时戳资本
TIMESTAMP CAPITAL
行业研究报告系列

去中心化身份研究报告

时戳资本行业研究报告-14

目录

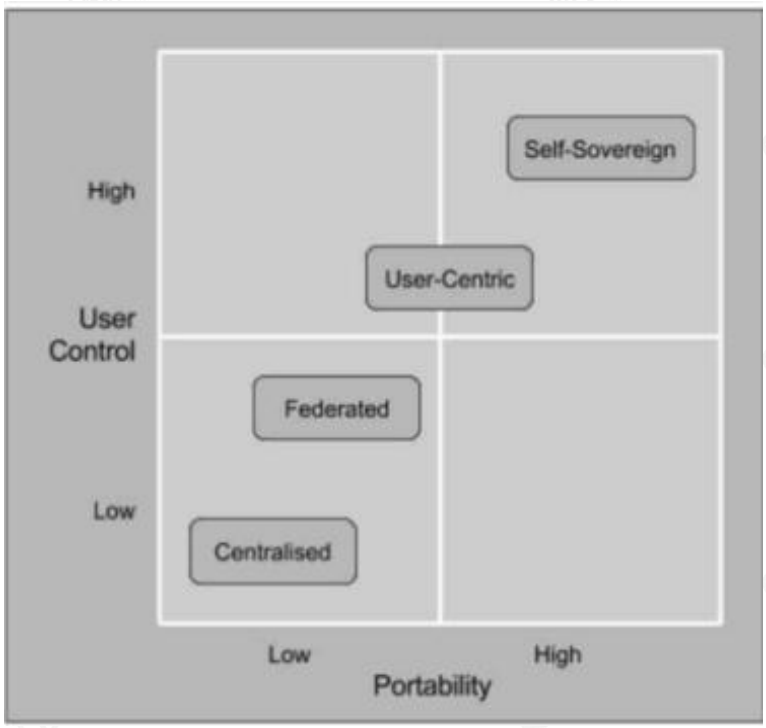
去中心化身份研究报告

一、概述

1. 身份的定义与发展历史

身份的概念非常广泛，涵盖了社会、政治、经济、文化等多个维度。通常，当我们在谈论“身份”的时候，我们所讨论的，更多的是社会人之间的关系，而这种关系，则以“身份标识”的形式呈现出来。社会中的每一个人都有多重身份关系，因此也就具有多个身份标识。例如我们用身份证、护照来标识自己作为中国公民的身份，用结婚证来标识自己作为丈夫或者妻子的身份等等。不仅只有自然人拥有身份，法人、社会团体、组织机构同样拥有身份。

随着互联网的出现和普及，身份有了另外一种表现形式，即数字身份。数字身份的演进经历了四个阶段，分别是：中心化身份、联盟身份、以用户为中心的身份以及自我主权身份。



（图 1：数字身份演进阶段）

1.1 中心化身份

中心化身份是由单一的权威机构进行管理和控制的。中央集权化的机构，像是 1988 年成立的 IANA（Internet Assigned Number Authority，互联网号码分配局）管理着国际互联网中使用的 IP 地址、域名和许多其他参数。到了 1998 年，ICANN（Internet Corporation for Assigned Names and Numbers，互联网名称与数字地址分配机构）成立，接管了包括管理域名和 IP 地址的分配等与互联网相关的任务。到了 1995 年，证书颁发机构（CA，Certificate Authority），作为负责发放和管理数字证书的权威机构，以及在电子商务中受信任的第三方，承担公钥体系中对用户的公钥进行认证，从而验证用户的身份。

中心化身份的本质是，中央集权化的权威机构掌控着身份数据，用户是否具有某一个身份，某一个身份是真实亦或是虚假，这些问题均由权威机构而非用户来决定。随着互联网的不断发展，网站数量的不断增加，中心化身份带来了许多混乱和限制。用户的身份数据和其他个人数据混乱而零碎地散落在互联网上，需要在几十个甚至上百个网站上处理对应数量的多个身份，然而这些身份却不为用户所控制。

尽管中心化身份是数字身份发展的最早阶段，但时至今日，互联网上的身份大部分仍是中心化的模式。数字身份由证书颁发机构、域名注册机构以及网站等所有。

1.2 联盟身份

20 世纪末，数字身份的发展获得了重大进展。中心化身份导致的身份数据的混乱而零碎等弊端，催生出了联盟身份这种由多个机构或联盟管理控制的身份体系。简单地说，用户的在线身份数据具备了一定程度的可移植性，例如允许用户登录某个网站时，可以使用其他网站的账户信息，类似于 QQ、微信或者微博的跨平台登录。

微软于 1999 年推出的 Passport 计划，首次提出了“联盟身份”的概念和解决方案。Passport 是一个由微软控制的中央式身份认证服务，提供了中央统筹式的单一登陆服务，允许用户通过一次登录就可以获得访问很多网站的权限，但是，这使得微软成为联盟的统筹中心，拥有极大的权力。

作为微软的竞争对手，Sun Microsystems 公司[1]针对微软推出的 Passport 方案，于 2001 年联合索尼、NTT DoCoMo 等 32 家公司成立了“自由联盟”(Liberty Alliance Project)，目的是建立开放标准的网络认证系统。自由联盟提供技术规范与商业指南来

[1] Sun Microsystems 公司：https://en.wikipedia.org/wiki/Sun_Microsystems

支持跨企业的身份认证服务，可以让不同的服务供应商加入一个联邦式的信赖网络中。[2]在这一时期，中央集权的力量被几个权威机构瓜分，这意味着，用户的身份数据，仍然被几个独立的权威机构控制。

1.3 以用户为中心的身份

2001 年，Identity Commons 开始整合所有有关数字身份的工作，并将工作重点集中在去中心化上，这也推动了 2005 年互联网身份工作组（IIW，Internet Identity Workshop）的创建。IIW 强调以用户为中心的身份，在创建在线身份的过程中，将用户放在首要和中心的地位。

以用户为中心的身份，希望实现的是用户通过授权和许可，可以决定身份的存储和使用以及将身份从一个服务共享到另一个服务。因此侧重于三个元素：用户的许可、互操作性以及基于用户对数据的完全掌控。

但是，以用户为中心的身份计划并没有获得成功。以 OpenID 为例，用户理论上可以注册属于自己的 OpenID，但是由于技术门槛较高，普通的互联网用户更倾向于在一个公共的并且相对可靠的网站上注册 OpenID 来登录到其他的网站。因此，用户注册的 OpenID 有着随时被网络提供商剥夺的风险，这意味着，用户并没有完全取得自己身份数据的掌控权。

1.4 自我主权身份

自我主权身份是以用户为中心的身份的进阶阶段，二者的共同之处在于，都以用户完全掌控自己的身份数据为出发点，但自我主权身份更进一步，数据的收集、存储和使用都去中心化地分布在一个生态系统中，同时对于个人身份的验证，允许其他的普通用户发表含有他人身份信息的声明（即下文将提到的“可验证声明”）。自我主权身份提供了三个必需的元素：单独控制、安全性和完全可移植性。它取消了上述三个阶段的集中外部控制。身份完全由个人(或组织)拥有、控制和管理。从这个意义上说，个人是他们自己的身份提供者——没有外部的一方可以声称为他们“提供”身份，因为身份本质上是他们的。个人的数字存在是独立于任何单一组织的。

---

2 《深度分析：选“自由联盟”还是微软 Passport》，http://tech.sina.com.cn/it/2003-11-20/1010258495.shtml

要使身份具有真正的自我主权，这种基础设施需要驻留在分散信任的环境中，而不是属于或由任何单个组织控制。分布式账本技术（或区块链技术）是实现这一目标的突破口。它第一次使多个机构、组织和政府能够合作，形成一个类似互联网的去中心化网络。在互联网上，数据被复制到多个地点，以抵御故障和篡改。虽然分布式账本技术已经出现了一段时间，但比特币和以太坊等新技术的出现，使其潜力得到了更大的发挥，尤其是在去中心化和安全方面。这些系统使用分布式账本和加密技术来创建不可变的身份记录。个人创建一个身份“容器”，可以这些系统使用分布式分类账和加密技术的组合来创建不可变的身份记录。个人创建一个身份“容器”，允许他们接受来自任意数量的组织(包括国家)的属性或凭证，在一个开放给任何组织参与的网络生态系统中接受来自任意数量的组织(包括国家)的属性或凭证。

2. 数字身份的现状

2.1 传统的身份体系——公钥基础设施（PKI）

传统的身份管理体系基于 PKI（Public Key Infrastructure）系统，即公钥基础设施。公钥基础设施的目的是从技术上解决网络身份认证、电子信息的完整性和不可否认性等安全问题。公钥基础设施是使用非对称加密算法的原理和技术实现并提供安全服务的具有通用性的安全基础设施。简单来说，PKI 就是创建、管理、存储、分发和撤销基于公钥加密的数字证书所需要的一套硬件、软件、策略和过程的集合。而这里说到的数字证书，是一种数字标识，可以理解为相当于护照、驾驶执照之类用以证明实体身份的证件。

数字证书是 PKI 的关键技术，可以实现可信的数字身份，通过和密码机制相结合，提供认证、授权或数字签名等服务，最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关（证书授权中心）的名称，该证书的序列号等信息。数字证书是一个用户的身份与其所持有的公钥的结合，在结合之前由一个可信任的权威机构——证书机构（Certificate Authority，简称 CA），来验证用户的身份，然后由 CA 对该用户的身份及对应公钥相结合的证书进行数字签名，来证明其证书的有效性。

字段	描述
版本(Version)	X.509证书版本号，目前取值1/2/3
证书序号(Serial Number)	该CA产生的证书的唯一标识号
签名算法标识符 (Signature Algorithm Identifier)	CA签名数字证书使用的算法
签名者(Issuer Name)	CA的可区分名字
有效期(之前/之后) (validity(Not Before/Not After)	该证书的有效日期，至少精确到秒
主体名(Subject Name)	证书持有者的名字
主体公钥信息 (Subject Public Key Information)	与公钥和公钥算法相关的信息

