A blockchain-encrypted file transfer architecture design

Jun Xia[1] Jun Zhong[2*] Rong Liang[3] Feng Long[4] Feng Liu[5]

1.R & D Department of Xingyi Xia Xia Science and Technology Development Co., Ltd., Xingyi, Guizhou, 562401, China
2. School of Economics and Management, Xingyi National Normal University, Xingyi, Guizhou, 562401, China
3. Hefei Datang Storage Technology Co., Ltd., Hefei, Anhui, 230088, China
4. Kexin Branch of Public Security Bureau of Qianxinan Buyi and Miao Autonomous Prefecture, Guizhou Province, Xingyi, Guizhou, 562401, China
5. Baboos (Shenzhen) Safety Technology Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

This paper aims to design and implement an encrypted file based transfer technology based on blockchain technology, so as to solve the security problems existing in the current file transfer system and improve the security and efficiency of file transfer. This paper introduces the development process of blockchain technology and its application prospects in file transmission, expounds the challenges facing the current file transmission system, and clarifies the core issues of research, that is, how to achieve efficient integration of encrypted transmission and blockchain technology. This paper summarizes the main research content of the paper, including the application of blockchain technology, the selection and implementation of encryption algorithm, system architecture design, etc., and describes the overall framework and technical route of the research in detail, and shows the research methods and technical tools used in the research process.

Keywords

Blockchain, encryption algorithms, file transfer, system design, and security evaluation

一种区块链加密文件传输架构设计

夏君 [1] 钟君 [2*] 梁荣 [3] 龙峰 [4] 刘丰 [5]

1. 兴义市夏秋科技开发有限公司研发部，中国 · 贵州 兴义 562401
2. 兴义民族师范学院经济与管理学院，中国 · 贵州 兴义 562401
3. 合肥大唐存储科技有限公司，中国 · 安徽 合肥 230088
4. 贵州省黔西南布依族苗族自治州公安局科信支队，中国 · 贵州 兴义 562401
5. 巴布斯（深圳）安全科技有限公司，中国 · 广东 深圳 518000

摘 要

本文旨在设计并实现一个基于区块链技术的加密文件基础传输技术，以解决当前文件传输系统存在的安全性问题，提升文件传输的安全性和效率。介绍了区块链技术的发展历程及其在文件传输中的应用前景，阐述了当前文件传输系统面临的挑战，明确了研究的核心问题，即如何实现高效的加密传输与区块链技术的有效集成。概述了论文的主要研究内容，包括区块链技术的应用、加密算法的选择与实现、系统架构设计等，并详细描述了研究的整体框架和技术路线，展示了研究过程中采用的研究方法和技术工具。

关键词

区块链；加密算法；文件传输；系统设计；安全性评估

1 引言

在需求分析及应用场景设计部分，探讨了区块链在各行业的应用现状；比较国内外研究现状，分析了不同研究进度基本原理和应用。还回顾了传统文件传输方法的优缺点及安全隐患，介绍了现代文件传输技术的发展趋势，探讨了区块链技术在提升文件传输安全性和效率方面的潜力。

在解决方案阐述及落地验证部分，本文定义了系统的主要功能需求，如文件加密、传输、存储等，并分析了系统在性能、安全性、可扩展性等方面的要求；划分了系统的主要组件及其功能，描述了各模块之间的交互关系和数据流动，制定了文件在区块链和链下存储的方案，选择适合的加

【作者简介】夏君（1973–），男，中国重庆人，硕士，高级工程师，从事密码学、分布式存储研究。

【通讯作者】钟君（1985–），布依族，中国贵州兴仁人，博士，正高级职称，从事数理统计学，概率论研究。

密算法对文件进行加密，设计了密钥的生成、分发和存储机制，制定了文件访问权限控制策略，通过送检国家密码检测验证了方案所具有的一定安全及可执行性。

在先进性及创新性部分，本文分析了去除属性状态后的一种密文体分布存储的优越性，以及分布节点去中心化建设者 (单位) 后，能创立一个自发可信的“网络工会”组织形式，进而来提升区块链自我分布式管理的不控制性，重点突出在当前区块链结构中创新增加密文体层，来支撑信息安全传输地作用，提出了在信息回链验真、多方应用、跨链技术方面的创新思路方向。

在技术先进性和创新性部分，从密文存储、分布式节点模型结构以及密文链、物理存储地址码为 CID 标识等方面，定义了文件传输中数据包的格式和内容，实现了文件的上传、下载和管理功能，构建了服务器端逻辑，实现了区块链节点的搭建与智能合约的部署，确保文件在传输过程中的安全性，优化了文件传输协议，提高了传输速度和效率。

