

Web3.0 “护照”（上） — 分布式数字身份法律性质初探

作者：夏彦 | 曾铮 | 林海立 | 蔡士睿

近期，上海市公布《上海市数字经济发展“十四五”规划》，提出“加快发展万物互联下的新一代身份认证技术，构建新型数字信任体系”“超前布局新一代网络形态，前沿探索多平台 OpenID（数字身份识别框架）、分布式数据存储、去中心化 DNS（域名解析系统）、端到端加密通信等 Web3.0（第三代万维网）关键技术”。其中，Web3.0 关键技术中的分布式数字身份标识符（Decentralized Identifier，简称“DID”）备受关注，根据证券时报于 2022 年 9 月 28 日的报道，近日区域性股权市场分布式数字身份在上海股交中心正式上线，创新性地解决了跨机构、跨行业的身份认证问题，这是 DID 在国内新增的又一个典型应用案例。

作为 Web3.0 世界的“护照”，DID 的出现和应用可能会带来全新的商业模式和社会交往方式，而链上身份的合法性和合规要求也逐渐成为区块链从业者和用户关心的话题。本文分为上下两篇，第一篇旨在分享我们从法律角度对 DID 业务模式、法律参与主体、法律关系以及 DID 法律性质的初步探析，第二篇我们将重点分析 DID 业务的主要法律参与主体（DID 发行者、DID 拥有者、DID 核验者）各自的合规要求和法律风险。

一、DID 的构成要素及主要类型

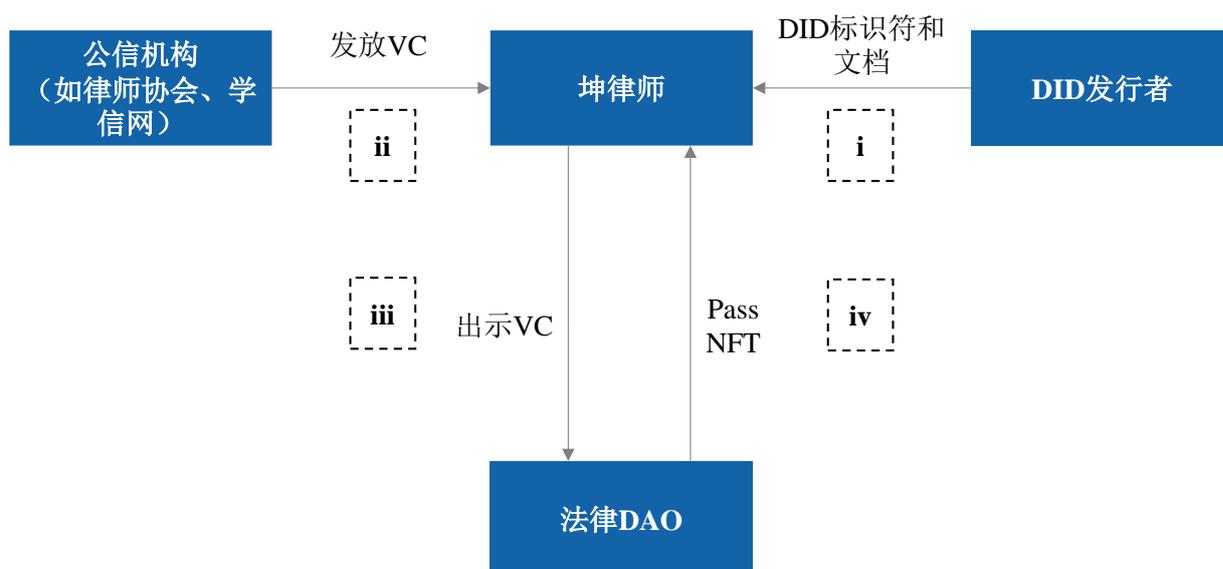
（一）DID 是什么？怎么用？

根据万维网联盟的定义，DID 的全称是 Decentralized Identifier，是一种可验证的、去中心化的数字身份形式¹。一般来说，标准的 DID 系统主要包括以下层次及要素：

