Article

Blockchain based Licensed Spectrum Fair Distribution Method Towards 6G-envisioned Communications

Mengjiang Liu , Qianhong Wu , Dawei Li * , Yiming Hei

Posted Date: 18 July 2023

doi: 10.20944/preprints202307.1224.v1

Keywords: 6G; Licensed spectrum distribution; Blockchain; Fairness

Article

Blockchain Based Licensed Spectrum Fair Distribution Method Towards 6G-Envisioned Communications

Mengjiang Liu, Qianhong Wu, Yiming Hei and Dawei Li *

School of Cyber Science and Technology, Beihang University, Beijing 100191, China; 343769896@qq.com
* Correspondence: lidawei@buaa.edu.cn;

Featured Application: This paper provides a fair, secure and distributed solution for the licensed spectrum distribution towards 6G.

Abstract: Spectrum distribution is a classical licensed spectrum accessing method in mobile communication networks. The licensed idle spectrum resources are authorized and distributed from spectrum owners to mobile users. However, the exponential growth of user capacity brings excessive load pressure on the traditional centralized network architecture. As lack of sufficient supervision and penalty measures, dishonest behaviors of spectrum owners and spectrum users will lead to the unfair status in the distribution process. As a result, the honest participants' interest will be harmed. As an important supporting infrastructure of Internet of things technology, 6G cannot completely follow the existing spectrum distribution method. Towards 6G network spectrum distribution, an blockchain based licensed spectrum fair distribution method is proposed. A lightweight consensus mechanism named as proof of trust (PoT) is applied to reduce computational power consumption and consensus time overhead. We deploy the method on the Ethereum test chain, theoretical analysis and experimental results demonstrate the fairness, effectiveness and security of the method.

Keywords: 6G; licensed spectrum distribution; blockchain; fairness

1. Introduction

The contradiction between the limited spectrum resources and the increasing bandwidth demand facilitates the evolution of the next generation of mobile communication paradigm. While 5G is being put into widespread commercial use, researches on 6G have been carried out. As we all know, licensed spectrum resources account for a considerable proportion of mobile communication service. Licensed spectrum access (LSA) can guarantee the licensed users' quality of service (QoS) at a high level. Different from 4G and 5G licensed spectrum distribution, 6G licensed spectrum distribution faces more challenges, including more connections, more decentralized locations and more security risks. The striking two distinguishing features from 6G to 5G are the introduction of terahertz band [1] and Space-Ground Integrated Network (SGIN) architecture [2]. Although terahertz communication technology can significantly improve data transmission rates, it also brings greater path transmission damage and smaller cellular coverage. That is to say more micro base stations are needed to realize ubiquitous and wide-area wireless communication coverage. The wider spatial distribution is exactly one of the important characteristics of SGIN. Hence, it is inevitable for Mobile Network Operators (MNOs) to change their current centralized business model to a more flexible and decentralized one. This irreversible evolution is driven by the emerging technologies, such as network virtualization, dynamic spectrum sharing, blockchain and so on.

Usually, in 4G and 5G mobile networks, MNOs distribute licensed spectrum resources according to user's service protocols agreed in advance. Licensed user's periodic demand will be satisfied in a certain coverage region according to current geographic location. These service protocols are regulated through binding Service Level Agreements (SLAs). Therefore, the present LSA spectrum access framework is called the distribution on demand model. Under this model, MNOs distribute the spectrum resources to different Primary Users (PUs) or Primary Base Station (PBS) according to their demand. Some dishonest users would exaggerate their spectrum demand or violate the spectrum using regulations, obtaining extra interest. The common misconducts include transmitting with a bigger power than permitted, using a different carrier frequency than allocated, and using spectrum for more time than permitted [3]. However, there lacks of effective supervision and punishment measures for the violations. As a result, the dishonest users can obtain extra illegal interest compared to the honest users. Obviously, this is unfair for the honest users. On the other hand, the existing research results usually assume that operators and MNOs are honest participants in the spectrum distribution process. This means that users believe the obtained bandwidth resources are the same as the nominal value. Nevertheless, MNOs are actually rational participants, the provided services may be discounted in order to obtain more benefits. For occasional and negligible service downgrades, users may not perceive without professional detection tools' help. But if it is the other way around, the MNO will be complained about, or even the users will switch to another telecom service provider. What's more, for the above two kinds of bad behaviors of users and MNOs, although the detection means have been rather available, but the supervision and audit means are still not rich.

To sum up the application status and related research results on 5G licensed spectrum distribution, the shortcomings of the present distribution model are mainly reflected in the following three aspects:

(1) **Unfairness between honest and dishonest users**. For some dishonest PBS and PUs, violations of spectrum access regulations would not bring serious consequences, but acquire extra incomings. These violations may hurt honest users' LSA authorities, leading to the unfairness in the spectrum distribution process.

(2) **Lack of supervision and audit mechanism**. It is difficult for users to defend their rights when the spectrum accessing service provided by MNOs is degraded. To guarantee the fairness between MNOs and spectrum users, there is an urgent need to introduce a transparent supervision and auditing mechanism to help users defend their rights.

(3) **Existing incentives are inefficient for the operators**. Under the present LSA mechanism, users belonging to a specific operator can only passively accept the LSA services provided by the MNOs. And MNOs obtain revenue from the upper tier operators. For them, there is no incentive to provide better service to users. For the PBS and PUs, misbehaviors in spectrum usage would not lead to disadvantage in subsequent spectrum access. Thus for the users there lacks the incentive to maintain good credit.

PBS and PUs play key roles in future 6G ultra-dense mobile networks, sufficient spectrum resources are of vital importance for them to serve for the subordinate user nodes. The present licensed spectrum distribution faces the challenges of unfair status and lacking of supervision and audit mechanism. Therefore, towards 6G-envisioned communications, how to effectively and fairly distribute the licensed spectrum from telecom operators to PBS and PUs is a problem that needs to be solved in the future. Moreover, to protect honest users' interest and encourage MNOs to provide better LSA services, a supervision and auditing mechanism is in urgent need. To summarize, a more fair licensed spectrum distribution or primary-level allocation method is the scientific question we are interested in.

