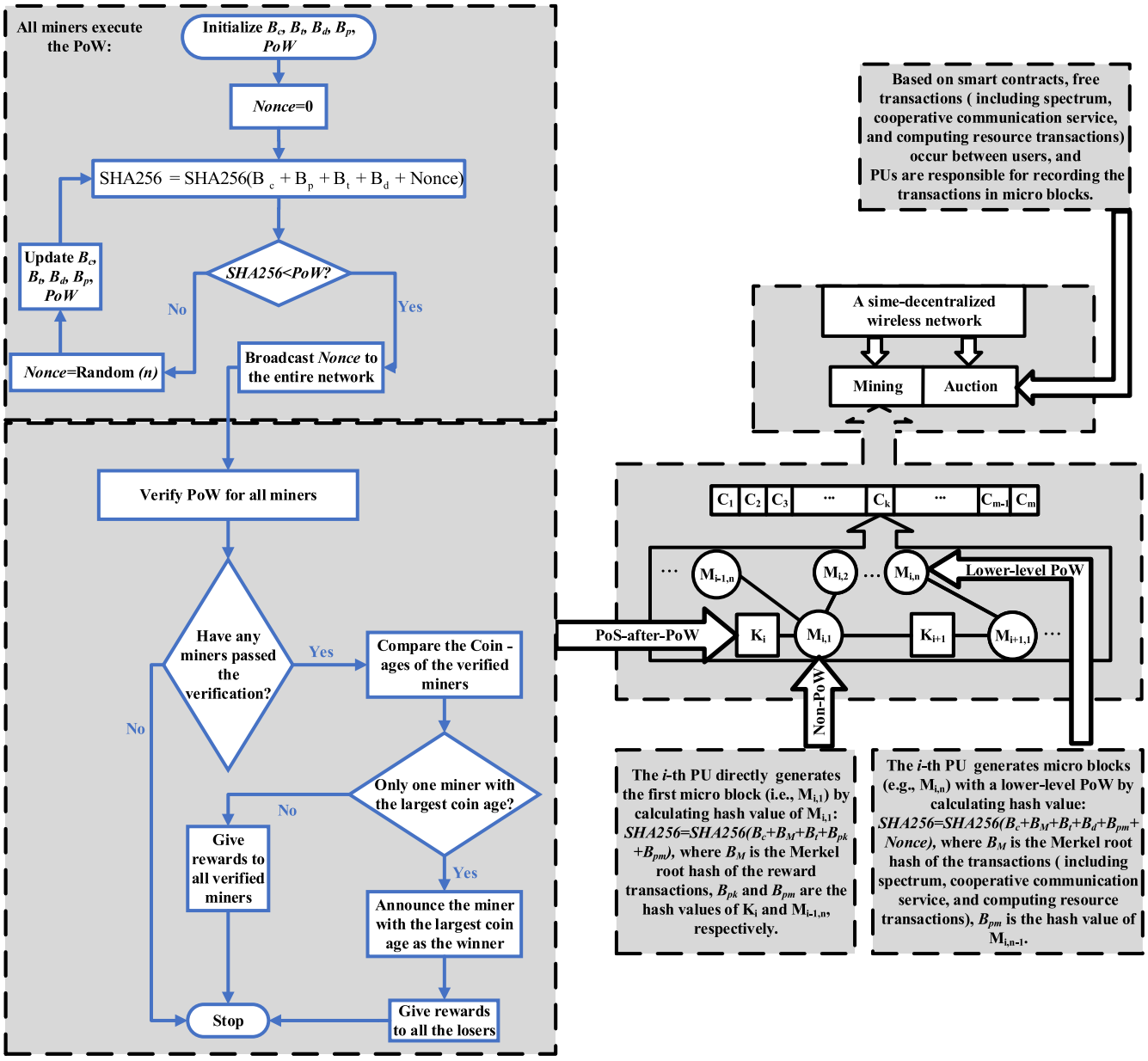


FIGURE 3. A flow chart of our blockchain based spectrum access mechanism.

is similar to a CR system with non-fixed primary users. The details will be discussed in the next section.

3) THE TRANSPORT PLANE

A node with a spectrum access license can transmit messages in P2P mode. However, once its transmission distance is limited or it wants to improve the throughput, it can turn to other nodes (including other edge nodes or fog access servers) for cooperative transmission. If the node needs other nodes to help achieving edge computing, fog computing or even cloud computing, it can also make requests within the time period when it holds the spectrum. As a reward, these cooperators can win Xcoin, which is also a transaction.

IV. BLOCKCHAIN BASED SPECTRUM ACCESS DESIGN

In this section, we propose a blockchain based spectrum access mechanism for the semi-decentralized wireless network, as shown in Fig. 3. We divide available spectrum resources into m orthogonal subchannels, and select two of these orthogonal subchannels as common channels.[3] The first common channel C_1 is used to broadcast common information, including blockchain update information, transaction

[3]The reason for dividing multiple channels is to use orthogonal frequency division multiplexing technology to improve spectrum utilization, and it is also convenient for users to choose channels that are more favorable for them to access (fading coefficients are different for different frequencies). The reason why the two control channels are separated is to eliminate interference to other channels.

information, auction information, and bidding information. The second common channel C_2 is only used for synchronization. Nodes can send a synchronization request and receive synchronization information via C_2. We assume that all channels are reliable and are equally divided into $T_1, T_2, \ldots, T_n, \ldots$ time slots. The slot length T_{slot} can be adjusted according to the system requirement.