- 基础层 — DID 标识符（Identifier）和 DID 文档（Document）
- 应用层 — 可验证声明（Verifiable Claims 或 Verifiable Credentials，简称“VC”）

我们以某法律 DAO 要求坤律师提供法律职业信息以决定是否对其颁发成员 Pass NFT 的模拟案例来介绍 DID 中的各个要素，并说明 DID 的使用流程：

¹ <https://www.w3.org/TR/did-core/>。



- 坤律师通过 DID 发行者的应用程序生成 DID 标识符和 DID 文档，DID 标识符就是一个字符串，类似护照号，DID 文档则主要记载了公钥，主要用于验证签名。因此，基础层的 DID 标识符和 DID 文档加起来相当于坤律师的护照，只不过这张护照现在还没有记录任何坤律师的个人信息，是空白的；
- 坤律师还需要往护照上放上法律职业信息，申请对应的 VC 则可以完成这一目的。坤律师可以向律师协会、学信网等公信机构（简称“公信机构”）提出 VC 发放请求，这些公信机构的数据库存有坤律师的律师执业情况、学历情况、公开的代理案件情况、公开发表论文情况等，可以向坤律师的 DID 发放 VC；由于 VC 上承载的个人信息很多，坤律师还可以进一步根据法律 DAO 要求的信息范围选择性地将 VC 中的一部分截取为 Verifiable Presentation，不提供法律 DAO 并不需要的信息；
- 坤律师向法律 DAO 出示 VC，法律 DAO 首先需要结合坤律师的 DID 确认该 VC 是坤律师提交的，然后需要确认该 VC 是对应的可信的公信机构出具的，以确保该 VC 是真实可信的；
- 法律 DAO 检查确认 VC 中的坤律师相关信息并确认符合要求后向坤律师提供 Pass NFT。

值得注意的是，在上述模拟案例 VC 验证流程中，法律 DAO 无法验证 VC 中所包含的信息本身的真实性，法律 DAO 仅能依赖律师协会、学信网等可信的公信机构对其出具的 VC 内容真实性的背书。因此，确认公信机构在可信列表中，是 DID 业务闭环需要解决的现实问题。

（二）DID 的主要类型

DID 实质上是加密数字身份，DID 拥有者可以选择（1）让 DID 核验者（Verifiers）核验其数字化加密的真实法律身份及其相关信息；或（2）让 DID 核验者（Verifiers）核验其数字身份在链上的匿名身份及行为信息。简而言之，DID 拥有者可以选择是否将其链上身份与其真实的法律身份（例如现实世界中国家机关通过登记户口、颁发身份证等方式提供的身份）相连通。因此，目前 DID 可以分为两种类型：

1. 链接 Web3.0 与现实世界：链上数字身份和链下法律身份的标识符

随着 Web3.0 技术和应用的不断发展，链上交易合规问题越来越受到各国监管部门的重视，越来越多的 Web3.0 项目运营方需要满足实名认证要求（如境外虚拟货币交易所），通过链下关系实现 DID 核

验，以解决该等场景下的合规问题。

2. 连通 Web3.0 世界：聚合链上数字身份的标识符

不同于 Web2.0 中的用户登录每一平台需要注册新的账号，用户在 Web3.0 的世界可以通过 DID 体系实现在不同平台的身份聚合，实现同一数字身份跨平台、跨链使用，用户在不同平台和区块链中的声誉、履历、信用、项目经验等可以得到聚合。此类 DID 项目的性质更加偏向于以太坊创始人所提出的“灵魂绑定（Soulbound）”，而不考虑该类 DID 是否一定要对应到现实主体。

需注意，是否将用户的链上身份与其真实的法律身份相连通，对于 DID 拥有者可能并无实质不同，但 DID 发行者以及 DID 核验者（Verifiers）的合规义务会有较大不同（具体请见本文下篇的分析）。

