**DID 赛道全网最详细梳理 + DID 灵魂三问**

[[](https://foresightnews.pro/column/detail/26)](https://foresightnews.pro/column/detail/26)

**[NFT Labs](https://foresightnews.pro/column/detail/26)**

**[2022-10-09 15:00](https://foresightnews.pro/column/detail/26)**

来源链接

订阅此专栏

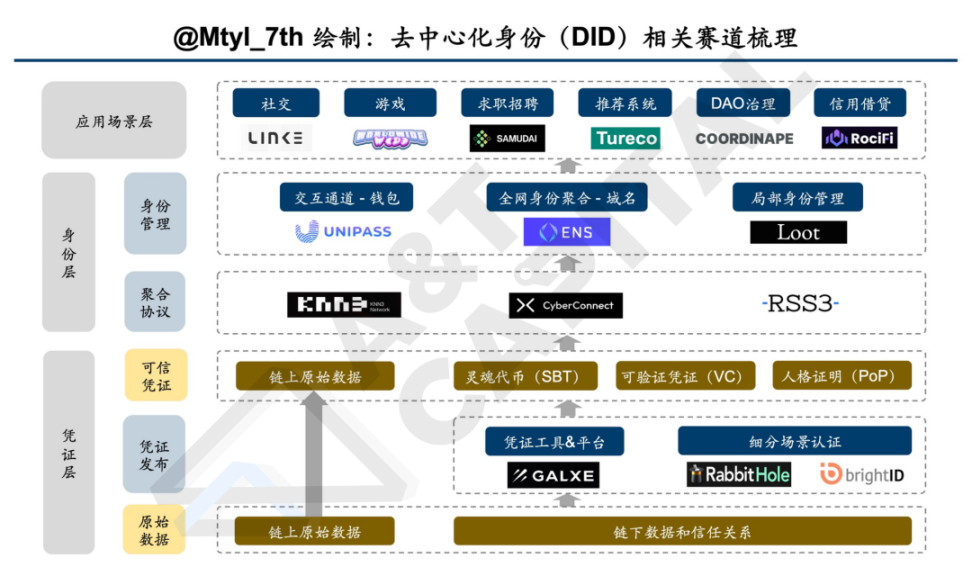
收藏此文章



*- 全文共 13896 字，阅读约需 13 分钟 -*  
**📻：被大家催了好多次的 NFT Labs 社群开张啦，不管你是 NFT 爱好者，链游玩家，交易者，亦或者是数字艺术家，都欢迎大家一起来交流想法，NFT to da moon～（进群方式：直接戳我【ID:lovebit98】就好！文末也有联系方式^ ^）**

***01 摘要***

* DID 现在一般是”去中心化身份“（Decentralized Identity）的简称，它是一种没有中心化机构做最终担保的数字身份，是 Web2”用户画像“概念在 Web3 的延伸和拓展.
* DID 相关的赛道主要分应用场景、身份、凭证三层。凭证层是 DID 的构成组件，身份层是 DID 的具体形态，应用场景层是 DID 的价值体现。
* DID 发展的最终形态，可能是每个用户都有一个唯一的全网身份，和多个细分场景的局部身份。用户通过域名来记忆、标识 DID，通过钱包来管理 DID 并和应用项目交互，通过钱包集成内的各种协议整合多条链上的不同凭证和局部身份。
* DID 当前并不是用户的直接需求，而更多是应用场景项目方的需求.
* DID 发展尚处于萌芽期，并且迭代较为缓慢，至今未有 DID 体系能积累起一定的网络效应；这主要缘于当前 Web3 非金融类应用项目发展的艰难。
* DID 一级投资的整体逻辑：从用户出发，应用先于协议



***02 前言：***

***DID，一个被泛用、甚至滥用的概念***

DID，是一个 Web3 领域的热门概念。在 Twitter 上，几乎每周都有讨论 DID 的 Twitter Space；在线下的各种 Web3 分享会中，DID 也是经久不衰的热门主题之一；在项目的融资 deck 上，无论是社交、GameFi、DeFi、NFT 等应用类项目，还是钱包、域名甚至公链等 infra/ 中间件类项目，都可能会把 DID 加入其叙事之中。

然而，如此高的热度，不免的让 DID 这个词被泛用、甚至被滥用：

* **在最初的时候，DID 的全称是“Decentralized Indentifiers”，直译”去中心化标识符“**。它是最具影响力的国际互联网技术标准机构”万维网联盟“（W3C），出于对 Web2 中心化身份体系的担忧，而牵头制定的一套标准。这个 DID 的概念，一开始和区块链 /Web3 其实没有直接的相关性，但如果你直接搜“DID”，依然能够看到不少文章所谈论的 DID 是这个具体的标准
* **而在现在的 Web3 交流中，DID 更多时候被看作是“Decentralized Identity”的简称，也就是泛指“去中心化（数字）身份”**。然而，去中心化身份本身也是一个缺乏明确定义的词汇，虽然初看每个人都能理解它大概的意思，但在不同场景下具体指的事情可能很不一样；而且在 Web3 的世界里，似乎做什么事情都能和它扯上关系。这也是为什么目前有关 DID 的讨论中概念较为混乱的原因。

**本文接下来所讨论的 DID，将采用后者”去中心化数字身份”的概念，并将以 DIDs 代指 W3C 的 Decentralized Indentifiers 标准以避免混淆**。

**本文分上篇和下篇。在上篇中，笔者将分应用场景层、身份层、数据层，对 DID 赛道做一个系统性的梳理，以帮读者理解各种概念之间的区别和联系；在下篇中，笔者将阐述一些有关 DID 赛道未来发展和早期投资的一些主观看法，以抛砖、供读者思考交流**。

***04上篇：***

**去中心化身份（DID）赛道全景解读**

**在 Web2，数字身份以平台为中心，同一集团内的不同产品间通过账号系统打通**。例如，腾讯的邮箱、游戏、金融等皆可使用同一账号；Google、Facebook 等互联网头部企业也均有自己的账号体系。这种身份体系虽然构建方便，但它的弊病也已经广为人知：平台相互之间的账号并不互通，以及用户没办法控制自己的身份数据。

**在当前的 Web3，用户的交互主要基于钱包地址，因此围绕地址的一系列活动构成了 Web3 最原生的数字身份**。但是创建新地址的成本几乎可以忽略不计，也少有人会把自己绑定在一个地址上。这就导致了用户可以随时放弃一个地址所代表的“身份”，也可以零成本创建大量的地址“身份”，进而导致限制了这种数字身份的应用场景。

DID 希望解决的问题，就是在去中心化的数字世界里，构建起对一个人身份的描绘。

**一、DID 的应用场景：假如我们已经有了一套成熟的 DID……**

**DID 是一个抽象的概念，为了更好的对它有一个直观的理解，让我们先屏蔽有关 DID 如何实现的细节，从应用场景出发：如果当前在 Web3 世界里已经有了一套成熟的 DID，它能做些什么？**

笔者把 DID 在应用场景层的叙事，大致分为两大类：**Reputation（声誉）和 Relationship（关系）。**

它们的主要区分方法，是假设如果你准备放弃你现有的“数字身份”，你能否在较短的时间内来重建一个可以代表你的新的身份？

如果是前者，那就是 Reputation 类；如果是后者，那就是 Relationship 类。

**1.1 Reputation：声誉 / 简历 / 社交展示面**

这类应用场景，**侧重于通过将数字身份简化为一些显性的可信标签，来对用户进行评价和分类，从而达到一个快速筛选的效果**。这里举三个具体的相关例子：信用借贷、求职招聘、陌生人社交

