基于区块链的电子证照共享与隐私保护方案

湛高峰，王晓峰，程　楠
（公安部第一研究所 信息安全部，北京 100048）

摘　要： 针对传统电子证照管理库设计依赖中心存储，边缘节点管理复杂且易遭受攻击导致隐私数据泄漏的问题，提出了一种基于区块链与可搜索加密技术的电子证照管理方案，实现了电子证照管理流程的去中心化及电子证照敏感信息的隐私保护。方案依靠智能合约解决电子证照数据链上链下存储与用证交易问题，基于属性的加密保证证照信息检索过程的数据安全。在分布式开发环境下实现了方案的部分模块并进行了试验，试验结果表明，方案具有去中心化、分布式可信存储、不可篡改等特性，能够满足电子证照管理的主体需求，具有一定的应用价值。

关键词： 区块链；电子证照；可搜索加密；智能合约；隐私保护
中图分类号： TP309　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2097-1788.2023.01.013
引用格式： 湛高峰，王晓峰，程楠. 基于区块链的电子证照共享与隐私保护方案[J].网络安全与数据治理，2023，42(1)：92-97.

Blockchain-based electronic license sharing and privacy-preserving scheme

Zhan Gaofeng，Wang Xiaofeng，Cheng Nan
(Department of Information Securiy，The Mininstry of Public Security's First Research Institue，Beijing 224000，China)

Abstract： The design of traditional electronic license management always relies on central storage，the management of edge nodes is complex and the central node is vulnerable to attacks，leading to privacy data leakage. To solve this problem，an electronic license management scheme based on blockchain and searchable encryption is proposed. The scheme realized the decentralization of electronic license management process and the privacy-preserving of sensitive information. The scheme relies on smart contracts to solve the problems of online and offline storage and license use transactions of electronic license data link，and uses attribute-based encryption technology to ensure the data security in query process. Some of the schme are implemented and tested in the distributed envrionment. The results show that the scheme has the characteristics of decentralization，distributed trusted storage，and non tampering，which can meet the main needs of electronic license management and has certain application value.

Key words： blockchain；electronic license；searchable encryption；smart contrast；privacy-preserving

0 引言

电子证照是数字化时代社会信用体系建立的重要一环[1]，电子证照管理系统是实现安全高效的证照创建、存储与使用共享的有效方案。传统的电子证照管理系统通常依赖核心部门的中心服务器，这种管理模式只占用少量资源，但在数据共享方面限制较大，且易遭受非法攻击导致中心、边缘节点数据泄漏。因此，如何实现电子证照管理的去中心化，实现证照数据共享过程的隐私保护，是构建电子证照管理方案的主要问题。

针对上述问题，学者们面向不同应用场景，提出了一些基于区块链技术的电子证照管理系统。2017 年闵旭蓉等[2]针对政务信息透明需求，提出一种基于区块链技术的电子证照管理平台，通过区块链的共同记账技术原理实现数据共享，实现了各部门政务信息的互联互通。2018 年，巢燕[3]同样针对“互联网+政务”场景提出一种基于区块链技术的电子证照管理系统，使用 Hyperledger Fabric 设计证照管理区块链，实现了各部门间数据共享、海量数据存储。2020 年，王浩亮等[4]针对传统智慧诚实系统

建设下的数据孤岛问题提出了一种基于区块链的去中心化电子证照共享交易系统,将电子证照上链存储,借助智能合约实现了电子证照的链上交易。2021 年,蔺悦霞等[5]针对水利能源场景,提出一种取水许可电子证照系统,系统采用标准中心化架构,实现电子证照的集中式管理。

上述研究方案中,区块链通常作为一个不可篡改的分布式账本来存储电子证照数据,由于区块链的可追溯特性,可以保证电子证照数据共享过程的透明。这些方案相较于传统的电子证照管理系统在安全性上有明显提升,但仍忽略了一些实际通信场景的安全问题。由于区块链交易使转账人和收款人绑定,敌手可以通过分析区块内容获得有效信息,且智能合约输入输出公开[6],可能造成隐私数据泄漏。为此,一些学者开始关注分布式存储系统下的访问控制与隐私保护问题。2018 年,Wang 等[7]提出了一个基于区块链的,结合 IPFS、以太坊和属性基加密技术的分布式存储框架,实现分布式存储中的数据共享;2021 年,Li 等[8]提出一种基于区块链并带有隐私保护的电子证照管理系统,采用属性基加密方式对电子证照数据进行加密,实现安全的电子证照数据共享。

