

Received November 30, 2021, accepted January 7, 2022, date of publication January 21, 2022, date of current version February 2, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145444

# Cooperative Communication Method Based on Block Chain for a Large Number of Distributed Terminals

HUI ZHI<sup>1</sup>, HONGJIE GE, AND YONG WANG

Key Laboratory of Computational Intelligence and Signal Processing (Ministry of Education), Anhui University, Hefei 230601, China

Corresponding author: Hui Zhi (zhizhi\_0902@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 62001001, by the Natural Science Foundation of Anhui Province under Grant 1508085QF125, by the College Natural Science Research Project of Anhui Province under Grant KJ2016A042, and by the Start-Up Research Foundation of Anhui University under Grant 01001770.

**ABSTRACT** The cooperative communication of distributed terminals has many performance advantages and wide application prospects. However, it lacks effective trust foundation between distributed terminals and lacks data security guarantee. Block chain naturally has the properties of transparency, tamper-proof, and full traceability. It can effectively solve the trust problem between untrusted terminals and ensure data security. Thus, we introduce block chain into the cooperative communication of large number terminals, propose a cooperative communication method based on block chain, design a multi-chain structure to reduce resource consumption, and give the detailed working procedure of the cooperative communication method. In the working procedure, we propose a source-relay pairing and pricing scheme based on Kuhn-Munkres algorithm (SRPP-KM) to solve the optimal source relay pairing and transaction price, and design a lightweight consensus mechanism based on intra-region dynamic delegated Byzantine fault tolerant (DDBFT) and interactive updates between regional chain and main chain to reduce resource waste and achieve fast consensus. Analyses show that the proposed method can establish trust foundation between terminals and promote cooperation between terminals. Simulation results show that the proposed method can obtain higher sum revenue of sources while satisfying relays' expected revenue and achieve faster consensus when compared with other methods.

**INDEX TERMS** Cooperative communication, large number of distributed terminals, block chain.

## I. INTRODUCTION

With the development of Internet of Things (IoT) technology, the number of mobile terminals (MTs) has experienced explosive growth, and wireless networks have developed in the direction of heterogeneity, super density and edge intelligence. To meet the requirements of increasing transmission rates, system capacity and quality of service (QoS), network service providers are configuring more base stations (BSs) or wireless access points for the wireless network. However, this method not only increases the investment of network construction and maintenance, but also brings more complex wireless interference, so it cannot meet the network requirements effectively. More effective methods need to be found, and cooperative communication is one of the effective

methods, where one mobile terminal (MT) can act as relay to forward data for another MT. Thus, the system capacity can be improved, the number of BSs can be reduced, and the network interference can be reduced. Moreover, with the increasing number of intelligent terminals, cooperative information transmission and data sharing among distributed intelligent terminals has become an important development direction of wireless networks. As shown in Fig. 1, there are many application scenarios and many performance advantages of the cooperative communication of distributed terminals. For example, it can simplify network deployment, make network configuration flexible and convenient, improve spectrum efficiency, increase network coverage and improve signal quality for terminals with poor channels. Moreover, it can be used for cognitive radio network [1], emergency communication [2], cooperation information transmission between heterogeneous intelligent terminals [3], etc. Therefore,

The associate editor coordinating the review of this manuscript and approving it for publication was Yue Zhang<sup>1</sup>.

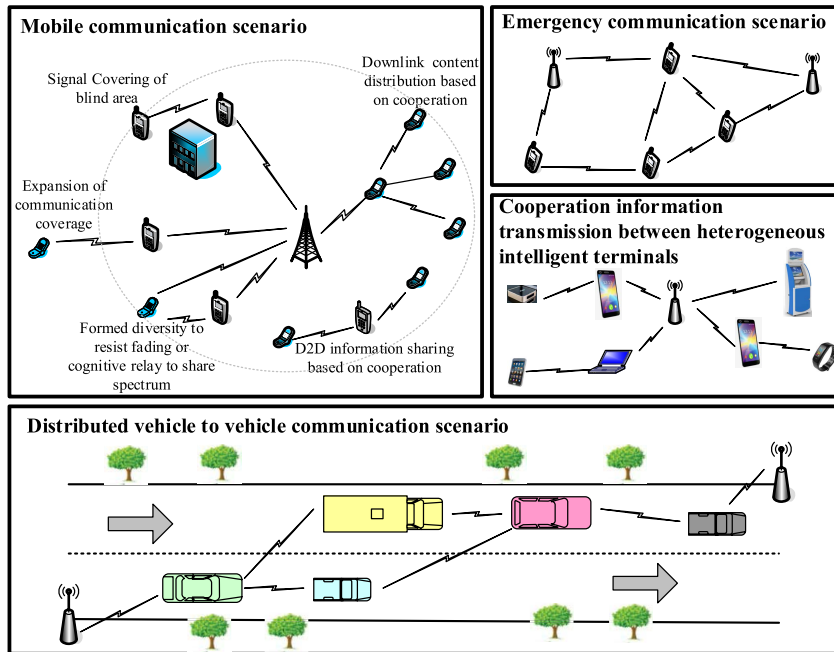


FIGURE 1. Application scenarios of cooperative communication of distributed terminals.

cooperative communication of large number MTs is an important research hot spot.

Although cooperative communication has many performance advantages and wide application prospects, terminals are selfish and it is difficult to establish mutual trust relationship directly. Most existing researches of cooperative communication were based on the assumption of complete trust between source and relay, in which the relay node voluntarily helps the source node to forward data [4]. However, in the real wireless network, it is difficult for distributed terminals to establish mutual trust relationship [5]. Taking the distributed vehicle to vehicle communication (shown in Fig.1) as an example, the relay vehicle needs to consume its own resource to forward data for source vehicle. If there is no effective economic behavior as the incentive mechanism, the selfish relay vehicle has no incentive to forward data for source vehicle. In addition, source vehicle may not trust relay vehicle due to the data tampering and privacy leakage at relay vehicle [6]. Therefore, we need to find an incentive mechanism to establish the trust foundation of distributed terminals, encourage terminals to cooperation, and improve the security of transmitted data.

Nowadays, there has been many researches about the incentive mechanism of cooperation communication, such as game theory [7], auction theory [8], social consciousness assistance [9], etc. But these incentive mechanisms [7]–[9] use a trust management center to coordinate management. Due to the existence of trust management center, the whole network becomes extremely vulnerable when the trust management center is attacked, and the security of transmitted data cannot be guaranteed.

The concept of block chain was first proposed by Satoshi Nakamoto in 2008 [10]. In recent years, the applications of block chain have developed rapidly, such as bitcoin payment system and Ethereum smart contract platform, etc. Block chain is a distributed ledger maintained by a peer-to-peer network, in order to make the transactions written in the ledger valid, the network participants must reach a consensus on these transactions. The operation of block chain network does not rely on any centralized trusted third-party. So block chain naturally has the properties of transparency, tamper-proof, and full traceability.

Existing researches on the application of block chain in wireless communication mainly focused on the terminal transaction and data privacy protection in IoT [11], computing task offloading in mobile edge computing [12], spectrum management [13], etc.

From [11]–[13], we can see that the trust between different individuals can be established through block chain. Therefore, this paper intends to introduce block chain (as an incentive mechanism) into cooperative communication of large number MTs to establish the trust foundation between MTs. In this block chain system, relay forwards data for source, can obtain the rewards (electronic money) paid by source. By writing this transaction information into block chain and making it public in an open and transparent manner, the deception between source and relay can be avoided, and relay can be motivated to forward data for source.

The main contributions of this paper are as follows:

1) We propose a cooperative communication method based on block chain for a large number of distributed MTs, design a multi-chain structure based on region division to reduce

resource consumption, give the detailed working procedure of the cooperative communication method.

2) We propose a source-relay pairing and pricing scheme based on KM algorithm (SRPP-KM). This scheme encourages terminals to cooperate through the transactions between source and relay, and uses Kuhn-Munkres (KM) algorithm to solve the optimal source-relay pairing and corresponding transaction price.

3) We propose a lightweight consensus mechanism based on intra-region DDBFT and interactive updates between regional chain and main chain (IRD-IURM). This consensus mechanism adopts consortium chain and DDBFT in each region, and it can reduce resource waste and achieve fast consensus.

## II. RELATED WORKS

### A. RELATED WORKS ABOUT COMBINATION OF BLOCK CHAIN AND COOPERATIVE COMMUNICATION

To the best of our knowledge, there has been very little research about the combination of block chain and cooperative communication, such as [14], [15]. Reference [14] added jammer at relay to prevent information from being eavesdropped on, and realized the transaction between source and relay's jammer based on an auction mechanism to ensure the security of the physical layer. The purpose of using block chain in [14] was to prevent information eavesdropping, whereas in our work, the purpose is cooperative information transmission. Thus, the model and analysis in [14] are totally different from ours.

Reference [15] introduced block chain into relay-assisted D2D communication to realize the incentive of cooperation between nodes. However, the system model in [15] is different from that in our work: reference [15] focused on the cooperation of a small number of terminals, while our work focuses on the cooperation of a large number of terminals. For a large number of terminals, the consensus mechanism consumes large terminal resources, so we design a multi-chain structure based on region division and a lightweight consensus mechanism in this paper to reduce resource consumption. By contrast, [15] did not mention what consensus mechanism should be used and did not consider the resource consumption of terminals.

### B. RELATED WORKS ABOUT CONSENSUS MECHANISM OF BLOCK CHAIN

Introducing block chain into the cooperative communication of large number MTs, we need to solve the problem of large resource consumption of consensus mechanism. In a distributed system of block chain, there is no management center, so a consensus mechanism is needed to ensure the reliability of block generation and verification. In existing consensus mechanisms, the proof of work (POW) protocol is one of the most important consensus mechanisms because of its simplicity and effectiveness. Its "mining" process is slow and long-term, takes up large computing resources and consumes a significant amount of energy. Its block verification

process requires many information exchanges, takes up large communication resources and affects the network throughput. For MT with limited resources and low delay requirements, it is difficult to deploy POW directly on MT.

Based on this, some researchers have proposed lightweight consensus algorithms, trying to reduce computing resource consumption, improve network throughput and reduce time delay of block verification. For example, [16] studied how to reduce the difficulty of "mining". Reference [17] introduced the consortium chain to solve the problem that ordinary devices cannot implement POW. The consortium chain can be regarded as a special block chain that maintains a distributed ledger through authorized institutions or some authorized nodes. In [18], POW was implemented on MT by offloading computing-intensive tasks (such as the consensus process) to an edge server. Reference [19] proposed proof of stake (POS) to replace POW, where the "miner" is selected based on the stakes that they are holding, and members with more stakes have higher chances to be "miner". [20] adopted delegated proof of stake (DPOS) consensus mechanism to reduce resource consumption. Similar to the POS or DPOS, [21] proposed a consensus mechanism based on user reputation, the user with the highest reputation is "miner". References [22] and [23] respectively used Byzantine fault tolerant (BFT) algorithm and dynamic delegated Byzantine fault tolerant (DDBFT) algorithm to reduce the information exchanges during block verification. The comparison of different consensus mechanisms in [16]–[23] is given in Table 1. For a certain number of terminals, the methods in [16]–[23] can reduce the computing resource consumption and execution time of consensus mechanism. However, these methods cannot be directly applied into the cooperative communication of large number MTs. For large number MTs, these consensus mechanisms [16]–[23] still consume large resources due to the large amount of information recorded and exchange, MT cannot bear such resource consumption. In addition, MT is mobile, and transaction information traceability of MT is still a problem need to be solved. So, it is necessary to find a lightweight consensus mechanism which is suitable for the cooperative communication of large number MTs.

