applied sciences

MDPI

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; liumengjiang@buaa.edu.cn (M.L.); qianhong.wu@buaa.edu.cn (Q.W.)
* 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. With a lack of sufficient supervision and penalty measures, dishonest behaviors of spectrum owners and spectrum users will lead to an 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, a blockchain-based licensed spectrum fair distribution method is proposed. A lightweight consensus mechanism named proof of trust (PoT) is applied to reduce computational power consumption and consensus time overhead. We deploy the method on the Ethereum test chain; a theoretical analysis and experimental results demonstrate the fairness, effectiveness and security of the method.

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

Citation: Liu, M.; Wu, Q.; Hei, Y.; Li, D. Blockchain-Based Licensed Spectrum Fair Distribution Method towards 6G-Envisioned Communications. *Appl. Sci.* **2023**, *13*, 9231. https://doi.org/10.3390/app13169231

Academic Editor: Christos Bouras

Received: 15 July 2023
Revised: 7 August 2023
Accepted: 11 August 2023
Published: 14 August 2023

1. Introduction

1.1. Research Background and Starting Point

The contradiction between limited spectrum resources and the increasing bandwidth demand facilitates the evolution of the next generation of a mobile communication paradigm. While 5G is being put into widespread commercial use, studies 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 a 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 emerging technologies, such as network virtualization, dynamic spectrum sharing, blockchain and so on. To address the unfair problem in the current licensed spectrum accessing mechanism, utilizing the blockchain technology is the study aim of this paper.

Usually, in 4G and 5G mobile networks, MNOs distribute licensed spectrum resources according to a user's service protocols agreed upon in advance. A 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 a 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 the spectrum for more time than permitted [3]. However, there lacks an 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, and 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 the users will even switch to another telecom service provider. Furthermore, for the above two kinds of bad behaviors of users and MNOs, although the detection means have been rather available, 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 with 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 with 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 a 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 an unfair status and lack of a 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 an 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 the Internet of Things (IoT) [5,6], secure storage [7,8] and supply chain

management [9,10]. In recent years, researchers in academia and industries are beginning to explore the use of blockchain technology for spectrum allocation [11–14].

1.2. Novelty and Contributions

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 MNO scenarios. The main contributions of the paper are listed as follows.

(1) We propose a blockchain-based spectrum resource distribution method, that is, BEAST, to apply it to a 6G LSA problem. By constructing a 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 a 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. Furthermore, for the MNO service degradation risk, a more efficient incentive mechanism combining economic incentive and credit incentive is proposed. The proposed incentive mechanism can surveil and audit an MNO service level.
(3) To evaluate the effectiveness and performance of BEAST, we deploy it on Ethereum test blockchain; both simulation results and a 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 a proof-of-trust-based regulation compliance framework to guarantee the fairness in spectrum distribution. We present a 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 with the regulations. Li M. proposes a spectrum distribution algorithm based on the idea of a proportional fairness algorithm, which uses the 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

The detection of the abnormal usage of a 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 a 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 the spectrum access moment, occupied frequency and transmitting power, and

separate the normal users from malicious ones with machine learning. A multi-attribute-based fairness-driven algorithm is proposed for the determination and interruption of SUs' services to ensure fairness among services in the network's resource utilization in [19].

2.3. Auditing Mechanism Based on Blockchain

Blockchain can be regarded as a time-stamped transaction 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 with 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 the cloud. To improve the efficiency of auditing multiple tasks, the mechanism is further extended to support batch auditing [20]. 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 a Merkle hash tree, is used. The scheme can authenticate block tags and support dynamic operation with integrity assurance [21]. 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 [22].

Table 1 summarizes the general characteristics of the existing related work. In this paper, we present a new architecture for fair and secure licensed spectrum distribution towards a future 6G network. Spectrum distribution is a common spectrum allocation technology. We first introduce the latest development status. We adopt the spectrum using behavior detection technology to discover the dishonest behaviors, which lead to the unfair flaws in the existing spectrum management. By adopting blockchain technology, a two-level fair licensed spectrum distribution model is proposed; besides fairness, the model can also provide security assurance defending against common cyber attacks.

Table 1. Characteristics summary of the existing related work.

Characteristics	Fairness	Malicious Behavior Detection	Auditability	Security and Privacy
[15]	√	×	×	×
[16]	√	×	×	×
[17]	×	√	√	×
[18]	×	√	×	√
[19]	√	×	×	√
[20]	×	×	√	√
[21]	×	×	√	×
[22]	×	×	√	√

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 a 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 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 a traditional centralized LSA system, a band manager executes the function of controlling channels accessing and providing information of the channel state. The centralized solution is not suitable for the large scale of the 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. A proof of work (PoW) consensus mechanism costs a lot of computation overhead, and proof of stake (PoS) is weak to a 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 1. 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.

