A Decentralized Model for Spatial Data Digital Rights Management

Yun Zhang [1,2,3,*], Zhi Tang [1,2] (iD), Jing Huang [1,2], Yue Ding [1,2], Hao He [1,2], Xiaosheng Xia [1] and Chunhua Li [4]

[1] School of Geography and Tourism, Anhui Normal University, Wuhu 241000, China; tangzhi0923@mail.ahnu.edu.cn (Z.T.); jinghuang@mail.ahnu.edu.cn (J.H.); yuedi012@mail.ahnu.edu.cn (Y.D.); hehao0121@mail.ahnu.edu.cn (H.H.); xiaoshengxia@mail.ahnu.edu.cn (X.X.)

[2] Engineering Technology Research Center of Resources Environment and GIS, Wuhu 241000, China

[3] Laboratory of Natural Disaster Process and Prevention Research of Anhui Province, Wuhu 241000, China

[4] School of Resources and Environmental Engineering, Anhui University, Hefei 230601, China; chunhuali@stu.ahu.edu.cn

* Correspondence: zy2009@mail.ahnu.edu.cn

check for updates

Abstract: The copyright of data is a key point that needs to be solved in spatial data infrastructure for data sharing. In this paper, we propose a decentralized digital rights management model of spatial data, which can provide a novel way of solving the existing copyright management problem or other problems in spatial data infrastructure for data sharing. An Ethereum smart contract is used in this model to realize spatial data digital rights management function. The InterPlanetary File System is utilized as external data storage for storing spatial data in the decentralized file system to avoid data destruction that is caused by a single point of failure. There is no central server in the model architecture, which has a completely decentralized nature and it makes spatial data rights management not dependent on third-party trust institutions. We designed three spatial data copyright management algorithms, developed a prototype system to implement and test the model, used the smart contract security verification tool to check code vulnerabilities, and, finally, discussed the usability, scalability, efficiency, performance, and security of the proposed model. The result indicates that the proposed model not only has diversified functions of copyright management compared with previous studies on the blockchain-based digital rights management, but it can also solve the existing problems in traditional spatial data infrastructure for data sharing due to its characteristics of complete decentralization, mass orientation, immediacy, and high security.

Keywords: distributed spatial data management; Spatial data infrastructure; Spatial data sharing; Blockchain; smart contract

1. Introduction

Spatial data are the core of geographic information science. Many international organizations and countries have established some scientific data sharing platforms, such as the US Oak Ridge National Laboratory Distributed Archive Center [1], China National Earth System Science Data Sharing Infrastructure [2], and Group on Earth Observations' Global Earth Observation System of Systems [3], to provide more spatial data to geoscientists. These infrastructure platforms provide good scientific data support for the development of geographic information science. However, some infrastructure platforms encourage researchers who use the spatial data of the platforms to share their research results with the platforms to promote the concept of data sharing from the national level to the individual

level. This spatial data sharing method had not been well applied, because data sharing without explicit copyright might lead to piracy of results.

In recent years, the enthusiasm and initiative of researchers to open and share spatial data in journals has been increasing. One benefit of this is that an increasing amount of scientists and publishers are aware of the advantages and necessity of open source research. The other advantage is based on the fact that scientific data publishing can solve the problem of spatial science data copyright in a better way. Spatial science data publishing refers to the simultaneous publication of results data by researchers when publishing a paper. The publisher will establish the correspondence between the paper and the data and, at the same time, the publisher uses a certain data protection statement to protect the published data. These infrastructure platforms allow for the authors of the academic papers to publish the data used and produced in their paper to a website for sharing, with explicit copyright ownership. The Data Science Journal established by the Committee on Data for Science and Technology, Earth System Science Data published by Copernicus Publications, and the Journal of Global Change Data & Discovery founded by the Institute of Spatial Sciences and Natural Resources Research are examples of such platforms. Digital rights management (DRM) refers to the techniques that are used by publishers to control the rights of protected objects [4]. Subsequently, the process of publishing spatial science data can be described as applying digital rights management to data sharing to solve the copyright problem of spatial science data. Since existing scientific data publishing schemes all use traditional digital rights management technology, these schemes have both their own shortcomings and shortcomings in traditional digital rights management technology, mainly including: (1) They are aimed at scientific data produced in scientific research papers, and non-scientists are basically unable to participate, which limits the scope of data sharing; (2) The application process is cumbersome in traditional digital rights management, the copyright registration takes a long time, and the review process is expensive. Moreover, the publication of the paper needs periodic review in spatial data publishing schemes, which increases the time cost of data sharing; (3) At present, most of the scientific data publishing systems are centralized, thus, if the server in the system fails, it will cause temporary or permanent inability to access services and data, which will cause immeasurable losses to both publishers and users; and, (4) The centralized digital rights management system has the risk of illegal tampering with copyright registration information that is caused by internal actors (such as a database administrator) and external actors (such as a hacker). It has been proven that blockchain technology can solve the above problems well.

Blockchain technology is essentially a distributed database technology [5] and it is one of the underlying technologies used in the Bitcoin. In 2008, Satoshi Nakamoto described the Bitcoin system in his paper [6] and implemented it in 2009. Since then, the bitcoin has become increasingly popular around the world. People have different opinions on the bitcoin, however, the blockchain technology behind bitcoin has received increasing attention and many scholars have begun to study this technology. Blockchain has not yet formed a unified definition in the industry, but the description of blockchain is basically similar in most studies [7–12]. We regard blockchain technology as a chained data structure, in which multiple data sets are arranged in chronological order. Cryptography, probability theory, and timestamp are used in these data sets to ensure that the data cannot be tampered with or forged. It is ensured that there is always a recognized and verifiable correct ledger in the entire network by attaching certain data generation rules to the data structure through the consensus mechanism, so that the ledger maintained by each node in the decentralized network is always consistent with the ledger maintained by other nodes in the network. Blockchain technology partly uses the consensus mechanism to ensure data consistency, and uses cryptography, probability theory, and timestamp techniques to ensure data security, hence allowing for trusted communication and information exchange between any nodes in the network without the need of a third-party trust authority. These characteristics indicate that blockchain technology has the advantages of complete decentralization, security, and tamper resistance. Due to its advantages, blockchain technology is considered by scholars to be useful in many fields, such as finance [13], supply chains [14], energy [15], medicine [16], real estate [17],

and copyright protection [18]. However, blockchain technology is largely aimed at decentralizing transactions between nodes in the Bitcoin system. If we want to apply blockchain technology to more fields, we need a more suitable medium, that is, the smart contract.

American computer scientist and cryptographer Nick Szabo first proposed the concept of the smart contract in 1994, defining it as "a computerized transaction protocol that enforces contract terms" [19]. The goal is to embed smart contracts in digital devices to significantly reduce the demand for third-party trust institutions in the execution of ordinary contracts. However, this concept was limited to the social environment and demand scenarios at that time and had not been widely used. People discovered that the main features of blockchain technology enable smart contracts to be perfectly applied in blockchain; hence, smart contracts have begun to show their powerful ability as a result of the birth of blockchain technology. In fact, the Bitcoin system already has smart contract function which is a bitcoin script based on the bitcoin bytecode language. Since the bytecode language is not a Turing-complete high-level language, it can only perform some operations that are based on the stack structure, which makes it impossible to perform complex operations, such as implementing loop statements [20]. As such, early smart contracts that are based on bitcoin systems can rarely contain complex logical structures. American programmer Vitalik Buterin proposed the concept of the Ethereum [21] in an attempt to solve both the problem of symbolic unity in Bitcoin and the problem of the bitcoin scripting language not having the ability to build a more advanced smart contract application. Ethereum has given a new definition to the term 'smart contract' that was proposed by Nick Szabo, and it has integrated Turing's complete smart contract programming language into the system, so that smart contracts with complex logic and diverse functions can be developed on the Ethereum blockchain. The Ethereum Virtual Machine (EVM) is the core of the Ethereum blockchain. Smart contracts that are deployed in the Ethereum blockchain are converted to bytecode input to run in the EVM [22], which supports high-level programming languages, such as Solidity (JavaScript-like) and Vyper (Python-like). EVM has greatly facilitated the development of smart contracts, decentralized applications, and made Ethereum become the most popular smart contract development platform in a short time. See the Ethereum Yellow Paper for more information on Ethereum principles.

