IDHub 白皮书

— 基于开放原则与主流区块链技术的去中心化数字身份应用平台 —

（V0.3.0 2017 年 8 月 18 日）

摘要

数字身份是每个人走进数字生活的钥匙，影响着社会运转和经济运行。然而数字身份的碎片化不利于用户管理自己的身份，主流的身份集中管理的手段需要完全信赖服务商的能力和自律。本文提出一种基于区块链的数字身份应用平台 ——IDHub，帮助用户们和身份验证者之间建立用户自主、去中心化的身份管理和统一、安全的身份验证机制。经过长期积累， IDHub 将成为每个用户“数字化永生”的数据燃料。

数字身份的业务模型以身份连接为核心，定义了完成真实身份与虚拟身份的连接的五种角色，同时分析经济激励及代币流转条件。数字身份的技术模型依据去中心化的思想，讨论了 IDHub 的最小实现单元的技术架构，以及与主流身份集中管理的差异和技术特点。IDHub 的应用场景广阔，如替代现有网站登录方式；公民权利相关的身份认证；可对接物联网、人工智能等新兴产业；未来，源于区块链的数字身份 IDHub 有机会成为区块链领域的公共身份平台。

IDHub 生态系统的构建是一个循序渐进的过程，本文重点分析了各个角色的利益，IDHub 的出现顺应各方需求。从整体上看，用户为中心的身份符合社会发展的方向，将推动信用社会科学地发展；从微观角度来看，用户将成为生态系统的最直接获益者；通过抑制用户数据的非法交易，各参与角色都能得到相应的收益。

1. 背景

1.1 引言

随着信息技术的发展，数字身份已经融入到社会发展的肌理，深刻改变着传统的社会运转、经济运行模式以及人们的生活形态。如今，数字身份已在各个场景得到广泛应用，比如个人信用贷款、网络支付交易、公共服务授权或使用数字化手段签署合同等。但数字身份碎片化、分散化的特点以及对有效性、真实性、唯一性的合理验证，为其应用和管理带来挑战。

数字身份由个人在社会活动中的全部身份碎片信息集合而成，涉及行为、财产、信用、声誉、隐私等相关信息，是宝贵的个人数字资产。数字身份的隐私和安全性是数字社会健康发展的前提。遗憾的是，随着数字身份的信息碎片被发送到政府、银行、电信、保险公司、中介等组织或个人手中，这些信息不仅比以往任何时候都更容易受到泄露风险，同时由黑客主动攻击演变成为的系统性风险也正在增大。2016 年，全球共发生 1800 起数据泄露事件，导致近 14 亿条个人数据记录外泄。在这些事件中，有 68%是由外部的恶意黑客发起，其中 19%被归为意外泄露，9%则由恶意内部人员造成。

数字身份在各服务提供商之间分散且孤立，缺乏一致性，用户办理不同服

务需要重复注册用户名和密码以及相同身份信息。但人们通常习惯以相同密码在多个网站注册，使得安全问题突显。此外，还会遭遇身份盗用、身份欺诈等问题。

鉴于身份信息的广泛分布和敏感性，公私钥非对称加密技术、ECDSA 签名算法和分布式总账技术（例如区块链）为上述问题提供了最佳解决方案。这些技术将身份所有权由集中式服务向前推至个人，使身份控制权回到个人手中，通常被称为“自主身份”。这种方法藉由分布式数据与计算，将其推到前沿，成为创建数字身份的最优选择。

至今，全球已有爱沙尼亚 e-Residence、新西兰 RealMe、瑞士 Swiss ID 以及英国、澳大利亚等国相继开展数字身份项目的探索与应用。数字身份已在全球政府部门、商业机构、社会组织以及个人用户之间形成共识。

1.2 区块链

区块链是基于分布式数据存储、点对点传输、共识机制、加密算法等技术的全新可信生态系统，是当今信息科技领域最具革命性的新兴技术之一。它通过网络中多个节点共同记账的方式，把数据（区块）按照时间顺序进行串联（链），形成时间顺序上可追溯，且不可篡改的交易记录。

区块链的核心价值在于实现不可篡改、安全可靠的分布式记账系统。基于密码学、分布式共识协议、点对点网络通信和智能合约等技术保障，使用区块链账本系统的多个参与者，无需额外的第三方担保机构，即可构成多方交易的信任基础。进而实现低成本、低延迟的信息交换和交易处理，实现数字价值的高效流通。

当数字身份遇上区块链，碎片化的数字身份有了以用户为中心的集中管理渠道，使身份数据的真实性、唯一性和有效性得到保障。同时规避服务提供商对身份数据进行垄断、监视或滥用权力的潜在风险。由于数字身份保存在区块链上，即使服务提供商决定停止服务，用户仍然可以有效保存身份，保证了数字身份的连续性。

