IDHub 数字身份白皮书

基于开放原则、区块链技术的去中心化数字身份应用平台

IDHub 团队 2017 年 10 月 20 日修订

(V0.4.2)

目录

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，与自主身份相关的关键技术，以及与主流身份集中管理的差异和特点。IDHub 的应用场景广阔，如游戏化；作为网站新型登录方式；公民权利相关的身份认证；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。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

作为下一代互联网的基础设施，区块链以分布式存储、点对点传输、加密技术、共识机制的特性，成功实现去中心化、不可篡改、可追溯、唯一可信任等优势，有效解决了价值高效传递问题，成为未来价值互联网的基石。目前，区块链技术已延伸至金融科技、数字身份、数字资产交易、物联网与互联网应用、供应链管理、政府公共管理与社会治理、能源管理、智能制造等多个领域，成为引领新一轮技术创新和产业变革的重要引擎。

作为最早一批涉足区块链领域的企业，世纪互联准确洞察区块链技术发展趋势，于2014 年率先开展区块链的技术研发和应用研究，并积极推动以区块链为核心，包括数字身份认证、个人数据空间等在内的新一代网信事业基础设施建设，致力于打造可持续发展的完整可信数字生态，为数字社会的全面发展、价值互联网的高效建设以及全新社会信用体系的重塑做出贡献。

我们认为，数字身份是进入数字社会的入口，影响着未来社会运转和经济运行。数字身份已在各个生活场景得到广泛应用，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，主流的身份集中管理手段需要完全信赖服务商的能力和自律，在传统身份管理模式下，个人身份经常遭遇身份泄露、身份盗用、身份欺诈等问题。区块链以其特性优势，可以将身份控制权由第三方管理机构重新放回个人手中，为用户塑造完整、可信的“自主身份”，成为构建数字身份的最佳技术手段。

1.1. 数字身份

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. 数字身份遇上区块链

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，数字身份可以去掉中间环节，最大限度降低用户隐私数据泄露的风险。

2. IDHub 数字身份

2.1. 数字身份概念

我们经常将“身份”称为赋予我们或我们拥有的事物，我们控制或呈现的事物，而不是使用更严格的术语，如“标识符”（Identifier）、“属性”（Attribute）或“凭据”（Credential）。国际电子技术委员会将“身份”定义为“一组与实体关联的属性”。

为改善交流和理解，我们首先明确使用“关联”而不是“身份”，用来描述身份系统中的具体身份。“关联”解释了如何在数字和现实世界系统中创建和应用身份。本质上任何身份的概念在有身份证明的人或实体存在下才会产生意义。换言之，“身份”指的是在不同情况下关联同一主题的信息。如果我们能识别一个主题，我们就可以知道一些他或她表面之下的东西。

数字身份用一串数字描述了实体的身份特征信息，这些信息表示了一个数字“标识符”与“属性”、“凭据”之间的关联，被描述的实体可以是：个人、组织或设备。通过数字身份，我们可以快速地实现身份系统的功能机制，用户可以方便的创建和应用身份信息。

我们把数字身份系统中的“属性”分为“现实属性”和“虚拟属性”两部分。“现实属性”是我们与个人、组织和政府等实体交互过程中被赋予的属性和获得的凭据，我们常说的“证明我妈是我妈”就属于现实属性范畴。“虚拟属性”是指在虚拟世界（如：网络游戏、网络社交、区块链）中的属性，举例来说，网络游戏经验值、比特币余额都属于虚拟属性范畴。

区块链技术的数字身份系统中“标识符”具有很高的安全性和用户自主性。我们看到区块链领域有两种身份“标识符”的表现形式：非对称密钥和智能合约定义“标识符”。我们可以把其中任何一种“标识符”与“现实属性”和“虚拟属性”绑定，实现基于区块链“标识符”的数字身份系统。

2.2. IDHub 相关定义

2.2.1. IDHub

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 平台将提供以下组件：智能合约定义“标识符”、提供连接现实身份与“标识符”的软件开发工具、基于区块链的身份应用钱包和原生的代币系统。

2.2.2. 智能合约定义“标识符”