It is not enough to conduct a completely decentralized system that is more complicated than the Bitcoin system through blockchain technology and smart contract technology, because the problem of data repository needs to be considered in general system design. For instance, the traditional centralized DRM system might use a central data server as a data repository to store and manage digital content. Server attacks or failures may lead to major problems, such as data loss, which is the main drawback of the traditional centralized system. In the blockchain system, data will be written to the blockchain along with the block to achieve the purpose of decentralized storage. However, the network bandwidth is limited. The larger the block capacity, the more data are carried in the network, and the slower the transmission speed of the network, hence reducing the operating efficiency of the entire blockchain system. In addition, the larger the block, the faster the growth rate of the data volume of the entire blockchain system. The cost of running a full node that stores all of the block data is getting higher and higher, which leads to a decrease in the number of full nodes in the system and risks the system becoming more centralized. The total size of the Bitcoin system has grown to 240 GB in the decade to date, although the Bitcoin system was originally designed to limit the block size to 1 MB. It can be seen that the amount of data that can be stored in the block is very limited. Spatial data have the characteristics of large data volume; hence, it is impossible to directly write spatial data into blockchain to achieve the purpose of decentralized storage. Therefore, a decentralized file storage system is needed for solving the storage problem of large files. The InterPlanetary File System (IPFS) [23] is an open source, peer-to-peer, content addressed, decentralized file system that can combine global computers to form a super file storage space, which enables the IPFS to have sufficient capacity to store large files and digital content. Each time that the IPFS receives a file, it will conduct a multiple hash calculation of Base58 encoding of the file to generate a unique hash value in the whole network as the file identifier. The generated hash value will be completely different after the file has been modified,

even if the file has only been changed a little bit. The node can access the corresponding file in the IPFS by the hash value. See the paper written by Benet for more information about the IPFS [23].

At present, many scholars used blockchain technology and IPFS technology to carry out related research on digital copyright protection. Kishigami et al. [24] introduced a super high definition video copyright management system that was based on blockchain, which allowed for the copyright owner to manage the user's license status at any time. However, the system only had two kinds of copyright management operations: authorization and stop authorization. Rinaldi [25] proposed a digital copyright management system while using blockchain. In this system, the Ethereum blockchain was used to manage copyright information, and a P2P file distribution system, which, similar to BitTorrent, was used to deliver the digital content. However, the method did not completely solve the problem of data loss caused by a single point failure. Meng et al. [26] designed an image copyright management system while using digital watermarking and blockchain technology. In the system, blockchain was used to securely store watermark information, copyright information, and digital content were stored in the InterPlanetary File System. Ma et al. [27] proposed a novelty digital copyright management trust model that was based on blockchain, namely DRMChain, which had reliable copyright protection capability and flexible external storage of decentralized digital content. However, the above two models lack the diversified copyright management functions, such as copyright information query or copyright transaction. In addition, some scholars have carried out related research on the application of blockchain technology in the protection of spatial data. Frey et al. [28] proposed a novel method for ensuring the secure sharing of geospatial wildlife data. This method uses blockchain technology to capture and log user query records and data server response records to enable effective post-event verification and accountability. Boulos et al. [29] discussed the application of blockchain technology in geospatial tagging data. They pointed out that the immutability of blockchain technology allows for the system to accurately construct real-world geographic events through proof of location, and a blockchain-style crowdsourced geographic information platform allows for the nodes to have full control over their own data, thus reducing the cost of data acquisition. Matney [30] states that the inherent characteristics of geospatial blockchain technology can make a privacy layer in the underlying architecture of web mapping applications in the era of intelligent web mapping. For example, geospatial blockchain technology can significantly improve data security when using identity information data for highly sensitive webpage mapping applications. These studies prove that blockchain technology can effectively protect data security, and effectively promote data sharing.

Inspired by previous research and, in order to solve the existing problems of digital rights management of spatial data in the spatial data infrastructure for data sharing, we believe that a digital rights management platform oriented to the public, that is instant, high-security, and decentralized, is needed. In this paper, we propose a spatial data digital rights management model (GDRM-OM) while using the advantages of blockchain technology, smart contract technology, and IPFS technology. This model is based on blockchain technology for establishing a decentralized spatial data digital rights management method in a peer-to-peer network that does not require a third-party trust organization to present an innovated spatial data infrastructure for data sharing. The digital content is stored in the IPFS to solve the data security problem of the traditional DRM system. The hash value of the digital content is stored as a field in the spatial data copyright information in the blockchain, thereby establishing correspondence between the copyright information and the digital content in the decentralized model. The use of the smart contract enables the model to perform digital rights management functions in real time, efficiently and automatically. Data service can also be monetized through smart contract according to the work of Migliorini [31] et al. Moreover, thus, the use of smart contract in the proposed model can not only help data owners to conduct the copyright management of their data, but also earn some incomes for their work. We design a smart contract to realize the registration, copyright information query, and use application of the spatial data, and use IPFS as the external digital content storage to make the entire process of spatial data digital rights management have completely decentralized nature and not affected by a single point of failure.

The main research objectives and contributions of this paper are summarized, as follows:

- We proposed a novel and decentralized spatial data digital rights management model. This model uses Ethereum blockchain as the bottom layer, uses smart contract for digital rights management of spatial data, and uses the InterPlanetary File System as spatial data external storage. This design allows for the model to run in a completely decentralized environment.
- We described the three algorithmic processes of copyright information registration, query, and use application in detail, designed the overall process of spatial data copyright management, and conducted preliminary implementation and functional testing of the model. At the same time, we used a smart contract code inspection tool to conduct code bug checks and perform vulnerability analysis for the security issues of the smart contract code. Finally, the five aspects of usability, scalability, efficiency, comparison of related models, and model security are discussed.
- The proposed model uses blockchain technology to allow for any node to apply for digital copyright of spatial data in a network without a central server. Nodes can directly perform copyright management operations (such as copyright usage application) with each other without a third-party trust institution. It solves important problems in traditional spatial data copyright management schemes, and can greatly facilitate spatial data sharing with clear copyright ownership. Furthermore, our smart contract can also monetize this data service.

2. Design

2.1. Blockchain Suitability for GDRM-OM

Currently, Bitcoin, Ethereum, and Hyperledger Fabric are included as mainstream blockchain systems that provide smart contract functionality. Table 1 shows the differences between them. The selected blockchain framework should be able to perform the function of "writing copyright information inside the blockchain and storing the digital content itself in the external storage" according to the design requirements of GDRM-OM, and the model should have the advantages of being oriented to the masses, being completely decentralized, having high security, and being capable of automated execution. Meanwhile, the selected blockchain should be able to implement smart contract applications with complex logic, ensure that everyone is free to participate in spatial data sharing, and directly initiate transactions with spatial data copyright owners without the need for a central authority. In addition, the copyright information registration service does not require a high amount of transaction per second, because it is not used as frequently as transfers. By summarizing these analyses and comparing the different blockchains in Table 1, it is not difficult to find that Ethereum as a public chain can effectively meet the requirements of the proposed model.

Table 1. Comparison of different blockchain platforms.

