

WEB3 INFRA SERIES

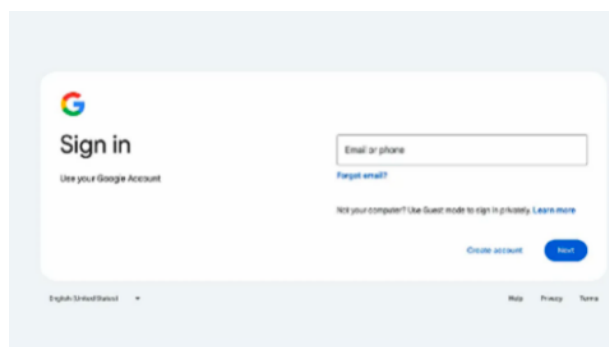
THE ROLE OF IDENTITY

IN WEB3 INFRASTRUCTURE

Web3 基础设施系列 | 身份在 Web3 基础设施中的作用

自互联网诞生以来，在线身份主要依赖于基于账户的体系，如电子邮件、用户名、密码及身份证号码等。这些机制本质上是一种“访问许可”的验证方式。

以谷歌账号为例，用户可以用其登录 Gmail、YouTube 或 Google Drive，但却无法直接在 Apple、Facebook 或政府服务中使用。这些身份标识符虽然曾是创新之举，但本质上是为封闭、孤立的系统设计的，难以跨平台迁移或互通。



今天，大多数用户依赖谷歌或苹果等平台来管理登录信息。然而，这种便利背后也隐藏着代价——这些平台掌控着用户身份的创建、数据的共享方式以及应用的访问权限。2018 年的“剑桥分析事件”揭示了这一体系的深层风险：

用户的身份信息、行为偏好乃至心理画像被平台未经授权地挖掘、打包并出售。这不是偶发漏洞，而是商业模式使然。

Web3 身份认证正是为解决这一结构性问题而提出的。它将身份控制权归还给用户，让凭证不再由平台集中保管，而由用户自主持有和管理。

Uptick 致力于打破平台锁定，基于模块化、跨链的基础设施，实现身份的可组合性与可移植性。不同于旧有体系造成的身份碎片化和访问壁垒，Web3 的可编程身份系统为身份的未来带来曙光。这不仅仅是数字护照的替代方案，或传统 KYC 的简单翻版，而是一个全新的、模块化的身份架构：它可在多个协议之间灵活调用用户角色、访问权限和凭证数据，且无需依赖中心化权威来协调。

这一转变彻底重塑了访问控制、合规机制及用户在多生态间的互动方式。在 Web3 世界中，身份不再是由平台发布和持有的资源，而是用户自己携带、掌控、并在不同场景中自主使用的主权资产。



2017年，Equifax 丢失了1.47亿人的数据，包括社保号码和财务记录，这深刻地提醒我们，

身份中心化以及摩擦会造成系统性风险。相比之下，去中心化身份则完全消除了单点故障。

要实现模块化的 Web3 技术栈正常运行，身份认证必须具备三大核心特性：可移植性、可验证性和隐私保护。这使得身份认证不仅仅是提

Decentralized identity is a programmable layer that defines how users move, what they can access, and how they're trusted.

供便利的前端功能或用户体验层，而是构成整个系统底层基础设施的关键组成部分。

更重要的是，身份认证不应只是帮助用户“登录”的工具，而应具备塑造系统运行逻辑和访问机制的能力，成为影响协议架构与生态协作方式的核心力量。

去中心化身份建立在三个核心组件之上：标识符、凭证和证明。

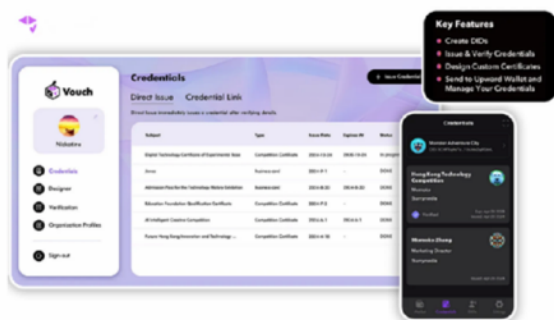
FROM STATIC PROFILES TO DYNAMIC CREDENTIALS

