Computer Science and Application 计算机科学与应用, 2023, 13(12), 2268-2281
Published Online December 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1312227

Hans汉斯

基于区块链的网络化协同设计数据存储与管理方案

黄光亮，周振兴

中航机载系统共性技术有限公司，江苏 扬州

收稿日期：2023年11月20日；录用日期：2023年12月18日；发布日期：2023年12月25日

摘　要

针对网络化协同设计过程中数据存储、共享或交互过程中权限管控、核心数据保护等方面存在的问题，提出基于区块链的数据可信存储和管理方案。采用IPFS文件系统存储文件，利用无证书密码体制对文件哈希摘要进行加密，将加密的哈希摘要上链存储，结合智能合约实现数据的可信传输、共享、存证及操作追溯。通过IPFS文件系统和区块链的结合，实现网络化协同设计数据的安全存储和管理。分析表明，该方案在数据安全性、访问控制、数据存证追溯等方面具有明显优势，能够满足多方协同设计场景数据保护的需要，且具有良好的系统性能。

关键词

区块链，IPFS，数据可信存储，网络化协同设计

Blockchain Based Secure Storage and Management Scheme for Networked Collaborative Design Data

Guangliang Huang, Zhenxing Zhou

AVICAS Generic Technology Co., Ltd., Yangzhou Jiangsu

Received: Nov. 20th, 2023; accepted: Dec. 18th, 2023; published: Dec. 25th, 2023

Abstract

In response to the challenges in data storage, sharing, permission control, and core data protection during the networked collaborative design process, a solution based on blockchain for trust-

文章引用: 黄光亮, 周振兴. 基于区块链的网络化协同设计数据存储与管理方案[J]. 计算机科学与应用, 2023, 13(12): 2268-2281. DOI: 10.12677/csa.2023.1312227

worthy data storage and management is proposed. The IPFS file system is employed to store files, and a certificate-less password system is used to encrypt the hash digest of the files. The encrypted hash digest is then stored on the blockchain, and, in conjunction with smart contracts, achieves trustworthy transmission, sharing, certification, and operation traceability of data. By combining IPFS file system and blockchain, the solution achieves secure storage and management of networked collaborative design data. Analysis shows that this approach has significant advantages in data security, access control, data certification traceability, and is capable of meeting the data protection needs in multi-party collaborative design scenarios with good system performance.

Keywords

Blockchain, IPFS, Trusted Data Storage, Networked Collaborative Design

1. 引言

工业互联网、云计算等技术的演进促进了网络化协同生产模式的发展，形成协同设计、协同制造、协同供应链等生产及管理体系。不断成熟的协同工具或平台为网络化协同提供了技术支撑，使得行业内不同企业间的协同成为可能。其中协同设计是关键环节，产生的数据是企业的核心资产，具有高价值、高保密性、企业独有等特点。参与网络化协同设计的企业间存在大量的数据共享和交互，这为企业核心数据的保护带来了新的挑战。如何保证协同设计过程中产生的数据不被恶意破坏、篡改，数据操作的记录真实可靠、全程可追溯，进而保护各企业的核心数据资产和知识产权，直接影响到网络化协同的意愿和研发设计效能。

网络化协同设计的模式是多个企业在同一平台开展设计研发工作，平台对硬件和软件资源以多租户的形式进行逻辑隔离，为每个企业用户提供独立的数据存储空间，从而避免数据的非法访问。从物理层面看，数据采用集中是存储模式，这种模式存在两方面的问题，一方面数据存储设备一旦在外界攻击下崩溃，必然导致数据丢失或破坏。另一方面，数据资产的保护很大程度上取决于各企业的管理能力和用户的安全意识，数据共享和交互的过程中一旦处理不当，则会造成数据的泄露。同时数据的集中存储存在特权账号管控或利用漏洞绕过监管而导致的安全问题。数据一旦被窃取、篡改、删除或破坏，势必对企业的安全生产带来严重威胁与损害。

区块链技术的出现为网络化协同设计数据的存储和管理提供了可信的解决方案。区块链技术具有独特的特点，其中包括去中心化、透明性、安全性、不可篡改性和智能合同等。它不依赖于单一中央权威，而是分布式的，使多个参与者能够共享和验证交易数据，增加了信任。数据在区块链上是公开的，但受到强大的加密保护，确保了机密性和完整性。一旦信息被添加到区块链上，几乎不可能删除或修改，从而确保了交易历史的安全性。此外，智能合同使自动化和自执行的合同成为可能，减少了第三方中介和减轻了风险。利用区块链技术对数据进行存储和管理，通过智能合约对数据设置访问权限条件，可以保证数据存储的可信可靠。

国内外不少研究人员在利用区块链来实现数据安全存储和共享方面作了探索和实践。文献[1]构建了企业隐性知识共享的激励模型。文献[2]提出了一种无需网关支持的面向区块链的访问控制方案。文献[3]

基于 IPFS 分布式存储系统与区块链技术实现了去中心化的音乐数据共享平台。文献[4]采用 IPFS 系统与区块链技术融合进行融媒体数据安全存储，降低了存储成本并节省了网络带宽。文献[5]提出一个基于区块链的电子健康记录数据安全存储共享方案。文献[6]在分析区块链关键技术的基础上，结合 IPFS 系统提出了一种基于联盟区块链技术的知识共享模型。文献[7]针对用户行为和授权信息的存证与监管等问题，提出一种基于联盟路的敏感数据共享方案。由于工业设计产生的数据往往体量大、数量多，区块链技术由于自身区块结构限制，在大数据量存储和吞吐效率方面难以满足存储和管理的要求。目前并没有使用 IPFS 结合区块链技术解决网络化协同设计过程中数据的安全存储、可信传输、操作追溯等方面的研究