在与国外 IPFS 分布式存储主要性能方面，进行了列表对比，可以看出其中的优缺点，但总体说本技术较优。

在结论与展望部分，本文总结了研究的主要发现和结论，讨论了研究的局限性和不足之处，阐述了本研究在理论方面的贡献和创新，从自身技术开发者角度出发，因为区块链自身防篡改、抗破解的“高安全性”特点，对于“人”的不可控因素，造成网络中传输信息不易监管的系统性风险。说明了研究成果在实际应用中的价值和意义，提出了基于当前研究的未来方向和可能的领域，探讨了区块链和加密技术的发展趋势及其对文件传输系统的未来影响。

2 需求分析及应用场景设计

区块链技术自 2008 年比特币诞生以来，在金融、物联网、供应链管理等多个领域得到了广泛应用，其核心思想是通过分布式账本和密码学技术实现信息的安全共享与存储。近年来，随着人们对隐私保护意识的增强以及对数据安全需求的日益增长，如何构建一个既高效又安全的文件传输体系成为学术界和工业界共同关注的问题。

在这一背景下，区块链加密文件传输系统应运而生，它不仅能够有效提升文件传输过程中的安全性，还能确保数据的完整性和可追溯性，为用户提供了更加可靠的数据交换平台。从领域重要性来看，该系统的研究有助于推动区块链技术在实际应用中的落地，促进相关行业的发展；对于个人而言，它也意味着能够更好地保护自己的隐私信息不被泄露或篡改，同时也可将非结构化数据信息标识为数字化标签，标注每一个数据信息成为独有的“数字资产”[1]。

目前，国内外学者针对此技术展开了广泛而深入的研究。国外方面，欧美国家在该领域起步较早，研究成果较为丰富。例如，斯坦福大学的一项研究表明，基于区块链的文件传输方案可以在保证数据安全的同时显著提高传输效率。另一项由麻省理工学院主导的研究则提出了一种新的加密算法，能够在不影响用户体验的前提下增强系统的安全性，例如 IPFS 分布式存储技术。国内方面，清华大学、浙江大学等高校也在积极进行相关探索，并取得了一系列突破性进展。其中，清华大学的研究团队开发出了一套适用于大规模网络环境下的区块链文件传输系统原型，初步验证了其可行性和有效性。

然而，尽管已有诸多尝试，但当前的此项技术仍面临不少挑战。一方面，如何平衡安全性和效率之间的关系仍然是一个亟待解决的问题；另一方面，由于区块链本身具有较高的能耗特点，如何在保障系统安全性的前提下降低运行成本也是研究人员需要重点考虑的因素之一。针对非结构化信息在数据资产标识方面，来适应更加复杂多变的应用场景。

综上，区块链加密文件传输系统的研究对于推动信息安全领域的发展具有重要意义。未来，随着理论研究和技术实践的不断深入，相信这一技术将逐步完善并得到更广泛的应用，为用户提供更加安全可靠的文件传输服务[2]。

3 解决方案阐述及落地验证

3.1 功能需求

功能需求的定义是系统设计至关重要的一步。通过对现有文件传输系统的分析以及用户需求的调研，我们明确了系统需要实现的主要功能，这些功能涵盖上链认证、文件加密、传输、存储、链接回溯等多个方面。

此技术核心功能之一，是为了保证文件在传输过程中的安全性，系统采用了国密的标准算法。在众多加密算法中，选择了国密 SM4 的对称加密算法，其具有较高的安全性且计算效率也较高，对传输明文内容进行加密。对于密钥管理部分，系统采用了国密 SM2 算法来生成公钥和私钥，从而确保密钥的安全性。系统还支持用户可随时更改密钥的功能，以便满足特定场景下的加密需求。

文件传输功能的设计需要考虑到多种网络环境下的传输效率和可靠性。系统支持多种传输协议，包括 FTP（File Transfer Protocol）、SFTP（Secure File Transfer Protocol）和 HTTP（HyperText Transfer Protocol）。为了提高传输速度。我们还实现了多线程传输功能，可以在多个线程之间分配传输任务，进一步提高传输效率。针对大文件传输场景，系统支持分块传输，将大文件分割成多个小块分别传输，从而减少单个文件传输所需的时间[3]。

文件存储是设计的另一个重要的功能。系统全程提供链上存储过程，不仅存储元数据信息，如时间、摘要、存证代码值、发送 / 接收账本号、公开公钥值等，实际的密文数据也存储于链上空间中。为了确保数据的完整性和安全性，系统采用了多重备份机制，在多个分布存储节点上保存密文文件副本。系统还实现了数据冗余技术，即使某个存储节点出现故障，也可以从其他节点恢复数据[4]。

除了上述主要功能外，系统还具备一些辅助功能。例如，用户权限管理功能，允许发放密码模块时厂家可以设置不同用户的访问权限，确保只有授权用户才能访问特定节点或功能。用户所有链上的操作记录，均记录在对应链上账本表之中，便于其他用户的实时审计和对账。为了方便体现我们传输技术的特性，我们设计一款可直接使用的机密计算软件“密件邮——ScyTale”，结合软件对应的物理密码模块，结合成可信执行环境（TEE），用户可以通过图形界面轻松上传、下载和管理文件。系统还支持文件锁定分享功能，用户可以指定账本生成分享链接，将文件发送给指定的接收者。