许多人仍然认为 Web3 身份是重新包装的 KYC，但它的真正价值在于其灵活性和支持它的分层基础设施。去中心化标识符充当凭证、属性和证明的主权容器，这些凭证、属性和证明可以在链上和链下进行颁发、更新或撤销。其底层是 DID，它是身份的持久锚点。

除此之外，还有可验证的凭证，例如年龄、认证、会员资格或资格。这些凭证可以由机构、



DAO、应用程序或其他用户颁发，用于证明身份或资格，而无需泄露不必要的数据。



除此之外，还有证明，它们验证了这些说法，但不会泄露底层数据。



这种分层模型赋予身份识别巨大的灵活性，使其能够适应各种用例，从内容访问和活动票务到借贷、治理和企业集成。因此，它更侧重于构建一个适应不同情境的系统，而不是普通的全局登录。它应该支持可组合性，并且能够在无许可和受监管的环境中运行。

This is what makes programmable trust possible.



Uptick 的 DID 系统符合 W3C 标准，并基于 Privado 的 Iden3。Iden3 的设计充分考虑了可移植性，允许用户跨平台携带已验证的属性，例如年龄、居住地或贡献者身份，而无需暴露个人数据，同时还能适应他们所交互的应用程序或资产的逻辑。

此类凭证已可直接使用 Uptick 的实时 DID 和可验证凭证平台 Vouch 进行颁发和管理。Vouch 负责处理从 DID 创建到凭证设计和颁发的所有流程，并支持基于 DID 的直接分发和通过二维码获取可认领链接。Vouch 还支持撤销和到期功能，允许凭证随着用户角色或条件的变化而调整。

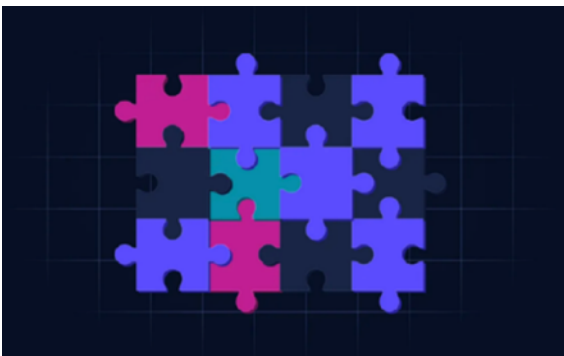


与传统的 Web2 模型相比，像 Vouch 这样的平台将身份从完全固定的状态转变为模块化、可动态调整的状态。用户无需在每个应用程序中都重新开始，而是可以随身携带自己的身份。

Composability is the core concept.

发行者决定共享什么、何时共享以及与谁共享。一个凭证可能用于证明资产的年龄，而另一个凭证可能用于解锁对私人 NFT 代币的访问权限，又一个凭证可能用于确认 DAO 成员资格。

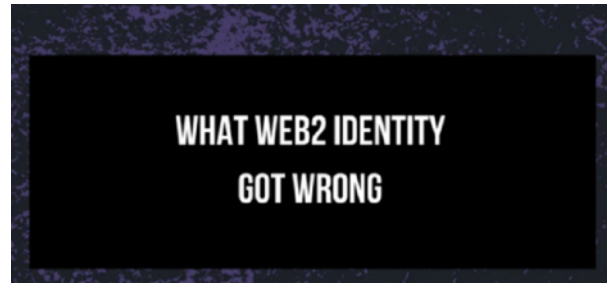
每个凭证都与具体情境相关，并会随着用户与资产状况、应用程序权限或治理逻辑的交互而演变。



