mathematics

MDPI

Article

A Privacy-Preserving Electromagnetic-Spectrum-Sharing Trading Scheme Based on ABE and Blockchain

Xing Pu [1], Ruixian Wang [2] and Xin Lu [1,*]

[1] The State Radio Monitoring Center, Beijing 100041, China; puxing@srrc.org.cn
[2] School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China; ruixian0226@gmail.com
* Correspondence: luxin@srrc.org.cn

Abstract: The electromagnetic spectrum is a limited resource. With the widespread application of the electromagnetic spectrum in various fields, the contradiction between the demand for the electromagnetic spectrum and electromagnetic spectrum resources has become increasingly prominent. Spectrum sharing is an effective way to improve the utilization of the electromagnetic spectrum. However, there are many challenges in existing distributed electromagnetic spectrum trading based on blockchain technology. Since a blockchain does not provide privacy protection, the risk of privacy leakage during the trading process makes electromagnetic spectrum owners unwilling to share. In addition, a blockchain only guarantees integrity, and the imperfect trading dispute resolution mechanism causes electromagnetic spectrum owners to be afraid to share. Therefore, we propose a privacy-preserving electromagnetic-spectrum-sharing trading scheme based on blockchain and ABE. The scheme not only designs an ABE fine-grained access control model in ciphertext form but also constructs a re-encryption algorithm that supports trading arbitration to achieve privacy protection for electromagnetic spectrum trading. Finally, we experimentally evaluated the efficiency of the proposed electromagnetic spectrum trading scheme. The experimental results show that the electromagnetic spectrum trading scheme we propose was highly efficient.

Keywords: electromagnetic spectrum trading; blockchain; privacy-preserving; access control

MSC: 94A60

Citation: Pu, X.; Wang, R.; Lu, X. A Privacy-Preserving Electromagnetic-Spectrum-Sharing Trading Scheme Based on ABE and Blockchain. *Mathematics* **2024**, *12*, 2908. https://doi.org/10.3390/math12182908

Academic Editor: Antanas Cenys

Received: 19 August 2024
Revised: 13 September 2024
Accepted: 13 September 2024
Published: 18 September 2024

1. Introduction

Electromagnetic spectrum management is the foundation of radio communication, the key to maximizing the effectiveness of electronic systems, and an important guarantee for the smooth flow of information. The electromagnetic spectrum used for traditional wireless services, such as mobile communications, television, and radio, is used in a fixed and exclusive manner, which results in a very unbalanced utilization of electromagnetic spectrum resources. In the cellular mobile band [1], the frequency bands are becoming quite crowded and spectrum resources are in short supply. Limited spectrum resources have constrained the development and application of various new technologies, especially in 4G [2], the Internet of things [3], and space satellites, which face a large number of electromagnetic spectrum "gaps". The existing electromagnetic spectrum allocation situation shows that almost all of the spectrum is occupied by the authorized services, and new business requisitions occupy the remaining available frequency bands, which not only significantly increases the economic burden of the new businesses but is also not conducive to the sustainable development of future wireless services. The paid sharing [4] of the electromagnetic spectrum has become an effective way to solve the above problems.

In recent years, with the popularity of cryptocurrencies, such as Bitcoin [5] and Ethereum [6], blockchain [7] technology has received increasing attention around the world. A blockchain-based distributed trading architecture provides a new solution idea for the

sharing of the electromagnetic spectrum. The sharing of the electromagnetic spectrum is directly transacted peer to peer between any nodes in the blockchain network without the intervention of a third party organization. The introduction of smart contracts [8] further realizes the automated execution and integrity assurance of electromagnetic-spectrum-sharing trading. The electromagnetic-spectrum-sharing trading model is shown in Figure 1.

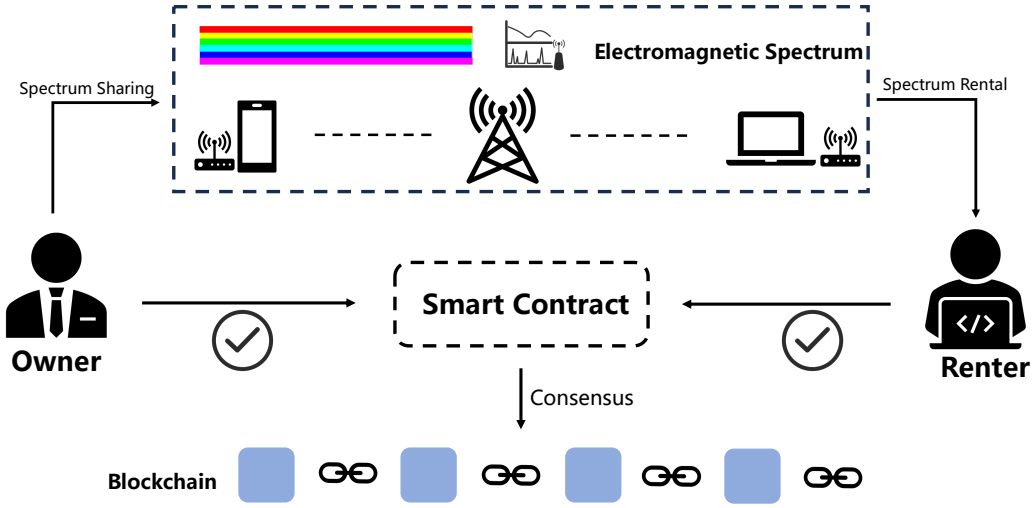

Figure 1. Electromagnetic spectrum sharing trading model.

However, electromagnetic spectrum trading still has the following challenges. **Challenge 1—lack of effective privacy protection:** the publicly auditable requirements of blockchain technology inevitably lead to the disclosure of trade secrets, such as electromagnetic spectrum resource information, transaction amounts, and lease times, by sharing with users during the trading process. **Challenge 2—access control cannot be implemented:** it is difficult for electromagnetic spectrum sharers to control trading objects that do not meet the attribute requirements from accessing the shared trading smart contract. **Challenge 3—lack of a dispute arbitration mechanism:** the particularity of electromagnetic spectrum resources makes it easy for disputes to occur during shared trading, and a distributed blockchain system that lacks a centralized arbitration agency cannot guarantee the fairness of trading.

To address the above problems and challenges, we propose a privacy-preserving electromagnetic-spectrum-sharing trading scheme based on ABE and a blockchain. To address **Challenge 1**, we built an electromagnetic-spectrum-trading smart contract in encrypted form to achieve privacy protection for the entire shared trading process. To address **Challenge 2**, we introduce the attribute-based encryption (ABE) [9] primitive that associates keys with user attributes to support fine-grained access control. To address **Challenge 3**, we propose a trading arbitration mechanism that is applicable to multiple arbitration nodes and design re-encryption algorithms that support a ciphertext update. Specific innovations are shown below:

1. We propose a privacy-preserving electromagnetic spectrum sharing trading scheme based on ABE and a blockchain. We introduce the attribute-based encryption (ABE) primitive to support fine-grained access control. Electromagnetic-spectrum-sharing users can customize access control policies to achieve privacy protection and data security.
2. We designed an arbitration mechanism for electromagnetic spectrum trading and proposed a ciphertext access algorithm suitable for multiple arbitration nodes, which supports ciphertext updates after arbitration is completed.
3. We designed experiments to evaluate the performance of the proposed electromagnetic-spectrum-sharing trading scheme. The experimental results show that our proposed scheme is efficient.