IDHub 支持区块链层面的价值转移与应用接口，它可以为区块链提供最基本的身份支持。一个身份个体在区块链上表现为三种智能合约的组合：代理、控制、注册。基于智能合约，IDHub 为用户提供了区块链身份的自主性和扩展功能。

代理合约

代理合约为用户分配一个区块链上的数字 ID，数字 ID 具有区块链所有的普通交易操作功能。

控制合约

控制合约保证用户对数字 ID 的完全自主性，可以实现更为复杂的区块链操作。

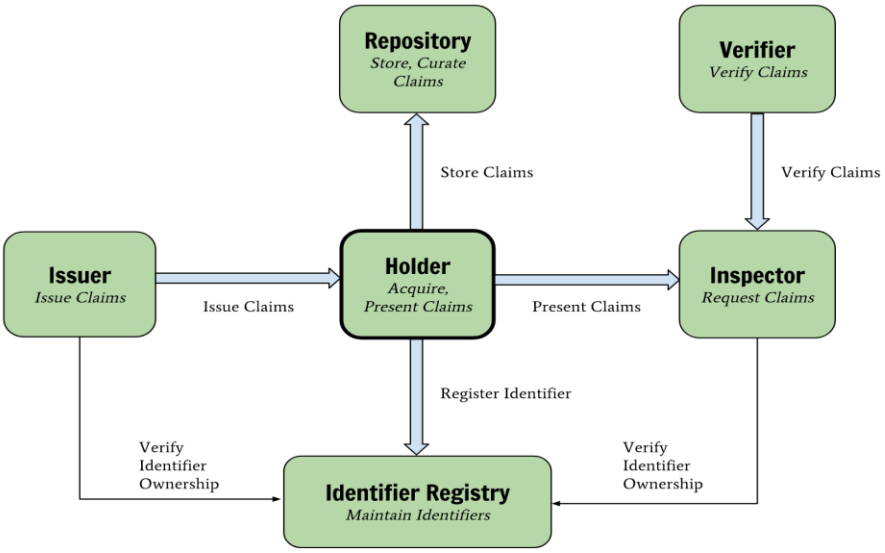
注册合约

注册合约实现了数字 ID 和身份属性的相关性，保障了数字身份的价值以及区块链所提供的公正性和安全性。

2.2.3. 现实属性的声明和声明管理

与 IDHub 数字身份（identity）相关联的属性称为声明（claims）。这个术语起源于基于声明的身份，一种断言（assert）数字身份的方式，独立于任何需要依赖它的特定系统。由于 IDHub 身份管理的主要目的是使身份所有者可以轻松地断言和证明身份的个人资料，凭证，奖励，学位等的属性。声明管理是 IDHub 的特色。

可验证声明的架构（Verifiable Claims Architecture）



可验证声明的构架必须区分核心角色的基本作用和其关系以及他们如何互动，角色是一种可能以许多不同的方式实现的抽象。角色的分离表明可能的标准化接口和/或协议。可验证声明构架中存在以下角色：

持有人(Holder)

从发行者（issuer）获得可验证声明，并有选择地将其提供给检查员（inspector）。持有人通常但并不总是可验证声明的主体。

发行者(Issuer)

向持有人发出可验证声明。

检查员(Inspector)

请求持有人的可验证声明，以便对其进行认证（authenticate）。

Identifier Registry

调解（mediate）全球唯一的数字身份（identity）创建和验证。注册管理机构必须以自主的方式管理数字身份。

Repository

存储和策划持有人的可验证声明。

Verifier

代表检查员核实可验证声明。例如，检查员可以通过某些行业特定的业务规则来提供更深入的验证。

2.2.4. 业务操作流程

创建

用户可以自由创建由智能合约构建而成的数字身份，并且将之与自己的密钥对绑定。用户可以通过自己的私钥实现交易控制、数据上链注册，并且可以设置数字身份代理以保证合约控制权的普适性。

系统会为用户提供构建数字身份的模块化功能，并集成必要的人性化操作方式。

认证

用户信息的现实价值可以通过公信力背书来保障。具有公信力的组织或个人可以为用户自由声明的信息背书，必要时可以将信息数据上链。认证模块通过具有公信力的组织或个人运用私钥对数据签名，第三方通过公钥验证的方式为 IDHub 用户提供现实价值的背书。