（图 2：数字证书构成 ）

PKI 体系所提供的数字证书，可以提供身份确认和加密通信的功能。举个简单的例子，假如用户 A 需要和一个自称为 B 的用户通信，B 会在通信开始时将数字证书发送给 A，通过这个数字证书，就证实了该用户就是 B 本人。由于数字证书中包含了公钥，A 便使用公钥将需要发送给 B 的内容进行加密，然后发送给 B。用公钥加密过的内容，只能用 B 自己才有的私钥才能解密。这样的话，如果 A 发送给 B 的内容被他人窃取的话，他人也无法解密。

由于数字证书由 CA 发布，因此 CA 的可信度与证书的可信度直接挂钩，也就是与整个 PKI 体系的可信度息息相关。在很多国家 CA 机构都是由政府主导建设，通常 CA 机构的熟练也是有限的，因此在 PKI 的系统中，用户身份的发布、管理、存储及撤销等都由中心化的权威机构所掌控，这也是传统的身份管理体系所存在的弊端。

2.2 去中心化身份存在的必要性和优势

从历史上看，我们在日常交往中需要的身份证件——护照、驾照、社保卡等，都是由民族国家和私营机构等中央机构颁发的。使用这种标识带来许多问题:（1）如果国家吊销个人凭证，个人可能会失去身份；（2）身份受到国家或地域的限制，某一民族国家颁发的身份，通常不被其他国家接受；（3）集中控制仅在一个司法管辖区或一个在线服务中。即使是上文所介绍的 PKI 体系，用户的身份也是掌握在中心化机构手中，用

户对于个人的身份数据并没有控制权。我们也常常可以看到用户身份数据被泄露的事件发生，例如，2018 年 Facebook 爆发数据泄露丑闻，掌控在 Facebook 手中的将近五千万的用户数据隐私被泄露；同样是在 2018 年，华住集团爆发了国内迄今为止规模最大的酒店信息泄露事件，约 5 亿条公民个人信息在暗网上被拍卖。这些大规模的数据泄露事件，对用户的隐私安全造成极大的威胁。

随着区块链技术的出现，新的身份管理模式也随之出现。基于区块链技术的去中心化的身份管理方法具有分布式数据存储、点对点传输、加密安全、共识确认等特征，可以有效解决身份验证和操作授权问题。区块链身份管理为数字身份提供安全且去中心化的解决方案，从而实现分布式信任模型。区块链技术通过在去中心化网络上提供自我主权身份来改变现有身份管理系统，因为共享多个 ID 可能导致安全问题和数据泄露。由于区块链实现了去中心化，因此它消除了任何交互和沟通之间的中介。区块链技术通过解决身份盗窃，重复 KYC（Know Your Customer）和缺乏对个人数据的控制等问题，有助于改善现有的身份管理。

通过区块链技术，使用自主权的数字身份允许用户真正拥有并控制自己的个人数据和资产。相对于传统的身份认证，基于区块链技术的数字身份认证具有保证数据真实有效、保护用户隐私安全、可实现跨部门、跨行业共享的特征，其优势在于：

（1）分散化（去中心化）：基于分布式账本进行使用和存储，避免了身份数据被单一的中心化的权威机构所控制；

（2）防篡改：基于区块链的不可篡改特性，身份数据也将难以篡改；

（3）控制权回到用户手中：用户掌握身份数据的控制权，是自我主权身份的特点和要求；

2.3 当前基于区块链技术的去中心化身份市场规模及趋势

2018 年基于区块链技术的身份管理市场规模大约是 9040 万美元，预计到 2025 年，市场规模将达到 73.084 亿美元，在 2018 年至 2025 年的预测期内以 83.2%的复合年增长率增长[3]。

市场的主要驱动因素是全球现有模型对安全性的担忧不断增加，对垂直行业对区块链身份标识解决方案的需求不断增长以及自我主权身份意识的提高。

[3] 数据来源：Global Blockchain Identity Management Industry 2018 Market Research Report, http://www.digitaljournal.com/pr/3851926%20target=#ixzz5jFocVU7X

区块链身份管理市场根据提供商分为 3 类：应用程序提供商，中间件提供商和基础设施提供商。这些提供商提供基于区块链的平台开发基础设施。在这些类型中，应用程序提供商类型是整个市场中增长最快的部分。

在地理覆盖范围方面，区块链身份管理市场已划分为 5 个主要区域，即北美，亚太（APAC），欧洲，中东和非洲以及拉丁美洲。北美在技术应用和基础设施方面被认为是最先进的地区。各种组织，包括政府都在积极采用区块链身份管理技术。

此外，由于资本的增加，初创企业数量的显著增长，预计亚太地区将以更高的速度增长。亚太主要国家或地区（如日本，澳大利亚，新西兰，香港和新加坡）的主要金融中心和政府组织为采用区块链身份管理解决方案提供了许多机会。但是，缺乏一套共同的监管标准和不确定的监管环境以及对用户真实性的担忧可能会阻碍各个地区市场的增长。

2.4 现有的一些典型的项目和模式

尽管区块链项目的应用落地一直是一个难以解决的难题，但是基于区块链技术的去中心化身份这一领域，其应用落地在技术和应用场景的实现上都相对容易。目前，全球已经发展了非常多的去中心化数字身份项目，以下展示了部分相对较为知名的项目：

项目名称	具体内容
微软 DID	微软开发的去中心化身份识别系统
Sovrin	一个区块链数字身份项目，由 Sovrin 基金会发起，现在已宣布将在“超级账本”联盟进行孵化
Uport	基于以太坊的数字身份应用，它可以进行用户身份验证并且与以太坊上其他应用进行交互，可以免密码登录
Evernym	Evernym 及其主权身份解决方案旨在相互交易的个人、组织和连接的设备之间建立信任体系
Civic	基于区块链和生物识别的多因素身份认证系统，可以在移动端无需用户名和密码的情况下进行准确安全的用户身份识别
ShoCard	一个使用区块链技术而构建的移动身份平台，该平台在保护用户隐私的同时提供了一个简单而直观的移动应用程序，用于进行明确的身份

	验证
IDHub	基于区块链技术的去中心化数字身份应用平台
Ontology 本体	新一代分布式信任链网,架构了一个分布式融合的信任体系，将信任的多样性在一体化的协议体系下进行协同，整合分布式多维实体认证体系及各类不同区块链体系与信息系统，纳入多源身份认证和多源信息交换协议，并提供不同分布式应用场景的开放基础模块，实现分布式 P2P 的信任体系，构建跨链、跨系统、跨行业、跨应用和跨终端的分布式信任基础设施

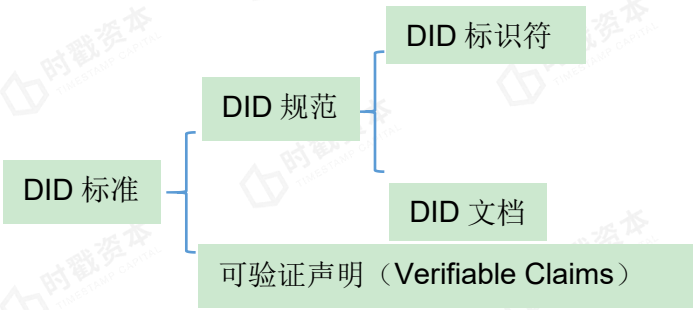
二、去中心化身份的开源标准和成果

代表自我主权身份的去中心化身份标识符，可以由用户直接创建和注册，这对于用户来说意义重大，因为标识符是任何身份和通讯系统的基础，没有标识符，实体之间无法建立直接的联系、传递消息或数据共享。

当前，去中心化身份所使用的开源协议标准主要有 W3C[4]的去中心化标识符（Decentralized Identifier,简称 DID)、W3C 的可验证证书(Verifiable Credentials）以及 DIF 基金会（Decentralized Identity Foundation，DIF）的 DID Auth（身份认证）。

另外，DIF 基金会也在 DID 领域中做了非常多重要的工作。

1.W3C 的 DID 标准



[4] W3C：World Wide Web，万维网联盟,创建于 1994 年，是 Web 技术领域最具权威和影响力的国际中立性技术标准机构。到目前为止，W3C 已发布了 200 多项影响深远的 Web 技术标准及实施指南.

1.1 DID 规范

W3C 的 DID 规范包含两大内容，分别是 DID 标识符和 DID 文档。

DID（Decentralized Identifier），即去中心化标识符，又叫全局唯一标识符，是用于可验证的“自我主权身份”的新型标识符。DID 通过使用生成具有足够熵的 128 位值的算法，使得碰撞的几率极小，也就是说，产生两个相同的 DID 几乎是不可能的，因此可以实现唯一性的特点。由于 DID 是基于区块链技术，使用分布式网络进行注册，因此不需要依赖于身份提供者、证书颁发机构或其他任何第三方，这种去中心化的特性意味着用户的身份数据掌握在其自己手中，对于 DID 具有完全的控制权。然而根据 Zooko 三角形理论[5]，没有任何标识符系统能够同时实现对人类有意义（易读、易记忆）、安全性和分散性（去中心化）这三个特性，通常一个标识符系统最多可以实现其中的两个特性，因此对于 DID 而言，它为用户提供了安全性和分散性，但是无法做到易读、易记忆，所以 DID 通常表现为“did：example：123456789abcdefghi”的形式。

DID 文档包含以下内容：DID 主题、公钥、身份验证、授权及服务端点。

DID 文档内容	具体内容
DID 主题	DID 主题，也就是 DID 文档所描述的该 DID。由于 DID 的全局唯一特性，因此在 DID 文档中只能有一个 DID。
公钥	公钥用于数字签名及其他加密操作，这些操作是实现身份验证以及与服务端点建立安全通信等目的的基础。如果 DID 文档中不存在公钥，则必须假定密钥已被撤销或无效，同时必须包含或引用密钥的撤销信息（例如，撤销列表）。
身份验证	身份验证的过程是 DID 主题通过加密方式来证明它们与 DID 相关联的过程。
授权	授权意味着他人代表 DID 主题执行操作，例如当密钥丢失的时候，可以授权他人更新 DID 文档来协助恢复密钥。
服务端点	除了发布身份验证和授权机制之外，DID 文档的另一个主要目的是为主题发现服务端点。服务端点可以表示主题希望公告的任何

