面向跨域分布式身份场景可信认证方法研究

仇碧杰，张裕昌，罗江，张峰，霍翔，梅钊源，秦梦瑶，陈敏，赵欣
（国网山西省电力有限公司信息通信分公司，山西 太原 030000）

摘　要：随着联盟链技术的发展，分布式身份技术（decentralized identity，DID）被广泛应用于物联网（Internet of things，IoT）设备认证。在物联网场景中，跨域认证的需求是普遍存在的。然而，现有跨域认证方法一方面依赖于中心化的权威机构，另一方面难以解决不可信颁发者肆意滥发证书的问题，解决该问题的挑战在于去中心化架构与实现中央监管的天然矛盾关系。针对以上问题，设计了一种高效的分级区块链异构联动框架，并基于该框架提出了可信认证方法，实现了分布式跨域认证的同时，缓解了不可信颁发者滥发证书的问题。最后，基于 Sepolia 以太坊测试链进行仿真测试。仿真结果证明，所提方法在实现安全跨域认证的同时，不会引起较大的开销。

关键词：物联网设备认证；跨域认证；信誉机制；不可信颁发者
中图分类号：TN915.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.WLW25196

Research on trustworthy authentication methods for cross-domain distributed identity scenarios

Qiu Bijie, Zhang Yuchang, Luo Jiang, Zhang Feng, Huo Xiang, Mei Zhaoyuan,
Qin Mengyao, Chen Min, Zhao Xin
State Grid Shanxi Electric Power Company, Information and Communication Branch, Taiyuan 030000, China

Abstract: With the development of consortium blockchain technology, decentralized identity (DID) has been widely used in device authentication in Internet of things (IoT) scenarios. Despite the demand of cross-domain authentication, existing methods, on one hand, rely on centralized authorities, and, on the other hand, struggle to address the issue of untrusted issuers wantonly issuing credentials. The core challenge stems from the intrinsic contradiction between decentralized system design and the implementation of centralized regulation. To address the above problems, an efficient hierarchical blockchain heterogeneous interconnection framework was designed. Based on this framework, a trusted authentication method was proposed. This method not only realized decentralized cross-domain authentication but also mitigated the problem of credential over-issuance by untrusted issuers. Finally, experiments based on the Sepolia ethereum testnet were conducted. The simulation results demonstrate that the proposed method achieves secure cross-domain authentication without incurring significant overhead.

Key words: IoT device authentication, cross-domain authentication, reputation mechanism, untrustworthy issuer

0　引言

随着联盟链[1]的发展，分布式身份（decentralized identity，DID）[2-3]凭借去中心化与强鲁棒性的特征，广泛应用于物联网[4]、电力系统[5]等场景中的设备认证。具体而言，颁发者、设备和验证者均将自己的身份标识与公钥的映射发布于联盟链[6]中，颁发者通过签名[7]的方式为设备签发初始化证书，设备本地保存该证书，在需要认证时先对初始化证书签名，生成展示凭证（credential presentation）发送给验证者，由验证者从联盟链中读取颁发者与设备的公钥分别验证两者的签名进行身份验证。然而，在

收稿日期：2025−12−08；**修回日期：**2026−09−10

现实应用中，身份认证通常呈现区域化特征[8-10]，即不同区域的节点分别维护该区域的联盟链，由于联盟链仅允许授权用户访问，不同联盟链难以实现数据共享与跨域认证[11]。

为了实现不同区域之间的跨域认证，现有方案可以分为两类，分别是基于中心化机构认证机制与链式颁发者认证机制。在基于中心化机构认证机制[8]这类方法中，不同区域的验证者均信赖一个中心化的权威机构，该机构对所有区域的联盟链均有访问权限，当需要跨域认证时，权威机构对展示凭证进行验证，并将结果返回给验证者。在链式颁发者认证机制[12]这类方法中，会选定一些中心和机构作为根颁发者，所有区域的颁发者均须由根颁发者进行认证，并持有由根颁发者颁发的颁发者证书。在跨域认证中，验证者首先验证颁发者证书，确认颁发者身份是由根颁发者认证后，再验证展示凭证中的内容。

尽管现有方法实现了分布式身份场景中的跨域认证，但是存在两方面的问题。（1）现有方案均依赖于中心化的机构，如基于中心化机构证书认证机制中依赖中心化的机构，而链式颁发者认证机制依赖中心化的根颁发者。这与分布式场景的完全去中心化的思想是相违背的[13]。（2）不可信颁发者恶意颁发错误证书[14]，由于现有方法缺失对证书颁发者的监管，依然存在不可信颁发者恶意颁发错误证书的问题。

解决以上问题的挑战在于去中心化架构与中央监管的天然矛盾关系。去中心化架构强调完全分布式，即不同的节点都有相同权力，即使监管者发现恶意行为，也难以迅速施加处罚或撤销权限。而监管机制则要求一定程度的集中控制与强制执行，两者在设计理念与信任假设上存在天然冲突。因此，如何在不破坏去中心化特性的前提下实现安全的跨域认证，并对证书颁发行为进行有效的监督，成为物联网场景中跨域认证研究中的关键挑战。

为了解决以上问题，首先，提出了一种高效的分级区块链异构联动框架，基于该框架，设计了一种面向跨域分布式身份场景的安全认证方案，在实现了分布式跨域认证的同时，缓解了不可信颁发者滥发证书的问题。具体而言，该分级区块链异构联动框架包括一条公有链与若干联盟链，其中，公有链用于存储公共信息，联盟链用于不同区域内的认证。其次，为了实现跨域认证，本文提出了分片默克尔树的数据结构，以计算接收该颁发者所有设备的承诺（commitment），并将颁发者与该承诺的映射公开至公有链中，以实现在跨域场景中验证者可以验证设备公钥的合法性。最后，为了缓解不可信颁发者滥发证书的问题，本文提出了颁发者信誉机制，该机制综合考虑了颁发者的活跃度与黑名单，并设计了对应的指标更新机制，以提升认证的安全性。本文的贡献总结如下。