**Web3 信用借贷**，希望能给用户账户地址打一个”信用分“，从而推算在信用借贷中质押可减免的额度。这种信用分，可以通过链下身份 / 资产证明来完成，也可以结合用户链上地址过往操作记录的分析。

**Web3 求职招聘**，希望能够在链上生成一个用户的简历，以便用户快速向 Web3 项目方 /DAO/ 社区等证明自己的能力，降低 Web3 求职招聘过程中的信息摩擦。简历中的工作经验、Web3 能力等认证，可以通过链上地址分析、前东家的多签钱包地址签名、Web2 公司邮箱认证等方式去完成。

**Web3 陌生人社交**（包括异性社交、兴趣社交等），希望快速构建对一个用户的标签描述。这种标签的描述可以取决于 NFT 的持有，例如 BAYC 的持有者可以被贴上“富有“的标签，各种兴趣类、社区类 NFT 的持有者也可以被打上对应的标签。用户可以把这些标签整合起来，放到自己的社交主页上去做展示；用户也可以根据这些标签快速筛选自己希望社交的对象、并对其兴趣偏好有一定初步的了解。

**1.2 Relationship：DID 的关系类应用场景叙事**

这类应用场景，**侧重于通过将数字身份视为用户在 Web3 数据的累积，来做一些更加复杂、综合的应用分析**。这里举四个具体的相关例子：

**Web3 推荐系统**，希望通过用户的 Web3 相关数据的累积，形成用户画像，再对此展开针对性的个性化推荐、广告展示等。这套用户画像的叙事，其实继承自移动互联网时代平台大厂的核心逻辑，已经被证明可行。并且在 Web3 中，不仅身份数据可以跨平台互通，用户也能拥有自身身份数据的所有权、开放共享权，这样构建的用户画像体系可能会比 Web2 更加用户友好。

**Web3 熟人社交**，希望通过用户在 Web3 社交互动的累积，形成一套用户的社交图谱，这种社交图谱可以被各种新的 App 所通用。这样，用户在使用新应用、进入新游戏的时候，就可以快速找到自己的熟人好友，而不必像 Web2 那样得自己重新加回来。

**Web3 游戏**，希望构建一套游戏账户系统（GameID），通过用户在 Web3 游戏数据的积累，来刻画用户在游戏方面的兴趣和能力。例如，A 用户可能在某几个 Web3 卡牌类游戏都有非常早期的参与记录，那么这些都可以被记录在 GameID 里面，这样如果新的卡牌游戏想寻找早期用户，就可以优先考虑 A 这样的人。

**DAO 投票治理**，有时候会希望进行”一人一票”的公平投票。但是如何证明一个人只投一次票，而非注册多个账户来刷票（女巫攻击），是一个难题。通过对用户地址历史记录的分析或者真人认证，就可以解决这个问题。

**1.3 两类应用场景之间的联系：由点到面，再由面到点**

其实，**Reputation 和 Relationship 类应用的关系并没有那么泾渭分明，更多的是一种网状交错的关系**。

**更准确的说，各种显性的可信标签像是“点”，随着时间的推移，这些点围绕着同一个身份不断累计，最终生成了有关用户画像的完整的”面“；当用户或者项目方真的要利用这个”面“的时候，也需要进行进一步的加工，把它简化为几个易于描述和理解的“点”**。

例如就 NFT 持有这件事情，在初期的时候，可能对一个用户只能打上 BAYC 持有者、Azuki 持有者等标签（点）；但随着时间的推移，如果我们发现每当有热门 NFT 出现，这个用户都会去参与交易（面），那么我们就可以做一个归纳分析，给他打上“热门 NFT 交易者”的标签（点）。

以上，基本上是所有 DID 在应用场景层面叙事的一个归纳总结。可以看出，它基本上涵盖了几乎所有 Web3 应用层的叙事，这也是为什么 DID 也被称为 Web3 应用的“身份基础设施”。

**二、原始数据形式和凭证：构成 DID 的各个属性究竟从何而来**

可能读者已经感觉到了，在上述不同的应用场景叙事之中，每个数字身份具体指代的东西其实不太一样，但它们都可以被称作“DID”。这里面，其实主要有两个关键问题：

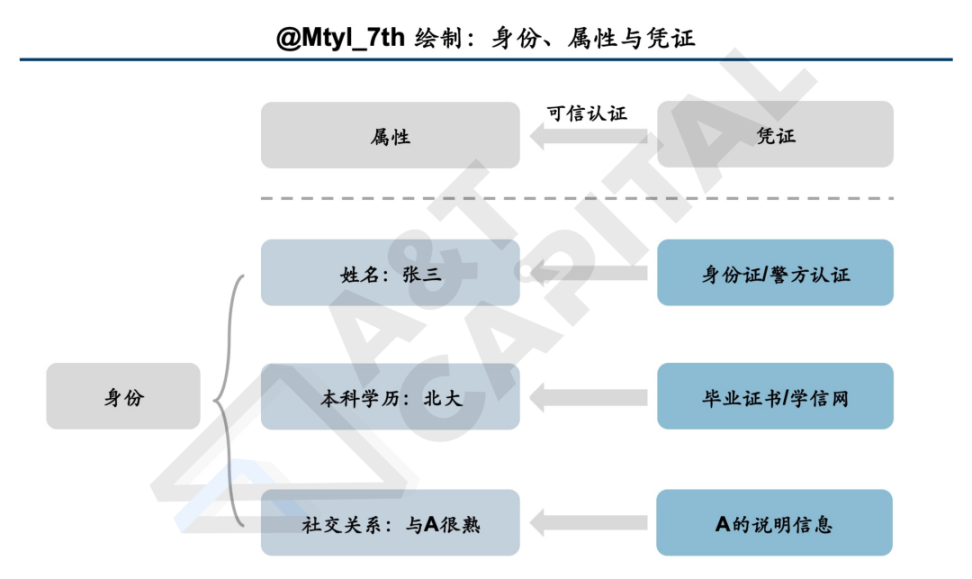
* 这个“去中心化身份”，它是由哪些具体的标签 / 属性 / 凭证组成的？比如，它希望连接的，是用户的 NFT 持有、链上交互记录，还是用户的社交关系，抑或是用户在链下的身份信息？
* 这个“去中心化身份”，它是聚合在哪个标识符（Identifiers，ID）之上的，或者是说面向外界交互的主要接口是什么？比如，我们是用一个 NFT、一个地址、还是一个域名来代表某个身份?我们怎么拿一个身份来和应用方互动？

理清楚这两个问题，就能看清楚在 DID 在身份层纷繁复杂的各类项目。

让我们先来思考第一个问题，即，构成 DID 的各个属性究竟从何而来。

**2.1 凭证：为什么对于去中心化身份很重要？**

先看以下例子：你新认识了一个人，他说“我是张三，1990 年出生，本科毕业于北京大学，和你的父亲很熟”。他有求于你，但是你因为某些原因，对他的自我介绍内容抱有极大的不信任。那他应该怎么向你证明他所说的事情的真实性呢？