授权

用户可以自由选择授予第三方获取自己信息数据的权利，通过系统授权模块的接口用自己的私钥签名，授权于第三方调用数据存储管理模块的接口来查询甚至使用自己的信息。数据存储管理模块会通过用户公钥验证授权签名的有效性，并保证权限范围以及时效性。

查询

系统集成了一套数据管理接口用于数据分享，经过用户授权的第三方或者用户自己可以很方便的用区块链浏览器查询数字身份链上数据，也可以调用数据存储模块的接口查询非上链数据。另外，系统可以返回第三方对应用或服务的查询结果，同时有效的保证用户的隐私。

2.3. 愿景

ID as a Service（IDaaS）：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。

ID as a Digital Asset：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。

ID as a Digital Life：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。

2.4. 适用场景

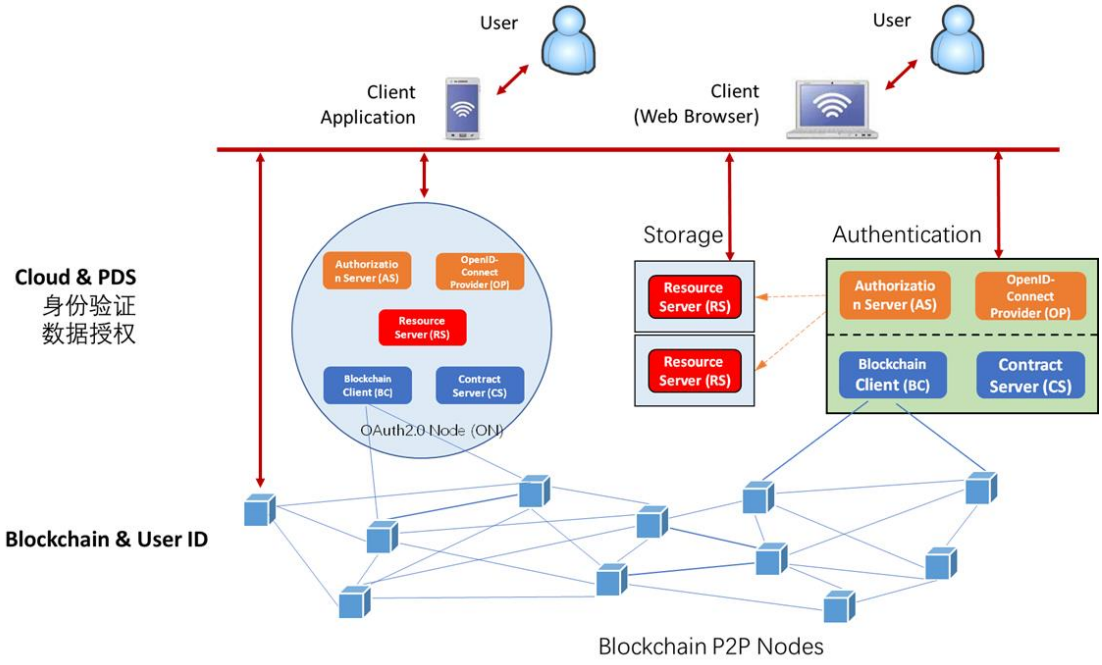
IDHub 是运行在区块链上的身份系统，能够满足多种的使用场景。

当用户需要同步或迁移分散在各个信息系统中的数据时，统一的身份标识符将很大程度减少数据迁移过程中的身份校验工作。尤其对于互不信任的信息系统之间的数据传输，IDHub 能发挥更大作用。

除此之外，IDHub 可作为特定区域的身份管理解决方案，帮助地方政府、居民建立安全的、可持续的和易拓展的身份系统。

3. 技术概述

3.1. 总体架构



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

用户通过终端设备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、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。