（1）提出一种高效的分级区块链异构联动框架，基于该框架，设计了一种面向跨域分布式身份场景的安全认证方案，在实现分布式跨域认证的同时，缓解不可信颁发者滥发证书的问题。

（2）为了实现跨域认证，提出了分片默克尔树的数据结构，并将承诺值公开至公有链中，以实现在跨域场景中验证者可以验证设备公钥的合法性。

（3）为了缓解不可信颁发者滥发证书的问题，设计了颁发者信誉机制与对应的指标更新机制，该信誉机制综合考虑颁发者的活跃度与是否被列入黑名单，从而提升认证的安全性。

（4）基于Sepolia以太坊测试链对所提方案进行测试，包括Gas开销[6]、时间开销与存储开销。

实验结果表明，本文方案在实现安全跨域认证的同时，并不会引入较大的开销。

1　相关工作

1.1　区块链

区块链[15]是一种分布式账本技术，数据以区块为单位进行存储，每个区块包含前一个区块的哈希值，通过密码学算法将区块按时间顺序依次链接，形成难以篡改的链式结构。区块链按照访问控制方式可分为3种：公有链、联盟链和私有链。公有链是对全球用户完全开放、无需许可即可参与的高度去中心化网络，如比特币[16]、以太坊[17]等；联盟链是由多个预选组织共同管理、仅有授权用户具有对联盟链数据的读写权限，如FISCO BCOS[18]、长安链[19]等，由于其灵活的访问控制特性，被广泛应用于物联网、电力网络等场景中；私有链是由单一组织独立控制、权限高度集中的封闭式网络。

1.2　分布式身份

随着区块链技术的发展，分布式身份应运而生，

分布式数字身份基于区块链技术，与传统认证方案相比，认证过程不依赖中心化的机构，用户具有自主管理自己身份与证书的权利，因而具备较强的鲁棒性并可以保护用户隐私。现有DID的方案围绕隐私保护与认证安全展开。为了实现隐私保护，Self-Key[20]使用零知识证明协议来最小化信息泄露；De Salve等[21]描述了一种适用方法，允许用户仅披露单个属性而不使签名失效；Yamamoto等[22]提出了基于关联数据的可验证凭证，以实现由多个发行方发出的一个或多个可验证凭证之间的选择性披露。为了实现认证安全，文献[23-24]针对企业身份场景进行优化，提出细粒度的身份权限管理与灵活的私钥恢复；LinkDID框架[25]中，提出了一种安全且高效的方法，该方法同时实现抗女巫攻击、抗证书重放攻击与高效的证书撤销；针对跨域场景，现有方案均依赖于中心化的权威机构，这与区块链系统中完全去中心化的思想相违背；另一方面，现有方法假设颁发者都是可信的，然而这一假设在现实场景中并不总是成立。这两个问题严重限制了DID在跨域场景中的落地工作，因此，亟须提出一种分布式的解决方案，实现跨域场景中的安全认证。

2　本文方案

传统DID方案不适用于跨域场景，因为传统方案中，颁发者与设备对证书签名，而验证者从本区域联盟中读取颁发者与设备的公钥，基于公钥验证签名。然而，在跨域场景中，联盟链仅允许授权用户访问链上数据的方式限制了验证者读取公钥这一操作；此外，颁发者的可信度难以进行审计。因此，本文提出了一种面向跨域分布式身份场景的安全认证方案，实现了分布式认证的同时，有效地缓解了由不可信颁发者导致的不安全认证问题。

2.1　总体框架

为了实现跨域场景中的安全认证，本文提出了一种高效的分级区块链异构联动框架，该框架包括一条公有链与若干联盟链，其中，公有链用于存储公共信息，联盟链用于不同区域内的认证，本文整体框架如图1所示，该框架在实现分布式跨域认证的同时，缓解了不可信颁发者滥发证书的问题。

鉴于公有链的公开属性，本文选择使用公有链存储公共信息。此外，与其他公开数据库（如星际文件系统（InterPlanetary file system，IPFS））相比，公有链通过链式结构确保数据的难以篡改性，提供了更高的安全性。公有链主要记录4方面内容，即颁发者列表、公钥承诺映射、颁发者信誉信息与证书撤销列表。（1）颁发者列表是指来自不同区域证书颁发者标识组成的颁发者列表，用于初步检查该颁发者是否已注册。（2）公钥承诺映射是指颁发者与其所有签发设备公钥的向量承诺（vector commitment）的映射，本文设计了分片默克尔树的数据结构，用于计算该向量承诺，该向量承诺允许在不泄露其他元素内容的前提下，证明某个元素是该向量中的成员。（3）颁发者信誉信息指颁发者的更新频率、交互次数、是否被列入黑名单等信息，以对颁发者行为进行约束与审计。（4）证书撤销列表记录着所有被撤销证书的唯一性标识

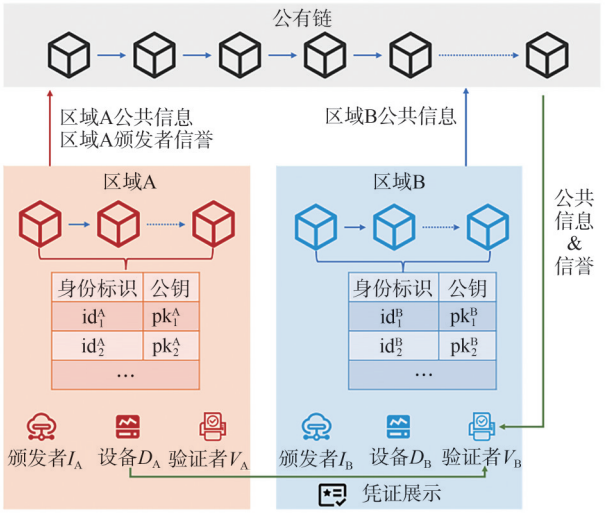

图1　本文整体框架

联盟链由不同区域内部维护，链上存储着该区域内身份标识与公钥的映射，用于本区域内的身份认证，但是不同区域之间的链上数据不共享，而是通过与公有链的交互实现跨域验证，从而支持跨区域可信认证。