In Fig. 3, we provide a flowchart of our blockchain based spectrum access mechanism, which is divided into two types of spectrum access methods: mining and auction. Each subchannel corresponds to a block chain, which is composed of key blocks and micro blocks. Nodes in the network can choose any blockchain to perform the mining process. If a key block is successfully mined, the node can become the PU of the channel corresponding to the blockchain. Other nodes that do not become a PU are secondary users. PU has the right to access and use the frequency spectrum of the subchannel. If the PU does not want to use the acquired spectrum, it can lease the spectrum to secondary users through auctions. Micro blocks are used to record transaction information, including spectrum, cooperative communication service, computing resource transactions and so on.

Next, we will describe the above process in detail.

A. MINING ACCESS PROCESS

In general, a fork should be avoided in the design of a blockchain system. However, our spectrum access mechanism does need to use forks to achieve better performance of spectrum resource management. The blockchain in our mechanism is a multi-chain system, in which each chain corresponds to one channel. In such a blockchain system, we put forward a key-micro blockchain protocol, called as Blockchain-KM. The blocks in Blockchain-KM are divided into two types, i.e., key blocks used for the replacement of spectrum owners and micro blocks used for recording transactions. Each block contains a hash value of the previous block. This blockchain structure has faster transaction processing speed and lower energy consumption without losing typical attributes of common blockchains. The proposed Blockchain-KM makes each blockchain of a channel become a chain with multiple rings, as shown in Fig. 4.

In the Blockchain-KM, there is a PU on each chain. The PU governs one period, generates micro blocks to record transactions, and is responsible for synchronization. As a reward, the PU will get a spectrum access license. Moreover, the PU helps other nodes complete blockchain synchronization and records transactions to obtain service fees. The system security guarantee is achieved through the public's supervision of PUs and the incentive mechanism of the blockchain-KM to motivate all nodes to comply with the rules. Next, we specify the implementation process of Blockchain-KM.

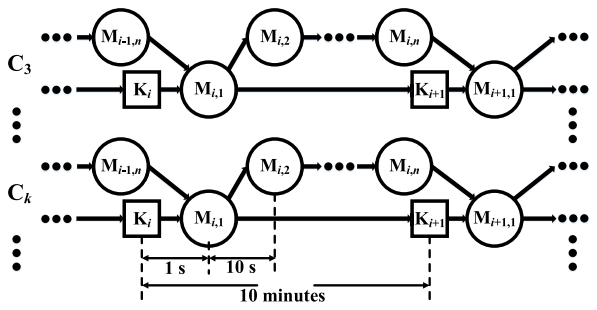


FIGURE 4. The multi-ring-blockchain structure.

1) THE GENERATION OF KEY BLOCKS

A key block is used to elect a new PU. It contains the hash value of the first micro block generated by the previous PU, the channel identifier, the time stamp, and the founded nonce value. To generate a key block is actually to calculate the hash value of the latest data and generate a new block. We can achieve key blocks generation by following six steps.

- A miner chooses a chain to run for a new PU, i.e., choosing a blockchain corresponding to a certain channel to mine. Then we obtain the selected channel identifier B_c.
- Update the hash value of the first micro block generated by the current PU, B_p.
- Update Timestamp B_t. Here, B_t is the current Greenwich Mean Time.
- Update the current difficulty value B_d. The difficulty value B_d is to determine how many times the miner needs to perform a hash operation to produce a legal block. For different network computing abilities, the difficulty value is automatically adjusted to make the time of generating a block basically unchanged. If the difficulty value is automatically adjusted every b blocks, and one block is expected to be generated every t minutes, then the difficulty value is updated as follows.

$$B_d = B_d^{(-1)} * \frac{t * b}{t_b}, \tag{1}$$

where $B_d^{(-1)}$ is the previous difficulty value and t_b represents the time spent in the past b blocks.
- Try different random numbers *Nonce* and perform hash calculations.

$$SHA256 = SHA256(B_c + B_p + B_t + B_d + Nonce). \tag{2}$$

- Perform PoW for verification. Compare $SHA256$ with a target value PoW to check if $SHA256$ is reasonable, where the target value PoW is calculated by

$$PoW = \frac{Target}{B_d}, \tag{3}$$

where *Target* is a constant with the first few digits being 0. The more the number of 0, the harder it is to mine. If $SHA256 \leq PoW$, the miner creates a new block and broadcasts the block to the entire network. Otherwise, repeat the previous steps.

The above steps to generate a key block can be summarized as **Algorithm 1**.

Generating a new key block does not mean the node will become a new PU due to the forking problem, i.e., many

Algorithm 1 PoW for Generating a Key Block

Input:
The selected channel identifier B_c;
The current B_t, B_d, B_p, PoW.
Output:
B_t, B_d, B_p, $Nonce$;
A new key block of the corresponding channel.

Set $Nonce = 0$;
Set $SHA256 = PoW + 1$;
while $SHA256 > PoW$ **do**
  Update $Nonce = Random(n)$;%Generate a new integer randomly.
  Update B_p and B_t;
  Update B_d according to (1);
  Update PoW according to (3);
end while
The node broadcasts the found new block to the entire network.
return $(B_t, B_d, B_p, Nonce)$

Algorithm 2 The Election of a New PU

Input:
Nodes that have generated key blocks via **Algorithm 1**.
Output:
The new user of the corresponding channel.

if The server (fog node) is available to provide services **then**
  The server is selected as a decision maker.
  if The current PU is available to provide services **then**
    The current PU is selected as a decision maker.
  else
    The previous PU is selected as a decision maker.
  end if
end if
The decision maker sorts *Coin-age* of all nodes who have generated key blocks at the same time.
Select the node with the oldest *Coin-age* as the new PU.
Set the *Coin-age* of the new user to 0.
Announce the result through the common channel.

nodes may generate a key block at the same time. In order to solve this problem, we propose a scheme based on PoS.