### C. RELATED WORKS ABOUT SOURCE-RELAY PAIRING IN COOPERATIVE COMMUNICATION

There are many studies about source-relay pairing (or the relay selection for source) in cooperative communication. For example, [24]–[30] and [1] introduced a series of relay selection methods to improve system performance, such as opportunistic relay, partial relay selection, hybrid relay selection, relay selection with inter-relay cooperation, etc. The relay selection methods discussed in [24]–[30] and [1] were selecting one or more relays for a single source, not applicable to multi-source scenarios (source-relay pairing situations). References [31]–[36] tried to study source-relay pairing for multi-source multi-relay cooperative wireless network. Among them, [31], [32] discussed selection cooperation or

TABLE 1. Comparison of different consensus mechanisms in related works.

Consensus mechanisms of block chain	References	Application scenarios	Advantages	Disadvantages
POW	[16],[18]	Bitcoin, Ethereum, etc.	Decentralization, high security	High computing resource consumption, long block confirmation delay, low transaction throughput
Consortium chain	[17]	Vehicular ad-hoc networks, etc.	High transaction throughput, low computing resource consumption	Low degree of decentralization, poor fairness between nodes
POS	[19]	Cardano, Algorand, Bigchain DB, etc.	Low computing resource consumption, Short block confirmation delay	Low degree of decentralization, vulnerability to security threats
DPOS	[20]	EOSIO	High transaction throughput	Low degree of decentralization
Consensus mechanism based on user reputation	[21]	/	High security, Reputation serves as the incentive	Poor fairness between nodes
BFT	[22]	Hot-Stuff	Decentralization, high security	Not applicable to the case of a large number of nodes
DDBFT	[23]	/	Its consensus confirmation is faster than that of BFT	Its degree of decentralization is lower than that of BFT

coding cooperation scheme to improve diversity order. References [33] and [34] studied source-relay pairing for cognitive secondary user network to reduce the interference to the primary receiver. Reference [35] pointed out that in order to improve the system performance, the optimal source-relay pairing can be achieved by exhaustive search, but the computation complexity of exhaustive search is high. To reduce the computation complexity of source-relay pairing, [35] proposed a low-complexity relay selection method using weighted bipartite graph model. Reference [36] proposed a subset selection (SSS) method to reduce computation complexity. In the SSS method, each source finds its own optimal relay sequentially, so we call it “sequential relay selection scheme” in this paper. However, [31]–[36] did not consider block chain, and did not have incentive mechanism for terminal cooperation. In our work, we introduce block chain into cooperative communication to motivate terminals to cooperate and propose a source-relay pairing and pricing scheme based on KM (Kuhn-Munkres) algorithm to complete source-relay pairing and transaction pricing in block chain. In addition, we use a bipartite graph similar to [35] to reduce the computation complexity of source-relay pairing, although the system model of [35] is different from ours.

The comparison of different source-relay pairing (or relay selection) methods in [24]–[36] is given in Table 2.

**III. SYSTEM MODEL AND MULTI-CHAIN STRUCTURE**  
**A. SYSTEM MODEL AND MULTI-CHAIN STRUCTURE**  
**BASED ON REGION DIVISION**

Considering a wireless network with many BSs and a large number of MTs, when the uplink channel quality of source MT is poor, or the power of source MT is low, it is necessary to use another MT as relay to forward data, i.e., relay cooperative communication. As mentioned, in order to establish trust foundation between source and relay, we intend to introduce block chain into cooperative communication. Relay that helps

source to forward data can obtain the reward (electronic money) paid by source. By writing this transaction information into block chain in an open and transparent manner, deceptive behavior between source and relay can be avoided. What is more, the rewards that relay obtains from source can encourage relay to cooperate.

For wireless networks with a large number of MTs, no matter what consensus mechanism is used, terminals need to exchange many information, which consumes large communication resources, affects network throughput and causes long block verification delays. Therefore, we consider dividing MTs into multiple block chains to form a multi-chain structure. This method can decrease the number of MTs in one block chain, reduce the resource consumption and the time delays of consensus process.

How to divide MTs into multiple block chains? We all know that source usually selects relay that is not far away from it. This indicates that both the relay selection and the transaction between source and relay are carried out in a certain area. Inspired by this idea, we use the method of regional division to form a multi-chain structure. As shown in Fig. 2, the whole network is divided into several regions according to location and distance, and each region is connected to the main chain of the cloud platform.

Fig. 2 shows the multi-chain structure based on region division. Each region has its own regional chain. In each region, the regional chain records the transaction information of MTs in the region, and BSs (in the region) store the regional chain. All regional chains are connected to the main chain of the cloud platform, so it forms a multi-chain structure. The main chain is responsible for the summary and storage of all regional chains’ information. The anchor link between the main chain and all regional chains is shown in Fig. 3. In Fig. 3, the blocks on regional chains and main chain show synchronously linear growth according to the time sequence of the system.

**TABLE 2.** Comparison of different source-relay pairing (or relay selection) methods in related works.

Broad classification	References	Source-relay pairing (or relay selection) methods	Experimental environments (or application scenarios)	Advantages (or important conclusions)	Disadvantages
Relay selection for single source	[24]	Best relay selection to maximize effective capacity	Single source and multi-relay, amplify-and-forward (AF) relaying	High effective capacity	They are not applicable to the multi-source scenarios, and they do not have incentive mechanism for terminal cooperation.
	[25]	SNR-suboptimal multiple relay selection	Single source and multi-relay, AF relaying	High signal-to-noise ratio (SNR), low computational complexity	
	[26]	Max-max relay selection (MMRS), hybrid relay selection (HRS) for relays with buffers of finite size	Single source and multi-relay, decode-and-forward (DF) relaying, relays are equipped with buffers	High SNR gain, low outage probability	
	[27]	Opportunistic relaying (OR), selection cooperation (SC)	Single source and multi-relay, DF relaying	The closed-form expressions for the outage and bit error probability (BEP) of OR and SC are obtained.	
	[28]	Partial relay selection	Single source and multi-relay, AF relaying, outdated channel estimates	The effect of outdated channel estimates on relay selection is summarized.	
	[1]	Relay selection considering both interference constraint and maximum power constraint	Cognitive relay networks (CRN), single source and multi-relay, DF relaying	The decrease in outage probability achieved by increasing the number of relays is greater than that of conventional relay networks.	
	[29]-[30]	Select-max relay, distributed switch and stay (DSS) relay, or relay selection with inter-relay cooperation	Jointing free-space optical (FSO) communication and radio frequency (RF) communication, Single source and multi-relay, DF relaying	Saving power, enhancing the reliability of the networks without generating interference	
Source-relay pairing for multi-source	[31]-[32]	Selection cooperation or coding cooperation	Multi-source and multi-relay, DF relaying or demodulate-and-forward relaying	High diversity order	They do not have incentive mechanism for terminal cooperation.
	[33]-[34]	Source-relay pairing according to link SNR or channel gain in the secondary network	Cognitive multi-source multi-relay cooperative networks, AF and DF relaying	Reducing the interference to the primary receiver	
	[35]	Relay selection based on the simplified metric using weighted bipartite graph model	Multi-source and multi-relay, DF relaying	High overall rate in interference-limited environment, low complexity	
	[36]	Full-set selection (FSS) and sub-set selection (SSS) based on max-min criterion	Multi-source and multi-relay, AF and DF relaying	The full spatial diversity is achieved.	

In the multi-chain structure, transaction data are parallel segmented and stored in different regional chains, so this structure can achieve high data concurrency, improve data processing speed and boost system throughput.

**B. COOPERATIVE COMMUNICATION MODEL IN ONE REGION**

Fig. 4 shows the cooperative communication model in one region, which is part of region 1 in Fig. 2. Assume there are  $I$  source nodes written as  $s_1, s_2, \dots, s_I$ , and  $J$  idle relay nodes without bad records written as  $r_1, r_2, \dots, r_J$ , where  $I \leq J$ . One BS is written as  $d$ . Each MT node is equipped with a single antenna, and BS is also equipped with a single antenna.  $h_{s_i r_j}, h_{r_j d}$  represent the channel state information (CSI) from  $s_i$  to  $r_j$ , from  $r_j$  to  $d$  respectively, and  $h_{s_i r_j}, h_{r_j d}$  are independent of each other. Assume all wireless channels are quasi-static Rayleigh fading and all channel coefficients

obey circularly symmetric complex Gaussian distribution. The direct links from sources to  $d$  are ignored due to large path loss, and relays adopt half-duplex amplify-and-forward (AF) strategy.

Assume that BS knows all CSIs. Then, BS makes the optimal one-to-one pairing for sources and relays, and determines transaction pricing for each pair. For details of the source-relay pairing and pricing based on KM algorithm, please refer to section V.A.

After source-relay pairing and pricing, cooperative communication is implemented in two time slots. In the first time slot, sources transmit their own data simultaneously using frequency division multiple access (FDMA) mode as shown in Fig. 5 [36], [37]. Assume  $r_j$  is paired with  $s_i$ , we write  $r_j$  as  $P(s_i)$  in Fig. 5, where  $i \in \{1, 2, \dots, I\}, j \in \{1, 2, \dots, J\}$ . The received data of  $s_i$  at  $r_j$  is

$$y_{s_i r_j} = \sqrt{p_{s_i}} h_{s_i r_j} x_{s_i} + n_{s_i r_j} \tag{1}$$



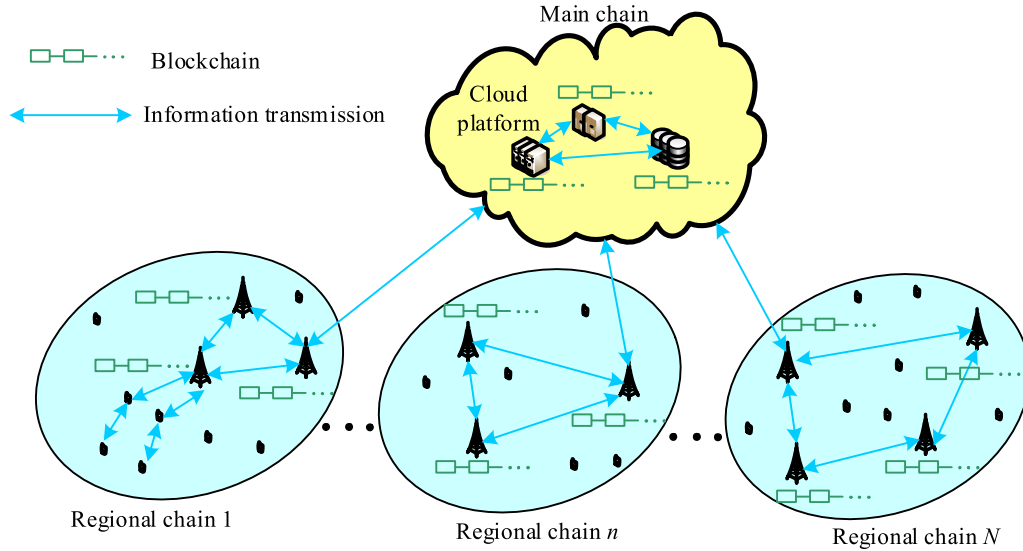


FIGURE 2. System model and multi-chain structure based on region division.

