

我要入驻

# DID行业研究报告

我们无法低估DID带给人类的意义，因为人是社会动物，而身份是社会关系的起点。

身份管理（ID）是计算机技术基础设施的组成部分，但是因为其简单而且无处不在，因此经常被大家理解为想当然的存在而被忽略。就像生活中我们一

出生就默认有了身份一样。但是，一旦我们丢失了ID之后或者像《谍影重重》电影里面的主人公被政府剥夺身份后，就会发现我们寸步难行。

正像现实世界里面ID是生活的基础组成部分，ID技术也是计算机的基础设施。我们打开电脑的时候，第一步就是要输入用户名和密码登陆系统，我们访问任何网站的时候，大部份的操作需要输入用户名和密码。

人类社会进入文明社会以来，这世界上大多国家都建立了完整的身份管理系统。国内用身份证或者驾照或者社会保险号，国际旅行用护照。互联网大概遵循了同样的发展道路：

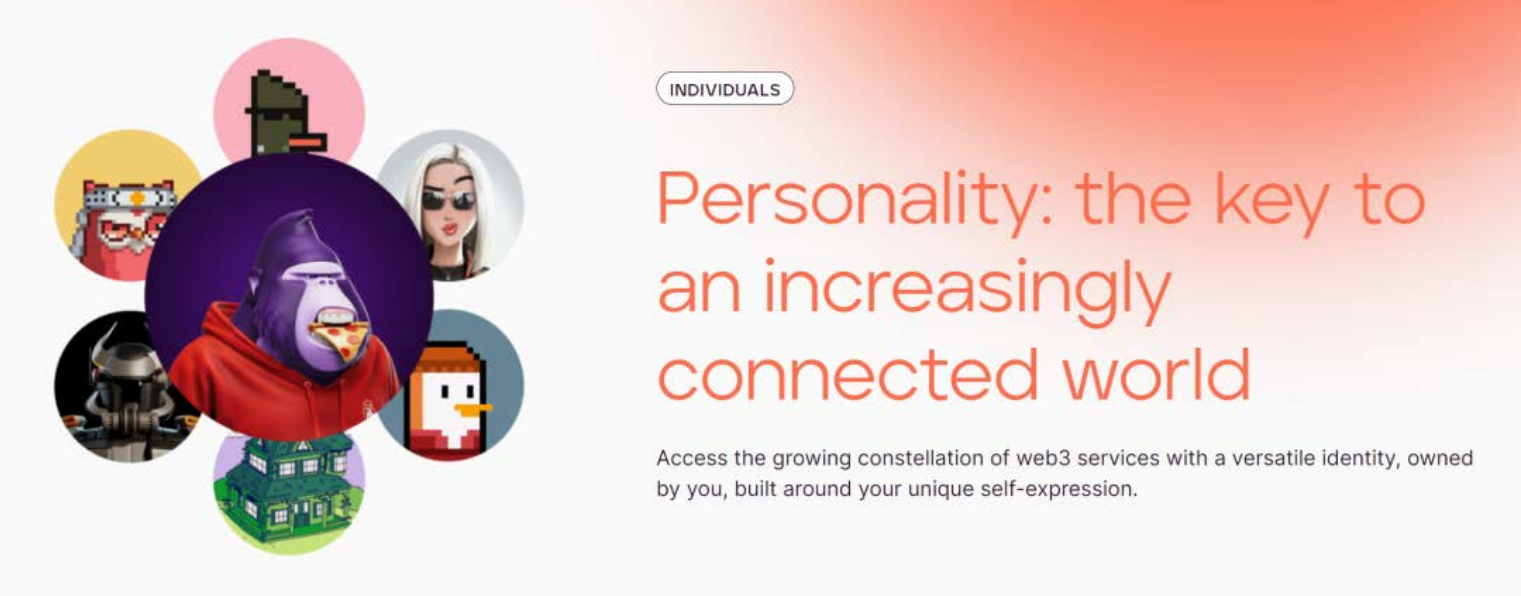
从1996年的“在互联网上没有人知道对方是条狗”的匿名时代，发展到了2004年Facebook成立后的实名社交时代。互联网也从一种信息获取手段发展到了电子商务和电子政务等重要工作效率手段。

可以预测到，区块链也会从现在完全匿名的状态，在未来一个周期发展到由DID去中心化身份（Decentralized Identity）支持的实名阶段。区块链至今缺乏对用户身份的支持，因此被过度的金融化而无法进入实用场景。而且，正如互联网的发展，网络平台效应在由用户控制的共享情况下产生的效用，要远远高于完全被公司控制（如Facebook）或者完全公有被政府控制（如道路）的机制。

当然，ID不仅仅包括人，还包括各种主体，比如：公司有营业执照和D-U-N-S@代码，手机有mac地址，我们可以统一将这些称为主体（subject）。

因此我们使用ID这个术语的时候，我们应该小心，有些人认为权威机构颁发的才叫ID，有些人认为任何一个机构都可以颁发由自己认证的ID。本文讨论的DID用的广泛意义的ID，比如用户自主生成的公密钥对就可以作为ID。

事实上，任何一个用户已经在使用DID，因为用户进入加密世界的第一步就是生成钱包，在比特币链上，你的比特币地址就是一个你的DID（比特币的设计并不友好，因为每一次交易都变更地址为了保护隐私）；在以太坊上，每个用户都拥有一个以公钥为地址的DID。不管广义还是狭义的ID，ID都必须在一定范围（namespace）内保证唯一性，而且生成ID的意义一般绑定一定的使用环境（context）。



和DID紧密相关但是没有必然关系的一个概念是Verified Credential(VC)。VC代表了一个由中心化主体（issuer）对一个主体（subject）发行（issue）的证书（credential）。传统上因为这个证书无法保真，因此issuer必须提供相应的查询验证服务，比如：在中国教育部提供了学历查询验证服务网站。因此，如果查询验证必须线下进行不够便利，就会刺激伪造证书和影响证书的使用效率；如果发行主体停止提供服务，就会影响证书的使用；如果证书有有效期经常需要更新，就会更麻烦。

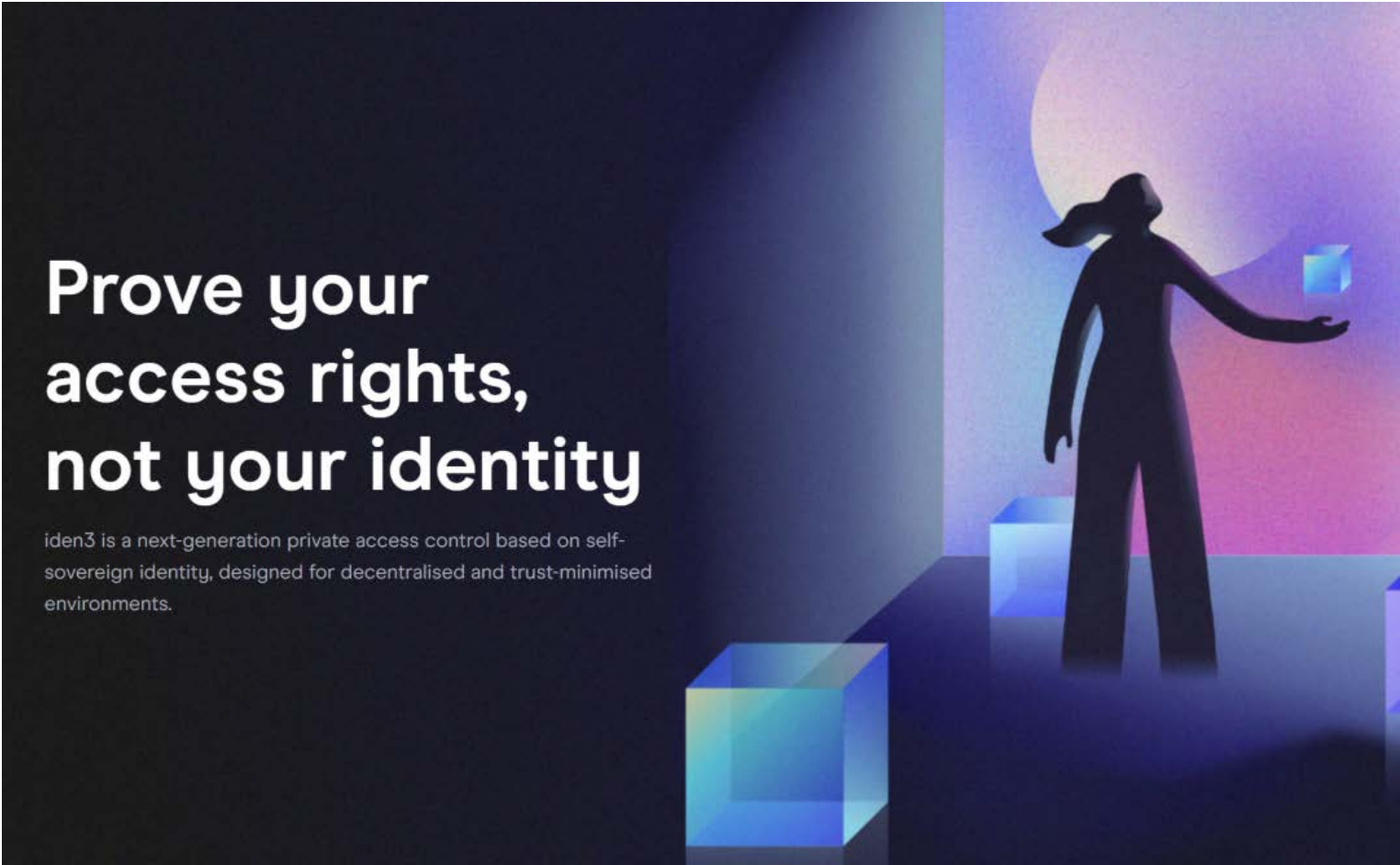
但如果基于加密技术的证书，就可以通过发行主体（issuer）的数字签名对证书进行签名，验证可以在加密算法数学的支持下单独进行，subject可以将VC放入自己的数字存储介质（repository，包括钱包）里面，在需要的时候提供给第三方（verifier）查看和验证。

虽然w3协议明确说明DID协议和其VC协议是完全分开的，可以独立存在的协议，但是其DID假设用户自主生成的公密钥对必须结合权威机构颁发的VC使用才有意义。w3的DID协议里面的公密钥对只是作为DID架构的支撑部分而存在，用来链接一个用户拥有的不同VC，以及解耦合VC查询，验证，展示对于发证机关的依赖。

而且，DID的存在不需要区块链，区块链技术支撑的DID地址解析和数据登记只是作为DID生态的一部分。但是，本文作者认为，作为数字原生的元宇宙的组成部分，一个subject可以完全脱离VC而存在，根据subject的元宇宙行为而独立于VC存在。就像在DeFi热潮中，大量用户根据公钥地址作为DAPP的账户系统参与DeFi交互，虽然不方便，用户还是通过Nansen等钱包地址标签来进行交流。

我认为，加密世界里面的NFT，gameFi，DeFi等大量的应用场景为原生的DID以及对应的链上信誉提供了足够的市场应用场景。这些设计哲学方面的不同，导致了w3的DID和区块链原教旨的DID有很大的不同。鉴于整个去中心化身份的技术刚刚起步，各个技术流派需要互相借鉴，本文的讨论不区分w3 DID和区块链原生DID技术。

另外，一个subject可以有多个ID，即一个人可以有多个身份；persona是一个相对概念，比如在国内使用身份证，跨国使用护照，那么护照和身份证相对于同一个主体就是不同的persona。



# Prove your access rights, not your identity

iden3 is a next-generation private access control based on self-sovereign identity, designed for decentralised and trust-minimised environments.

经常和ID管理联系在一起的概念还包括验证（authentication）和授权（authorization）。验证指第三方（verifier）通过issuer或者加密算法验证主体身份的过程；验证身份之后，第三方根据自己的政策（policy）授予主体对应的权利范围，这个过程称为授权（authorization），简单举例，当我们登陆一个论坛的时候，输入用户名和密码的过程称为验证，网站会根据我们是管理员还是普通用户会授予我们相应的读帖和删帖的权利。对用户权利管理的政策经常会被称为Access Control List(ACL)。

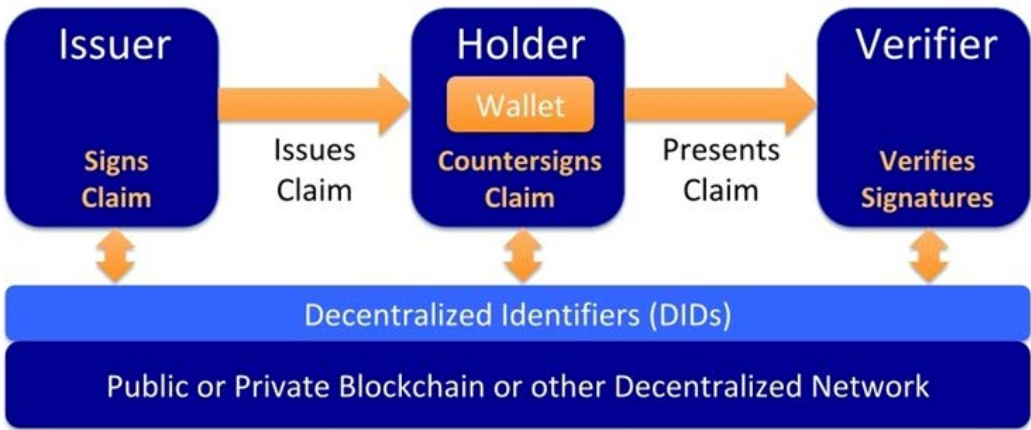
一个ID可以有很多属性（attributes），一组属性可以定义角色（roles），这样提供ID应用场景的管理员可以方便的基于自己定义的访问限制列表（Access Control List），按照不同的属性或者角色授予（authorize）不同的ID不同的权限。比如：Tom（subject）第一天入职公司Big（issuer），领到了66的工号（ID），他的名字Tom为属性（attribute），分配的工作岗位为信息管理员（roles），赋予（authorize）了相应的可以进出机房的权利（ACL）。

在DID出现之前，所有的ID都是由一个中心主体（issuer）基于某种政策（policy）授予一个主体，这个中心主体因此有权利授予或者取消某个个体获得ID的权利；有时候，这个中心主体必须为第三方（verifier）提供对应的验真查询服务（比如Tom更换工作后，新的雇主希望做背景调查核实Tom是否真的为Big工作过）。因此，subject依赖于issuer的服务，issuer如果停止服务或者拒绝服务，就会对subject使用ID的权利造成影响。

我们无法低估DID带给人类的意义，因为人是社会动物，而身份是社会关系的起点，不依赖于发行方的身份自由是自由的起点，有了身份，才能讨论包括财产权的各种权利，就如同注册账户后才能使用网站的权利。当我们拥有一个不依赖于任何主体而生成和使用的身份主体的时候，才能讨论建立数据拥有权。因此DID的设计理念经常被称为自我主权身份（SSI, Self-Sovereign Identity）。

因为没有了一个中心化的身份发行方提供查询验证服务，DID与传统ID管理技术（IAM）最大的区别是，谁来生成这个ID？以及当你声称（claim）你拥有或者控制这个ID的时候，你如何证明你是你自己？

# DIDs enable digitally signed **verifiable claims**



DID是人类历史上第一次给予了subject自己证明是自己的一个技术。

DID基于密码学技术自我生成一对公密钥，公钥作为自己的ID，密钥作为自己控制对应公钥的证明。为了关联自己的其他中心化的身份，如果发行主体提供VC服务，就可以非常简单的通过验证签名VC来关联；如果发行主体不提供，则subject可以声明（claim）拥有某个中心化ID或者链下身份，然后通过第三方验证（attestation）服务来关联。

在我们深入探讨DID行业之前，我们小结一下，DID的特征和术语。

ID代表的主体（subject）可以是人，公司或者任何一个物体；

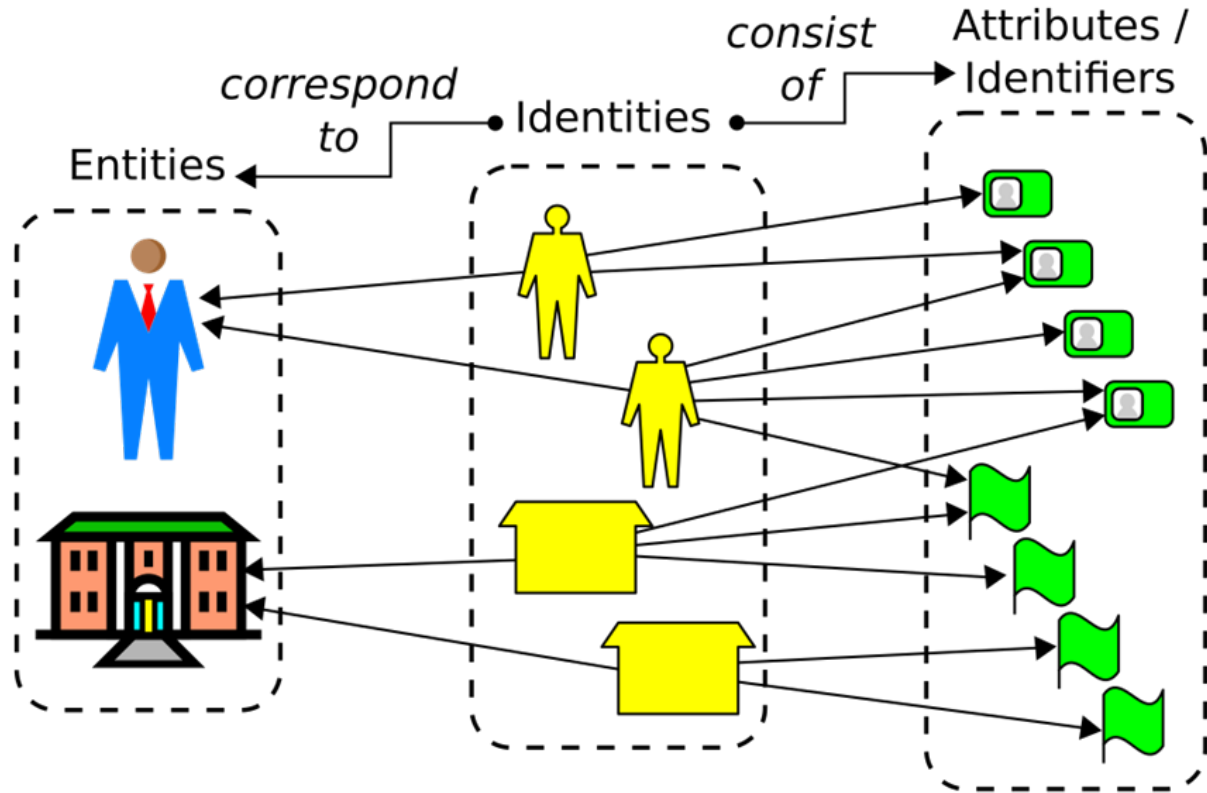
ID在一个范围（namespace）内必须是唯一的；

ID一定有一个发行方（issuer或者传统IAM中称为Identity Provider），DID的发行方是subject自己；

issuer需要为第三方（verifier或者传统IAM中Relying Party）提供查询和验证服务，DID的验证由加密算法的数学公式提供；

一个声明（claim或者statement或者assertion）包括自我声明或者第三方声明，需要提供对应的验证（verify或者attest）机制；这种验证机制有时候是确定性的，比如一个人声明他拥有1个比特币，可以通过验证他是否控制一个超过一个比特币的地址验证；验证机制有时候是概率性的，比如一个人声明他拥有Java编程能力，这个声明需要以前的同事背书，虽然拥有编程能力的熟练程度是一个概率；

身份天生具有场景特征，人们在不同的场景使用不同的身份（persona）；而职能（role）定义了一个属性（attributes）集合，代表了一类用户经过认证（authenticate）后被赋予不同的权利范围（ACL）。





由于DID和VC的技术基于加密算法，这给零知识证明的应用提供了空间。当用户需要验证年龄需要出示自己身份证的时候，不再需要担心验证者顺便看到了自己的家庭住址；当用户需要证明自己的资产满足某个条件时候不需要让对方知道准确的资产总额。

在整理好这些概念之后，我们来深入学习DID的行业，中间我们会穿插着对比传统的ID管理概念对比。以下的讨论分为几部分：**DID**的应用场景，**DID**的技术架构，**DID**的挑战，**DID**的行业公司，我们公司设计方案。

## 一、身份管理的发展以及DID与IAM的联系和区别

身份管理的发展经过了4个历史阶段，中心化身份管理(centralized identity)，联盟身份管理(Federated Identity)，以用户为中心的身份管理 (user centric identity)，用户自主身份管理 (Self-Soverein Identity)。

第一阶段在互联网发展早期，中心化的组织IANA（1988年）为机器分配IP地址，ICANN（1998）分配域名，而Certificate Authorities(CA)认证电子商务网站；为了扩张，这些设计都采用了树形组织架构，虽然不是一个中心，但是树形结构仍然被根（root）控制；1991年发明的PGP加密算法以及衍生的web-of-trust架构为后续的去中心化身份提供了基础，相对于CA的中心化管理，PGP允许任何一个人生成CA证书，由于PGP针对电子邮件的使用场景，而电子邮件由中心化的服务机构控制，因此PGP并没有实现完全的去中心化，加以其他各种原因，PGP只在加密爱好者群体里面流行，比如，早期区块链的开发者包括中本聪都使用PGP签名；

第二阶段为发生于2000年左右的联盟身份管理阶段，1999年微软发布了Microsoft Passport，支持一个ID跨多网站联盟，但是这个设计围绕着微软设计，因此微软成了中心；在对立阵营，Sun Microsystem发布了Liberty Alliance(2001)，针对以微软为中心的弱点，提出了像联盟区块链（POS）一样的多中心架构，正如POS没有发展起来，这种多中心架构并不受用户欢迎；