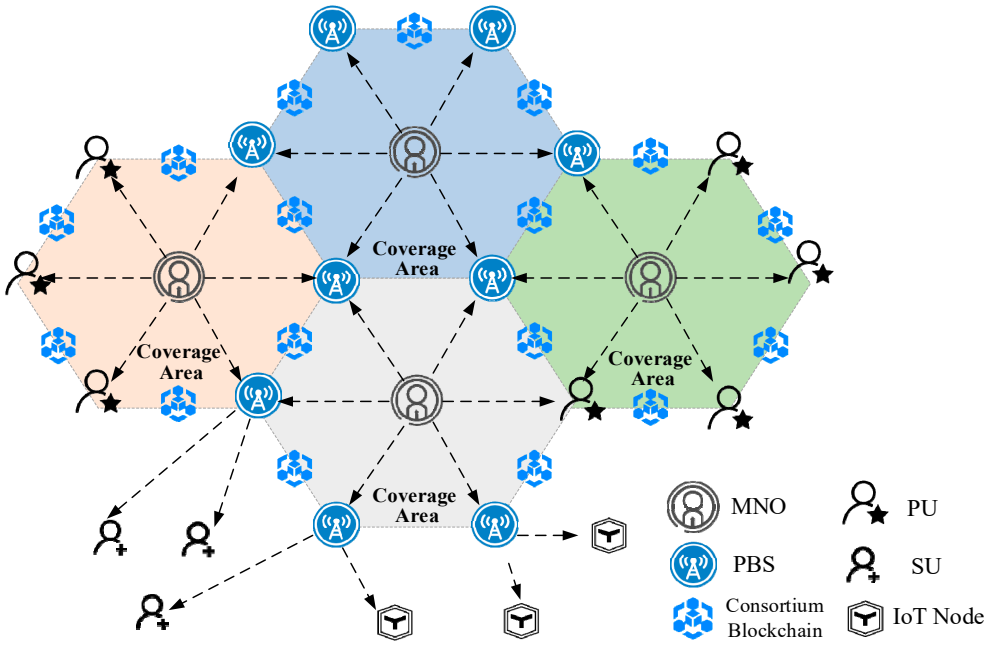

Figure 1. BEAST system model.

Based on the above three aspects of a demand analysis, we consider the BEAST in a 6G LSA network as a blockchain-enabled spectrum resource 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 using 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, and they can connect to and access the consortium blockchain through the full node. Compared to a traditional centralized LSA system, a smart contract on the consortium blockchain takes over the role of band manager to control channel accessing and provide channel state information in BEAST.

3.2. System Process

At first, in order to better understand the working process, we made a variant definition table as shown in Table 2.

Table 2. Parameters 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 with 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 participate 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, represent an MNO address and spectrum receiver address, and BW represents a distributed bandwidth. UR is using regulations about the spectrum access, such as power control, occupation span and transmitting frequency. The main steps involved in a spectrum distribution workflow include the following six steps. The algorithm flow of BEAST is also given in Algorithm 1. And to enhance clarity, a block diagram illustrating the main components and process of BEAST is shown in Figure 2.

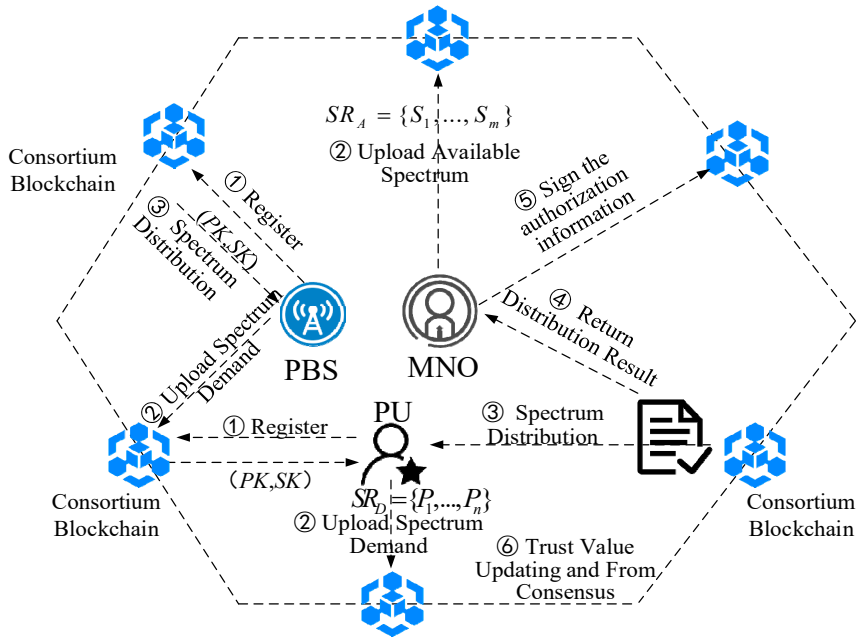

Figure 2. Block diagram of spectrum distribution algorithm process.