[5] Zooko 三角：以 Zcash CEO，Zooko Wilcox 的名字命名，是网络中命名系统的三个理想性质的三难选择困境。
安全：当你查找一个名字时，你能够得到正确的结果，而不是一个假名。
去中心化：没有中心化权威机构控制所有的名字。
可理解的：名字是人们可以记住的，而不是某一长串随机的字符。
Zooko 声称数字名称是无法同时包含以上 3 种性质的。

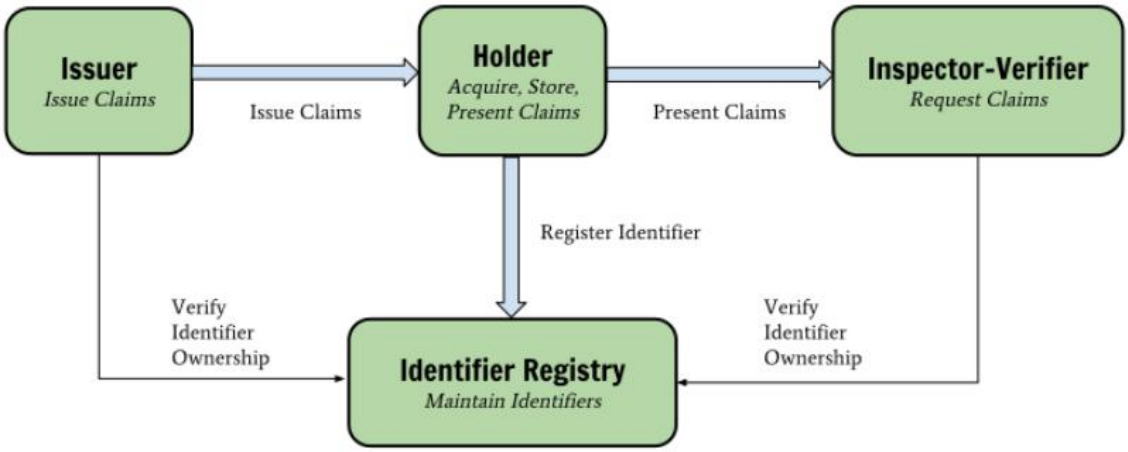
	类型的服务，包括用于进一步发现、身份验证、授权或交互的去中心化身份管理服务。

1.2 可验证声明（Verifiable Claims）

1.2.1 可验证声明概述

DID 和 DID 文档本身不携带任何用户的个人身份信息，例如用户姓名，家庭住址，电话号码等等。将 DID 绑定到现实世界中的实体（例如个人或公司）的过程，体现在 W3C 的可验证声明的规范中。

可验证声明，为证明实体的身份数据提供了一个数据模型，包括关于身份实体的可以核查的信息和背景，例如姓名，身份证，家庭住址，大学学位等。随着人们在生活和工作中对互联网的依赖越来越强，但是人们很难在网络上以可验证的方式传输诸如身份证明，驾驶执照，教育资格和医疗保健数据等凭证，同时又能达到保护个人隐私的目的。用户基于受信任方发布的即时传送的可信任声明，可以迅速地建立起彼此之间的信任。



（图 3 ：可验证声明）

在可验证声明的系统中，声明通常由这样几部分组成：

发行者（Issuer）——创建声明的实体，例如政府、银行、大学等机构和组织；

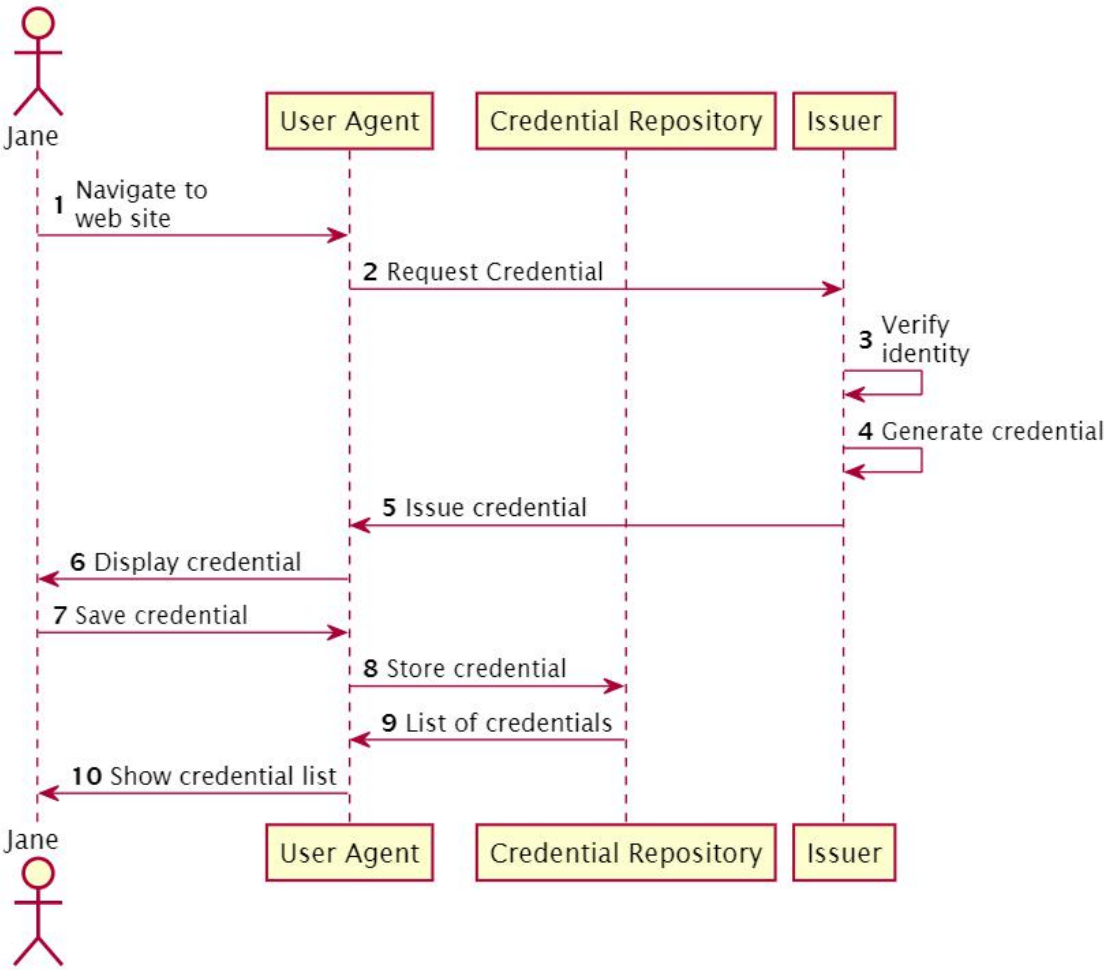
验证者（Inspector）——接收可验证的声明进行验证，并用于某种类型的服务；

持有者（Holder）——收到并持有可验证声明的实体，与声明中所描述的实体，可能不是同一个实体；

可验证的数据注册表（Identifier registry）—— 维护主体标识符，例如员工数据库，政府数据库，分布式账本技术（即区块链技术）等。

1.2.2 可验证声明用例

1.2.2.1 如何创建可验证声明？下图阐明了用户创建可验证声明的流程：



（图 4 ：创建可验证声明）

具体步骤为：

a. Jane 首先要求她的用户代理[6]帮她获得关于她身份的可验证声明；

b. 用户代理将 Jane 的物理文件（比如身份证、大学文凭、驾驶执照等）连接到能够验证其身份的发行者；

c. 发行者检查文件；

[6] 用户代理：管理 DID 和相关数据的应用程序

d. 当发行者觉得文件符合要求，就会为 Jane 生成一个可验证声明，这个声明包含了与 Jane 之前提供的文件相关联的身份信息；

e. 发行者将 Jane 的可验证声明发给 Jane 的用户代理；

f. Jane 获得声明并进行查看，确保其正确反映自己的身份信息；

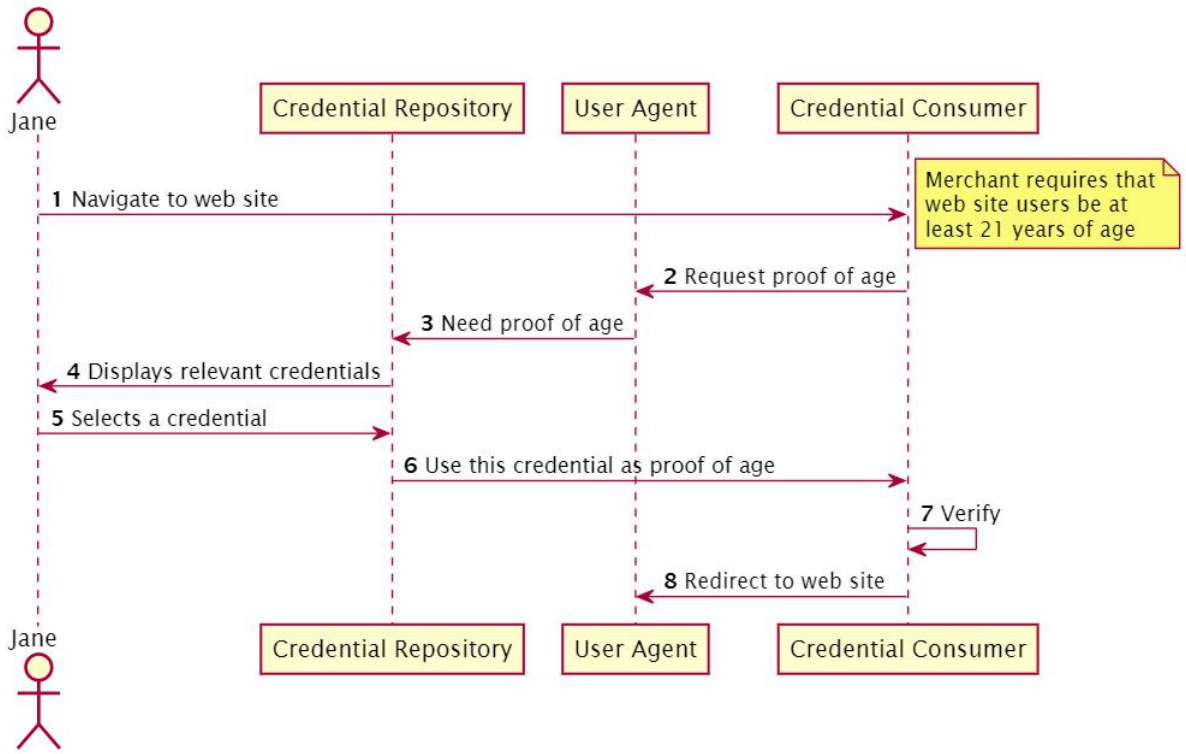
g. 当 Jane 对声明确认并认可后，她指示她的用户代理保存该可验证声明，以便将来可以使用它；

