DOI:10.19729/j.cnki.1009-6868.2018.06.006
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181124.1856.002.html

基于区块链的电子数据存证的设计与实现

Design and Implementation of Electronic Data Storage and Certificate System Based on Blockchain

冒小乐/ MAO Xiaole[1]
陈鼎洁/CHEN Dingjie[2]
孙国梓/ SUN Guozi[1]
(1. 南京邮电大学,江苏 南京 210023;
2. 复旦大学,上海 200433)
(1. Nanjing University of Posts and Telecommunications, Nanjing 210023, China;
2. Fudan University, Shanghai 200433, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0028-007

摘要: 设计了一种基于区块链的电子数据存证系统,该系统充分利用了区块链的去中心化、不可篡改性等特性,将数据关键信息锚定在主链上,同时控制了不同用户对电子数据的访问权限,有效解决了电子数据存证存在的安全问题。为用户提供了数据上传、下载、查询、比对和授权等服务,同时引入了分布式存储技术和用户积分机制,增加系统的可靠性。

关键词: 区块链;智能合约;去中心化;分布式存储;电子数据

Abstract: An electronic data storage and certificate system is designed in this paper. This system makes full use of the decentralization and non-tampering of the blockchain. The key data information is anchored on the main chain, and the access rights of different users to electronic data are controlled. Thus, the security problems of existing mechanisms are resolved. The system provides users with data upload, download, query, comparison and authorization services. The distributed storage technology and user integration mechanism are introduced to increase the reliability of the system.

Key words: blockchain; smart contract; decentralization; distributed storage; electronic data

区块链作为一项新兴科技,运用了分布式存储、共识机制、点到点(P2P)网络、加密算法等技术,它实质上是提供拜占庭容错以保证一致性的去中心化分布式数据库。与传统的数据库将读写数据库的权限完全交付给某个公司或管理员的中心化方式不同,区块链以去中心化和去信任的方式允许全球范围内任何有能力的节点成为区块链网络的成员之一,享受与其他所有节点同等的读写操作权利,集体维护区块链的运行。最终,区块链系统中的所有节点通过共识机制同步彼此的数据信息,以保证在区块链网络中所有数据的一致性和可靠性。

电子数据是现代高科技的产物,它需要我们对它进行存储并且防篡改。电子数据具有易创建、易存储、易传输和高利用率等特点,是可靠、有证明力度的电子数据证据。数据存证首先要对数据按类型进行很好的存储保存,并且还要对数据的可信性、完整性有很好的保障,并且还要方便对数据进行存储、共享、验证、分享等操作。区块链技术可以保障完善的安全加密性和用户验证。

目前电子存证还有几个问题需要解决:(1)存证过程中自动化程度不高;(2)存证过程中电子数据存证风险较大;(3)第三方机构法律处理流程繁琐;(4)电子数据安全缺失;(5)双方信任缺失。

在文章中,我们提出了一个安全的、可扩展的电子数据存证系统,该系统采用数据与用户对应映射关系查找来确保对电子数据池的高效访问控制。我们设计了一个基于区块链的数据存证方案,允许数据用户/所有者在身份验证后,从电子存储库访问电子数据。数据存储主要进行分片冗余算法和分布式存储保证数据安全性,并且系统引入用户积分机制,保证系统负载均衡。验证和后续服务封闭在系统内部,写入区块并成

收稿日期:2018-10-23
网络出版日期:2018-11-24
基金项目:国家自然科学基金(61502247)、数学工程与先进计算国家重点实验室开放基金课题(2017A10)、信息网络安全公安部重点实验室开放课题(C17611)

为区块链的一部分。

1 区块链研究的相关工作

1.1 区块链主要应用方向现状

XIA Q在他们的研究中简要地解决了医疗数据共享系统中的访问控制管理问题，主要设计了一个基于区块链的数据共享方案[1]，允许数据用户/所有者在身份验证和加密密钥验证后，从共享存储库访问电子病历。SIFAH E B等人也提出了基于区块链的共享医疗数据方案，重点在于提供数据访问控制、出处和审计的同时[2]，在云服务提供商之间共享医疗数据。SHAE Z提出了一个用于临床试验和精密医学的区块链平台架构，并讨论了各种设计方面问题，并对技术要求和挑战提供了一些见解[3]。

VO H T等人研究了一个基于区块链的即付即用的汽车保险应用，系统透明地保存记录并根据运行时间条件执行智能合同，确保所有与用户有关的数据都被透明地记录下来[4]。XU R等人提出了一种基于区块链的网络媒体数字版权管理方案，该方案可以利用区块链的这些功能来实现网络媒体的有效生产管理、版权管理、交易管理和用户行为管理[5]。