1.3 智能合约

1995 年，密码学家尼克·萨博（Nick Szabo）首次提出“智能合约”概念，是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。自比特币诞生后，人们意识到比特币的底层技术区块链天生可以为智能合约提供可信的执行环境。

智能合约有效消除第三方供应商，合约验证和执行的整个过程将随用户间的直接交易而变得快速。合约保存在分布式账本上时，不存在放错或丢失的风险，连接到网络的每一个身份数据都有一份合约副本，所有数据都公平地运行在每一个验证节点上，从数据结构和算法上保证没有人可以篡改数据和作弊获利。同时，通过自动执行的智能合约，IDHub 可以去掉中间环节，最大限度降低用户隐私数据泄露的风险。

1.4 IDHub 概要介绍

IDHub 是建立在开放原则之上，基于区块链技术的去中心化数字身份应用平台，具备良好的技术兼容性与功能拓展性。

IDHub 的使命是:

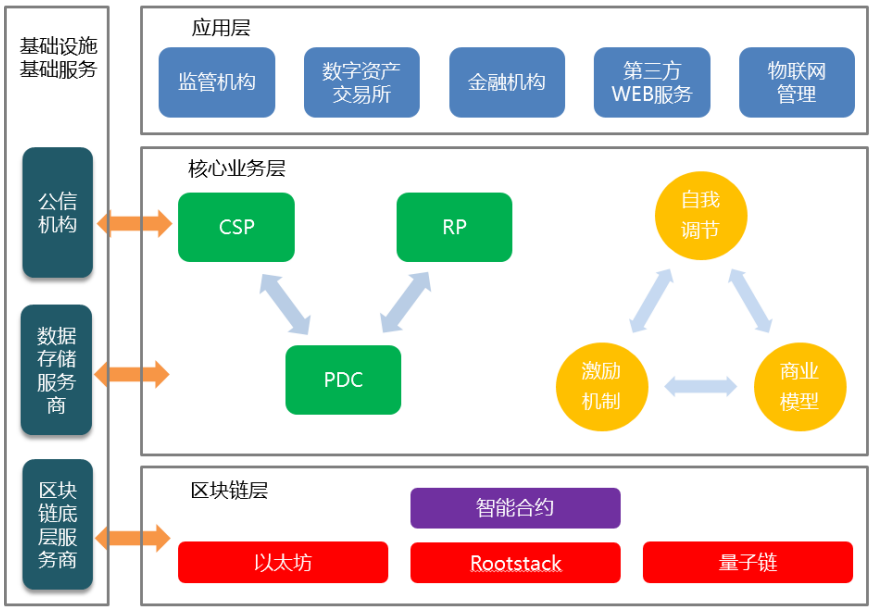
1）搭建面向数字经济的可信生态体系。随着“去中心化”运动和区块链技术的发展，用户将享有更多个人数据和更大的身份控制权。但个人掌握的数据可信度较低，IDHub 通过盘活权威机构已有的数据为个人数据资产背书，打造快捷、有效的信任体系，促进基于数字资产的可信生态体系建设，最终实现数字经济的繁荣。

2）取代传统账户体系，打造进入数字社会的标准身份接口。每个人所管理的账户数量在迅速扩张，但账户信息和内容却被电信、银行等服务提供商所管理和控制，切换起来十分困难。因此，在以用户为中心的数字社会中，账户与应用分离成为必然趋势。IDHub 通过创建标准身份接口的形式对账户与应用进行分离，用户自主管理数字资产，可以便捷地变现数字资产或更换服务提供商。

3）为边缘人工智能（Edge AI）提供数据燃料，为“数字化永生”创造基础。IDHub 将可信数据放置于用户的个人数据中心（PDC）中，为每个人创建数字版的“对应体”，向建立在 PDC 上的 Edge AI 提供最真实和原始的数据燃料。

