 **当前位置:** 主页 > 区块链 > 技术 > 区块链一定需要代币吗

去中心化身份DID：Web3通行证

2021-12-06 15:09:25 | 来源：金色财经 | 作者：金色财经 Maxwell

ETH怎么挖矿 2021年最详细以太坊（ET...

这篇文章主要介绍了去中心化身份DID: Web3通行证的相关资料，希望这篇关于Web3通行证的文章，能够帮助到各位朋友可以对Web3通行证有一个深入的了解。



随着WEB3的发展，人们越来越认识到去中心化身份系统DID的重要性。近日Amber Group发表研报“去中心化身份DID: Web3通行证”，介绍了DID概念和当前的DID生态系统，并深入研究了选定的构建Web3身份最前沿的几个项目。

引言

互联网是在没有人的原生身份层的情况下创建的。正因为如此，数字身份问题被归为网站和应用程序。这种孤立的方法可能适用于互联网的早期，但现在有数十亿人在线，其缺点变得越来越明显。尽管反复被证明是不安全的模型，但用户名和密码仍然是主要范式。普通人必须在70到80个密码之间折腾，从而导致明显较差的用户体验。事实上，有数百万美元的商业业务是为帮助企业和个人管理其分散的帐户而建立的，例如Okta、1Password和Dashlane。最重要的是，用户实际上并不拥有他们的在线身份。相反，他们从公司和中心化实体那里租用它。因此，他们很容易面临数字身份被黑客攻击、操纵、审查或完全丢失的风险。

Web3从根本上嵌入了经济转移，它的出现重新强调了创建强大的身份系统。尽管与DeFi、NFT和DAO相比，去中心化身

份 (DID) 在很大程度上是一个被忽视的话题，但我们将其视为支持原生Web3应用程序的关键技术原语。如果我们创建一个共享的、灵活的和有弹性的身份层，我们可以通过创建更广泛的设计空间来彻底释放创新的步伐。

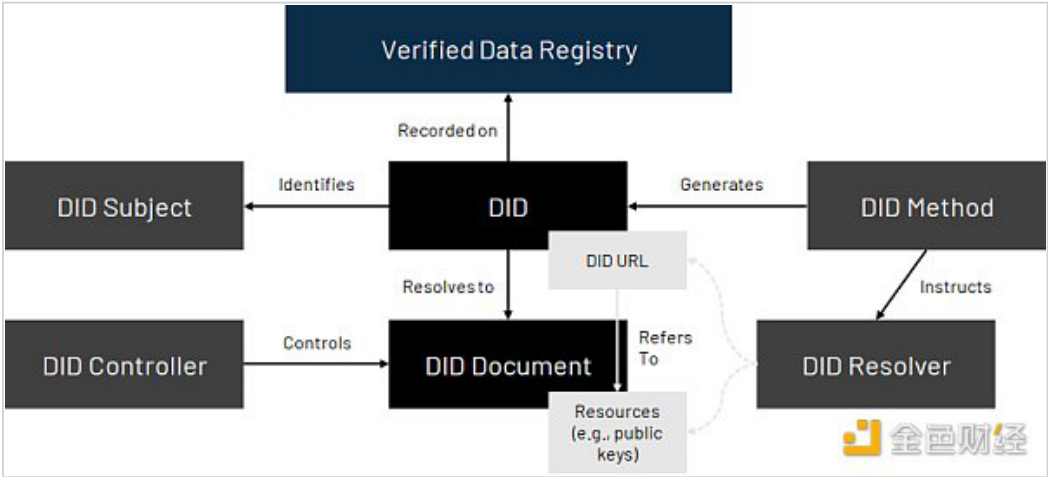
在本报告中，我们在高层次上介绍了关键的DID概念和当前的DID生态系统，并深入研究了选定的构建Web3身份最前沿的几个项目。

去中心化身份 (DID)

W3C的DID规范是广泛接受的标准，可确保身份系统可以跨不同网络 and 平台进行互操作。

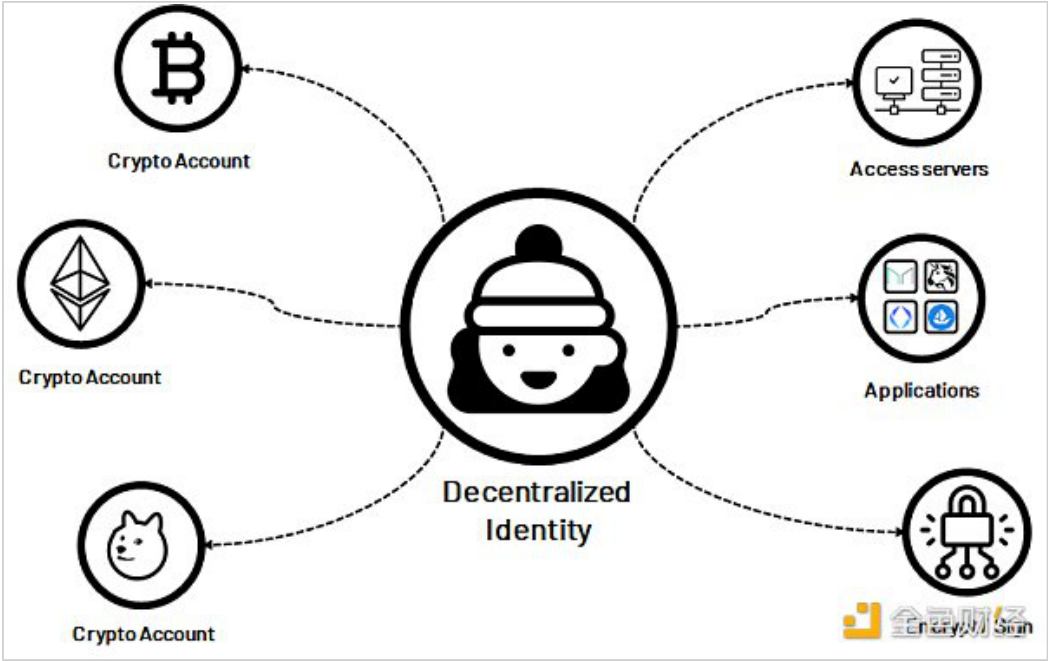
DID架构的概述如下图所示。一个DID是在互联网上的地址，人们可以拥有和直接控制。它可用于查找关联的DID文档，其中包含与DID关联的信息。DID文档包含相关信息以启用用例，例如登录、数据加密、通信等。密码证明，例如数字签名，允许实体证明对这些标识符的控制。