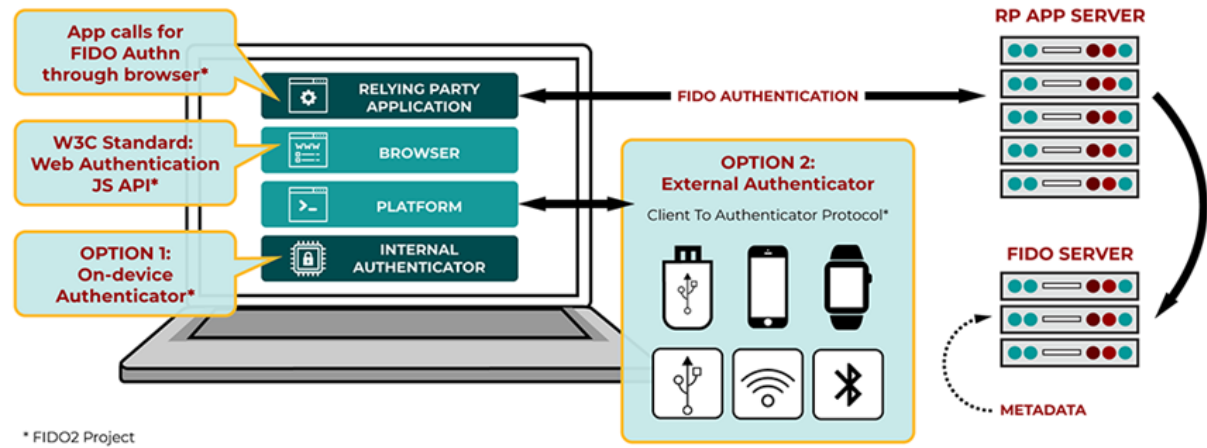
第三阶段为以用户为中心的设计，The Augmented Social Network在2000年提出了以用户为中心和用户拥有对身份的控制权的身份管理设计理念，提出了persistent online identity的设计原则；去中心化身份管理的爱好者在2001年成立了Identity Common和Internet Identity Workshop，发展了以用户为中心（user centric）的设计理念，该组织成员参与设计和推广了OpenID，OpenID Connect，OAuth，FIDO。OpenID允许用户搭建自己控制的身份或者使用支持OpenID的服务提供商，而且用户可以在OpenID的服务商之间自由切换。Google和Yahoo因为都是OpenID成员，所以Google和Yahoo的用户可以在支持OpenID用户的网站登陆。因为绝大多数用户不可能搭建自己的服务器或者使用不知名的第三方服务商，结果是大量的用户仍然使用Google和Yahoo等超级平台的账户，OpenID的去中心化再次失败；但是OpenID的经验被Facebook学习，Facebook利用强大的流量资源，吸引了Facebook Connect被大多数网站接受，大量的用户行为数据被Facebook收集并且滥用。

第四阶段的关键词是用户自主管理（Self-Soverein Identity，SSI）的身份管理，Kim Cameron通过定义10个原则仔细定义了SSI，包括Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimization, Protection。DID协议作为SSI的实现形式在2022年成为了W3C的推荐协议。

IAM通常有一个发行主体（IdP，identity provider）提供身份的发行，查询（directory），验证（validate），取消（revoke）服务；IAM通常包括LDAP，Active Directory，SSO，Identity Federation，SAML，oAuth，OpenID，WebID，Higgins。

DID的发行主体是自身，验证通过公密钥算法，但是为了方便找到和联系其他ID，DID依然需要一个中心化的查询服务，通常DID的查询技术通过区块链来实现，因为只有区块链能够对应DID的去中心化要求，如果由一个中心化的服务器提供查询，那么DID的去中心化就没有意义。

FIDO是国际上最通行的无密码认证标准，使用公私钥机制，完成用户认证。



其核心是：

- 设备中存储的用户公私钥
- 挑战应答机制完成认证

DID的认证部分学习了FIDO的机制。

## 二、DID的应用场景

除了传统的身份管理的应用场景，由于DID的生成和验证不再依赖于发行机构，而且具有可编程性，因此DID的应用场景打开了全新的应用空间，下面的探讨主要集中于原来中心化ID因为技术限制无法应用或者应用效率过低的场景，以及在加密和web3行业的应用场景。

### 1.验证真实身份

当前的区块链应用DAPP完全基于用户匿名的区块链地址，如果能够绑定用户的真实身份（通常指由国家颁发的身份证或者护照或者驾照或者社会保险证明），将会为DAPP的应用场景打开新的空间。由于这些中心化身份的颁发部门通常不提供网络验证服务或者w3标准的VC，因此这些验证服务通常需要中心化的第三方服务商提供，这类解决方案通常称为proof of Huamanity或者proof of Humanhood，这类公司包括BrightID和WorldCoin。

### 2.消除spam和空投薅羊毛

互联网由于接入和传输信息廉价并且匿名，造成了大量spam应用；在区块链应用中，当交易成本（gas fee）足够低的时候（就像Solana的链），或者spam的收益足够高的时候，就会造成如今的区块链充满了spam交易和薅羊毛。

由于DID的生成同样廉价，而且用户为了保证隐私或者拥有不同场景使用不同身份的合理应用权利，一个用户可以轻易生成很多DID，因此单单DID技术仍然无法消除spam，需要结合验证真实身份或者下面要提到的链上信誉一起使用。

3.支持链上信誉分

ID的生成和使用经常伴随着相应的应用场景，单独的ID仅仅具有识别（identifier）作用，具有很小的应用价值。信用分作为现代社会中人的身份的重要属性，为人的生活中获取第三方的服务提供了便利性，在美国，信用机构Experian可以帮助人们申请信用卡和贷款；在中国，芝麻信用可以免除用户支付租用单车和充电宝的押金。

在区块链应用中，如果用户的地址（DID）伴随着第三方权威机构给予的信誉分，DAPP就可以赋予不同的用户不同的权利。比如：一个曾经参与了AAVE早期应用的地址大概率是一个经验丰富的DeFi用户，可以优先批准该用户称为测试用户；一个被验证过为合格投资人的用户可以合规的参与项目。

链上信誉分通常由第三方提供，与传统的信用机构不同的是，链上信誉分服务机构应该将算法公开；而且由于区块链数据的公开透明容易获得，信誉分服务机构很难形成数据垄断，用户和DAPP有权利采用自己喜欢的服务机构。

4. 参与DAO的治理

DAO作为区块链行业倡导的下一代线上合作组织形式，需要对参与者进行身份验证和授予相应的权利。如今大多数DAO仍然通过链下的真人验证方式（包括邮箱和视频），并且不能程序化使用，大大限制了DAO的应用范围。如果拥有了可编程的DID身份，DAO可以根据用户的链上信誉和真实身份，赋予对应的权利。

5. 支持DeFi的KYC以及定制投资产品服务

通过DID，互联网应用可以为不同的用户提供不同等级的服务。例如，一个有良好还款记录的实体可以低利息或者低质押率获得贷款。Compound和Aave创建了像Compound Treasury或Aave Arc这样的单独的资金池，针对可以在美国监管制度下合规的机构投资者。

三、 DID与SBT的联系与不同

2022年5月，Vitalik提出了SBT的概念，赋予一个人或者主体一个不可转让的代币，集合了这个主体的众多属性，一个用户可以针对不同的属性生成不同的SBT，因此一个主体可以拥有多个SBT。SBT处于ERC20和NFT的中间状态，弥补了原来不能满足的一类资产需求，他们虽然是唯一的但是不能够被转让的市场需求。

简单来说，SBT的技术基于区块链原生的智能合约；而DID设计基于互联网基因的链接数据模型来设计。

Vitalik的论文更多的从应用场景的角度描写了绑定身份的不可转让的token的必要性，但是并没有提出具体的技术方案。



SBT的论文主要从token以及智能合约出发来设计用户身份，而w3c的DID标准规范主要从URI指向的文档来存储ID信息；基于智能合约设计可以允许可编程隐私保护，可编程身份授权等功能，而且完全具有链上，w3c基于URI文档的设计不依赖区块链而依赖于第三方的存储空间，可编程功能需要第三方设计机制来支持。相对于基于URI的API设计，基于token的技术框架来设计有一个巨大的优势，那就是让DeFi快速崛起的乐高可组合性。

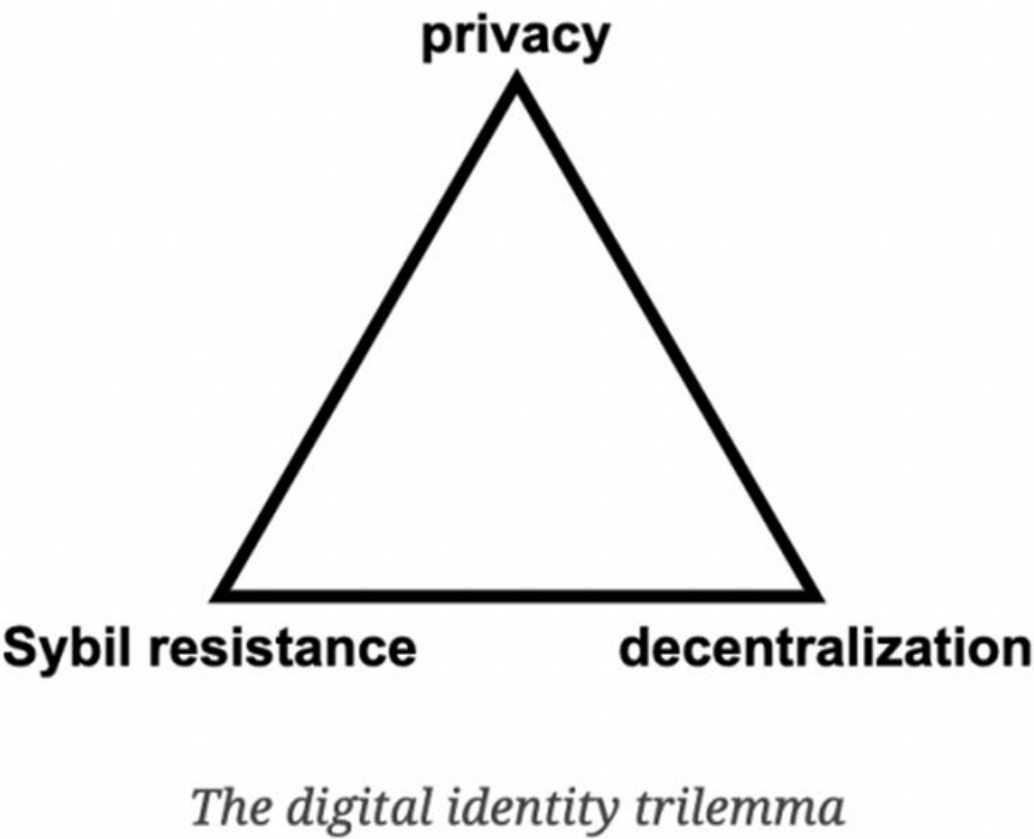
四、 DID的技术挑战

由于DID的去中心化特征，产生了隐私保护和验证机制的挑战。

对 DID 有所了解后，我们不难发现，去中心化身份也存在一个三角形难题：隐私、去中心化，抵抗 Sybil。如今的加密项目仍需要在三者之间取二舍一。

今天的区块链生态系统几乎普遍牺牲了对 Sybil 的抵抗来换取去中心化和隐私，如比特币、以太坊等。他们不依赖中央机构来记录身份，用户在创建钱包

地址时不必披露任何个人信息，但结果是，使用这些地址作为唯一标识的项目容易受到 Sybil 攻击。



然而当人们试图解决 Sybil 抵抗的问题时（如 KYC），就会牺牲隐私为代价，并增加了对其他身份识别形式的依赖，而这些身份识别形式既不保护隐私也不去中心化。

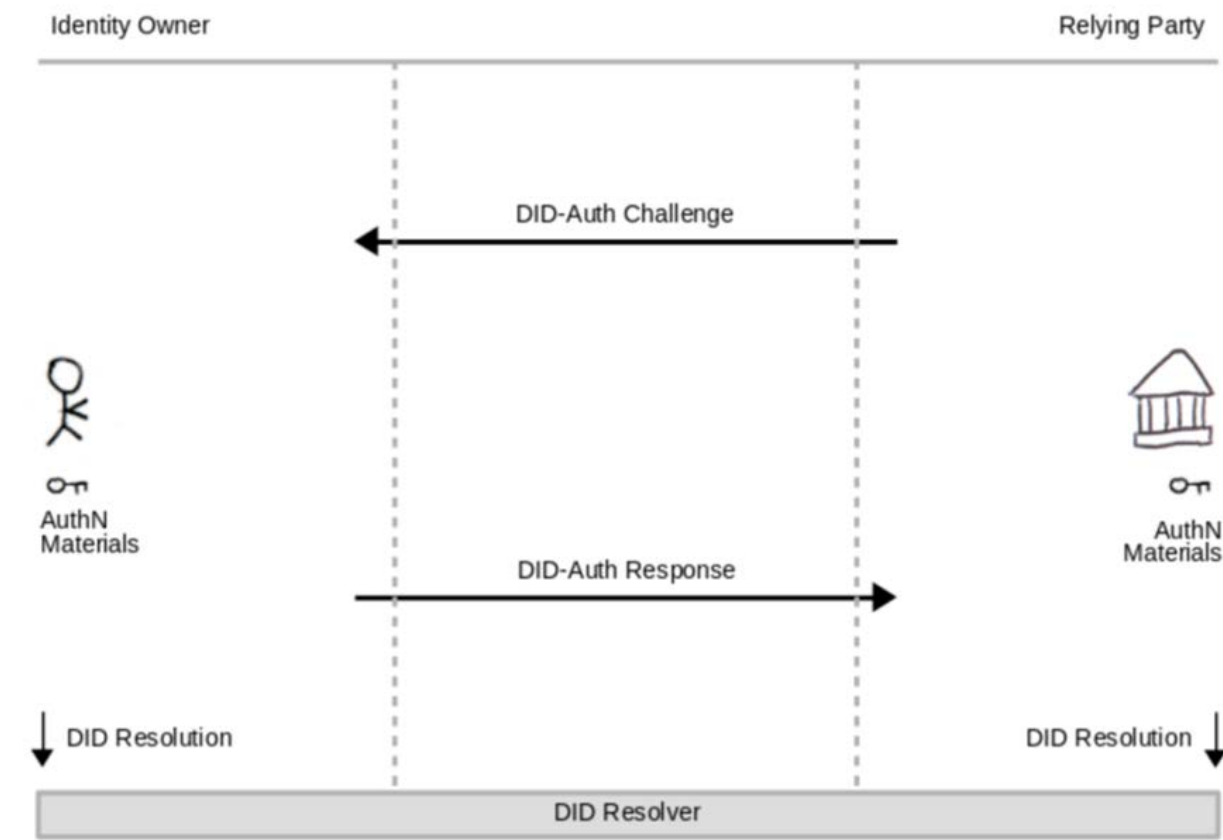
零知识证明技术（ZK）的发展为解决隐私保护提供了一条道路，ZK允许用户只披露验证方需要的信息；链上信誉的发展会为了解决Sybi攻击提供解决方案。

另外，每一个公链都有自己的DID？还是会有单独的DID公链？账户系统作为区块链的基础部分，ETH，Near，Polygon，BSC都发展了自己公链的DID系统，在用户端，钱包作为这些DID的聚合器；有的创业公司通过超级ID的方式来聚合不同的DID。

## 五、DID的设计原则和技术架构

DID的设计秉承了web2.0中以用户为核心的设计，由应用方发起挑战，用户向应用服务端证明，用户是DID持有者。这一步骤，W3C将其设计为标准的挑战应答机制：

DID Auth: High-Level Overview



在这个设计中，由第三方应用下发挑战信息，用户使用DID Document中对应的证明私钥，完成签名，已向对方验证自己身份。

我们可以看到，在认证流程中，DID的认证流程，就是基于传统的FIDO完成。FIDO对于DID的另一个价值，在于密钥的保管。DID的核心是用户私钥，按照现有钱包的设计，私钥通常存储于浏览器钱包、冷钱包中，对于浏览器钱包，恢复方式是通过用户主口令以及助记词。这种方式在安全性、易用性上皆有不足，安全性上容易被黑客盗取、钓鱼，易用性上需要用户记忆10几个助记词。而FIDO在今年，彻底解决了这个问题。FIDO联盟同苹果、谷歌、微软一道推出的PassKey和手机认证器，可以将私钥在不同设备中同步，使用用户指纹、人脸进行身份验证。

由于DID的去中心化特征和公开透明，我们需要尽最大的可能性包含用户的隐私，包括只对验证人提供必需的信息；避免任何人可以通过相关性跟踪用户；避免验证人之间互通信息（比如通过对不同的验证人使用不同的ID）。

DID需要包括以下模块：

- 1.DID生成模块：需要用户完全自主可以生成，而且可以定义有效期和适用条件以及范围；
- 2.DID的地址解析（非必须）：用来完成DID到用户IP地址的映射（只有边缘节点的设计需要）；
- 3.DID的地址映射（非必须）：因为DID经常由非常长的公钥字符串代表，非常用户不友好，因此一般需要提供用户友好的DID地址到公钥的映射。

六、DID的行业公司

为了技术讨论的完整性，这部分不仅仅讨论DID技术公司，还讨论了整个DID产业链中的项目。

目前 DID 赛道的产品功能较为分散。未来是像 Unipass 那样朝 Web3 的入口方向发展，与钱包所融合？还是作为承上启下的枢纽，提供对使用者认证、信用评分等服务以方便上层应用运行？还是通过短期内与 Web2 平台所融合，与 Web2 共存的方式来强化可靠性和有效性？

DID行业的相关公司可以形成DeFi一样的乐高组合。比如，project galaxy通过收集各个协议或者dapp对应各个地址的使用行为形成的凭证（VC，因为区块链数据的透明性和开源，这些VC可以由dapp生成和验证或者由Galaxy主动收集生成），这些围绕单个地址收集的VCs构成了这个地址的DID和其attributes，在Galaxy中称为Galaxy ID。

1. 标准协议

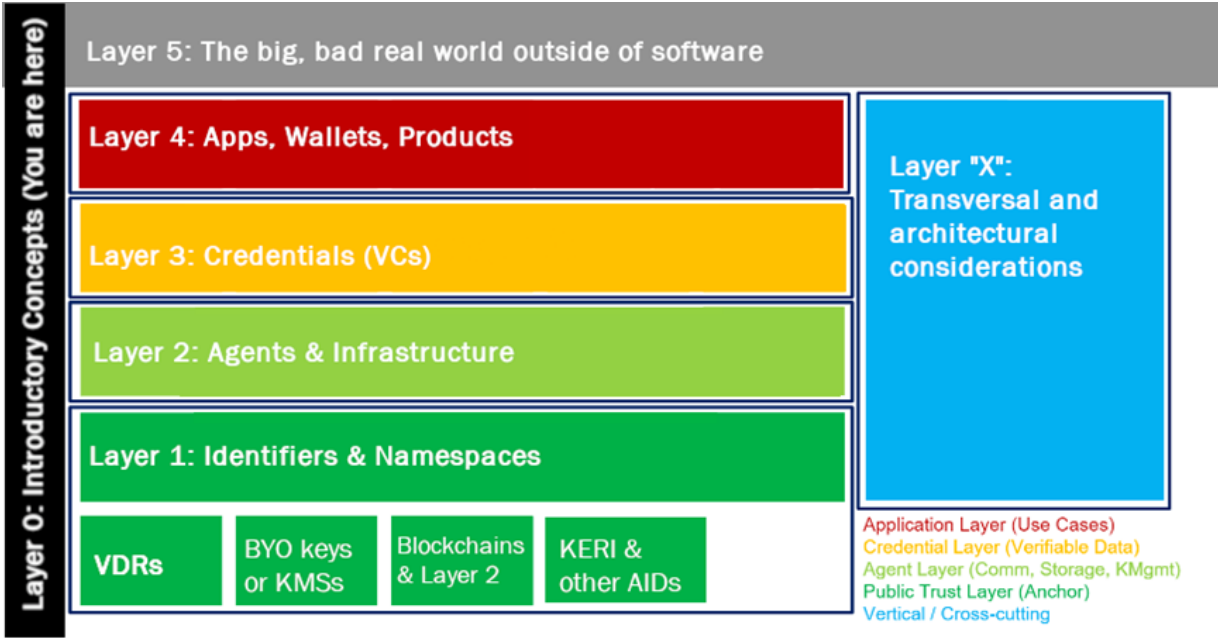
1.1 W3C

由WWW的设计师Tim-Bern Lee发起，并且于2022年7月19号成为规范建议。这是如今最为权威的DID设计规范，上述的设计讨论都是关于这个规划。

1.2 DIF (Decentralized Identity Foundation)

由web2.0时代的KOL Identity Woman Kaliya建立，成员包括微软和block等企业，这是一个推广DID的组织，并没有颁发任何标志。DIF认为的DID框架如下：





1.3 ID2020

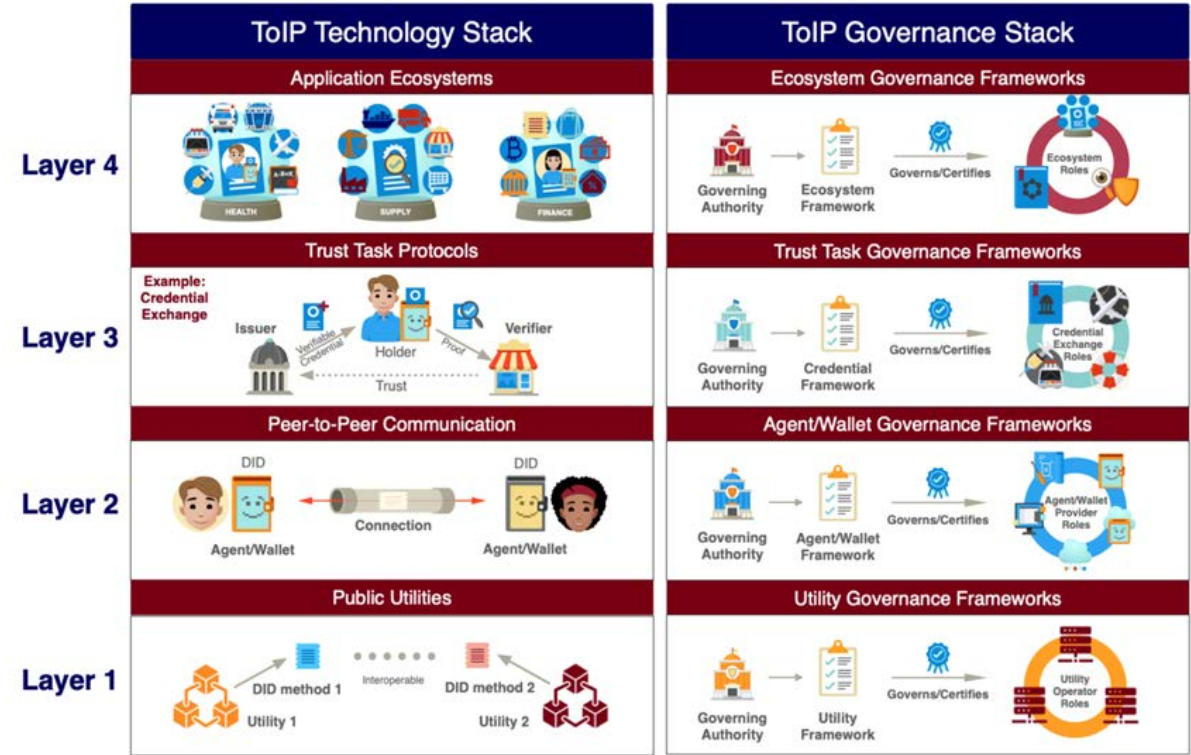
成立于2016年，宣传数字身份的机构，成员包括微软，没有发布任何技术规范或者协议。