Name	Bitcoin	Ethereum	Hyperledger Fabric
Category	Public	Public	Consortium
Node restrict	None	None	Only authorized nodes
Node permissions	Fully peer	Fully peer	Only licensed nodes can operate on the blockchain
Consensus mechanism	PoW	PoW, PoS	SOLO, Kafka, PBFT
Incentive mechanism	bitcoin	ether	None
Smart contract development language	OP_RETURN	Solidity, Vyper	Golang, Java
Smart contract operating environment	Stack based	EVM	Docker
Is Turing complete	No	Yes	Yes
Transaction per second	7–15	7–15	1000

2.2. Architecture

The architecture of GDRM-OM includes a blockchain base layer, smart contract layer, data repository layer, spatial data layer, interface layer, browser layer, and user layer. The model architecture is divided into two parts from the interface layer: spatial data copyright management and spatial data storage. As shown in Figure 1, in the part of spatial data copyright management, the blockchain base layer is the Ethereum blockchain, which is the basis of the entire spatial data digital rights management process, and the data generated by copyright management operation will be written into the underlying blockchain, except the digital content itself. In the smart contract layer, the smart contract will be converted to bytecode and deployed to EVM to run on the Ethereum blockchain. The blockchain base layer and the smart contract layer can be collectively referred to as the blockchain layer. The blockchain layer and data repository layer are in a parallel relationship. As the base layer of the model, they do not interfere with each other directly and are independent of each other. Copyright registration, copyright information query, and spatial data use application functions that are implemented in the smart contract layer. The smart contract layer and the spatial data layer interact with the browser through the interface. The browser provides users with a graphical user interface for each function. The user layer contains the copyright owner node and other user nodes, but the copyright owner node can also obtain data from other copyright owners from the system. There is no obvious dividing line between these two types of nodes, and it is mainly divided according to the behavior of the node. It can be regarded as other user nodes if the node only obtains data from the system and never registers copyright. As a decentralized file system, IPFS can store digital content in a distributed network. The combination of IPFS and Ethereum enables the model architecture to abandon the central server. The digital copyright management process of spatial data has the advantages of complete decentralization, tamper resistance, and high security through such a design. Therefore, we use IPFS as a data repository to store spatial data in a decentralized manner in the spatial data storage part. The user uses the interface to store the spatial data in the data repository through the browser. The status of the spatial data in the data repository is sent to the smart contract through the communication between the interfaces, and finally records it in the blockchain.
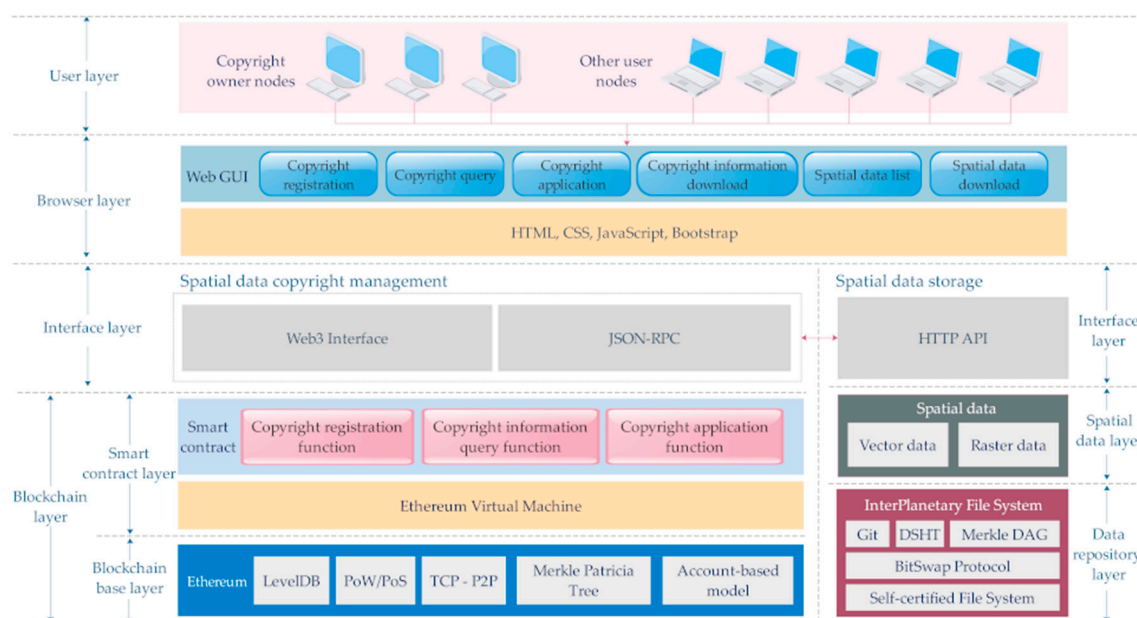

Figure 1. Architecture of spatial data digital rights management model (GDRM-OM).

2.3. Copyright Information Structure

The amount of data in the digital content itself is relatively large, and the limitation of the capacity of the blockchain system makes it impossible to directly store the digital content on the blockchain. Although we can solve the problem by storing the digital content in the decentralized external storage, it still requires a certain amount of processing fee (Gas fee) to write data into the Ethereum blockchain. It is obvious that the handling fee is proportional to the amount of data. We minimize the copyright information attribute while considering the scalability of the system when designing the copyright information structure in order to avoid the high handling fee and reduce the registration cost of spatial data copyright information, and determine the copyright attribution of a spatial data with a small structure, such as that shown in Table 2.

Table 2. Spatial data copyright information structure.

Field	Data type	Description
ID	uint	Unique identifier of spatial data
Name	string	Name of spatial data
Year	uint	Year of spatial data
Category	string	Category of spatial data
ImageHash	string	Hash of spatial data screenshot in IPFS
DescHash	string	Hash of spatial data description in IPFS
GeoDataHash	string	Hash of spatial data in IPFS
Price	uint	Price of spatial data for use application
RegisterTime	uint	Copyright registration time of spatial data
Owner	address	Owner Ethereum address of spatial data

1. *ImageHash*: For spatial data, especially vector data, users can directly crawl spatial coordinates and attribute information of data in front end if data are displayed in a browser front-end page. We added this field to the copyright information structure to prevent this. The field is used to store the screenshot hash value of spatial data uploaded to IPFS and browser interface displays data screenshot instead of original spatial data.

2. *GeoDataHash*: Copyright information is stored in the Ethereum blockchain and the digital content of spatial data is stored in the IPFS. The one-to-one correspondence between copyright information and spatial data can be established through this field.

3. *Price*: We used a transaction to solve this problem in order to write the usage record of data into the blockchain. We believe that copyright owners may have a payment sharing requirement in the future, thus this field was added for the considering of the scalability of the system. At this stage, the default value of this field is 0.

4. *RegisterTime*: This field takes an integer type and the actual stored value is a timestamp.

2.4. Smart Contract

We designed three smart contract processing procedures, and previously described in detail some mapping relationships that need to be used in the algorithms, aiming at the three basic functions of spatial data copyright information registration, copyright information query, and spatial data use application.