DID架构的基本组成部分



总之，DID充当身份中心。因为用户控制着他们的中心，他们可以决定何时、与谁以及在什么条件下透露他们的数字身份元素。随着DID标准的广泛采用，用户不会被锁定在单一的生态系统或孤立的方法中。

DID为用户提供控制、安全、隐私和便携性



DID允许新用例

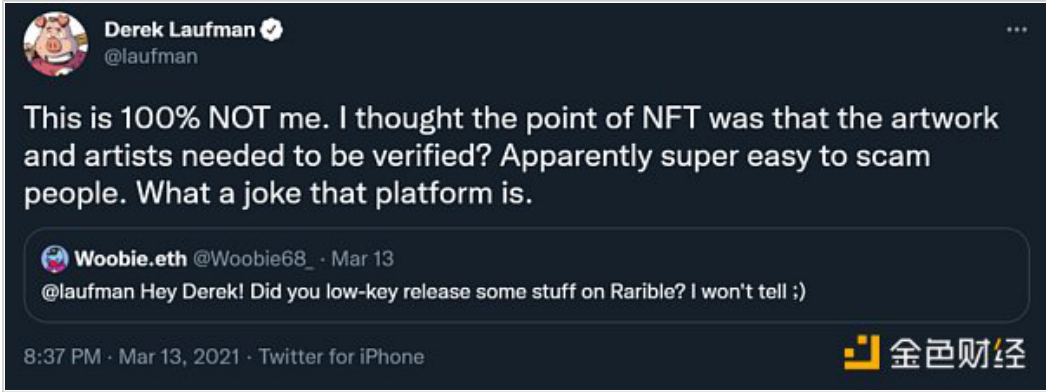
在现实世界中，身份是运转良好的社会不可或缺的一部分。护照使政府能够识别其公民的身份，驾照使公民能够主张道路的权利，大学学位授予有资格的学生等。

同样，DID将使高价值的互联网经济活动成为可能。下面，我们重点介绍DID可以解决的一些当前Web3 痛点。

NFT——真实性和身份

欺诈和抄袭继续困扰着艺术家和创作者。例如，漫威超级英雄大冒险的数字艺术家和设计师德里克·劳夫曼（Derek Laufman）在他不知情的情况下看到他的作品在NFT平台Rarible上拍卖。类似的故事屡见不鲜。

NFT欺诈继续困扰艺术家

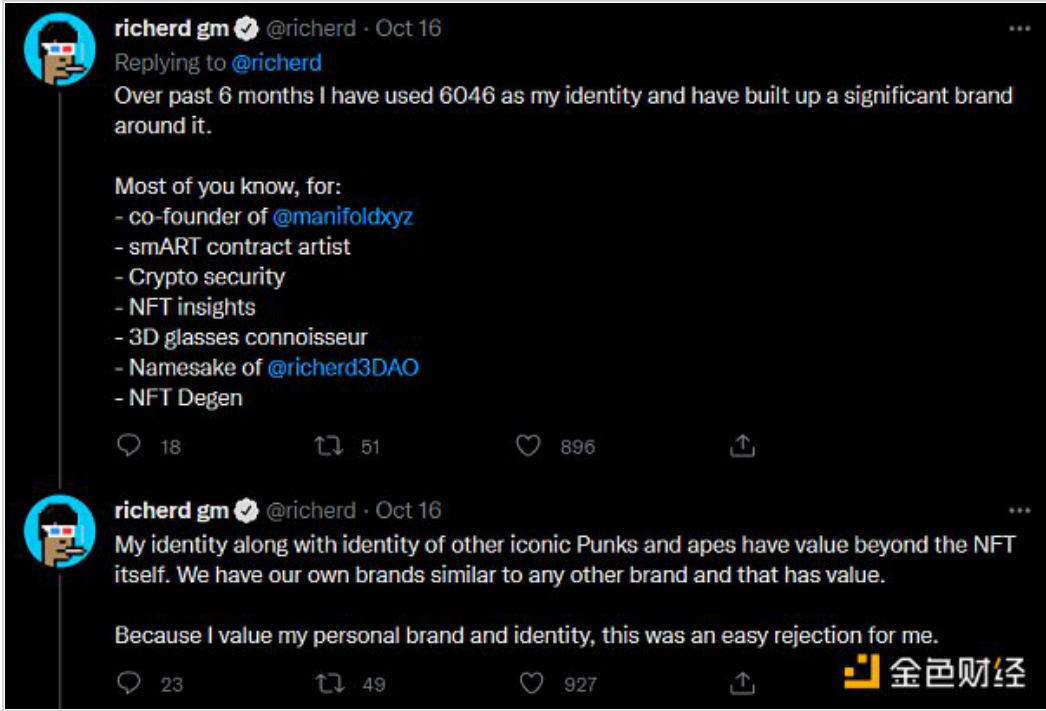


来源：推特

强大的DID基础设施解决了这个问题。应用程序可以建立在DID基础上，以允许创建者证明他们创建了代表数字或物理资产的NFT。买家和卖家也将能够验证数字艺术品的出处。DID还可以帮助促进艺术家与其社区之间的更多参与，例如将NFT所有权限限制为社区成员以限制黄牛的投机或为选定的持有者提供独家NFT内容。

更广泛地说，NFT可以作为去中心化身份的一个锚点。已经好几个用户不仅通过用户名而且还通过NFT项目来识别他们的在线身份。例如，Manifold联合创始人richerd说，他拒绝了950万美元的加密朋克NFT报价，因为他将加密朋克视为他的身份和品牌。

NFT作为在线身份



来源：推特 (@richerd)

解锁DeFi的下一阶段

迄今为止，抵押贷款一直是DeFi增长的支柱。但由于加密金融协议旨在完全去信任和无需许可，因此它们通常需要过度抵押。例如，在MakerDAO上通过ETH获得的贷款需要130-170% 的抵押率。这推动了去年DeFi的增长，但抵押品要求将用例限制在主要是希望利用杠杆的加密货币交易者。对于大多数人来说，他们想借钱的原因是他们还没有所需的钱。

