Smart contract-based secure cooperative spectrum sensing algorithm

Chu Ji1,2 and Qi Zhu1,2

Abstract
Spectrum sensing is the key technology of cognitive radio. In this article, we apply blockchain technology in spectrum sensing process and propose a related algorithm based on reputation. The algorithm builds a system model based on smart contract in blockchain and applies blockchain asymmetric encryption algorithm and digital signature technology in the process of secondary users’ transmitting local judgments to the secondary user base station. The algorithm can resist spectrum sensing data falsification (SSDF) attack launched by malicious users. This article comprehensively considers the channel error rate, detection probability, secondary user base station budget and remaining energy of the secondary users (SUs) and then establishes the SU’s utility function as well as the game model. By solving the Nash equilibrium, the SU determines whether it uploads sensing data. Finally, the SU base station selects registered SUs by calculating and updating their reputation, obtaining the final judgment by voting rule. With simulations, we prove that the algorithm proposed in this article increases the accuracy and security of spectrum sensing and can effectively resist SSDF attack.

Keywords
Cooperative spectrum sensing, blockchain, smart contract, game theory, reputation mechanism

Date received: 23 February 2021; accepted: 7 October 2021

Handling Editor: Yanjiao Chen

Introduction
With the vigorous advances in the mobile Internet and the Internet of Things, people’s demand for spectrum resources is even more urgent.1 Traditional radio spectrum allocation is a fixed allocation strategy, which prevents the spectrum resources from being fully utilized. Cognitive radio technology is a spectrum sharing technology which has a significant role in improving spectrum utilization.2 Spectrum sensing is the key technology of cognitive radio systems. When spectrum sensing is performed by a single SU, it is easily affected by shadow effects, multipath fading and other factors, so it is difficult for a single SU to make correct local judgments. Multi-user cooperative spectrum sensing can overcome these difficulties, but it will bring some conditions such as malicious SU collusion attacks and tampering of sensing data,3 which will seriously affect the performance and efficiency of spectrum sensing. Blockchain technology can effectively solve these problems.4 People have conducted in-depth research on spectrum sensing technology. Khasawneh et al.5 proposed a routing algorithm to perform spectrum sensing and realize spectrum management. They defined a parameter to measure SUs’ sensing behaviors and encoded...
sensing data. To optimize spectrum sensing performance and power allocation, Karimi et al.\textsuperscript{5} proposed a probabilistic spectrum access scheme. Hu and Zhu\textsuperscript{7} applied incentive mechanism of crowdsensing in cooperative spectrum sensing and proposed a relative algorithm based on game to maximize the utility of SU. Kotobi et al.\textsuperscript{8} proposed a puzzle-based spectrum sharing auction mechanism. For SUs who want to buy available spectrum, a puzzle is set as a threshold, and only the first SU who solves the puzzle correctly can obtain the right to use it. Zhu et al.\textsuperscript{9} presented a reverse Vickery auction incentive mechanism (RVA-IM) and conducted research and analysis on provider selection, payment determination and QC process. From the perspective of behavioral economics, Liu and Gao\textsuperscript{10} studied the influence of user loss aversion on the results of spectrum sensing and proposed an incentive mechanism based on user loss aversion. However, the above researches do not consider the security issues of spectrum sensing. Since incentive mechanism is actually a transaction between SU base station and SUs, the above articles lack a reliable mechanism to ensure the security of transactions and to defend the attack of malicious users.

Blockchain technology can guarantee the security of transactions. Blockchain is a chain-type data structure connected in chronological and is order based on blocks.\textsuperscript{11} It does not require a third party to interfere and monitor. Blockchain uses cryptography technology, consensus mechanism and some other technologies to maintain a set of tamper-resistant ledger records among mutual distrust or weak trust SUs so as to ensure the consistency, authenticity, security and reliability of data shared by nodes in the distributed network,\textsuperscript{12} and blockchain can effectively resist malicious attacks. He et al.\textsuperscript{13} proposed an incentive mechanism in the application of crowdsensing based on blockchain, which quantifies the contribution of SUs to distribute payments and uses digital watermarking technology to process the sensing data uploaded by SUs. Sun and Xiong\textsuperscript{14} established a consortium blockchain on multiple authorized local base stations, regarded the use of spectrum resources as a transaction and proposed a loan-based payment scheme, giving an optimal pricing strategy. The importance role of consensus mechanism in blockchain technology and the comparison of the two main consensus mechanisms Proof of Work (PoW) and Proof of Stake (PoS) are shown in literature.\textsuperscript{15} PoW is that the node with the largest computing power will eventually win the mining, while PoS means that the node with more coins will mine blocks more easily. Bayhan et al.\textsuperscript{16} proposed the Spectrum Sensing as a Service (Spass) system model and two-threshold based voting (TTBV) algorithm via smart contracts. The algorithm can ensure that malicious users will be excluded. Chen et al.\textsuperscript{17} established a data transaction framework based on consortium blockchain and proposed an iterative double auction mechanism. The mechanism aims to prompt buyers and sellers to submit their bids as well as determine how many and how much of the spectrum resources they want to transact. Kotobi and Bilin\textsuperscript{18} proposed a blockchain verification protocol that uses the First Come First Service (FCFS) auction mechanism for transactions. They also introduced a virtual currency called Specoins to pay fees in spectrum transactions. However, the above literatures rarely consider the existence of malicious users at the stage of selecting users by the SU base station and lack a practical selection mechanism. In addition, these researches do not consider the reputation of SUs or apply smart contract to spectrum sensing.