二、DID 与传统数字身份的主要区别

（一）DID 可以实现 DID 拥有者对自身身份信息的拥有

在 Web1.0 及 Web2.0 时代，用户在网络空间所使用的虚拟账号均依附于各大网络平台，用户在各大网络平台注册多个不同账号并使用，其账号相关数据储存在各大网络平台的数据库中，该等方式主要存在两个特点：

- 首先，除了根据网络平台相关协议明确约定用户可以享受的知识产权等相关权益外，用户对于其在网络平台账号上形成的数据可能无法形成实际控制，从而无法分享该等数据所带来的收益；
- 其次，不同平台之间的用户虚拟账号可能并不相通，因此用户也无法对其网络身份实现独立的管理和使用，只能依赖于形成虚拟账号的网络平台。

但在 DID 体系下，DID 拥有者在区块链上形成自己可以独立管理和使用的加密地址，通过持有该地址的密钥对链上数字身份信息进行控制和管理，从而实现 DID 拥有者对自身身份信息的拥有。

（二）DID 可以更好实现 DID 拥有者的个人隐私保护

在 Web2.0 网络平台注册账户，用户可能需要向网络平台提供一些个人信息进行绑定，例如身份证号、手机号码、电子邮箱地址等，而目前不少网络平台存在违规收集和使用用户个人信息的情况，引发了用户对数据泄露及隐私保护的担忧。但在 DID 体系下，DID 拥有者向 DID 核验者证明自身身份主要通过展示 VC 及相应的签名信息进行，而且 DID 拥有者可以对自身的身份信息进行可选择性的披露，并不需要展示全部自身信息，此外，区块链上仅存储 DID 拥有者的 DID 信息，而不会存储 DID 拥有者不希望披露的个人信息，从而使得个人隐私得到了更好的保护。

为更好地理解 DID，我们总结了 Web3.0、Web2.0、Web1.0 中数字身份的主要区别：

比较项	Web3.0	Web2.0	Web1.0
功能	Read, Create & Own	Read & Create	Read
账户形式	随机私钥+去标识化公钥	用户自定义，一般为账号+密码，也可应用人脸或指纹	用户自定义，账号+密码

比较项	Web3.0	Web2.0	Web1.0
共识性	跨应用共识，同一 DID 可以在不同应用中使用	一般限于本应用内，亦有通过 A 应用的账户授权登录 B 应用的“联盟性共识”	限于本应用内
数据控制和权益享有主体	拥有者	网络服务提供者等非用户主体，用户仅享有访问、修改、删除等请求权	网络服务提供者等非用户主体，用户仅享有访问、修改、删除等请求权
存储方式	存储于区块链或分布式账本	存储于中心化机构控制的服务器中	存储于中心化机构控制的服务器中
隐私性	一般无需出示可识别至个人的关键信息	需展示可识别至个人的关键信息，如手机号	需展示可识别至个人的关键信息，如手机号
交互方式	用户↔用户	用户↔中心化机构↔用户	用户↔中心化机构

三、DID 业务法律参与主体及其法律关系

从以上 DID 的业务模式可以看出，DID 业务主要包括四个法律参与主体：DID 发行者、DID 拥有者、DID 核验者和公信机构，彼此之间的法律关系如下：

（一）DID 发行者&DID 拥有者：发行者向拥有者提供的一项网络服务

DID 可以视为发行者向拥有者提供的一项网络服务，因此，二者之间可能存在网络服务合同法律关系，DID 发行者基于网络服务合同法律关系得以向 DID 拥有者主张支付服务费用、遵守 DID 使用规则等，DID 拥有者则可以基于网络服务合同法律关系要求 DID 发行者向其提供能满足其使用目的且稳定的 DID 服务。

需注意，网络服务合同一般是网络服务提供者事先拟定好的格式合同（常见的有网站使用协议、网络产品服务协议、隐私政策等），用户在注册时对格式合同进行点击确认，从而建立网络服务合同法律关系，DID 发行者与 DID 拥有者亦是如此。