降低或完全取消抵押品要求是将DeFi引入大规模采用的关键。拥有强大的DID层可以允许“链上”信用评分，为用户提供基于信用的贷款。此外，由于用户直接控制他们的信用评分，他们可以更好地监控和调整他们的借贷行为。因此，DID提供了进一步民主化去中心化金融系统的机会。

此外，对金融应用程序拥有强大的身份层可以解决DeFi中的其他当前问题，例如：

通过对实际成员进行身份验证并减少机器人稀释空投事件的可能性来改善代币空投的公平分配。

使用DID来限制对DeFi池的访问，以减少垃圾邮件/女巫攻击或通过提供合规工具来识别交易对手，使机构能够参与进来。

通过照亮可信任的参与者以正和方式行事，引导用户穿越以太坊的黑暗森林。

去中心化自治组织 (DAO)

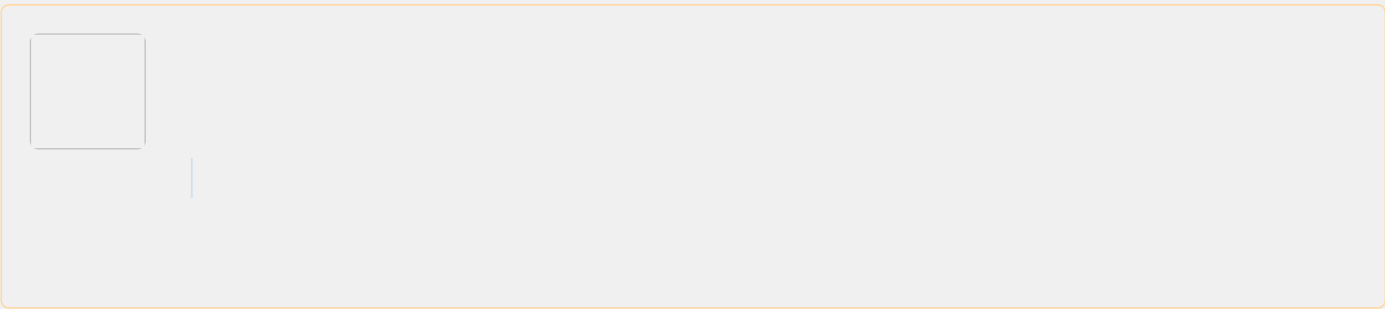
DAO通常使用基于代币的治理来进行投票、影响力和优先级。这通常是有道理的——大型代币持有者在游戏中拥有最多的皮肤——但它可以排除或减少可能没有大量资本的积极贡献者。尽管成员可以在DAO内建立自己的声誉，但他们可能需要在新环境中从头开始建立信誉。

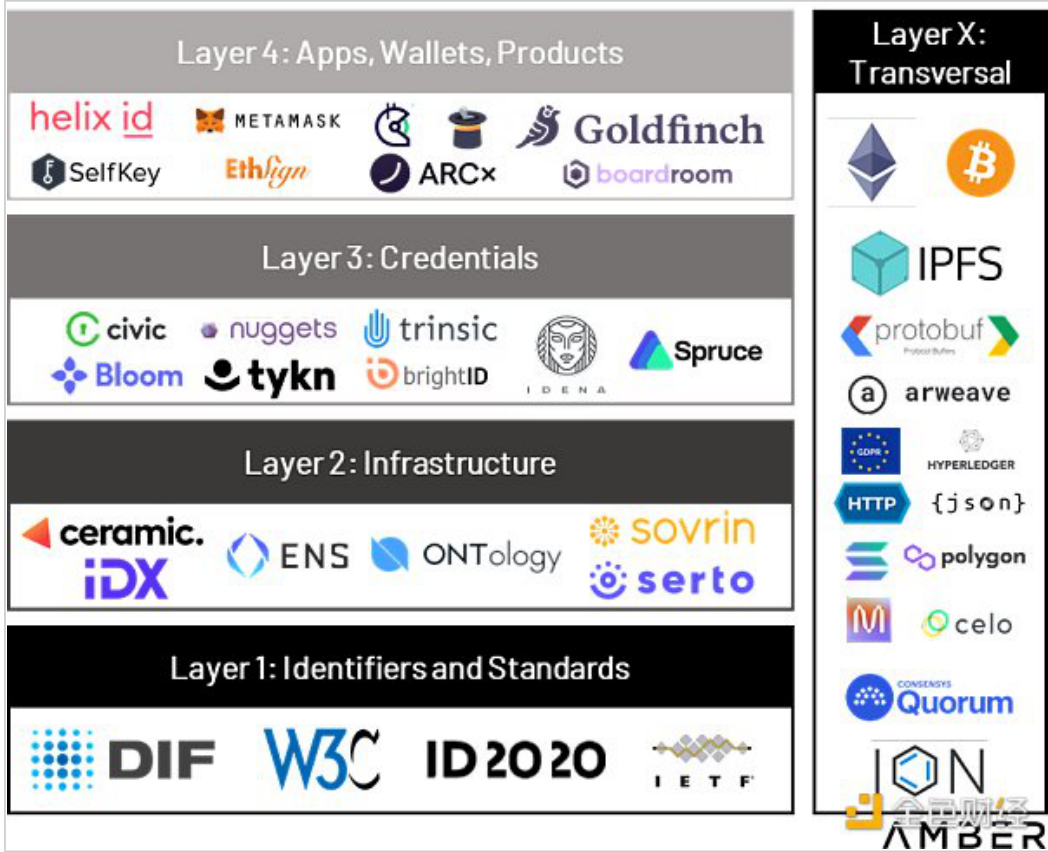
DID可以在多个DAO中保护用户的声誉。将凭证从一个DAO移植到另一个DAO反映了我们在物理世界中已经享有的声誉可移植性，防止活跃的贡献者不得不从零开始。此外，其他WEB3环境，如在参与Gitcoin，出版物Mirror，或代码贡献Radicle，有助于进一步的DAO找到合格的候选人。