基于以上结构，本文设计了新的证书颁发、使用与证书验证过程。对于证书颁发，传统方案中，颁发者仅需对相关信息进行签名，即可生成初始证书，本文为了实现跨域认证，设计了新的颁发流程。具体而言，首先，颁发者对公钥的向量承诺进行更新，使验证者可以验证设备公钥的合法性；之后，生成成员证明，即证明该设备的公钥被公有链上的承诺值包含；最后，对相关信息进行签名操作，以

保证初始证书的真实性与难以篡改性。对于证书使用，传统方案中，设备仅需使用私钥对初始证书进行签名即可，但是这种方式难以解决不可信颁发者的问题，为了支持对颁发者信誉相关指标的统计工作，本文设计了新的交互式证书使用方法，主要思想是验证者与设备完成认证过程，则验证者与设备双方分别向公有链上传签名，来保证结果可验证，此外，本文对签名信息引入随机性，以避免签名信息固定导致设备通过多次上传验证者签名来恶意增加交互次数。对于证书验证，传统方案中，验证者只需从联盟链中读取颁发者与设备的公钥，验证颁发者与设备的签名是否合法，并检查证书是否被撤销即可，但是从联盟链中读取公钥的操作在跨域场景中难以实现。因此，本文设计了新的证书验证策略，首先，验证者初步验证颁发者的合法性；之后，验证设备公钥的合法性，即验证设备的公钥是否被对应的承诺值所包含；之后，验证颁发者的信誉值，以验证颁发者是否可信；最后，验证该证书是否已被撤销。

2.2　分片默克尔树

为了实现高效的向量承诺生成，本文提出了分片默克尔树的数据结构。如图2所示，分片默克尔树由一个映射与多个默克尔树组成，这种设计在实现高效检索的同时，有效地避免了单次改动需要改变整个结构，提高了效率。本文通过将颁发者认证过的所有设备公钥打包进分片默克尔树，仅将分片默克尔树的向量承诺上传至公有链的方式，实现跨域场景中验证者仍然可以验证设备公钥的有效性。

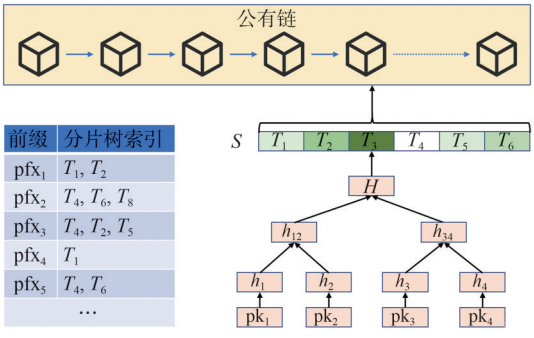

图2　分片默克尔树的数据结构

多个默克尔树的设计可以有效地避免单次改动需要改变整个结构。传统默克尔树[26]是一种基于树结构的向量承诺，输入是一个向量，其中，叶子节点分别存储向量每个元素的哈希值，非叶子节点存储其子节点拼接后的哈希值，该结构允许在不泄露其他成员元素的前提下，证明某个元素属于该向量。在传统方案中，如果进行元素更新，则需要对整个树进行修改。因此，本文设计了多个默克尔树的结构，每个默克尔树的总的元素个数是固定的，如果该树已满，则须创建新的默克尔树，从而实现高效添加与检索。之后，将每个默克尔树的根节点$[T_1, T_2, \cdots, T_n]$进行拼接，从而得到整体根值S，将S公布到公有链中。由于本文采用了默克尔树的结构，实现了在不透露其他公钥信息的前提下，证明某个公钥被这个承诺值所包含。

尽管多个默克尔树的设计可以有效地提高效率，但这种方式的检索效率比较低，因为每次检索公钥均须遍历所有的公钥。为此，本文以多个默克尔树为基础，添加一个映射关系，为减少存储开销，该映射的键是公钥的前k位，值是该公钥对应的根节点值。由于仅使用公钥的前k位前缀pfx作为键，所以可能存在一个键对应多个值的情况，实现了仅对部分树进行检索操作，提高了检索效率。注意这里，k越大，映射导致的存储开销越高，但检索效率也越高；k越小，存储开销减小，而检索效率降低，需要权衡。该结构一方面实现了快速检索，只需访问部分默克尔树进行公钥检索；另一方面实现了在不泄露其他公钥的前提下，证明某个公钥被包含在该承诺值中。

与稀疏默克尔树（sparse Merkle tree，SMT）相比，本文所针对的场景是高效的向量承诺生成，以支持跨域认证中的高效验证，该场景会涉及大量的公钥插入或删除操作，以及生成成员证明的操作，而非面向固定键空间的键值对存储。与SMT相比，在存储开销方面，本文方案存储开销为$O(N+2^k)$，而SMT存储开销为$O(Nd)$，其中，d为SMT的深度，通常为固定常数（如256），可通过合理选择k以提高存储效率；在更新操作计算开销方面，本文通过引入基于公钥前缀的分片机制，将公钥集合划分为多个子默克尔树，从而将单次更新复杂度从$O(\mathrm{lb}\,N)$降低至$O(\mathrm{lb}(N/2^k))$；在查询与成员证明计算开销方面，SMT通过键路径直接定位元素，查找与证明复杂度为$O(\log N)$，相比之下，本文方法需要先根据前缀定位候选子树，再在子树中查找目标元素并生成成员证明。在无额外索引的情况下，最坏情

况下的复杂度为$O(N/2^k)+O(\mathrm{lb}(N/2^k))$，通过合理选择前缀长度$k$，可以显著地缩小候选子树规模，从而在实际场景中有效地控制查找开销。

本文基于分片默克尔树，设计了新的证书颁发、使用、验证流程。本文将颁发者的身份标识记作$\mathrm{id_I}$，颁发者私钥记作$\mathrm{sk_I}$，颁发者公钥记作$\mathrm{pk_I}$；设备的身份标识记作$\mathrm{id_H}$，设备私钥记作$\mathrm{sk_H}$，设备公钥记作$\mathrm{pk_H}$；验证者的身份标识记作$\mathrm{id_V}$，验证者私钥记作$\mathrm{sk_V}$，验证者公钥记作$\mathrm{pk_V}$。颁发者$\mathrm{id_I}$与设备$\mathrm{id_H}$来自同一区域，验证者$\mathrm{id_V}$属于另一区域，本文以如何使$\mathrm{id_V}$跨域验证$\mathrm{id_V}$证书的合法性为例，介绍本文设计的证书颁发、撤销、使用、验证流程。