2. IDHub 业务模型

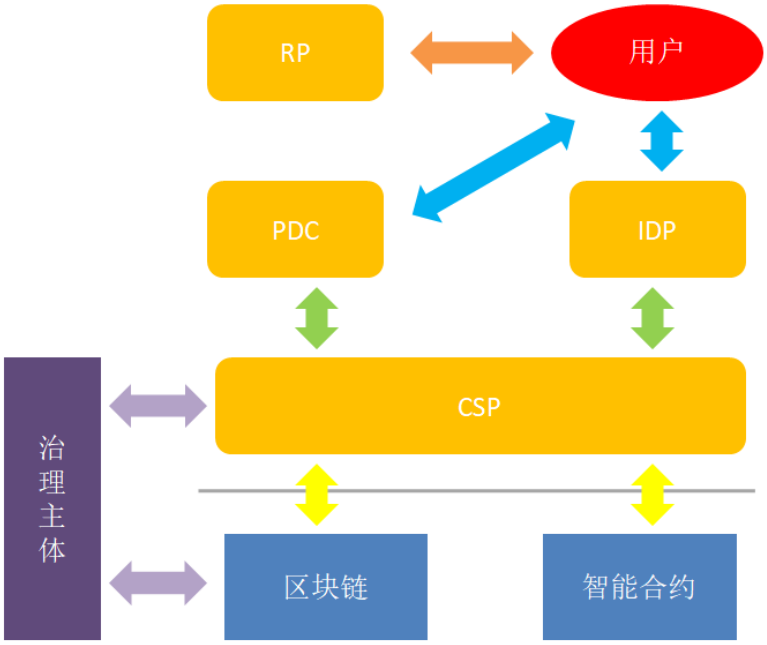
2.1 业务模型总体框架



IDHub 数字身份应用平台旨在建立去中心化的数字身份统一标准接口，成为具有真实性保障的身份信息管理系统。依靠底层区块链和智能合约服务，核心业务层可以解决数据真实有效、交互、存储、隐私等关键问题，并伴随扩展机制发展生态系统。随着扩展机制逐渐完善，个人或组织都可以参与到生态系

统建设当中，通过提供基础设施、基础服务或各种上层应用来获得激励或利润，实现基于 ID as a Service（IDaaS）的、完备的可信生态，极大提升数字身份在社会流转中的价值，成为信用效能的放大器。

2.2 IDHub 关键角色定义



IDHub 系统中的关键角色有：User、Identity Provider(IDP)、Relying Party(RP)、Governance Body(GB)、Personal Data Center(PDC)。

1）User： 拥有唯一身份标识的个人或组织，拥有 IDHub 身份信息自主权。

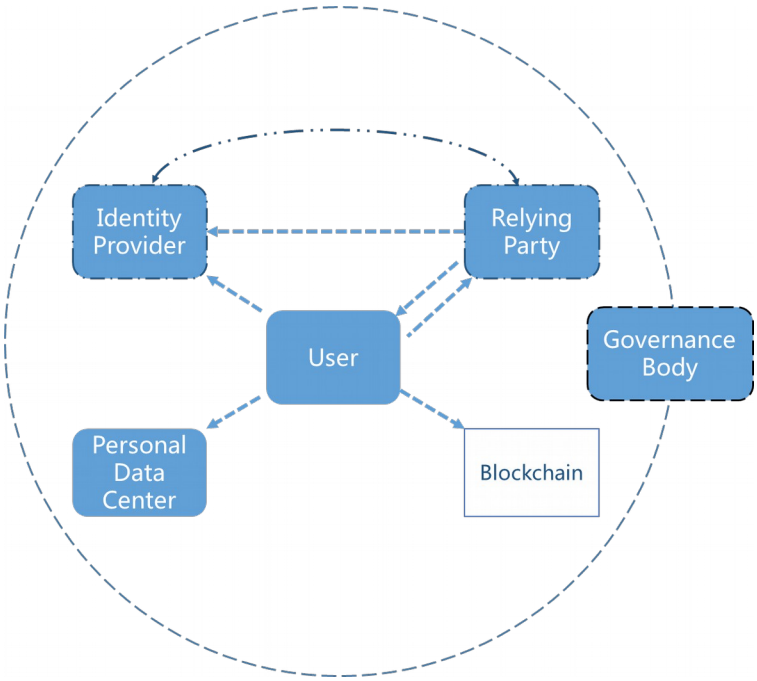
2）Identity Provider： 掌握用户数据的传统中心化服务商，在某种意义上可以提供真实、准确和完整的用户数据，可以为用户身份信息提供权威背书，来获得一定激励。

3）Relying Party： 提供应用层服务并接受 IDP 对于用户身份的背书，允许用户享受他们所提供的服务以获得利益。

4）Personal Data Center： 提供可信赖的用户数据存储服务和基于用户

5）Governance Body： 治理主体提供系统的监督，维护自我调节机制，对其他角色的商业模型和激励机制具有一定影响力。

2.3 信息和代币的流转机制



我们相信 IDHub 应用层和业务层之间的代币流转会自动形成一个均衡局面，但是区块链层的资源消耗需要代币，同时核心业务层需要一个良好的代币流转机制来保证用户身份的真实和安全。因此，以下代币流转规则是非常重要且必须的:

1）用户应该支付代币给 IDP 获得后者对用户的背书。

2）RP 应该支付代币给用户来获得用户的数据；当数据的真实性较重要时，RP 应同时支付代币给用户和 IDP 获得有背书的用户数据。

3）用户可以依靠代币获得 RP 所提供的各种服务。

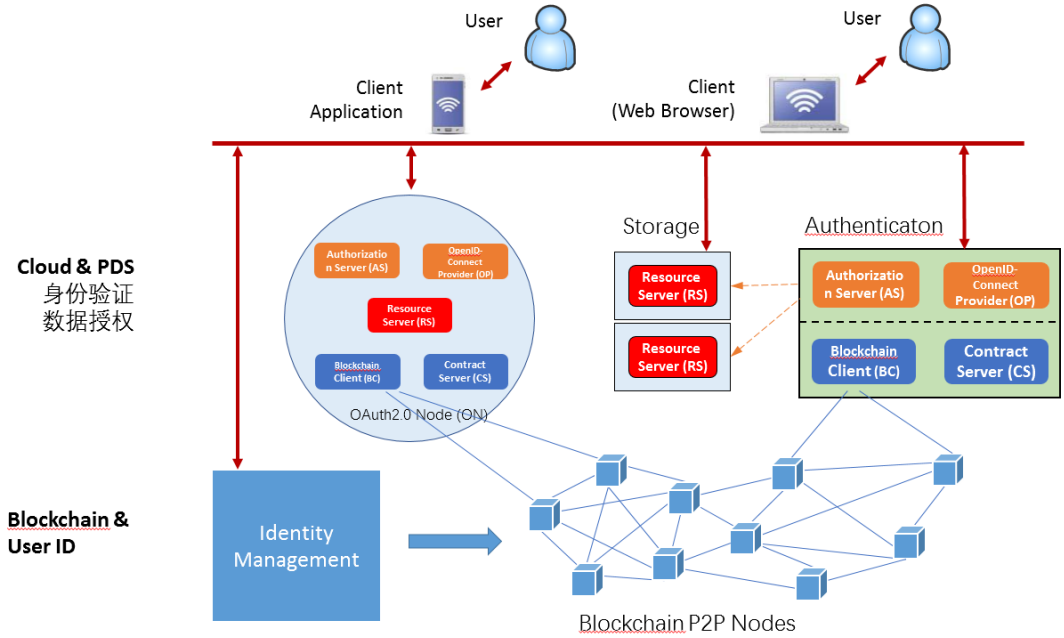
4）若有需要，用户将支付代币给 PDC 获得数据托管服务。

5）当用户与 IDP 达成一致意愿，将数据分享在区块链上获得不可篡改的属性时，用户应为数据上链所产生的费用买单。

6）RP 与 IDP 有时角色可以互相转换，如支付宝即拥有用户数据，又有强烈的意愿获得更多场景下的用户信用，从而得出更精准的用户信用评分。

3. IDHub 技术模型

3.1 技术架构



IDHub 利用智能合约技术搭建出数字身份应用平台。从架构上，可以分为：区块链底层和平台层。

3.1.1 区块链底层

IDHub 是建立在开放原则之上，基于区块链底层技术的去中心化数字身份应用平台，具备良好的技术兼容性与功能拓展性。在平台支持上，IDHub 将会同时支持多种主流区块链底层技术，如 Ethereum、Rootstock、Qtum 等。最终，IDHub 将根据开发社区自主选择的结果，重点支持特定的底层链。

目前各种区块链底层都不够完善，如以太坊在交易量陡增的状况下网络几乎瘫痪、Rootstock 采用的双向侧链技术因算力不均容易遭到 51%攻击、量子链仍处于前期测试阶段等。从长远来看，我们相信随着区块链的跨链交互技术逐渐成熟，数字身份作为用户进入数字社会的入口，有必要走向专用于身份管理的区块链。IDHub 在区块链技术成熟时将迁移至具有跨链功能的数字身份专用子链上。

3.1.2 平台层

除具备入口的功能外，IDHub 还是一个可以提供身份服务的平台。IDHub 底层由区块链节点构成 P2P 网络，每个节点在网络中都能向平台层提供服务。平台层包括相互独立的用户身份管理功能模块和用户身份验证功能模块。身份管理完全由用户自主控制，身份验证由网站自由选择验证形式。

用户身份管理

用户通过身份管理模块能够轻松自主地管理身份，包括：创建、恢复、角色管理等。

创建身份：用户通过智能合约创建数字身份，支付一定费用给矿工，即可获得一个全球唯一且永久的标识符，即 IDHub 数字身份。

恢复身份：用户在创建身份的同时，可以设置一种或多种恢复身份的方式，

当用户私钥遗失时，可以用创建时预设的方式恢复身份。

角色管理：用户在不同平台可以选择不同的访问角色，平台只记录该角色的行为信息。

用户身份验证

IDHub 平台层是建立在区块链节点之上的服务。平台层通过 Contract Server 能够访问用户记录在区块链上的公开数据信息，以及更换公私钥的完整记录。通过用户的公钥平台可以校验用户的签名信息，以确定用户的身份，实现用户登录、授权等操作。

