元界 数字身份白皮书

修订历史

版本	描述	作者	日期	邮箱
V1.0	初稿	黄蓁林、 陈 浩 、 Ahemed	201706	

目录

摘要 Abstract

Metaverse Project （简称 MVS，中文名元界）。

元界是一个基于公有区块链技术体系的去中心化平台，涵盖了数字资产和数字身份。元界通过构建一个 2B2C 通用技术平台，将资产数字化，例如我们可以将珍稀物品（艺术品/古董）数字化、知识产权数字化、票据基金等收益权数字化，提升市场运作效率，通过数字身份，将一个一个的价值孤岛连接成价值互联网络。

数字身份将基于元界的生态体系搭建，根据元界区块链提供的底层功能，围绕 BaaS 及钱包来开展数字身份的应用，以期为各行各业提供可验证、可授权的基础设施服务。

1 介绍

实际场景中的身份问题通常以“你是谁”开始。互联网的兴起，使得数字身份在各个行业中的应用变得越来越普遍，同时，很多企业和个人也意识到了数字身份的重要性。随着大众与服务提供商的互动显著增加，用户名和密码成为我们进行身份验证的常见方式。但是，这样做存在一些问题，比如与各类中心化机构建立联系需要创建一个数据库环境，有些技术不过关的身份提供商很容易受到攻击。此外，目前的身份系统由于彼此之间不互通，存在重复登记的问题，并且，在不同环境下，某一方的身份证明会反复被要求提供，这样做会浪费大量时间和资源。

随着科技的迅猛发展和进步，很多目前的商业模式、流程以及解决方案在新兴技术崛起之前都不存在。在这些新技术中，最具突破性的是区块链技术，它能像互联网最开始兴起一样改变许多行业。该技术首先用于比特币，现在正为金融、供应链以及防伪等行业存在的问题寻找解决方案。最重要的是，区块链上的数字身份应用正被区块链和身份专家进行广泛研究。此刻，有超过 40 个区块链身份项目正在投入研究，无论是在公有区块链上创建应用程序，还是把 PKI 与区块链相结合，数字身份都还有很长的路要走。

1.1 身份问题：区块链中缺失的环节

在当前的区块链生态系统中，存在一系列不同的区块链协议和实施方案。所有身份问题都会进入这样一个程序，即：证明谁拥有什么和谁做了什么。虽然匿名性在比特币这样的协议中具有一些优势，但是当区块链技术及其应用在全球实施时，匿名性并不是一个强大的特质。我们需要知道我们正在处理的是什么，我们通过名字对人们的身份进行识别，而不是一串数字。而在许多公有区块链协议中，身份问题常常被忽略。这是一个缺失的环节，因为它可以让区块链数字资产的概念蓬勃发展，并让区块链上的金融应用在数字银行体系和其它金融机构中发挥作用。

因此，在协议级别嵌入数字身份是有意义的，它使得用户可以更方便的为公有链上的应用程序构建可验证的功能。此外，我们还注意到了邀请中间人到链上所具备的价值，因为它们在用数字身份去证明和验证某人的声明时起到了关键作用。

2 数字身份（Avatar）

2.1 元界介绍

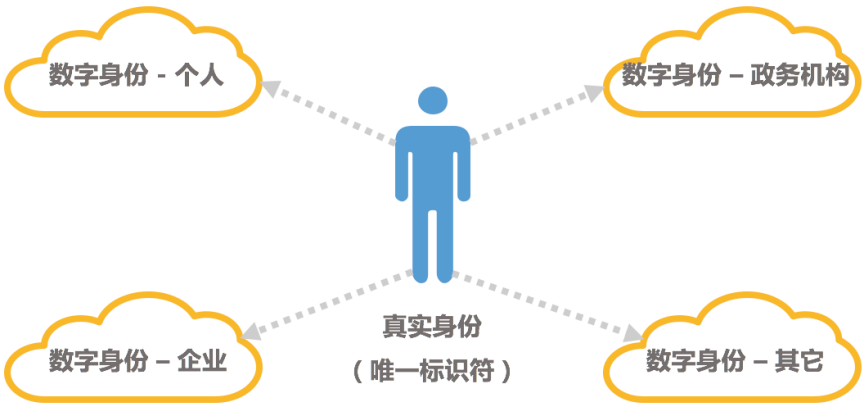
元界旨在为广大用户（无论是个人、企业还是政府机构）提供方便安全的基于区块链的基础设施。元界的三大核心要素是数字资产、数字身份和价值中介，其目的是建立一个具备智能属性的网络，它们将为元界上的所有去中心化应用提供协议级的支持。