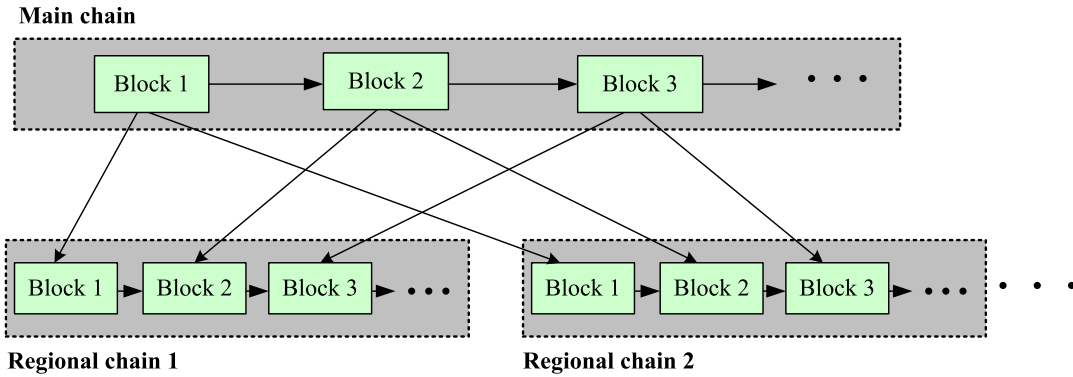


FIGURE 3. Anchor link between main chain and regional chains.

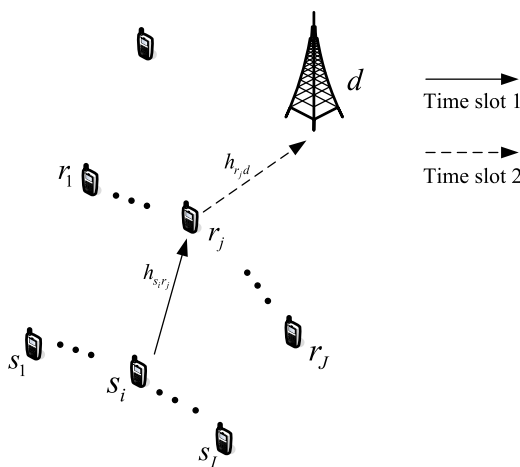


FIGURE 4. Cooperative communication model in one region.

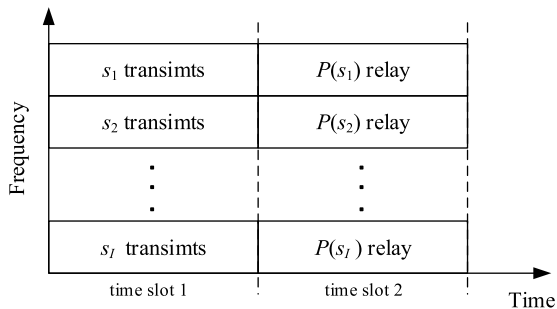
where  $x_i$  is the transmission data of  $s_i$ , and  $\mathbb{E}\{x_{s_i} \cdot x_{s_i}^H\} = 1$ .  $p_{s_i}$  is the transmission power of  $s_i$ ,  $n_{s_i r_j}$  is the corresponding additive white Gaussian noise (AWGN) and  $n_{s_i r_j} \sim \mathcal{CN}(0, \sigma_{s_i r_j}^2)$ .

In the second time slot, relays forward data according to source-relay pairing results. Assume  $r_j$  is paired with  $s_i$ ,  $r_j$  forwards the data of  $s_i$  using FDMA mode as shown in Fig. 5. In detail,  $r_j$  multiplies the received data  $y_{s_i r_j}$  with an amplification factor  $\rho_{i,j}$  and then forwards it to BS, where  $\rho_{i,j} = \frac{\sqrt{p_{r_{i,j}}}}{\sqrt{p_{s_i} |h_{s_i r_j}|^2 + \sigma_{s_i r_j}^2}}$  is set to satisfy the power constraint at the relay node, and  $p_{r_{i,j}}$  is the transmission power of relay  $r_j$  corresponding to source  $s_i$ . Thus, the received data of  $s_i$  at BS is

$$y_{r_j d} = \rho_{i,j} y_{s_i r_j} h_{r_j d} + n_{r_j d} \tag{2}$$

where  $n_{r_j d}$  is the corresponding AWGN, and  $n_{r_j d} \sim \mathcal{CN}(0, \sigma_{r_j d}^2)$ . Combining (1) and (2), the received data of  $s_i$  at BS can be rewritten as

$$y_{r_j d} = \frac{\sqrt{p_{s_i} p_{r_{i,j}}} h_{s_i r_j} h_{r_j d}}{\sqrt{p_{s_i} |h_{s_i r_j}|^2 + \sigma_{s_i r_j}^2}} x_{s_i} + \frac{\sqrt{p_{r_{i,j}}} h_{r_j d}}{\sqrt{p_{s_i} |h_{s_i r_j}|^2 + \sigma_{s_i r_j}^2}} n_{s_i r_j} + n_{r_j d} \tag{3}$$



**FIGURE 5. Frequency division multiple access (FDMA) mode of cooperative communication.**

Thus, the received signal-to-noise ratio (SNR) of  $s_i$  at BS is

$$\gamma_{s_i r_j d} = \frac{p_{s_i} \beta_{s_i r_j} p_{r_i j} \beta_{r_j d}}{p_{s_i} \beta_{s_i r_j} + p_{r_i j} \beta_{r_j d} + 1} \quad (4)$$

where  $\beta_{s_i r_j} = |h_{s_i r_j}|^2 / \sigma_{s_i r_j}^2$ ,  $\beta_{r_j d} = |h_{r_j d}|^2 / \sigma_{r_j d}^2$ . The achievable rate from  $s_i$  to BS based on a unit bandwidth is

$$Q_{s_i r_j d} = \frac{1}{2} \log_2(1 + \gamma_{s_i r_j d}) \quad (5)$$

where the multiplier 1/2 is from the dual-hop transmission in two time slots [1], [31].

**IV. WORKING PROCEDURE OF COOPERATIVE COMMUNICATION METHOD BASED ON BLOCK CHAIN**

In order to establish trust foundation among untrusted terminals and encourage terminals to cooperate, this paper proposes a cooperative communication method based on block chain for a large number of MTs. Figs. 6 (a), (b), (c) show the working procedure of this method. The detailed working procedure is as follows:

(1) Sources broadcast their request information. Sources broadcast their request information simultaneously using FDMA mode, and all idle relays and BS receive the request information. The request information of  $s_i$  includes the wallet address of  $s_i$ , transmit power of  $s_i$  and so on.

(2) All idle relays that receive request information send response information to BS. Sending response information means it agrees to be relay. The response information of  $r_j$  includes its expected minimum revenue  $\xi_j$ . Note that BS excludes the relays with bad records, and the remaining idle relays are  $r_j, j \in \{1, 2, \dots, J\}$ .

(3) BS finds the source-relay pairing and corresponding pricing. Using source-relay pairing and pricing scheme based on KM algorithm, BS pairs the sources and relays (without bad record) one to one, and gets the corresponding relay transmission power and transaction pricing for each pair. BS notifies the pairing results to all sources and relays. For detailed descriptions of the source-relay pairing and pricing scheme based on KM algorithm, see section V.A.

(4) Cooperative communication is carried out according to the source-relay pairing results. All source-relay pairs perform cooperative communication. For the detailed process of

cooperative communication, see section III.B. Take source-relay pair  $s_i$  and  $r_j$  as an example. The electronic money  $\pi_{i,j}$  in the wallet of  $s_i$  is locked, and the relay  $r_j$  cooperates with  $s_i$  to communicate. Then, BS verifies the integrity of the received data and returns the verification results to  $s_i$  and  $r_j$ . If  $r_j$  tampers with or discards  $s_i$ 's data, BS records that  $r_j$  has a bad record and broadcasts the record to other BSs.

(5) For each successful source-relay pair, source pays electronic money to relay. Take source-relay pair  $s_i$  and  $r_j$  as an example. If BS returns the verification results that  $r_j$  successfully forwards data for  $s_i$ , then the electronic money  $\pi_{i,j}$  in the wallet of  $s_i$  is automatically transferred to the wallet of  $r_j$ .

(6) Transaction information is recorded in block chain. The consensus mechanism based on intra-region DDBFT and interactive updates between regional chain and main chain (IRD-IURM) is used to record the transaction information and relays' bad records in block chain. For detailed descriptions of IRD-IURM consensus mechanism, see section V.B.

**V. SOURCE-RELAY PAIRING AND CONSENSUS MECHANISM**

**A. SOURCE-RELAY PAIRING AND PRICING SCHEME BASED ON KM ALGORITHM (SRPP-KM)**

According to the process of cooperative communication, BS excludes the relays with bad records at first, and then pairs the remaining relays with sources. Thus, we describe the optimal source-relay pairing and pricing as an optimization problem, and solve this optimization problem.

Our purpose is to maximize the sum revenue of all sources while satisfying the expected revenue of each relay, so the optimal source-relay pairing and pricing problem can be rewritten as

$$\begin{aligned} P1: \quad & \max_{p_{r_i j}, \pi_{i,j}, \alpha_{i,j}} \sum_i \alpha_{i,j} \\ & \times \left( \frac{\mu}{2} \log_2 \left( 1 + \frac{p_{s_i} \beta_{s_i r_j} p_{r_i j} \beta_{r_j d}}{p_{s_i} \beta_{s_i r_j} + p_{r_i j} \beta_{r_j d} + 1} \right) - \pi_{i,j} \right) \\ \text{s.t. } & C_1 : \pi_{i,j} - \varepsilon p_{r_i j} \geq \xi_j \\ & C_2 : 0 < p_{r_i j} \leq p_{\max} \end{aligned} \quad (6)$$

The optimization objective function

$$\sum_i \alpha_{i,j} \left( \frac{\mu}{2} \log_2 \left( 1 + \frac{p_{s_i} \beta_{s_i r_j} p_{r_i j} \beta_{r_j d}}{p_{s_i} \beta_{s_i r_j} + p_{r_i j} \beta_{r_j d} + 1} \right) - \pi_{i,j} \right)$$

represents the sum revenue of all sources, where  $\alpha_{i,j}$  is source-relay pairing coefficient,

$$\alpha = \begin{bmatrix} \alpha_{1,1} & \cdots & \alpha_{1,J} \\ \vdots & \ddots & \vdots \\ \alpha_{I,1} & \cdots & \alpha_{I,J} \end{bmatrix}$$

is pairing matrix, and

$$\alpha_{i,j} = \begin{cases} 1, & r_j \text{ is paired with } s_i \\ 0, & r_j \text{ is not paired with } s_i. \end{cases}$$

