区块链

元宇宙（十）：DID，元宇宙的信用基石

DID 去中心化数字身份，元宇宙最重要的基础设施之一。身份是个体的属性集合，社会经济运行的基石。数字身份包含标识符、属性、凭证等数据要素，传统互联网的身份模型中，用户没有统一的标识符，数据身份无法互通且有安全隐私隐患，数字凭证也因为数据孤岛的问题难以大规模使用。这种身份模型在互联网早期比较适用，但随着数字经济的深化，成为阻碍数字世界的基础设施，而 DID 的出现将成为元宇宙重要的基础设施。

去中心化标识符 DIDs 通过打造应用间互认的身份系统，从而实现去中心化数字身份。由万维网联盟 W3C 推进的 DIDs 标准构建了一套多平台互通的身份系统，由用户控制标识符及对应的数据，控制应用对数据的读写范围和时间。DIDs 从基础设施支持了可验证凭证的大规模应用，参与者可以更低成本的发行凭证、验证凭证。例如，Ceramic 以 DIDs 的方式为 Web3 应用提供身份数据管理服务，目前已经接入 400 多个项目。

灵魂绑定账户，构建原生的数字身份。以太坊创世人 Vitalik 在今年提出了灵魂绑定通证的概念（SBT），即不可转移的 NFT。从技术属性来看，NFT 是天然的凭证，也在实践中被常用作验证身份的凭证。但可转移性限制了作为凭证的应用发展，而 SBT 对于用户来说，相当于一种开放且低成本的数字凭证。拥有大量 SBT，如学历、活动证明、工作证明、项目证明、俱乐部证明等等，可以描绘一个用户的数字画像。这种数字身份是完全数字原生，它可以与现实身份不产生任何关联，但在数字世界中存在社会性。

平衡开放和隐私。灵魂代币改变了数字画像的模式，用户从被动的被贴标签，变成了主动地可知地寻找标签，主动权和控制权回到了用户手中。由于链上信息的开放性，会产生信息过度暴露的问题，对此有几个解决方案，其技术复杂度和功能有所不同包括 SBT 映射链下隐私数据、零知识证明用于验证结果等等。

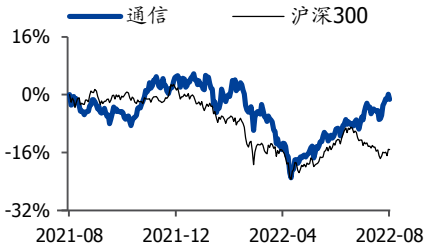
身份数据开放互通，创建 Web3 跨生态可信凭证。数字身份解决了 Web2 时代个人信用无法跨平台互通的痛点，将数字画像从基于应用收集数据的封闭型转为基于开放数据和可信凭证的开放型，而链上数据的开放可信性也让 Web3 简历、Web3 社交名片、无抵押借贷得到更好的应用。但不可忽视的是，数字身份的兴起或将使得 Web3 养号贩卖的黑产更加严重，相关反制措施也值得关注。

投资建议：去中心化身份是元宇宙发展的前置条件，有着巨大潜力与社会性。“地址+私钥”的账户范式转移是 Web3 数字身份发展的第一步，确定性最强，钱包、域名、数字签名收益。数字凭证是发展空间最大的赛道，关注目前链上凭证基础设施，将受益于 SBT 概念落地。基于数字身份的“去中心化信用贷”是 Defi 大规模推广的关键，值得期待。

风险提示：代码漏洞风险；区块链政策监管风险。

增持（维持）

行业走势



作者

分析师　宋嘉吉
执业证书编号：S0680519010002
邮箱：songjiaji@gszq.com

相关研究

1、《通信：下半年通信行业出口怎么看？》2022-08-14
2、《通信：低估值高成长三剑客》2022-08-07
3、《通信：北美云 Q2 高景气，有哪些预期差？》2022-07-31

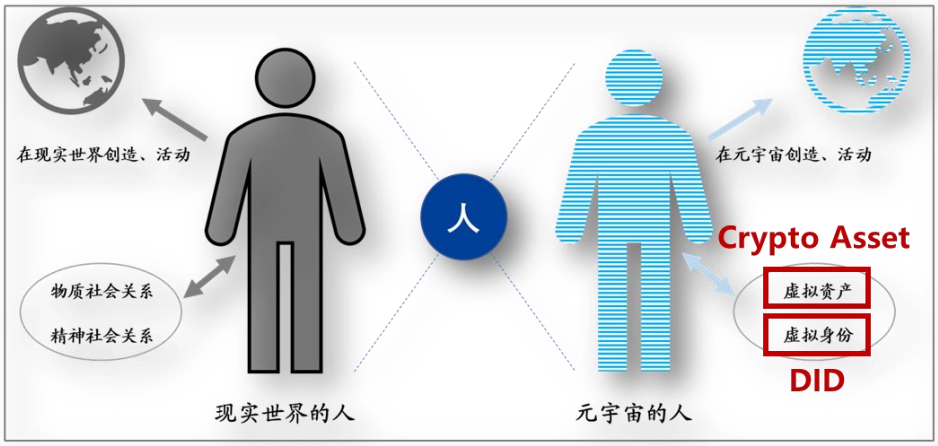
内容目录

图表目录

传统互联网的数字身份以平台为中心，同一集团内的不同产品间通过账号系统打通，例如腾讯的邮箱、游戏、金融等皆可使用同一账号，但腾讯体系以外，该账号却不能通行。在去中心化身份（Decentralized Identity，DID）中，用户成为自己数字身份控制者。用户可以控制自己的身份数据，允许什么信息被记录，什么信息被谁读取使用，可以跨平台转移使用。

从技术角度看，DID 试图解决互联网目前的发展瓶颈，使得更丰富的数字经济活动能够实现。现实世界中，身份系统是社会运行和经济活动不可缺少的一部分，身份证、学历、驾照等证明我们的身份和资质；同时，声誉和信用更是商业和金融得以拓展的关键。一套可以跨越平台的身份记录，使得互联网下一阶段的发展成为可能。

图表 1：元宇宙的构成与映射



资料来源：公开资料、国盛证券研究所

DID 是元宇宙的基础，身份模型不革新，互联网应用难以从“工具”变成“世界”。在 WEB3 可组合性与金融属性的加持下，DID 快速迭代，并将改变数字世界。

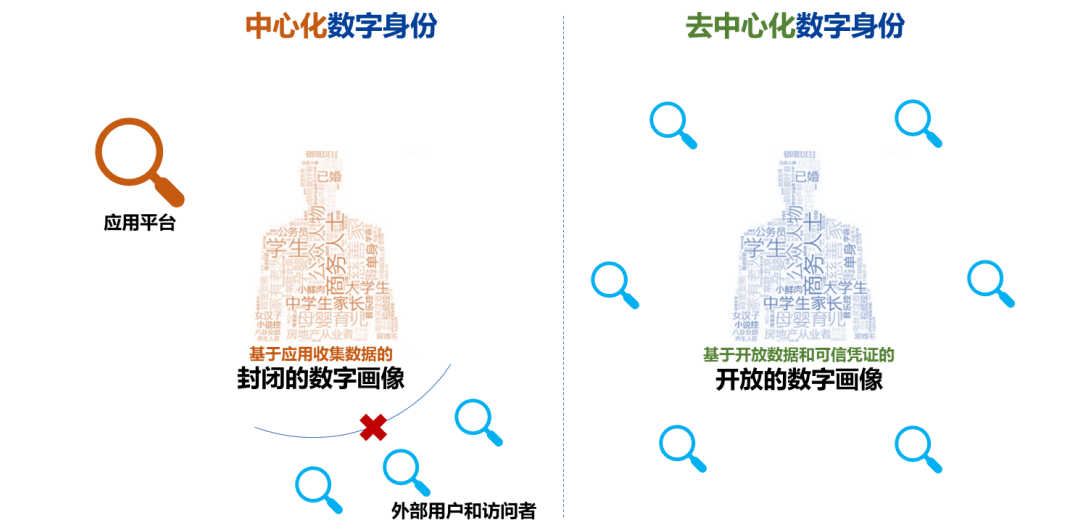
图表 2：数字身份的对比

	传统互联网	去中心化标识符（DIDs）	灵魂绑定账户
标识符	分散的账号	统一的标识符 连接所有账号	以太坊地址
身份数据	由应用存储控制	可信数据库、用户控制	链上+链下，用户控制
凭证	数据库分散的记录	可验证凭证VC	灵魂绑定代币SBT
特点	用户缺少控制权，身份数据脆弱且封闭	用户控制、数据互通、凭证应用场景广	数据可信且开放、原生的数字身份（可与现实身份无关且有社会性）

资料来源：公开资料、国盛证券研究所

DID 互通开放，是基于开放数据和可信凭证的数字画像。数据的互通保障了数字身份在 Web3 中的开放性与可识别性，而先前通过用户的数据所构成的“立体可信的数字形象”也不再仅仅为应用平台所掌控，而是面向了所有用户。

图表 3：数字身份的对比



资料来源：公开资料、国盛证券研究所

1. 元宇宙需要新的数字身份

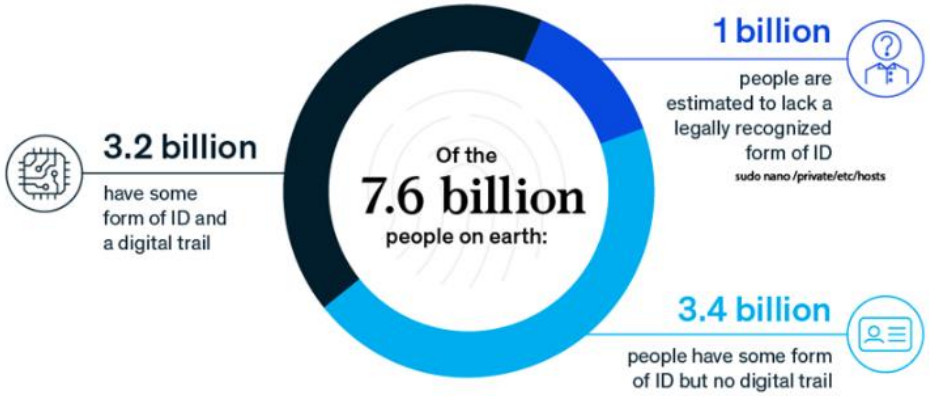
身份是社会经济运行的基石，数字世界的进一步发展，需要一套可靠互通的数字身份系统。但在传统互联网模式下，我们有大量的账号，身份不统一，应用存储着我们的身份数据，既不可靠也不互通。在互联网早期较为孤立、较为工具化的时代，这种方式并无问题，但现在我们的数字身份价值提高、互联网对现实的渗透加强，这套身份模型以展示出诸多弊端。

1.1 什么是数字身份？

数字身份解决了“我是我”（标识符识别身份）、“我是谁”（属性描述身份）以及“证明我是谁”（凭证验证身份）的问题。

身份，个体的属性集合，社会经济运行的基石。在现实生活中，身份伴随我们一生，代表着个人在社会活动中扮演的角色，可以包含性别、年龄、职务等诸多属性，通过身份可以对每个人进行识别和区分。**国际标准化组织将身份定义为“与实体相关的属性集”**，在运行良好的社会里，公民身份服务由政府提供。我们现有公民身份，才有绑定于其上的学生身份、法人身份、驾驶员身份，社会经济运行离不开安全可靠的身份系统。基于身份的实体声誉和信用，更是商业和金融得以拓展的关键。

图表 4：全球的身份情况



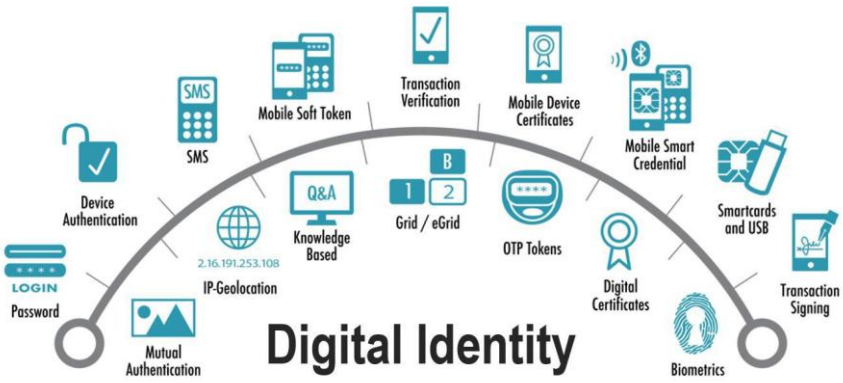
资料来源：世界经济论坛、国盛证券研究所

数字身份是标识符和对应的属性数据。严格来看，网络空间中的实体都拥有数字身份，包括人、设备、组织、应用，通过数字身份来被区分和辨认。本文主要从用户和互联网应用的角度讨论数字身份，所谓的身份就是用户的标识符和属性集合。唯一标识符实现对用户的识别，通常由注册机构发行，比如我们的网络账号。标识符对应的属性能够反应用户的特性与本质，使得用户能够在网络活动中被应用和他人识别，比如我们在账号个人信息中的电子邮件、性别等等，数字身份标识着网络活动中的每一个实体。

图表 5：数字身份的构成

资料来源：公开资料、国盛证券研究所

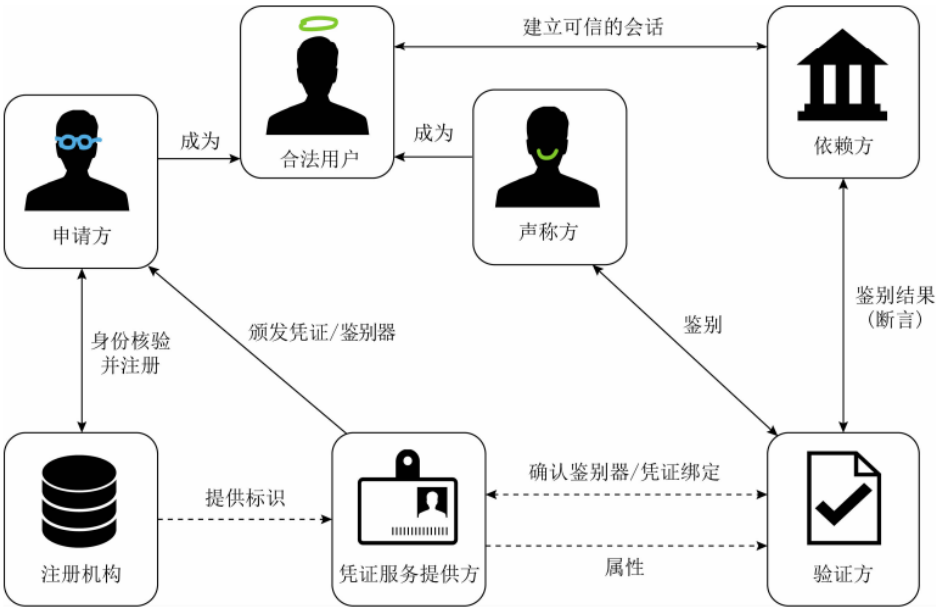
图表 6：数字身份标识网络空间的实体



资料来源：公开资料、国盛证券研究所

数字凭证用于确定用户的数字身份和属性是否属实。既然数字身份唯一识别某个实体，那么必然引申出验证数字身份的概念——凭证。类比到现实中，学历是我们的属性，那么学历证书就是验证我们属性的凭证。国标《信息安全技术术语》中对于“凭证”的定义为：“**为确定实体所声称的身份而提供的数据**”。整个业务流程还涉及到凭证的签发方，需要验证凭证的依赖方，以及验证凭证的验证方。

图表 7：数字身份模型

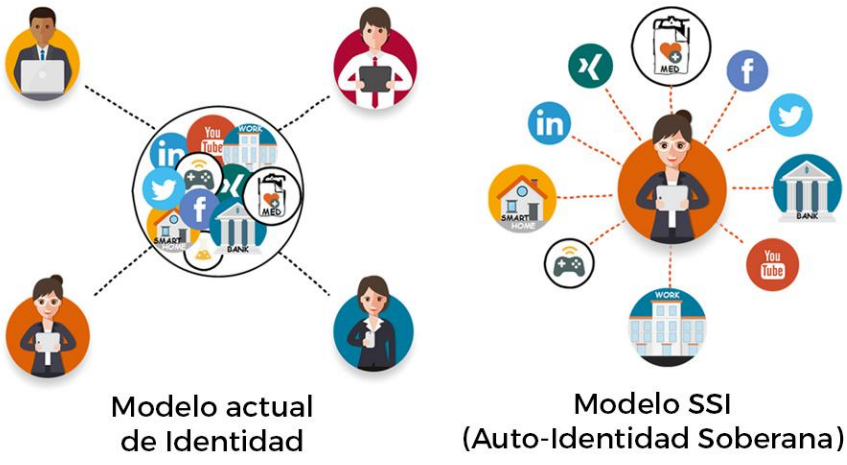


资料来源：《数字身份安全治理研究》李俊、柴海新、国盛证券研究所

什么是好的数字身份系统？数字身份系统在技术上有着多个评价维度，2018 年达沃斯世界经济论坛提出：一个好的数字身份应该满足这 5 个要素。

1） **可靠性：**好的数字身份应具备可靠性，建立起用户对数字身份的信任。用户能有效行使自己身份的权利，以证明他们有资格获得某些服务；
2） **包容性：**任何需要的人都可以建立和使用数字身份，不会被身份系统所歧视（例如禁用），也不会面临身份删除的风险；
3） **可用性：**数字身份易于建立和使用，提供多种服务的交互和访问；
4） **灵活性：**用户可以选择如何使用他们的数据，决定谁来使用、使用范围和时间；
5） **安全性：**安全性包括保护个人、组织或各种设备免遭身份盗用和滥用，不会出现未经授权的数据使用和侵犯人权等。

图表 8：自主控制数字身份 SSI 图示



资料来源：ResillienteDigital、国盛证券研究所

用户画像，即用户数据标签化。随着互联网活动的扩大，围绕着用户身份产生了大量数据。互联网公司内保存了用户大量的原始数据和业务数据，用户的一切行为在企业面前是可追溯和分析的，如何更有效的利用这些数据进行精细化运营，这便需要用户画像。通过收集用户的社会属性、消费习惯、偏好特征等各个维度的数据，进而对用户或者产品特征属性进行刻画。用户画像的主要用途是定向广告投放与个性化推荐，是数据驱动运营的基础。

数字画像是从我们的数据集合中推测的属性，而非我们自己声称的属性。在当前的模式，用户只对数字画像有感知而没有知情权和控制权，譬如 AI 推荐的内容符合用户的偏好，尽管用户没有声明过自己的偏好。

图表 9：用户画像

资料来源：公开资料、国盛证券研究所

图表 10：数据标签

用户画像前：行为日志 ⇨ 网络日志 ⇨ 服务日志

用户画像后：

用户 ID	年龄	性别	教育程度	兴趣
2124214	27	男	高中	{汽车：0.1，体育：0.3}
2235325	35	女	博士	{科技：0.2，电影：0.7}

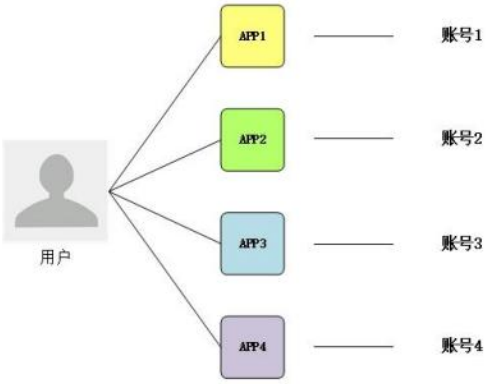
资料来源：大数据 DT、国盛证券研究所

传统模型不适应 Web3 新环境，数字经济需要新基石。数字身份的重要性在提高，一套账号不仅是访问服务的凭证，更代表着用户的数字形象、社交网络、虚拟资产等数据资产。互联网从最开始没有身份层面的原生设计，数字身份交由应用服务提供商处理，这种模式更适用于较为简单且孤立的早期互联网，而如今显示出一系列问题，阻碍了数字经济活动的进一步拓展。

1.2 传统互联网数字身份的问题：脆弱、封闭

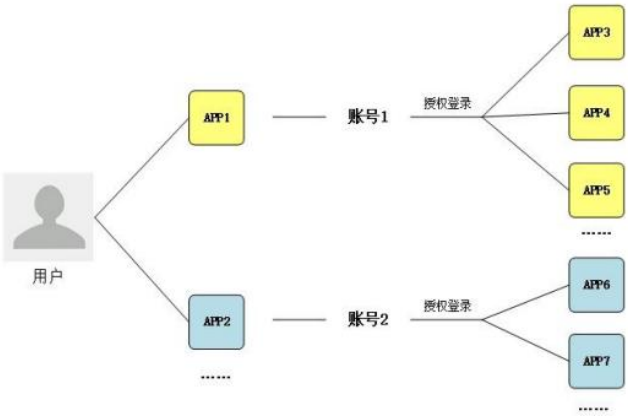
互联网应用平台负责数字身份的注册和身份数据的管理。传统互联网发展以中心化服务为特征，网络应用提供商各自管理账户，用户通过向特定应用注册账户密码的方式来创建自己的数字身份，数字身份数据由应用服务商管理。随着社交网络的发展，许多服务提供商倾向于通过联盟身份的方式获取用户信息，即用户能够使用某个服务的凭证登录到另一个服务，甚至允许不同的服务共享有关用户的详细信息，这种方式为用户身份提供了一定的可以移植性。但带来了更严重的数据问题，数据被科技巨头高度垄断，数据风险与隐私泄露也日益严重。大家可能都有过类似的经历：不同平台的密码设置要求不同，登录后多个账户名和密码难以记住。

图表 11：一对一登录方式



资料来源：《区块链技术下的身份研究》邹琳、国盛证券研究所

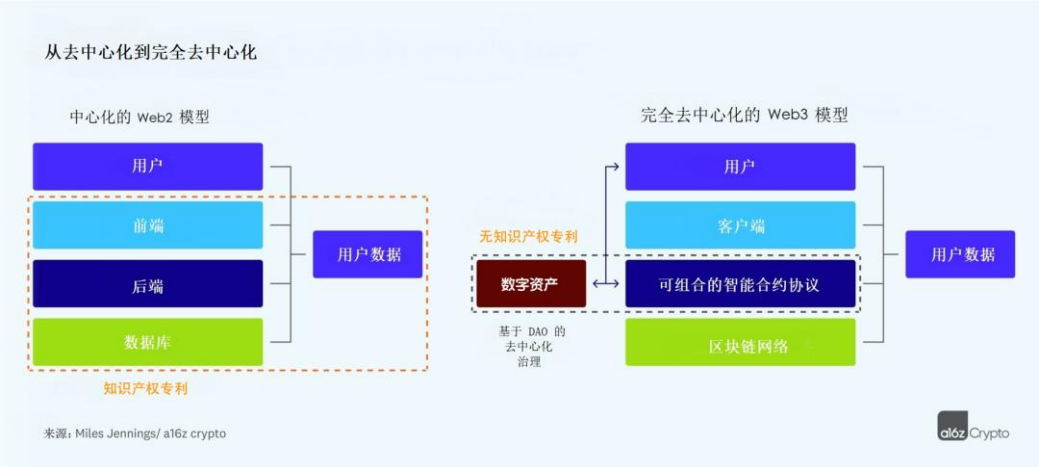
图表 12：一对多授权登录方式



资料来源：《区块链技术下的身份研究》邹琳、国盛证券研究所

现有数字身份的脆弱和封闭，使得用户无法相信在目前的模式下，他们所构建的数字身份是有着长久意义的。账号密码数量的增加的同时，也带来了泄露、盗用账号的风险。当平台停止运营时，用户的数据难以迁移，所构建的数字身份便被抹去了。而用户的身份权利也没有十足的保障，毕竟应用可以对特定用户关上访问自己数据的大门。这种脆弱的身份模型，阻止了互联网应用的进一步发展。

图表 13：数字身份模型对比



资料来源：a16z、国盛证券研究所

1）“账号-密码”认证方式难以匹配日趋复杂的应用生态。通过注册账号密码识别用户的方式产生于互联网早期，在互联网应用较为孤立的时期较为合适。而当互联网应用快速发展时，用户的账号密码数量会不断累积。据 NordPass 统计，平均一个人拥有大约 100 个密码，这一数字还在持续上涨。这不仅影响着用户体验，还带来了安全问题。根据 Ponemon 的统计，53%的人完全依靠自己的记忆来记住密码，而 51%的人在工作和个人账户中重复使用相同的密码。用户有着共有密码的习惯，同时大部分人不会经常更新密码，这导致密码在大规模数据泄漏事件中暴露的可能性就越大。

图表 14：Collection 1-5 事件，在 2019 年暴露了超过 27 亿对邮箱密码

资料来源：intego、国盛证券研究所

2）用户身份数据的可靠和互通。在现有模型下，用户并没有真正拥有线上账户。事实是他们从公司和中心化的组织租赁账户。因此，用户被暴露在数字身份被黑、被操控、被监管、或是丢失的风险。2017 年，征信企业 Equifax 遭黑客攻击，导致 1.43 亿用户的个人信息被泄露，其中包括姓名、社会安全号、住址等等重要内容。2018 年，Facebook 将 5000 多万用户信息提供给剑桥分析公司一事更是引发全球关注。身份数据无法迁移，个人数据分散在不同的平台里。用户需要在不同应用反复填写相似的信息，个人数据分散在不同的平台，随着应用生态复杂度的提高，现有框架难以维系。

图表 15：2020 数据泄露关键词

资料来源：安全 419、国盛证券研究所

3）不互通的数字凭证。平台 A 给用户的身份确认，在平台 B 上是无效的。目前的数字凭证大多都是通过信息系统的简单数据记录来实现，易于修改和伪造，并且经常暴露出不必要的信息。例如电子会员卡，虽在便利性上有所提升，但仍面临数据孤立、易丢失、不安全、隐私泄漏的问题。凭证是当前数字身份的弱项，很少存在发证方与验证方不同的应用场景。