PoS can offer interest based on the amount and timing of the virtual currency. In the PoS mechanism, the virtual currency held by one node will generate Coin-age (the age of coin[4]) over time. We consider that once a coin is spent to complete a transaction, the Coin-age of the coin used for the transaction will be reset to be zero. This means that the initial Coin-age of coins is 0, regardless of how the coins are obtained. In addition, once a node successfully finds a block recognized by the public, the Coin-age of all coins it owns is reset to 0. Assuming the annual interest rate is 0.05, every time a node consumes 365 Coin-age, it will get 0.05 coins as interest.

When using the PoS mechanism, we can compare the Coin-age of the two miners if they found a block at the same time, and then determine the oldest user as the winner of the mining process. Note that each node receives messages at a different speed. When two or more messages that find a block arrive at a node with a time difference less than $t_{\min}$, we believe that a block is found by multiple miners at the same time. Then the server will announce the new user is the ultimate winner. Yet, in case the server cannot provide the service (e.g., denial of service, DOS), we still need to have a node to announce the winner. It is reasonable to consider the current spectrum license owner (the current PU) to announce the new PU as the winner. In the worst case, the winner will be announced by the previous PU if the current PU is also failure. The election process of a new PU can be summarized as **Algorithm 2**.

[4]The concept of Coin-age can be explained as a simple example: each coin produces 1 Coin-age per day, that is, holding 10 coins for 30 days is equivalent to have 300 Coin-age.

Note that these nodes who have generated key blocks, though not eventually PU, should be rewarded with a certain amount of virtual currency, which in turn encourages miners to mine.

2) MICRO BLOCKS

Once a new PU is enthroned, the right to use the corresponding spectrum will be transferred to the new PU. The new PU has the right to generate micro blocks to help nodes in the network record transactions to get reward.

A transaction is effective only if it is recorded in micro blocks by a user. The user can use the virtual currency contained in the transaction only in the case that the transaction is verified. Therefore, users expect their transaction can be verified and record in a micro block as soon as possible. To motivate a PU to record transactions, the PU can charge transaction fees. In this case, the PU naturally wants to record as many transactions as possible for obtaining more rewards. To prevent a malicious PU from submerging the system with micro blocks, we set the maximum rate of micro blocks generation. The generation interval between two micro blocks cannot be less than a threshold. Therefore, micro blocks should be generated by a lower-level PoW, the difficult value of which is lower than that of the PoW in generating a key block.

After receiving the new PU's enthronement message, nodes will connect the new key block to the first micro block generated by the former PU. However, the new key block is not connected to other micro blocks, which will cause the floating of the micro blocks. Thus, it is necessary to create a micro block immediately once a PU is enthroned, so as to connect all blocks (including key blocks and micro blocks) with the hash values of their headers. To speed up this process, PoW is not required for the first micro block, i.e., the first

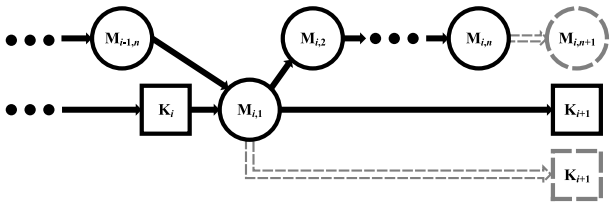


FIGURE 5. Forks in a multi-ring-blockchain.

micro block is generated by non-PoW. The non-PoW means that PUs does not need to calculate a qualified *Nonce*.

The header of the first micro block is different from other micro blocks generated by the same PU. The header of the first micro block contains the channel identifier B_c, the Merkle root hash of these reward transactions B_M, the time stamp B_t, the hash value of the new key block B_{pk}, and the last micro block generated by the former PU B_{pm}.

After generating the first micro block, the new PU generates micro blocks by a lower-level PoW based on the hash value of the first micro block. The block body of these micro blocks (except the first micro block) contain spectrum transactions that has not been recorded at the current moment. The block header of these micro blocks contain the channel identifier B_c, the Merkle root hash of these spectrum transactions B_M, the time stamp B_t, the hash value of the first micro block B_{pm}, a lower-level difficult value B_d, and a random number *Nonce*.

Fig. 4 illustrates the multi-ring-blockchain structure. In the figure, C_i represents the blockchain of the i-th channel. The circles and squares represent micro blocks and key blocks, respectively. K_i is the key block generated by the i-th user, and $M_{i,k}$ is the k-th micro block generated by the i-th user. Here, 1 seconds, 10 seconds and 10 minutes are examples referred to Bitcoin.[5] The blocks in the figure is connected though the previous hash value, which cannot be tampered with. Once a block is tampered with, its hash value will change, and then affect the following blocks.