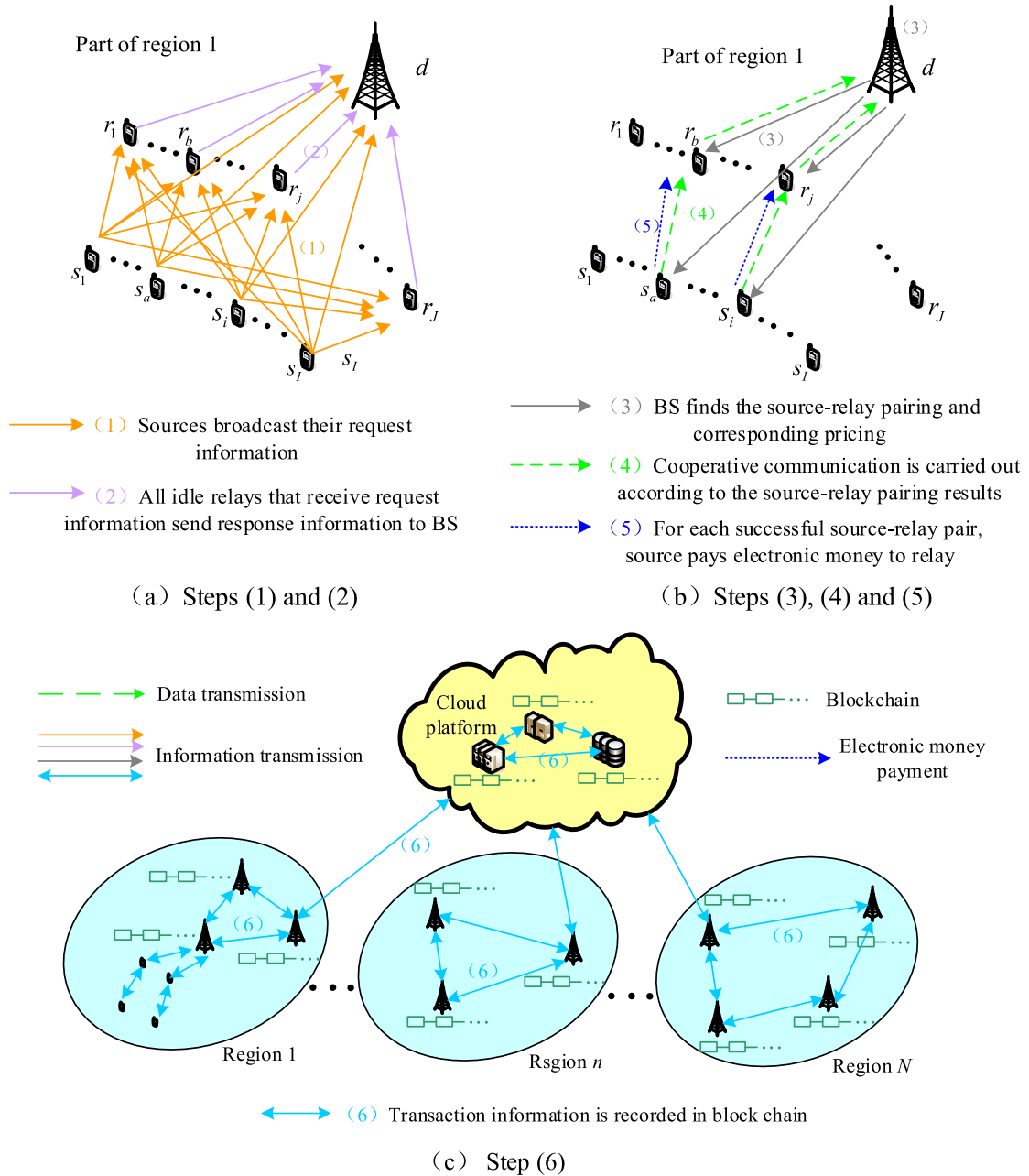


FIGURE 6. Working procedure of cooperative communication method based on block chain for a large number of MTs.

In addition,  $\sum_j \alpha_{i,j} = 1$ , i.e., each source can only be paired with one relay.  $\sum_i \alpha_{i,j} = 1$  or  $0$ , i.e., each relay can only be paired with one source or not be paired with source.  $\mu$  means the revenue (electronic money) for per unit achievable rate, and the expression of achievable rate is shown in expression (5).  $\pi_{i,j}$  is the transaction pricing between  $s_i$  and  $r_j$ . Condition  $C_1$  means that the expected revenue of relay  $r_j$  is not less than  $\xi_j$ .  $\xi_j$  is a fixed value, and  $\xi_j > 0$ .  $\varepsilon$  is the cost for per unit transmission power. Condition  $C_2$  indicates the maximum transmission power limitation for  $r_j$ . Because source  $s_i$  needs to pay relay  $r_j$  electronic money  $\pi_{i,j}$ , with an

increase in the relay revenue, the source revenue decreases. Similarly, with an increase in the source revenue, the relay revenue decreases. The source revenue and relay revenue are opposite variables, so it is impossible to find the optimal solution of the two variables at the same time. Therefore, the objective of optimization problem P1 is to maximize the source revenue while satisfying the relay revenue.

The solution process of problem P1 can be divided into two steps: first, find the optimal  $p_{r_i,j}$ ,  $\pi_{i,j}$  for each pairing of  $s_i$  and  $r_j$  (i.e., optimal transmission power and pricing problem); and second, find the optimal pairing coefficient  $\alpha_{i,j}$  for all sources and relays (i.e., the optimal pairing problem).



Thus, the optimal transmission power and pricing problem for each pairing  $s_i$  and  $r_j$  is written as problem P2:

$$\begin{aligned} \text{P2: } \max_{p_{r_{i,j}}, \pi_{i,j}} \Psi_{i,j} &= \frac{\mu}{2} \log_2 \left( 1 + \frac{p_{s_i} \beta_{s_i r_j} p_{r_{i,j}} \beta_{r_j d}}{p_{s_i} \beta_{s_i r_j} + p_{r_{i,j}} \beta_{r_j d} + 1} \right) - \pi_{i,j} \\ \text{s.t. } C_1 : \pi_{i,j} - \varepsilon p_{r_{i,j}} &\geq \xi_j \\ C_2 : 0 < p_{r_{i,j}} &\leq p_{\max} \end{aligned} \quad (7)$$

After solving problem P2, the optimal pairing problem is P3:

$$\text{P3: } \max_{\alpha_{i,j}} \sum_i \alpha_{i,j} \Psi_{i,j} \quad (8)$$

For problem P2, the smaller the  $\pi_{i,j}$ , the larger the  $\Psi_{i,j}$ , so we can get that  $\pi_{i,j}$  should equal its minimum value in order to maximum  $\Psi_{i,j}$ , i.e.,  $\pi_{i,j} = \varepsilon p_{r_{i,j}} + \xi_j$ . Thus, problem P2 can be written as problem P4 equivalently:

$$\begin{aligned} \text{P4: } \max_{p_{r_{i,j}}} \Psi_{i,j} &= \frac{\mu}{2} \log_2 \left( 1 + \frac{p_{s_i} \beta_{s_i r_j} p_{r_{i,j}} \beta_{r_j d}}{p_{s_i} \beta_{s_i r_j} + p_{r_{i,j}} \beta_{r_j d} + 1} \right) \\ &\quad - (\varepsilon p_{r_{i,j}} + \xi_j) \\ \text{s.t. } C_2 : 0 < p_{r_{i,j}} &\leq p_{\max} \end{aligned} \quad (9)$$

$\Psi_{i,j}$  is a convex function with respect to  $p_{r_{i,j}}$ , so the optimization problem P4 has an optimal solution, and the optimal solution satisfies the following expression (10):

$$\frac{\partial \Psi_{i,j}(p_{r_{i,j}})}{\partial p_{r_{i,j}}} = \frac{\mu}{2 \ln 2} \cdot \frac{p_{s_i} \beta_{s_i r_j} + 1}{(p_{s_i} \beta_{s_i r_j} + p_{r_{i,j}} \beta_{r_j d} + 1) p_{r_{i,j}}} - \varepsilon = 0 \quad (10)$$

Let  $\Delta = \frac{2 \ln 2 \cdot \varepsilon}{\mu}$ ,  $\Lambda_{i,j} = p_{s_i} \beta_{s_i r_j} + 1$ . We can get the optimal solution of (10), which is

$$p_{r_{i,j}}^* = \frac{1}{2 \beta_{r_j d}} \left[ -\Lambda_{i,j} \pm \sqrt{\Lambda_{i,j}^2 + 4 \beta_{r_j d} \frac{\Lambda_{i,j}}{\Delta}} \right] \quad (11)$$

Let  $\Gamma_{i,j} = \frac{1}{2 \beta_{r_j d}} \left[ -\Lambda_{i,j} + \sqrt{\Lambda_{i,j}^2 + 4 \beta_{r_j d} \frac{\Lambda_{i,j}}{\Delta}} \right]$ . Adding condition  $C_2$ , the optimal solution for P4 (i.e., P2) is

$$p_{r_{i,j}}^* = \begin{cases} \Gamma_{i,j}, & \text{for } \Gamma_{i,j} \leq p_{\max} \\ p_{\max}, & \text{for } \Gamma_{i,j} > p_{\max} \end{cases} \quad (12)$$

Taking the optimal solution of  $p_{r_{i,j}}$  into the objective function of (7) and  $\pi_{i,j} = \varepsilon p_{r_{i,j}} + \xi_j$ , we can get the value of  $\Psi_{i,j}$  and  $\pi_{i,j}$  corresponding to the optimal solution.

For problem P3, we need to find the optimal pairing coefficient  $\alpha_{i,j}$  for sources and relays. This is equivalent to finding the maximum weight matching of a bipartite graph. Sources and relays are subsets of the bipartite graph, and the connection weight of two subsets is the optimal solution  $\Psi_{i,j}$ . The Kuhn-Munkres (KM) algorithm [38] is an effective algorithm to solve this problem, so we use it to solve P3 and call this an optimal source-relay pairing algorithm. Detailed descriptions of the optimal source-relay pairing algorithm are shown in Algorithm 1, where the top marks of  $s_i$  and  $r_j$  are  $t_{s_i}$  and  $t_{r_j}$  respectively, and the augmenting path marks of  $s_i$  and  $r_j$  are  $l_{s_i}$  and  $l_{r_j}$  respectively for all  $i \in \{1, 2, \dots, I\}$ ,  $j \in \{1, 2, \dots, J\}$ .

---

#### Algorithm 1 Optimal Source-Relay Pairing Algorithm

---

Initialization: Initialize top marks (i.e., let  $t_{s_i} = \max_j \Psi_{i,j}$ ,  $t_{r_j} = 0$  for all  $i, j$ ), and let  $i = 1$ .

(1) Initialize augmenting path marks (i.e., let  $l_{s_i} = 0$ ,  $l_{r_j} = 0$  for all  $i, j$ ), and use **Algorithm 2** (pairing algorithm for source  $s_i$ ) to find the relay paired with  $s_i$ .

(11) If the pairing is successful, update the pairing coefficient  $\alpha_{i,j}$ , and then  $i = i + 1$ , judge whether  $i > I$ ; if  $i \leq I$ , return to step(1), i.e., pairing for next source; if  $i > I$ , jump to step (2).

(12) If the pairing is not successful, modify the top marks of the sources and relays in the augmenting path (i.e., for all  $i, j$ , if  $l_{s_i} = 1$ ,  $l_{r_j} = 1$ , then  $t_{s_i} = t_{s_i} - \Delta$ ,  $t_{r_j} = t_{r_j} + \Delta$ ), return to step (1), i.e., pairing for source  $s_i$  again until the pairing is successful.

(2) Output pairing matrix  $\alpha$ .

---



---

#### Algorithm 2 Pairing Algorithm for Source $s_i$

---

Initialization: Put the source  $s_i$  into the augmenting path (i.e.,  $l_{s_i} = 1$ ) and let  $j = 1$ .