2.4.1. Mapping Relationships

We designed four mappings through the spatial data unique identifier attribute as a key to express the relationship between spatial data, spatial data copyright owner, and hash value of spatial data in IPFS, as shown in Figure 2. Table 3 shows the abbreviations and corresponding full names in the mappings.
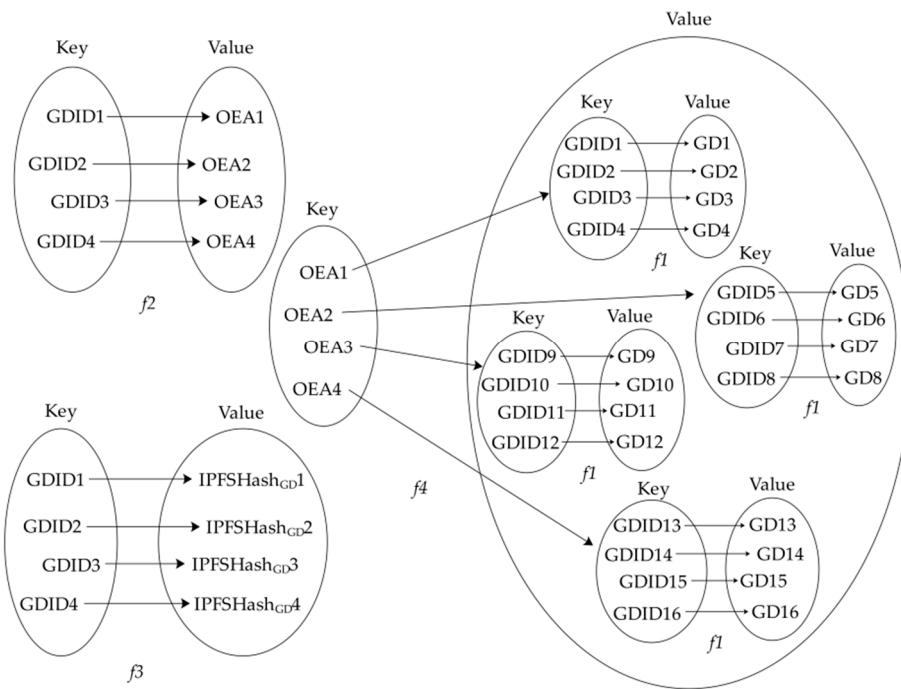
Figure 2. Mapping relationships in GDRM-OM.

Table 3. Abbreviations and corresponding full names in mappings.

Abbreviations	Full Names
OEA	Owner Ethereum Address
GDID	Geo-data ID
GD	Geo-data
IPFSHashGD	Hash of Geo-data in IPFS

1. Spatial data unique identifier mapping: Each spatial data should have a unique data identifier, so the mapping relationship between spatial data and the data identifier can be denoted as *f1*: $GDID \rightarrow GD \,|\, GDID > 0$, $GD \neq NULL$.

2. Spatial data attribution mapping: Each spatial data should belong to only one copyright owner, and each spatial data has a unique data identifier. Therefore, a mapping relationship between the data's unique identifier and copyright owner is established, and it can be denoted as *f2*: $GDID \rightarrow OEA \,|\, GDID > 0$, $OEA \neq NULL$.

3. Spatial data IPFS hash mapping: When each spatial data is stored to IPFS, a unique hash value is generated, thus the mapping relationship can be denoted as *f3*: $GDID \rightarrow IPFSHash_{GD} \,|\, GDID > 0$, $IPFSHash_{GD} \neq NULL$.

4. Spatial data copyright owner mapping: A copyright owner might own the copyright of multiple spatial data, hence a two-layer mapping relationship is used to express the correspondence between the copyright owner and the spatial data, being denoted as *f4*: $OEA \rightarrow (f1: GDID \rightarrow GD) \,|\, OEA \neq NULL$, $GDID > 0$, $GD \neq NULL$.

2.4.2. Design of Smart Contract

The spatial data digital rights management process while using smart contract should be user-friendly and efficient, thus minimizing the time spent by users in the copyright management process, immediately processing user copyright management applications and returning copyright management result to users in real time. Therefore, we have designed three copyright management algorithms for this purpose. Figure 3 shows the main steps of spatial data copyright management

using smart contract. In the copyright registration process, IPFS will return the spatial data hash value when copyright owner uploads spatial data to IPFS, and then the copyright owner can initiate a registration application to the copyright management smart contract. The smart contract judges whether the current spatial data has been registered according to the IPFS hash value of the spatial data. The current copyright application process will be rejected if the spatial data has been registered in the blockchain. If not, the current copyright application process will be successfully completed. In the copyright query function, copyright owners and data users can query copyright information of spatial data from the blockchain at any time through the smart contract. The smart contract will first query the OEA and the price (default is 0, which means that the spatial data is shared for free) of spatial data in the copyright information of spatial data from the blockchain when a user applies for spatial data by the smart contract, and then the user can initiate a transaction to the copyright owner according to the OEA and the price. The smart contract will return the spatial data IPFS hash to the user and the user will request the IPFS network to download the spatial data according to the hash when the transaction is successful.
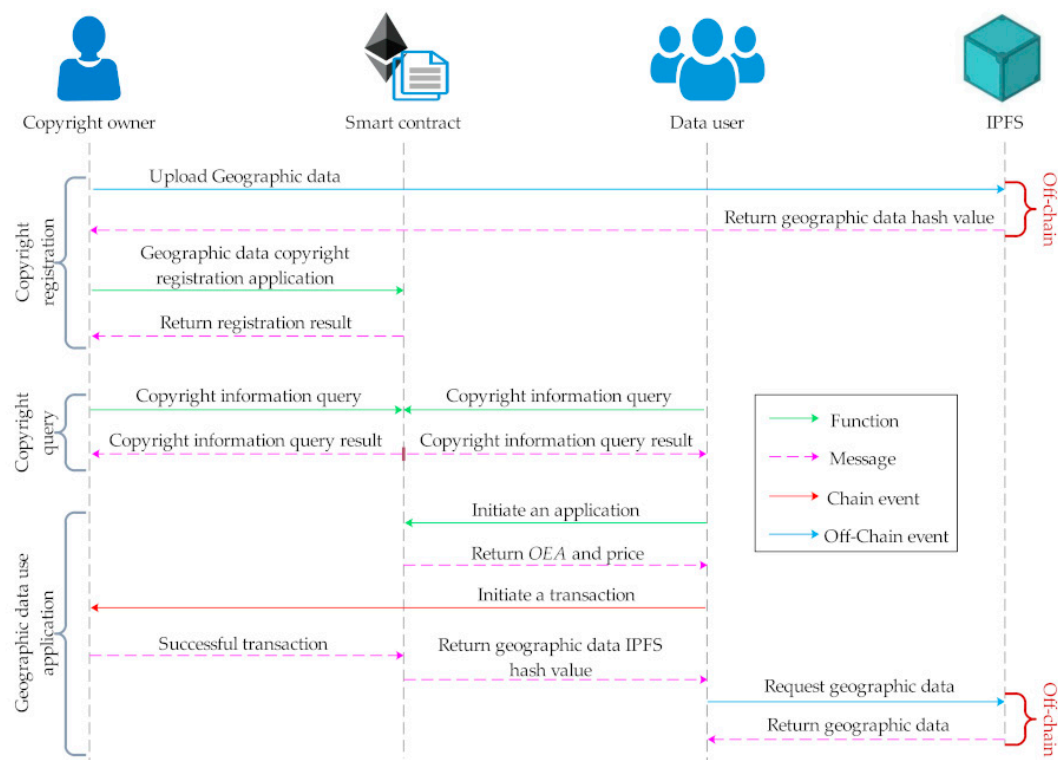

Figure 3. Spatial data copyright management function flow.

Anyone who complies with legal provisions and copyright protection rules can use the spatial data copyright information registration function to register their own spatial data to share the data. Algorithm 1 shows all of the steps in the copyright registration process of spatial data that nodes upload data to IPFS and register data copyright with Ethereum blockchain through smart contract. Any node can use the copyright registration application function, but the copyright registration process will only continue when the spatial data hash value has not been written to the blockchain previously according to the flow of Algorithm 1. The copyright registration application process of the node will stop immediately and the smart contract will return the ID of the registered spatial data to the node if the hash value of the spatial data uploaded by the node already exists in the blockchain.

