DIDA

《DIDA白皮书》

分布式数字身份产业联盟

2020年8月

前 言

本白皮书参与编写的单位（排名不分先后）：北京百度网讯科技有限公司、微众银行、溪塔科技、中钞区块链技术研究院、飞天诚信科技股份有限公司、国家金融 IC 卡安全检测中心、腾讯云计算(北京）有限责任公司、浦发银行、亿联银行。

本白皮书主要编写人员（排名不分先后）：张开翔、韩丹、汪佳伟、李璇、王玉操、张亚宁、卢缃梅、平庆瑞、潘镥镥、曾梓杰、张利琴、刘雅静、杨波、张彦超、刘江、刘鑫、黄超、郭林海、马文婷、张增骏。

本白皮书的评审专家（排名不分先后）：蔡吉人（中国工程院院士，国家信息化专家咨询委员会委员）、陈静（国家信息化专家咨询委员会委员，中国人民银行科技司原司长）、李京春（中国信息安全标准委员会(TC260)安全评估组(WG5)组长，中国信息协会信息安全专委会副主任委员）、马智涛（微众银行副行长兼首席信息官）、詹榜华（北京数字认证股份有限公司董事长，北京商用密码行业协会会长）、徐恪（清华大学计算机系副主任）。

目 录

第一章 联盟定位，愿景，目标，计划

分布式数字身份产业联盟（DID-Alliance，简称 DIDA）由中钞区块链技术研究院与飞天诚信科技股份有限公司共同发起，联合百度、国家金融 IC 卡安全检测中心、杭州城市大脑有限公司、杭州银行、京东数科、浦发银行、奇安信、山东区块链研究院、腾讯云、微众银行、西安大数据、溪塔科技、亿联银行、中国电信研究院、中国银联电子支付研究院（排名不分先后）成立的非营利性社会组织。联盟秉持“让数字世界互信互连”的基本愿景，以“共建分布式数字身份基础设施，打造可信开放数字新生态”为联盟主要使命。

“身份”与每个人都息息相关，人们都在不同的地方拥有不同的身份属性，身份即一个人所有的属性和行为的集合。在现实生活中，我们拥有身份证、护照、驾照、企业工牌等，在以往，我们使用这些有着物理介质、或者部分电子化的凭据形式给出身份证明，但在互联网这个的大环境中，如何构造合理并可信的身份证明关系，使其具备数字化、网络化的特质，是值得探讨的课题。

另一方面，目前的互联网应用尚未脱离互信互通的困境，数据孤岛和数据滥用的问题依旧存在。随着新基建等浪潮推动，价值互联网是进化的方向，人们日益重视隐私保护，数据成为生产要素，于是身份和相关凭据、数据的可信互通成为迫切的需求。

我们认为，在政策、技术和市场的共同驱动下，分布式数字身份技术终将成为数字化进程的必然选择。联盟的工作目标是希望最大化地挖掘分布式数字身份技术的潜能，推动互联网技术的发展，促进分布式数字身份技术与现有生态的融合。

DIDA 将从以下四个方面入手开展工作：

深入研究分布式数字身份技术。联盟将致力于了解、跟进全球分布式数字身份的最新动态，深入研究包括去中心化公钥基础设施（DPKI）、密码学、凭证在内的各项核心技术，探索分布式数字身份的多种技术演进路线，促进分布式身份技术的交流与传播。

促进分布式数字身份的行业应用。作为我国分布式数字身份行业中领先的产业组织，联盟致力于探索分布式数字身份的应用场景，搭建合作交流平台，组织产、学、研开展合作，在促进成员共同发展的同时，为社会提供基于分布式数字身份的跨域协同项目示范。

搭建中国的分布式数字身份网络。全球分布式数字身份网络以互联互通作为目标，联盟将参考国际最佳实践，结合国内厂商搭建的基础设施，通过提供开源工程、制定规范等方式，促进中国分布式数字身份网络的落地和互联互通。

与国际分布式数字身份接轨。作为本土企业与国际数字身份联盟和标准化组织的桥梁，联盟致力于加强国际间交流与合作，一方面，促进分布式数字身份相关国际标准的带入和本土化，另一方面，通过国际间项目合作促进全球互联互通的确认和发展。

第二章 行业现状分析

情报和市场研究平台 MarketsandMarkets 最新报告中指出，2019 年全球数字身份解决方案市场规模达到 137 亿美元，到 2024 年，该市场预计将增长至 305 亿美元，预测期内（2019-2024 年）的年复合增长率（CAGR）为 17.3%。

在分布式数字身份诞生之前，人们的身份信息其实或多或少已经数字化，但数字化不意味着网络化、可信任，以及可以便捷且合法合规的互联互通。本节从观摩行业现状开始，并展望分布式数字身份的发展。

2.1 现有数字身份痛点分析

从我们熟悉的互联网业务来看，用户的身份和数据已经一定程度上数字化和网络化，互联网公司通常也具备一整套处理认证和访问控制的业务系统。出于便利性考量，大多数互联网应用的数字身份以用户名密码为主，并结合真实身份认证完成实名验身。互联网的账户体系通常从属于应用领域，如社交、电商等领域分别采用不同账号，这就使得用户要重复注册很多的账号密码。

其次，出于运营主体和运营壁垒考量，互联网业务在应用层面并不互联互通，跨应用的业务实现难度很大，尤其对于需要用户确权操作的跨应用业务，可能需要更改整个业务架构，以使得不同应用领域的用户身份。

互联网巨头依靠平台效应垄断市场，利用用户数据作为护城河，产生了大量价值，但用户对自己的数据并未拥有话语权和价值收入。用户的数字身份的关键控制点即账号密码，由服务商控制，对用户来说，仅为租借和使用服务商的服务，服务商可以决

定账号禁用、服务终止，更进一步，由于利益驱使，围绕着用户数据发生的非法收集、数据泄露和买卖行为防不胜防，损害用户安全。

随着数字社会的发展，金融、政务、交通等实体经济领域也融合了大量的互联网因素，其原有的、基于物理介质和实体身份的认证体系在进化过程中，已经遭遇互联网服务类似的问题，由于实体经济的地域性特征更浓，安全等级要求更严，蕴含的价值更高，隐私挑战更大，事关国计民生，所以，身份认证带来的问题会更加突出。

综上所述，我们将其归结到三个痛点问题：

1、重复认证、多地认证的问题

例如，在金融场景下，同一公民去不同的银行开户需要分别进行 KYC，用户体验繁琐，身份数据相互重叠，数据可能存在差异甚至冲突。多头建设的身份体系在浪费资源的同时，也存在诸多数据共享和使用上的障碍，不同企业主体间的数据信息分别存储，无法综合利用。

2、身份数据隐私与安全问题

用户身份信息散落在各个企业级的身份认证者手中，用户对自身信息的使用不够审慎，或者企业对用户身份进行信息验证都会引发身份信息的暴露，甚至对用户隐私信息造成严重侵犯。其次，用户身份信息在各家企业的服务器上存储，不同的企业对数据安全的重视程度和措施强度不同，使得用户的数据泄漏是一个木桶效应的问题，任何一处被攻破，用户的隐私即被泄露。用户个人信息维护成本昂贵。数据显示，欧盟地区，仅英国每年的身份确认成本已经超过 33 亿英镑，约等于 290 亿人民币。

3、中心化认证效率和容错性问题

在传统的 PKI 系统中，数字证书是认证的核心，它由相对权威的 CA 机构签发的。一方面，这种中心结构可能存在性能问题，其涉及证书的所有操作，任务繁重，可能

成为性能短板拖累效率，如庞大的已撤销证书列表的有效分发。另一方面，单中心的结构容易使其成为攻击的目标，一旦上级 CA 机构被攻破，则与之相关联的下级 CA 也会受到牵连。

2.2 分布式数字身份标准

2.2.1 分布式数字身份介绍

在政策、技术、市场因素的共同驱动下，产生了一种新的数字身份形态——分布式数字身份，它用分布式基础设施改变应用厂商控制数字身份的模式，让用户控制和管理数字身份，通过将数据所有权归还用户从根本上解决隐私问题。

要使身份具有真正的自我主权，这种基础设施必然需要驻留在分散信任的环境中。区块链技术的出现让自我主权身份的实现终于找到了突破口，作为分布式体系里的代表性技术，区块链有望成为分布式数字身份的技术基础。区块链技术用哈希链的数据结构改变了电子数据易被篡改的属性，用“区块+共识算法”解决分布式系统的数据一致性问题，拜占庭容错能力保证跨实体运行的系统不受少数节点恶意行为的影响，从而解决业务层面的信任难题，有望在服务商之间搭建互联互通的协议。

W3C 提出了基于区块链的分布式数字身份 DID 的概念，分布式数字身份具有以下优势：

1）安全性：身份所有者身份信息不被无意泄露，身份可以由身份持有者持久保存，身份信息提供可符合最小披露原则；

2）身份自主可控：用户可以自主管理身份，而非依赖可信第三方；身份所有者可以控制其身份数据的分享。

3）身份的可移植性：身份所有者能够在任何他们需要的地方使用其身份数据，而不需依赖特定的身份服务提供商。

当然，区块链技术只是用于实现分布式数字身份的基础技术之一，分布式数字身份的版图中无论是技术、生态还是行业法规还有更广泛的内涵和外延。

2.2.2 分布式数字身份主流协议与规范

正如互联网建立在 TCP/IP 等协议提供的网络连接能力上，分布式数字身份也建立在一系列为互联网身份而定制的协议规范基础上。

国际电子技术委员会对“身份”的定义是“一组与实体关联的属性”，分布式数字身份也不例外，W3C 的 DID 规范和可验证凭证规范分别定义了代表实体的身份标识符及与之关联的属性声明，其共同支撑了分布式数字身份基础模型——可验证凭证流转模型的有效运转。

图 1-分布式数字身份基础模型——可验证凭证流转模型

分布式数字身份主要规范作为对可验证凭证基本模型的支撑，尤其是对于 DID 层面的信任框架的保障，通过 DKMS、DID-Auth、DIDComm 等一系列协议和标准，提供了分布式数字身份自主可控、可信交换、隐私保护等特点。

2.2.3 分布式数字身份的支撑体系

为了使人们能够随时、随地使用分布式数字身份，且具有良好的用户体验和丰富的应用场景，需要一系列基础设施来支持。

自底层向上，用户分别需要分布式账本提供对身份自主权的支持、代理组件提供用户管理身份和与其它实体通信的工具、凭证应用工具提供用户身份凭证流转支持。此外，当用户数据使用云存储代替本地存储时，还需要个人数据存储组件提供安全的数据管理服务。

2.2.4 分布式数字身份主流国际组织与应用场景

2.2.4.1 分布式数字身份主流国际组织

分布式数字身份出现的历史虽短，但发展速度快，受到了极高关注。 目前国内外已经问世的和分布式数字身份相关的项目已经超过 200 个，其中一部分加入了 DIF（https://identity.foundation/）即分布式数字身份基金会，该基金会旨在推动基于区块链的分布式数字身份管理协议的通用化和标准化。DIF 成员包括 IBM，微软，NEC，埃森哲，区块链组织超级账本，R3，以太坊企业联盟，金融机构 MasterCard，国内也有多个组织加入，如微众银行等。