3) FORKS

A fork may occur when more than two blocks are generated at the same time. Take Fig. 5 as an example. There are two kinds of forks in the multi-ring-blockchain. In this case, we should avoid forks by using the PoS mechanism. If PoS cannot solve this problem, all nodes that discover key blocks at the same time cannot become a new PU. Then they will be rewarded with a certain amount of virtual currency as compensation. For the conflict between a micro block and a key block, the fork problem can be avoided as long as all nodes wait for one more time slot after receiving the micro block. And the nodes may connect the micro block to the blockchain if a new key block is not received after a time slot; otherwise, the micro block will be discarded.

[5]The average time for a block to be generated is 10 minutes in Bitcoin system [28].

4) SYNCHRONIZATION AND THE ADDITION OF NEW NODES

Synchronization is to ensure the consistency of the blockchain data at each node, and miners need the hash value of the previous block to perform mining, so synchronization plays an important role in the blockchain. When a node is offline for a long time, the node needs to synchronize the current data, including the blockchain and users' information $v_i, i \in \{1, 2, \ldots\}$. All synchronous data is transmitted through the second common channel C_2. The node who wants to get the synchronization data needs to broadcast a synchronization-request frame (SRF) in C_2. Then, fog access servers will send the synchronous data after receiving the SRF. Yet, if the server denies providing services, the current PU is responsible for sending the synchronous data. Also, the previous PUs are in charge of synchronization if the current PU does not respond.

If a new node wants to join in the network, it needs to broadcast a join-request frame (JRF) as well as its public key in C_2. After receiving the JRF, fog access servers will assign an ID to the node and broadcast to the entire network. Then the synchronous data also needs to be broadcast by the servers. Similarly, if the servers denies providing services, the current user and the previous users may respond it in turn.

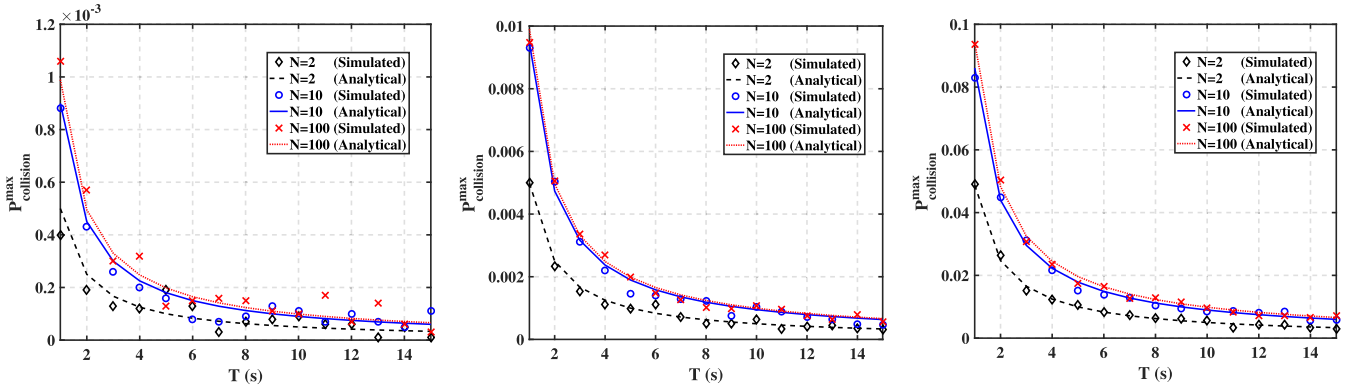
B. THE MARKET-BASED ACCESS MECHANISM

Once the PU is determined, the system can evolve into a dynamic cognitive radio network (CRN). All methods to improve the performance of CRNs can be used in the blockchain based spectrum management framework. In particular, the market-based access mechanism, including the auction-based spectrum access mechanism and the pricing-based spectrum access mechanism can be used more effective in our system. The reason is that we exploit a smart contract-based trading mechanism. Using blockchains and smart contracts to conduct spectrum transactions can achieve faster transaction speed. All transactions are recorded in micro block of the blockchain and updated by miners. The blockchain is then used to validate all transactions, so as to improve and secure leasing of spectrum.

After a miner obtains a spectrum license, it can use it by himself or lease to other users. We do not introduce the specific leasing strategies due to existing extensive researches.

C. THE COOPERATIVE COMMUNICATION STRATEGY

Cooperative communication [46] is regarded as an effective way to improve network performance. A user can select other users as cooperative relays to improve system throughput. In return, the user need to pay for assistance by other users. The transactions can also be completed through blockchains, which may increase the transaction speed. Therefore, the system performance can be further improved when using cooperative communication. We also omit the details of cooperative communication systems because of numerous existing references [47].



(a) $t_{\min} = 1$ ms (b) $t_{\min} = 10$ ms (c) $t_{\min} = 100$ ms

FIGURE 6. The collision probability for different parameters.

D. EDGE COMPUTING WITH NON-REAL TIME DATA

If an edge user has a computing task that requires the cooperation of other nodes, the user can release the task after getting a spectrum license. If the task is difficult, the user can invite multiple people to complete it together, i.e., distributed edge computing.[6] Other edge users can bid a computing task and get virtual currency rewards after completion. Note that edge computing is only applicable to non-real time data in our system. The reason is that the process of spectrum sensing takes a certain time, which may not satisfy the real-time requirements.

V. EVALUATION AND ANALYSIS

Since there are no existing similar models and methods, in this section, we only analyze the performance of the proposed blockchain based spectrum access mechanism.

A. MINING SIMULATION

In our experiments, we exploit replaced a Poisson process to achieve the PoW and define the mining power of a miner is h_i, $i \in 1, 2, \ldots, N$, where N is the maximum number of miners. Then, some assumptions list as follows.