如果他想证明他的姓名、年龄，他可以出示他的身份证，甚至可以和你一起去派出所走一趟来证明这身份证是他本人；如果他想证明他的学历，他可以出示他的毕业证书，或者是给你发个学信网的证明；如果他想证明他和你的父亲很熟，他可以联系你父亲来找你说明。反过来说，如果他有求于你、很想证明自己的身份，但当你希望他提供上述的具体凭证的时候他却无法提供，那么你就有足够的理由去怀疑他陈述的真实性。

因此我们可以看到，**一个身份，是由许多个属性组成的，例如刚才张三对自己的陈述中，所涉及的姓名、出生年、学历、社交圈等属性。但是，如果没有相应具体的凭证，这些属性是没有可信度的，而多数应用场景不会去采纳一个没有可信度的数字身份**。**由于在 Web3 中，一个身份的属性来源更加多样、潜在使用方更加广阔，难以找到一个中心化的总担保方，因此对每个属性的凭证验证就显得更加突出**。

**2.2 凭证原始数据来源的分类**

**所以，当我们在研究一个 DID 的具体构成的时候，其实我们关注的就是具体的凭证**。

**用户的链上数据，由于区块链底层的不可篡改特性，是最天然、直观的凭证数据来源**。甚至这种信任，可以只基于底层公链，而不需要具体的凭证发行方。比如，要证明钱包地址 A 确实向钱包地址 B 转过钱，只需查对应的链上信息即可。这种没有凭证发行方的信任，是其它几种凭证数据来源所不具备的，也是区块链的核心魅力之一。有不少 Web3 的工具类产品，做的就是链上数据的整合分析。

**不过，在目前的 Web3 世界中，链上数据主要以转账、DeFi 交互、NFT 交易 / 持有为主，它所能带来的身份信息是有局限性的**。然而**在现实世界中，很多时候我们信任一个凭证的前提，都是信任一个凭证的发行方，而这种信任关系的构建却是在 Web2 或者是现实世界之中的。很多时候，我们很难把整个验证过程完全放到链上，例如驾驶证 —— 即使再怎么数字化，考试本身还是发生在现实世界之中的。**

当前，将 Web2、现实世界中的数据和信任关系做成可信的凭证的形式，主要有以下三种：SBT、VC、PoP。

**2.2.1 灵魂绑定代币（SBT）**

SBT(Soul Bound Token)，即灵魂绑定代币，是 2022 年 5 月 Vitalik 等人在发布的”Decentralized Society“一文中所阐述的新概念。

**由于 SBT 目前并没有一个通用的明确标准，其实现在的 SBT 可以被简单理解为 Non-Transferrable Token，即“不可转让的代币”**。事实上，以这种代币为形式的凭证早就存在了，比如 POAP、Project Galaxy 所颁发的凭证。

**SBT 的实现是最为简单的，也天然具备非常好的互通性、公开性**。并且，由于 SBT 是链上原生的，它也可以作为一个链上数据分析方法的”结果凭证“，比如链上信用评分。

**SBT 主要的问题在于其公开性所引起的用户隐私相关问题**。SBT 的公开性使任何人都可以轻易地对一个人进行关联和推断，而且可能让隐私无从遁形，并刺激了某些形式的歧视。例如，一个有种族主义倾向的雇主，可能会因为偷看求职者的钱包显示其参加过黑人生命关怀组织活动，而对潜在雇员产生歧视。

理论上，通过 ZK 技术和 SBT 的结合，可以实现用户的隐私保护。但这不仅涉及到具体的技术实现上的一些难点，也可能会影响到 SBT 的公开性和互通性。

**2.2.2 可验证证书（VC）**

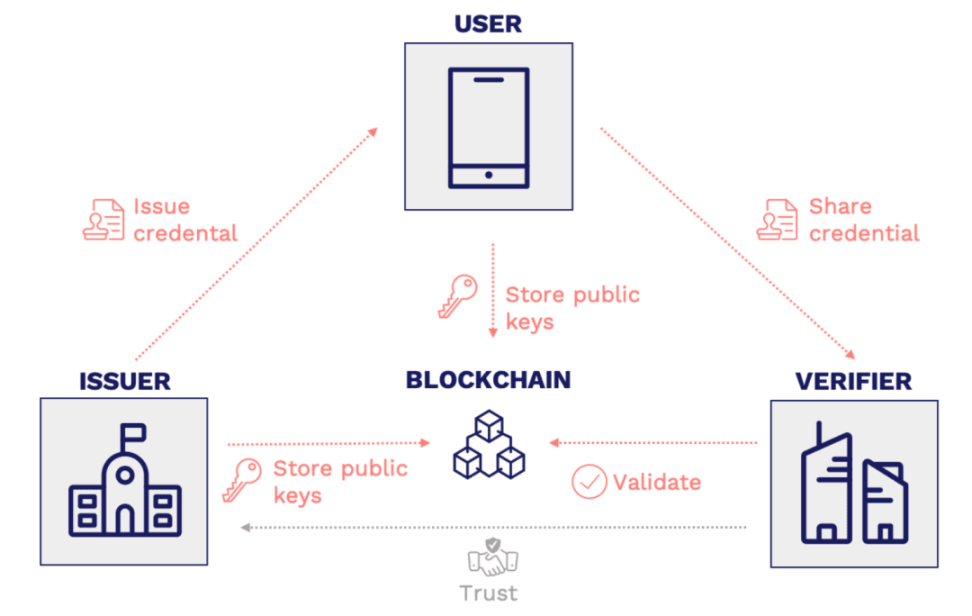
Verifiable Credentials，直译“可验证证书”。

在本文的开头有提到，最早在没有区块链的时候，就有一些人开始思考数字世界的去中心化身份问题了，VC 也是 W3C 提出的概念、标准体系内的一部分。

让我们通过下面这个跨国驾照认证的例子来直观理解 VC：

* 假如一个德国人 Hans 获得了驾照，那么就可以向申请德国官方，用其去中心化标识符（DIDs）来颁发并签名一个 VC。这个 VC 以数字文档的形式存在，是 Hans 取得驾驶证的凭证，由 Hans 自己保存。
* 如果 Hans 到澳大利亚并开始自驾游，需要出示自己的驾照时，他就可以向澳大利亚政府出示他从德国官方这里拿到的 VC；澳大利亚官方在看到了这个经过德国官方 ID 签名过的数字文档以及上面的信息之后，就可以认为 Hans 具备驾驶的能力。

虽然，严格意义上 VC 的具体撰写有一套 W3C 定义的标准，里面的去中心化标识符也是 W3C 体系内的 DIDs。**但从 Web3 的视角来看，广义上用钱包地址去代替这个去中心化标识符，在基本逻辑上是行的通的，下图就展示了用户、VC 发行方、VC 验证方之间的关系**：



可以看出，**VC 相比于 SBT，其主要优势在于对用户隐私的保护，用户可以天然的对自身的信息进行可选择性披露**。并且，它的实现可以和区块链技术无关，也就是对于 Web2 也有很好的兼容性。

