2019 IEEE 19th International Conference on Communication Technology

Blockchain Based Spectrum Sharing Algorithm

Sicheng Han
Nanjing University of Posts and Telecommunications
Nanjing, China
e-mail: 871095487@qq.com

Xiaorong Zhu
Nanjing University of Posts and Telecommunications
Nanjing, China
e-mail: xrzhu@njupt.edu.cn

***Abstract*—We propose a spectrum sharing algorithm based on blockchain and game theory. Unlike traditional spectrum sharing methods which use a centralized platform, our algorithm takes the decentralization and high-level trust advantages of blockchain for operators to share free spectrum and improve the utilization rate. Our system is built on consortium blockchain in which operators can trade spectrum directly. Consortium blockchain is used to authenticate members waiting to join, record information of all the transactions and ensure that it cannot be tampered by cryptography, consensus algorithm and other methods. In addition, the operators will use the game theory to specifically share spectrum between each other in our model. The operators will make their optimal sharing strategy based on game theory. Simulation results show that the proposed algorithm can effectively improve the spectrum utilization of operators and increase their revenue.**

Keywords-blockchain; decentralization; spectrum sharing; game theory

I. INTRODUCTION

Spectrum is an important part of wireless communication, and to meet the needs of different applications in the future, it is necessary to ensure the most efficient use of wireless spectrum.In traditional spectrum allocation mode, each operator has its own authorized frequency band, and these frequency bands are only allowed to be used by the operator itself. This static allocation way leads to low spectrum utilization, which is far from meeting business growth. Therefore, it is necessary to study the spectrum sharing strategy among operators, so as to improve the imbalance between different operators in time, space and frequency band, improve the spectrum utilization rate and alleviate the problem of spectrum resource shortage. Spectrum sharing is recognized as one of the effective means to improve spectrum utilization.

Blockchain is a technology of collectively maintaining a reliable database through decentralization and de-trust. Blockchain technology provides a trusted channel for information and value exchange in an untrusted environment. Aiming at the problems existing in current spectrum sharing scheme and the advantages of the blockchain, this paper proposes a spectrum sharing mechanism based on blockchain, which can ensure that every spectrum transaction can be safely and reliably saved in the block and has no need to pay for a third-party platform. In addition, it can ensure that free spectrum can be shared in real time and efficiently, thus saving the operator's cost and improving the overall spectrum utilization at the same time.

Blockchain has been used in a variety of scenarios by these researchers which provides great reference value for our paper. [1] proposed a new type of distributed cloud architecture based on blockchain, and combined with software-defined network (SDN), so that the controller fog node can meet the design requirements at the edge of the network. The distributed cloud architecture provides low-cost, secure and on-demand access to the most competitive computing infrastructure in Internet of Things (IoT). [2] proposed a multi-layer security model of IoT based on blockchain. The model divides the entire IoT into two parts: the edge layer and the advanced layer. [3] proposed a blockchain-based smart home framework that includes three main layers: cloud storage, coverage, and smart home. Each smart home is equipped with an always-on, high-resource device called“miner”that handles all communications inside and outside home. [4] combined blockchain with big data system and proposed a method to overcome the shortcomings of existing identity verification through blockchain technology. [5] proposed a blockchain-based traffic network architecture (Block-VN) in smart cities. It's a secure and reliable architecture that operates in a distributed manner to create a new distributed transport management system.

The main contribution of this paper is building spectrum sharing system using blockchain technology, especially the consortium blockchain. This is not only an important application field of blockchain but also a new attempt of spectrum sharing method. The existing way of spectrum sharing is basically to set up a platform to connect users who need to rent spectrum and lease spectrum. In this way, the platform has a large voice. In addition, the platform needs a lot of human resources to maintain and the data is not disclosed, which results in high additional costs for the trading party and difficulties in dealing with disputes. By contrast, the adoption of blockchain technology has more advantages, mainly because it can establish a decentralized system without too much resource maintenance, and ensure the trust of traders through technical means, which can make the two sides of the transaction directly connect, saving costs and making the transaction more flexible.

