中国移动 研究院
China Mobile CMRI

基于区块链的数字身份研究报告

（2020 年）

中国移动研究院

前　言

在传统互联网时代，设备、终端、软件、服务、应用等实体都需要唯一的数字身份，方能实现实体标识、相互识别。数字身份是建立信任关系的基础，也是实现数字空间治理的前提，只有准确识别实体，才能对实体的行为和信誉进行持续评估和管理。数字证书作为一种常见的数字身份凭证，具有应用灵活、安全性高等特点，在互联网中得以广泛应用。随着以 5G 为代表的万物互联新时代的到来，智慧城市、物联网、数字孪生不断普及，无论是联网设备之间交互，还是连接这些设备和人的协作体系，都迫切需要基于数字身份和认证体系构建数字世界的安全基础。然而，在实际应用过程中，基于公钥基础设施的传统数字证书体系难以适用于新的实体身份认证场景，面临证书颁发流程长、证书配置效率低、状态管理实时性差、跨 CA 机构证书互信复杂等问题。

区块链技术具有分布式记账、多方共识、数据防篡改等特性，可在设备商、运营商、服务商、用户以及其他可信机构之间建立信任，构建安全的分布式身份认证体系，为万物互联数字世界中的软硬件提供身份标识，并在此基础上建立面向未来的数字身份治理体系。

本研究报告将聚焦以数字证书作为凭证的数字身份认证技术，分析在具体实践中遇到的问题，提出基于区块链技术的数字身份认证应用方案，并介绍其在移动通信网络中的应用场景。

参与本研究报告撰写的主要专家包括：中国移动通信研究院何申、粟栗、阎军智、杨波、王珂、杭小勇、刘福文等，中国信息通信研究院云计算与大数据研究所庞伟伟，区块链技术与数据安全工业和信息化部重点实验室潘妍、李卫、李磊、余宇周等，吉大正元信息技术股份有限公司刘岱、李健、刘飞宇、韩璇等，在此表示感谢。

目 录

1 引言

在互联网时代，数字身份分散在各个软硬件产品中，用于在网络中实现对各软硬件实体的身份认证。基于公钥密码学的 PKI（公钥基础设施，Public Key Infrastructure）技术是一种常见的用于网络实体数字身份认证的解决方案。PKI 技术起源于互联网，主要用于解决身份认证、数字签名、密钥协商等安全问题。随着物联网、智慧城市等应用场景的快速推广以及应用领域的不断拓展，网络设备、终端设备的安全需求越来越受到重视，因此 PKI 技术逐步引入到移动蜂窝网、物联网、车联网等移动通信场景，但是在移动通信网络的具体应用中，PKI 存在便捷性等方面的问题。本技术报告在分析传统 PKI 体系在移动互联网实践中遇到的问题的基础上，提出基于区块链的数字身份认证系统，包括系统架构、技术方案、应用案例等内容，为万物互联的数字世界软硬件提供身份认证服务，构建加强面向数字孪生新时代的安全治理体系。

2 传统数字身份技术在移动通信网中的问题

2.1 通信网身份凭证通常分为对称和非对称两种方式

在通信网中，为了实现对设备、终端、软件、服务、应用等网络实体的身份认证，通常需要为这些网络实体分配对应的身份凭证，网络实体利用身份凭证向认证方证实自己的身份。该身份凭证可分为对称和非对称两种方式。若采用对称方式，则要求认证方存储被认证网络实体的身份凭证，若认证方无法获取网络实体的身份凭证，则无法实现认证。若采用非对称方式，则身份凭证仅在对应的被认证网络实体进行存储，认证方只需信任被认证网络实体的身份提供方，即可实现对被信任网络实体的认证，该方式由于更加灵活，在移动通信网中有着广泛的应用。

2.2 PKI 数字证书是通信网中实现身份认证的重要凭证

PKI 是用于实现基于公钥密码体制的密钥和数字证书的产生、管理、存储、分发和撤销等功能的基础设施，广泛应用于数据加解密、数据完整性保护、数字签名、身份认证等多种场合，以及 IPSec、TLS 等多种安全协议，为通信网中包括网络设备、终端、软件在内的各种软硬件实体，以及通信网用户提供了基本的安全服务，在信息安全领域扮演着非常重要的角色。

PKI 身份凭证包括私钥和公钥证书（又称数字证书）两个部分，其中私钥由网络实体秘密保存，数字证书包含证书持有者的信息、证书签发机构的信息、持有者的公钥、证书有效期、证书用途、证书签发机构对该数字证书的签名等信息，用于证明证书拥有者身份、确保信息的机密性、完整性及不可抵赖性。数字证书由证书认证授权中心（简称 CA，Certification Authority）签发。CA 是一个权威的、可信任的、公正的第三方机构，负责验证用户申请信息的可信性，包括证书的认证、证书内容审核、证书有效时间管理以及证书的颁发、更新、撤销和归档等。CA 是 PKI 体系的核心，是信任的基础。只有信任根 CA，才能通过根 CA 对证书的有效性和真实性进行认证。

2.3 传统 PKI 数字证书在实践中存在诸多不便

(1) 证书批量配置效率低

用户在配置和使用证书时，首先需要向 CA 机构申请证书。CA 机构签发证书后，用户需要将签发的证书配置或安装至目标设备或服务器中。传统互联网和物联网应用中，应用类型较多的一种证书是服务器证书。一般情况下，该类型证书的申请和配置都采用人工方式。但在移动通信网、物联网、车联网等场景中，大量的网络设备和终端设备需要配置数字证书，根据具体场景，证书可能分别来自第三方 CA 机构、设备商自建 CA 或者运营商 CA。由于涉及数量巨大，导致这些场景下证书配置的效率较低。如何快速、高效地实现私钥和证书的批量配置