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 a 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, $SR_A = \{S_1, \ldots, S_m\}, S_i \geq 0,\ 1 \leq i \leq m$. In $|SA|$, n PBS and PU spectrum accessing demands form another set, $SR_D = \{P_1, \ldots, P_n\}, P_i \geq 0,\ 1 \leq i \leq n$. Both sets are uploaded to the blockchain. The sending messages are respectively packed as transactions, which can trigger the spectrum distribution smart contracts. In this step, the MNOs need to pay a deposit proportional to their claimed available spectrum resources to prevent MNOs from claiming idle spectrum resources arbitrarily.

Step 3. Executing spectrum distribution smart contract. Upon receiving the message, a 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 a timestamp array, $t_d = \{t_{d1}, t_{d2}, \ldots, t_{dn}\}$, to represent the successive sorting of the arrival moment of users' spectrum demand. The corresponding trust value of each user is $TV = \{TV_1, TV_2, \ldots, TV_n\}$. As described earlier, to encourage the 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 a user is calculated as follows.

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

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

Step 4. Generating a transaction. Once completing spectrum distribution tasks, the 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 performed locally with the MNO, and then it uploads the signature result to the blockchain.

We define E and D as, respectively, the encryption and decryption process of the symmetric encryption algorithm, and K is the symmetric encryption key. We define Enc and Dec as, 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, it first verifies the identity of MNO—$VerifySig_{PK_{MNO}}(sig) \stackrel{?}{=} H(E_K(M_A)||Enc_{PK_{PUi}}(K))$. If the verification is passed, then it 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 a user's trust value. The trust value is accumulated through the collected transactions. When strong nodes collect transactions, they also broadcast the new generating block to the network for consensus. After the consensus procedure, the block is recorded on the global ledger. And the trust value of the spectrum users is 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_{ir}
Input:
$User_{add}$, $User_{deposit}$, $User_{time}$, *ServiceRecord*
Input:
an address of suspect $suspect_{add}$
1: BEGIN
2: StartTime=Localtime();
3: Initialize *VoteCounter*
4: Initialize *ValidatorList*
5: Initialize *Cache*
6: Initialize $PU_{addlist}$ as an empty list for PUs
7: $User_{add}.User_{deposit}$= $User_{deposit}$
8: $User_{add}.User_{time}$= $User_{time}$
9: $User_{add}.User_{Spectrum}$= $User_{deposit}$/($User_{time}$* unit price)
10: Uploading available resources SR_A= {S_1,. . .,S_m}
11: Uploading spectrum demands SR_D= {P_1,. . .,P_n}
12: MNO sends $MNO_{deposit}$
13: Initialize t_d= {t_{d1},t_{d2},. . .,t_{dn}}
14: Initialize TV= {TV_1,TV_2,. . .,TV_n}
15: Define priority index $\Pr_i = \frac{1}{1+\ln(t_{di}+1)} \bullet \frac{\omega}{1+e^{-TV_i}}$
16: Call formula X to get the priority index of the PU
17: Spectrum distribution according to $\Pr_i$
18: Update the *ServiceRecord*
19: Return result to MNOs
20: Generate a transaction TX_{dis_t}
21: Sign the transaction
22: Trust value upgrading
23: Distribute spectrum and update the *ServiceRecord*
24: **if** arbitration time T_{arb} has not expired **then**
25: Receive vote
26: **end if**
27: **if** a majority of the votes are cast **then**
28: $MNO_{depositpool}$[$suspect_{add}$]-=Pen_{fee}
29: **if** $suspect_{add}$ belongs to PBS **then**
30: MNO_{tr}[$suspect_{add}$]-=1
31: **end if**
32: **end if**
33: Generate a block
34: END

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 established an assessment mechanism with the trust value as the core component. Furthermore, we constructed a PoT consensus mechanism based on the trust value.

4.1. Trust Value

In BEAST, the trust value indicates the spectrum user's trust degree during the spectrum occupation period. The trust value signifies a participant's performance and commitment toward the standardized use of the licensed spectrum resources. In most of the present work on a trust-based consensus mechanism, a linear or quasi-linear trust value updating model is adopted. This means that a spectrum user with a 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 [11,23]. To make up for the above weakness, we embed the penalty of misbehaviors

into the trust value assessment method. The technical approaches to identify users' violating behaviors in an LSA coverage area are well researched in articles [24,25]. Compared to the above two articles focusing on misbehavior surveillance and detection, our research focuses on the trust value establishment mechanism.