本文针对网络化协同设计数据可信存储和管理的问题，提出了一个基于区块链的数据存储和管理解决方案。方案利用 IPFS 文件系统的存储特性，通过无证书密码体制对设计数据的哈希摘要进行加解密操作，将加密的哈希摘要数据存储在区块链上，利用区块链去中心化、不可篡改、可追溯等特点，构建一个针对网络化协同设计的数据传输、共享、存证、操作追溯的可信管理方案，实现多方协同设计下数据的安全可信存储。

2. 相关知识

2.1. 区块链技术

区块链技术具有高度透明、去信任、去中心化、匿名、可追溯等特性，能够通过分布式共识机制实现去中心化的点对点数据共享，为中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决途径。区块链系统一般由应用层、合约层、激励层、共识层、网络层、数据层等 6 个部分组成。区块链是一个链式分布式存储结构，每一块中包括了交易的信息以及前一块的 hash 值，区块之间通过存储的前一区块 hash 值首尾相连，若区块信息被篡改，则当前区块的 hash 值会改变，由区块的存储结构可知，当一个区块 hash 值被篡改，所有的区块的 hash 值都会随之改变，这其中的工作量巨大且不易实现，使得区块链拥有了其不可篡改的特性。区块链的链式存储结构如图 1 所示。

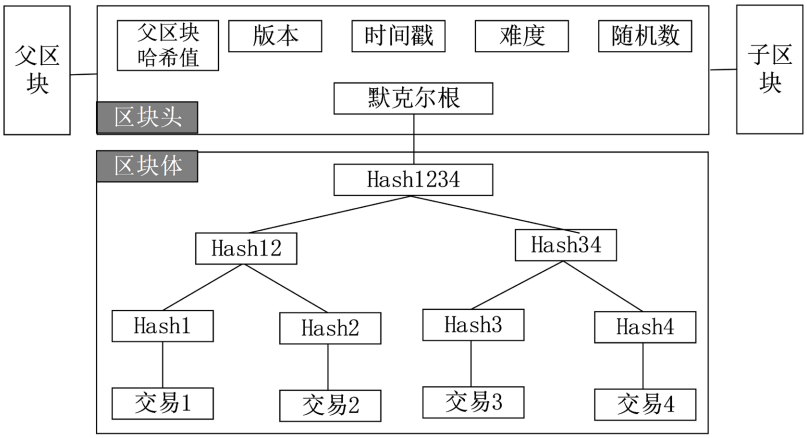

Figure 1 The chain-like structure of blockchain
图 1. 区块链的链式结构

区块链分公链、联盟链和私有链三种形态。其中，联盟路相较私链联盟链具有更多操作空间，相较公链具有更好的安全机制，因此联盟路是应用最广泛的区块链形态，具有最大的商业用价值。联盟链内可存在多个组织机构进行共同维护，链内节点可分群组管理，不同群组由不同组织机构负责，实现不同功能与应用，多个群组在链中共同完成记账功能。

2.2. 区块链智能合约

智能合约的概念由 NickSzabo 在 1994 年首次提出[8]，是“执行合同条款的计算机协议”，它是一段布置在区块链上在满足特定条件下自动执行的程序代码。区块链智能合约具有多重特点，包括自动执行、不可篡改性、透明性和高度可编程性。这些合约是基于区块链上的代码，能够根据预设的条件自动执行，无需中介人介入。由于其不可篡改的性质，合同一旦部署便难以修改，确保了交易的可信性。合同的执行过程是公开透明的，可供参与者查看，从而增加了信任度。最重要的是，智能合约非常灵活，可以用于多种应用，从金融交易到供应链管理，开启了无数创新和自动化的可能性，提供更高效、透明和安全的交易方式。智能合约相当于一张电子合同，该合同只要启动开始执行，双方即可完成真实可信的交易。在大部分的区块链平台上，智能合约可以通过高级语言(Golang、Rust、Solidity、TinyGo、C++等)来编写，经过编译后以二进制文件、WASM、EVM 字节码的形式存储在区块链中，用户可以通过发送交易来触发执行智能合约中的代码。

2.3. IPFS 数据存储技术

IPFS (InterPlanetary File System)星际文件传输系统，是一个利用点对点传输建立的分布式超媒体分发协议，提供了永久的去中心化存储文件的方法。IPFS 是通用目的的基础架构，基本上没有存储上的限制。大文件会被切分成小块，下载的时候可以从多个服务器中同时获取。IPFS 的网络是不固定的，细粒度的，分布式的网络，可以很好的适应内容分发网络的要求。这样的设计可以很好的共享各类数据，包括图像，视频，数据库，甚至整个操作系统。当要查询一个文件时，运行着 IPFS 节点的计算机会询问其所有对等点是否存在这个特定哈希值(hash 值)的文件，若存在，则只需输入存储文件时返回的 hash 值，IPFS 系统就会根据文件检索表和内部的路由表自动查找并合并各文件块组成原始文件，拥有该文件的节点将会返回整个文件。

IPFS 基于内容寻址，将信息保存到 IPFS 节点中，IPFS 系统将会返回基于该信息计算得出的唯一哈希值。哈希值与信息内容一一对应，即使只对信息内容做轻微修改，也会得到完全不同的哈希值。当 IPFS 被请求一个文件哈希时，它会使用一个分布式哈希表找到文件所在的节点，取回文件并验证文件数据。IPFS 可存储的文件格式不受限制，存储空间也不受限制，具有通用性。当文件大小超过数据块容量大小时，会被网络分块上传，获取该文件时只需要从多个节点一起下载即可。

