区块链和去中心化身份 - 企业准备好迎接自我主权身份（SSI）吗？

2021 年 3 月 29 日，领英区块链版块发布了文章《区块链和去中心化身份-企业准备好迎接自我主权身份（SSI）吗》，主要介绍了 SSI 技术、SSI 技术应用案例等内容。文章主要内容如下:

新冠疫情期强化了对数据隐私、透明数据流动性和可靠数字信息的需求，使 SSI 的使用范围不断扩大。越来越多的公司正在试用 SSI 技术，一些项目已从概念验证阶段转移到生产阶段，加快了 SSI 的研究步伐。

一、什么是 SSI 技术？

SSI 技术是去中心化数字身份解决方案的总称。在 SSI 中，个人的隐私信息以数字格式存储且完全只处于数据所有者的控制之下。信息是以数字证书的形式提供，可以保存确认个人身份的任何信息，也可以以物理形式发行。证书交换通常发生在证书颁发机构、证书持有者和证书验证方三个参与者之间。未经持有者允许，任何信息都不能在发行方和验证方之间共享。证书有效性的任何变更信息都登记在区块链上。证书的验证是自动的（通常通过扫描二维码进行），并且不需要与签发机构进行任何联系，使得整个过程非常快速、灵活、可扩展和节约成本。因区块链上永远不会存储任何私人信息，所以 SSI 在设计上符合欧盟通用数据保护条例（GDPR）的要求。

SSI 的主要特点是去中心化，去中心化也是将该技术与其他集中式数字身份解决方案区分开来的关键因素。集中式数字身份解决方案将一些用户的个人数据存储在中央数据库中，授予用户访问其服务的权限（通常是通过帐户）。在用户体验方面，需要为每个存储数据的组织、服务、网站等创建和管理单独的凭证、密码和登录，增加额外的负担；在组织方面，集中式数字身份解决方案成本高昂，同时反复发生的数据泄漏事件表明保持最高的安全标准和持续预防网络攻击也是困难的。去中心化的 SSI 可以有效解决这些问题，是信息存储和共享的最佳方式。数据提供者公民在存储和分发其个人数据的过程中处于主导地位。

二、SSI 技术的应用案例

（一）旅行通行证移动应用程序。新冠疫情加大了人员流动中对健康证明的需要，即核酸检测结果和疫苗接种记录要便于携带、非接触和易于核查。国际航空运输协会（IATA）与 SSI 技术提供商 Evernym 合作，一直在试用旅行通行证（Travel Pass Initiative）。旅行通行证是一个数字凭证方案，可供乘客、航空公司、政府、边境管制当局和其他系统参与者即时核查旅行和健康文件，包括与新冠肺炎相关的文件。这些证件由乘客在一个应用程序中保存和管理，该应用程序还允许他们检查在给定位置需要哪些文件，找到最近的测试中心等。航空公司或任何边境管制机构通过扫描二维码来验证证件，使过程快速和无接触。该证书包括哪个机构已颁发该证书、证书持有者的身份以及证书是否有

效的信息。通过旅行通行证，航空公司可以平稳地管理旅客流量。重要的是，该解决方案基于所有航空公司的同一套标准，以确保最大程度的互操作性和对凭据中锁定信息的识别。

（二）金融与银行业的应用。银行部门 SSI 最明显的用例可能是了解你的客户（KYC）和尽职调查等流程的标准化和规模化。当前，由于监管限制，整个银行生态系统在共享信息的过程中的互操作性级别非常繁琐，甚至常常是不可能的。一个共享的数字身份标准将提供一种可靠的方式来识别整个银行生态系统中的个人身份，同时为银行客户提供各种新服务--贷款、保险、财富管理等的便利。波兰桑坦德银行开始开发 SSI 解决方案，项目将在银行和与之合作的财富管理机构之间建立一个安全的联系渠道，SSI 将取代这两个机构之间需要独特的点对点集成基础架构的数据共享方式。

（三）可验证的全球法人识别编码（vLEI）数字证书。全球法人识别编码基金会（GLEIF）最近提出在金融监管领域应用 SSI 的典型案例 vLEI。GLEIF 与来自不同部门和行业的利益相关者合作，致力于建立 vLEI 数字证书应用框架，为法人实体提供包含全球法人识别编码（LEI）数字证书的访问权限。应用 SSI 基础设施将取代目前有关机构访问和确认实体 LEI 数据的手动流程，SSI 将为企业实体提供与其法人相关的数字和安全身份识别数据，它还允许进行批准业务交易、在供应链中交易或监管报告等其他业务操作。同时，允许任何有关机构能够迅速和轻松地

对这类数据进行核查，从而在法人实体之间建立信任链。

（四）瑞士电信的 SSIGate 应用。瑞士电信旗下的瑞士创业公司瑞士区块链开发了 SSI 在企业间数据共享过程中的相关应用，是 SSI 技术在商家对商家的营销关系（B2B）环境的典型应用。SSIGate 解决方案应用了 Hyperledger 生态系统基础架构（Indy 和 Aries），为制药行业的供应商提供了一种经济高效，可扩展且有效的途径。目前，每家制药公司根据行业监管框架，对新的供应商采用不同的尽职调查程序。因此，每当有新的供应商加入时，整个尽职调查过程都会重复。据瑞士电信称，同一行业公司的入职调查问卷有 80%是重叠的。SSIGate 为供应商在完成注册程序后提供数字证书，该证书可以由其它制药公司进行验证，而不需要重复相同的过程。这样的解决方案不仅使新供应商的加入速度更快，而且具有显著的成本效益。

三、基础设施供应商和技术标准

从零开始构建 SSI 基础架构是一件相当复杂的事情，尤其是对小型企业来说，开发新技术解决方案可能不大现实。幸运的是市场提供了各种各样的具有不同程度的成熟度和支持级别的外包服务，从软件开发工具包(SDK)、现成的用户应用程序、应用程序接口(API)，一直到咨询和支持，使 SSI 方案更加可用和切实。如，SSI 技术的倡导者 Evernym 公司牵头建立了唯一一个专门为身份建立的公共分类帐，并为开源 Hyperledger 技术堆栈（尤其是 Hyperledger Indie）贡献了代码库。SSI 基础架构提供商

Trinsic，它向客户提供现成的 SSI 钱包方案、钱包 SDK 和凭证 API。

为最大限度提高 SSI 技术解决方案的互操作性，需要围绕通用的技术标准开展工作。从技术角度来看，SSI 基础结构通常分为三个不同的层，应考虑并应用通用标准：第一层是分散标识符（DID）层，一种标准的开放协议，用于在多方之间建立唯一、私有和安全的连接。第二层是可验证的凭证层，用于发布、保存和验证受保护数据的标准开放式“数字数据水印”协议。第三层是公钥注册表，用于存储连接和数据所有者公钥的地方。从组织上看，分散身份基金会 DIF、Hyperledger、Trust OverIP 基金会或 ID2020 联盟等组织和基金会对于建立数字身份的开放标准特别重要。

虽然人们早已认识到，迫切需要为互联网用户和从个人数据中受益的企业提供公平的竞争环境，但企业如何从 SSI 中具体获益却不那么明确。目前越来越多的项目采用 SSI 说明企业正在缓慢但肯定地从商业角度认识到 SSI 的价值，并正在学习如何利用这项技术。

原文链接：

https://www.linkedin.com/pulse/blockchain-decentralised-identity-enterprises-ready-ssi-slater/?trackingId=EZCtyY1STkGbGcd0wpSxJA%3D%3D