Blockchain-Based Privacy-Preserving Dynamic Spectrum Sharing

Zhitian Tu[1](✉), Kun Zhu[1,2], Changyan Yi[1,2], and Ran Wang[1,2]

[1] College of Computer Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing, China
{tzt,zhukun,changyan.yi,wangran}@nuaa.edu.cn
[2] Collaborative Innovation Center of Novel Software
Technology and Industrialization, Nanjing, China

Abstract. For improving the utilization and alleviating the shortage of spectrum resources, centralized database-based dynamic spectrum sharing system has been proposed. However, the centralized architecture is often considered to be nontransparent and more vulnerable to be attacked. To address the above issues, in this work, we propose a blockchain-based dynamic spectrum sharing framework. The distributed architecture based on blockchain technology can bring advantages including decentralization, openness, transparency, immutability and auditability. Considering that the introduction of blockchain technology in spectrum sharing will also bring privacy issues, we design a differential privacy-based privacy-preserving double auction mechanism. The auction can be implemented in smart contracts running on the blockchain. The proposed double auction mechanism is proved to satisfy differential privacy, individual rationality, computational efficiency, and truthfulness. The extensive experiments demonstrate the effectiveness of the proposed dynamic spectrum sharing scheme.

Keywords: Dynamic spectrum sharing · Blockchain · Privacy preservation · Double auction

1 Introduction

The International Telecommunication Union has predicted that the international mobile communication spectrum demand will reach 1340 MHz–1960 MHz by 2020. The contradiction between supply and demand of future spectrum resources will be extremely prominent. To get out of this dilemma, spectrum sharing has been proposed to improve spectrum utilization and alleviate shortage of spectrum resources by sharing idle resources. Such spectrum management method can be divided into two categories: static spectrum sharing and dynamic spectrum sharing [1]. Since the spectrum utilization of the static spectrum sharing is limited, dynamic spectrum sharing has gradually become the major trend in the academia and industry so as to further improve the spectrum utilization [2].

D. Yu et al. (Eds.): WASA 2020, LNCS 12384, pp. 444–456, 2020.
https://doi.org/10.1007/978-3-030-59016-1_37

A database-based spectrum access system can reduce the management cost of the system, improve the spectrum utilization, and further increase access levels among users. In such a system, users or devices do not need to sense the surrounding wireless environment to opportunistically access spectrum resources. Federal Communications Commission (FCC) promotes dynamic spectrum sharing in 2015 and launches Citizens Broadband Radio Services (CBRS) at 3.5 GHz [3]. CBRS dynamically manages different types of wireless traffic through a centralized spectrum access database system to improve spectrum efficiency [4]. However, a centralized database is often considered costly and more vulnerable to be attacked.

Recently, blockchain technology has attracted great interest of the academic community for its potential capability to overcome the shortcomings of the centralized architecture. Blockchain is viewed as a digital ledger designed to keep a traceable, transparent, accessible, verifiable and auditable distributed record [5]. And this digital ledger can be safely updated without a central intermediary [6]. Blockchain can be viewed as a low-cost alternative for database system to dynamically allocate spectrum resources. Blockchain-enabled dynamic spectrum sharing has attracted the attention of some researchers from both academia and industry. In [7], the blockchain technology is regarded as a distributed database to record the history of shared spectrum access by individual users. And secondary users decide how to opportunistically access spectrum referring to the historical information stored in the blockchain. In [8], blockchain is deployed as a distributed database and a trading platform to decide on resources allocation for sharing and record every spectrum resource transaction and access information of PUs and SUs. In [9], the author discussed the operation process of the blockchain-based dynamic spectrum sharing system in detail from the perspective of cryptography and designed a series of mechanisms to protect the privacy of SUs.

However, these schemes mainly focus on the concept of bringing blockchain for dynamic spectrum sharing, while not providing specific mechanism design for spectrum sharing in blockchain. Moreover, users' transaction information is recorded in the form of blocks in blockchain-based spectrum resource trading platform. The transaction information contains the users' information. Users' private information may be recorded in these transactions. And any node in the blockchain can easily obtain the information recorded in the block. Thus, users' privacy cannot be guaranteed. And few existing works consider are discussing in depth how to take advantage of tools provided by blockchain technology, likely smart contracts, to achieve a privacy-preserving spectrum resource sharing in an untrust environment.