DID生态系统

DID生态系统可以分解为多个层，其中上面的每一层都建立在底层协议之上。我们利用并稍微修改了DIF的4层身份模型，以通过其主要关注点映射当前的DID项目，但需要注意的是，这是一个简化模型，大多数项目都超越了一层。

分层的去中心化身份生态系统





资料来源: DIF、Amber Group

第1层: 标识和标准

标准、标识和命名空间创建公共信任层，确保标准化、可移植性和互操作性。它们还允许网络注册和管理DID方法，为开发人员和用户提供网络ID系统的规则和上下文。

去中心化身份基金会（Decentralized Identity Foundation, DIF）是这一层的关键参与者，也是生态系统的基石。它充当开发、讨论和管理为DID堆栈创建和维护可互操作和开放生态系统所需的所有活动的中心。

第2层: 基础设施

基础设施和代理框架允许应用程序彼此直接交互和可验证的数据注册。这些解决方案包括通信、存储和密钥管理。我们强调Ceramic和ENS作为构建DID基础设施前线的项目（尽管ENS 的分类可能存在争议，但我们将其置于基础设施层，因为

我们预计凭证和应用程序将在未来构建在ENS之上)。

第3层: 凭证

必须管理、更新和交换凭证。该层旨在解决DID如何协商控制证明和身份验证，以及在身份所有者之间安全地传递数据。BrightID是该领域的一个著名项目。它是一个拥有超过30,000个用户的社交身份网络，允许人们向应用程序证明他们没有使用多个帐户，从而最大限度地减少女巫攻击的机会。

Vitalik Buterin关于BrightID的潜在应用



来源：推特 (@VitalikButerin)

第4层: 应用程序、钱包和产品

这一层可能是读者最熟悉的，旨在为消费者提供现实世界的用例和价值。一些项目，例如Goldfinch（无抵押贷款），使用专有的唯一实体检查，但旨在在成熟时利用去中心化的ID解决方案。相比之下，其他应用程序已经利用了现有的DID技术，例如TrueFi（具有链上信用评分的无抵押贷款）、Gitcoin（公共产品融资）和Ethsign（去中心化电子协议）。

X层: 横向

这些项目在很大程度上超越了任何单个层面，并在多个层面产生影响。例如，欧洲的GDPR数据保护法对生态系统的所有领域都有影响。

DID生态系统中的代币估值

Name	Ticker	Price (USD)	FDV (US\$mn)	Description
ENS	ENS	40.91	4,091	Public profiles for Ethereum addresses
Ontology	ONT	0.98	981	DID blockchain with data attestation and marketplace
Civic	CIVIC	0.60	597	Identity verification for KYC & AML
SelfKey	KEY	0.02	96	Non-custodial DID wallet
ArcX	ARCX	0.38	38	Decentralized on-chain credit and reputation scoring protocol
Bloom	BLT	0.15	23	Decentralized identity attestation and credit scoring
Ikena	IDNA	0.14	11	Proof of person blockchain - mining node is linked to identity
BrightID	BRIGHT	0.38	9	Social identity network to prove unique identities

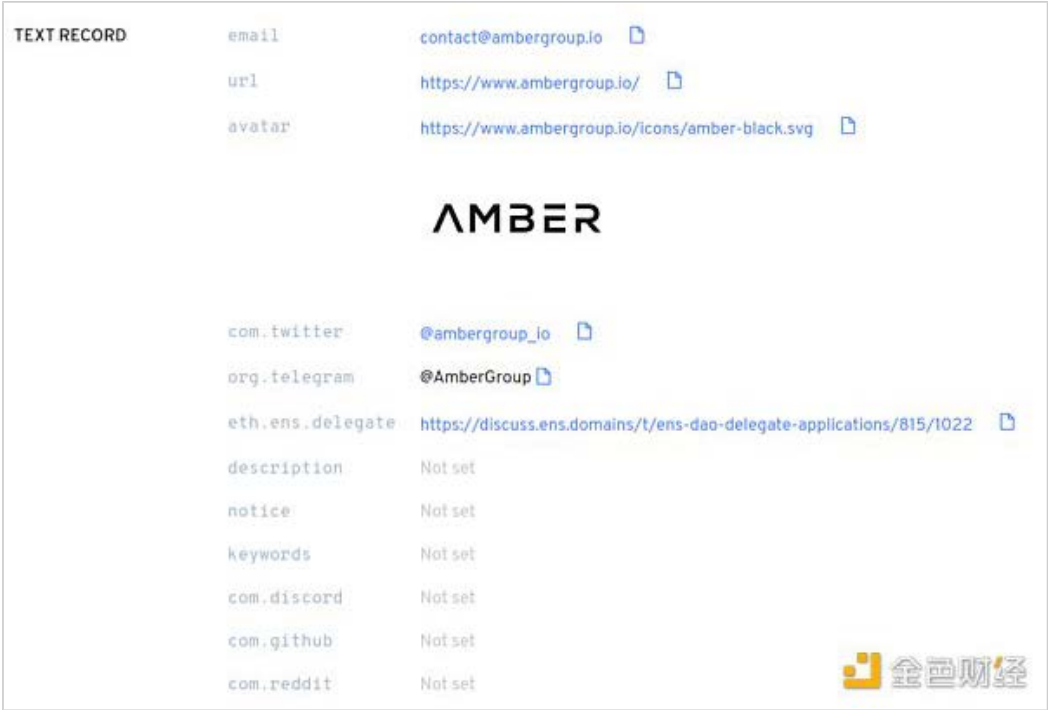
资料来源：CoinGecko，截至2021年11月22日的Coinmarketcap

一些DID项目

ENS——以太坊的公开profile

以太坊名称服务 (ENS) 是一种基础工具，可将任何以太坊地址转换为公开profile。它的主要工作是将人类可读的名称映射到机器可读的标识符。你可以输入“amberfin.eth”，而不是使用“0x7fc7a9694A09077e137f953108265ad59cCF5ba3”进行交易。并且由于ENS的分层性质，拥有该域的任何人也可能拥有子域。例如，因为Amber Group拥有“amberfin.eth”，它也可以创建“pay.amberfin.eth”。ENS域还可以有文本记录，允许用户存储与一个标识符相关联的各种数据。此设置不涉及中央实体或公司。