随着我们的生活变得更加数字化，元界及其核心要素将利用互联网的优势为用户展开一个数字化的虚拟世界。数字身份的持有者将能够轻松地处理任何类型的资产，并允许企业和社区通过许多形式来支持自己，最终促使我们走向价值互联网之路。

2.2 数字身份的本质

元界的数字身份是独特的，身份识别模块将被内置于协议中，并开发有辅助支持它的应用程序。用户具有确定的自主身份，即用户可以完全控制自己的身份，这就意味着不必依赖中央实体或第三方进行身份验证。用户拥有真正意义上的自主身份，可以创建、签署、验证，同时与用户进行交互的人也能够证明其身份。此外，这些拥有自主数字身份的用户能够选择性地披露他们的信息。

数字身份是虚拟世界不可分割的一部分。就其本身而言，数字身份可以采取任一形式，如个人或价值中介（机构和实体）。 因此，个人在不同的场所可以拥有不同的数字身份，如职场身份和家庭身份，但这些最终都是以用户的现实身份为基础。



用户可以通过数字身份在元界建立自己的声誉，同时这也会改进我们交换价值的方式。它可以通过数字签名、验证要求和交易来实现这一目的，并逐步树立起可以被市场上其他数字身份和价值中介检查和验证的声誉基础。对于一些中心化实体，如果他们的服务器崩溃，那么它们多年树立的身份和声誉将永远消失。元界则不同，用户的数字身份及其声誉将受到区块链的保护。

2.3 适用案例

在区块链协议中嵌入一个身份系统，这样的适用案例有很多。

拥有许多不同的数字身份，例如一个数字身份可以向乙银行说明某用户已经在甲银行开设了帐户，正由于此，乙银行将授权用户开立一个银行帐户，理由是该用户已经在甲银行开设了一个帐户。在同一法律管辖内，这一案例可以在银行间进行复制。

除此之外，数字身份也适用于数字版权等领域，终端用户将能够使用他们的数字身份来声明版权或其他资产，除了授权他们的认证信息外，用户也能够授权他人访问私有数据如声誉、信用等数据。

3 技术概述

元界的账本包含三种类型：**数字资产账本，数字身份账本，Data-feed 账本；**
与元界等数字资产账本一样，数字身份的账本也是基于 ETP 的交易体实现；
我们在分析了诸多案例后发现，数字身份的核心功能只有两个：身份验证、操作授权；

故我们提出了以下设计目标：

- 数字身份能够体现与数字资产的关联关系——**资产关联关系**；
- 数字身份能够导入链下数据，并且在对应关系中能够提现 Oracle 信用背书的特性——**Data-feed**；
- 数字身份能够统一管理多个互联网应用的身份信息——**应用管理**；
- 数字身份的能够提供不可篡改的信用数据集——**信用数据可采集**；

3.1 数字身份的定义

数字身份是用户所拥有的主私钥所对应的账户的 Profile 信息的统称。Profile 拥有一个全网唯一标识，在元界中，我们称该标识为 DID（Digital Identity，可类比比特股的别名）。数字身份包括 Oracle 的角色和普通用户的角色，任何数字身份都可以作为 Oracle 和普通用户参与在数据身份的应用中来。

Profile 包含以下信息：

* 个人交易记录

- 统计级别，记录明细，无需额外存储

* 资产信息

- 统计级别，UTXO 明细，无需额外存储

* 自定义描述字段

- 自定义字段具有时效性，使用该字段应当指明在哪个高度区间有效，该记录可变更，对应不同区块高度有效。

- 该字段以 key:value 的形式提现，没有上限，但是使用该字段个数的所收取的费用服从指数函数。

- 需要额外存储

（其中统计级别的信息会在下面的“信用数据可采集”中详述）

3.2 数字身份的操作流程

3.2.1 创建

任何用户都可以创建数字身份，并与自己的主私钥绑定。

如果用户创建完数字身份，并未绑定任何主私钥，那么该 DID 相当于一个未经认证的账号，无法使用数字身份的任何功能与应用。

已在元界区块链上登记资产的主私钥持有者也可以选择不关联绑定任何数字身份，这是一个主动的过程，元界不会为用户自动创建数字身份，数字身份的关联权掌握在主私钥持有者手中。