IPFS 具有以下优点：① 下载速度快。它使用的 BitTorrent 协议，使数据在 IPFS 网络上的传输速度更快。② 安全性高。它去中心化的特性，让知识存储更加安全，不会因为一个节点出现故障而导致数据文件无法下载或上传。③ 低冗余。IPFS 是按内容寻址的块存储模型，根据内容寻址在全局命名空间中明确地识别每个文件，降低了网络存储的冗余。

2.4. 无证书密码体制

无证书公钥密码体制由 Al-Riyami 和 Paterson 提出[9]。无证书密码体制是一种密码学方法，它允许双方在通信中验证对方的身份而无需使用传统的数字证书或公钥基础设施(PKI)。在这种体制下，通信双方依赖于密码技术和共享的密钥来确保通信的安全性和身份验证。这种方法相对于传统的证书基础设施更为灵活，减少了复杂的证书管理。在无证书公钥密码体制中，密钥生成中心绑定与用户身份并生成公私钥对，且密钥生成中心不能获知任何用户的私钥[10]。鉴于以上优势，应用前景将随着数字化社会的不断发展而扩大，为各行各业提供更高级别的安全性和便利性，尤其在无证书签名方法、无证书代理重加密等方面的应用[11]。

3. 方案设计

网络化协同设计数据存储在基于 IPFS 的数据可信存储系统中，通过对关键数据加密解密实现数据的访问权限控制。在数据拥有者获得 IPFS 系统返回的数据哈希值之后，首先利用无证书密码体制中的公私钥对生成方法建立与自己身份相关的公钥和私钥，将数据哈希值通过特定公钥完成加密处理生成哈希密文。在具有权限的用户在链上获取交易信息后，可以使用自己的私钥对哈希密文进行解密，使用解密后的哈希明文即可在 IPFS 系统中下载指定文件。

3.1. 访问控制机制

访问控制机制的实现采用无证书密码体制，无证书数字签名体制的算法由七部分组成。而算法所涉及到的成员有：签名者 A、验证者 B 和密钥生成中心 KGC 三方面。七部分算法功能描述如下：

(1) 系统初始化算法实现的功能是：在系统输入端输入参数 λ，在输出端输出主密钥 SK 和系统参数 K。

$$\mathrm{SysParGen}(\lambda) \to \mathrm{K,SK}$$

(2) 秘密值生成算法实现的功能是：在系统输入端输入参数 K 和用户身份 ID，在输出端输出用户秘密值 X。

$$\mathrm{USKGen}(\mathrm{K,ID}) \to \mathrm{X}$$

(3) 部分私钥生成算法实现的功能是：在系统输入端输入参数 K、系统主密钥 SK 和用户身份 ID，在输出端输出用户部分私钥 PSK。

$$\mathrm{PSKGen}(\mathrm{K,ID,SK}) \to \mathrm{PSK}$$

(4) 私钥生成算法实现的功能是：在系统输入端输入参数 K、用户部分私钥 PSK 和秘密值 X，在输出端输出用户私钥 SK。

$$\mathrm{SKGen}(\mathrm{K,X,PSK}) \to \mathrm{SK(a)}$$

(5)公钥生成算法实现的功能是：在系统输入端输入参数 K 和用户的秘密值 X，在输出端输出用户的公钥。

$$\mathrm{PKGen}(\mathrm{K,X}) \to \mathrm{PK(a)}$$

(6) 签名算法实现的功能是：在系统输入端输入代签名的消息 Info、用户的身份信息 ID 和用户的私钥 PK，在输出端输出一个签名。

$$\mathrm{SigGen}(\mathrm{Info,ID,PK}) \to \mathrm{Sig(a)}$$

(7) 验证算法实现的功能是：在系统输入端输入消息、签名、系统公开参数、签名人公钥和身份信息，如果签名为真，则在输出端输出 A，否则在输出端输出 B

$$\mathrm{Verif}(\mathrm{Info,Sig(a),K,PK(a),ID}) \to \mathrm{A(T)}\,|\,\mathrm{B(F)}$$