h. 用户代理与 Jane 的凭证存储库进行通信，指示它存储新的声明；

i. 凭证存储库将凭证清单返还给用户代理；

j. 用户代理将凭证清单展示给 Jane。

1.2.2.2 如何使用可验证声明？下图阐明了用户使用可验证声明的流程：



（图 5：使用可验证声明 ）

具体步骤为：

a. Jane 想要在网上商城购物；

b. 商店要求 Jane 年满 21 岁并且提供证据进行证明（通过与用户代理连接的 API 接口）；

c. Jane 的用户代理要求她的证书存储库（Credential Repository[7]）提供证明；

d. 证书存储库会提供几份可验证声明（例如护照、身份证和驾驶证）来进行证明；

e. Jane 选择其中的一份可验证声明进行核实并共享给商店；

f. 证书存储库将 Jane 选中的这份可验证声明返回给用户代理所支持的 API 调用，然后 API 调用将这份可验证声明传递给商店；

g. 商店服务器将验证这份声明是否有效以及是否满足要求；

h. 商店指示用户代理将验证的声明展示给它。

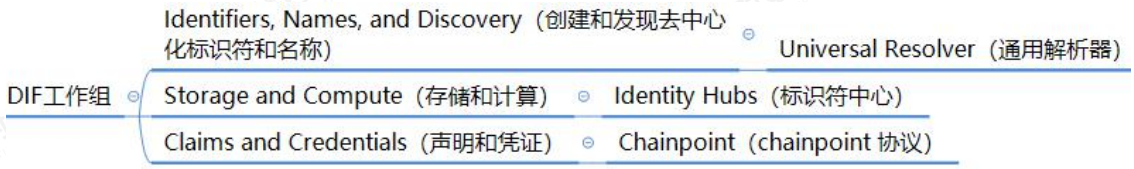
1.3 DID Auth

DID Auth，指的是对身份的验证。在早期的身份协议中，我们只能表达诸如“根据身份提供者 X，我的标识符是 Y”这样的陈述，但从来没有真正表达过“我是我”。因此，DID Auth 要解决的问题，就是如何证明“我是我”。DID Auth 可以定义为身份所有者在各种设备上（比如 web 浏览器、移动设备等）的帮助下向他人证明他们对自己的 DID 享有控制权的过程。DID Auth 包括建立相互验证的通信通道以及对网络站点和应用程序进行身份验证的能力。DID 可以是一方向另一方证明对 DID 控制权的单向过程，也可以是双方相互证明对 DID 控制权的双向过程。

2.Decentralized Identity Foundation（DIF）的工作成果

Decentralized Identity Foundation，即 DIF，成立于 2017 年，是一个致力于提高基于区块链建立的身份系统互操作性和标准的联盟。DIF 的一个目标是为身份验证创建通用协议，类似于金融交易的全球标准，或者超越国界的 DNS 协议。DIF 目前分为三个工作组，按功能区域划分，旨在建立并推动由开源代码支持的新兴标准规范。这三个工作组分别致力于解决三个功能领域的问题：（1）在分布式系统（如区块链和分布式账本）中创建和发现去中心化标识符和名称；（2） 安全，加密，保护隐私的存储和数据计算；（3）生态系统参与者及其客户将 DID 签名的声明集成到他们的应用和服务中。如下图所示：

[7] 凭证存储库是一个标识符注册表，通常是一个应用程序，用于存储和保护对持有者凭证和可验证声明的访问。



（图 6：DIF 工作组 ）

2.1 创建和发现去中心化标识符和名称（Identifiers, Names, and Discovery）

去中心化身份的关键部分是如何在没有中心化的标识符系统（例如电子邮件）的情况下识别人员、组织或设备。DIF 该工作组的成员从事的是协议和系统的开发工作，这些协议和系统支持跨底层分布式系统(如区块链和分布式账本)创建、解析和发现去中心化标识符和名称。主要的系统是通用解析器（Universal Resolver）。

在传统的身份识别和认证体系中，身份标识符一直被控制在中心化的权威机构手中。而通用解析器，可以帮助用户基于自我主权身份的理念，重新构建身份体系和结构，不再需要中心化的机构来主导注册、维护和撤销标识符的工作。通用解析器的功能是发现、检索和解析与身份标识符相关联的信息，通过解析给定的标识符，以发现公钥、服务端点以及与标识符相关联的其他元数据。

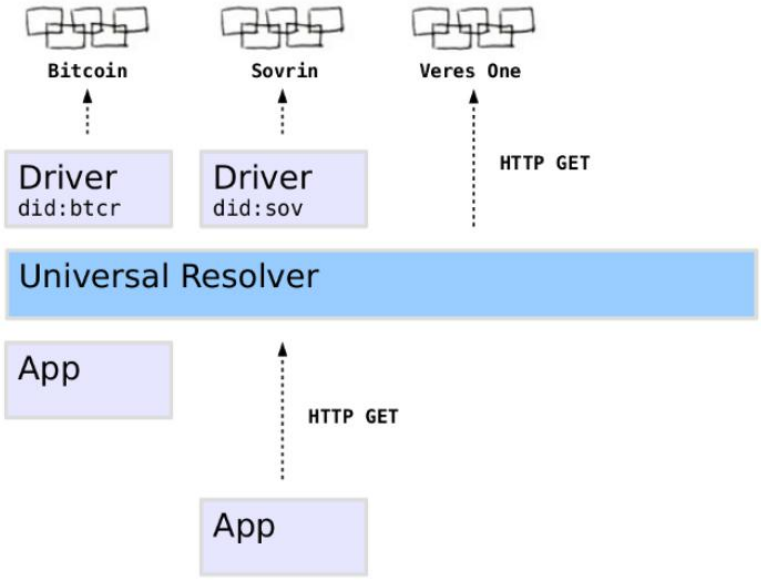
通用解析器提供了统一的界面，用于解析任何类型的去中心化标识符，这使得更高级别的数据格式（例如上文提到的可验证声明）和协议，无论使用哪一种区块链系统（例如比特币系统或 Sovrin 系统），都可以构建在标识符层之上。

通用解析器利用一组支持多种类型的标识符的驱动程序（driver）来提供一种标准的方法，通过调用 Docker 容器[8]，Java API 或远程 HTTP GET[9]可以轻松实现驱动程序的添加，具有高度可扩展性。驱动程序用于跨越区块链系统内查找和解析去中心化标识符，并返回标识符文档对象(DDO)， DDO 则封装了与标识符关联的 DPKI（去中心化公钥基础设施，与中心化的公钥基础设施，即 PKI 相对）元数据。

---

[8] Docker 容器是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的 Linux 机器上，也可以实现虚拟化。容器是完全使用沙箱机制，相互之间不会有任何接口(类似 iPhone 的 app)。几乎没有性能开销,可以很容易地在机器和数据中心中运行。最重要的是,他们不依赖于任何语言、框架包括系统。

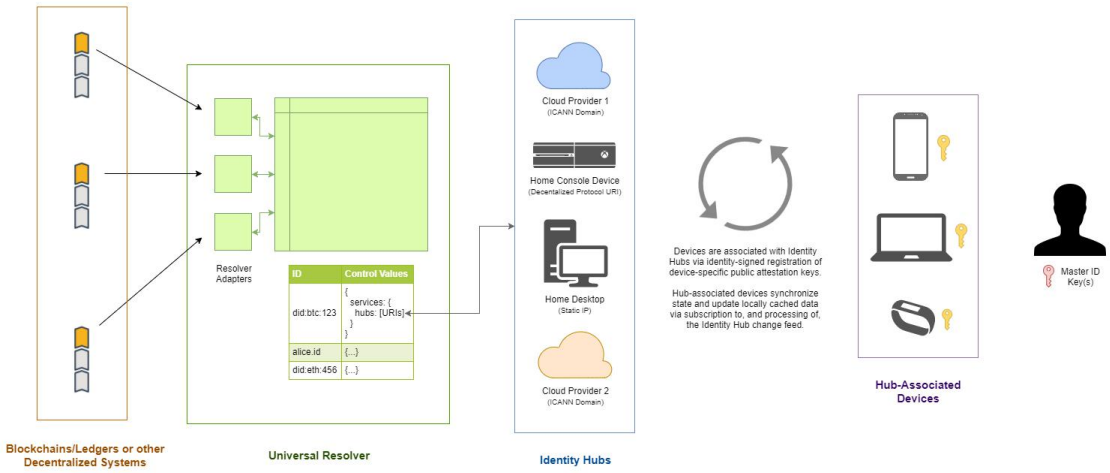
[9] HTTP GET：超文本传输协议（HTTP）的设计目的是保证客户机与服务器之间的通信。HTTP 的工作方式是客户机与服务器之间的请求-应答协议。web 浏览器可能是客户端，而计算机上的网络应用程序也可能作为服务器端。在客户机和服务器之间进行请求-响应时，两种最常被用到的方法是：GET 和 POST。
GET - 从指定的资源请求数据。
POST - 向指定的资源提交要被处理的数据