Amber Group的ENS记录



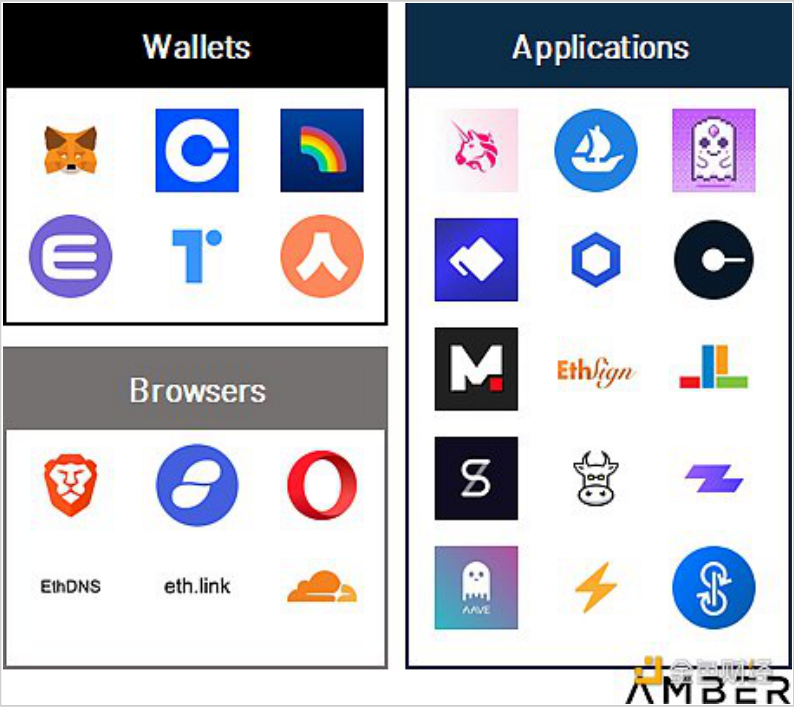
ENS的用例继续增长。ENS完整集成到DNS于今年8月启动，因此你可以将加密货币发送到“example.com ”而不是“example.eth ”。此外，.eth域名还可用于构建去中心化网站。例如，以太坊联合创始人Vitalik Buterin利用这种DNS集成以及IPFS在https://vitalik.eth/上创建了一个强大且抗审查的网站。

ENS可能会在可移植和去中心化身份的未来发挥关键作用。它注册为DID表示，允许将ENS名称包装为DID以促进互操作性。许多Web3用户已经使用ENS作为他们的标识符。一项对约 300名以太坊用户的调查发现，约64%的人已经拥有ENS，链上分析表明ENS用户平均拥有 2.5个域。随着附加功能的推出（例如NFT头像支持）以及dApp越来越多地采用ENS，Web3 用户很可能会越来越多地使用ENS作为他们在以太坊上的事实上的公共身份。

Uniswap上支持ENS名称和头像

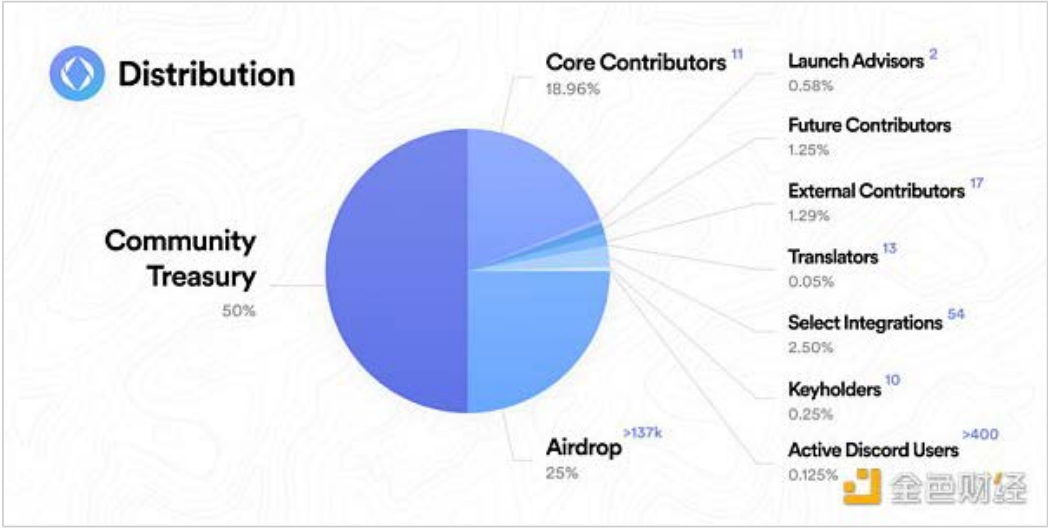


ENS生态系统



11月2日，ENS宣布通过接受DAO代表的申请和空投ENS治理代币来实现去中心化治理。空投占总供应量的25%；余额将分配给社区金库和贡献者。分配基本上为过去（先前的贡献者和用户）提供了总代币的一半，为未来（社区金库）提供了一半。

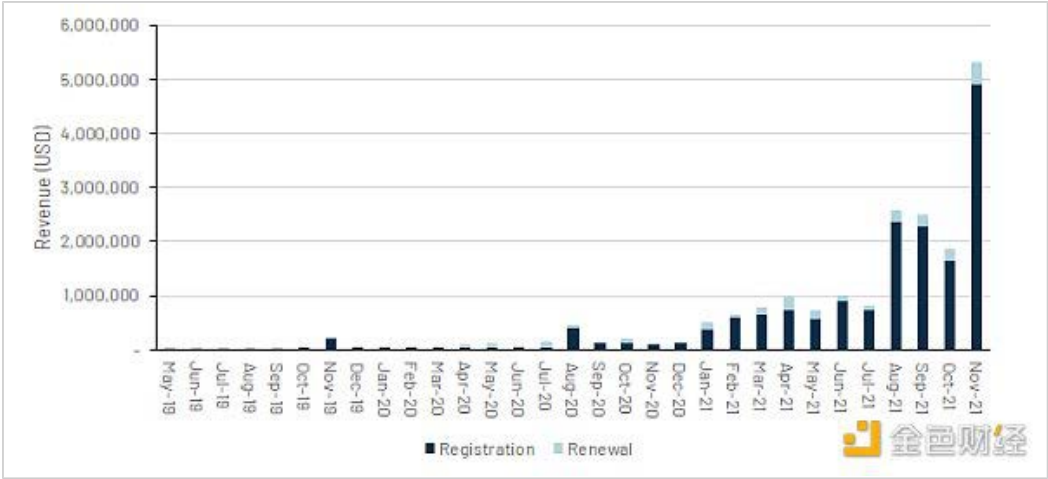
ENS代币分配



ENS代币持有者仅持有DAO的治理权，不会获得额外的货币价值。独一无二的是，ENS代币持有者被要求签署ENS章程，其中强调了关键原则——例如执行产权、避免寻租行为以及与全球命名空间整合——以领取他们的代币。因此，ENS代币最令人兴奋的方面之一是它是市场如何为数字公共产品定价的一项盛大实验。