平台层的使用形式有两种：自建服务节点和依赖中立验证服务。

自建服务节点是指：有实力的公司能搭建完整的身份验证节点，并使用自建的验证服务为用户的登录提供保障。

依赖中立验证服务是指：由中立验证服务技术的平台提供身份验证服务，信赖该提供者的其他网站可以通过公开的认证授权协议以较低的成本使用身份验证服务。

3.1.3 名词定义

OAuth2.0 Node(ON)：以用户为中心管理数据的完整单元。包括：Authorization Server（AS）、OpenID-Connect Provider（OP）、Resource Server（RS）、Blockchain Client（BC）和 Contract Server（CS）。

Authorization Server（AS）：保护 RS 中的资源由用户行为所控制的服务器。

OpenID-Connect Provider（OP）：实现请求方和用户客户端的身份认证。对于用户客户端而言，它通过用以证明所有权的对称密钥或非对称密钥对执行认证。

Blockchain Client（BC）：区块链的完整节点。

Contract Server（CS）：管理智能合约和执行智能合约结果的模块。

Resource Server（RS）：以用户为中心管理用户资源，保护数据，并能够响应数据分享请求的服务器。

Identity Management（IM）：任何人都可以搭建的数字身份管理模块，实现用户数字身份的注册、公开信息修改、身份恢复等功能。

3.2 IDHub 与身份验证中心比较

身份验证服务因跨企业的用户具有核实身份的需求而产生，并逐渐规范形成标准协议，如 OAuth。目前最常见的应用场景是授权登录，如用微信、微博、facebook。验证中心的好处是：可以跨平台访问，将原本分散的账号集中到少数的验证中心上。

然而，这种验证模式本质上是提供服务的网站放弃对用户的身份验证，完全信任中心化服务的验证结果。验证中心获得越多网站信任，就越有可能成为黑客们攻击的焦点。

IDHub 数字身份平台将验证中心原本的用户身份管理迁移到区块链上，利

用非对称密钥保护用户私钥，同时各网站可架设验证服务校验用户身份。IDHub 不仅具备验证中心的优点，同时具备区块链的分布式、以用户为中心的特点，使得:

1、避免造成用户数据垄断，用户身份不会被少数 ID Provider 恶意控制。

2、用户连接服务商接口一致，可以提高服务商对接 IDHub 的开发效能，同时便于服务商对接更多第三方平台。

3、身份认证信息在区块链上可被校验，保证结果不被篡改。

3.3 产品特点

3.3.1 智能合约定义数字身份

IDHub 是运行在区块链上，由用户进行自主控制，通过智能合约定义的去中心化应用(DApp)。IDHub 数字身份具备更高的身份自主权，创建者对身份信息具有完全的控制和主导权，并且不依赖集中式的第三方进行创建或验证。

3.3.2 多类型身份合约

IDHub 身份可以支持多种形式，包括: 个人、设备、实体或机构，提供多类型的身份合约，以满足不同形式的身份需求。个人的身份由合约的创建者完整控制，设备的身份会被指定的个人或实体进行管理。

3.3.3 数字身份的链下认证方法

IDHub 不仅支持身份与区块链进行互动，控制数字资产的流转，参与区块链上投票，而且通过我们自主设计的认证方法实现链上身份与链下数据的连接。用户在区块链上的身份是以合约地址作为标识，链下的身份通过密钥的方式进行标识。我们通过智能合约将链上与链下的身份自动关联，实现身份的一致，让数字身份的使用更加灵活。

3.3.4 OAuth2.0 Node 设计框架

OAuth2.0 Node 是由 T. Hardjono 教授提出的，是以用户为中心的、用于用户管理数据的完整单元。IDHub 采用这套设计框架搭建数字身份的使用环境，满足用户可以自由选择: 1、分享数据给任何实体; 2、使用任意实体提供的数据分享服务。未来，用户能够通过智能合约开通或移除这些服务。

3.3.5 证书信息在区块链上可验证

数字证书是权威第三方对用户的行为或声明信息进行的证明，其他任何实体能够识别和验证这些材料。IDHub 数字证书通过将原信息单向加密后记录在区块链上，任何拿到数字证书原信息的个人不仅能够验证签名的真实性，还可以通过区块链上的记录确定获取证书发行的时间。采用这种做法，当发行机构的密钥失窃或机构注销时，依然能够保证数字证书有效性。

4. IDHub 数字身份平台的应用场景

4.1 公民权利

基于区块链技术的数字身份系统可以高效地保证用户信息的真实性、有效性、唯一性与复用性，这对于用户行使法律赋予的公民权利具有重要意义。

用数字身份系统为用户的固定资产信息、学历技能认证、纳税信息以及合法的行政权利等提供保障，IDHub 的代币经济模型能保证这些信息安全且高效地认证和使用。用户可以自由选择是否公开某一条信息、可以决定是否授权某条明文信息给第三方等，这些权利可以让用户放心的使用 IDHub，它为用户信息提供了很好的隐私性。