（二）DID 发行者&DID 核验者：可能存在民事合作法律关系

DID 核验者接受 DID 发行者的商业前提是其认可 DID 发行者区块链加密技术的可靠性，二者之间是否建立法律关系并非“认可”存在的必要基础。实践中，虽然 DID 发行者与 DID 核验者之间在链上通过智能合约进行了一系列的数据交互，但二者可能是分别与 DID 拥有者建立了法律关系，二者之间可能并无法律关系。

需注意，基于 DID 发行者与 DID 核验者之间可能会有建立长期合作的商业诉求，例如 DID 核验者将声誉良好的 DID 发行者列为战略合作伙伴，将 DID 发行者的公钥加入其可信任列表，在这种情况下，两者可能会建立合作合同法律关系。

（三）DID 拥有者&公信机构：行政法律关系或民事合作法律关系

公信机构大致可分两类，一类为政府或其他具有公权力背景由政府型公信机构，另一类是市场上广泛认可的商业型公信机构。公信机构同意为 DID 拥有者提供 VC，对政府型公信机构而言可能是出于履行其公权力职能的需要，从而在 DID 拥有者与公信机构之间产生行政法律关系；对商业型公信机构而言则可能需要基于其与 DID 拥有者之间的认证服务合同等民事法律关系。

DID 拥有者创建并使用连通链上数字身份和链下法律身份的 DID，通常是基于验证本人真实法律身份的需求，例如应对 DID 核验者的法定 KYC 要求，在该等情况下公信机构可能是公权力背景由政府型公信机构。反之，DID 拥有者创建并使用聚合链上数字身份的 DID 时，公信机构可能是商业型公信机构。

（四）DID 核验者&公信机构：可能存在民事合作法律关系

在 DID 使用过程中，对于政府型公信机构而言，DID 核验者基于对公信机构的信赖从而信赖其为 DID 拥有者出具的 VC，虽然该信赖主要是来自国家力量的背书，但由于 VC 并不是政府型公信机构向 DID 核验者出具，因此 DID 核验者和政府型公信机构之间可能并不就此发生法律关系；对于商业型公信机构而言，信赖可能来自该等公信机构的市场地位、品牌与信誉，也可能基于 DID 核验者与该等公信机构的合作合同法律关系。

（五）DID 拥有者&DID 核验者：视具体服务而定

DID 拥有者与 DID 核验者出示或验证 DID，往往是为了建立法律关系，二者之间建立的法律关系决定于 DID 拥有者通过 DID 实施的行为实质。例如，DID 拥有者使用其 DID 在某链上借贷平台上申请借款，平台作为核验者通过核验 DID 确定 DID 拥有者是合格的借款方，并向其提供了一笔借款，该等情形下 DID 拥有者和 DID 核验者之间建立的是借款合同法律关系。

四、DID 在中国法下的法律性质探析

虽然 DID 相比于 Web2.0 的身份在去中心化、隐私保护等方面都有诸多优势，但 Web3.0 建设目前仍处于发展阶段，不少项目的网络安全相比于 Web2.0 还没有那么成熟，私钥泄露、区块链地址受到攻击等情况亦时常发生，因此 DID 也存在被盗取或非法使用的可能。DID 拥有者此时可以主张哪些合法权益？我们从中国法的角度，简要分析 DID 法律性质如下：

根据《民法典》第一编“总则”第五章“民事权利”的规定，民事权利主要分为财产权、人身权和其他民事权利和利益三大类，其中，财产权主要包括物权、债权、知识产权、股权及其他投资性权利、数据、网络虚拟财产权等，人身权主要包括人格权和身份权。

（一）DID 本身可能并不构成财产权或人身权

首先，DID 本身并不具有经济价值。DID 的创建过程表现为在区块链上通过加密计算随机生成，其本身并未凝结无差别的人类劳动；其次，DID 并无独立的价值，其依赖于特定主体的控制或行为而实现自身用途。换言之，DID 本身应当与 DID 指向的信息分开对待，DID 本身实际上是一种确认拥有者满足某种要求或享有某种权利的凭证，是一把打开保险箱的钥匙，其重要程度依赖于保险箱中的财物的价值，其本身并不具有满足人类所需的经济价值。