（图 7： 通用解析器系统）

2.2 存储和计算（Storage and Compute）

数据的安全、加密、隐私存储和计算是分布式身份系统的重要组成部分。用户除了对标识符和名称的创建需要自主权以外，同样需要对数据的存储享有完全的权利，以实现只有用户才能访问自己的身份数据的目的。DIF 为了实现对于身份数据的存储和交互，设计开发了 Identity Hubs（标识符中心），将用于身份交互和去中心化应用的个人数据库进行加密。



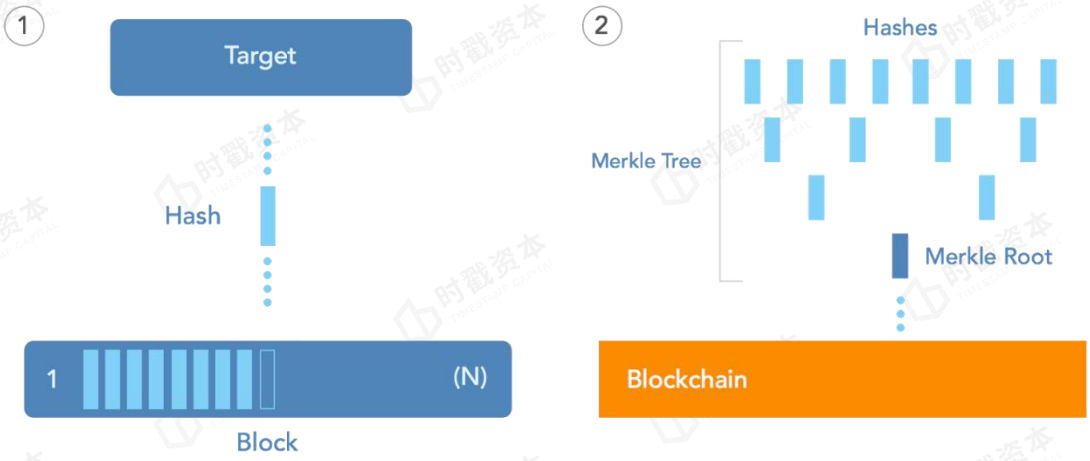
（图 8：Identity Hubs 架构）

2.3 声明和凭证（Claims and Credentials）

不同于中心化的身份管理系统，在去中心化的身份管理系统中，关于用户身份的声明和凭证并不由中心化的权威机构发布，因此对身份声明和凭证的验证是实体之间建立信任的关键。用于数据验证的 Chainpoint 协议，是一种在区块链中最大限度地锚定数据并生成区块链收据的提高区块链可伸缩性的标准。每个收据都包含验证数据所需的信息，而无需依赖可信的第三方。Chainpoint 的工作原理可分为三个步骤，分别是：（1）将数据锚定在区块链上；（2）创建区块链收据。

2.3.1 将数据锚定在区块链上

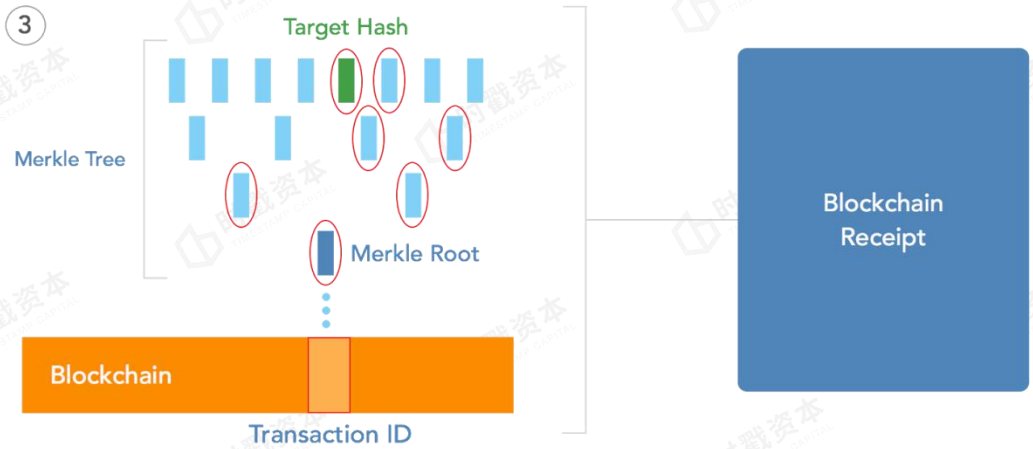
要将数据锚定在区块链中，首先需要使用标准哈希函数(如 SHA-256)来生成目标数据的唯一哈希值。多个哈希组合成一个块。这些块定期用于生成 Merkle 树，并且 Merkle 根通过交易发布到区块链中。通过将多个哈希整理到 Merkle 树中并发布 Merkle 根，我们可以使用单个交易在区块链中锚定大量数据。



（图 9：数据锚定 ）

2.3.2 创建区块链收据

区块链收据提供了在特定时间内存在某些数据的证据。它包含证明单个哈希是 Merkle 树的一部分所需的所有信息，Merkle 树的根在区块链的交易中发布。通过跟踪从 Merkle 根到目标哈希的路径，我们可以生成一个 Merkle 证明，证明 Merkle 树中有任何一个元素，而不需要知道整个树。这些元素可用于创建至少包含目标哈希、Merkle 证明、Merkle 根和交易 ID 的区块链收据。



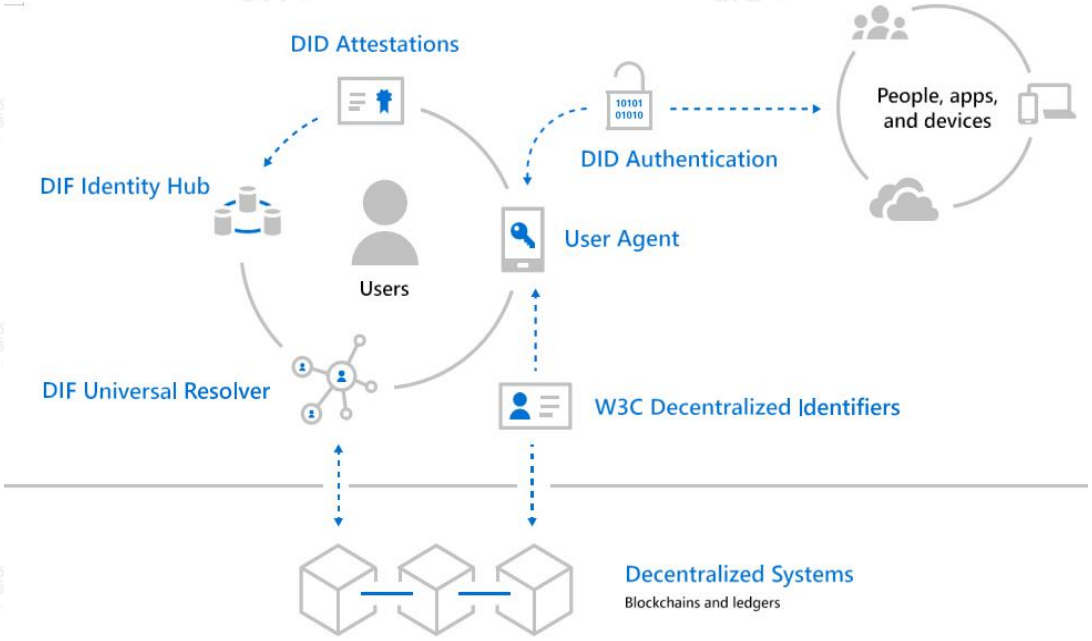
（图 10：创建区块链收据 ）

三、应用案例

对于去中心化身份的研究其实远在区块链技术兴起之前就已经开始，并且在全球范围内都得到广泛的关注和讨论。目前，基于区块链系统的去中心化身份的项目可以分成两类，第一类偏向于应用，解决重复 KYC 这类的问题，例如微软的去中心化身份系统、ShoCard；另一类解决的是自我主权身份的创建和使用，通过一个去中心化的身份系统来实现，例如 Ontology（本体）、Sovrin 这一类的公链项目。

1. 微软去中心化身份系统

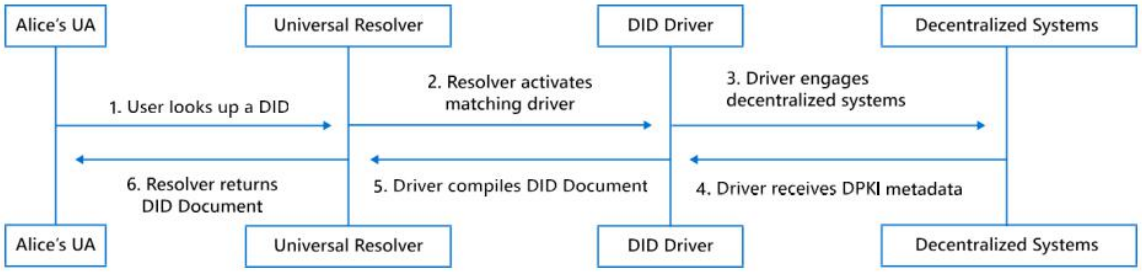
基于 W3C 的 DID 开源标准以及上述 DIF 一系列的协议和规范，微软开发了一套去中心化身份识别系统，可以说是一线大型互联网公司首次公开拥抱去中心化技术。但是 W3C 的 DID 标准和 DIF 的协议与规范都还在制定与更新的过程中，微软作为前两者的合作方，其开发的 DID 系统也处在非常早期的阶段。以下是该系统的架构设计：