The rest of this paper is organized as follows. Section 2 reviews and summarizes the related work on electromagnetic spectrum sharing trading. Section 3 introduces preliminaries. Section 4 introduces the system model and architecture. Section 5 describes the algorithmic details of our proposed scheme. Section 6 evaluates the performance of the scheme. Finally, we conclude this paper in Section 7.

2. Related Works

Electromagnetic spectrum sharing has become an effective way to improve spectrum utilization. Michele et al. explored the development of spectrum policy and spectrum technology to enable sharing between different stakeholders in the spectrum above 100 GHz, which emphasized that sharing is essential to allow each stakeholder to make full use of that spectrum [10]. Zhou et al. proposed a blockchain-based privacy-preserving, incentive-compatible, and efficient spectrum-sharing framework for the challenges of implementing large-scale spectrum sharing in 5G heterogeneous networks [11]. In order to cope with the identity privacy and data security issues in secure spectrum sharing, Zheng et al. proposed a smart contract-based spectrum-sharing transaction scheme for multi-operator wireless communication networks [12]. There are also some studies of spectrum sharing trading that were based on game theory. Huang et al. studied the auction mechanism for a shared spectrum and proposed two auction mechanisms for allocating received power. Finally, they designed an iterative distributed bidding update algorithm and specified the conditions for the algorithm to globally converge to the auction Nash equilibrium [13]. Regarding the spectrum-sharing problem between a primary user and multiple secondary users, Dusit et al. studied the stability conditions of the dynamic behavior of the spectrum-sharing scheme in 2008 and used a non-cooperative game to obtain the spectrum allocation of secondary users [14]. In the same year, Dusit et al. used the Bertrand game model to analyze the impact of several system parameters, such as spectrum substitutability and channel quality, on the Nash equilibrium, and proposed a distributed algorithm to obtain the solution to this dynamic game and solve the spectrum-pricing problem in radio networks [15]. Yang et al. proposed two game models that interact with each other to form a final Stackelberg DSL game for dynamic spectrum leasing (DSL) schemes [16].

Privacy protection is a key issue in electromagnetic spectrum sharing. Park et al. reviewed key security and privacy threats that affect spectrum sharing, proposed a threat categorization methodology, described representative examples of each threat category, and discussed threat countermeasures and enforcement techniques [17]. Clark et al. developed a generic spectrum-sharing system architecture to formulate a multi-utility user privacy optimization problem to achieve a balance between privacy and performance [18]. Clark et al. also proposed an analytical approach to protect user privacy using adversary techniques and obfuscation policies for spectrum access systems [19]. Li et al. proposed PeDSS, which is a privacy-enhanced and database-driven dynamic spectrum sharing framework that protects privacy without the need for a trusted third party [20]. Clark et al. evaluated the use of perceptual and interface obfuscation methods in spectrum-sharing systems, identified key design parameters in a formal model of the sharing system architecture, and conducted a thorough simulation study of real use cases to quantify privacy and performance [21]. Cui et al. demonstrated the redistribution of spectrum sharing among stakeholders and studied how the governance of public resources affects the distribution of rights in the spectrum [22]. Finally, Bhattarai et al. outlined the main current technical and regulatory reforms in electromagnetic spectrum sharing by focusing on current efforts to manage electromagnetic spectrum-sharing methods for users with heterogeneous access and interference protection rights [23].

The above schemes consider privacy protection but none of them consider access control policies. Attribute-based encryption's (ABE's) fine-grained access control algorithms provide new solution ideas. Qiao et al. surveyed mainstream papers, analyzed the main functions of the required ABE systems, and classified them into different categories [24]. In 2007, Bethencourt proposed a system for implementing complex access

control of encrypted data that is called ciphertext policy attribute-based encryption. In this scheme, the encrypted data can be kept confidential, even if the storage server is untrusted. In addition, this method can resist collusion attacks [9]. Subsequently, Lewko et al. further proposed a multi-authority attribute encryption (ABE) system [25] in 2011, where one party can act as an ABE authority by simply creating a public key and publishing private keys to different users that reflect its attributes. Users can encrypt data based on a Boolean formula of attributes published by any selected set of authorities. Goyal et al. developed a new encryption system called key policy attribute-based encryption (KP-ABE) for the fine-grained sharing of encrypted data [26]. In this encryption system, ciphertexts are labeled with sets of attributes, and private keys are associated with access structures that control which ciphertexts a user can decrypt. In addition, ABE has a wide range of applications. In 2020, Zhang et al. summarized attribute-based encryption (ABE) for cloud computing access control and first proposed classification and comprehensive evaluation criteria for ABE [27]. Lai et al. considered a new requirement for ABE with outsourced decryption: verifiability, which allows for efficient checking of whether the transformation is done correctly [28]. Yao et al. proposed a lightweight pairing-free ABE scheme based on elliptic curve cryptography (ECC) to address security and privacy issues in the Internet of things [29]. Akinyele et al. proposed a privacy protection scheme for electronic medical records (EMRs) on mobile devices using attribute-based encryption [30]. Ge et al. first proposed an attribute-based encryption reliable outsourcing decryption scheme based on blockchain smart contracts, where mobile devices can verify whether the cloud service provider returns the correct decryption result [31]. Therefore, ABE-based access control for electromagnetic-spectrum-sharing trading is feasible.

3. Preliminaries

In this section, we review the preliminary knowledge and related concepts involved in the scheme. First, we list the cryptographic primitives used in the encryption and decryption processes. Then, we introduce the concepts and explanations of blockchain and smart contracts.

3.1. Cryptographic Primitives

Next, we introduce the bilinear mapping, access structure, and secret-sharing scheme used in the attribute-based encryption algorithm.

3.1.1. Bilinear Maps

Definition 1 (Bilinear maps)**.** *Assume that* $\mathbb{G}_0$ *and* $\mathbb{G}_1$ *are two multiplicative cyclic groups of prime order p. Let g be the generator of* $\mathbb{G}_0$*. The bilinear map e can be expressed as* $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$*. Therefore, for any* $a, b \in \mathbb{Z}_p$*, we have the following three properties:*

1. *Bilinearity:* $\forall u, v \in \mathbb{G}_1, e\left(u^a, v^b\right) = e(u, v)^{ab}$.
2. *Computability:* $\forall f, h \in G_1, e(f, h)$.
3. *Non-degeneracy:* $e(g, g) \neq 1$.