1.4 IETF

作为互联网的主要技术组织，在DID方面的参与主要在于结合DID和DNS。

1.5 Trust over IP Foundation

由Linux基金会支持的有300多个机构参与的非盈利组织，集中探讨如何在互联网上促进信任关系的建立，DID作为核心基础技术如何支撑在网上建立信任关系，致力于为互联网开发一套类TCP一样的技术框架。



2. 基础设施公司

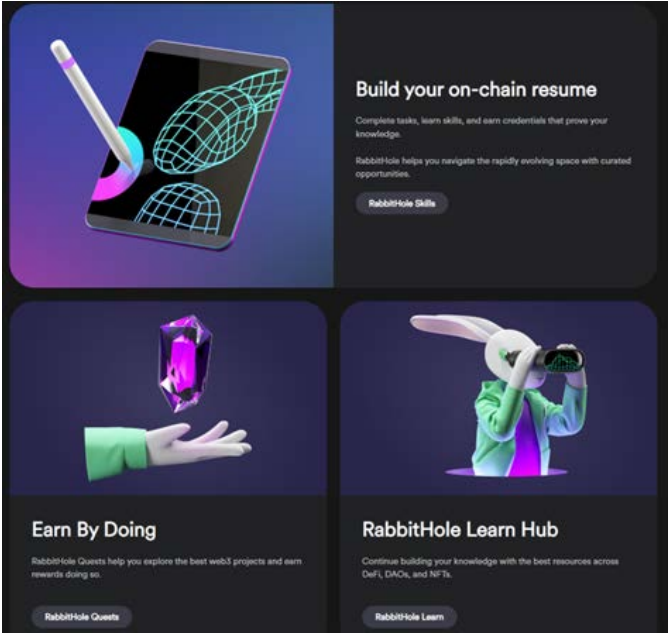
2.1 Ceramics

当我们讨论DID的时候，紧密关联的是如何存储ID控制的数据。

Ceramic 是一个基于 IPFS 构建的去中心化的、可跨链的、能管理动态内容数据的数据库服务。在可变性、版本控制、访问控制和可编程逻辑等层面弥补了 IPFS 的一些短板。在 Ceramic 上，每条信息都被表示为一个只附加的 (append-only) 提交日志，称为流 (stream)。每个流 (stream) 都是一个存储在 IPLD 中的有向无环图 (DAG)，有一个不可改变的名称，称为 StreamID，和一个可验证的状态，称为 StreamState。一个流 (stream) 在概念上类似于 Git 树，每个流 (stream) 可以被认为它是自己的区块链、分类帐或事件日志。Tile Documents 是 Ceramic StreamType 的一种，经常被用作身份元数据（如档案、社交图、链接的社交账户）、用户生成的内容（如博客文章、社交媒体）、DID 文件、可验证的凭证等的数据库替代物。



该协议并不依赖任何特定的区块链。相反，它可以被概念化为一个“文档链”，其中验证一个特定文档的状态只需要用户同步给定文档的数据。用户不需要像大多数区块链网络（如比特币、以太坊）通常做的那样来同步整个网络的状态。因此，不存在全局性的文件分类账。DID 用于登录 Ceramic 应用程序。每个事务或对数据流的更新都由用户（帐户）的 DID 进行身份验证。在 DID 之上，Ceramic 开发了 IDX 标准，用以聚合多种跨链数据类型关联到 DID 相关的用户数据。Ceramic 的关键工具之一是 IDX，这是一个跨链身份协议，提供了一个统一的存储库，所有的应用程序都可以注册并发现与用户的 DID 相关的数据源。它可以被认为是一个去中心化的用户表。因此，IDX 允许用户控制他们的身份和数据，而不锁定任何单一的应用程序，并轻松地保护和移植他们的跨应用程序的数据。同时，它允许开发人员建立数据丰富的应用程序，而不强迫用户在每个应用程序上重新创建相同的数据。



Ceramic 是 DID 技术栈（stack）中的一个重要的中间件。一些建立在 Ceramic 网络之上的项目包括：

**Boardroom**：一个 DAO 的治理管理平台，使用 Ceramic 的平台来存储提案评论。

**RabbitHole**：鼓励人们使用 Web3 项目的应用程序，允许他们获得积分和加密货币。RabbitHole 使用 Ceramic 的网络将多个 Web2 和 Web3 账户连接成一个统一的、跨链的 DID，并允许用户的声誉跨越其他 Web3 应用程序。

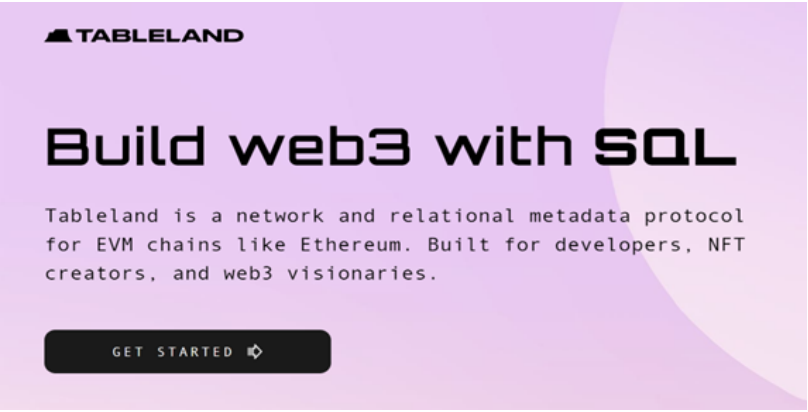
2.2 Lit Protocol



支持定义去中心化的权限控制政策，DAPP和DAO可以根据用户的DID授权用户的行为范围。在LIT SDK的支持下，dapp可以将用户的数据加密后存储

到Filecoin, Airwaves, Ceramic, Tableland, 如果其他用户希望访问这些数据, 数据拥有者会收到消息进行授权或者拒绝, 得到授权的用户可以访问和解密这些数据。

2.3 Tableland

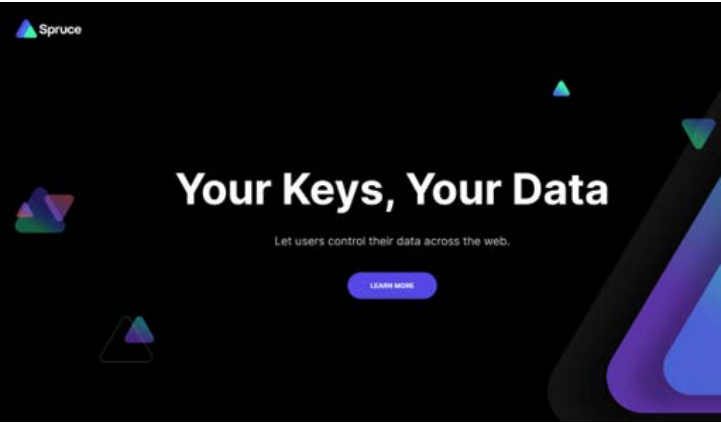


通过将NFT的数据存储在支持SQL的去中心化的链下存储, 而链上数据控制对线下存储的访问控制以及NFT的元数据。现在支持以太以及其二层网络和Polygon网络。

3. DID协议公司

3.1 Spruce Spruce

是一个数字身份认证系统, Spruce于2021年11月完成750万美元融资, Ethereum Ventures和Electric Capital领投。2022年4月20日, 其完成3400万美元A轮融资, a16z领投, Ethereum Ventures、Electric Capital、Y Combinator、Protocol Labs 等参投。



主要产品包括:

DIDKit, 按照DID协议开发的一个跨平台的DID开发包;

login.xyz (Sign-In with Ethereum, SIWE) , 允许用户用以太坊地址登陆;

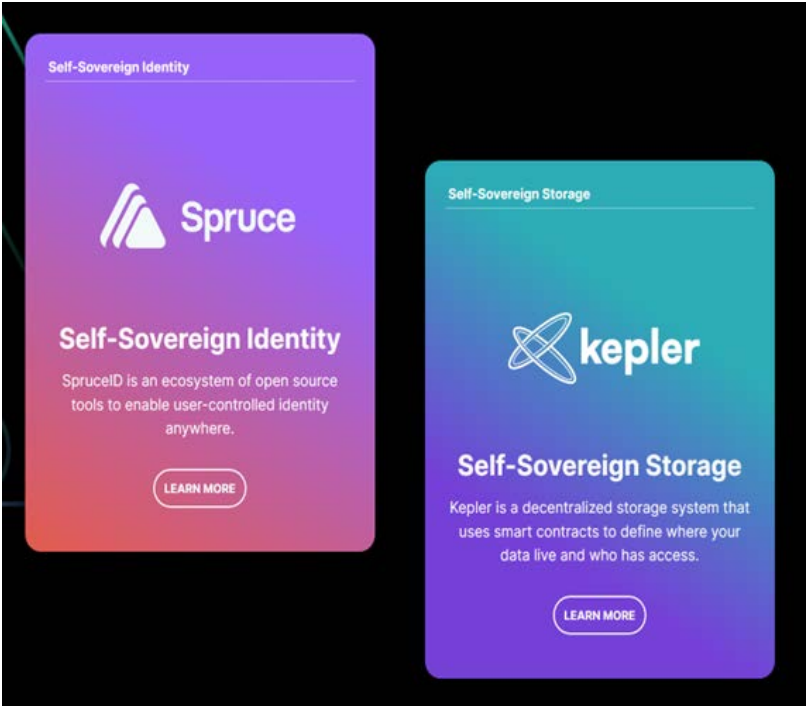
Kepler, 一个去中心化的存储方案;

rebase, 用来将id映射到公钥, 可以以去中心化、安全和公正的方式访问DeFi 应用程序。

Credible, 基于DIDKit开发的例子移动钱包, 支持w3的DID和VC标准;

Spruce与以太坊基金会、ENS合作构建了身份验证标准化系统 Sign-In with Ethereum (EIP-4361), 支持用户直接使用他们的加密钱包与web2或web3应用程序连接, 并控制其身份数据;

Keylink, 将现有系统帐户链接到加密密钥对。这是一个正在开发中的工具。帐户的身份验证使用广泛采用的协议组合, 如 OpenID connection 和 FIDO2。密钥的范围涵盖从加密密钥到 API 凭据。

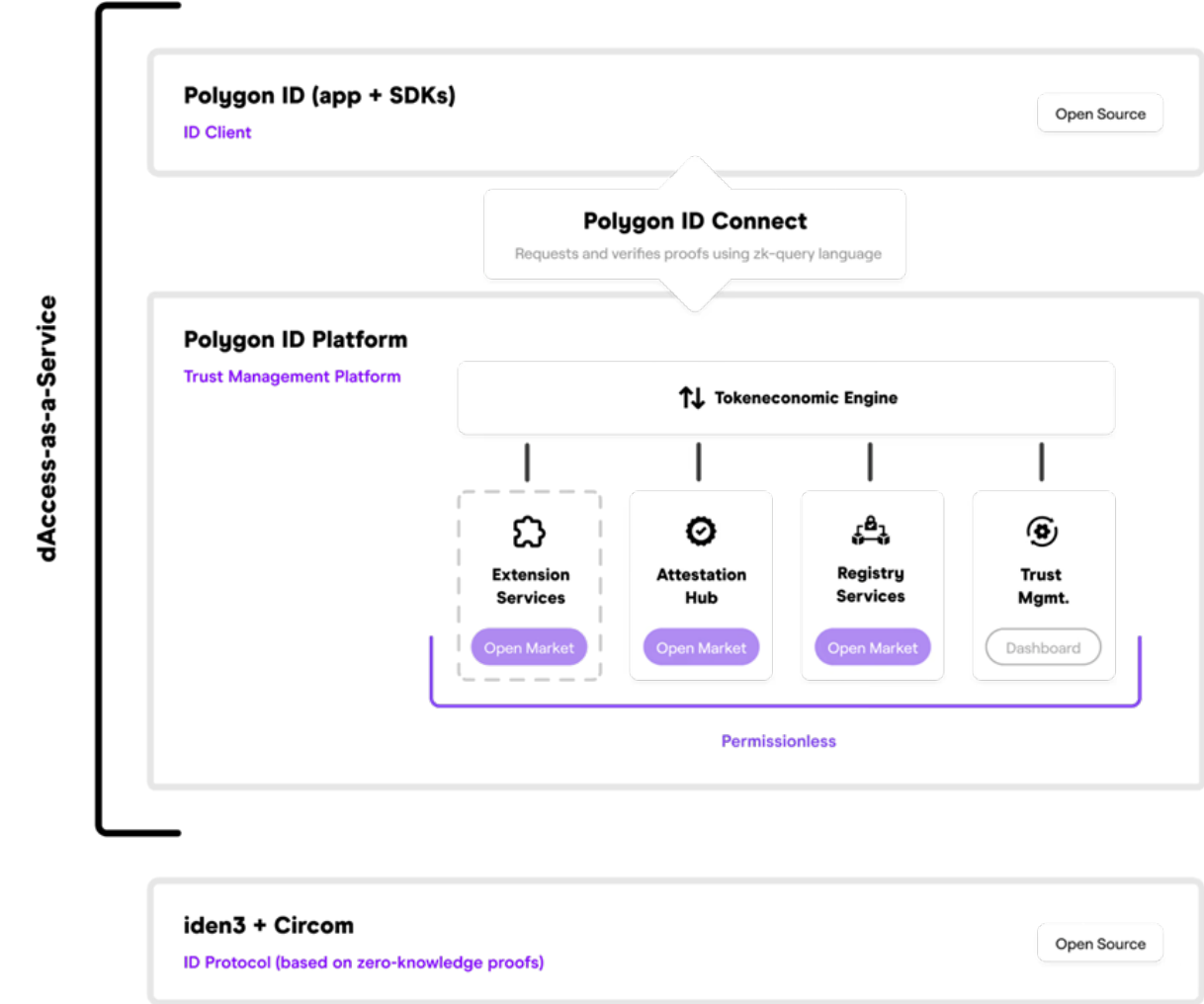


SpruceID 和 Kepler 是 Spruce 公司的两大护城河，为数字认证提供了一套闭环逻辑体系。此外，Spruce 不会做测试网，直接在以太坊主网发布。在营收方面，项目方明确提出不会发行 Token，虽然官方并没有明说，但收入有可能会来源于服务商给予的服务费用。Spruce 目前已经支持的链有Ethereum、Polygon、Tezos和Solana，合作项目包括Ceramic和Celo。

在公司层面，Spruce 能帮助公司实现用户增长。以在 3 月 Spruce 和 Auth0 身份管理平台达成的合作为例，使用 Web3 钱包作为身份来源，Spruce 扩展了Auth0 平台。

3.2 Polygon ID

基于IDEN协议由Polygon开发，服务polygon网络的应用，应用零知识证明来保护用户的隐私，促进建立网上的信用关系。



3.3 IDEN3

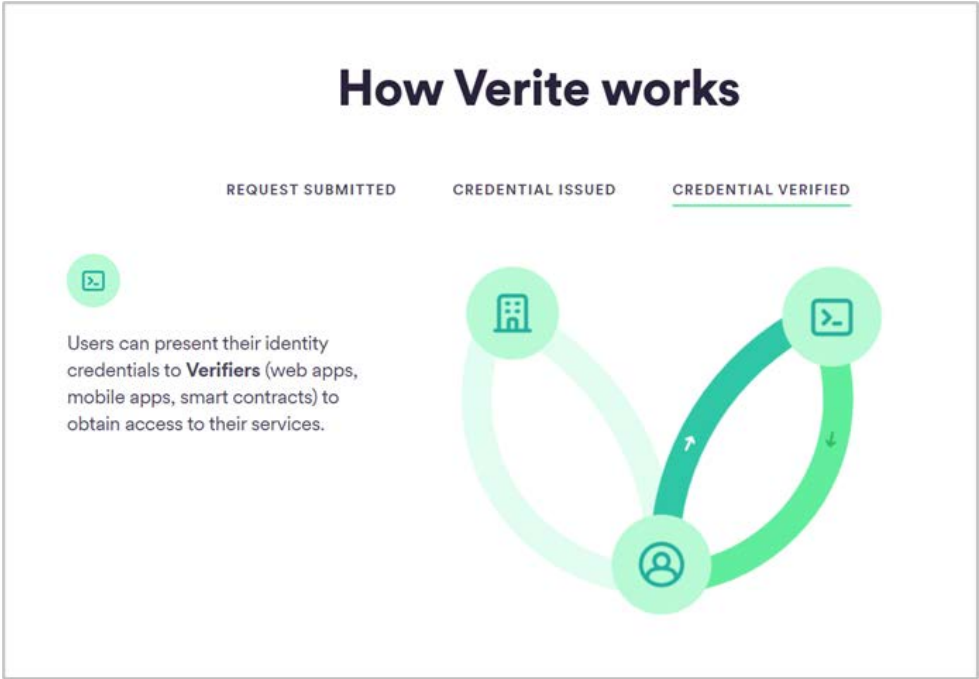




在以太坊运行的基于零知识证明开发的访问权限限制框架，主要特点包括：

- 通过zkProof生成和验证；
- 定义了proof-query语言；
- 支持多种DID协议；
- 支持P2P之间的通讯；
- 支持claim的管理；
- 去中心化的naming服务；
- 支持key rotation和recovery；

3.4 Verite Verite



是由USDC发行方Circle联合Block、Coinbase和Centre等公司推出的去中心化身份标准，旨在使任何组织能够发布和验证参与加密经济的用户和机构所具有的数字身份凭证，包括 KYC 验证、认可的投资者身份、社会声誉、NFT 出处跟踪等，而无需参与者披露个人数据，具有可组合和可互操作。同时，这些凭证是可移植的、不可破坏的，并且可以像数字资产一样被存储在加密钱包中。同时，凭证归用户所有，允许完全控制不同组织或协议访问身份证明的时间和方式。作为一组开源协议，Verite是去中心化的，没有一个实体拥有使用或开发的权限。

该身份框架将使机构能够参与链上借贷协议，并确保所有交易对手都经过 KYC，使机构能够安全地访问DeFi，例如支持根据认可的投资者身份或任何指定属性访问许可池或证券交易，能够为缺乏传统身份识别形式的个人和实体提供参与 DeFi 的机会，帮助创建更具全球包容性的金融体系，并通过信用评分凭证提高资本效率的潜力，可以更精确地匹配借款人的声誉，从而降低抵押品要求。

该项目的其它生态合作方包括 Algorand、Compound Labs、ConsenSys、Hedera Hashgraph、Phantom Technologies、Solana Foundation 等。

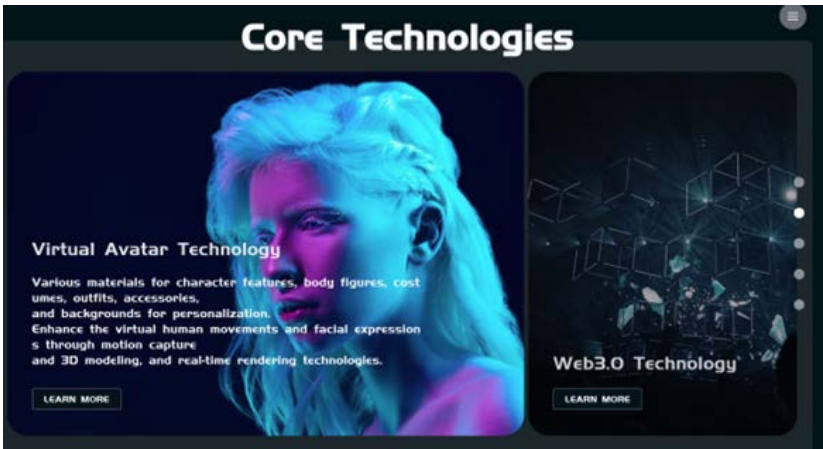
3.5 Sovrin



成立于2016年美国的犹他州，Sovrin运行一个联盟区块链，需要被允许才能参与运行验证节点，用户通过手机app（agent）控制自己的身份，并且与Sovrin链以及其他的agent进行交互。

4. VC公司

4.1 lifeForm



币安投资孵化的DID可视化身份管理软件，成立于2021年，提供了avatar创作软件，用户可以自由生成自己的3D形象，结合DID的SDK来驱动元宇宙合作伙伴的用户身份。

4.2 Disco.xyz



用Ceramic存储用户的VC的管理软件，现在只支持以太坊，用户可以为自己或者其他用户生成VC，可以链接自己的Twitter，Discord，域名到自己的profile。

4.3 proof of humanity

Digital Government IDs

✓ Pros

Simple and easy to scale.

✗ Cons

Vulnerable to rogue nation states duplicating or censoring identities.

Reverse Turing Tests

✓ Pros

Decentralized and still fairly simple.

✗ Cons

Requires all users to meet at the same time and is vulnerable to AI.

Social Graph Analysis

✓ Pros

Decentralized and easy to scale.

✗ Cons

Very complex and vulnerable to advances in AI.

Proof Of Humanity

✓ Pros

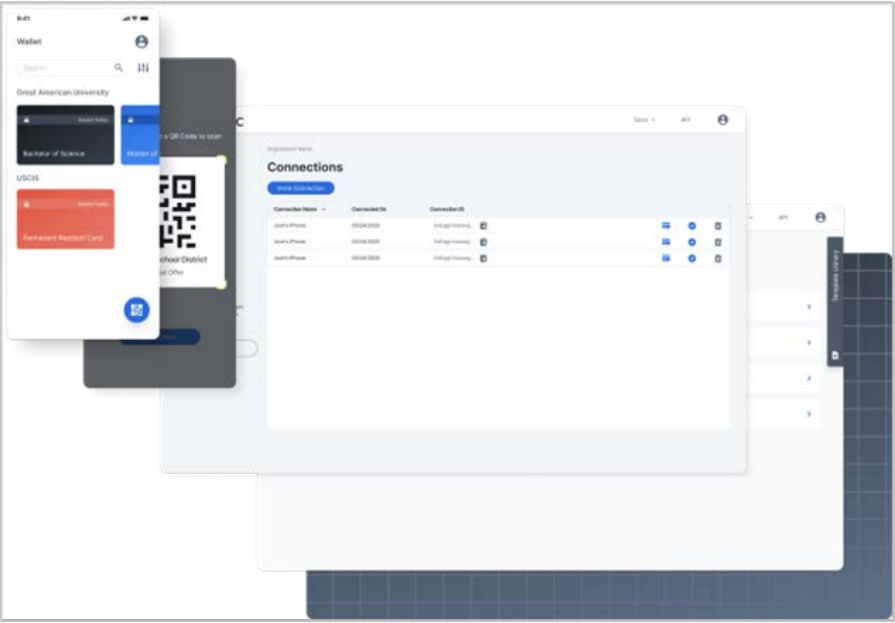
Decentralized, AI-resistant, and economically incentivized.