为了提高本技术的可扩展性和兼容性，我们还提供机密 SDK 接口方式，确保技术与第三方平台之间的轻松耦合。支持多种编程语言和开发框架，开发者可以根据需要选择合适的开发工具进行二次开发。提供了丰富的文档和技术支持，帮助开发者快速上手并进行系统定制 [5]。

3.2 系统组件划分

为了实现一个高效且安全的区块链加密文件传输系统，首先需要对系统进行合理的组件划分。系统组件划分是系统设计的基础，它不仅有助于明确各个部分的功能，还能提高后续开发和维护的效率。系统主要由机密计算软件、硬件密码模块和区块链节点三大部分组成，每个部分都有其特定的功能和职责。

3.2.1 机密计算软件

负责用户界面的设计与实现，为用户提供友好且直观的操作界面。前端主要包括登录及更改公私钥、上传及下载密文界面、查看本人及他人账本、明文防篡改核验、明文传输链转关系、本地文件加密等管理界面。登录及更改公私钥界面需要实现用户的口令验证功能，同时具有更改口令时可选择密码硬件模块生成全新的公私钥值的过程，确保只有经过口令认证的用户才能访问系统。上传及下载密文界面则需要支持将明文进行次机密计算成一种字符状态，送入密码芯片进行加密后，将密文文件的上传和下载操作，文件上传用户可以设定密文在网络中的生存时段、是否指定接收者账本、生成“区块存证”后是否进行广播等，与区块链智能合约相关的编程参数设定，并能正确接收区块链节点上合约共识后的“区块存证”代码，用于网络信息资产的交互凭据 [6-7]。

3.2.2 硬件密码模块

为国密认证的密码芯片，负责通过机密计算软件，将明文转换的一种字符状态下的信息进行加密，内部生成一个真随机数，采用 SM4 加密所有字符，然后在用 SM2 加密这个随机数，最后按照加密顺序，将所有加密密文信息进行封装成“电子信封”状态，通过机密计算软件上传区块链，硬件密码模块如图 (1)/ 电子信封流程如图 (2)

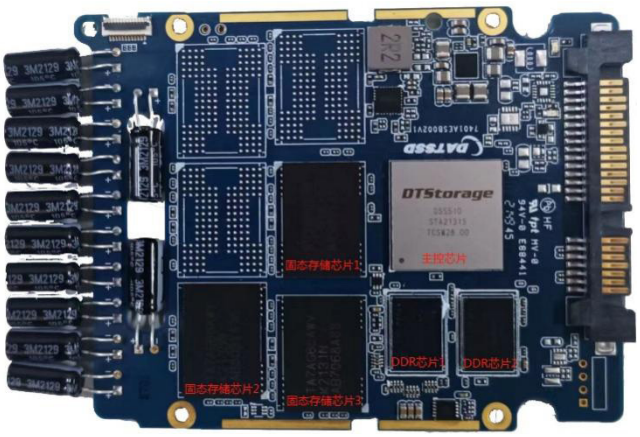

图 1：硬件密码模块

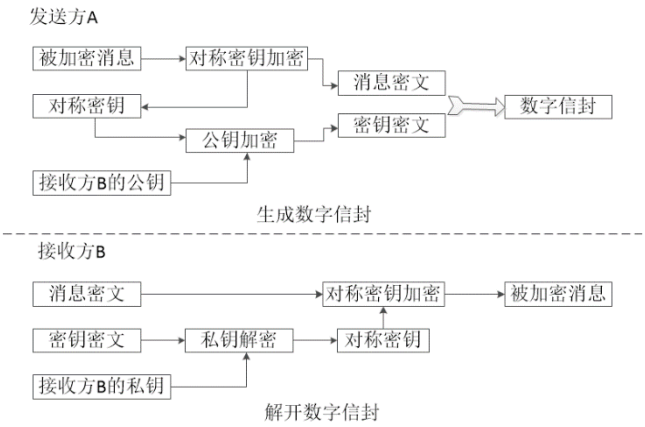

图 2：电子信封流程

反之硬件密码模块通过机密计算软件，将接收到的密文进行 SM2、SM4 解密出明文字符状态送出到机密计算软件，由其还原出所接收明文 [8]。

因此通过软硬件组合的方式，形成不用在计算机内存中运行核心加、解密计算的过程，最大限度来保证电子信封密钥随机数以及账本私钥值的安全，进而如图 (3) 所示满足安全可信计算空间 (TEE) 要求，组合为一种“硬钱包”。