ENS产生了近2000万美元的收入，主要来自新域名的注册，这些收入将进入DAO国库。

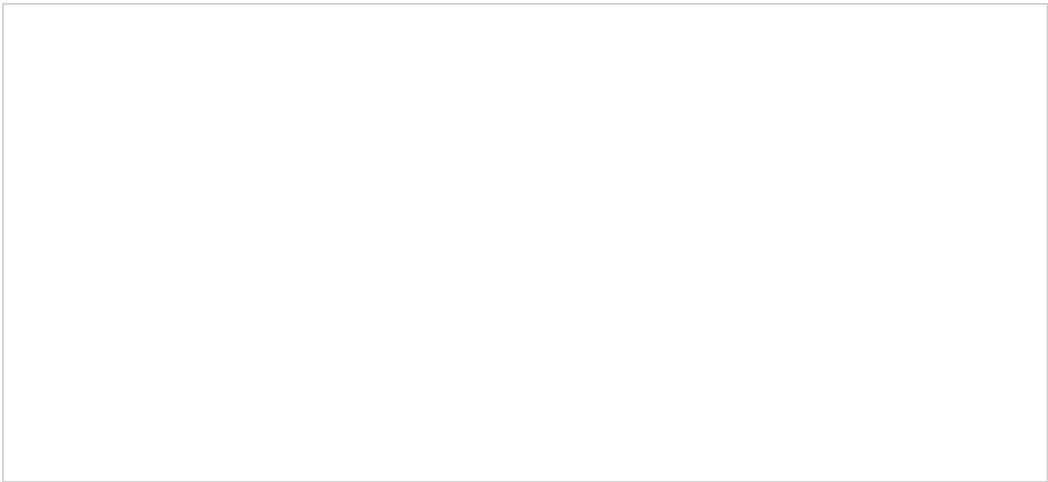
ENS月收入



资料来源：Dune Analytics (@makoto)

ENS每笔交易的收入也有所增加，这表明用户注册域名的时间更长，保护更高价值的域名（即较短的域名），或两者兼而有之。

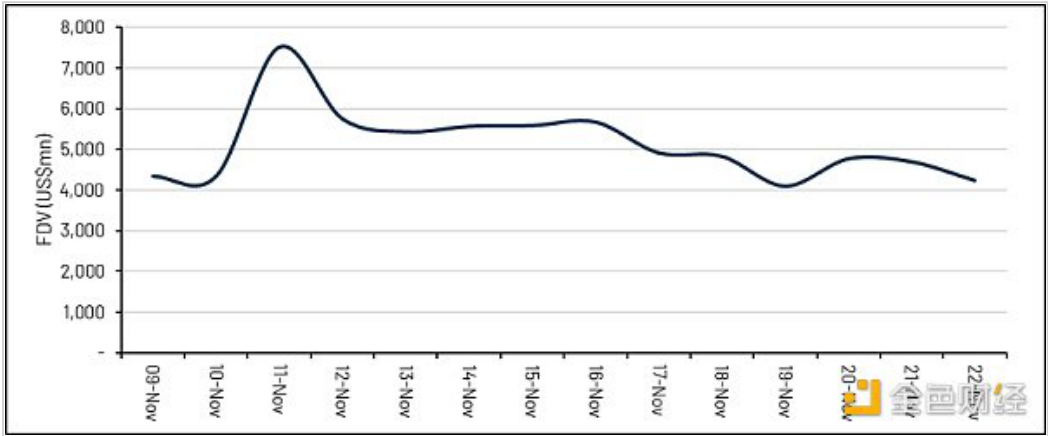
ENS每笔交易收入



资料来源：Dune Analytics (@makoto)

在触及约84亿美元的日内高点后，ENS的完全稀释市值目前为42亿美元，这意味着过去12个月的市盈率为236倍。

ENS市值（完全稀释）



来源：CoinGecko

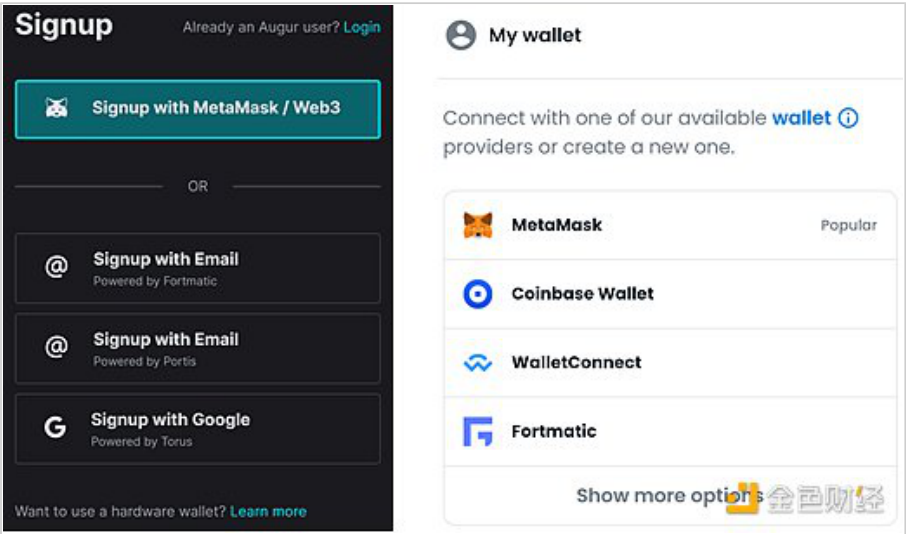
Metamask——区块链应用程序的网关

在新的技术范式中，用户交互最频繁的解决方案往往对行业的未来发展有着巨大的影响。类似于浏览器是Web1（Netscape、Internet Explorer、Google Chrome）和Web2应用程序（Facebook、Instagram、Netflix、Spotify）的战场，钱包很可能成为Web3的战场。