✗ Cons

More complex.

利用web-of-trust和Inverse-Turing-Test来验证DID是否绑定的subject是真人，来抵抗Sybil攻击，并且可以认领UBI代币。

4.4 Trinsic




一个支持SSI的技术全栈解决方案，按照SaaS计费提供免费和付费软件服务。包括钱包SDK，工具软件，和专家顾问支持。支持VC的存储和验证，数据共享，VC登陆。

4.5 Quadrata

# Quadrata Offerings

## SYBIL RESISTANT DID


UNIQUE IDENTIFICATION



Prevent unfair advantage with unique identification

## COMPLIANCE INFRASTRUCTURE


REALTIME MONITORING



All-in-one Web3 KYC/AML plugin with ongoing monitoring

## SEAMLESS USER ONBOARDING

WEB UI & SOLIDITY SDK



Swift passport creation with just few lines of code

产品为Quadrata Passport，为元宇宙提供防Sybil攻击的基于链上KYC的DID解决方案，支持以太坊和Polygon，包括用户passport的AML风险分和位于哪个国家。用户的passport由发行者负责验证和颁发，现在的发现者有SpringLabs。另外，它是TrueFi的合作伙伴。由Dragonfly投资。


4.6 BrightID

# Proof of Uniqueness

Get Started


## Identity is a human right.

BrightID is a social identity network that allows you to prove that you're only using one account. It's the holy grail of digital identity.




### Non-Invasive

BrightID requires no personal information. It lets you prove your humanness without risking your privacy.



### Accessible

Access to identity is a human right. BrightID is designed so that everyone can use it.



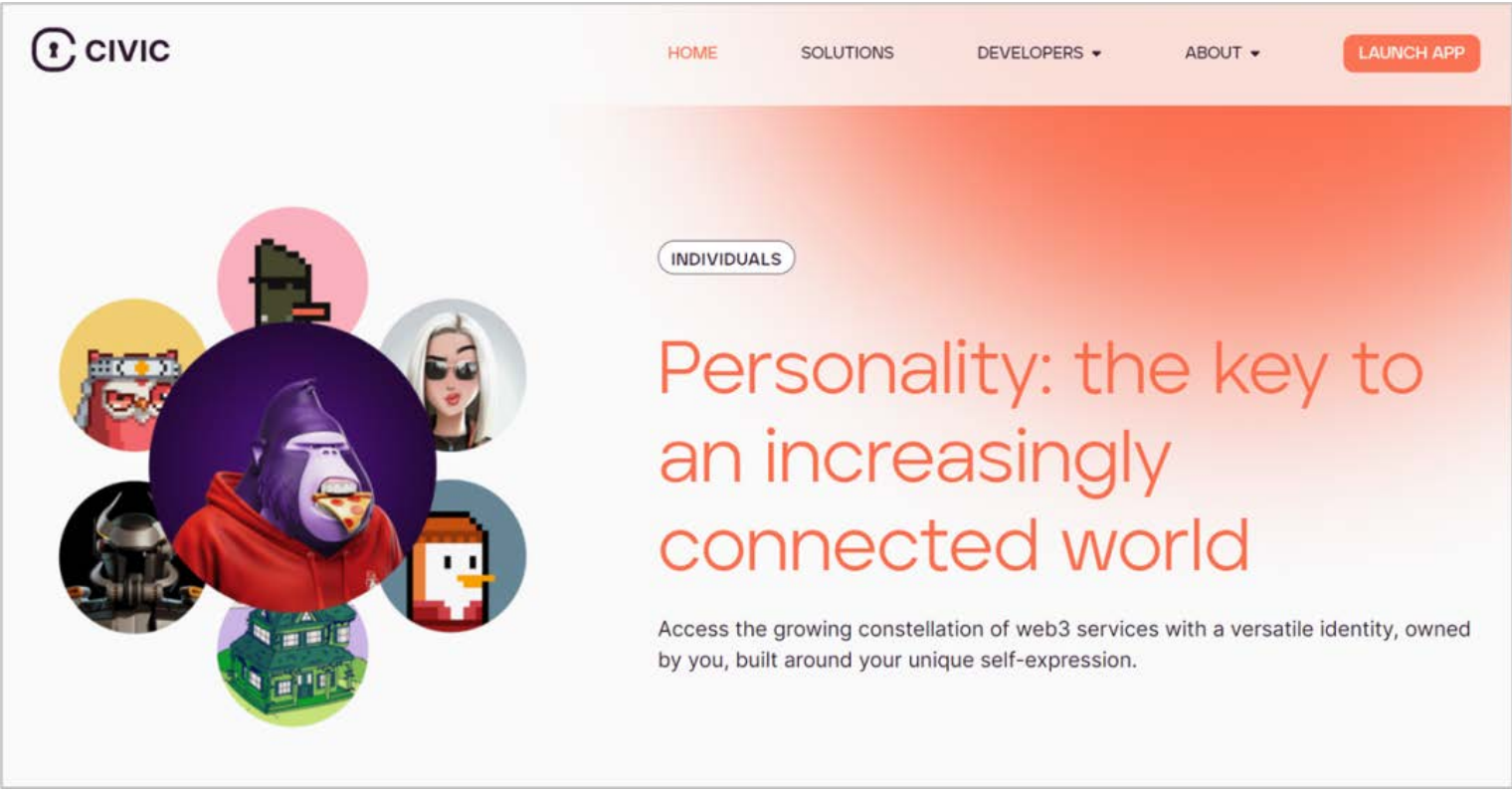
### Open Source

Everything is transparent, free, and open-source because identity is a public good.

一个通过与项目方进行视频会议验证用户真人身份的项目。由于得到了vitalik和Gitcoin的支持因此获得了大量的用户。

4.7 Civic

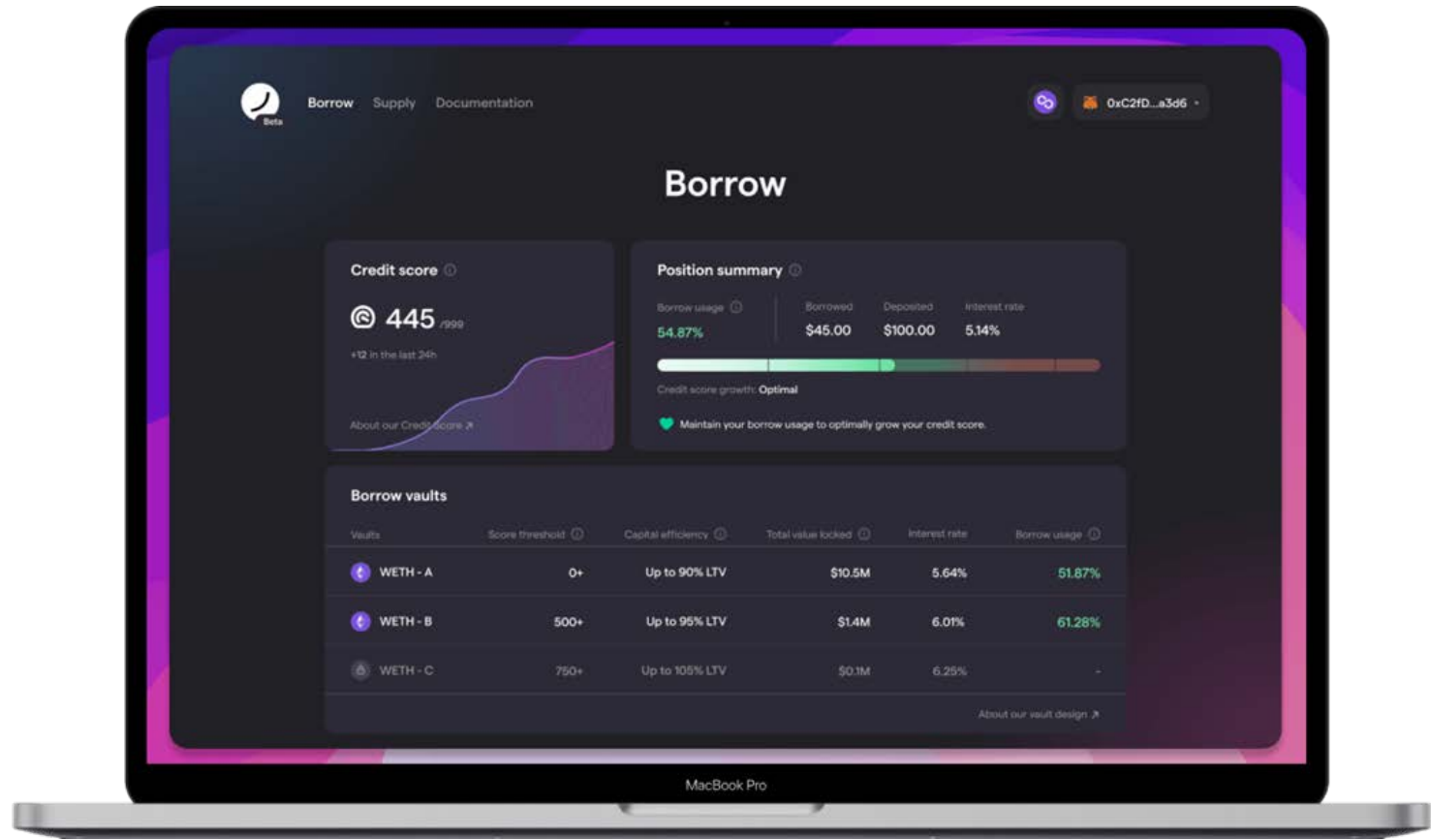




通过人工验证护照，身份证，驾照，居住证等证件来验证真人，服从OFAC的规定。支持多链，集合用户所有的NFT。

5. 应用公司

5.1 [ARCx](#)



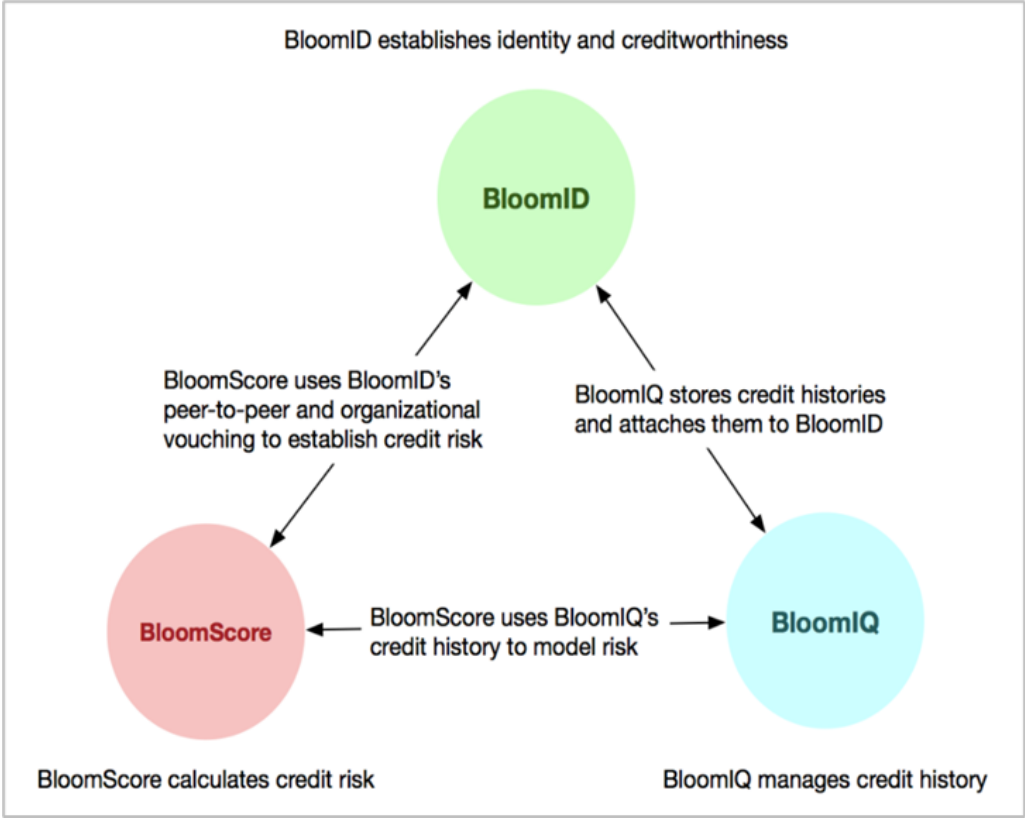
Arcx.money 目前免费向用户发放 DeFi Passport，并通过处理和参考大量数据为持有者建立信用积分。信用分将通过分析持有者的以太坊地址历史活动来确定，其范围设置为 0 到 999 分，该信用分确定了协议为用户提供的抵押率。在申领 Passport 后，用户会受到激励，通过在多个「游戏」中最大化自己的分数来提高自己的链上声誉，这样他们就可以获得各种好处，例如以更低的抵押率进行借贷。

5.2 Goldfinch



一个去中心化的贷款协议，允许放贷人给印度，墨西哥，尼日利亚，以及其他东南亚国家的线下用户贷款，这些用户可以支付10%以上的利息，并且和加密货币行情没有相关性。放贷人分为优先劣后级，由劣后人申请贷款人进行评估。该项目的投资人包括a16z，coinbase，以及一些有影响力的个人。

5.3 Bloom



2018年成立，基于以太坊和IPFS的去中心化的信用分项目（其信用分称为BloomScore），通过联盟网络验证用户的身份，通过credit staking机制互相背书建立信任网络。Bloom不仅仅服务加密行业还与传统信用行业竞争服务传统行业，相对于传统信用公司包括FICO，Bloom的竞争优势包括针对现存信用行业存在的问题提出解决方案，包括用户的信用分无法跨境，信用的评估只通过历史数据，贷款人无法评估跨境申请人，贷款申请人的资料无法保护隐私，以及信用数据被垄断。

Bloom协议包括BloomID，BloomIQ（BloomID的借贷记录），BloomScore（信用分）。发了ERC20代币，BLT提供了消费者版，企业版，以及开发者版。对于消费者提供：和Transunion共同提供免费的信用分监控服务；免费的身份保护和报警服务。

5.4 Galaxy Galaxy

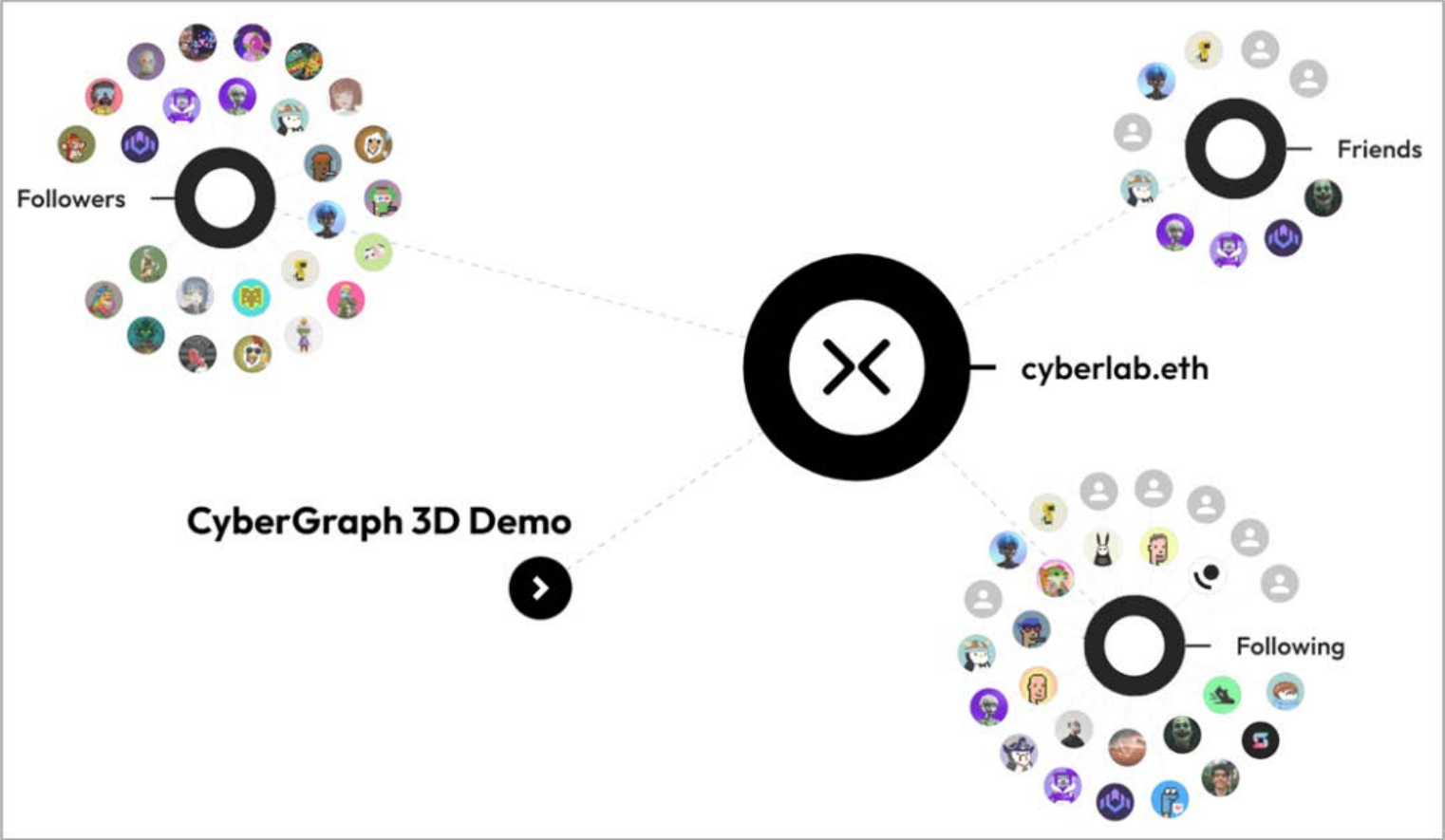


是一个proof of achievement，包含线上和线下的数据，线上的凭证自动生成的，例如：uniswap和opensea交易员，成为成为链上 LinkedIn。

Galaxy提供了开发包，项目方可通过 Project Galaxy 的 NFT 基础设施与链上凭证数据网络构建和分发 NFT 徽章，来对社区成员进行管理。官方称之为 Galaxy OAT（链上成就代币），这记录了用户的所有成就。这些用户行为数据形成的凭证大有用处，相当于自身的个人简历标记用户着曾获得的成就。对于普通用户来说，可以使他人可通过用户过去的成就更加了解自己。对于开发者来说，除了上文举例的评判信用进行发放贷款、公会凭借凭证招纳人才之外，还可奖励社区贡献者。以及根据用户的具体行为，对用户有一个基础判断，从而准确的定位到目标客户。所有 OAT NFT 的元数据都将存储在由 IPFS 和 Filecoin 提供支持的 NFT.Storage 上。官方表示迄今为止，已有 100 多个合作伙伴在 Project Galaxy 上发起了 500 多个活动。目前 Project Galaxy 有 3000 多个 credential 标签，完成了 3000 多个基于信用的活动。

Project Galaxy 前段时间宣布完成 1000 万 美元融资，其中有许多知名投资方，由 Multicoins Capital 和 Dragonfly Capital 领投。目前该项目支持 Ethereum、Polygon、Fantom、Solana、BNB Chain、Arbitrum 和 Avalanche 七条公链。

5.5 Cyberconnect



CyberConnect 是一个多链去中心化社交图谱协议，构建了一个可拓展的标准化社交图谱模块，通过搜索引擎，能搜到具体地址的 follower、POAP 和 Galaxy 凭证。其数据通过 Ceramic 存储在 IPFS 上，为 DApp 提供通用数据层。虽然社交图谱数据对所有人开放，但只有用户可以完全控制自己的社交图谱，即添加、删除和更新相关 dapp 链接。

5.6 Litentry



Litentry 是波卡生态的去中心化身份聚合器，支持跨多个网络链接用户身份。用户可以通过其提供的安全工具管理自己的身份，Dapp 可以获得跨不同区块链的身份所有者的实时 DID 数据。目前基于该项目的去中心化身份项目包括 My Crypto Profile、Web3Go、Polkadot Name System、PokaSignIn 等。

Litentry 建立了一个三层信用计算基础设施用以支持 DID 的管理：

源数据层。身份分析员获得数据的源平台，如 Etherscan、The Graph、Onfinality 和其他数据提供商。

地址分析层。主要是作为一个提供数据分析的外部服务器，如 Nansen, Chainalysis，以及即将推出的 Litentry whitelist 等地址分析平台。

身份聚合层。Litentry 生成属于同一身份的地址关系，然后从地址分析层获取相应的地址分析数据，并进行加权计算。

5.7 Unipass



# A SEEDLESS and GASLESS User Experience for Your Web3 Apps

Build Now Try POC



Unipass 是一个多链统一加密身份，即元宇宙通用护照，用户可以通过一个 Unpass ID 聚合多个社交（Web2）账号，给予用户评分、标签、展示用户的 NFT、支持基于电子邮件的社交身份恢复，以及支持基于 Token 的社群、zoom 会议、论坛访问。支持向特定 Token 持有者发送消息。提供基于电子邮件的非托管社交恢复钱包解决方案。可以通过无密钥的方式控制用户的加密身份。还可以通过加密方式验证多链地址甚至社交帐户。

