applied sciences

MDPI

Article

A Blockchain Solution for Remote Sensing Data Management Model

Quan Zou [1], Wenyang Yu [2,*] and Ziwei Bao [1]

[1] School of Computer Information and Science, Centre for Research and Innovation in Software Engineering, Southwest University, Chongqing 400715, China; qzou2014@swu.edu.cn (Q.Z.); a1906266789@email.swu.edu.cn (Z.B.)
[2] Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China
* Correspondence: yuwy@aircas.ac.cn

Abstract: A large number of raw data collected by satellites are processed by the production chain to obtain a large number of product data, of which the secure exchange and storage is of interest to researchers in the field of remote sensing information science. Authentic, secure data provide a critical foundation for data analysis and decision-making. Traditional centralized cloud computing systems are vulnerable to attack and, once the central server is successfully attacked, all data will be lost. Distributed ledger technology (DLT) is an innovative computer technology that can ensure information security and traceability, is tamper-proof, and can be applied to the field of remote sensing. Although there are many advantages to using DLT in remote sensing applications, there are some obstacles and limitations to its application. Remote sensing data have the characteristics of a large data volume, a spatiotemporal nature, global scale, and so on, and it is difficult to store and interconnect remote sensing data in the blockchain. To address these issues, this paper proposes a trustworthy and decentralized system using blockchain technology. The novelty of this paper is the proposal of a multi-level blockchain architecture in which the system collects remote sensing data and stores them in the Interplanetary File System (IPFS) network; after generating the IPFS hash, the network rehashes the value again and uploads it on the Ethereum chain for public query. The distributed data storage improves data security, supports the secure exchange of information, and improves the efficiency of data management.

Keywords: blockchain; remote sensing data management; distributed ledger technology; trusted service; security

Citation: Zou, Q.; Yu, W.; Bao, Z. A Blockchain Solution for Remote Sensing Data Management Model. *Appl. Sci.* **2023**, *13*, 9609. https://doi.org/10.3390/app13179609

Academic Editor: Vincent A. Cicirello

Received: 31 July 2023
Revised: 13 August 2023
Accepted: 15 August 2023
Published: 25 August 2023

1. Introduction

The application field and direction of remote sensing are more and more extensive. With the development of remote sensing technology, and the rich popularization of remote sensing data, remote sensing has developed from a scientific research technology to a global and popular technology. In 2014, the National Integrated Earth Observation Data Sharing Platform, the core technical facility of China's Global Earth Observation System of Systems (GEOSS), realized the interconnection and unified data service of eight satellite centers for the first time [1]. This indicates that the earth observation data sharing in China has entered the stage of social sharing.

In the traditional satellite remote sensing industry chain, multiple upstream and downstream data centers often form independent "data islands" because they cannot trust each other, which leads to a low degree of trust in data sharing. At the same time, more and more massive data collected by proximity sensors (drones, internet of things sensor networks, open government data, etc.) are being used to assist in real-time and more accurate earth observation. However, the providers of such data are often the owners of untrusted research institutions or start-up companies, and may even be the general public.

So, the use of such data could also be damaging. Therefore, it is urgent to solve the problems of mutual trust, data authenticity, and confidentiality among users and institutions in the remote sensing industry chain in remote sensing image data distribution and storage, to strengthen the sharing and interconnection of remote sensing data.

Data security sharing is the first major challenge in collaborative network systems. The main problem is that not all participants in the system are willing to share their raw data. To promote earth science data sharing, many countries and organizations have made explorations and attempts. Early attempts through privately negotiated data sharing, remote sensing data in the present earth observation group (GEO), world data system (WDS) and international data of science and technology commission (revealed), and other international institutions, rely mainly on data policy to help earth observation data sharing. Organizations have also set up some centralized data-sharing platforms to provide data services; for example, the geospatial data cloud platform of the Network Center of the Chinese Academy of Sciences, the Natural Resources Remote Sensing Cloud service platform of Land Satellite Remote Sensing Application Center of the Ministry of Natural Resources, Remote Sensing Market cloud platform of Remote Sensing Group of Chinese Academy of Sciences [2], the Natural Resources Remote Sensing Cloud service platform of Land Satellite Remote Sensing Application Center of the Ministry of Natural Resources [3], and the Sentinel data of European Space Agency [4]. Although cloud computing has evolved over the years, data security and trusted computing remain major challenges in current cloud computing applications. To solve these problems, many scholars have conducted research and put forward many models, including data integrity testing and secure multi-party computing. However, most solutions face problems, such as an excessive computational complexity or lack of scalability. Moreover, cloud computing is centralized computing; once the central server goes down or other errors occur, the data will be inaccessible, untraceable, and face a great risk of tampering.

With the success of Bitcoin, the blockchain technology, as its underlying core technology, has gradually attracted the attention of a large number of scholars, and the blockchain technology has been developing continuously. Blockchain technology [5] is an emerging data sharing and application technology. It uses a peer-to-peer network, consensus mechanism, smart contract, cryptography, and other technologies to avoid the traditional centralized system that is highly dependent on the central authority, and has a high trust cost, poor reliability, and low-security credibility problems. The application of blockchain technology has been extended to digital finance, the internet of things, intelligent manufacturing, supply chain management, medical care, people's livelihood, and other fields, and offers a good strategy to solve data security, data sharing, and data rights confirmation.

At present, blockchain technology has been applied to many fields. As remote sensing applications have become indispensable support for many industries in the world, a trusted remote sensing information service has become a new user demand in a considerable number of countries around the world. Blockchain technology also provides feasible solutions for remote sensing information services. The decentralized, traceable, and unchangeable characteristics of a blockchain can efficiently solve the problems existing in traditional remote sensing data information services, such as a single point of failure, unauthorized tampering, data leakage, data traceability, and so on. At present, the Open Geospatial Consortium [6], the European Space Agency [7], and NASA [8] have all started to introduce blockchain technology into the study of geospatial data. Some domestic institutions and enterprises have also started to develop blockchain platforms for remote sensing data, such as Spatial Information Industry Blockchain Alliance, Beidou Aerospace Group and Digital China Research Institute, Oracle and Yungeng Agriculture, and Internet of Things Industry Research Institute of Zhejiang University. M. Pincheira et al. [9] proposed a blockchain-based system to share and retrieve data without the need for a central authority, which can provide trusted data for remote sensing applications and guarantee the data integrity. Cedeno Jimenez, J. R. and Zhao, P. et al. conducted a literature review on the use of blockchain technology for geographic spatial data sharing and crowdsourcing activities

in reference [10]. Two Geospatial blockchain infrastructures have been fully developed, conceptually (FOAM [11] and D-GIS [12]). Through the benchmarking of projects such as FOAM, D-GIS, and other promising solutions developed in the field, the research findings contribute to the current studies and lay the foundation for future decentralized data sharing infrastructure for geographic spatial data, prioritizing immutability, anonymity, consistency, and consensus-based systems. In reference [13], a comprehensive review of the literature regarding the application of blockchain technology to geographic spatial data was conducted, particularly focusing on the aspect of protecting the privacy and integrity of geographic spatial data. In conclusion, the research on applying blockchain technology to geographic spatial data has gained increasing attention, but remains relatively limited. A. Mendi et al. [14] generated a blockchain-based land registry system for Turkey. At present, blockchain technology is still in the development stage, and its application in many fields has not been fully verified. Its performance, operation and maintenance cost, functional integrity, and many other aspects need to be improved. The application of blockchain technology in the field of geosciences is in the preliminary exploration stage. At present, there has been preliminary theoretical exploration and application research in such fields as map data sharing [11], water resource management [15], air pollution index measurement [16], cadastral data management and updates [17], and property rights protection in geological resources [18]. Although these studies have investigated data recording, real-time tracking, product traceability, and other aspects of the experiment, there are still many problems that remain unresolved. These features put forward new requirements for blockchains.

