基于区块链技术的学生档案信息安全共享方法

殷艳菲[1]
YIN Yanfei

摘 要 针对现有共享方法在学生档案信息共享时存在档案信息篡改问题，首先引入区块链技术，对学生档案信息安全共享方法进行设计，利用区块链技术，构建学生档案共享可信性保护框架；然后在框架的保护下，完成学生档案信息共享密钥的生成与分发；最后通过秘密值与秘密份额的设定，实现学生档案信息秘密安全共享。通过对比实验可知，新的共享方法可以保证学生档案信息共享的安全性，在共享时不会被不具备共享权限的用户非法获取档案信息，且档案信息内容不会被篡改，为学生档案的管理提供更有利的技术支撑条件。

关键词 区块链技术；档案；共享；安全；信息；学生

doi：10.3969/j.issn.1672-9528.2024.02.036

0 引言

学生档案信息可以全面记录并反映学生在各个时期的发展情况。作为培养高素质人才的主要场所，学校的档案管理工作直接关系到高校学生知识、文化素养和健康人格的塑造[1]。然而，受实际情况的限制，传统的档案管理模式存在着一些问题，如档案管理意识淡薄、档案管理制度不完善、数字化程度不够等。为了从根本上改善这些不足，学校应当利用信息技术，深入挖掘高校档案的资源价值，以全面满足学校师生对档案资源的利用需要[2]。在此基础上，高校应从当前面临的实际困境出发，增加对学生档案资源建设的投资，寻求最优的途径。学生档案信息的共享是指将各类档案资源通过网络或其他方式进行共享。在共享之前，首先需要对信息资源进行整合。整合是指将来自不同数据源的信息整合在一起，并按统一的编码形式进行分类，以便于信息的共享。信息的共享则是将整合后的资源通过网络实现传输，以此让用户可以更加方便地获取到所需的档案信息资源。同时，需要明确的是，信息的共享必须建立在资源安全的基础上。因此，必须要制定一系列安全措施，如加密和权限管理等，确保档案中的信息不会被非法获取或篡改，保障学生的个人利益免受损害。

基于此，为了促进学校档案管理工作智慧化、数字化建设和发展，本文将结合区块链技术，开展对学生档案信息安全共享方法的设计研究。

1. 山西应用科技学院 山西太原 030000

1 基于区块链技术的学生档案共享可信性保护框架

引入区块链技术当中的分布式账本、共识机制以及非对称加密算法，建立一个针对学生档案信息共享的可信性保护框架[3]，提出一种基于区块链技术的电子文件可信保证方案。在电子文件可信保护中，最关键的是要保证其准确性、可靠性及真实性，通过保证学生档案从创造、产生、使用以及各个环节的可信度来保证其可信度。从这个意义上来说，区块链技术最大的优点，就是它的可靠性和安全性[4]。图 1 为基于区块链技术建立学生档案共享可信性保护框架基本结构。

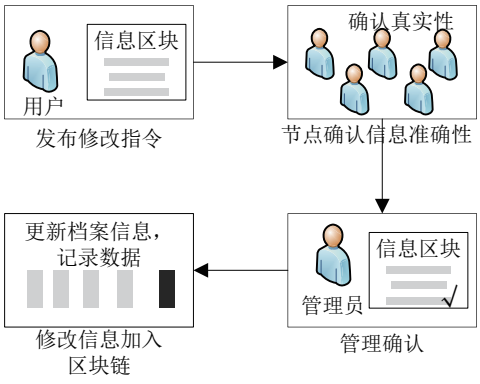

图 1 可信性保护框架基本结构示意图

在整个框架中，将区块链的基础贯穿到学生档案管理的全生命周期中。利用区块链的可追溯性和真实性确保学生档案的任何操作都会被区块记录。随着时间的推移，会对学生档案的内容进行修改[5]。修改包含新增内容和更新内容。将修改后的档案信息分别传送到区块链中进行保存。可将学生档案信息存储在区块链的分布式账本当中，在区块链结构创建后，用户所发出的所有账本改变指令的全体集合核心工作

原理为：

$$S(t+1)=F(S(t),B(t+1)) \quad (1)$$

式中：S 表示账本当前状态；B 表示区块链上的区块；F 表示状态函数；t 表示时刻。根据账本的状态，判断修改后的学生档案信息是否可以存储在该账本当中[6]。分布式账本，简而言之，就是一个家庭需要记账，每个家庭的成员都要按照家里的规矩来记录，每一次记录，都要经过半数以上的成员的同意，如果一个家庭的成员想要修改账本，必须经过其他所有的成员的同意，然后才可以进行修改，而且修改的痕迹会出现在每个家庭的账本上，而这份账本在每一个家庭成员的手中都有一个独一无二的、真实的账本作为备份。在区块链中，所有存储的文件都是被锁定的，通过智能合约和非对称密码学来控制文件的权限，通过密码学来保护账本。在应用到学生档案信息共享中时，通过分布式账本按照一致同意的规则，对档案信息中各个节点的内容进行更新，以此可以有效防止学生档案中的信息内容被非法篡改[7]。

利用区块链技术中的哈希值算法，对存储在分布式账本中的学生档案信息进行初步加密处理，以此提高保存过程中学生档案信息的安全性[8]。哈希值算法的表达式为：

$$hash=floor(M/S(t+1)\times a) \quad (2)$$

式中：*hash* 表示区块链上分布式账本中存储的学生档案信息哈希值；*floor* 表示向下取整运算；M 表示次幂；a 表示哈希系数。利用上述哈希值算法，对存储在分布式账本中的学生档案信息进行初步加密。将加密后的学生档案信息从各个节点上写入到区块链上[9]。在这一过程中，为了减轻区块链的运行负担，需要确保学生档案信息中没有不完整信息、错误信息和重复信息，以此提高运行效率，方便后续对学生档案信息的安全共享[10]。同时，在区块链的智能合约当中，对各个存储节点制定规则，各个节点需要在获取到其他节点一致通过的情况下，才能够针对不符合要求的信息进行修改。对于学生档案中存在的多元数据而言，智能合约的引入可以进一步提高学生档案信息的真实性，为后续安全共享提供可靠数据。

2 学生档案信息共享密钥生成与分发

在完成对基于区块链技术的学生档案共享可信性保护框架建立后，结合区块链技术中的非对称加密算法，对学生档案信息进行加密。在这一过程中，需要生成用于实现学生档案信息共享的密钥，并将其分发给具备访问权限的用户[11]。若不对学生档案的写权限加以约束，任何人都可以通过自己的私钥在档案上写信息，这种现象与学生档案信息的安全共享要求严重不符[12]。针对这一问题，为了确保学生档案信息的准确性和专业性，同时避免学生的隐私信息泄露，可信授权允许学生自己随时读自己的档案，但不能写信息，而其他用户只有在获得了权限后才能够写或读信息[13]。可信授权分别为不同用户生成并分发读密钥和写密钥，具体步骤如下。第一步，通过运行 RSA 的密钥生成该算法生成密钥中所需的各项参数 $(p,q,e,d,f(hash))$，其中参数 p、q、e、d、f 均为保密的参数，其中 p 表示学生本人，q 表示共享用户，e 表示写密钥，d 表示读密钥，f 表示生成函数。

第二步，为共享用户 d_i 随机选取一个写密钥 e_{i1}，计算写密钥 e_{i1} 的相关写密钥 e_{i2}，并将其发送给服务提供商，其中 e_{i2} 应当满足下述公式条件：

$$e_{i1}e_{i2}=d \bmod f(hash) \quad (3)$$

第三步，为共享用户 p_j 随机选取一个读密钥，读密钥可用 d_{j1} 表示，同样按照上述写密钥的逻辑，为其计算与读密钥 d_{j1} 相关的读密钥 d_{j2}，并将其发送到服务供应商。其中 d_{j2} 同样需要满足一定条件才能够发送，条件为：

$$d_{j1}d_{j2}=d \bmod f(n)-e_{i1}e_{i2} \quad (4)$$

按照上述步骤，结合生成的可公开的信息，结合 CP-ABE 算法，为每一个共享用户生成相应的属性密钥。首先，共享用户可以随机选取一个已知的参数 k，并结合参数 k 生成一个具有双线性特点的参数，同时随机选取两个指数、一个安全的非对称加密算法和一个安全的哈希函数。由学校保存主密钥，其表达式为：

$$MK=(d_{j1}d_{j2},g^a) \quad (5)$$

式中：*MK* 表示主密钥；a 表示选取的指数；g 表示生成的双线性参数集合中的某一参数。

然后，在此基础上，运行 CP-ABE 密钥生成算法，为每一名共享用户生成属性密钥。针对每一个属性，都需要以随机的方式获得一个不同的参数。

最后选择 RSA 算法，为每个学校生成签名密钥对，用于在紧急情况下申请存在该位置上的秘密份额，可授权中心首先对该名用户的身份进行验证，在验证通过后，向服务提供商申请学生档案的访问权限[14]。学校选择一个相同的安全签名算法，为每一个具备授权访问权限的共享用户生成签名密钥对，用于在特殊情况下申请秘密份额，在验证其身份和事件后，向中心提交访问学生档案的申请。

3 学生档案信息秘密安全共享

为进一步提高学生档案信息的安全性，设计一种全新的秘密共享模式。当学生用户首次在个人档案系统中注册时，为用户随机选择一个且唯一的秘密值，并将其划分为三个部分，其中任意两个部分的秘密份额都可以正常恢复出秘密值的哈希值，利用该方法可为用户获取学生档案访问权限提供证明[15]。将可以访问学生档案的用户大致划分为三类，一类

为用户可随身携带的 Ukey，一类为口令，一类为学生档案管理中心。对应存储的每个秘密份额均不相同。秘密份额的生成过程是作为秘密分发者随机选择参数对其进行转换，转换后，公开参数，并由学生档案管理中心秘密持有未公开参数。学生档案管理中心随机选择一个多项式，为上述三类可访问学生档案信息的用户生成并分发共享私钥，共享私钥可表示为：

$$D_{MK} = g_1^{q(i)} F(MK)^r \tag{6}$$

式中：D_{MK} 表示生成的共享私钥；$g_1^{q(i)}$ 表示公开参数；$F(MK)^r$ 表示加密多项式。在这一过程中应当注意，学生档案管理中心只完成一次对共享私钥 D_{MK} 的计算，对于不同学生的档案而言，在档案管理中心，只有其对应的秘密值是不同的。学生档案管理中心将生成的共享私钥发送给服务提供商，通过这种方式约束学校对学生档案的访问权限。只有能够正确恢复出秘密值的哈希值的用户才能够得到学生档案密文信息。为进一步实现在共享的过程中获取到学生档案的私密保护和细粒度访问控制，可设置适当的访问和共享控制策略，允许拥有相关属性的共享用户拥有对学生档案的读权限。采用 CP-ABE 算法中的加密算法，对学生档案信息读密钥进行加密，并将加密后的内容存储在云服务器当中。为了提高学生档案信息的安全性，在最初创建学生档案时，可按照下述方式进行加密。首先，由档案管理人员在密钥空间当中随机获取到一个非对称的密钥 k；然后通过运算非对称加密算法 E 实现对一个新学生档案的加密；最后，加密后的学生档案为 M，再利用该学生档案当中的写密钥 e_{i1} 以及加密选取的对称密钥 k，生成一个如下述公式所示的密文：

$$C = (C_{i1} = E_k(M), C_{i2} = k^{e_{i1}} \bmod D_{MK}) \tag{7}$$

式中：C 表示生成的密文。由档案管理中心将具备上述公式所示结构的密文发送给服务提供商。当收到某一用户发送的密文时，此时由服务提供商首先对学生以及共享用户的身份进行验证，再利用共享用户提供的写密钥重新加密该密文，以此得到新的密文，对该密文进行共享可以确保学生档案的安全性，防止其他未授权用户的非法访问。除此之外，区块链技术具备极强的可验证性和可追溯性，能够确保学生档案中的信息不被篡改。在对学生档案信息秘密安全共享时，可选用双链结构，其中一条链负责共享查询，另一条链负责存储信息。通过这种双链结构的应用可以实现共享查阅与存储的分离，并通过双链锚定实现对存储在链上的数据进行安全保护和验证。在区块链结构上，任何用户角色都是匿名的，共享的过程中不会暴露用户的身份信息。

4 对比实验

本文针对学生档案信息安全共享问题，结合区块链技术，设计了一种全新的安全共享方法，为了进一步验证该方法的应用性能，以及与其他现有共享方法相比是否能够有效解决存在的问题，开展下述对比实验研究，其实验环境配置如表 1 所示。

表 1 实验环境配置

CPU	Inter Core i5
RAM	16.0 GB
操作系统	Windows10 64 位
GPU	NVIDIA 1050
Python 版本	Python3.7
CUDA 版本	10.0
PyTorch 版本	1.10
数据集	Mnist

实验过程中，以某高校学生档案为基础，为确保不对学生的隐私造成威胁，学生档案中的信息均经过特殊处理，将其作为此次实验的实验集。分别利用本文提出的基于区块链技术的共享方法（实验组）、基于 RSA 加密算法的共享方法（对照 A 组）和基于 Hadoop 云平台的共享方法（对照 B 组），对实验集中进行共享。首先针对三种共享方法在实际应用中的安全性进行对比，选择五名学生的档案进行共享。然后将五名学生档案的编号为 Files-01、Files-02、Files-03、Files-04、Files-05 在这一过程中，记录具备共享权限用户获取到的学生档案信息量分别为 1 253.1 Mbit、1 326.4 Mbit、1 526.3 Mbit、1 635.4 Mbit、1 534.2 Mbit，则不具备共享权限用户非法获取到的学生档案信息量为 Mf，并将结果记录如图 2 所示。

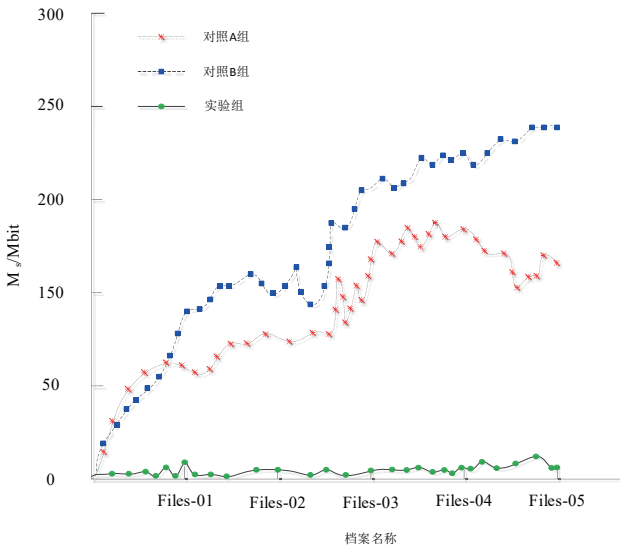

图 2 三种共享方法共享安全性对比

结合图 2 中记录的内容对三种共享方法的共享安全性进行对比分析。通过分析得出，三种共享方法应用下均能够

为具备共享权限的用户提供学生档案中的所有信息，但在共享的过程中，只有实验组共享方法可以确保不具备共享权限的用户非法获取的学生档案信息量在 0.0 ～ 0.2 Mbit 范围内，这一范围内的信息量不会对学生的隐私安全造成威胁。而对照 A 组和对照 B 组共享方法应用下，不具备共享权限用户非法获取到的学生档案信息量分别超过 150.0 Mbit 和 240.0 Mbit，无法保证非法获取到的信息不是学生隐私信息，无法确保学生信息安全权益不受损。

在此基础上，为了进一步验证三种共享方法的防篡改能力，仍然以上述五个学生档案作为实验研究对象，分别利用多种不同的篡改方式，在学生档案信息共享的过程中对其进行篡改攻击，并记录学生档案中被篡改的信息量，以此验证三种共享方法各自的防篡改效果。将得到的实验结果进行记录，如表 2 所示。

表 2 三种共享方法防篡改效果记录表

学生档案	实验组被篡改信息量 /Mbit	对照 A 组被篡改信息量 /Mbit	对照 B 组篡改信息量 /Mbit
Files-01	0	123.2	241.2
Files-02	0	144.3	243.8
Files-03	0	112.3	223.4
Files-04	0	124.2	254.3
Files-05	0	122.3	242.3

对表 2 中记录的实验结果进行分析得出，实验组共享方法可以确保学生档案信息在共享的过程中不被篡改，被篡改信息量可以达到 0 Mbit 水平。而对照 A 组和对照 B 组共享方法在应用过程中无法达到实验组共享方法的防篡改效果和水平，学生档案在共享时被篡改量分别控制在 110.0 ～ 150.0 Mbit 范围内和 220.0 ～ 255.0 Mbit 范围内，篡改部分信息会严重影响到学生档案信息的可靠性和真实性。因此，本文提出的基于区块链技术的共享方法可以实现对学生档案信息的安全共享，一方面确保学生档案信息不会被不具备共享权限的用户非法获取，另一方面共享过程中具备极高的防篡改能力，确保学生档案信息的可靠性。

5 结语

本文结合区块链技术，设计了一种全新的学生档案信息安全共享方法，并通过将新的共享方法与现有共享方法比较，验证了新共享方法的应用优势。在当前互联网背景下，学生档案服务需要进行不断的改革和创新，才能够顺应当代创新驱动发展战略。通过不断学习和引进新兴技术，解决以前遗留的问题，以此确保学生档案的安全，同时更便于学生档案信息管理的高效便捷，实现全面利用与共享。

参考文献：

[1] 潘彬彬 , 沈利成 . 关于博物馆第一次全国可移动文物普查档案信息共享的思考 [J]. 档案与建设 ,2023(4):79-81.

[2] 陈智杰 . 高质量发展视域下 档案信息资源共享的必要性、可行性及实现路径 [J]. 兰台内外 ,2023(10):1-3.

[3] 董婉婷 . 基于分布式区块链和 RSA 加密的医疗档案信息共享策略研究 [J]. 电子设计工程 ,2022,30(22):131-135.

[4] 李月 , 刘丽丽 . 网络环境下高等职业技术院校档案信息资源共享模式与策略研究 [J]. 杨凌职业技术学院学报 , 2022, 21(3): 32-34.

[5] 王大众 . 逐步实现全国档案信息共享利用“一网通办”：全国档案查询利用服务平台正式上线 [J]. 中国档案 , 2022(8): 14-15.

[6] 段新宇 , 王志丽 . 高校人事档案信息资源共享安全风险及防控对策探讨 [J]. 赤峰学院学报 (自然科学版), 2022, 38(7): 48-51.

[7] 彭荟吉 . 基于“互联网 +”背景下的区域性高校档案信息资源共建共享模式新探 [J]. 兰台内外 ,2021(16):7-9.

[8] 王韵哲 , 潘世萍 , 史爱丽 , 等 . 企业登记档案信息资源共享利用研究 : 以北京市市场监督管理局为例 [J]. 北京档案 , 2022(5): 30-33.

[9] 范雨欣 . Hadoop 云平台 MapReduce 下数字档案信息资源共享平台的优化 [J]. 兰台世界 ,2022(5):107-110.

[10] 卞咸杰 . 大数据时代档案信息资源共享平台数据存储系统的设计与实现 [J]. 档案与建设 ,2021(2):20-25.

[11] 张林华 , 原婧妍 , 王璐琪 , 等 . 档案公共服务发展的必由之路：档案信息资源共享的必要性、可行性及实现路径 [J]. 秘书 , 2022(1):84-95.

[12] 许雯婷 . 基于联盟区块链技术的高校档案信息资源共享模式探究 : 以粤港澳大湾区为例 [J]. 中国多媒体与网络教学学报 (中旬刊), 2022(1):184-187.

[13] 张占武 . 高校档案信息资源共享在互联网环境下的有效建设研究 [J]. 浙江档案 , 2021(10):57-59.

[14] 黄兆贺 . 新时期不动产登记档案信息共享基本现状及对策建议 [J]. 城建档案 , 2021(10):88-90.

[15] 许桢桢 . “互联网 +”下优化档案信息资源共享服务的策略研究 [J]. 黑龙江档案 ,2021(3):180-181.

【作者简介】

殷艳菲（1981—）， 女，山西运城人，研究生，助教，研究方向：信息化管理。

（收稿日期：2023-11-02）