II. SYSTEM MODEL

We establish a spectrum sharing model based on blockchain. The blockchain provides a decentralized

978-1-7281-0535-2/19/$31.00 ©2019 IEEE

distributed architecture that allows users to trade directly without the involvement of a third-party platform and without worrying about trust. We build two blockchain systems, one is the public chain and the other is the consortiuim chain. In the process of spectrum sharing, one party opens the spectrum usage right to the other party, and the other party must pay the corresponding spectrum coin. Here spectrum coin is a kind of digital currency or virtual currency, specially used for spectrum trading. The public chain built in this paper does not participate in spectrum sharing, but acts as an interface between spectrum coins and cash, any user can log in to the public chain to purchase spectrum coins with real money. The public chain is based on the architecture of Ethereum, and the operating mechanism and trading mechanism are basically the same as the Bitcoin blockchain system. We build a distributed peer-to-peer spectrum trading system based on the consortium chain architecture, as shown in Figure 1. The consortium blockchain is generally oriented to enterprise users, and an enterprise that conducts business cooperation constitutes an consortium to jointly maintain the blockchain. The characteristic of consortium blockchain is that users who want to participate in the chain require permission, which is generally open only to members of the consortium. Not everyone can participate in the transaction like Bitcoin. Different users have different permissions, and each type of users can only view data within their own permissions.

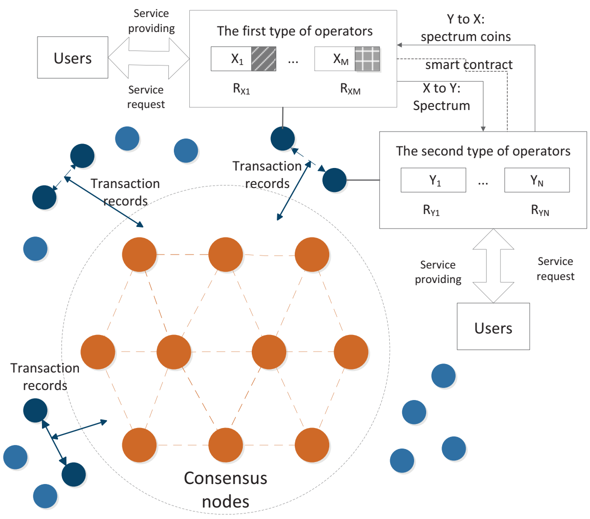

Figure 1. The system model of blockchain-based spectrum sharing mechanism

Consortium blockchain has the characteristics of authentication node authorization mechanism, multi-level encryption mechanism, consensus mechanism, high performance intelligent contract execution engine, data management and so on. Considering the needs of business applications for security, privacy, regulation, audit and performance, consortium blockchain improves the entry threshold and adds business features such as security, privacy and regulatory audit, which is an exploration of the application of blockchain technology in commercial field. The consortium blockchain is the most suitable solution for spectrum sharing using blockchain considering user privacy and transaction efficiency. However, the public blockchain is not suitable for the scenario of our research because all users can query information equally and some people who do not have spectrum may publish false information.

As shown in the figure, there are two types of users in the system, all of which are operators with a certain number of licensed spectrum. We define the first type of operators as operators with free spectrum, denoted by X, who can share their own spectrum to obtain certain benefits. The second type of operators are those with limited spectrum resources, denoted by Y. They need to rent spectrum from the first type of operators to provide services for their end users. During the rent term, the right to use the spectrum leased by X is completely owned by Y, and X shall not interfere.

A. *Transaction Process*

The transaction process will start with user login, where the users who log into the blockchain are two types of operators. The operators will get the information of authenticated transactions stored on the consortium blockchain mainly including the price and quantity of spectrum and the renting time when they log in. After that, the first type of operators with free spectrum will broadcast on the chain, informing all other operators that they have the spectrum to share. The second type of operator applies to the first type of operator for spectrum renting, including the demand and the time required for renting. The first type of operator will offer a price due to an algorithm based on game theory and if the second type of operator is satisfied, the deal can be done.

Assuming that the first type of operator X_i and the second type of operator Y_j are satisfied with the price and have decided to make a transaction, X_i will generate a transaction list and write all the information into the list. The contents of the transaction list are the frequency band information of the spectrum rented by X_i, the amount of spectrum (Hz), the total price, the time for rent and the addresses of both parties of the transaction. If there are additional requirements, both parties can negotiate to form a detailed smart contract attached to the transaction list before it is generated. Then X_i will get a hash value by linking the hash value of last transaction with the public key of Y_j and running a hash encryption algorithm. The value X_i got will be encrypted by its private key and attached as digital signature at the end of the transaction list and sent to Y_j's address along with the spectrum coin to be paid. Finally X_i will calculate the ID of the transaction list and broadcast it to the entire network together with the list.