Since Nakamoto proposed Bitcoin [4] in 2008, the concept of blockchain has attracted worldwide attention. As an open decentralized ledger system, blockchain effectively combines cryptography and distributed consensus mechanisms to ensure data transparency and tamper resistance. Moreover, blockchain technology is also widely applied to many fields such as Internet of Things (IoT) [5,6], secure storage [7,8] and supply chain management [9,10]. In recent years, researchers in academia and industry are beginning to explore the use of blockchain technology for spectrum allocation [11–14]. Utilizing the unique characteristics of blockchain and combining the 6G application scenarios, we propose a Blockchain based spEctrum primAry-level diStribution meThod

(BEAST), which can realize fair and secure primary-level spectrum distribution. To the best of our knowledge, our achievement is one of the first works aiming at 6G licensed primary-level spectrum fair distribution towards multiple MNOs scenarios. The main contributions of the paper are listed as follows.

(1) We propose a blockchain based spectrum resources distribution method, that is BEAST to apply for 6G LSA problem. By constructing proof-of-trust consensus module, the method can be used to protect the honest participants interest and penalize the dishonest participants, realizing fair spectrum distribution from MNO to PUs and PBS.

(2) By constructing PoT based LSA regulation compliance framework, the behaviors of spectrum users are assessed. The proposed framework can encourage the PUs and PBS to behave as honest users. What's more, for the MNOs service degradation risk, a more efficient incentive mechanism combining economic incentive and credit incentive is proposed. The proposed incentive mechanism can surveil and audit MNOs service level.

(3) To evaluate the effectiveness and performance of BEAST, we deploy it on Ethereum test blockchain, both simulation results and theoretical analysis show that the proposed method has good performance on fairness and security.

The rest of the paper is organized as follows, Section 2 introduces the related work to this paper. Section 3 describes the system composition and working process of BEAST. In Section 4, the trust value construction process is given, then the PoT procedure and incentive mechanism are described. we construct proof-of-trust based regulation compliance framework to guarantee the fairness in spectrum distribution. We present theoretical analysis and numerical results for the proposed algorithms in Section 5. We summarize the whole paper in Section 6.

2. Related Work

2.1. Spectrum distribution

Spectrum distribution is a main wireless channel access mechanism, where bandwidth is shared from MNOs to PUs and PBS. This mechanism is also called the primary-level spectrum distribution. In the literature [15], a novel LSA spectrum distribution algorithm is proposed, which can penalize users violating the LSA spectrum using rules by introducing a penalty mechanism. At the same time it provides extra spectrum as incentive to the users complying the regulations. Li proposes a spectrum distribution algorithm based on the idea of proportional fairness algorithm, which uses dynamic calculation of the user distribution weight values and the interference value of the current available spectrum resources. Through the dynamic adjustment of the device allocation weight value during the distribution process, a more fair spectrum distribution is achieved [16].

2.2. Spectrum using behavior detection

Detection on abnormal usage of spectrum is the premise for spectrum management. For 6G spectrum distribution, spectrum usage behavior detection is the key component to build the trust value assessment mechanism and to further realize fair spectrum distribution. Liu et al propose an algorithm for detecting abnormal behaviors based on electromagnetic data mining. The method is of good accuracy and real-time performance [17]. In the literature [18], blockchain technology and machine learning are applied to detect malicious users in the IoT network. The proposed method can store the data including spectrum access moment, occupied frequency, and transmitting power, and separate the normal users from malicious ones by machine learning.

2.3. Auditing mechanism based on blockchain

Blockchain can be regarded as a time-stamped transactions recording system, which can record all transactions that have occurred on the blockchain. The transactions recorded on the blockchain are open, transparent, decentralized and hard to tamper with. To better evaluate the spectrum accessing service provided by the MNOs, it is important to supervise and audit the MNOs behaviors. Wang et al propose a novel auditing mechanism supporting public auditing on shared data stored in

doi:10.20944/preprints202307.1224.v1

the cloud. To improve the efficiency of auditing multiple tasks, the mechanism is further extended to support batch auditing [19]. Shang et al design an identity-based dynamic data auditing scheme that is capable of performing dynamic auditing for big data storage service. To guarantee the correctness of the data update each time, a data structure namely Merkle hash tree is used. The scheme can authenticate block tags and support dynamic operation with integrity assurance [20]. For the illegal authorization and key disclosure risks, Hei et al design a blockchain based auditing scheme, the auditor in the scheme can detect the malicious behaviors. Two smart contracts on Ethereum are respectively adopted to trace the two misbehaviors [21].

3. BEAST System Model

A more attractive and effective mechanism for the 6G licensed spectrum distribution application scenario is proposed in this section, that is BEAST. As an emerging distributed ledger technology, blockchain and smart contract can be a quick and cost-effective alternative for fair and secure licensed spectrum distribution. In the following, we will describe the BEAST system composition and working principle.

3.1. System composition

We have implemented a blockchain-based prototype to demonstrate the feasibility of our method, the system composition is shown in Figure 1. The BEAST design principles and starting point can be summarized in the following three aspects.

(1) **Decentralization**. In traditional centralized LSA system, band manager executes the function of controlling channels accessing and providing information of channel state. The centralized solution is not suitable for the large scale of 6G network and widely distributed network architecture. Decentralized architecture can reduce the computational load on the central servers and reduces the probability of a single point of failure.

(2) **Lightweight consensus**. As proof of work (PoW) consensus mechanism costs a lot of computation overhead, and proof of stake (PoS) is weak to coin age accumulation attack. To improve the instantaneity of spectrum distribution, a lightweight consensus protocol is needed.

(3) **Auditable**. In most of the existing schemes, the participants are regarded as honest ones. Whereas, the MNOs, PBS and PUs are assumed to be rational participants according to the actual application scenarios in BEAST. PBS and PUs may violate the channel using regulations sometimes as described in Section I. In addition, MNOs may offer degraded accessing services when there are not sufficient available spectrum resources. For the above two dishonest behaviors, a surveillance and auditing mechanism is of great need.