Currently, the blockchain still has the problem of the difficulty in storing remote sensing data in the blockchain, which is also a difficulty in the combination of blockchain technology and remote sensing data sharing. Remote sensing data are large-scale and high-dimensional, and contain significant geographic spatial information. Storing such data on the blockchain may pose limitations regarding the storage capacity. Additionally, remote sensing data often involve sensitive geographic spatial information, such as terrain and land use. The decentralized and transparent nature of a blockchain may raise concerns regarding privacy and security. While a blockchain can provide a certain level of data protection through encryption techniques, challenges related to data privacy and security still need to be addressed. To overcome these issues, there are potential solutions, such as multichain and access control mechanisms.

The distributed ledger of a blockchain can trace and verify the source and integrity of remote sensing data. Through the utilization of smart contracts and the consensus mechanism of a blockchain, a decentralized system for assessing the quality of remote sensing data can be established. Participants can submit their assessment results and reach consensus through the consensus algorithm. This can enhance the reliability of the data and reduce the inaccuracies caused by individual errors or malicious attacks.

To summarize, this paper intends to make full use of the advantages of a blockchain to research remote sensing data sharing methods, by taking advantage of a blockchain's decentralized, secure, and reliable features, and preventing tampering. Addressing the question, this article on the chain architecture and the block of data structure, on the one hand, will improve the existing blockchain model, according to the business functions of the internal need to build more chain structures and, on the one hand, design and build a data interoperability information model, using the research content of the traceability of the production process, and the block storage model, to form an efficient and distributed remote sensing data blockchain storage scheme, to ensure data security and efficient access.

The decentralized, secure storage and sharing of remote sensing data based on a blockchain will facilitate reliable sharing of remote sensing data around the world, help more people to participate in, and access, geospatial information services, and help spread geospatial information more widely. This will lay the foundation for the reconstruction of spatial data facilities, and provide data and technical support.

The purpose of this paper is to address the issues of storage centralization and the centralized verification of data integrity services in cloud storage scenarios, while maintain-

ing a balance between safety and high performance. To accomplish this, a secure storage solution for remote sensing product data based on multiple blockchains is proposed, and a prototype system is developed for experimental validation. This paper is organized as follows. Section 2 analyzes the relevant issues and work. The specific remote sensing data interoperability system architecture and the block data structure applied to the remote sensing production chain are introduced in Section 3. Section 4 introduces the realization of the prototype system and related experiments, and analyzes the experimental results. Section 5 discussion the potential drawbacks and limitations to this approach. Finally, conclusions and discussions of future work are presented in Section 6.

2. Problem Description

2.1. Characteristics of Remote Sensing Data

Remote sensing data refer to the remote sensing images obtained via various remote sensing techniques, which are multi-level, multi-angle, multi-spectral, multi-temporal, and multi-dimensional data with temporal, spatial, and spectral dimensions. Based on the above definition, the remote sensing data are abstracted into the following types, $T_i = \{Key_i, Time_i, Space_i, imageinfo_i, rsinfo_i\}$. The Key_i is the hash value generated by the hashing operation of T_i, $Space_i$ is the spatial attribute, and $Time_i$ is the temporal attribute, $imageinfo_i$ represents the metadata of this image itself, such as the image type, size, scale, etc. And $rsinfo_i$ means remote sensing information, includes satellite and sensor information [19].

At the same time, remote sensing data also have the characteristics of big data, with massive remote sensing datasets as the main dataset, and comprehensive other auxiliary data from multiple sources, and using big data thinking and means to focus on the theory, method, technology, and activities of obtaining valuable information from massive remote sensing datasets of multiple sources, multiple media, multiple frequency bands, and multiple resolutions.

At present, the main challenges facing the management and production of remote sensing big data are as follows.

1. Data credibility problem

From satellite data acquisition to product visualization for public services, the production process of remote sensing data faces various challenges that cause data unreliability. (a) The source of the auxiliary data, such as proximity sensors, is unreliable. (b) Starting from the satellite data reception, the remote sensing data will go through multiple pre-processing steps, such as geometric correction, radiometric correction, atmospheric correction, etc., and then various value-added products will be obtained through various algorithms. Throughout the life cycle, the complex process leads to the possibility of errors [20]. It is difficult to assess the accuracy of the remote sensing data processing steps in the process, which leads to unreliable final decision knowledge. (c) There is a risk of falsification in processing and circulation, and the data are recorded in a centralized platform, meaning that there is a possibility of data being attacked and tampered with, both of which can cause unreliable data to be in circulation. The result of these factors is that the quality of the data that users eventually obtain cannot be guaranteed. This is one of the main challenges in remote sensing data production and management.

2. The issue of data traceability and confirmation of rights

The traceability of remote sensing data to confirm rights refers to determining the ownership attribution and using the rights attribution of remote sensing product data. This issue and the credibility issue are complementary to each other. If we can successfully trace the source of, and clarify, the data attribution issue, then these problem data can also find the source of, and provide the basis for, the credibility of the data.

The current production process of remote sensing products cannot be authentically traced because of the lack of reliable accounting books for data processing, although the process of data processing can be recorded throughout the data–information–knowledge

life cycle. The ownership of product data is often unclear. The traditional means of validation uses the model of submitting proof of ownership and expert review, which lacks technical credibility and has uncontrollable factors, such as potential tampering. Improving the transparency of the process of realizing the value of remote sensing data, and providing users with authentic and reliable datasets are other major issues in remote sensing big data management.

3. Data sharing problem

In the current context of the big data era, using multiple remote sensing data sources for information extraction has become a major trend. In the current remote sensing data production process, it is almost impossible to produce multi-source remote sensing products under the premise of ensuring the privacy of non-public data. At present, multi-data centers use a data aggregation mode for data sharing and trading among units, and the data sharing process requires intermediate institutions for aggregation, which poses problems, such as complex business processes, data leakage, and non-traceability. In addition, the willingness of remote sensing production workers to share product data is low, and the driving force is insufficient at present; the lack of auditing and of effective evaluation of the shared data makes it difficult to guarantee the quality of the shared data; the problem of data validation after sharing, and the inability to validate the rights, will affect the motivation of data sharing. These are other important challenges faced regarding remote sensing products.