3.1.2. Access Structure

Definition 2 (Access structure [9])**.** *Let* $\{P_1, P_2, \ldots, P_n\}$ *be a set of parties. A collection* $\mathbb{A} \subseteq 2^{(P_1, P_2, \ldots, P_n)}$ *is monotone if* $\forall B, C : B \in \mathrm{A}$ *and* $B \subseteq C$*, then* $C \in \mathbb{A}$*. An access structure is a collection* $\mathbb{A}$ *of non-empty subsets of* $\{P_1, P_2, \ldots, P_n\}$*,* $\mathbb{A} \in 2^{(P_1, P_2, \ldots, P_n\}} \backslash \{\varnothing\}$*. The set in* $\mathbb{A}$ *is called the authorized set, and the set not in* $\mathbb{A}$ *is called the unauthorized set.*

3.1.3. Linear Secret-Sharing Schemes

Definition 3 (Linear secret-sharing schemes (LSSS) [32])**.** *When the following conditions are met, the secret-sharing scheme* Π *of a group of participants is linear:*

1. *The shares of all parties form a vector over* $\mathbb{Z}_p$.

2. *We generate a shared generator matrix of l rows and n columns for* Π. *For all* $i = 1, 2, \cdots, l$, *in the* i'*th row of M, we use the function* $P(i)$ *as the row label. A column vector* $v = (s, r_2, \ldots, r_n)$ *is generated, where* $s \in \mathbb{Z}_p$ *is the secret to be shared and* $r_2, \ldots, r_n \in \mathbb{Z}_p$ *are randomly chosen; then, Mv is the vector of l shares of the secret s according to* Π. *The share* $(Mv)_i$ *belongs to party* $P(i)$.

3.2. Blockchain and Smart Contracts

3.2.1. Blockchain

The origin of blockchain technology is indeed closely linked to Bitcoin [5]. As the underlying technical framework of Bitcoin, it has gradually developed and independently become a technology with wide application potential. Blockchain technology provides a new solution for trust and value transfer in modern society through its unique design principles, namely, decentralization, trustlessness, data immutability, and collective maintenance.

1. **Decentralization and trustlessness**: One of the core advantages of a blockchain is its decentralized nature, which means that there is no single central point of control for the entire network, and all participants jointly maintain the security of the network and the integrity of the data. At the same time, the trustless mechanism ensures reliable transmission and storage of data, even in the absence of direct trust between participants in the network through cryptographic algorithms and consensus mechanisms. This mechanism greatly reduces the risk of single-point failures that may exist in traditional centralized systems and improves the overall stability and security of the system.
2. **Consensus mechanism**: A blockchain achieves coordination and consistency among nodes in the network through a consensus mechanism. The consensus mechanism is the core component of blockchain technology, which determines how to reach a consensus in a distributed system to ensure the accuracy and consistency of data. Common consensus mechanisms include proof of work (PoW) [33] and proof of stake (PoS) [34]. These mechanisms encourage nodes in the network to actively participate in verifying and recording transactions through economic incentives and algorithm design, thereby maintaining the stable operation of the entire system.
3. **Integrity**: The data structure of the blockchain is stored in a chain, and each block contains the hash value of the previous block, which forms an unalterable chain data structure. Once the data are written into the blockchain, it is almost impossible to tamper with the data unless more than 51% of the computing power in the network is controlled (under the PoW mechanism). This data immutability makes the blockchain an ideal choice for recording important transactions and asset ownership.

3.2.2. Smart Contracts

A smart contract is a computer program based on blockchain technology that is designed to automatically execute according to the conditions of a contract or agreement. Smart contracts have the following characteristics:

1. **Automatic execution**: when the terms of the contract are met, the smart contract will be automatically executed without human intervention.
2. **Transparency**: the execution process and results of smart contracts are visible to all users on the blockchain, which ensures the transparency of transactions.
3. **Unalterable**: due to the decentralized and distributed nature of a blockchain, smart contracts cannot be tampered with once deployed.
4. **Security**: a blockchain's encryption technology and consensus mechanism provide a high level of security for smart contracts.

Smart contracts write the contract terms into the blockchain in the form of computer code. When the preset conditions are met, the smart contract will automatically execute the corresponding operations. These operations can be transfers, data records, notifications,

etc. The execution process of smart contracts is completely controlled by code and is not affected by human factors.

4. Model and Goals

In this section, we introduce the system model, threat model, and design goals of the proposed electromagnetic-spectrum-sharing transaction scheme.

4.1. System Model

The main entities in our proposed scheme are the electromagnetic spectrum owner, electromagnetic spectrum renter, trading arbitration node, electromagnetic-spectrum-sharing smart contract, and electromagnetic-spectrum-sharing trading blockchain. The definition of each entity is as follows:

- **Electromagnetic spectrum owner (ESO)**: Authorized users of the electromagnetic spectrum are individuals, organizations, or institutions approved by the regulatory agency who are willing to share the resource with other users. Authorized users of the magnetic spectrum can profit from the paid sharing of electromagnetic spectrum resources during idle time.
- **Electromagnetic spectrum renter (ESR)**: A user or system that obtains the right to use spectrum resources through a sharing agreement. In electromagnetic spectrum sharing, spectrum-sharing users are similar to "renters". They use spectrum resources in accordance with the provisions of the sharing agreement and bear corresponding obligations and responsibilities.
- **Trading arbitration node (TAN)**: A trading arbitration organization that consists of a series of nodes in the blockchain. When a dispute occurs in an electromagnetic-spectrum-sharing trade, the trading arbitration node obtains the trading contract through a ciphertext access algorithm and makes an arbitration decision.
- **Electromagnetic-spectrum-sharing smart contract (ESSSC)**: Users can sign a lease agreement with spectrum resource holders through smart contracts to specify the lease term, rent, usage conditions, etc. Smart contracts can automatically execute preset rules and conditions, improve the efficiency and accuracy of spectrum sharing, and ensure the authenticity and credibility of the spectrum sharing process.

The architecture of our proposed electromagnetic-spectrum-sharing trading scheme is shown in Figure 2. First, the system is initialized and relevant keys are generated. After the system initialization, the ESO formulates access policies and encrypts the shared electromagnetic spectrum transaction information based on their attributes. The ESR uses their attributes as keys to decrypt in order to view the trading information and then make pairings. The combination of the matched ESO and ESR jointly formulate the ESSSC and broadcast it for publication in the blockchain.

Once a dispute occurs in an electromagnetic-spectrum-sharing trade, the two parties can request a TAN to intervene and execute the judgment. The TAN decrypts the parameters shared with the two parties to view the ESSSC. The TAN will make an arbitration based on the ESSSC and return the arbitration result. After the trading arbitration is completed, the system executes the ciphertext update procedure.

