文章编号：2095-2163(2023)11-0281-05 中图分类号：TP393 文献标志码：A

基于区块链的不动产电子证照存储与查询研究

夏学亮[1]，刘 超[2]，刘从军[1,3]
（1 江苏科技大学 计算机学院，江苏 镇江 212100；2 镇江市不动产登记交易中心，江苏 镇江 212003；
3 江苏科大汇峰科技有限公司，江苏 镇江 212003）

摘 要：大数据时代下，传统纸质载体逐渐被电子证照取代。政务部门在办理有关业务时，需要审查不动产相关证照。针对现有不动产电子证照存在跨部门、跨区域共享困难、数据易泄露和存取效率低的问题，本文提出了一种基于链上链下相结合的不动产电子证照安全存储与查询方案，该方案采用分布式存储技术和区块链结合，实现了去中心化的不动产电子证照安全存储，并向政务部门提供证照查询接口，实现对不动产电子证照文件的完整性验证。安全性分析表明该模型可以保证证照数据安全存储。实验表明，该模型在保证安全性的前提下，具有良好的证照查询效率。

关键词：区块链；安全存储；不动产电子证照；完整性验证

Research on real estate electronic license storage and verification based on Blockchain

XIA Xueliang[1], LIU Chao[2], LIU Congjun[1,3]
(1 School of Computer, Jiangsu University of Science and Technology, Zhenjiang Jiangsu 212100, China;
2 Zhenjiang Real Estate Registration and Trading Center, Zhenjiang Jiangsu 212003, China;
3 Jiangsu KeDa Huifeng Technology Co., Ltd., Zhenjiang Jiangsu 212003, China)

Abstract: In the era of big data, traditional paper carriers are gradually replaced by electronic certificates. The government departments need to review the real estate related licenses when handling relevant businesses. To solve the problems of cross department and cross region sharing difficulties, data leakage and low access efficiency in the existing real estate electronic licenses, this paper proposes a secure storage and query scheme for real estate electronic licenses based on the combination of on chain and off chain. This scheme uses distributed storage technology and block chain to achieve decentralized secure storage of real estate electronic licenses, and provides a license query interface to government departments, realizing the integrity verification of real estate electronic license documents. The security analysis shows that the model can ensure the safe storage of license data. The experiment shows that the model has good license query efficiency on the premise of ensuring security.

Key words: blockchain; secure storage; electronic license of real estate; integrity verification

0 引 言

为推进政务服务“一网通办”[1]，国务院办公厅印发了进一步推进政务服务的方案，要求加快不动产电子证照应用推广和跨部门、跨区域互认共享[2]。一些政务部门数据共享不及时，部门协作困难，监管缺失，无法验证用户出示的不动产电子证照真实性，造成为用户办理部分业务时电子证照不可信的问题[3]。传统的不动产电子证照一般采用中心化方式存储[4]，容易被篡改，数据存储量大，如何确保在原始数据提交、处理及管理过程中各阶段的数据一致性、以及如何确保能快速响应电子证照越来越频繁的应用请求，已然成为需要考虑和解决的重要问题[5]。而且具有中心化结构的服务器，在数据安全性和隐私方面存在诸多问题[6]。

区块链具有去中心化、防篡改的特性[7]，不少部门把业务数据存放到区块链上，以备查证，提高办事效率[8]。文献[4,9]提出了不动产电子证照的建设思路和系统框架。文献[10]提出了基于区块链的电子证照库共享交易系统，但无法满足大规模的

作者简介：夏学亮(1997-)，男，硕士研究生，主要研究方向：信息安全、智能信息处理。
通讯作者：刘从军(1968-)，男，高级实验师，硕士生导师，主要研究方向：智能信息处理、信息安全、云计算。Email：391986831@qq.com

收稿日期：2022-11-21

证照管理。文献[11]提出了一种去中心化的分布式存储模型,但存在数据被篡改的风险。文献[12-13]提出了基于联盟链的电子证照隐私保护方法和系统的实现,但系统开销大,查询效率不高。

针对上述问题,本文设计了一种基于区块链的不动产电子证照安全存储与查询模型。该模型通过链上和链下结合,将不动产电子证照数据指纹、证照索引等信息上传区块链,保证数据的安全性;同时将不动产电子证照加密存储在链下的分布式数据库中。本方案既能存储大量的不动产电子证照数据,又能减轻区块链的存储压力;同时,该方案向政务部门提供证照密文查询接口,验证用户出示的不动产电子证照是否可信,推进可信电子证照办理政务,减少群众携带纸质证照的烦恼。将不动产电子证照编号作为主要关键词查询,能很好地提高查询效率。