个人信息隐私性由用户完全做主，不过需要注意的一点是，信息的公开程度取决于用户和服务提供商（或第三方等）的双方意愿。

1）**固定资产认证**：省去诸多繁琐的手续与文件，IDHub 用密码学保证固定资产安全性和隐私性。

2）**纳税信息**：安装 IDHub 的手机应用程序可以自动控制与记录用户的税务信息，税务监管将会更加高效便捷。

3）**学历技能认证**：不用再担心证书剽窃，这一问题将从根源得到解决。想像一下，可能求职的时候，双方都不需要见面，IDHub 的身份信息足够说明一切。

4）**行政权利**：只需通过 IDHub 用户就可以随时随地的办理政府业务或者行使政治权利，同时还可以证明你的合法身份。

4.2 用户登录管理

除了进行具有现实价值的身份锚定，IDHub 也具有很好的匿名性和即时性。假设用户希望使用一次性的网络服务，比如网上点餐、匿名评论新闻等，他可以用 IDHub 的应用程序智能登录服务商网站而不需要注册。我们希望最终用户使用 IDHub 就可以满足全部互联网服务需求，而不需要注册和管理分散的服务商网站账号。

IDHub 会建立一种网络服务的生态系统。鉴于 IDHub 基于区块链技术，任何使用 IDHub 平台的服务商都处于平等地位，任何服务商都可以方便地接入 IDHub 平台或成为解决方案的一部分。由于 IDHub 的生态系统采用高安全性的验证技术，所以服务商可以放心地使用 IDHub 所提供的用户验证信息。

4.3 全球化信用凭证

区块链技术对于重塑金融交易和服务的重要性不言而喻，而身份和信誉则是重中之重。无论是用户还是金融机构，都希望有一套完全可信的信用和资产管理机制，而现行的 IDV 服务成本则显得过于高昂。

基于 IDHub 数字身份平台可以建立具备公信基础的信用管理机制，配合发展迅速的人工智能技术，对用户数据进行行为分析并将信用结果记录在不可篡改的区块链账本中。这样可以准确地评估或监管信用，一方面保障用户的信用由自己完全掌控，另一方面防止中心化作恶和用户信誉滥用等。

IDHub 可以帮助金融行业建立起全球可见信用管理账本，账本所记录的信用信息都经过安全加密而不用担心用户隐私泄露。阅读明文记录的权限取决于法律规定或用户授权，重要的是，大数据分析可以很好地帮助我们建立抽象的信用模型，而区块链可以保证信息绝对安全可靠。基于此，IDHub 可以将数字

身份与信用账本高度集成，也就是说，重要的信用就是用户身份的一部分。未来，IDHub 可以在数字货币交易、消费金融授信增信、国际支付与结算、票据与供应链金融、证券发行与交易、合规征信与反欺诈、保险索赔处理等金融场景实现高效、低成本的广泛应用。

1）**KYC**：在用户同意授权信息可读性的基础上，信用账本将极大降低金融行业的授信、征信、增信成本，且复用性极高。

2）**担保证明**：用户仅通过展示信用账本上的一条记录就可以获得巨大的担保价值。

4.4 新兴技术的身份支持

随着人工智能和物联网等新兴技术的蓬勃发展，个人隐私、个人数据和用网安全等带有明显身份特点的安全问题更加突显。通过IDHub 的可信身份基础，我们可以创建以人工智能或物联网技术主导的区块链应用来为我们的生活提供服务。

IDHub 的代币模型可以为这种多层应用提供经济化的帮助，这不仅可以帮助应用在区块链上的消耗，还可以使应用建立一套完整的规则以便激励、监管用户或者组织的参与行为。另一方面，身份信息的概念不仅适用于人类，新兴技术领域中的对象也会具有“身份”的概念。IDHub 中的身份信息加密、组织方式同样适用于它们。这种数据架构有助于新兴技术产品的智能化管理，IDHub 会为这些应用场景提供高度集成的区块链服务。

1）**智能家居**：IDHub 的应用程序可以很好的帮助用户管理属于自己的物联网产品，比如智能家居。重要的是，IDHub 可以有效阻止恶意攻击者盗用物联网产品。