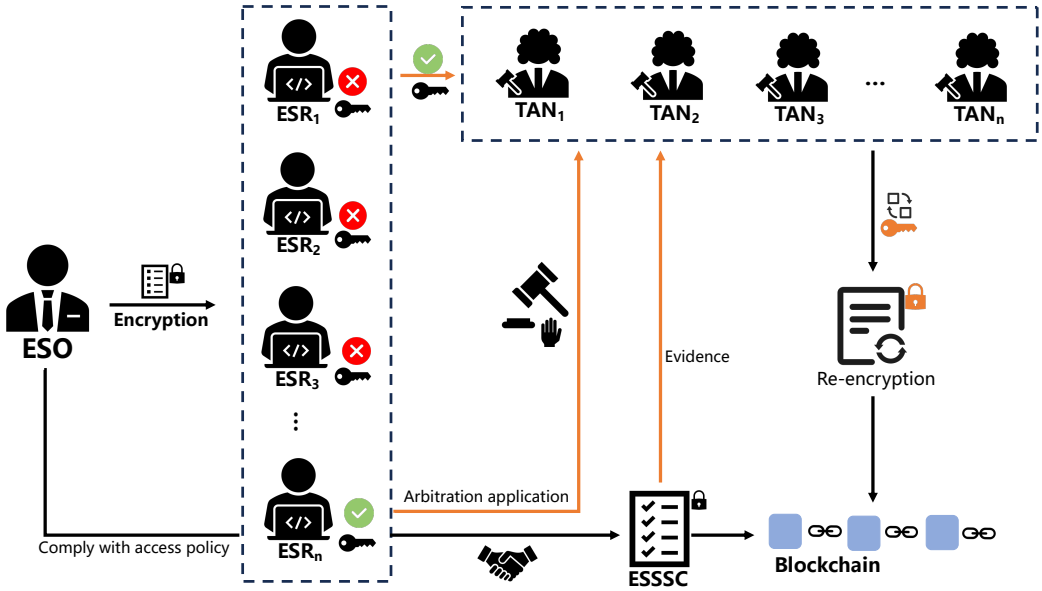

Figure 2. Architecture of the electromagnetic-spectrum-sharing trading scheme.

4.2. Threat Model

In this section, we construct a threat model for the proposed electromagnetic-spectrum-sharing trading scheme.

- **ESO and ESR**: We assumed that both the ESOs and ESRs are honest but curious. ESOs will share the electromagnetic spectrum honestly, but they always want to maximize their own interests. Therefore, they always want to obtain more information in the deal-matching and dispute-arbitration phases in order to make pricing decisions. However, this motivation often leads to the exposure of users' private information and the fairness of trading is difficult to ensure.
- **TAN**: We assumed that the TAN is also honest but curious. The arbitration process of electromagnetic-spectrum-sharing transactions requires a TAN to decrypt the transaction contract to obtain arbitration evidence, but the decryption process will inevitably expose the access policy formulated by the ESO. Although the TAN will faithfully implement the arbitration procedure and ensure the fairness of arbitration, they have the motivation to observe the access policy and make illegal profits.
- **Blockchain**: We assumed that the blockchain is a secure and trusted distributed electromagnetic-spectrum-sharing trading network. A blockchain ensures that nodes in the network reach consensus on transaction data through a consensus mechanism. This mechanism helps to prevent malicious nodes from tampering and attacking the transaction data, and it guarantees the security and stability of electromagnetic-spectrum-sharing trading. Theoretically, it is feasible to launch a 51% attack [35] against a blockchain network that adopts the Byzantine consensus, but the cost of its implementation is so great that we consider its possibility to be negligible. In addition, malicious attacks, such as Sybil attacks, selfish mining, and scalability attacks, on blockchains can theoretically damage blockchains, but these attacks will consume a lot of resources of the attacker, and researchers also gave many solutions that make them ineffective. Therefore, this is beyond the scope of this paper, and we believe that the above attacks will not occur.

4.3. Design Objectives

In this section, we formulate the design goals of our proposed electromagnetic-spectrum-sharing trading scheme in terms of security, privacy, and efficiency.

- **Security**: It was our goal that electromagnetic-spectrum-sharing trading can still be executed securely under the threat model. We needed effective access control methods to ensure that potential attackers whose identities do not comply with the access policies

set by users cannot participate in the electromagnetic spectrum sharing. In addition, we needed secure encryption algorithms to keep user trading information safe. Finally, it was particularly important to prevent malicious arbitration nodes from manipulating the arbitration results and undermining the fairness of the dispute arbitration.

- **Privacy**: Privacy protection is one of the most critical features of electromagnetic-spectrum-sharing trading. Among them, trading information and fine-grained access control policies are the most core privacy information that we needed to protect. The scheme needed to ensure that both types of information cannot be observed by adversaries. On the other hand, we also needed to develop access policy information protection algorithms for arbitration nodes to prevent privacy leakage.
- **Efficiency**: The electromagnetic-spectrum-sharing trading market is huge, and the system needs high execution efficiency to cope with highly concurrent trading requests. Therefore, we needed to experimentally verify the execution efficacy of our proposed electromagnetic-spectrum-sharing trading scheme.

5. Electromagnetic-Spectrum-Sharing Trading Scheme

We present the algorithmic details of the electromagnetic-spectrum-sharing trading scheme in this section.

5.1. System Initialization

5.1.1. Set Up

The initialization procedure begins by generating the relevant public parameters in the algorithm. $\mathbb{G}_0$ is assumed to be a multiplicative cyclic group with prime order p and generators g. Then, a series of parameters $\alpha, \beta, a, b \in \mathbb{Z}_p$, $h_1, \ldots, h_U \in G_0$ is randomly selected. The user master key is denoted as $CMK = \{\alpha, \beta, a\}$. The user public key PK is represented in the following form:

$$PK = \left\{ g, e(g,g)^{\alpha}, e(g,g)^{a}, g^{\beta}, g^{b}, g^{1/b}, h_1 \ldots h_U \right\}.$$

5.1.2. Key Generation

Based on the public key PK, the user master key CMK, the electromagnetic spectrum shared user attribute set S, and the initialized parameter α, the system generates the following shared user private key.

$$\left\{ K = g^{\alpha} g^{\beta t + a}, L = g^{t}, x \in S, K_x = h_x^{t} \right\}.$$

5.2. Electromagnetic Spectrum Trading

After the initialization of the system is complete, the ESO first develops a fine-grained access policy based on the type of intended object of the electromagnetic-spectrum-sharing trading. Then, the ESO encrypts the information of electromagnetic spectrum sharing and the smart contract to form a two-level ciphertext. The second-level ciphertext includes the basic trading information, such as the electromagnetic spectrum parameters, sharing duration, and price. The first-level ciphertext contains the trading smart contract, determines the specific trading terms, and is used as evidence for dispute arbitration. The ESR that complies with the access policy first decrypts the second-level ciphertext to view the basic information of the trading, and the interested ESR further interacts with the ESO and decrypts the first-level of the ciphertext.