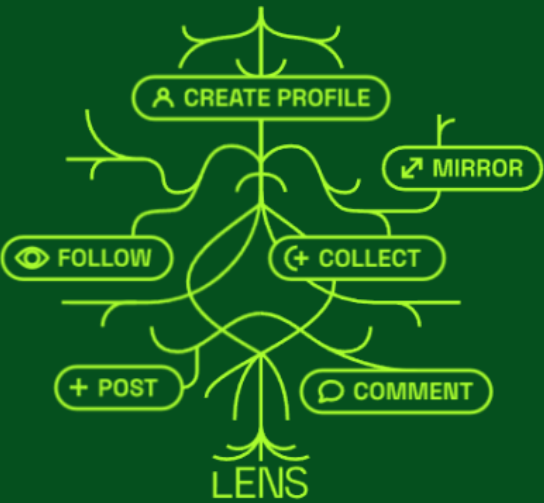
web3身份聚合：基于密码学实现多链多账户的聚合。通过这种聚合方式，可以将用户在不同链上不同地址的行为聚合到一个身份ID中，实现信任的传递。简单说就是可以最大程度提升用户的链上行为评分。

web2身份验证：在智能合约中提供验证电子邮件地址、Twitter 账户、Discord 账户的能力，从而在 Web3 中原生提供 Web2 身份信息。

单点登录与访问门户：通过使用unipass id，进行多应用的统一登录。并为用户提供统一的web3门户导航。

5.8 Lens协议

## EXPLORE THE ROOTS



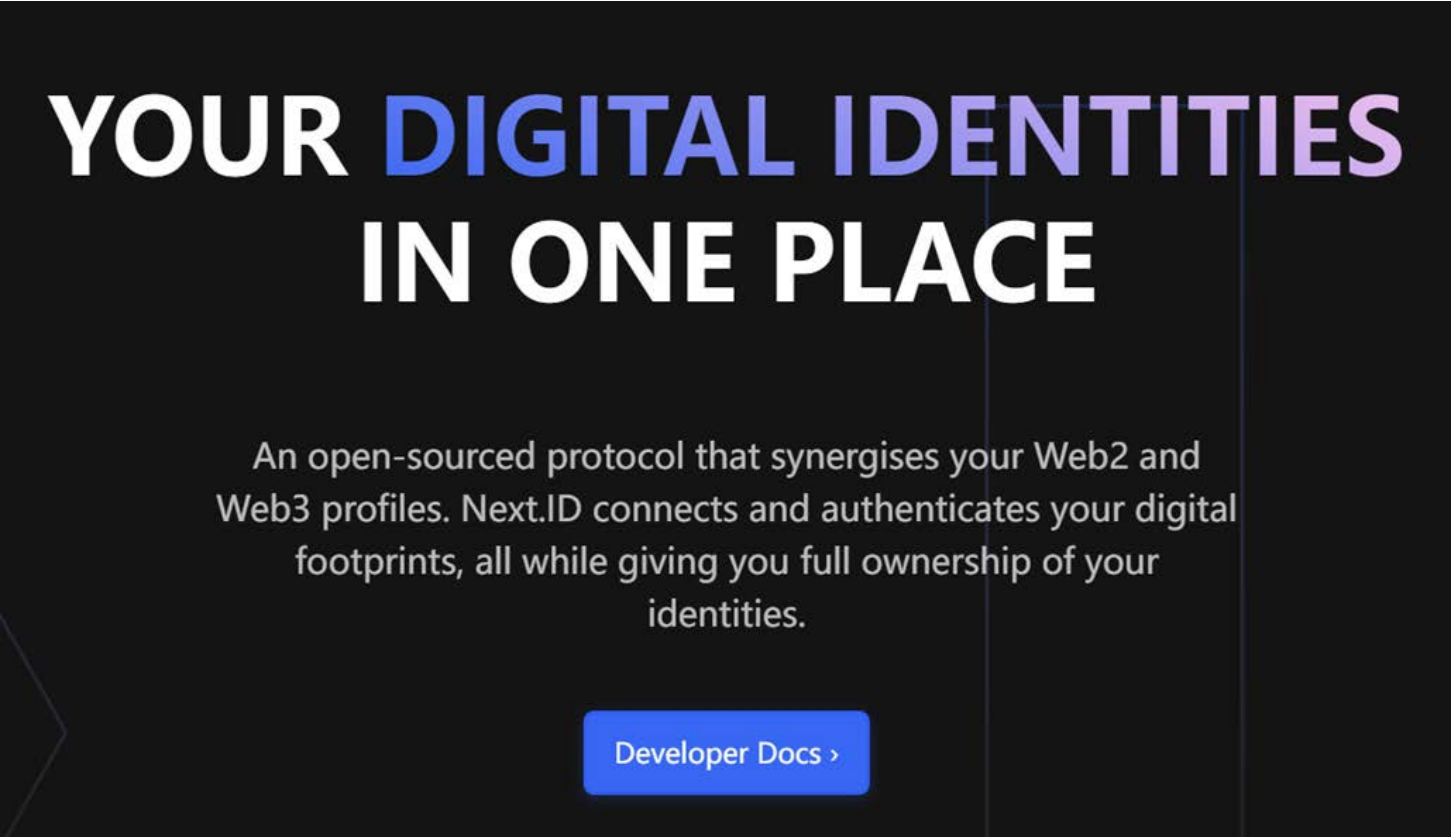
## DIG INTO THE KEY FUNCTIONS

Mint a profile, follow others, create and collect any publications, completely on-chain.

Lens Protocol 是 Aave 团队在 Polygon 上开发的可组合的去中心化社交图谱，具有一般的社交媒体功能，例如个人资料编辑、评论、转发帖子等。不同的

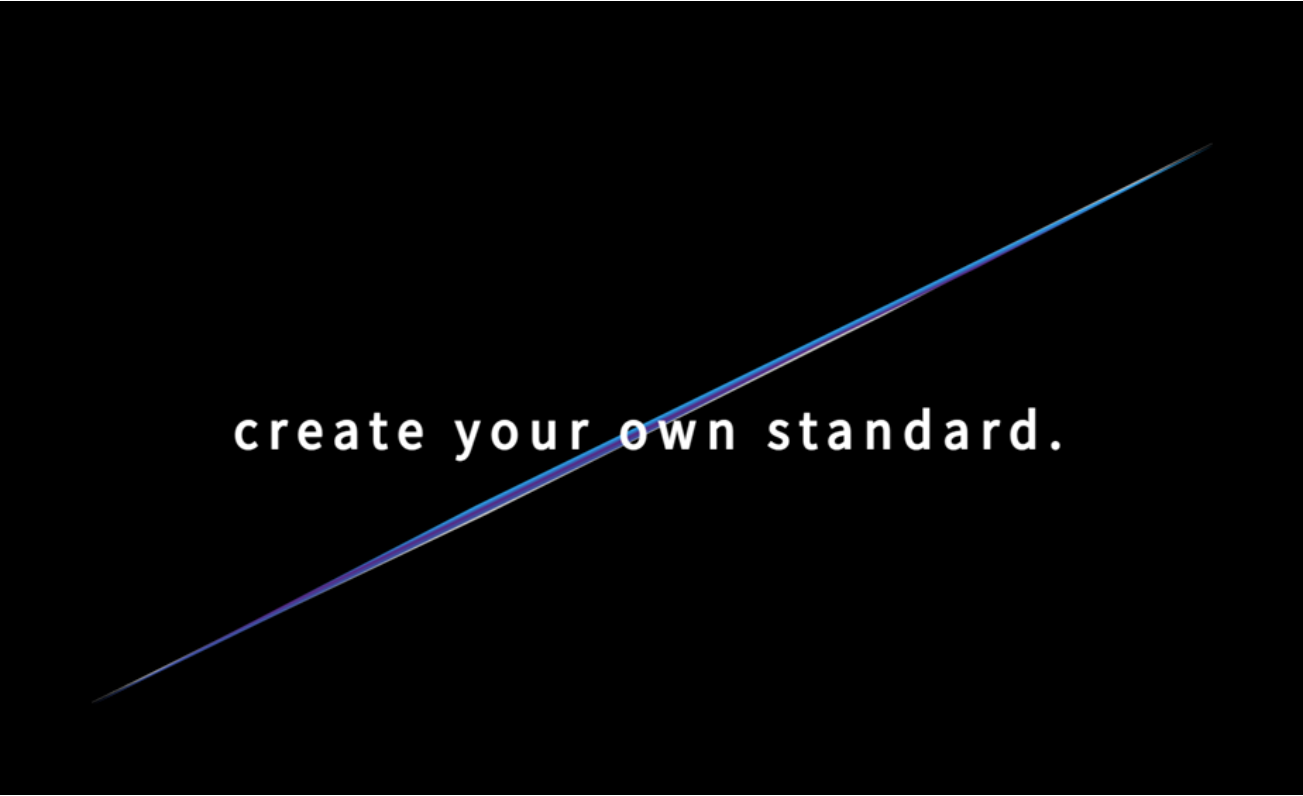
是，Lens Protocol 支持 NFT，用户拥有和控制其所创作的所有内容。用户通过 Profile NFTs（个人档案 NFT）查看自己历史足迹、发布的艺术内容，通过平台上关注他人获得 Follow NFT（跟随者 NFT）。该协议也允许开发者使用模块化组件在 Lens 上任意搭建自己的社交应用，鼓励开发者开发提升产品体验的新组件，外部其他应用也可以接入 Lens，并且共享 Lens 生态的优势。

5.9 Next.ID



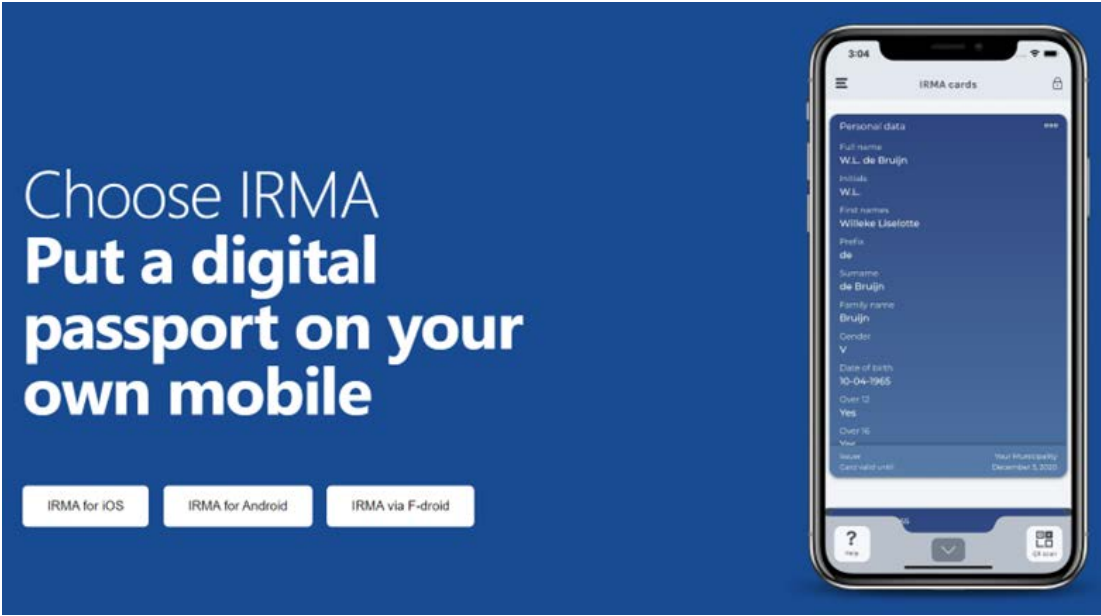
全球第一个Decentralized-Identity-As-A-Service (DIaaS)的协议，整合了Web2 and Web3数字身份为用户生成avatar，为dapp开发者创造便利。

5.10 aut.id



为DAO和web3社区提供基于DID角色的权限管理，产品包括Expansion（帮助开发者集成用户角色），dAut（DID验证），Dashboard（DAO管理模块）AutID（用户信息展示和NFT ID）。AutID只能通过参与社区获得而不能购买获得和转让。

5.11 IRMA.app



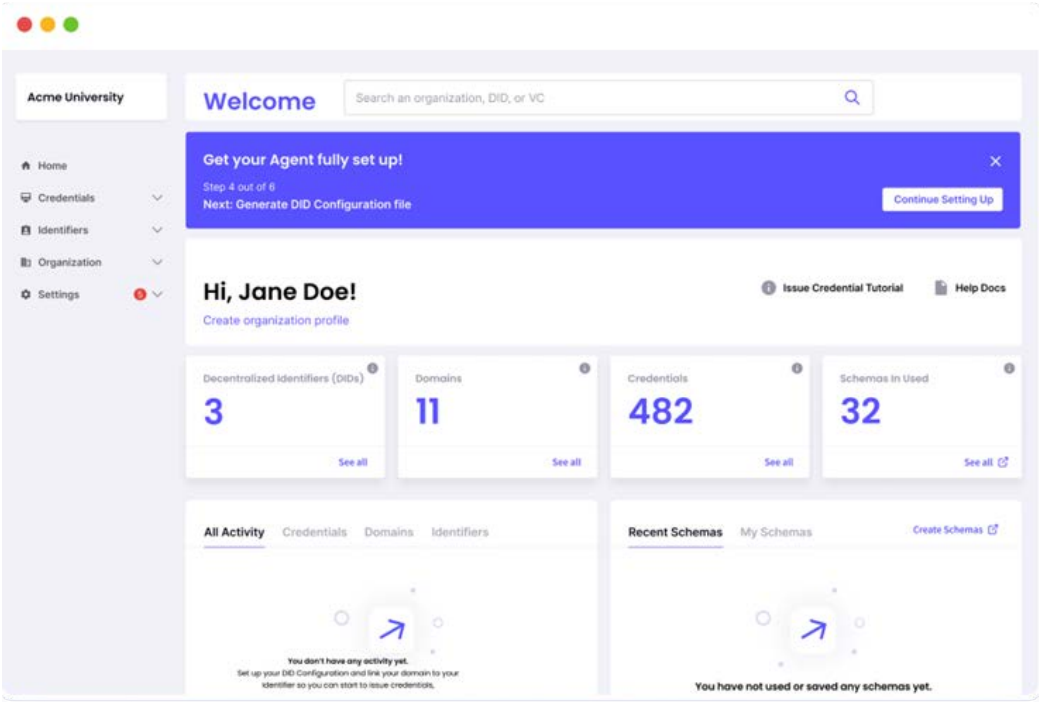
由荷兰Privacy by Design Foundation开发维护主要被荷兰网站使用的以用户为中心的身份管理app，用户可以在app自主生产身份信息，可以在支持IRMA网站通过二维码登陆。

5.12 Veramo



由早期的uPort分拆出来的DID技术框架，其产品围绕着agent（类钱包），支持ETH-DID，web-DID（DNS域名）和DID-key（公密钥），支持数据管理，密钥管理，connect登陆，产品形态包括API，SDK，命令行和移动端。

5.13 Serto



由早期的uPort分拆出来针对企业应用场景的DID解决方案。

5.14 ENS

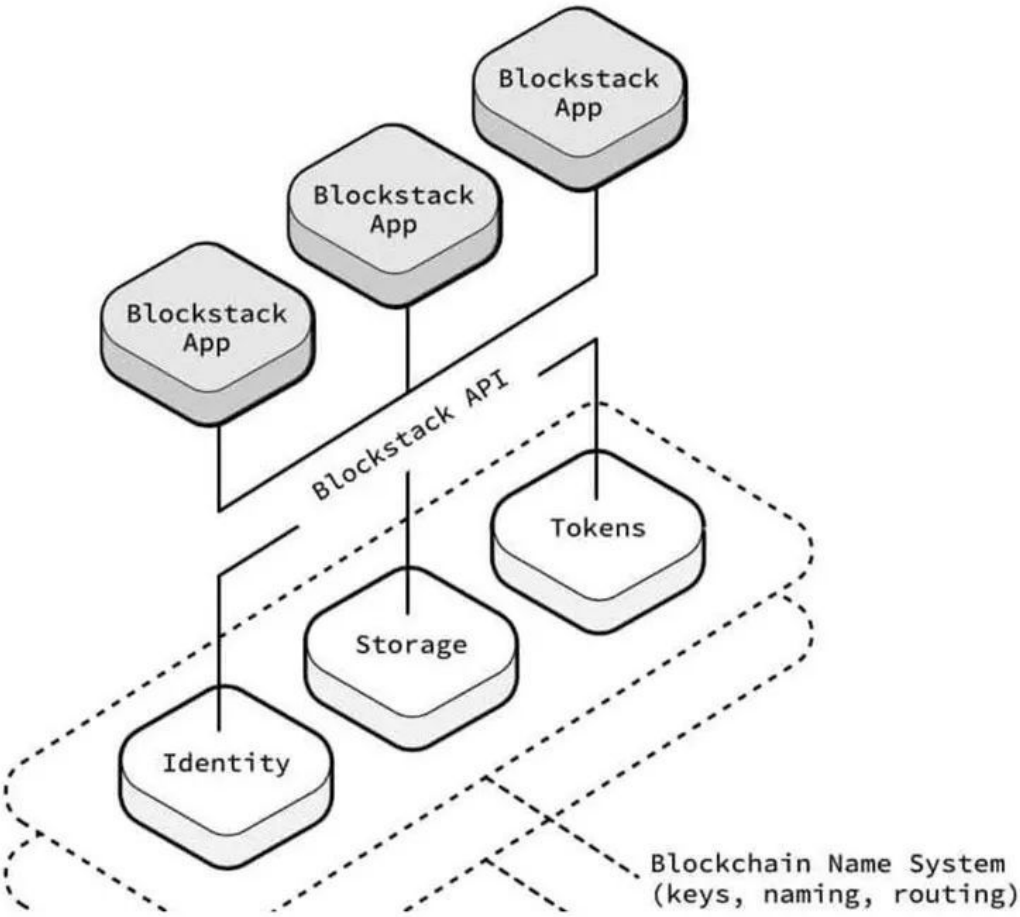


通过绑定以太坊钱包地址，为用户提供以太坊上的域名服务，用户可以链接Twitter，discord以及头像，配合IPFS可以建立完全去中心化的网站，最有影响力和潜力的DID方案。ENS的根由一个多签地址控制，

5.15 .bit

起源于Nervos网络的类ENS的方案。

5.16 blockchat



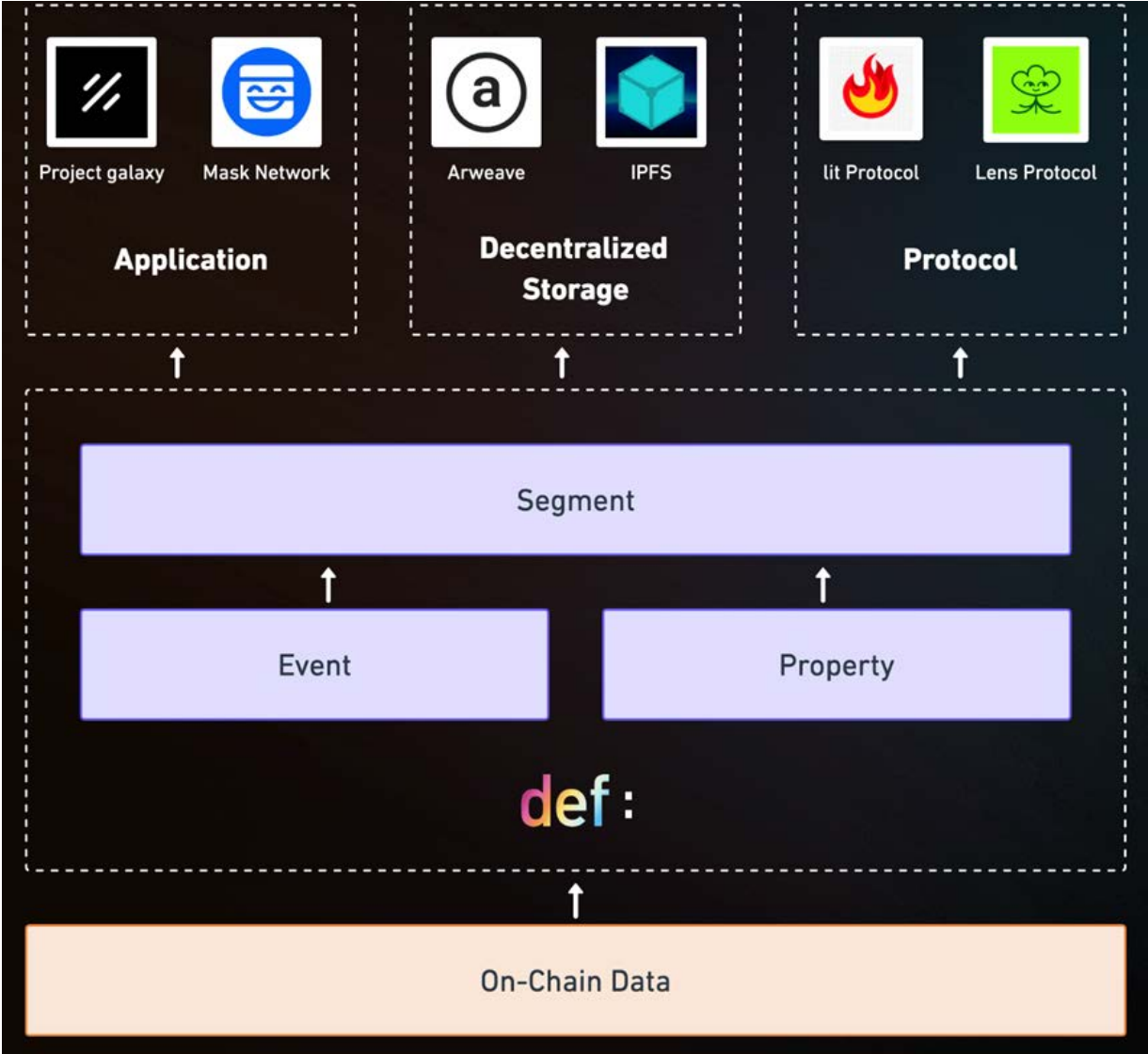
基于Blockstack开发的去中心化加密聊天软件，数据存储在用户控制的存储空间（由Blockstack支持），用区块链技术验证通讯录。未来将支持支付和类snapchat的功能。



