中钞信用卡产业发展有限公司
杭州区块链技术研究院

络谱 ID

分布式身份体系

重新定义互联网身份层

中钞信用卡产业发展有限公司

杭州区块链技术研究院

2019 年 03 月

回顾互联网发展历史，有许多里程碑意义的第一次：

1985 年 3 月 15 日，第一个互联网域名注册；

1991 年 8 月 6 日，第一个网站上线；

1993 年 1 月 6 日，第一条即时通信消息发送；

那么，第一个互联网身份是何时诞生的呢？

这个答案也许难以追溯，不仅由于年代的久远，而且在于互联网虽然提供了信息高速公路，但并没有提供中立、开放、标准的身份层，即使是“身份”的定义也不够清晰，基于互联网的身份互信是长久以来一直存在的问题。

对此问题的研究已经超过 20 年，如今终于积累了足以实现突破的成果。

我们推出络谱 2.0——络谱 ID，为重新定义和填补互联网身份层而来。

目 录

1. 缺失的身份层

1.1 问题

目前互联网的身份存在一些显而易见的问题，已为人所熟知：

●身份互认问题。不同机构之间的身份数据隔离，用户身份难以互认互通。

●重复认证问题。在不同应用、不同场景下重复执行类似的身份认证。

●安全性问题。用户信息被大量复制保存，面临泄露及被篡改的风险。

●身份欺诈问题。用户的身份易被盗用，带来欺诈风险。

在处理这些问题上，已经出现了一些办法。例如单点登录，在多个应用中用户只需要注册认证一次就能够访问所有相互信任的应用。例如人脸核身，通过连接政府部门的数据库和人脸识别验证用户真实身份。这些打通数据孤岛的方式，确实取得了一定成效。

然而毫不讳言地说，这条路已经碰到了屏障——任何单一机构无法连接能认证用户不同身份信息的所有机构。

“身份”具有强烈的社会关系性质，一个人无法仅靠自己证明自己的身份，通常需要借助他人和其他机构的关系背书。但是能提供身份认证的机构是分散的，而不同的互联网服务需要认证用户的不同身份信息，这些信息往往来源于多个认证机构，这构

成了互联网身份问题的基本矛盾：

首先，认证机构大多没有义务为有认证身份需求的机构开放自己的数据库和验证能力。

其次，由于担心安全和隐私问题，认证机构试图对外提供认证服务和数据时也面临种种顾虑和风险。

最后，分散的认证机构和分散的认证需求方的对接必然没有效率。

这是互联网身份问题绕不开的症结和悖论。通过打通数据孤岛的方式能解决一部分问题，但仅仅是一部分。在接通多个认证机构的过程中，存在的问题既不在于技术上难以实施，也不在于业务上各方完全没有意向，而是这道屏障难以逾越。

解决问题需要新的思路。

1.2 启发

传统的做法有时候能够给予新的启示。

在物理世界中，用户使用证件来证明身份信息，例如身份证、护照、社保卡等。这些证件是由一个可信的机构颁发的，其他人和机构则信任这些凭证所包含的信息。一些情况下，持有物理证件就证明了证件上的身份信息归属于用户。

然而，证件难以数字化。这在于物理证件的信息向他人出示时，并不会转移证件的权属。但数据流转时便难以控制。所以，用户难以在互联网上证明某个身份信息属于自己。

重新审视身份：“身”，代表的是一个客观的人。“份”，代表的是人的身份信息。身份指的是哪一个“身”，是什么样身份信息的人。身份信息是可以传播、交换的，但唯有“身”是必须自己控制的，否则就无法证明自己的身份，必须区分。这个“身”，在物理世界就是用户自己。但在互联网上，大多数服务基于“用户名-口令”的方式，不是真正完全属于用户控制的。“身”和“份”混淆，都存储于中心化数据库，用户却丧失了对“身”的控制。

1.3 解决之道

现存的互联网身份解决方案不能为用户提供自主掌握的身份，也无法解决身份数据在不同应用之间共享问题。

实现互联网身份协议层的解决之道是采取一种回归本源的做法：用户向认证机构请求核准签发数字身份凭证，并根据自身的需求，向应用方提供其可验证数字身份凭证以获得相关授权服务。这种情况下，身份数据通过身份持有人合法授权流转，认证机构也不用担心对接成本和对接的安全问题。