5.2.1. Encryption

An LSSS access structure $(\mathcal{M}, \rho)$ is generated based on the access policy developed by the ESO. The function $\rho(i) \in \{A_1, A_2, \ldots A_U\}$ represents the position of a certain restriction attribute set by the ESO in the matrix $\mathcal{M}$. Therefore, $\mathcal{M}$ is represented as a $\rho \times n$ matrix, where ρ represents the number of attributes set by the ESO, and n is the

variable defined by the LSSS conversion method. Each row of $\mathcal{M}$ represents an attribute class, and each column represents the variable of the attribute value. For each row in the matrix, a vector $\vec{v} = (s, y_2, y_3, \ldots, y_n) \in \mathbb{Z}_p^n$ are randomly selected to calculate and obtain a new parameter $\lambda_i = \mathcal{M}_i \cdot \vec{v}$. Finally, $s, f_0, r_1, r_2, \ldots, r_l \in \mathbb{Z}_p$ is randomly selected and the following encryption calculation on the two-level plaintext is performed:

$$\tilde{C}_1 = M_1 \cdot e(g,g)^{\alpha s}$$

$$\tilde{C}_2 = M_2 \cdot e(g,g)^{\alpha s} / e(g,g)^{f_0 s} = M_2 \cdot e(g,g)^{(\alpha - f_0)s}$$

$$C' = g^s$$

$$\hat{C} = g^{c\lambda_i}$$

$$\forall 1 \le i \le \ell, C_i = g^{\beta\lambda_i} h_{\rho(i)}^{-r_i}$$

$$\hat{D}_i = e(g,g)^{\beta\lambda_i} e\left(g, g^{f_0}\right)^{\lambda_i} = e(g,g)^{(f_0+\beta)\lambda_i}$$

$$D_i = g^{r_i}.$$

In summary, the complete ciphertext can be expressed as follows:

$$< \tilde{C}_1, \tilde{C}_2, C', \hat{C}, \forall 1 \le i \le \ell, \{C_i, \hat{D}_i, D_i\} > .$$

5.2.2. Decryption

The ESR that complies with the access policy obtains the information of electromagnetic spectrum sharing by decrypting the second-level ciphertext and applies for the trading. Then, the ESR receives the relevant parameters from the ESO to decrypt the first-level ciphertext.

1. *Decrypt the second-level ciphertext:* ESR matches its own attribute set with the access policy of the ciphertext. If the ESR attribute set S meets the access policy, the decryption is successful. Assuming $I \subset \{1, 2, \ldots, \ell\}$, $I = \{i : \rho(i) \in S\}$, the Lagrange interpolation polynomial is used to solve the equation $\sum_{i \in I} \omega_j \lambda_j = s$ with the coefficient set $\{\omega_i | i \in I\}$.

$$F_1 = \frac{e(C', K)}{\prod_{i \in S} \left(e(L, C_i) e(D_i, K_x) e(g,g)^{(f_0+b)\lambda_i}\right)^{\omega_i}}$$

$$= \frac{e\left(g^s, g^{\alpha} g^{\beta t + a}\right)}{\prod_{i \in S} \left(e\left(g^t, g^{\beta\lambda_i} h_{\rho(i)}^{-r(i)}\right) e\left(g^{r(i)}, h_x^t\right) e(g,g)^{(f_0+a)\lambda_i}\right)^{\omega_i}}$$

$$= \frac{e(g,g)^{\alpha s} e(g,g)^{ats} e(g,g)^{as}}{\prod_{i \in S} \left(e(g,g)^{\beta t \lambda_i} e(g,g)^{(f_0+a)\lambda_i}\right)^{\omega_i}}$$

$$= \frac{e(g,g)^{\alpha s} e(g,g)^{\beta t s} e(g,g)^{as}}{e(g,g)^{\beta t s} e(g,g)^{(f_0+a)s}}$$

$$= e(g,g)^{(\alpha - f_0)s}.$$

Therefore, the second-level ciphertext can be decrypted by the following calculation:

$$\frac{\tilde{C}_2}{F_1} = \frac{M_2 \cdot e(g,g)^{(\alpha - f_0)s}}{e(g,g)^{(\alpha - f_0)s}} = M_2.$$

2. *Decrypt the first-level ciphertext:* By viewing the second-level plaintext, the ESR transmits a trading request to the ESO. The ESR receives the security parameter g^{f_0} from the ESO and performs the computation to decrypt the first-level ciphertext:

$$\frac{\tilde{C}_1}{F_1 \cdot e\left(g^s, g^{f_0}\right)} = \frac{M_1 \cdot e(g,g)^{\alpha s}}{e(g,g)^{(\alpha - f_0)s} e(g,g)^{f_0 s}} = M_1$$

After the decryption is completed, the ESO and ESR sign the smart contract and upload it into the blockchain. The blockchain system completes the consensus agreement and the smart contract is automatically executed. The electromagnetic spectrum trade is completed.

5.3. Request for Arbitration

If the paired ESO and ESR have a dispute regarding a trade, they can apply to a TAN for arbitration. Once the dispute arbitration process starts executing, the ESO and ESR each share a secret parameter and use it to encrypt the arbitration message to be transmitted to the TAN. Specifically, the ESO randomly generates a parameter $\epsilon \in \mathbb{Z}_p$, shares ϵ with ESR through a secure channel, and completes the following calculation:

$$K_1 = F_1 \cdot e(g^{\epsilon}, g^s) = e(g,g)^{(\alpha - f_0 + \epsilon)s}$$

$$F_2 = \frac{\tilde{C}_1}{M_1}$$

$$K_2 = F_2 \cdot e(g^s, g^{\epsilon}) = e(g,g)^{(\alpha+\epsilon)s}.$$

The ESR obtains g^{ϵ} and calculates

$$\tilde{C}_1' = M_1 \cdot (g,g)^{\epsilon s} \cdot e(g^s, g^{\epsilon}) = M_1 \cdot e(g,g)^{(\alpha+\epsilon)s}$$

$$\tilde{C}_2' = M_2 \cdot e(g,g)^{(\alpha - f_0)s} \cdot e(g^s, g^{\epsilon}) = M_2 \cdot e(g,g)^{(\alpha+\epsilon-f_0)s}.$$

Then, the ESO and ESR transmit the binaries $< \tilde{C}_1', \tilde{C}_2' >$ and $< K_1, K_2 >$ to the TAN, respectively. After receiving the ciphertext and binary pairs, the TAN performs the following decryption calculation to obtain the electromagnetic-spectrum-sharing trading plaintext and start the arbitration procedure:

$$\frac{\tilde{C}_2'}{K_1} = \frac{M_2 \cdot e(g,g)^{(\alpha - f_0 + \epsilon)s}}{e(g,g)^{(\alpha - f_0 + \epsilon)s}} = M_2$$

$$\frac{\tilde{C}_1'}{K_2} = \frac{M_1 \cdot e(g,g)^{(\alpha+\epsilon)s}}{e(g,g)^{(\alpha+\epsilon)s}} = M_1.$$

5.4. Re-Encryption

After the arbitration is completed, the ESO randomly selects $f_1 \in \mathbb{Z}_p$ to update the ciphertext to ensure that the TAN cannot view the trading plaintext information again, and the re-encrypted first-level ciphertext cannot be decrypted by other ESRs that meet the access policy. This design implements privacy protection for access policies and trading information.

$$\hat{D}_i' = e(g,g)^{(f_0+a)\lambda_i} e\left(g^{b\lambda_i}, g^{f_1/b}\right) = e(g,g)^{(f_0+f_1+a)\lambda_i}.$$

The ciphertext update is complete. If the ESR needs to decrypt the first-level ciphertext, it must interact with the ESO to obtain the shared parameters.