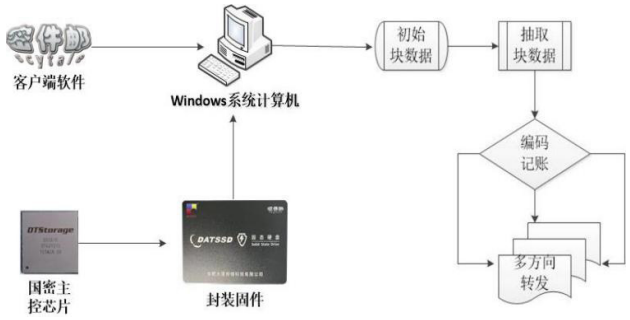

图 3：密码模块 + 机密软件，组成可信计算空间 (TEE) 一种不可分割的“硬钱包”形态

3.2.3 区块链节点

主要负责接收机密计算软件上传的电子信封密文，进行一种合约管理维护分布式账本过程，当发现有一个新电子

密文时，采用发明专利《一种安全高速的信息采集查询系统》(专利号：ZL 2015 1 0664481.0) 中所表述的“通过查询未使用过的硬盘存储地址代码来标识信息的方法”，来锚定每一次上链的新密文体，如图 (4) 所示每一个节点同样需要工作量的查询计算 (类似安全多方计算（SMPC）)，最后共识出唯一区块存证代码、通过这样的智能合约共识方式，整体组成一个联邦学习机制（FL），若只知道 “区块存证”的结果值，而不通过我们的区块链回链识别技术，是不可能推算出“密文信息”内容 [9-10]。

物理寻址方式

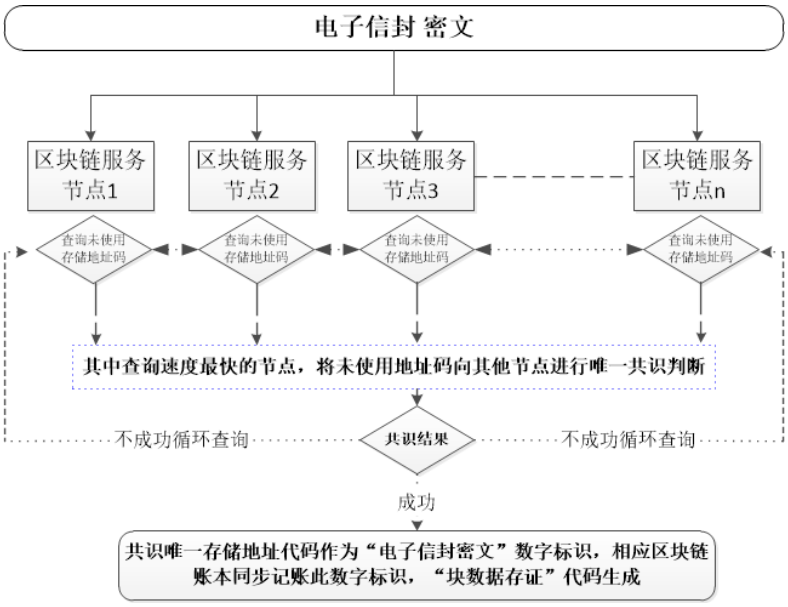

图 4：区块链存证生成流程

(1) CHS（柱面 - 磁头 - 扇区）寻址

传统机械硬盘通过 C 柱面 (Cylinder)、H 磁头 (Head)、S 扇区（Sector）、定位数据。

转换公式（CHS → LBA）：

LBA=CÍ(Hmax × Smax)+H × Smax+(S−1)

u Hmax : 每个柱面的磁头数

v Smax : 每个磁道的扇区数

w S : 目标扇区号 (通常从 1 开始)

(2) LBA（逻辑地址）

现代硬盘和 SSD 普遍采用 LBA，直接通过线性编号访问扇区。

逆向转换公式（LBA → CHS）：

$$C = \left\lfloor \frac{LBA}{H_{max} \times S_{max}} \right\rfloor$$

$$H = \left\lfloor \frac{LBA \mod (H_{max} \times S_{max})}{S_{max}} \right\rfloor$$

$$S = (LBA \mod S_{max}) + 1$$

当所有节点合约共识成功后都将记录到相应分布式账本之中，其中包括记账时间、存证代码、密文摘要、密文来源、留存时段、所用公钥值等元数据信息，同时线下每一个加密后的密文结果，存储为不少于节点总数 51% 的密文主体文件，并用共识产生的“区块存证”代码做为密文标识名称。

3.2.4 整体系统

由此我们设计出了一种非线上加解密、不依靠中心化 CA 加密机制、公 / 私密钥及密文存储均为分布式的混合区块链体系，因为电子密文信封线上不可破解性，所有物理节点计算机，均非由开发者来建设及运维。从数据管理者角度出发，也解决了数据管理者去中心化问题，所产生的“区块存证”实质也是将非结构化数据信息进行了“数字化标识”，可按照传链频次计数，有效体现其数据需求的经济价值所在 [11-12]。