By utilizing the emerging blockchain technology, the consistency of a user's trust value at each node on the blockchain can be guaranteed. The trust value of each spectrum user is modeled, recorded and also agreed to with other nodes on the consortium blockchain. Since available spectrum resources and users accessing demand have obvious time-varying characteristics, PU and PBS behaviors during different occupation periods 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, and the longest period that a spectrum user occupies the channel is denoted as T_{occ}. It is obvious that $T_g \neq T_{occ}$. And if $T_{occ} < T_g$, a 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 $100 + d_{\text{token}}$, where d_{token} is the amount of the token that is deposited in the account. The later time-varying trust value is calculated with the following formulation.

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

where $I(.)$ denotes the indicator function. If the argument is true, $I(.) = 1$, and if not, $I(.) = 0$. $N_{v,n}$ 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 the blockchain consensus algorithm is to ensure the consistency of ledgers on different nodes. The proof of work (PoW) consensus mechanism costs a lot of computation overhead, and proof of stake (PoS) is weak to a coin age accumulation attack. A lack of consensus certainty will lead to an uncertain delay in transaction confirmation, which is not applicable for a nearly real-time 6G spectrum distribution scenario. For the following two considerations, we design a PoT consensus mechanism instead of PoW and PoS. First, the trust value is the representation of spectrum usage behavior, and the trust value can be regarded as a reference for spectrum distribution priorities. Second, compared to other consensus mechanisms, 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 partially synchronous, which is the same as the Bitcoin network [4].*

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

The core idea of PoT is to ensure that each node in the consortium blockchain network maintains an agreed upon trust value ledger, recording the trust value of each user. Bitcoin adopts the PoW consensus protocol. The first node that solves the hard problem obtains 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 with the validators who are nominated using the leader. A PoT consensus process diagram is illustrated in Figure 2. 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.

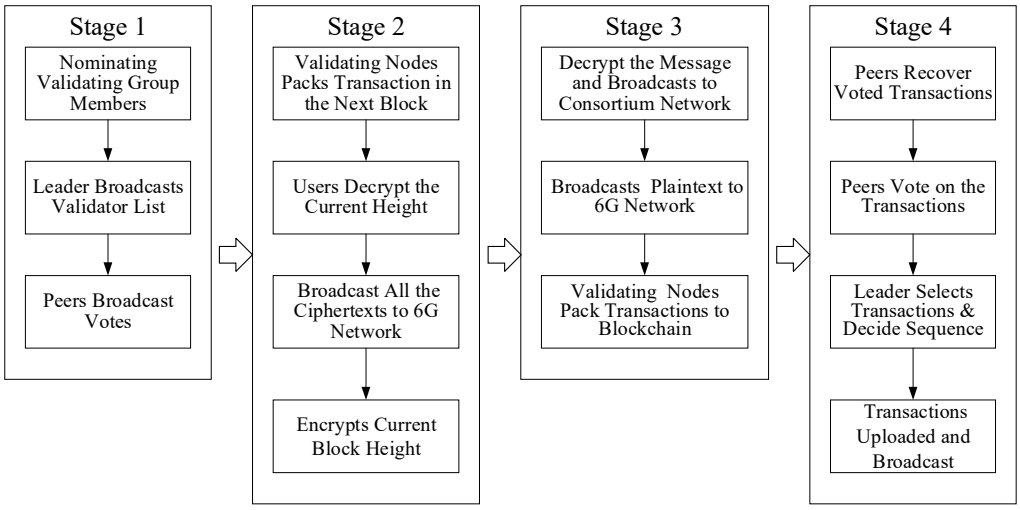

Figure 3. PoT consensus process.

In Stage 1, a leader election and nominating validating group members are completed. If a certain candidate receives enough votes from the majority peers, then they become a leader legally. And they will lead the consensus procedure until the end of their 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}.

The main task finished in Stage 2 is to pack transactions into the next block with the validating nodes. The current height of the block h is encrypted with each validator's public key, pk_v, using the leader, generating ciphertext, C_h. If a member on the 6G network receives the message and can decrypt C_h, then they are 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 their 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 of 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 upon by every participant and cannot be manipulated by 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 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 obtain a *gas* reward for collecting transactions through a smart contract. Thus, to actively participate in the PoT consensus further, the leader and the validator should be paid an 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 a block withholding attack and deprivation of the incentives. The trust value reward is calculated with the following formulations [27].

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

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

Assume that 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 the present moment. $Count_{reward}$ 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 with 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 results in a block-accounting balance between miners. Otherwise, block generation will be very difficult, and further limits the speed of spectrum accessing. For different selection functions, the divisor d can be differently set to optimize the consensus protocol.

