 DOI: https://doi.org/10.12345/daglyqyfzyj.v2i7.19613

The Practical Application of Blockchain Technology in File Management under the Empowerment Transaction Model

Bing Xue

China Railway Engineering Design Consulting Group Co., Ltd., Beijing, 100041, China

Abstract

Under the empowerment transaction model, the practical application of blockchain technology in file management mainly focuses on ensuring the authenticity and integrity of file information and improving the efficiency of file management. The practical application of blockchain technology in file management under the empowerment transaction model is mainly reflected in ensuring the authenticity and integrity of file information and improving the efficiency of file management. These applications not only improve the efficiency and quality of archives management, but also provide a strong guarantee for the long-term preservation and utilization of archives. This paper mainly studies the underlying transaction model of blockchain, and applies the new transaction model in file management to explore the practical application of blockchain technology in file management under the empowerment transaction mode.

Keywords

archives management; empowerment trading mode; blockchain technology; apply

赋权交易模型下区块链技术在档案管理中的实际应用

薛冰

中铁工程设计咨询集团有限公司，中国·北京 100041

摘　要

在赋权交易模型下，区块链技术在档案管理中的实际应用主要聚焦于保证档案信息的真实性、完整性以及提升档案的管理效率。赋权交易模型下区块链技术在档案管理中的实际应用主要体现在确保档案信息的真实性和完整性、提升档案管理效率等方面。这些应用不仅提高了档案管理的效率和质量，还为档案的长期保存和利用提供了有力保障。论文主要研究区块链底层交易模型，并在档案管理中运用新交易模型，探究赋权交易模型下档案管理工作中对区块链技术的实际应用。

关键词

档案管理；赋权交易模型；区块链技术；应用

1 引言

社会经济全球化的现如今，大众对档案管理提出更高要求，并提出档案数字化的理念。现如今的数字档案存储方式多选择中心化存储，使得档案被修改、丢失问题仍旧存在。区块链产生与发展后，在档案管理领域应用区块链技术的研究者也逐渐增多。区块链技术是根据时间排序的数据块，主要被用于交易信息与信息资源的记录，各数据块均有数字指纹，这一数字指纹是依照哈希函数计算该数据块指纹和前数据块指纹所产生的数字序列 [1]。2018 年，谭海波等学者借助区块链、IPFS 以及智能合约技术进行档案的管理，现阶段该系统被初步试用于中科院档案管理馆。论文主要研究区块链底层交易模型，并在档案管理中运用新交易模型，探究赋权交易模型下档案管理工作中对区块链技术的实际应用。

【作者简介】薛冰（1983–），男，中国陕西吴堡人，本科，高级工程师，从事档案管理研究。

2 相关技术

2.1 档案管理中的区块链技术发展过程

区块链技术以去中心化、透明、安全的特点，近年来受到了广泛关注。其基本原理是通过建立可靠的对等网络，将数据记录以区块的形式连接起来，形成一条无法篡改的链条。每个区块包含一定数量的交易数据以及指向前区块的引用，确保数据的完整性和真实性 [2]。随着信息技术的迅猛发展，档案管理面临着数字化、智能化转型的压力，同时也面临着信息安全、隐私保护等方面的挑战。传统的档案管理方式已经无法满足日益增长的档案存储、查询、共享需求。此外，档案的真实性和完整性也面临着巨大的威胁。因此，探索新的档案管理方式，提高档案管理效率，保障档案安全，成为当前档案管理面临的重要任务。区块链技术以其独特优势，在档案管理中展现出巨大的应用潜力。以爱尔兰国家电子健康档案（NEHI）为例，该项目应用区块链技术，将患者的医疗档案存储在一个去中心化的数据库中，并通过智能

合约实现数据的访问和交换。这不仅保护了患者的隐私和信息安全，还提高了医生的工作效率。此外，比利时医疗数据共享平台和美国华盛顿州立大学医学中心的区块链研究项目也展示了区块链技术在数字医疗档案中的成功应用。

2.2 UTXO 模型

UTXO（Unspent Transaction Output）模型是比特币和其他一些加密货币所使用的一种交易记录方式。这种模型与传统的账户 / 余额模型（如银行账户、支付宝账户等）有着显著的区别。多个 UTXO 可以组合使用以支付更大的金额，而单个 UTXO 也可以被拆分以用于支付较小金额。但请注意，UTXO 作为支付单元时必须是完整的，不能像实物货币那样部分使用。UTXO 模型使得比特币在可审计性、透明性和效率上更优于传统金融系统。因为所有的交易历史都被记录在区块链上，任何人都可以查看和验证，这增加了系统的透明度和可信度。可见，UTXO 模型是比特币等加密货币所使用的独特交易记录方式，它通过记录未花费的交易输出来追踪和验证资金的流动 [3]。这种模型与传统的账户 / 余额模型不同，具有一些独特的优点，使得加密货币在交易过程中更加安全、透明和高效。

