基于区块链技术的高校学生信息管理与共享平台构建研究

赵 鹏[1] 张凯欣[1]
ZHAO Peng ZHANG Kaixin

摘 要 教育信息化纵深发展背景下，针对教育数据治理中存在的异构系统间数据孤岛、隐私泄漏风险及跨域协同效能不足等瓶颈问题，文章提出了一个基于区块链技术的多主体协同治理框架。通过构建联盟链架构整合高校、教育行政部门与企业节点，设计链上链下协同存储机制，包括核心学籍信息的哈希加密上链存证和非结构化数据的加密存储。创新性引入零知识证明技术，构建“验证 - 响应”机制，使企业无需获取明文即可核验学历证书等关键信息的真实性。通过智能合约实现学生信息的动态权限控制，支持多粒度隐私授权与访问追溯。该架构利用区块链不可篡改特性保障数据完整性，借助密码学技术强化隐私保护，结合 IPFS 降低存储冗余，有效解决传统中心化系统的单点风险与信任缺失问题。

关键词 区块链；零知识证明；IPFS 存储

doi：10.3969/j.issn.1672-9528.2025.09.038

0 引言

在“互联网 + 教育”行动计划持续推进与《中国教育现代化 2035》战略框架深化的背景下[1]，教育信息化作为教育现代化的重要引擎，其数据治理效能直接影响着教育改革进程。当前教育领域[2]面临三大核心挑战：首先，信息生态的割裂化问题突出。不同的教育机构、行政部门以及市场主体在技术标准的选择上存在显著差异，这在无形之中形成了数据流通的壁垒。其次，数据主权与安全防护之间存在失衡现象。传统的中心化存储架构存在明显的系统性风险。当数据库遭受网络攻击或出现操作失误时，学生的隐私数据极有可能被泄露，这不仅侵犯了学生的个人权益，也对教育数据的安全性和可靠性构成了严重威胁。最后，跨系统协作效能亟待提高。在现有的模式下，学生在升学就业、跨境交流等重要场景中，仍然需要提交大量的实体证明材料。依赖人工核验的认证机制不仅效率低下，而且由于人为因素的干扰，存在信息失真[3]的潜在风险。这种低效的信息流转模式已无法满足数字化时代教育领域快速发展的需求，亟须进行优化和改进。

区块链技术[4]凭借去中心化、不可篡改、高透明度等显著特性，为教育信息管理领域提供了创新性的解决途径。通过将学生在校成绩、奖惩记录、学位证书、学籍管理及毕业信息等上链，每当有新的学生信息或更新需要记录时，平台上的参与节点会通过共识机制来决定哪些信息可以被添加到区块链上。企业可以使用零知识证明来验证学生信息的真实性，而无需将完整的信息公开保护学生的个人隐私。在平台中使用集成 IPFS（interplanetary file system）文件存储系统[5]，可显著增强数据的分布式存储能力，提高数据访问效率，同时降低数据存储成本。该系统还能有效强化信息的真实性与可追溯性，推动教育信息的高效流通与互信。

近年来，国际范围内，以麻省理工学院（MIT）为代表的知名高校已开展运用区块链技术发行数字学位证书的尝试，其目的在于保障学历的真实性，强化防伪功能。国内，Lyer 等人[6]描绘一种综合教育模型，该模型以学生为中心，并利用区块链技术提供安全性、真实性、不变性、长寿性、数据信息的安全存储、去中心化、无中介、可靠性和数据完整性。Ding 等人[7]将区块链引入教育领域，设计基于智能合约的成绩存证系统，实现操作留痕与流程自动化，然而采用明文上链策略导致敏感信息暴露风险，反映出早期区块链应用对链上隐私保护的忽视。Omkar 等人[8]构建的多角色协同 SIMS 平台虽实现教务流程数字化，却缺乏对数据共享场景的隐私风险评估机制，特别是在大规模数据流动时难以防范二次传播风险。张达[9]提出高校信息管理体系动态修复模型，通过漏洞模式识别提升系统鲁棒性，但其改良路径未能突破中心化架构的固有局限。Jiang 等人[10]构建的去中心化信息共享系统利用区块链不可篡改特性，使数据操作可追溯性达到交易级精度。Yu 等人[11]在区块链的教育上进行了深刻的