其次，DID 不可交换。DID 的作用在于确认拥有者的主体身份，是现实身份在虚拟世界的投射，或

是虚拟主体线上身份的合集，具有极强的绑定属性；如果允许随意转让 DID，则无疑允许受让方以出让方的身份进行社会交往，这显然违背了基本的社会关系法则和 DID 的创设初衷。

因此，我们理解 DID 本身可能没有具备经济价值和可交换的财产属性，因此可能不被认定为财产权。此外，DID 本身并不会跟拥有者链下的法律身份相关联，可能与拥有者链下的法律身份相关联的是 DID 指向的 VC 中的个人信息。因此，DID 本身可能不被认定为人身权。

（二）DID 能否被认为是财产权的权利凭证存在一定不确定性

如前所述，DID 本身可能不具备财产属性，但 DID 的 VC 中的数据是否具有财产属性，DID 能否被认为是财产权的权利凭证，也存在一定不确定性。

首先，如果 VC 中记录的是 DID 持有人链上资产、交易、活动的相关数据，该等数据是否具有相应的经济价值，能否被大数据公司等机构商用，具有一定的不确定性；如果 VC 中记录的是 DID 持有人的链下个人信息，其可能也不具备可交换的财产属性。

其次，目前《民法典》对于数据、网络虚拟财产权并无明确的定义，因此 VC 中的信息能否被认定为数据、网络虚拟财产仍有一定不确定性；并且《民法典》对数据、网络虚拟财产持有人享有的民事权益也暂无明确的规定。

但是，如果 VC 中记录了持有人的债权或知识产权，并且通过该 VC 可获取持有人的债权或知识产权，则此种情形下 DID 可能被认为属于财产权的权利凭证。

（三）DID 可能被认为是人身权的权利凭证

如果 DID 仅是聚合链上数字身份的标识符，并不与持有者的法律身份相挂钩，则 DID 所指向和记录的内容可能并不涉及人身权。如果 DID 是连通链上数字身份和链下法律身份的标识符，DID 的使用方式为对外展示去标识化的公钥，从而避免直接出示个人信息，因此通过 DID 无法直接识别到现实法律主体，但 DID 业务的关键环节是验证 VC 从而建立信任机制，验证 VC 后可能直接获取持有人的法律身份，在该情形下，DID 可能被认为是人身权的权利凭证，原因在于：

首先，VC 中可能记录了 DID 持有人链下的个人信息，而个人信息属于前述《民法典》的保护范畴，具有非常强的身份属性，盗取和非法使用个人信息也会违反《个人信息保护法》的规定。因此，盗取和非法使用 VC 中的个人信息，DID 持有人的身份权会受到侵犯。

其次，如果侵权人在区块链上对 DID 持有人进行侮辱、诽谤，或侵犯 DID 持有人的隐私，在通过 DID 可识别出 DID 持有人真实身份的情况下，DID 持有人的人格权也会受到侵犯。

五、结语

值得注意的是，DID 业务在中国的发展仍处于早期阶段，尚无明确统一的行业标准。并且 DID 在中国法下的法律性质和地位目前并无明确的法律规定，实操层面司法机构对于 DID 法律性质及民事权利保护的案例也较少。本文的分析为我们基于现行法律框架进行的尝试性分析，如未来立法和司法机构对该等问题进行进一步明确，我们将适时与大家做进一步探讨。本篇我们尝试探讨了 DID 业务的基础法律问题，下篇我们将进一步对 DID 发行者、DID 拥有者和 DID 核验者的合规要求及法律风险，进行更加深入的剖析，敬请期待。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

夏彦

电话： +86 755 3680 1989

Email: yan.xia@hankunlaw.com