成为万物互联时代的迫切需求。

为了解决批量证书配置问题，通常采用如下两种方式：

- **生产线灌装**：设备商在生产线上将证书灌装进入设备，这些证书可以向第三方 CA 机构购买，也可以由设备商自建 CA 签发。前者将增加设备成本，后者则带来了 CA 系统建设、维护的成本。
- **在线申请**：设备入网上线时以在线方式申请证书，例如采用 CMP（Certificate Management Protocol，证书管理协议）在线申请 CA 证书，这种方式仍需要被 CA 机构信任的初始安全凭证，否则 CA 机构无法确认证书申请的真实性。此外，还可能存在大量设备集中申请的情况。

产生该问题的根源在于数字证书的产生过程与数字证书的信任域紧耦合，即，信任某 CA 机构的依赖方形成一个信任域，该 CA 机构签发的数字证书可以在该信任域使用，数字证书一旦形成，则其使用范围就仅限于所处的信任域。在实际应用中，许多设备在生产阶段无法确定其未来部署时所处的信任域，难以确定签发证书的 CA 机构，因此，导致生产商难以在设备生产过程中与 CA 机构紧密配合，在生产线实现数字证书的批量灌装。

(2) 多 CA 互信复杂

用户证书只能由所属 CA 的根证书进行验证，不同 CA 之间的证书不能相互验证。针对该问题目前有如下几种解决方案，但每种解决方案都存在一定的局限：

- **权威 CA 列表**：为了实现对证书的验证，依赖方需要维护所有可能涉及的 CA 的根证书，这些根证书被称为权威 CA 列表。该方式对依赖方有较高要求，每一个依赖方需要重复地配置自己的权威 CA 列表，识别所有可能的根证书。此外，权威 CA 列表还可能发生变化，无论是维护权威 CA 列表自身，还是在已经部署的设备中更改权威 CA 列表，代价都比较高。
- **CA 交叉认证**：通过 CA 为其他 CA 签发证书的方式，可以扩大 CA 的信任范围。交叉可以是单向的，也可以是双向的。当 CA 数量较少时，交叉认证可以很好地解决 CA 互信问题。但大量 CA 之间进行两两交叉

认证时，就会形成复杂的网状结构。另外，一般情况下只有安全级别低的 CA 会给安全级别高的 CA 签发交叉证书，证书策略经过多次映射之后会使证书用途大大受限。

- **桥 CA：**该方案类似现实生活中行业协会中介的信任关系。每一个 CA 与桥 CA 相互信任后，就能够同时成为该桥 CA 系统中信任方和被信任方。当 CA 数量较多时，采用桥 CA 可以避免两两交叉认证的弊端，但桥 CA 运营方的选择是个难题，桥 CA 运营方的可信程度直接决定了互信关系的可靠程度。

(3) 内网设备无法使用 CRL/OCSP

在运营商网络、企业内网中，有部分部署于内网的设备需要支持数字证书验证（即作为证书的依赖方），需要连接互联网使用 CRL/OCSP 协议查询证书状态，但这些设备不具备连接互联网的能力。TLS 扩展方案（RFC 4366）希望能够解决上述问题，但要求服务器端访问 OCSP 服务器获取证书状态信息，仍无法适用于服务器端和客户端都处于内网的场景。此外，还可以采用定期导入 CRL 列表的方式，该方式增加了管理开销，且由于数据不是实时更新，也存在安全隐患。

(4) CRL/OCSP 单点故障

传统的 PKI 数字证书采用中心化结构，难以避免 CRL/OCSP 单点故障问题。2016 年 10 月，知名数字证书颁发机构 GlobalSign 证书撤销服务器出现故障并影响了多个大型网站，包括维基百科、金融时报，以及国内的京东商场、淘宝、天猫等。由于 CRL 和 OCSP 服务由 CA 机构提供，一旦由于 CA 机构自身原因或遭受安全攻击等原因不能提供该服务，将影响使用相应 CA 机构数字证书的用户。

3 区块链为数字身份带来的机遇

3.1 基于区块链构建数字身份认证体系的可行性

区块链数据以分布式的方式存储于多个节点之中，破坏任意节点均不会导致区块链数据丢失。因此，在区块链基础上构建 PKI 系统，将数字证书及其状态信息记录到区块链中，可以解决传统 PKI 技术单点失效问题。

区块链具有去中心化的特性，由多个可信参与方共同形成的联盟链，多个参与方共同对数字证书进行验证，将通过参与方验证的数字证书记录到区块链中，那么这些数字证书就可以被区块链所有参与方认可。如果这些参与方都是 CA 机构，那么联盟链就在多个 CA 机构之间建立起信任关系，可以解决多 CA 互信难的问题。

利用区块链的智能合约及共识机制，可实现数字身份的在线审核。证书用户例如设备商可以先产生数字证书，由多个参与方共同对这些数字证书进行审核验证，验证通过之后才能记录到区块链中。这将传统先申请证书再配置证书的应用逻辑，改变为先产生配置证书再发布证书，可以有效提升证书批量配置的效率。由于区块链中节点可访问所有区块数据，通过在网络边界部署区块链节点，获取区块链中证书信息，提供证书状态查询服务，可以解决内网设备无法访问互联网 CRL/OCSP 服务器的问题。

利用区块链中通道的思想，可实现信任域的按需建立。为了保护证书用户隐私，也为了实现更加高效的数字身份认证，区块链各参与方可根据业务和实际需要，在互信的相关方之间建立通道，在该通道中实现数字证书的审核和发布。采用此方式，可以灵活地建立证书信任域，同时还可以防止域外参与方获取信任域内的信息。

3.2 基于区块链构建数字身份认证体系的原理

在传统 PKI 技术中，权威 CA 机构对申请证书的用户进行身份鉴别，鉴别通过后根据用户提交的公钥信息为用户签发数字证书。本质上，CA 机构将公钥与身份绑定在一起，签发数字证书供用户使用。

在区块链上构建 PKI 数字证书管理系统，可以 PKI 数字证书管理系统为核心，构建数字身份认证体系。传统 CA 机构对证书用户身份鉴别的方式，以 CA 联盟的方式搭建区块链数字证书管理系统，将经过各 CA 机构鉴别的证书记录到区块链当中，以此仍然可以将公钥证书与具体用户建立对应关系。使用该方式记录到区块链中的证书由于经过了多个 CA 机构的共识，可以有效解决多 CA 互信问题。