Smart contract is a computer transaction agreement that executes the contract digitally on the blockchain. These transactions are transparent, traceable and irreversible. Based on blockchain technology, this article proposes a secure cooperative spectrum sensing algorithm to improve the accuracy and efficiency of spectrum sensing while resisting MU attacks. We regards the SU base station and each SU as a node on the blockchain and transform the entire spectrum sensing process into the automatic execution of smart contracts on the blockchain. The algorithm first defines the utility function of the SU, establishes the optimization problem of maximizing the utility of the SU and obtains the optimal sensing time of the SU in the way of game. The SU base station adopts a reputation mechanism proposed in this article to select SUs and exclude malicious SUs. Finally, the SU base station adopts voting rule to make the final judgment according to the weight of each user’s reputation value. The main contributions of this article are summarized as follows:

1. We construct a cooperative spectrum sensing system model based on smart contract of blockchain to execute the entire spectrum sensing process automatically. Once trigger conditions are met, the smart contract will execute automatically on the blockchain, which realizes the autonomy of transactions and improves overall efficiency. During the stage of SUs upload local judgments, we use asymmetric encryption technology to encrypt and digitally sign the uploaded data, so as to prevent malicious users from impersonating as normal SUs to upload low-quality sensing data and reducing the probability of normal SUs being selected.

2. We propose a SU utility optimization algorithm using game theory. Since SUs report sensing data to the SU base station wirelessly, there must be errors during the transmission. Therefore, channel error rate is considered in
this article, which is closer to the actual situation. We define the SU utility function based on the detection probability, reward, channel error rate and the remaining energy of the SU, and then calculate the unique Nash Equilibrium. Once all SUs achieve the Nash Equilibrium, the utilities of SUs are maximized and cannot be improved by deviating from current strategies. We prove the existence of Nash equilibrium and obtains the closed expression of the optimal sensing time.

3. We design a reputation mechanism for the SU base station to distinguish malicious users from normal ones by comprehensively considering their historical sensing behaviors and detection probability. The SU base station checks the historical sensing behaviors of each SU from the blockchain and updates their reputation values. In the fusion stage, the fusion center assigns different weights to each SU according to their reputation values and obtains the final judgment by voting rule.

The rest of this article is arranged as follows. We describe the system model and smart contract model in Section II. We formulate the optimization problem and prove the existence of the Nash Equilibrium in the game in Section III. We propose a reputation mechanism in Section IV. The results of simulations and analyses are shown in Section V. Finally, the conclusion is summarized in Section VI.

System model and smart contract model

System model
As shown in Figure 1, a cognitive radio network consists of a SU base station, a primary user, N SUs and some malicious users, which are all nodes on the blockchain. The SU base station publishes spectrum sensing tasks via smart contract. Each SU calculates their own utility according to utility function, and they will accept sensing task once the utility is larger than the average utility. SUs perform local spectrum sensing tasks through energy detection and send the encrypted sensing data to the SU base station. Then the SU base station selects SUs by their reputation and uses voting fusion algorithm to make the final judgment.

The SU uses energy detection to sense the spectrum. \( \text{SNR} \) represents the ratio of the signal received by SU from primary user to its noise, and SU’s detection probability \( P_{di} \) is

\[
P_{di} = Q \left( \frac{Q^{-1}(P_{fi}) - \sqrt{i_j f_s \text{SNR}_i}}{\sqrt{2 \text{SNR}_i + 1}} \right)
\]

Where \( P_{fi} \) represents the false alarm probability of SU \( i \). It’s the probability that the SU misjudges the absence of the primary user as present. \( t_i \) represents the sensing time of the SU \( i \), \( f_s \) represents the sampling frequency and \( f_{sf} \) represents SU’s sampling points. \( \text{SNR}_i \) represents the signal-to-noise ratio of the SU. \( Q \) function is a complementary cumulative distribution function. Its expression is

\[
Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-\frac{t^2}{2}} dt
\]

After the SU base station receives the sensing data reported by SU, it uses the voting rule to process the data. The voting rule is that the system sets a voting threshold \( k \). When \( k \) or more SUs among \( n \) users support the judgment of the presence of the primary user, the system judges that the primary user exists, so the voting rule is also called \( k/n \) rule. The detection probability \( P_D \) and false alarm probability \( P_F \) of the voting rule are

\[
P_D = \sum_{j-k}^N \sum_{u_i=j} \prod_{i} P_{di}^u (1 - P_{di})^{1-u_i}
\]

\[
P_F = \sum_{j-k}^N \sum_{u_i=j} \prod_{i} P_{fi}^u (1 - P_{fi})^{1-u_i}
\]

Where \( P_{di} \) and \( P_{fi} \) are the detection probability and false alarm probability of SU \( i \) respectively. \( u_i \) is the local judgment of SU \( i \)

\[
u_i = \begin{cases} 
1, & \sum_{i=1}^N E_i \geq k \\
0, & \sum_{i=1}^N E_i < k
\end{cases}
\]