3.3 技术落地验证

网络节点中的密文体是一个“电子信封”状态，并分布到所有节点之中，没有完整的密文段，均不符合“暴力破解”、“字典攻击”、“频率分析”、“已知明文攻击”、“选择明文攻击”、“侧信道攻击”等原理破解基础特性，也不符合采用 John the Ripper、Hashcat 等哈希算法破解工具的应用前提，在我们所提供的密文体样本如图 (5)，所展示的内容为一个文件转换成字符后的加密结果片断，其中的“电子信封”架构，也是同步加密其中，这样就进一步提高了破解手段的难度，上述多种破解方法和工具，在试验性破解过程时，均未成功实现最终破解出明文的结果 [14-15]。

在实际用户使用过程中，获得用户的推荐，同时软硬件组合可信执行环境（TEE），所有加解密及传输、分布存储算法流程，2022 年通过国家密码管理局实物检测，通过相关密码检测。报告摘要如图 (6)，得以有效实际验证

4 技术先进性及创新性

4.1 先进性

通过我们区块链传输技术可以将各行各业乃至个人数

图 5：密文体样本截图

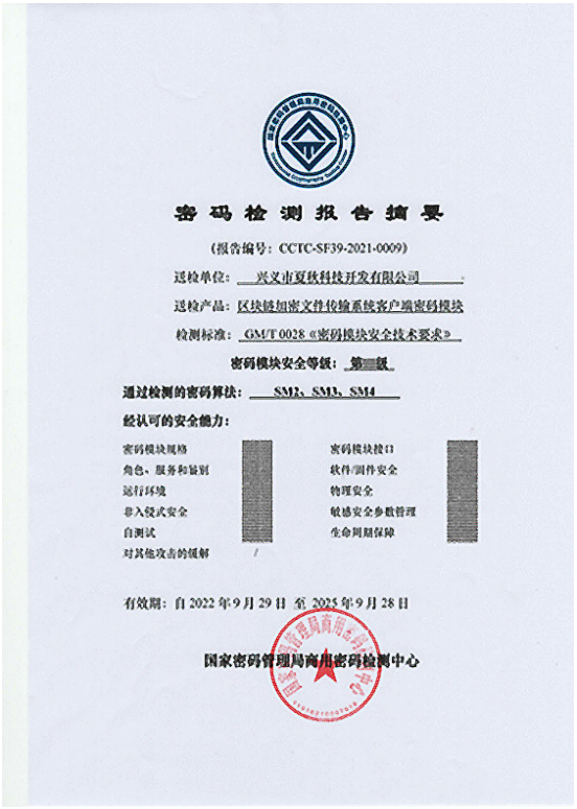

图 6：区块链加密传输国密检测报告摘要

据，加密生成一个个去除了行业属性标签的“区块存证”代码，全部“混合”到区块链体系之中，侵入节点仅从 40 位代码是无从知晓，其所携带的信息属于什么行业，更难以分析出所关心的数据信息类型，存储架构模型如图 (7)。

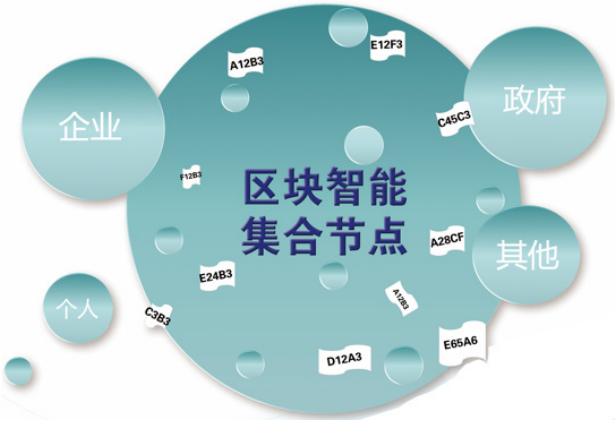

图 7：无属性密文存储架构模型

区块链技术中的分布式节点建设完全不掌握在开发者管辖范围内，任何组织及个人都可以提供自己的硬件计算机及网络，来加入这个体系之中，真正成为一个去中心化管理的“自主可信网络工会”组织形式，单个节点的“加入”及“离开”完全自由，均不会影响整个体系的运转机制，从传统中心化管理者角度出发，就有效地“剥夺”了系统开发者的数据控制权力，因此节点机加入数量越多，其整体区块链体系的稳定性和运算速度也就越强，网络架构模型如图 (8)。

4.2 创新性

在经典区块链账本、链条结构的基础性功能之上，我们又创新增加了一层“密文体”的信息加载层，但如何管理新增“密文体”层与链条层和账本层有效关联呢？我们将相同明文上链的加密信息按照图 (9) 这样形成独立的“DNA”链关系架构，因此当有无数不同密文上链后，都将形成无数个这样结构的“DNA”链关系架构 (也可理解为一种新型数据关系结构)。

在体系中只要能获取到任意账本中的“存储地址代码”(称之为区块存证) 标识值，就可顺利的知道对应锚定的“密文层”文件，但只知道“密文层”文件，是不能正确解密还原明文，还需要对应的线下“私钥”密码模块“硬钱包”才能完成最终接收解密流程 [16-17]。