Based on the above three aspects of demand analysis, we consider the BEAST in 6G LSA network as a blockchain-enabled spectrum resources distribution mechanism. The system composition is shown in Figure. 1. Under this framework, MNOs from different telecom operators intend to distribute the spectrum resources to the PBS and PUs, who are the spectrum consumers. They occupy the licensed channels themselves or redistribute the channels to the Second Users (SUs). The redistribution process is namely the secondary-level distribution. As shown in Figure 1, MNOs, PBS and PUs are connected by the consortium blockchain network. Compared to the public blockchain, the consortium blockchain can better fit for the 6G mobile network for its security and consensus efficiency. And only the nodes with sufficient computing power work as blockchain full nodes maintaining the global ledger, decreasing the maintenance cost. The rest of the nodes work as light nodes, they can connect to and access the consortium blockchain through the full node. Compared to traditional centralized LSA system, smart contract on the consortium blockchain takes over the role of band manager to control channels accessing and provide channel state information in BEAST.

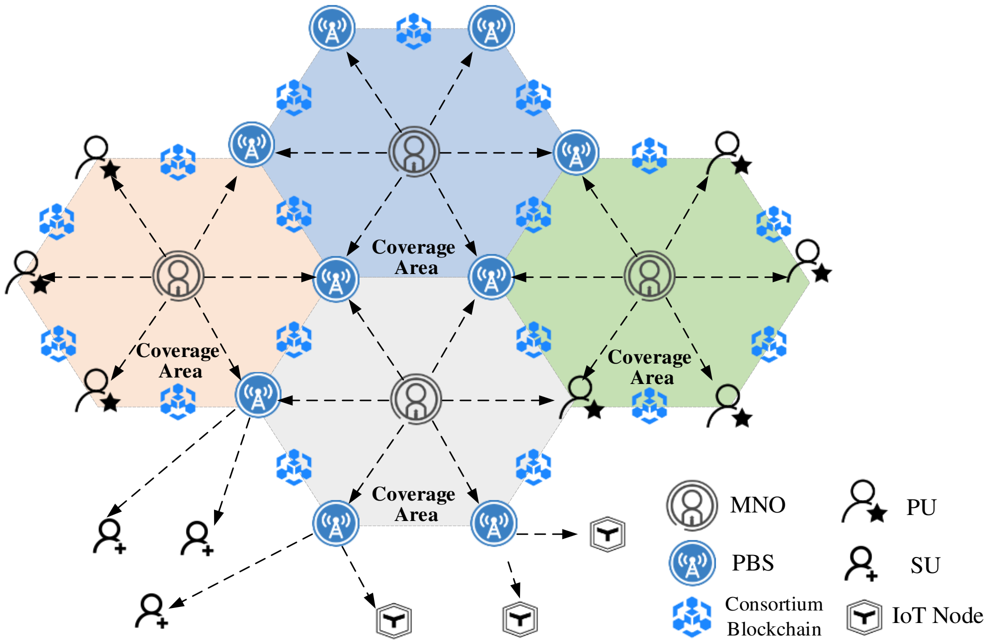


Figure 1. BEAST System Model.

3.2. System process

At first, in order to better understand the working process, we make a variant definition table as shown in Table 1.

Table 1. Parameter Used in the System Process.

Parameter	Description	Parameter	Description
MNO$_{add}$	MNO address	R_{add}	Spectrum receiver address
BW	Distributed bandwidth	UR	Spectrum using regulations
TR_i	Trust value	SR_A	Available resources set
SR_D	Spectrum demands set	t_d	Arrival timestamp
TX_{dis_t}	Spectrum distribution transaction	TV	Trust value
Pr$_i$	Priority index	Tr_{th}	Trust value threshold
n_{miner}	Registered miners	$Count_{reward}$	Blocks generated within the reward cycle
E_{block_min}	Expected minimum number of generated blocks	$C_{duration}$	Competition cycle

The interactions among MNOs, PBS and PUs can be described as “transactions” that are recorded by the blockchain nodes in networks. The nodes with strong computing power are responsible to collect spectrum distribution records from the MNOs. The strong nodes are also responsible to generate and publish new blocks. Meanwhile, the consensus process is reached among these strong nodes. The nodes without sufficient computational power can check transactions on the blockchain, but they have no right to participant in the consensus process.

A general expression of a spectrum distribution transaction can be denoted as $SD_{tx}:\{MNO_{add}\,||\,BW\,||\,R_{add}\,||\,UR\}$. Where MNO$_{add}$ and R_{add} respectively represents MNO address and spectrum receiver address, BW represents distributed bandwidth. UR is the using regulations about spectrum access, such as power control, occupation span and transmitting frequency. The main steps involved in a spectrum distribution workflow includes the following six steps. The algorithm flow of BEAST is also given in the Figure 2.

Step 1. System initialization. The PBS and PUs with spectrum access demand in a certain coverage area become legitimate entities after registering on the consortium blockchain. A pair of keys including public key *PK* and private key *SK* are sent to them, together with an initial trust value TR_i. The PBS and PUs generate several wallet accounts with *PK* to conduct transaction with others.

Step 2. Uploading demand and available spectrum resources. The available spectrum resources owned by *m* MNOs in a certain service area $|SA|$ form a set $SR_A = \{S_1,...,S_m\}, S_i \ge 0,\ 1 \le i \le m$. In $|SA|$ *n* PBS and PUs spectrum accessing demands form another set $SR_D = \{P_1,...,P_n\}, P_i \ge 0,\ 1 \le i \le n$. Both two sets are uploaded to the blockchain. The sending messages are packed as transactions respectively, which can trigger the spectrum distribution smart contracts. In this step, the MNOs needs to pay a deposit proportional to its claimed available spectrum resources to prevent MNOs from claiming idle spectrum resources arbitrarily.

