# 区块链技术何以赋能微证书治理：基于信任的技术逻辑与实施进路

# How Can Blockchain Technology Empower Micro-Credential Governance: A Trust-Based Technical Logic and Implementation Path

赵婕雯 [1]
[1]Monash University Malaysia Campus
* ashleyyanchu@163.com

**【摘要】** 建立不同利益相关主体间的信任机制是微证书高质量发展的关键。区块链技术具有数据透明、不易篡改等优势，被认为是解决信任与安全问题的理想方案。通过信任重塑、存证范式与价值流转的技术逻辑架构，实现其从信息传递到传递价值的变革。基于 PBFT 重建信用、链上链下协调原则强化隐私性，以 UTXO 打破跨域互认壁垒，推进微证书的广泛认可。具体实践路径是通过治理架构、机制创新与技术支撑，构建三级嵌套的联盟链信任体系，选择存量先行与增量互认的学分置换路径，搭建链上链下映射的数据交互机制，探索终身教育数字化治理新范式。

**【关键词】**区块链技术；微证书治理；信任；技术逻辑；实践路径

***Abstract:*** *Establishing trust among different stakeholders is crucial for micro-credentials' high-quality development. Blockchain, with data transparency, immutability and traceability, is an ideal solution to trust and security issues. A technical framework of trust reconstruction, evidence preservation and value circulation enables transformation from information to value transfer. Specifically, it reconstructs PBFT-based credit, strengthens regulation and privacy via on-chain and off-chain coordination, breaks cross-domain recognition barriers with UTXO, and boosts micro-credential adoption. Practical paths include building a three-level nested consortium chain trust system via governance, mechanism innovation and technical support; adopting an "existing credentials first, incremental mutual recognition later" conversion approach; establishing an on-chain/off-chain mapping data interaction mechanism; and exploring a new paradigm for lifelong education digital governance.*

**Keywords:** blockchain technology, micro-credential governance, trust, technical logic, practical paths

## 1. 引言

在数智化加速发展背景下，个体学习模式已从传统的学历积累转向分散化、网络式技能获取（能力提升），微证书（Micro-credentials）作为终身学习成果的数字化认证工具，逐步成为连接正规教育与劳动力市场的关键介质（OECD, 2023）。但是随着微证书在技能认定领域应用规模的不断扩大，其基于中心化权威背书与单向授权的传统治理模式已难以适应数字化实践的动态需求。一方面，当中心化机构的有限验证能力无法支撑分布式学习场景时，信任链条呈现出高度脆弱性，一旦核心节点的数据公信力受损或发生单点故障，整个认证生态便会陷入停滞。另一方面，面对认证主体与数据规模的指数级增长，依赖单一机构声誉的信任机制在公信力维系方面呈现出滞后性，容易导致认证生态陷入高伪造风险与高验证成本并存的困境（Casino, Dasaklis & Patsakis, 2019）。区块链作为集成分布式网络、加密技术与智能合约等特性的新一代数字技术，可凭借数据透明、不易篡改、可追溯的内生优势（中华人民共和国工业和信息化部, 2021），将信任置于算法与共识机制的刚性约束之下，从而重构微证书

的信任生成与流通逻辑。因此，本研究拟从微证书所面临的实践困境，深入探究区块链技术何以赋能微证书治理，即通过技术信任重构教育认证的底层逻辑与治理架构，从而为构建开放互通、安全可信的终身教育数字化治理新范式提供理论与实践指导。

## 2. 数智化背景下的微证书实践困境

随着数智技术的迅猛发展，技术在为微证书提供服务的同时，也带来信任危机与挑战。

2.1. 机构信用背书的单向度依赖风险

微证书的信任机制对机构信用背书的单向度依赖，本质上源于基于声誉的信任构建所固有的信息不对称性。从信任关系的联结逻辑来看，发证主体的声誉与证书可信度呈现出强锚定效应，这一特性导致微证书信任体系呈现出单向依附特征（Rodrigues,et al., 2022）。一方面，现行微证书体系的信任逻辑建立在发证机构单方权威之上，其信任架构在提升初期认证效率的同时也埋下隐患。一旦发证主体因管理疏漏或利益驱动而违规发放虚假微证书，其声誉受损将引发链式反应，波及该机构先前颁发的所有微证书并致使其公信力归零。另一方面，中心化的信用传导机制对于中小机构或新兴教育平台构成较高准入门槛，使得产业创新力量因缺乏历史声誉积累而难以获得对等的社会认可，导致其被限制在信任体系的边缘，无法获取微证书市场的核心参与权与话语权，进而制约微证书生态体系的建构与健康发展。