在上述理论的基础之上，我们还创新实现相同的明文，通过不同的密码模块加密都会产生不同的“区块存证”，但接收人无论使用哪一个“区块存证”最终解密收到的一定都是相同明文内容，进而也实现了隐私计算中“多方安全计算”机制，在通过区块链账本记录流程，我们又可以非常方便快捷的知道不同“区块存证”代码指向的是同一个明文数据，认证流转关系图 (10)。

同样任何信息传输无关第三方，也可使用自身密码模块协助佐证信息是否被篡改。通过“密件邮”机密软件的“账本回链”功能，来回溯所有传输过程，回链截图 (11)。

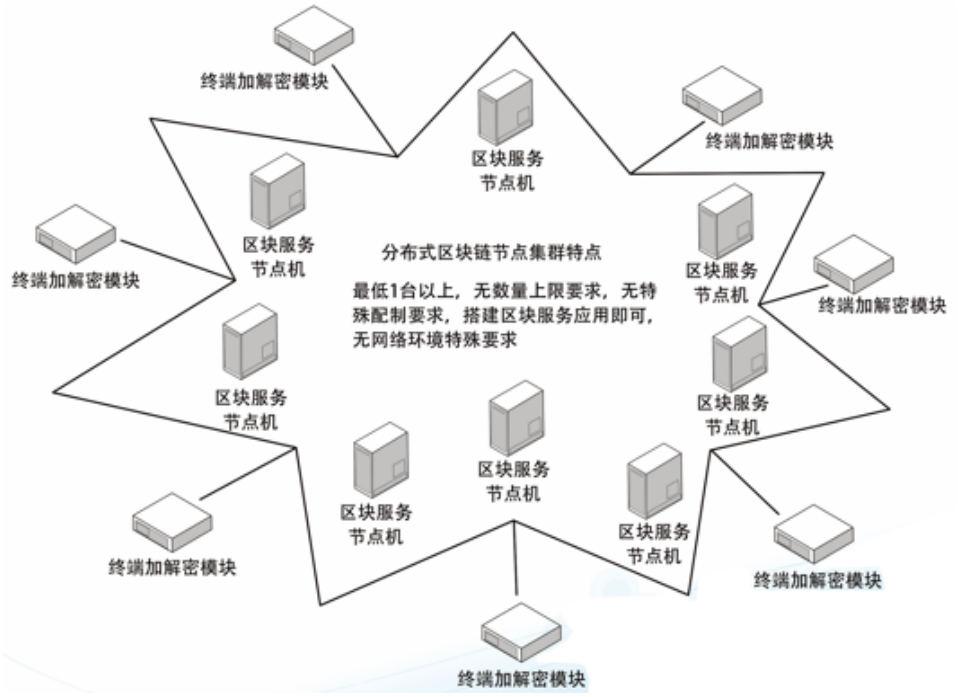

图 8：分布式网络节点架构模型

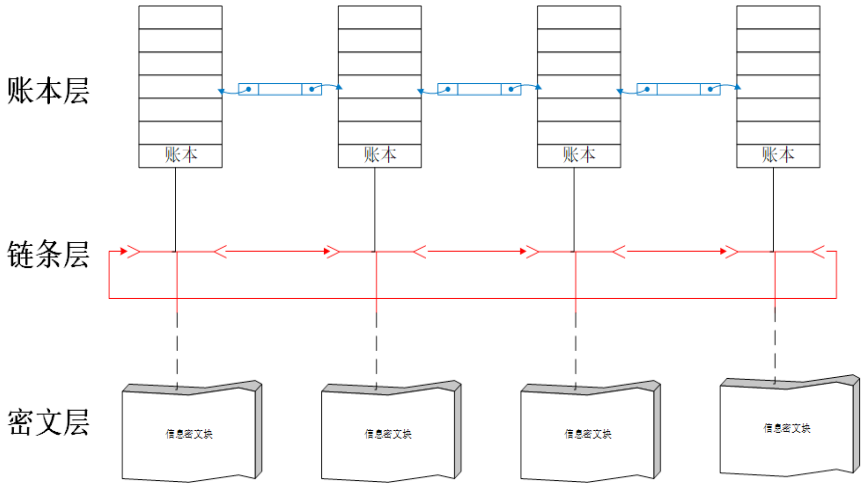

图 9：密文链条关系架构

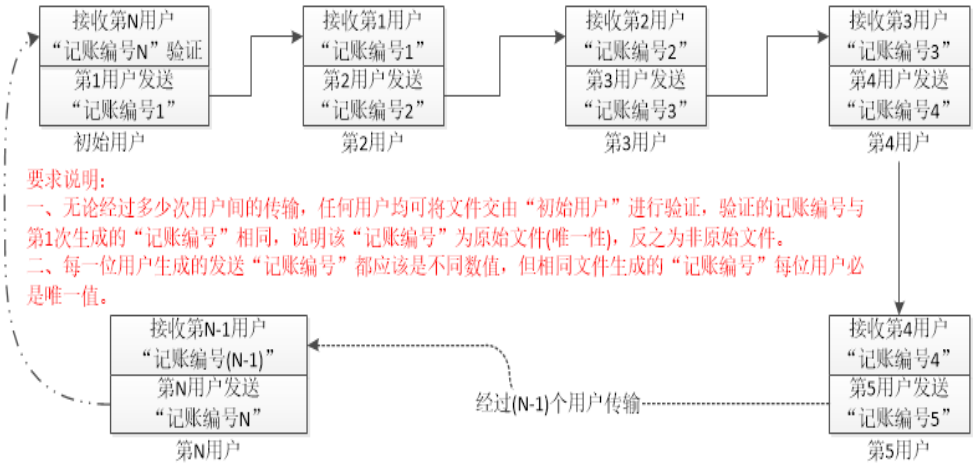

图 10：认证流转关系