6. Security Analysis

We analyzed the algorithmic security of our proposed electromagnetic-spectrum-sharing trading scheme in terms of security, confidentiality, and privacy and present the results in this section.

6.1. Security

The security of the ABE algorithm is based on the assumptions of some mathematical challenges, such as the bilinear Diffie–Hellman problem [36] and the discrete logarithm problem [37]. These assumptions are considered to be difficult to break with the current computing power. On the other hand, the security of the ABE algorithm relies on the confidentiality of the private key. The private key is generated based on the user's attributes and the system's master private key. The private key generation process ensures that only authorized users (i.e., those with the correct attributes) have access to a valid private key.

6.2. Confidentiality

In the ABE algorithm, the encryption process encrypts the plaintext using a public key and an access policy to generate a ciphertext. This encryption process ensures that even if an attacker has both the public key and the ciphertext, they cannot decrypt the data directly unless they also have the attribute private key that satisfies the access policy.

6.3. Privacy

The ABE algorithm controls access to the data by defining the attributes of users and access policies for the data. A user's attributes represent their identity, role, permissions, and other characteristics, while the access policy defines which combinations of attributes are capable of decrypting specific encrypted data. This mechanism ensures that only users with the correct combination of attributes can access the data.

7. Performance Analysis

We analyzed the performance of the proposed electromagnetic-spectrum-sharing trading scheme through experiments and presented the results in this section. On the one hand, we experimentally evaluated the execution efficiency of the ABE algorithm we used in the encryption and decryption stages. On the other hand, we designed comparative experiments to measure the performance differences between the proposed scheme and other similar schemes.

In order to control the variables, we conducted comparison experiments in the same experimental environment. The experiments ran on an Intel i5-8250U (1.60 GHz with 4 GB RAM) platform with 8 GB of physical memory. The system software version of the platform was Ubuntu 18.04.4 and a Java pairing encryption library 2.0.0.

7.1. Algorithm Performance

Through our analysis, we found that the main cost of the scheme was concentrated in the computational time overhead of the encryption and decryption phases, while the time overhead of the other steps was negligible in comparison. Based on the above analysis, we compared the computational efficiency of the redesigned ABE algorithm based on the matrix access structure in this scheme with that of the original CP-ABE [9] algorithm using the tree access structure.

We denote t_A, t_M, and t_E as the average time for the algorithm to execute the addition, multiplication, and exponentiation operations once, respectively. T_E and T_D denote the time overheads of the encryption and decryption process, respectively. And N_A denotes the number of attributes in the access policy. T_E and T_D denote the time overheads of the encryption and decryption processes, respectively. N_A denotes the number of attributes in the access policy. Therefore, we propose the following expressions for T_E and T_D in the scheme:

$$T_E = (N_A + 1)t_A + (4N_A + 5)t_M + (4N_A + 6)t_E$$

$$T_D = N_A^* t_A + (12 + 4N_A)t_M + 6N_A^* t_E.$$

According to the repeated experiments, we concluded that in our experimental environment, the average time consumed for an exponential operation was 2.7 ms, the average time consumed for a multiplication operation was 1.5 ms, and the time overhead of the

addition operation was almost negligible compared with the exponential and multiplication operations. The experiment fixed the size of the encrypted data to be 1 kB, and the number of encryption and decryption times were both 1 time. The time overhead was recorded by changing the value of NA. The time overheads of encryption and decryption phases are shown in Figure 3 and Figure 4, respectively.

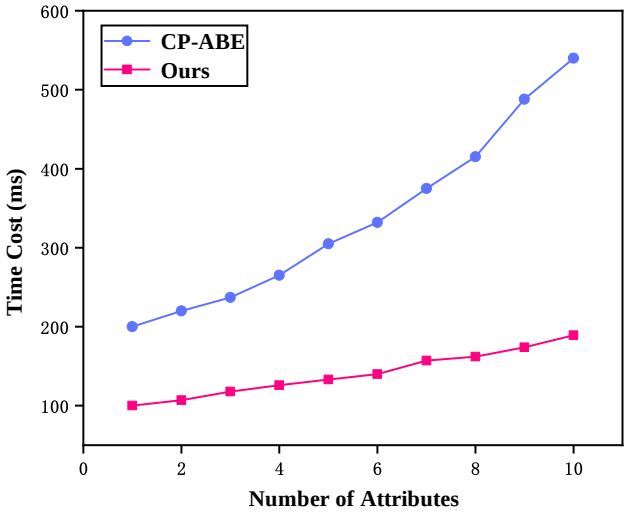

Figure 3. Comparisonof encryption computation times between CP-ABE in [9] and our algorithm.

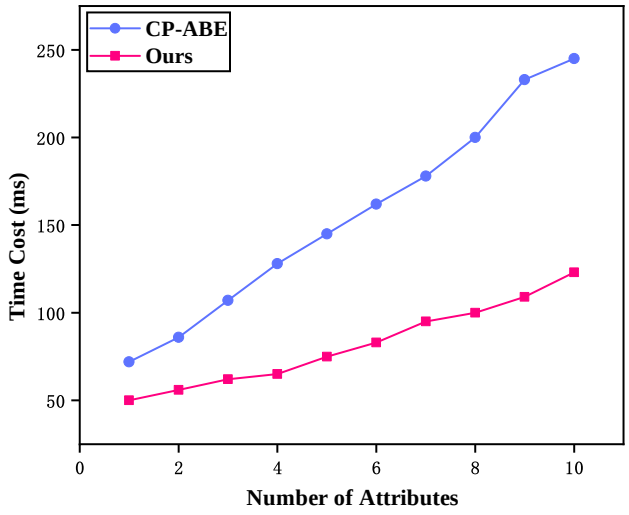

Figure 4. Comparison of decryption computation times between CP-ABE in [9] and our algorithm.

Based on the data shown in Figures 3 and 4, the following conclusions could be drawn. The time overhead of both the matrix-access-structure-based ABE algorithm in our proposed scheme and the traditional CP-ABE algorithm in the encryption and decryption phases increased continuously with the increase in the number of access policy attributes. However, the performance of the reconstructed ABE algorithm in our scheme was higher than that of the CP-ABE algorithm in the encryption and decryption phases under any N_A, and this performance gap became more and more obvious with the increase in the number of policy attributes.

7.2. Scheme Performance

To evaluate the execution efficiency of our proposed electromagnetic-spectrum-sharing transaction scheme, we selected two attribute encryption schemes that were both based on the linear secret sharing scheme (LSSS) access structure [38,39] and designed comparative

experiments to analyze the time overhead of the encryption and decryption steps in the schemes.