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

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

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

where $Count_{penalty}$ is the number of blocks that a miner generated within the penalty cycle $C_{penalty}$, and $C_{penalty} = 2 \times C_{duration} = 4 \times n_{\text{miner}}$. $E_{block\_\min}$ is the expected minimum number of blocks generated with a miner with the maximum trust value in a competition cycle, $C_{duration}$. The aim of introducing 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 a corresponding trust value according to the percentage of completion. $Trust_{MAX}$ is the top limit for the trust value; in this way, the trust value will not grow infinitely.

4.3.2. Incentive Mechanism for Spectrum Providers

In an actual scenario, there is usually more than one MNO belonging to different telecom operators in the $|SA|$. Nowadays, the spectrum users tend to embed two Subscriber Identity Module (SIM) cards in smart devices. More and more smart devices support choosing telecom operators intelligently and accessing the idle spectrum provided with 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 the trust value, the MNO will also be penalized regarding the deposit currency in the spectrum distribution smart contract.

5. Protocol Analysis

The properties of 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 the 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 a misbehaving user's trust value and further decrease the priorities in the later spectrum distribution rounds. With this way, an honest user's spectrum access rights are guaranteed first, 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 the 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 with 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 with 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 a high trust value and validators not related to 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 with the validators. And the transaction lists are encrypted without revealing them to other validators.

5.2. Security

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

5.2.1. Prevention of Selfish Mining Attacks

In the 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 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, a 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. Prevention of Overbooking Attacks and Repudiation Attacks

In an ideal scenario, our aim is to establish an environment where honest PBS and PUs can seamlessly access licensed spectrum resources based on their requests. And simultaneously, honest MNOs can be duly rewarded for delivering competent services. However, the practical landscape is often marred by self-interested entities that prioritize their personal gains, potentially undermining the welfare of other stakeholders. In the ensuing discussion, we delve into two distinct but concerning attack vectors: overbooking attacks and repudiation attacks, respectively orchestrated with malicious PBS and MNOs. Subsequently, we present compelling proof demonstrating our system's resilience against these adversarial maneuvers.

Definition 1. *Ensuring Security against Overbooking Attacks.*

Assume the presence of an adversary denoted as $\mathcal{A}$, endowed with control over a set of available spectrum resources, SR_A, within a defined geographical area, SA. Concurrently, we have honest PBS and PUs that have articulated their spectrum requirements, thereby

establishing a spectrum demand set, SR_P. We declare that $\mathcal{A}$ has successfully executed an overbooking attack if, during any stage of system execution, a subset of demands, SR', extracted from SR_P, is deceitfully deemed as satisfactorily fulfilled, and significantly, the cardinality of SR' surpasses that of SR_A. We assert that a system can effectively thwart $\mathcal{A}$'s overbooking attacks if the probability of their successful execution is insubstantial and negligible.

This formal articulation encapsulates our commitment to fortify a system against overbooking attacks. By stipulating conditions that deter the illicit expansion of resource allocations with adversarial agents, we ensure the equitable distribution of spectrum resources to legitimate users, precluding any undue advantages from being exploited. Our comprehensive defense strategy effectively safeguards against overbooking attacks through a meticulous amalgamation of the following technologies: blockchain, digital signatures and public key encryption. This harmonious blend forms a potent one-shot solution that guarantees a system's resilience against the insidious overbooking menace. We will now delve into the intricate workings of this defense mechanism, expounding upon the intricate interplay of these components and elucidating how they collectively form an impregnable barrier.

The crux of our approach hinges upon a fundamental protocol that mandates each MNO to proactively publish authorization information tailored for the intended PBS or PU beneficiary. This authorization information, crucial for delineating resource access rights, is meticulously endorsed with a digital signature, which is subsequently embedded within the unalterable fabric of the blockchain. In this context, the blockchain stands as an immutable ledger, a distributed network of trust where every participant's contribution is validated with the majority. Herein lies the first line of defense. A potential attacker's capability to tamper with this transcript of authorization information is severely restricted. The steadfast integrity of the blockchain rests upon the collective honesty of the majority of its validators. Thus, the attacker's capacity to manipulate the information is negated by the robustness of this decentralized consensus. The second layer of defense materializes through the indomitable unforgeability of digital signatures. These cryptographic seals unequivocally link each authorization entry to a specific MNO, establishing an incontrovertible connection between the sender and the content. Any attempt to counterfeit or fabricate this signature, a herculean endeavor, is met with insurmountable cryptographic barriers. As such, the authenticity of the transcript is unassailable, preserving the sanctity of the authorization process.