针对区块链访问控制的研究也有很多，例如：ZYSKIND G等人提出当使用第三方移动服务时，需要解决隐私保护问题。与现有应用程序不同，平台只允许用户根据存储在区块链中的访问控制策略[6]更改使用权限。HARDJONO T更详细地描述了基于区块链的访问控制管理的系统，该系统为试图执行交易的实体提供匿名操作但可以进行身份验证，与前面系统相比，在用户匿名实体方面做出了更全面的考虑[7]。

在安全、云存储等方面，业界也有进一步的考虑：LIANG X等人提出了一种使用区块链技术的分散且可信的云数据起源架构。基于区块链的数据来源可以提供防篡改记录，实现云中数据的透明度，增强源始数据的隐私性和可用性[8]。TRAN A B等人提出了一个基于浏览器的工具，用于用户注册的管理和部署，并调用区块链上的智能合约[9]。

1.2 区块链存证方向现状

李兆森等人在基于区块链的电子数据存证应用研究中，从电子数据存储应用场景出发，研究如何将业务与区块链技术相结合，提出一种优化当前数据存储的方法，以此高效地为用户服务[10]。李小良等人在网络犯罪中电子证据的收集及保全分析中探讨网络犯罪中电子证据的收集含义，分析电子证据收集在网络犯罪中的特殊性，提出收集和保存电子证据的方法[11]。徐蕾等人在基于区块链的云取证系统中，采用区块链的分布式数据库特点——首尾相连的链式结构技术，设计了一中去中心化、可验证、不可篡改的系统[12]。邓秀珍等人提出网贷平台电子数据保存的欠缺与对策，提出电子数据保存形式不规范、存证平台的中立性问题不明确、电子数据保存的具体数据技术不明确、存证方面的内容审核、存证服务的收费，以及存证服务的失效等一系列的问题[13]。

电子数据的形式比较混乱，不能有效地统一数据格式，使数据存储的过程更加繁琐。电子数据存储中存在很大的数据安全隐患，中心化的存储方式可能会造成数据被篡改和遗失等风险，使得整个系统不完全可信。其次，电子数据在获得验证结果的等待时间较长，获得结果滞缓，使用户无法及时有效获得结果，不能及时给出相应信息，系统效率低下。我们致力于解决电子数据在目前遇到的各种问题，并研究了基于区块链技术来解决电子数据存证问题的现状。

2 区块链存证的架构设计及技术原理

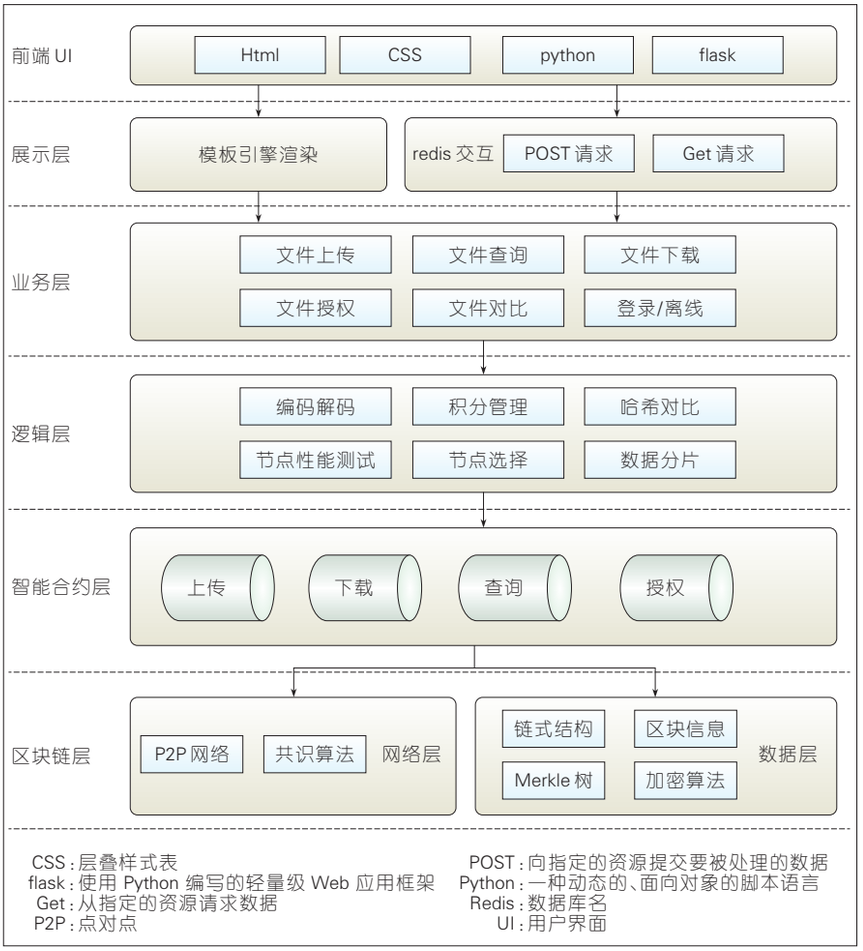
本系统的设计采用浏览器/服务器（B/S）体系结构，分为4层，从上至下依次为：应用层、逻辑层、智能合约层和区块链层，如图1所示。