W3C 组织的 DID 工作组成立于 2019 年 9 月，主要任务是制定 DID 规范，DID 规范包括对 DID URL 方案标识符、数据模型、DID 文件语法等的标准化。截至目前，该工作组已有来自全球的多个机构，包括 GS1、微软等，以及国内的工信部信通院等。目前 DID 的规范和技术方案已经初步成型，W3C 的 DID 规范

（https://w3c.github.io/did-core/）和相关协议认可度较高，是行业采用的主要参考，其他还有基于以太坊的多个 EIP 提案的实现，在工业物联网层面，也存在 Handle，Ecode 等多种标识规范。各项规范和协议在设计思路、细节风格上虽然有一定的差异，其核心都是为了解决身份标识、权威认证、可信验证、高效互通、隐私保护等核心问题。

目前在 W3C 的 DID 注册表中已注册了 50 多个厂家的 DID method 实现，在应用落地的过程中，通常针对不同场景中的不同需求采取了不同的实现方案。我们将介绍基于 W3C 组织 DID 协议规范的海外主要应用场景与案例，通过对这些应用场景与具体案例的分析，有助于我们理解不同分布式数字身份方案的价值。

2.2.4.2 可验证企业网络

- VON

VON 全称 Verifiable Organization Network，即可验证企业网络，是 Sovrin 协议的开源项目 Hyperledger Indy 的应用。该项目是加拿大不列颠哥伦比亚省政府关于实现可分享企业（组织）数据的开放、统一和可信网络的一项探索，该网络通过流转有关企业资质的可验证凭证，减少了那些需要和请求企业（组织）数据的应用服务的人们的工作量，因为基于 VON 可以从受信任的来源轻松获得这些数据。VON 为政府数字服务提供者提供了极大改善其用户服务体验的可能性。

2.2.4.3 分布式数字身份管理

- ShoCard

ShoCard 是较早尝试分布式数字身份管理的项目，它利用分布式账本为用户绑定标识符和现有的可信凭证（如护照、驾照），记录验证历史，为用户提供分布式的可信身份。旅行者使用移动终端对身份证件拍照，将元数据加密存储在本地，将可验证信息存证于区块链，当用户出示证件进行验证时，身份验证方除了验证物理证件，还可验证区块链记录。

- **IdentiCAT**

2019 年 9 月，西班牙加泰罗尼亚自治区政府宣布启动用户主权的分布式数字身份项目 IdentiCAT，这是欧洲第一个开放的数字身份。IdentiCAT 提倡用户控制自己的数字身份和相关数据，构建在分布式账本基础上，居民通过自己的软件管理数字身份，维护隐私。

- **瑞士楚格市居民数字身份 Zug Digital ID**

从 2017 年 9 月开始，瑞士楚格市为全市约 30,000 公民提供分布式电子身份 eID，该身份基于去中心化身份平台 uPort 在以太坊区块链（Ethereum）上实现，eID 的所有者可以使用移动应用程序提供身份信息，依赖方可以通过区块链检查数字签名来验证数据的真实性。所有个人数据仅存储在单独的移动电话上，经过加密，公民完全可以控制要发布的信息以及向谁发布的信息。eID 可以用于多个城市特定服务，例如城市公共事物公民投票，城市共享自行车 AirBie 服务等。

- **Thales Gemalto’s Trust ID Network**

Thales Gemalto’s Trust ID Network 是一个基于区块链的分布式数字 ID 平台，基于 R3 区块链平台构建，允许服务提供商简化客户身份管理和简化尽职调查流程，支持最终用户完全控制自己的身份。作为数字身份系统，它引入多个 ID 验证源，并符合数

据隐私合规性要求，可用于构建一个国家身份计划，或者在行业内部形成联盟身份计划。

2.2.4.4 KYC 客户身份分析

- **Synechron’s Self-sovereign KYC**

Synechron 设计和构建的 CorDapp 在 Corda 区块链中网络支持了交换和管理客户的 KYC 数据，39 个实体在 Microsoft Azure 区块链服务平台中部署并总共运行了 45 个节点。银行参与居多，包括荷兰银行，阿尔法银行，塞浦路斯银行等。银行可以在区块链网络上请求访问客户的 KYC 测试数据，而客户可以批准请求并撤消访问权限。客户还能够更新其身份数据，然后自动对所有具有访问权限的银行进行更新。

- **韩国的 NongHyup（NH）银行区块链 ID 卡**

韩国的 NongHyup（NH）银行已经引入基于区块链的移动 ID 系统，新的移动 ID 系统基于区块链技术，通过智能手机（而非传统的 ID 卡）实现方便的身份验证。该项目旨在有效保护其个人身份数据的前提下，面向个人提供更好的服务：基于区块链的 ID 服务将用于通勤和管理进入办公室的访问权限，将来，计划扩展移动 ID 卡，使其方便设置服务的约会和付款。

- **加拿大银行分布式数字身份**

加拿大一些领先的银行正在支持新的基于区块链的数字身份网络。由多伦多的 SecureKey Technologies 开发，Verified.Me 结合了在线银行凭证，生物识别技术和移动运营商有关人们手机的信息，以进行多因素验证。CIBC，Desjardins，RBC，Scotiabank，TD，BMO（蒙特利尔银行）和加拿大国家银行等多家加拿大银行都在支持这项服务。

该服务利用了 Telus，Bell 和 Rogers 拥有的合资公司 EnStream 的数据，这些数据提供有关与用户智能手机有关的因素的身份信息。该服务可以帮助明显改善客户体验，并满足 KYC 和反洗钱（AML）的义务。

- **阿塞拜疆中央银行分布式数字身份**

阿塞拜疆中央银行表示，2020 年第一季度阿将采用基于区块链的数字 ID 系统。该系统在转移到信贷组织的个人数据的安全性以及远程处理大多数操作方面具有广阔前景。在初始阶段，阿塞拜疆中央银行（CBA）将为法人和个人开设远程帐户；在最后阶段，该项目的目标是将其他银行服务和自动化的资金监控系统包括在内，以防止恐怖主义融资和洗钱。CBA 指出，采用该系统的直接结果将是“将 CBA 转变为开放银行业务”。

2.3 分布式数字身份整体框架

分布式数字身份一般采用多层框架，如下图是一种典型的分布式数字身份三层架构。

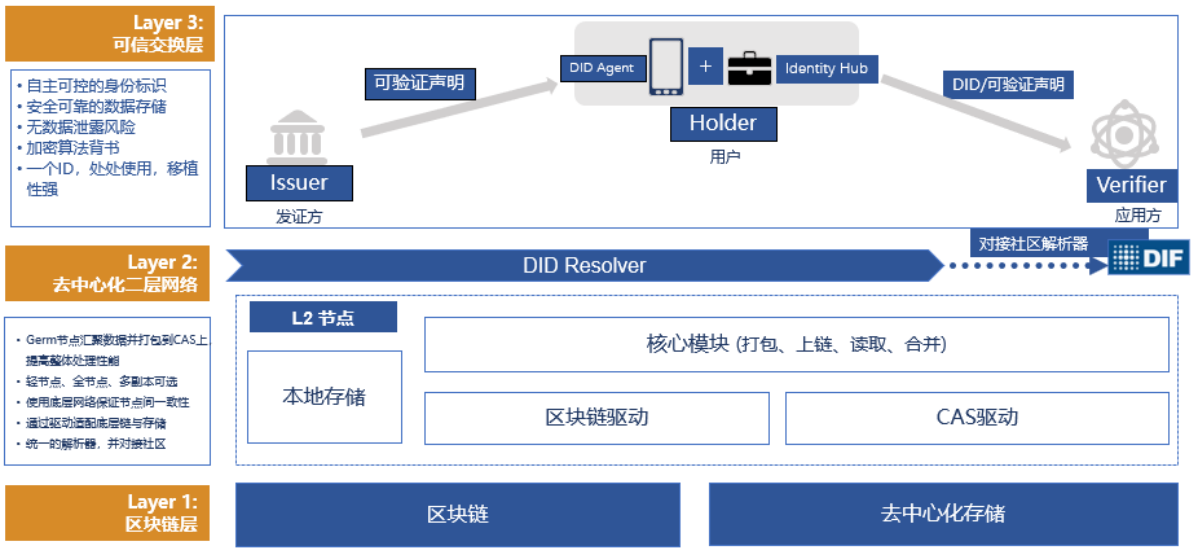

图 2-分布式数字身份三层架构

2.3.1 分布式账本层

分布式账本层是整个方案的基础设施，提供了对 DID 文档（DID Document）以及其他需要分布式存储内容的数据存储锚定。DID 文档可以直接通过区块链网络存储，在对数据隐私关注更高的情况下也可以结合分布式存储使用，DID 文档内最关键的是 DID 与公钥的对应关系，通过区块链锚定这些身份数据的对应关系。

2.3.2 DPKI 网络层

构建分布式数字身份体系，要满足大规模的数字身份使用场景，需要建立一个大型的服务系统。而一般的区块链网络受限于性能和扩展性，无法满足上层业务场景使用需求，因此在分布式账本层的基础上，可以进一步抽象出 DPKI 二层网络，通过分布式的二层网络解决区块链的扩展问题。

DPKI 网络层对上层提供了统一的 DID 解析服务，即 DID Resolver，此服务可以同时对接例如 DIF 社区等不同的 DID 生态，保证 DID 生态间的互认。

DPKI 节点会把上层的 DID 相关的操作打包，创建一个链上交易，并在交易中嵌入该操作批次的哈希，从而提高系统的整理处理性能。使用 DPKI 节点也可以隔离上层业务对底层区块链存储的差异性，对业务层和存储层进行解耦。

2.3.3 可信交换层

可信交换层是 DID 系统中各个生态参与方互相建立安全身份认证与数据交换层，从角色上一般会分为用户、发证方、验证方等。用户通过用户代理(User Agent)注册链上身份获得 DID，并依托 DID 向发证方申请各类可验证凭证，最终向验证方提供 DID 和可验证凭证完成验证流程，典型的身份验证流程如 DID-Auth 等。

第三章 主流 DID 协议和规范

近年来，围绕分布式数字身份，由多个标准组织、开源社区、分布式数字身份联盟共同努力，推进了一系列分布式数字身份相关技术标准和协议的制定，主要包括：

- 万维网联盟(W3C)推动中的分布式标识符(DID)和可验证凭证(Verifiable Credential)规范
- 重启可信网络（RWOT）工作组的 DID Auth 规范
- 结构化信息标准促进组织（OASIS）的 分布式密钥管理 DKMS 规范
- 去中心化身份基金会（DIF）推动中的 DIDComm 协议

分布式数字身份主要规范是对作为对可验证凭证流转基本模型的支撑，尤其也是对于 DID 层面的建立分布式数字身份信任框架的保障，为应用间的互联互通提供共同的数据格式、通信协议等前提条件。

3.1 DID（W3C）

基于区块链技术的分布式数字身份是 一种自我主权的、可验证的、新型数字身份。W3C 为这种身份定义了“分布式数字身份标识符规范”（Decentralized ID, DID）——一种新型的全球唯一标识符。

分布式标识符（DID）的用途包括以下两个方面：其一，使用标识符来标识 DID 主体（人员，组织，设备，密钥，服务和一般事物）的特定实例；其二，促进实体之间创建持久加密的专用通道，而无需任何中心化注册机制。它们可以用于诸如凭证交换和认证。