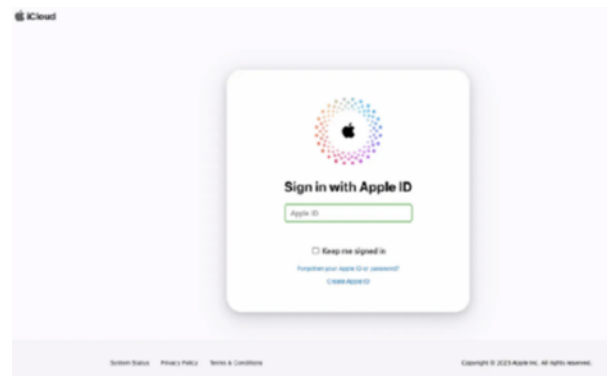
身份并非单一的档案，而是由一些可以协同运作的更小部分组成。

DID、凭证和证明各自服务于一个角色，它们可以单独发布、选择性地公开，并在需要时组合使用。这解锁了广泛的用例，从社交声誉、合规逻辑、链上凭证到基于角色的访问，所有这些都依赖于相同的基础架构。

身份成为用户和应用程序之间的连接层，为交互添加上下文，并帮助系统识别行为，而不是依赖于基本的访问控制。本质上，与可验证身份相关的交互越多，网络就越有用，互操作性就越强。



在 Web2 中，身份与账户绑定，并由平台控制。你使用谷歌、Facebook 或电子邮件登录，平台保存你的数据，设置权限，并最终决定结果。这在封闭的环境中行得通，但在依赖共享上下文和分布式信任的生态系统中却无法扩展。

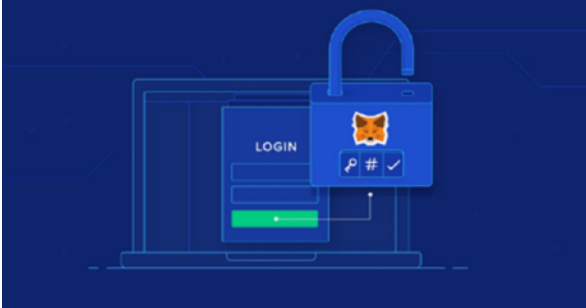


这种模式意味着用户每次使用新应用时都必须重新建立信任。每个平台都构建了自己的“孤岛”，彼此之间无法关联身份或历史记录，因此每次用户迁移，信任都会重置。这使其变成了一项商业资产，而不是用户效用，而且由于数据无法随用户迁移，因此也会降低速度。

Web3 infrastructure can't just copy the same model.

正如我们在本文开头所言，身份应该是模块化、可移植且可验证的，无需依赖中间层，并且应该与无需许可的访问、透明度和用户控制保持一致。

简单地在链上重建登录系统 错失了重点。否则，我们最终会遇到同样的问题，只是采用更炫酷的 Web3 格式。



去中心化身份颠覆了这种结构，因为用户管理其凭证，应用程序验证凭证，但实际上并不存储凭证，从而随着时间的推移建立起可信的交互。声誉可以跨越生态系统，而无需锁定于单一提供商，身份成为堆栈的一部分，而不是顶层服务。

在钱包集成、访问流程或登录方法方面，身份通常被视为前端关注点，但身份在堆栈中的位置更深，支持资产级权限、基于角色的治理、委托授权和声誉加权逻辑。

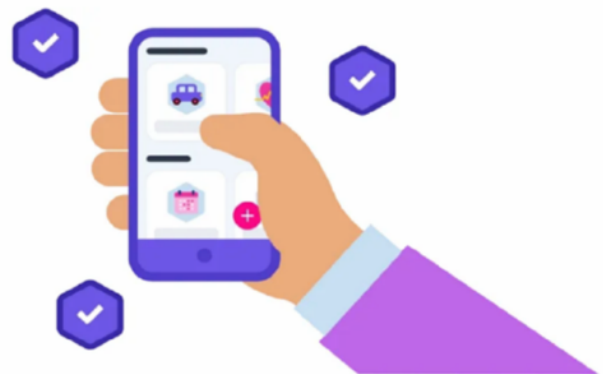
这定义了谁可以在什么条件下采取行动，以及为什么允许采取行动。去中心化身份允许智能合约在不依赖中心化监管的情况下强制执行合规性，从而无需存储用户数据即可访问代币。它还将现实世界的凭证与数字交互连接起来，而不会破坏隐私或去中心化。这样，身份就成为了在运行时强制执行逻辑的可编程系统的基础层。