受 Wang 等[7]工作的启发,为了确保电子证照数据的有效存储与安全管理,本文基于区块链智能合约与属性基加密(Attribute-Based Encryption,ABE)技术,设计并实现了一种安全有效的电子证照管理系统。智能合约的设计思想来自以太坊[9],实现电子证照信息的发布、共享与浏览功能,并且使用基于属性的加密来确保细粒度的电子证照数据的访问控制。

1 知识背景

1.1 区块链技术

区块链最早由 NAKAMOTO[10]提出,作为比特币底层基础的点对点分布式网络技术,比特币区块链是第一个出现的公共区块链网络。比特币区块链是一个分布式、不断增长、共享的区块分类账[11]。2014 年,以太坊(Ethereum)[9]作为一个新的公共区块链被提出,以太坊基于新的智能合约实现分布式计算,以去中心化的特性解决了比特币区块链扩展性不足问题,广泛应用于金融、科学、政务、医疗、教育等领域。

在物联网领域,区块链技术的引入可以使分布式系统突破对中心服务器的依赖,使用区块链的共识机制解决信任问题[12]。现有电子证照的管理同样属于分布式存储问题,结合区块链技术可以实现系统的去中心化,进一步提高系统安全性。

1.2 智能合约

智能合约(Smart Contract)最早由 Szabo[13]提出,是一种以信息化方式传播、验证或执行合同的计算机协议,允许在没有第三方的情况下进行可信的交易并且交易具有可追踪性和不可否认性。智能合约并不绑定区块链技术,其最初的定义是关于法律的自动化合同。近年来,智能合约在区块链和其他分布式账本技术中获得了更新的含义:是防篡改的计算更新分类账状态的程序[14]。智能合约针对不同性质的自动化任务来执行任意逻辑。

智能合约是一段代码和数据的集合,可以部署在以太坊网络上,通过以太坊虚拟机(Ethereum Virtual Machine,EVM)解释成字节码进行执行。EVM 内运行的每一步操作实际上同时在被所有节点所执行,保证了智能合约在同一时刻状态的一致性。同时智能合约有自己的账户,在时间或事件的驱动下能自动执行一些功能,如可以在相互之间传递信息,修改区块链的状态(比如账户信息)等。

1.3 双线性映射

设 G 和 G_T 是素数 p 的两个乘法循环群,g 代表 G 的生成元,双线性映射[15]$\hat{e}:G\times G\rightarrow G_T$ 满足以下条件:

双线性:对任意 $a,b\in Z_p$,有 $\hat{e}(g^a,g^b)=(g,g)^{ab}$;

非退化性:$\hat{e}(g,g)\neq 1$;

可计算性:对 $g_1,g_2\in G$,计算 $\hat{e}(g_1,g_2)$ 是可行的。

2 系统架构

本系统在以太坊的基础上设计开发。以太坊是一个通用区块链平台,与标准的比特币区块链相比,以太坊的交易场景更加简单,且以太坊的智能合同可以解决数据完整性问题,实现客户端-服务器架构,适合跨层级、跨领域的分布式电子证照管理系统的开发。