At this point, all nodes on blockchain knows that a transaction happened between X_i and Y_j. The transaction proposal will then be submitted to endorsement nodes for simulation execution and endorsement and return the result. They will verify the transaction at the same time. If the verification fails, the endorsement nodes will directly send a message to inform both parties of the transaction that it is invalid. Else if successfully verified, the transaction will be broadcast to the sorting nodes. The sorting nodes will receive the transaction information including the endorsement of proposal signature and simulation execution results, and give the transactions an order. After this process, the sorting nodes will submit the transactions in the cache to the consensus nodes according to the order. The consensus nodes will reach a consensus about the transaction according to the consensus algorithm, that is, all the consensus nodes put new transaction record into local cache and wait for the creation of new block. When the new block is created, it will also be broadcast to all nodes until the new block is connected to current blockchain in every node's database. This is the process by which accounting nodes reach a same state about transaction information and blocks through consensus algorithm.

B. Consensus Algorithm

Considering that the main players in spectrum sharing are basically operators, and the number of participants is not many, and the consortium blockchain itself has participation authentication, we believe that the possibility of Byzantine failure is very low, and thus use the Raft algorithm to achieve consensus between nodes.

The Raft algorithm divides nodes into clusters, each of which typically contains five nodes (servers), allowing up to two servers to fail [6]. The servers in each cluster have three states: leader, follower and candidate. Under normal working conditions, a cluster has only one server as the leader, the rest are followers. Candidates only exist during the leader election. A follower is responsible for accepting and processing messages from the leader and other followers. The leader is responsible for receiving external messages and sending messages to the external and its followers. The algorithm has two main processes, one is the leader election and the other is the consensus accounting process.

Leader election occurs before the consensus or when the current leader fails. Suppose a cluster contains N servers, each of which can be a candidate at the time of election and send requests to other servers to elect themselves. There is usually only one candidate and all the other servers agree to elect it as the leader, but if a server has not received a message from the candidate for a long time, it can elect itself. The server with a final number of votes greater than N/2 will become the leader of the cluster. If the leader fails or crashes, then a follower will automatically become the candidate, then new leader will be re-selected as the process described above to continue accounting.

The Raft algorithm's accounting process has several main steps. First, the leader receives the transaction information sent by the sorting nodes, and then adds the transaction information to local ledger in order and broadcasts it to the follower nodes, requiring followers to add the transaction to their local ledger too. After writing the transaction record to local ledger, followers will reply to the leader a successfully written message. When the leader receives the successful written message from all the followers, the consensus on new transaction is completed. When the local cache transactions of the leader node reach a certain number or after a certain period of time, the leader will create a new block and ask followers to link the new block information to their local blockchain in the same way. This process is performed in all clusters at the same time, and finally messages will be sent between the leaders of all clusters to confirm whether the contents of the new block are the same (judged by the hash value). Theoretically, all new blocks created by the leader should be the same, and if there are differences, all nodes will take most of the same new blocks as the real new block and add it to local blockchain.

III. SPECTRUM SHARING ALGORITHM BASED ON GAME THEORY

In order to attract the second type of operators, there is a competitive relationship between the first type of operators, which can be considered as a non-cooperative game. The strategy of the game is price.

For the first type of operator, s_i represents its policy space and U_i is its utility function. The first type of operator's policy space is its price for renting spectrum to the second type of operator, denoted as p_i. The shared spectrum amount is represented by b_i, so its utility function is:

$$U_i = c_1 b_i + c_2 p_i b_i - c_3 M_i (B_i^{req} - k_i^p \frac{W_i - b_i}{M_i})^2 \qquad (1)$$

M_i is the number of end users connected to the first type of operator X_i, W_i is the total spectrum quantity owned by X_i, B_i^{req} represents the bandwidth required for connection and k_i^p is the utilization of frequency band of X_i, which is related to modulation technology, base station distribution density and the location of base station, and $k_i^p = B_i^{req}/(W_i/M_i)$.

We consider the spectral difference between operators and express it by v, the value range of v is [0,1], 0 means that the spectrum of each operator is completely different, and the second type of operators cannot switch between these spectrum, 1 means that the spectrum of each operator is completely the same. Besides, we use η to represent spectrum occupancy. While η=0, the spectrum is completely free and there is no information transmission and when η=1, the spectrum is fully occupied, and there is no free spectrum available to rent. We can get the utility function of the second type of operators from [7] :

$$S(b) = \sum_{i=1}^{N} b_i k_i^{(s)} (1 - \eta_i) - \frac{1}{2} (\sum_{i=1}^{N} b_i^2 + 2\upsilon \sum_{i \neq j} b_i b_j) - \sum_{i=1}^{N} p_i b_i \qquad (2)$$

$k_i^{(s)}$ represents the spectrum utilization rate of X_i before sharing.