此外，网络设备的身份与自然人的身份具有很大不同。自然人具有法律、经济、生物、社交等多种属性，分别需要由不同的机构进行鉴别。网络设备的身份具有物理属性和网络属性，其中物理属性例如设备型号、硬件 ID、MAC 地址等，网络属性例如 IP 地址、网络标识等。物理属性由设备商提供和背书，网络属性由设备部署和运营机构分配和背书。因此，在为网络设备申请身份证书时，权威机构仅需确认该身份归属于相应的设备商或运营机构即可。

根据上述特点，设备生产商或设备运营机构还可以自行为设备生产数字证书，且分别为数字证书相应的身份信息进行背书。在提交区块链时，验证节点仅需要鉴别相应的设备生产商和运营机构的信息，通过之后将证书记录到区块链中。由于数字证书由用户自行产生，因此可以提高证书配置效率，解决批量配置问题。此外，在提交区块链进行验证时，还可以指定相应的参与节点或者通道进行验证，建立数字证书的信任域。

目前，ITU-T、GSMA、CCSA 等国内外标准组织均已开展针对区块链 PKI 领域的技术研究与标准制定工作。

4 基于区块链的数字身份关键技术

4.1 系统架构

图 4-1 展示了基于区块链的数字身份认证系统的技术架构，其中主要列出了数字身份认证系统所特有和必需的功能组件，未列出区块链系统所需的所有功能组件。

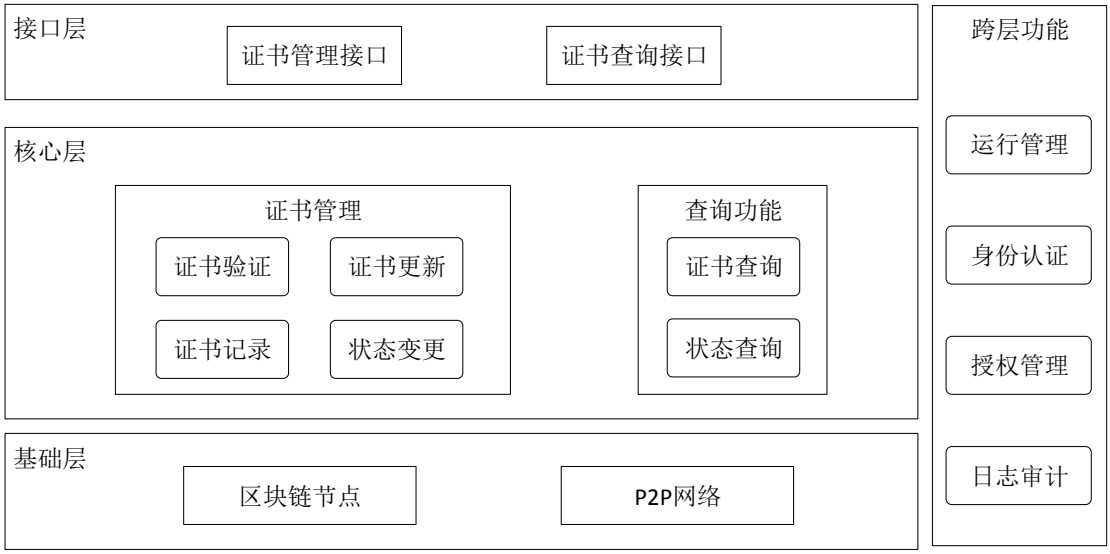

图 4-1 基于区块链的数字身份认证系统架构

各个层次和组件分别描述如下：

(1) 基础层

基础层提供区块链系统正常运行所需的硬件设备，以及之上的运行环境和基础组件，包括区块链节点和 P2P 网络两部分：

- **区块链节点**：提供系统所需的计算和存储资源，并提供共识算法和智能合约所需的处理和执行环境；
- **P2P 网络**：提供点到点之间的高效通信。

(2) 核心层

核心层主要提供数字证书管理及查询功能，证书管理功能包括：

- **证书验证**：验证数字证书的正确性，包括格式验证、公钥验证、ID 验证等内容；
- **证书记录**：将经过验证的数字证书发布到区块链当中，证书及其状态信息将记录到区块链中；
- **证书更新**：证书到期之前对证书进行更新，可分为密钥更新和有效期更新，证书更新信息经验证后，更新后的证书及其状态信息将记录到区块链中；
- **状态变更**：状态变更包括证书挂起、证书解挂，证书撤销，状态变更信息需要经过区块链节点验证，经验证后，变更后的证书及其状态信息将记录到区块链中。

查询功能包括：

- 证书查询：提供数字证书完整信息的查询功能。
- 状态查询：提供数字证书状态查询功能，获取证书的最新状态；

(3) 接口层

接口层主要提供与证书管理和应用相关的接口，具体包括：

- **证书发布及变更服务**：提供数字证书发布、证书更新、状态变更等功能；
- **证书状态查询服务**：提供数字证书状态查询和数字证书查询功能。

(4) 跨层功能

提供与系统相关的运行管理、身份认证、授权管理，以及日志审计相关的功能，主要包括：

- **运行管理**：提供对系统运行状态的监控，对异常问题的处置，以及对系统策略的管理等功能；
- **身份认证**：对用户身份进行验证的过程，以确认用户对资源访问和使用的权限；
- **授权管理**：授权用户访问和使用资源的权限的功能；