Step 3. Executing spectrum distribution smart contract. Upon receiving the message, smart contract completes the distribution process according to the supply and demand as well as the trust value of each PBS and PU. During this process, we first define an timestamp array $t_d = \{t_{d1}, t_{d2}, ..., t_{dn}\}$ to represent the successively sort of arrival moment of users spectrum demand. The corresponding trust value of each user is $TV = \{TV_1, TV_2, ..., TV_n\}$. As described earlier, to encourage regulated use of the spectrum and realize fair distribution, t_d and *TV* are combined to decide the distribution order of priority. The priority index of the user is calculated as follows.

$$\Pr_i = \frac{1}{1+\ln(t_{di}+1)} \bullet \frac{\omega}{1+e^{-TV_i}} \tag{1}$$

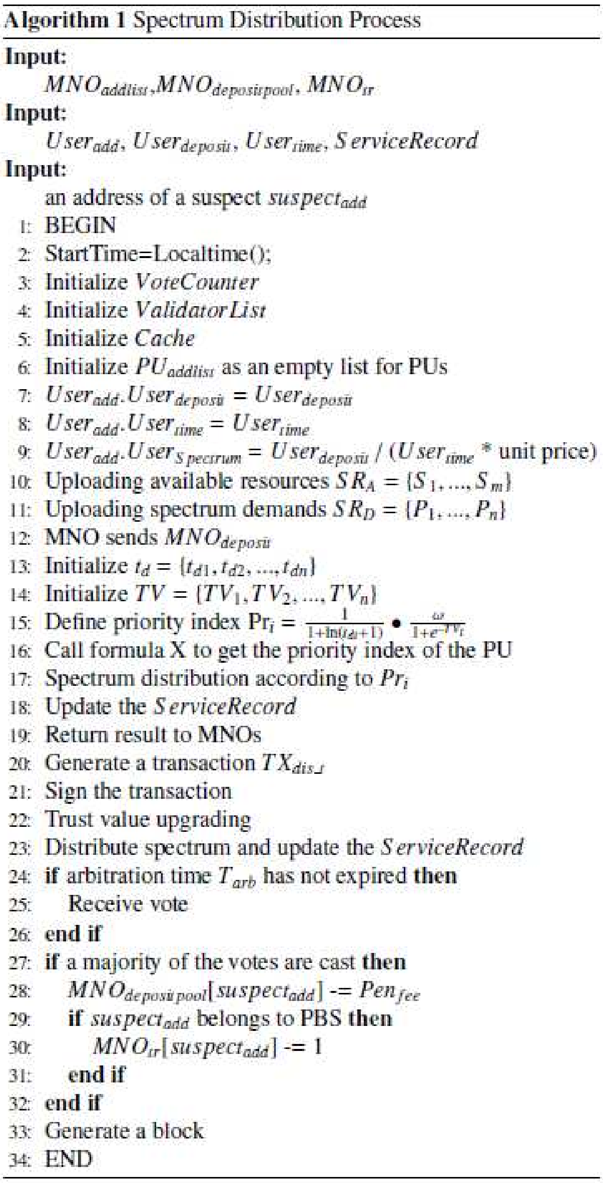
where ω is the weight index to adjust the influence of trust value on priority index. ω can be adjusted from 0 to 1.

Step 4. Generating a transaction. Once completing spectrum distribution tasks, smart contract returns the distribution results to MNOs. Then a transaction TX_{dis_t} is generated within a certain time. Meanwhile, TX_{dis_t} is signed with *PK*.

Step 5. Signing and encryption. MNO signs the authorization information for channel access with the symmetric encryption algorithm and asymmetric encryption algorithm. The signing process is done locally by the MNO, and then uploads the signature result to the blockchain.

We define *E* and *D* are respectively the encryption and decryption process of the symmetric encryption algorithm, and *K* is the symmetric encryption key. We define *Enc* and *Dec* are respectively the encryption and decryption process of the asymmetric encryption algorithm, and *K* is the symmetric encryption key. (PK_{MNO}, SK_{MNO}) and (PK_{PUi}, SK_{PUi}) are respectively the public and secret key pairs. The authorization information is denoted as M_A. MNO first uploads $(E_K(M_A), Enc_{PK_{PUi}}(K), sig)$ to the blockchain, where $sig = Sig_{SK_{MNO}}(H(E_K(M_A) \| Enc_{PK_{PUi}}(K)))$. After PU obtains the message on the blockchain, he first verifies the identity of MNO, $VerifySig_{PK_{MNO}}(sig) \overset{?}{=} H(E_K(M_A) \| Enc_{PK_{PUi}}(K))$. If the verification is passed, then he computes $K = Dec_{SK_{PUi}}(Enc_{PUi}(K))$, and computes $M_A = D_K(E_K(M_A))$.

Step 6. PoT consensus process. In BEAST, we propose a lightweight consensus mechanism named Proof of Trust (PoT) based on the user's trust value. The trust value is accumulated through the collected transactions. When strong nodes collects transactions, they also broadcast the new generating block to the network for consensus. After consensus procedure, the block is recorded on the global ledger. And the trust value of the spectrum users are updated according to their regulation compliance performance during the spectrum occupation period. The detail designs and performance evaluation of PoT will be discussed in section 4.



```
Algorithm 1 Spectrum Distribution Process
Input:
    $MNO_{addlist}$, $MNO_{depositpool}$, $MNO_{tr}$
Input:
    $User_{add}$, $User_{deposit}$, $User_{time}$, $ServiceRecord$
Input:
    an address of a suspect $suspect_{add}$
BEGIN
StartTime=Localtime();
Initialize $VoteCounter$
Initialize $ValidatorList$
Initialize $Cache$
Initialize $PU_{addlist}$ as an empty list for PUs
$User_{add}.User_{deposit} = User_{deposit}$
$User_{add}.User_{time} = User_{time}$
$User_{add}.User_{Spectrum} = User_{deposit}$ / ($User_{time}$ * unit price)
Uploading available resources $SR_A = \{S_1, ..., S_m\}$
Uploading spectrum demands $SR_D = \{P_1, ..., P_n\}$
MNO sends $MNO_{deposit}$
Initialize $t_d = \{t_{d1}, t_{d2}, ..., t_{dn}\}$
Initialize $TV = \{TV_1, TV_2, ..., TV_n\}$
Define priority index $\mathrm{Pr}_i = \frac{1}{1+\ln(t_{di}+1)} \bullet \frac{\omega}{1+e^{-TV_i}}$
Call formula X to get the priority index of the PU
Spectrum distribution according to $Pr_i$
Update the $ServiceRecord$
Return result to MNOs
Generate a transaction $TX_{dis\_t}$
Sign the transaction
Trust value upgrading
Distribute spectrum and update the $ServiceRecord$
if arbitration time $T_{arb}$ has not expired then
    Receive vote
end if
if a majority of the votes are cast then
    $MNO_{depositpool}[suspect_{add}]$ -= $Pen_{fee}$
    if $suspect_{add}$ belongs to PBS then
        $MNO_{tr}[suspect_{add}]$ -= 1
    end if
end if
Generate a block
END
```

Figure 2. Spectrum distribution algorithm.