2.1 系统模型

系统架构如图 1 所示,主要包括六个部分:证照发布方、证照使用方、证照持有方、智能合约、区块链、可信机构组织。

证照发布方:负责为证照持有者发布电子证照,

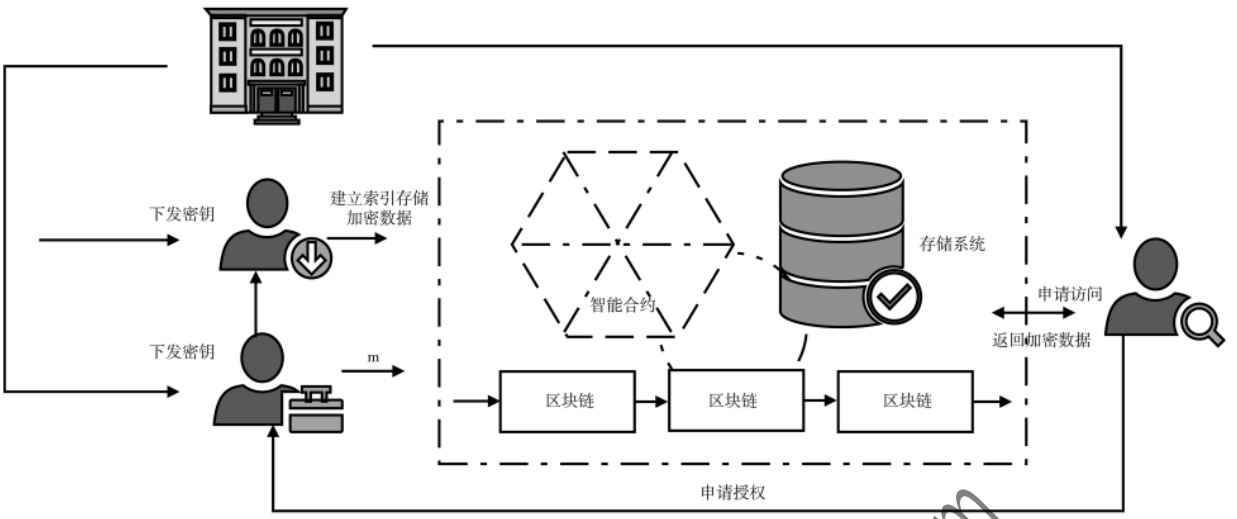

图 1 系统模型

可以上传数据密文至存储系统,并将密文索引发布至区块链。

证照持有方:电子证照数据的持有者,证照持有方执行访问控制策略,根据自身电子证照信息生成签名信息可使用密钥加解密电子证照数据,可以为证照使用方的访问请求进行授权。

证照使用方:需要使用电子证照数据的第三方,使用方在获取持有方授权后,可以使用持有方提供的搜索令牌与关键词进行检索,并通过可信机构提供的属性密钥进行数据解密。证照使用方获取电子证照数据时,首先向证照持有方申请授权,获得持有方属性令牌。然后向区块链系统发送访问电子证照的请求,以获取对应的电子证照数据索引,最后使用索引获得电子证照数据密文。

可信机构:负责系统的管理,初始化阶段可信机构为整个系统选择公共参数,系统的参与者需要在可信机构进行注册,在验证注册用户的身份后,可信机构会为系统的参与者生成属性密钥。

存储系统:负责存储电子证照数据密文与电子证照数据相关的信息及其签名。

区块链:负责存储电子证照数据密文索引。

智能合约:其核心为电子证照的操作过程,区块记录内容为加密的电子证照。智能合约需完成电子证照发布、取用接口,发布电子证照的过程需有可信机构组织、证照发布方、证照持有方签名,发布成功的电子证照密文索引在区块上。

电子证照的共享实质为证照持有方将电子证照的副本交易给目标用户的过程,该过程由证照发布方、证照使用方、证照持有方、可信机构通过以太坊智能合约实现。副本的有效性可由电子证照 hash 值与原始区块中记录的电子证照 hash 值对比,以校验真实性,并将共享过程记录在区块链中。

完整的电子证照信息上传与访问经过如下步骤:

(1)数据用户认证注册。

(2)可信机构为电子证照持有方与证照发布方生成属性密钥。

(3)数据用户基于文档集合的索引,然后生成密文索引并将其外包给区块链。

(4)证照使用方获得持有方授权,使用持有方身份与关键字构造一个加密的令牌,通过安全信道将其发送给证照使用方。

(5)使用方向区块链发送带有加密令牌的访问请求,区块链上的“会计节点”接收到令牌后,调用智能合约接口执行搜索,获得匹配的键值对与区块链交易 ID,使用返回的区块链交易 ID 获得密文索引,将密文索引发送给使用方。

(6)使用方发送带有密文索引的访问请求,存储系统验证数据访问者的属性是否满足访问控制策略,若满足则发送密文给使用方。

2.2 区块链网络架构

区块链网络架构如图 2 所示。区块链一些节点保有一份完整的、最新的区块链拷贝,这样的节点被称为“全节点”。另外还有一些节点只保留了区块链的一部分,这样的节点被称为“轻量级节点”。每个节点都参与全网的路由功能,同时也可能包含其他功能。每个节点都参与验证并传播交易及区块信