1 区块链技术

1.1 区块链概念

区块链由中本聪提出,起源于比特币,是一种新型的应用模式[14],涵盖了点对点传输、分布式数据存储、密码学技术、共识机制等多种计算机技术。区块链主要特征有去中心化、开放性、以及可追溯性[15]。

1.2 区块链数据结构

区块链是一个又一个区块组成的链条。区块分为区块头和区块体。区块头利用时间戳把区块进行有序的排列连接,主要存储有关该区块的关键信息,区块体则存储交易信息。区块包含版本号、时间戳、Merker 根、交易数据与上一个区块的链接的哈希值。区块结构如图 1 所示。

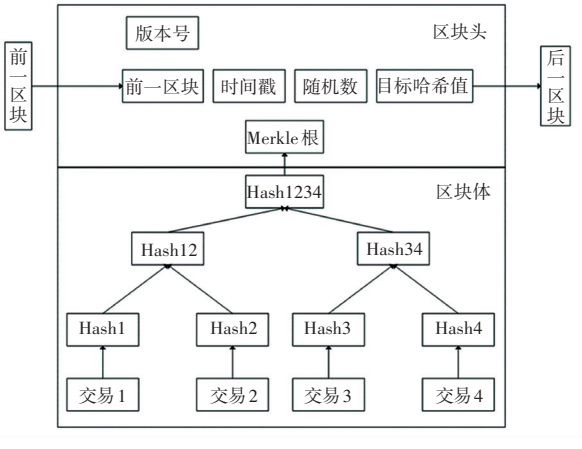

图 1 区块链数据结构

Fig. 1 Blockchain data structure

1.3 哈希算法

哈希算法能将不同的明文散列为固定二进制字符串,计算的结果为哈希值,也称数据指纹或者数字摘要[16]。哈希算法具有单向不可逆,输入敏感的特性,如果输入不同,则哈希值不同。目前,主流的哈希算法有 SHA-224、SHA-256 和 SHA-512。

1.4 共识算法

共识机制是为了保证在分布式系统中维护数据的一致性而设计的[17]。本文构建联盟链存储和共享不动产电子证照数据的区块链系统,采用委托权益证明共识算法(DPOS)[18]。该算法通过股东投票方式选出代表获得记录和验证权,大幅缩短了共识达成时间,可达到秒级验证[19]。

2 基于区块链的不动产电子证照安全存储与共享

2.1 不动产电子证照数据的存储架构

不动产电子证照安全存储模型如图 2 所示。由图 2 可知,不动产电子证照安全存储模型主要包括以下实体:

(1)分布式数据库系统(Distributed Data-base System,DDBS)。不动产电子证照存储在 DDBS 中,为了保证不动产电子证照数据的隐私性,通过加密算法进行存储。

(2)不动产登记中心。负责上传本地不动产电子证照文件。

(3)政务部门。该模型对政务部门提供不动产电子证照查询接口,同时验证证照数据完整性。

(4)数据区块。为了防止不动产电子证照数据被篡改、内容不可信,本文模型将在区块体交易记录中存储不动产电子证照数据指纹、不动产电子证照元数据,以保证政务部门查询以及进行证照数据完整性验证。在区块中,每一条交易记录有 3 个元组:不动产电子证照数据指纹、元数据和公钥。

(5)区块链。记录交易。

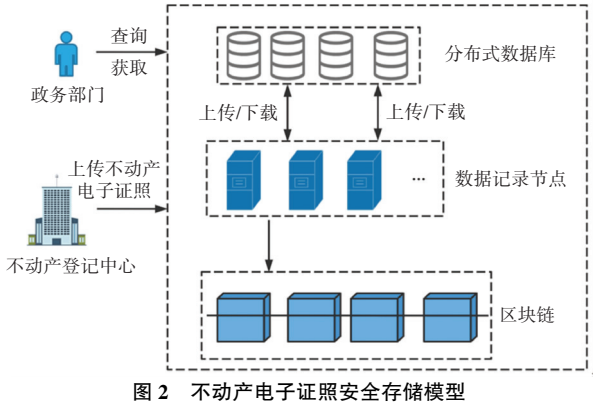

图 2 不动产电子证照安全存储模型

Fig. 2 Secure storage model of real estate electronic license

2.2　不动产电子证照数据的预处理

为了实现不动产电子证照的安全存储以及密文查询和完整性验证，不动产登记中心上传时应对不动产电子证照文件进行预处理。

(1)根据不动产电子证照文件生成不动产电子证照元数据。将权利人、不动产电子证照编号、不动产单元号、时间戳等信息从不动产电子证照文件中提取出来作为关键词，得到关键词集合 $KW = (KW_1, KW_2, \cdots, KW_n)$，作为不动产电子证照的元数据。