权限验证包括用户签名和认证流程，具体过程介绍如下：

1) 数据拥有者 A 调用系统参数 K 和用户私钥 SK 对数据摘要密文进行签名，并返回签名结果。

2) 具有查看权限的用户 B 通过传入哈希摘要密文信息、签名、系统公开参数 K、数据拥有者 A 的 ID、公钥 PK，对签名的有效性进行确认。

认证流程示意如图 2 所示：

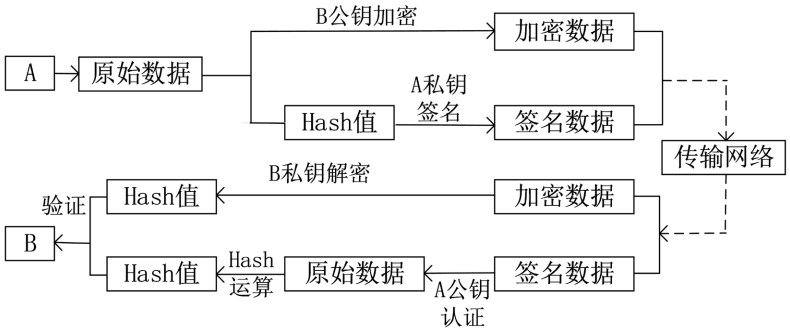

Figure 2. Signature authentication process
图 2. 签名认证过程

3.2. 数据传递

数据传递指网络化协同设计过程中，文件基于 IPFS 文件系统和区块链技术在拥有者和使用者之间的可信传递，过程如图 3 所示：

1) 文件拥有者将文件存入 IPFS 系统，并对文件哈希摘要明文加密，将加密后的文件哈希摘要密文存入区块链系统；

2) 文件使用者在区块链上获得相关信息后，向文件拥有者请求数据授权，文件拥有者同意后向文件使用者发送签名等认证信息；

3) 文件使用者经过访问控制模块认证后，触发区块链系统数据下载智能合约；

4) 区块链系统返回文件哈希摘要密文，密文经访问控制模块解密后，获得文件哈希摘要明文；

5) 文件使用者向 IPFS 系统传入文件哈希摘要明文，下载原始文件。

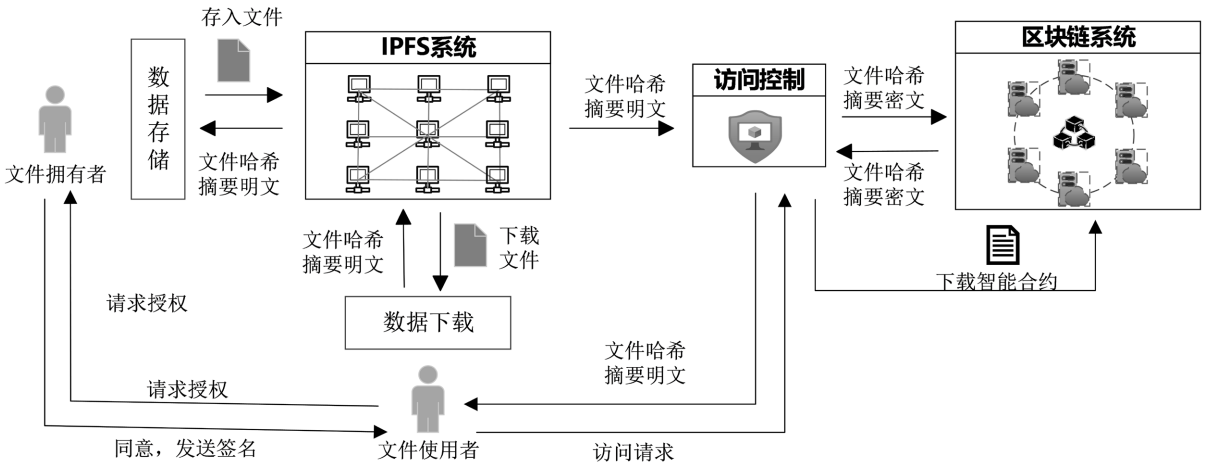

Figure 3. Data transmission process
图 3. 数据传递过程

3.3. 数据存证

网络化协同设计产生的数据，数据创造者或拥有者可以将数据的证明信息存入区块链，利用区块链不可篡改、可追溯等特点证明数据的归属，确保数据的完整性、防篡改伪造等，这一过程也称为锚定。基于区块链的数据存在是知识产权声明的重要手段，可以作为法律取信的证据。数据存证的过程如图 4