(a) Judge whether relay  $r_j$  is in the augmenting path (i.e., judge whether  $l_{r_j}$  is equal to 1).

(a1) If  $r_j$  is in the augmenting path ( $l_{r_j} = 1$ ),  $j = j + 1$ , judge whether  $j > J$ ; if  $j \leq J$ , return to step (a); if  $j > J$ , jump to step (b).

(a2) If  $r_j$  is not in the augmenting path ( $l_{r_j} = 0$ ), judge whether  $s_i$  and  $r_j$  can be paired according to the top marks of  $s_i$ ,  $r_j$  and weight  $\Psi_{i,j}$  (i.e., judge whether  $t_{s_i} + t_{r_j} = \Psi_{i,j}$ ).

(a21) If  $s_i$  and  $r_j$  can be paired, put  $r_j$  into the augmenting path ( $l_{r_j} = 1$ );

If the  $r_j$  has been paired, use **Algorithm 2** to re-pair the original paired source of  $r_j$ ; if the original paired source of  $r_j$  is re-paired successfully, return a success flag and end the algorithm 2 for  $s_i$ ; if the original paired source of  $r_j$  is re-paired failed, jump to step (b).

If the  $r_j$  has not been paired, then  $s_i$  and  $r_j$  are paired, return a success flag and end the algorithm 2 for  $s_i$ .

(a22) If  $s_i$  and  $r_j$  cannot be paired,  $j = j + 1$ , judge whether  $j > J$ ; if  $j \leq J$ , return to step (a); if  $j > J$ , jump to step (b).

(b) Return a failure flag and end the algorithm 2 for  $s_i$ .

---

### B. LIGHTWEIGHT CONSENSUS MECHANISM BASED ON INTRA-REGION DDBFT AND INTERACTIVE UPDATES BETWEEN REGIONAL CHAIN AND MAIN CHAIN (IRD-IURM)

In each regional chain, if POW is deployed on MTs, the ‘‘mining’’ process at terminal is slow and long-term, takes up large computing resources and produces large energy consumption. The block verification process needs MTs to exchange verification information, this takes up large communication resources and affects network throughput. Thus, for MT with limited resources and energy, and mobile

communication with low delay requirements, POW is not suitable to be directly deployed on MTs. To reduce the resource consumption of MT and decrease block verification delays, this paper adopts a consortium chain in each region. Tasks with high resource consumption, such as “mining” and consensus process, are implemented at BSs. As shown in Fig. 2, in each regional chain, only BSs are responsible for “mining” and verifying new blocks.

For the consortium chain in each region, if all BSs compete “mining”, their calculations are meaningless when they do not obtain the accounting right, this will cause computing resource waste. In the process of block verification, verification information needs to be exchanged between BSs. When the number of BSs is large (although only a few BSs are shown in Fig. 2, there may be many in practice), the communication consumption will affect network throughput and cause long block verification delays. To reduce computing waste, improve network throughput and decrease the block verification delay in each region, we consider DDBFT consensus mechanism [23], in which the selected main representative BSs are responsible for accounting in turn, and the BFT algorithm is used to audit and verify block. What’s more, DDBFT has the advantages of fairness and dynamic of delegated representative BSs and fast block verification.

Fig. 7 shows the process of IRD-IURM consensus mechanism. The detailed descriptions of Fig. 7 are as follows.

<1> Download blocks. All MTs download blocks from BSs in the region.

<2> Vote for BSs. MTs vote for BSs in the region according to the downloaded blocks. The representative BSs are selected based on the MTs’ voting. That is, BSs are sorted according to the number of votes they received from more to less. The first  $Q$  BSs with more votes are selected as representative BSs, and the remaining BSs are candidate BSs.

<3> Request to record transaction information. MTs that have participated in transactions broadcast their transaction information, and all BSs receive and record their transaction information. When the time of block generation arrives, MTs request BSs to record transaction information.

<4> Consensus prepare. The main representative BS generates a block and requests consensus, where the main representative BS is selected from representative BSs in turn for each “mining”. After receiving request record information from MTs, the main representative BS of the round packages all recorded transaction information and relays’ bad records to generate a new block, and then broadcasts the new block to other representative BSs and requests other representative BSs to verify whether the information recorded in the block is correct.

<5> Consensus confirm. After receiving the new block and consensus request from main representative BS, other representative BSs verify the new block according to the transaction information and relays’ bad records they have previously recorded. Each of them broadcasts the verification result to all other representative BSs. After receiving verification success messages sent by more than half of the representative BSs, the new block reaches a consensus, each

representative BS adds the new block to the block chain. Then, the system scores each representative BS according to its honesty in the process of consensus preparation and consensus confirmation.

<6> BSs reply to MTs. The BSs send the record results to MTs.

<7> Interact with the main chain of cloud platform. After new block is added to the regional chain, the regional chain completes the information exchange with the main chain of cloud platform, and updates the anchor link. The anchor link between regional chains and main chain can be seen in Fig. 3. Then, return to step <3>, i.e., when it is time to generate the next block, the next representative BS, as the main representative BS, is responsible for “mining” in turn. Until the end of a round of “mining”, turn to step <8>.

<8> Update representative BSs and candidate BSs. After a round of “mining”, the representative BSs are sorted according to their scores from high to low. The last  $M$  representative BSs with lower scores are changed to candidate BSs, and the top  $M$  candidate BSs with higher scores are changed to representative BSs, where  $M < Q$ . In this way, representative BSs and candidate BSs are updated according to DDBFT. Then, return to step <3>

According to the working process of IRD-IURM and the characteristics of DDBFT [23], we can get that as long as the number of malicious representative BSs does not exceed  $Q/3$ , it can ensure that the error message sent by malicious nodes will not be recognized by other nodes, and this will not lead to Byzantine fault tolerance.

### C. THE TRANSACTION TRACEABILITY WHEN MT MOVES AMONG DIFFERENT REGIONS

Due to the mobility of MT, MT may move among different regions, so the transaction information of one MT may be stored in different regional chains. How can we solve the transaction traceability problem when MT moves among different regions? That is, how can we trace the source of payment currency for each transaction? The red anchor link in Fig. 8 shows the tracing of transactions when MT moves among different regions. We intend to modify the structure of each transaction record in blocks, add the regional number, block ID and transaction number of the payer’s last transaction before each transaction record in each regional chain. If the payer’s last transaction is in another region, then this transaction can be connected to the payer’s previous regional chain through the anchor link of regional chains and main chain. The anchor link of regional chains and main chain is shown in Fig. 3. Thus, we can trace the source of payment currency for each transaction. The relay’s bad record can also be traced and recorded in this way, we will not repeat the description.

## VI. SIMULATION RESULTS AND ANALYSES

### A. SIMULATION RESULTS OF SOURCE-RELAY PAIRING AND PRICING SCHEME

In order to show the performance of the proposed source-relay pairing and pricing scheme, we compare it with the sequential relay selection scheme in [36], random pairing

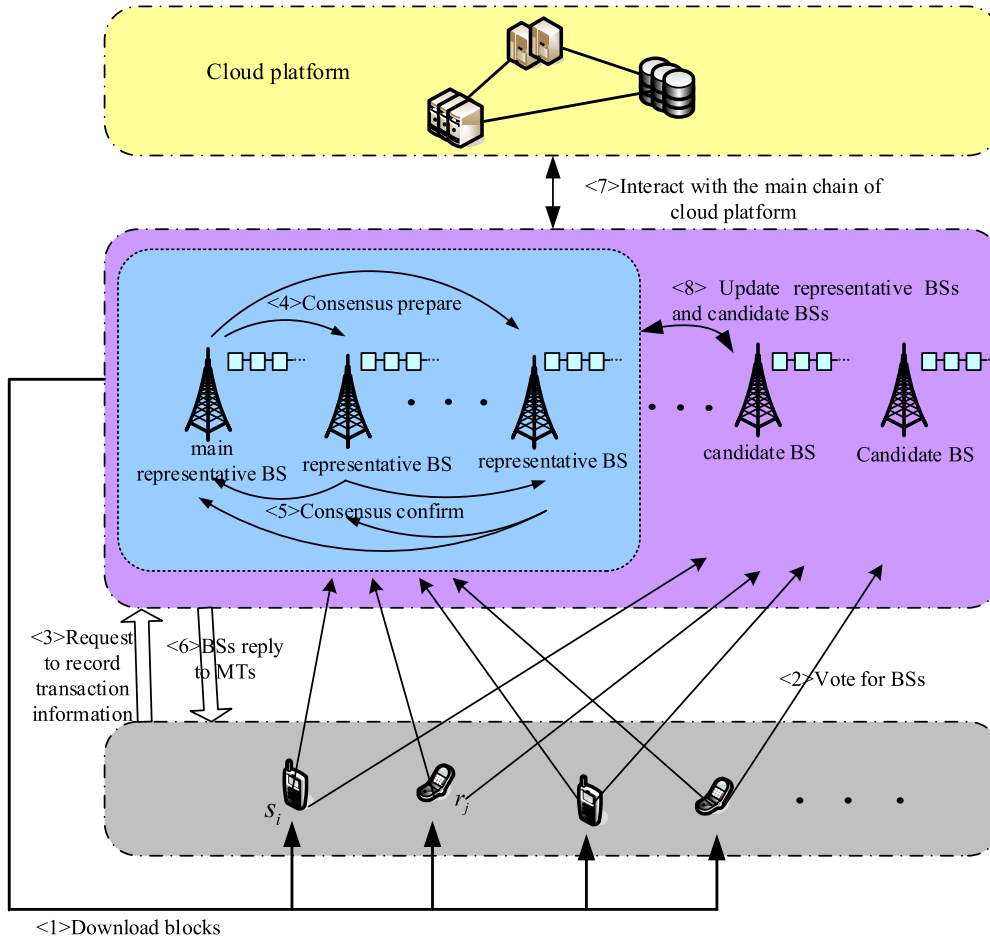


FIGURE 7. Process of IRD-IURM consensus mechanism.

scheme and fixed pairing scheme through Matlab simulations. In the following figures, “SRPP-KM” means the proposed source-relay pairing and pricing scheme based on KM algorithm (SRPP-KM). “Sequential relay selection scheme” means the subset selection (SSS) method in [36], where each source finds its own optimal relay in sequential order. “Random pairing scheme” means random source-relay pairing for each time, and each pair finds its optimal relay transmission power and pricing. “Fixed pairing scheme” means that fixed source-relay pairing is always used.

In the simulations, the number of source nodes is set to  $I = 3$ , the revenue of per unit achievable rate is  $\mu = 10$ , the cost of per unit transmission power is  $\varepsilon = 1$ , the expected minimum revenue of each relay is  $\xi = 1$ , i.e.,  $\xi_j = 1$  for all  $j \in \{1, 2, \dots, J\}$ . In order to simulate the wireless communication of the distributed terminals, all channels are quasi-static Rayleigh fading, and  $h_{s_i r_j} = g_{s_i r_j} / \sqrt{d_{s_i r_j}^v}$ ,  $h_{r_j d} = g_{r_j d} / \sqrt{d_{r_j d}^v}$ , where  $d_{s_i r_j}$  and  $d_{r_j d}$  represent their corresponding distances, and  $g_{s_i r_j} \sim \mathcal{CN}(0, 16 \times 10^4)$  and  $g_{r_j d} \sim \mathcal{CN}(0, 16 \times 10^4)$  represent their corresponding channel fading characteristics respectively. Assume the coordinates of the three source nodes are  $(0, 15)$ ,  $(0, 10)$ ,  $(0, 5)$ , and the coordinate

of BS is  $(20, 10)$ .  $J$  relay nodes are uniformly distributed over the square area with dimension  $20 \times 20$ . Path loss index  $v = 4$ , all noise variances are equal to 1, all  $p_{s_i}$  are equal to  $p_s$ .