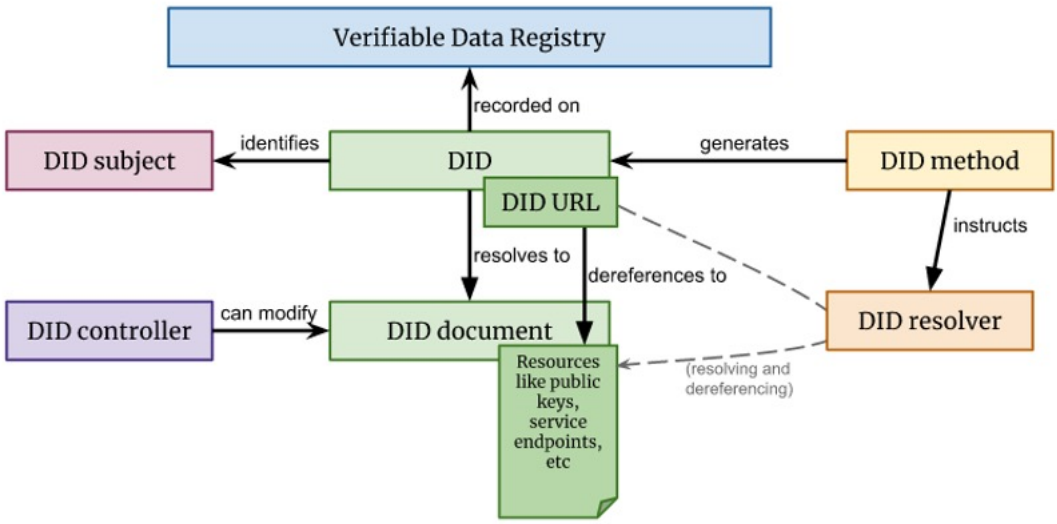

图 3- 分布式数字身份对象与 DID Doc（引自 W3C DIDcore）

DID 是将 DID 对象（DID）与 DID 文档（DID Doc）相关联的 URL，一个实体可以具有多个 DID，甚至与另一个实体的每个关系可以关联一个或多个 DID（成对假名和一次性标识符）以保护隐私性，身份所有者通过证明拥有与绑定到该 DID 的公钥相关联的私钥来建立 DID 的所有权。

一个 DID 的定义具有以下形式："did:" + <did - method> + ":" + <method 特定的标识符>

这类似于一种名字空间的表达，<did - method>通常是实现并注册了特定 DID 操作方法的厂商名称的缩写，比如 did:nist:0x1234abcd。考虑到方便与其它基于 Internet 的标识符一起使用，method 特定的标识符通常是 URL 或 URI 标识符。

DID Method 是一组公开的标准操作，通过它们可以创建，解析，更新和删除 DID。这些方法允许 DID 在身份管理系统中注册，替换，轮换，恢复和到期。目前已实现的 DID Method 集中登记在由 W3C CCG 工作组维护的分布式标识符注册表中，如果现有分布式 DID Method 不适用，可能需要向此注册表添加新方法。为了向该注册表添加新方法，实现者必须：

- 实现新 DID 方法，至少已完成实验版本。
- 在 https://w3c-ccg.github.io/did-spec/上创建一个描述新 DID 方法的规范，该规范可公开获得并旨在与 DID 规范保持一致。
- 确保规范中的标题包含版本号。

作为 DID 方法的一部分，DID 解析器（DID resolver）允许将 DID 作为输入，并返回 DID Doc 的相关元数据，该元数据遵循诸如 JavaScript Object Notation（JSON）及其相关的链接数据 JavaScript 对象符号（JSON-LD）的数据格式定义。

DID Doc 是一个通用数据结构，它包含与 DID 验证相关的密钥信息和验证方法，提供了一组使 DID 控制者能够证明其对 DID 控制的机制。根据 W3C 的规范定义，DID Doc 由以下标准元素组成：

- 统一资源标识符（URI），用于标识允许各方阅读 DID 文档的术语和协议
- 标识 DID 文档身份主体的 DID
- 用于认证，授权和通信机制的一组公共密钥
- 用于 DID 的一组身份验证方法，以向其他实体证明 DID 的所有权
- 针对 DID 的一组授权和委派方法，以允许另一个实体代表他们进行操作（即保管人）
- 服务端点集，以描述在何处以及如何与 DID 身份主体进行交互
- 创建文档的时间戳记[可选]
- 文档上次更新的时间戳[可选]
- 完整性的密码证明（例如，数字签名）[可选]

需要注意的是，考虑隐私保护等相关法律，身份应尽可能避免被归集，尤其对于非公示性个人身份，通常考虑用成对假名或一次性 DID 来表达。

3.2 Verifiable Credential（W3C）

分布式数字身份标识符在 ID 层面提供了自我主权的技术实现，但并未附加与该数字身份实体相关的现实世界属性，因此不是一个完整的数字身份表达。

参照现实世界中物理凭证的使用场景和核心模型，W3C CCG 发布了可验证凭证（verifiable credential）规范，该规范定义了可在实体之间交换的凭证格式，用以提供对于实体的属性说明。

可验证凭证是由发行人签名加密的防篡改凭证，具有密码学安全、隐私保护和机器可读的特点。凭证通常由至少两组信息组成。 其一表示可验证的凭证本身，包含凭证元数据和声明。 其二表示数字证明，通常是数字签名。

图 4-实体、标识符与可验证凭证

为了增强隐私保护，相关规范还定义了可验证表述（verifiable presentation），用于证明实体在特定场景下的身份角色属性。可验证表述是一种防篡改的描述，它来自一个或多个可验证凭证，并由披露这些凭证的主体用密码签名。无论是直接使用可验证凭证，还是从可验证凭证中获得的数据构造身份证明，DID 身份证明都将以“可验证表述（verifiable Presentation）”的方式进行出示。可验证的描述通常由以下内容组成：

- 唯一标识描述（presentation）的 URI
- 标识对象类型的 URI
- 从中推出（描述）的一个或多个可验证凭证（credential）或数据
- 可验证表述（presentation）的创建者 URI（例如 DID）
- 身份主体的密码证明（例如，数字签名）

“可验证表述”的数据格式可以进行密码验证，但其本身并不包含可验证凭证。

可验证凭证支持与身份持有者所关联的属性信息基于密码学方式进行签发与验证，从而确保凭证的权威性、和隐私保护性。可验证凭证同时支持可撤销能力，凭证的创建者负责通过撤销机制撤销已经发出的凭证，验证方则相应需要具有灵活高效地验证凭证是否已处于被撤销状态的能力。

3.3 DID-Auth （RWOT）

DID 验证的目的是让用户证明自己拥有某身份 DID —— 用户只要证明自己拥有该 DID 公钥匹配的私钥即可。通过 DID 验证后，不同个体之间能建立可信任且更长久的通信管道，以便在此之上协商交换其它资料，例如可验证凭证。

DID-Auth 与其它身份验证方法类似，依赖于“ 挑战-响应”方式。身份所有者（代理）所遇到身份验证挑战的方式以及挑战的格式将视情况而定，例如：根据挑战发起者是否预先了解待验证方 DID，挑战信息中可能包括也可能不包括对方 DID。

DID-Auth 并不是一个具体协议，而是一种实现框架。目前，许多不同项目正在以不同的方式实现“ DID-Auth”，它们可能使用了不同的数据格式，传输机制和协议。DID-Auth 实现的具体协议工作正在推进中，目前在探索如何与现有的成熟身份验证框架结合，例如 OIDC 和 WebAuth，以推动 DID 规范的应用。

例如，DIF 起草的“ SIOP DID 配置文件”（SIOP DID）是 DID Auth 与 OpenID Connect（OIDC）结合的规范，通过将用户身份钱包集成到 Web 应用程序的方法，将基于 DID 的身份认证方式集成到注册/登录应用的过程中，为每个人提供强大的、分布式的隐私和安全性保证。

3.4 DKMS（OASIS）

如何无需依赖具有密钥访问或控制权限的第三方，实现所有者自我管理密钥和证书的能力？分布式密钥管理系统(DKMS)的解决之道在于标准化身份钱包的工作机制，这部分涉及到以下组件：DID 层、身份所有者云钱包、云代理，边缘代理、边缘钱包。

DKMS 规范了身份钱包应如何管理密钥生命周期——创建，恢复，备份和吊销密钥的各个方面，并说明了：分布式数字身份可能需要什么密钥及其用途，应该在哪里存储和保护它们，如何从丢失或破坏中恢复，如何根据需要轮换它们，以及在不再需要该密钥时撤销并通知公众。密钥可以分发给其他实体，但必须由其所有者控制。

DKMS 使用以下密钥类型：

- 主密钥：不受密码保护的密钥。 它们是手动分发的，也可以是最初安装的，并受到程序控制和物理或电子隔离的保护。
- 密钥加密密钥：用于密钥传输或其他密钥存储的对称或公共密钥。
- 数据密钥：用于对用户数据提供加密操作（例如，加密，身份验证）。

密钥保护遵循分级保护的思想，一级密钥用于保护较低级别的项目。 因此，主密钥的安全性是整个系统的关键，应考虑采取特殊措施来保护主密钥，包括严格限制访问和使用、，硬件保护以及仅在共享控制下提供对密钥的访问等。

除了密钥种类设计、密钥生命周期管理、密钥恢复机制，《DKMS 设计与架构 4.0》还补充了密钥生命周期管理中的代理策略，细化了边缘代理与云代理基于 DKMS 协议进行所有标准 DKMS 密钥管理操作的流程，确保在引入云端代理的同时，整体代理方案依然具有高安全性和隐私保护特征，支持真正的分布式 PKI。

DKMS 设计必须是基于开放标准和开放系统的，DKMS4.0 已于 2019 年 3 月发布，进入公开公众审查和评论流程，以准备将 DKMS 提交给 OASIS 等标准开发组织进行正式标准化。

3.5 DIDComm（DIF）

“协议”是交互双方必须共同遵从的一组约定，如怎么样建立连接、怎么样互相识别等。现有互联网应用交互的 Web API 协议方式基于 C/S 结构的假设，从信息交互和安全角度都是非对等的，并不适合 DID 对等交互的需求。

在 DID 通信世界，消息协议是分布式的。这意味着该协议没有监督者来保证信息流，强制双方行为并确保一致性。DIDComm 协议通过双方对规则和目标的共同理解和共识达成互动，这与 WebAPI 方式下依赖中心化的规则管理有很大的不同。

DID 持有者在数字世界通过各自的代理软件进行交互，他们基于预定义的 DIDComm 消息协议，启动特定交互-连接，维护关系，颁发凭据，提供证明等。DIDComm 设计目标如下：

- 确保安全性
- 具有隐私保护
- 可互操作
- 与传输方式（协议）无关
- 可扩展性

为了保证安全和私有，协议应当是分布式的，互操作性意味着 DIDComm 应该跨编程语言，区块链，供应商，OS /平台，网络，法律管辖区，地域，加密和硬件以及跨时间工作。

DIDComm 使用 DID 持有人本人身份钱包所提供的公钥密码技术实现 DPKI 安全通信，而不是第三方的证书和在其他方登记注册的密码，其安全保证独立于它所基于的数据传输方式，是非会话保持方式的；当需要进行身份验证时，所有各方都以相同的方式对等进行。