2.2. 过程性数据缺失引发的监管盲区

在微证书的认证机制中，过程性数据采集与披露缺位导致认证流程中的监管环节出现结构性盲区，进而削弱认证结果的可信度。从核心缺陷来看，当前微证书的效力仅源于静态电子印章，缺乏可追溯、可审计的学习证据链条以及过程透明度的专项验证机制。这一监管盲区的形成，主要源于传统微证书平台的验证逻辑大多停留在结果导向的判定层面，即仅能反馈证书的真伪状态而无法还原认证背后的过程性证据（丁利敏, 2022）。尤为关键的是，由于缺乏对颁发时间、评审依据及审核流程等关键元数据的透明化展示，外部审计机构难以对认证质量进行实质性监督，导致内部人员利用数据权限批量伪造或篡改记录的操作难以被及时察觉（赵志群&刘丹, 2024）。此外，现有静态数据库架构难以有效支持证书状态的动态更新，使得已被撤销的失效证书在信息不对称的环境中仍具备可验证性，进而出现学历欺诈现象。

2.3. 跨域互认受阻导致的价值流通壁垒

微证书治理体系因缺乏统一的技术标准与数据规范，难以通过灵活组合实现微证书学习成果的社会化变现（张黎&周霖, 2023）。目前的互认实践局限于特定的利益联盟内部，若超出既定的合作链条，微证书的流通属性便会因技术接口不兼容或信任标准不一致而失效。不同教育机构与培训平台之间存在封闭性的数据围墙，导致学习者必须在多重系统中重复提交材料以完成身份验证与成果认定，违背终身学习所倡导的成果累积与灵活转换原则。从深层影响来看，数据主权的丧失使得学习者的能力图谱被迫分割在异构的平台体系之中，进而导致微证书作为终身学习通用货币的流通价值被稀释，这种人为制造的信息壁垒最终成为制约微证书认证机制向开放融合方向演进的主要障碍。

## 3. 区块链赋能微证书治理的技术逻辑

区块链本质上是一种由多方共同维护、通过密码学保障安全的分布式账本技术（Distributed Ledger Technology, DLT）（Nakamoto, 2008）。虽然该技术起源于数字货币的底层架构，但其去中心化、不可篡改及过程可追溯的特性，为解决微证书治理中的信任赤字提供了技术解。

在教育治理视角下，完全去中心化的公有链因效率低下且缺乏准入机制，难以与隐私与监管要求较高的学历认证体系相匹配。相比之下，兼具公开透明与适度隐私保护的联盟链

（Consortium Blockchain）构成了微证书治理的最优技术架构。联盟链通过许可制准入机制，构建一个半中心化的多主体协同网络（Zheng et al., 2017），其网络拓扑结构包含三类核心节点：由高校、政府及行业龙头组成的共识节点（Consensus Nodes），作为治理权力的核心持有者，负责其交易验证与区块生成；由用人单位或学习者接入的客户端节点（Client Nodes），负责发起微证书颁发请求与查询；以及具备审计权限的监管节点（Regulatory Nodes），可查看全量数据但不干预共识过程，确保治理过程符合国家教育主权与监管要求（Dib, 2018）。这种架构通过身份认证与 TLS/SSL 加密通信确立网络边界，既打破传统数据孤岛，又避免泛滥去中心化带来的治理失序，为微证书的生成、流转与互认构建较为坚实的底层逻辑。

3.1. 信任重塑：基于 PBFT 共识的多中心协同见证机制

在传统微证书体系中，证书的可信度系于发证机构的单边商业信誉，一旦中心化机构出现管理疏漏或利益驱动下的滥发行为，整个信用体系即面临崩塌风险。区块链技术介入的核心价值，在于通过共识算法将机构信任转化为基于数字信任。在联盟链架构下，微证书的颁发不再是单一主体的单向授权，而是一个由多方参与的分布式共识过程。而实用拜占庭容错算法（PBFT）能够在保留部分中心化管理效能的同时，提供高效的容错能力（Yao et al., 2021），可作为微证书治理的核心共识机制。具体而言，PBFT 算法的设计目标，是在存有恶意节点的环境下保证系统状态的一致性。只要网络中作恶或故障节点的数量不超过总节点数的三分之一，系统即可达成共识。这意味着任何虚假证书的生成都需要同时攻破网络中超过三分之一的权威节点，其造假成本呈指数级上升，一定程度上抑制了单点欺诈的可能性。