Spectrum sensing based on smart contract
The essence of blockchain is a distributed network. It combines multiple technologies, such as asymmetric encryption technology, consensus mechanism, smart contract and peer-to-peer transmission. Asymmetric encryption technology can ensure the security of the transaction while smart contract can realize its programmability and autonomy. Applying blockchain technology to the spectrum sensing process can enhance the convenience and security of sensing execution. Smart contract runs on the blockchain. It’s a piece of code that writes the contract into the blockchain in a
digital form. When the content of the contract is satisfied, the code will be automatically executed, which not only avoids the complicated manual operation, but also ensures both parties cannot violate the contract. Due to the characteristics of the blockchain, data cannot be deleted or modified. The entire process is open and transparent and the source can be traced, which greatly avoids malicious attacks that interfere with the normal execution of the contract. The decentralized characteristic of the blockchain can also improve the efficiency and cost advantages of smart contract.

Blockchain is actually a database system which can be distributed in various places and can operate in coordination. The traditional database system presents the characteristics of centralization, while the blockchain, on the contrary, is decentralized. Distributed users, as long as they are connected to the blockchain network, can be a node on the blockchain. All nodes have the rights to read and write data in the database system. The operation is updated synchronously for all nodes. Blockchain is composed of many blocks. A block is composed of block header and block body. Block header records the initial information of the block, such as the hash value of the previous block, the timestamp, the blockchain protocol version, the root hash value of the Merkle tree of the block body, etc. The block body stores the detailed transaction data. The “chain” of the blockchain means the hash pointer and each block is connected in series through the hash value of the previous block stored in its own block header, thus forming a blockchain.

As shown in Figure 2, the SU base station publishes spectrum sensing tasks and proposes task requirements including collection time, budget, geographic location restrictions and frequency band range. Then it uses blockchain-supported programming languages such as Solidity to write tasks into smart contract codes and publishes the written smart contract. Miners package it and write it into the blockchain. Although the smart contract is published on the blockchain, it will not execute automatically in that corresponding trigger conditions must be satisfied. In this article, the trigger condition is that the SU chooses to accept the task after viewing the content of the task and register on the smart contract. After the smart contract is released on the blockchain, the SU base station broadcasts the address of the smart contract on the blockchain. Interested local sensing nodes can retrieve the content of the contract through the address and view the requirements of the sensing task. It calculates its own utility according to its preferences, remaining energy, geographic location, estimated reward and other factors. If the utility is greater than the average of all SUs’ utility, the SU accepts the spectrum sensing task and registers on the smart contract. The smart contract then selects registered nodes with the consideration of its budget, the asked price of SUs and their reputations. Selected nodes start to carry out the sensing task, then they upload sensing results to the SU base station with their digital signatures. The SU base station decrypts and fuses the sensing data as well as pays rewards.

Digital signature is another characteristic of blockchain. Through the verification of the digital signature, the information can be guaranteed not to be tampered during the transmission. Digital signature can also ensure the security of the information and resist malicious attacks. Digital signature is composed of digital digest and asymmetric encryption technology. First, the information is shortened into a fixed-length string through digital digest technology. Then the digest is encrypted using asymmetric encryption technology to form a digital signature. In order to prevent malicious users from impersonating normal SUs or tampering with the sensing data of normal ones, in which case
normal SU’s reputation and probability of being selected will be reduced, we apply blockchain digital signature technology to the process of SU base station verifying spectrum data. Each spectrum sensing device register on the blockchain network, that is, generate a pair of public key and private key \( (key_{public}, key_{private}) \) locally, where the public key is publicly visible and the private key is stored locally and only visible to the user itself. As shown in Figure 3, when the SU \( i \) uploads the sensing data \( Data \) to the SU base station, a hash algorithm is used to generate sensing data digest \( digest_{Data} \) and then the private key \( key_{private}^i \) is used to encrypt the digest to generate a digital signature \( sign_{digest} \). The SU \( i \) attaches the digital signature to the sensing data and uploads it to the SU base station together. After receiving it, the SU base station decrypts the digital signature \( sign_{digest} \) with the public key \( key_{public}^i \) of the SU \( i \) to obtain the digest of the sensing data \( digest_{Data} \). Then it uses a hash algorithm on the sensing data uploaded by the SU \( i \) to obtain \( digest_{Data}^i \). If the result obtained is consistent with the digest obtained by decrypting the digital signature, that is, \( digest_{Data}^i = digest_{Data} \), it can be proved that the sensing data is uploaded by the SU \( i \) and has not been tampered with by malicious users.

**SU sensing time game**

If the channel between the SU and SU base station is ideal, the sensing results of local SUs can be accurately reported to the SU base station through the control channel. However, actually the wireless channel is often influenced by fading and interferences, which cause bit errors in the transmission and deteriorates the performance of spectrum sensing. Assume that the channels between all SUs and SU base station are independent and identically distributed. The channel error rate is \( P_e \).
There are two possibilities for the SU base station to receive the judgment of the local SU as 1: the local judgment sent by the SU is 1 and it is successfully received without being affected by the channel error, or the local judgment sent by the SU is 0, however, due to the influence of the channel error, 0 is changed to 1. There are also two possibilities when the SU base station receives the judgment of the local SU as 0: the local judgment sent by the SU is 0 and is successfully received without being affected by the channel error, or the local judgment sent by the SU is 1, however, due to the influence of the channel error, 1 is changed to 0.