- **日志审计**：以安全的方式收集和维护系统运行相关的日志，支持对系统的审计管理。

4.2 组网方式

基于区块链的数字身份认证系统网络架构如图 4-2 所示。

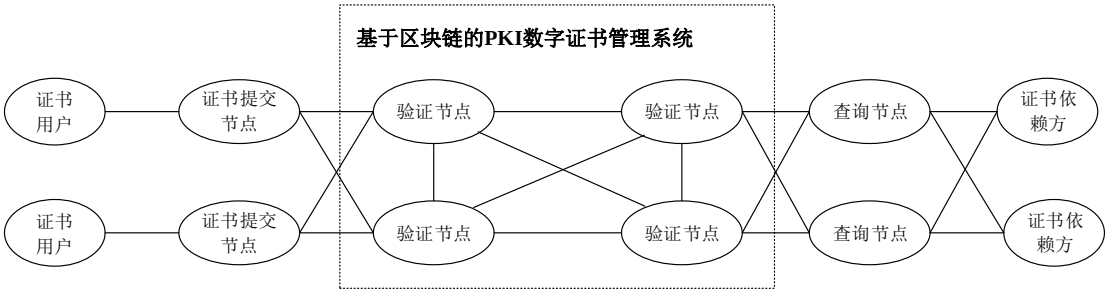

图 4-2 基于区块链的数字身份认证系统网络架构

如上图所示，其中包含证书用户、证书依赖方、证书提交节点、验证节点、查询节点，其核心是基于区块链的 PKI 数字证书管理系统。各角色的功能如下：

- **证书用户**：是数字证书的实际拥有者；
- **证书依赖方**：指的是信任证书系统的使用者；
- **证书提交节点**：用于向区块链系统提交数字证书发布请求，以及数字证书更新请求，证书提交节点是可信节点，证书提交节点负责对证书用户进行认证，确保提交证书的正确性，类似于传统技术中的 RA；
- **验证节点**：用于验证用户发布证书的合法性，验证用户提交的证书更新以及状态变更请求，产生新区块，验证节点可以由设备商、运营商、业务供应商，以及证书认证机构等担任，类似于传统技术中的 RA 和 CA；
- **查询节点**：用于提供数字证书状态查询服务。查询节点可以由具有公信力的机构承担，也可以由用户按需自行搭建，类似于传统技术中的 OCSP 查询服务。

4.3 数字证书管理

与传统 PKI 技术类似，基于区块链的 PKI 数字证书管理系统涉及证书发布

申请、证书发布、证书更新、证书撤销/挂起/恢复、证书使用等流程。

(1) 证书发布申请

数字证书在被记录到区块链系统之后才可被依赖方使用。证书在生效之前，证书用户首先向证书提交节点提交证书发布申请。证书提交节点对待发布的证书进行验证，对证书内容进行背书，并在提交区块链时对发布申请进行签名保护。

(2) 证书发布

区块链系统在接收到证书发布申请之后，通过验证证书发布节点签名、验证待发布证书内容（如 DN 项）与证书发布节点身份一致性等方式，对证书提交节点以及提交的证书进行验证，验证通过后在区块链中记录用户提交的数字证书以及证书状态。

(3) 证书更新

证书到期之前用户需要更新证书以保证证书使用的连续性。证书更新可不变更密钥，但从安全性考虑，应更新密钥。证书更新需要通过证书提交节点发起，证书用户使用原私钥对证书更新请求进行签名保护。

(4) 证书撤销

若发生私钥泄漏等安全事件，需要进行证书撤销。证书撤销由证书用户或者证书提交节点发起。

(5) 证书使用

在证书使用过程中（例如现有的 TLS、IPSec 等安全协议），证书用户将证书摘要或完整证书提交给依赖方，依赖方接收到证书摘要或完整证书后，向区块链证书查询节点查询证书及证书状态，验证证书的合法性和有效性。

(6) 证书查询

查询节点根据查询请求向证书依赖方提供证书及证书状态查询服务，该过程与 OCSP 类似。

4.4 数字证书格式

为了与现有技术兼容，推荐使用 ITU-T X.509 标准格式的数字证书，但可根据业务系统需要对证书格式进行优化。

(1) 证书序列号字段（Serial Number）

证书序列号由 CA 机构自行定义，要求在 CA 内部唯一，主要用于 CRL。但在采用自签名数字证书时，证书的状态记录在区块链当中，不再使用 CRL。此外，自签名证书由用户自行产生，引入序列号将引发序列号冲突。因此可对数字证书序列号字段进行简化。

(2) 签发者字段（Issuer）

签发者字段用于标识数字证书的签发者。若采用自签名数字证书，签发者字段与使用者主体名称字段（Subject）完全相同，此时可以进行简化。

(3) 有效期字段（Validity）

有效期字段用于标识数字证书的有效期。在区块链中，每个区块都有明确的产生时间。利用这一特点可以将证书记录到区块的时间作为有效期的起点，当证书因安全性或其他原因不再使用时，将证书状态变更为“撤销”，作为证书有效期的终点。通过此方式，有效期字段也可进一步进行简化。

(4) 基本约束（Basic Constraint）

证书的基本约束中“cA”标识位取值为“false”，以确保该自签名证书不是 CA

根证书[1]。

此外，还可采用更加简洁的方式，仅保留证书实体用户的 ID 与公钥信息，区块链系统提供用户 ID 与公钥的记录功能和查询功能。此时，用户与依赖方需要支持纯公钥的安全机制。

4.5 数字身份管理

数字身份可以分为实名身份和匿名身份。

实名身份指网络设备的真实身份，例如设备型号、硬件 ID、MAC 地址等物理属性，或者域名、IP 地址、网络标识等网络属性。实名身份的管理与传统 PKI 技术类似，证书提交节点负责对用户的身份进行验证，确保数字证书中的身份信息与证书用户的真实身份一致。物理属性由设备商提供和背书，网络属性由设备部署和运营机构分配和背书。证书提交节点在向区块链系统提交数字证书的同时，还需要提交用于证明用户身份的信息，验证节点将对这些信息进行验证。

匿名身份可以由用户自行产生，在证书中不含有用户的身份信息。证书中 Subject 的信息仅作为标识信息，对用户的身份验证在具体应用中进行。业务应用系统需要使用其他方式对用户进行身份认证（如用户名+口令、人工审核等方式），并将该证书和认证后的用户建立对应关系，此时该证书可用于对该用户的身份认证。此外，由于 DN（Distinguished Name，标识名）项中不含有证书用户的身份信息，有助于保护证书用户的隐私。