All of the nodes can query all the registered spatial data copyright information by using the copyright information query function, which can prevent infringement caused by non-subjective factors and assist in solving copyright disputes. Algorithm 2 describes the process of spatial data

copyright information query. It determines whether the ID of the spatial data input by user has already existing in the blockchain firstly to prevent malicious input. The query is directly terminated if the ID does not exist. If it does exist, the smart contract will query the information from the blockchain.

In addition to providing copyright information query capabilities, we want to keep the application record on the blockchain and allow for the copyright owner to view all of the applications of the spatial data at any time; the transaction function in the Ethereum blockchain works well for this purpose. The transaction record will be written into the blockchain once an application occurs, thus we utilize the transaction function in the Ethereum blockchain to design the spatial data use application function. The node needs to take the spatial data use application function to initiate a transaction to the copyright owner if it wants to use spatial data provided by a copyright owner. In this way, all data usage records will exist in the transaction record of the data copyright owner ethereum account. Algorithm 3 presents the detailed process of spatial data use application function.

Algorithm 1. Spatial data copyright registration function.	
	Input: *F* is the form containing spatial data copyright information that the user fills in the browser
1	Serialize *F* to get *F′*
2	URL decoding for *F′* to get *P*
3	Upload spatial data screenshot to IPFS to get the hash of screenshot (*IPFSHashImage*)
4	Upload spatial data description to IPFS to get the hash of description (*IPFSHashDescription*)
5	Upload spatial data to IPFS to get the hash of spatial data (*IPFSHashGD*)
6	Call the post-deployment spatial data digital rights management smart contract, which will automatically record OEA. If the contract is not deployed, should first deploy the contract and initialize the spatial data index *GeoDataIndex* = 0
7	Call the smart contract to query the data on the Ethereum to traverse spatial data IPFS hash mapping (*f3*)
8	**if** *IPFSHash$_{GD}$* ∈ *f3* **then**
9	Tell the node to fail to register
10	Tell the node that the spatial data unique identifier has been registered
11	**end**
12	**else**
13	Let *GeoDataIndex* increase by 1
14	Let *GDID* = *GeoDataIndex*
15	Generate registration time (*RegisterTime*)
16	Store *OEA* to spatial data attribution mapping (*f2*) using *GDID*
17	Store *IPFSHash$_{GD}$* to *f3* using *GDID*
18	Store each parameter in *P* and *GDID* and *RegisterTime* to spatial data copyright owner mapping (*f4*)
19	Call the smart contract to write data to Ethereum blockchain
20	Copyright registration is completed
21	**end**

Algorithm 2. Spatial data copyright query function.

	Input: *GDID*
1	Call the post-deployment spatial data digital rights management contract to obtain *GeoDataIndex*
2	**if** *GDID* ∉ *GeoDataIndex* **then**
3	Inform the node that the *GDID* entered is incorrect and cannot query the corresponding spatial data copyright information.
4	**end**
5	**else**
6	Call the smart contract to read the *f4* mapping stored in the blockchain and return the spatial data copyright information
7	Call the smart contract to read the *f2* mapping stored in the blockchain and return OEA
8	**end**

Algorithm 3. Spatial data use application function.

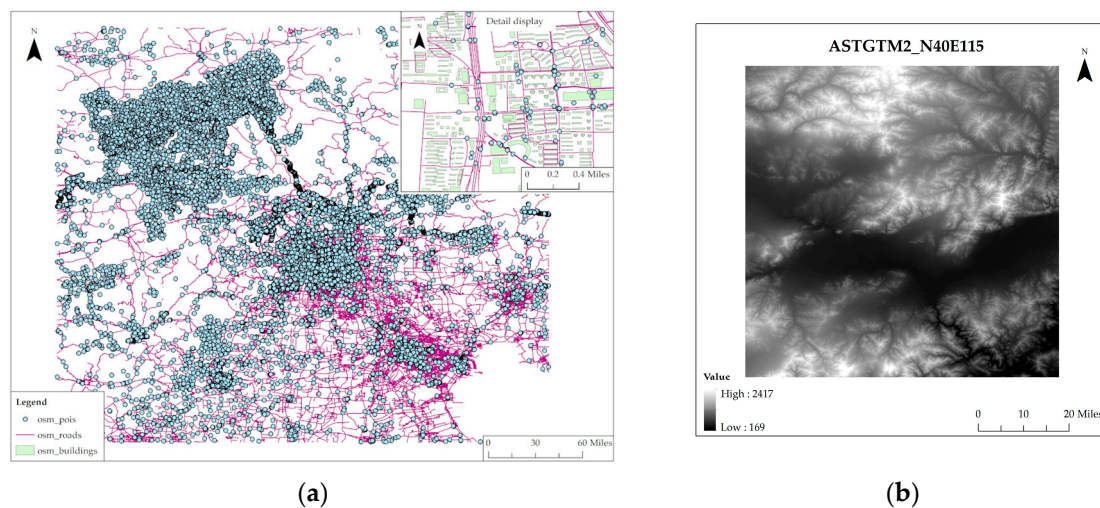|	**Input: *GDID***
1	Call the post-deployment smart contract to read the *f2* mapping stored in the blockchain and return OEA
2	Call the smart contract to read the *f4* mapping stored in the blockchain, return the price of the spatial data, default is 0 at this stage.
3	The current node initiates a transaction with the OEA
4	**if** Successful transfer **then**
5	Allow nodes to download data
6	**if** Node requests to download data **then**
7	Call the smart contract to read the *f4* mapping stored in the blockchain, return hash of spatial data in IPFS
8	Download data from IPFS using the hash value
9	**end**
10	**end**
11	**else**
12	Application failed
13	**end**

3. Results

3.1. Implementation and Results

We implemented and developed a decentralized spatial data copyright management prototype system based on the designed model architecture. We built the prototype system that was based on the Ethereum blockchain and used the go-ipfs client as the decentralized external data storage. We mainly used Truffle, Solidity, Node.js, JavaScript, and Webpack as development tools for smart contract application development. The detailed development environment is shown in Table 4, and the system main interface is shown in Figures 5–7.

Table 4. Development environment and tools.

Entry	Value
Operating system	Windows 10 18362.175 based on x64
RAM	24G
CPU	Inter i5-7300HQ
Blockchain	Ethereum
Develop tool	truffle@4.1.10, solidity@0.4.23, node@10.15.3, JavaScript, Webpack
External storage	go-ipfs@0.4.20
Main API	js-ipfs-api@17.1.3, web3@0.20.1
Browser	Google chrome@78.0.3904.70
Wallet extension	Metamask@7.6.1
Test network	Ropsten

The Ropsten network is a test network of the Ethereum blockchain, which is basically the same as the Ethereum main network environment. The nodes in the network can apply for free ether for testing. We deploy the smart contract in the Ropsten network to perform spatial data digital rights management functional testing on our machine. The smart contract address that is deployed in the Ropsten test network is 0xB8936539A4ed01C1bF0400da73D64d2f22821080. The vector type spatial data used in the test were the shapefile vector dataset in OpenStreetMap, including pois, roads, and buildings. The range of the latitude and longitude of test dataset are 113.963°~118.493° E and 38.302°~42.125° N, and the coordinate system of test dataset is GCS_WGS_1984. The raster type spatial data used in the test were the DEM data from ASTER GDEM, and the data identification is ASTGTM2_N40E115. Taking the vector type data as the example, the data are stored in the personal geodatabase of ArcGIS. The IPFS hash value of the personal geodatabase is QmWUSzKegRqJZsjdxpDxqgbs9iYazVUggeFUtr3YXmvRaF. Figure 4 shows the overview of the test data.

Figure 4. Testing Data: **(a)** Vector type; **(b)** Raster type.

The function interface of spatial data copyright registration is shown in Figure 5. The system will allow the node to download the copyright information stored in JSON format when the copyright registration application is successfully completed. The copyright information of the sample data is shown in Table 5.