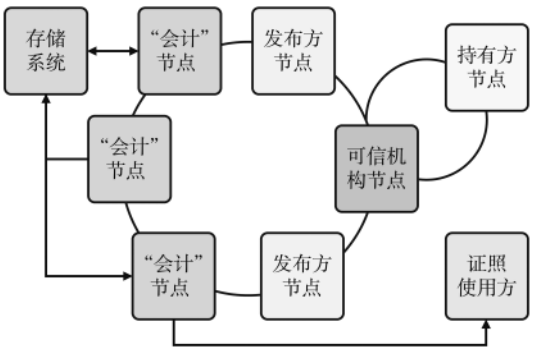

图 2 区块链网络架构

息，发现并维持与对等节点的连接。根据所提供的功能不同，各节点可能具有不同的分工，一些节点可调用智能合约搜索接口，执行索引搜索功能，称为会计节点。各工作节点组成 P2P 网络架构，以扁平 flat 拓扑结构相互连通。

3 系统流程

3.1 系统初始化

可信机构选择阶数为素数 p 的乘法循环群 $\boldsymbol{G}$ 和 $\boldsymbol{G}_T$，一个 $\boldsymbol{G}$ 的生成元 g，以及一个双线性映射 $\hat{e}:\boldsymbol{G}\times\boldsymbol{G}\rightarrow\boldsymbol{G}_T$，定义哈希函数 $H_1:\{0,1\}^*\rightarrow\boldsymbol{Z}_p$，$H_2:\{0,1\}^*\rightarrow\boldsymbol{G}$，并定义加解密函数 SE=(SE.Enc，SE.Dec)。之后，随机选择 $(\alpha,\beta)\in\boldsymbol{Z}_p$，计算 $g_1=g^{\alpha}$，$h=g^{\beta}$，$Y=\hat{e}(g,g)^{\alpha}$。最终，可信机构发布公共系统参数 $PP=(\boldsymbol{G},\boldsymbol{G}_T,e,p,g,H_1,H_2)$，生成公钥 PK 与私有的系统主密钥 MK。

3.2 用户注册

证照发布方的准入由区块链网络中的可信机构进行认证与管理。数据用户的注册与认证管理也可委托给证照发布方。数据用户包括证照持有方和证照使用方，每个成功注册的数据用户都获得系统分配的全局标识 GID，用于建立用户密钥并标识用户真实身份。

3.3 属性赋值

可信机构在区块链上部署了一个用户管理合约。合约输入 GID 以确定用户的身份。如果用户 GID 为证照使用方，则根据其访问的部门资质信息为其分配相应的属性。如果用户 GID 是经过身份验证的使用方，则会将其电子证照的属性分配给他。

3.4 密钥生成

可信机构基于用户 GID 的属性集 A 为每个用户生成私钥 SK_u。随机选择 $x\leftarrow\boldsymbol{Z}_p$，计算 $K_1=g^{(\alpha+x)/\beta}$，$K_2=g^{1/\beta}$，$K_3=g^{x}$。对每一个属性 $a\in A$，随机选择 $S_a\in\boldsymbol{Z}_p$ 并计算 $K_a=H_2(a)^{S_a}K_3$，$K_a^{'}=g^{S_a}$。之后可信机构通过安全信道将 $SK_u=(a,K_1,K_2,K_a,K_a^{'})$ 发送给标识为 GID 的用户。

3.5 数据加密和上传

证照发布方为用户生成电子证照数据，通过可信机构部署的合约将数据密文的 hash 值、时间戳、交易发起者、发布方签名等信息上传到区块链，并得到返回的交易 Id。证照持有方可以浏览电子证照数据，区块链记录所有数据共享交易信息。

具体加密流程如下：证照持有方随机选择对称密钥 k，加密电子证照数据 EL 得 SE.Enc(EL)，上传 SE.Enc(EL)至存储系统，并获得相应的索引地址 URL(SE.Enc(EL))。之后根据电子证照数据密文生成关键字索引与电子证照密文数据索引，将索引提交给证照发布方，并生成加密的关键字索引与密文索引。