4.6 认证策略管理

在具体实现中，可以为不同的场景制定相应的认证策略，该策略将明确验证节点对证书的验证方式、验证内容及验证规则。例如，如果证书由设备商节点提交，则需要确保证书中 DN 项携带的设备商信息与证书提交节点一致；在证书内

[1] 证书基本约束“cA”是一个布尔型的变量，来自于 IETF RFC5280，有别于认证授权中心 CA。

容验证中，需要确保证书 DN 项的唯一性；针对自签名证书，需确保证书的基本约束中“cA”标识位取值为“false”，以确保该自签名证书不是 CA 根证书；此外，还可以定义验证节点验证成功的条件，比如大多数节点验证成功、全部验证节点验证成功、满足一定数量的节点验证成功等。

4.7 过期数字身份记录优化

区块链中通常包含所有的历史交易，随着交易量的增加，整个区块链所占用的空间会越来越多，对节点存储资源和计算资源的需求会越来越高，因此需要考虑系统节点因存储完整的区块链数据所占用的资源开销。

数字证书系统与货币交易系统相比具有一个显著特点，即数字证书具有有效期。电子货币交易涉及到交易的回溯与验证，因此需要有完整的历史交易数据。对于数字证书系统而言，数字证书在超过有效期或证书被撤销之后就不再使用，即使需要备份，其备份的时间期限要求也短于货币交易系统。

根据上述特点，可以对区块链系统的存储空间进行优化。具体方法为，如果某一区块中所有证书均已失效（已过期或被撤销），那么可以将该区块的区块体从区块链中删除，仅需保存这些区块的区块头。保留区块头可以保证整个区块链的完整性，删除区块体则可以减少区块链占用的存储空间，避免区块链存储空间无限制的增长，同时也可以提升对区块中数字证书的检索效率。

5 基于区块链数字身份应用案例

5.1 网络设备身份认证

在通信网中，有大量设备需要进行双向的身份认证。PKI 是一种常见的用于网络设备进行双向身份认证的技术，常用的协议有 IPSec 和 TLS 等。此时，设备管理员需要为这些设备申请并配置数字证书。在具体操作中，可以通过 CMP 等

在线方式进行数字证书的申请以及证书更新，也可以由设备商或运营商的管理人员向 CA 申请证书，之后将证书配置到设备中。这两种方式都需要向 CA 中心提交申请，之后等待 CA 中心的响应，直至获取到 CA 中心签发的证书以后，才可以将证书配置到设备当中。通信网中还存在大量设备不支持在线证书管理。对于这些设备，需要设备管理人员负责密钥的产生以及证书的配置工作，效率较低，还可能造成密钥泄露。

在基于区块链数字身份认证体系中，设备商可以在设备生产线产生和配置证书，在设备出厂或入网的时候，将设备的证书信息通过设备商节点上报至基于区块链的 PKI 数字证书管理系统。采用此种方式可实现大批量设备的证书配置，提升证书配置效率。

该应用案例涉及的网络架构如图 5-1 所示，其中证书提交节点是设备商节点、运营商节点、CA 机构节点，验证节点由设备商、运营商、CA 机构共同组成，每个节点仅能提交归属于自己设备的数字证书。具体操作流程如下：

1) 设备商为每个设备产生自签名数字证书，自签名证书中携带设备商信息，例如，在 DN 项中注明设备商名称，然后将自签名证书提交给证书提交节点；
2) 证书提交节点会验证数字证书的内容和设备身份，验证通过后向区块链系统发布证书发布申请，其中包括自签名数字证书，以及证书提交节点的签名信息；
3) 验证节点在接收到来自证书提交节点新提交的证书后，对证书格式及内容、以及签名信息进行验证。如果证书提交节点是设备商节点，还需确保证书中 DN 项携带的设备商信息与证书提交节点一致。验证节点达成共识后，将新提交的数字证书记录到区块链中。

利用通道的概念，证书用户即设备商在提交证书中还可以指定通道，将数字证书提交给相应的通道进行验证。此时，一个通道相当于一个信任域，数字证书将仅能在该通道中被信任和使用。在移动通信网中，许多网络设备不具备移动性，或者具备有限的移动性。因此，设备商可以与一个或多个运营商建立通道，在设

备入网之前，证书提交节点将设备证书提交给相应通道的节点进行验证，一方面可以实现按需选择数字证书的信任域，另一方面可以避免证书信息泄露给信任域之外的节点。

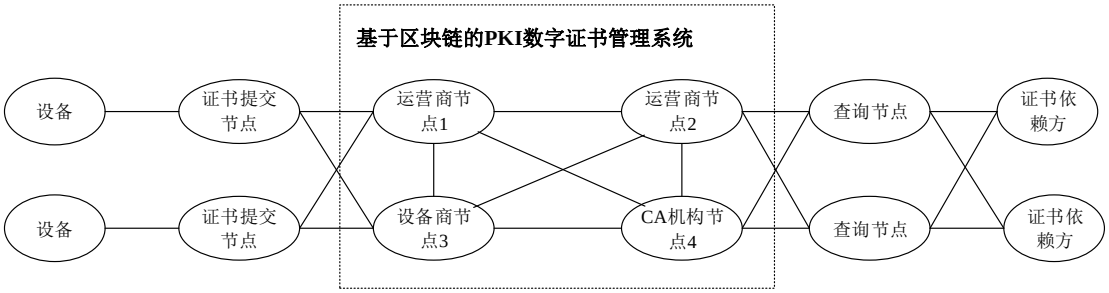

图 5-1 网络设备认证场景中基于区块链数字身份认证体系网络架构

网络设备在进行身份认证时，证书依赖方需要利用设备的数字证书，对证书的合法性进行验证。图 5-2 以常用的网络设备认证协议 IPSec 为例，描述了网络设备与网关之间的认证流程，主要过程如下：