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。

3.2. 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。

3.3. Solidity 和智能合约

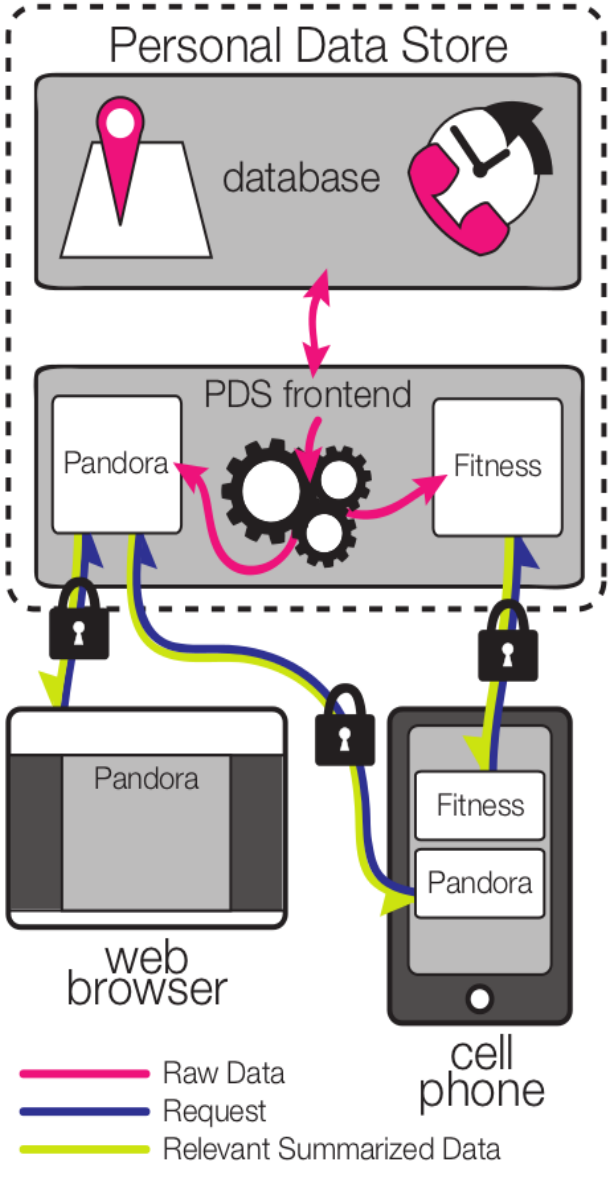
Solidity 是一种面向智能合约的、语法类似 JavaScript 的高级编程语言。它的基础环境是当前最广泛使用的以太坊虚拟机 EVM。智能合约为我们提供了一个通用密钥管理解决方案，同时使之成为持久的身份标识符。这个身份标识可以表示为一个智能合约地址或传统的公钥。因为智能合约可以由其他的智能合约控制，他们可以通过编程来实现密钥恢复逻辑。这种控制逻辑的灵活性给安全的密码学身份增加易用性和自主管理。

基于智能合约的数字身份可以用于多种类型：个人、设备、实体或机构。基于智能合约的身份标识符是自主的，意味着是由创建者完全拥有和控制的，并且不依赖中心化第三方进行创建或验证。核心功能是可应用于广泛的用例，如声明、动作或交易进行数字签名和验证。由于可与区块链互动，用户通过数字身份亦可控制数字资产如数字货币或代币化的资产。

3.4. OpenPDS

巨量资料时代来临，许多应用仰赖着分析用户数据来达到更好的用户体验，这的确可望能为企业或社会带来革命性的变化，但伴随而来的议题便是属于用户个人隐私的数据就极有可能暴露，虽然各国的法规大多会规范企业在收集用户数据时需要先取得用户的同意，但美中不足之处是用户为了使用该服务按下同意按钮就相当于概括接受了所有服务条款，用户往往也没能注意到背后还有许多定义不清的约定规则，用户隐私与用户体验是时候需要有个取得平衡甚至双赢的解决方案。

美国麻省理工学院长期致力于开发 OpenPDS，一个可以让用户存储个人数据，用户以外的所有应用或服务只能获取有限或所需的部分数据。



OpenPDS 最重要的亮点就在于能以“是”或“否”来返回应用或服务的查询，在 SafeAnswers 这个安全的框架下对用户数据进行计算，如果从技术的视角来阐述，SafeAnswers 仅允许代码的共享，不允许数据的共享，就如同一黑盒子般保护着用户的个人数据，但又能给出足以提升用户体验的满意答案，而 SafeAnswers 也自带能避免服务或应用透过穷举式的查询来取得用户的真实数据。 OpenPDS 为用户隐私及使用体验提供了一个双赢的解决方案，并且能在数字身份丰富的应用场景中扮演 Oracle 的角色，Oracle 是区块链上自动取得数据的一个可信任节点。