Fig. 9 shows the comparison of sum revenue for different source-relay pairing schemes when  $J = 3$ . It can be seen that the revenue of all schemes increases with an increase in  $p_s$ . This result can be obtained from the objective function in expression (9). The proposed pairing scheme SRPP-KM can achieve higher sum revenue than other schemes, that is because the KM algorithm in SRPP-KM can get the optimal pairing to maximize the sum revenue while other schemes cannot obtain the optimal solution.

Fig. 10 shows the sum revenue of different source-relay pairing schemes changes with the number of relay nodes when  $p_s = 10$ dB. As seen from Fig. 10, the sum revenue of random pairing scheme and fixed pairing scheme shows little change because they have nothing to do with the number of relay nodes. The sum revenue of SRPP-KM and sequential relay selection scheme increases with an increase in the number of relay nodes, this is because both SRPP-KM and sequential relay selection scheme have the process of finding and pairing the optimal relay in order to maximize the sum

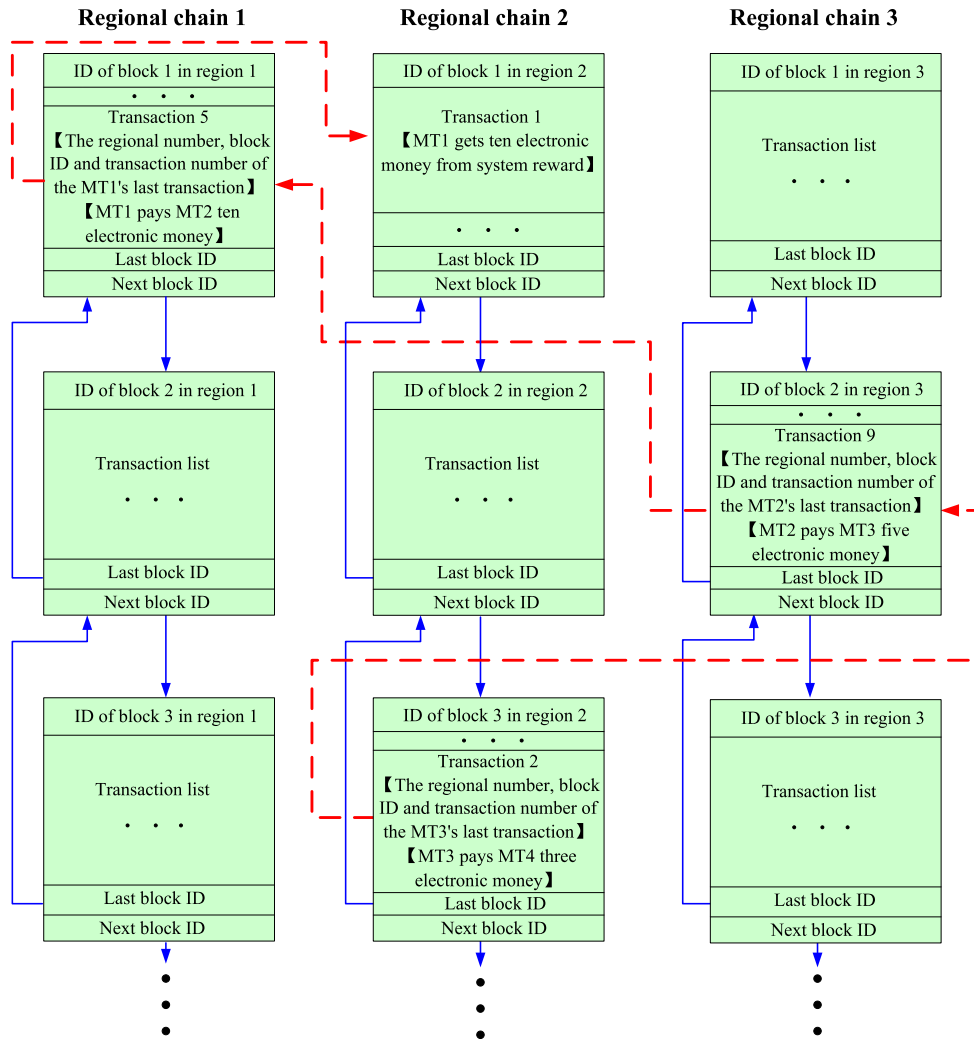


FIGURE 8. Transaction traceability when MT moves among different regions.

revenue. The greater the number of relay nodes, the more choices, and the higher the sum revenue.

Fig. 11 shows the comparison of sum transaction pricing for different source-relay pairing schemes when  $J = 4$ . From expressions (11), (12) and  $\pi_{i,j} = \varepsilon p_{r_{i,j}} + \xi_j$ , we can get that transaction pricing  $\pi_{i,j}$  is an increasing function of  $p_s$ . Thus, in Fig. 11, the sum transaction pricing of all schemes increases with an increase in  $p_s$ . The sum transaction pricing of SRPP-KM and sequential relay selection scheme is lower than that of random pairing scheme and fixed pairing scheme, that is because their optimal solutions  $p_{r_{i,j}}$  and  $\pi_{i,j}$  for selected relays are lower in order to maximize the sum revenue. Moreover, the sum transaction pricing of SRPP-KM is lower than that of sequential relay selection, this is because SRPP-KM can find the optimal pairing with lower transaction price, while sequential relay selection scheme only finds the pairing for each source in a certain order, which is not the optimal pairing and cannot get the optimal transaction price. That is to say, when compared with sequential relay selection,

SRPP-KM can obtain higher source revenue at lower transaction price.

Fig. 12 shows the comparison of sum transaction pricing for different source-relay pairing schemes when  $p_s = 10\text{dB}$ . Fig. 12 shows similar results to those in Fig. 11. In addition, we can see that the sum transaction pricing of random pairing scheme and fixed pairing scheme shows little change when the number of relay nodes increases, that's because they have nothing to do with the number of relays. The sum transaction pricing of SRPP-KM and sequential relay selection scheme decreases with an increase in the number of relay nodes. This is because the greater the number of relay nodes, the more choices, the higher the sum revenue, and the lower the transaction price.

### B. SIMULATION AND ANALYSIS RESULTS OF IRD-IURM CONSENSUS MECHANISM

In this section, we compare the proposed IRD-IURM consensus mechanism with POW [18], POS [19] and DPOS [20]

consensus mechanisms through simulations and analysis. In order to fairly compare these four consensus mechanisms, we simulate all these consensus mechanisms in the multi-chain structure based on region division, POW, POS, DPOS and IRD-IURM are used in each region, and their interactive updates between regional chain and main chain are the same. In simulations, we use Java language, RESTful service architecture and lightweight JSON data exchange format to build the block chain system. The calculation configuration parameters are as follows: Operating System—windows, Memory—16RAM, CPU—Inter Core i5-10400, JDK—8. In order to test the block delay and maximum transaction throughput of each consensus mechanism, we introduce the transaction simulation module in simulations, which can provide enough transaction data for block generation and consensus.

In simulations, POW [18] refers to bitcoin block chain, the difficulty value of its hash calculation is set to 7, that is, the first 7 bits of the hash value obtained by hash calculation are 0. All the difficulty values of hash calculation for POS, DPOS and IRD-IURM are set to 0, because they do not have “mining” competition. POS [19] refers to alogrand block chain, and uses Byzantine agreement (BA) consensus algorithm based on verifiable random functions (VRFs). DPOS [20] refers to EOSIO block chain and uses DPOS+BFT consensus algorithm, all nodes vote and select 21 consensus nodes, and then the 21 nodes achieve block consensus through the BFT algorithm. For IRD-IURM, the number of representative BSs is  $Q = 6$ , the update number of representative BSs and candidate BSs is  $M = 3$ . The capacities of each block (CEB) for POW, POS, DPOS and IRD-IURM are set to 512M, 10M, 10M and 10M respectively. The average numbers of transactions recorded in per Mbit block (ATPMB) for POW, POS, DPOS and IRD-IURM are set to 6, 4200, 4200, 4200 respectively. In addition, the total number of MT nodes is  $N_u = 500$ , and the total number of BSs is  $N_B = 50$ . It is assumed that during region division, the BSs and users are equally divided into 5 regions, so there are 100 MTs and 10 BSs in each region, POW, POS, DPOS and IRD-IURM are used in each region. Figures 13, 14 and Table 3 show the simulation and analysis results in one region.

In order to show that the proposed IRD-IURM consensus mechanism can achieve rapid consensus, the block delay of different consensus mechanisms in one region is show in Fig. 13. The block delay includes the delay of random number calculating and the delay of block consensus. Compared with the calculating delay and consensus delay, the delay of “miner” selection in POS, DPOS and IRD-IURM can be ignored, so we omit it in simulations. As can be seen in Fig. 13, the block delay of POW is much greater than that of POS, DPOS and IRD-IURM, this is because POW needs “miner” competition, network delay may cause several versions of the chain or two members finding two blocks simultaneously, this delays the block consensus significantly. Whereas in POS, DPOS and IRD-IURM, they omit the process of “miner” competing, select the “miner” based on

stakes or voting, so their chains only have one version, plus their difficult value of hash calculation is lower than POW, so their block delay are much smaller than POW. The block delay of POS is greater than that of DPOS, and the block delay of DPOS is greater than that of IRD-IURM. That's because the numbers of nodes participating in consensus in one region for POS, DPOS and IRD-IURM are 110, 21 and 6 respectively. The more nodes participating in consensus, the greater the delay of block consensus, and the greater the block delay. In conclusion, compared with POW, POS and DPOS, proposed IRD-IURM can achieve rapid consensus.

Fig. 14 shows the comparison of the number of transactions recorded in blocks for different consensus mechanisms in one region. During simulations, it is assumed that 12000 transactions are generated per second. The definition of transaction throughput (TT) is the number of transactions recorded in blocks per unit time, i.e.,

$$T_{tran} = \frac{N_{tran}}{\Delta t} \quad (13)$$

where  $T_{tran}$  represents the TT,  $N_{tran}$  is the number of transactions that is recorded in blocks during  $\Delta t$  time. Figure 14 actually shows the relationship between TT and the time delay. The slope at a certain point of the curve in figure 14 represents the TT of the curve at this time. It can be seen that the TT of IRD-IURM outperforms the TT of other three consensus mechanisms. Therefore, proposed IRD-IURM is suitable for a large number of distributed terminals with a large number of transactions. The detailed TT results of different consensus mechanisms can be seen in Table 3.

Table 3 shows the comparison of simulation and analysis results of different consensus mechanisms in one region. From the simulation results, we can see that proposed IRD-IURM can achieve shorter average block delay (ABD) and higher TT than POW, POS and DPOS, these are consistent with the results in Figures 13 and 14.

In addition, according to the simulation results in Table 3, we found that the following TT calculation expression can be summarized for each consensus mechanism,

$$TT = \frac{CEB \times ATPMB}{ABD} \quad (14)$$

The detailed analysis of time complexity, number of messages and number of rounds during block consensus is given as follows.