(2)创建倒排索引：用由(1)得到的元数据来创建密文关键词集合 $EKW = (EKW_1, EKW_2, \cdots, EKW_n)$。提取包含每一个密文关键词的不动产电子证照文件 Fi，将其当作一个元组插入到索引链表中。索引结构如图 3 所示。

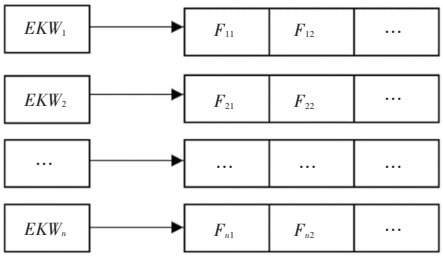

图 3　倒排索引结构

Fig. 3　Inverted index structure

不动产电子证照数据在链上存储时，为了保证索引的安全性，区块链负责管理索引。为了方便证照数据查询，本文扩展了区块头字段，来存储预处理后的不动产电子证照文件索引，如图 4 所示。

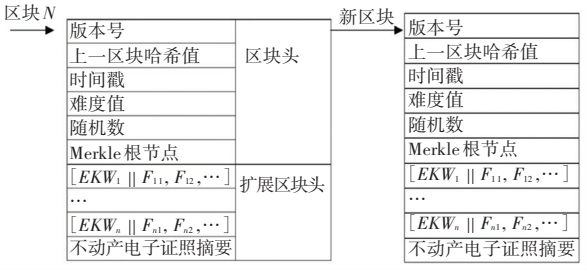

图 4　扩展的区块链结构

Fig. 4　Extended blockchain structure

2.3　不动产电子证照数据的安全存储

为了实现不动产电子证照数据的采集并进行安全存储，表 1 列出了所用符号及含义。

表 1　符号和含义

Tab. 1　Symbols and meanings

符号	符号含义
i	不动产登记中心
N_j	第 j 个数据记录节点
PK_i, SK_i	实体 i 的公钥和私钥
$TimeStamp$	时间戳
$Encrypt\_PK_i$ /m	用实体 i 的公钥加密 m
$Sign\_SK_i$ /m	用实体 i 的私钥对 m 签名
$Hash$/ m	用实体 i 的私钥对 m 签名
$MetaData$	元数据
$a \| b$	元素 a 连接元素 b
$Record$	消息记录

不动产电子证照数据的采集存储过程具体如下：

(1)不动产登记中心以自身的公钥作为标识，提交上传请求至本地数据记录节点，表示如下：

$$i \rightarrow N_j : Request = (Req \| PK_i) \quad (1)$$

(2)本地数据记录节点收到请求后，对不动产登记中心的公钥进行验证。

(3)不动产登记中心用自己的私钥对不动产电子证照数据指纹进行数字签名，同时使用自身的公钥加密数据。具体描述如下：

$$i \rightarrow N_j : Sign = Sign\_SK_i(hash(m)) \quad (2)$$

$$Record = Encrynt\_PK_i(Data \| Sign \| TimeStamp) \quad (3)$$

(4)上传的不动产电子证照数据由本地数据记录节点收集，在分布式数据库进行加密存储，同时向数据记录节点提交元数据。

(5)数据记录节点的工作量证明：每隔10 min收集的数据被数据记录节点 N_j 合并成数据集合，数据记录管理权限由工作量证明确定，具体描述为式(4)：

$$Data\_gather = \{TimeStamp \| MetaData\} \quad (4)$$

(6)数据记录节点间的区块共识过程：本文区块共识使用 DPOS 共识算法进行。

2.4　不动产电子证照查询及文件完整性验证

为了保证不动产电子证照数据的隐私性，不动产电子证照数据加密存储在分布式数据库中。同时为了方便快速查询不动产电子证照信息，本文采用可搜索加密技术进行查询。下面给出了证照密文查询以及证照文件完整性验证过程，如图 5 所示。