4. Proof of Trust based Consensus Mechanism

To encourage the users to obey the spectrum regulations and to encourage the MNOs to provide better services, we have established an assessment mechanism with trust value as the core component. Furthermore, we construct a PoT consensus mechanism based on trust value.

4.1. Trust value

In BEAST, trust value indicates the spectrum user's trust degree during the spectrum occupation period. The trust value signifies participant's performance and commitment toward standardized use of the licensed spectrum resources. In most of the present work on trust based consensus mechanism, a linear or quasi-linear trust value updating model is adopted. This means that the spectrum user with high trust value will keep a high trust value in the next several spectrum distribution rounds. Moreover, the penalty measures to dishonest spectrum users are not reflected in the linear or quasi-linear model [22,23]. To make up the above weakness, we embed the penalty of misbehaviors into the trust value assessment method. The technical approaches to identify users violating behaviors in a LSA coverage area are well researched in the articles [24,25]. Compared to the above two articles focusing on misbehaviors surveillance and detection, our research focuses on the trust value establishment mechanism.

By utilizing the emerging blockchain technology, the consistency of the user's trust value at each nodes on the blockchain can be guaranteed. The trust value of each spectrum user is modeled, recorded and also agreed by other nodes on the consortium blockchain. Since available spectrum resources and users accessing demand have obvious time-varying characteristics, PUs and PBS behaviors during different occupation period may differ over time, and the corresponding trust value will change accordingly. In our design, the time cost to generate a new block is denoted as T_g, the longest period that a spectrum user occupies the channel is denoted as T_{occ}. It's obvious that $T_g \neq T_{occ}$. And if $T_{occ} < T_g$, user's trust value will be updated at the end of T_g. If $T_{occ} > T_g$, the trust value will be updated in the next new block generating period. The initial trust value of each user is set to 100+d_{token}, where d_{token} is the amount of token that is deposited in the account. The later time-varying trust value is calculated by the following formulation.

$$TV_i = (100 + d_{\text{token}}) \times \lim_{W \to \infty} \frac{\sum_{j=t-W}^{t-1} I(\text{Violating at } j)}{\sum_{j=t-W}^{t-1} I(\text{Acces}\sin\text{g at } j)} = (100 + d_{\text{token}}) \times \frac{N_{v,n}}{N_{a,n}} \tag{2}$$

where, $I(.)$ denotes the indicator function. If the argument is true, $I(.) = 1$, and vice $I(.) = 0$. $N_{v,n}$ and $N_{a,n}$ denote the number of times that the corresponding behavior is counted respectively. According to the above formulation, a high trust value correlates to good behavior and a low trust value correlates to bad behavior.

4.2. PoT procedure

The essence of blockchain consensus algorithm is to ensure the consistency of ledgers on different nodes. As Proof of Work (PoW) consensus mechanism costs a lot of computation overhead, and Proof of Stake (PoS) is weak to coin age accumulation attack. The lack of consensus certainty will lead to uncertain delay in transaction confirmation, which is not applicable for nearly real-time 6G spectrum distribution scenario. For the following two considerations, we design a PoT consensus mechanism instead of PoW and PoS. First, trust value is the representation of spectrum usage behavior, and trust value can be regarded as a reference for spectrum distribution priorities. Second, compared to other consensus mechanism, PoT is a lightweight and efficient consensus mechanism. Inspired by the research results in [26], a lightweight consensus mechanism, PoT for blockchain based spectrum distribution is proposed in this section. And the PoT consensus establishment mechanism is described. We list the basic assumptions in the following.

Assumption 1. *The consortium blockchain network for 6G spectrum distribution is partial synchronous, which is the same as Bitcoin network [4].*

Assumption 2. *We assume that the consortium blockchain network is an ideal network in terms of reliable connection and low-latency broadcast channel.*

The core idea of PoT is to ensure that each node in the consortium blockchain network maintains an agreed trust value ledger, recording the trust value of each user. Bitcoin adopts the PoW consensus protocol. The first node that solves the hard problem gets the right to publish the block, and other nodes verify the block. In the PoT consensus protocol, the node with the highest trust value generates the block and publishes it. The block is verified by the validators who are nominated by the leader. The PoT consensus process diagram is illustrated in Figure 3. Under this architecture, the consortium blockchain ledger management organization includes three roles, the leader, candidates and followers. As shown in Figure 3, the consensus process includes the following four stages.

In Stage 1, leader election and nominating validating group members are completed. If a certain candidate receives enough votes from the majority peers, then he becomes a leader legally. And he will lead the consensus procedure until the end of his term. The newly elected leader first nominates a list of transaction validators and broadcasts the list to the consortium blockchain. Each of the nominated validator's trust value should be bigger than a predefined threshold Tr_{th}.