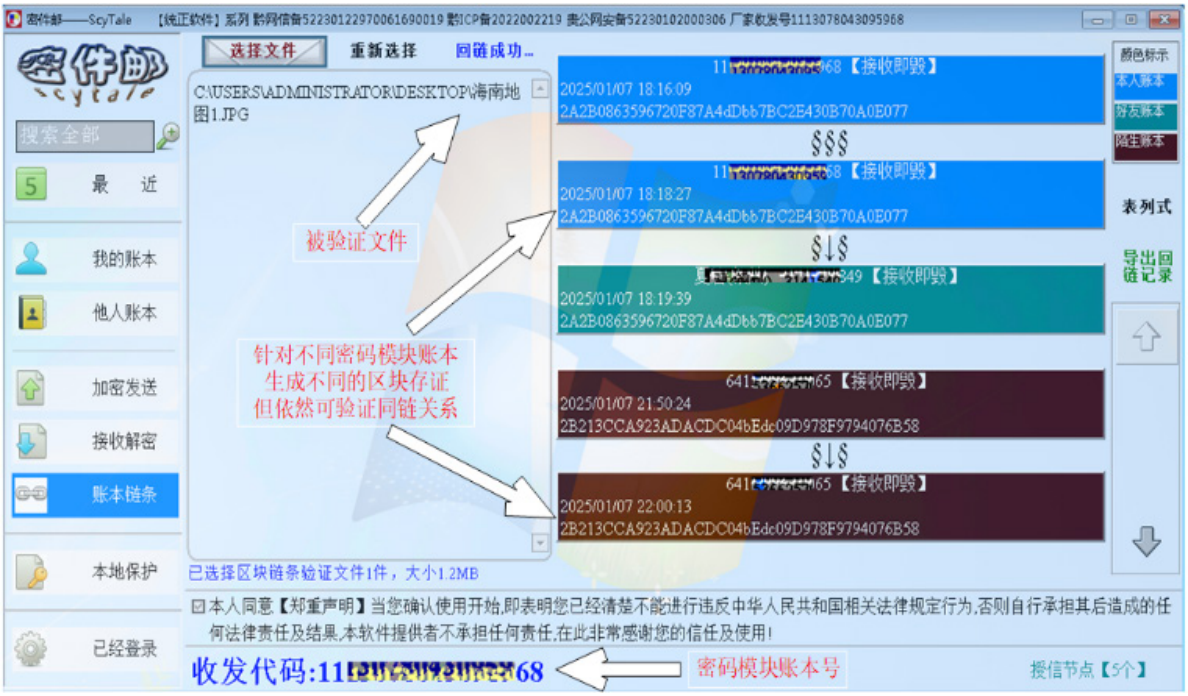

图 11：相同文件通过不同密码模块上链后，回链截图

5 与国外 IPFS 分布式存储的主要性能对比

架构对比项	IPFS 架构	本架构	结果
存储架构	分布	分布	=
CID 标识	哈希值	存储地址码	≠
检索来源	哈希表	区块账本表	≠
存储形态	明文	密文信封	√
存储方式	链上和链下	链上	×
寻址方式	内容	CID 标识	≠
同节点数下检索定位	20 秒	22 秒	≈
单一分块容量	256K	3M	√
同步下载	支持	支持	=
同数据去重	去重	不去重	≠
最长存储时效	永久	30 年	×
最短存储时效	不详	下载即毁	≠
密钥管理模式	软密钥	硬密钥	≠
加密算法	国际	国密	≠
抗 DDoS 攻击	支持	支持	=
抗审查性	支持	支持	=
有独立区块链作支撑	没有	有	√
独立传输追溯能力	不能	能	√
本地密文在分布存储	不能	能	√