Next, we briefly describe the feasibility of comparing the contrasting schemes with our proposed scheme. The attribute encryption scheme with trusted authentication based on blockchain [38] proposes a fully policy-hidden CP-ABE scheme based on the linear secret sharing scheme (LSSS) access structure and blockchain for public cloud data sharing. Both our scheme and the scheme in [38] use ABE and blockchain techniques for the sharing of different objects. Reference [39] proposes an efficient, fine-grained big data access control scheme with privacy-preserving policies. Both our scheme and the scheme in reference [39] use ABE-based techniques to achieve user privacy protection. Therefore, all the above schemes are applicable as comparison schemes.

We compared the time overheads of the three schemes in the two main steps of encryption and decryption by separately varying the number of access policy attributes. In particular, we classified decryption into two different scenarios: decryption success and decryption failure. Finally, we measured the time overhead for each of the two different scenarios.

The results of the encryption phase of the experiment are shown in Figure 5. We obtained the following two observations. First, the time overhead of all three schemes was positively correlated with the number of attributes in the access policy. Second, for the same number of attributes, the encryption time of our proposed scheme was the lowest; although this advantage was not very obvious, it was enough to show that the performance of our scheme could meet the design goal.

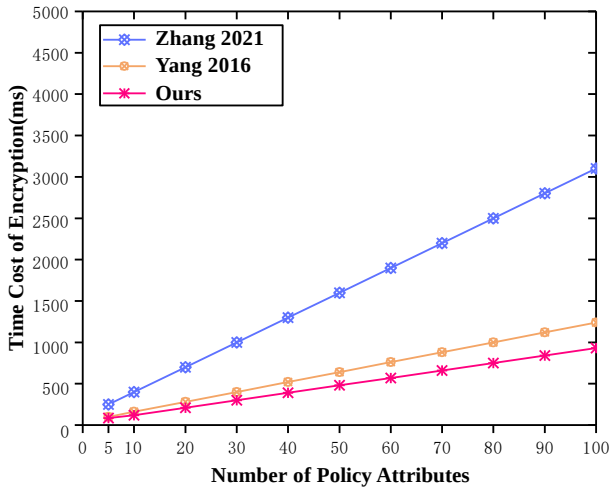

Figure 5. Performance comparison of encryption [38,39].

The experimental results of the decryption phase are shown in Figures 6 and 7. It is easy to see that the time overhead of the decryption operation became longer with the increase in the number of attributes in the access policy, regardless of whether the decryption was successful or not, and this performance degradation became more and more obvious. Nevertheless, the decryption time overhead of our scheme was lower than the comparison scheme in both cases. The performance requirements for electromagnetic-spectrum-sharing trading were met.

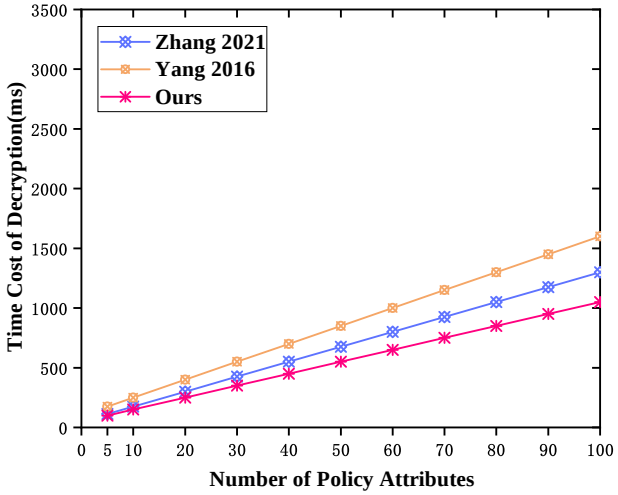

Figure 6. Performance comparison with correct private key decryption [38,39].

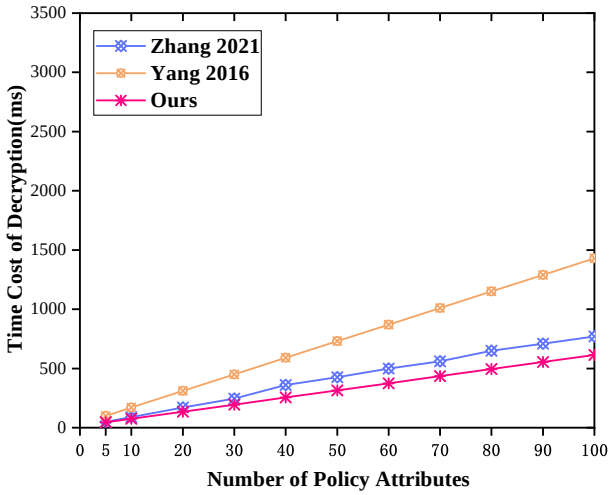

Figure 7. Performance comparison with incorrect private key decryption [38,39].

7.3. Transaction Delays

In order to verify the performance difference between our proposed scheme and the existing blockchain-based electromagnetic-spectrum-sharing trading system, we designed a comparative experiment to measure the latency by changing the number of miners [40].

According to Figure 8, the system latency of the two schemes gradually decreased with the increase in the number of miners and tended to stabilize when the number of miners was four. This was because as the number of miners increased, the overall computing power increased, and the speed of generating new blocks became faster, which resulted in a reduced latency. The processing power peaked when the number of miners was four, and thus, a further increase in the number of miners had limited impact on the latency. In addition, the latency of the electromagnetic-spectrum-sharing transaction we proposed was lower than that of the comparison scheme under any number of miner nodes, and the performance was excellent.

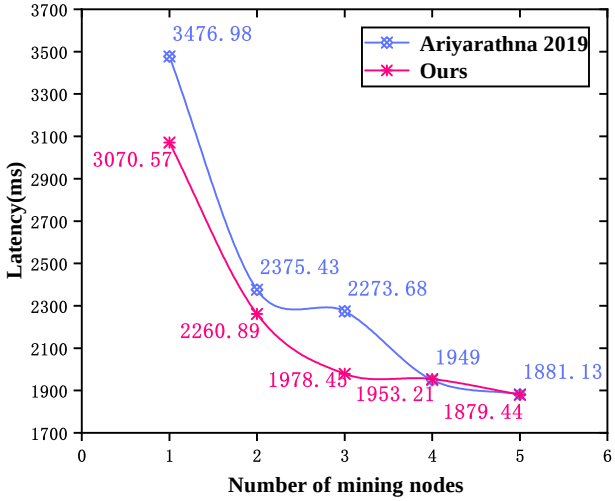

Figure 8. Transaction delays under different numbers of miners [40].

8. Conclusions

This paper proposes a privacy-preserving electromagnetic-spectrum-sharing trading scheme based on a blockchain and ABE, which supports fine-grained access control by introducing attribute-based encryption (ABE) primitives. Electromagnetic-spectrum-sharing users can customize the access control policies to achieve privacy protection and data security. In addition, this paper also presents the design for an arbitration mechanism for electromagnetic spectrum trading, proposes a ciphertext access algorithm suitable for multiple arbitration nodes, and supports ciphertext updates after arbitration is completed. Finally, we analyzed the performance of our proposed scheme by designing comparative experiments. The experimental results show that our proposed electromagnetic-spectrum-sharing trading scheme achieved privacy protection with high efficiency.