主要的 DIDComm 相关规范包括：DIDComm 消息结构规范，DIDComm 消息加密规范，DIDComm 相关传输规范。基于 DIDComm 结构建立的协议除了：建立 DID 连接、凭证请求与签发、身份验证等，还可以针对各种丰富的主题进行自定义。

第四章 分布式数字身份的支撑体系

身份管理系统广泛用于提供用户身份，同时管理组织内部和网络服务上的身份验证、授权和数据共享。

传统的身份管理系统中，组织可以存储与之交互的每个用户的凭据（例如密码），在联盟身份模型中，他们可以通过第三方来存储相关信息。由于控制身份信息的实体的特权位置，可能引发隐私保护问题和由于数据高度集中带来的不平等性。此外，传统的身份系统是中心化的，通常会有单点故障隐患和缺乏互操作（可移植）性的问题。

基于区块链技术的分布式数字身份管理有助于解决以上问题：它们可以支持用户控制自己的标识符和凭证的托管，转换数据治理模型，减少对受信任中介的依赖性，并使用户和企业从中受益。用户可以自己管理自己的身份数据，并在知情和授权的基础上将其公开给依赖方；企业可以依靠可验证的用户信息来简化其运营，而不必自己充当数据托管人并处理相关的成本和风险（例如，基础架构，安全性和法规遵从性）。

分布式数字身份区别于中心化身份系统的最大不同在于：分布式数字身份体系分解了标识符和凭证体系结构，且标识符体系和凭证体系都应贯穿分布式的实现，从而支持创建分布式互操作的生态系统。分布式数字身份凭证的发行，呈现和验证是在一系列协议和技术中进行的。相关栈包括四层：分布式账本层，代理层，凭证交换层，治理层，这些层如图 1 所示。本文的其余部分将详细讨论每一层。

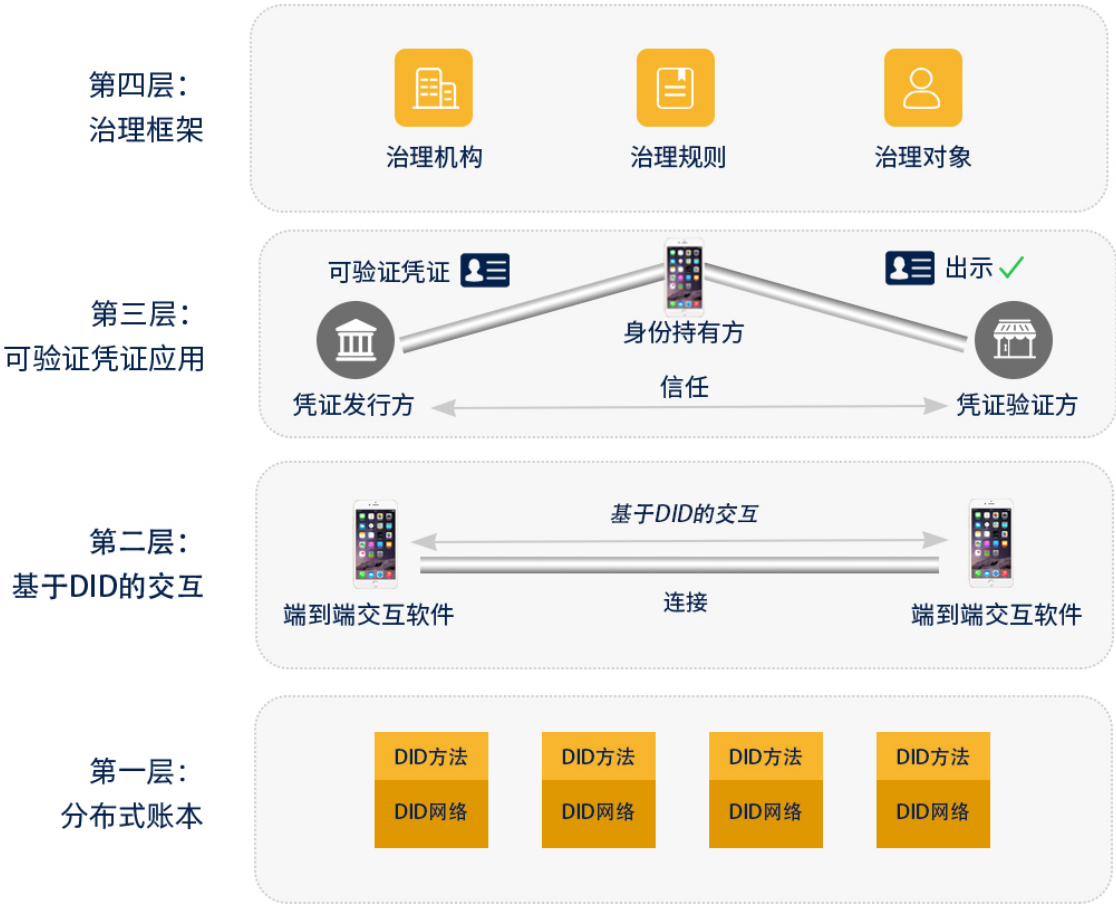

图 11-分布式数字身份分层架构

对参与分布式数字身份生态系统的用户来说，自底层向上分别需要分布式账本提供身份注册，代理软件（服务）提供所有者身份管理和实现与他人通信，凭证工具提供凭证流转和验证功能。此外，当用户数据使用云存储代替本地存储时，还需要云服务商提供安全的数据托管服务。

4.1 分布式账本

代表实体身份的全球唯一分布式标识符应该如何存储和提供访问？人们如何访问它们？为了使身份真正具有自主权，这种基础设施需置于分布式信任的环境中，而不属于任何单一组织所控制的环境，分布式账本（区块链）正是这样一种创新技术。自主权身份 DID 锚定于分布式账本，以避免被特定中心化服务所掌控。

区块链通过充当公共密钥基础结构（PKI）的受完整性保护的“公告板”来支持密钥和标识发现，在大多数情况下，基于 PKI 的“公告板”形成标识符管理系统（DID 方法实现），除了密钥和标识符外，可验证凭证也可能依赖于区块链实现流转、验证。

考虑分布式账本专门用于支持身份交易，应具有以下几个重要属性：

- **可公开访问** - 此分布式账本是公共可访问的，因此任何人都可以在没有中介的情况下使用它。通过在尽可能广泛的范围里部署分散节点网络，实现即使一个或多个节点关闭或无法运行，人们仍可以随时访问该网络。
- **可信验证** - 分布式账本的每个节点都运行分布式数字身份账本，分布式账本能够生成状态证明，客户端可以使用状态证明来了解分类账的状态，而不必下载和访问整个分类账。 每个状态证明都包含一个时间戳，以便客户端可以确定状态证明是否足够适合他们的用例或是否需要刷新。 这使得它非常适合用于证书验证，在该验证中客户端可能会在一段时间内无法访问互联网，从而需要离线验证，这是普遍采用数字证书的关键要求。此外，状态证明可以交叉锚定在其他分布式账本上，以提高可靠性，可信赖性。
- **操作成本低廉** -考虑作为分布式数字身份需要成为广泛可用的基础设施，账本上的交易验证应该是成本低廉的，账本访问应尽可能便宜，以覆盖更广泛的网络受众。

分布式账本中应为分布式标识符提供以下属性（能力）：

- **不可重新分配 - DID 是永久性，持久性和不可重新分配的。** 永久性确保标识符始终引用同一实体。 因此，DID 比可以重新分配的标识符（例如域名，IP 地址，电子邮件地址或手机号码）更具私密性和安全性。 永久性对于身份持有者的控制和自我主权至关重要。
- **可解析** - DID 基础结构通过全局分散的 key-value 结构存储，其中 DID 充当 key，DID Doc 充当 value。DID 解析是指在 DID 账本中查找特定 DID Doc 的操作。

可加密验证的 DID 与加密密钥相关联，控制 DID 的实体可以使用这些密钥来证明 DID 所有权（DID-Auth）。彼此直接交换了 DID 的各方（称为对等方）可以通过解析 DID 实现相互身份验证并加密其通信。

分布式数字身份体系并不局限于区块链技术，更不绑定到唯一的区块链平台上，其系统模块可能基于不同的区块链平台实现，甚至是非区块链的其他分布式账本实现。为了确保不同系统的 DID 数据互联互通，一是要求实现厂商按照统一的 DID 规范定义和实现 DID 数据对象，二是对于不同的 DID 操作实现，通过全球统一的 DID 实现方法注册，以达成不同系统间的 DID 查询与解析，实现 DID 互联互通。

4.2 身份代理

在数字环境中，人和组织（有时是设备）无法直接产生和消费数字信息、存储和管理数据，分布式数字身份系统中代表身份所有者执行自主权身份相关的数字权益的“数字代表”软件被称为代理组件。

代理是一种笼统的说法，它通常包括：负责对外消息通信的代理组件（agent），支持分布式密钥管理的钱包组件(wallet)，以及用户数据存储组件(hub)。代理(agent)组件是分布式数字身份的对外接口，调用了本地的数字身份钱包和数据组件。

代理软件通常包括客户端代理和服务器端代理。客户端代理主要加载在用户的智能手机、汽车、笔记本电脑等终端设备上，终端设备具有私有属性，终端代理主要用来管理用户身份私钥，个人秘密，以及本人身份凭证等；服务器端代理实现了可寻址的网络端，主要用来为其客户端代理提供以下服务：持久的 P2P 消息服务；协调身份所有者的多个客户端代理；加密数据存储与共享；身份所有者密钥的加密备份等。

每个代理所关联的钱包都有其自己的密钥，密钥不会在代理之间复制。设备代理的使用高度分散，因为所有密钥和凭证都存储在互联网终端设备之中。尽管云代理托管在云中，但它们也可以分散管理，由合格的服务提供商（称为代理商）负责运维。与边缘代理一样，云代理始终完全在拥有它的个人或组织的控制之下，身份所有者应该能够轻松切换代理。此外，代理商无权访问存储在云代理中的数据。 通常，云代理数据是加密存储的，只能由设备代理使用存储在最安全的终端设备中的密钥解密，因此云代理商不会有通常的数据蜜罐风险。

代理的安全策略必须健全，事故或恶意不应损害所有者对身份控制权的掌握，倘若出现问题应该具有快速解决的能力。代理基于 DKMS 标准存储、管理，以及使用密钥和凭证，这不仅为身份所有者的隐私和自主权带来了好处，而且支持人们从事故和攻击中恢复。

DID 持有者应能够通过各自的代理软件，在数字世界安全进行交互，而不需要依赖特定的第三方。基于已定义的 DIDComm 消息协议，代理之间可以直接实现：交互连接、凭证请求，以及凭证验证等交易。DIDComm 标准正在制定中，它旨在成为所有

自主权互动中的面向未来的通用语言。代理到代理之间的通信不必依赖特定的第三方进行，它具有以下两个重要特征：

- 基于消息，异步和单工

当今，移动和 Web 开发中的主要范例是双工请求响应。通常调用具有特定输入的 API，随即在同一通道上获得具有特定输出的响应。然而，许多代理不能很好地模拟 Web 服务器，比如移动设备，它们以无法预测的时间间隔关闭，并且缺少与网络的稳定连接。

代理交互的基本范例是基于消息、异步和单工方式的。代理 X 通过通道 A 发送消息。稍后，它可能会通过通道 B 从代理 Y 接收响应。相比 Web 范式，代理之间的交互更接近电子邮件范式。