1) 网关接收到设备提交的数字证书后，向区块链数字证书查询节点查询设备证书状态；
2) 区块链数字证书查询节点查找证书最新状态，并反馈给网关；
3) 网关根据证书状态进一步验证设备证书的有效性，验证通过后执行后续步骤。

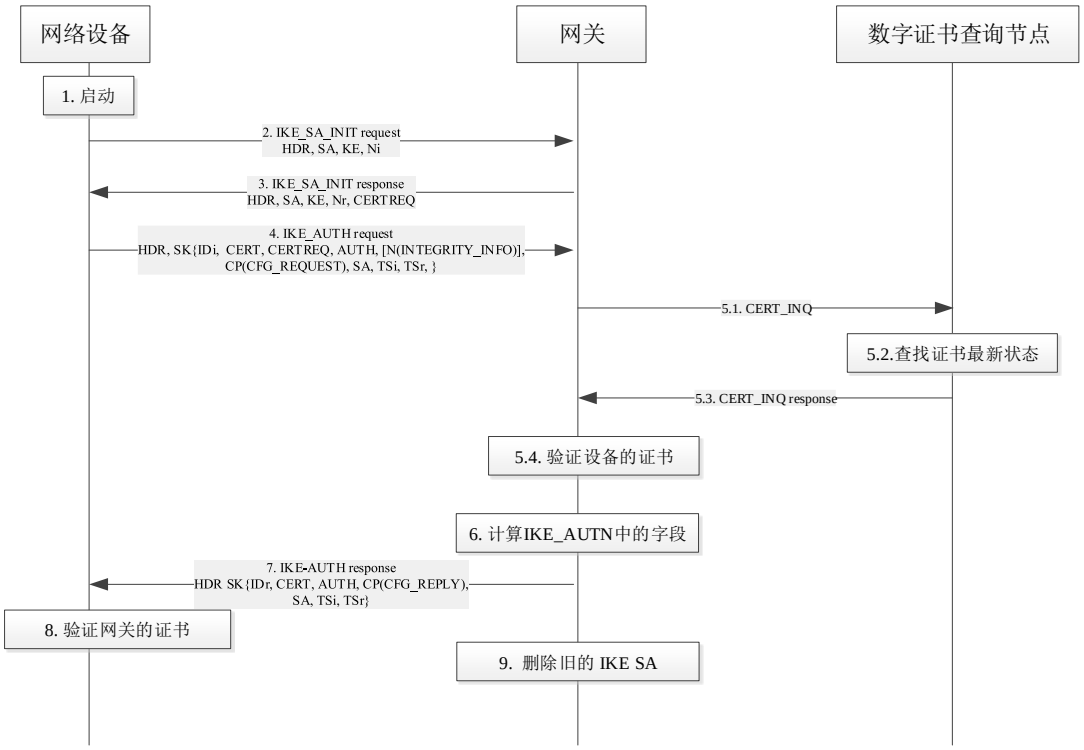

图 5-2 基于区块链数字身份认证体系的设备认证流程

5.2 跨 CA 证书互信

CA 根证书是 PKI 技术的信任锚点，只有信任某个 CA 根证书，才能信任该 CA 签发的数字证书。为了解决多 CA 互信问题，多个 CA 机构可以加入区块链建立联盟。用户在提交证书申请时，由基于区块链 PKI 数字证书管理系统中多个 CA 节点进行验证。这样，依赖方只要信任其中任何一个 CA，就信任区块链 PKI 数字证书管理系统的中所有证书，从而实现多个 CA 证书的互信。

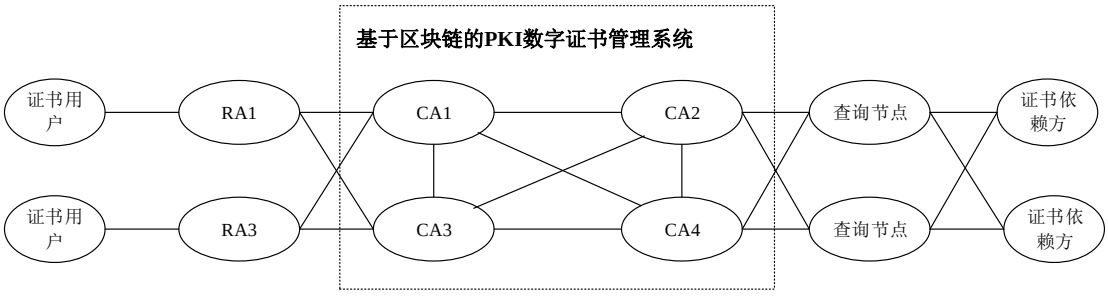

图 5-3 多 CA 互信场景中基于区块链的数字身份认证体系网络架构

此应用场景中，用户证书由传统 CA 机构签发，证书提交节点由 CA 机构的

RA 或 RA 代理承担，验证节点由各个参与的 CA 机构承担，网络架构如图 5-3 所示。证书申请及发布流程如下：

1) 证书用户向证书提交节点提交证书申请/证书更新/证书撤销等证书管理请求，所属 CA 机构依据自己的策略对证书用户的身份和证书请求进行鉴别。鉴别方式与 CA 机构传统鉴别方式相同；
2) 鉴别通过之后证书提交节点所属 CA 机构为用户签发证书/签发更新后的证书/撤销用户证书，并且向区块链系统发送证书发布请求/证书更新请求/证书撤销请求；
3) 上述证书发布请求/证书更新请求/证书撤销请求经过其他 CA 节点共识后，证书信息将以新区块的形式记录到区块链系统中。记录到区块链系统中的证书将被所有参与的 CA 机构认可；
4) 依赖方在接收到用户证书之后，首先验证该证书是否由自己信任的 CA 机构签发。若是，则可在本地采用传统方式进行验证；否则，可向区块链数字证书系统查询证书及其状态。