Uptick 在协议层面集成了 DID 模块，这意味着身份是核心基础设施的一部分，每个身份都被设计为直接与资产逻辑、许可系统和应用层连接，因此它被视为一个经过深思熟虑的设计组件。

每个 DID 都锚定了一组可验证的凭证，这些凭证可以定义资产访问权限、触发合规性检查或支持跨应用程序的声誉系统。这样，我们就能够在资产层面强制执行凭证规则，例如，某种代币可能需要居住证明，而另一种代币可能只允许经过验证的贡献者访问。

每种资产都可以定义自己的条件，并在交互时根据具体情况应用，从而避免瓶颈，并允许在不影响整体灵活性的情况下进行许可。



RWA 可能需要居住证明，而另一个可能需要投资者认证，或者 DAO 投票可能仅限于经过验证的贡献者。特定于资产的规则提供了精确度，但不会造成中心化的瓶颈。

这些是模块化的凭证检查，应用于交互点。Uptick 的 DID 结构旨在充当一个权限层，在整个资产生命周期中随资产一起移动。可验证的凭证始终保持关联，因此所有权和资格可以在任何地方进行检查，无需中心化协调或重置。

凭借跨链功能和内置的零知识证明支持，允许用户在不泄露个人数据的情况下验证声明，这种基础设施设计实现了身份可移植性，无需锁定，也无需监控即可实现合规性。



声誉是身份的长期体现，它反映了赋予身份权重的行动、验证和关系。在荷马史诗传统中，这被称为 kleos，即通过行为而非头衔赢得的荣耀。

从某种意义上说，Web3 建立在同样的理念之上，将行为转化为系统能够识别的持久信号。Web3 声誉正在开始取代信用评分、信任评级和静态用户资料，而无需中心化存储或固定身份，从而实现通过参与而增长的分布式信任。这也为信用委托、DAO 治理和创建者激励开辟了新的模式，人们可以拥有贡献者徽章、已验

证的交付历史记录或一系列凭证，这些凭证可以塑造用户与系统的交互方式。

Access, risk levels, and voting power can all adjust dynamically based on reputation inputs.

声誉还能提供抗女巫攻击的能力，而无需实名，因为它允许系统根据行为而不是身份披露来评估用户，这对于任何希望保持无需许可的开放网络来说都至关重要，因为它可以过滤掉垃圾邮件和欺诈行为，使信任变得与环境相关，是赢得的，而不是被赋予的。



REPUTATION

Uptick 正在构建一个模型，其中声誉作为一个可移植、可验证的层存在，通过参与获得，并在应用程序逻辑中与资产层和身份层一起直接引用。去中心化客户关系管理 (DCRM) 可以追踪已验证的操作、贡献历史记录和情境反馈，而无需在中心化服务中聚合用户数据，因此应用程序无需个人信息或永久标识符即可识别行为。

这意味着每个操作都可以为更广泛的用户画像做出贡献，而无需中心化实体进行聚合。

PRIVACY ISN'T OPTIONAL

一个有效的身份识别系统应该优先考虑隐私。这并不意味着隐藏所有信息，而只是意味着让用户自主决定何时披露哪些信息。当凭证包含法律地位、病史或财务信息等方面时，这一点尤为重要，因为这些数据一旦泄露，可能会被滥用。

Without privacy, composability loses its value.