3.6 数据检索

证照使用方想要检索电子证照数据时，首先获取证照持有方的授权。可根据持有方关键字以及自身私钥 SK 生成一个搜索陷门。

证照使用方首先输入自己的私钥 SK 与想要搜索的关键字 k，并计算 $T=K_2^{H(k)}$，$T_u(k)=T*K_1$，证照使用方通过关键字 k 生成搜索陷门 $T_k=(T_u(k),a,t_a=K_a,t_a^{'}=K_a^{'})$。调用在区块链上部署的智能合约，合约输入用户 GID 和陷门 T_q，并调用搜索算法进行搜索。

搜索算法根据访问结构 T 关联的属性返回数据密文索引 CI。当且仅当用户 GID 的属性集 A 满足访问结构 T，且查询关键字 k 等于索引关键字 w，才能返回密文索引 CI，所有相关的操作信息均会自动添加到区块链中。之后证照使用方提交密文索引，可根据密文索引获得存储系统对应的电子证照数据密文 SE.Enc(EL)，使用对称密钥 k 解密。

4 系统分析

4.1 效率评估

本文区块链系统基于以太坊搭建，数据用户和服务对等点的实验环境所使用的操作系统为 64 位 Windows 系统，处理器为英特尔酷睿 i5 3.5 GHz。利用JPBC 2.0.0 库进行智能合约的部署。对方案进行

了部分实现并对系统进行了测试,测试中统计了电子证照数据加密阶段和解密阶段的运行时间与索引生成时间。之后与文献[7]、文献[8]中的分布式存储共享方案进行了分析对比。

图 3 模拟可信机构节点生成系统的主密钥与为用户生成私钥的过程,通过随机采样生成 32 B 属性密钥。AES 对称密钥生成约耗时 0.6 ms,非对称密钥对生成耗时约为 0.5 ms。