In summary, when facing remote sensing data, a blockchain still has certain problems in the data sharing and supervision mechanism, trusted data sharing mode, and data access control. In order to achieve the safe and efficient sharing of remote sensing data, the data-sharing business has the following needs: (1) the sharing of remote sensing data requires the administrator to authenticate and manage the members involved in data sharing, to prevent malicious members from participating in data sharing; (2) due to the sensitivity of remote sensing data, and the characteristics of big data, it is necessary to adopt a storage method with high security, to guarantee the safety of remote sensing data storage; (3) the adoption of a trusted data sharing mode to get rid of the complicated process and inefficiency caused by the need for intermediate organizations to summarize the traditional sharing mode; (4) data resources and data sharing records are traceable, to increase the possibility of recourse for data misuse.

2.2. Research on Data Storage Architecture of Blockchains

Compared with traditional databases, a blockchain also has many shortcomings in terms of performance. In terms of data storage, as all nodes in a blockchain system keep a copy of the blockchain, the increasing growth in data makes storage more and more difficult. To address this problem, researchers have proposed several expansion schemes, such as modifying the block capacity [21], converting the originally single-chain data structure to a directed acyclic graph (DAG) [22], or shifting complex computations and high-frequency transactions to be performed off-chain, and storing the final results on the blockchain. The modifications in block capacity and directed acyclic graphs are mainly improved from the blockchain architecture, to enhance the whole network's transaction processing capacity. However, this approach is mostly limited by the number of nodes and transactions in the network, with limited performance improvement, and it tends to exacerbate the risks of blockchain centralization and security attacks. One solution is to move computation and high-frequency transactions off-chain. This solution separates off-chain computation from on-chain storage. It can effectively improve blockchain performance, while guaranteeing a certain degree of decentralization. However, off-chain scaling faces problems, such as off-chain computation security and difficulty in supporting complex operations (e.g., smart contracts). Therefore, in-depth research on decentralization, security, and performance needs to be conducted in a specific study concerning the characteristics of remote sensing data and applications.

The traditional blockchain represented by Bitcoin introduces a single-layer chain structure in terms of blocks, which is used to guarantee the tamper-evident nature of data

on the chain. The block header and the block body, together, constitute a complete block. The block header stores the antecedent parent block hash, the transaction set Merkle root, etc., and the transaction data are stored in the block body. Currently, most blockchain systems are using single-chain architecture, such as the PoC project of the Japanese network bank, and the common ledger model of the European Central Bank.

With the increase in data stored on the blockchain, research has found that the single-chain architecture has corresponding bottlenecks, in terms of performance, capacity, privacy, and scalability, which are insufficient to manage the data, and a double-chain structure blockchain was invented, inspired by the DNA structure. The double-chain structure blockchain means that two chains can compute in parallel, and each chain can use different hardware; the double-chain structure not only maintains the characteristics of the original blockchain, but also improves the computing speed and scalability. In domestic and international research, according to the needs of each application, scholars have proposed their double-chain structure. To solve the characteristics of the single-chain structure without supervision and legal protection [23], G. Wu et al. [24] proposed a double-chain structure of a supervisory blockchain and transaction blockchain, to separate supervision and transaction. C. Xie et al. [25] proposed a dual-chain structure of a transaction blockchain and data blockchain for the blockchain-based tracking of agricultural products, which solved the security problem and ensured that the data would not be maliciously tampered with or destroyed. W. Ren et al. [26] used a combination of an ETH public chain and an agricultural sample data chain to improve the security level. S. Chen et al. [27] proposed a user blockchain and fog aggregation blockchain, again to enhance security. To alleviate the block data storage inflation problem, Shengqiao Gao et al. [28] established a double-chain structure of main and summary chains, which allows users to choose the appropriate storage mode according to their needs, which is also a more mainstream double-chain structure.

In some research, the constructed multiple blockchains are called a multi-chain structure, and rely on the multi-chain structure to solve problems that cannot be solved by one blockchain; that is, scaling, data sharing, security, etc. Polkadot [29] is a famous heterogeneous multi-chain framework, which is a system comprising a relay chain connecting multiple parallel chains, where the relay chain is responsible for consistency, and the parallel chain is responsible for validity. A multichain [30] implements multiple private chains running simultaneously, but the chains are isolated and independent from each other. A parallel blockchain [31], proposed by Yuan Yong and Feiyue Wang, is also a multi-chain structure that relies on the approach of parallel intelligence theory combined with blockchain technology to add practical computing power and more decision-making capability to the blockchain. Tsai et al. [32] proposed a new blockchain, "Beihang Chain", that combines an account blockchain (ABC) and transaction blockchain (TBC). Liang Hao [33] and others proposed a user blockchain, transaction blockchain, and agricultural information chain. The architectural form of the blockchain has become more and more flexible, and more suitable for each application. However, the existing multi-chain structure is not very good in terms of the consensus efficiency and transaction throughput, and it is not suitable for the storage of large data.

As the amount of file storage increases, the storage cost will also become more and more expensive. Moreover, the traditional blockchain combined with the centralized cloud storage platform data storage scheme has the risk of overstepping and tampering with the cloud storage platform. In this context, the Interplanetary File System (IPFS), a peer-to-peer network for storing and sharing data in a distributed file system, was born. The network uses content addressing to uniquely identify each file, a feature that is well-suited to distributed data storage. Therefore, many studies [34–36] use IPFS as the underlying data storage, in combination with a blockchain, to achieve the effect of storing shared big data in blockchain, to reduce the storage burden on the blockchain.

At present, in blockchain-based data management, most of the researches mainly focus on a single-chain structure, with which it is difficult to reach an effective balance between consensus efficiency, security, and cost. In particular, the research in the field of remote sensing does not make full use of the features of public, federated, and private chains according to the characteristics of the remote sensing industry. Meanwhile, the data throughput of a single-chain structure is low, and far from sufficient to support diverse remote sensing applications. Therefore, it is necessary to break through the blockchain performance constraint and propose a new blockchain structure, to support the on-chain demand of diversified remote sensing industries.

In summary, the application of blockchain technology in the field of geosciences is still in the nascent stage, mainly focusing on the exploration of applications in data copyright and data encryption, etc. These explorations show that the introduction of blockchain technology to the process of geosciences data sharing, to solve certain sharing problems, has good application prospects. However, the research on using blockchain technology for remote sensing data sharing is still extremely limited, and most studies are still in the exploration stage. In view of the above challenges, this study proposes using blockchain technology to overcome the challenges in data tampering detection, process documentation, process accuracy assessment, and privacy protection.

3. The Architecture of the System

3.1. Trusted Interoperability Service of Remote Sensing Data

The remote sensing information from imaging to remote sensing product output roughly goes through the following processes: remote sensing data acquisition, data processing, image processing, information extraction/fusion/integration, and product output, in which various errors are introduced, due to various influences, such as the operation and environment, and these errors will eventually produce uncertainties in the remote sensing products, including uncertainties in the remote sensing imaging mechanism, uncertainties in the processing process, and uncertainty in the information product evaluation.