具体的共识执行流程呈现出严密的逻辑闭环（详见图 1）。当培训机构或院校完成学员考核并提交颁发微证书的请求时，该交易请求首先被广播至网络。其次，主节点将交易包含的元数据按序打包成候选区块，每一个区块收尾相连。上一个区块的最终状态是下一个区块的起始状态。当区块形成链条后。这部分区块将被打包成一页账本后，参与记账机制并启动 PBFT 三阶段协议，即预准备、准备与提交。随后，各共识节点对区块内容的合法性进行独立验证并相互广播签名。最终，当超过法定数量的节点达成一致后，该区块被正式追加至本地账本并同步至全网。这一过程将教育评价从中心权威定义转变为多中心协同见证，每一个微证书的生成都是联盟成员集体背书的结果。此外，PBFT 算法支持高并发与快速确认的特性，也有效解决了公有链处理效率低下的问题，使其能够承载大规模教育认证场景下的实时交易需求。

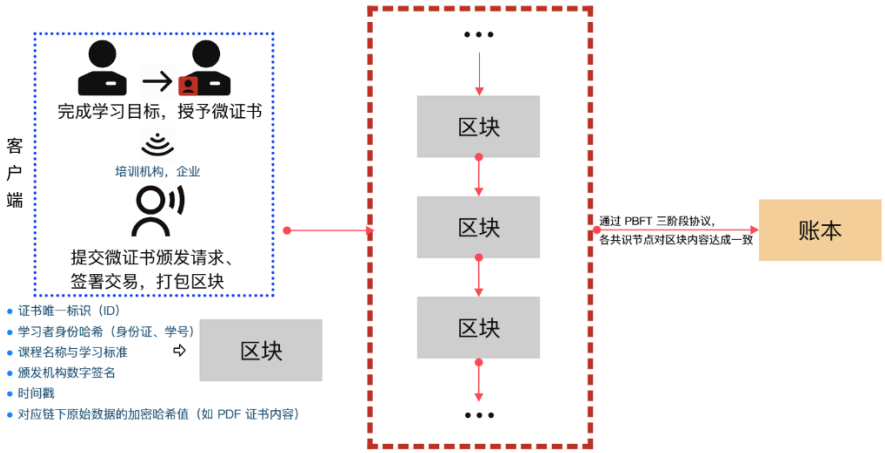


图 1 基于区块链的微证书存证示意图

3.2. 存证范式：链上链下协同的证据闭环与隐私保护

微证书的验证过程长期面临透明度与隐私权的二律背反，传统验证依赖中心化平台的黑箱操作，用户仅能获得真与假的结果，却无法知晓审核依据与过程，且由于数据归属于平台，

学习者缺乏对个人数据的掌控权。区块链技术通过结构化的上链存证，将验证过程转变为可审计的“白盒”模式。考虑到教育数据的敏感性，直接将原始数据上链会带来不可逆的隐私泄露风险。因此，技术架构应采用“链上索引+链下存储”的混合模式，即系统仅将如证书唯一标识 ID、学习者身份哈希、课程标准代码、颁发机构数字签名及时间戳等关键元数据写入区块，形成不可篡改的数字指纹。而包含详细个人信息的原始电子文档则存储于链下的加密数据库或分布式文件系统（IPFS）中，并通过加密索引与链上记录建立一一对应的映射关系。

双层存储架构在保障隐私的同时，也会提升验证的便捷性与可信度。当用人单位或第三方机构需要验证微证书时，无需依赖特定中心服务器的响应，任何获得授权的节点均可通过公开接口查询链上记录。验证者只需计算待验文件的实时哈希值，并与区块链上存证的哈希值进行比对。若两者一致，即可确保证书内容自颁发以来未被任何一方篡改。此外，针对更高层级的隐私需求，系统还可引入零知识证明（Zero-Knowledge Proof）技术，允许学习者在不透露具体分数或身份细节的前提下，向验证者证明其拥有某项资质，如“证明已满 18 岁”或“证明成绩合格”而不展示具体年龄或分数（邵文莎,于倩&韩磊, 2025）。基于证据链的验证逻辑，不仅实现了数据的防篡改与可追溯，更将数据所有权真正归还给学习者，使数据可用不可见成为微证书治理的新常态。

3.3. 价值流转：基于 UTXO 模型的学分银行互操作机制

微证书的重要价值在于其流通性，即实现不同教育机构间学习成果的等值互认与学分转换。我国现行的学分银行制度旨在搭建终身学习成果认证、积累与转换的制度性平台，但在技术落地层面，常受困于异构系统间的数据壁垒、复杂的换算规则以及缺乏统一的价值度量标准（苏显春, 2025）。引入区块链的未花费交易输出模型（Unspent Transaction Output，UTXO），能够为学分银行提供数字化记账范式（Nakamoto, 2008）。不同于传统银行账户基于余额的记账模式，UTXO 模型关注的是交易过程与资产溯源。在这一模型下，学分不再是数据库中的静态数字，而是作为由一系列输入与输出链接而成的历史流，每一笔学分的产生、转移与消耗都须引用此前未被使用的输出，确保同一笔学习成果不会被重复兑换，从而解决学分认定中的套利风险。

