区块链赋能网络教育数据安全访问管控策略
——评《区块链原理及其安全技术应用研究》

教育数字化转型提速,但数据泄露、非法篡改频发,传统中心化系统权限管控混乱,易遭单点攻击,信任基石动摇。为了确保证书真实、资源版权清晰、隐私不被滥用,可利用区块链的去中心化与不可篡改特性,构建“可用不可见”的访问控制。

《区块链原理及其安全技术应用研究》一书针对区块链技术的具体应用,既系统剖析分布式账本、共识机制等核心原理,又针对网络攻击、合约漏洞等现实安全问题,给出了具体的技术防御思路。书中亦探讨了隐私保护与合规平衡术问题,并对跨链、扩容等趋势进行预判,颇具借鉴应用价值。

书名:区块链原理及其安全技术应用研究
作者:党莹,党维,张江霄
出版社:中国原子能出版社
ISBN:9787522131061
出版时间:2023 年 11 月
定价:76 元

基于网络教育数据的安全防护目标,可基于智能合约与属性基加密方式构建去中心化自治管控体系,斩断单点故障根源。传统网络教育系统习惯于将所有数据集中放在一台服务器或一系列相关的服务器群组中,一旦服务器被破解,其中保存的学校及师生的各种敏感信息都面临暴露风险。基于此,学校等教育机构应利用区块链的分布式记账特点,利用智能合约和属性基加密方式,将信息保存在不同的网络节点。具体而言,先建立一套“代码即规则”的访问控制体系,一切学校和师生的信息,如成绩、课题、个人信息等,都交给预设的智能合约体系审核并录入,后续的查询访问和修改等工作,亦由智能合约根据设定条件进行授权。以修改成绩信息为例,根据智能合约设定条件,只有同时满足“任课教师身份 + 特定时间段 + 教学管理系统触发”这三个条件时,才能解锁修改权限,且每一次的修改行为都会基于区块链技术流行无法篡改的时间戳和哈希值,形成全链路的“数字足迹”,方便后续行为溯源追责,这一设计让任何违规操作都无所遁形。除此之外,针对不同层次的数据安全需求,可引入属性基加密机制。与“全有或全无”的传统安全访问模式相比,属性基加密方式允许定义极其复杂的访问策略,如学校可设定“仅限计算机学院大三学生、在校园网 IP 段内且 GPA 大于 3.0”的条件才能解密某份科研数据集,如此既防止了外部攻击,亦有效遏制了内部人员的越权访问。

为了提升网络教育数据的安全防护水平,可部署自我主权身份与零知识证明的隐私计算防线,实现数据在“可用不可见”的情况下实现价值提取。在教育大数据应用中,最大的矛盾在于既要共享数据以挖掘价值,又要保护师生的绝对隐私。如果简单划一对数据进行脱敏,往往会牺牲数据的可用性,导致数据挖掘价值下降;如果直接共享各种敏感数据,则无异于裸奔。面对此种情况,则可利用自我主权身份与零知识证明的结合破解这一问题。学校等教育机构要推动教育身份认证从“平台赋权”向“用户主权”转变,在自我主权身份模型下,师生的数字身份不再由某个教育平台独占,而是存储在用户自己的加密钱包中。学历证书、技能徽章、选课记录等凭证以可验证凭证的形式存在,用户在需要证明身份时,只需出示由学校私钥签名的“证明”,而无需暴露底层的原始数据。这一做法既彻底消除了因平台倒闭或被黑导致的身份丢失风险,更让跨校、跨区域的学分互认成为可能,因为验证方只需校验链上的签发记录,无需连接学校的中心数据库。更为关键的是,利用零知识证明技术,工作人员可以在不泄露具体信息的前提下完成验证。在区块链 + ZKP 的架构下,学生只需生成一个密码学证明,系统验证该证明为真即可通过,而无需知道学生的具体个人信息。

总之,网络教育数据安全的未来,不在于修修补补的防火墙,而在于底层逻辑的彻底革新。基于区块链技术去中心化的智能合约管控架构,筑牢了防御的“盾”;通过隐私计算与主权身份体系,锻造了共享的“矛”。双策并用,建立起一个既开放又安全、既高效又可信的网络教育信息生态系统。

(赖昌美副教授,夏奔副教授/赣州职业技术学院)