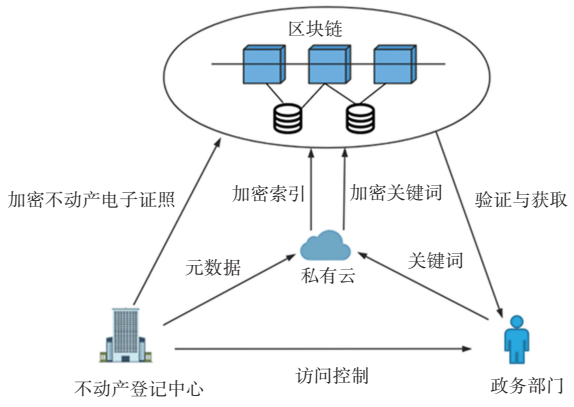

图 5 查询与验证数据完整性过程

Fig. 5 Integrity of querying and verifying data

(1)政务部门→私有云:用户办理相关业务时(公安户籍管理、居民子女入学、工商注册登记、缴税纳税等),向政务部门出示不动产电子证照,工作人员获取用户提供的不动产电子证照原件,调用查询接口,输入关键词(证照开始时间+权利人或不动产电子证照电子编号+不动产单元号等)进行查询。私有云获取政务部门查询请求后,系统先在链上查询政务部门所需时间段的不动产电子证照信息;此后通过区块链上面的时间戳找到不动产电子证照目标区块。

(2)政务部门←私有云:根据区块链存储的索引信息得到不动产电子证照数据密文,返回给政务部门。政务部门解密数据密文,查看不动产电子证照数据。

(3)政务部门↔区块链:在查询到相关不动产电子证照数据的同时,根据区块交易记录政务部门获取相关不动产电子证照数据指纹,将该数据指纹与用户出示的不动产电子证照计算得出的数据指纹,进行比对,若两者一致,说明用户出示的不动产电子证照 f 未经篡改,证照可信,继续办理相关业务。若两者不一致,说明用户出示的不动产电子证照被恶意篡改,电子证照不可信,终止办理相关业务。

2.5 安全性分析

(1)数据隐私性问题。不动产登记中心利用加密算法将电子证照密文上传至分布式数据库中,同时使用系统预设的哈希算法(SHA-256)计算出每个不动产电子证照文件的哈希值,链上只保存了哈希值以及加密的证照元数据,有效保护了用户的证照隐私,节约了链上宝贵的存储空间。

(2)数据完整性问题。链下使用分布式数据库存储加密数据,链上保存原始数据哈希值,如果数据被篡改,则哈希值改变。而且每一个节点数据都有备份,可有效防止数据丢失,以保证其完整性。

(3)数据可追溯性问题。节点采集到的不动产电子证照数据都需附上数字签名等信息,可以据此保证节点的合法性和数据来源的真实性。

本文将基于区块链的不动产电子证照安全存储方案与一些电子证照存储方法进行方案对比,结果见表 2。

表 2 存储方案对比

Tab. 2 Comparison of storage schemes

方案	区块链	加密	完整性验证	链上链下分离存储	链下查询
文献[12]	×	×	√	×	√
文献[10]	√	×	√	×	×
文献[11]	√	×	√	×	√
本文方案	√	√	√	√	√

3 仿真实验

不动产电子证照的联盟链使用 Java 语言进行开发,jdk 版本为 1.8。该链部署在 3 台物理机和 4 台 VM(ubuntu16.04)虚拟机中,即该链有 7 个节点;Hadoop 文件存储系统作为链下的分布式数据库,同时伪分布式集群环境在 1 台物理机上进行搭建,版本为 Hadoop3.2.2。

为了验证在确保安全性的前提下本文所提方案的查询效率,本文将使用倒排索引的证照查询方法与传统的区块链上查询证照的方法进行查询时间对比,不动产电子证照元数据保持相同数量存储在数据区块中,随着不动产电子证照的一直增加,记录 2 种方案的证照查询时间。本文以某市不动产登记中心 2020~2021 年的办理的不动产电子证照为测试数据集进行查询,不动产电子证照数量从10 000增加到300 000,随着证照数量的不断增加,记录查询方案耗费的时间。实验过程中,每个测试数据均为实验运行 20 次所取的平均值,2 种查询方案查询耗时对比如图 6 所示。

从图 6 中可以看出,由于不动产电子证照存储规模的不断扩大,2 种方案的查询时间也慢慢变长,本文所提出的链上查询方案在提高安全性的基础上,查询耗时以较慢的趋势增加,传统区块链查询的方法耗时的增长趋势较快,本文方案在增长速度上明显较好。本文链上查询使用倒排索引,查询效率和区块数量有关,时间复杂度为 $O(|KW| * |N|)$,其 中 $|N|$