采用此方式时，由于不同 CA 机构的认证策略不同，因此传统方式中的认证策略不再适用，可为基于区块链的数字身份认证系统制定认证策略。

5.3 适配 TLS/DTLS 协议

对于支持 PKI 能力的物联网设备，可采用本技术方案提升 PKI 技术的应用效率，提高证书配置效率，并且可节约认证过程中的带宽资源。

设备商可在物联网设备生产阶段自行产生和配置证书，在设备出厂或入网的时将设备的证书信息发布至基于区块链的 PKI 数字证书管理系统。

设备认证过程中，可采用 TLS/DTLS 等安全协议，但采用上述协议需要向认证方传输完整的数字证书。利用本文的技术方案，可通过传输证书标识信息代替完整的数字证书，节约带宽资源。图 5-4 以 TLS 协议为例，介绍了基于区块链数字认证体系的物联网设备认证流程。

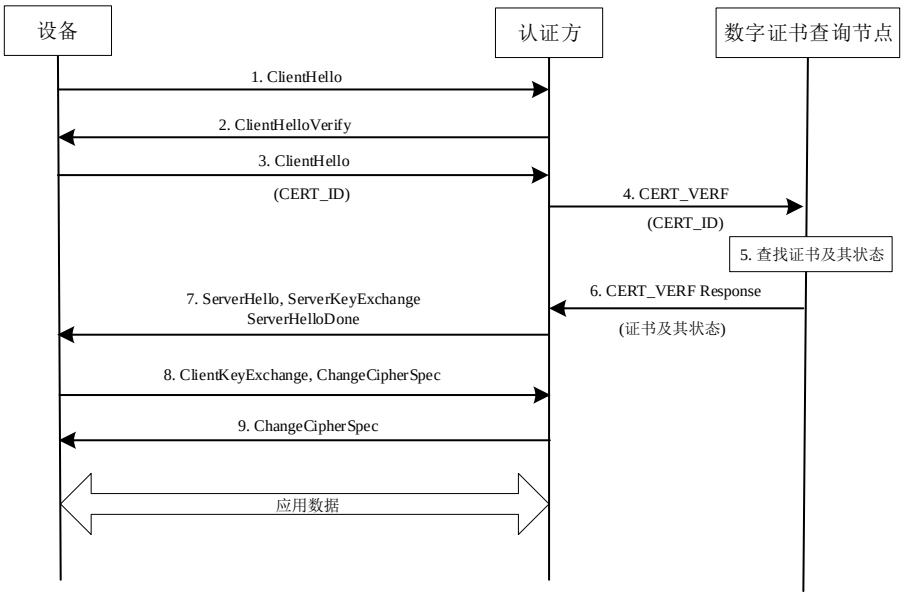

图 5-4 基于区块链数字认证体系的物联网设备认证流程

该图中设备与认证方之间的交互遵循标准的 TLS 协议，在步骤 3 的 ClientHello 消息中，携带设备证书标识信息取代完整的设备证书，以节约带宽资源。认证方在接收到设备提交的证书标识信息（CERT_ID）之后，向区块链数字证书查询节点查询证书（步骤 4）。查询节点根据证书标识信息查找相应的证书及其状态，并将证书及状态返回给认证方（步骤 5 和步骤 6）。之后，认证方根据证书及其状态对设备进行认证，并进行后续 TLS 握手流程。

5.4 智能硬件数字身份管理

在智能穿戴、智能交通、智能家居、医疗、机器人等领域，智能硬件有着巨大的应用需求。为了实现对智能硬件设备的身份认证，可以在这些设备中配置唯一的身份标识信息。PKI 数字证书是最常用的身份标识方式之一。通常有两种证书申请方式：一种是设备商自建 CA，为自己的设备签发数字证书；另一种是向第三方 CA 机构购买数字证书。第一种方式需要设备商建设并维护一套 CA 系统，且这套 CA 签发的证书很可能不被其他机构信任，为了被其他机构信任，还可以与第三方 CA 机构进行桥接。第二种方式实现简单，但购买数字证书的成本较高。

利用区块链数字身份管理技术，设备商可以为设备配置相应的自签名证书，通过证书提交节点将自签名证书上传至区块链数字身份认证系统。该证书通过区块链节点共识之后记录到区块链中，被系统参与节点所认可。在提交至区块链时，设备商还可以选择区块链中的节点或者通道所组成的信任域，将数字证书发布至相应的信任域中。设备商无需自建 CA，也无需向第三方 CA 机构购买数字证书，可降低 PKI 技术的应用成本，还可以灵活选择信任域。

在设备进行身份认证过程中，依赖方可以利用区块链数字身份认证系统对设备的身份进行认证。具体可以采用 DTLS/TLS/IPsec 等标准协议，也可采用其他协议，依赖方仅需在证书状态查询环节向区块链节点发起查询，其他过程与传统 PKI 机制相同。

5.5 软件/服务的数字身份管理

在微服务软件架构中，一个大型应用程序和服务可被拆分为数十个微服务。微服务通过扩展组件来处理功能瓶颈问题。开发人员只需要为额外的组件部署计算资源，可以更有效地利用计算资源。微服务另一个特点是更快且更容易更新，当开发者对应用程序进行变更时，可以更新应用程序的单个组件，而不会影响其他的部分。由于这些特点，微服务得到越来越多的应用。

为了实现微服务之间的调用，这些微服务需要正确地发现与识别，首先服务向服务注册中心进行注册，还可以向服务注册中心进行服务查询，从而获取其他服务的信息，实现服务调用。为了实现不同服务之间的安全调用，服务注册中心可以作为区块链数字认证系统中的证书提交节点。每个服务可以在向服务注册中心注册时，向其提交自己的数字身份证书。当其他服务调用该服务时，可以在区块链中查询身份证书的有效性。具体如下：

1) 服务注册中心可作为证书提交节点，或者通过其他证书提交节点连接至区块链数字身份认证系统；
2) 服务 A 可以产生与自己身份相一致的身份证书，该证书可以由 CA 机构