Author Contributions: Conceptualization, X.P.; methodology, R.W.; software, X.L.; validation, X.L.; formal analysis, X.L.; data curation, R.W.; writing—original draft, X.L.; writing—review and editing, X.P. All authors read and agreed to the published version of this manuscript.

Funding: This work was supported by the Ministry of Industry and Information Technology under grant 23100002022102001.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shi, Q.; Liu, L.; Zhang, S.; Cui, S. Device-free sensing in OFDM cellular network. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1838–1853. [CrossRef]
2. Akyildiz, I.F.; Gutierrez-Estevez, D.M.; Reyes, E.C. The evolution to 4G cellular systems: LTE-Advanced. *Phys. Commun.* **2010**, *3*, 217–244. [CrossRef]
3. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
4. Thakur, P.; Singh, G. Power management for spectrum sharing in cognitive radio communication system: A comprehensive survey. *J. Electromagn. Waves Appl.* **2020**, *34*, 407–461. [CrossRef]
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Busuness Review. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 16 August 2024).
6. Buterin, V. Ethereum white paper. *GitHub Repos.* **2013**, *1*, 22–23.
7. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
8. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.B.D.; Xia, X.; Feng, Y.; Xu, B. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* **2019**, *47*, 2084–2106. [CrossRef]

9. Bethencourt, J.; Sahai, A.; Sahai, A. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.
10. Polese, M.; Cantos-Roman, X.; Singh, A.; Marcus, M.J.; Polese, M.; Cantos-Roman, X.; Singh, A.; Marcus, M.J.; Maccarone, T.J.; Melodia, T.; et al. Coexistence and spectrum sharing above 100 GHz. *Proc. IEEE* **2023**, *111*, 928–954. [CrossRef]
11. Zhou, Z.; Chen, X.; Zhang, Y.; Mumtaz, S. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. *IEEE Netw.* **2020**, *34*, 24–31. [CrossRef]
12. Zheng, S.; Han, T.; Jiang, Y.; Ge, X. Smart contract-based spectrum sharing transactions for multi-operators wireless communication networks. *IEEE Access* **2020**, *8*, 88547–88557. [CrossRef]
13. Huang, J.; Berry, R.A.; Honig, M.L. Auction-based spectrum sharing. *Mob. Netw. Appl.* **2006**, *11*, 405–408. [CrossRef]
14. Niyato, D.; Hossain, E. Competitive spectrum sharing in cognitive radio networks: A dynamic game approach. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2651–2660. [CrossRef]
15. Niyato, D.; Hossain, E. Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 192–202. [CrossRef]
16. Yang, C.; Li, J. Pricing-based dynamic spectrum leasing: A hierarchical multi-stage Stackelberg game perspective. *IEICE Trans. Commun.* **2013**, *96*, 1511–1521. [CrossRef]
17. Park, J.M.; Reed, J.H.; Beex, A.A.; Clancy, T.C.; Kumar, V.; Bahrak, B. Security and enforcement in spectrum sharing. *Proc. IEEE* **2014**, *102*, 270–281. [CrossRef]
18. Clark, M.; Psounis, K. Optimizing primary user privacy in spectrum sharing systems. *IEEE/ACM Trans. Netw.* **2020**, *28*, 533–546. [CrossRef]
19. Clark, M.; Psounis, K. Can the privacy of primary networks in shared spectrum be protected? In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; pp. 1–9.
20. Li, H.; Yang, Y.; Dou, Y.; Park, J.M.J.; Ren, K. PeDSS: Privacy enhanced and database-driven dynamic spectrum sharing. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1477–1485.
21. Clark, M.; Psounis, K. Achievable privacy-performance tradeoffs for spectrum sharing with a sensing infrastructure. In Proceedings of the 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola, France, 6–8 February 2018; pp. 103–110.
22. Cui, L.; Gomez, M.M.; Weiss, M.B. Dimensions of cooperative spectrum sharing: Rights and enforcement. In Proceedings of the 2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN), McLean, VA, USA, 1–4 April 2014; pp. 416–426.
23. Bhattarai, S.; Park, J.M.J.; Gao, B.; Bian, K.; Lehr, W. An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research. *IEEE Trans. Cogn. Commun. Netw.* **2016**, *2*, 110–128. [CrossRef]
24. Qiao, Z.; Liang, S.; Davis, S.; Jiang, H. Survey of attribute based encryption. In Proceedings of the 15th IEEE/ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD), Las Vegas, NV, USA, 30 June–2 July 2014; pp. 1–6.
25. Lewko, A.; Waters, B. Decentralizing attribute-based encryption. In *Advances in Cryptology—EUROCRYPT 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 568–588.
26. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2006; pp. 89–98.
27. Zhang, Y.; Deng, R.H.; Xu, S.; Sun, J.; Li, Q.; Zheng, D. Attribute-based encryption for cloud computing access control: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–41. [CrossRef]
28. Lai, J.; Deng, R.H.; Guan, C.; Weng, J. Attribute-based encryption with verifiable outsourced decryption. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1343–1354.
29. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112. [CrossRef]
30. Akinyele, J.A.; Pagano, M.W.; Green, M.D.; Lehmann, C.U.; Peterson, Z.N.; Rubin, A.D. Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*; Association for Computing Machinery: New York, NY, USA, 2011; pp. 75–86.
31. Ge, C.; Liu, Z.; Susilo, W.; Fang, L.; Wang, H. Attribute-based encryption with reliable outsourced decryption in cloud computing using smart contract. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 937–948. [CrossRef]
32. Cramer, R.; Damgård, I.B.; Döttling, N.; Fehr, S.; Spini, G. Linear secret sharing schemes from error correcting codes and universal hash functions. In *Advances in Cryptology—EUROCRYPT 2015*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 313–336.
33. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2016; pp. 3–16.

34. Li, W.; Andreina, S.; Bohli, J.M.; Karame, G. Securing proof-of-stake blockchain protocols. In Proceedings of the Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, 14–15 September 2017; pp. 297–315.
35. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
36. Maurer, U.M.; Wolf, S. The diffie–hellman protocol. *Des. Codes Cryptogr.* **2000**, *19*, 147–171. [CrossRef]
37. Odlyzko, A.M. Discrete logarithms in finite fields and their cryptographic significance. In *Advances in Cryptology—EUROCRYPT '8*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 224–314.
38. Zhang, Z.; Zhang, J.; Yuan, Y.; Li, Z. An expressive fully policy-hidden ciphertext policy attribute-based encryption scheme with credible verification based on blockchain. *IEEE Internet Things J.* **2021**, *9*, 8681–8692. [CrossRef]
39. Yang, K.; Han, Q.; Li, H.; Zheng, K.; Su, Z.; Shen, X. An efficient and fine-grained big data access control scheme with privacy-preserving policy. *IEEE Internet Things J.* **2016**, *4*, 563–571. [CrossRef]
40. Ariyarathna, T.; Harankahadeniya, P.; Isthikar, S.; Pathirana, N.; Bandara, H.D.; Madanayake, A. Dynamic spectrum access via smart contracts on blockchain. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.