6 结论与展望

本技术构架从密钥保护就基于一种密码硬件芯片之中，完全与当前中心化 CA 加解密方式不同，任何需要远程传输的数据信息，均通过自己手中的密码模块进行加解密，同时锁定数据确权、通过与现有国外 IPFS 分布式存储技术对比，本技术从 CID 标识方法、密钥管理模式等诸多方面对比，具有一定的优势，特别是我们集成的区块链的特性，独立或通过接口均可提供多样化的应用场景，并且全密文方式远程安全交互，有效防止“网络爬虫”及今后“人工智能”在网络中“非授权”挖掘数据过程，如何在现代网络资源环境中，不依靠中心化平台就可安全交互传输“不公开”的数据信息，这就需要一种新型高安全的传输技术手段来实现，本技术方案在此问题上将具有广泛的实用需求价值。

做为一种区块链基础性底座技术，通过 SDK 机密接口方式能非常方便的实现不同中心化系统之间“重要信息数据”的隐私交互过程，例如：患者在 A 医院所拍 CT 检查影像文件，通过本区块链技术上传互联网集群公共节点之中，并将生成的 40 位“区块存证”代码告之患者本人，患者本人到 B 医院后就可通过此 40 位“区块存证”获得 A 医院的 CT 检查结果，从而减少患者重复检查的时间及费用成本，同时 B 医院中心化信息系统也不需要去申请访问 A 医院的中心化信息系统的过程，医院双方均可实现最大限度的系统安全保障。(当然 A 医院是可授权有哪些医院可以看检查结果)

在提升了自身较高安全性的前提下，确实也存在非常大的网络信息监管风险，信息传输中“人”的行为风险成为最大不可控因素，会对目前网络舆情监管造成巨大冲击，物理节点可自主化建立模式，从而使以往网络收集、阻止某些信息，失去了核心抓手，为此如何正确引导使用本项技术，与监管部门研究相关政策方案，又产生了一个全新的课题。

涉及对称和非对称加密、电子封装算法、隐私计算等多重运算的同时使用较为耗时，目前我们也只能一次性加密传输最大 192M 以内的非结构化文件，如何进一步提升当前传输容量，需要从加密芯片和更优算法两个方面的改进来

突破。

从有利于数字资产发展方向来看，数字资产交易实质就是种“可信数据安全交互 + 计价”的组合过程，我们采用一种轻量级应用的系统构架，便利人们将大量带有信息的非结构化数据，进行独立的“数字化标注”转换过程，由此提供的数字“区块存证”代码，就成为了数字资产交互的应用凭证，为数字资产的实用性落地提供支撑。

从自身信息安全需求出发，当有无数个节点提供者组建起“区块链节点工会社群”，做为一种免费的公共“密文云存储”体系，给未来网络生态提供支撑，进而实现从数据生产端到服务应用端共同来形成 Web3 的基础技术架构体系，推动当前“系统定义数据属性”，向未来“数据定义系统属性”的理论方向发展。

参考文献

[1] Blockchain private file storage-sharing method based on IPFS.P Kang, W Yang, J Zheng - Sensors, 2022 - mdpi.com

[2] When blockchain meets distributed file systems: An overview, challenges, and open issues.H Huang, J Lin, B Zheng, Z Zheng, J Bian - IEEE Access, 2020 - ieeexplore.ieee.org

[3] Blockchain and interplanetary file system (IPFS)-based data storage system for vehicular networks with keyword search capability.N Sangeeta, SY Nam - Electronics, 2023 - mdpi.com

[4] Blockchain based searchable encryption for electronic health record sharing.L Chen, WK Lee, CC Chang, KKR Choo… - … computer systems, 2019 – Elsevier

[5] 庹小忠.基于区块链的加密信息备份系统研究与设计.西南石油大学,2017-06-01

[6] 高捷.基于块链的文件存储系统设计.计算机产品与流通,2019-05-2

[7] 罗鑫.基于区块链的可信存储系统设计与实现.黑龙江大学,2019-04-20

[8] 赵阶旭.区块链存证系统设计与实现.广东技术师范大学,2022-06-01

[9] 王楠 翟峰 曹永峰 冯云 张伟.基于区块链技术的数据共享系统.科学技术与工程,2022

[10] 段平.基于区块链及分层加密技术的数据传输控制系统设计[J].计算机测量与控制,2020,28(10):76-80.

[11] 陈何清. 基于区块链的IMIX传输系统的设计与实现[D].南京大学,2016.

[12] 霍颖瑜,钟勇.基于区块链技术的用户信息加密存储系统设计[J].现代电子技术,2021,44(21):60-64.

[13] 刘金魁.基于同态加密的区块链数据安全传输方法研究[J].信息通信,2019,No.201(09):1-2.

[14] 韩妍妍,张齐,闫晓璇等.基于区块链的电子文件流转设计与实现[J].计算机应用,2020,40(11):3357-3365.

[15] 周全. 基于区块链的边缘设备数据安全传输方法研究[D].南京邮电大学,2021.

[16] 张涛,伍前红,唐宗勋.基于比特币区块链的隐蔽信息传输研究[J].网络与信息安全学报,2021,7(01):84-92.

[17] 常汉杰,付赛红,石志明.浅谈区块链对于文件存储系统的变革[J].计算机时代,2019,No.321(03):101-104.