（图 11：微软去中心化身份系统 ）

微软的 DID 系统搭建在区块链系统之上，系统中的去中心化标识符（W3C Decentralized Identifiers）、通用解析器（DIF Universal Resolver）、标识符中心(DIF Identity Hub)、DID 凭证(DID Attestations)和 DID 验证(DID Authentication)在上文中都有介绍，此处不再赘述。而用户代理（User Agent）是一个应用程序，帮助用户创建 DID、管理数据和权限，以及签名和验证与 DID 链接的声明。微软将提供一个类似钱包的应用程序，可以作为管理 DID 和相关数据的用户代理。用户代理应用程序集成了一个 DID 注册的有效负载，其中包括密钥引用、标识符中心（Identity Hubs）服务端点和恢复所需的公共值，即用户代理程序集成了 DID 注册的有效信息，并将这些有效信息推送到去中心化系统上（例如分布式账本）。同时程序中还设置了密钥恢复的功能。

根据上图所示，用户首先使用用户代理程序生成自己的 DID，并且生成与 DID 信息相关联的身份声明和凭证，存储在 Identity Hub 中，系统以外的个人或组织通过 DID Authentication 程序进行验证。



（图 12：查找 DID 流程）

上图所描述的是在系统中搜索、查找其他 DID 的流程，也就是通用解析器（Universal Resolver）所起到的功能。

（1）用户代理程序与通用解析器通信；

（2）通用解析器激活匹配的驱动程序；

（3）驱动程序与区块链系统接合；

（4）区块链系统返回 DPKI 元数据给驱动程序；

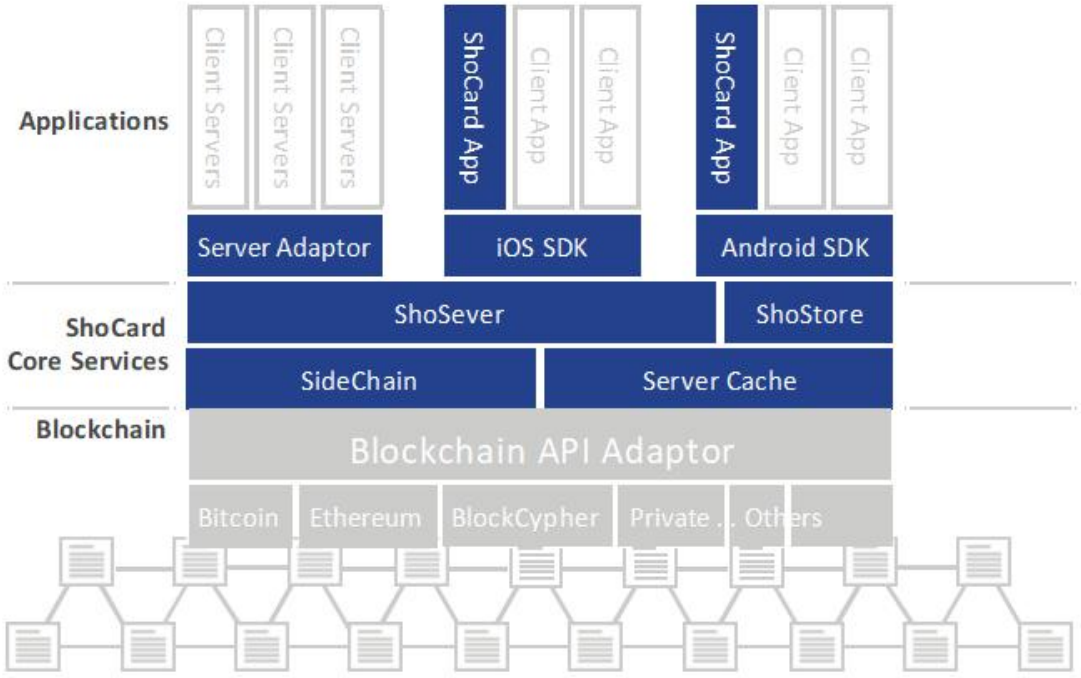
（5）驱动程序编译 DID 文档并传递给解析器；

（6）解析器将文档传递给 UA 程序。

通过这样一个流程，用户代理程序就搜索到了一个 DID。

2. ShoCard

ShoCard 于 2015 年 2 月创立，是一个基于区块链的身份管理生态系统，用户可以在其中拥有和保护自己的数字身份。他们决定与谁以及何时分享他们的个人数据。第三方可以使用区块链验证该数据的真实性，而不需要信任其他集中式第三方进行担保。用户在 ShoCard 区块链内创建信息的时候需要提供现有的能够证明自己身份的证件和电子签名等信息，此后 ShoCard 就会生成对应的公钥和密钥，只需要通过授权 ShoCard 身份验证，就能直接读取区块链内的信息，极大简化互联网上的身份验证流程操作。



（图 17：ShoCard 系统组成）

如上图所示，ShoCard 区块链的核心组件包括如下几部分：

（1）ShoCard 服务层：ShoCard 服务层用作不同应用程序和服务器以及区块链之间的安全通信管道。所有消息都由客户端签名，并使用另一方的公钥加密，ShoCard 服务永远无法解密数据。写入到区块链的任何记录都由记录的所有者签名，ShoCard 服务器只执行“写”。因此，它作为一个安全的通信管道，没有能力提取信息。ShoCard 服务层负责管理所有客户端 sdk 和区块链之间的接口。

（2）ShoCard 侧链：存储写入区块链的各种证书的验证代码。侧链用于保存认证数据。每条记录都经过哈希算法，这些哈希每隔 20 分钟左右就会被写入公共区块链，作为工作的证明。

（3）Blockchain 高速缓存：区块链缓存保存区块链的本地副本，以便更快地进行读取访问，这样验证就可以独立于公共区块链进行管理。

（4）ShoCard 区块链适配器：ShoCard 区块链适配器将接口抽象到维护工作证明的区块链，因此 ShoCard 服务层可以保持高效。区块链适配器层允许 ShoCard 系统的其余部分保持区块链无关性。

ShoCard 核心功能是提供身份认证，并解决重复 KYC 的问题，即当用户第一次将身份证件和信息上传到 ShoCard 平台上并认证后，认证的记录即被保存下来，后续的验证就会变得非常简洁。

ShoCard 较早涉足区块链身份管理领域，相对成熟，形成了自己的落地产品，最典型的是与 SITA 航空合作的基于区块链的数字身份认证 APP。人们在跨国旅行时，在机场安检的过程中要不断出示护照、登机牌、面部核验等信息，这些信息组成的数字身份是个人与服务商互动的关键，服务流程[10]如下：

（1）注册环节：用户在终端下载 APP 后自动生成 ShoCard—DID 和关联公私钥对，用户使用该 APP 对身份证件(如护照、驾照等)拍照，APP 会读入证件上的元数据（如姓名、护照号等），加密并存储在 APP 上。读取的数据经哈希、加密等处理并创建验证字段后发到区块链，同时对姓名、护照号等元数据哈希处理，再用存储在 APP 上的私钥签名后发送到成员接口服务器用于记录区块链的验证字段。

（2）完成注册后，用户进行第一次认证

①第一步与正常的案件相同，检查用户的物理证件并与本人进行核对。

②步骤①通过后，用户可通过 APP 出示二维码，商家扫码连接到成员管理服务器。

③商家在成员管理服务器中查询并获取与用户相对应的在区块链上的身份记录，验证用户的所有权，包括：用户出示的 ShoCardID 与记录是否一致、电子信息与物理证件是否一致、商家机器对用户面部进行识别的结果与证件记录是否一致。

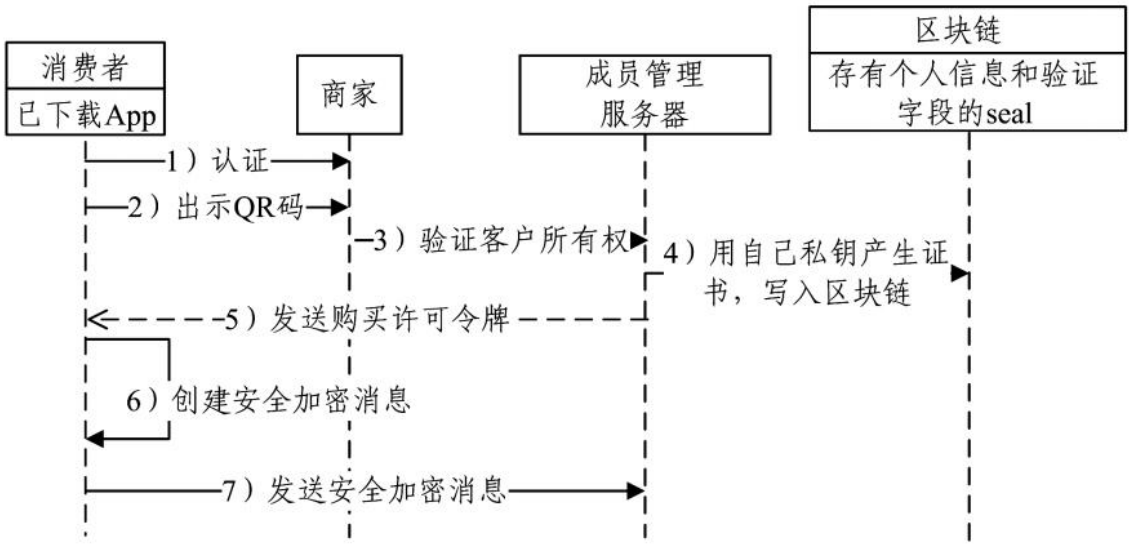
④验证用户的所有权通过后，商家请求成员服务器对用户验证通过，成员服务器生成认证证书，证书包括 ShoCardID、证件照片、认证通过令牌。对证书进行哈希处理签名后得到“证明”并发送到区块链存储，并在服务器存储索引“证明”的位置。