A convergence of these elements culminates in the crystallization of the transcript as irrefutable evidence of rendered services. This transcript holds not merely a testament of authorization, but an immutable record of service provisioning, indelibly inscribed in the blockchain's annals. The MNO's accountability and service commitments are etched into the very foundation of the system. The central idea of this design lies in its proactive deterrence against overbooking attacks. The stringent prerequisites for participation preclude any malicious MNO from exploiting the system. A would-be attacker, contemplating an overbooking gambit, is compelled to confront an impregnable barrier—the imperative of possessing adequate resources to substantiate their service claims. This serves as a self-enforcing safeguard, rendering overbooking attacks an unviable and ultimately futile endeavor.

In conclusion, our multi-faceted approach, integrating blockchain technology, digital signatures and public key encryption, engenders a formidable fortress against overbooking attacks. The meticulous orchestration of these components not only thwarts potential attackers' attempts to manipulate the system but also fosters a holistic ecosystem where resource allocation remains equitable, reliable and immune to adversarial influence. This fortified defense stands resolute, poised to ensure the unimpeded and just access to spectrum resources for legitimate users.

Definition 2. *Security against repudiation attacks*.

Let us consider the presence of an adversary denoted as $\mathcal{A}$, having control over a set of PB and PUs. We declare that $\mathcal{A}$ has successfully executed a repudiation attack if it issued a repudiation against the fact that it has received an access to the demanded spectrum resources. We affirm that a system can robustly counteract $\mathcal{A}$'s repudiation attacks if the likelihood of their effective execution remains minimal and negligible.

Our security approach integrates encryption through the Public Key Infrastructure (PKI) as a foundational shield, bolstering the trustworthiness of our system. By encapsulating posted authorization details beneath an impervious layer of cryptographic secrecy, we ensure that this information remains accessible solely to its intended recipient. This one-way encryption mechanism guarantees that only the targeted PBS/PU possesses the decryption key, preserving the sanctity of the data while enabling the authorized entity to unveil its contents effortlessly. The strategic fusion of public key encryption and the immutable blockchain architecture forms an unassailable bulwark against repudiation attempts. Dishonest parties, motivated to distort the truth by disavowing the services rendered with honest MNOs, find themselves thwarted by the cryptographic constraints. Any endeavor to deny the reception of services collides with an insurmountable cryptographic barrier, as the encrypted authorization data form an indelible proof imprinted upon the blockchain. The integration of digital signatures further seals this record, rendering it impervious to manipulation or falsification.

In essence, our security framework not only assures the veracity of service transactions but also reinforces the credibility of MNO contributions. The cryptographic safeguards quell repudiation endeavors, establishing a steadfast assurance that dishonest PBS/PU entities cannot undermine the system's integrity by falsely repudiating legitimate services. This fortified protection, enshrined within the marriage of encryption and blockchain, ensures the steadfastness of service provisioning while championing the principle of accountability and transparency.

5.2.3. Censorship Resistance

BEAST is designed to provide robust censorship resistance, ensuring that both honest PBS and PUs can reliably obtain spectrum resources within a reasonable timeframe, free from the interference or obstruction of malicious participants or MNOs. This property is not only crucial for maintaining fairness but also for upholding the democratic principles of equal access to resources. To guarantee this vital aspect of BEAST, we strategically implemented and rigorously enforced a priority index mechanism. This priority index is meticulously calculated, taking into account two critical factors: the temporal arrival of the resource request and the trustworthiness assessment of the requester.

In essence, the priority index acts as an equitable determinant, ensuring that honest nodes with a higher trust value are granted a correspondingly elevated priority index. This priority index, in turn, becomes the key factor in dictating the order in which spectrum resources are allocated. By placing high-priority requests at the forefront of the allocation queue, we achieve a streamlined and efficient process that optimally serves the needs of legitimate users.

Crucially, the integrity of this priority-based approach is fortified with the immutability and transparency of the blockchain. Each and every demand for spectrum resources is meticulously documented and indelibly recorded within the blockchain's secure framework. This distributed and tamper-proof ledger ensures that every honest MNO can accurately perceive and access the spectrum demands lodged with the PBS and PU nodes. This visibility, rooted in blockchain's transparency, empowers honest MNOs to promptly recognize and respond to resource requests in accordance with their priority index.

As a synthesis of these intricately woven mechanisms, our system exhibits a robust and compelling ability to resist censorship. The amalgamation of priority indexing, trust evaluation and blockchain-backed transparency culminates in a framework where honest PBS and PUs are equipped with the means to surmount any adversarial attempts at censorship with malicious actors or MNOs. In this fashion, we are confident that our

system's architecture comprehensively safeguards the principle of censorship resistance, reinforcing the fundamental ideals of impartial access and the equitable distribution of vital spectrum resources.