UTXO 模型能够可视化微证书的价值流转路径（详见图 2）。以典型的跨机构学分转换场景为例，假设学生 1 通过在发证机构 1 和发证机构 2 的学习，分别获得了 30 学分和 20 学分的 UTXO 输入，其总可用学分为 50 学分。当该学生申请进修学校 1 的课程置换时，需支付 25 学分。在区块链交易中，系统会将上述两笔 UTXO（30+20）作为交易输入，生成两笔新的输出：一笔 25 学分转入进修学校 1 的地址，另一笔 25 学分作为找零返还至学生 1 的地址。这一过程清晰地记录了每一分学分的来源（Source）与去向（Destination），使得教育评价的每一次流转都可被审计与追溯。若发现某证书对应的课程质量不达标，监管节点可发起作废交易的指令，标记并冻结相关联的学分流转。其技术逻辑是将抽象的教育评价转化为可量化、可追溯的数字资产，打破机构间的行政壁垒，构建起开放、流动的终身学习价值网络。

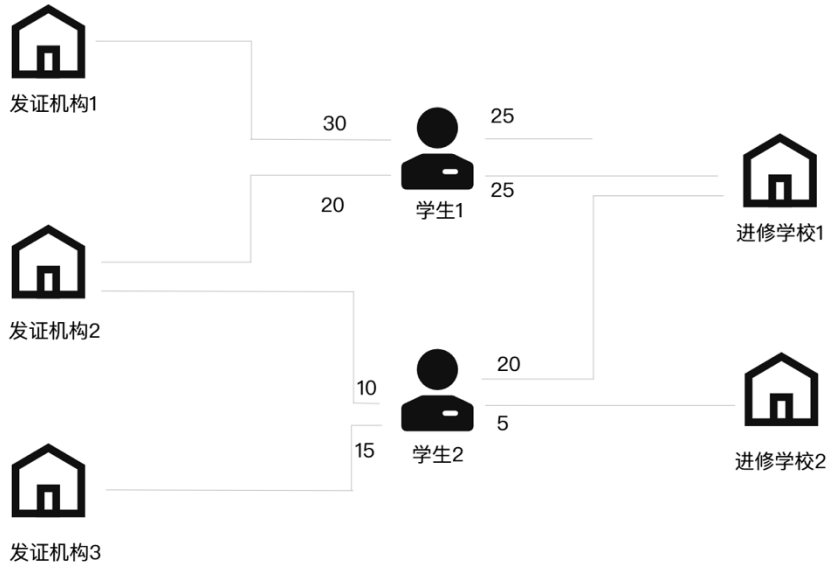


图 2 微证书跨主体流转示意图

## 4. 区块链赋能微证书治理的实践路径

基于数字化赋能的有机融入，微证书的治理须依托现有教育治理体系，构建层级清晰、权责明确、技术可行的联盟链架构，推动区块链微证书在全国范围内的大规模化应用。

### 4.1. 治理架构：构建三级嵌套的联盟链信任体系

基于我国教育行政管理的科层制特征，应构建以国家开放大学作为教育部直属的终身教育核心平台，牵头建立覆盖中央—省级—机构三级的微证书联盟链(Chen,et al., 2024)。该架构根据信任评级与职能分工，将网络节点划分为监管节点、共识节点与背书节点三个层级。

在监管节点上，可设置主管部门，其核心职责在于制定全网互认规则、审计全网数据合规性以及处理链上争议。更为关键的是，监管节点掌握准入许可权，即对新加入的节点进行资质审查与授权，确保联盟链的参与主体始终在国家政策法规的框架内运行。在共识节点上，国家开放大学作为教育部直属的终身教育核心平台，具备天然的枢纽地位与政策执行能力，该层级节点拥有读、写、记的权限。它们负责运行 PBFT 等共识算法，验证微证书交易的合法性，并维护分布式账本的一致性。通过政策授权与技术能力的双重加持，确保认证数据的不可篡改与永久保存。在背书节点上，作为微证书的主要供给方，须考虑到该层级主体多元利益诉求，系统需对其权限进行严格限制，仅授予读、写功能。背书节点负责发起微证书的颁发请求并查询链上信息，但不参与核心账本的共识记账。其发布的微证书有效性，需经由共识节点的验证与监管节点的审计，从而形成发起、验证、监督的信用保障机制。