在自主身份控制层面，区块链技术促进了用户自主掌握私钥等用密钥进行身份控制方式的使用，显示了电子签名和区块链技术在确认不可篡改的用户操作方面的潜力。通过这一种方式，使用户能够完全掌握自己的身份控制。

在用户身份信息认证方式上，自上而下的单一机构认证和单

点登录的联盟互信的模式无法覆盖全面多元的用户身份认证需求。用户身份信息源于社会关系，其认证也需要回归社会关系。采用一种经由社会关系传递信任的办法，实现用户身份信息的认证。

基于此思路，我们设计了络谱 ID——一个分布式数字身份体系。

2. 络谱 ID

2.1 溯源

正如区块链建立在几十年来密码学和分布式系统研究的成果之上，络谱 ID 亦汇集了对数字世界如何认证身份问题的众多的探索和创新：

1991 年，一类网络保密协议——PGP 组织提出了分布式数字身份的第一个雏形，并提出不依赖于中心化服务机构就能建立用户之间信任的信任网概念。然而这一理念在当时过于超前，并没有可实现的基础技术，以致于注册于中心化服务的“账户”一直在扮演用户“身份”的角色。

直到区块链技术的出现为数字身份奠定了技术基础。用户拥有区块链上的“身份”终于不受中心化服务的限制，用户在区块链上的意愿表达不可篡改。这极大地加速了问题解决的进程。

区块链技术逐渐为人所知后不久，多次重新启动信任网（Rebooting the Web of Trust）研讨会召开，推动了各界技术力量对解决方案的研究，并提出诸多数字身份的实现目标、原则。

发布多项影响深远标准的 W3C 组织，也提出了多项数字身份相关的标准，以便建立在不同国家、区块链上的数字身份能够相互识别和认证。

至此，填补互联网身份层的主要拼图已然具备。

中钞区块链技术研究院团队是国内最早研究区块链技术的团队之一，致力于为数字经济打造公共基础设施。我们意识到，区块链是数字身份的基础和关键，数字身份亦是区块链重要且不可替代的应用场景。推动基于区块链的数字身份的建设和应用，是做区块链的人的使命。

2.2 简介

络谱 ID（BROPID）是一个分布式数字身份体系，为互联网应用的用户身份认证和身份数据流转提供中立、开放、标准化的服务。络谱 ID 基于区块链技术，旨在突破以单一机构为中心的、数据库直连的认证方式的局限，通过分布式、开放性的认证模式，将可信的身份服务扩大到更大范围的用户，不仅包括自然人用户，也包括法人和可计算设备，从而夯实互联网不同身份之间业务的可信身份基础。

络谱 ID 是基于络谱可信登记开放平台（BROP）的底层区块链运行的，是一个不依赖于中心化机构的开放网络服务。络谱 ID 的设计符合国际组织关于分布式身份的系列规范，未来支持与不同分布式数字体系下数字身份的互认。

中钞区块链技术研究院致力于搭建络谱 ID 的基础设施和标准，作为一个分布式数字身份体系的创始建设者，推动生态参与方的共建、共用、共享。

2.3 目标

络谱 ID 分布式身份体系具有以下特点，也是络谱 ID 实现的目标：

1、用户身份自主

用户完全拥有、控制和管理他们的身份。这意味着：

用户的身份数据是自主控制的，身份所有者完全控制身份数据的访问；

用户基于身份的操作是自主控制的，该身份的真实意思表示能够被确信证明，不仅仅是通过服务器的操作记录的方式；

用户的身份是可移植的，用户能够在任何他们想要的地方使用他们的身份数据。这就不同于当前单点登录的方式，需要在互信任的应用中用户的账户才能通用；

2、提高身份认证方的数字化服务能力

当前具有身份认证能力的机构，如公安、民政等政府部门，如医院等事业单位，以及一些互联网巨头，面临越来越多的身份认证请求。但身份认证方既没有义务，也没有能力对接数量庞大的有认证用户身份需求的机构。

络谱 ID 将实现数字身份的公共服务，身份认证方只需要完成

其本来应该完成的工作——向用户颁发各类身份证明（以数字化的方式实现），需求方就能验证用户真实身份信息。这大大减少了身份认证方对外提供用户身份数据的安全担忧，保障了公民数据安全，也优化数字社会治理能力与服务能力。

3、了解用户无需通过第三方

对于一个互联网应用来说，应用验证用户身份或获取其他用户数据只需要找到用户，不需要经过第三方账户登录接入等审批，也不需要经过数据中介。

首先这降低了应用的对接成本。意味着应用无需对接多个身份数据源，只要经过用户同意就能访问用户身份数据。这大大减少了对接多个身份数据源的成本，阻止了数据孤岛的形成，降低了业务对接难度。

其次，这将减少认证用户身份的成本。络谱 ID 的用户身份信息结合区块链可以追溯和验证信息来源，确认数据的可信度，具有可验证的标准化格式，不仅减少人工审核工作，也为将来数字智能社会的治理提供可能。

最后，所有身份数据来源于用户，出于用户自主授权，合法合规，降低了用户信息收集和使用的风险，也会激活新的使用场景和创造新的应用价值。

3. 总体架构

3.1 数字身份

世界经济论坛（WEF）近期将数字身份定义为“独特属性的集合，用于描述一个实体并确定该实体可以参与的相关事务”。这个定义中“实体”和“属性”缺一不可，与前文所述的“身”和“份”的拆借不谋而合。属性是对实体的身份信息描述，而实体就是用户自己。数字化以后，“实体”必须寻找一种数字化表达，这种数字化表达就是身份标识，一个唯一独特的身份标识以将不同的身份标识区分开。

因此，络谱 ID 的数字身份分为两个层面：

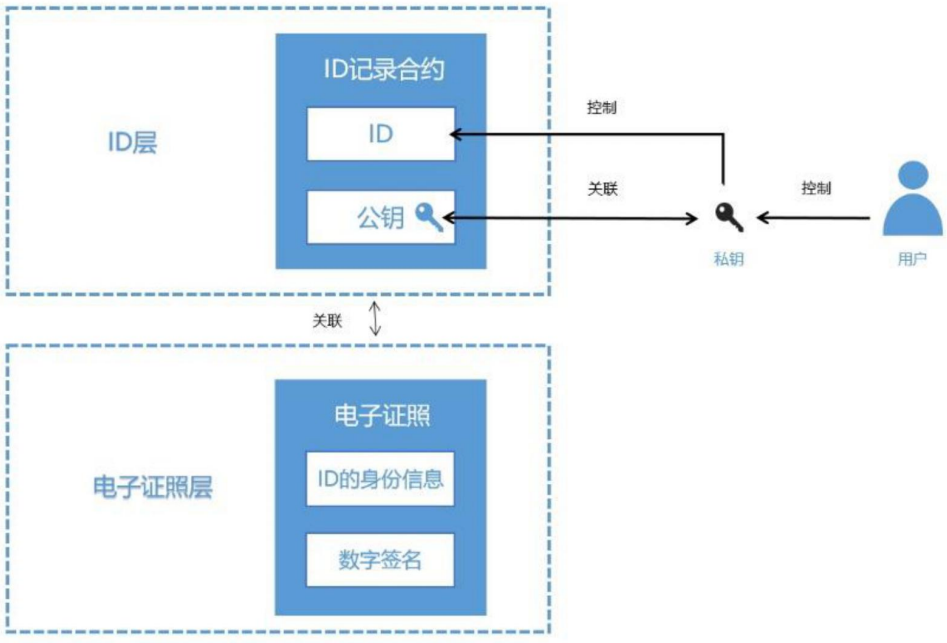

图. 数字身份双层设计

一是身份标识层面，即 ID 层。用户在 ID 层将具有络谱 ID 体系内全局唯一的持久化身份标识符（下文称 ID）。这是一串独特而唯一的字符串，与一对非对称密钥相关联，被用以代表用户。用户可以拥有多个 ID，以用于在不同场景和应用代表用户。

ID 的实现载体是 ID 记录合约。ID 记录合约是一类智能合约，登记了一个非对称密钥的公钥和 ID 的关系等身份信息。用户通过掌握公钥对应的私钥来控制该 ID。并代表用户实现与区块链上其他智能合约的交互。

二是数字证照层面。数字证照由能够证明用户身份的认证方签发，申明 ID 所指向用户的身份信息。

数字证照是用数字签名追溯出处的数据报文，便于流转。该数据报文数字签名的验证要素——公钥等其他信息仍存放于 BROP 区块链等公开可信的载体上，使数字证照的出处能够被验证。

这种将 ID 和数字证照分层拆解的设计，既使身份信息的流转和验证变得便利，同时使用户能够对 ID 具有完全自主的控制，简明而健壮，符合“身份”的本义。

另一方面，络谱 ID 鼓励用户控制多个 ID，分别用于不同的场景和应用使用。这避免了统一 ID 在不同场景的业务相关联，从而实现对用户身份信息的安全、自主、可移植应用的支持。

3.2 分布式身份信任框架

络谱 ID 实现数字身份可信的基本框架，建立在一个分布式信

任网之中。在这个信任网里，证明用户身份的发证方、需要被证明身份的用户、需要验证用户身份和获取用户数据的应用方进行多方协作，共同完成用户身份数据的流转和应用。

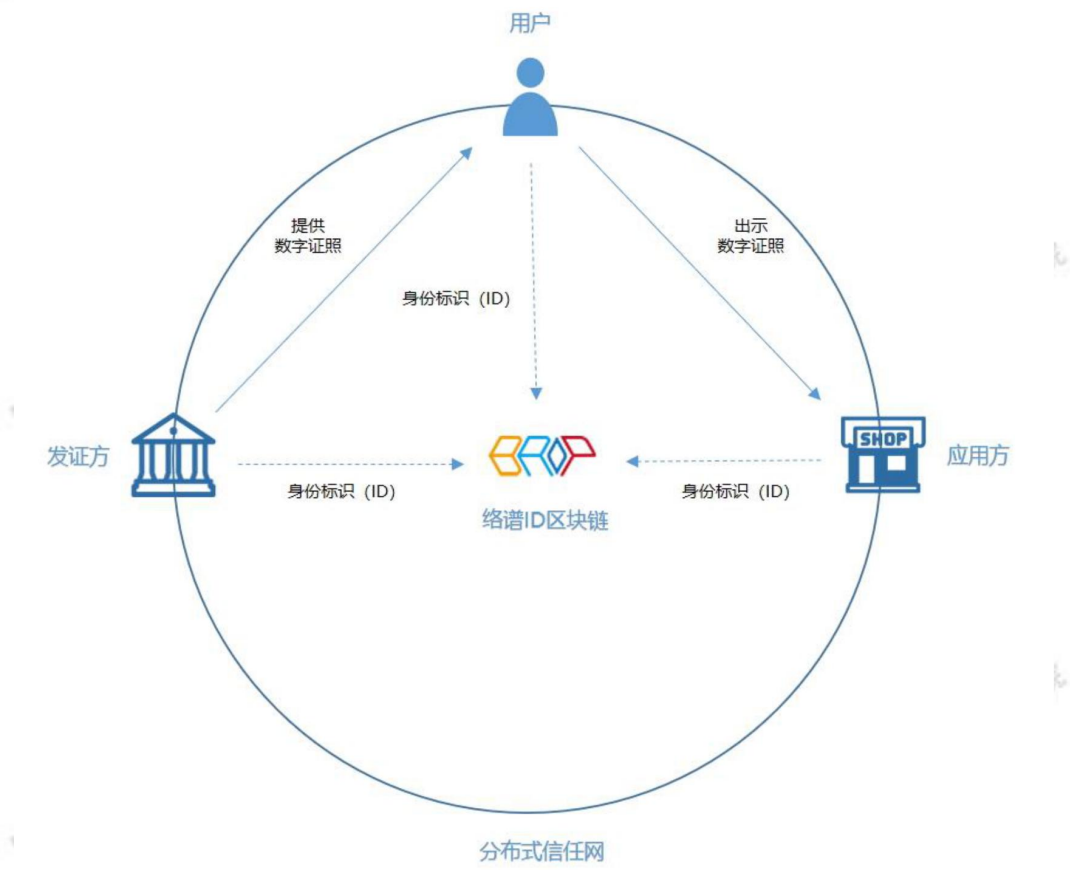

图. 身份信任框架

分布式信任网是数字身份的基础，其核心是不可篡改的络谱 ID 区块链。区块链实现了用户可自主生成和控制器身份标识的 ID 层，标记身份标识的通信方式。多方通过接入工具接入分布式信任网，以区块链为依据，建立不同身份标识之间的安全通信，为数字证照的流转建立前提。

络谱 ID 的身份信任框架是分布式的：

首先，用户的 ID 不是由单一机构赋予的，而是由用户在区块链这一分布式账本上生成的，是完全自主的并且受用户自主控制的。

其次，应用方验证用户身份信息，并不直接连接发证方获取数据，而是直接从用户处获取，通过发证方公开密钥计算并验证用户提供信息的真实性；

最后，发证方不局限于权威机构，数字证照被采信取决于是否为应用带来信任和价值。这些都扩大了信任的范围，将可信数字身份扩大到更大的人群、组织、可计算设备，从而实现不同身份间的可信数字交互，最终形成网状分布式的的信任网络。