⑤成员管理服务器向用户颁发认证通过证书。

⑥用户收到证书后就存储在 APP 上，那么之后再遇到商家要求进行认证时，就可以使用 APP 中存储的信息进行认证。

⑦先对终端 APP 的“安全加密消息”进行整体签名，再用对称密码加密发送给成员管理服务器(用户终端也有备份)以供以后检索，其中对称密钥存储于本地终端。

[10] 董贵山等，基于区块链的身份管理认证，计算机科学第 45 卷第 11 期



（图 18：用户的第一次认证）

（3）第二次及以后认证

由于第一次认证已经通过，用户的身份凭证和信息已存储在本地终端，因此当用户到了不同地区，用户终端(可以无网络)的认证过程会变得很简单，具体如下：

1)商家要求认证；

2)用户出示二维码和对称密钥给商家；

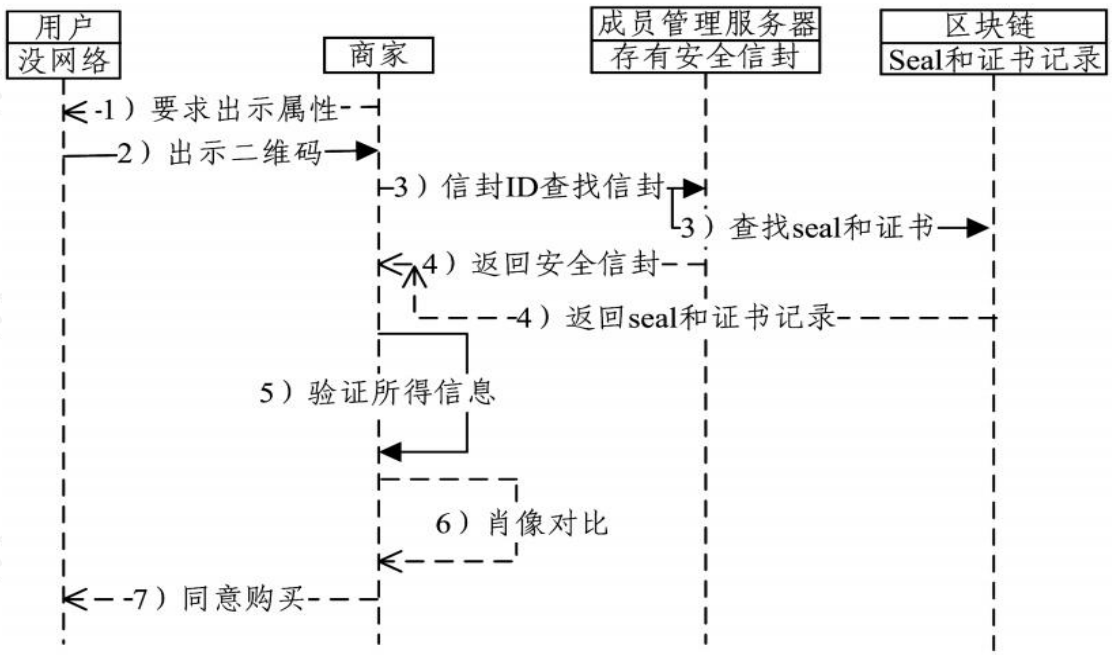
3)商家通过扫描二维码来连接到成员管理服务器以查询区块链上的相关资料；

4)区块链和成员管理服务器将相关资料返回给商家；

5)商家收到资料后，APP 自动执行以下操作：用户公钥验证安全加密信息和区块链元数据；验证物理证件照片等信息并与安全加密消息进行对比；用前一用户公钥来验证证书、证书对应区块链的记录和证件照，以及上一商家的许可令牌；

6)与用户肖像进行比对；

7)通过验证。

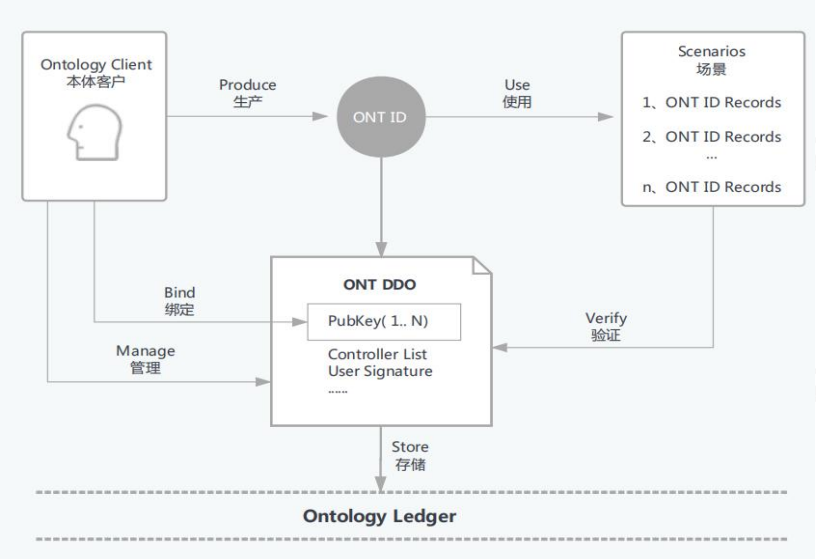


（图 19：用户的第二次认证）

3. Ontology 本体

Ontology 本体（以下简称“ONT”）项目于 2017 年成立，想要解决的核心问题是人与人之间的信任问题。本体信任网络架构了一个去中心化的融合的信任体系，将信任的多样性在一体化的协议体系下进行协同，整合去中心化的多维实体认证体系及各类不同区块链体系与信息系统，纳入多源身份认证和多源信息交换协议，并提供不同分布式应用场景的开放基础模块，实现分布式点对点的信任体系，构建跨链、跨系统、跨行业、跨应用和跨终端的分布式信任基础设施。

具体到 ONT 的身份系统，ONT ID 是一个去中心化的身份标识协议。每一个 ONT ID 都会对应到一个 ONT ID 描述对象（ONT DDO），用于记录 ONT ID 的控制人公钥等属性信息。描述对象作为公开信息以储存于本体网络底层的分布式账本中。



（图 15：ONT 网络身份系统）

ONT ID 协议体系主要包括：（1）身份标识协议（DID）；（2）可信声明协议；（3）多源认证协议。

（1）身份标识协议

① 生成 ONT ID

ONT ID 由每个用户自己生成。其生成算法保证了两个 ONT ID 重复的概率极小，同时在向本体网络注册时，共识节点会检查该 ID 是否已被注册。

② 自主管理

ONT 网络利用数字签名技术保障用户对自己身份标识的管理权。ONT ID 在注册时即与用户的公钥绑定，从而表明其所有权。对 ONT ID 的使用及其属性的修改需要提供所有者的数字签名。用户可以自主决定 ONT ID 的使用范围，设置 ONT ID 绑定的密钥，以及管理 ONT ID 的属性。

③多密钥绑定

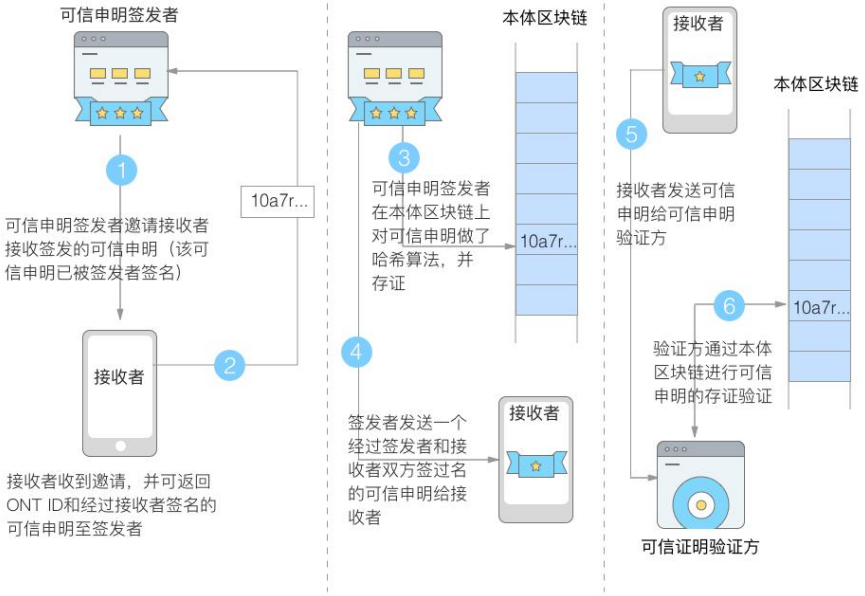
ONT 网络支持多种国内、国际标准化的数字签名算法，如 RSA、ECDSA、SM2 等。ONT ID 绑定的密钥需指定所使用的算法，同时一个 ONT ID 可以绑定多个不同的密钥，以满足用户在不同的应用场景的使用需求。

④授权控制

ONT ID 的所有者可以授权其他 ONT ID 代替本人行使对 ONT ID 的管理权，如修改 ONT ID 对应的属性信息，在密钥丢失时授权其它 ONT ID 重设密钥等。ONT ID支持针对每条属性项的细粒度的权限管理，以及“与”、“或”、“m/n”等多种的访问控制策略。

（2）可信声明协议

可信声明协议可以理解为 W3C 的 DID 规范中的可验证声明。可信声明协议涉及三种角色，分别是签发者、持有者（接收者）以及验证者，整个工作流程包含三个部分：请求声明、签发声明和验证声明。



（图 16：可验证声明协议工作流程）

（3）多源认证协议

ONT 网络中的身份认证采用的是多源认证的形式，包括外部信任源认证和网络实体之间的认证。

①外部信任源认证包括自我导入和信任锚导入。自我导入指的是用户通过社交媒体、银行UKEY 签名等方法来绑定现实信任，该模式利用了现实世界已有的信任（比如微信、Facebook、银行等等）。首先用户在 ONT 上添加一个外部信任源的证明地址，用户接着在该证明地址上提供一个可验证声明，当第三方需要验证用户的外部身份时，首先在本体网络中读取到用户信任源的证明地址，然后到这个地址去获取可验证声明，最

后验证该可验证声明即可；信任锚通常是那些经过了实名认证，且在社会中由一定公信力或声望的政府单位、企事业单位、非盈利组织以及社会名人等。成为信任锚需要遵守本体链委员会发布的一系列标准。信任锚使用自有的认证方式对被认证实体进行认证后，对被认证实体签发一个可验证声明。声明中不需要包含被认证实体的真实身份信息，仅记录实体及认证服务的 ONT ID，作为该服务的认证结果证明即可。