In this paper, we first propose a blockchain-based dynamic spectrum sharing platform. Transactions are recorded in the blockchain in the form of blocks. And every node can monitor, verify all transaction information and run smart contracts. A privacy-preserving double auction mechanism is designed to run on blockchain network in the form of smart contract. And the mechanism can protect users' privacy, increase social welfare, and improve spectrum resource utilization in an untrusted environment of blockchain network. Then, we formulate a winner determination problem in the double auction mechanism as an integer linear programming (ILP) problem. We take advantage of Hungarian algorithm to solve this ILP problem. Based on the allocation results, the clearing price is calculated. In the scenario of blockchain application, we introduce asymmetric encryption and differential privacy during the bidding and transaction processes to protect the privacy of users. And the proposed double auction mechanism is proved to satisfy differential privacy, individual rationality, and truthfulness. We conduct extensive experiments and the experimental results demonstrate the effectiveness of our proposed blockchain-based dynamic spectrum sharing scheme.

The rest of the paper is organized as follows: we first provide a detail description of our proposed framework of dynamic spectrum sharing based on blockchain in Sect. 2. In Sect. 3, we introduce our system model and preliminaries of spectrum trading and privacy preservation. In Sect. 4, we theoretically prove that the proposed double auction mechanism satisfies differential privacy, individual rationality, computational efficiency, and truthfulness. In Sect. 5, we present our performance evolution results. Finally, we draw a conclusion in Sect. 6.

2 The Proposed Blockchain-Based Framework for Dynamic Spectrum Sharing

In this section, we describe the operation of the blockchain-based spectrum sharing system we proposed in detail. This system is built on consortium blockchain. Consortium blockchain can achieve partial decentralization and high efficiency [10]. Each node on consortium blockchain usually has a corresponding physical institution or organization. Participants are authorized to join the blockchain network and form a stakeholder consortium to jointly maintain the operation of the blockchain. The system architecture based on the consortium blockchain can effectively reduce latency and improve system throughput.

2.1 Architecture Components

This system is composed of three entities, as is depicted in Fig. 1. We divide users into two types, spectrum providers (SPs) and spectrum demanders (SDs). SPs obtain resources from some official institutions, like FCC, by competing with other PUs or acquire resources from PUs by competing with other SUs through cooperation sharing or non-cooperative sharing as mentioned in [7]. Due to changes in SP's spectrum requirements or usage scenarios, some of their spectrum resources become idle. In order to increase spectrum utilization and users' revenue, SPs desire to share their idle spectrum resources. The other entity is SD that dying for spectrum resources. For more efficient allocation, we introduce local aggregators (LAGs) as the third entity to be the smart contract manager

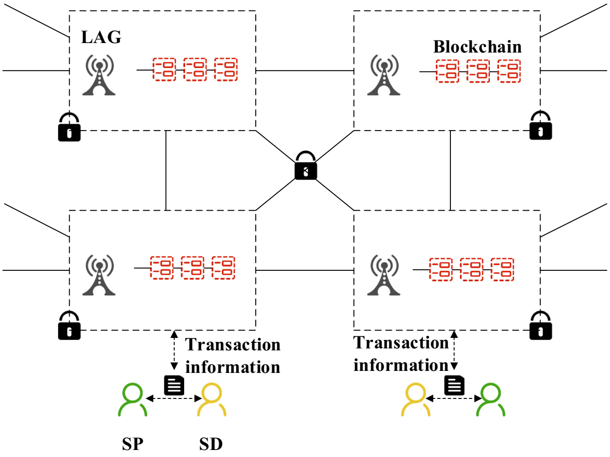


Fig. 1. Structure of our proposed blockchain-based spectrum sharing system

and auctioneer in this system. Since lots of users may not have sufficient computing power to support resource allocation, we select local aggregators to match resources and maintain the operations of the smart contract and blockchain.

2.2 Smart Contracts Designed for Privacy Preservation and Spectrum Sharing

We are using the truffle framework to develop a decentralized application (Dapp) for SDs, SPs, and LAGs. Every transaction slot, a LAG is selected as the auctioneer, establishes a smart contract and records a public key for RSA encryption in the smart contract. After being verified by the CA, users that have paid a certain amount of deposit is allowed to join this blockchain. Once a fraud occurs, the deposit of the node incurred will be fined.