零知识证明在协议层面强制执行，允许用户在不泄露底层数据的情况下证明自身资格。选择性披露是指在不完全访问的情况下进行部分验证，而加密的元数据即使在公共网络上使用也能确保凭证的私密性。

这为可编程信任构建了一个安全的基础，让用户可以控制显示的内容、时间和对象。资格取代身份，因此您无需姓名或护照号码即可铸造代币或在 DAO 中投票，只需证明满足条件即可。

这就是去中心化身份的魅力所在，无需暴露即可进行验证。



隐私保护身份是实现受监管的 DeFi、企业治理和机构资产发行的关键。如果没有它，Web3 将会受到很大限制，甚至倒退到中心化。然而，有了它，所有类型的用户和用例都可以存在于链上并跨境运行。

Uptick 的凭证平台 Vouch 支持选择性披露、过期和撤销，确保凭证在各个系统之间可用且相关。作为其持续发展路线图的一部分，它还支持零知识证明发行路径。这使得凭证持有者可以在与 dApp、DAO 或资产系统交互时选择性地披露数据，所有这些都通过一个锚定在 Uptick 基础设施上的 DID 进行，然后方便地存储在 Upward 钱包中。

本质上，它充当一个安全凭证库，并在 dApp 或 DAO 使用期间提供基于 ZK 的交互接口。

THE ROLE OF IDENTITY IN A MODULAR WEB3 STACK

有人可能会认为去中心化身份只是用户的一个基本概念，但它实际上是一个系统级组件，在模块化的 Web3 堆栈中，身份是将一切连接在一起的关键。

Decentralized identity allows open systems to apply rules.

访问控制、资产管理、合规性、治理和社区参与都依赖于它。身份连接模块、产品和生态系统，赋予系统上下文、连续性和精确性。

这为用户提供了跨应用程序的一致性，开发者可以定义权限逻辑而无需设置障碍。机构可以在不损失监管清晰度或可用性的情况下进入 Web3，因此，身份使结构化参与成为可能，而无需为每个应用程序建立新的信任模型。



Uptick 将身份视为核心基础设施组件，与资产生命周期引擎、数据服务和治理模块协同工作。身份赋予资产意义，资产定义交互，数据连接两者。当这些部分可组合时，基础设施将变得更加适应性，这使其能够支持。

WHERE THE IDENTITY LAYER IS HEADED

身份正在从基于账户的系统转向可验证、可组合的凭证。随着这种转变，信任源于行为而非平台分配，交互也变得具有情境性、默认私密性，并且跨网络兼容。身份将与代币、钱包和数据馈送并列，成为 Web3 堆栈的核心层。这种转变改变了开发者处理访问控制的方式，因此他们无需为每个新应用重建身份逻辑，而是可以使用随用户移动的凭证，直接在资产或应用级别定义权限规则。然而，支持这种模型需要将身份视为堆栈一部分的基础设施。

Uptick 提供了这一基础，因为该协议包含一个去中心化身份 (DID) 系统、模块化凭证逻辑，以及对基于零知识的验证的内置支持，所有这些都与资产逻辑、访问控制和治理模块集成在一起。Uptick 的身份系统支持选择性披露，而像 Vouch 这样的平台（已集成在 Uptick 堆栈中）允许这些凭证一次性签发并跨不同系统使用，从而使开发人员无需直接管理用户数据即可执行权限规则。凭证能够在不暴露底层数据的情况下证明资格，并且由于零知识支持是该架构的一部分，用户可以在不泄露个人信息的情况下满足条件。这使得从隐私投票、受监管的资产访问到开放系统内的合规性检查等各种应用成为可能。前路漫漫，但随着身份不断发展，它正在成为定义跨网络系统的信任、访问和协调的基础层，它在设计上是可编程和可移植的，并且旨在将控制权掌握在用户手中。



hello@uptickproject.com



[@Uptickproject](https://twitter.com/Uptickproject)



[@Uptickproject](https://t.me/Uptickproject)



[Uptick Network](https://discord.com/invite/UptickNetwork)



[Uptick Network](https://www.youtube.com/UptickNetwork)