- 消息级安全性，对等身份验证

传统 Web C/S 模式下，传输级别（TLS）提供了 Web 安全性，但这种安全并不是消息本身的独立属性。在异步单工工作模式下，传统的 TLS，登录和会话有效期这些措施都是不切实际的，无法继续用来支撑通讯的安全性。

代理交互使用 DID 持有人本人身份钱包所提供的公钥密码技术实现 DPKI 安全通信，而不是第三方的证书和在其他方登记注册的密码，其安全保证独立于它所基于的数据传输方式，是非会话保持方式的；当需要进行身份验证时，所有各方都以相同的方式对等进行。

概括来说，身份代理组件实现身份所有者自主管理身份密钥，代表身份所有者（也可以代表 IoT 设备,宠物等的控制者,或者是未成年人或难民的监护人或受托管理人），按照点对点消息协议实现与其它身份所有者代理的交互。

4.3 凭证交换

凭证交换主要解决以下问题：确定发行方的代理如何向凭证持有者发布凭证，凭证验证者如何向凭证持有者请求信息，以及凭证持有者如何从其凭证中提取证明使验证者信任。

图 6-凭证流转与相关角色

凭证交换的核心是密码学技术，主要用于证明可验证凭证或可验证表述中的信息完整性与真实性。有许多类型的加密证明，包括但不限于传统的数字签名技术和基于零知识证明的匿名凭证技术。

可验证凭证和可验证表述中的密码学证明可以采用传统数字签名技术，由数据的签发者对数据内容计算数字签名后将数字签名附在数据内容后，以保证数据的接收者确

认数据来源的不可抵赖、数据内容未被篡改。此外，由于可验证表述是经由凭证动态打包而成，因此可增加动态认证部分功能，用于防范凭证流转过程中的重放攻击。凭证在各个对手方之间的流转流程在技术上不做限制，如若场景对传输信道有较强加密需求，可以规范数据通道认证、数据通道建立及传输的特定协议，达到任意 DID 身份所有者之间均可通信的目的。

凭证持有人可以使用零知识证明（ZKP）以最少的披露共享来自多个凭证的信息。ZKP 是一种加密技术，可让用户共享信息而不会放弃其安全性和隐私性。ZKP 使用加密技术来证明持有人对验证者的声明，而不会泄露验证者不需要的任何其他信息。

零知识证明必须具有三个属性才能使用：

1. **完整性：**如果陈述是正确的，则验证者相信证明的结果。
2. **健全性：**如果陈述为假，则持有人无法创建虚假证据，以使核实者认为该陈述属实。
3. **零知识：**除了证明中的内容外，验证者不会了解有关持有人的任何其他信息。

一个典型的例子是出生日期。身份证通常是证明年龄的主要手段。但是，这种类型的标识还包含其他有价值的私人信息，例如经常被盗用的家庭住址信息。ZKP 将身份证的数字副本转换为身份证凭证中特定信息的加密证明。在使用时，用户可以根据请求者身份，控制在该特定数字副本上实际提供给他们显示的信息。

在凭证持有人需要证明其年龄的各种情况下，分布式数字身份钱包均可创建 ZKP。ZKP 技术使身份所有者能够快速，轻松且安全地验证自己已年满 18 岁，21 岁或 65 岁，而不必实际共享特定的出生日期。

凭证的特性包括机器可读、可撤销、可远程验证。其中可远程验证包含凭证的发行方身份可远程验证和凭证内容可远程验证：通过凭证中记录发行方公开 DID 身份，

验证者不需联系发行方即可验证身份；通过公开的凭证发行声明中记录发行方密钥、凭证数据格式等信息，验证者不需关联发行方即可验证凭证内容。

4.4 身份数据中心

身份数据中心是连接在一起并链接到给定实体的链外加密个人数据存储。它们可以用于安全地存储身份数据（直接在用户设备上或在用户指定的云存储服务上），并在所有者批准此类共享时进行细粒度分享。

用户的个人设备，特别是移动端设备在数据存储方面有容量限制，可能导致用户的客户端代理在进行本地凭证存储时无法保存全部的个人凭证记录，这种情况下，可以考虑使用分布式存储对用户凭证进行云端托管。

DIF 发起 ID-hub 协议和开源软件工程支持在云服务上提供安全的身份隐私数据存储。一个用户可以使用多个个人数据存储，通过注册到用户控制的 DID 提供云存储服务的寻址。ID-hub 协议定义了个人数据组件对外提供的统一接口，用于解决数据组件各实例间数据同步如何进行共享复制，以及为确保用户的控制权而实现的数据序列化导出。

身份数据中心组件的特点是安全、可用和可共享。与传统云存储服务不同，ID-hub 定义的接口与供应商和平台无关。且云端数据由身份所有者的密钥加密，无论从 Apple 平台迁移到 Android 平台，还是从 Google 云服务迁移到 amazon 云服务，个人数据不会受到影响。即使黑客、恶意系统管理员或利用机器学习算法的数据挖掘者获得了个人的数据存储，这些数据因使用个人持有的密钥加密而无法被识别和盗用。

4.5 委员会和治理

尽管 DID 网络是分散的，但它仍在社区驱动的治理流程下运行，其目标是最大程度地增强对 DID 网络作为全球身份网络的可信性。此治理过程对于产生一个既可以满足政府和司法部门对数据安全性，隐私权，保护性和可移植性要求，又可以确保个人对身份数据共享拥有主权的系统至关重要。

委员会概念的引入，可以作为整个生态的社会关系的信任根基础。委员会的职责可能包括但不限于：负责 DID 底层账本的开放运维策略的制定和落实，对于在分布式数字身份系统提供数据背书服务的权威方的认证，以及为其提供在分布式账本上的实名身份公示。

在此基础上，委员会可提供一系列用于治理或监管的工具套件供各个 DID 身份所有者访问，如可信时间戳服务、监管报表服务、黑白名单维护、数据模板注册维护服务等。

第五章 领域应用场景和案例

在应用落地的过程中，通常针对不同场景中的不同需求采取了不同的实现方案。通过以下分布式数字身份在国内的应用案例（项目）的分析，有助于我们理解在不同场景下分布式数字身份方案的价值。

5.1 WeIdentity

WeIdentity 是一套分布式多中心的实体身份标识及可信数据交换解决方案，实现了一套符合 W3C DID 规范的分布式多中心的身份标识协议，和符合 W3C VC 规范的可验证数字凭证技术。通过前者，分布式多中心的身份注册、标识和管理成为可能，实体（人或物）的现实身份实现了基于区块链的链上身份标识，同时实体可以通过私钥或默克尔证明方式控制这些身份标识。通过后者，实体可以将现实世界中各类描述实体身份、实体间关系的数据，如身份证、借条、票据、医疗检测记录等进行标准化，并使用基于 DID 规范的非对称密钥的数字签名技术进行签名，生成可验证的“凭证”，及对凭证进一步生成链上存证。WeIdentity 同时支持对凭证的属性项进行选择性披露，并通过链上授权，合法合规地完成隐私保护前提下的实体间可信数据交换。

5.2 分布式数字身份 + 教育身份：腾讯云可信教育数字身份（教育卡）

当前，在教育领域，面向“学籍、学历、证照、档案、考试、录取、资助、转学、版权”等实际应用，亟需实现跨部门、跨业务、跨区域的应用共享。过去没有统一可信的教育数字身份，大大增加了业务应用链的服务成本：首先，同一用户在不同的业

务下，呈现多种账户及密码，管理难度大；其次，业务平台或用户需要承担更多的发放用户证书的经济成本，造成重复投资；三是不利于开展业务数据跨链共享，实现跨链共享首先要解决不同链的用户身份互认。

可信教育数字身份（教育卡）是遵循国家密码法、电子签名法、网络安全法等法律法规，面向在校学生、教师、毕业生签发的、具有法律效力的可信数字身份标识。依托腾讯云区块链平台提供的分层互联协议、可信身份、多方治理等特性，并采用国产密码技术，创新性的集合了法定身份信息、教育人员身份信息、网络身份信息的三大身份，形成可信的教育数字身份标识并实现统一认证 ，具有法律效力，打造教育信息可信制度凭证。

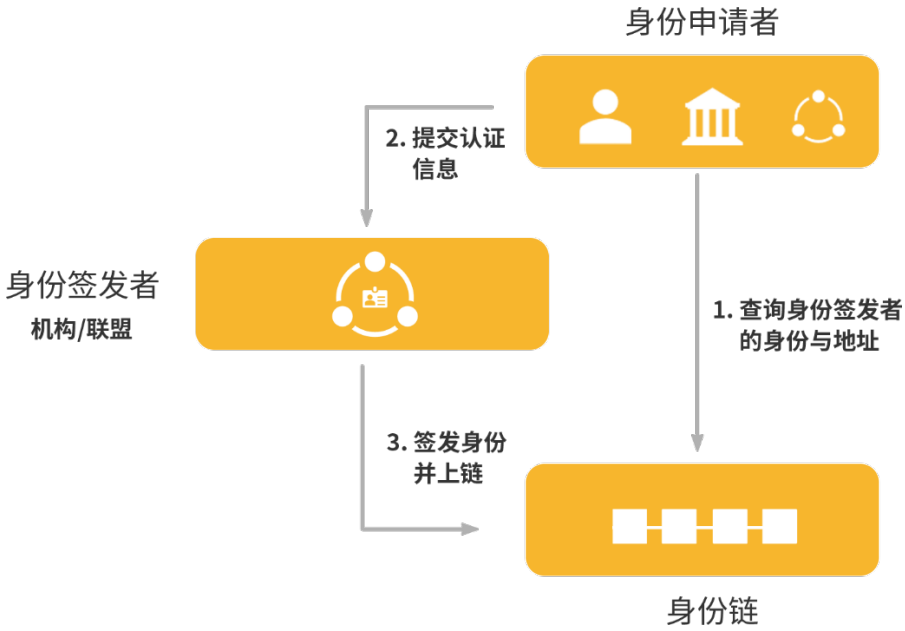

图 7-数字身份签发上链流程

可信教育数字身份为“学历学籍、综合素质评价、教育招生考试、个人终身学习”等建立教育可信数字档案平台与可信教育可信档案链，实现教育可信数字档案在全国范围内的“跨学校、跨系统、跨地区、跨行业”的互信互通与安全共享。解决了“网

络教育身份可信认证、数字签名、数据加密、个人隐私安全保护、全证据链法律保障、网络行为的不可抵赖”等安全需求。

5.3 分布式数字身份 + 投票：网贷机构良性退出平台

为稳定金融市场，化解 P2P 机构引发的金融风险，深圳市互金协会发布《深圳市网贷机构良性退出指引》，要求决策事项在网上投票表决。投票表决流程涉及身份验证、债权确认、公告送达等金融级安全要求和技术，但普通投票平台难以解决其中的痛点问题：一，投票冒充、抵赖、篡改的情况时有发生，数据未能形成有效证据链，结果易受质疑，而发生纠纷时又难以判定；二，缺乏隐私保护机制，投票人信息安全得不到保障。

深圳市互联网金融协会联合微众银行共同搭建“网贷机构良性退出统一投票表决系统”，运用区块链技术解决网贷机构清退流程中的互不信任问题，如图 8 所示。

用户基于人脸识别和数字证书认证方式，确认出借人的身份，为每一位用户生成系统内独一无二的 WeID。在确认用户身份及用户授权的前提下，将投票信息填入 WeID，为每位投票用户生成可验证凭证 Credential，并生成凭证摘要 Hash 上链。此过程既可防止投票过程中存在他人伪冒的情况，又避免了将投票人的全部敏感信息上链，在保护用户隐私的同时，避免了投票冒充、抵赖、篡改等情况发生，确保投票结果公正性。投票联盟链上各机构对 Credential 的数据内容项进行验证，在无法破解用户 WeID 并反向推出用户真实身份的情况下，独立地抽取投票内容信息，并通过链上智能合约统计投票结果。

图 8-网贷机构良性退出统一投票表决系统

5.4 分布式数字身份 + 版权保护：“人民版权”平台

在既有技术条件下，网络内容版权保护存在较多痛点：一、确权难，传统版权登记周期长、流程繁、成本高，版权对应的内容收益难定义、难统计、难追踪；二、取证难，数字作品易复制、易传播、难溯源，调查取证手段匮乏、耗时长、成本高；三、维权难，侵权行为认定难，传统的侵权诉讼流程复杂，诉讼成本高、时间长，被侵权方需要投入巨大人力物力进行维权。

基于区块链技术搭建的人民版权保护平台可大幅降低司法过程中的证据取证与保全成本，用传统手段 1/2 的价格便可完成确权、维权全流程，如图 9 所示。

基于 WeIdentity 方案，平台为每位实名认证的作者生成 WeID；当作者提交作品原创申请时，平台为作品基于登记时间、作品名、核心摘要等信息生成数字指纹 DNA，同时为每篇作品和对应的作者之间的原创关系生成凭证 Credential，生成凭证摘要上链，在链上存证 DNA 数据。当前，人民版权平台正在拓展更多媒体场景化接入，并通过打通链上的侵权取证及诉讼流程实现版权保护及版权交易的全线上化和自动化。

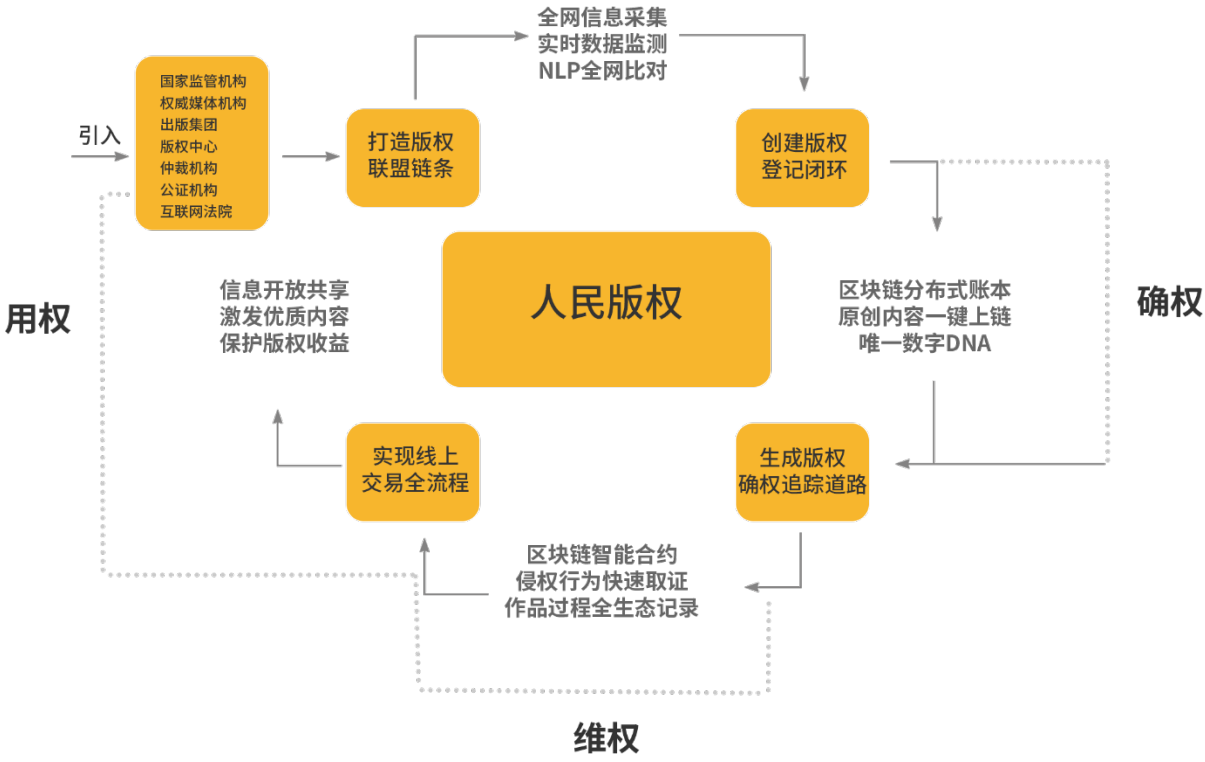

图 9-人民版权保护平台

5.5 分布式数字身份 + 证书管理：澳门智慧城市之证书电子化项目

澳门居民在找工作或办理其他事务的时候，经常需要出示自己的证书或证明，一方面纸质证书的管理成本高，使用次数、场景、流程都受限制，另一方面用人单位或者其他机构很难验证证书真伪，通过人工或第三方验证的方式往往耗时长、效率低。同时，多机构间的信息传递，可能因道德风险及操作风险导致用户隐私泄露。基于以

上原因，澳门本地的个人数据隐私保护相关法规要求用户数据在不同机构间传输的时候需要居民提供授权书进行确认，流程复杂且时效性较差。

为此，澳门政府基于 WeIdentity 方案推出了证书电子化项目，实现安全高效的跨机构身份标识和数据合作，提升澳门居民的服务体验。

澳门居民通过进行实名认证后，用户代理会为其生成独一无二的 WeID，并由用户身份验证服务提供方为用户基于此 WeID 生成用户的 KYC Credential。用户访问接入证书电子化项目的联盟链上的其他机构时，只需出示自己的 WeID 及 KYC Credential，便可认证身份并执行业务。若出现用户丢失了本地存储的电子凭证，证书验证方可以通过机构后台，在获取用户链上授权的基础上，通过区块链连接证书发行方后台并拉取 Credential 原文。

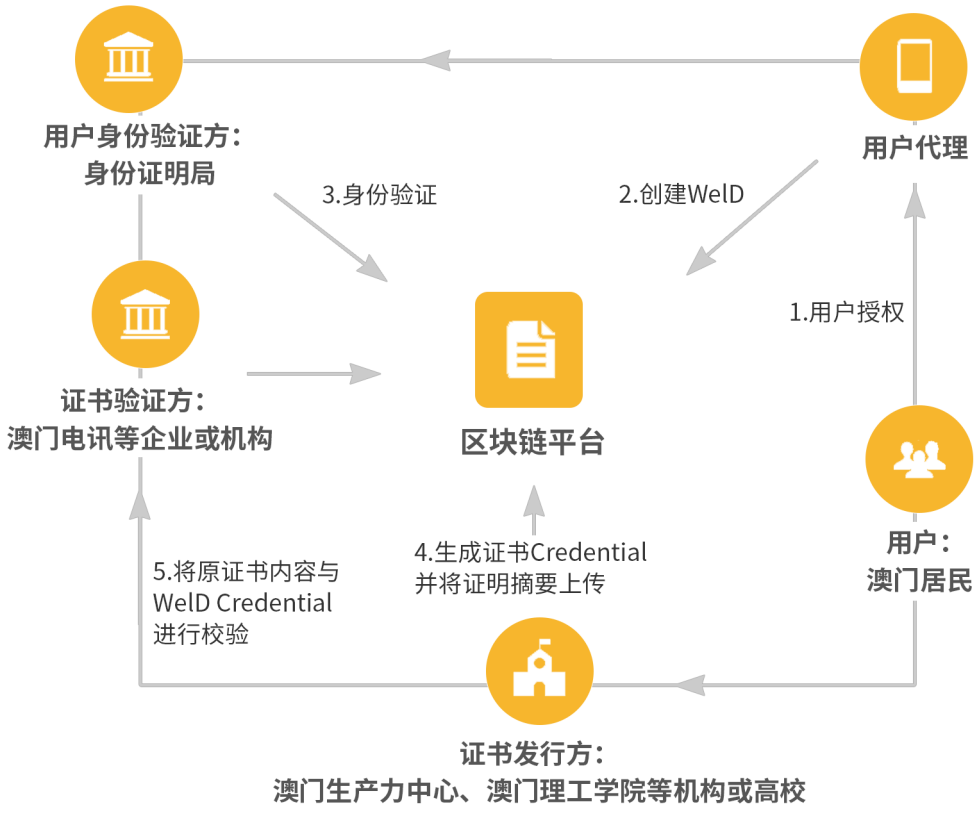

图 10-澳门智慧城市证书电子化项目

5.6 基于物联网 + 数字身份的智慧停车系统

现有的停车场主要有业主、停车场平台、车主三方参与，通常由业主委托停车场平台运营管理其停车业务。但是由于停车设备直接连接到停车场平台，由平台方独自运营和管理，所以无法保证平台方提供的交易信息的真实性，有可能存在伪造、变造交易信息，套取业主资金的行为。平台方无法自证清白，业主无法完全信任平台方，而一旦出现问题和纠纷，双方则会对账困难且无可信服的对账依据。

溪塔科技在物联网领域引入 DID 技术构建基于区块链网络的物联网身份认证系统。通过业主方、停车场、监管机构、金融机构共同搭建区块链平台，原有的停车场业务流程无需变化，通过内置可信区块链芯片的方式赋予闸机、摄像头等智能设备可信 DID 身份，实现设备端数据关键信息直接上链。由此来保证设备端数据透明真实、不可篡改，业主和监管方可以使用链上数据对平台数据进行验证和对账，提高平台方可信度，降低商业摩擦，提升效率。

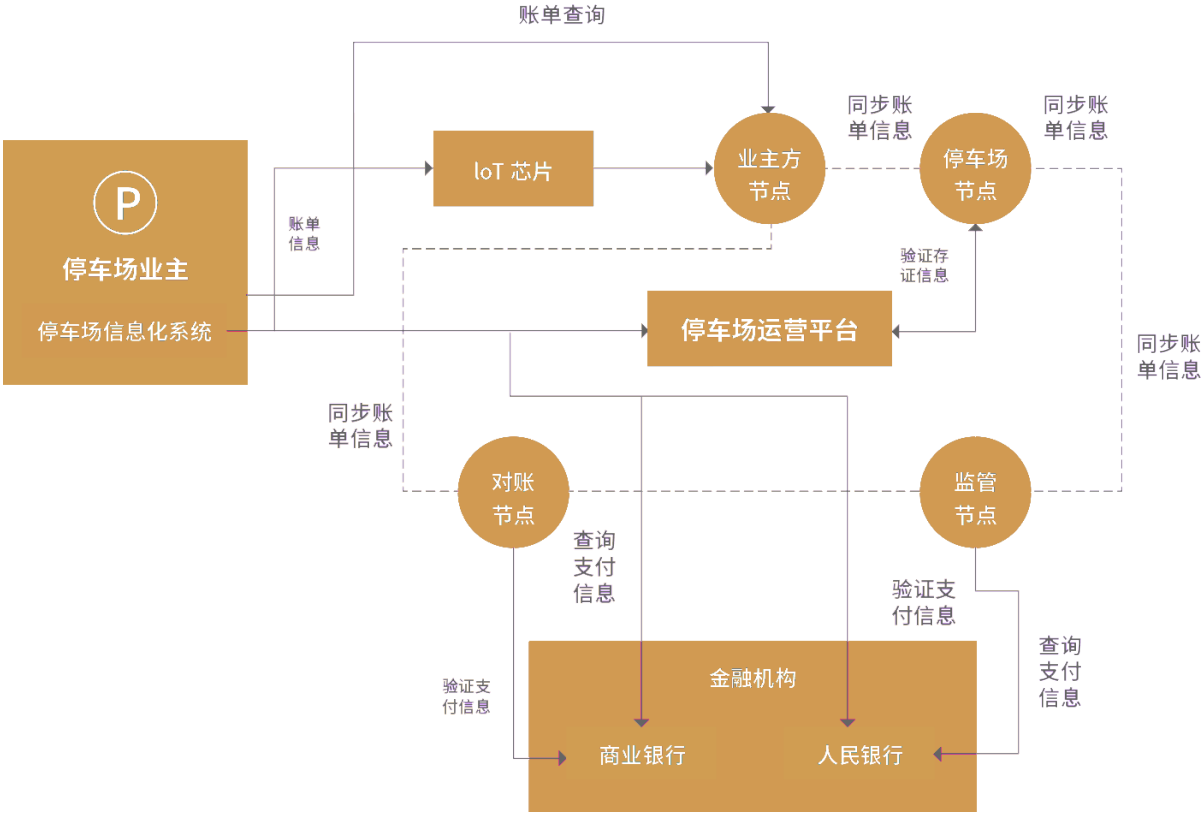

图 11-基于区块链网络的物联网身份认证系统

5.7 分布式数字身份+电子车牌： 腾讯领御 TUSI DID 电子车牌应用

电子车牌（Electronic Vehicle Identification, EVI）是基于物联网无源射频识别（RFID）技术的细分、延伸及提高的一种应用。它的基本技术措施是：利用 RFID 高精度识别、高准确采集、高灵敏度的技术特点，在机动车辆上装有一枚电子车牌标签，将该 RFID 电子车牌作为车辆信息的载体，并由在通过装有经授权的射频识别读写器的路段时，对各辆机动车电子车牌上的数据进行采集或写入，达到各类综合交通管理的目的。

图 12-TUSI-DID 电子车牌应用

通过在电子车牌中加载 TUSI-DID 应用，实现物理标签卡（电子车牌）与 TUSI-DID 的唯一车辆身份管理，在将电子车牌作为汽车唯一账号和标识，接入区块链系统；向用户提供带有定制芯片的电子车牌，在远距离扫描技术作用下，实现车辆交通过程中的各种扣费，用户使用手机 APP，能够随时查阅和缴费；公安交通管理部门，可以通过接入区块链的节点，利用节点所特有权限，对所有车辆相应信息进行管理、监督、查看和保护。相应的第三方监管及服务厂商，通过区块链服务来实现 TUSI-DID 电子标识卡片的认证，信息获取等功能。

第六章 分布式数字身份建设面临的挑战和应对

从前几章可以看到，目前分布式数字身份体系的涵义已经比较清晰，其必要性、重要性、急迫性得到体现，而且已有诸多主体在研发相关技术和开展应用。总的来说，整个领域尚在高速发展的阶段，这个过程依旧面临不少挑战。联盟的使命是聚合产业力量，寻求共识，共同研究和探索，以务实的技术和应用实践成果应对诸多挑战。

6.1 技术储备

分布式数字身份在技术方面牵涉面较广，只要和身份验证、身份标识、安全传输、海量存储、可信验证、隐私保护等等相关的技术都有所涉猎。

在身份验证方面，除了传统的“面签”之外，数字化的验身已经是相对成熟的做法，基于面部识别、虹膜、声纹、指纹等生物特征，即可验身，并达到在线支付和银行（二类户开户）的严密性要求。在要求更苛刻的场景，对验身技术的要求会更高，包括更低的错误率、更快的反应速度、更强的安全性等。联盟将通过实践推动数字化验身和分布式数字身份的结合，以提升用户体验和拓展场景。

分布式数字身份系统通常运行在区块链网络上，技术平台选型很重要。公链受限于监管合规风险、经济模型波动性过大等问题，难以成为实体行业所用的基础平台。联盟链技术从 2015 年起被广泛关注，目前国内外均有不少优秀的方案，国外的包括 Hyperledger 的 Fabric，R3 的 Corda 等，国内联盟链平台有中钞区块链技术研究院的络谱平台，金链盟的开源项目 FISCO BCOS，百度 XuperChain，溪塔科技的 CITA 平台等。联盟链平台强调安全可控、支持国密算法、高性能高可用、拥抱监管合规，有利于和

实体产业深度结合。目前区块链行业在网络和数据的大规模化、跨链互操作等方面有积极投入，分别推出了相应解决方案，正在逐步被大规模的应用验证。

在密码学和隐私保护措施方面，以零知识证明、同态加密、安全多方计算、联邦学习为代表的方案在保护性方面有良好的表现，这些方案理论较为复杂，部分算法要求多次交互，或生成的数据过大，导致在实际运行时的性能、用户体验依旧有提升的空间。目前联盟各成员均有在相应领域的研究投入，陆续提出解决方案，效果可期。

对于行业性的分布式数字身份体系，目前需要向 PKI 寻求信任根，如到 CA 中心申请 CA 证书等。分布式公钥基础设施(DPKI)是 PKI 的进化版，DPKI 基于包括但不限于区块链在内的分布式账本方案，可以达成信息的难以篡改和全局共享，通过多方共识达成互信，不再依赖集中式的服务。实际上 DID 规范只是 DPKI 的一部分，DPKI 体系的工业化实现，还依赖更多的基础服务如通用数据解析器、全局寻址系统、分布式响应服务系统等，以及要求对原有 DNS，CA 等基础服务进行改造。

最后，配套设施完备是分布式数字化身份应用普及的必要条件，联盟将在海量数据存取、高速网络、个人安全硬件、多样化的终端接入方面给出实用性方案，以满足行业和广大用户的功能和体验性需求。

6.2 行业应用

在数字经济发展的推动下，对分布式数字身份的应用需求也越来越旺盛。分布式数字身份是应用的基础组件，本身并不能提供完整的应用体验和商业模式、治理模式，需要和场景深度结合，包括 KYC 以及后续的主体认定、资格鉴证、风控授信等。

在分布式的应用里，参与者众多，数据控制点和流动方向会呈现跨主体态势。与之前中心化模式相比，分布式应用会带来不同的业务体验和协作关系变更，可能导致业务流程进行相应重构，以基于分布式的底层架构，为最终用户提供丰富的功能、良好的用户体验，以及在安全合规的前提下实现商业和社会价值。

分布式数字身份体系和业务应用有着相辅相成，螺旋式发展的关系。应用和业务本身越具有“分布式”和“数字化”的特点，网络化和分散性越强，对分布式数字身份的要求越高，反之则无强需求；而分布式数字身份体系的技术和模式越成熟，就更能为应用打好基础，使应用的运作无需为身份可信性和隐私问题困扰。

同时，分布式数字身份以及相应的可信数据验证和交换，也会催生出更多的创新业务场景，带来新的商业模式。届时，数据的价值，数据的保护和流通成本，应该取得良好的平衡，需要解决谁为数据买单、如何定价、如何分账等一系列商业问题，以及明确相应的责权和义务。

随着新基建带来的新一轮信息工业建设热潮，整个社会将越来越数字化，在金融等领域的“分布式商业”趋势越来越明显，无论是银行、证券、保险、工业制造、物流、社会管理...都出现需要多方对等互补、追求规则透明、高效可信运作的协作模式，分布式的技术和运营模式会更加深入民心。联盟在发展分布式数字身份的研究的同时，逐步探索和场景的结合，谨慎试点，大胆验证，在实践中完善优化。

6.3 标准和规范建设

在全球范围内，分布式数字身份的研究从最初的单一项目、单一技术研究进入到超大型技术公司为主导的标准化研究进程，技术规范已经初步成型，以 W3C 组织的

DID 为代表的规范形成了 1.0 版本，获得行业较为广泛的接受，该规范依旧在迭代更新中。在标准和规范方面，仍有以下挑战存在。

身份服务互联互通有待改善：既有的各项分布式数字身份规范的理念大同小异，都会强调在分布式环境里达成互通性。但各协议在数据结构、接口设计、交互流程细节上依旧存在一定的差异。更进一步的，各厂商方案即使参照同一个规范来实现，细节也会有所不同，体现在通信协议、数据存储、交互步骤、安全控制等环节，导致互相之间的互通、互认、互验尚不能无缝贯通，也缺乏权威的检验准则。

行业和领域覆盖性有待加强：各分布式数字身份协议的内容主要是覆盖基本概念、基础数据结构和核心交互流程，协议本身没有也不会定义面向行业的规范，如社会治理、金融、工业、互联网业务等，各行业在运用协议规范时，对参与角色的责权利、安全等级、可用性、技术指标都有不同的要求，需要针对行业制定更具体的标准和规范。如在跨行业、跨领域时，遇到的标准问题会更加复杂。

和既有标准的结合有待明确：目前各项分布式数字身份规范影响的主要是创新的领域如区块链、数字经济等，传统领域既有的众多的标识体系尚未和分布式数字身份紧密结合，如物联网、工业标识、骨干网络标识等。需要研究和分析既有的标识体系是否可以、是否需要和分布式数据体系结合，以及结合的方式和层次。

我们希望通过联盟的努力，与有关部门合作，建立和完善相关技术标准体系，加快相关标准的统筹与实施。

- 加强对规模巨大、变化迅速、关系复杂的实体标识标准的研制；
- 加强对不同类型实体的电子凭证标准研究，重点研制电子凭证的互操作、基于可信环境或安全芯片的电子凭证等标准；

- 加强对不同类型实体的鉴别标准研究，加快研制基于风险控制的身份鉴别标准，并确保基于风险的鉴别具有应用可识别性和互操作性；
- 加强身份管理和服务的安全性以及互操作性标准的研制，重点研发身份信息管理的隐私保护类标准、身份服务的互联互通标准等；
- 重点研制针对多级鉴别、细粒度授权的标准，研制互联互通的授权协议。

综上所述，在分布式数字身份领域，还需要进一步强化和制定相应的标准和规范。首先明确方向，聚焦完成度已然较高的协议，进行扩充和发展；然后求同存异，兼容并包，跟进和融合其他相关协议规范，力求覆盖面更广、适用性更强、更具备产业可操作性，以满足和实体经济数字化方向相符的需求，并使现存规范可以平滑的向分布式数字身份时代持续演进。

6.4 法律法规的发展

合规一直是国内安全领域中出现最为频繁、最为重要的主题。分布式数字身份带来新的协作模式和商业模式，也会带来相应的商业风险、道德风险、操作性风险。世界各国的都针对数据安全和隐私保护出台了一系列的法律法规，以欧盟的《通用数据保护条例》(GDPR)为代表，包括美国、日本的一系列法律，都以加强个人权利保护、强化经营者责任和促进经营者自发性的举措为导向。我国也出台了一系列相关的法律法规，包括《电子签名法》《网络安全法》，人民银行《个人金融信息保护技术规范》等(更多有关法律法规参见附录)。