为区块数量，| *KW* | 是关键词数量。由于不动产电子证照的独特性，将不动产电子证照编号作为主要关键词，能够提高查询效率。传统的区块链查询证照根据区块顺序进行查找，区块数量越多，查询时间越长，随着证照数量的增多，耗时也快速增加。本文方案查询耗时的增加并不快速，总体来说，本文中查询方案的效率性能较好。

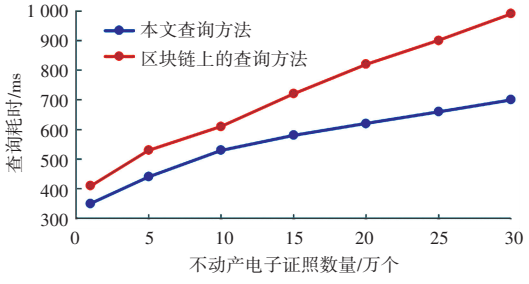

图 6　不动产电子证照查询时间

Fig. 6　Query time of real estate electronic licenses

4　结束语

本文设计了一种基于区块链的不动产电子证照安全存储与查询方案。该方案通过使用链上链下结合的方法，既能实现不动产电子证照的大量存储，也能防止不动产电子证照信息被恶意篡改，保证了电子证照的安全可信。同时，在不占用计算资源的情况下采用 DPOS 共识算法，确保了不动产电子证照数据的一致性；此外，本方案对政务部门提供了不动产电子证照密文查询接口，政务部门可以通过查询关键词获取相关的不动产电子证照信息，验证不动产电子证照文件完整性。该方案保证了不动产电子证照数据的完整性、安全性、隐私性以及可信，同时为推进可信不动产电子证照办理政务提供了一条新的思路。

参考文献

[1] 张飞，韩欢欢，李冬青. 基于区块链与电子认证的不动产登记电子证照系统的设计与实现[J]. 江苏科技信息，2019，36(35)：42-46.
[2] 刘彬. 我国“区块链+政务”发展现状及对策研究[J]. 现代营销，2020(12)：24-25.
[3] 雷飞，周海洋，潘轶. 南京市不动产登记电子证照建设及应用研究[J]. 住宅与房地产，2020(27)：15-16.
[4] 欧翔，周鹏. 基于区块链的不动产电子证照应用系统建设研究[J]. 现代信息科技，2022，6(2)：21-24.
[5] 崔久强，王虎. 电子证照服务平台研究及应用[J]. 电子技术与软件工程，2020(7)：243-245.
[6] 王新华，金刚，赵喜军，等. 电子认证在可信电子证照中的应用[J]. 信息安全研究，2016，2(6)：543-547.
[7] 何蒲，于戈，张岩峰，等. 区块链技术与应用前瞻综述[J]. 计算机科学，2017，44(4)：1-7.
[8] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J]. 网络与信息安全学报，2016，2(11) ： 11-20.
[9] 闵旭蓉，杜葵，戴逸聪. 基于区块链技术的电子证照共享平台设计[J]. 指挥信息系统与技术，2017，8(2)：47-51.
[10] 王浩亮，廉玉忠，王丽莉. 面向电子证照共享的区块链技术方案研究与实现[J]. 计算机工程，2020，46(8)：277-283.
[11] 郝琨，信俊昌，黄达，等. 去中心化的分布式存储模型[J]. 计算机工程与应用，2017，53(24)：1-7.
[12] 李行健. 基于区块链的电子证照隐私保护方法[D]. 衡阳：南华大学，2021.
[13] 巢燕. 基于区块链的电子证照管理系统的设计与实现[D]. 南京：南京大学，2018.
[14] 何蒲，于戈，张岩峰，等. 区块链技术与应用前瞻综述[J]. 计算机科学，2017，44(4)：1-7.
[15] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.
[16] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41(5)：969-988.
[17] 谭敏生，杨杰，丁琳，等. 区块链共识机制综述[J]. 计算机工程，2020，46(12)：1-11.
[18] 王化群，吴涛. 区块链中的密码学技术[J]. 南京邮电大学学报(自然科学版)，2017，37(6)：61-67.
[19] 陈东丰，黄晓鑫. 基于区块链的数据非对称加密与解密机制[J]. 网络安全技术与应用，2022(10)：27-28.