The original intention of the remote sensing data trusted interoperability technology is to build a complete trust chain, from data acquisition to product production, in the entire remote sensing data processing system. Due to the non-objectivity of the actual operation, the remote sensing service itself may cause uncertainty and untrustworthiness in the results, due to different algorithm selections and process selections. Only through sorting out its scientific nature, can the origin and process of a remote sensing product image on the chain be explained, and then it can be mathematically deduced, and strictly and scientifically processed, to obtain credible results.

After remote sensing images are acquired from satellite sensors, they are shared, collaborated, and fused between data storage centers. The products are dependent on various parameters in the production process. Facing the same target, the results obtained via different processing operations show different reliability. Therefore, remote sensing data products should be combined with the complete parameters on their own chains, to promote and ensure the scientificity, traceability, and high reliability of the production results, and to provide more reliable information for user decision-making.

To address the above problems, in order to realize the requirements of traceability over the whole course of remote sensing data changes and information tamper-proofing, this paper will design and build an interoperable meta-information model. including the characteristics of the Earth observation data sources and the service records of the processing process, as shown in Figure 1.

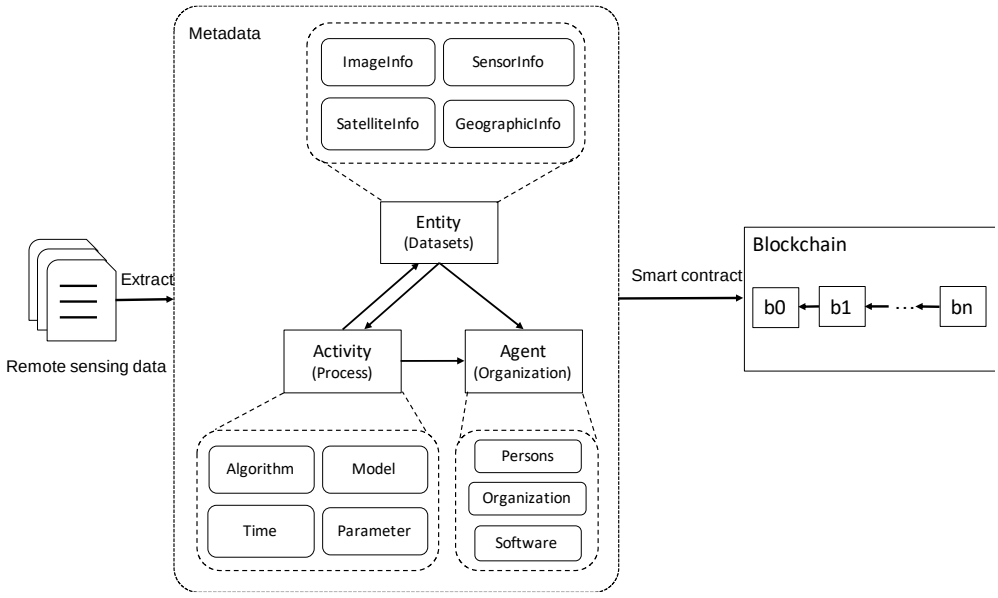

Figure 1. The interoperable meta-information model (own elaboration, based on PROV model [37]).

3.2. Architecture of Remote Sensing Data Sharing Model Based on a Multi-Level Blockchain

For a single-chain structure in current blockchain-based data management, it is difficult to reach an effective balance between consensus efficiency, security, and cost, and it is not suitable for big data storage. In this paper, we store the original data, data summary, and transaction data separately, study the multi-chain model suitable for remote sensing big data storage, and design multiple chains with a parallel execution, to achieve a high performance as well as a low protection cost, while ensuring data security and privacy security. In this paper, we study the combination method of public and federated chains, further conduct in-depth research on data storage methods in terms of security and performance, focus on the characteristics of remote sensing industry chains, and design a remote sensing blockchain with a high concurrency of transactions.

As the storage capacity of a blockchain is limited, and remote sensing data are large, with one datum needing to occupy hundreds of gigabytes of storage space, it is not very realistic to store all remote sensing data on the blockchain, and it could introduce a confidentiality risk. Therefore, in order to provide better on-chain data storage, this paper proposes storing remote sensing data under the chain, and building a data-sharing chain between the remote-sensing-data owners, which stores the hash value of the remote sensing data under the chain for on-chain storage, and ensures the consistency of the hash value of the remote sensing data stored by each remote-sensing-data owner based on the consensus mechanism of blockchain, to realize remote sensing sharing among the remote-sensing-data owners.

Combining the characteristics of remote sensing applications, this paper proposes a remote sensing data storage model based on a multi-chain structure combining a public chain and an alliance chain, and designs a three-layer blockchain storage architecture, including an IPFS storage layer, remote sensing industry alliance chain layer, and remote sensing open data public chain layer. Using the IPFS storage layer to store remote sensing raw data and remote sensing product data after processing is convenient for the management and processing of big data, and means that it is not easy to be attacked by others. As remote sensing data are highly specialized compared to general data, in addition to remote sensing image information, they also need to save their descriptive information regarding the remote sensing image data themselves, including spatial, spectral, and temporal dimension information, etc. They need to save metadata information, especially for easy searching. The information hash value is transmitted through the blockchain, and data transmission

and sharing are realized through IPFS, to achieve secure data sharing. The architecture diagram is shown in Figure 2.

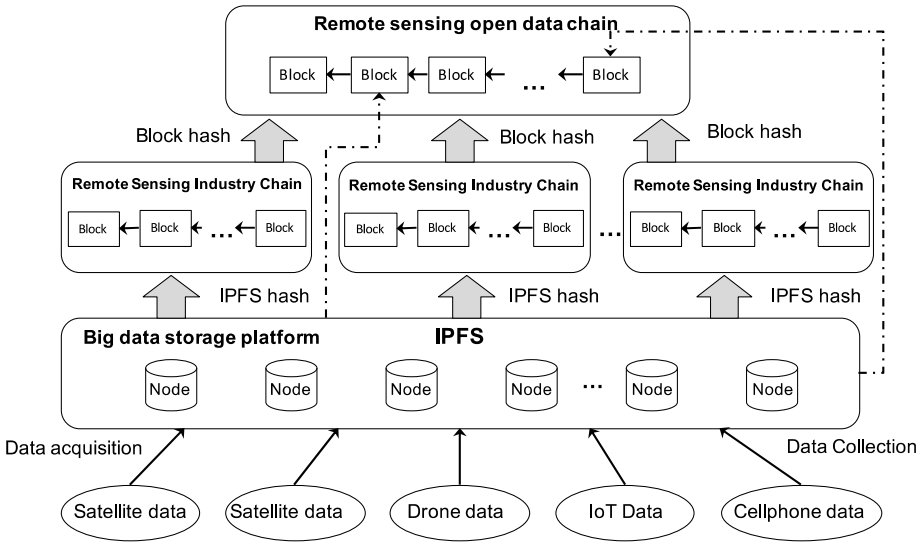

Figure 2. Multi-chain structure blockchain architecture (own elaboration).