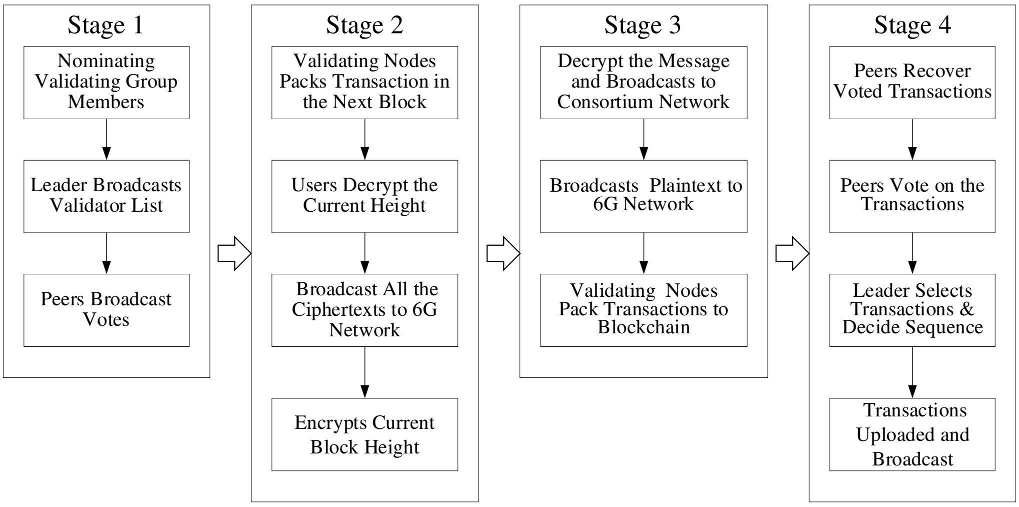

Stage 1
Nominating Validating Group Members
Leader Broadcasts Validator List
Peers Broadcast Votes
Stage 2
Validating Nodes Packs Transaction in the Next Block
Users Decrypt the Current Height
Broadcast All the Ciphertexts to 6G Network
Encrypts Current Block Height
Stage 3
Decrypt the Message and Broadcasts to Consortium Network
Broadcasts Plaintext to 6G Network
Validating Nodes Pack Transactions to Blockchain
Stage 4
Peers Recover Voted Transactions
Peers Vote on the Transactions
Leader Selects Transactions & Decide Sequence
Transactions Uploaded and Broadcast

Figure 3. PoT Consensus Process.

The main task finished in Stage 2 is to pack transactions into the next block by the validating nodes. The current height of the block h is encrypted with each validator's public key pk_v by the leader, generating ciphertext C_h. If a member on the 6G network receives the message and can decrypt C_h, then he is a legal validator.

In Stage 3, the message is first decrypted and broadcasted to the consortium blockchain. Second, the message is sent to the 6G network. Each consortium ledger management node recovers the voted transactions for each validator. Each consortium ledger management node votes on the transactions. Finally, the leader in his term will count the votes and package the verified transactions.

In Stage 4, the nodes that hold and maintain the ledger first recover the voted transactions. Then the nodes vote on the verified transactions. The leader chooses the transactions with the majority votes and determines the sequence of the transactions that have occurred. In the end, the transactions are uploaded and published on the consortium blockchain. Simultaneously, a unique token is authorized to the corresponding user to access to the 6G network.

Through the above design, the online trust value has the similar function of digital currency. And the trust value is agreed by every participant and cannot be manipulated by the third parties.

4.3. Incentive Mechanism

4.3.1. Incentive Mechanism for Spectrum Users

In the PoT mechanism, there is no need for the nodes to calculate the hash puzzles. Therefore, how to generate a new block is a crucial issue in the proposed consensus mechanism. The block can be constrained as a fixed size of transactions. The nodes can generate new blocks only if they have collected a certain transactions. In the traditional public blockchain consensus process, the miners will receive a certain quantity of transaction fees as rewards for mining the block successfully. Miners in Ethereum will get *gas* reward for collecting transactions through smart contract. Thus, for further actively participating in the PoT consensus, the leader and the validator should be paid extra trust reward. In order to encourage users to follow the spectrum usage rules, a trust value module is embedded in the proposed PoT consensus method. Apart from the rewarding *gas*, the reward also includes the trust value. This trust based incentive mechanism can effectively defend against block withholding attack and deprive of the incentives. The trust value reward is calculated by the following formulations [27].

$$T_{reward}=\frac{Count_{reward}}{\frac{C_{reward}}{C_{duration}}\bullet\frac{TV_i}{Trust_{MAX}}\bullet E_{block\_\max}}\text{, if } T_{reward}>1\text{,then } T_{reward}=1 \tag{3}$$

$$TV_i=TV_i+\frac{(1-T_{reward})(Trust_{MAX}-TV_i)}{d},d\geq 1 \tag{4}$$

Assuming the number of the registered miners on the consortium blockchain is n_{miner}. And $C_{duration}=2\bullet n_{\text{miner}}$ represents a certain number of blocks before now. $Count_{reward}$ is the number of blocks that a miner generated within the reward cycle C_{reward}. $E_{block\_\max}$ is the expected maximum number of blocks generated by a miner with the maximum trust value in a competition cycle $C_{duration}$. The rewarded trust value is set to 0 when the expected maximum number of blocks is reached. Generally, E_{block} should be set large enough, so that it will not go to the most extreme situation that a block-accounting balance between miners. Otherwise, block generation will be very difficult, and further limiting the speed of spectrum accessing. For different selection functions, the divisor d can be set different to optimize the consensus protocol.

For the block withholding attack, the corresponding malicious miner should be penalized, the penalty function of the miner n is expressed as following:

$$E_{penalty}=\frac{Count_{penalty}}{\frac{C_{penalty}}{C_{duration}}\bullet\frac{TV_i}{Trust_{MAX}}\bullet E_{block\_\min}}\text{, if } E_{block\_\min}>1\text{, then } E_{block\_\min}=1 \tag{5}$$

$$TV_i=TV_i-\frac{(1-E_{penalty})TV_i}{d},d\geq 1 \tag{6}$$

where $Count_{penalty}$ is the number of blocks that a miner generated within the penalty cycle $C_{penalty}$, and $C_{penalty}=2*C_{duration}=4*n_{\text{miner}}$. $E_{block\_\min}$ is the expected minimum number of blocks generated by a miner with the maximum trust value in a competition cycle $C_{duration}$. The aim to introduce this adaptive parameter is that if a miner can generate blocks satisfying the minimum expected number in a period of time, the miner will not be penalized, otherwise it will be deducted corresponding trust value according to the percentage of completion. $Trust_{MAX}$ is the top limit for trust value, in this way the trust value will not grow infinitely.