2）**人工智能网络**：IDHub 会为人工智能网络带来设定一致、有效的设备注册、授权及完善的生命周期管理机制，有利于提高人工智能设备的用户体验和安全。

4.5 成为所有区块链的公共身份

比特币区块链的匿名性会带来很高的信任风险，而现实世界的业务必须建立在充分信任的基础之上，区块链的大规模应用需要数字身份为之提供信任基础。

IDHub 旨在建立去中心化完全可信的数字身份生态系统，任何个人、机构或者组织等都可以自由平等的参与进来。生态系统中的每个角色（不仅是个人）都拥有自己的区块链数字身份，这些数字身份将会给他们提供法律层面上的保障。生态系统中的每个成员都可以发挥自己的优势来获得激励，譬如分享个人信息、提供传统网络服务、底层区块链服务、信息托管服务和信息认证服务等，重要的是成员在IDHub 上的合法身份，还可以帮助其在现实中的业务开发相应的区块链应用来参与生态系统运行，IDHub 在这方面具有很好的兼容性。

从另一个角度来说，区块链的发展需要传统行业的支持。比如传统电信行业的巨大潜力：小型区块链可能提供不了绝对意义上的安全，公有区块链的安

全性能的保证需要巨大的算力支持，而且良好的通信网络会大幅提高区块链产品的用户体验。

事实上，任何 IDHub 生态系统中的成员都可以是 P2P 网络中的对等节点，这取决于成员的真实意愿。最重要的是，IDHub 会为成员提供极具价值的信任支持，并有完整且合理的激励、监管和惩罚机制。生态系统中的任何成员都可以放心使用或提供各种各样的区块链服务，IDHub 对此具有良好的扩展性。

5. IDHub 生态系统构建

5.1 社会价值

1）提升公民的信息安全和信用意识，规范公民行为

2）构建数字人生的完整档案

3）推进去信任的自治社会

5.2 参与方的利益

IDHub 生态系统包含五个核心角色：User、Identity Provider(IDP)、Relying Party(RP)、Governance Body(GB)、Personal Data Center(PDC)。

5.2.1 User 的利益

用户是使用 IDHub 生态系统的最核心的参与者和最直接的受益者，主要体现在隐私管理、身份安全和操作便利等方面。

隐私管理:

- 用户将可以完全控制由哪些 IDP 拥有其属性
- 在 IDP 将用户属性交给 RP 之前，需要经过用户同意
- 在业务处理过程中进行传输的将会是所需最少的用户信息量

身份安全:

- 用户属性（的操作）只能由符合系统信息处理及存储标准和要求的实体进行
- 数字属性存储将使身份信息抵御损坏，破坏或丢失的情况
- 用户将有能力分散其身份信息，当某个 IDP 遭受数据泄露、数据被清除或被盗的情况时创建应急方案，并减少数据泄漏对用户的影响

操作便利:

- 数字身份和数字属性传输将简化和改善交易中的用户体验，消除用户在交易过程中对于跟踪多种身份验证方法（例如用户名和密码）以及手动提交个人信息的需要
- 属性将以数字方式转移，消除人为错误和之后信息修复的可能性
- 用户将能够轻松地更新其 IdP 所持有的信息，并且不必处理基于不准确或过时信息执行的交易
- IDP 的利益
- 身份提供商管理着大量的用户数据，转型为去中心化身份提供商能在提升管理用户数据同时带来诸多好处。
- 收入的增长：IDP 可以完成 RP 的身份交易；这将允许他们通过每笔交易的费用或其他商业模式将身份服务转化为经济收入。

明确风险和责任: IDP 将明确他们在出现数据丢失或破坏，或违反身份规

定标准等情况时的责任。

强化定位: 鉴于他们对用户的了解及在信用方面建立起的地位，IDP 将能够与用户建立牢固的关系，并将自己定位为数字经济的关键部分。

产品和服务的改善:

- IDP 将增加对详细和可靠的用户信息的访问，以使他们能够更好地定制流程，产品和服务
- IDP 可以开始利用非标准用户属性来更好地管理和评估风险（例如健康记录）
- 安全的数字身份协议和数字属性传输将改善用户体验，并扩展 IDP 可以在线安全提供的服务数量

5.2.2 RP 的利益

依赖方使用 IDHub 获得用户授权，从不同的 IDP 处获得该用户的数据。IDHub 为 RP 带来了诸多好处，为更高质量的服务建立基础。

信息准确性:

- RP 可以访问与其产品或服务所要求的保证级别相匹配的经过验证的可信身份信息；这将消除对信息补救，以及通过收费的第三方服务进行信息交互检查的需求
- 数字属性交换将消除交易中人为错误的可能