1. 太原师范学院 山西晋中 030619

[基金项目] 山西省科技战略研究专项重点项目“山西省信创产业科教融汇、产教融合的模式与实施路径研究”（202304031401011）

研究。Sura 等人[12]提出的三模型架构则通过模块化智能合约实现课程注册、成绩录入等核心业务的链上重构，但上述研究均未有效解决两大关键问题：一是未建立适应教育管理特性的动态访问控制机制，二是缺乏零知识证明等隐私增强技术的系统化集成，导致敏感字段仍存在泄露隐患。

本文探讨了基于区块链技术的高校学生信息管理与共享平台，利用区块链的去中心化和不可篡改特性，实现学生信息的高效、安全、透明管理，并促进高校与企业间的信息共享。研究的创新点包括：构建去中心化学生信息共享平台，简化企业验证学生学历的流程，提高招聘效率，同时保护学生隐私；采用零知识证明技术，实现验证方在不获取完整信息的情况下核验学生信息，学生可自主控制信息访问权限；利用 IPFS 进行链外存储，减轻区块链存储负担，降低存储成本，提高访问效率。

1 相关知识

1.1 区块链技术

自 2008 年 Nakamoto 最早提出“比特币”[13]概念，其底层技术区块链开始受到关注，区块链技术是一种去中心化的分布式账本技术，旨在提供一种安全、透明的方式来记录和验证交易。它通过将数据组织成一系列区块，并利用密码学技术链接起来形成链式结构，从而确保了数据的一致性和不可篡改性。每个区块包含了一定数量的交易记录，以及一个指向前一个区块的哈希值，这样就形成了一个不断增长的链条。图 1 是区块链体的结构。

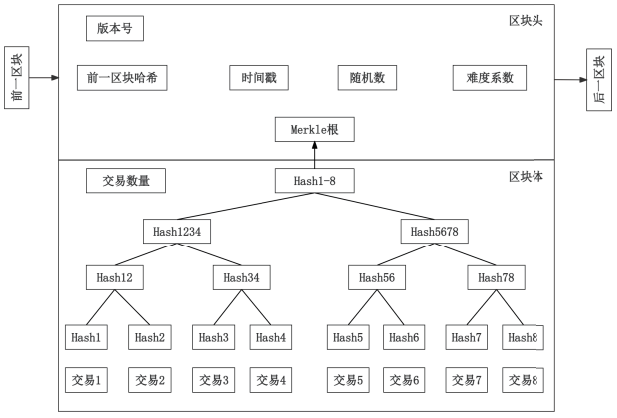

图 1 区块链结构体

1.2 IPFS 存储

星际文件系统[14]（IPFS）通过内容寻址识别网络中的文件，旨在替代 HTTP 协议。是一个分布式、点对点的超媒体协议，目标是提高网络速度、安全性、开放性和去中心化。IPFS 为文件提供唯一哈希地址，重复上传同一文件会得到相同地址，其去重复机制有效减少数据冗余。结合去中心化，系统效率更高，避免存储浪费。IPFS 整合到链外存储，解决区块链网络的可伸缩性问题，数据永久存储，防止篡改和故障。IPFS 体系结构由 4 个主要组件构成：分布式哈希表（DHT）、自认证文件系统（SFS）、比特交换协议（BitSwap）和默克尔有向无环图结构（Merkle DAG）。

1.3 零知识证明

零知识证明[15]概念的初衷是为了解决密码学中的难题，即如何在不泄露敏感信息的情况下证明某个论断的正确性。对于一个 NP 问题 L 存在一个论断 $x \in L$，证明者 P 需要通过拥有的证据 π 说服验证者 V 相信 $x \in L$，即“证明”，同时证据 π 不会泄露 P 的任何私有信息，即“零知识”。基于 Groth16 协议的零知识证明过程，主要有三个步骤。