（1）应用层：主要包含图1中的前端用户界面（UI）、展示层和业务层。前端UI主要负责为用户访问系统提供可视化的Web界面。当获取用户提交的请求后，将用户请求信息发送给逻辑层进行核心计算；等待后台数据处理完毕后，再将用户信息通过Web界面直观地反馈给用户。用户既可以是需要保全数据的客户，也可以是需要下载数据进行公证的第三方机构。

（2）逻辑层：系统核心功能的实现层。根据应用层为用户提供的六大功能界面，逻辑层需要分别给出对应模块的实现方法。其中，基于传输控制协议（TCP）的Socket多线程并发模块是整个逻辑层能够顺利运行的框架基础，系统利用该模块实现多节点之间数据的可靠传输。进一步地，运用里所码的编码解码方式对电子数据进行分片处理，引入用户节点性能测试模块，对节点性能进行排序，用于数据的上传和下载功能模块；引入Hash比对模块检测文件数据是否保存完整；引入用户积分模块，保障系统的负载均衡；引入用户注册、登录功能记录用户信息，方便对用户进行管理。

（3）智能合约层：部署在以太坊上，并与系统进行交互。智能合约层主要负责将逻辑层的数据处理结果（如电子数据及其分片的指纹信息、用户节点的积分信息等）锚定到区块链层的存储区内。系统智能合约主要由若干的结构体组成（如文件、纪录、用户等），并以此结构方式存储电子数据的关键信息。该方法显著地提高了系统查询电子数据的效率，增强了系统的运行速率。

（4）区块链层：系统的去中心化数据库，存储系统交互产生的数据信息。其中，网络层承担信息通信，产生新区块，维护区块链网络稳定运



▲图 1 系统功能架构图

行；数据层保存着整个系统所有上传下载的关键信息。

借助区块链的新兴技术，把电子数据记录分布式存储在区块链上，并结合 Reed-solomon 码、时间戳、哈希算法、模糊层次分析法、理想优基点、客户关系管理（RFM）积分模型和智能合约等技术，我们设计并搭建了基于区块链的分布式存储系统。系统主要对数据进行冗余分片，根据用户需求，将数据分成 n 个信息片和 m 个冗余片，再将数据分片进行分布式存储。对系统存储主机信息进行采集，结合模糊层次分析法和理想优基点，计算出系统存储主机的网络综合性能评分，保证系统数据存储的负载均衡。并根据智能合约去中心化的特点，使用哈希算法进行数据的完整性验证，使用共识算法保障计算节点间数据的一致性。我们设计了一种去中心化的、可验证的分布式存储系统。基于该系统提供的功能，用户可以是双边或多边，等公检法第三方机构共同参与下，自动实现电子数据存证的事务处理和存证机制等。

2.1 区块链技术

区块链是所有节点共享的交易数据库，这些节点基于交易协议参与到网络中来。区块链包含每一个曾在系统中执行过的交易，根据这些交易信息，人们可以找到任何时候、任一个地址的信息。如果把区块链作为一个状态机，则每次交易就是试图改变一次状态，而每次共识生成的区块，就是参与者对于区块中交易导致状态改变的结果进行确认的结果。

在实现上，首先假设存在一个分布式的数据记录账本，这个账本只允许添加，不允许删除。账本底层的基本结构是一个线性的链表，这也是其名字“区块链”的来源。链表由一个个“区块”串联组成，后继区块记录前导区块的哈希值。新的数据要加入，必须放到一个新的区块中，而这个块（以及块里的交易）是否合法，可以通过计算哈希值的方式快速检验出来。任意维护节点都可以提议一个新的合法区块，然而必须经过一定的共识机制来对最终选择的区块达成一致。

2.2 智能合约

智能合约是以太坊中最为重要的一个概念，即以计算机程序的方式来缔结和运行各种合约。在 20 世纪 90 年代，SZABO N 等人就提出过类似的概念[14]，但一直因为缺乏可靠执行智能合约的环境，而被当作一种设计理论。区块链技术的出现，恰好补充了缺陷。