In order to get the maximum value of the second type of operators' utility function, we need to solve:

$$\frac{\partial S(b)}{\partial b_i} = k_i^{(s)} (1 - \eta_i) - b_i - \upsilon \sum_{j \neq i} b_j - p_i = 0 \qquad (3)$$

After solution we can get:

$$D_i(p) = b_i = \frac{[k_i^{(s)}(1-\eta_i) - p_i][\upsilon(N-2)+1] - \upsilon \sum_{j \neq i} [k_i^{(s)}(1-\eta_j) - p_j]}{(1-\upsilon)[\upsilon(N-1)+1]} \qquad (4)$$

Using the function of p_i to represent b_i and substitute it into the utility function of the first type of operator, we can obtain:

$$\frac{\partial U_i}{\partial p_i} = -\frac{c_1[\upsilon(N-2)+1]}{(1-\upsilon)[\upsilon(N-1)+1]} + c_2 D_i(p) + \frac{2c_3 k_i^p[\upsilon(N-2)+1]}{(1-\upsilon)[\upsilon(N-1)+1]}[B_i^{req} - k_i^p \frac{W_i - D_i(p)}{M_i}] \tag{5}$$

Taking partial derivative of equation 8 with respect to p_j, we can obtain:

$$\frac{\partial^2 U_i}{\partial {p_i}^2} = -2c_2 \frac{[\upsilon(N-2)+1]}{(1-\upsilon)[\upsilon(N-1)+1]} - 2c_3 \frac{(k_i^p)^2}{M_i}\{\frac{[\upsilon(N-2)+1]}{(1-\upsilon)[\upsilon(N-1)+1]}\}^2 \tag{6}$$

It's not hard to know that equation 6 must be lower than or equal to 0, so the game model we established has a Nash equilibrium.

Nash equilibrium is a combination of a series of strategies, so that the strategy of each player in the combination is the optimal strategy when considering the strategies of other players. The set $P^*=\{p_1^*, ..., p_i^*, ..., p_n^*\}$ represents the Nash equilibrium of the game, if and only if $p_i^*=R_i(p_{-i}^*)$. Where p_{-i}^* refers to the optimal policy set of all other first type operators except X_i. Substituting all the parameters into (5), then let the derivative of (5) to be 0 and solve the it, we can finally get the Nash equilibrium solution p_i^* of the game.

IV. SIMULATION AND RESULTS ANALYSIS

We simulate the algorithm proposed above and will show some of the results. We consider that only two first type of operators (X_1, X_2) participate in the game, they will give their optimal price based on the other one's price and their own utility.

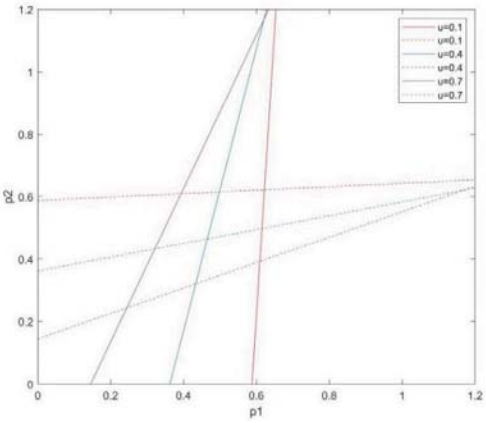

Figure 2. Nash equilibrium in symmetric case

We set the number of the first type of operators is N=2, and the total spectrum of each first type of operator is $W_1=W_2=20$MHz, and the number of connections of end users is $M_1=M_2=10$, $BER^{tar}=10^{-4}$, the service rate required by each first type of operator is $B_1^{req}=B_2^{req}=2$Mbps, weight $c_1=0.25$, $c_2=c_3=1$. The received SNR of the second type of operators are 15dB, the spectrum replacement coefficient v and spectrum occupancy rate η both vary within [0,1]. We consider the symmetric case, in which $\eta_1=\eta_2=0.5$.

Figure 2 shows the relationship between the price p_1 of X_1 and p_2 of X_2 in symmetric case.There are 6 lines in the figure, which can be divided into two groups. Among them, the solid lines are the curves of p_1 changing with p_2, and the other three dotted lines are the curves of p_2 changing with p_1.

We can see that p_1 and p_2 are positively related to each other regardless of who is the independent variable. The intersection of the two lines of the same color in the figure is the equilibrium price at the current value of v. It can be seen that the larger v is, the lower the equilibrium price is. This is because when v is small, the second type of operators have a certain preference for the choice of spectrum, and will not be affected by the price greatly. But with v increasing, the preference will become less obvious, the second type of operators will have more alternative choices and the competition will be more intense.