2.3 证书颁发与撤销

为了支持跨域认证，本文设计了新的证书颁发流程，并且支持证书撤销，以实现安全的跨域认证。与传统证书颁发方案仅需签名操作不同，本文中，颁发者需要进行向量承诺更新、成员证明生成与签名操作。与传统证书撤销方案类似，本文通过将证书唯一性标识公布在区块链中的方式来实现证书撤销[23]。

2.3.1 向量承诺更新

首先，颁发者$\mathrm{id_I}$判断$\mathrm{pk_H}$是否已被本地的分片默克尔树包含，如果已包含，则跳过向量承诺更新步骤，否则将$\mathrm{id_H}$对应的公钥$\mathrm{pk_H}$添加进由颁发者本地维护的分片默克尔树中。添加操作可以分为两种情况：如果当前分片默克尔树中有子默克尔树未满，则将$\mathrm{pk_H}$添加进未满的默克尔树中，具体而言，先将$\mathrm{pk_H}$取哈希，并将哈希值与相邻的兄弟结点进行拼接取哈希得到其父结点，进行递归式操作，直至得到新的默克尔根T_{H}，将整体根值S中的对应位置进行替换；如果当前所有默克尔树均已满，则仅以$\mathrm{pk_H}$为元素，构建新的默克尔树，并将其根节点添加进整体根值中，从而得到更新后的整体根值S'，并将更新后的整体根值上传至公有链中，以便验证过程中验证者可以直接读取。此外，还须对映射进行更新，先取$\mathrm{pk_H}$的前k位前缀pfx作为键，如果该键已存在，则将该公钥对应默克尔树的根节点值添加进键对应的值中；否则，添加一个新的映射，其键为pfx，值为T_{H}。

2.3.2 成员证明生成

生成$\mathrm{pk_H}$对应的默克尔证明MP，默克尔证明是由目标叶子节点，即$\mathrm{pk_H}$对应节点出发，到默克尔树根节点路径上的一系列兄弟节点哈希值所构成的证明数据，例如，图2中，$\mathrm{pk_1}$的默克尔证明$\mathrm{MP}=\{h_2,h_{34}\}$，其中，$h$为节点的哈希值。

2.3.3 签名

颁发者使用自己的私钥对相关信息进行签名，以保证这些信息的真实性与难以篡改性，相关信息包括：证书的唯一性标识（universally unique identifier，UUID），该标识由颁发者生成，颁发者的身份标识$\mathrm{id_I}$、设备的身份标识$\mathrm{id_H}$、设备的属性attr、默克尔证明MP，即：

$$\mathrm{msg_I}=\mathrm{hash}(\mathrm{UUID}\|\mathrm{id_I}\|\mathrm{id_H}\|\mathrm{attr}\|\mathrm{MP}) \tag{1}$$

$$\mathrm{Sig_I}=\mathrm{sign}(\mathrm{sk_I},\mathrm{msg_I}) \tag{2}$$

其中，$\mathrm{sign}(\cdot)$是签名函数，$\mathrm{hash}(\cdot)$是哈希函数，如SHA256等，$\mathrm{sign}(\mathrm{sk_I},\mathrm{msg_I})$代表使用私钥$\mathrm{sk_I}$对消息$\mathrm{msg_I}$进行签名，$\|$代表字符串拼接操作。颁发者初始证书为：

$$\mathrm{Cert_I}=\{\mathrm{id_I},\mathrm{id_H},\mathrm{attr},\mathrm{MP},\mathrm{Sig_I}\} \tag{3}$$

2.3.4 证书撤销

本文支持证书撤销，当颁发者发现设备由于被攻击等原因存在作恶或不正当行为时，颁发者可以通过将对应UUID发布至公有链的方式对证书进行撤销操作，验证者发现正在验证的证书UUID已被公布至公有链时，则认为该证书已被撤销，认证失败。

2.4 证书使用

在传统方案中，尽管设备对初始证书进行签名的方式可以实现证书的不可转让性，但在不可信颁发者存在的场景中，这种方式难以支持对颁发者信誉相关指标的统计工作，因此，本文设计了新的交互式证书使用方法，以支持对交互次数的统计操作。

交互式证书使用流程如图3所示，由验证者与设备共同完成认证过程，通过双方向公有链上传签名的方式保证交互次数的统计结果的可验证性。引入随机数Z作为挑战值的方式引入随机性，以避免签名信息固定导致的恶意增加交互次数行为。

具体而言，本文设计的证书使用过程包括以下4个步骤。

（1）协商挑战值。验证者随机生成一个挑战值Z，并将Z发送给设备，设备收到后，回复$Z+1$，以表明自己正确接收Z，并同意以Z作为挑战值，进行交互次数统计操作。

（2）设备挑战值签名。设备使用自己的私钥对

挑战值进行签名，生成签名$\mathrm{Sig}_{\mathrm{H}}^{Z}$，并将$Z$与$\mathrm{Sig}_{\mathrm{H}}^{Z}$拼接后得到$Z\|\mathrm{Sig}_{\mathrm{H}}^{Z}$，将$Z\|\mathrm{Sig}_{\mathrm{H}}^{Z}$公布到公有链上，公有链验证$\mathrm{Sig}_{\mathrm{H}}^{Z}$的合法性后，将其记录在链上，表明设备已开始验证流程。

（3）证书签名。设备对$\mathrm{Cert}_{\mathrm{I}}$进行签名，即$\mathrm{Sig}_{\mathrm{H}}=\mathrm{sign}(\mathrm{sk}_{\mathrm{H}},\mathrm{Cert}_{\mathrm{I}})$，生成凭证展示$\mathrm{Cert}_{\mathrm{H}}=\{\mathrm{Cert}_{\mathrm{I}},\mathrm{Sig}_{\mathrm{H}}\}$，并将$\mathrm{Cert}_{\mathrm{H}}$发给验证者。