- Whether the calculation of a mining machine produces a legal block can be considered as a random event, and all hash calculations are independent of each other.
- Each hash calculation has a corresponding computational difficulty, defined as D. This determines the difficulty to find a legal block.
- Each hash calculation has the probability of $\frac{1}{D2^{256}}$ to produce a legal block, e.g., 256-bit hash calculation has 2^{256} hash values.

Next, we present **Lemma 1** to describe the time T that the expected time for our system to produce a legal block. Here, T can be adjusted by D to an expected value, referring to Section IV-A.

[6]The user can also apply for computing based on cloud servers or fog servers, but it needs to pay extra fees to occupy shared resources.

Lemma 1: The time T obeys the exponential distribution with the parameter α, the probability distribution function (PDF) of which can be given by

$$f_T(t) = \begin{cases} \alpha e^{-\alpha t} & t > 0 \\ 0 & t \le 0, \end{cases} \tag{4}$$

where $\alpha = \sum_{i=1}^{N} \alpha_i$ and $\alpha_i = \frac{h_i}{D2^{256}}$.

Proof: See Appendix A. □

Based on **Lemma 1**, we can analyze the collision probability in the blockchain based spectrum access mechanism. It can be described by the probability that two nodes find a key block at the same time, which can be given by **Lemma 2**.

Lemma 2: Given N, T, $\{\alpha_i\}_{i=1}^{N}$, and $t_{\min}$, we can calculate the probability of collision that is given by

$$P_{collisoin} = \sum_{m=1}^{N} \frac{\alpha_m}{\alpha_m + \beta_m} \left(1 - e^{-\beta_m t_{\min}}\right), \tag{5}$$

where $\beta_m = \sum_{j=1, j\neq m}^{N} \alpha_j$.

Proof: See Appendix B. □

Furthermore, we can summarize an insight into the collision probability, which is shown as **Proposition 1**.

Proposition 1: When the abilities of all nodes are equal, i.e., $\alpha_1 = \alpha_2 = \ldots = \alpha_N = \frac{\alpha}{N}$, the collision probability is the largest and can be calculated as follows.

$$P_{collisoin}^{\max} = 1 - e^{-\frac{(N-1)\alpha}{N} t_{\min}}. \tag{6}$$

Proof: See Appendix C. □

In addition to the above theoretical analysis, we also provide the experiment results, as shown in Fig. 6. Assuming all nodes have the same computational abilities in the experiments, we analyze the maximum collision probability based on different parameters. Note that we do not introduce the PoS mechanism that can further reduce the collision probability in the experiments. It can be seen that the collision probability is low under various parameters. And the collision probability increases as the number of nodes increases but does not exceed a certain upper limit, which shows that our blockchain based spectrum access mechanism has advantages

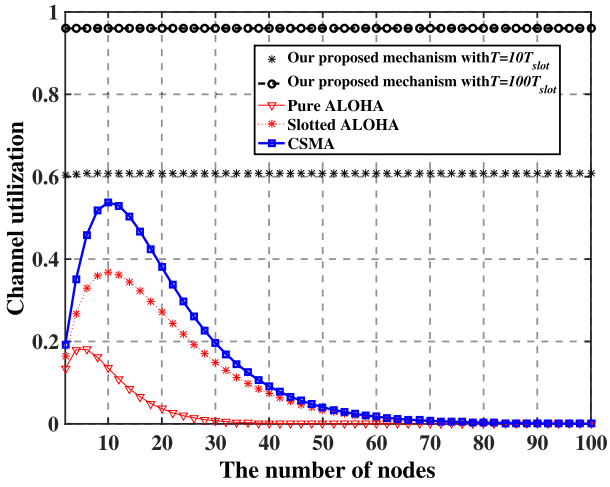


FIGURE 7. Comparison of spectrum access mechanisms.

when facing a large number of devices participating in spectrum access. This can be explained from **Propositon 1**:

$$\lim_{N\to\infty} P_{collisoin}^{\max} = 1 - e^{-\alpha t_{\min}}. \tag{7}$$

In reality, T and $t_{\min}$ should be set according to system requirements. Here, we present the impact of these parameters on the system in Fig. 6. The collision probability decreases as T increases, but increases along with the increase of $t_{\min}$. The reason is that the shorter T is the faster the key block is generated. It leads to the faster replacement of the previous user. In this case, nodes may be not willing to participate in auctions to lease spectrum due to easy mining. Thus, T should be set a little longer.

The proposed microblock strategy provides users with an alternative spectrum access opportunity. It is not only guarantee transaction speed but also has robustness to forking. If a node is eager to access spectrum to transmit messages as soon as possible, it may participate in the spectrum auction. On the contrary, if a node is not in a hurry to access spectrum, it may conduct mining. And the spectrum resource acquired in the mining way can be used for a longer period. In addition, $t_{\min}$ depends on the network scale. Taking into account the communication delay, $t_{\min}$ should be set slightly larger when the coverage of the network is larger.