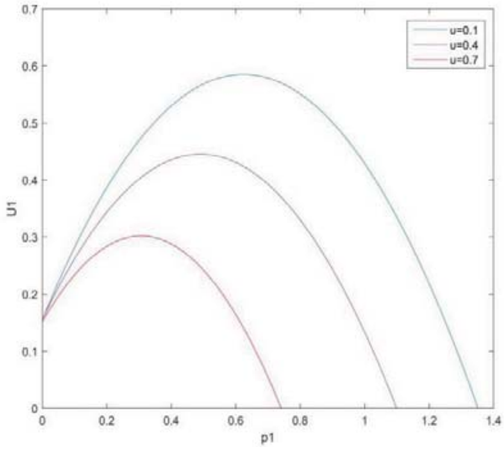

Figure 3. The relationship between utility and price in symmetric case

Figure 3 is the relationship of the utility function U_1 of the first type of operator X_1 with the change of the price p_1 in the symmetric case. The three curves correspond to the case of $v = 0.1$, $v = 0.4$, and $v = 0.7$. It can be seen from the figure that as p_1 increases, U_1 will first increase and then decrease. When p_1 is equal to the equilibrium price p_1^*, the utility of the first type of operator X_1 reaches the maximum value, which also explains the equilibrium price is the optimal price. Comparing the three curves in the figure, we can see that as v increases, the utility value goes smaller and the price when the utility is zero goes smaller, either. This is also because when v increases, the difference between spectrum of different operators becomes smaller and so lower the competitiveness. In such situation, X_1 can only successfully rent a little spectrum, the utility will no doubt become lower. Besides, while $p_1=0$, the utility of the three curves are basically equal, which are about 0.17.

Figure 4 shows the relationship between spectrum utility rate and η of an operator. We suppose that all first type of operators have the same η. In the figure, the blue line is the initial spectrum utility rate of a first type of operator when connects to the blockchain system and it is equal to η. The red line and green line are the spectrum utility rate after one transaction and five transactions.

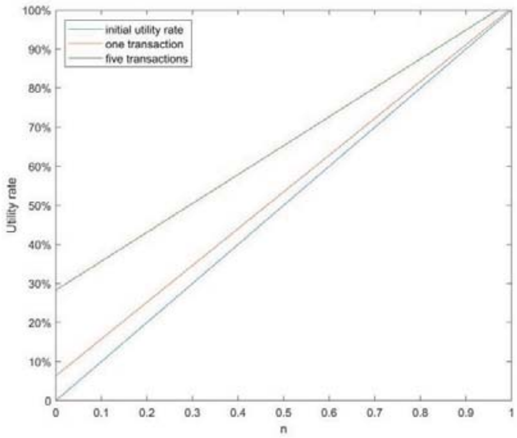

Figure 4. Spectrum utility rate of one operator

We can see from the picture that the blochchain-based spectrum sharing system can greatly improve the spectrum utility rate of operators. Besides, the more free spectrum an operator has, the more improvement on spectrum utility rate it will get. .

V. CONCLUSION

We build a spectrum sharing system between operators based on consortium blockchain, where the first type of operators with free spectrum can rent it to the second type of operators who need more spectrum to obtain benefits. Every successful transaction between the two types of operators will be stored in the block and finally recorded in the nodes of the consortium chain. In general, our spectrum sharing algorithm effectively improves the spectrum utilization rate of operators and it not only guarantees the security but also saves a large amount of management costs compared to the traditional way which uses a central platform.

ACKNOWLEDGEMENT

This work was supported by Natural Science Foundation of China (61871237) and Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (16KJA510005).

REFERENCES

[1] Pradip Kumar Sharma, Mu-Yen Chen,Jong Hyuk Park. A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT. J. IEEE Access,2017, PP(99):1-1.

[2] Cheng Li, Liang-Jie Zhang. A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. C. 2017 IEEE International Congress on Internet of Things (ICIOT), 2017:33-41.

[3] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. C. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017: 618 – 623.

[4] Nazri Abdullah, Anne Hakansson, Esmiralda Moradian. Blockchain based approach to enhance big data authentication in distributed environment. C. 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017: 887 - 892.

[5] Sharma P. Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. J. Journal of Information Processing Systems, 2017, 13(1):184-195.

[6] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm[C]// Usenix Conference on Usenix Technical Conference. USENIX Association, 2014:305-320.

[7] Niyato D , Member S , Hossain E , et al. Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion. J. Selected Areas in Communications IEEE Journal on, 2008, 26(1):192-20.