5.17 bluesky

致力于提供去中心化社交的技术框架。

5.18 Def network

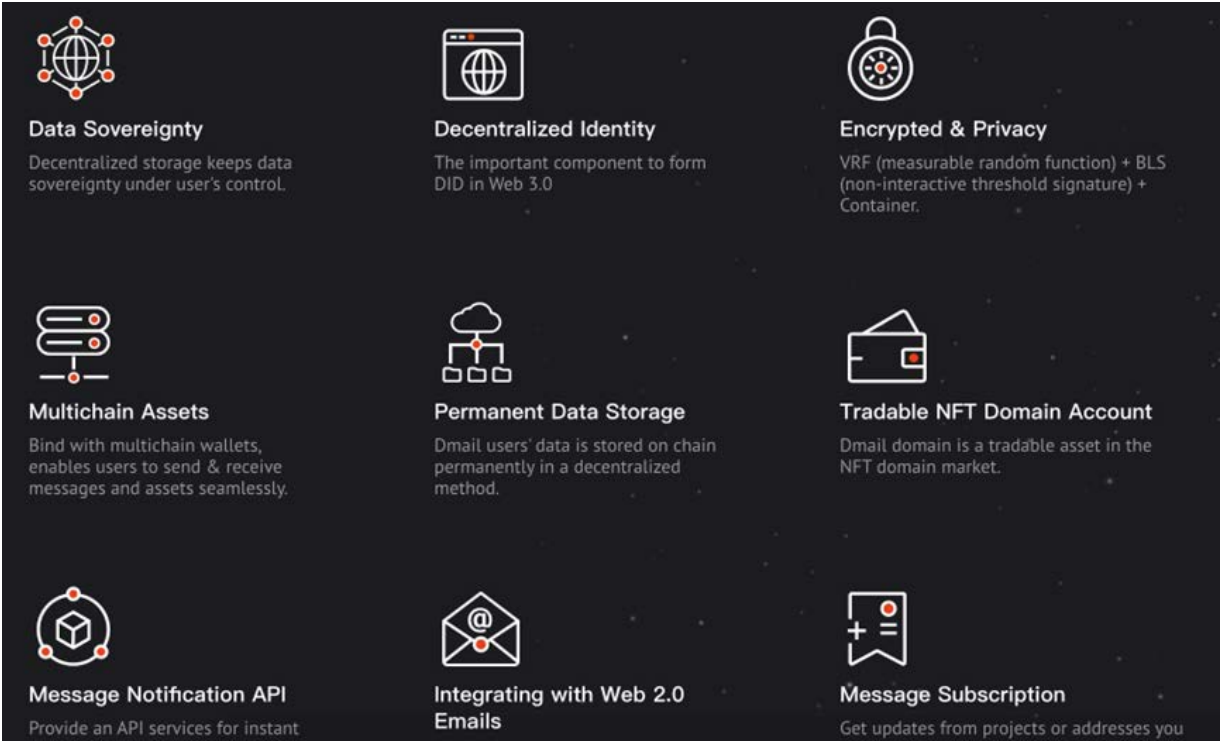


通过在线协作标记用户地址，收集分析地址的行为数据并且整理成开发者友好的数据格式，包括NFT鲸鱼， smart money。

5.19 DeGenScore

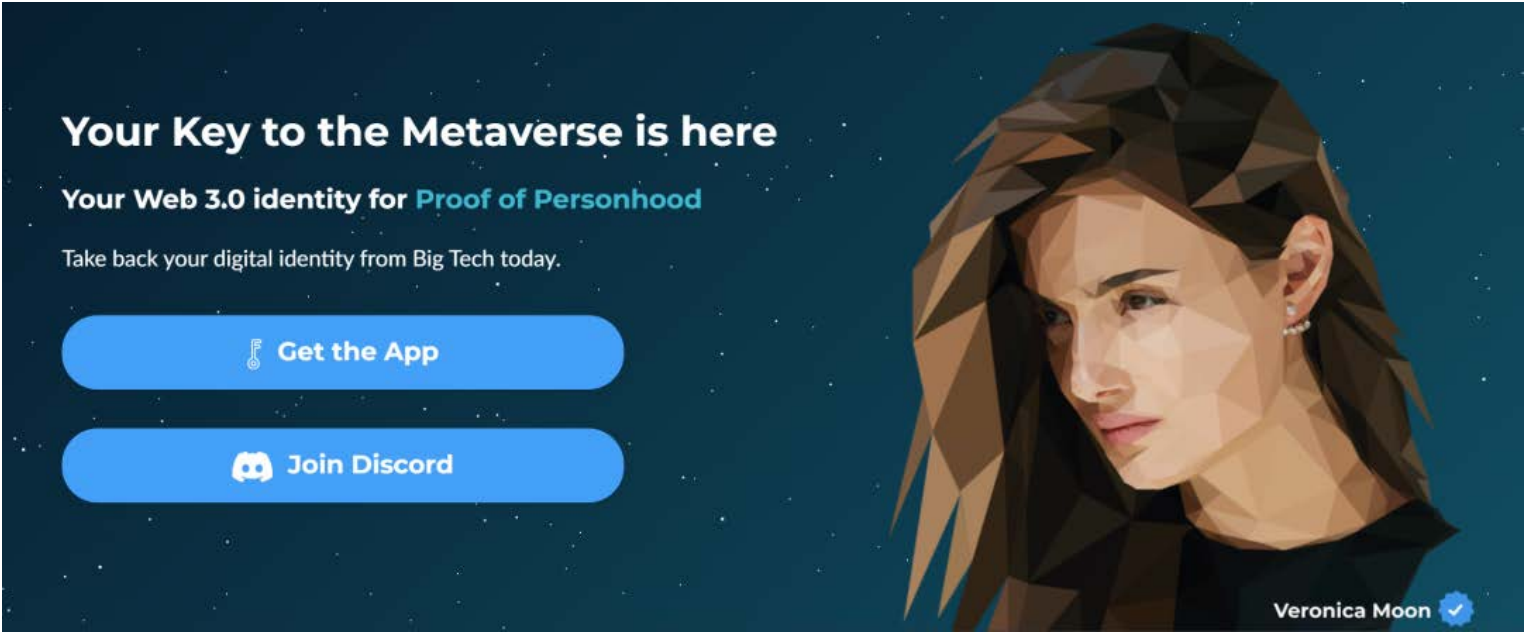
根据地址的行为数据计算出一个数值。

5.20 Dmail



基于Dfinity开发的web3.0的在线协作平台，包括消息通讯，资产管理，数据存储，以及在线协作平台。提供去中心化的邮箱以及个人存储空间。

5.21 SelfKey



成立于2017年，为代币发行提供KYC服务，产品为钱包，支持DID，发行了代币KEY，数据存储在用户本地，通过由律师，银行，会计师，公证员组成的验证网络验证用户身份。

5.22 boardroom

一个DAO的聚合网站，帮助用户查询，管理，投票，代理授权自己参与的DAO。

5.23 helix.id



## Your Digital Wallet

✔ Take back control

Your data, in your hands. You alone decide what happens with your personal data. helix id is made for you.

🔒 Cryptography makes it happen

New gen data protection. Your data is individually encrypted and protected by Blockchain technology.

★ More than just an app

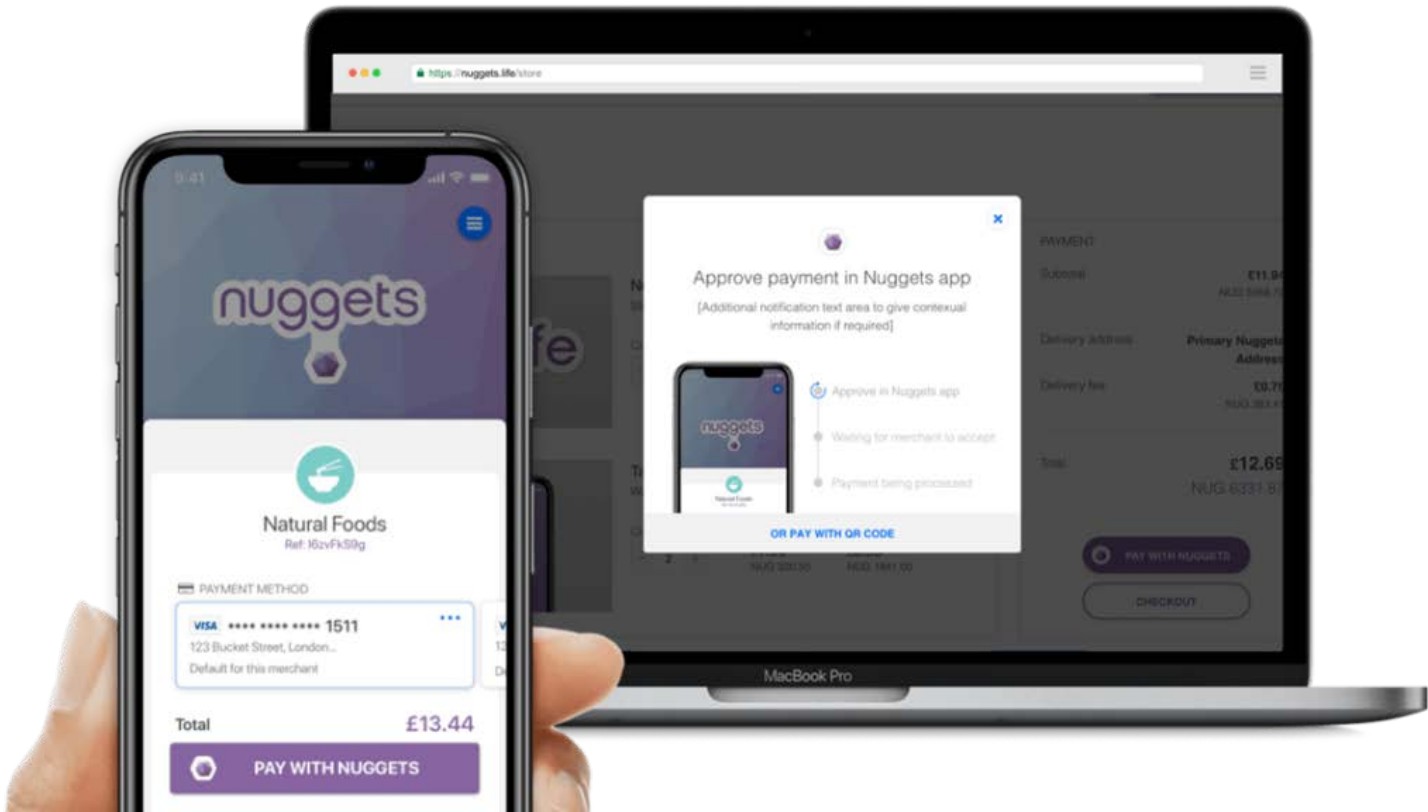
1-click registration and an integrated marketplace make your digital life simple.

📱 Always by your side

Your digital me in one app. Anytime available. Secure and only yours.

位于德国法拉克福的融合了web2和web3的身份和数据管理钱包软件。

5.24 nuggets.life



支持基于IPFS的个人数据云存储，支持银行级别的安全认证，w3c的DID和VC规范，ZKP，链上信誉分，基于2FA的支付，可授权可审计的数据使用权限管理。

5.25 tykn.tech

为网站开发者提供基于区块链的SSO登陆服务。

5.26 ION

基于比特币二层网络的Sidetree协议的身份网络，由DIF基金会开发，并且是Jack Dorcsey的web5的技术基础。

5.27 MintKudos

基于SBT开发的位于Polygon的Kudos代币。

5.28 SourceCred

根据算法为社区的成员的贡献度打分并且奖励token，像信誉分一样，Cred不能转让。

5.29 Coordinape

# Reinventing Compensation for Web3

DAO-native solution to contributor rewards, feedback, and all things people.

[Get Started](#)[Schedule a Walkthrough](#)

与SourceCred一样，根据算法为DAO成员的贡献提供打分和奖励，合作的项目方包括Bankless，PoolTogether。

5.30 Context

根据Twitter好友的钱包地址，推荐钱包地址和提供NFT的mint消息。

5.31 DeepDAO

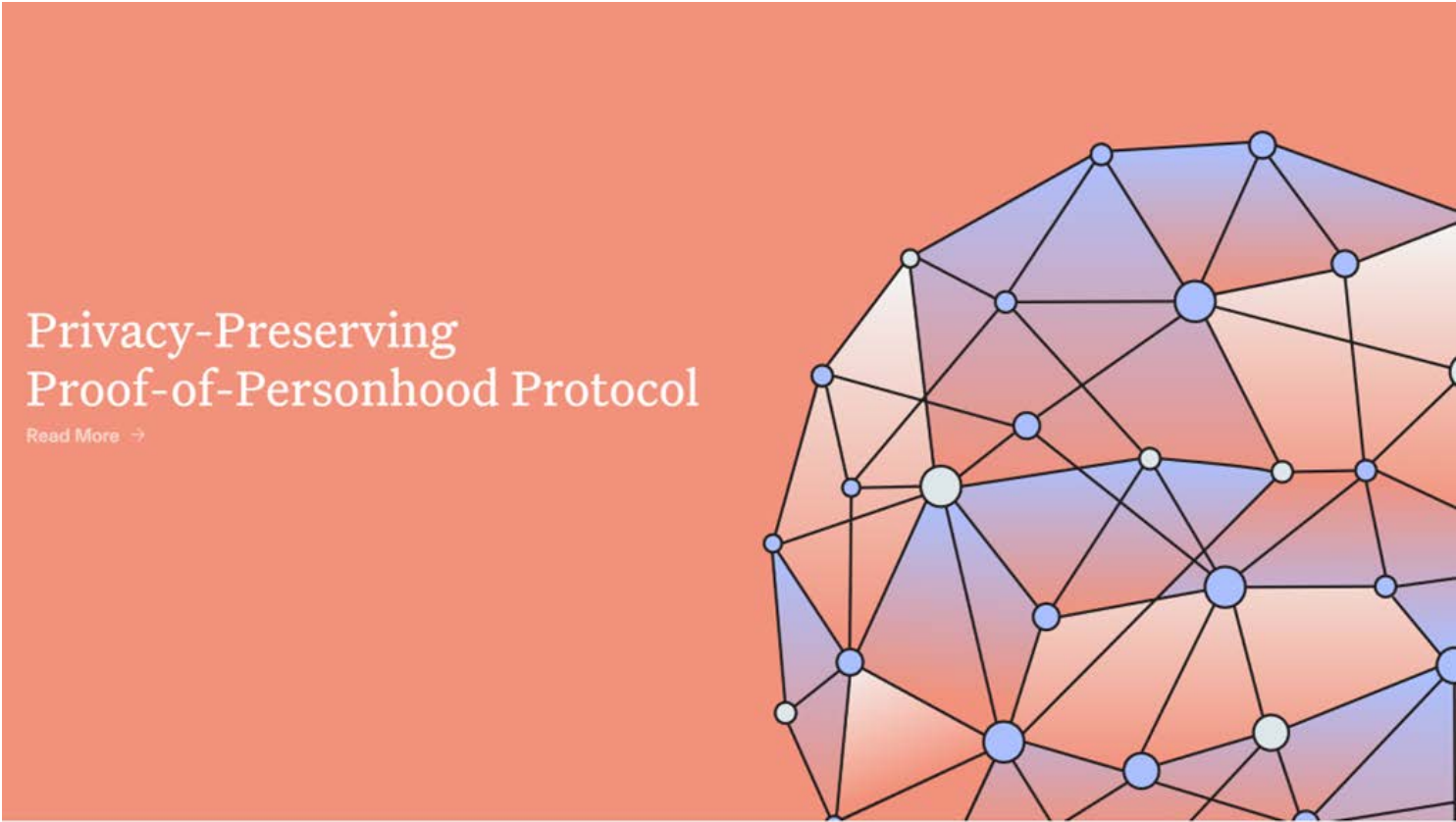
DAO的聚合和推荐网站。

5.32 Tally

DAO的操作系统，提供关于DAO的软件工具，包括生成，加入，投票，以及增长用户工具。

5.33 WorldCoin



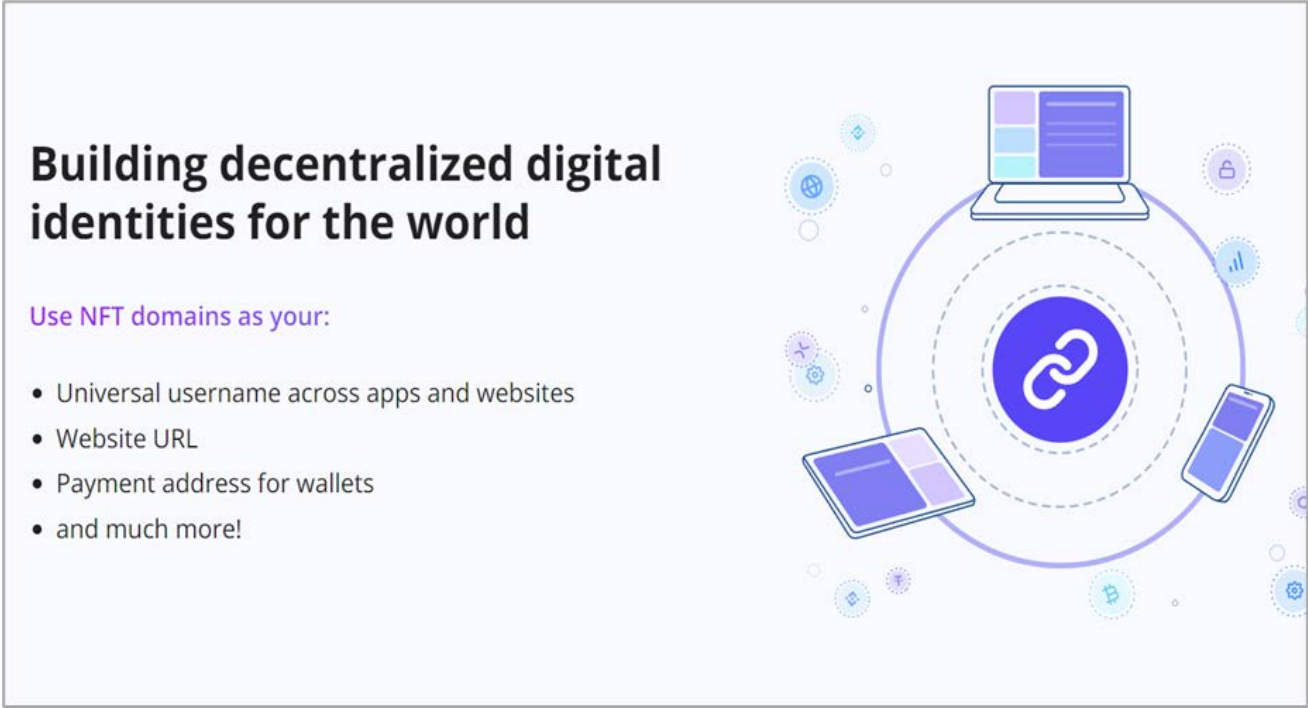


著名的通过虹膜验证真人和唯一性并且给予WorldCoin（WLD）的项目，通过Orb运营商验证真人。

5.34 Proof of Competence

用户通过完成一系列任务来获取自己能力的证明，而项目方获得了用户流量。

5.35 Unstoppable




类ENS一样的为钱包地址注册域名。

5.36 SpringRole

# Build Your On-Chain Proof-Of-Work Portfolio

SpringRole is a platform where professionals demonstrate their work, get verified, give tenable endorsements, get into communities, and more - everything on the blockchain!