所示：

1) 文件拥有者将文件存入 IPFS 系统，系统返回文件哈希摘要明文；

2) 文件拥有者将文件摘要明文加密后，将生成的文件摘要密文存入区块链系统；摘要加密前可以增加时间戳、数字水印等附加信息；

3) 取证时，文件拥有者触发查询智能合约，获取文件哈希摘要密文，文件拥有者利用自己的身份 ID、秘钥等信息对密文进行解密，获得文件哈希摘要明文；

4) 解密后的摘要明文及时间戳、数字水印等信息可以证明文件的合法拥有者文件拥；另外可将链上、链下存储的摘要明文进行比对，确定文件是否被篡改。

3.4. 数据共享

网络化协同设计过程中，存在大量的交流协作和数据流转，数据共享是文件拥有者发起定向的文件传输，实现协作的同时保护数据的安全。数据共享过程如图 4 所示：

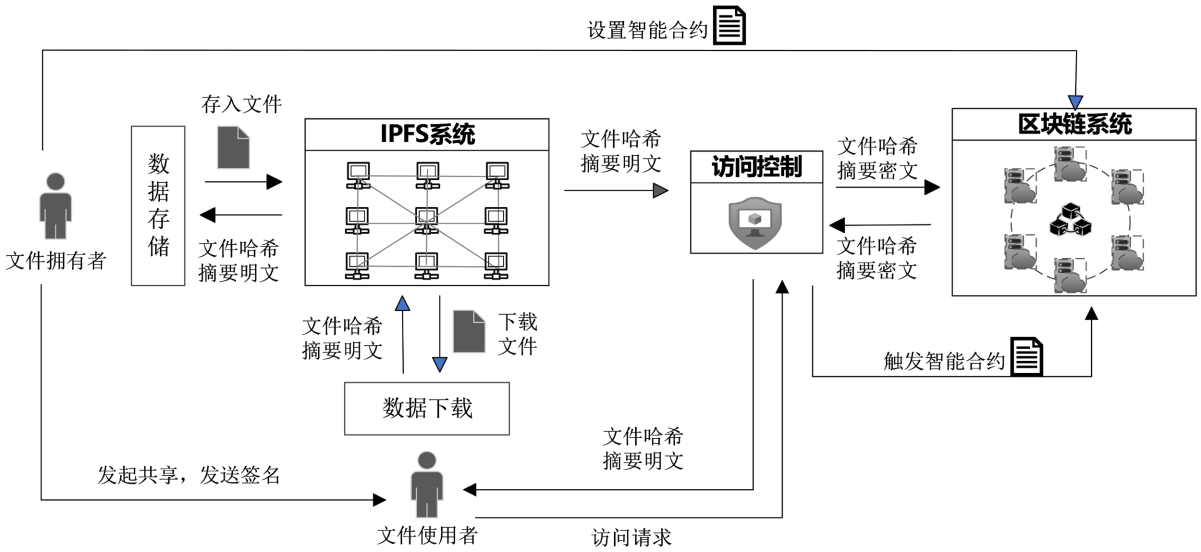

Figure 4. Data sharing process
图 4. 数据共享过程

1) 文件拥有者将文件存入 IPFS 系统，并对文件哈希摘要明文加密，将加密后的文件哈希摘要密文存入区块链系统；

2) 文件拥有者发起共享，并向文件使用者发送签名等信息；同时在区块链系统上设置智能合约；

3) 文件使用者获得区块链交易信息后，利用自己的相关信息触发智能合约，获取文件哈希摘要密文；

4) 文件使用者通过访问控制模块对文件摘要哈希密文进行解密，获得文件摘要明文；

5) 文件使用者向 IPFS 系统传入文件哈希摘要明文，获得文件拥有者向其共享的文件。

3.5. 数据操作追溯

数据操作记录追溯的作用是追踪和记录数据的操作历史，包括数据的创建、修改和访问，以确保数据的合法性、完整性和安全性。数据操作追溯可帮助识别和应对潜在的数据泄露或滥用问题，为安全审计提供可信的手段，特别在网络化协同设计场景下，提高数据管理的透明度和可信度。

数据操作记录追溯过程与存在过程类似，将数据操作日志、系统日志等信息按一定周期存入 IPFS 文

件系统，并将摘要信息加密上链存储，使操作记录信息完整可信，确保数据操作可追溯。

4. 系统实现

4.1. 系统方案

本文提出的基于区块链的网络化协同设计数据可信管理方案由区块链、访问控制单元、IPFS 文件系统、区块链服务系统、区块链服务 API 和应用系统组成，系统方案框架如图 5 所示。方案利用 IPFS 文件系统服务集群提供数据存储服务，节约区块链资源，离链存储庞大的设计数据。区块链系统由物理资源和区块链平台软件构成，提供去中心化的区块链基础服务。

IPFS 文件系统和区块链系统结合，实现数据摘要上链存储，数据主体链下存储，弥补区块链大数据存储的不足。权限管控单元与区块链节点协同，提供签名、验证等密码服务，同时为区块链服务系统提供加解密、哈希运输等服务。区块链服务系统是用户与底层数据存储、区块链等底层基础资源连接的中间层，纵向为用户提供数据上链、下链、查询、存证等功能，同时提供智能合约编排功能，横向以 RESTful API 形式为应用系统提供存证、分享、记录追溯等服务接口，实现应用系统数据到区块链的无缝衔接。

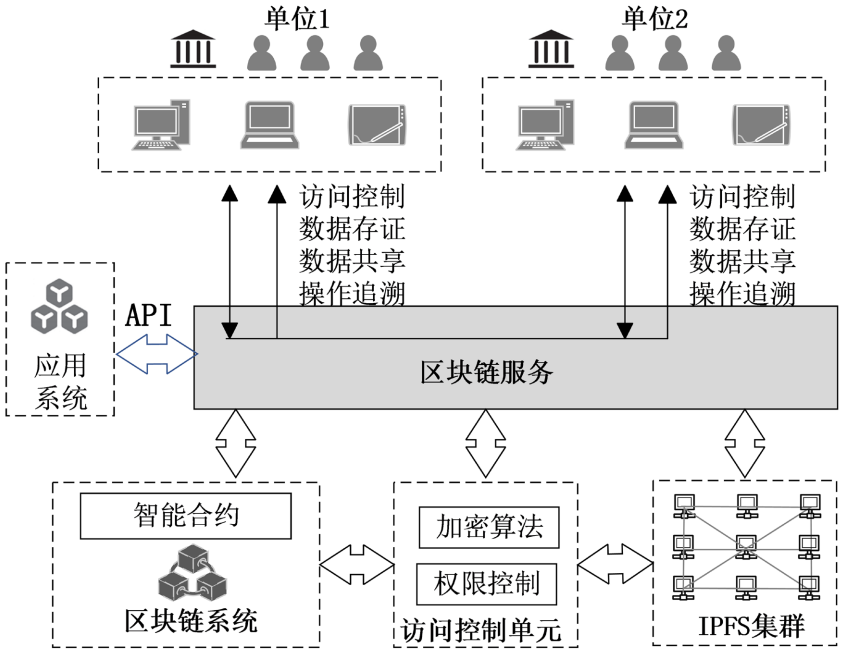

Figure 5. System scheme framework
图 5. 系统方案框架

参与网络化协同设计的各单位用户基于本方案可以实现数据的可信存储和管理，包括数据权限的严格管控、数据的可信传递、关键数据存证、协作数据的共享、数据操作过程的追溯等。同时可在使用设计相关的应用系统过程中，根据需要调用区块链服务，对设计过程数据进行可信管理。

4.2. 开发实现

(1) 区块链服务系统实现

区块链服务系统用户与区块链平台直接的中间层，连接用户和应用系统，提供区块链基础服务，包括数据存储、数据查询、数据下载、数据存证、访问认证等。区块链服务系统框架如图 6 所示。