In Fig. 7, we compare the performance of our proposed blockchain based spectrum access mechanism with the existing approaches (i.e., Pure ALOHA [48], Slotted ALOHA [49] and CSMA [50]) in terms of channel utilization. Here, the channel utilization means the proportion of the number of time slots used to transmit users' private information to the total number of time slots. During the implementation of our mechanism, we counted 10,000 time slots and set two different implementation schemes: $T = 10T_{slot}$ and $T = 100T_{slot}$, where $T_{min} = T_{slot}$. We assume that the probability that each node wants to transmit a message is 10%, that is, not all nodes want to send a message in a certain time slot. As we can see from Fig. 7, when the number of nodes in the network is large, the channel utilization of the existing methods will decrease sharply. However, our proposed schemes are less affected by the number of nodes. It is worth noting that as T increases, the channel utilization of our mechanism increases. This is because the replacement of the spectrum usage right will cause communication overheads, and these overheads will occupy some time slots. A smaller T means more frequent replacement of the spectrum usage right, and the proportion of overheads will increase, thus leading to a decrease in channel utilization.

B. SECURITY ANALYSIS

We analyze the secure performance of the proposed framework from the following aspects.

1) ACCESS SECURITY

Nodes must be verified before accessing spectrum. A system can stop malicious nodes from access spectrum if nodes do not participate in mining or auctions. Moreover, if a node maliciously occupies channels regardless of the network consensus, it can be easily discovered by the public and classified into the malicious list. Therefore, complying with network rules is more in line with interests of nodes themselves.

2) TRANSACTION SECURITY

Only transactions confirmed by both sides can be verified. Each transparent transaction is verified, and then stored in a block. Since blockchain is treated as a distributed data set, the transaction may be stored at many distributed nodes, which avoids tampering by malicious nodes.

3) RESISTANCE TO SINGLE POINT ATTACK

Although our network is semi-decentralized, there may still be a single point failure problem. For example, servers for synchronizing data and nodes for generating micro blocks may be rebellious or attacked by malicious nodes. This will lead to a single point of failure and trigger a denial of service. Therefore, we propose the scheme that the current PU and the previous PUs work together to generate micro blocks and assist servers to achieve synchronization, so as to avoid single-point attacks. PUs can be rewarded by obeying the rules of completing tasks, which eliminates the motivation for betrayal.

4) SOLUTION TO CENTRALIZED COMPUTATIONAL ABILITY

The single PoW mechanism not only consumes energy, but also has the problem of centralized computational ability. If a node wants to take full control of the entire network, it needs to have more than 51% of the computational ability of the entire network, which is obviously impossible. However, it is possible for some collusive malicious nodes to achieve 51% of the computational ability. Therefore, we adopt the mechanism of PoS-after-PoW to achieve network consensus. In this case, the entire network can only be controlled when malicious nodes control 51% of the computing power as well as 51% of Coin-age, which is difficult to achieve. Even if

malicious nodes control the network, it is impossible to control all the time, because Coin-age will be cleared after use.

C. APPLICABILITY ANALYSIS

Blockchain is indeed a technology that consumes resources and incurs a lot of overhead. Our blockchain based spectrum access mechanism also suffers from these limitations. Therefore, when designing microblocks, we reduce the difficulty of PoW, and only allow PUs to generate microblocks to reduce energy consumption. To reduce storage resource consumption, edge devices store recent blockchain data, and all the data is stored in the cloud center or fog access servers, which can be retrieved if necessary. This three-level storage method can also avoid a single point of failure and ensure decentralization. Although we have put effort into designing our scheme to alleviate these limitations involving resource consuming, the participating devices are still required to have excess resources to support the operation of the blockchain system. In addition, because the process of obtaining spectrum takes time, our spectrum access mechanism is limited in the real-time transmission of data.

VI. CONCLUSION

In this paper, we pioneer a blockchain-based spectrum access mechanism for unlicensed spectrum in semi-decentralized wireless networks. The proposed spectrum access mechanism can be applied to the non-real time data transmission and processing for edge computing in CPSSs due to existing a certain access delay. We make full use of mining in blockchains to solve spectrum contention. A Blockchain-KM protocol is proposed to achieve spectrum allocation and transaction recording in a network. In the proposed Blockchain-KM protocol, our blockchain is a private chain with a multi-ring structure, in which two types of blocks (key blocks and micro blocks) are adopted. A node needs to mine a key block by the proposed PoS-after-PoW mechanism to become a licensed user. For those nodes that do not become the licensed user, we propose a blockchain based spectrum leasing mechanism. The transactions in auctions are recorded in micro blocks that are generated by a lower-level PoW to reduce transaction delay. In addition, we analyze the collision of key blocks and present the performance analysis of the blockchain-based spectrum access mechanism. In future work, we will study blockchain-based spectrum auction mechanisms, blockchain-based cooperative transmission and cloud-fog-edge computing schemes. In view of the drawback of PoW consuming resources, we will also study other lightweight consensus algorithms to apply to our framework.

APPENDIXES

APPENDIX A
PROOF OF LEMMA 1

Based on the previous definitions and assumptions, the number of legal blocks that the miner M_i can produce per second obeys the Poisson distribution with the parameter $\alpha_i = \frac{h_i}{D2^{256}}$. Then, the time X_i required for the miner M_i to produce a legal block obeys the exponential distribution with the parameter α_i. The cumulative distribution function (CDF) of X_i can be given by

$$F_{X_i}(x) = \begin{cases} 1 - e^{-\alpha_i x} & x > 0 \\ 0 & x \leq 0. \end{cases} \tag{8}$$

Since one of miners produced a legal key block, the mining process ends. Therefore, the time T for the system to generate a legal block should be

$$T = \min\{X_1, X_2, \ldots, X_N\}. \tag{9}$$

Accordingly, the CDF of T can be given by

$$F_T(t) = 1 - \prod_{i=1}^{N}[1 - F_{X_i}] = \begin{cases} 1 - e^{-\alpha t} & x > 0 \\ 0 & x \leq 0 \end{cases} \tag{10}$$

where $\alpha = \sum_{i=1}^{N} \alpha_i$. And then we can obtain the PDF of T. This completes the proof of **Lemma 1**.