The copyright registration application transaction hash value in the Ropsten network is 0 × 70361baf7aa9215f846dce623fbf01d15f7bbb3eb32d71af1419346ad842a8ad. Table 6 shows the detailed information of the block where the transaction is located.

Figure 5. Copyright registration interface.

Table 5. Copyright information for sample data.

Field	Value
Spatial Data ID	2
Spatial Data Name	Test vector dataset
Spatial Data Category	Basic spatial information data
IPFS Hash of Data Image	QmdBZdh69C5gbT7Xki7XMgXi8YNxwkRKtZTAy7Q5GJvxTs
IPFS Hash of Spatial Data	QmWUSzKegRqJZsjdxpDxqgbs9iYazVUggeFUtr3YXmvRaF
IPFS Hash of Data Description	QmSC3kRvunUwdWaTCPv98ALGfHWs8u6LnNnEAFpgXTq98X
Price	0 ether
Register Time	11/28/2019, 5:30:04 PM
Owner Ethereum Address	0 × 901d6b6692f5334c4fdcd4b92a9651b054467bed
Transaction ID	0 × 822f97d000b32fe141171ea3f131a97ffd3cc94c52a0c020bae44d30d41095cd

Table 6. Block information.

Field	Value
difficulty	9311588739
extraData	0 × 41746c616e7469632043727970746f
gasLimit	8000029
gasUsed	7987304
hash	0 × 02dd512eb9af15c0cf97f6e99624fc3995690f071b5d1899350a5933b8429a7c
logsBloom	0 × 001da40211672102424824c0010c84082000010810b1002141061008060400070824 6a7013 12400801244440042211c610030282238420220230041030341e19109006008600a2a81034 0108612308441dd0900890f008640166202215300401008516002a8014200a00848a1421ac 2880802a084a126801918bd410810084000218910a202201a0920110100628a820600c9668 435222844080000048000004030021 8b000624002a7a041041060200542c12445880224000 188a009100685008024003e90400c211000412cd8408680c03010d440a000810014106f168f 10002b02244882d1400810011a02180022b02ce002240054d210ca5a202800f0060
miner	0 × d7a15baeb7ea05c9660cbe03fb7999c2c2e57625
mixHash	0 × 00001b269734ca03b207c871bee76928c0fb8f2e686d41f0d9e5d8460b8113b9
nonce	0 × 28b767ceae9006ff
number	6863746
parentHash	0 × 5b4f4eb3fca2b62f8a15dd850907e20d80ec2f6a6124d157fce0a7239b09cb7a
receiptsRoot	0 × d0e9420f1206baf138d15cddbfee92b2b5b46e37c7f4be860024a0b996dc9403
sha3Uncles	0 × 1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
size	8823
stateRoot	0 × f28954d377bd9927c746d150338f36c10a4ce47402516506aed2c291606f34f9
timestamp	1574933404
totalDifficulty	28665894671071599
transactions	34 transactions in this block
transactionsRoot	0 × 89f0aae5abdc879fa7a994d6f9bbf27e08ae2481daadfbf03b5ca1fd979e46cc
uncles	[]

The confirmation waiting time for this registration is about 0.5~1 minute. We used the ID of the newly registered spatial data for the copyright information query, and Figure 6 shows the result. Except

for the IPFS hash of the spatial data, which is not publicly displayed, other copyright information stored in the blockchain can be viewed. If a user wants to use this data, the user can apply for this data in the spatial data list. As shown in Figure 7, the data can be applied in the data detail page, and the spatial data can be downloaded after the application process is successfully completed.
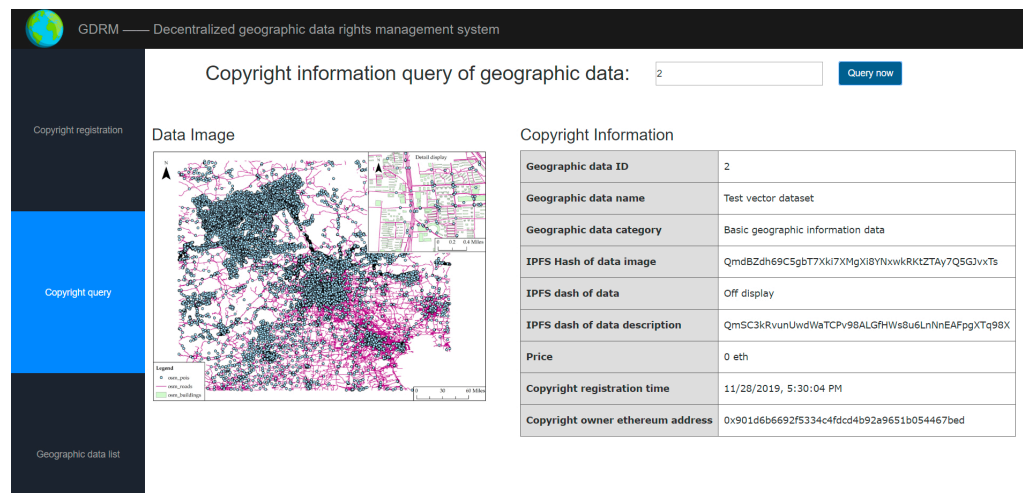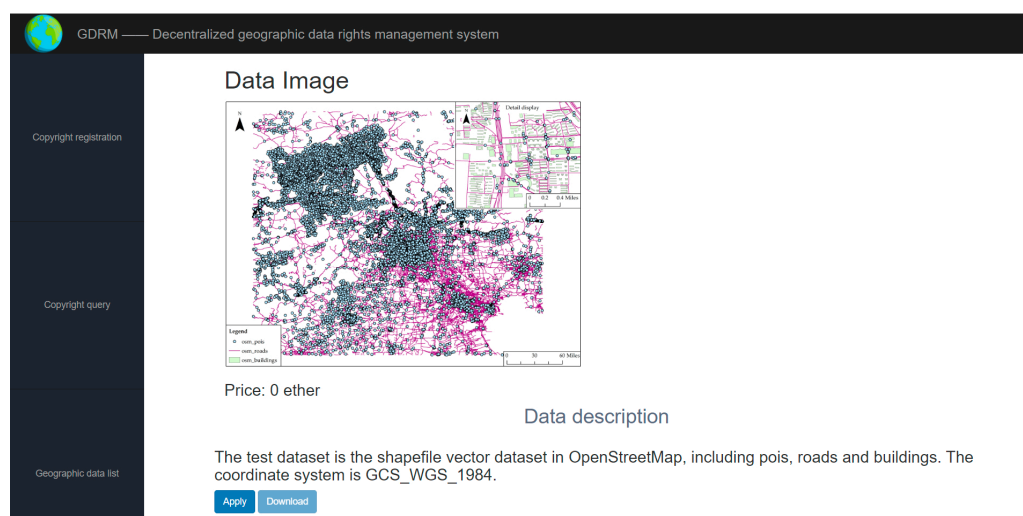

Figure 6. Copyright information query interface.

Figure 7. Spatial data use application interface.

3.2. Smart Contract Code Vulnerability Analysis

Including the DAO incident (Fu et al., 2019) in 2016, the safety accidents in Ethereum originated from the smart contract application and they were not related to the Ethereum blockchain. Ethereum as an open source project has not found any vulnerabilities since 2014, but smart contracts, as an application running on Ethereum, can directly interact with Ethereum, and its security directly relates to the economic interests of Ethereum. Therefore, vulnerability testing must be performed on smart contracts to prevent smart contracts from being attacked in the development of blockchain applications. Smart contract security checks have become an important part of ensuring contract stability which has caused people to pay attention to the security issues of smart contracts. Recent studies [32–36] focused on the security of the smart contract in Ethereum, analyzed the vulnerabilities of Ethereum smart contract from the aspects of the Ethereum underlying structure, analyzed the smart contract bytecode running environment and the intrinsic mechanism of smart contract programming language,

and pointed out the causes of security incidents that have occurred and the programming grammar that may lead to security vulnerabilities. Table 7 shows common vulnerabilities.