如果你曾经与Web3应用程序进行过交互，那么你很可能使用过Metamask。Metamask由 ConsenSys于2016年推出，是一种非托管加密货币钱包，允许用户与以太坊区块链和任何与以太坊兼容的网络（例如，Polygon、Arbitrum、Avalanche）进行交互。


尽管并非严格专注于去中心化身份，Metamask作为事实上的应用程序，每月有超过2100万活跃用户访问其以太坊地址。并行Web2单点登录 (SSO) 选项，几乎所有与EVM兼容的Web3应用程序都将提供“使用Metamask登录”。

Augur（左）和 OpenSea（右） 的登陆选项



Metamask作为更广泛的DID解决方案可能是什么样子的强大模型，并突出了自我主权的承诺和危险。因为Metamask用户拥有自己的私钥，他们真正拥有钱包中的资产。无需信任第三方的安全性和托管。此外，用户可以将资产从一个应用程序无缝移动到另一个应用程序。例如，在SuperRare上购买的NFT可以很容易地在OpenSea上出售，从而限制了平台锁定并增强了便携性。客户体验也可以说得到了改善——用户无需处理复杂的注册程序和管理多个用户名/密码，只需连接他们的Metamask钱包即可尝试新应用程序。虽然看起来“连接钱包”看起来很支离破碎，重要的是，这些钱包基于同样的账户系统，你可以把其他web3账户导入这个钱包。

将帐户导入Metamask

 METAMASK

< Back

Import an account with seed phrase

Enter your secret twelve word phrase here to restore your vault.

Seed phrase

Paste seed phrase from clipboard


☐ Show seed phrase

New password (min 8 chars)

Confirm password

☐ I have read and agree to the [Terms of Use](#)

Import



然而，黑客和骗局比比皆是。Web3用户必须对其钱包的安全性保持高度警惕，以免他们失去对所有资产的控制。即使只是丢失钱包的种子短语也可能导致资金的永久损失。因此，一些用户可能仍然更愿意将帐户安全和管理委托给第三方托管人。

Metamask有望逐步过渡到去中心化治理。ConsenSys创始人Joseph Lubin最近表示，Metamask将在不久的将来推出代币。Metamask高级软件工程师Erik Marks表示，该项目“对让项目社区拥有的想法绝对持开放态度”，尽管该团队希望Metamask代币的用例具有吸引力。一些人推测，如果Metamask确实执行空投，使用Metamask交换功能将是主要决定因素。

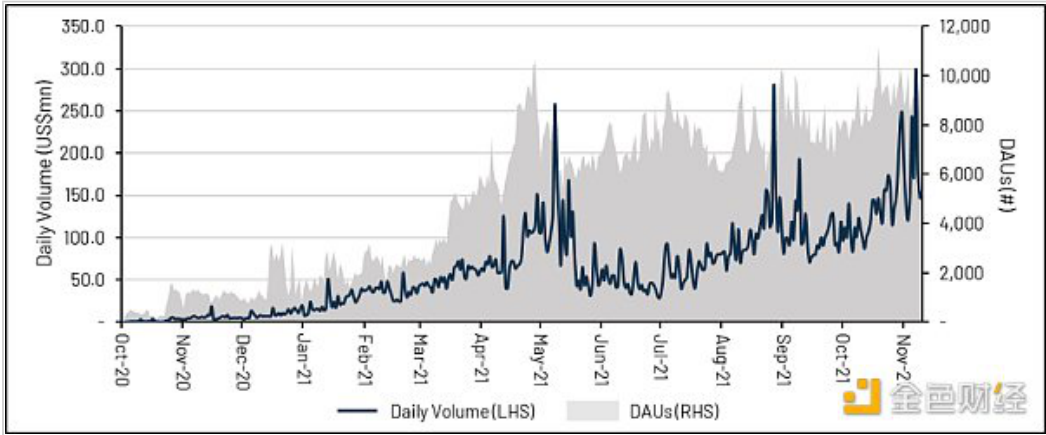
Consensys首席执行官关于Metamask代币



来源：推特 (@ethereumJoseph)

Metamask主要通过其嵌入的交换功能获利，该功能聚合来自去中心化交易所聚合器、做市商和DEX的数据，并增加0.85%的交换费用。自今年年初以来，Swap功能的采用率显著增加——Metamask上个月从交易中赚取了大约4000万美元的收益。

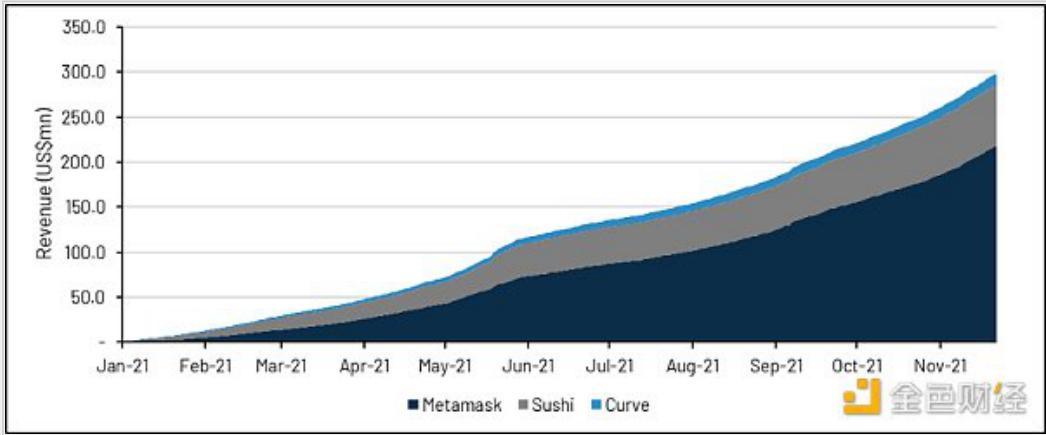
Metamask Swap在以太坊L1上的每日交易量和DAU



资料来源：Dune Analytics (@tomhschmidt)