Other common attacks include identity forgery, data tampering, data theft, etc. Data theft is a kind of passive attack, which mainly destroys the confidentiality of information. Data tampering is a kind of active attack, which mainly destroys the integrity and availability of information. And a forgery attack is when an attacker simulates a legitimate identity and sends false information. These attacks can be solved with blockchain technology and other mature technologies.

5.3. Experiments

We deploy our algorithm on the Ethereum test chain, and the time cost and gas cost of the three main function in the spectrum distribution smart contract are obtained. Table 3 shows the cost for different functions of our contract. For different kinds of 6G wireless applications in the future, the time cost is within the acceptable range for the users.

Table 3. 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

In this paper, we propose a blockchain-based spectrum primary-level distribution method (BEAST) to realize fair and secure spectrum distribution in a 6G network. BEAST introduces a trust-value-based PoT consensus to improve block generating efficiency. BEAST is modeled under the universal composability (UC) security framework and evaluated in the Ethereum test chain. Compared to the fair allocation scheme based on penalties in [15] and weight-value-based scheme in [16], our method achieves two-level fairness. That is, the fairness among spectrum users and the fairness in the consensus protocol. Meanwhile, compared to the others, in addition to providing privacy protection, BEAST can provide similar privacy preservation and security guarantees to a blockchain-based spectrum allocation scheme, such as Block6Tel [29], the scheme in [30] and TCPP [11]. Furthermore, due to the introduction of PoT, BEAST improves the transaction efficiency from a seconds to milliseconds grade, which is more suitable for the various near real-time applications.

6. Conclusions

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. The incentive mechanism with the credit value as the core can encourage MNO to provide better services and encourage users to use spectrum resources regularly. And based on this method, a lightweight consensus mechanism, PoT, is proposed. The PoT consensus mechanism effectively reduces the difficulty of block generation and improves the transaction efficiency. We implement a prototype of our protocol on the 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 a 6G network. This provides a foundation for further enhancements in the 6G spectrum resources' smart and automatic allocation.

Nonetheless, BEAST still has some limitations. For example, the blockchain-based decentralized spectrum sensing technology needs to be further enhanced. Then, the accuracy and rationality will be further improved. During this process, the relative technology

including deep learning and artificial intelligence would be integrated. The proposed incentive mechanism also provides a heuristic scheme for the potential multiple telecom operators application scenario, which can be the subjects of future work.

Author Contributions: Conceptualization, M.L. and Q.W.; methodology, M.L.; validation, Y.H. and D.L.; writing—original draft preparation, M.L.; writing—review and editing, M.L.; supervision, D.L.; project administration, D.L.; funding acquisition, Q.W. 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; Natural Science Foundation of China through projects U21A20467, 61932011 and 61972019; Beijing Natural Science Foundation through project M21031; CCF-Huawei Huyanglin Foundation through project CCF-HuaweiBC2021009; and the Academic Excellence Foundation of Beihang University for PhD Students (Yiming Hei).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author, upon reasonable request.

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.