文章中，我们在智能合约的编写过程中，定义了文件、纪录、成员和用户 4 个结构体变量，分别存储电子数据文件的关键信息、电子数据文件分片的关键信息、用户资料和电子数据文件的所有关系。基于上述 4 个变量，我们依次编写了电子数据信息的上传、电子数据信息的查询、电子数据的授权、用户信息的更新和用户信息的查询。考虑到以太坊数据写入的速度较慢，容易影响用户体验，因此采用异步请求方式（sendAsync）执行事务，以此来加快电子数据的查询传输速率。

2.3 密码学

哈希函数是密码学的一个重要分支，它是一种将任意长度的输入变换为固定长度的输出且不可逆的单向密码体制。哈希函数主要运用于数字签名和消息完整性验证。

本文中我们采用哈希算法，主要的过程为：发送方采用单向哈希函数对消息进行计算，得到摘要并发送消息和摘要。接收方将接收到的消息，按同样方式进行哈希函数计算，并将新得出的结果与发送方的原摘要结果进行比对。如结果一致，说明消息完整。在本系统中，摘要信息的不可变，保证了需要存证信息的完整性和真实性。将需要存证的电子数据放在区块链中，避免数据被恶意篡改。

2.4 Reed-solomon 码

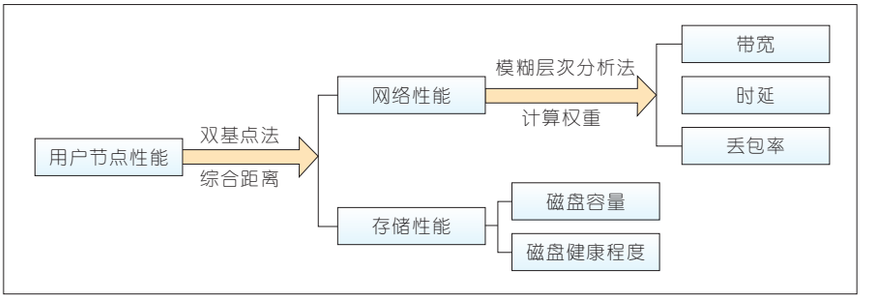
Reed-Solomon 码是一种定义在域上的线性编码方法，该编码方法将 k 个源数据变换生成 l 个编码数据。与前向纠错码（FEC）编码思想一致，我们采用 Reed-Solomon 码来实现数据包层的 FEC 编码变换[15]。

当用户上传电子数据时，系统首先会对电子数据进行分片处理。分片工作主要依赖里所码的编码实现。用户需要提供2个重要参数：信息分片数目和冗余分片数目。系统根据上述2个参数和待上传文件的大小，调整出恰当的编码缓冲区大小，完成对文件的分片处理。

2.5 多目标节点决策模型

作为一个电子数据存证系统，本系统依赖于多个用户节点共同完成电子数据的存证保管工作，这一过程涉及到对多用户节点的选择。文章中，我们设计了如何挑选出系统当前性能最优的若干节点并协同完成分布式的存储工作。图2展示了用户节点性能评估的主要设计过程。

对比以太坊依靠各节点的计算力使之持续运转，本系统主要依靠各节点的存储算力。因此，决定对用户节点的性能评估从网络性能和存储水平2方面展开。其中，网络性能的高低影响电子数据分片的传输速度，存储水平的高低影响电子数据分片的存储可靠性。网络性能的参数比重通过模糊层次分析法（FAHP）计算



▲图2 用户节点性能评估框架

出。然后通过双基点法（TOPSIS）计算各优基点与理想/反理想优基点的欧氏距离，得出综合距离并进行节点顺序排名。

3 区块链存证的系统工作步骤

我们制定了数据共享机制，以确保数据的安全性和出处。存证系统的详细流程如图3所示，主要分为6个步骤。

（1）用户登录本系统后，该用户节点首先向系统各节点广播本节点性能文件，系统合约成员类获取用户信息，并通过用户节点获取到其他用户节点的性能信息，为后面的数据分片存储获取性能主机的值。

（2）用户上传需要存证的文件，将文件的关键信息写入到合约文件类中去，以此建立用户和数据的对应映射关系。

（3）系统利用冗余分片算法对上传的电子数据进行分片，然后根据前面获取的节点性能信息选取若干最优性能的节点，用于存储系统的分片数据。

（4）系统根据性能评分排序选中的节点，对不同的节点进行数据分发，并将分发的信息返回给智能合约，包括数据分片存储的IP地址、分片存储的绝对路径和数据分片的哈希值等。