4.3.2. Incentive Mechanism for Spectrum Providers

In actual scenario, there are usually more than one MNOs belonging to different telecom operators in the $|SA|$. Nowadays, the spectrum users tend to embed two Subscriber Identity Module (SIM) cards in the smart devices. More and more smart devices support choosing telecom operators intelligently and accessing the idle spectrum provided by corresponding MNOs. Assuming the unit price of mobile data traffic is the same, users will certainly choose the MNOs with better service quality and better reputation. As rational participants in the 6G spectrum distribution, MNOs aim to obtain more economic income. Therefore, the MNOs also have to maintain a good trust value. We can adopt the similar trust value evaluation method as described in Section 4.1. One difference is that if the MNO is found to provide degraded services through surveillance and auditing, in addition to the loss of trust value, the MNO will also be penalized the deposit currency in the spectrum distribution smart contract.

5. Protocol Analysis

The properties on fairness and security of BEAST are analyzed in this section.

5.1. Fairness

The fairness in the 6G-envisioned BEAST includes two levels. The first level is that spectrum allocation algorithm is fair for the spectrum users and the algorithm does not favor any user operator with more resources. This absolute fairness means that all the users obtain spectrum resources on a "first-come, first-served" basis. To protect the interest of the honest users, BEAST will decrease the misbehaving user's trust value and further decrease the priorities in the later spectrum distribution rounds. By this way, the honest users spectrum access rights are first guaranteed, realizing a relative fairness. The second level means that the consensus protocol is neutral, power-separated and impartial. And it is resistant to collusions among the participants in the consensus process. To achieve the second level fairness, there are three key designs in PoT consensus. The first design is to separate the roles of transaction validation and ledger management. The transaction validating process is accomplished in the 6G network by the validators, who vote on whether a transaction can be packed into the new block. And the nodes on the consortium blockchain can only vote on the transaction lists passed by the validator group members. That is to say the nodes cannot add new transactions. In this way, the power-separation is realized. The second design is to choose the validators based on the following two priority conditions: validators with high trust value and validators not related with the current transactions. In this way, the neutrality and impartiality are guaranteed. The third design is the introduction of Shamir's secret sharing scheme, the identity information of other participants cannot be obtained by the validators. And the transaction lists are encrypted without revealing to other validators.

5.2. Security

Theoretical analysis shows that BEAST performs well at defending against selfish mining attacks, overbooking attacks and repudiation attacks.

5.2.1. Selfish Mining Attacks

In blockchain network there may exist selfish miners leveraging a special strategy in order to obtain larger revenue than what they deserve. This behavior is named as selfish mining. Selfish mining can prevent honest miners from mining blocks on the latest block and waste the efforts of honest miners [28]. The selfish miners keep carrying out mining blocks secretly until the fork from the main chain is longer than the main chain. In our proposed scheme, since new generating blocks are not based on the computing power that one node or a group of nodes possess in common, in this way, selfish mining attack can be avoided. Furthermore, a certain node can neither know the specific nodes involved in the current or the next consensus process nor learn which node will be selected as the leader.

5.2.2. Overbooking Attacks and Repudiation Attacks

Our scheme aims at ensuring that honest PBS and PUs could obtain licensed spectrum as requests, and honest MNOs could get rewards after providing qualified services. However, we notice that dishonest MNOs are motivated to perform overbooking attacks, which harms the interests of honest PBS and PUs. Specifically, an MNO has a fixed amount of spectrum resources which could serve a certain number of users; once he decided to overbook his resources, some user will not be able to obtain the requested spectrum. On the other hand, dishonest PBS and PUs may repudiate that they have received spectrum provided by a specific MNO and thus harm its reputation. Although repudiation attacks do not give direct benefits to PBS and PUs, we find it possible as PBS and PUs may be corrupted by the competitors of the target MNO.

We defend against both overbooking attacks and repudiation attacks using a one-shot solution, which combines the blockchain technology, digital signatures, and the public key encryption. Technically, we request every MNO to post the authorization information for the target PBS/PU, along with a digital signature on the blockchain. As long as the majority of the blockchain validators remain honest, attackers cannot manipulate this transcript of sending authorization information.

Meanwhile, the unforgeability of digital signatures ensures the transcript can only be generated by the specific MNO. Putting them together, this transcript becomes an evidence of providing services. Then, the MNO cannot perform overbooking attacks, as she must own enough resources to provide evidence of serving ablity. Moreover, the posted authorization information is encrypted under the PBS/PU's public key, thus only the target PBS/PU can decrypt this information and use this designated spectrum. Therefore, the dishonest PBS/PU cannot repudiate that an honest MNO has provided qualifying services.

5.3. Experiments

We deploy our algorithm on Ethereum test chain, the time cost and gas cost of the three main function in the spectrum distribution smart contract are obtained. Table 2 shows the cost for different functions of our contract. For future 6G different kinds of wireless applications, the time cost is within the acceptable range.

Table 2. Time cost and gas cost of the main function.

Function name	Time cost (ms)	Gas cost
PBSetup()	14.6	407,350
askForSpectrum()	0.25	101,322
arbitration()	0.27	45,788
Total	15.12	554,460

6. Conclusion

This paper deals with the licensed spectrum management for 6G networks. Blockchain technology is introduced to solve the unfairness flaw during the spectrum distribution process. And blockchain can also provide surveillance and auditing to the MNOs service performance. To encourage the standardized use of spectrum resources, a trust value assessment method is built. And based on this method, a lightweight consensus mechanism PoT is proposed. We have implemented a prototype of our protocol on Ethereum test chain. The theoretical analysis and experimental results demonstrate that BEAST can be a suitable scheme for 6G licensed spectrum distribution. To the best of our knowledge, our approach is the first one that provides fair and secure licensed spectrum distribution for 6G network. This provides a foundation for further enhancements in the 6G spectrum resources smart and automatic allocation. And the proposed incentive mechanism also provide the heuristic scheme for the potential multiple telecom operators application scenario, which are the subjects of future work.