3.5. JWT

身份属性的有效性通过由 JSON Web Token（JWT）实现的认证来保证。JWT 是一种开放标准（RFC 7519），其定义了一种紧凑且独立的方式，以在各方之间以 JSON 对象的形式安全传递信息。该信息可以通过数字签名验证和授信。JWT 的结构由标题，有效载荷和签名三个部分组成。标题由令牌的类型（即 JWT）和使用的散列算法组成，如 ES256k 或 RSA。有效载荷包含了一些声明，而这些所谓声明是指关于实体及其附加元数据的声明。其中一些固定声明包括 iss（发行方），exp（到期时间），sub（主题），aud（观众）等。签名则是通过使用专用密钥和标题中指定的算法对编码的头部和编码的有效载荷进行签名来获得的。签名用于验证 JWT 的发行者，并确保该消息在传输过程中保持完整。

3.6. Merkle 树

身份属性的证明是有价值且敏感的。一个令人满意的凭证管理系统应满足最低限度的披露原则，该原则规定身份系统应披露有助于交易所需的特定实体的最低信息量，而不需要再多的信息。遵循这一原则的原因是保持隐私，并减轻信息披露的潜在副作用。Merkle 树的性质适合最低限度的披露原则。Merkle 树是一种每个叶节点都标有数据块，而每个非叶节点用其子节点标记的加密散列算法进行标记的树。Merkle 树允许高效和安全地验证大型数据结构中的内容。通过提供适当的散列来实现最低限度的信息披露，从而只公开所需要的数据。

3.7. 身份图

身份图是身份之间行为的一种表示。在身份图中，节点就是身份，而连线就是行为。行为包括以好友身份添加，认可，评论和交易等。在区块链上，（我们）将这些行为转变为交易。身份的信誉可以根据交易日志计算。由于将应用程序视为通过数据块流进行通信的异步进程的网络，基于数据流的编程适用于处理身份图中的数据流。而重点在于应用数据及为产生所需输出而应用于其的变换。该网络在进程的外部进行定义。

IDHub 系统中的每个身份都由一个树和一个图表示。身份的声明和证明存储在 Merkle 树中，与其他身份的交互则以身份图的形式进行存储。

3.8. Kademlia

IDHub 存储区块链上的数据索引和分布式存储系统中的数据值，例如 Kademlia。区块链以其透明度和稳定性而闻名。区块链上的数据是不可更改的，除非攻击者占据了大部分块的计算能力——而这是不现实的。Kademlia 是一个点对点分布式哈希表，哈希表记录了不同哈希值进行异或运算的结果（XOR）。由于是基于异或运算的新型度量拓扑，Kademlia具有可靠的稳定性及性能，且具有延迟最小化路由，无延迟故障恢复和对称单向拓扑等令人满意的特点。Kademlia使用并行异步查询来避免故障节点的超时延迟，靠节点记录用户存在的算法抵御了一些基本的拒绝服务攻击。由于使用分布式存储系统，IDHub 比集中式身份系统（如 Aadhaar）更为安全可靠。通过存储前加密更是能进一步增强安全性。其中，“加盐”是加密工具的一个理想示例，它是一个用于网络通信，加密，解密和签名的高速库。

3.9. 现有数字身份比较

对比项	IDHub	Uport	Civic	Air
ID发行方	任何人	ConsenSys	Civic	SPHRE
账号管理	以用户为中心， **多类型身份合约管理**	以用户为中心， 身份合约管理	以 ID Provider 为中心， 中心化网站	以 ID Provider 为中心， 中心化网站
身份使用范围	**链上和链下** 在身份管理合约中准确记录换 Key 操作，实现身份与链下公私钥的绑定	**链上和链下** 仅记录身份「标识符」与用户公私钥的当前关系信息	仅信任 Civic 的网站	仅信任 SPHRE 的网站
数据存储	公开数据：IPFS 隐私数据：用户手机 / PDS 上链服务不保存用户信息	所有数据：IPFS（隐私数据存在 IPFS 会有泄露风险）	用户手机保存 上链服务不保存用户信息	用户手机保存
数字证书	任何人可在区块链上校验	无	任何人可在区块链上校验	任何人可在区块链上校验
推广模式	社区+商业推广	社区推广	商业推广	商业推广
区块链平台	Ethereum、RootStock、Qtum	Ethereum	RootStock	Hyperledger