（5）当用户需要对电子数据进行下载或查询访问操作时，系统根据用户请求、用户授权请求，将用户信息与需要访问的数据建立对应的映射关系，然后用户便可以进行操作。

（6）系统从合约中读取到电子数据的相关存储信息，通过存储信息获得电子数据存储的位置，并下载电子数据分片，还原数据并比对文件哈希值，以验证电子数据的完整性。

基于区块链智能合约的存证系统的主要任务是对电子证据进行上传、保全、查询、比对和下载。本系统基于去中心化设计，不再需要系统管理人员，转而使用智能合约进行数据交互。系统主要功能有4个特性：安全性、完整性、机密性和可授权性。

（1）系统的安全性。使用基于Reed-Solomon的编码方式进行分布式存储，在节点主机被攻击、磁盘损坏等分片被丢失的情况下仍然可以还原文件，同时分布式还可以降低中心化服务器被内部篡改的风险。

（2）系统的完整性。使用哈希算法SHA-256对文件进行完整性校验，并把校验存储于区块链智能合约中。

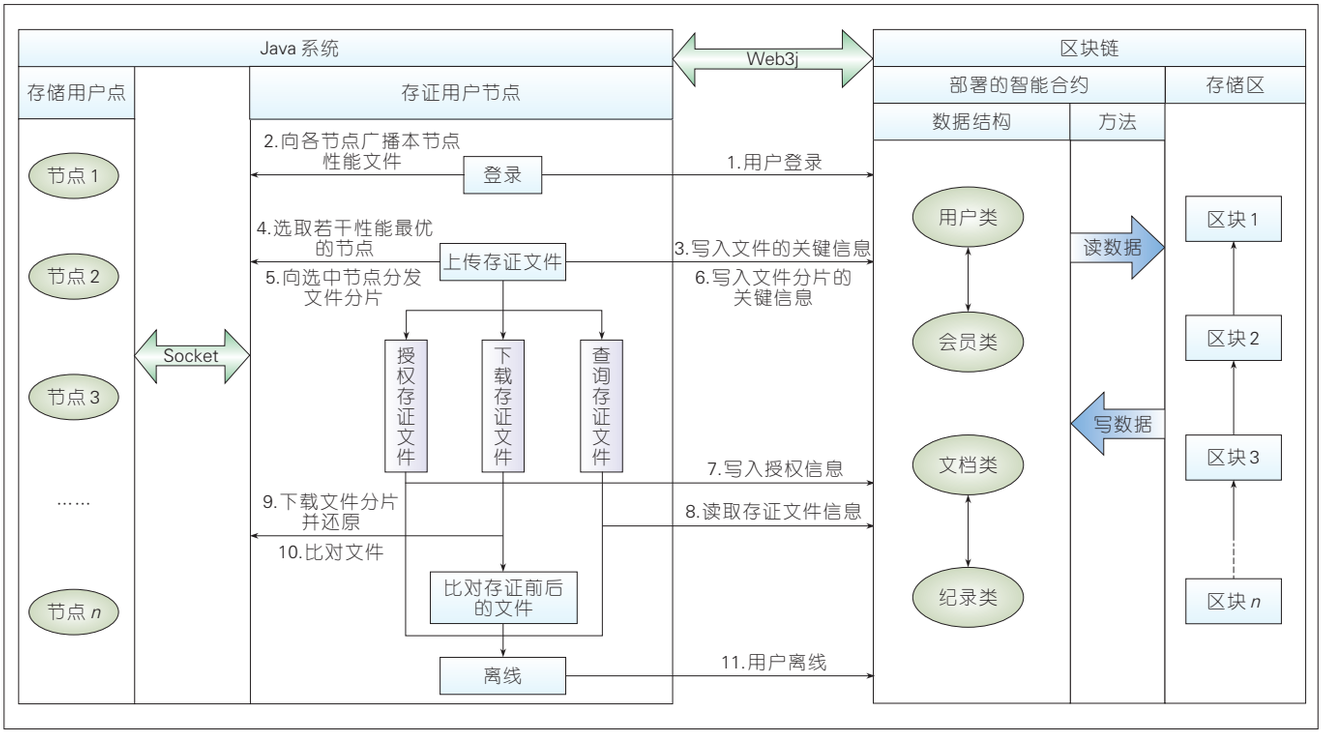
（3）系统的机密性。去中心化分布式存储，可以保证任一单一存储节点无法得到完整文件信息，更不可能还原信息，这可防止存储主机被黑或者内部人员泄露信息。