（1）首先，零知识证明依据椭圆曲线关系 R 完成初始设置，生成证明密钥 pk 和验证密钥 vk，并分发给相应的证明者 P 和验证者 V。

（2）然后，P 根据待证明论断 x 得到的参数 u、w、密钥 pk 以及关系 R，生成证据 π，并发送给 V。

（3）最后，V 根据证据 π、参数 u、密钥 vk 以及关系 R，验证论断 x 是否成立。

采用零知识证明可以为上述论断 x 的证明过程赋予了 3 个关键性质，这些性质在确保了整个证明过程不会泄露证明者的任何信息，同时保证论断 x 的证明结果是可信的。

（1）完备性：如果证明者 P 提供的论断 $x \in L$ 是真实的，验证者 V 不相信 P 提供的论断的可能性为 0；

（2）可靠性：如果证明者 P 提供的论断 $x \in L$ 是伪造的，那么验证者 V 相信 P 提供的论断的可能性为 0；

（3）零知识性：在证明的过程中，验证者 V 只能从证明者 P 接收到证据 π，而不会获得关于 P 的其他知识，也不能从证据 π 中获取任何信息。

2 系统模型

基于区块链技术高校学生信息管理与共享研究管理平台，需充分考虑教育[16]时代背景与实际工作需要，如图 2 所示，将区块链、IPFS 等技术应用其中，协调好高校内部、高校与政府间多种类型主体的利益需求与价值关系，解决高校信息数据存储和共享存在的问题。基于国内外研究成果，使用联盟区块链来构建高校学生信息管理与共享平台，平台为了提高区块链数据的可信性和安全性，由各级教育行政部门实施常规监管。

（1）监管中心（regulatory center, RC）：负责密钥的生成和存储。监管中心承担系统公共参数的生成，并在系统初始化时生成主密钥。当用户向监管中心发起注册请求时，监管中心会为请求注册的用户生成对应的密钥，并通过安全通道发送给用户。用户的身份信息将被安全地存储在监管中心中，同时公钥的 SHA256 哈希值会被传输到联盟区块链以进

行备份。

（2）学生（data owner, DO）：学生在首次注册时应在系统中注册，监管中心为每个学生分配公私密钥对，学生使用自己的公钥对加密后的信息，以证明信息的真实性和完整性。学生可以授予学校或企业访问相关数据的权限，并设置访问记录的时间限制。

（3）学校（school, DO）：负责生成和维护学生的电子档案（如成绩单、个人信息等），并将加密后的信息上传到IPFS。学校使用对称加密算法加密学生的敏感信息。以实现安全快速地加密和访问控制。

（4）企业（data user, DU）：企业需要访问学生信息时，必须通过零知识证明验证其身份。企业从学校或学生处获得授权后，可以访问相关的学生信息。

（5）IPFS（interplanetary file system）：负责存储加密后的学生信息，并返回一个唯一的 CID。

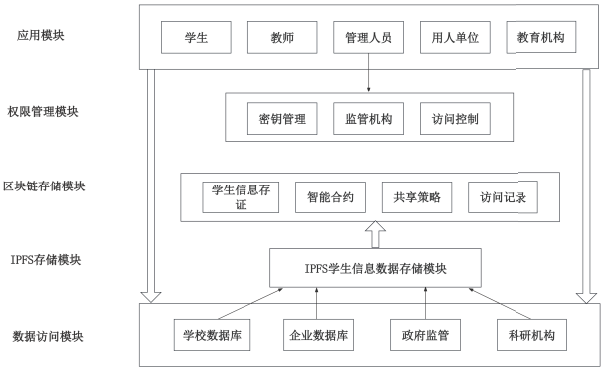

图 2 高校学生信息管理与共享系统模型架构

3 功能实现

本研究旨在研究构建一个基于区块链技术的高校学生信息管理与共享平台，利用分布式账本技术（Hyperledger Fabric）与零知识证明、IPFS 存储相结合，设计出高效、安全、透明的数据存储和共享策略。本章详细描述了平台的实现方案，首先介绍了高校学生信息存储策略，包括系统初始化、信息加密、IPFS 存储等关键环节；然后讨论了信息共享策略，重点介绍了零知识证明在平台中的应用，确保信息隐私保护的同时实现数据的有效共享。

4 系统设计与初始化阶段

系统初始化阶段包括实体注册、身份验证、密钥生成与分发等步骤，确保平台的用户身份的唯一性与数据安全性。

4.1 实体注册与身份验证

系统的初始化首先从实体注册开始。平台中的参与实体包括学校、企业、学生等各种角色。每个实体需要向监管中心提交注册请求，包含其唯一标识符（ID）和身份验证信息（如姓名、联系方式、学历等）。这些信息将用于确认每个实体的身份，并为后续的身份验证和密钥生成打下基础。