签发，也可以是自行产生的自签名证书；

3) 服务 A 在向服务注册中心进行注册时，提交自己的身份信息以及证书信息。如果证书中的身份信息正确，那么服务注册中心将该身份以及证书提交至区块链数字认证体统，由系统中的验证节点共同验证证书的正确性，并将经过验证的证书记录到区块链中；

4) 服务 B 在调用服务 A 时，服务 A 将提供自身的证书信息，服务 B 向区块链系统查询证书的正确性与有效性，对服务 A 进行验证，并可以利用经过验证的证书建立安全通信连接。

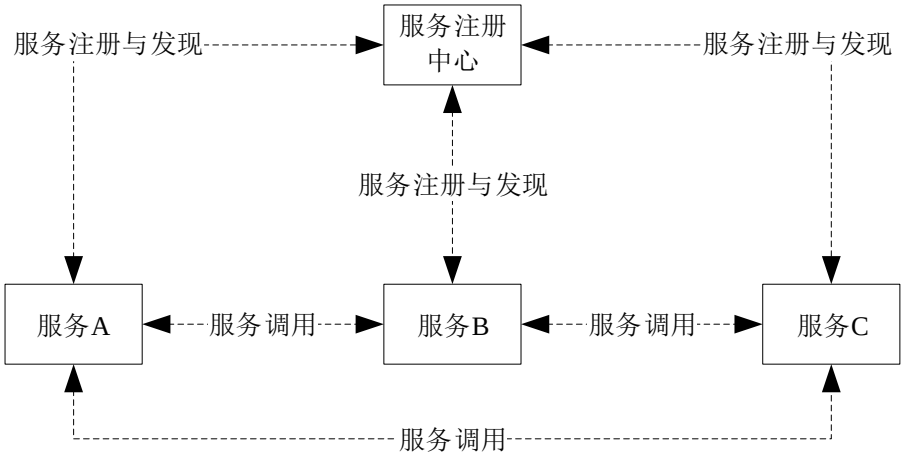

图 5-5 微服务注册、发现与调用过程示意图

6 总结与展望

6.1 优势与挑战

较传统 PKI 数字证书认证相比，基于区块链的解决方案具有如下优势：

1) 可以在设备生产线批量产生和配置数字证书，提高数字证书配置的效率和安全性；

2) 将数字证书产生过程与建立信任域的过程解耦，证书用户可以灵活地按需建立信任域；

3) 可以实现多个 CA 机构之间的互信；

4) 设备商无需建设和维护 CA 系统，降低成本；
5) 在内网和互联网边界部署查询节点，可以解决内网设备无法使用 CRL/OCSP 服务的问题，同时可以提高查询效率；
6) 查询节点分布式部署，可避免传统解决方案中的 CRL/OCSP 单点故障问题。

与此同时，基于区块链的解决方案也面临一些限制与挑战：

1) 需要为区块链解决方案制定证书策略，其中包括背书和验证策略等内容，且不同通道、不同的信任域可能采用不同的证书策略；
2) 自签名数字证书仅能够用于信任域内的身份认证，不能用于签名；
3) 区块链技术自身仍在发展当中，其安全性将影响数字身份认证系统的安全性。

6.2 技术展望

基于区块链的数字身份技术的愿景是设备、终端、软件、服务、应用天生自带身份、自成秩序，构建更加安全、可信的数字世界。

（1）基于分布式信任环境，构建安全基础设施

区块链的分布式、不可篡改、可信追溯等安全特性为万物互联时代下的数字身份管理提供了分布式信任基础。在基于区块链的数字身份认证体系之上，构建去中心化的安全基础设施，促进设备商、供应商、终端用户等多参与方之间的身份管理与数据共享，实现不同设备、不同参与方之间的任务协同。

（2）加快技术融合，建立更广泛的信任交互关系

随着 5G 的逐步应用普及，物联网、车联网、工业互联网、无人驾驶、智慧城市等领域将发生深刻变革。区块链将为设备与设备之间的大规模协作提供信任支撑。区块链与新一代信息技术的融合，将更有助于实现分布式网络下的身份认证，建立更广泛的信任交互关系，加速应用场景落地。

（3）跨域互联，区块链助力信任体系演进

在分布式网络基础上，区块链以块链式结构聚集身份证书，以共识同步的形式共享不同信任域的证书信息和信任链，为实现跨域身份认证提供了便捷条件。在基于单一联盟链的身份认证管理系统的基础之上，推进区块链与传统 PKI 和标识密码体系、区块链与区块链之间的跨域信任互联，助力数字身份信任体系的演进。

缩略语列表

缩略语	英文全称	中文含义
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G	5th Generation	第五代（移动通信网络）
CA	Certification Authority	认证授权中心
CCSA	China Communications Standards Association	中国通信标准化协会
CMP	Certificate Management Protocol	证书管理协议
CRL	Certificate Revocation List	证书撤销列表
DN	Distinguished Name	标识名
GSMA	Global System for Mobile Communications Association	全球移动通信系统协会
IP	Internet Protocol	网际互连协议
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector	国际电信联盟电信标准分局
MAC	Media Access Control	媒体存取控制
OCSP	Online Certificate Status Protocol	在线证书状态查询协议
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构
TLS	Transport Layer Security	安全传输层协议

参考文献

[1] GB/T 20518-2018, 信息安全技术 公钥基础设施 数字证书格式[S]. 2018.

[2] 3GPP TS 33.320, Security of Home Node B (HNB) and Home evolved Node B (HeNB) [S].

[3] 3GPP TS 33.310, Network Domain Security (NDS); Authentication Framework (AF) [S].

[4] ITU-T X.509, The Directory: Public-key and attribute certificate frameworks [S]. 1997.

[5] IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [S]. 2008.

[6] GSMA SGP.21, RSP Architecture [S]. 2017.

[7] GSMA SGP.22, RSP Technical Specification [S]. 2017.

[8] 中国通信标准化协会. 基于区块链的数字证书管理技术研究[S]. 2019.

[9] 阎军智, 彭晋, 左敏等. 基于区块链的 PKI 数字证书系统[J]. 电信工程与技术标准化. 2017.11:16-20.