**VC 的主要问题，在于它本身虽然有一套相对公认的标准，但这套标准需要 DIDs 做支撑（详见后文），而 DIDs 的推进相对缓慢**。如果项目方或者 Web3 社区要自己定一套 VC 的运作流程标准，那么怎么去推广这条标准，也会是一个难点。

**2.2.3 人格证明（PoP）**

人格证明（Proof of Personhood），主要做的事情通过同链下真人信息绑定的方式，来证明数字身份的唯一性。Proof of Humanity，BrightID，和 IDENA，都是其中的代表项目。

具体的实现，主要通过 KYC 和视频人脸识别两种技术。**KYC 是交易所盛行的经典认证方式，通过 KYC，一个数字身份就会和你在链下的法律实体信息（姓名、国籍等）绑定；人脸识别，如 BrightID，主要将你的人脸信息录入数据库中，确保在一个项目 ID 系统里面一个人只能注册一个 ID**。

**可以看出，PoP 类认证在当前最直接的应用场景是抗女巫攻击。另外，在各国都在考虑加密货币监管的大背景下，KYC 有可能会成为一个“合法身份”组建的必要条件**。

**2.3 凭证类的相关项目**

**可以看出，虽然去中心化数字身份的具体构成可能很复杂，但归根到底，主要由以下四大类凭证构成：链上原始数据、SBT、VC、PoP**。

严格意义上，SBT 也是链上原始数据的一部分，但 SBT 一定是通过某种方法再次加工过的，并且其信任可能依赖于发行方；而对链上原始数据的信任只需要基于对底层公链的信任。

和凭证相关的具体 Web3 项目又有哪些类型呢？

多数情况下，**许多凭证的认证规则有很高的互通性**，比如说验证用户是否在链上完成一笔交易，验证用户是否帮忙转发了项目方的 Twitter，或者说验证这个用户背后的真人是不是第一次尝试获取凭证。在这个背景下，凭证的发布方本身并不需要做一套发布凭证的工具。

**因此这个细分领域不少的项目类型，其实是凭证发布的工具 / 平台**。以 Project Galaxy 为例，项目方可以在 Project Galaxy 上发布任务，用户可以通过在平台上完成任务并做认证后，获取项目方发放的凭证。

**但在一些复杂的情况下，凭证的发布方希望自己设计规则来给用户进行认证，特别是在一些较为复杂、评价存在一定主观性的场景**。之前提到的人格证明类凭证，也可以归为凭证发布类的项目。

其它的例子如：

* Rabbithole 是“学习认证”类项目的代表，它提供各种 Web3 称号的认证（如 NFT Creator，Explorer 等），这些就需要用户完成较为复杂的任务；某种程度上，这里面的逻辑和在线网课的结业证书很像，Rabbithole 也可以说是“Web3 在线教育”的一种雏形。
* ARCx 希望根据每个 DeFi Passport 持有者的信用分来量化其链上地址的信誉度。信用分将通过分析持有者的以太坊地址历史活动来确定，其范围设置为 0 到 999 分，该信用分确定了协议为用户提供的抵押率。对于信用分高的地址而言，DeFi Passport 能够提供有竞争力的借贷抵押。
* FirstBatch 希望通过读取用户在 Web2 社交媒体的授权数据，用 AI 在链上生成用户的兴趣标签，并用 ZK 技术进行隐私保护。

**三、身份层：应用场景和凭证的连接，具体的 DID 形态**

我们已经讨论了 DID 具体的应用场景，也讨论了 DID 身份的具体构成 —— 凭证。**而将应用场景和凭证连接起来的，就是身份层项目所做的事情**。例如，域名、钱包、社交图谱、地址关联分析……

**如何区分一个项目到底是不是在做身份聚合？这里笔者提出一个判断方法：如果一个项目（或项目模块）做的事情，既没有在具体面向用户的场景里面用到 DID，也没有给用户生成新的凭证，主要做的事情是各种”绑定“和”连接“，那么它大概率就是身份聚合层的项目**。

但是怎么做一个 Web3 的身份聚合，不同类型的项目给出了不一样的路径和思考方式。它们大体可以分为两大类：对链上原始数据、各种凭证的加工聚合，以及面向用户、帮助用户实现数据主权的身份管理工具。

**3.1 信息聚合协议**

**用户的链上数据，往往分散在多条公链、多个项目智能合约之内，因此需要把它们经过加工和聚合以后才能形成一个身份**。许多项目，做的就是这样的一个信息聚合的协议。

这些协议，往往没有直接面向用户的产品，它们主要是面向项目方和其它协议的，可以相互之间进行合作于信息聚合。举例如下：

* Cyberconnect 希望做一个链上社交图谱，聚合用户的社交关系数据
* KNN3 Network 希望通过对 Footprints 关联分析、Cyberconnect 等其它社交图谱的整合，来构建在多条链上的用户社交关系图谱
* RSS3 希望做一个链上的内容和社交信息的聚合，之后可能会往 Web3 的信息分发、推荐系统方向发展

而下面几类身份管理工具类项目，都希望给用户提供主动的身份管理能力，是用户实现数据主权的直接工具。

**3.2 身份管理工具 - 钱包**

**钱包直接面向用户，是当前公认的”Web3 入口“。虽然它本身不太能说是一个 DID 的应用场景，但它是一个天然的连接应用场景和用户所持凭证的通道**。

一个理想的”DID 钱包”可能是这样的：**首先，它能够聚合所有主流公链的地址，在具备基本签名、转账等交易的同时，整合用户在不同链上碎片化的数据；其次，它能够显示用户所拥有的各种 SBT/VC/PoP 凭证，在和应用项目交互的时候，用户可以自主授权向项目披露哪些数据，从而帮助用户实现数据主权**。不少钱包都会提到 DID 的叙事，如 Unipass，ABT Wallet，Selfkey 等。

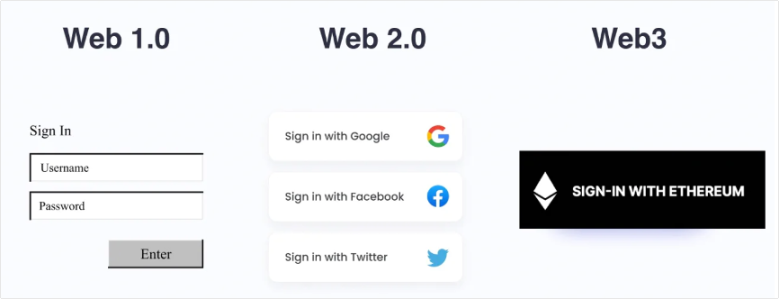
不过，当前主流的 Metamask 等钱包并不具备这些功能。一个重要原因是，它们基本都是 EOA 钱包，而这类钱包基本只支持链上地址最原生的操作 —— 查询和转账。而智能合约钱包，有望在钱包功能上实现更多的扩展。DID 钱包相关的技术落地其实有不少挑战，不过也非常值得我们期待。

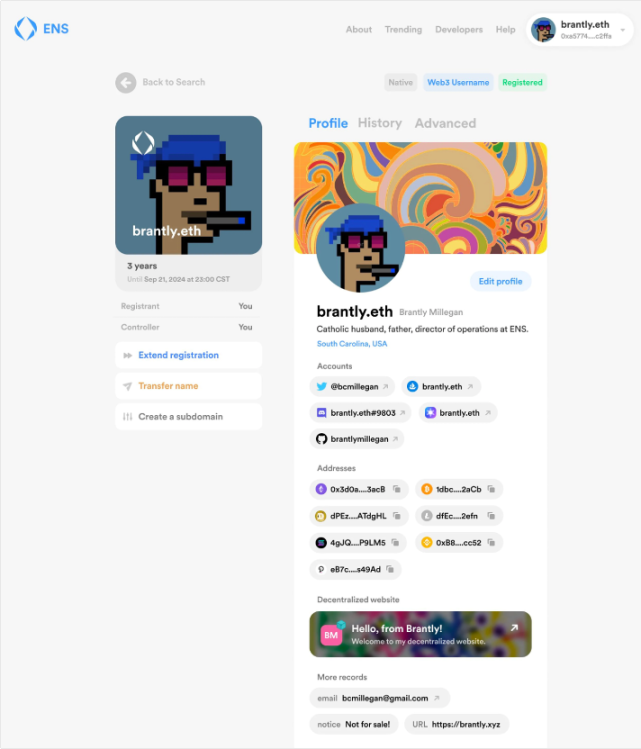
**3.3 身份管理工具 - 域名**

虽然我们每个人都有一个独一无二的身份证号，但在日常生活中，我们一般会用”姓名“来作为一个人身份的标识符（虽然可能会有重名），因为它更便于日常交流。

Web3 的世界，同样也有这样的问题：**虽然人们目前的交互主要基于钱包地址，但没人会愿意记那一长串字符串。如果说 Web3 的数字身份需要一个”姓名“，那么域名类项目所做的事情，就是希望成为这个”姓名**“。

ENS 是域名中知名度最高的项目，它有以太坊基金会的官方支持，提供.eth 后缀域名的注册服务，现在已经有了近 180 万的注册量。值得注意的是，SpruceID 在和 ENS 合作，在推进 EIP-4361: Sign In With Ethereum。如果该项提案顺利实施，这将取代 Connect Wallet，让域名于钱包地址之上、成为 Web3 的入口。另外，ENS 也希望通过域名中一系列身份的整合，来完成自己”Web3 姓名“的愿景。





另一个值得关注的域名项目是 Space ID，它有币安官方的支持，提供.bnb 后缀域名的注册服务。Space ID 也希望将.bnb 域名与用户在不同链上的多个地址，用户的 Twitter 等 Web2 账户进行 id，成为一个 Web3 领域的 Universal name。相比于 ENS，Space ID 的产品迭代速度和落地速度会显得更快。

除了 ENS 和 Space ID 以外.bit、Unstoppable Domain 近期也完成了较大额的融资。它们讲的和 DID 相关的叙事，基本上大同小异。

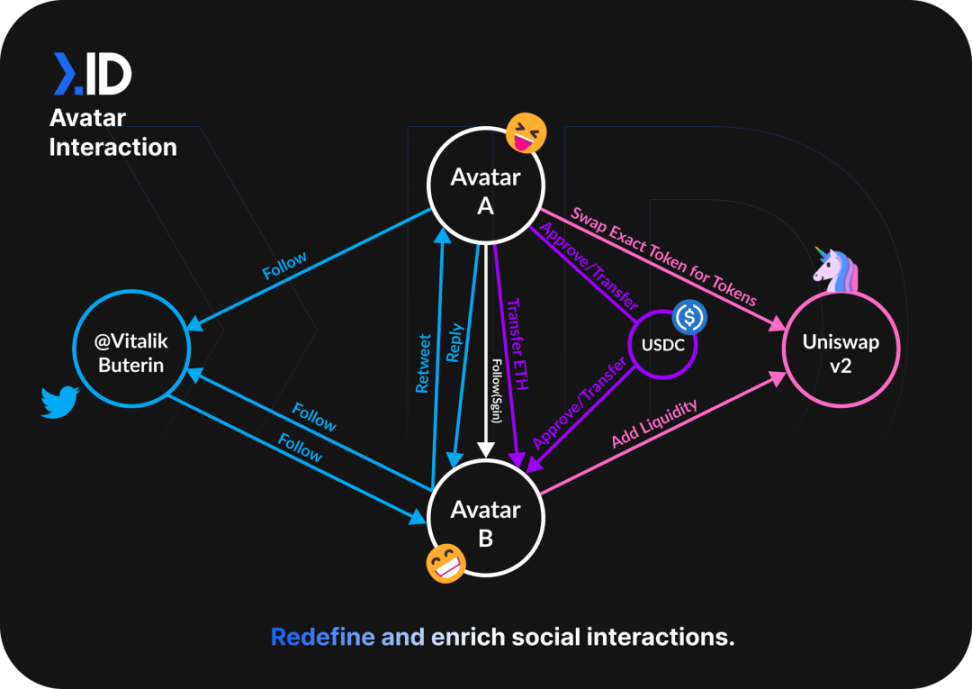
**值得注意的是，域名和钱包虽然都可以作为身份管理工具，但它们在角色定位上是很不一样的。它们在理论上并不冲突，而是可以紧密合作：钱包可以用一个域名作为钱包账户名的替代，并将其作为和应用方交互时的”姓名“；域名也可以整合多个链上地址甚至多个钱包账户。**

**3.4 其它身份管理工具 - 以 Next.ID 为例**

也有一些身份管理类产品，对身份管理实现的具体理解有别于之前的几类项目，但做的事情核心主要也是各种连接和聚合，并且不局限于特定领域，希望做一个全网身份的整合。下面以 Next.ID 为例，这是 Mask Network 做的一个身份管理类的新产品。

**和不面向用户的身份聚合 protocol 项目不同，Next.ID 是一个面向用户的产品**。在 V1 版本中，用户可以通过 Mask Network，来实现 Web2 各平台账号、Web3 各公链钱包地址的连接和聚合，并且能够做主动的身份管理；相比于域名和 DIDs，可以说 Next.ID 也是在做一个统一数字身份层面的聚合，并没有强调一个显性的标识符，而是希望在聚合身份之后将其做成一个基础设施，供 App 调用。假如 Next.ID 之后开始推广自己的域名，或者是推广 Mask 账户用户名等标识符，那么它做的事情和 Space ID、ENS 等域名项目就会有一定的重合度了。

但除了用户侧的聚合以外，开发者可以通过 Next.ID 的 Avatar 体系，实现将自己产品中用户账号之间的具体操作和 Next.ID 互通，如下图所示；它在一定程度上可以做很多身份聚合类的 protocol 想做的事情，也可以选择和这些 protocol 合作，将它们再做聚合。



**来源：Next.ID 官方文档**

**3.5 局部场景身份管理工具**

**3.5.1 GameID**

除了一些希望做一个用户全网数据大聚合的身份管理工具项目以外，也有一些基于局部场景打造身份管理工具的项目。

比较好理解的例子，是**聚合用户各种链上游戏信息的 GameID，如去年比较火爆的 Loots。**

GameID 里面的 ID，更多是指在一个生态系统内部互通的账号体系，类似于 Web2 中盛大账号、QQ 号，它们只想做用户在这个生态系统内部的特征描绘，并不是想做一个代表用户全网数字身份的大聚合。

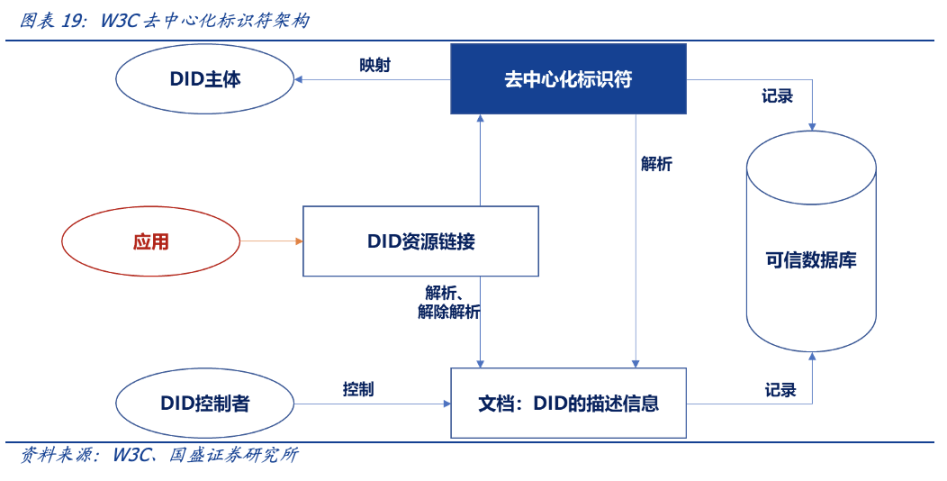
因此，与其说它是 DID，不如所说它是用户 DID 的一个局部碎片、一块拼图。

例如，张三注册了域名 zhangsan.eth，他的“盛大’ID 是 123456，里面有 5 个来自不同”盛大系“游戏项目的凭证；他的”腾讯“ID 是 567890，里面有 9 个来自”腾讯系“游戏项目的凭证。那么虽然“盛大”和”腾讯“可能都有一个专门的身份管理工具帮助用户管理对应的平台账户，但在它们都可以被 zhangsan.eth 这个”Web3 姓名“所聚合，成为 zhangsan.eth 身份的一个标签。

**3.5.2 DIDs**

经过多年的研究和讨论，W3C 终于在 2022 年 7 月推出了去中心化标识符（DIDs，decentralizedidentifiers）的 v1.0 正式标准。**作为”DID“最初的定义，理清楚 W3C 的 DIDs 和现在的 Web3 DID 体系之间的关系，也是有必要的**。

W3C 标准的去中心化标识符架构中，用户直接控制着标识符和对应的文档。APP 能够在用户许可下读取 DID 链接的文档从而实现业务，文档中包含了数字身份相关信息，如签名、加密数据等等。用户通过加密签名证明对 DID 的所有权。用户的数据存储在可信的数据库内（如区块链），身份数据并不依赖 APP。



DIDs 有三个组成元素，如下图所示：DID scheme，类似于 http、ipfs 等方法声明；DID Method，是一个具体方法的标识符，每一个想建 DIDs 身份体系的项目都可以去申请一个，例如腾讯可以为 QQ 申请一个 tencentqq 的标识符；DID Method-Specific Identifier，是一个具体的 id，它有什么用取决于具体项目方的定义，例如腾讯可以用 *did:tencentqq:123456789* 来指代你的 QQ 号 123456789。



DIDs 的详细运作流程和技术细节，相对复杂，这里就不展开详细介绍了。

**DIDs 某种程度上和 Web3 域名是竞争关系**，这里把 DIDs 和域名的主要区别做个对比：

1. **在可读性上，DIDs 相比于域名而言更缺少用户层面的可读性**，但由于 DID Method 的存在，它可以多带一层语义、有更好的灵活性
2. **在信息聚合的潜力上，DIDs 加上与之配套的 VC 等验证方法，理论上可以聚合更多链下信息**，特别是权威机构提供的数字凭证；而目前域名类项目的数据聚合还是以链上信息为主，如果要更好的链下信息聚合，可能需要与之配套的 VC 标准
3. **在数据存储上，DIDs 的数据存储并未指明**，可以直接存在公链上，也可以存在一些去中心化数据网络上（比如 Ceramic Network），甚至也可以直接给用户自己存储；域名类项目的数据存储都是在链上的

**总体而言，DIDs 这套体系，是一个自上而下设计的，更全面、兼容性更好的标准**。也有不少采用 DIDs 路线去实现数字身份的项目，如 Ontology。

**但是，DIDs 的用户可读性缺失问题，长期来看很难成为用户日常生活中记忆的”Web3 姓名“，再加上用户在不同的 DID Method 里面可以有不同的 DIDs，使得 DIDs 从长期来看可能会是一个被域名所聚合的对象，因此可以将它称为“细分场景 / 局部身份管理的标识符”。另外，虽然理论上 DIDs 对链下信息有很好的兼容性，但出于利益考虑，当前 Web2 公司鲜有基于 DIDs 做相关的推荐，DIDs 如何推广也是个问题**。

**3.6 身份管理工具：全网身份 vs 局部身份**

GameID、DIDs 的这种局部身份聚合特点，也引出了对身份管理的总体性和局部性的思考：

**如果你的身份管理产品不能、或者做不到对用户全网数字身份产品的聚合，也就是没有成为用户的“Web3 姓名”，那么由于链上数据的互通性，你的 ID 可能就会成为那些更大的身份管理产品的一部分**。例如，**小的 GameID 被大的 GameID 聚合，GameID 被.eth 域名所聚合，甚至.eth 域名也可以被.bnb 域名聚合**。前文提到的 DIDs，之后也很可能会成为这种”局部身份“。甚至某种程度上，单个钱包地址也可以说是一个“局部身份”。

**不过，局部身份管理工具也有其存在的价值，因为它可以就具体的应用场景打造更多功能，而这是全网身份管理工具不一定会做的，不然它就会变的臃肿**。比如，在一个 GameID 管理平台里面，用户可能可以根据其它 GameID 的信息展示，来交同一个 MMORPG 内相同魔法职业的玩家为好友，但如果一个钱包 / 域名项目要做多个那么细分的功能，就会提高产品的复杂度，从而面临许多产品设计上的挑战。

**四、对 DID 未来发展的终极形态的思考**

**首先，未来每一个人都会有一个与个人日常生活深度绑定的数字身份：**

* **这个 DID 每个人只能有一个（通过 PoP），通行于 Web3 全网，甚至可能通过 KYC 等方式和用户的现实身份所绑定，从而更好的和链下世界所互动。**
* **Web3 域名，是这个 DID 的唯一标识符，也就是用户在 Web3 的名字。**
* **用户通过一种功能远比现在强大的多的钱包，来管理这个 DID；在钱包内部，可能集成了多个身份聚合协议，来实现用户多地址、多合约的数据聚合，全面的展现用户在各条链、各个地址上的凭证、局部身份、关系图谱等，作为一个整体用户画像。**
* **用户通过钱包，和社交、招聘、DAO 治理等应用场景交互。通过加密技术，用户可以自主控制项目方获取数据的权限，从而实现数据主权归用户所有。**