注册请求（R）：每个参与平台的实体必须提交其注册信息给监管中心。注册信息包括实体的唯一标识符（ID）和必要的身份验证信息（Info）。这些信息将用于唯一识别平台中的实体。学校在注册时需要提供其名称、认证资质、法定代表人等；企业则需要提供营业执照号、法人信息等；学生则需提供学号、个人信息、课程成绩等。

身份验证（V）：监管中心根据提交的注册信息进行校验，验证其真实性。验证结果为布尔值，True 表示验证通过，False 表示验证失败。如果验证通过，系统将继续生成该实体的公私钥对。只有验证通过的实体才能进入下一步密钥生成流程。通过这一验证环节，平台确保所有注册的实体都是合法的、身份真实的，从而为后续的数据安全交换提供可靠的身份保障。

4.2 密钥生成与分发

在完成实体的身份验证后，监管中心将为每个合法实体生成公私钥对。

密钥生成（G）：身份验证通过后，监管中心为每个实体生成一对公私钥。公钥用于加密数据，私钥则用于解密加密数据。生成的公私钥对与实体的唯一标识符（ID）绑定，以确保每个实体都有唯一的公私钥。PubKey 是公钥，PrivKey 是私钥。在平台的实际应用中，公钥将分发给其他实体，以便加密消息或验证签名，私钥则由该实体自己保管，用于后续数据的解密和签名。

公钥分发（D）：在生成公私钥对后，监管中心将通过安全通道将公钥分发给注册实体。公钥的分发确保平台中所有参与方都能安全地使用加密技术进行通信，保护数据的安全性。PubKey 会被发送到注册实体，供其用于加密数据或验证签名。由于公钥是公开的，任何其他参与实体均可以通过公钥加密发送数据或验证数据的完整性，但无法直接获取或解密私密数据。

私钥存储（S）：与公钥的分发不同，私钥仅由实体自己保管，且需要严格的保护措施。监管中心将依据安全要求对私钥进行存储，确保私钥不会泄露或丢失。平台保证了私钥的安全存储，防止未授权访问或滥用，确保通信过程中的数据加密与解密的安全性。

4.3 信息加密与存储策略

为了确保平台内学生信息的隐私性与安全性，本平台采用了对称加密与非对称加密相结合的方式来保护敏感数据（如学生的个人信息、成绩单、学位证书等）。该加密方案能够保障数据在存储和传输过程中不被非法访问、篡改或泄露。图 3 是学生信息数据链上、链下存储流程图，确保了每个环节的安全性与高效性。

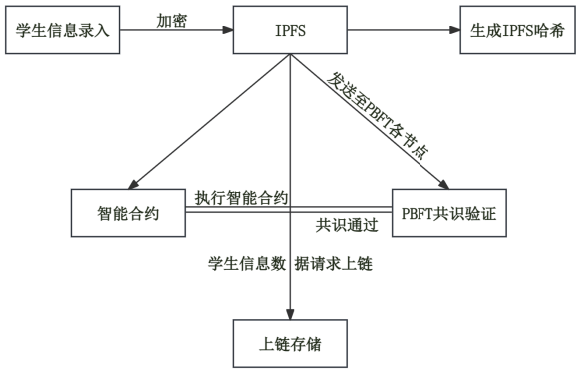

图 3 学生信息数据链上、链下存储流程图

4.3.1 对称加密与非对称加密结合

首先，平台会为每次会话生成一个临时的对称密钥 K_sym。该密钥用于在平台内对学生的敏感数据进行加密。生成对称密钥的过程采用随机数生成器，以确保每个会话的密钥唯一且不可预测。对称密钥加密技术具有较高的加密与解密效率，适合用于大规模数据的加密。

对称密钥 K_sym 由平台中的学校或数据拥有方生成，并仅在当前会话有效。当数据需要加密时，K_sym 被用来加密学生的敏感信息。由于密钥是临时生成并且会话结束后失效，因此其安全性得到了保障。生成的对称密钥 K_sym 将用于加密学生的敏感数据（如成绩单、学位证书、个人信息等）。该过程使用对称加密算法 AES（高级加密标准）进行加密。AES 是目前最广泛使用的对称加密算法之一，它能够在不牺牲安全性的情况下提供高效的加密性能。