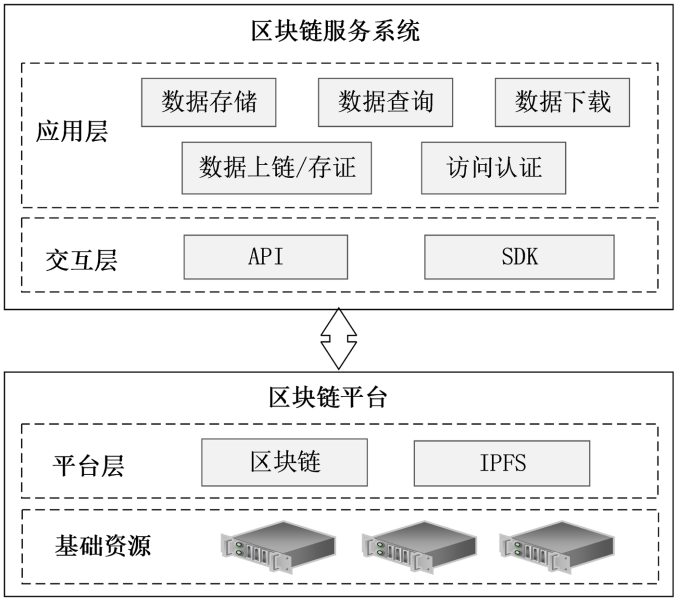

Figure 6. Blockchain service system
图 6. 区块链服务系统

1) 应用层：应用层向用户提供区块链相关的系统服务，包括：数据存储、数据查询、数据下载、数据上链/存证、访问认证。

- 数据存储：提供数据分布式存储功能，帮助数据拥有者将数据存入 IPFS 系统，IPFS 系统完成数据的分片存储后，根据数据生产文件摘要哈希值，并返回给数据拥有者。数据拥有者确认进行数据存储操作后，数据存储模块对文件摘要哈希值进行加密，并将加密后的数据上传至区块链系统。
- 数据查询：提供链上数据查询功能，根据区块链本身的准入机制要求，授权用户满足认证条件，触发查询智能合约，并输入该数据交易的唯一标识符，从区块链系统获取交易的哈希摘要密文。
- 数据上链/存证：提供数据上链功能，帮助数据拥有者实现数据的存证。过程是数据拥有者发起数据上链智能合约，将网络化设计数据集的哈希值写入区块链交易上链。该笔交易上链后会生成一个唯一标识符，数据需要流转或共享时，将该标识符为特定的用户授权，授权用户可以通过该标识符获得交易信息，进行认证或获取数据。
- 访问认证：提供用户对数据的访问控制和管理功能，通过无证书加密机制进行数据哈希的加解密，并对数据的使用权限进行控制，保证数据的安全性和隐秘性，避免数据的非法使用。

2) 交互层：屏蔽底层平台差异，连接上层应用层与下层平台提供相应的 API 和 SDK。主要负责应用层的应用对底层资源的调用、交互、信息的传递，同时提供与应用系统对接的 API 接口。

3) 平台层：包含区块链平台和 IPFS 文件系统。IPFS 文件系统负责完整数据的存储并返回给用户数据哈希摘要，同时根据哈希摘要对存储的数据进行下载。区块链平台主要负责用户的权限管理、调用智能合约完成各类区块链功能。

(2) 智能合约开发

智能合约部署在区块链系统中，可根据业务需要开发部署，本方案主要的智能合约包括数据存证合约、数据共享合约、数据下载合约、数据查询合约、数据追溯合约等。智能合约定义了数据、记录、用户结构体变量，存储数据文件的关键信息、数据文件分片的关键信息、用户资料和数据文件的所属关系。基于结构体变量编写智能合约，各智能合约的描述如下：

1) 数据存证合约功能：用户提交数据，合约计算数据的哈希值并将其写入区块链，生成一个不可更改的数据存证。用于将数据的哈希值和元数据存储到区块链上，确保数据的完整性和不可篡改性。数据共享合约：定义了数据分享规则，包括哪些地址或用户有权访问数据，以及访问的权限级别。允许数据所有者定义和控制数据的共享规则，实现安全的数据分享。