（4）验证者挑战值签名。验证者验证证书的合法性后（具体流程见第2.5节），使用sk_{V}对挑战值Z进行签名操作，得到签名$\mathrm{Sig}_{\mathrm{V}}^{Z}$，将$\mathrm{Sig}_{\mathrm{V}}^{Z}$发布至公有链上，则公有链上记录的该颁发者与验证者的交互次数加1。

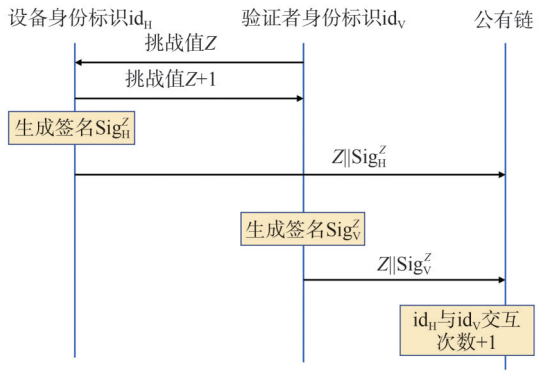

图3　交互式证书使用流程

2.5　证书验证

由于联盟链数据不共享，且颁发者不可信，传统方案中验证者从联盟链中读取颁发者与设备的公钥的操作难以实现。因此，本文设计了新的证书验证策略，该验证策略主要包括4个步骤，分别是颁发者签名验证、设备签名验证、颁发者信誉验证、撤销信息验证。

2.5.1　颁发者签名验证

验证者从$\mathrm{Cert}_{\mathrm{H}}$中检索得到对应的颁发者身份标识$\mathrm{id}_{\mathrm{I}}$，并在公有链中查看该颁发者是否已注册，检索对应的公钥pk_{I}，验证颁发者签名。

2.5.2　设备签名验证

验证者首先基于承诺验证设备公钥pk_{H}的合法性，并基于pk_{H}验证设备的签名。具体而言，第1步，验证者验证S是否被记录在公有链上；第2步，验证T_i是否被S包含；第3步，验证默克尔证明，即将默克尔证明中的元素两两拼接，递归式取哈希，得到根节点，并对比计算得到的根节点T_i'与$\mathrm{Cert}_{\mathrm{H}}$中记录的$T_i$，如果比对成功，则该$\mathrm{pk}_{\mathrm{H}}$是合法的，并基于$\mathrm{pk}_{\mathrm{H}}$验证设备的签名。

值得注意的是，由于整体根值是频繁变动的，而生成的初始化证书是相对固定的，因此在验证S是否被记录在公有链上时，只需验证被记录即可，无须验证S是最新的，因为这一步仅验证公钥的合法性，即id_{I}为id_{H}颁发过证书，证书撤销操作将对UUID进行公开以实现撤销，因此，这里无须对S的时效性进行验证。

2.5.3　颁发者信誉验证

为了缓解不可信颁发者肆意颁发错误证书的行为，本文提出了颁发者信誉验证机制，该机制考虑两方面因素，第1是该颁发者是否已被拉入黑名单，第2是颁发者是否足够活跃，以缓解不可信颁发者的问题。验证者需要验证两方面的内容，分别是黑名单检查与活跃度检查。

针对黑名单检查，本文设计了分布式的举报机制，允许来自不同区域的颁发者以抵押数字资产的方式对颁发者进行举报，如果举报超过一定数量，则将该颁发者写入黑名单。验证者一旦发现该颁发者已被列入黑名单，则认证失败。具体而言，本文设计了分布式的举报机制，当某一验证者发现某设备的身份不符或属性造假的问题时，该验证者可以通过向区块链抵押一部分数字资产的方式，举报该颁发者是恶意颁发者，抵押数字资产的方式是为了增加举报门槛，以限制验证者恶意举报的行为。如果区块链收到来自不同验证者超过一定数量T的举报，则将该颁发者列入黑名单，并将抵押的数字资产退还给验证者。验证者一旦发现该颁发者被列入黑名单，则认为该颁发者不可信，认证失败。

针对活跃度，本文设计了基于加权平均的颁发者活跃度量化机制，活跃度的量化综合考虑更新公钥承诺的次数r_1、id_{I}与id_{V}的交互次数r_2。针对公钥承诺的次数，公有链中，操作都是可审计的，因此，更新公钥承诺的次数可直接通过统计调用智能合约的次数得到。针对id_{I}与id_{V}的交互次数，本文设计了交互式的认证策略，通过id_{I}与id_{V}对随机数上传签名的方式，双方完成认证流程，分别上传签名，公有链节点验证后，将id_{I}与id_{V}的交互次数加1。最后，本文基于更新次数、交互次数，加权平均计算该颁发者的信誉值，即：

$$R=\lambda_1\cdot r_1+\lambda_2\cdot r_2 \tag{4}$$

其中，λ_1和λ_2是权重参数，取值范围均为[0, 1]，用

来控制更新公钥承诺的次数及 id_I 与 id_V 的交互次数两个因素的相对重要性。之后，验证颁发者的活跃度是否高于一定阈值 R_T，如果该颁发者活跃度超过这个阈值，则认为该颁发者是可信的，否则验证失败。

本文所提的黑名单机制提供了一种强约束的安全保障，用于快速识别并隔离已确认的恶意颁发者，其本质可视为基于历史行为的二值化信誉判定。活跃度指标基于链上可审计的行为（包括公钥承诺更新与认证交互）进行量化：一方面，在无须引入复杂信任建模的情况下，能够有效地刻画颁发者的行为稳定性与参与程度；另一方面，认证交互在一定程度上反映了不同域之间的信任关系，从而隐式体现跨域信任传递特性。此外，由于相关行为记录存储于公有链上并对所有参与方开放，不同区域的验证者可以基于统一且可验证的数据源进行判断，从而在无需显式信任传播机制的前提下，实现跨域信任的隐式共享。