②网络实体之间的认证，指的是实体通过本体网络中已通过身份认证（通过“外部信任源”的形式）的实体来认证身份。

4. Sovrin

Sovrin 是一个致力于实现自我主权身份的公链项目，于 2015 年由 Evernym 公司创立。2016 年 9 月，Sovrin 基金会在伦敦成立，由受托人组成的董事会和技术管理董事会构成。2017 年初，Sovrin 基金会将开源代码库移交给 Linux 基金会，变成了 Hyperledger Indy 项目。因此 Sovrin 的核心代码由 Hyper Ledger Indy 项目进行开发。

Sovrin 系统利用区块链技术解决的是身份认证问题。Sovrin 的身份标识符遵循了 DID 规范，Sovrin 区块链为 DID、可验证声明以及身份验证的证据提供了可以锚定的地方。在 Sovrin 系统中，用户身份包含了身份标识符（DID）、可验证声明及凭证等内容。身份认证的数据库会被主要存放在 Sovrin 区块链中。Sovrin 网络是由分布在世界各地的多个节点，每个节点都有一份分布式账本。管理员负责验证身份交易。

Sovrin 采用了一种“公共许可”的分布式账本设计理念。通过 Sovrin 身份网络，Sovrin 基金会授予“节点”加入网络的权限。这与比特币和以太坊所使用的“无许可”账本(在这些账本中，任何人都可以加入该网络)截然不同。“公共可访问”意味着 Sovrin 对所有人开放，但并不意味着所有 Sovrin 身份数据都是公共的。事实上，Sovrin 系统中的身份数据是私有的，只能在其所有者同意的情况下共享。

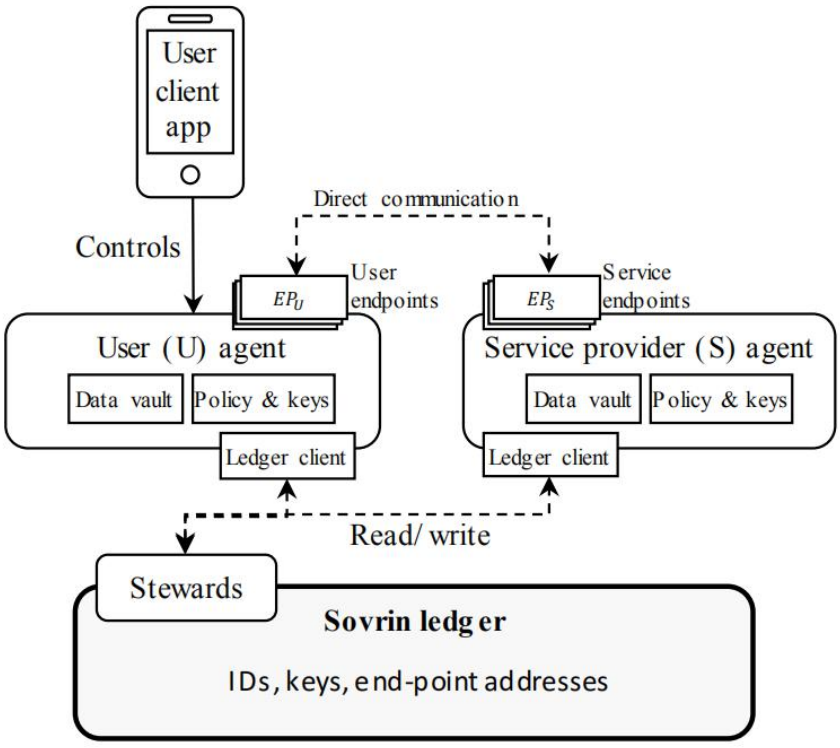
（图 13：Sovrin 技术堆栈）

Sovrin 的身份堆栈可以分为三层，分别是底层的区块链账本（Sovrin Ledger），其上是 Sovrin 代理（Sovrin Agents）以及最上层的 Sovrin 客户端（Sovrin Clients）。

用户通过客户端程序（Clients）与 Sovrin 区块链（Sovrin Ledger）进行交互，并控制代表他们的代理（Agents），以促进与网络上其他代理的交互。只有合法遵守 Sovrin 信托框架的管理员才能在账本上进行输入。用户和组织依赖于可寻址的网络点代理。标识符、密钥和端点地址则存储在区块链上。代理是始终可寻址和可访问的网络端点。用户可以在自己的服务器上运行代理，但更有可能的是，他们会要求专门的中介机构(代理机构)为他们运行代理。代理还提供备份服务和身份属性凭据的加密存储。

客户端程序还帮助用户管理存储在用户移动设备上的密钥。Sovrin 提供了一种密钥恢复机制，该机制依赖于用户选择一组受托人。当用户要求这样做时，达到指定人数的受托人必须签署一个新的身份记录事务，并且由管理员进行验证。

此外，Sovrin 还采用了零知识证明技术，保护用户数据的隐私和安全。



（图 14：Sovrin 系统架构）

四、总结

微软的首席身份架构师 Kim Cameron 曾说，“互联网是没有身份层的”，因为互联网的寻址系统基于识别网络上的物理端点(机器)，而人并不是网络上的端点。因此，互联网没有办法唯一地识别人的身份。区块链技术的发展，帮助人们重新思考身份识别和认证的解决方案，通过使用去中心化标识符、可验证声明等技术来解决互联网身份层缺失的困境。同时，在微软、Facebook 等互联网巨头的推动下，基于区块链技术的去中心化身份管理系统，应该会是区块链技术应用落地最早的领域之一。

但是，去中心化身份管理系统并不能完全摆脱中心化的元素。例如在 Sovrin 这个项目中，存在着管理员这个角色，而目前成为管理员的都是一些大公司，这种机制可能会催生一批以大公司为代表的超级节点，存在着中心化的风险。再看 ShoCard 这个项目，用户依赖于 ShoCard 平台所提供的身份认证体系，如果平台不复存在，那么用户将无法使用身份认证系统。

作者：时戳资本分析师 冯琳

fl@8btc.com

2019 年 3 月 26 日

参考文献：

【1】清华大学互联网产业研究院，区块链技术应用白皮书 2018

【2】董贵山等，基于区块链的身份管理认证，计算机科学第 45 卷第 11 期

【3】曾凡平，中国技术大学，数字证书与公钥基础设施

【4】为什么我们需要去中心化数位身份？「自我主权」的觉醒，
https://www.chainnews.com/articles/712203048155.htm

【5】以去中心化身份为起点，走出数字信任的“囚徒困境”，
http://finance.sina.com.cn/blockchain/roll/2018-10-10/doc-ifxeuwws2815639.shtml

【6】浅析微软的区块链去中心化身份识别系统 DID，
https://www.easyaq.com/news/1644208597.shtml

【7】王瑜琨，IBM 赵振华：去中心化身份解决方案，
https://www.jinse.com/news/bitcoin/267765.html

【8】Jason Chang,【SSI】通往自我主权身份之路（1）——身份的演进史，
https://bihu.com/article/1693159

【9】身份证明，虚拟身份证明，分布式身份证明！首发！？科普知识 ，
http://www.sohu.com/a/260019351_100285689

【10】微软计划推出区块链身份识别系统，
http://v1.8btc.com/microsoft-is-pushing-new-blockchain-id-products

【11】本体分布式身份框架(ONTID)，
https://github.com/ontio/ontology-DID/blob/master/README_cn.md

【12】Ontology DID 身份标识协议规范，
https://github.com/ontio/ontology-DID/blob/master/docs/cn/ONTID_protocol_spec_cn.md

【13】W3C，Decentralized Identifiers (DIDs) v0.11，https://w3c-ccg.github.io/did-spec/

【14】W3C，Verifiable Credentials Data Model 1.0，
https://www.w3.org/TR/verifiable-claims-data-model/

【15】W3C,Verifiable Claims Use Cases,https://www.w3.org/TR/verifiable-claims-use-cases/

【16】Sovrin whitepaper

【17】Sovrin Board of Trustees，Sovrin Provisional Trust Framework

【18】Drummond Reed，Jason Law & Daniel Hardman，The Technical Foundations of Sovrin

【19】ShoCard whitepaper

【20】Ontology whitepaper

【21】Decentralized Identity Foundation，The Rising Tide of Decentralized Identity，
https://medium.com/decentralized-identity/the-rising-tide-of-decentralized-identity-2e163e4ec663

【22】Markus Sabadello 等，Introduction to DID Auth，https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md

【23】Phil Windley，How Sovrin Works，http://www.windley.com/archives/2016/10/how_sovrin_works.shtml

【24】Markus Sabadello 等，DID Auth: Scope, Formats, and Protocols，https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/topics-and-advance-readings/DID%20Auth:%20Scope%2C%20Formats%2C%20and%20Protocols.md#did-auth-scope-formats-and-protocols

【25】Markus Sabadello 等，Universal-Resolver Introduction，https://github.com/decentralized-identity/universal-resolver/blob/master/docs/driver-development.md

【26】Markus Sabadello，DID Auth and the little I-am-me，https://medium.com/@markus.sabadello/did-auth-and-the-little-i-am-me-ec14d757ff09

【27】Oliver Terbu，The Self-sovereign Identity Stack，https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45

【28】Adam Powers，Understanding Decentralized IDs (DIDs)，https://medium.com/@adam_14796/understanding-decentralized-ids-dids-839798b91809

【29】DIF Identity Hubs，https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md

【30】Markus Sabadello，A Universal Resolver for self-sovereign identifiers，https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

【31】Paul Dunphy and Fabien A. P. Petitcolas，A First Look at Identity Management Schemes on the Blockchain

【32】Dr Garrick Hileman & Michel Rauchs，GLOBAL BLOCKCHAIN BENCHMARKING STUDY

【33】Atif Ghulam Nabi，Comparative Study on Identity Management Methods Using Blockchain