SPs store the specific information of their idle spectrum resources in the Inter Planetary File System (IPFS) and create the corresponding hash addresses to record these addresses in smart contract. SUs can consult these information to get their valuation. Users obtain the encrypted public key stored in the smart contract to encrypt their real bids and send them to the smart contract. After a certain time, the smart contract decrypts the encrypted information stored in the blockchain and calculates the parameters to operate the differential privacy mechanism. Users obtain these parameters from smart contract to generate encrypted bids and send their encrypted bids as well as tokens to the smart contract. After reaching the final deadline of the transaction, the LAG that initiated the contract obtains the bidding information of all users.

And the LAG calls computing resources to get the final resource allocation result. The LAG stores the bid information and allocation plan in the IFPS and stores the hash address from IPFS in the blockchain. Users and other LAGs can obtain the hash address by interacting with smart contract and obtain the allocation scheme and bidding information in the IFPS. Users and LAGs can verify the allocation plan according to the bidding information. Based on the verification results, nodes in the blockchain will vote on the distribution plan. The smart contract collects votes and determine whether to adopt this allocation scheme. According to the verified allocation scheme, the smart contract will automatically complete the transaction process. The software architecture is shown in Fig. 2.

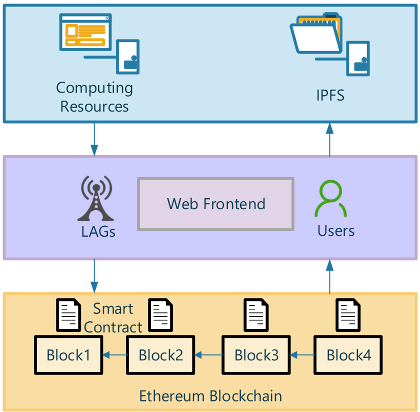


Fig. 2. The software architecture of our proposed spectrum sharing system

3 Privacy-Preserving Double Auction

3.1 System Model

We assume that SPs and SDs share resources that will take effect in the future within a fixed time period T through transactions. We assume that each SP has one idle channel during time period T. SPs will rent their idle spectrum resource for benefits. Meanwhile SDs desire one channel to meet their needs for data transmission in T period. The market can reflect changes in supply and demand in a timely and flexible manner, transmit information on supply and demand, and achieve a reasonable allocation of resources. Thus, we decide to take advantage of double auction to allocate and price resources. In order to protect the privacy of SPs and SDs during the auction, we have proposed privacy-preserving double auction mechanism.

3.2 Proposed Privacy-Preserving Double Auction Mechanism

In this double auction mechanism, we assume that the utility of SD j is the difference between the valuation and the payment of the spectrum resource he obtains.

Definition 1 *(An SD's Utility): The utility of SD j that participating in spectrum trading is:*

$$U_j = \sum_{i \in M} v_{j,i} x_{j,i} - \sum_{i \in M} p x_{j,i}, \tag{1}$$

where $x_{j,i}$ means SD j successfully obtain SP i's idle spectrum resource and M is the collection of SPs.

Similarly, the utility of SP i can be defined in this way.

Definition 2 *(An SP's Utility): The profit of SP i that participating in spectrum trading is defined as:*

$$L_i = p \sum_{j \in N} x_{i,j} - s_i \sum_{j \in N} x_{i,j}. \tag{2}$$

N is the collection of SDs.

Social welfare is defined as the difference between SDs' utility and SPs' utility.

Definition 3 *(Social welfare): The social welfare of this trading platform is defined as:*

$$\begin{aligned} SW &= \sum_{j \in N} U_j - \sum_{i \in M} L_i & (3)\\ &= \sum_{j \in N} \sum_{i \in M} v_{j,i} x_{j,i} - s_i \sum_{i \in M} \sum_{j \in N} x_{i,j} & (4)\\ &= \sum_{j \in N} \sum_{i \in M} x_{j,i} \cdot (v_{j,i} - s_i). & (5) \end{aligned}$$

Differential privacy is a method in cryptography that aims to provide a method to maximize the accuracy of data queries when querying from a statistical database while minimizing the chance of identifying its records.