由于分布式网络的宽泛性，数字化的流动的灵活性，在新模式和新业务里，多方参与的协作架构里的责权利有所变化，在遵循既有法律法规的前提下，分布式数字身份领域还需要关注在新模式下的可实行性。

首先，数据的主权交给个人，特定个人的能力和意愿，与数据的价值、所承担的责任是否匹配？其次，数据在分布式网络里流动范围，如跨行业、跨境等，是否应该有所限制，如何限制？然后，分布式环境里有跨领域、跨地域的多方参与，发证、验证、授权等交互流程在不同主体名下的分布式账本节点上发生，如产生纠纷，如何定责，适用哪个地域、哪个领域的哪款法例？最后，整个体系的可信性和互通性，更多依赖新型的算法，那么法律法规对技术的接受和认可程度是否能支持行业探索？此外，利用大数据对用户行为进行追溯，其中涉及诸多法律问题，尚缺乏对应的法律法规予以解决。同样，这也是分布式数字身份下一步需要解决的问题。

完整法律法规的制定不会一蹴而就，针对行业应用，尤其是和国计民生有关的部分，本着“技术中立，风控优先，有法必依”的原则，应该抓住业务本质，遵守所在行业、所营业务的基本合规要求，规范运作。有关部门将敦促、监管相关的业务严格执行既有法规，同时，根据业务的发展，给出新的指导意见。

第七章 总结和展望

继往开来，数字身份的发展进程可分为 4 个阶段。

第一个阶段是“中心化身份”，由权威机构进行管理和控制。比如互联网早期，IANA 这样的组织确定了 IP 地址的有效性，ICANN 确定了仲裁域名的有效性，CA 帮助互联网站点证明其身份的真实性。这样做的弊端是用户被锁定在了单一管理机构中，他们在各个站点中的身份彼此割裂，并毫无自主控制权。

第二个阶段是“联盟身份”，初步具有了分布式特性，由多个机构或者联盟管理控制。比如微软的 Passport 计划，它允许用户在多个站点上使用相同的身份账号。但这样做的最终结果是集中式授权被划分为几个强大的巨头组织。

第三个阶段是“以用户为中心的身份”，核心是每个人都应该有权控制自己的数字身份。ASN 小组、Identity Commons、IIW 社区都为此做了很多努力。最终的成果是我们在登陆应用时，可以选择多种身份验证方式，比如手机、微信、微博账号、Facebook 等账号，但这样做的隐患是，这些服务节点有权关闭我们的账户，并使我们同时丧失多个站点的身份。

第四个阶段是“自我主权身份”（即分布式数字身份），为互联网建立一个统一的身份层，允许人们、组织和事物拥有他们自己的主权身份，管理属于他们自己的身份信息。

目前，分布式数字身份现在还处于初期阶段，国际国内由技术公司主导的行业规范和应用方兴未艾，百花齐放的同时，也需要寻求共识，共建生态。随着互联网社会生态越来越健全，人们对于数据产权的重视，消费者对数据平权（互联网服务商和用

户应该拥有平等的权利）的需求将会越来越大，这些声音现将会再进一步推动分布式数字身份的发展，更加清晰地反映出互联网社会的真实需求。

联盟也希望积极推动分布式数字身份相关技术规范和标准的建立，努力探寻更多适合分布式数字身份的应用落地的场景，建立拥有中国特色的分布式数字身份体系架构，并加强国际交流合作，与国际标准的分布式数字身份接轨。

长期看来，随着法律法规基础设施的不断完善，分布式数字身份技术将会进化出现符合其自身发展的标准化、法律规范等相关配套设施，来发挥其最大的作用。分布式数字身份的目标旨在加强相应监管的同时保证用户的隐私，实现数据真正掌握在用户自己手中。

为了更好地促进数字经济的发展，展望未来 WEB3.0 的重要基础设施，适应人们越来越丰富的数字生活，有必要尽早在网络安全底层治理和数据隐私保护层面进行思考，发展自主可控的信息安全技术，构建面向全社会的、安全的、便利的分布式数字身份体系，解决现有网络数字身份的安全、隐私、互通和所有权问题，进一步推进互联网数字身份的健康发展和相关可信网络设施的建设。

附录一：相关法律法规

[1]. GDPR：欧洲联盟于 2018 年发布全新的欧盟（EU）隐私法《通用数据保护条例》（General Data Protection Regulation，GDPR），GDPR 协调整个欧盟的数据隐私法律，并规定公司如何收集、存储、删除、修改及以其他方式处理欧盟公民个人数据。它适用于处理欧盟公民个人数据的任何公司，无论该公司是否在欧盟有任何实体存在，或者是否有任何欧盟客户

[2].《中华人民共和国网络安全法》2016 年我国发布第一部全面规范网络空间安全管理方面问题的基础性法律《中华人民共和国网络安全法》，其中明确规定“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认”

[3].《中国人民共和国电子签名法》由全国人大常务委员会于 2004 年通过，在 2019 年进行了修正，确立电子签名人身份认证的法律地位，促进电子签名认证服务的快速发展

[4].《关于加强网络信息保护的决定》为了加强对个人信息的保护，第十一届全国人大常委会于 2012 年通过了《关于加强网络信息保护的决定》，工信部于 2013 年发布了《电信和互联网用户个人信息保护规定》

[5].《信息技术 安全技术 隐私保护框架》（ISO/IEC 29100：2011）ISO/IEC JTC1/SC27 WG5（身份管理与隐私保护标准工作组）

[6].《信息技术 安全技术 部分匿名及不可链接鉴别需求》（ISO/IEC 29191:2012）ISO/IEC JTC1/SC27 WG5（身份管理与隐私保护标准工作组）

[7].《身份管理中的用户身份信息保护等级评估准则》和《在应用 RFID 技术中保护个人可标识信息的指导原则》（ITU-T X.1275） ITU-T 制定，用以对身份管理过程中身份提供方和依赖方的隐私保护等进行评估

[8].《个人身份信息机密性保护指南》（NIST SP 800-122） NIST

[9].《派生个人身份验证（PIV）凭据指南》（NIST SP 800-157）NIST

[10].《用于个人身份验证的生物识别规范》（NIST SP 800-76-2）NIST

[11].《在物理访问控制系统（PACS）中使用 PIV 证书的建议》（NIST SP 800-116）NIST

[12].《电力行业的身份和访问管理（草案）》（NIST SP 1800-2）NIST

[13].《信息安全技术个人信息安全规范》针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，从国家标准层面，明确了企业收集、使用、分享个人信息的合规要求，为企业制定隐私政策及个人信息管理规范指明了方向。

[14].《数据安全管理办法（征求意见稿）》《信息安全技术个人信息安全规范（征求意见稿）》《信息安全技术数据出境安全评估指南（征求意见稿）》对《网络安全法》框架下核心内容有细化和延伸。

[15].《个人金融信息（数据）保护试行办法（征求意见稿）》规定了个人金融信息保护，包括以保护个人金融信息为核心目标，按个人信息全生命周期，对个人金融信息收集、使用、存储、展示、对外提供、跨境流动的不同应用场景进行了全面细致的规定;

[16].《中国人民银行金融消费者权益保护实施办法（征求意见稿》相关章节专门规定了消费者金融信息保护。

附录二：协议规范

[1]. Reed D, Sporny M, Longley D, Allen C, Grant R, Sabadello M (2019) Decentralized Identifiers (DIDs) v1.0 – Data Model and Syntaxes for Decentralized Identifiers. (W3C Credentials Community Group). Available at https://www.w3.org/TR/did-core/

[2]. Sporny M, Longley D, Chadwick D (2019), Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web. (W3C Credentials Community Group). Available at https:// https://www.w3.org/TR/vc-data-model/

[3]. Longley D, Sporny M (2020), Linked Data Proofs 1.0 - Draft Community Group Report 03 March 2020. (W3C Credentials Community Group). Available at https://w3c-ccg.github.io/ld-proofs/

[4]. Decentralized Identity Foundation (2019), Well Known DID Configuration. Available at https://identity.foundation/.well-known/resources/did-configuration/

[5]. Decentralized Identity Foundation (2019), Self-Issued OpenID Connect Provider DID Profile. Available at https://identity.foundation/did-siop/

[6]. Reed D, Law J, Hardman D, Lodder M(2019), (Evernym Inc.), Available at https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md

[7]. Hardman D, Curren S, Buchner D (2019), Rhythm and Melody: How Hubs and Agents Rock Together. Available at https://www.hyperledger.org/blog/2019/07/23/rhythm-and-melody-how-hubs-and-agents-rock-together

[8]. Sporny M, Kellogg G, Lanthaler M (2014) JSON-LD 1.0 - A JSON-based serialization for linked data. (W3C). Available at https://www.w3.org/TR/json-ld/

[9]. Hughes A, Sporny M, Reed D (2019) A Primer for Decentralized Identifiers - An introduction to self-administered identifiers for curious people. (W3C Credentials Community Group). Available at https://w3c-ccg.github.io/did-primer/

[10]. Sabadello M (2017) A universal resolver for self-sovereign identifiers. (Medium - Decentralized Identity Foundation). Available at https://medium.com/decentralizedidentity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

[11]. Decentralized Identity Foundation (2019) DIF Identity Hubs. Available at https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md

[12]. Sabadello M, Den Hartog K, Lundkvist C, Franz C, Elias A, Hughes A, Jordan J, Zagidulin D (2018) Introduction to DID Auth. Rebooting the Web of Trust VI. Available at: https://nbviewer.jupyter.org/github/WebOfTrustInfo/rebooting-the-web-of-trustspring2018/blob/master/final-documents/did-auth.pdf

[13]. W3C Recommendation (2019). Web Authentication: An API for accessing Public Key Credentials Level 1. Available at : https://www.w3.org/TR/webauthn/

[14]. Barker E, Smid M, Branstad D, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130

[15]. Guy A, Lamers D, Looker T, Sporny M, Zagidulin D, Bluhm D, Hamilton Duffy K (2019) Encrypted Data Vaults. Rebooting the Web of Trust IX. Available at https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/finaldocuments/encrypted-data-vaults.pdf

[16]. Hyperledger (2019) Hyperledger Aries Proposal. Available at https://wiki.hyperledger.org/display/HYP/Hyperledger+Aries+Proposal

[17]. Allen C (2016) The Path to Self-Sovereign Identity (lifewithalacrity.com). Available at https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[18]. IPFS (2019) IPFS. Available at https://ipfs.io

[19]. ZKProofs (2019) Zero-Knowledge Proofs. Available at https://zkp.science

[20]. VON (2019) Verifiable Organizations Network. Available at https://vonx.io

[21]. Sovrin (2019) Sovrin. Available at https://sovrin.org

分布式数字身份产业联盟

www.did-a.org.cn

让数字世界互信相连

共建分布式数字身份基础设施 打造可信开放数字新生态

北京市海淀区学清路9号汇智大厦B楼17层

mishuchu@did-a.org.cn

日常事务：

郭秉静 15811012030

陈　欣 15068111381

廖　莎 13269642294

工 作 组：

卢缃梅 15157114656