The remote sensing industry chain needs to perform a parallel cut of data according to the needs of remote sensing application business functions, in order to achieve the business requirements and security requirements of data isolation. As each full node in the single chain in the current blockchain technology system owns all the data in the whole network, it cannot meet such application requirements. This paper designs a 1 + N multi-chain structure based on remote sensing application research, including a public chain and multiple independent alliance chains, which partition business logic and data processing, support the parallel processing of multiple transactions, and asynchronously write to the public chain transaction ledger after the transaction is completed.

Specifically, the Remote Sensing Open Data Chain (hereinafter referred to as RSOC), provides a content-based search for the public, and provides remote sensing products produced in the remote sensing alliance chain, such as flood monitoring maps, to the public, and the public provides open data based on incentive mechanisms, and accesses data based on smart contracts.

The Remote Sensing Industry Consortium Chain (hereinafter referred to as RSIC) is built on the basis of the public chain. The verified and game-tested remote sensing trust services are situated on the basic public chain, and each alliance chain is built on the basic public chain. There may be some private data and private deployment on the alliance chain, while there are open data on the public chain, and the data are mainly used for deposition and basic trust services.

The problem of trustworthy data interaction between different agency nodes and between the general public and remote sensing agencies must be considered when designing a multi-chain structure combining public and coalition chains. The specific idea is that the alliance chain combines related remote sensing data centers according to remote sensing applications, shares remote sensing raw data among the chains, and realizes the shared alliance among different remote sensing industry institutions, and nodes on the same chain maintain the same data, thus promoting the collaborative development of upstream and downstream users in the remote sensing industry chain. All organizations among the alliance chains share remote sensing metadata and transaction data, as well as consensus protocols and smart contracts, but do not share raw data between chains, in order to protect data privacy. Each alliance chain ensures the integrity and traceability of a remote sensing industry chain, and the alliance chains interact with each other through public chains.

Each chain consists of different nodes, and the nodes on the same chain maintain the same data, while the nodes on different chains maintain different data, so that the data on different chains are isolated from each other. At the same time, the nodes in the system can join different chains, according to their own working needs, and then, that node will only synchronize the data on the relevant chain. Such a storage method can reduce, to a greater extent, the number of data that nodes in the system need to synchronize and store, shorten the time consumption required for data synchronization, and reduce the storage space required for data storage. The data on different federated chains are isolated from each other, which can realize the data concurrent operation of different chains, and improve the system concurrency.

IPFS can assist different blockchain networks in transferring information and files. The multi-chain structure combining public chain and federated chain can break through the function and performance constraints of a single chain, and has a good performance of high concurrent transactions, while taking into account the isolation and protection of privacy data, to meet the diversified business needs in the remote sensing field.

3.3. Block Data Structure Serving Large-Scale Remote Sensing Applications

For different remote sensing data providers with different requirements for data security, suitable blockchain data structures are designed for multi-chain structures, respectively. This study constructs a new data structure in the blockchain as a prerequisite basis for remote sensing data storage and sharing.

In view of current problems, such as large differences in the quality of Earth observation information products, and no unified evaluation index of information products for domain applications, we study the block storage model based on the open and recordable features of access to data, and operation process information under the interoperable environment, and form an efficient and distributed blockchain storage scheme for remote sensing data, to ensure security and efficient access to data. Blockchain technology can make the data in the blockchain more valuable. By multiple nodes participating in data recording together and verifying the accuracy and validity of their information with each other, they can achieve the all-around confirmation and verification of information, thus eliminating uncertainty and reaching consensus.

The blockchain stores the data storage records of different users and the data storage addresses on IPFS, and the stored records are guaranteed not to be tampered with, as they generate unique hash values through hash functions. This study analyzes the remote sensing data storage aspect and proposes a generic block data structure, to store the related data with state attributes and remote sensing attributes, and to query them based on the uniqueness of the path.

The raw remote sensing data are stored on IPFS, and when the file is uploaded to the IPFS node for storage, the node will organize the file in the Merkle Directed Acyclic Graph (Merkle DAG) format for block storage and, after the storage is completed, the file will be represented by the root hash number of the Merkle DAG, and the user can build the network from IPFS via Distributed Hash Table (DHT) Get the file. Through hashing the recorded data blocks and storing the hash values in the blockchain, there is no need for nodes to have massive storage space. Once the content is modified, the corresponding hash value will also change, and cannot be matched with the hash value in the blockchain, ensuring the unmodifiability of the content. The hash value ensures that the data are trustworthy and has not been tampered with, so that accurate backtracking can be achieved, and the property rights of the data are guaranteed.

As remote sensing data have a strong professionalism compared with general data, in addition to remote sensing image information, they also needs to save their descriptive information of the remote sensing image data themselves, including spatial, spectral, and temporal dimensional information, etc. They need to save metadata information, especially for easy finding; through metadata, we can easily query the remote sensing data we want to access, without exposing confidential data at the same time. Therefore, we divide the

remote sensing raw data into two files, remote sensing image data, and metadata, and perform a hash calculation on them separately.

In the multi-chain structure designed in Section 3.2, the public chain is used as the main chain to store the remote sensing open data and the summary of the federated chain blocks. Considering the different identities of the data providers, the remote sensing data center should provide a data-sharing platform between them, to facilitate collaborative operations, while the open data providers should ensure data trustworthiness, and data privacy protection, to solve the problems of mutual trust, and data authenticity and confidentiality. As shown in Figure 3, this paper divides the public chain blocks into two types; one is to record the various transaction data in the alliance chain, which are recorded as Class A blocks. At the same time, because it is a public chain, the data are all public, which is convenient for transactions between various alliance chains through the public chain, which is obtained via the synchronization of the alliance chains; the other type is the class B block, which is obtained by the general public after they have submitted open data.

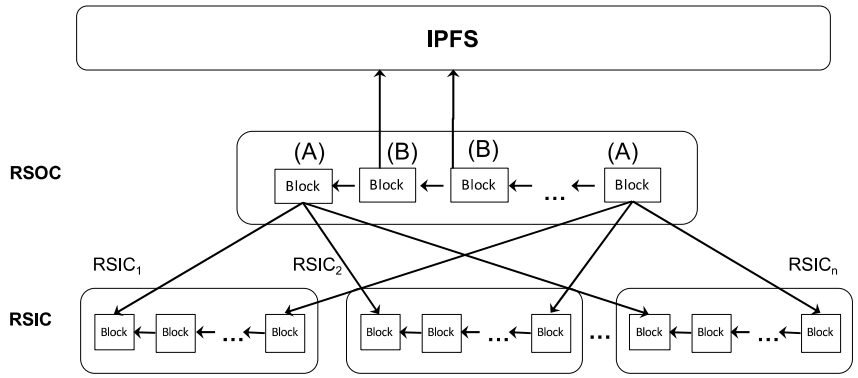

Figure 3. Block data structure (own elaboration).

The data storage structure of this blockchain system is based on the design idea of Ethernet. The remote sensing information blocks form a chain structure in a linear way, consisting of a block header and a block body.

The data block of the public chain is referred to as the main chain block, and the main chain block body includes the ledger transaction data and the IPFS hash value of the telemetry metadata. The public searchable data recorded by the transaction data with storage incidentally store information, such as the serial number of the coalition chain where the corresponding telemetry data are located, the block height, and the block hash value of the block where the data are located in the coalition chain.