Definition 4 *(ϵ-differential Privacy [11]). A randomized mechanism $\mathcal{M}$ gives ϵ- differential privacy if for all data sets $\boldsymbol{D}_1$ and $\boldsymbol{D}_2$ differing on a single user, and all $s \subseteq range(m)$,*

$$\Pr\left[\mathcal{M}\left(\mathbf{D}_1 \in \mathcal{S}\right)\right] \leq \exp(\epsilon) \times \Pr\left[\mathcal{M}\left(\mathbf{D}_2 \in \mathcal{S}\right)\right], \tag{6}$$

where $\epsilon \geq 0$ is a small constant.

Laplace mechanism and exponential mechanism are the most commonly used mechanisms that satisfy ϵ-differential privacy [12]. For Laplace mechanism, its main idea is to add noise that following Laplace distribution into the data set that is to be submitted. Exponential mechanism mainly deals with some algorithms whose output results are non-numeric. The bids submitted by SPs and SDs are continuous. Thus, the Laplace mechanism is chosen to protect users' privacy in the double auction scheme we proposed.

Definition 5 *(Laplace Mechanism [11]). Given a function $f : \mathcal{D} \to \mathcal{R}^d$ over a dataset $\mathcal{D}$, mechanism $\mathcal{M}$ provides the ϵ-differential privacy if it follows*

$$\mathcal{M}(D) = f(D) + \mathrm{Lap}(\Delta f/\epsilon), \tag{7}$$

where the noise $\mathrm{Lap}(\Delta f/\epsilon)$ *is drawn from a Laplace distribution with mean zero and scale $\Delta f/\epsilon$.*

Definition 6 *(l_1-sensitivity [11]). Let $f : \mathcal{D} \to \mathcal{R}^d$ be a deterministic function. The l_1-sensitivity of f is:*

$$\Delta f = \max_{x,y \in \mathcal{R}^d} \|f(x) - f(y)\|_1, \tag{8}$$

We use l_1-sensitivity to represent the largest difference between the values of f of any two neighboring datasets.

In the blockchain, each node can obtain information in blocks easily by querying its local blockchain copy. And these blocks include users' bids and other information. The bid information implies some hidden information of users. In order to protect the privacy of users in such an open and transparent environment in blockchain network, we decided to introduce a differential privacy mechanism. Let $\tilde{s_i}$ denote additive noise l_i that follow the Laplace distribution to spectrum provider SP_i's bid value s_i as:

$$\tilde{s_i} = s_i + l_i. \tag{9}$$

Similarly, $\tilde{b_j}$ denotes additive noise l_j to SD_j's bid value b_j.

4 Solution and Analysis

4.1 Winner Determination

We maximize social welfare, as the goal of the resource allocation problem. The social welfare is defined as follows:

$$\max_{\mathbf{X}} \quad \sum_{j=1}^{J}\sum_{i=1}^{I} x_{j,i} \cdot (v_{j,i} - s_i) \tag{10}$$

$$\text{s.t.} \quad x_{j,i} \in \{0, 1\}, \tag{11}$$

$$\sum_{j=1}^{J} x_{j,i} \le 1, \forall i \in \{1, 2, ...I\}, \tag{12}$$

$$\sum_{i=1}^{I} x_{j,i} \le 1, \forall j \in \{1, 2, ...J\}. \tag{13}$$

I and J represent the total number of SPs and SDs respectively. The first constraint indicates that this problem is actually a decision problem, that is, whether to give the channel of SP i to SD j according to the contribution to social welfare based on this decision. Since we assume that the entire system is deployed in a smaller area, the spectrum resources of the same channel cannot be reused by geographical division. So we set the restriction that spectrum resources cannot be reused. And the winner determination problem is an linear programming problem (ILP). And ILP is well known as NP. Thus, the winner determination problem is also NP.