3.2.2 验证

Profile 能够提供有效的证明链，该证明链能够提供该数字身份下的客观事实。对于用户来说，首先需要证明的即该数字身份属于我：通过把交易绑定到 DID 上即可（交易域包含 DID 信息）。

3.2.3 授权

首先需要弄清楚授权的场景，授权往往是和交易相关的。授权过程往往是伴随着下述场景的：假设 A 请求 B 的数字身份信息：资产信息。目的是核对 B 的资产，然后才能提供服务。这样会出现两种可能：

第一种是 B 的链上资产非常多，ETP 有 100 万个，那么 B 在收到请求时，直接授权 ETP 资产信息给 A 即可。

第二种是 B 的链上资产不多，但是链下资产比较多，传统的做法是 B 需要将资产转换成 ETP 进行授权，目前元界推荐的做法是发行自己的资产，并让 Oracle 对资产进行证明，这之后该资产也作为有效资产进入数字身份的信息中。

- **授权过程：**

A 向 B 发送一个验证资产的请求，该请求触发一个脚本，脚本去验证目标账户的资产信息，随后返回一个结果，该结果是 A 加密的结果，B 并不知道哪个结果是对应验证通过的信息。并且请求也是一个加密信息，B 并不知道 A 的具体请求，但是知道请求哪一项信息。而对于个人交易记录、资产记录，只需链上进行授权访问，原理相同。

对于个人自定义字段，与资产的 Oracle 证明类似，（没有经过 Oracle 认证的字段信息也可以授权，但是不推荐）。

如果个人定义的字段是非公示信息，比方说邮箱手机号，则无需进行 Oracle 认证，如果是证明类信息如学历证明，则需要 Oracle 认证。

- **认证过程：**

个人自定义信息认证

使用 Oracle Data-feed 进行背书。引入第三方 Oracle，该 Oracle 在链上公示所有 Profile，供公众查询监督，并且 Oracle 通常是机构，机构也应当在官网公示自己的 Profile 和 DID 信息。

B 首先在自定义字段处填写需要证明的信息，Oracle 需要使用自己的主私钥匙对其签名，并动用一个比较大额的币天对该字段进行背书。

A 可在链上请求该字段的信息，包含 Oracle 背书信息，则 A 可认为 B 的信息有效，A 可继续对 B 提供服务。

3.2.4 查询

由于数字身份一开始已经引进 DID 标识的概念，因此，可以把 DID 标识作为在场外交易的主体，具备在交易市场中创建交易的功能。

通过在交易市场中的地址查询栏中输入 DID，我们可以查询到该 DID 正在发布哪些交易请求，以及公开市场中的历史交易记录。反过来，某一 DID 在市场上的交易行为和记录，同样可以用作构建数字身份的数据。

3.3 资产关联关系

数字身份与主私钥是一对多的关系，一个数字身份可以对应多个主私钥；数字身份与资产必定是一对多的关系，发行的资产必定属于某个地址，某个地址必定属于某一个数字身份。数字身份不可转移和销毁，对应用户现实中的关系是可变更的。

3.3.1 数字身份与数字身份的关系

数字身份与数字身份之间的关系只表现在链下，比方说数字身份 A 下面只有一项数字资产 A 公司，数字身份 B 下面只有一项数字资产 B 公司。若 A 公司收购 B 公司，那么数字身份 A 和 B 可在线下公示该资产所属关系的变动，但链上无法体现这种所属关系，即不能体现数字身份 B 属于数字身份 A。

某个数字身份下的资产可以转移给另一数字身份，但是这种转移行为只能作为信用评级中的数据留痕，而不去体现两个数字身份间的任何关系。

3.3.2 数字身份与资产的关系

数字身份与资产的关系，体现在数字身份下面资产的转移。仍然是上面的例子，A 公司收购 B 公司，在线下达成协议后，B 公司的资产代币在线上转移给 A 公司资产代币所在的地址，完成了资产的登记工作。此时，数字身份 B 不再持有 B 公司这项资产，数字身份 A 的构建成分包括了 A 公司和 B 公司。