The federation chain maintains the actual transactions in each chain, and the data block is called the slave chain block. The IPFS hash value in the block body contains the hash value of the remote sensing data block, and the hash value of the remote sensing metadata.

4. Experiment

In this section, we provide experimental simulations for the system proposed in this paper. The evaluation was performed on an Ubuntu 20.04 system, with a Core i5 CPU and 8GB RAM. The network speed is 50 Mbps. We accessed IPFS through the browser front-end, uploaded remote sensing pictures, and transferred the hash generated via IPFS to the blockchain through the web and node.js servers, and the hash data were stored in the blockchain through smart contracts.

The solution proposed in this paper uses the RSIC, RSOC blockchain, and IPFS network. The specific blockchain in this article is built using Geth (go-ethereum). The parts related to smart contracts are written via solidity.

4.1. Data Upload Efficiency

In the prototype system designed in this paper, the remote sensing data are successfully uploaded to IPFS and the blockchain. The data upload time to IPFS storage is shown in the Figure 4.

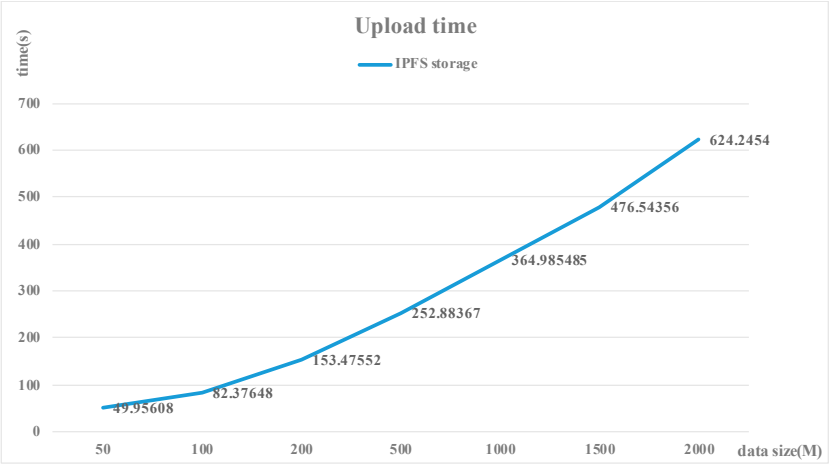

Figure 4. The upload time of remote sensing data to IPFS (own elaboration).

The main chain in multiple blockchains is Ethereum, which provides a content-based public search. The secondary chain is built for a specific remote sensing data production application system. Firstly, a large number of remote sensing data are transmitted to IPFS. The IPFS network stores the entire set of data received, while redirecting the data to the consortium chain: RSOC. Secondly, the RSOC chain stores hashes and metadata in blocks and generates RSOC block hashes. Finally, the block hash that can be made public is uploaded to the Ethereum main chain and stored in the block.

4.2. Data Provenance

Another important goal of this system is to complete the traceability of data. From the metadata stored in the block, the remote sensing image data on IPFS can be obtained. In this section, we show the results of using the Remix IDE [38] to achieve provenance. Remix is an IDE that allows us to create, compile, and deploy smart contracts. It also provides an environment for executing transactions and interacting with smart contracts. Firstly, we use Remix to create and deploy our smart contract. To interact with this smart contract, we use the Web3 Provider to connect Remix with our blockchain. In Figure 5, we display the produced remote sensing product information, using Remix.

Smart contracts play a crucial role in facilitating and automating various aspects of remote sensing data sharing and information services within a blockchain framework. Firstly, developers need to define a smart contract that includes attributes, permission rules, and transaction rules related to remote sensing data. Data providers register their data through the smart contract and store descriptive information and relevant attributes within the contract. This may include the data source, time range, resolution, and other details. Data consumers publish their specific requirements for remote sensing data through the smart contract. Once the attributes and rules between data providers and consumers are automatically matched, the contract will execute the data transaction. This process is supervised and recorded. Through the leveraging of smart contracts, remote sensing data sharing and information services can be automated, streamlined, and made more efficient. Smart contracts bring transparency, immutability, and trust to the data sharing process, creating a secure and reliable environment for stakeholders to collaborate and exchange data within a blockchain network.

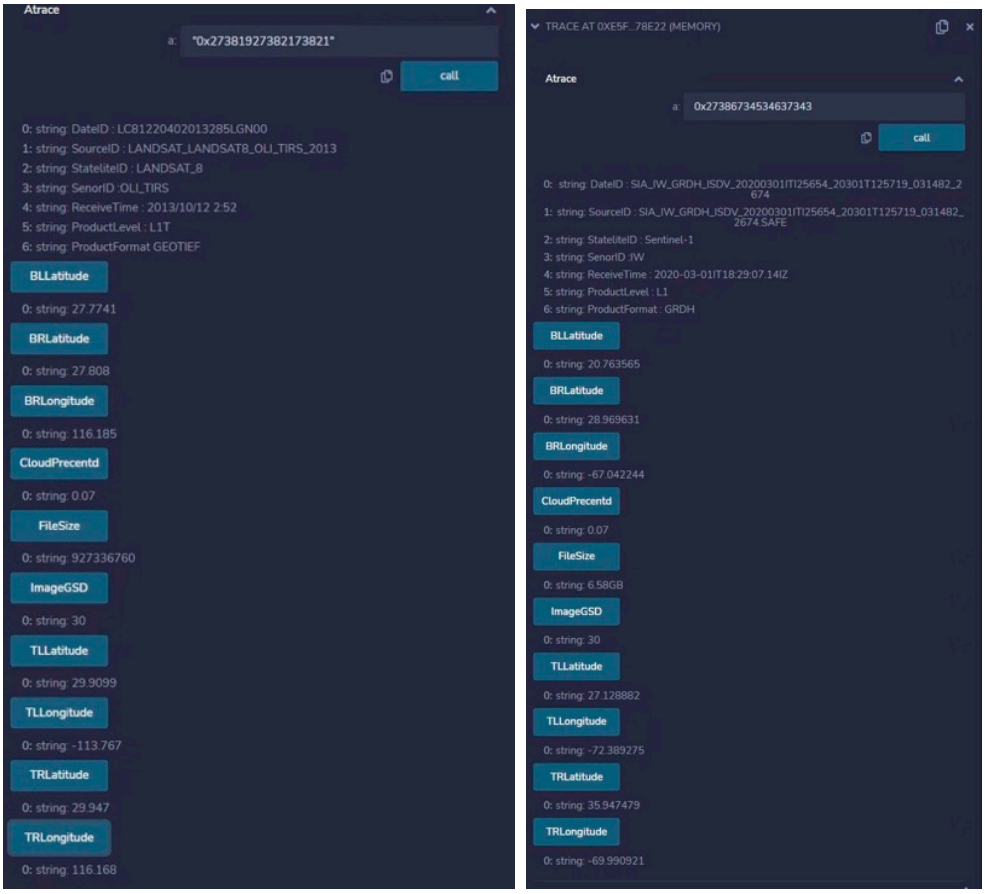

Figure 5. We read remote sensing data information using Remix (own elaboration).