2.5.4　撤销信息验证

验证者通过读取公有链的方式，查看该展示凭证的UUID是否被区块链中的撤销列表所包含，如果被包含，认证失败，否则，认证成功。验证者对 Z 进行签名，得到签名 Sig_V^Z，并将签名 Sig_V^Z 上传至公有链，公有链节点认证后，id_I 与 id_V 的交互次数加1。

2.6　安全性分析

本文对所提的认证机制进行了系统性的安全性分析。相较于基线方案，本文方案的优势主要体现在以下两个方面：（1）采用分布式认证架构，更符合DID的设计理念，避免对单一中心节点的依赖，从而在一定程度上降低单点失效与集中式滥用带来的系统性风险；（2）引入基于信誉的评估机制，有效地降低了恶意证书颁发者的作恶影响范围。需要指出的是，分布式架构的安全性已在既有研究中得到了充分讨论，因此，本文将分析重点放在信誉机制所带来的安全性提升，从可量化角度出发，评估恶意证书被成功验证的风险。设系统中共有 I 个证书颁发者，每个颁发者平均颁发 C 个证书，其中，恶意颁发者的占比为 m（$0 < m < 1$）。恶意颁发者对单个证书实施恶意签发的概率为 p_m，且每个证书平均被 q 个验证者验证。在未引入信誉机制的情况下，由恶意颁发者导致的恶意证书通过验证的总次数期望为：

$$N_0 = I \cdot C \cdot m \cdot p_m \cdot q \tag{5}$$

在本文所提的机制中，设基于黑名单机制识别恶意颁发者的概率为 p_b，基于活跃度机制识别恶意颁发者的概率为 p_a。假设两种识别机制相互独立，则恶意颁发者至少被一种机制识别的概率为：

$$P_{\text{detected}} = p_a + p_b - p_a p_b \tag{6}$$

相应地，恶意颁发者未被识别的概率为：

$$P_{\text{undetected}} = (1 - p_a)(1 - p_b) = 1 - p_a - p_b + p_a p_b \tag{7}$$

因此，引入信誉机制后，由恶意颁发者导致的恶意证书通过验证的总次数期望可近似表示为：

$$N_1 = I \cdot C \cdot m \cdot p_m \cdot q \cdot (1 - p_a)(1 - p_b) \tag{8}$$

由于 $(1 - p_a)(1 - p_b) < 1$，因此有 $N_1 < N_0$。该结果表明，本文所提的信誉机制能够在期望意义下有效地降低恶意证书通过验证的总次数，从而提升系统的整体安全性。

3　仿真测试

本文对所提框架进行了性能测试。首先，将相应的智能合约部署到Sepolia以太坊测试链；随后，从以下4个问题展开测试工作。

问题1　调用不同智能合约是否会造成较大的Gas开销？

问题2　默克尔树的容量不同是否影响证书的颁发、使用和验证的时间开销？

问题3　在该区域内设备数固定的前提下，前缀 k 的取值，是如何影响存储开销的？

问题4　与基线方案对比，本文方案是否造成了较大的时间开销？

需要指出的是，本文所提方案并不依赖于特定的区块链平台，在理论上可适用于任意支持智能合约执行与数据可验证存储的区块链系统。本文选择Sepolia以太坊测试链进行实验，主要基于其代表性：以太坊作为当前最典型的智能合约平台，其执行模型（以太坊虚拟机）、Gas计费机制以及状态存储方式已成为事实上的行业标准，并被大量区块链系统（如Avalanche[27]等）借鉴。因此，在该平台上的实验结果具有较好的代表性。

3.1　实验环境

本文实验在搭载Apple M2处理器、8 GB内存的MacBook Air计算机上开展，所使用的Node.js版本为18.13.0。本文使用Solidity 0.8.17、Truffle 5.7.2开发框架与Infura节点服务部署智能合约，使用Python 3.10.9进行本地维护，分别使用Web3 5.31.3

与Pymerkle 6.1.0进行分片默克尔树与智能合约调用。

针对问题1，不同操作导致的Gas开销见表1，Gas开销是区块链中用于评估计算资源的指标，从表1中可以看出，由于颁发者注册、承诺更新与信誉相关指标统计造成的Gas开销在29 377~77 688范围内，不会造成比较大的Gas开销。

表1　　不同操作导致的Gas开销

操作		Gas开销
颁发者	注册	50 889
承诺	更新	51 780
黑名单机制	举报	77 688
	新增	50 824
	删除	36 728
交互次数	初始化	29 377
	更新	58 565

针对问题2，本文测试了默克尔树的容量对证书的颁发、使用和验证的时间开销的影响，由于默克尔树是二叉树的结构，因此测试时，本文设置默克尔树容量分别取[8, 16, 32, 64, 128]，分别测试不同取值下的时间开销。证书颁发与使用时间开销如图4所示，从图4可以看出，容量的大小不会显著影响时间开销，颁发操作与使用操作均可在毫秒级别内完成。证书验证时间开销如图5所示，由于证书验证操作由4个步骤组成，分别是设备签名验证、颁发者签名验证、颁发者信誉验证与撤销信息验证，因此，对这4个步骤的时间开销分别进行了展示。从图5中可以看出，颁发者信誉验证步骤与其他步骤相比，造成了较大的时间开销，这是因为该步骤涉及多次公有链数据的读取操作，尽管如此，该步骤可以对颁发者信誉进行评估，以缓解不可信颁发者肆意颁发错误证书的行为。总体而言，验证操作的时间开销在0.25 s左右，可在亚秒级别的时间内完成，说明本方案的高效性。