After SDs and SPs obtain the obfuscation function from execution result of smart contract from order blockchain, they add noise to their original bids according to the parameters in the obfuscation function. The winner determination problem in the spectrum sharing scheme we proposed can be regarded as an $0-1$ ILP problem. Thus, this WDP problem for the maximum social welfare can be thought as an assignment problem. So we express our WDP problem as a standard form of assignment problem as:

$$\min_{\mathbf{X}} \quad \sum_{j=1}^{J}\sum_{i=1}^{I}(\tilde{s}_i - \tilde{v}_{j,i})x_{j,i} \tag{14}$$

$$\text{s.t.} \quad \sum_{j=1}^{J} x_{j,i} \leq 1, \forall i \in \{1, 2, ...I\}, \tag{15}$$

$$\sum_{i=1}^{I} x_{j,i} \leq 1, \forall j \in \{1, 2, ...J\}, \tag{16}$$

$$x_{j,i} \in \{0, 1\}. \tag{17}$$

With the standard form of the assignment problem, the Hungarian algorithm can be exploited to solve the problem and obtain the optimal solution efficiently. The computational cost is dominated by the Hungarian method with the complexity of $O\left(n^3\right)$.

4.2 Clearing Price Determination

After solving the optimization problem, a resource allocation scheme that meets the optimization objective we proposed can be obtained. We suggest a simple but reasonable pricing strategy in such a static double auction scheme running on the blockchain. We prosume that n SDs and m SPs are matched according to the execution result of the algorithm. In this allocation result, $\underline{b}_n$ is the lowest matched bid and $\bar{a}_m$ is the highest matched ask of channels. we take use of the k-double auction(k-DA)[13] to decide the clearing price as:

$$p_c = k\underline{b}_n + (1-k)\bar{a}_m. \tag{18}$$

And k is a parameter between 0 and 1. When the number of users participating in spectrum sharing increases, this auction is able to converge to being strategy-proof and truthful bidding [14].

4.3 Theoretical Analysis

In this section, we analyze the properties of the proposed privacy-preserving double auction scheme. We first show that the proposed mechanism can achieve individual rationality.

Theorem 1. *The privacy-preserving double auction scheme satisfies individual rationality.*

Proof: According to the policy of winner determination and pricing, the payment must less than or equal to the bid. The clearing price is $p_c = k\underline{b}_n + (1-k)\bar{a}_m$. We assume that SP i and SD j are in the winner set. The utility of SP i is $L_i = s_i - p_c$. And the utility of SD j is $U_j = v_{j,i} - p_c$. And k is a parameter between 0 and 1. $U_j \geq 0$, $L_i \geq 0$ for all winners. Therefore, we prove that individual rationality is satisfied.

Next, we will prove that the auctioneer obtains non-negative utility.

Theorem 2. *The privacy-preserving double auction scheme satisfies budget balance.*

Proof: In our proposed scheme, an auctioneer also acts as a block manager. It can get its commission from the generation of the block as an auctioneer in the form of tokens, which is also recorded into a block. Thus, the auction scheme will keep a budget balance.

Then, we will show that the proposed mechanism has the property of truthfulness. No participant can obtain a higher utility by misreporting its true valuation.

Theorem 3. *The privacy-preserving double auction scheme satisfies truthfulness.*

Proof: The privacy-preserving double auction scheme we proposed has the property of truthfulness if any SP and SD can not obtain a better utility through misreporting their true valuation for spectrum resources. We focus on the SPs and envision four situations:

1. We consider the scenario where a SP is not selected in the winner set no matter whether he gives his true valuation. In this case, the SP will obtain zero utility. SPs can not obtain better utility by misreporting his true valuation.
2. We consider the scenario where a SP is selected as in the winner set only when he bids truthfully. If he gives a higher bid than his valuation, he is not selected as a winner seller and obtains zero utility. If he gives a lower bid than his valuation, he receives a negative utility. Consequently, SPs can not obtain better utility through misreporting his true valuation.
3. We consider the scenario where a SP is selected as in the winner set only when he bids untruthfully. In this case, his valuation equals the clearing price. If the SP gives a higher bid, he does not obtain the spectrum resource and finally receives a zero utility. If the SP gives a lower bid, he obtains a negative utility. Therefore, the SP's untruthful bidding can not achieve high utility.

4. We consider the scenario where a SP is selected in the winner set no matter whether he gives his true valuation. In this case, the SP is charged the same clearing price p_c when he bids truthfully and untruthfully. Thus, the SP can not obtain better utility through misreporting his true valuation.