图 4 演示了数据加密与索引生成,加密并生成数据索引耗时约为 8 ms。

假设 n 表示属性的数量,双线性映射操作时间为 P,E 表示循环群中的指数运算,分析本方案与文献[7]、文献[8]的理论计算开销,结果如表 1 所示。

最后,比较了本文方案与文献[7]、文献[8]建立索引时的性能,如图 5 所示。

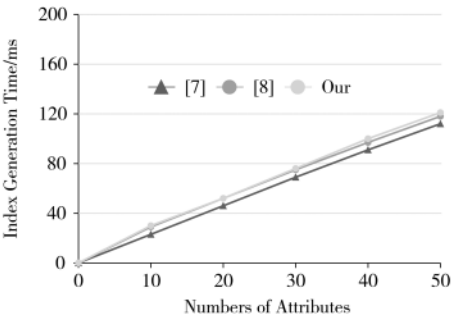

图 5 索引建立时间开销

4.2 安全性分析

对本系统在防篡改、隐私保护、可验证性、安全密钥管理等方面进行非形式化的安全性分析。与相关方案对比如表 2 所示。

表 2 计算开销对比

	防篡改	隐私保护	可验证性	密钥管理安全
文献[7]	√	×	×	×
文献[8]	√	√	×	√
本文方案	√	√	√	√

防篡改:电子证照数据经过对称加密并存储在独立于区块链的存储系统中,相应的索引和对称密钥被加密并存储在区块链中,因此电子证照数据和索引难以被篡改。

隐私保护:系统中的每一个用户均使用一个随机生成的 GID 匿名地参与区块链交易,且区块链索引和链外存储模式提供了隐私保护。

可验证性:所有与电子证照数据共享和搜索相关的操作都记录在防篡改的区块链上,可以提供有效的验证和匿名的跟踪。

安全密钥管理:每个随机生成的对称密钥对电子证照数据进行加密,相应的索引同样进行加密,并存储在区块链中。可信机构通过区块链在各节点建立信任,确保密钥管理的安全性。

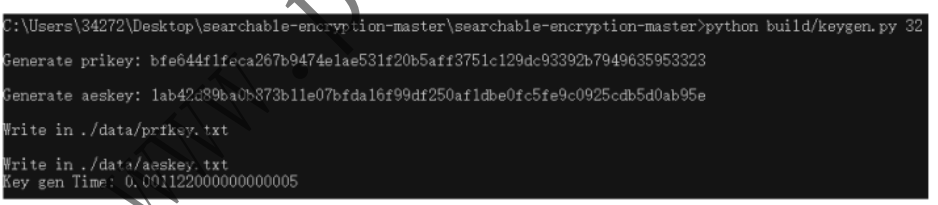

图 3 密钥生成

图 4 索引生成

表 1 计算开销对比

	Setup	KeyGen	Encrypt	Trapdoor	Search	Decrypt
文献[7]	$nE+nP$	$2nE$	$(1+2n)E$	$4E$	–	$2P$
文献[8]	$3E$	$(2n+2)E$	$(2n+1)E+P$	–	$O(1)$	$2P$
本文方案	$2E+P$	$(2n+2)E$	$(1+2n)E+P$	E	$(1+2n)P$	$2P$

综上，本方案可以完成电子证照数据的密文存储与索引上链工作，数据用户可以有效地检索电子证照密文数据。与现有一些方案相比本方案具有更好的安全性，只引入少量的计算开销，能够满足电子证照管理的主体需求。

5 结论

本文针对电子证照管理中的去中心化共享与隐私保护问题，使用区块链与可搜索加密技术设计并实现了一个安全的电子证照管理系统。利用区块链技术对现存运行方案不足之处进行优化，能有效简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。实验表明，本文的电子证照管理系统有去中心化、分布式可信存储、不可篡改等特性，该系统有助于电子证照跨地区管理，有利于构建良性的社会信用生态。

参考文献

[1] 麦庆达，黄小敏.区块链+分布式商业打破“数据孤岛”的工程性研究[J].中国经贸导刊(中)，2020(6)：140－143.

[2] 闵旭蓉，杜葵，戴逸聪.基于区块链技术的电子证照共享平台设计[J].指挥信息系统与技术，2017，8(2)：47－51.

[3] 巢燕.基于区块链的电子证照管理系统的设计与实现[D].南京：南京大学，2018.

[4] 王浩亮，廉玉忠，王丽莉.面向电子证照共享的区块链技术方案研究与实现[J].计算机工程，2020，46(8)：277－283.

[5] 蔺悦霞，艾尼瓦尔·达吾提，郑策，等.新疆水利电子证照共享服务平台系统设计与实现[J].水利信息化，2021(4)：80－84.

[6] PRASTUDY F，SARAH M，REBEKAH M，et al.Quisquis：a new design for anonymous cryptocurrencies[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communication Sercurity，New York：ACM Press，2019：649－678.

[7] WANG S，ZHANG Y，ZHANG Y.A blockchain－based framework for data sharing with fine－grained access control in decentralized storage systems[J].IEEE Access，2018，6：38437－38450.

[8] LI X，TAN M.Electronic certificate sharing scheme with searchable attribute－based encryption on blockchain[J].Journal of Physics Conference Series，2021，1757(1)：1－8.

[9] BUTERIN V.A next－generation smart contract and decentralized application platform[EB/OL].(2014－xx－xx)[2022－09－15].https://ethereum.org/en/white－paper/.

[10] NAKAMOTO S.Bitcoin：a peer－to－peer electronic cash system[EB/OL].(2008－11－01)[2022－02－17].https://bitcoin.org/bitcoin.pdf.

[11] ELEAVEN T R，BROWN R G，YANG D.Blockchain technology－infinance[J].Computer，2017，50(9)：14－17.

[12] KHAN M，SALAH K.IoT security：review，blockchain solutions，and open challenges[J].Future Generations Computer Systems FGCS，2018，82：395－411.

[13] NICK S.Formalizing and securing relationships on public networks[J].First Monday，1997，2(9)：1－21.

[14] VITTORIO C，GUIDO P.Standardizing smart contracts[J].IEEE Access，2022，10：91203－91212.

[15] 结城浩.图解密码技术[M].北京：人民邮电出版社，2015.

(收稿日期：2022－11－18)

作者简介：

湛高峰(1977－)，男，硕士，副研究员，主要研究方向：网络信息安全。

王晓峰(1989－)，女，硕士，工程师，主要研究方向：网络信息安全。

程楠(1983－)，女，硕士，助理研究员，主要研究方向：信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部