数字身份在互联网领域是一个经久不衰的议题。结合区块链的自主、安全、不可篡改等特点，有一些项目已经开始区块链与数字身份的融合。上表列举其中 3 个受关注度较高的项目与 IDHub 进行对比。

从身份自主角度，IDHub 不仅把数字身份的属性控制权交给用户，还把标识的控制权真正“还给”用户。Civic 和 Air 的做法是把用户属性内容进行加密和上链，但用户的标识仍由中心化网站控制，身份的使用范围也限制在网站内部和网站合作伙伴之间。uPort 使用智能合约定义数字身份，将标识的控制权交给用户，但在应用服务层没有提供第三方平台直接与智能合约互动的工具，所有链下应用交互都需要访问 uPort 网站接口，违背了身份自主的本质。

从数据管理角度，IDHub 将用户属性数据分为公开数据和隐私数据，用不同的方式进行保存，保障用户数据的安全。Civic 和 Air 都没有讨论公开数据的问题，隐私数据采用用户手机保存，并将可供校验的 hash 值记录在区块链上。uPort 将全部数据放在公开的 IPFS 中，对隐私数据进行非对称加密处理，只有拥有对应私钥的用户才能数据解密。uPort 对隐私数据的处理方法在私钥丢失或被窃时有一定的数据安全风险。

从区块链类型的角度， 我们认为数字身份应建立与应用范围一致的区块链底层上。IDHub 对区块链选择保持充分的灵活性和开放性，未来将兼容多种区块链底层技术。为了让 IDHub 数字身份尽快实现，初期有较大可能采用以太坊区块链进行实作。

4. 应用场景

4.1. 游戏化

游戏化提升了用户体验。用户所扮演的角色就是他们自己。通过学习新技能，结交新朋友，参观新地点或进行运动，用户将进一步提升到新的等级。

日常任务是一项每天赚取经验的简单任务，例如提交一份发票副本。当用户的经验达到一定水平时，他们将获得奖章。对此进行的评估和相应设备是通过消耗 IDHub 代币（IDH）来获得的。用户的配置文件将被可视化为雷达图。每个轴代表一个属性类型。健康轴线包括跑步距离、卡路里消耗、体重、血压和电子病历。连接轴包括同事、同学、家谱以及在 Facebook，LinkedIn 或 Twitter 上的朋友。财产轴包括存款证明、证券存折、土地所有权以及加密货币钱包地址。信用轴线包括交易、信用卡、税务、犯罪和贷款各项记录。技能轴线包括 Cousera 证书和在 GitHub 上的承诺。价值轴线包括由用户提供并发布在 IDHub 论坛上的产品或服务。旅游轴线包括参观过的城市和住宿记录。考虑到隐私问题，用户决定披露哪条轴线（的信息）。

4.2. 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。

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。

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。

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。

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。

4.3. 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。

4.4. 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. 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 希望我们的利益相关者——从用户到发行方——拥有更安全和自主的身份管理机制。

6. IDHub 团队

核心团队

曲明
IDHub 创始人
互联城市咨询委员会（CCAB）理事会成员

陈振国
IDHub 技术总监
曾任亚太线上CTO、威睿科技联合创始人&CTO

苏育民
IDHub 研发总监
台湾大学创业创新MBA

李骁宇
IDHub 核心工程师
北京交通大学硕士

谢承璋
IDHub 核心工程师

林展民
IDHub 核心工程师
台湾政治大学理学硕士

姚泽乾
IDHub 研发工程师

李嘉淇
IDHub 研发工程师

王沛智
IDHub 商务拓展经理
伯明翰大学硕士

吴茜
IDHub 市场总监
英国大众传播和媒体研究硕士

薛玉成
IDHub 市场公关经理

曹磊
IDHub 市场经理

TASYA
IDHub 社区运营

顾问

元道
世纪互联创始人
中关村区块链产业联盟理事长

上野嘉久
世纪互联董事兼牵头VC投资人
Synapse Holdings创始人

Powered by
21VIANET

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