Therefore, SPs can not achieve higher utility by misreporting their true valuation. Similarly, we can conclude that SDs can not obtain higher utility by misreporting their true valuation as well. Thus, the privacy-preserving double auction scheme satisfies truthfulness.

Differential privacy ensure that the change in any users bid will not bring a significant change to the result of the proposed mechanism to avoid the inference attack. We prove that the proposed mechanism satisfies ϵ-differential privacy.

Theorem 4 *(ϵ-differential Privacy). Our privacy ϵ-preserving double auction scheme satisfies ϵ-differential privacy.*

Proof: We present a Laplace-based winner determination and pricing policy as the main logic of smart contracts to protect the privacy of the valuation information of SPs and SDs in the blockchain-based dynamic spectrum sharing scheme. We add randomly distributed noise following Laplace distribution Lap($\Delta f/\epsilon$) to each user's bid information. The proof of *Definition 6* can be found in [15].

5 Performance Evaluation

In this section, we evaluate the performance of the blockchain-based privacy-preserving mechanism on spectrum trading and bid privacy preservation.

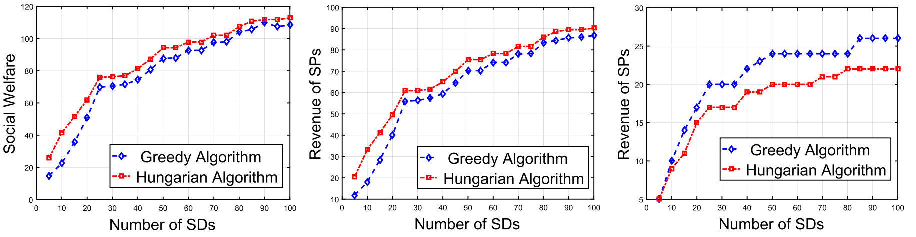
5.1 Simulation Setup

We take advantage of the truffle framework to build this platform. The smart contract was written by the remix tool and deployed on the test chain. Web3.js is adopted to interact with the smart contract. The server built by python is started locally and the function of solving resource allocation problem is realized on the server. Related code implementation can be consulted on https://WWW.github.com/ZhitianTU-NUAA/Dapp.

In the resource allocation problem we introduced, the number of SPs is set to 30 while the number of SDs varies from 5 to 100 with a step of 5. We assume that each SP's resources can only be exploited exclusively by one SD due to the small geographic distance between each user for simplicity. The bids of users are random picked over $(5, 10]$. All the results are averaged over 100 times.

5.2 Performance on Spectrum Trading

To solve the problem of resource allocation, we introduced Hungarian Algorithm[16]. And we set one allocation scheme based on the Greedy algorithm



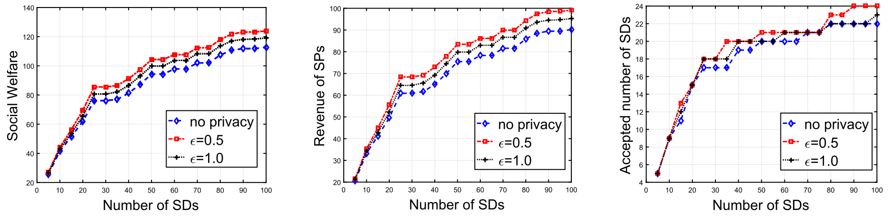
(a) Social welfare (b) Revenue of SPs (c) Accepted number of SDs

Fig. 3. Performance on spectrum trading

as a comparison. Figure 3a and Fig. 3b show that the Hungarian algorithm can be used to allocate spectrum resources to obtain the maximum social welfare and SPs' revenue, compared to Greedy algorithm under the same number of SDs. However, the utilization of spectrum resources cannot be taken into account at the same time. The Greedy algorithm considers from the perspective of SPs. And for each spectrum resource of SP, the corresponding SD who can provide the maximal social benefit is selected as the winner. So, the Greedy algorithm can obtain a higher spectrum resource utilization rate compared to Hungarian Algorithm, as is shown in Fig. 3c. Since there may be a situation during the transaction process that no SD can give a bid higher than the price a certain SP asks, some transactions will fail.