### 4.2. 机制创新：存量先行与增量互认的学分置换路径

针对当前学分银行互认标准尚未统一的现状，微证书体系的推广应采取存量先行与增量互认并行的渐进策略。一方面，在体系建设初期，重点在于利用区块链技术长效、不可篡改的特性，解决学习成果的记录与确权问题。基于微证书上链具有数字存证功能，系统优先将学习者的碎片化学习经历、技能认证等数据写入区块链，形成可追溯的证据链条。在建立学习成果储蓄所的基础上，确保数据的真实性与安全性，为未来的价值评估积累原始资本。另一方面，随着国家资历框架与学分银行网点的完善，体系逐步由存向兑过渡。基于链上积累的可信数据，依据统一制定的学分转换规则，智能合约将自动执行学时与学分的换算，将学时

转换成可视化的分数。微证书不仅作为静态的记录，也成为可流通的通行凭证，在不同院校、企业与区域间实现流转与价值变现，最终建成服务全民终身学习的交易网络。

4.3. 技术支撑：搭建链上与链下映射的数据交互机制

在教育场景中，构建链上存证与链下存储的双层映射机制，以平衡隐私保护、系统性能与数据可信度。

首先，实行链下数据的物理隔离存储，确立数据管理主权。考虑到区块链的存储成本与吞吐量限制，将大体积的非结构化数据（如证书 PDF 源文件、实训视频）以及高敏感度的隐私信息（如身份证号等个人信息），均存于链下的中心化数据库中。值得注意的是，敏感个人信息明文不可上链，仅保留教育机构对原始数据的控制权。这不仅降低链上负载，也确保教育机构对原始数据的管理主权，便于在发生错账或需要撤销时进行合法操作。其次，利用哈希锚定实现链上存证，保障数据不可篡改。哈希算法将哈希值作为密码层面的唯一数字指纹，具有单向不可逆的特性。链上仅写入经脱敏处理的关键元数据（如颁发机构 ID、证书类型）以及原始数据的哈希值（Hash）。任何针对链下原始文件的微小篡改，都会导致重新计算出的哈希值发生剧烈变化，从而无法与链上记录匹配，有利于解决证书真伪辨识与责任追溯问题。最后，针对身份隐私问题，引入分布式数字身份（DID）技术或基于学信网学籍号的加密标识，记录其唯一的加密身份标识（ID Hash）。在验证环节，验证者提交原始文件与授权身份，系统通过重算哈希值并与链上指纹比对，若一致即证明文件或数据未篡改。这种机制既解决了隐私保护与公开验证之间的矛盾，又为微证书的社会化流通奠定基础。

## 参考文献

丁利敏. (2022).终身学习视野下欧盟微证书运动:主要举措、发展特征及相关启示.成人教育,42(05),86-93.

邵文莎,于倩&韩磊. (2025).融合区块链技术的非正规与非正式学习成果微认证体系构建与实施路径.中国成人教育,(05),62-70.

苏显春. (2025).数字化背景下学分银行转型之路:理论、实践与突破.中国成人教育,(22),74-80.

张黎&周霖. (2023).赋能数字化时代终身学习:澳大利亚教育微证书探析.外国教育研究,50(06),80-96.

赵志群&刘丹. (2024).欧盟高等教育微证书项目：现实动因、运行体系与保障机制.大学教育科学,(06),79-89.

中华人民共和国工业和信息化部.关于加快推动区块链技术应用和产业发展的指导意见[Z/OL]. 2021-05-27[2026-01-22].https://www.miit.gov.cn/jgsj/xxjsfzs/wjfb/art/2021/art_aac4af17ec1f4d9fadd5051015e3f42d.html.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics, 36, 55-81.

Chen, X., He, S., Sun, L., Zheng, Y., & Wu, C. Q. (2024). A survey of consortium blockchain and its applications. Cryptography, 8(2), 12.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. Int. J. Adv. Telecommun, 11(1), 51-64.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

OECD. (2023). Micro-credentials for lifelong learning and employability: Uses and possibilities. OECD Publishing.

Rodrigues, B., Franco, M., Killer, C., Scheid, E.J., Stiller, B.(2022). On Trust, Blockchain, and Reputation Systems. In: Tran, D.A., Thai, M.T., Krishnamachari, B. (eds) Handbook on Blockchain. Springer Optimization and Its Applications, vol 194. Springer, Cham.

Yao, W., Ye, J., Murimi, R., & Wang, G. (2021). A survey on consortium blockchain consensus mechanisms. arXiv preprint arXiv:2102.12058.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.