Formal verification methods refer to a special mathematical-based technique used in the field of computer science, especially in software engineering and hardware engineering. These methods are employed to specify, develop, and verify software and hardware systems, in order to enhance their security, reliability, and robustness. In the context of smart contracts, formal methods can be applied to verify the correctness of the contract code, assisting in preventing costly errors and security breaches. Through the explicit definition of the requirements and specifications of smart contracts, and the use of formal methods with descriptive languages, the functionality of the system can be ensured. Formal analysis methods describe functions that can be used to verify programs. Formal methods employ property specifications to define the properties and requirements that the system should satisfy, ensuring the system's compliance with expected behavior. Formal verification tools are used to check if the contract model satisfies the predefined property specifications. These tools can automatically or semi-automatically detect potential errors, conflicts, or inconsistencies. Finally, based on the results of formal verification, necessary fixes and improvements can be made. [39,40]

4.3. Security and Availability

The remote sensing data trusted and traceable storage system designed in this paper is more secure than the traditional system. As mentioned above, traditional remote sensing data storage is a centralized technology based on cloud computing or cluster computing. Once the central server is destroyed, the data in it will be tampered with and destroyed. Although the public chain is a completely decentralized technology, its upload and download performance is slow, meaning that it is difficult to meet the throughput of large-scale data in global monitoring applications. At the same time, participation in the consensus process by people unrelated to the production process of a particular remote

sensing product is redundant. Although the upload and download speed of the alliance chain is greatly improved compared with the public chain, incomplete decentralization means that it is constrained by the central node, and the network also has hidden dangers, such as witch attacks.

Therefore, this paper considers a hybrid chain design method, and the multi-chain structure, IPFS storage network, and Ethereum technology jointly build a more reliable remote sensing data sharing system. This is mainly because: (1) The availability of the prototype system benefits from the ability to store various remote sensing data. Remote sensing images are stored separately on IPFS, and their stored hash values are stored in blocks together with metadata, which not only protects the data privacy, but also ensures user interaction with the system. (2) The designed RSIC and RSOC hybrid chain transmits data through IPFS and is applied to the remote sensing data sharing network. The hash value transmitted by IPFS is stored in RSIC, and the public product data hash block on RSIC is uploaded to RSOC, and the security is verified through the comparison of the hash value. (3) All transactions are recorded and stored in the immutable ledger of the blockchain, thus providing a high degree of transparency and traceability for the production of each datum in a secure, trusted, reliable, and efficient manner. (4) The "IPFS + blockchain" method not only retains the advantages of the decentralization and security of the blockchain, but also solves the long-standing problem of scalability, and can store remote sensing big data.

5. Discussion

The paper discusses the potential benefits of using blockchain technology for remote sensing data sharing, and it is important to consider the potential drawbacks and limitations of using blockchain technology for remote sensing data sharing. Here are some key points to consider:

Scalability: Blockchain technology faces scalability challenges, particularly when dealing with large-scale remote sensing datasets. The decentralized nature of blockchains requires every node in the network to process and store a copy of the complete blockchain. This can result in increased storage requirements and slower transaction processing times as the numbers of data grow, potentially hindering real-time data sharing and analysis.

Computational Complexity: Blockchain transactions involve complex consensus algorithms, cryptographic operations, and validation processes. These operations require substantial computational resources, including processing power and energy consumption. Handling large volumes of remote sensing data on a blockchain could lead to significant computational complexity and may require powerful computing infrastructure.

Regulatory and Legal Concerns: Blockchain technology operates across borders, which raises regulatory and legal considerations. Compliance with data protection regulations, intellectual property rights, and any restrictions on data sharing in specific regions needs to be carefully addressed. Ensuring compliance with local laws and regulations while utilizing a blockchain for remote sensing data sharing may present challenges.

Addressing these challenges and limitations will be critical for the successful implementation of blockchain technology in the context of remote sensing data sharing. A careful evaluation of trade-offs, and the consideration of alternative approaches are required to mitigate these limitations, while still harnessing the potential benefits offered by blockchain technology.

Currently, we have conducted some prototype experiments in the Asia Oceania GEO (AOGEO) data hub project. These experiments focused on data transmission, traceability, and security. These experiments serve as an initial exploration within these areas. Moving forward, it is likely that further experimentation will be conducted in various other projects to broaden our understanding and application.

6. Conclusions

In this paper, we propose a data storage security solution for remote sensing products based on multiple blockchains, that provides an accountable and distributed storage

environment for storage participants. Firstly, the storage structure of the block is proposed as a trusted representation of shared data. Then, a data model for sharing data requests and services based on a blockchain is proposed, which makes data sharing more credible. Finally, through the Ethereum blockchain platform, the prototype system is designed and simulated. Multi-chain solutions with IPFS storage solve the problems of storage centralization, the centralized verification of data integrity, and denial of service in cloud storage scenarios. They offer a higher level of security than traditional cloud storage and Ethereum. Our implementation and evaluation of the prototype system show that it is a highly viable solution in terms of the data storage speed, traceability, security, and availability. The storage scenario in this paper still has a few challenges; for example, data could be encrypted for further security.

Author Contributions: Conceptualization, Q.Z. and Z.B.; Methodology, Q.Z. and W.Y.; Software, Q.Z. and Z.B.; Validation, W.Y.; Formal Analysis, Q.Z. and W.Y.; Investigation, Q.Z.; Resources, Q.Z. and Z.B.; Data Curation, W.Y. and Q.Z.; Writing—Original Draft Preparation, Q.Z.; Writing—Review and Editing, Z.B. and W.Y.; Visualization, Z.B.; Supervision, Z.B. and W.Y.; Project Administration, Q.Z. and Z.B.; Funding Acquisition, W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China, grant number 2021YFE0117300.

Data Availability Statement: The data for this study are available within the. Data used in this study were derived from the following resources that are available in the public domain: [Geospatial data cloud, Computer Network Information Center, Chinese Academy of Sciences: https://www.gscloud.cn/sources accessed on (23 May 2023)].