Author Contributions: Conceptualization, Mengjiang.Liu and Qianhong.Wu; methodology, Mengjiang.Liu; validation, Yiming.Hei and Dawei.Li; writing—original draft preparation, Mengjiang.Liu; writing—review and editing, Mengjiang.Liu; supervision, Dawei.Li; project administration, Dawei.Li; funding acquisition, Qianhong.Wu. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Key R&D Program of China through project 2020YFB1005600, the Natural Science Foundation of China through projects U21A20467, 61932011, 61972019 and Beijing Natural Science Foundation through project M21031 and CCF-Huawei Huyanglin Foundation through project CCF-HuaweiBC2021009.

Data Availability Statement: We encourage all authors of articles published in MDPI journals to share their research data. In this section, please provide details regarding where data supporting reported results can be found, including links to publicly archived datasets analyzed or generated during the study. Where no new data were created, or where data is unavailable due to privacy or ethical restrictions, a statement is still required. Suggested Data Availability Statements are available in section "MDPI Research Data Policies" at https://www.mdpi.com/ethics.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

doi:10.20944/preprints202307.1224.v1

References

1. Taghvaee H, Pitilakis A, Tsilipakos O, et al. Multiwideband terahertz communications via tunable graphene-based metasurfaces in 6G networks: Graphene enables ultimate multiwideband THz wavefront control[J]. IEEE Vehicular Technology Magazine, 2022, 17(2): 16-25.
2. Zhang J, Tang Y, Ye T, et al. SFC-Based Service Provisioning for 6G Satellite-Ground Integrated Networks[C]//2021 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2021: 951-956.
3. Butt M M, Macaluso I, Galiotto C, et al. Fair dynamic spectrum management in licensed shared access systems[J]. IEEE Systems Journal, 2018, 13(3): 2363-2374.
4. Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system[J]. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008, 4(2).
5. Du M, Wang K, Liu Y, et al. Spacechain: A three-dimensional blockchain architecture for IoT security[J]. IEEE Wireless Communications, 2020, 27(3): 38-45.
6. Ling X, Le Y, Wang J, et al. Hash access: trustworthy grant-free IoT access enabled by blockchain radio access networks[J]. IEEE Network, 2020, 34(1): 54-61.
7. Du Y, Duan H, Zhou A, et al. Enabling secure and efficient decentralized storage auditing with blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 3038-3054.
8. Yin H, Zhang Z, He J, et al. Proof of Continuous Work for Reliable Data Storage Over Permissionless Blockchain[J]. IEEE Internet of Things Journal, 2021, 9(10): 7866-7875.
9. Zhu Q, Kouhizadeh M. Blockchain technology, supply chain information, and strategic product deletion management[J]. IEEE Engineering Management Review, 2019, 47(1): 36-44.
10. Muessigmann B, von der Gracht H, Hartmann E. Blockchain technology in logistics and supply chain management—A bibliometric literature review from 2016 to January 2020[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 988-1007.
11. Ye J, Kang X, Liang Y C, et al. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks[J]. IEEE Internet of Things Journal, 2022, 9(15): 13263-13278.
12. Zhang H, Leng S, Wu F, et al. A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT[J]. IEEE Internet of Things Journal, 2021, 9(11): 8012-8023.
13. Zhou Z, Chen X, Zhang Y, et al. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks[J]. IEEE Network, 2020, 34(1): 24-31.
14. Xiao Y, Shi S, Lou W, et al. Decentralized spectrum access system: Vision, challenges, and a blockchain solution[J]. IEEE Wireless Communications, 2022, 29(1): 220-228.
15. Butt M M, Galiotto C, Marchetti N. Fair and regulated spectrum allocation in licensed shared access networks[C]//2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2016: 1-6.
16. Li M. A Spectrum Allocation Algorithm Based on Proportional Fairness[C]//2020 6th Global Electromagnetic Compatibility Conference (GEMCCON). IEEE, 2020: 1-4.
17. Liu X, Shi R, Hee B, et al. Detection on abnormal usage of spectrum by electromagnetic data mining[C]//2019 IEEE 4th International Conference on Big Data Analytics (ICBDA). IEEE, 2019: 182-187.
18. Miah M S, Hossain M S, Armada A G. Machine Learning-based Malicious Users Detection in Blockchain-Enabled CR-IoT Network for Secured Spectrum Access[C]//2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). IEEE, 2022: 1-6.
19. Wang B, Li B, Li H. Oruta: Privacy-preserving public auditing for shared data in the cloud[J]. IEEE transactions on cloud computing, 2014, 2(1): 43-56.
20. Shang T, Zhang F, Chen X, et al. Identity-based dynamic data auditing for big data storage[J]. IEEE Transactions on Big Data, 2019, 7(6): 913-921.
21. Hei Y, Liu J, Feng H, et al. Making MA-ABE fully accountable: A blockchain-based approach for secure digital right management[J]. Computer Networks, 2021, 191: 108029.
22. Ye J, Kang X, Liang Y C, et al. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks[J]. IEEE Internet of Things Journal, 2022, 9(15): 13263-13278.
23. Li L, Liu J, Cheng L, et al. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(7): 2204-2220.
24. Yang L, Zhang Z, Zhao B Y, et al. Enforcing dynamic spectrum access with spectrum permits[C]//Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing. 2012: 195-204.
25. Jin X, Sun J, Zhang R, et al. Specguard: Spectrum misuse detection in dynamic spectrum access systems[J]. IEEE Transactions on Mobile Computing, 2018, 17(12): 2925-2938.
26. Zou J, Ye B, Qu L, et al. A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services[J]. IEEE Transactions on Services Computing, 2018, 12(3): 429-445.

27. Wang E K, Liang Z, Chen C M, et al. PoRX: A reputation incentive scheme for blockchain consensus of IIoT[J]. Future Generation Computer Systems, 2020, 102: 140-151.
28. Kang H, Chang X, Yang R, et al. Understanding selfish mining in imperfect bitcoin and ethereum networks with extended forks[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 3079-3091.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.