事实上，Metamask Swap功能的收入增长大大超过Sushiswap和Curve收入的增长。

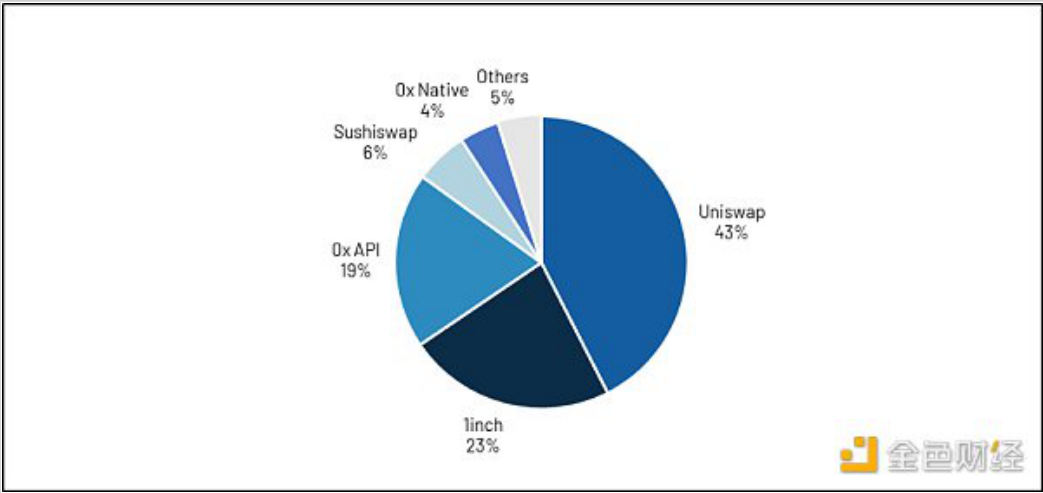
Metamask收入相对于DeFi协议收入



资料来源: Dune Analytics(@momir)

Uniswap和1inch, 分别是领先的以太坊DEX和DEX聚合器, 构成了Metamask流动性来源的大部分。

Metamask Swap的流动性来源



资料来源: Dune Analytics (@momir), 2021年11月21日

Metamask代币的潜在估值范围很广。股票估值没有直接可比性，但ConsenSys最近的股权融资（2亿美元，估值32亿美元）可以粗略估计Metamask代币的价值（之前Sky Mavis以30亿美元的估值融资，对应Axie代币市值40-50亿美元）。直接代币比较也表明市值范围很广。按每个 MAU 500至1,000美元算，潜在估值范围为105至210亿美元。

对ConsenSys的估值进行基准测试

Name	Ticker	Valuation (US\$mn)	MAUs (mn)	Valuation / MAUs
Equity				
Robinhood	HOOD	29,118.2	18.9	1,540.6
Coinbase	COIN	73,625.8	7.4	9,949.4
Square	SQ	110,000.0	40.0	2,750.0
PayPal	PYPL	253,397.2	361.0	701.9
Revolut	Private	33,000.0	3.3	10,000.0
Ledger	Private	1,500.0	1.5	1,000.0
ConsenSys	Private	3,200.0	21.0	152.4
Tokens				
xDEFI	XDEFI	313.8	0.1	5,230.8
Brave	BAT	1,636.0	5.0	327.2

资料来源: 公开文件、Capital IQ、CoinGecko、Amber Group估计

Ceramic

Ceramic是一个公共的、去中心化的数据网络，用于管理互联网上的动态和可变信息。它通过创建称为Ceramic流的灵活原语，使开发人员能够在没有数据库或服务器的情况下构建应用程序。

在Ceramic上，每条信息都表示为一个仅附加的提交日志，称为流。每个流都是一个存储在 IPLD中的有向无环图 (DAG)，具有称为StreamID的不可变名称和称为StreamState的可验证状态。流在概念上类似于Git树，每个流都可以被认为是它自己的区块链、账本或事件日志。Tile 文档是一种Ceramic StreamType，经常用作身份元数据（例如，个人资料、社交图、链接的社交帐户）、用户生成的内容（例如，博客文章、社交媒体）、DID 文档、可验证的凭据等。

该协议不依赖于任何特定的区块链。相反，它可以被概念化为“文档链”，其中验证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（例如比特币、以太坊）通常那样同步网络的整个状态。因此，没有文件的全局分布式账本。

Ceramic的关键工具之一是IDX，这是一种跨链身份协议，它提供了一个统一的存储库，所有应用程序都可以在其中注册和发现与用户DID关联的数据源。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，而不会被任何单个应用程序锁定，并且可以轻松跨应用程序保护和移植他们的数据。同时，它允许开发人员构建数据丰富的应用程序，而无需强迫用户在每个应用程序上重新创建相同的数据。

Ceramic是DID技术堆栈中的关键中间件。一些建立在Ceramic网络之上的项目已经看到了牵引力和市场契合度，包括：

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

RabbitHole：通过允许人们赚取积分和加密来鼓励人们使用Web3项目的应用程序。RabbitHole 使用Ceramic网络将多个Web2和Web3帐户链接成一个统一的、跨链的DID，并允许用户的声誉跨越其他Web3应用程序。

ArcX：一个去中心化的应用程序，通过颁发“DeFi 护照”来提供链上信用评分和身份。

结论

互联网可能是本世纪最重要的发明。在过去的二十年里，它改变了社会信息流的基本性质：媒体、政治、新闻、教育、社会互动等。然而，即使经济活动越来越多地从原子转移到字节，我们的在线身份仍然缺乏真实的所有权，并且在平台内保持孤立。

随着价值互联网的出现，将需要强大的DID解决方案，通过启用新用例来使Web3成为主流。我们仍处于早期阶段，但未来是光明的。并且由于DID标准的可组合性和互操作性，每个新应用程序产生的动力都会相互融合。我们预计DID解决方

案的突出地位将在未来几年内继续呈指数级增长，并开启Web3应用程序的下一个主要周期。

以上就是去中心化身份DID：Web3通行证的详细内容，更多关于区块链Web3通行证资料请关注脚本之家其它相关文章！

2021-03-18