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. Li, G.Q.; Zhang, H.Y.; Zhang, L.C.; Wang, Y.Y.; Tian, C.Z. Development and trend of Earth observation data sharing. *J. Remote Sens.* **2016**, *20*, 979–990. [CrossRef]
2. Gscloud. Geospatial Data Cloud. Available online: http://www.gscloud.cn (accessed on 23 May 2023).
3. Sasclouds. Natural Resources Satellite Remote Sensing Cloud Service Platform. Available online: http://sasclouds.com/chinese/home (accessed on 23 May 2023).
4. Eurpean Space Agency(ESA). Copernicus Open Access Hub. Available online: https://scihub.copernicus.eu/ (accessed on 23 May 2023).
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 23 May 2023).
6. OGC DWG. Available online: https://www.ogc.org/projects/groups/bdltdwg (accessed on 23 May 2023).
7. Eurpean Space Agency (ESA). Blockchain and Earth Observation. Available online: https://eo4society.esa.int/wp-content/uploads/2019/04/Blockchain-and-Earth-Observation_White-Paper-April-2019.pdf (accessed on 23 May 2023).
8. Mandl, D. Bitcoin, Blockchains and Efficient Distributed Spacecraft Mission Control. Available online: https://ntrs.nasa.gov/api/citations/20170009470/downloads/20170009470.pdf (accessed on 23 May 2023).
9. Pincheira, M.; Donini, E.; Giaffreda, R.; Vecchio, M. A Blockchain-Based Approach To Enable Remote Sensing Trusted Data. In Proceedings of the IEEE Latin American GRSS & ISPRS Remote Sensing Conference (LAGIRS), Santiago, Chile, 22–26 March 2020; pp. 652–657. [CrossRef]
10. Cedeno Jimenez, J.R.; Zhao, P.; Mansourian, A.; Brovelli, M.A. Geospatial Blockchain: Review of decentralized geospatial data sharing systems. *AGILE GIScience Ser.* **2022**, *3*, 29. [CrossRef]
11. FOAM. FOAM. The Consensus Driven Map of the World. Available online: https://foam.space/publicAssets/FOAM_Whitepaper.pdf (accessed on 23 May 2023).
12. Leka, E.; Lamani, L.; Selimi, B.; Deçolli, E. Design and Implementation of Smart Contract: A Use Case for Geo-Spatial Data Sharing. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electron, Microelectron (MIPRO), Opatija, Croatia, 20–24 May 2019. [CrossRef]
13. Zhao, P.; Cedeno Jimenez, J.R.; Brovelli, M.A.; Mansourian, A. Towards geospatial blockchain: A review of research on blockchain technology applied to geospatial data. *AGILE GIScience Ser.* **2022**, *3*, 71. [CrossRef]

14. Mendi, A.; Demir, Ö.; Sakakli, K.; Cabuk, A. A New Approach to Land Registry System in Turkey: Blockchain-Based System Proposal. *Photogramm. Eng. Remote Sens.* **2020**, *86*, 701–709. [CrossRef]
15. Khatri, Y. IBM Blockchain Assists Groundwater Pilot in Drought-Prone California. Available online: https://www.coindesk.com/ibm-blockchain-assists-groundwater-pilot-in-drought-prone-california (accessed on 23 May 2023).
16. Yohan, H.; Byungjun, P.; Jongpil, J. A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications. *Procedia Comput. Sci.* **2019**, *155*, 728–733. [CrossRef]
17. Torun, A. Hierarchical Blockchain Architecture for a Relaxed Hegemony on Cadastre Data Management and Update: A Case Study for Turkey. Uctea International Geographical Information Systems Congress. Available online: https://www.researchgate.net/publication/321485252_Hierarchical_Blockchain_Architecture_for_a_Relaxed_Hegemony_on_Cadastre_Data_Management_and_Update_A_Case_Study_for_Turkey (accessed on 23 May 2023).
18. Zhang, M.D.; Gao, Z.J. A discussion of blockchain application in the intellectual property protection of geological big data. *China Min. Mag.* **2019**, *28*, 9–14. [CrossRef]
19. Zou, Q.; Li, G.Q.; Yu, W.Y. MapReduce functions to remote sensing distributed data processing—Global vegetation drought monitoring as example. *Softw. Pract. Exp.* **2018**, *48*, 1352–1367. [CrossRef]
20. Jing, G.F. Analysis on Remote Sensing Credibility and Trusted System Interoperability. *Remote Sens. Inf.* **2020**, *35*. [CrossRef]
21. BIP. Bitcoin Improvement Proposals. Available online: https://github.com/bitcoin/bips (accessed on 23 May 2023).
22. COTI. Currency of the Internet. Available online: https://github.com/coti-io (accessed on 23 May 2023).
23. Wasim, M.U.; Ibrahim, A.A.Z.A.; Bouvry, P.; Limba, T. Law as a service (LaaS): Enabling legal protection over a blockchain network. In Proceedings of the 2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT, Irbid/Amman, Jordan, 9–11 October 2017. [CrossRef]
24. Wu, G.F.; Yu, P.; Wang, K.K. Transaction regulatory research on double-chain blockchain. *Comput. Eng. Appl.* **2020**, *56*, 116–123. [CrossRef]
25. Xie, C.; Sun, Y.; Luo, H. Secured data storage scheme based on block chain for agricultural products tracking. In Proceedings of the 2017 3rd International Conference on Big Data Computing and Communications, Chengdu, China, 10–11 August 2017. [CrossRef]
26. Ren, W.; Wan, X.T.; Gan, P.C. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Future Gener. Comput. Syst.* **2021**, *117*, 453–461. [CrossRef]
27. Chen, S.; Yang, L.; Zhao, C.; Varadarajan, V.; Wang, K. Double-Blockchain Assisted Secure and Anonymous Data Aggregation for Fog-Enabled Smart Grid. *Engineering* **2020**, *8*. [CrossRef]
28. Gao, S.Q.; Liu, X.L.; Gao, Y.P. Optimized model of dual-chain storage of food supply chain data based on blockchain. *FoodMachinery* **2020**, *36*, 63–70. [CrossRef]
29. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. White Paper. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 23 May 2023).
30. Multichain. Available online: http://www.multichain.com/ (accessed on 23 May 2023).
31. Yuan, Y.; Wang, F.Y. Parallel blockchain: Concept, methods and issues. *Acta Autom. Sin.* **2017**, *43*, 1703–1712. [CrossRef]
32. Tsai, W.T.; Blower, R.; Zhu, Y.; Yu, L. A system view of financial blockchains. In Proceedings of the 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), Oxford, UK, 29 March–2 April 2016; pp. 450–457. [CrossRef]
33. Liang, H.; Liu, S.; Zhang, Y.; Lv, K. Multi-blockchain application technology for agricultural products transaction. *Smart Agric.* **2019**, *1*, 72–82. [CrossRef]
34. Hoffman, A.; Becerril-Blas, E.; Moreno, K.; Kim, Y. Decentralized security bounty management on blockchain and IPFS. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 6–8 January 2020. [CrossRef]
35. Reen, G.; Mohandas, M.; Venkatesan, S. Decentralized patient centric e-Health record management system using blockchain and IPFS. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019; pp. 1–7. [CrossRef]
36. Tiwari, A.; Batra, U. IPFS enabled blockchain for smart cities. *Int. J. Inf. Technol.* **2021**, *13*, 201–211. [CrossRef]
37. Gao, Y.; Chen, X.; Du, X. A Big Data Provenance Model for Data Security Supervision Based on PROV-DM. *Model IEEE Access* **2020**, *8*, 38742–38752. [CrossRef]
38. Remix. Remix—Ethereum IDE. Available online: https://remix.ethereum.org (accessed on 23 May 2023).
39. Krichen, M.; Lahami, M.; Al–Haija, Q.A. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022. [CrossRef]
40. Abdellatif, T.; Brousmiche, K. Formal Verification of Smart Contracts Based on Users and Blockchain Behaviors Models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018. [CrossRef]