APPENDIX B
PROOF OF LEMMA 2

Define $Y = \min\{X_1, \ldots, X_{m-1}, X_{m+1}, \ldots, X_N\}$, then we can deduce that Y obeys the exponential distribution with the parameter $\beta_m = \sum_{j=1, j\neq m}^{N} \alpha_j$ based on **Lemma 1**. The PDF of Y is as follows.

$$f_Y(y) = \begin{cases} \beta_m e^{-\beta_m y} & y > 0 \\ 0 & y \leq 0. \end{cases} \tag{11}$$

If the miner M_m first finds a legal key block, the probability that other miners also find a legal key block at the same time can be calculated as

$$\begin{aligned} P_m &= P\{X_m > 0, Y > 0, Y \geq X_m, Y - X_m < t_{\min}\} \\ &= \int_0^{\infty} f_{X_m}(x_m) \int_{x_m + t_{\min}}^{x_m} f_Y(y) dy dx_m \\ &= \int_0^{\infty} [e^{-\beta_m x_m} - e^{-\beta_m (x_m + t_{\min})}] \alpha_m e^{-\alpha_m x} dx_m \\ &= \frac{\alpha_m}{\alpha_m + \beta_m}(1 - e^{-\beta_m t_{\min}}). \end{aligned} \tag{12}$$

Then we can calculate the final collision probability as

$$P_{collision} = \sum_{m=1}^{N} P_m = \sum_{m=1}^{N} \frac{\alpha_m}{\alpha_m + \beta_m}(1 - e^{-\beta_m t_{\min}}). \tag{13}$$

The proof of **Lemma 2** is complete.

APPENDIX C
PROOF OF PROPOSITION 1

Given N, T and $t_{\min}$, we should solve the following problem to obtain the maximum collision probability.

$$P1: \max_{\{\alpha_i\}_{i=1}^{N}} P_{collision} \tag{14a}$$

$$s.t. \sum_{i=1}^{N} \alpha_i = \alpha. \tag{14b}$$

After reorganization, **P1** can be transformed into

$$P2: \min_{\{\alpha_i\}_{i=1}^{N}} \frac{\sum_{i=1}^{N} \alpha_i e^{\alpha_i t_{\min}}}{\alpha e^{\alpha t_{\min}}} \tag{15a}$$

$$s.t. \sum_{i=1}^{N} \alpha_i = \alpha. \tag{15b}$$

Obviously, **P2** is a convex optimization problem that can be easily solved using the Lagrangian multiplier method. Here, the solution process is omitted. Ultimately, we can get the optimal solution as $\{\alpha_1 = \alpha_2 = \ldots = \alpha_N = \frac{\alpha}{N}\}$. The proof of **Proposition 1** is complete.

ACKNOWLEDGMENT

The authors would like to thank all reviewers who have helped improve this manuscript.

REFERENCES

[1] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: Privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1868–1878, Dec. 2017.

[2] J. Mao, W. Tian, Y. Yang, and J. Liu, "An efficient social attribute inference scheme based on social links and attribute relevance," *IEEE Access*, vol. 7, pp. 153074–153085, 2019.

[3] X. Wang, L. T. Yang, X. Xie, J. Jin, and M. J. Deen, "A cloud-edge computing framework for Cyber-Physical-Social services," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 80–85, Nov. 2017.

[4] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6492–6499, Dec. 2019.

[5] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 144–153.

[6] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE J. Sel. Areas Commun.*, to be published.

[7] X. Wang, L. T. Yang, L. Kuang, X. Liu, Q. Zhang, and M. J. Deen, "A tensor-based Big-Data-Driven routing recommendation approach for heterogeneous networks," *IEEE Netw.*, vol. 33, no. 1, pp. 64–69, Jan. 2019.

[8] P. Kolodzy and I. Avoidance, "Spectrum policy task force report," *Federal Commun. Commission*, vol. 40, no. 4, pp. 147–158, Nov. 2002.

[9] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, "Spectrum prediction in cognitive radio networks," *IEEE Wireless Commun.*, vol. 20, no. 2, pp. 90–96, Apr. 2013.

[10] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.

[11] R. H. Tehrani, S. Vahid, D. Triantafyllopoulou, H. Lee, and K. Moessner, "Licensed spectrum sharing schemes for mobile operators: A survey and outlook," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2591–2623, 4th Quart., 2016.

[12] X. Wang, L. T. Yang, Y. Wang, X. Liu, Q. Zhang, and M. J. Deen, "A distributed tensor-train decomposition method for Cyber-Physical-Social services," *ACM Trans. Cyber-Phys. Syst.*, vol. 3, no. 4, pp. 1–15, Oct. 2019.

[13] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Apr. 24, 2018, doi: 10.1109/TNSE.2018.2830307.

[14] Y. Song, K. W. Sung, and Y. Han, "Coexistence of Wi-Fi and cellular with Listen-Before-Talk in unlicensed spectrum," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 161–164, Jan. 2016.

[15] X. Xing, T. Jing, H. Li, Y. Huo, X. Cheng, and T. Znati, "Optimal spectrum sensing interval in cognitive radio networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2408–2417, Sep. 2014.