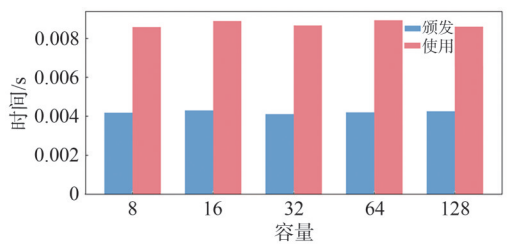

图4　证书颁发与使用时间开销

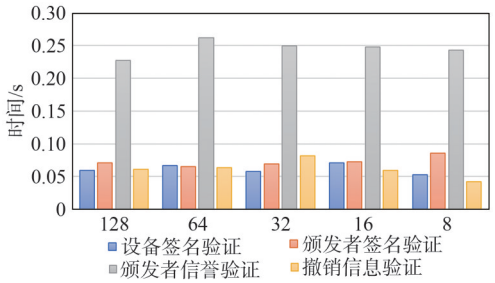

图5　证书验证时间开销

针对问题3，本文测试了在设备数量固定的前提下，前缀k的取值对存储开销的影响。在这里，分别设置设备总数为512、1 024、2 048，前缀分别取1~6，k与映射个数的关系如图6所示，k对存储开销的影响如图7所示，从图中可以看出，随着k的增加，映射个数随之增加，因而具有更高的检索效率，但是存储开销也会随之增加。在本文实验设置中，当设备总数为512与1 024、$k=6$时，映射个数等于设备总数，即使再增加k，也不会进一步提高检索效率。

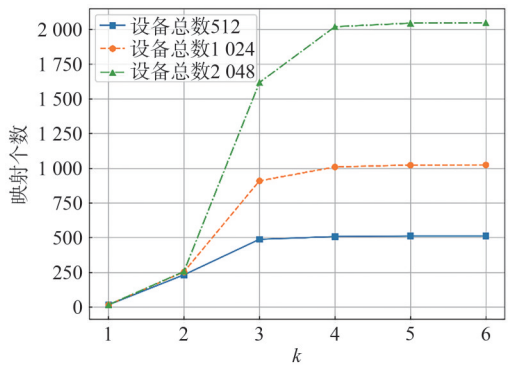

图6　k与映射个数的关系

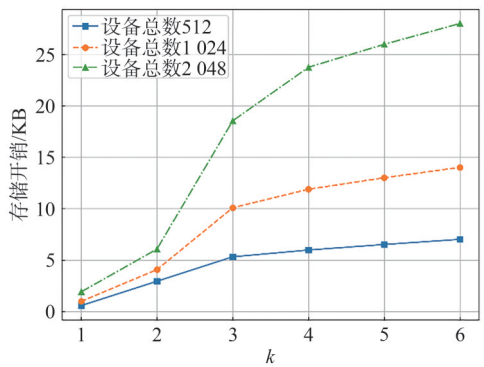

图7　k对存储开销的影响

针对问题4，本文方案与基线方案性能对比如图8所示，展示了与基线方案（基于中心化机构的认证机制、链式颁发认证机制）相比，本文方案在

凭证颁发、凭证使用与凭证验证阶段的时延对比。实验设置了 32 768 个设备，设置 $k = 3$。从结果可以看出，在凭证颁发阶段，本文方案与其他基线方案的时延基本一致，未引入额外开销。在凭证使用阶段，本文方案的时延略高于其他两种基线方案，主要原因在于，为支持对颁发者信誉相关指标的统计，本文要求设备对挑战值执行额外的签名操作。尽管该步骤带来了一定的时间开销，但能够为后续的信誉评估提供可靠依据。在凭证验证阶段，本文方案的时延相比链式颁发认证机制约增加 0.05 s。这主要是由于本文引入了基于区块链的信誉统计机制，验证者需要额外访问链上信息以完成信誉评估。虽然该过程增加了验证时延，但基于信誉评估可有效地降低颁发者作恶的风险。

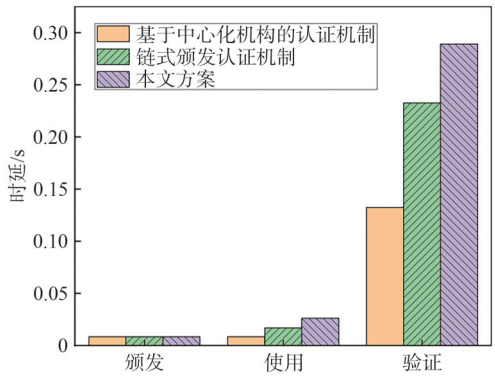

图 8　本文方案与基线方案性能对比

4　结束语

鉴于现有跨域认证方案依赖权威机构且难以解决不可信颁发者肆意滥发证书的问题，本文设计了一种高效的分级区块链异构联动框架，并基于该框架提出可信认证方法。具体而言，首先，提出了分片默克尔树的数据结构，并通过公有链存储公共信息的方式，以分布式的方式实现跨域认证；其次，为了缓解不可信颁发者滥发证书的问题，提出了颁发者信誉机制，该机制综合考虑了颁发者的活跃度、交互性与是否被列入黑名单，以提升认证的安全性。实验结果证明了该方法在实现了安全跨域认证的同时，不会引起较大的开销。

参考文献：

[1] Alamer A. A security and privacy-preserving consortium blockchain-based accessing control in mobile crowdsensing[J]. IEEE Access, 2025, 13: 53815-53834.

[2] Yin J, Xiao Y, Feng J, et al. DidTrust: privacy-preserving trust management for decentralized identity[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(3): 3105-3120.

[3] Xu W J, Deng J M, Yu J L, et al. Blockchain-based verifiable decentralized identity for intelligent flexible manufacturing[J]. IEEE Internet of Things Journal, 2025, 12(16): 32366-32378.

[4] Akli A, Chougdali K. IOTA-assisted self-sovereign identity framework for decentralized authentication and secure data sharing[J]. IEEE Access, 2025, 13: 80191-80205.

[5] Kilthau M, Asman M, Karmann A, et al. Integrating peer-to-peer energy trading and flexibility market with self-sovereign identity for decentralized energy dispatch and congestion management[J]. IEEE Access, 2023, 11: 145395-145420.

[6] Dang R R, Li H, Yang A, et al. Decentralized identity system for high-value commodity supply chain based on consortium blockchain[C]//Proceedings of the 2023 4th International Conference on Big Data Economy and Information Management. New York: ACM Press, 2024: 337-343.

[7] Zhang Z N, Ren W, Zhang X C, et al. A blockchain and signature based scheme for cross-domain authentication with decentralized identity[J]. Computer Standards & Interfaces, 2025, 94: 103994.