3.4 链下数据管理——Data-feed

- **链下数据与资产登记**

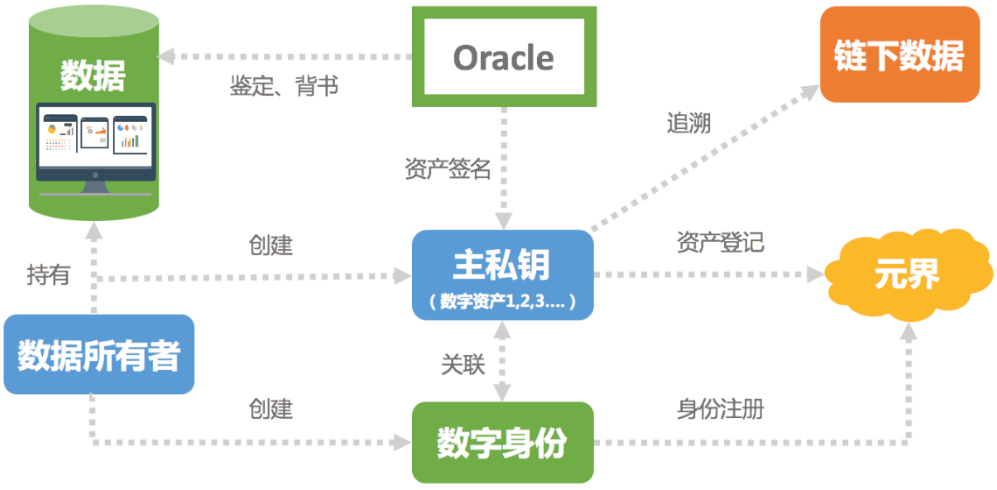
链下数据指的是那些没有记录在区块链上的数据，那将是数据结构更为复杂，数据体量更为庞大的数据。我们将要做的就是将链下数据和对应的数字身份关联起来。

这就跟现实世界中的权益类登记有些相似，即由某个权利人创造出来的智力劳动成果经由专门的权益类评定机构进行评审和鉴定后，满足条件的将登记为专门的权益。今后想要借用该项权益的人需要付费给其所有者来获得使用权。除此之外，所有者也可以通过一定的手续转卖该项权益的所有权，并获取一定的收益。

同样的，在元界的生态当中，每项数据都应该有其对应的所有者。我们也可以将每项数据看作是每笔资产或者说是一个代币。该代币上包含了这笔数据的详细信息以及这笔数据的所有者。那么，为了保证这笔数据来源的真实性以及有效性，我们需要引入 Oracle 对这笔数据进行背书，不同类型的数据需要不同的 Oracle 提供不同的鉴定标准或字段进行评审。最后将由 Oracle 用其私钥对这笔数据进行签名以表示该笔数据资产的有效性。经由这些流程过后，数字身份就对某项数据相互关联了起来，我们可以将这笔具有所有权的数据称之为**有效链下数据**。

与数字身份相关联的有效链下数据的登记，大致需要以下四步：

1、 拥有数据的用户在元界建立其数字身份，并提供其自定义格式的数据，将数据打包提交给负责数据鉴定与背书的 Oracle；
2、 具备鉴定数据资格的 Oracle（数字身份的一种）鉴定该数字身份所提交的数据的有效性、真实性；
3、 经数据所有者和 Oracle 签名后的资产将通过主私钥与数字身份绑定；
4、 其他用户可以在数据所有者的授权之下，查看该数据资产所代表的详细信息。



我们知道，某些权益类资产在持有时是可以产生收益给其所有者的。那么在元界中，由于数字资产与链下数据相关联，因此数字资产同样也能给其所有者带来收益。数字化链下数据，将为其带来流动性，链下数据可以被份额化，同时被多个数字身份持有，而各份额的所有者可将该数字资产转卖给其他的数字身份。

- **链下数据与预测市场**

区块链业内的预测市场，本质是对于链下数据的一种集合，在预测时，数据可以期权的形式表现出来。作为一种金融类应用工具，预测市场是链下数据的另一类管理形式，我们鼓励第三方基于元界区块链搭建预测市场的应用。

3.5 应用管理

在传统互联网应用中，其数据库都是以中心化形式进行管理，这就注定了其账户信息及账户资产信息无法跨平台进行流动。例如支付宝账户无法用来登录微信应用，微信的资产余额也无法在支付宝应用中进行使用。