Get Verified

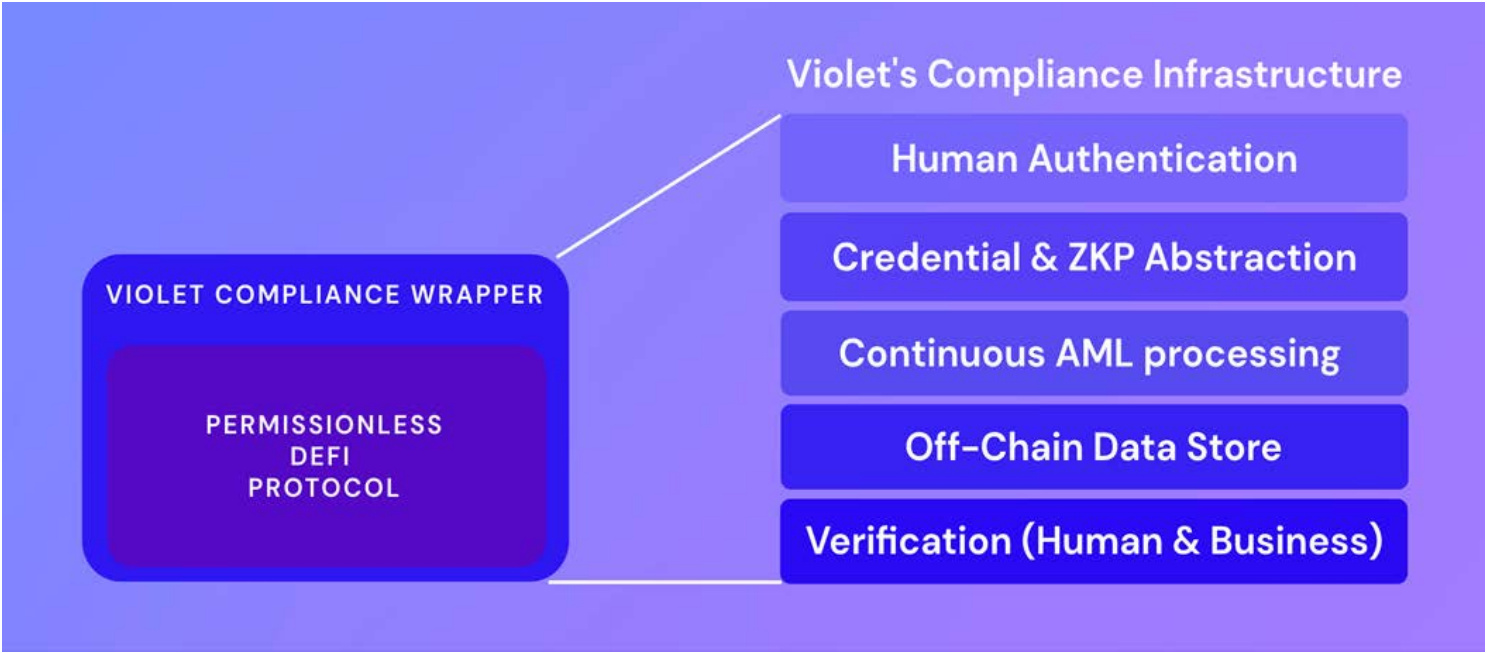


区块链上的linkedin，通过建立链上身份信息和朋友认证获得Spring代币。

5.37 Mazury

区块链上的linkedin。

5.38 Violet



基于二层网络的，由链上和链下数据支持的KYC和AML的身份认证网络。

5.39 Yup

一个管理和分享内容获得YUP代币的内容网络，产品包括浏览器插件。

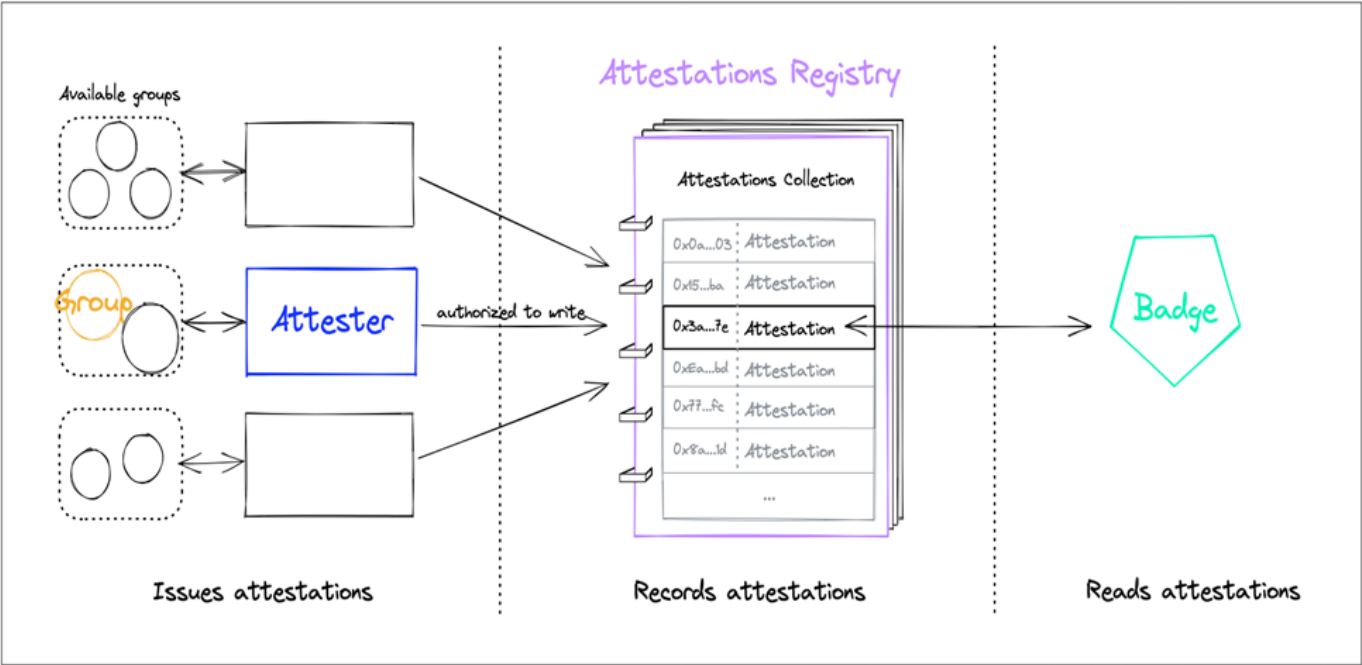
5.40 Prysm

赋予群聊共同投资和管理代币和NFT的功能。

5.41 backdrop

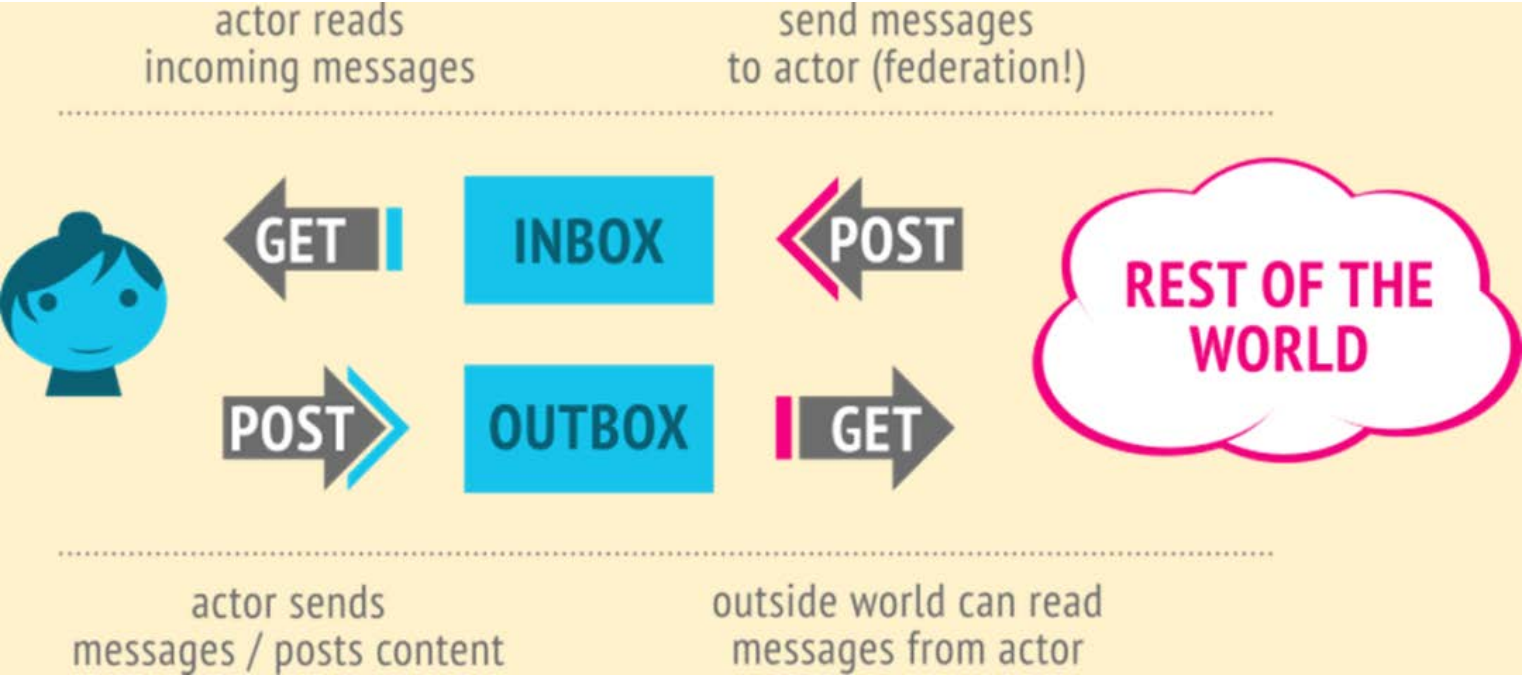
管理DAO社区的平台。

5.42 sismo



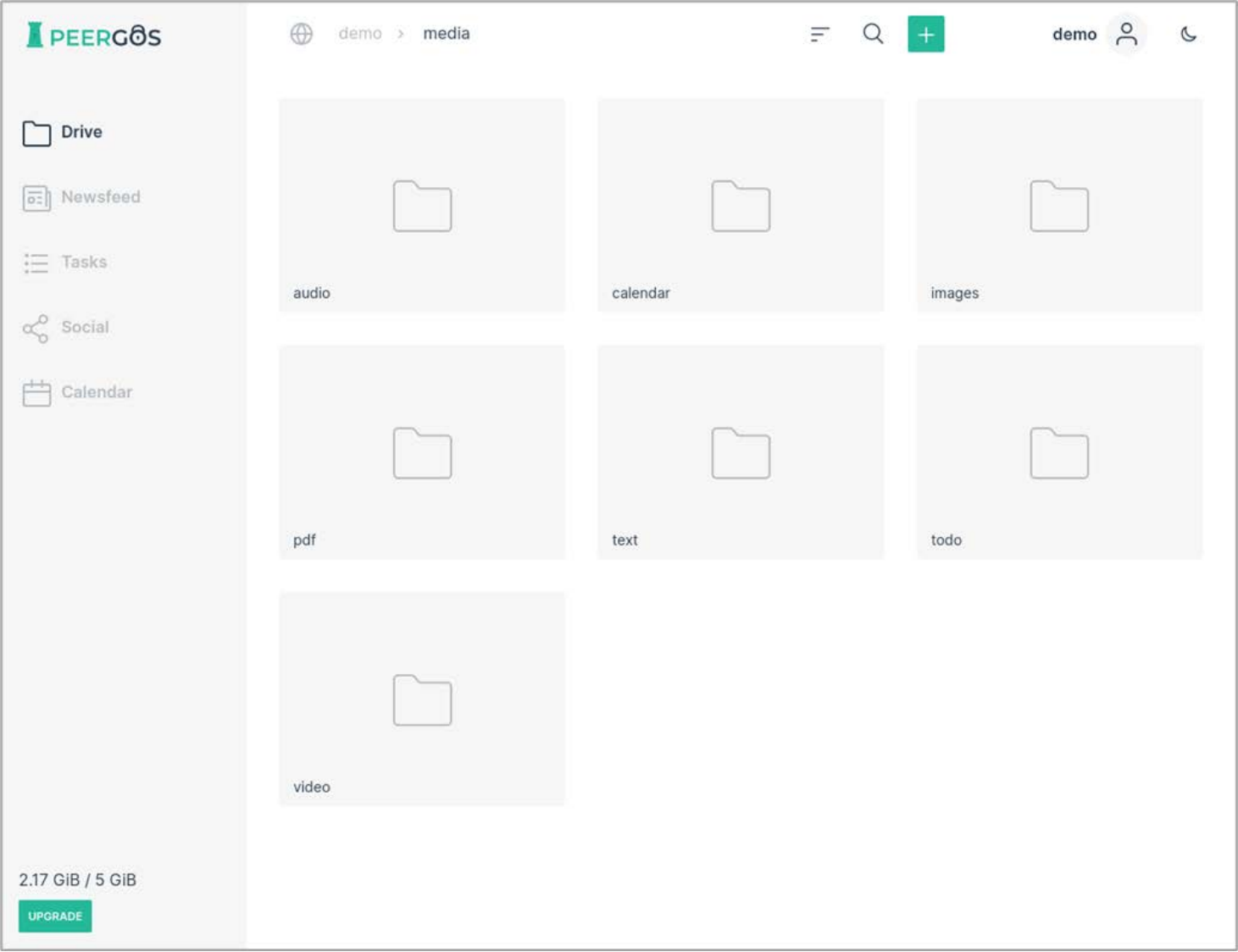
运行在Polygon上的去中心化的用户身份验证协议，支持ZK Attestations。

5.43 ActivityPub (spritelyproject)



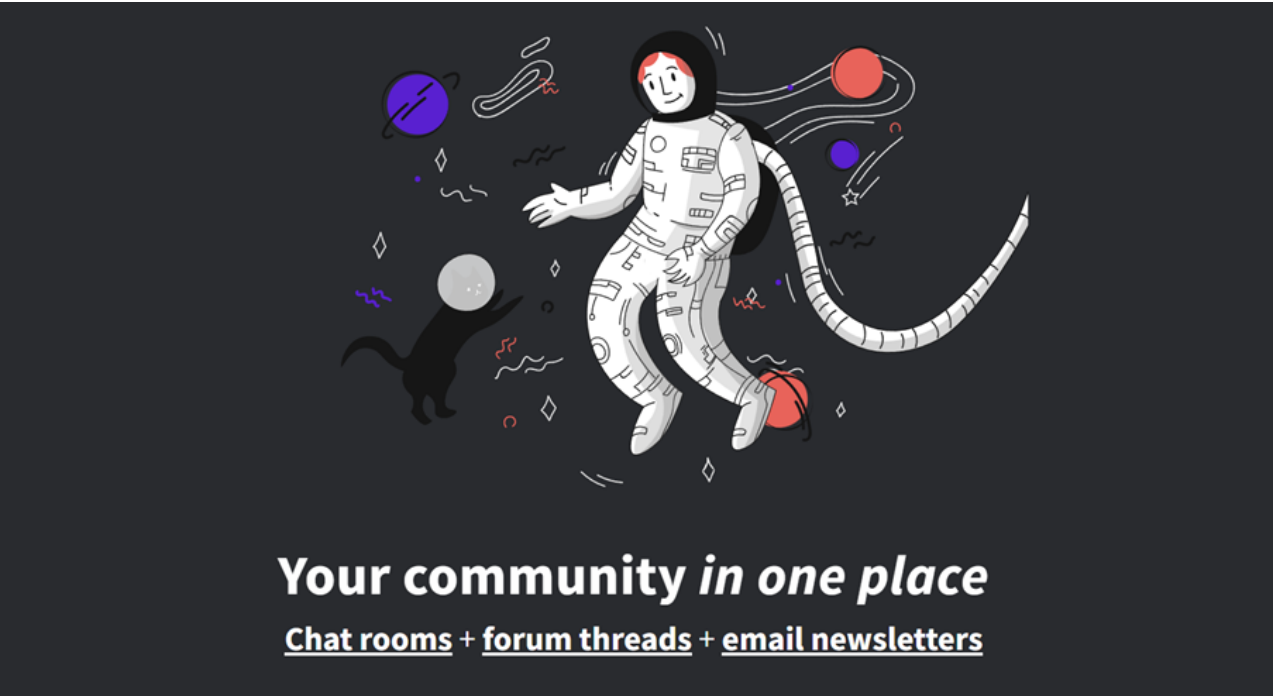
一个基于联盟节点的社交网络协议，2018年被W3C批准为推荐协议。用户被单个节点管理，用户之间通过webfinger发现，可以建立关注关系，通过类邮件的形式通讯。

5.44 Peergos



一个基于IPFS为用户提供身份文件存储和DAPP登陆服务的技术框架。用户由独立的peergos服务器管理，用户可将钱包地址链接到一个中心化服务器保证唯一的先来先到的域名。

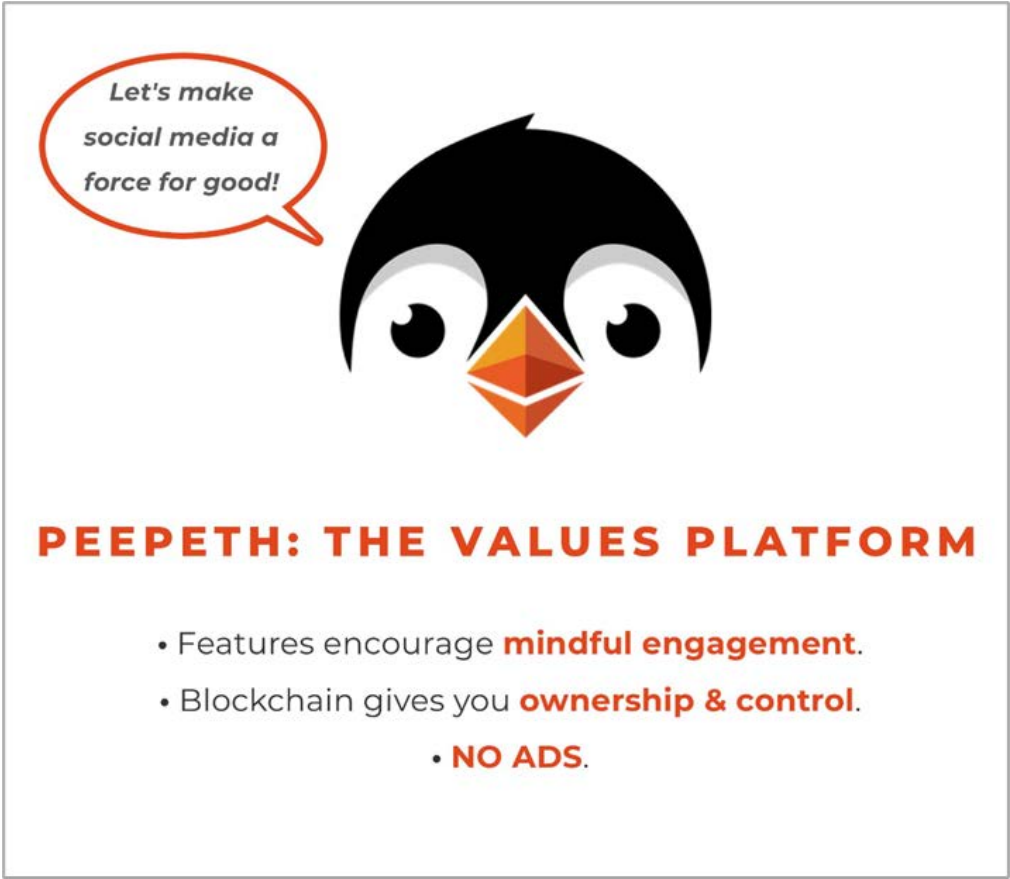
5.45 Aether



一个去中心化的Reddit，用户身份基于公钥，可以关联一个不唯一的nickname，运行flood network协议，每个用户运行全节点存储所有内容，需要0-10分钟更新和同步内容。



5.46 Peepeth



基于IPFS和以太坊的微博，用户的身份是一个以太坊地址，微博内容存储在IPFS。

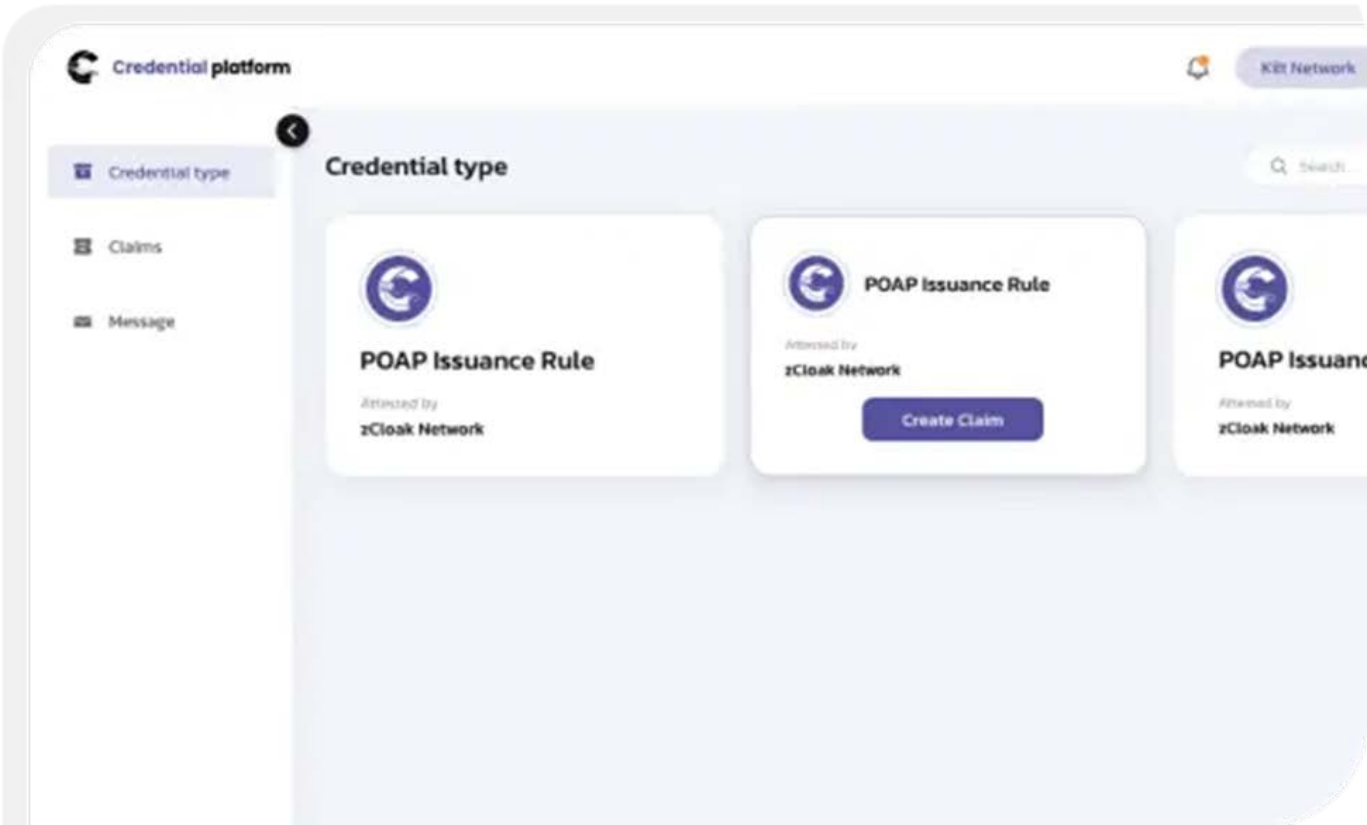
5.47 Diaspora

2010年上线的基于联盟服务器的去中心化的社交网络，兼容 Friendica and Hubzilla。节点称为POD，管理用户的注册，通过webfinger发现用户，通过Salmon Magic Signatures协议进行加密通讯。

5.48 Mastodon

2016年上线的基于联盟服务器的去中心化的微博。由节点服务器管理用户注册以及用户的数据，通过webfinger发现用户。

5.49 zCloak



一个基于ZK技术的身份管理钱包。

5.50 LTO

网络 一种区块链即服务 (BaaS) 模型，组织可以将其整合到其现有系统中，从而获得区块链架构的优势。这也为这些网络上的节点和参与者提供了共享和验证数字身份的基础设施。LTO区块链上的DID（身份的公共地址）。

```
did:lto:3JcHcZ3dbRkbEUgs9GsddQyG3QDXj7nkwJZ?nonce=Gnrwes4G8LBfsJWxCCd9ks
```

此外， LTO使用Chainlink预言机创建跨链去中心化身份。因此，其他链上的身份也可以在LTO网络上表示。

一个基于以太坊公钥的LTO DID地址。

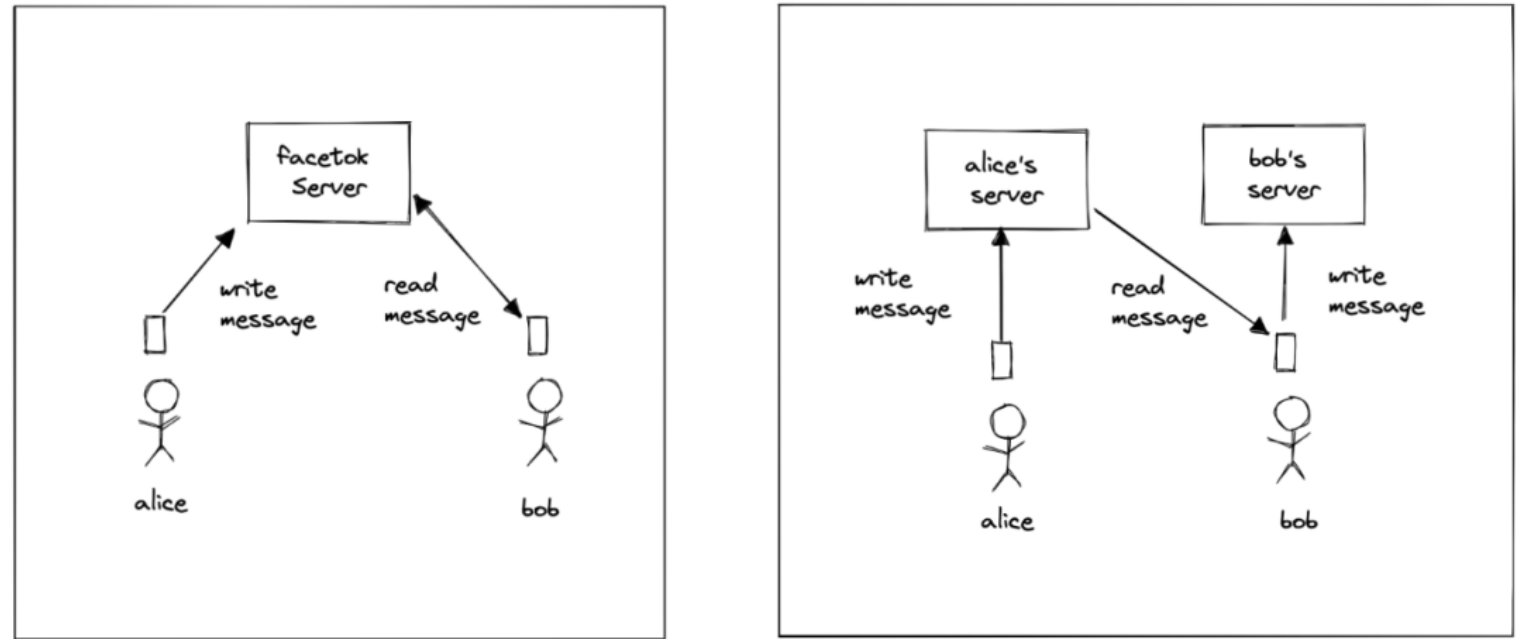
```
did:ethr:0xf3beac30c498d9e26865f34fcaa57dbb935b0d74
```

5.51 Farcaster



Farcaster 由Coinbase 前高管 Dan Romero 和 Varun Srinivasan在 2020 年提出的 RSS+演化而来。Farcaster 是一个社交网络，去中心化且足够分散。当两个用户在网络上能够找到彼此并进行交流。该协议是一个开放协议，类似邮箱一样可支持众多客户端。我们可以自由地在应用程序之间移动其社交身份，社交图谱和身份会随着用户而转移，用户永远拥有与其受众的关系而不受应用程序的限制。开发者也可以自由在网络上构建带有新功能的程序。

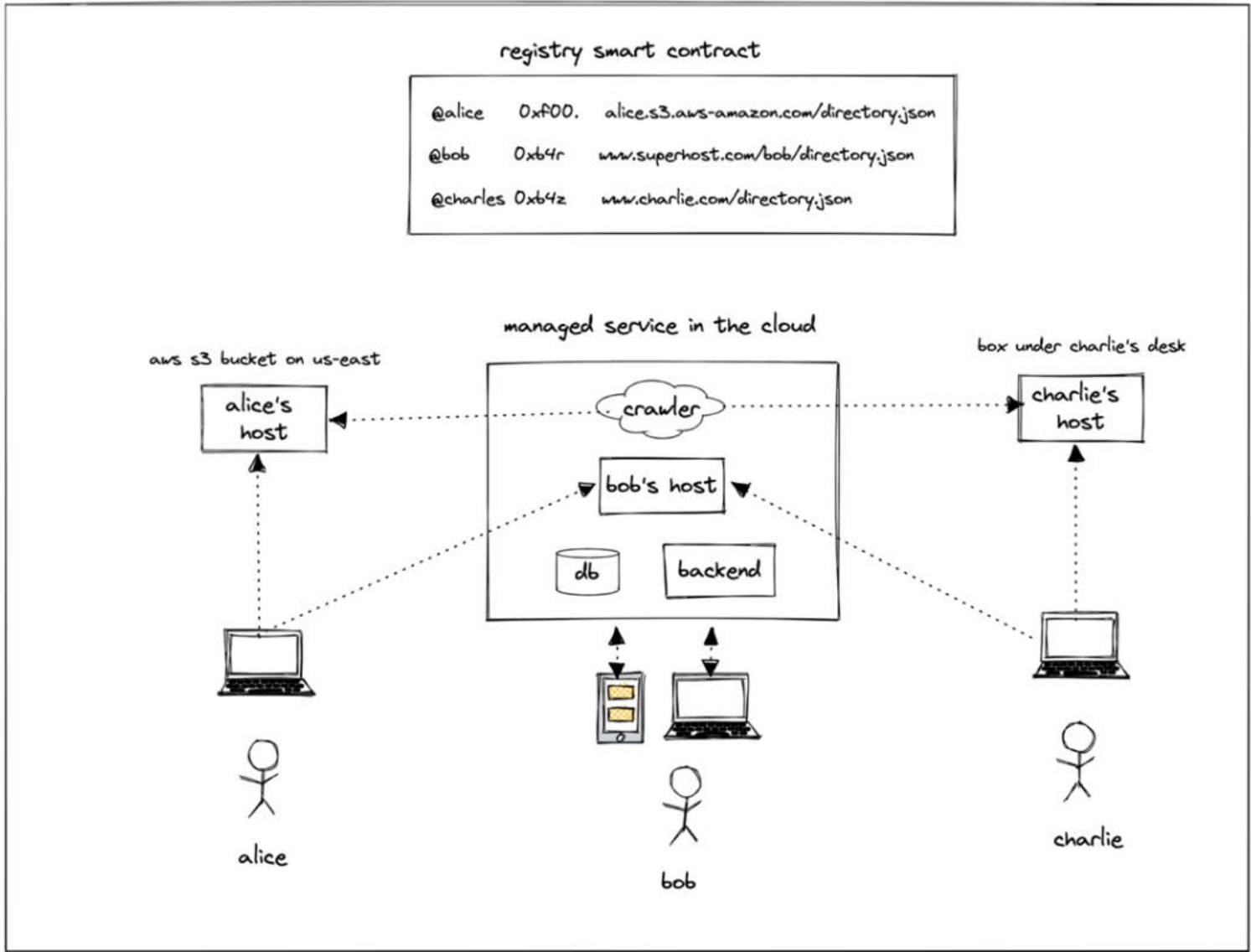
Farcaster 身为一个去中心化的社交网不仅关乎用户所表达的内容，还关乎用户可以在链上证明什么。用户可以连接自己的钱包地址展示自己的 NFT，也可通过 NFT 作为过往行动的证明。甚至可以在其上构建客户端应用程序来在 Farcaster 网络上广播消息，以及读取来自任何用户的消息。



Farcaster 分为链上注册表（On-Chain Registry）与链下主机（Off-Chain Hosts）两个重要组成部分。其中，用户可在链上注册表中 Claim 自己唯一性的用户名，且注册表还用于存储用户的主机 URL（网址），并用作类似网络的「DNS（域名）系统」。因为 Farcaster 的架构意味着用户数据可能存在于不同的服务器上，所以用户需生成一个新的以太坊地址，Claim 一个唯一的用户名，用户名还须与有效的主机 URL 相关联。这样用户想要阅读其他人的消息时，可以向注册表这个智能合约询问他们的主机 URL，然后从主机访问他们的消息。

注册表还设有一系列安全措施以保护用户的安全与隐私。如：只有用户可以更新其主机 URL，而且用户还可以通过使用其地址的私钥对消息进行散列和签名来保护消息。不仅如此，收件人可以检查消息签名并验证它来自哪位用户的地址，该地址也拥有相应的用户名，举例来说，如果用户收到声称来自 @alice 的消息，可以向注册表索取 @alice 的公钥并验证签名是否来自 @alice 的私钥。

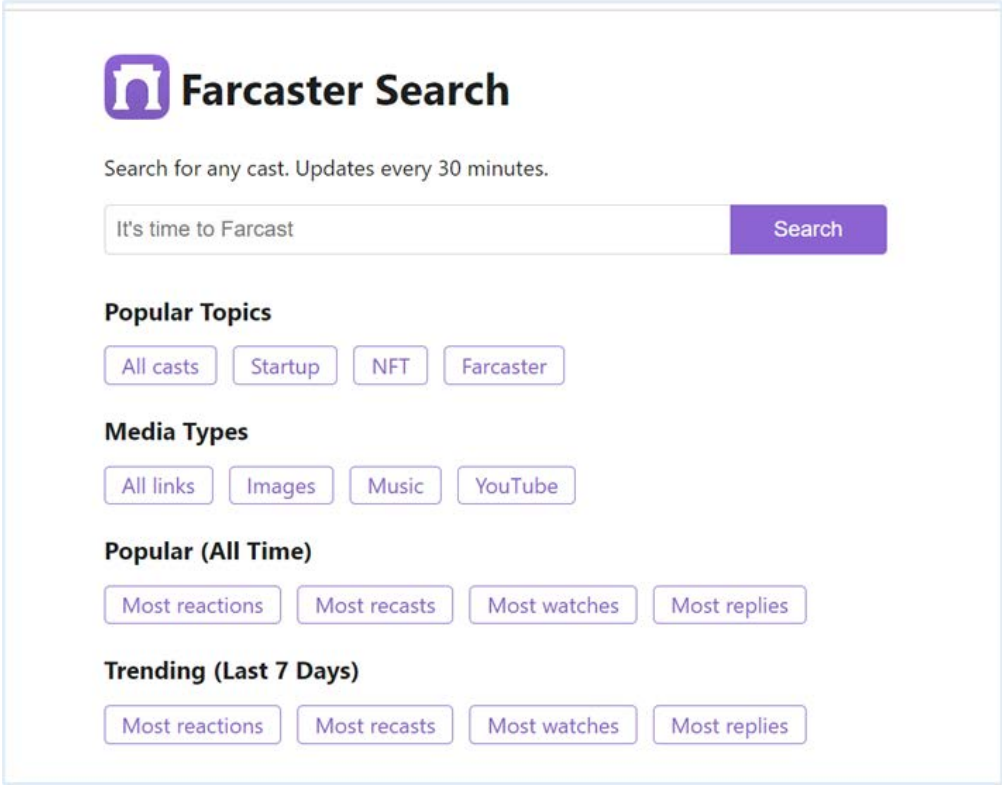
链下主机则用于存储用户的社交数据，只要使用自己的私钥签署，用户可以在任何网络服务器上托管自己的内容，有自托管和使用托管主机两种方式可供选择。



如若用户选择自托管，则无需通过第三方即可使用 Farcaster 网络。用户需要了解如何设置和操作 Web 服务器，下载相应客户端应用程序，可使用该应用程序将消息发布到服务器并从网络上的其他服务器获取消息来实现自托管，官方也表示当前正在构建一个用于自托管的参考开源客户端。

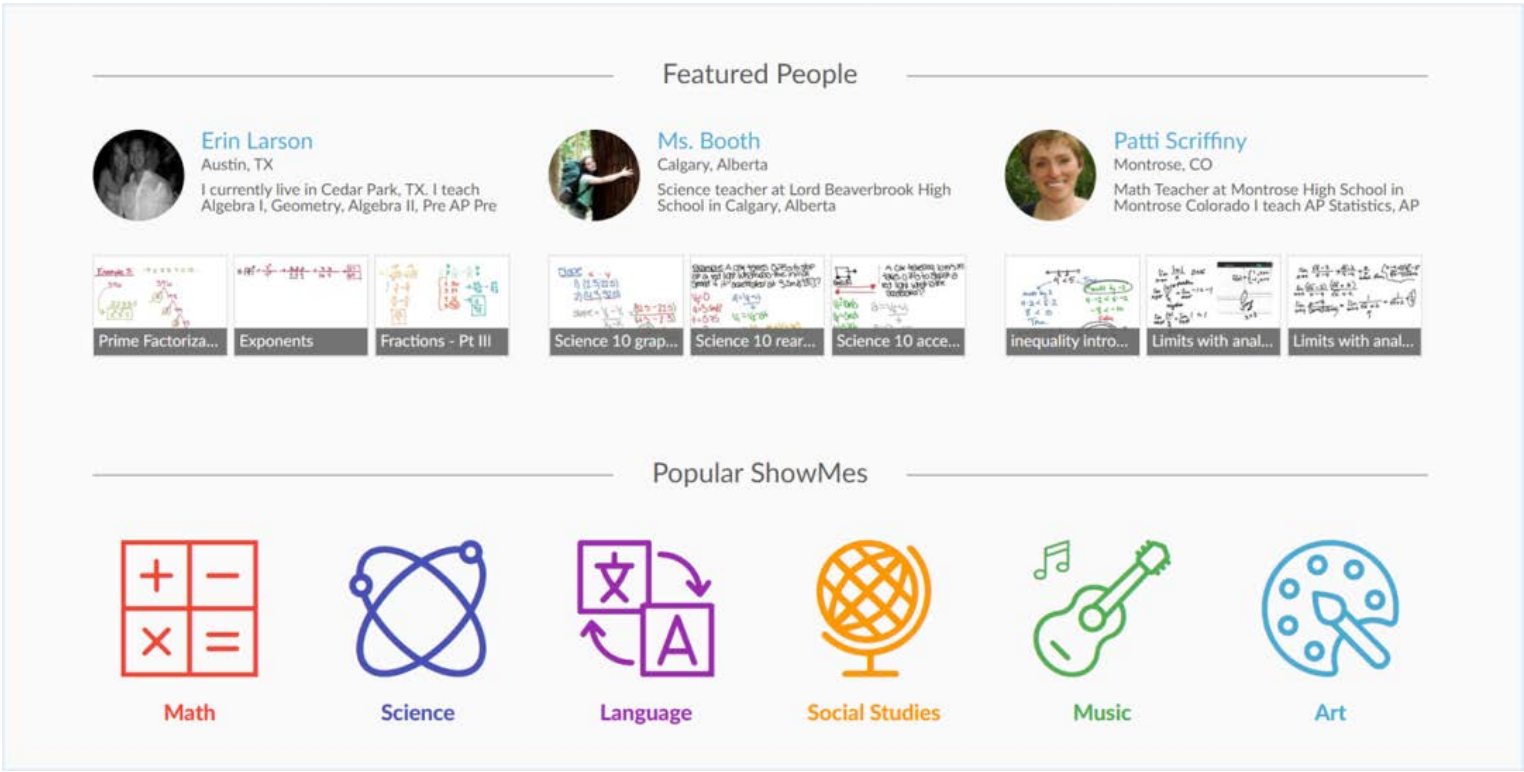
在使用中，用户需要配置更多的基础设施和知识才能实现算法摘取信息流等复杂功能，虽说完全自托管功能有限，仅可发送消息及读取来自单个用户的消息等，但对于 Farcaster 网络来说，重要的是自托管可以确保用户始终能够在没有网守的情况下发送和接收消息，这是 Farcaster 网络能通过充分去中心化测试的前提。如若用户选择托管主机，相对来说可得到最佳的用户体验。托管主机可以简化上传消息、抓取网络数据来提供推荐的信息，提供使用该网络的客户端应用程序。类似于 Gmail 之于电邮、Github 之于 Git，使用托管主机可以做中心化社交网络可以做的所有事情。Farcaster 团队也在运营一个托管主机，当前处于测试阶段，仅限邀请用户参加。





目前，已经有几个基于该协议构建的应用：Instacaster – 所有构建在Farcaster之上的图像都在这里发布 Searchcaster – 在平台上搜索任何演员阵容 CastRSS – Farcaster的RSS提要 Configcaster – 当用户为应用程序/网站使用“连接钱包”时，他们的配置会自动导入，应用程序可以请求任何敏感数据，并由用户单击一下即可批准。

5.52 链上行为NFT化平台ShowMe



ShowMe是一个NFT社交网络，通过俱乐部订阅的模式为创作者和粉丝提供交互服务，它试图链接Web2和Web3，打造一个基于订阅模式的NFT社交网络。

为链上用户身份画像，ShowMe首先提出了PONA（Proof of NFT Achievements）证明机制，即「NFT成就证明」，它是指所有用户在俱乐部中的行为（如收藏NFT、提出优质提案等）都会被记录并保存为NFT，每个成就也会以「NFT徽章」的形式进行表彰。我们目前看到的链上数据多为金融类的交易数据，而行为数据很少。ShowMe把用户的行为通过NFT沉淀到链上，当数量足够多时，用户的标签和画像就会更加清晰；它还通过链上可自动升级的NFT徽章体系，以等级、任务和活动等多种类型的NFT来捕捉更多的链上行为，使每个用户的画像更加明确化。精细化的用户行为可以为Web3.0应用提供用户的精准管理，比如，持有活动NFT的用户可以优先获得NFT项目活动的策展权，高等级NFT的持有者可以参与新NFT项目的首批铸造折扣活动等。

5.53 Idena



类BrightID的一个通过验证码验证真人身份的应用。每个操作Idena验证器节点的独特人类都可以开始开采Idena。

5.54 用户完成任务获得奖励的项目

除了以上应用，还包括用户完成任务获得奖励的项目，Layer3.xyz，Kleoverse，rabbithole，POAP。

5.55 Dauth

一个结合去中心化验证和oAuth来链接web2的身份和web3身份的协议。

另外，还有一系列仅仅只有抽象概念的项目，faceDAO，DeChat，Govrn等。

报告作者：田鸿飞，远望资本创始合伙人

参考文献 **Reference**

[https://en.wikipedia.org/wiki/Self-sovereign\\_identity](https://en.wikipedia.org/wiki/Self-sovereign_identity)

[https://en.wikipedia.org/wiki/FIDO\\_Alliance](https://en.wikipedia.org/wiki/FIDO_Alliance)

[https://en.wikipedia.org/wiki/Initiative\\_for\\_Open\\_Authentication](https://en.wikipedia.org/wiki/Initiative_for_Open_Authentication)

<https://en.wikipedia.org/wiki/WebAuthn>

<https://news.marsbit.co/20220805060417260630.html>

<https://identity.foundation/>

<https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>

<https://www.spruceid.com/>

<https://techcrunch.com/2022/04/20/decentralized-identity-startup-spruce-wants-to-help-users-control-their-sign-in-data/?tpcc=tcplustwitter>

<https://mirror.xyz/fscglobal.eth/HLjBVcSVHj6qVZomNjkY3Vv1yt-EVSkZF3iO2kAdT2c>

<https://www.circle.com/en/verite>

<https://www.circle.com/blog/unlocking-decentralized-identity-with-verite>

<https://news.marsbit.co/20220429123915297078.html>

<https://gitlab.com/bluesky-community1/decentralized-ecosystem/-/blob/master/README.md>

<https://news.marsbit.co/20220121211628019910.html>

[https://zhuanlan.zhihu.com/p/555071064?utm\\_id=0](https://zhuanlan.zhihu.com/p/555071064?utm_id=0)

<https://www.chaincatcher.com/article/2077977>  
<https://www.chaincatcher.com/article/2077119>  
<https://www.chaincatcher.com/article/2071137>  
<https://www.chaincatcher.com/article/2069269>  
<https://www.chaincatcher.com/article/2068523>  
<https://www.chaincatcher.com/article/2066938>  
<https://www.chaincatcher.com/article/2064892>  
<https://www.theblockbeats.info/news/31502>  
<https://d.cobo.com/public/Cobo+ventures+SocialFi+%E6%B7%B1%E5%BA%A6%E8%A7%A3%E6%9E%90.pdf>  
<https://news.marsbit.co/20220618102147694622.html>  
<https://news.marsbit.co/20220613201227975149.html>  
<https://news.marsbit.co/20220608124336519785.html>  
<https://trustoverip.org/>  
<https://d.cobo.com/public/Cobo+ventures+SocialFi+%E6%B7%B1%E5%BA%A6%E8%A7%A3%E6%9E%90.pdf>  
本文来自微信公众号“[远望资本iVision](#)” (ID:iVisionVC),

+1  
24

好文章，需要你的鼓励



评论千条，友善第一条  
登录后参与讨论  
提交评论0/1000  
你可能也喜欢这些文章 [造哥说](#) 特邀作者



[GPT-4重要缔造者、OpenAI 首席科学家：人工智能不吃人](#)



[给冰岛保护方言，给摩根史丹利当实习生，GPT-4已经开始赚钱了](#)



[百度步谷歌后尘：文心一言发布，股价最高跌去近10%](#)



[文心一言对比ChatGPT：百度催生“不完美小孩”](#)





[云游戏就是云未来，阿里元境 x Unity x 长江学者这样说](#)



[扎克伯格，打工人瑟瑟发抖](#)

[Meta再宣万人大裁员，技术岗最先毕业，小扎写「小作文」找借口](#)



[Bard加急测试](#)

[谷歌向微软宣战，谷歌类ChatGPT装进办公「全家桶」，升级版Big](#)



[腾讯大模型技术斩获两项世界冠军，已落地微信搜索](#)



[文心一言 vs GPT-4实测，百度背水一战交卷](#)



浩哥说  
特邀作者

迅雷创始人程浩跟你聊互联网、创业、投资、生活  
发表文章44篇

最近内容

- [论所有权的终结，以及基于NFT的版权解决方案](#)  
2023-03-14
- [远望资本程浩：以太坊会垄断公链吗？](#)  
2023-01-06
- [DID行业研究报告](#)  
2022-09-08

[阅读更多内容，戳这里](#)

报道的项目



D加用车网  
我要联系  
中高端用车服务平台

提及的项目

[查看项目库](#)



[ata](#)



[立信数据科技](#)



[个推](#)





## Board

展开更多

下一篇

## 华为苹果“隔空对决”，年轻人：别打了，我换还不行吗？

## 不换机的年轻人还是没绷住

2022-09-08

## 关于 $^{36}\text{Ar}$

- [城市加盟](#)
- [寻求报道](#)
- 我要入驻
- [投资者关系](#)
- 商务合作
- [关于我们](#)
- 联系我们
- [加入我们](#)

[网络谣言信息举报入口](#)

## 热门推荐

- [热门资讯](#)
- [热门产品](#)
- [文章标签](#)
- [快讯标签](#)

## 合作伙伴

- 
- A staircase diagram with 10 steps, each containing a question mark icon.

本站由 [阿里云](#) 提供计算与安全服务 违法和不良信息举报电话：010-58254120 举报邮箱：jubao@36kr.com [网上有害信息举报](#)

© 2011~2023 北京多氮信息科技有限公司 | [京ICP备12031756号-6](#) | [京ICP证150143号](#) | [京公网安备11010502036099号](#)

意见反馈