加密过程：使用 K_sym 对学生的敏感数据 M 进行加密，生成加密数据 $E(M, K\_sym)$。数据的加密过程是对称的，即加密和解密使用相同的密钥，这使得加密和解密过程非常高效。其中，M 为学生的敏感数据，$E(M, K\_sym)$ 为加密后的数据。为了确保对称密钥 K_sym 的安全性，平台采用非对称加密技术对 K_sym 进行加密。具体来说，为确保密钥传输安全，采用接收方公钥加密方案。设数据使用者（如企业）的公钥为 PK_DU。这里使用的是椭圆曲线加密算法（ECC）中的 ECIES（椭圆曲线集成加密方案）。ECIES 是一种基于椭圆曲线密码学的非对称加密方案，能够有效保护密钥交换过程的安全性，并确保密钥在传输过程中不被窃取或篡改。程中的高度安全性，防止了敏感信息的泄露和未授权访问。

4.3.2 IPFS 存储与去中心化

加密后的学生信息需要进行安全地存储与管理。为了提高数据存储效率，并避免传统集中式存储带来的风险（如单点故障、数据泄露等），平台采用了去中心化存储方案，即使用星际文件系统（interplanetary file system, IPFS）来进行加密数据的存储。

（1）数据上传

加密后的数据包（E(M, K_sym）和其加密后的对称密钥 E(K_sym, S_school) 将被上传至 IPFS 网络。数据被分成若干块，每块数据被加密并上传到 IPFS 网络中。每个数据块都有一个唯一的内容标识符（CID），确保相同的数据始终具有相同的标识符。通过分布式存储，IPFS 不仅提升了数据的访问效率，也使得数据更加稳定和可靠。

（2）生成 CID

当数据上传到 IPFS 后，IPFS 会为每个数据生成唯一的内容标识符（CID）。CID 是通过对数据内容进行哈希运算得到的，因此相同的数据内容每次上传都会生成相同的 CID。这样，CID 成为每个文件的唯一标识符，确保数据在整个网络中的唯一性。CID 是不可篡改的，因此能够有效防止数据被伪造或篡改。

4.4 信息共享与零知识证明技术应用

信息共享策略的核心目标是确保学生的隐私得到有效保护，同时允许经过授权的第三方在必要时对学生信息进行验证和监管。为了平衡数据共享和隐私保护，零知识证明允许在不泄露具体数据内容的前提下，证明某个声明的真实性，因此成为信息共享中一个关键的隐私保护工具。图 4 是学生信息数据共享流程图。

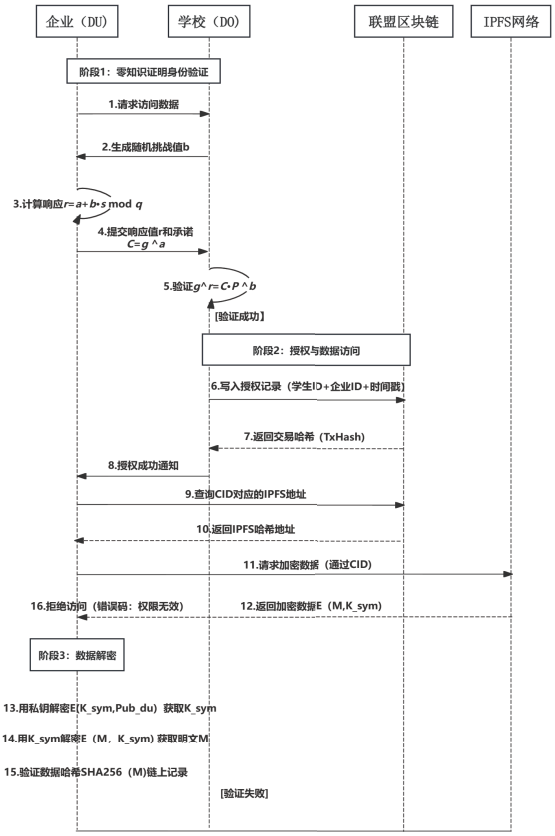

图 4 学生信息数据共享流程图

学生的学位信息由学校管理，而企业在无需获取具体数

据的情况下，可通过零知识证明协议验证其真实性。整个认证流程包括 4 个主要环节：首先，企业声明自己掌握某个秘密值，并生成相应的证明；接着，学校向企业发送随机挑战，以确保验证的随机性和安全性；随后，企业基于自身秘密值和挑战值计算响应数据，并返回给学校；最后，学校利用公开参数验证计算结果，以确认企业是否具有访问权限。若验证成功，企业即可获得学位认证结果，而无需直接接触学生的详细信息。