服务定制: RP 可以通过请求访问超过完成传统交易需求的身份信息，为用户提供更多的定制产品和服务。

服务规定: 更可靠和准确的身份协议将使 RP 更有能力区分非法和合法用户，并相应地拒绝或提供服务。

减少交易中断: 更简化的用户体验将消除完成交易的障碍（例如，忘记登录信息，需要账户创建，拒收计费信息等），从而降低用户的交易中断率。

降低风险和责任: RP 将明确他们在出现数据丢失或破坏，或违反身份规定标准等情况时的责任。

5.2.3 PDC 的利益

个人数据中心通过 IDHub 为用户提供数据基础设施服务，从传统的以企业为中心的服务模式转型为以用户为中心的服务模式。

收入的增长: 用户基数大，数据管理的需求在迅速增加，未来将为 PDC 提供商带来可观的收入增长。

降低管理费用: 更简化用户开通 PDC 的服务流程，费用通过智能合约自动结算，将一定程度降低日常管理费用。

明确风险和责任: PDC 将明确他们在出现数据丢失或破坏，或违反身份规定标准等情况时的责任。

5.2.4 GB 的利益

治理主体并不能直接从生态系统中获得经济的收益，但更有秩序的数字身份系统，将带给治理主体监管效率的提升。

资产跟踪:

- 监管机构将能够更有效地追踪资产发起及其所有权，增加追踪犯罪活动轨迹的能力
- 可追溯资产重估，确保资产重估不会超过其总价值

实体的透明性视图: 监管机构可以访问跨层次的法律实体的综合视图，增

加其评估系统性风险和管理稳定性的能力。

提高合规性:

- 获得信任的身份信息将增加 FIs 在其管辖范围内符合反洗钱，KYC 和其他法规的能力
- 获得受法律实体和资产身份信任的信息将使 FIs 更准确地检测洗钱和其他可疑交易
- 访问可信的数字属性将使 FIs 在某种程度上自动执行其合规流程，从而允许监管机构增加合规审查所需的频率

数据标准化: 数据收集和存储的标准化，减少数据聚合过程中的摩擦。

5.3 IDHub 的竞争者是谁

IDHub 的竞争者包含两个层面: 一是现有用户管理的方式，如账户密码、第三方授权等。二是用户隐私数据的非法交易市场，这是个由需求驱动且政府难以取证和处罚的市场。

5.3.1 现有用户管理的方式

随着互联网蓬勃发展，用户管理的方式也层出不穷。这些方式有丰富的理论和技术支撑，新的用户管理模式也有很强大的用户体验，如 Google 两步验证。但本质上是提供服务的网站放弃对用户的身份验证，完全信任中心化服务的验证结果。验证中心获得越多网站信任，就越有可能成为黑客们攻击的焦点。

IDHub 从用户管理的安全性和用户体验两方面同时能够满足未来互联网发展的用户管理需要。用户身份的使用权安全地把握在用户手中，进而取代现有的用户管理方式。

5.3.2 用户隐私数据的非法交易市场

“我的数据我做主”的口号早已深入人心，但市场上交易用户数据并泄露用户隐私的现象却十分常见，IDHub 将有机会改变这种现状。

一方面，IDHub 提供安全的匿名的标识。这一标识能够将用户在不同平台的行为有效的统一起来。当两个平台需要交换用户的数据，他们可以在不泄露用户姓名、身份证号的条件下完成数据交换。

另一方面，IDHub 提供可靠的用户授权数据的方式，如果数据交换有利于用户，平台可以向用户发起请求，得到授权后合法地从另一个平台得到用户数据，这一过程所需的价值交换可以通过代币进行传输。

数据交易的市场广阔，IDHub 帮助市场创造合法的交易路径，将终结用户隐私数据的黑市交易，同时分享市场带来的利益。

6. 结论

随着数字社会的发展，用户身份和个人数据对信息服务商的过度依赖正在成为一个问题。这种情况为实现去中心化的数字身份应用平台和安全存放个人数据的平台创造一个独特的机会。

为了建立这个去中心化的数字身份平台，它不仅需要一条适合发行代币支付和交易的区块链，而且还需要支持所有用户管理和使用身份信息的自主权限，

以及制定安全有效的流动的激励措施。

最终，这些发行的代币可能被用于越来越多的区块链平台，最大限度地发挥身份的自主管理特点，成为每一个人进入数字社会的入口。IDHub 希望我们的股东——从用户到发行方——拥有更安全和自主的身份管理机制。

7. 参考文献

[1] T. Hardjono, Ed. Decentralized Service Architecture for OAuth2.0. https://tools.ietf.org/html/draft-hardjono-oauth-decentralized-00.html

[2] Yan Z, Gan G, Riad K. BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS[C]//Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on. IEEE, 2017: 138-144.

[3] World Economic Forum, Deloitte. A Blueprint for Digital Identity. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[4] Human Dynamics, MIT Media Lab. OpenPDS Software. http://idcubed.org/wp-content/uploads/2012/11/OpenPDS-software-from-Human-Dynamics.pdf

[5] Solid. Solid Specification. https://github.com/solid/solid-spec

[6] Civic. https://www.civic.com/

[7] Uport. Uport: A Platform for Self-sovereign Identity. https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf