区块链：下一代数字身份认证体系的基石

2020-12-08

如何在互联网的世界中，证明“我是我”？在 A 网站认证过了身份信息，到了 B 网站又需要认证一次？手持身份证拍照上传、人工审核，流程太繁琐？多个账户密码记不清、容易混，管理起来困难？自主主权的数字身份（Self-soverieign identity, SSI）正是可以解决这些问题的理念。

SSI 是数字身份运动中的观念，指只有用户自己拥有全部的、完整的数字身份信息，没有其他管理者和组织参与的数字身份体系。在 SSI 的理念中，用户拥有属于自己的去中心化的惟一身份标识（Decentralized identifiers, DIDs），用户可以完全控制自己的身份信息，可以在任何时候使用、更新或者彻底删除信息。用户可以创建并管理自己的可验证证明（Verifiable Credentials），自主决定在什么时候使用和分享自己的证明信息，而不需要请求其他中心化的机构、通过机构授权来使用自己的个人数据。

使用 SSI 的系统，所有的密钥信息都可以通过数字身份钱包进行管理，使用一个账号就可以登录所有的网站。在钱包终端中，用户可以随时向权威机构申请签发证明，包括身份证、驾驶证、居住证等各种形式的证件，都将以数字证明的形式储存在手机或电脑上。数字证明拥有机器可读、机器可验证的特性，不但可以放心地展示给第三方应用，第三方应用还可以在没有人工干预的情况下，直接验证证明的有效性，不需要签发机构的参与。

得益于区块链技术的不断发展，SSI 理念的实现逐渐成为可能。区块链系统本身就是点对点网络，天然拥有去中心化的特性，结合独特的数据结构设计和密码学技术的应用，加上共识算法在多节点数据同步方面的优秀能力，区块链不但能够保护数据的隐私安全，而且数据一旦写入系统便任何人无法篡改，为数据提供了极高可信度的储存环境。在 SSI 系统的建设中，将区块链作为可验证数据的数据中心（Verifiable data registry）无疑是最好的选择。

SSI 目前已经有诸多先例。2017 年，Sovrin 基金会发布了世界上首个公开的用于自主主权的数字身份的分布式账本网络，整个系统运行在开放标准以及公开源码的 Sovrin 协议之上，由 Linux 基金会的 Hyperledge Indy 项目维护。Sovrin 在 2018 年公布的白皮书中自问自答，“为什么网络世界中没有像物理世界一样可以用来证明身份的证书？直到区块链技术的出现，我们解决了这个问题！”结合 W3C 的 DIDs，Sovrin 提出了完整的数字身份和证明的解决方案。Sovrin 的主意一直都很明确，就是一定要构建和使用公开的、任何人都可以访问的、像比特币和以太坊一样的区块链网络。

eSSIF-Lab（European Self-Sovereign Identity Lab）是另一个案例。欧洲区块链联盟提出的 EBSI（The European Blockchain Services Infrastructure）是一个横跨欧洲的分布式节点网络，提供跨境的公共服务，有 28 个成员国签署了相关声明。eSSIF-Lab 项目是 EBSI 的一部分，由欧盟委员会资助，旨在促进 SSI 成为下一代开放、可信、安全的数字身份解决方案。欧盟曾在 2014 年 7 月 23 日建立了针对欧盟共同市场电子交易的电子身份识别和可信服务的法规 eIDAS（electronic IDentification, Authentication and trust Services），2019 年 5 月，eIDAS 宣布支持基于 W3C 相关规范的自主主权的数字身份。

微软在相关领域也表现活跃，2018 年 10 月，微软发布《去中心化的身份》白皮书，介绍了基于区块链的去中心化数字身份系统建设的技术方案，包括 DIDs 规范、去中心化的数据系统、DID 用户终端、DID 通用解析器、DID 身份中心、DID 认证系统、去中心化的客户端和服务等核心模块，详细说明了各模块组件以及各种角色在系统中的交互流程，为 SSI 系统的建设提供了非常好的模板。目前，微软已经提供公开的服务平台，可以体验相关的产品和能力。

此外，构建在以太坊和 IPFS 网络上的 uPort、使用自研区块链和支持第三方 DApp 的 Blockstack、能够适配比特币网络的 ShoCard 等都是优秀的案例。国内的厂商和机构也在进行相关的工作，如蚂蚁链提供的分布式身份服务 DIS（Decentralized Identity Service）、腾讯云的数字身份标识解决方案、微众银行的基于区块链的分布式多中心的技术解决方案 WeIdentity 等，都利用了区块链去中心化、数据高度可信的技术特点，构建了可靠的数字身份标识和认证体系。

区块链是一项极具潜力的先进技术，具有非常广阔的发展前景和应用空间，无论是国家政策的支持还是实际案例的应用，都体现出区块链未来的无数种可能。我们也在积极探索和推进区块链相

关的技术发展和场景落地，将区块链与同态加密、联邦学习、多方计算、零知识证明等前沿技术结合起来，使用最优秀的技术能力，促进下一个互联网时代的到来。