（4）系统的可授权性。用户上传保存的文件除了由用户自己访问之外，还可以由被用户授权的第三方来访问。

系统主要的六大模块功能，将在以下的小节中详细介绍。

3.1 系统数据保全功能

系统先根据用户分片需求计算



▲图3 系统详细流程图

出本次保全用户所需花费的积分，然后获取区块链中用户对应积分值进行积分数值更新。当用户积分值 c 大于上传操作花费 m 时，系统才提供上传功能。若是积分值 c 小于 m 时，系统会提醒用户积分不足，无法进行上传操作，如图4所示。

3.2 系统上传功能

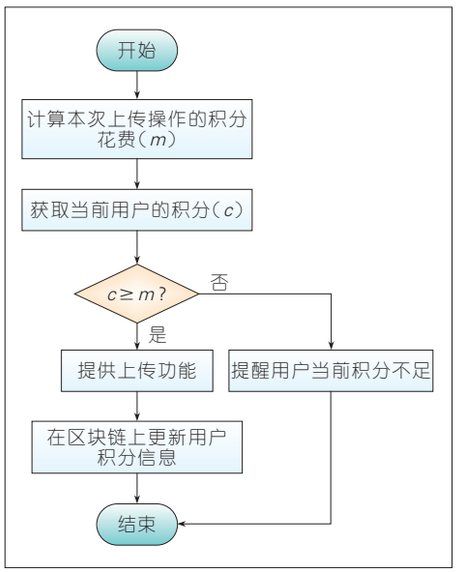
用户首先在本系统注册，提交完注册信息后就拥有注册用户初试积分，同时用户所在主机会在对系统内的主机发送请求，提出电子数据上传操作，并获取到系统其他主机的性能，计算出系统所有主机性能评分情况。然后系统会根据用户设定的电子数据分片数目，将数据进行分片并将其进行存储分发，同时将文件分片信息写入到区块链中，并更新用户在区块链上对应的积分数值，具体如图5所示。

3.3 系统数据查询功能

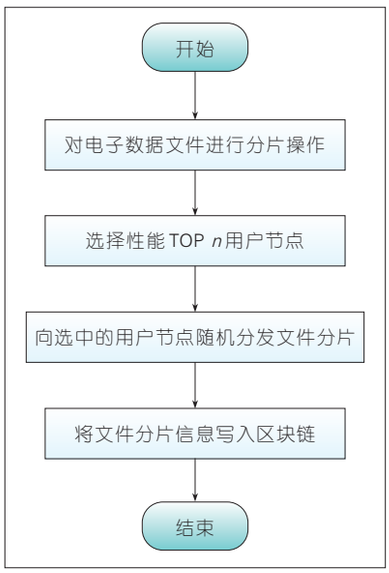
在本系统中，用户可以即时查询获取文件的电子数据。根据电子数据用户隐私需求，电子数据仅该用户自己可见（在默认情况）。当用户需要查看其他用户的电子数据时，先给出需要查看文件的序号，系统根据文件序号查询区块链上文件序号对应用户的用户名。当文件属于查看用户的用户名时，则可以查看用户数据；如果文件不属于该用户名类，则文件不能被查看，具体如图6所示。

3.4 系统数据下载功能

当用户下载文件时，系统先判断用户是否拥有该文件的访问权限，如



▲图4 系统保全流程图

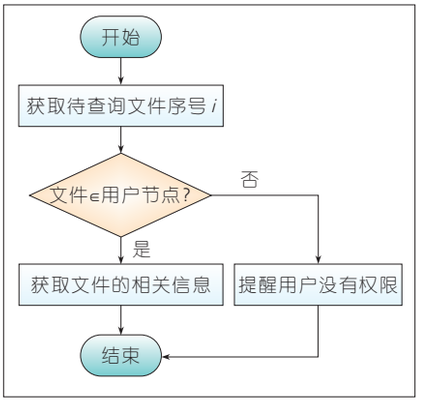


▲图5 系统上传流程图

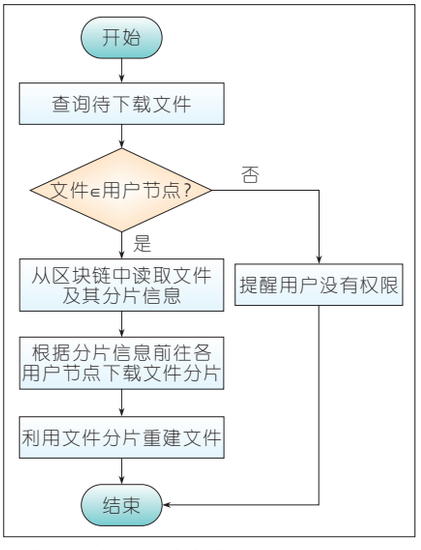
果拥有权限，系统从区块链合约中读取该文件的分片信息，根据分片信息获取分片存储主机地址和路径，然后下载数据分片并重新组合数据。这与上一步的电子数据查询功能类似，用户下载的数据文件必须获得相应的授权，以此保证用户的隐私安全，具体如图7所示。