[16] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

[17] D. Vassis and G. Kormentzas, "Performance analysis of IEEE 802.11 ad hoc networks in the presence of exposed terminals," *Ad Hoc Netw.*, vol. 6, no. 3, pp. 474–482, May 2008.

[18] X. Wang, L. T. Yang, H. Li, M. Lin, J. Han, and B. O. Apduhan, "NQA: A nested anti-collision algorithm for RFID systems," *ACM Trans. Embedded Comput. Syst.*, vol. 18, no. 4, pp. 1–21, Jul. 2019.

[19] A. Sultana, X. Fernando, and L. Zhao, "An overview of medium access control strategies for opportunistic spectrum access in cognitive radio networks," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 5, pp. 1113–1141, Sep. 2017.

[20] C. Raman, R. D. Yates, and N. B. Mandayam, "Scheduling variable rate links via a spectrum server," in *Proc. 1st IEEE Int. Symp. New Frontiers Dyn. Spectr. Access Netw. DySPAN*, Nov. 2005, pp. 110–118.

[21] R. Yates, C. Raman, and N. Mandayam, "Fair and efficient scheduling of variable rate links via a spectrum server," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2006, pp. 5246–5251.

[22] Y. Zhang, C. Lee, D. Niyato, and P. Wang, "Auction approaches for resource allocation in wireless systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1020–1041, 3rd Quart., 2013.

[23] M. R. Hassan, G. C. Karmakar, J. Kamruzzaman, and B. Srinivasan, "Exclusive use spectrum access trading models in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2192–2231, 4th Quart., 2017.

[24] W. Lee and B. C. Jung, "Pricing-based distributed spectrum access for cognitive radio networks with geolocation database," *IET Commun.*, vol. 11, no. 5, pp. 733–738, Mar. 2017.

[25] F. Li, K.-Y. Lam, X. Li, X. Liu, L. Wang, and V. C. M. Leung, "Dynamic spectrum access networks with heterogeneous users: How to price the spectrum?" *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5203–5216, Jun. 2018.

[26] K. Kotobi and S. G. Bilen, "Blockchain-enabled spectrum access in cognitive radio networks," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2017, pp. 1–6.

[27] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[28] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[29] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.

[30] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang, and Y. You, "Human resource information management model based on blockchain technology," in *Proc. IEEE Symp. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2017, pp. 168–173.

[31] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "ZkCrowd: A hybrid blockchain-based crowdsourcing platform," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4196–4205, Jun. 2020.

[32] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Adaptive and Adaptable Learning*. Cham, Switzerland: Springer, 2016, pp. 490–496.

[33] C. Noyes, "BitAV: Fast anti-malware by distributed blockchain consensus and feedforward scanning," 2016, *arXiv:1601.01405*. [Online]. Available: http://arxiv.org/abs/1601.01405

[34] Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, and Z. Liang, "Man-in-the-browser-cache: Persisting HTTPS attacks via browser cache poisoning," *Comput. Secur.*, vol. 55, pp. 62–80, Nov. 2015.

[35] J. Wang, Z. Cai, and J. Yu, "Achieving personalized k-Anonymity-Based content privacy for autonomous vehicles in CPS," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4242–4251, Jun. 2020.

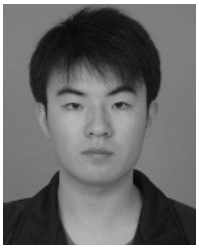
[36] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intell. Syst. Accounting, Finance Manage.*, vol. 25, no. 1, pp. 18–27, Jan. 2018.

[37] J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, and J. Liu, "A position-aware merkle tree for dynamic cloud data integrity verification," *Soft Comput.*, vol. 21, no. 8, pp. 2151–2164, Apr. 2017.

[38] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[39] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[40] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.
[41] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.
[42] I. Eyal, A. E. Gencer, and R. V. Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *Proc. Usenix Conf. Netw. Syst. Design Implement.*, 2016, pp. 45–59.
[43] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352, 2018.
[44] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, pp. 117–121.
[45] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
[46] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.
[47] A. S. Shah and M. S. Islam, "A survey on cooperative communication in wireless networks," *Int. J. Intell. Syst. Appl.*, vol. 6, no. 7, p. 66, 2014.
[48] M. Kaynia and N. Jindal, "Performance of ALOHA and CSMA in spatially distributed wireless networks," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1108–1112.
[49] C. Namislo, "Analysis of mobile radio slotted ALOHA networks," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 4, pp. 583–588, Jul. 1984.
[50] G. Bianchi, L. Fratta, and M. Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in *Proc. PIMRC 7th Int. Symp. Pers., Indoor, Mobile Commun.*, Oct. 1996, pp. 392–396.



XIN FAN received the B.E. and M.E. degrees from the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China, in 2016 and 2018, respectively. He is currently pursuing the Ph.D. degree with Beijing Jiaotong University. He was a Visiting Scholar with the Department of Electrical and Computer Engineering, George Mason University. His research interests include wireless communications and physical layer security.

YAN HUO (Senior Member, IEEE) received the B.E. and Ph.D. degrees in communication and information system from Beijing Jiaotong University, Beijing, China, in 2004 and 2009, respectively. Since 2011, he has been a Faculty Member with the School of Electronics and Information Engineering, Beijing Jiaotong University, where he is currently a Professor. From 2015 to 2016, he was a Visiting Scholar with the Department of Computer Science, George Washington University. His current research interests include wireless communication theory, security and privacy, cognitive radio, and signal processing.