2.3 脚本

在区块链技术中，脚本扮演着至关重要的角色。它们是确保区块链交易正确执行、验证数据完整性和安全性的核心组成部分。脚本定义了交易的条件和规则，只有满足这些条件的交易才会被网络中的节点接受并写入区块链。因此，脚本是维护区块链网络稳定性和安全性的关键。在区块链网络中，脚本的执行和验证是确保交易有效性和安全性的关键步骤。当一个新的交易被提交到网络中时，网络中的节点会运行该交易的脚本代码，以验证其是否符合规定的条件和规则。如果脚本执行成功并返回有效结果，则该交易将被认为是有效的，并被写入区块链中。否则，该交易将被拒绝。

比特币的脚本是比特币系统中的一个核心组成部分，它负责验证和确认比特币交易的合法性和有效性。常见的比特币脚本类型及功能：① P2PK（Pay to Public Key）：这是一种简单的交易方式，其中锁定脚本包含收款人的公钥，而解锁脚本包含签名和公钥。通过公钥验证签名来确认交易的有效性。② P2PKH（Pay to Public Key Hash）：这是一种更常用的交易方式，它通过公钥的哈希值（而非公钥本身）来减少锁定脚本的大小。解锁脚本包含签名和公钥，通过公钥的哈希值来找到对应的公钥并验证签名 [4]。③ P2SH（Pay to Script Hash）：这是一种更复杂的交易方式，它允许使用更复杂的脚本（如多重签名）来进行交易。锁定脚本包含一个赎回脚本的哈希值，而解锁脚本包含赎回脚本和满足赎回脚本条件的证据。

3 赋权交易模型

3.1 模型提出背景

现阶段的区块链技术交易多选择 account、UTXO，这两大模型多被用于虚拟货币交易中，关键在于中心化交易，有效防止数字货币双花。具体应用时，虚拟货币交易并不能规避非具体交易存在的问题 [5]。例如，交易的并非具体虚拟货币，多为交易双方权限，交易期间并不会有具体数额产生，多是通过数字或符号所表示权限，由此就要由新交易模型解决该问题。该研究通过改进 UTXO 模型，提出赋权交易（ET）模型。UTXO 模型内，一次交易的多笔交易输入相当于交易输出和，如公式（1）所示。而 ET 模型内，一次交易输入则大于交易输出和最大值，具体见公式（2）。

$$\sum Q_{in}\{x_1,x_2,...,x_n\}=\sum Q_{out}\{x_1,x_2,...,x_m\} \quad (1)$$

$$x_n \succ Q_{\max}\{x_1,x_2,...x_m\} \quad (2)$$

3.2 ET 模型交易数据存储结构

3.2.1 传统数据存储结构

传统的数据存储结构通常可以归纳为以下几种类型，每种类型都有其特定的特点和适用场景：①顺序存储结构。把逻辑上相邻的结点存储在物理位置相邻的存储单元里。结点间的逻辑关系由存储单元的邻接关系来体现。该结构通常借助于程序设计语言中的数组来实现。优点：访问元素的时间都相同，因为每个元素的存储位置都可以通过简单计算得到。不必耗费额外的空间，数据元素之间的关系由它们在存储器中的邻接关系来表示。②链式存储结构。数据元素可以存放在不连续的内存单元中。数据元素之间的逻辑关系是通过指示数据元素存储地址的指针来表示的。该结构存储空间的利用比较灵活，数据元素的增减操作比较方便。③索引存储结构。按照某种性质把一个大表的元素划分成若干个子表，每个子表中的元素具有相同的性质。同时建立一个索引表，索引表中的每个索引项对应一个子表，并给出该子表的起始地址、长度和性质。该结构需要对大量数据进行快速查找和访问的情况，如数据库系统中的索引结构。

3.2.2 ET 模型改进存储结构

该研究中，选择二进制数 C_{total} 形式对文档内权限值进行储存，这一数值多是由拥有权限值集合得到，即：$Q\{C_1,C_1,...C_i,...C_n\}$，集合内，$C_i$ 表示该权限制于 C_{total} 二进制内的第 i 位。C_{total} 数值的公式为：

$$C_{total}=2^{C_1-1}+2^{C_2-1}+...+2^{C_i-1}+...+2^{C_n-1} \quad (3)$$

例如，交易时的存储交易权限空间大小是 1Byte，多分为两个存储过程，如图 1 和图 2 所示。若是主权限（数据生命周期内权限最大值），主权限就会在最高位存储。如果不是主权限，就要在后权限存储、前权限存储中间位置存储。

算法一：UTXO 数据存储。

输入：在不在主权限和前权限存储、后权限存储的位置。

输出：权限的具体存储位置。①存储位置在 $C_{topdigit}$；②存储位置在 $(C_{prePower}+C_{NexPower})/2$。

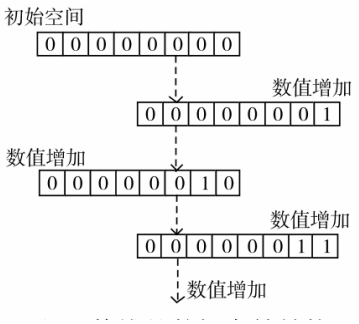

图 1 传统数据存储

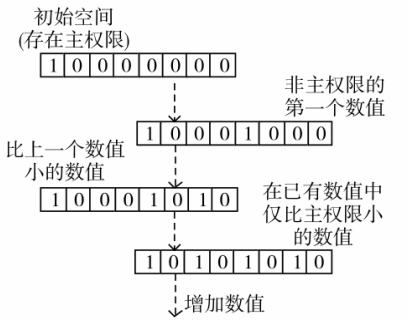

图 2 UTXO 数据存储

3.3 ET 模型的容量扩充

在讨论 ET 模型的容量扩充时，需要明确以太坊面临的主要挑战之一是随着网络使用量的增长，交易速度和吞吐量的问题。以下是几种主要的 ET 模型容量扩充技术和方法的清晰归纳：①分片（Sharding）。分片是将整个网络划分为多个较小的、独立的“分片”，每个分片可以并行处理交易，从而提高整个网络的吞吐量。②状态通道（State Channels）。状态通道允许两个或多个参与者在以太坊网络之外进行大量的小额交易，然后将最终状态更新回以太坊主链。③零知识证明（Zero-Knowledge Proofs，ZKPs）。零知识证明是一种密码学技术，允许一方在不透露任何额外信息的情况下，向另一方证明某个陈述是真实的。在以太坊中的应用：例如 zkSync，使用零知识证明来验证交易，从而在不牺牲安全性的前提下提高交易速度。可见，ET 模型的容量扩充是一个多方面的挑战，需要综合考虑技术复杂性、安全性、去中心化程度和实施难度等多个因素。

4 方法实现

文中提出一种基于 Fabric 的联盟链，其中 5 个结点都是联盟链的支持结点，而这些结点通过 Web 页对 API 的存取来与其进行通信。一份档案具有三种不同的权利：AM，AO，SI。一份档案必须有 AO。当档案有必要时，将会有 AM。若 AM 或 AO 将档案中的某些可读取权利授予第三方，那么将存在第三个，也就是 SI。如果是在 AM 中，那么一个档案的总 C_{total} 的二进制数字是 1。档案总计的二进位数字为 1，这表明 AO 的许可位于中心。接下来将以时序图的形式展示在该文中将区块链用于档案储存处理的若干情形。

情景 1：一个使用者请求储存他自己的个人资料。在该方案中，当预设使用者尚未取得公开与私有密钥时，使用者可以透过 API 获取相应的私有密钥、公开密钥、私钥加密后的档案哈希值以及与之相关的区块资讯。其中五个签字节点能够存储用户的公共密钥，经过私钥加密的档案哈希码，以及事务存储的区块的数据。

情景 2：档案所有者将档案授权给其他用户。在这个方案中，预设的是，未配置档案所有者使用者和未配置档案所有者使用者均已申请了相应的公钥专用密钥。

论文的用户节点是经由网络来模仿网际网络连接来存取认证结点，使用者节点所存取的界面则是使用 Web 界面。用户可以通过 Web 页面的接口与认证节点进行连接，从而完成对文章 hash 信息的存储。

5 结语

总而言之，随着区块链技术发展速度越来越快，基于区块链的应用逐渐增多。该研究中的赋权交易模型就是对区块链下 UTXO 模式做出的优化与完善，档案授权中应用区块链技术，确保区块链可以应用到无特定数字交易。在已有的研究中，ET 模式表现出了很好的稳定性，即使是经过了很多次的买卖，一个存档仍然可以维持很短的时间。ET 模式是针对无特定数字的交易，因此 ET 模式也可以用于其他的行业，例如软件的版权交易，影视作品的版权交易。

参考文献

[1] 李严,陈世平.基于赋权交易模型的区块链技术的档案管理研究[J].计算机应用研究,2021,38(1):28-32+38.

[2] 胡呈梅.基于区块链技术的铁路项目档案管理信息系统设计[J].自动化技术与应用,2023,42(2):114-116+125.

[3] 张新淼.区块链技术下的沉浸式加密档案管理研究与设计[J].网络空间安全,2023,14(1):81-84+95.

[4] 沈航.医院综合档案管理中区块链技术的运用前景分析[J].办公自动化,2023,28(14):56-58.

[5] 宋瑶.大数据环境下区块链技术在高职院校电子档案管理中的创新应用[J].信息记录材料,2024,25(3):87-89+92.