[8] Xu N, Xie T X, Ding K, et al. Blockchain-based cross-domain authentication techniques in decentralized identity[C]//Proceedings of the 2025 IEEE 11th Conference on Big Data Security on Cloud (BigDataSecurity). Piscataway: IEEE Press, 2025: 64-70.

[9] Zhang Z N, Xiong R T, Di X Y, et al. CroAuth: a cross-domain authentication scheme based on blockchain and decentralized identity[C]//Proceedings of the 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE Press, 2024: 2016-2021.

[10] Jeyakumar I H J, Kubach M. A trust implementation model for cross-domain decentralized identity ecosystems: architecture, use case, and implementation[J]. Procedia Computer Science, 2025, 254: 10-19.

[11] Alamer A. A security and privacy-preserving consortium blockchain-based accessing control in mobile crowdsensing[J]. IEEE Access, 2025, 13: 53815-53834.

[12] Fartitchou M, Lamaakal I, El Makkaoui K, et al. BlockMEDC: blockchain smart contracts for securing Moroccan higher education digital certificates[PP]. V1. arXiv(2024-10-08)[2025-10-08], arXiv: 2410.07258.

[13] Maram D, Malvai H, Zhang F, et al. CanDID: can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 1348-1366.

[14] Ta T A, Hui X Y, Chau S C. Ring referral: efficient publicly verifiable ad hoc credential scheme with issuer and strong user anonymity for decentralized identity and more[C]//Proceedings of the 2025 IEEE Symposium on Security and Privacy (SP). Piscataway:

IEEE Press, 2025: 184-202.

[15] Nahom Abishu H, Sun G L, Habtamu Yacob Y, et al. Multiagent DRL-based consensus mechanism for blockchain-based collaborative computing in UAV-assisted 6G networks[J]. IEEE Internet of Things Journal, 2025, 12(4): 4331-4348.

[16] 黄永洪, 关琪, 肖敏, 等. 一种基于地址编码的高效区块链隐蔽通信模型[J]. 重庆邮电大学学报(自然科学版), 2026, 38(2): 223-231.
Huang Y H, Guan Q, Xiao M, et al. Efficient blockchain covert communication model based on address encoding[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2026, 38(2): 223-231.

[17] 王俊岭, 边俊君, 刘佳年, 等. 以太坊经典网络双自私矿工策略的马尔可夫链模型与收益分析[J]. 计算机应用, 2026, 46(5): 1526-1533.
Wang J L, Bian J J, Liu J N, et al. Markov chain model and profit analysis of two-selfish-miner strategy in ethereum classic network[J]. Journal of Computer Applications, 2026, 46(5): 1526-1533.

[18] Chen C L, Zhan W B, Tsaur W J, et al. Constructing a secure charity NFT auction platform using fisco bcos blockchain for enhancing transparency and traceability[J]. IEEE Access, 2024, 12: 36924-36941.

[19] 勒川. “长安链”破解区块链自主可控“根问题”[J]. 中关村, 2025(5): 88-89.
Le C. “Changan Chain” solves the “root problem” of blockchain autonomy and controllability[J]. Zhongguancun, 2025(5): 88-89.

[20] Dunphy P, Petitcolas F A P. A first look at identity management schemes on the blockchain[J]. IEEE Security & Privacy, 2018, 16(4): 20-29.

[21] De Salve A, Lisi A, Mori P, et al. Selective disclosure in self-sovereign identity based on hashed values[C]//Proceedings of the 2022 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2022: 1-8.

[22] Yamamoto D, Suga Y, Sako K. Formalising linked-data based verifiable credentials for selective disclosure[C]//Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Piscataway: IEEE Press, 2022: 52-65.

[23] Yang H J, Song R, Chen B, et al. MoDID: decentralized identity management for multiple owners[C]//Proceedings of the ICC 2024-IEEE International Conference on Communications. Piscataway: IEEE Press, 2024: 2022-2027.

[24] Yang H J, Xie B, Wang J H, et al. Privacy-preserving and secure decentralized identity management for multiple controllers[C]//Proceedings of the GLOBECOM 2024-2024 IEEE Global Communications Conference. Piscataway: IEEE Press, 2024: 541-546.

[25] 周子愚, 陈珊珊. 基于默克尔树结构的多链溯源技术[J]. 计算机工程与设计, 2025, 46(5): 1327-1334.
Zhou Z Y, Chen S S. Multi chain traceability technology based on Merkel tree structure[J]. Computer Engineering and Design, 2025, 46(5): 1327-1334.

[26] Zhang D M, Xie L, Tao Y, et al. NMFT: a copyrighted data trading protocol based on NFT and AI-powered merkle feature tree[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 13041-13054.

[27] De Candia A, Conte D, Golpayegan H A, et al. Symmetry breaking and avalanche shapes in modular neural networks[J]. Frontiers in Computational Neuroscience, 2026, 20: 1744991.

[作者简介]



仇碧杰（1990– ），男，国网山西省电力有限公司信息通信分公司高级工程师，主要研究方向为电力光缆、设备、设施运行维护等。



张裕昌（1997– ），男，国网山西省电力有限公司信息通信分公司工程师，主要研究方向为电力光通信技术。



罗江（1983– ），男，国网山西省电力有限公司信息通信分公司高级工程师，主要研究方向为电力通信工程及运行管理。



张峰（1989– ），男，国网山西省电力有限公司信息通信分公司高级工程师，主要研究方向为电力通信运行管理。



霍翔（1995– ），男，国网山西省电力有限公司信息通信分公司工程师，主要研究方向为电力通信系统检修。



梅钊源（1998– ），男，国网山西省电力有限公司信息通信分公司工程师，主要研究方向为电力通信传输网运维。



秦梦瑶（1991– ），女，国网山西省电力有限公司信息通信分公司高级工程师，主要研究方向为电力数据通信网架构优化与网络安全。



陈敏（1993– ），女，博士，国网山西省电力有限公司信息通信分公司工程师，主要研究方向为电力通信大容量传输网运维及优化。



赵欣（1991– ），女，国网山西省电力有限公司信息通信分公司工程师，主要研究方向为电力数据网络运维检修。