Table 7. Common smart contract vulnerabilities.

Vulnerability name	Cause
Reentrancy attack	Attack through a callback function in a smart contract.
Call to the unknown	The function name error or inexistence causes no function matching.
Integer Overflow and Underflow	The result value is greater than the maximum value that the type can store due to an operation error or other reason, or less than the minimum value that the type can store.
Keeping secrets	Variables of type private are not guaranteed to be invisible in Solidity.
Ether lost in transfer	Sending ether to a compliant empty address will result in loss of ether.
Unpredictable state	The contract status is uncertain due to the uncertain execution order of the transactions in the block.
Generating randomness	Pseudo-randomness generated by hackers manipulating hash values or timestamps.
Timestamp dependency	Miners can set the timestamp to be beneficial to themselves when mining.
Dangerous delegatecall	Using delegatecall for function calls can result in that allow the caller to call functions of arbitrary addresses.

Mythril, a smart contract security verification tool that was developed by Bernhard Muller, can detect more than twenty smart contract potential security vulnerabilities that were proposed by recent studies including the above common threats. The tool is integrated into the Ethereum compiler Remix to provide developers with visual vulnerability code location and modification tips. We used this tool for code checking to verify the security of the spatial data digital rights management smart contract. The smart contract we developed has no errors or warnings according to Figure 8, which indicated that there are no dangerous vulnerabilities in the smart contract code. The smart contract has high security.
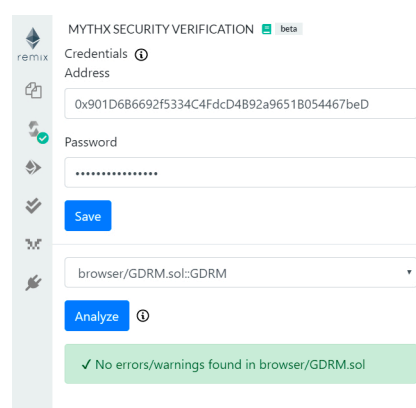

Figure 8. Code vulnerability detection result.

4. Discussion

4.1. Usability

In the proposed model, the Ethereum blockchain and IPFS are used as the underlying architecture, and the smart contract is used for digital rights management, which make the model automatically process the copyright management operations initiated with nodes, without manual review when the conditions are met. In addition, IPFS, as a globally interconnected file system, can store massive amounts of data easily and solve the problem of large amounts of spatial data without difficulty. We integrated and improved the functions and advantages of the blockchain-based digital rights management model in previous work, and realizes the diversified copyright management functions, including copyright information register, copyright information query, and copyright application. Blockchain technology is used to manage the spatial data copyright in the proposed model, in contrast to the traditional centralized spatial data publishing infrastructure platforms. Such design ensures that any individual who complies with the copyright protection regulations can share their own spatial data; hence, the participants of spatial data sharing are no longer just scientific research personnel. The spatial data copyright information in the centralized system is vulnerable to illegal tampering, but the proposed

model can effectively resist all kinds of tampering for spatial data copyright information due to the unchangeability of blockchain technology. Meanwhile, in the model of this paper, IPFS is used as the external storage of digital content to store the spatial data in the decentralized file system, which completely solves the spatial data security problems, such as data loss caused by a single point failure. The design of the architecture makes the model highly available.

4.2. Scalability

There is a slight lack of consideration on the scalability requirements of rights management functions in the existing research on blockchain-based digital rights management technology; with that in mind, we maintained the price field when designing the spatial data copyright information structure. At this stage, the field value defaults to 0. This field can be opened in the future if there is a demand for paid usage, allowing for the copyright owner to set the price of the spatial data. At present, the spatial data copyright management functions realized by smart contracts include copyright registration, copyright query, and spatial data use application, but it can continue to develop smart contracts to add new functions to the system in the future.

4.3. Efficiency

The data in the block can no longer be changed once the block is written into the blockchain, for digital rights management, it means that the copyright information registration is completed and will take effect immediately once the copyright information is successfully written into the blockchain. The block forging time of the mainstream blockchain is basically maintained at a few minutes [10,37]; hence, the authentication time of the spatial data digital copyright registration process could shorten by ten minutes, or even a shorter time, by using blockchain technology, which is more efficient than the traditional spatial data publishing infrastructure platforms. We tested the model on the Ropsten network, and the transaction waiting time is approximately 0.5~1 minute when registering for spatial data copyright. The copyright application review time of the China National Copyright Administration is about 30 working days [38] and the United States Copyright Office is about four to seven months [39], which illustrates that the proposed model has higher efficiency when compared with the traditional spatial data copyright management method. Moreover, the Ropsten network is basically similar to the Ethereum main network environment, but, in reality, the network environment (transaction waiting time) of the main network will be more stable, which means that the proposed model will perform better in practical applications.

4.4. Performance Comparison with Related Work

Some previous research on blockchain copyright management and current geographic data publishing schemes were mentioned in the first chapter of this paper, and we can compare the schemes with our proposed GDRM-OM scheme. Table 8 lists the detailed comparison with the related schemes. As can be seen from Table 8, as compared with the first scheme, the proposed model is protected from single points of failure, and it adopts an automated auditing method, which improves security, reduces labor costs, and improves event processing efficiency. Our model architecture is completely decentralized as compared with other models, with more perfect copyright management functions, and it can share digital content in a more secure situation. In general, our model has more outstanding performance.

Table 8. GDRM-OM scheme comparison with traditional geographic data publishing scheme and related work [24–27].

No.	Scheme	Decentralized Rights Management	Decentralized Data Storage	Affect by a Single Point Failure	Copyright Management Function	Publication of Copyright Information	Publication of Digital Content	Content Encryption	Audit Mode	Audit Time
1	geographic data publishing scheme	No	No	Yes	Registration, query, application	Yes	Yes	Unknow	Manual	Depends on journal publishing period
2	Kishigami et al. [24]	Yes	No	Yes	Registration, application	Yes	No	Yes	Auto	Real-time
3	Rinaldi [25]	Yes	Yes	No	Registration, query, application	Yes	No	Yes	Auto	Real-time
4	Meng et al. [26]	Yes	Yes	No	Registration, query	Yes	Yes	Yes	Auto	Real-time
5	Ma et al. [27]	Yes	Yes	No	Registration, query	Yes	No	Yes	Auto	Real-time
6	GDRM-OM	Yes	Yes	No	Registration, query, application	Yes	No	Yes	Auto	Real-time

4.5. Security of GDRM-OM

The security of the model mainly depends on the security of the underlying architecture. We mainly use blockchain technology, smart contract technology, and IPFS technology in the design of the underlying architecture of GDRM-OM. Blockchain technology uses a variety of encryption algorithms, such as hash algorithms, elliptic curve encryption algorithms, etc. These algorithms can effectively ensure the security of data. In addition, Satoshi Nakamoto [6] also performed a strict mathematical proof of the high security of the blockchain system in his paper. Since the development of blockchain technology, practice has proven that multiple platforms using this technology, such as Bitcoin, Ethereum, and Hyperledger, have extremely high security. The security of smart contracts has been analyzed in Section 3.2 and it will not be repeated here. The content encryption technology, shared storage technology, and multiple node backup technology of IPFS make it a secure decentralized data repository, solving the single point of failure problem in the centralized data server, and effectively protecting the privacy and safety of spatial data. Moreover, we have conducted the spatial data copyright use application function in the design of the model function, and this function logs all user information of spatial data to the blockchain through transactions, which enables user tracking, facilitating post-event review and accountability, and promoting the secure sharing of spatial data.