Denote \( P(u_0) \) as the probability that the primary user does not exist, \( P(u_1) \) as the probability that the primary user exists, so that the correct sensing probability \( P_c^i \) and incorrect sensing probability \( P_{inc}^i \) of SU \( i \) are

\[
P_c^i = P(u_i)P_{di} + P(u_0)(1 - P_{fi})
\]
\[
P_{inc}^i = P(u_i)(1 - P_{di}) + P(u_0)P_{fi}
\]

The probability that the SU base station receiving the local judgment of the SU \( i \) is correct \( P_c^i \) and incorrect \( P_{inc}^i \) are

\[
P_c^i = P_c^i(1 - P_c) + P_{inc}^iP_c
\]
\[
P_{inc}^i = P_c^iP_c + P_{inc}^i(1 - P_c)
\]

Where \( P_c \) is error rate. Assuming that the SU adopts the DPSK modulation, the error rate of the receiving end using incoherent demodulation is \( P_c = \frac{1}{2}e^{-\gamma}, \) where \( \gamma \) is the signal-to-noise ratio of the SU base station receiving the SU signal.

The final expression of the voting rule used by the SU base station is

\[
P_D = \sum_{j = k}^{N} \sum_{u, u_j} \prod_i (P_c^j)^u_i(1 - P_c^j)^{1 - u_i}
\]

\[
= \sum_{j = k}^{N} \sum_{u, u_j} \prod_i \left[ P_c^j(1 - P_c) + P_{inc}^jP_c \right]^{u_i}
\]

\[
[1 - P_c^j(1 - P_c) - P_{inc}^jP_c]^{1 - u_i}
\]

\[
= \sum_{j = k}^{N} \sum_{u, u_j} \prod_i \left\{ (1 - P_c^j) [P(u_i)P_{di} + P(u_0)(1 - P_{fi})] + P_c^j[P(u_1)(1 - P_{di}) + P(u_0)P_{fi}] \right\}^{u_i}
\]

\[
[1 - (1 - P_c^j)(P(u_i)P_{di} + P(u_0)(1 - P_{fi}))]
\]

\[
- P_c^j[P(u_1)(1 - P_{di}) + P(u_0)P_{fi}] \right\}^{1 - u_i}
\]

\[
(10)
\]

For a SU, the benefit of participating in spectrum sensing is to get a reward from the SU base station, which is related to the sensing accuracy. The sensing accuracy is related to the sensing time. The longer the time, the higher the accuracy. However, the SU also needs to pay a certain cost to sense the spectrum. When performing tasks, the SU will consume energy. The longer the sensing time, the greater the energy consumption paid. So the utility is a comprehensive consideration of rewards, sensing time, and energy consumption. For a SU, when the remaining energy is small, it is unwilling to participate in sensing tasks, so the remaining energy factor is considered in the utility function. Therefore, the utility function is the difference between the sensing reward and the cost

\[
u_i = \alpha \cdot \frac{P_{inc}^i}{\ln E_i} - B \cdot \frac{t_i}{\ln E_i}
\]

(11)

Where \( \alpha \) and \( \beta \) are coefficients, \( B \) is the budget of the sensing task, \( t_i \) is the SU’s sensing time and \( E_i \) is the remaining energy of the SU \( i \). The former part of the utility represents the reward of the SU and the latter part represents the sensing cost.

In formula (11), only the sensing time can be determined by the SU. In order to optimize its own utility, the SU needs to determine its own optimal sensing time, so the optimization problem can be expressed as

\[
\max_{h} \frac{\alpha}{\sum_{i=1}^{N} P_{inc}^i} \cdot B - \beta \cdot \frac{t_i}{\ln E_i}
\]

(12)

There is a game among \( N \) SUs and the game strategy of each SU is the sensing time. Since every SU is rational and selfish, they will aim to maximize their own utilities. Nash equilibrium is the best result that each SU can get in the game. When other SUs keep their strategies unchanged, every SU’s strategy is the best strategy and any SU can’t get higher reward by only changing its own strategy.

Game theory is a mathematical method to study competitive phenomena among players. In a game, players are interrelated with each other. Each player will not only affect other players, but also be affected by other players’ strategies. These strategies will affect the final overall decision. Formula (11) shows that the utility of each SU has relations with its sensing time, detection probability and remaining energy as well as other SUs’ detection probabilities. Therefore, the SU can take part in a game to maximize its utility.

Equilibrium refers to the optimal strategy combination of all players in the game. Nash equilibrium refers to the strategy of the players in the game reaching a stable state, that is, when the strategies of other players remain unchanged, any player’s strategy is optimal. In the game \( G = \{S_1, S_2, \cdots, S_N; u_1, u_2, \cdots, u_N\} \), suppose a certain strategy combination is \( s^* = (s_1^*, s_2^*, \cdots, s_N^*) \),
the strategy $s_i^*$ of any player $i$ is the optimal strategy for the strategies $s_{-i} = (s_1^*, s_2^*, \cdots, s_{i-1}^*, s_{i+1}^*, \cdots, s_N^*)$ of other players, namely

$$u_i(s_1^*, s_2^*, \cdots, s_{i-1}^*, s_i^*, s_{i+1}^*, \cdots, s_N^*) \geq u_i(s_1^*, s_2^*, \cdots, s_{i-1}^*, s_i, s_{i+1}^*, \cdots, s_N^*), \forall s_i \in S_i$$ (13)

When the above condition is satisfied, $s^* = (s_1^*, s_2^*, \cdots, s_N^*)$ is the Nash equilibrium of game $G$.

In the game $G = \{S_1, S_2, \ldots, S_N; u_1, u_2, \ldots, u_N\}$, when the following three conditions are met simultaneously, it can be considered that there is a Nash equilibrium:

1. The game is a finite and non-empty set;
2. Strategy set $S$ is a non-empty set of Euclidean space;
3. The utility function is strictly concave.

The following is the proof of the existence of Nash equilibrium in the SU sensing time game:

The strategy set of the SUs is $(t_1^*, t_2^*, \cdots, t_N^*)$ and the optimal utility of the SUs is $u_i(t_1^*, t_2^*, \cdots, t_N^*)$. The first two conditions are easily satisfied in that the game set is finite and not empty. At the same time, the strategy is also not empty. To prove the third condition, we only need to prove that the second-order derivative of $u_i$ with respect to $t_i$ is less than 0. To calculate the derivative, the first step is to expand formula (11) to express all the terms related to $t_i$ in detail. According to formula (11),

The first-order derivative of $P_d$ with respect to $t_i$ is

$$P'_d = \frac{\sqrt{\text{SNR}}}{\sqrt{2\pi(2\text{SNR})} + 1} \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}}$$ (14)

Where $m = \frac{Q^{-1}(p_i) - \sqrt{\text{SNR}}}{\sqrt{2\text{SNR}} + 1}$.

For simplicity, let $P(u_0) = P(u_1) = \frac{1}{2}$, so that

$$P'^c = \left(\frac{1}{2} - P_e\right)P_d + \left(P_e - \frac{1}{2}\right)P_h + \frac{1}{2}$$

$$= \left(\frac{1}{2} - e^{-\gamma}\right)P_d + \left(\frac{1}{2} - e^{-\gamma} - 1\right)P_h + \frac{1}{2}$$ (15)

So the derivative of $u_i$ with respect to $t_i$ is

$$\frac{\partial u_i}{\partial t_i} = \alpha \cdot \beta \cdot \left(\frac{1}{2} - e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c$$

Let $s = \alpha \cdot \beta \cdot \frac{\sqrt{\text{SNR}}}{2\sqrt{2\pi(2\text{SNR})} + 1}$, so that

$$\frac{\partial u_i}{\partial t_i} = s \cdot \left(\frac{1}{2} - e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}} - \beta \frac{1}{\ln E_i} \cdot e^{-\frac{t_i}{\sqrt{2}}}$$ (17)

So the second-order derivative of $u_i$ with respect to $t_i$ is

$$\frac{\partial^2 u_i}{\partial t_i^2} = s \cdot \left(\frac{1}{2} - e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}} + \beta \cdot e^{-\frac{t_i}{\sqrt{2}}} \cdot L$$ (18)

Where

$$L = \left(\frac{mQ}{2} - \frac{1}{2}t_i\right) \sum_{i = 1}^N P'^c - \left(\frac{1}{2} - \frac{1}{2}e^{-\gamma}\right) \cdot \frac{Q}{\sqrt{2\pi}} \cdot e^{-\frac{t_i}{\sqrt{2}}}$$ (19)

Where

$$Q = \frac{\sqrt{\text{SNR}}}{\sqrt{2\text{SNR}} + 1}$$ (20)

It's obvious from the formula of $s$ that the coefficient, budget and signal-to-noise ratio are all positive, so $s > 0$. Due to the signal-to-noise ratio $\gamma > 0$, it can be seen from the image of the function $f(\gamma) = \frac{1}{2} - \frac{1}{2}e^{-\gamma}$ that when $\gamma > 0$, $f(\gamma) \in (0, 0.5)$. Also because of $t_i^{-1} \cdot e^{-\frac{t_i}{\sqrt{2}}} > 0$, the previous terms of $L$ in formula (18) are all positive. Because $m \leq 0$ and $Q > 0$, so $L < 0$, therefore $\frac{\partial^2 u_i}{\partial t_i^2} > 0$, and there exists a Nash equilibrium in the SU sensing time game.

Since the second-order derivative of $u_i$ with respect to $t_i$ is less than 0, its first-order derivative decreases monotonically, and $m \leq 0$, that is, $Q^{-1}(P_i) - \sqrt{\text{SNR}} \leq 0$.

So $t_i \geq \left(\frac{Q^{-1}(P_i)}{\text{SNR} \sqrt{\text{SNR}}}\right)^2$. When $t_i$ taking the minimum value

$$\left(\frac{Q^{-1}(P_i)}{\text{SNR} \sqrt{\text{SNR}}}\right)^2, m = 0, s \cdot \left(\frac{1}{2} - \frac{1}{2}e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}} = s \cdot \left(\frac{1}{2} - \frac{1}{2}e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}} = 0$$. When $t_i \to \infty,$

$$s \cdot \left(\frac{1}{2} - \frac{1}{2}e^{-\gamma}\right) \cdot \sum_{i \in N \setminus \{i\}} P'^c \cdot \frac{1}{\sqrt{t_i}} \cdot e^{-\frac{t_i}{\sqrt{2}}} \to 0$$. In that $\frac{\beta}{\ln E_i} > 0$,

so when $t_i \to \infty, \frac{\partial u_i}{\partial t_i} < 0$, that is, there exists a negative value for the first-order derivative of $u_i$ with respect to $t_i$. Therefore, if the maximum value of the first-order
derivative of \( u_i \) with respect to \( t_i \) is greater than 0, then there is an optimal sensing time \( t_i^* \) such that \( u_i \) has a maximum value, which can be obtained by solving the following equations

\[
\begin{align*}
\left\{ \begin{array}{l}
\alpha \cdot B \cdot \left( \frac{1}{2} - \frac{1}{2} e^{-\gamma} \right) \cdot \sum_{i \in \mathcal{N} \setminus \{i\}} \frac{P_{rc}^i}{\sqrt{\left( \frac{\sqrt{SNR_i}}{2\sqrt{SNR_i} + 1} \right)}} > 0 \\
Q^{-1}(P_{rc}^i) - \sqrt{SNR_i} \leq 0
\end{array} \right.
\end{align*}
\]

if the maximum value of the first-order derivative of \( u_i \) with respect to \( t_i \) is less than 0, then the optimal sensing time \( t_i^* \) is \( \left( \frac{Q^{-1}(P_{rc}^i)}{\sqrt{SNR_i}} \right)^2 \).

When the detection probabilities of other \( N - 1 \) SUs are known, each SU can obtain the optimal sensing time according to its own utility function and hence obtain its maximum utility. There is a game among \( N \) SUs. Nash equilibrium is the state in which each SU performs the spectrum sensing task and upload sensing data to the SU base station. Then the SU base station fuses the sensing data and pays the sensing reward, which is the former part of the SU utility function.

**User selection method based on reputation mechanism**

**Reputation mechanism**

The SUs receiving the task sense the signal transmitted by the primary user and make a local judgment. Then they send the local judgment to the fusion center which merges the local judgments to make the final judgment. In order to find and eliminate malicious users, this article proposes a reputation mechanism. The SU base station checks the historical sensing behaviors of each SU from released blocks and updates reputation continuously according to the number of times the SU sensed tasks successfully in the past as well as the detection probability of this sensing task. In the fusion stage, the fusion center assigns different weights to each SU according to different reputations. The higher the reputation is, the more weight SU will get. On the contrary, the malicious SUs will be given lower weights or even be excluded in the final judgment. In this way, the accuracy of the final judgment is improved. In order to avoid malicious SUs, the SU base station publishes the updated reputation on the blockchain, which not only prevents tampering, but also is publicly visible to all SUs.

In the user selection stage, the SU base station sorts SUs according to the selection function

\[
s(i) = \frac{T_i^k}{c_i} \tag{22}
\]

\[
c_i = \alpha \cdot \sum_{i=1}^{N} P_{rc}^i \cdot B \tag{23}
\]

Where \( T_i \) is the reputation value of the SU \( i \) in the time slot \( k \). \( c_i \) is the asked price of the SU \( i \). The SU base station sorts the selection function in descending order and selects several users from large to small. Each time a SU is selected, the SU base station minus the asked price of that SU from the budget until the budget is used up or all registered SUs are selected. Selected SUs perform the spectrum sensing task and then upload sensing data to the SU base station. The SU base station makes a final judgment based on the weights of selected SUs and their sensing results. After that, the SU base station updates their reputation based on historical sensing behaviors and the detection probabilities of this task.

The local sensing result of the SU \( i \) in time slot \( k \) is \( d_i(k) \) and the fusion center merges their local sensing results of all selected SUs with voting rule is

\[
\hat{d}(k) = \sum_{i=1}^{N} w_i(k) d_i(k) \tag{24}
\]

Where \( w_i(k) \) is the weight of SU \( i \)'s reputation \( T_i^k \) in time slot \( k \), which is

\[
w_i(k) = \begin{cases} 
\frac{T_i^k}{\sum_{i=1}^{N} T_i^k}, & \text{selected} \\
0, & \text{else}
\end{cases} \tag{25}
\]

Then the SU base station compares \( \hat{d}(k) \) with the threshold and obtains the final judgment \( d(k) \)

\[
d(k) = \begin{cases} 
1, & \hat{d}(k) \geq \frac{1}{2} \\
0, & \text{else}
\end{cases} \tag{26}
\]

Assuming that the maximum storage length of the SU base station for the sensing behaviors of the SU is \( L \), then we can get the correct times \( P \) and incorrect times \( G(P + G \leq L) \) of their sensing behaviors. The update of the reputation \( T_i^{k+1} \) in time slot \( k + 1 \) is
Algorithm 1. Cooperative spectrum sensing algorithm based on reputation mechanism.

1. Initialization: \( t_i, T(i) = 0, W = \emptyset \)
2. While (true)
3. \( l = l + 1 \)
4. for \( i = 1 : N \)
5. Obtain \( P_{ci}(t_i) \) from formulas (6) and (7)
6. Calculate \( t_i^* = \arg \max u_i, u_i^* = \max u_i \)
7. end for
8. if \( |t_i^* - t_i| < \varepsilon \)
9. \( [t_i, u_i] = [t_i^*, u_i^*] \)
10. end if
11. end while
12. if \( u_i^* \geq \text{sum}(u_i)/N \)
13. \( [t_i, u_i] = [t_i^*, u_i^*] \)
14. end if
15. Update reputation \( T(i) \) from formula (27)
16. Calculate \( c(i) \) and \( s(i) \) according to formulas (22) and (23); sort \( s(i) \) in descending order and store it in \( A(i) \)
17. if \( B = 0 \)
18. \( W \leftarrow A(i), B = B - c(i) \)
19. end if
20. Output: \( W \)

\[
T_i^{k+1} = \left( \frac{P}{P + G} + \frac{P_{ci}}{\sum_{j=1}^{N} P_{cj}} \right) T_i^k \quad (27)
\]

Algorithm

This article proposes a cooperative spectrum sensing algorithm based on reputation mechanism. First, the optimal sensing time and optimal utility of each SU are solved. If the optimal utility of the SU is greater than the average utility, then it participates in the spectrum sensing task. Then the SU base station updates the reputation of each SU and sorts the selection function in descending order to select SUs from large to small with the constraint that the budget is positive. The specific processes are shown in Algorithm 1.

Performance evaluation

To evaluate the performance of the algorithm proposed in this article, we set the coordinate of the SU base station as (0,0) and 100 SUs are distributed in a circular area with a radius of 100 meters randomly. The center of the circle is SU base station. The remaining energy of SUs is random from 20% to 100%. We set sampling frequency \( f_s = 20MHz, \alpha = 2.5, \beta = 2 \), false alarm probability \( P_f = 0.05, P(u_0) = P(u_1) = \frac{1}{2} \) and the budget of SU base station \( B = 250 \). The channel propagation model of this article is large-scale fading and the coefficient is 3.

Figure 4 simulates the convergence evolution of the utility of four random SUs. It is clearly that the SU utility can realize stability after about four iterations. From the convergence it is obvious that Nash equilibrium exists. The Nash equilibrium is not necessarily the optimal utility of each SU, but a globally stable state of all SUs. Meanwhile, the corresponding sensing time is the optimal sensing time for each SU. When the strategies of other players remain unchanged, any player in the game cannot obtain higher utility by changing its own strategy.

Figure 5 shows the performance comparison of the number of SUs and their utilities when the budget varies from 200 to 500. It is observed that when the
number of SUs is constant, a higher budget makes the higher utility. The reason is that when the budget is higher, the reward of each SU also increases. Since the cost of SU has not changed, the utility increases. When the budget remains unchanged, more SUs results in the decrease of the average utility. The reason is that when the budget is assigned to more SUs, the reward available to each SU is reduced. As a result, the utility decreases. Compared with literature, the SUs in this article can obtain higher utility. The sensing cost of SU in literature may be higher, so the utility is lower.

Figure 6 simulates the performance impacts of the budget on detection probability. It is clearly that the detection probability of the SU increases with the growth of the budget which is better than literature. The reason is that when the budget grows, the SU can get higher reward. As a result, the utility will increase and more SUs will be willing to take part in spectrum sensing. SUs will increase their sensing time so as to increase the probability of being selected in the process of gaming. Because of this reason, the detection probability will also increase. Literature is failed to consider SU’s remaining energy, so the difference in sensing time among SUs is slightly and the detection probability of literature is lower.

Figure 7 simulates the utility of a SU when the remaining energy changes from 20% to 100%. From the figure it can be seen that the greater the remaining energy of the SU, the larger the utility. The reason is that when the remaining energy of the SU is greater, the lower its spectrum sensing cost. Yet the reward of the SU is only related to the budget of the SU base station and the detection probability of the SU and has nothing to do with its remaining energy, so its utility is also greater. When the remaining energy is larger than 70%, the utility tends to be stable. This is because the remaining energy in the utility function of this article is a logarithmic function. It can be seen from the property of the logarithmic function that when the independent variable is relatively large, the function value becomes stable. In that literature doesn’t take the impact of the remaining energy of the SU on utility into consideration, the utility of the algorithm in literature is lower than that in this article.

Figure 8 simulates the influence of reputation on detection probability. It is clearly that when the
number of SU is certain, less the number of malicious users brings higher detection probability. In the process of increasing the number of malicious users from 0 to 15, the detection probability has decreased, but it can still be maintained at a high level. When the number of SUs is 100, the detection probability with no malicious user is about 0.92, and that of 15 malicious users is about 0.86. When the number of malicious users is 5, the detection probability of literature\textsuperscript{21} is significantly lower than that of this article. This is because literature\textsuperscript{21} does not consider the existence of malicious user attacks and there is no reasonable and feasible SU selection mechanism. Proposed algorithm in this article can effectively identify malicious users and reduce the probability of malicious users being selected to participate in spectrum sensing, so as to increase the accuracy and security of spectrum sensing and resist SSDF attacks.

Figures 9 and 10 simulate the influence of different values of coefficients $\alpha$ and $\beta$ on the utility respectively. It can be seen that no matter what value $\alpha$ or $\beta$ takes, the utility of the algorithm in this article is higher than that in literature\textsuperscript{21}. When $\beta$ is fixed, the larger the value of $\alpha$, the greater the utility. This is because when the value of $\alpha$ is larger, the reward of the SU is larger. While the cost is constant, so the utility is larger. When $\alpha$ is fixed, the utility of SU will hardly change with the change of $\beta$, and the larger $\alpha$ is, the greater the utility is. This is because when $\beta$ grows, it means that the cost of SU participating in spectrum sensing increased, so the utility is relatively smaller. When the utility is less than the threshold, the SU will not take part in the task. Without considering the influences of coefficients on utility in literature\textsuperscript{21}, SU’s utility is lower than ours.

### Conclusion

We have introduced a secure cooperative spectrum sensing algorithm based on reputation mechanism with blockchain technology of smart contract and digital signature. With comprehensive consideration of channel bit error, detection probability, the budget of SU base station and SU remaining energy, we establish the utility function of SU, proving that a Nash equilibrium is existed in the game between SUs and solving the optimal spectrum sensing time of each SU. Then the SU base station selects registered SUs by calculating and updating the reputation of each SU. Finally, performance analyses show that our algorithm increases accuracy and security of spectrum sensing which effectively helps resist SSDF attacks.

### Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: this work was supported by National Natural Science Foundation of China (Grant No. 61971239, 61631020).
References

1. Eappen G and Shankar T. A survey on soft computing techniques for spectrum sensing in a cognitive radio network. *SN Comput Sci* 2020; 1(6): 1–36.
2. Rapetswa K and Cheng L. Convergence of mobile broadband and broadcast services: a cognitive radio sensing and sharing perspective. *Intell converg Netw* 2020; 1(1): 99–114.
3. Hu F, Chen B and Zhu K. Full spectrum sharing in cognitive radio networks toward 5G: a survey. *IEEE Access* 2018; 6: 15754–15776.
4. Fu X, Wang H and Shi PC. A survey of blockchain consensus algorithms: mechanism, design and applications. *Sci Chin Inform Sci* 2020; 64(2): 121101.
5. Khasawneh M, Azab A and Agarwal A. Towards securing routing based on nodes behavior during spectrum sensing in cognitive radio networks. *IEEE Access* 2020; 8: 171512–171527.
6. Karimi M, Sadough SMS and Torabi M. Improved joint spectrum sensing and power allocation for cognitive radio networks using probabilistic spectrum access. *IEEE Syst J* 2019; 13(4): 3716–3723.
7. Hu M and Zhu Q. Secondary user utility optimization algorithm on cooperative spectrum sensing. In: *Proceedings of the IEEE 5th international conference on computer and communications (ICCC)*, Chengdu, China, 6–9 December 2019, pp.463–467. New York: IEEE.
8. Kotobi K, ainwaring PB and Bilen SG. Puzzle-based auction mechanism for spectrum sharing in cognitive radio networks. In: *Proceedings of the IEEE 12th international conference on wireless and mobile computing, networking and communications (WiMob)*, New York, 17–19 October 2016, pp.1–6. New York: IEEE.
9. Zhu X, An J, Yang MS, et al. A fair incentive mechanism for crowdsourcing in crowd sensing. *IEEE Intern Things J* 2016; 3(6): 1364–1372.
10. Liu JQ and Gao M. Incentive mechanism of crowdsensing based on loss aversion. *J South Chin Univ Technol Nat Sci Ed* 2019; 47(8): 96–104.
11. Hewa T, Ylianttila M and Liyanage M. Survey on blockchain based smart contracts: applications, opportunities and challenges. *J Netw Comput Appl* 2021; 177: 102857.
12. Han X, Yuan Y and Wang FY. Security problems on blockchain: the state of the art and future trends. *Act Automat Sin* 2019; 45(1): 206–225.
13. He YH, Li MR, Li H, et al. A blockchain based incentive mechanism for crowdsensing applications. *J Comput Develop* 2019; 56(3): 544–554.
14. Sun J and Xiong G. Credit payment for radio resources transactions based on consortium blockchain in SCMA mMTC. *Act Electron Sin* 2019; 47(8): 1677–1684.
15. Cao B, Li Y, Zhang L, et al. When internet of things meets blockchain: challenges in distributed consensus. *IEEE Netw* 2019; 33(6): 133–139.
16. Bayhan S, Zubow A and Wolisz A. Spass: spectrum sensing as a service via smart contracts. In: *Proceedings of the IEEE international symposium on dynamic spectrum access networks (DySPAN)*, Seoul, South Korea, 22–25 October 2018, pp.1–10. New York: IEEE.
17. Chen C, Wu JJ, Lin H, et al. A secure and efficient blockchain-based data trading approach for internet of vehicles. *IEEE Trans Veh Technol* 2019; 68(9): 9110–9121.
18. Kotobi K and Bilen SG. Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Veh Technol Mag* 2018; 13(1): 32–39.
19. Liang YC, Zeng YH, Peh ECY, et al. Sensing-throughput tradeoff for cognitive radio networks. *IEEE Trans Wirel Commun* 2008; 7(4): 1326–1337.
20. Zhou P, Yuan W, Liu W, et al. Joint power and rate control in cognitive radio networks: a game-theoretical approach. In: *Proceedings of the IEEE international conference on communications*, Beijing, China, 19–23 May 2008, pp.3296–3301. New York: IEEE.
21. Yang DJ, Xue GL, Fang X, et al. Incentive mechanisms for crowdsensing: crowdsourcing with smartphones. *IEEE ACM Trans Netw* 2016; 24(3): 1732–1744.