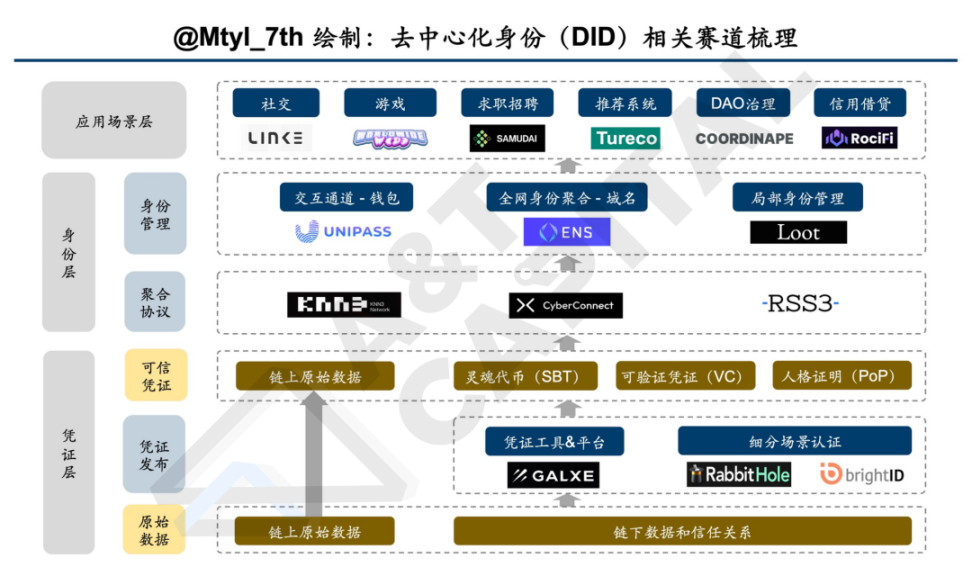
**其次，每一个人在一些局部场景（比如游戏平台），或者是一些无需 PoP 的场景，拥有多个不同的数字身份，从而在不同的场景下展现不同的自我。用户可以自由控制这些身份之间的相互连接，在特定的场景使用对应的身份。**

**五、上篇总结**

通过以上的梳理，希望以后当读者再看到一个项目在讲 DID 相关的叙事的时候，能清楚的知道这个”DID“指的是具体什么样的“去中心化身份”：**是在讲某类具体凭证的发布，还是在讲各种凭证聚合为身份的过程，还是在讲用户对身份的管理，抑或是在讲这套身份体系的具体应用场景**？

**非常值得提的一点是，一个 DID 相关的项目往往会做不止一层**；比如说，之前分析的 Next.ID 既向域名那样做用户侧的身份交互，也会向很多身份 protocol 那样做身份聚合；ARCx 既准备做信用评分凭证的发布，也会做与之相关的应用。

下图是一个对 DID 相关赛道的梳理，作为上篇的收尾。



***04 下篇：***

***DID 灵魂三问***

在下篇中，笔者将通过三个问题，阐述一些自己对 DID 领域的思考理解：

* **DID 现在究竟是谁的需求？**
* **为什么 DID 还处于萌芽期，且发展缓慢？**
* **DID 赛道，应该怎么投？**

**一、DID，现在究竟是谁的需求？**

**1.1 DID，现在不是用户的需求**

通过之前的梳理，可能不少读者已经发现了，**在很多情况下 DID 本身并不是用户的直接需求**！从产品经理的视角来看，DID 如果要面向用户，往往要通过具体的应用场景。

**试想，如果你现在没有具体的应用需求，你有兴趣去主动获取各种凭证（比如去 BrightID 做个视频人脸认证），或者到一些身份聚合 / 管理工具 (比如 Next.id)，把自己的邮箱、Twitter、各钱包地址都 Connect 起来么？相信大多数用户是不会的**。

虽然如果项目方提供一定激励，也肯定能够吸引一些用户，但 DID 类产品的特性，决定了单纯靠这种激励本身难以带来用户的持续留存，这和 NFT、GameFi 等其它类别项目不太一样。

**从长期来看，随着 DID 发展的逐渐健全，用户对个人身份数据的管理和利用的意识也会越来越高，那么有可能会出现对身份管理的需求先于具体应用场景的情形**。但在 DID 赛道还处于萌芽期的当下，这是不太可能发生的。

**1.2 DID，是应用场景项目方的需求**

其实，受益于 DID 更多的，还是具体应用场景的项目方。无论是基于凭证的快速筛选，还是快速获取用户在 Web3 的画像，都会给在冷启动阶段的项目方带来直接的增益。

不过，应用场景在真正用 DID、构建 DID 的时候，未必要和用户强调 DID 这个概念，它是抽象在产品的逻辑之中的。所以，更多的时候 DID 这个概念出现于项目的叙事和大家的讨论中，而不是具体的应用场景中，也就不奇怪了。

**二、为什么 DID 赛道还处于萌芽期，且发展缓慢？**

公认的事实是：DID 的概念可以追溯到 Web2 时代，从去年 11 月 ENS 发币后开始火爆，但现在 DID 赛道还处于萌芽期。虽然和 DID 相关的项目非常多，但至今 DID 的形态都还没有定论，也没有哪一个 DID 体系的数据积累已经有出现网络效应的迹象。

在理清楚 DID 的发展需要具体应用场景之后，不难理解这个问题：这和当前 Web3 发展的”超金融化“，非金融类 Web3 项目发展缓慢有关。当我们去看和 DID 叙事相关的应用场景的时候，可以发现几乎所有非金融类的 Web3 项目，都可以引入 DID 叙事。

因此，要回答这个问题，本质上是要回答为什么各个 DID 相关的 Web3 应用场景相关的赛道发展缓慢。

**2.1 Web3 非金融类应用场景发展缓慢的三个原因**

**笔者认为下面三条逻辑，适用于所有的 Web3 非金融类应用场景类项目的分析**，包括社交、游戏、招聘等。（钱包等偏工具属性的项目不在讨论范围内）

1. **Web3 应用的用户体验，当下和对应的 Web2 应用差的很远**。无论是产品的使用门槛、网络延迟还是操作费用，都高于 Web2。
2. **Web3 应用的用户基数，远小于 Web2，且分散在世界各地**。这不仅阻碍了现实世界和链上世界的联通，也给网络效应的积累带来了更多的困难。
3. **现在处于熊市周期，不少用户的资产亏损、链上活动频率降低，甚至也已经有些用户开始像 2018 年那样怀疑整个行业，直接“退圈”；这使得 Web3 应用类项目的启动更加艰难**

上述这些每一条，都可能是一个 Web3 应用场景类项目难以发展的重要原因。那是不是 Web3 应用类项目就没有发展机会了呢？并不是。**在一些 Web3 原生、Web2 做不了的场景，即使有上面问题，相关的产品也能够体现出它的价值。**