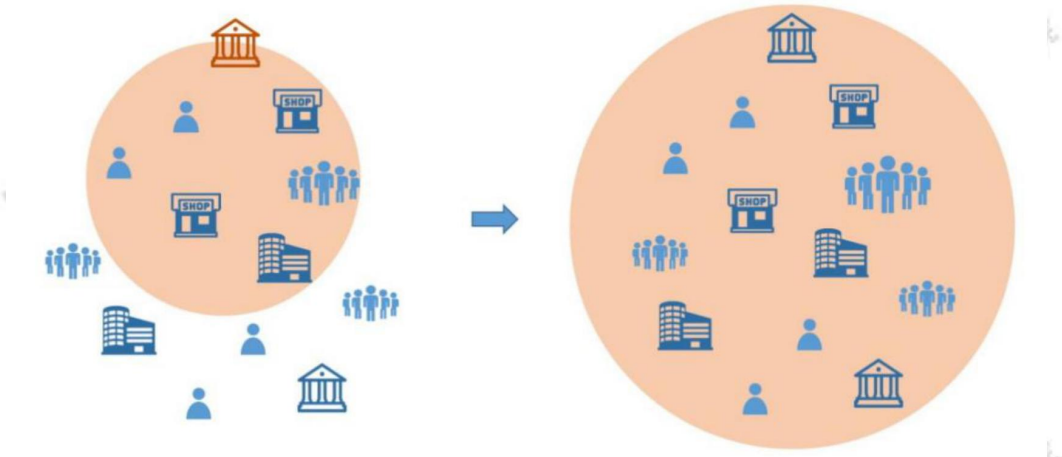

图. 从中心化单一信任到分布式网络信任

3.3 生态参与方

络谱 ID 是一个中立、开放的身份层网络，无论是普通用户、企事业单位都能加入络谱 ID 生态的运营，并从中获取自身的业务价值。

3.3.1 发证方

发证方是向用户创建并签发数字证照的机构或个人。

络谱 ID 将与政府部门、事业单位合作，向用户提供基础的例如实名身份认证的数字证照，即带有其数字签名认可的身份信息证明文件。这将不仅方便用户，也将为发证方带来价值：

1、简化证件在线验证服务，提高数字化服务能力

无需单独建设提供验证证件真伪的服务。只需要发出数字证照，应用方就能验证发证人真实身份和证照真伪。

2、便于政策制定方进行标准的推行

政策制定方只要制定统一的数字证照规则，由各下属发证业务方按照规则发行数字证照。政策制定方维护系统投入少，大大降低业务成本。同时可以跟踪分析各地的政策执行情况。

3.3.2 应用方

应用方是有验证用户数字证照需求的机构或个人。

相对于应用方现在的身份认证和用户数据获取方式而言，络谱 ID 为应用方增多了了解用户的方式，有更多的用户数据可获取

和选择，并且具有以下优势：

1、合法合规获得可信的用户身份数据。所有信息由可信的发证方认证，经过用户自己授权，结合区块链可以追溯和验证信息有效性。

2、减少对接。应用方无需对接多个身份信息源，不依赖于发证方服务，也不需要接受第三方登录式的接入审批。只要接入络谱 ID 网络，找到用户，就能获取并验证用户数据。

同时，应用方不仅限于互联网应用，络谱 ID 也支持线下验证用户的方式。

3.3.3 其他合作方

络谱 ID 也欢迎其他合作方的加入：

1、技术合作方

与中钞区块链技术研究院一起推进络谱 ID 基础设施的开发和升级。

2、软件服务商

提供络谱 ID 生态下用户终端等相关产品的开发和运营，为各方提供更加良好的体验。

3、系统集成方

帮助发证方和应用方的接入络谱 ID，拓展络谱 ID 网络的应用和服务价值。

3.4 主要设施

络谱 ID 是一个分布式身份体系的开放网络。网络因参与方按共同的规范交互而存在，并不独属于任何人。但网络得以运行的基础设施需要被提供和维护。中钞区块链技术研究院作为络谱 ID 的创建者，提供了这些基础设施。

3.4.1 络谱 ID 区块链

络谱 ID 区块链是络谱 ID 的基础，是基于络谱可信登记开放平台的底层区块链。区块链的主要特征是一个多节点共同维护的公开账本，以保证该公开账本记录的不可篡改。作为分布式账本，络谱 ID 区块链主要用来记载 ID 的身份记录，也记录有关数字证照流转的存证。