3.5 系统数据比对功能

系统在获得数据分片后，对分片进行哈希计算，得到每个分片的哈希值后，与之前原数据存储在智能合约中的哈希值进行比对、验证。如果哈希值相同，则系统返回数据未被改动；反之，则提醒用户数据已经被篡改。另外，考虑到分布式存储的容错性，如果出现部分分片丢失，只要丢失的分片数量小于系统数据冗余分片数量，系统仍然能够还原数据源文件，具体如图8所示。



▲图6 系统查询流程图



▲图7 系统下载流程图

3.6 系统数据授权功能

考虑到系统的功能需求，我们要对用户的个人隐私进行保护，所以系统默认用户的电子数据是用户个人所拥有，他人在没授权情况下无法查看。用户可以授权给他人，被授权用户可以查看被授权的文件和电子数据。授权主要将授权用户的公钥输入系统与待授权文件建立映射关系，并写入区块链，则完成授权，具体如图9所示。

4 系统功能测试与评估

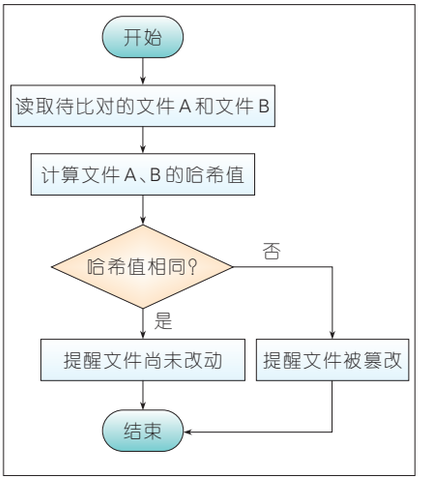
我们提出的区块链存证系统拥有以下功能。

（1）系统为存储应用程序中的所有数据访问提供实时审核。我们使用电子数据文件作为数据单元，对数据对象的所有操作进行审计，并使用区块链进行记录。通过这种方式，可以收集和监测控制所有电子数据访问情况。

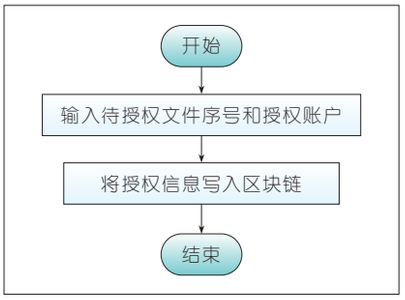
（2）系统为文件安全纪录保存提供防篡改时间戳。对于每条电子数据，我们都会将数据上传到区块链网络，我们创建了不可改变的文件数据指纹，并且通过验证区块链数据对比来检测对系统数据的任何更改。

（3）系统为用户数据提供隐私保护。用户访问记录在区块链网络中是匿名的。数据源是无法查询到用户账户。匿名保存体现在2个方面：一方面，由于用户ID被散列随机，所以用户身份不会和源数据连接到一起；另一方面，也实现了每个用户之间的不可连接性，尤其是对于被授权数据的上传用户保护。

文章中，我们对基于区块链的电子数据存证系统进行功能测试，分析该系统功能的可用性、界面的合理性和数据交互的正确性等。



▲图8 系统比对流程图



▲图9 系统授权流程图

为了验证该系统可使用性和扩展性，实验模拟了系统在局域网下的数据分布式存证。测试环境为：在局域网内，部署了4台linux服务器，同时运行服务端程序，与客户端进行数据同步交互。

针对以上系统实验，我们进行了压力测试。在验证时，我们设置相同的区块生成时间，然后分别选取不同的时段进行数据验证。我们共选取了50组不同大小的电子数据文件（文件大小从23 kB到3 900 kB不等），并依次将文件按照系统提供功能进行验证，然后记录并对比系统完成一次流程的时长，另外操作的数据类型也不同，以此获得更多数据的评估时间。另外，我们专注于为每个起源数据请求区块链存证的效率。通过计算可得出：每次运行操作1条记录，平均每条数据大小为1 054.7 kB，平均耗费时间为4～7 s。对于每次

不同数据的操作，都会记录不同文件操作的所花费的平均时间，并最后计算获得结果如表1。

▼表1 实验结果评估表

操作类型	文件平均大小/kB	平均消耗时间/s	数据验证率/%
文件上传	1 054.7	7.3	100
文件查看	1 054.7	5.8	100
文件下载	1 054.7	4.4	100
文件对比	1 054.7	4.7	100