5.3 Performance on Bid Privacy Preservation

Figure 4 illustrates the social welfare and revenue of SPs as well as the accepted number of SDs under different differential privacy parameters respectively in our proposed auction scheme. With the increasing number of SDs, social welfare grows rapidly at the beginning and then gradually approaches a certain maximum. Revenue of SPs and the number of accepted SDs will gradually increase in a similar way, as is revealed in Fig. 4b and Fig. 4c. Adding noise to users' bids will cause some certain disturbance to the result of social welfare, revenue of SPs and the accepted number of SDs. When ϵ decreases, the disturbance becomes larger. ϵ indicates the degree of privacy protecting. When the parameter ϵ is small, it can largely guarantee users' privacy in differential privacy. But this also lead to a result that users have to add more noise to their bids which will result in less data availability.



(a) Social welfare

(b) Revenue of SPs

(c) Accepted number of SDs

Fig. 4. Performance on bid privacy preservation

6 Conclusion

In this paper, we introduce blockchain technology in spectrum resource sharing and propose a blockchain-based spectrum resource sharing platform. A privacy-preserving double auction mechanism is designed to run on the blockchain network in the form of smart contracts to protect users' privacy, reach reasonable allocation of spectrum resources and improve spectrum resource utilization in an untrusted environment. And the proposed double auction mechanism is proved to satisfy differential privacy, individual rationality, computational efficiency and truthfulness. The experimental evaluations show that blockchain-based privacy-preserving dynamic spectrum sharing scheme has the ability to improve spectrum trading efficiency and protect users' privacy.

References

1. Peha, J.M.: Approaches to spectrum sharing. IEEE Commun. Mag. **43**(2), 10–12 (2005)
2. Zhao, Q., Sadler, B.M.: A survey of dynamic spectrum access. IEEE Sig. Process. Mag. **24**(3), 79–89 (2007)
3. Sohul, M.M., Yao, M., Yang, T., Reed, J.H.: Spectrum access system for the citizen broadband radio service. IEEE Commun. Mag. **53**(7), 18–25 (2015)
4. Yrjölä, S.: Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept. In: Marques, P., Radwan, A., Mumtaz, S., Noguet, D., Rodriguez, J., Gundlach, M. (eds.) CrownCom 2017. LNICST, vol. 228, pp. 128–139. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76207-4_11
5. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., Zhang, Y.: Blockchain and deep reinforcement learning empowered intelligent 5g beyond. IEEE Netw. **33**(3), 10–17 (2019)
6. Kumar, S.P., Yeon, M.S., Hyuk, P.J.: Block-VN: a distributed blockchain based vehicular network architecture in smart city. In: Annual Symposium on Foundations of Computer Science, vol. 13, no. 1, pp. 184–195 (2017)
7. Weiss, M.B.H., Werbach, K., Sicker, D.C., Bastidas, C.E.C.: On the application of blockchains to spectrum management. IEEE Trans. Cognit. Commun. Netw. **5**(2), 193–205 (2019)

8. Kotobi, K., Bilen, S.G.: Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access. IEEE Veh. Technol. Mag. **13**(1), 32–39 (2018)
9. Grissa, M., Yavuz, A.A., Hamdaoui, B.: Trustsas: a trustworthy spectrum access system for the 3.5 GHZ CBRS band. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pp. 1495–1503, April 2019
10. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564, June 2017
11. Frank, M., Kunal, T.: Mechanism design via differential privacy. In: FOCS vol. 7, pp. 94–103 (2007)
12. Wang, Z., Li, J., Hu, J., Ren, J., Li, Z., Li, Y.: Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pp. 2053–2061, April 2019
13. Mark, S., Steven, W.: Bilateral trade with the sealed bid k-double auction: existence and efficiency. J. Econ. Theory **48**(1), 107–133 (1989)
14. Kazuo, M.: Online double auction mechanism for perishable goods. Elsevier Electron. Commer. Res. Appl. **13**(5), 355–367 (2014)
15. Cynthia, D., Aaron, R., et al.: The algorithmic foundations of differential privacy. Found. Trends® Theoret. Comput. Sci. **9**(3–4), 211–407 (2014)
16. Harold, K.W.: The Hungarian method for the assignment problem. Naval Res. Logist. Q. **2**(1–2), 83–97 (1955)