2) 数据下载合约：通过数据内容 hash 值从存储系统中获取相应的原始数据。对应的输入是数据内容 hash 值，输出是文件类型的数据。

3) 数据查询合约：根据数据拥有者信息查询区块链存储系统，得到内容 hash 值。输入是数据拥有者信息，输出是数据的内容 hash 值。

4) 数据追溯合约：记录数据的变更历史，使得用户可以追溯每个数据项的修改、时间戳和相关操作者。确保数据的透明性、完整性，以及提供不可篡改的数据记录。

下面是一个简单的区块链数据追溯合约的 Solidity 语言伪代码示例

```
contract DataTraceabilityContract {
    address public 所有者; // 合约所有者
    uint public 数据计数; // 存储的数据数量
    // 定义数据结构体，包括数据的哈希值和相关信息
    struct DataEntry {
        bytes32 哈希值; // 数据的哈希值
        string 数据信息; // 数据的相关信息
    }
    // 存储数据的映射，以数据哈希为键
    mapping(bytes32 => DataEntry) public dataEntries;
    // 构造函数，合约初始化时设置所有者
    constructor() {
初始化所有者(msg.sender);
初始化数据计数(0);
    }
    // 修饰器，只有合约所有者可以执行某些操作
    modifier onlyOwner() {
        require(msg.sender“仅数据拥有者可执行此操作”);
        _;
    }
    // 添加数据到区块链
    function addData(哈希值, 数据信息) public onlyOwner {
        if (数据长度> 0) {
修改哈希值；
            修改数据信息；
            增加数据计数；
        } else {
            返回提示：数据信息不能为空；
        }
```

```
    }
    // 查询数据追溯信息
    function getDataInfo(哈希值) public view returns (string memory) {
        if (哈希值对应的数据信息>0) {
返回数据信息;
        } else {
提示 "未找到匹配数据";
        }
    }
    // 修改数据信息
    function modifyDataInfo(哈希值,数据信息) public onlyOwner {
        if (新数据长度>0) {
修改数据信息;
        } else {
提示：新数据信息不能为空;
        }
    }
    // 删除数据
    function deleteData(哈希值) public onlyOwner {
        if (哈希值对应的数据长度> 0) {
删除数据;
减少数据计数;
        }
    }
    // 获取数据计数
    function getDataCount() public view returns (uint) {
返回数据计数;
    }
}
```

(3) 区块链平台搭建

区块链平台选择 Hyperledger Fabric 作为基础架构，版本选用 Fabric-sample。编译部署 Solidity 智能合约，将数据哈希上链，提供交易上链、存储、交易查询等功能，合约基于 Fisco Bcos 的 EVM 运行。分布式存储系统选择 IPFS 星际文件系统并部署在 Linux 系统中，利用 JPBC 库实现基于 CL-PKC 的无证书密码体制。系统测试的开发环境是部署在 2 台 8 核 3 G 内存的虚拟主机中，系统为 CentOS7，此外还配置 Docker、Docker-compose 等依赖工具。

4.3. 系统分析

(1) 安全性分析

1) 数据安全性

数据以分布式方式存储在 IPFS 系统，摘要采用无证书密码体制方式加密，数据拥有者将私钥、签名

等信息放置于智能合约中并预置访问权限，只有授权用户才可以访问链上数据。因此，即使攻击者通过链上节点获得文件密文，由于没有访问权限，攻击者无法得知数据拥有者信息，也无法解开密文信息。在整个过程中，除数据拥有者和授权使用者外其余参与者均无 获得任何明文消息，数据机密性得以保证，为数据安全存储和传递提供了保障。

2) 访问控制

基于区块链构建可靠可信网络，利用加密技术和智能合约对数据的传输和共享进行精确的访问权限控制。数据摘要等特征信息加密存储于区块链上，签名和认证过程利用加密机制实现。数据共享或获取过程利用区块链智能合约进行控制，只有具有权限的用户可获取加密的数据摘要，通过权限控制模块认证后，解密获得摘要明文，从而获得原始数据。整个过程精细化地控制对数据的访问权限，拒绝非授权的访问或未经允许的网络传输，并对数据的访问和传输留痕审计，对可疑操作提出警示。

3) 数据存证追溯

基于区块链对数据进行存证，将数据摘要、归属、水印等信息进行加密或签名，宣称自身对数据的所有权，标志所有权和操作权，并将确权记录生成凭据在区块链上进行存证。在传输时，用发送方的数字签名验证数据的权属，相关的授权和验证记录、传输操作在区块链上进行存证和审计。数据的所有权、使用情况有争议时，利用区块链网络获得可信背书，尤其适用于知识产权保护。此外，数据拥有者通过比对原始数据的 Hash 值和链上保存的数据特征是否一致，对数据的一致性和完整性进行校验。数据操作追溯上，将对数据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) 功能分析

本文提出的总体方案可用于网络化协同设计产生的文档、图纸、图片、音视频等各类数据的安全存储、传输、共享、存证、追溯，方案普适性强。本文方案将数据摘要信息加密，通过认证方式基于区块链进行可信传输，记录操作进行了上链存证，将区块链平台与数据存储平台进行结合，与各类业务系统进行对接，具有可靠、安全、防抵赖、防特权、节约资源等优点。另一方面，本方案采用私有链方式部署，规模达到一定程度后可向联盟链放心扩展，方案从可拓展性角度看具有一定的限制。本方案与其他方案的功能对比如表 1：

Table 1. Comparison of functions in different schemes
表 1. 不同方案功能对比

方案	数据类型	区块链方案	存储方案	操作存证	加密	授权模式	经济成本	可拓展性
EduRSS [12]	教育记录(文本)	公有链	私有服务器	无	无	https	较高	好
Tan [13]	档案数据(文档)	公有链 + 联盟链	私有 IPFS 集群	无	无	https	高	好
Niu [14]	电子病历(文档)	私有链 + 联盟链	私有服务器	无	无	单独发送	较低	较好
Zhang [15]	电子病历(文档)	联盟链	云存储	无	无	单独发送	较低	一般
Wang [16]	电子证照(图像)	私有链	私有服务器	无	无	单独发送	低	弱
本文方案	设计数据、成果等(文档、图纸、图片等)	私有链 + 联盟链	私有 IPFS 集群	有	有	链上同步	较低	一般

(3) 性能分析

本文所提方案区块链系统仅存储加密的文件摘要信息和操作记录，不存在性能瓶颈，主要的性能限制在于 IPFS 系统数据存取性能。针对 IPFS 系统性能进行测试，对 IPFS 系统查询测试，设计 8 个测试组，每组 1000 条查询，共进行 8000 次查询，测试衡量标准为每秒交易数 TPS (Transactions Per Second)。TPS 是一个关键的性能指标，通常用于衡量一个系统、网络或平台在单位时间内可以处理的交易数量。