For POW [18], all nodes in the region use computing power to find a random hash number that meets requirements, the node that first finds the random number will get the accounting right (i.e., to be leader) and generate a new block. During POW consensus, the leader broadcasts the new block to other nodes, other nodes verify and record it. So the number of rounds for message transmission is 1, the number of nodes participating in consensus is the sum of the number of BSs and MTs in the region, that is  $N_{POW} = 110$ . The number of messages transmit during POW consensus is  $N_{POW}$ , the time complexity of POW consensus algorithm is proportional to



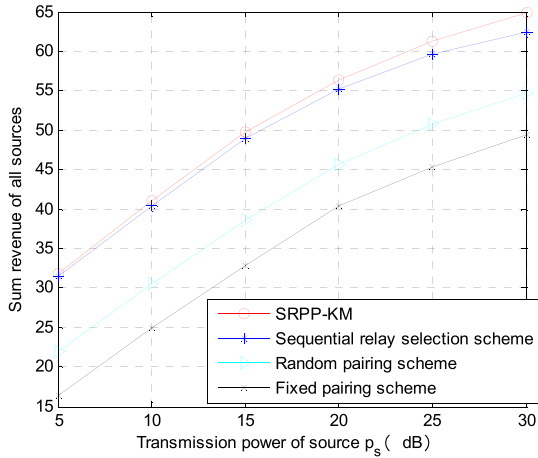


FIGURE 9. The sum revenue of all sources versus the transmission power of source.

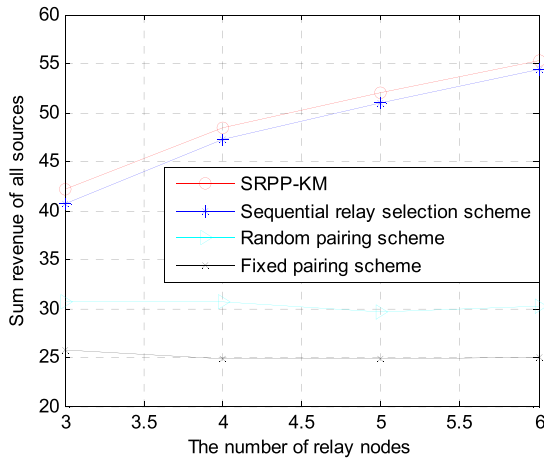


FIGURE 10. The sum revenue of all sources versus the number of relay nodes.

the number of messages transmit, so the time complexity of POW consensus is  $O(N_{POW})$ .

For POS [19], referring to alogorand block chain, POS selects the leader based on their stakes, and uses Byzantine agreement (BA) consensus algorithm based on verifiable random functions (VRFs), i.e., an improved BFT consensus. All nodes in the region participate in consensus, so the number of nodes participating in POS consensus is  $N_{POS} = 110$ . According to the characteristics of BFT consensus [23], the number of rounds of message transmission is 3, the three rounds are consensus pre-prepare, consensus prepare, consensus confirm respectively. So the number of messages transmit during POS consensus is  $2N_{POS}^2 - 3N_{POS} + 1$ , the time complexity of POS consensus algorithm is  $O(2N_{POS}^2)$ , which is the basic time complexity of BFT consensus.

For DPOS [20], referring to EOSIO block chain, all nodes vote and select 21 consensus nodes, the leader is selected from the 21 consensus nodes, and then the 21 nodes achieve block consensus through the BFT algorithm. So, similar to POS, the number of rounds for message transmission during DPOS consensus is 3, the number of messages transmit

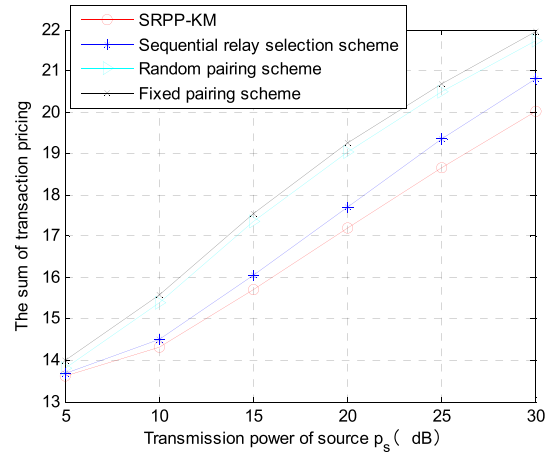


FIGURE 11. The sum of transaction pricing versus the transmission power of source.

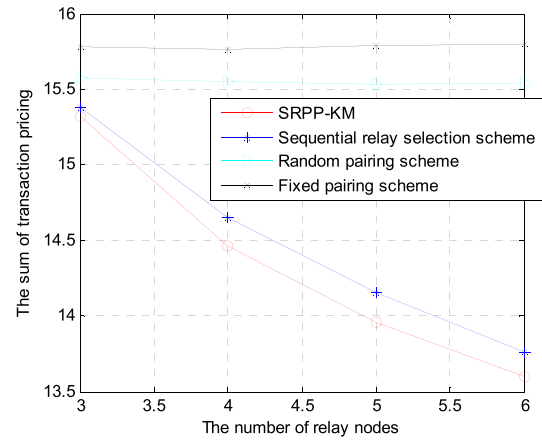


FIGURE 12. The sum of transaction pricing versus the number of relay nodes.

during DPOS consensus is  $2N_{DPOS}^2 - 3N_{DPOS} + 1$ , the time complexity of DPOS consensus algorithm is  $O(2N_{DPOS}^2)$ , where the number of nodes participating in DPOS consensus is  $N_{DPOS} = 21$ .

For IRD-IURM, in one region, 6 representative BSs (i.e., consensus nodes) are selected based on voting from MTs, and the main representative BS (i.e., leader) is selected from the 6 representative BSs, then 6 representative BSs achieve block consensus through the DDBFT algorithm. DDBFT consensus changes the three rounds of message transmission in BFT into two rounds of message transmission, which are consensus prepare and consensus confirm. So the number of rounds for message transmission during IRD-IURM consensus is 2. According to the characteristics of DDBFT consensus [23], the number of messages transmit during IRD-IURM consensus is  $N_{IRD}^2 - N_{IRD}$ , and the time complexity of IRD-IURM consensus is  $O(N_{IRD}^2)$ , where the number of nodes participating in IRD-IURM consensus is  $N_{IRD} = 6$ .

From the analysis results in Table 3, we can see that proposed IRD-IURM has less messages transmission and lower time complexity during consensus when comparing with POW, POS, DPOS.

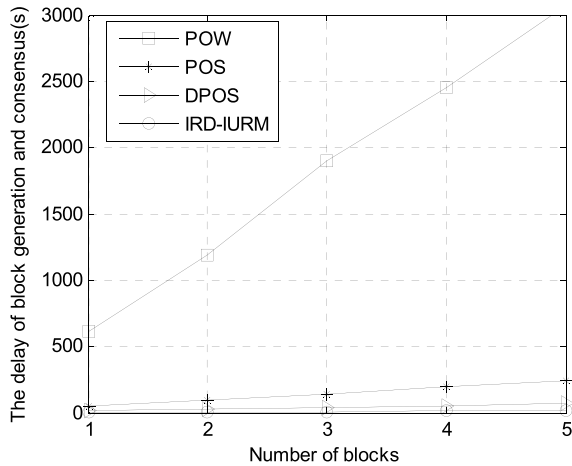


FIGURE 13. Comparison of block delay for different consensus mechanisms in one region.

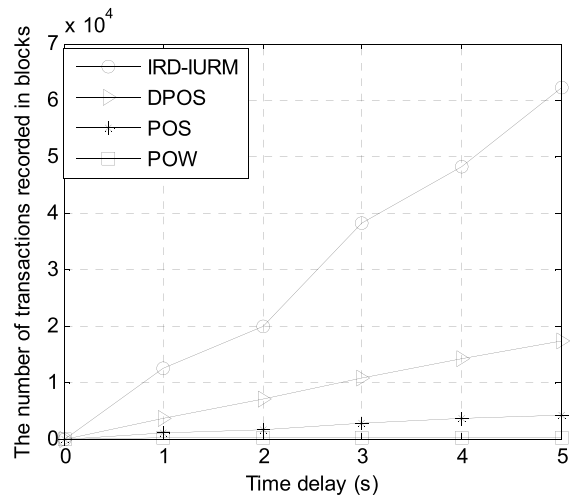


FIGURE 14. Comparison of the number of transactions recorded in blocks for different consensus mechanisms in one region.

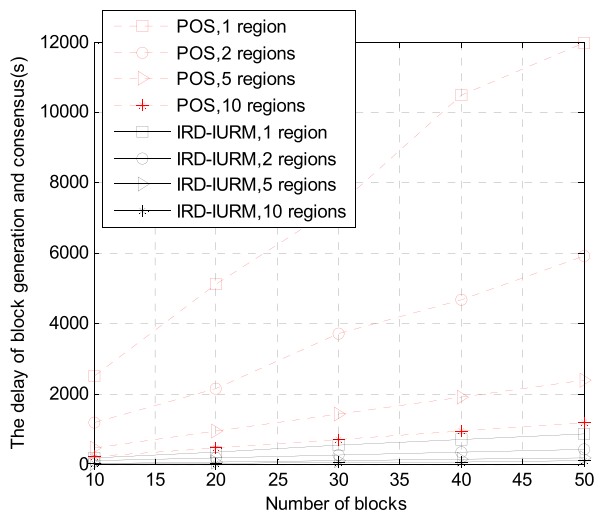


FIGURE 15. The influence of region division on block delay.

Figure 15 shows the influence of region division on block delay. Simulation parameters are the same as those in

TABLE 3. Comparison of simulation and analysis results of different consensus mechanisms.

Characteristic		POW [18]	POS [19]	DPOS [20]	IRD-IURM
Simulation parameters	Capacity of each block (CEB)	512M	10M	10M	10M
	Average number of transactions recorded in per Mbit block (ATPMB)	6	4200	4200	4200
	Difficulty value of hash calculation	7	0	0	0
Simulation results	Average block delay (ABD)	605 s	48 s	14 s	3.5 s
	Transaction throughput (TT)	6	875	3080	12401
Analysis results	Number of rounds during consensus	1	3	3	2
	Number of nodes participating in consensus	$N_{POW}=110$	$N_{POS}=110$	$N_{DPOS}=21$	$N_{IRD}=6$
	Number of messages transmit during consensus	$N_{POW}$	$2N_{POS}^2 - 3N_{POS} + 1$	$2N_{DPOS}^2 - 3N_{DPOS} + 1$	$N_{IRD}^2 - N_{IRD}$
	Time complexity during consensus	$O(N_{POW})$	$O(2N_{POS}^2)$	$O(2N_{DPOS}^2)$	$O(N_{IRD}^2)$

figures 13, 14 and Table 3. In addition, it is assumed that the number of nodes participating in consensus is directly proportional to the number of nodes in the region. “IRD-IURM, 1 region” means there is only one region and the region uses IRD-IURM consensus mechanism, i.e., there is no region division. “IRD-IURM,  $n$  regions” means BSs and MTs are equally divided into  $n$  regions, then IRD-IURM consensus mechanism is used in each region. Other legends can be explained similarly. From figure 15, we can see that IRD-IURM can achieve smaller block delay than POS, this is consistent with the result in Figure 13 and Table 3. What’s more, for the same consensus mechanism, the more regions are divided, the smaller the block delay. That’s because the more regions are divided, the fewer BSs and MTs in each region, thus the fewer nodes participating in consensus, and the shorter the block delay. DPOS and POW can also get the similar results, so we omit them in figure 15. This simulation experiment is carried out on the premise of a sufficient number of transactions. If the number of transactions is limited, the number of regions divided needs to be selected according to the number of transactions. For example, for the IRD-IURM consensus mechanism, simulation parameters are the same as those in Table 3. Since the number of transactions that can be recorded per second is about 12000 in each region, if the whole network has 60000 transactions per second, it is appropriate to divide the whole network into 5 regions. If it is divided into 2 regions, transactions cannot be recorded in blocks in time, resulting in transaction accumulation in each region. If it is divided into 10 regions, the number of transactions in each region is small, resulting in a waste of capacity space of each block in each region. Similarly, If the whole network has 36000 transactions per second, it is appropriate to divide the whole network into 3 regions.