References

1. Taghvaee, H.; Pitilakis, A.; Tsilipakos, O.; Tasolamprou, A.C.; Kantartzis, N.V.; Kafesaki, M.; Cabellos-Aparicio, A.; Alarcón, E.; Abadal, S. Multi-wideband terahertz communications via tunable graphene-based meta surfaces in 6G networks. *IEEE Veh. Technol. Mag.* **2022**, *17*, 16–25. [CrossRef]
2. Zhang, J.; Tang, Y.; Ye, T.; Sun, Y. SFC-based service provisioning for 6G Satellite-Ground Integrated Networks. In Proceedings of the 2021 IEEE/CIC International Conference on Communications in China (ICCC), Xiamen, China, 28–30 July 2021; pp. 951–956.
3. Butt, M.M.; Macaluso, I.; Galiotto, C.; Marchetti, N. Fair dynamic spectrum management in licensed shared access systems. *IEEE Syst. J.* **2018**, *13*, 2363–2374. [CrossRef]
4. Nakamoto, S.; Bitcoin, A. A Peer-to-Peer Electronic Cash System. Bitcoin. Volume 4. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 July 2023).
5. Du, M.; Wang, K.; Liu, Y.; Qian, K.; Sun, Y.; Xu, W.; Guo, S. Spacechain: A three-dimensional blockchain architecture for IoT security. *IEEE Wirel. Commun.* **2020**, *27*, 38–45. [CrossRef]
6. Ling, X.; Le, Y.; Wang, J.; Ding, Z. Hash access: Trustworthy grant-free IoT access enabled by blockchain radio access networks. *IEEE Netw.* **2020**, *34*, 54–61.
7. Du, Y.; Duan, H.; Zhou, A.; Wang, C.; Au, M.H.; Wang, Q. Enabling secure and efficient decentralized storage auditing with blockchain. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 3038–3054. [CrossRef]
8. Yin, H.; Zhang, Z.; He, J.; Ma, L.; Zhu, L.; Li, M.; Khoussainov, B. Proof of continuous work for reliable data storage over permissionless blockchain. *IEEE Internet Things J.* **2021**, *9*, 7866–7875. [CrossRef]
9. Zhu, Q.; Kouhizadeh, M. Blockchain technology, supply chain information, and strategic product deletion management. *IEEE Eng. Manag. Rev.* **2019**, *47*, 36–44. [CrossRef]
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. *IEEE Trans. Eng. Manag.* **2020**, *67*, 988–1007. [CrossRef]
11. Ye, J.; Kang, X.; Liang, Y.C.; Sun, S. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks. *IEEE Internet Things J.* **2022**, *9*, 13263–13278. [CrossRef]
12. Zhang, H.; Leng, S.; Wu, F.; Chai, H. A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT. *IEEE Internet Things J.* **2021**, *9*, 8012–8023. [CrossRef]
13. Zhou, Z.; Chen, X.; Zhang, Y.; Mumtaz, S. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. *IEEE Netw.* **2020**, *34*, 24–31. [CrossRef]
14. Xiao, Y.; Shi, S.; Lou, W.; Wang, C.; Li, X.; Zhang, N.; Hou, Y.T.; Reed, J.H. Decentralized spectrum access system: Vision, challenges, and a blockchain solution. *IEEE Wirel. Commun.* **2022**, *29*, 220–228. [CrossRef]
15. Butt, M.M.; Galiotto, C.; Marchetti, N. Fair and regulated spectrum allocation in licensed shared access networks. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; pp. 1–6.
16. Li, M. A Spectrum allocation algorithm based on proportional fairness. In Proceedings of the 2020 6th Global Electromagnetic Compatibility Conference (GEMCCON), Xi'an, China, 20–23 October 2020; pp. 1–4.

17. Liu, X.; Shi, R.; Hee, B.; Chen, M. Detection on abnormal usage of spectrum by electromagnetic data mining. In Proceedings of the 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), Suzhou, China, 15–18 March 2019; pp. 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. In Proceedings of the 2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Bilbao, Spain, 15–17 June 2022; pp. 1–6.
19. Khan, A.U.; Abbas, G.; Abbas, Z.H.; Tanveer, M.; Ullah, S.; Naushad, A. HBLP: A hybrid underlay-interweave mode CRN for the Future 5G-based internet of things. *IEEE Access* **2020**, *8*, 63403–63420. [CrossRef]
20. Wang, B.; Li, B.; Li, H. Oruta: Privacy-preserving public auditing for shared data in the cloud. *IEEE Trans. Cloud Comput.* **2014**, *2*, 43–56. [CrossRef]
21. Shang, T.; Zhang, F.; Chen, X.; Liu, J.; Lu, X. Identity-based dynamic data auditing for big data storage. *IEEE Trans. Big Data* **2019**, *7*, 913–921. [CrossRef]
22. Hei, Y.; Liu, J.; Feng, H.; Li, D.; Liu, Y.; Wu, Q. Making MA-ABE fully accountable: A blockchain-based approach for secure digital right management. *Comput. Netw.* **2021**, *191*, 108029. [CrossRef]
23. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
24. Yang, L.; Zhang, Z.; Zhao, B.Y.; Zheng, H. Enforcing dynamic spectrum access with spectrum permits. In Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing, Bellevue, WA, USA, 16–19 October 2012; pp. 195–204.
25. Jin, X.; Sun, J.; Zhang, R.; Zhang, Y.; Zhang, C. Specguard: Spectrum misuse detection in dynamic spectrum access systems. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2925–2938. [CrossRef]
26. Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. *IEEE Trans. Serv. Comput.* **2018**, *12*, 429–445. [CrossRef]
27. Wang, E.K.; Liang, Z.; Chen, C.M.; Kumari, S.; Khurram Khan, M. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Gener. Comput. Syst.* **2020**, *102*, 140–151. [CrossRef]
28. Kang, H.; Chang, X.; Yang, R.; Misic, J.; Misic, V.B. Understanding selfish mining in imperfect bitcoin and ethereum networks with extended forks. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 3079–3091. [CrossRef]
29. Patel, F.; Bhattacharya, P.; Tanwar, S.; Gupta, R.; Kumar, N.; Guizani, M. Block6Tel: Blockchain-based spectrum allocation scheme in 6G-envisioned communications. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 1823–1828.
30. Li, Z.; Wang, W.; Wu, Q.; Wang, X. Multi-Operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework. *IEEE Trans. Cogn. Commun. Netw.* **2023**, *2*, 3–15.