对于研发团队一般在数千人至万人之间的集团性企业来说，大部分研发人员使用本地资源进行设计开发工作，经验数据表明以网络化模式并发进行协同设计的研发人员约为十分之一，对 IPFS 系统的 TPS 性能要求不高，一般在 1000 左右。测试结果为 IPFS 系统平均 TPS 约为 850，如图 7 所示，并可通过横向扩展 IPFS 系统节点数来提高性能。测试结果表明，IPFS 作为协同设计数据链下存储方案，可满足基于区块链的数据可信存储系统性能需求。

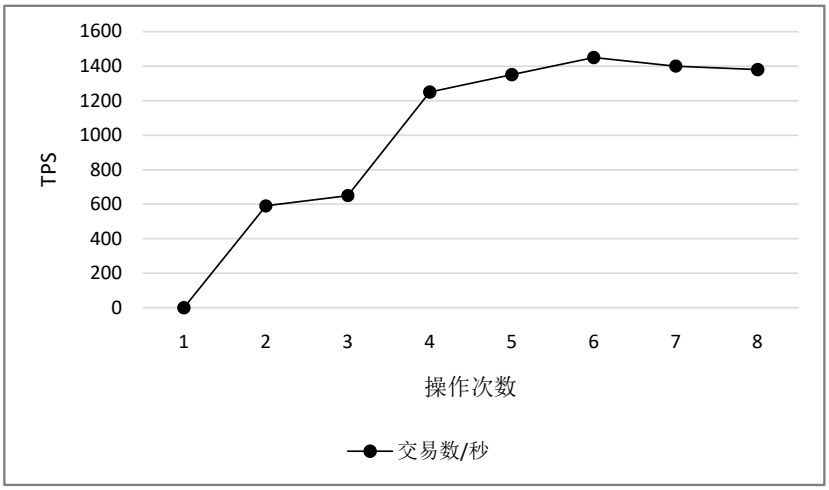

Figure 7. Performance test results
图 7. 性能测试结果

5. 结束语

本文针对网络化协同设计过程中数据可信存储和传输的问题，提出基于区块链的数据安全存储传输方案。使用无证书密码体制并结合区块链智能合约对数据权限进行管控。利用区块链和 IPF 文件系统不可篡改的特点，IPFS 中存储原始数据，对应数据的加密 Hash 值存储在区块链中，降低了数据集中存储的风险，加强数据的安全性。分析结果表明，本文所提的方案在数据安全存储、数据可信传递、数据存证和追溯等方面有突出表现。下一步将继续与应用系统的接口以及丰富智能合约的功能以实现更多场景的数据可信存储和传输管理，构造更加安全的数据管理模型。

参考文献

[1] 杨湘浩, 刘云. 企业隐性知识共享激励机制研究[J]. 中国管理科学, 2012, 20(S1): 80-83.

[2] Zhang, X.S. Poslad, S. and Ma, Z. (2018) Blockchain-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in E-Health. *IEEE Global Communications Conference* (*GLOBECOM*), Abu Dhabi, 9-13 December 2018, 1-7.

[3] 高文涛, 张桂芸. 基于联盟区块链和 IPFS 的音乐共享模型[J]. 天津师范大学学报(自然科学版), 2020, 40(2): 68-74.

[4] 朱彦霞, 张雪萍, 华南, 罗刘敏. 基于 IPFS 及区块链的互联网融媒中心平台设计[J]. 电子设计工程, 2021,

29(18): 10-16.

[5] 成丽娟, 祁正华, 史俊成. 基于区块链的 EHR 数据安全存储共享方案[J]. 南京邮电大学学报(自然科学版), 2020, 40(4): 96-102.

[6] 黄郑正, 张晓蝶, 赵金辉, 等. 基于区块链的知识共享机制的设计[J]. 重庆理工大学学报(自然科学), 2021, 35(9): 143-151.

[7] 冯政鑫, 唐寅, 韩磊, 等. 基于区块链的敏感数据安全共享方案[J]. 信息安全研究, 2022, 8(4): 364-373

[8] NICKS (1994) Smart Contracts. http://szabo.best.vwh.net/smart.contract.html

[9] Al-Riyami, S.S. and Paterson, K.G. (2003) Certificateless Public Key Cryptography. 9*th International Conference on the Theory and Application of Cryptology and Information Security*, Taipei, 30 November-4 December 2003, 452-473. https://doi.org/10.1007/978-3-540-40061-5_29

[10] 孙华, 孟坤. 标准模型下可证安全的有效无证书签密方案[J]. 计算机应用, 2013, 33(7): 1846-1850.

[11] Zhao, Y., Hou, Y., Wang, L., *et al*. (2020) An Efficient Certificateless Aggregate Signature Scheme for the Internet of Vehicles. *Transactions on Emerging Telecommunications Technologies*, **31**, e3708. https://doi.org/10.1002/ett.3708.

[12] Li, H. and Han, D. (2019) EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. *IEEE Access*, **7**, 179273-179289.

[13] 谭海波, 周桐, 赵赫, 等. 基于区块链的档案数据保护与共享方法[J]. 软件学报, 2019, 30(9): 2620-2635.

[14] 牛淑芬, 陈俐霞, 李文婷, 等. 基于区块链的电子病历数据共享方案[J/OL]. 自动化学报, 2021: 1-11. https://doi.org/10.16383/j.aas.c190801

[15] 张磊, 郑志勇, 袁勇. 基于区块链的电子医疗病历可控共享模型[J]. 自动化学报, 2021, 47(9): 2143-2153.

[16] 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.