## VII. DISCUSSION

In this section, we discuss the benefits of introducing block chain into cooperative communication.

(1) Establish trust foundation between untrusted MTs.

Using block chain, relay that helps source to forward information can obtain the reward paid by source. When the number of malicious representative BSs does not exceed  $Q/3$ , the source-relay transaction information is correctly written into blocks and is open and transparent to all terminals, thus the fraudulent behavior between source and relay can be avoided. In addition, the payment is automatically executed by smart contract, the source cannot refuse to pay and the relay cannot deny the payment of source. Thus, block chain can establish trust foundation between untrusted MTs.

(2) Encourage MTs to participate in cooperation.

Using block chain in cooperative communication, relay can get rewards paid by source, and this can encourage relay to forward information for source.

(3) Improve the security of data transmission.

After the cooperative communication of each source-relay pair, BS verifies the integrity of the received data. If relay tampers with or discards source's data, BS records that this relay has a bad record. When the number of malicious representative BSs does not exceed  $Q/3$ , relays' bad records are correct, open and transparent to all terminals, so if a relay tampers data, it will have bad record, and other sources will not choose it as a relay. Thus, the IRD-IURM consensus mechanism can prevent malicious relay from tampering information, and improve the security of data transmission.

## VIII. CONCLUSION AND FUTURE WORK

This paper introduces block chain into cooperative communication of a large number of MTs, and proposes a cooperative communication method based on block chain. First, a multi-chain structure based on region division is designed to reduce resource consumption. Then, the detailed working procedure of this cooperative communication method is designed. In the working procedure, a source-relay pairing and pricing scheme based on KM algorithm (SRPP-KM) and a lightweight IRD-IURM consensus mechanism are proposed. Analyses show that the proposed cooperative communication method can establish trust foundation between untrusted terminals, encourage terminals to cooperate. Simulation results show that SRPP-KM can obtain higher source revenue while satisfying relay revenue when compared with other source-relay pairing schemes. The IRD-IURM consensus mechanism can achieve fast consensus.

This paper focused on the design of cooperative communication method based on block chain. There remain a number of open problems need to be solved. Our future works are as follows:

(1) Source-relay pairing problem when network state changes.

In a real network, the location of the terminals and the channel conditions between terminals may be changing, it is challenging for the system to provide timely feedback

on this information and make accurate judgments. Existing source-relay pairing schemes are computationally complex and time-consuming, and cannot sense and dynamically adapt in time according to network state changes. Machine learning is an effective way to solve such problems, so we intend to study a fast pairing method based on machine learning in our future work.

(2) Source-relay pairing problem when the number of sources and relays is random.

The source-relay pairing and pricing scheme based on KM algorithm (SRPP-KM) in this paper is a one-to-one pairing of source and relay on the premise that the number of sources is less than the number of relays. However, in practice, the number of sources and relays is random, so it is difficult to meet the condition that the number of sources is less than the number of relays, and it is difficult to be fixed into one-to-one pairing. Therefore, we will further study the pairing of one source to multiple relays, and the pairing of multiple sources to one relay in our future work.

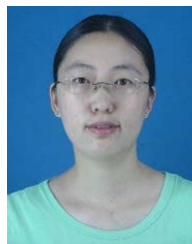
(3) The problem of dynamic region division

In this paper, the multi-chain structure adopts the fixed region division, which does not consider the need to re-divide the regions due to the movement of MTs. Moreover, fixed region division easily leads to a large number of transactions in some regions, which are difficult to record in block in time, or a small number of transactions in some regions, which waste the capacity space of block. In the next research, we will discuss the dynamic region division method to ensure that each region can achieve the best performance.

## REFERENCES

- [1] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.
- [2] S. Kandeepan, K. Gomez, T. Rasheed, and L. Reynaud, "Energy efficient cooperative strategies in hybrid aerial-terrestrial networks for emergencies," in *Proc. IEEE 22nd Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2011, pp. 294–299.
- [3] P. Zhang, F. Wang, L. Tu, and S. Diouba, "Performance analysis and diversity-multiplexing tradeoff in virtual antenna array," in *Proc. 2nd Int. Conf. Future Gener. Commun. Netw.*, Dec. 2008, pp. 226–229.
- [4] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004, doi: 10.1109/TIT.2004.838089.
- [5] C. Long, T. Chen, and X. Guan, "Cooperative amplify and forward in the presence of multiple selfish relays: Performance analysis," in *Proc. Can. Conf. Electr. Comput. Eng.*, May 2008, pp. 2045–2050.
- [6] D. P. M. Osorio, H. Alves, and E. E. B. Olivo, "On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2268–2281, 2020.
- [7] B. Wang, Z. Han, and K. J. R. Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using Stackelberg game," *IEEE Trans. Mobile Comput.*, vol. 8, no. 7, pp. 975–990, Jul. 2009.
- [8] B. Cao, G. Feng, Y. Li, and M. Daneshmand, "Auction-based relay assignment in cooperative communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 4496–4501.
- [9] Y. Meng, C. Jiang, H. Chen, and Y. Ren, "Cooperative device-to-device communications: Social networking perspectives," *IEEE Netw.*, vol. 31, no. 3, pp. 38–44, May/Jun. 2017.
- [10] S. Nakamoto. (May 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>

- [11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [12] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
- [13] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019.
- [14] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. Assadhan, and S. Lambotaran, "Blockchain-based distributive auction for relay-assisted secure communications," *IEEE Access*, vol. 7, pp. 95555–95568, 2019.
- [15] Y. Gao, M. Wu, Y. Xiao, P. Yang, B. Fu, and D. Wang, "Blockchain enabled distributed cooperative D2D communications," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Istanbul, Turkey, Jun. 2019, pp. 1–6.
- [16] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, "Proof of contribution: A modification of proof of work to increase mining efficiency," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, Jul. 2018, pp. 636–644.
- [17] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.
- [18] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.
- [19] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, 2019, pp. 51–68.
- [20] W. Zheng, Z. Zheng, H.-N. Dai, X. Chen, and P. Zheng, "XBBlock-EOS: Extracting and exploring blockchain data from EOSIO," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102477.
- [21] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, in Lecture Notes in Computer Science, Gold Coast, QLD, Australia, 2018, pp. 666–681.
- [22] T. Crain, V. Gramoli, M. Larrea, and M. Raynal, "DBFT: Efficient leaderless Byzantine consensus and its application to blockchains," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Nov. 2018, pp. 1–8.
- [23] X. Liu, "Research on performance improvement of blockchain based on dynamic delegated Byzantine fault tolerant consensus algorithm," M.S. thesis, Dept. School Comput., Zhejiang Univ., Zhejiang, China, 2017.
- [24] H. Zhi, F. Wang, and Z. Huang, "Effective capacity analysis for wireless relay network with different relay selection protocols," *IEICE Trans. Commun.*, vol. E101.B, no. 10, pp. 2203–2212, Oct. 2018.
- [25] Y. Jing and H. Jafarkhani, "Single and multiple relay selection schemes and their achievable diversity orders," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1414–1423, Mar. 2009.
- [26] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, Mar. 2012.
- [27] D. Michalopoulos and G. Karagiannidis, "Performance analysis of single relay selection in Rayleigh fading," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3718–3724, Oct. 2008.
- [28] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, May 2012.
- [29] N. D. Chatzidiamantis, D. S. Michalopoulos, E. E. Kriezis, G. K. Karagiannidis, and R. Schober, "Relay selection protocols for relay-assisted free-space optical systems," *J. Opt. Commun. Netw.*, vol. 5, no. 1, pp. 92–103, Jan. 2013.
- [30] O. M. Kandelusy and N. Kirsch, "Buffer-aided relaying network with free space optical (FSO) inter-relay links and radio frequency (RF) end-to-end links," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1587–1591, May 2021.
- [31] E. Beres and R. Adve, "Selection cooperation in multi-source cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 118–127, Jan. 2008.
- [32] M. D. Renzo, M. Iezzi, and F. Graziosi, "On diversity order and coding gain of multisource multirelay cooperative wireless networks with binary network coding," *IEEE Trans. Veh. Technol.*, vol. 62, no. 3, pp. 1138–1157, Mar. 2013.
- [33] H. Huang, N. C. Beaulieu, Z. Li, and J. Si, "On the performance of underlay cognitive multisource multirelay cooperative networks," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 605–608, Apr. 2015.
- [34] O. M. Kandelusy and N. J. Kirsch, "Cognitive multi-user multi-relay network: A decentralized scheduling technique," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 2, pp. 609–623, Jun. 2021.
- [35] D. Lee and S. Choi, "Low-complexity interference-aware single relay selection in multi-source multi-destination cooperative networks," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Gold Coast, QLD, Australia, Dec. 2012, pp. 1–5.
- [36] X. Zhang, M. Hasna, and A. Ghrayeb, "Performance analysis of relay assignment schemes for cooperative networks with multiple source-destination pairs," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 166–177, Jan. 2012.
- [37] J. N. Laneman and G. W. Wornell, "Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks," in *Proc. Conf. Rec. IEEE Global Telecommun. Conf.*, Taipei, Taiwan, Nov. 2002, pp. 77–81.
- [38] N. Chen, H. Tian, and Z. Wang, "Resource allocation for intra-cluster D2D communications based on Kuhn–Munkres algorithm," in *Proc. IEEE 80th Veh. Technol. Conf. (VTC-Fall)*, Vancouver, BC, Canada, Sep. 2014, pp. 1–5.



**HUI ZHI** received the M.S. and Ph.D. degrees in communication and information engineering from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and 2013, respectively.

Since 2013, she has been a Teacher with Anhui University, Hefei, China. She is currently a Researcher with the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. Her current research inter-

ests include block chain, cooperative communications, network coding, and wireless sensor networks.



**HONGJIE GE** received the bachelor's degree in communication engineering from Dalian Polytechnic University, in 2020. He is currently pursuing the master's degree in electronics and communication engineering with Anhui University, China.

Since 2020, he has been engaged in wireless communication research at the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. His research interests include block chain, device-to-device communication, mobile edge computing, and the IoT communication.

Mr. Ge's awards and honors include the Second-Class Comprehensive Scholarship of Dalian Polytechnic University.



**YONG WANG** received the bachelor's degree in communication engineering from Tongling College, in 2019. He is currently pursuing the master's degree in electronics and communication engineering with Anhui University, China.

Since 2019, he has been engaged in wireless communication research at the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. His research interests include block chain in cooperative communication, cellular mobile communication, and mobile edge computing.

Mr. Wang's awards and honors include the Anhui University Academic Scholarship and the Tongling College Class Scholarship.

...