表1显示：系统对数据检索的速率一般，数据验证对比结果正确率达到百分百，也就是说系统可以完整地对数据进行存证。

5 结束语

本文的主要贡献如下：

（1）提出了一种将电子数据存证与区块链技术相结合的系统，电子数据的存证用于对各类数据的存储和验证，区块链技术用于对获取到的电子数据进行固定保存。

（2）应用了电子数据的分布式存储方式，对数据进行冗余分片，保证了数据的存储安全性。并在系统中引入积分制度，按照用户上传存证和提供存储方式进行积分的数据变化，维持系统的负载均衡，保证了系统的安全性和稳定性。

借助区块链这一全新技术，我们将电子数据的“数字指纹”存储在区块链上，并利用智能合约、分布式存储、容错编码、多属性决策等技术，设计并实现了基于区块链的电子数据存证系统。系统基于区块链的去中心化和不可篡改的属性，保证了电子数据的真实性、完整性和唯一性。此外，本系统针对用户还制订了积分制度，以保证系统能吸引更多用户，继而提高本存证系统的可靠性。

我们还开发了一个简易的基于区块链的电子数据存证系统，该系统主要是在局域网内进行主机分布式存储，未来还需要进一步优化，实现可以广域网内进行分布式存储。另外，我们认为区块链所使用的共识机制是PoW，此机制时间周期较长，资源需求过高，可以进行优化。我们所提的系统客户端与服务器端通信过程中，采用的是明文通信方式，存在安全隐患，后面可以使用对称加密来完善安全性。

致谢

本文的工作得到了南京邮电大学李华康老师的指导和帮助，雷鹏同学承担了部分试验工作，谨致谢意！

参考文献

[1] QI X, EMMANUEL B S, ABLA S, et al. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments [J]. Information, 2017, 8(2):44. DOI: 10.3390/info8020044
[2] XIA Q, SIFH E B, ASAMOAH K O, et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain [J]. IEEE Access, 2017, (5): 14757-14767. DOI:10.1109/access.2017.2730843
[3] ZOYIN S, JEFFREY N. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine[C]//2017 IEEE 37th International Conference on Distributed Computing Systems. USA: IEEE, 2017:1063-6927. DOI: 10.1109/ICDCS.2017.61
[4] XIA Q, HOANG T V E, LENIN M, et al. Blockchain-Based Data Management and Analytics for Micro-Insurance Applications [C]// CIKM '17 Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. USA: ACM, 2017: 2539-2542. DOI: 10.1145/3132847.3133172
[5] XU R Z, ZHANG L, ZHAO H, et al. Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology[C]//2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). USA: IEEE, 2017. DOI: 10.1109/ISADS.2017.21
[6] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]//Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). USA: IEEE, 2015: 180-184. DOI: 10.1109/SPW.2015.27
[7] HARDJONO T, SMITH N. Cloud-Based Commissioning of Constrained Devices Using Permissioned Blockchains [C]// Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS '16, 2016.USA:ASM,2016. DOI:10.1145/2899007.2899012
[8] LIANG X P, SHETTY S, TOSH D, et al. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability[C]//2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). USA:IEEE, 2017: 468-477. DOI:10.1109/CCGRID.2017.8
[9] AN B T, XU X W, WEBER I, et al. Regerator: a Registry Generator for Blockchain[C]// CAiSE 2017 Forum and Doctoral Consortium Papers. Germany: CAiSE, 2017: 81-88
[10] 李兆森, 李彩虹. 基于区块链的电子数据存证应用研究[J]. 软件, 2017, 38(8): 63-67
[11] 李小良. 网络犯罪中电子证据的收集及保全分析[J]. 法制与社会, 2016, (32): 258-259. DOI:10.19387/j.cnki.1009-0592.2016.11.270
[12] 徐蕾. 基于区块链的云取证系统[D]. 四川:西南科技大学,2017
[13] 邓秀珍, 周恒. 网贷平台电子证据保存的欠缺与对策[J]. 金融电子化, 2016(10): 30-31
[14] 王春宇,张守坤.智能合约与金融合约[J].商, 2016(6):198
[15] 黄宏博, 肖峻岭, 佟俐鹃. 基于Reed-Solomon算法的QR码纠错编码[J]. 计算机工程, 2003, 29(1): 102-104

作者简介

冒小乐，南京邮电大学在读硕士研究生；主要研究方向为区块链相关技术。

陈鼎洁，复旦大学在读硕士研究生；主要研究方向为区块链相关技术。

孙国梓，南京邮电大学教授；主要研究方向为电子数据取证、区块链技术；先后主持和参加基金项目10余项，获得3项科研成果奖；已发表论文100余篇，被SCI/EI检索60余篇。