5. Conclusions

We have proposed a decentralized spatial data digital rights management model that is based on the Ethereum and IPFS platforms and established a decentralized, instant, mass-oriented, and high-security digital copyright management innovative method for spatial data while using smart contract to provide a novelty spatial data infrastructure platform for spatial data sharing. The design of the proposed model is independent of third-party trust institutions in the process of spatial data copyright management, and it can effectively solve the existing problems in the spatial data publishing infrastructure platforms. Our proposed model can promote the secure sharing of spatial data with clear data copyright ownership and provides a novel idea for spatial data infrastructure construction. Based on the proposed model functions and features, we have listed three possible cases for use:

- Scientific research data sharing: When scientific researchers publish scientific research results, they also need to publish relevant data to help other researchers to reproduce the results of their papers. Illegal acts, such as data piracy and theft of results, are likely to occur if the copyright of the data cannot be well protected. Our model can manage and protect data copyright in the process of scientific research data sharing.
- Business: In the design process of our model, the application of data usage rights is implemented through transactions. Subsequently, commercial companies can use this model to achieve paid sharing of business data. In addition, individual data producers can also use the smart contract to monetize data, and be able to obtain some due incomes in the process of data sharing.
- Crowdsourced geographic information platform: In a crowdsourced geographic information platform, users contribute to the platform by uploading their own data. However, most of the platforms are open source and will not consider the copyright ownership of the data. The cost of data abuse and piracy is very low. Our model can be used in these platforms to clarify the copyright information of each piece of data uploaded by each user, providing a more effective solution for quantifying user contributions and protecting the interests of data producers.

However, there are three key issues and shortcomings that need to be solved in the practical application of the model: (1) IPFS uses the hash of the data for content retrieval. Once the data are modified, the hash will change accordingly. Geographic data are easy to modify, which makes them extremely prone to data infringement, thus the proposed model requires additional detection algorithms to identify whether there is an infringement in a copyright registration process of a node. Fortunately, this issue has been solved in another paper. (2) During the copyright application process, the Ethereum account is anonymous, although we achieved user tracking. In the post-examination, only the node

Ethereum address can be tracked and the true identity of the node cannot be known. This brings some difficulties to accountability after the fact. We hope to solve this problem by eliminating account anonymity in future research. (3) In some circumstances, data owners may want to update copyright information, such as replacing data content information, but the copyright information update function is not implemented in this paper, and we will address this problem in future work.

References

1. Yow, T.G.; Jennings, S.V.; Grubb, J.W.; Smith, A.W. Inside an Environmental Data Archive WWW Site. In *Environmental Software Systems*; Denzer, R., Swayne, D.A., Schimak, G., Eds.; Springer US: Boston, MA, USA, 1997; Volume 2, pp. 168–174. [CrossRef]

2. Wang, J.L.; Zhu, Y.Q.; Xie, C.J. Network platform design and development for Earth system science data sharing. *Earth Sci. Front.* **2006**. [CrossRef]

3. Kimball, J.S. Earth Observation of Global Change: The Role of Satellite Remote Sensing in Monitoring the Global Environment. *Eos Trans. Am. Geophys. Union* **2008**, *89*, 294. [CrossRef]

4. Liu, Q.; Safavi-Naini, R.; Sheppard, N. Digital Rights Management for Content Distribution. In Proceedings of the Australasian information security workshop conference on ACSW frontiers, Adelaide, Australia, 1 January 2003.

5. Underwood, S. Blockchain beyond bitcoin. *Commun. ACM* **2016**. [CrossRef]

6. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 13 January 2020).

7. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**. [CrossRef]

8. Lansiti, M.; Lakhani, K.R. The truth about Blockchain. *Harv. Bus. Rev.* **2017**, *95*, 119–127.

9. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2017**. [CrossRef]

10. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]

11. Yong, Y.; Wang, F. Blockchain: The State of the Art and Future Trends. *Acta Autom. Sin.* **2016**, *42*, 481–494. [CrossRef]

12. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data, Honolulu, HI, USA, 25–30 June 2017.

13. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain Technology in Finance. *Computer* **2017**, *50*, 14–17. [CrossRef]

14. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]

15. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]

16. Xia, Q.; Sifah, E.; Asamoah, K.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]

17. Veuger, J. Trust in a viable real estate economy with disruption and blockchain. *Facilities* **2018**, *36*, 103–120. [CrossRef]

18. Savelyev, A. Copyright in the blockchain era: Promises and challenges. *Comput. Law Secur. Rev.* **2018**, *34*, 550–561. [CrossRef]

19. Smart Contracts. Available online: https://web.archive.org/web/20011102030833/http://szabo.best.vwh.net:80/smart.contracts.html (accessed on 13 January 2020).

20. Bartoletti, M.; Pompianu, L. An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.

21. A Next-Generation Smart Contract and Decentralized Application Platform. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 13 January 2020).

22. Ethereum: a secure decentralised generalised transaction ledger. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 13 January 2020).

23. IPFS - Content Addressed, Versioned, P2P File System. Available online: https://github.com/ipfs/papers/blob/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf (accessed on 13 January 2020).

24. Kishigami, J.; Fujimura, S.; Watanabe, H.; Nakadaira, A.; Akutsu, A. The Blockchain-Based Digital Content Distribution System. In Proceedings of the 2015 IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud), Dalian, China, 26–28 August 2015.

25. Rinaldi, J. Peer to Peer Digital Rights Management Using Blockchain. Master's Thesis, University of the Pacific, Stockton, CA, USA, 2018.

26. Meng, Z.X.; Morizumi, T.; Miyata, S.; Kinoshita, H. Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018.

27. Ma, Z.F.; Jiang, M.; Gao, H.M.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, *89*, 746–764. [CrossRef]

28. Frey, R.M.; Hardjono, T.; Smith, C.; Erhardt, K.; Pentland, A.S. Secure sharing of geospatial wildlife data. In Proceedings of the Fourth International ACM Workshop on Managing and Mining Enriched Geo-Spatial Data, Chicago, IL, USA, 14 May 2017; p. 5.

29. Kamel Boulos, M.N.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [CrossRef] [PubMed]

30. Matney, J.A.; Supak, S.K.; Slocumb, W.S. From GIS as a Service to the Geospatial Blockchain: The Future of the Intelligent Web Mapping. *Environments* **2019**, *12*, 12.

31. Migliorini, S.; Gambini, M.; Belussi, A.; Combi, C. The Blockchain Role in Ethical Data Acquisition and Provisioning. In Proceedings of the PIE@CAiSE, Rome, Italy, 3–4 June 2019.

32. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on Ethereum smart contracts (SoK). In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 24–25 April 2017.

33. Dika, A.; Nowostawski, M. Security Vulnerabilities in Ethereum Smart Contracts. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.

34. Grishchenko, I.; Maffei, M.; Schneidewind, C. A semantic framework for the security analysis of ethereum smart contracts. In Proceedings of the International Conference on Principles of Security and Trust, Thessaloniki, Greece, 16–19 April 2018.

35. Jiang, B.; Liu, Y.; Chan, W.K. ContractFuzzer: fuzzing smart contracts for vulnerability detection. In Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, Montpellier, France, 3–7 September 2018.

36. Luu, L.; Chu, D.-H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.

37. Pustišek, M.; Kos, A. Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 410–419. [CrossRef]

38. Registration Processing Times and FAQs. Available online: https://www.copyright.gov/registration/docs/processing-times-faqs.pdf (accessed on 13 January 2020).

39. Registration Processing Times. Available online: http://www.ccopyright.com.cn/index.php?optionid=1084 (accessed on 13 January 2020).