**2.2 To C 的信用借贷，中短期内是伪命题**

（To B 信用借贷更多牵涉到 CeFi 的逻辑，因此此处主要讨论 To C 的信用借贷）

**信用借贷，是 DID 的应用场景中最金融化的。这也是一个经常出现的议题，因为现有的 DeFi 几乎都是超额质押，资本利用效率低，理论上信用借贷可以提高用户的资金利用效率，Web3 用户对此也会有较强的需求**。

**然而，笔者认为，To C 信用借贷在中短期内（比如三年内），都是一个伪命题，或者是一个极其小众的领域**。

**最主要的原因，在于 Web3 世界并没有像 Web2 那样，对不偿还的贷款有追索机制**。因此不偿还贷款的极限代价，是失去一套链上身份的可用性。

有人可能会说，数字身份本身也是值钱的，你可能不希望放弃你用了多年的地址、域名等身份标识，包括上面的各种凭证和关系数据的累积。但问题是，扪心自问，多数 Web3 用户当前的链上身份又能值多少钱？如果能够”信用贷款”100U，多少用户可能想着不还钱、宁愿重建身份？除非信用审核的门槛极高，但这也会让其变成一个极其小众的产品。

有人可能会说，如果做 KYC、人脸识别，可能得以规避这个问题。然而事实上，在各不发达国家的乡村地区，不值钱的个人真实身份数据比比皆是。想一想大家日常看到的”某交易所 KYC 账号批量出售“等信息吧，只要“信用额度”高于一个身份的构建成本，就会出现职业的“养号”用户，批量构建满足要求的身份，然后不还贷款，薅项目方的羊毛。

To C 信用借贷的成熟，可能需要等待整个 DID 体系的成熟：一方面，随着各种高价值凭证和各种数据关系的积累，数字身份的构建成本、放弃门槛也会越来越高；另一方面，随着各国监管的渗透，Web3 的贷款可能也会建立起法律追索机制，这会提高用户不还贷款的代价。

**三、DID 赛道一级投资的逻辑是什么？**

在这里，笔者分享一部分个人对 DID 赛道一级投资的整体思考：

* 整体逻辑：从用户出发，应用先于协议
* 具体优先级：身份管理 > 应用场景 > 凭证发布 > （不面向用户的）身份聚合 protocol

**3.1 整体逻辑：从用户出发，应用先于协议**

这里的“应用”，是广义的“面向用户”概念，包括具体场景、身份管理、凭证发布；“协议”，泛指不直接面向用户的各种 protocol 产品，它们往往以 API 调用的形式，服务于应用项目方或者其他协议。

有一些协议项目方，可能是这样思考的：作为一个协议，我会不断的说服更多的应用项目方来接入我的协议，这些应用可能多数只是昙花一现，少数可能发展不错，但无论如何，我的数据都积累起来了，开始有了数据壁垒和网络效应；这样我的价值也越来越高，会有越来越多的应用层项目来找我合作；最后，我就可以对 API 收费，或者是提供相关增值服务。诚然，上述逻辑是有已经道理的，也是有走通的可能性的。

但笔者主要出于以下原因，更偏向于应用优先：

* 首先，在数据的流向上，应用一定先行于协议，从而会有更大的主动权。协议与应用之争乍看有点像“先有鸡还是先有蛋”，但其实不是。因为前文已经论述过了，DID 数据的积累，依赖于用户在具体应用场景的互动。
* 其次，协议项目方做的东西，可能并不成熟，还在概念 / 测试阶段；即使成熟了，也可能并不能很好的满足应用项目方的需求。应用方与其反馈给协议方、期待其迭代，不如自己做一个。
* 更现实一点来看，数据壁垒、网络效应这种如此优秀的、已经被 Web2 验证的叙事，在赛道发展的萌芽期，没有任何优秀、有野心的应用项目团队会主动放弃这个叙事，而把这种价值的捕获完全交给其他项目方做的协议。

毕竟，当前 Web3 应用类项目的融资本身就很艰难了，应用项目方为什么不自己把协议相关的 DID 叙事也讲了，来作为其估值支撑呢？比如，先通过应用本身吸引用户参与、积累数据，然后将用户在应用内的数据协议化，给相关的合作伙伴、生态系统使用，从而进一步积累数据，最终发展成为一个 DID 体系。这个叙事很多时候是完全讲的通的。

再加上多数 DID 的协议其实缺少技术壁垒，壁垒更多体现在一定的工程复杂度上；对于优秀的团队而言，在一开始就自研协议，难度不会很高；即使应用项目方初期为了产品快速迭代用了其它的协议，如果应用真的能够获得一定成功，项目方也可能会考虑自研协议，来提升项目的发展上限。

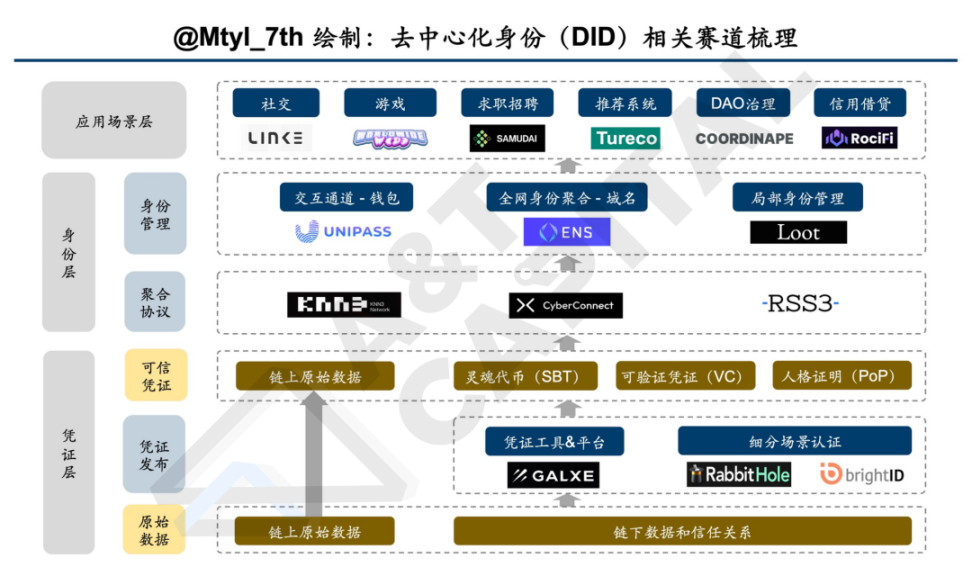
**3.2 具体值得关注的细分赛道**

优先级：身份管理 > 应用场景 ≈ 凭证发布 > （不面向用户的）身份聚合 protocol

身份管理工具类的项目：以钱包、域名类项目为优先。毕竟在未来笔者对 DID 的终极形态构想中，这两者都占据着非常核心的位置。

应用场景类的项目：之前说到，更多的机会出现在 Web3 原生的应用需求、而不是 Web2 产品的复刻。基于凭证的 Web3 招聘，基于 NFT 的兴趣社交 / 异性社交等，都是属于这种不可替代的 Web3 场景。

凭证发布类项目：凭证发布工具 / 平台这块，可能会跑出 1-2 个头部的通用项目，和数个细分应用场景的相应工具；具体的凭证发布类项目如果能提供高价值的凭证，那也是值得关注的。



<https://foresightnews.pro/article/detail/15908>