3.4.2 络谱 ID 服务平台

络谱 ID 服务平台为发证方和应用方接入使用络谱 ID 提供服务。发证方和应用方使用络谱 ID 需要进行 API 的对接和 SDK 的使用嵌入，使当前的业务系统能接入络谱 ID。因此络谱 ID 服务平台将提供发证方和应用方的接入服务，包括 API 的提供、SDK 的提供、解决方案设计等。

按照统一的规范、标准、协议，发证方和应用方亦可以不通过络谱 ID 服务平台接入使用络谱 ID。但络谱 ID 服务平台为接入提供了易用的工具，简化了使用络谱 ID 的工作。

3.4.3 络谱 ID 用户终端

用户与络谱 ID 服务平台、络谱 ID 区块链、发证方、应用方进行通信，实现各种身份相关事务需要软件系统支持。中钞区块链技术研究院提供的络谱空间 APP 是实现了这种功能。

络谱空间 APP 是络谱 ID 用户终端的示范实现，是用户接入络谱 ID 的入口和工具。通过络谱空间 APP，用户可以使用络谱 ID 的功能与服务，并且自主控制自己的数字身份。

络谱空间 APP 的主要功能是数字证照的管理，用于数字证照的申领、保存、流转。即帮助用户向发证方申领数字证照，将获取的数字证照安全地进行存储，响应来自应用方的请求出示数字证照以证明身份。

除此之外，其他合作方只要按照统一的规范、标准、协议，其他合作方也可以自行开发实现这种功能的络谱 ID 用户终端给用户使用。

4. 应用愿景

4.1 统一身份识别入口

络谱 ID 提供了一个开放、标准的身份识别方式，将逐步补充和替代现有的中心化的、非标准化的、范围局限的身份识别方式，成为用户向应用方证明自身身份的入口。

这将解决重复身份认证问题。用户不必在每一个应用方的应

用系统都进行类似但难以复用的人脸核身等身份认证。用户获取证明自身身份的数字证照后，可以在不同应用场景下出示以完成身份验证，而不需要这些应用方之间相互信任。

这将解决身份欺诈问题。目前应用方认证用户身份和反欺诈需要投入较高的 IT 系统建设成本和人工审核成本。但数字证照提供了可验证身份信息来源的方式，应用方可以通过验证数字证照，获取可信的用户身份信息。

络谱 ID 可简化账户的注册登录流程，提供了应用方确认用户真实身份的全新方式，用数字签名确认用户操作行为，使用户行为更加可信。

4.2 分布式声誉评价

声誉即社会对某一身份的评价。身份存在于多种社会关系中，任何与用户具有社会关系的机构或个人都掌握一定有关用户的身份信息。传统以某一机构为中心采集用户数据形成用户声誉或信用评价的，注定无法覆盖全面的用户信息。

络谱 ID 分布式和开放性的特点允许机构、个人都参与到声誉评价中来，并且赋予这种评价以可验证、可流转的范式。机构和个人都可以作为发证方对他人发出数字证照，以自身名义对他人的活动进行评价，以便他人向第三方证明自己的声誉。声誉评价可以进一步结合可选的公开算法，形成基于分布式声誉评价的信用分。区别于中心化机构发布的信用分，用户不用担心自己的信

用分被某一机构隐蔽地篡改和任意地调降。

4.3 以用户为中心的数据流转

无论如何发展不同业务系统之间的连接，总是存在一些数据孤岛因为政策、利益、技术等原因无法打通，从而无法发挥出数据流通的价值。

基于络谱 ID 数字证照流转的模式，数据需求方不再需要构建复杂的 IT 系统，逐一对接不同的数据源，而是从所连接的用户出发，基于络谱 ID 标准申请授权访问其相关数据。络谱 ID 支持不同形式的身份数据业务请求，这种数据获得的途径是准确、快捷而合乎隐私保护需求的。新的数据流转方式以用户为中心，将进一步释放数据的价值，创造新的应用场景。

5. 结论

络谱 ID 将提供一个中立、开放、标准化的数字身份服务，弥补现有互联网缺失的身份协议层，实现用户身份自主控制、便利地分布式身份识别。络谱 ID 分布式身份体系籍以对身份本义的探索，将助力人们打开通往可信数字世界的大门。