5 结论与展望

本研究构建了基于区块链技术的新型学生信息治理架构，凭借分布式账本不可逆的存证特性达成全流程的可信追溯。技术方案运用分层加密机制，在拜占庭容错共识算法的保障下，实现数据安全上链，极大提高了系统的容灾韧性以及操作的可审计性。面对海量教育数据的存储挑战，本研究创新性整合星际文件系统（IPFS）构建分布式存储网络，借助内容寻址技术确保教育档案的永久可溯。技术的关键突破在于引入零知识证明的可验证声明机制，此机制可让学生在求职核验等具体场景中自主披露特定信息项，在切实保障个人隐私权的基础上，达成资质验证的“最小化披露”原则，从而有效协调数据流通与安全监管的双重需求。后续研究将聚焦于研发跨链验证网关实现长三角高校联盟链数据互通。通过构建“标准 - 技术 - 场景”协同创新体系，探索学历互认机制，在保障数据主权前提下提升教育信息流通效率。后续研究将着重致力于研发跨链验证网关，以此达成长三角高校联盟链的数据互通目标。

参考文献：

[1] ZHU Y. New national initiatives of modernizing education in China[EB/OL].(2019-09-01)[2025-05-25].https://www.mendeley.com/catalogue/4f0b37a2-9ea9-328a-a17d-c901c695fe4d/.DOI:10.1177/2096531119868069.

[2] QIN C S, FAN B. Factors that influence information sharing, collaboration, and coordination across administrative agencies at a Chinese university[J]. Information systems and e-business management, 2016, 14(3): 637-664.

[3] AN M, FAN Q Y, YU H, et al. Blockchain technology research and application: a systematic literature review and future trends[EB/OL].(2023-06-26)[2025-06-13].https://arxiv.org/html/2306.14802v2.

[4] BIN SAIF M, MIGLIORINI S, SPOTO F. Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain[J]. Future internet, 2024, 16(3): 98.

[5] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].(2008-10-31)[2025-05-12].https://nakamotoinstitute.org/library/bitcoin/.

[6] LYER S S. Adopting a student centric education blockchain system[J].International journal of information and communication sciences, 2022, 7(3): 48-65.

[7] DING Y Y, XU J S. Blockchain-based student information management system[C/OL]//2023 4th International Conference on Information Science, Parallel and Distributed Systems (ISPDS) . Piscataway:IEEE,2023[2025-04-12]. https://ieeexplore.ieee.org/document/10235657.DOI:10.1109/ISPDS58840.2023.10235657.

[8] OMKAR G, VIKAS S, DATTATRAY S,et al. Student information management system[J]. International journal of engineering development and research, 2023, 4(4):4610-4613.

[9] 张达 . 基于区块链和星际文件系统技术的高校师德档案信息数据共享平台建构策略 [J]. 档案学研究 ,2024(2):126-133.

[10] JIANG P, FENG Y H, DAI Y H. Design of college student information sharing system based on blockchain[C]//2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). Piscataway:IEEE,2021: 568-572.

[11] YU J, XU F, LI Y F. Research and design of student archives management system based on consortium blockchain[J]. Journal of computational methods in science and engineering, 2023, 23(5): 2313-2322.

[12] ALI M I S, FAROUK H, SHARAF H. A blockchain-based models for student information systems[J]. Egyptian informatics journal, 2022, 23(2): 187-196.

[13] BOLFING A.Bitcoin [EB/OL].[2025-05-14].https://cn.investing.com/crypto/bitcoin/btc-usd&.

[14] BENET J. IPFS-content addressed, versioned, P2P file system[EB/OL]. (2014-07-14)[2024-04-15].https://doi.org/10.48550/arXiv.1407.3561.

[15] WU H X, WANG F. A survey of noninteractive zero knowledge proof system and its applications[EB/OL].(2014-05-04)[2025-03-13].https://doi.org/10.1155/2014/560484.

[16] ALAMMARY A, ALHAZMI S, ALMASRI M, et al. Blockchain-based applications in education: a systematic review[J]. Applied sciences, 2019, 9(12): 2400.

【作者简介】

赵鹏（1973—），男，山西太原人，博士研究生，教授，研究方向：软件工程、大数据、区块链。

张凯欣（2000—），女，山西大同人，硕士研究生，研究方向：区块链。

（收稿日期：2025-04-22 修回日期：2025-09-15）