数字身份的诞生便可以解决账户无法跨平台使用和账户资产无法跨平台流通的痛点。用户只需一个元界的账号，就能在不同的应用平台之间进行登录和访问，且可在这些应用中共用元界钱包中的资产。

应用管理的流程：

首先，这些应用平台本身必须在元界中注册为数字身份，并在自己的数字身份上定义出自己的标识符。接着使用这个数字身份，关联相应的主私钥，将元界钱包服务配置进其应用之中。

接下来，这些应用平台的用户需要在元界上注册数字身份，用于在各应用平台之间互相登录。当用户使用数字身份在各应用平台登录时，可以选择性的将身份信息授权给应用平台，而无需再次注册和认证身份信息。

当用户想要使用跨地域的应用时，这样操作也节省了账户注册时的繁琐过程，用户也无需在不同的应用中，以不同格式的身份信息去做一些实名制（例如 AML 和 KYC），只要一个数字身份，便能在各个应用平台进行访问。应用平台只需根据用户授权出来的信息以平台自有的一些规则来判断该用户能够使用哪些权限下的功能。

用户的数字身份并不隶属于任何一个中心化的应用平台，拥有数字身份的用户无需担心自己的数字身份被任何一个应用平台删档、泄漏甚至篡改里面的资金或者信息，因为用户能够选择性的将自己数字身份中所绑定的信息授权给其他应用平台，未经授权的信息，该平台

则无法读取。所以，我们能看出数字身份的所有权和使用权是真正意义上完全掌握在用户手中的，只有用户自己才能决定数字身份中资产的增减。这样做，不但保护了用户的身份安全及隐私，还保障了其资产的安全。

3.6 信用数据可采集

（元界区块链本身不提供信用评级，但是会为信用评级提供客观有效的数据集）

数字身份的信用数据采集，根据该数字身份下面资产的各项情况来确定，具体统计信息包括：交易记录统计、资产信息统计及风险识别。在数据搜集完成后，对三个类别中能够数据化指标化的信息作出综合分析，把某一数字身份的相关统计信息按照在全网相关信息下所占百分比来表示。

数字身份持有者可以授权给第三方应用，由第三方交易平台提供这些资产在交易平台的价格数据，并作为统计依据。目前提出了以下三种统计类信息：

3.6.1 交易记录统计

元界上的资产转账，会在区块链上留下转账记录。数字身份拥有人确认是否将相应的一个或多个主私钥用来构建数字身份，钱包可以根据接入的区块浏览器数据，对每个地址的每笔交易情况进行分析，并根据以下几个维度来确定某一数字身份下面的多个地址的交易信息：

- ✧ 一定时间内每个地址资产的转入转出数量：按照资产占总资产数的百分比来确认
- ✧ 一定时间内每个地址资产的转入转出金额：如果资产有接入交易市场，则按照资产在市场中的交易价格来确认金额（价格可以按照日线 MA20 的价格来确认）；如果资产没有接入交易市场，则按照在钱包内资产转让时付出的其它代币的交易市场价格（比如 ETP）来确认价格，ETP 的价格确认方法同上。

3.6.2 资产信息统计

针对数字身份对应的主私钥下的资产，做一个资产信息统计。这部分主要统计三个信息：

- ✧ 对该身份所持有的资产进行类别的判断：
  - 金融资产（数字货币，即 ETP/BTC/ETH 等，应收账款及附加利息，衍生品等）
  - 实物资产（对应现实中的实物型资产，包括房屋及建筑物、运输设备、机器等）
  - 无形资产（对应现实中没有实物的资产，包括专利权、著作权、土地使用权等）
- ✧ 各资产占该数字身份总资产的权重：金融资产、实物资产及无形资产这三大类在该数字身份里的总资产占比
- ✧ 各资产占全网同类资产的权重：计算出金融资产、实物资产和无形资产中，每项具体资产占各自总量的百分比，再根据在市场中最后三次交易的价格计算出权重，若某项资产没有交易记录，则不被记录到权重中，以此来鼓励资产流动，即促使资产所有者在网络上创建出交易记录。在统计过程中做如下判断：
  - 资产是否存在过往交易记录
  - 如果进行过交易，则在市场交易记录里提取最后三次交易的平均价格

某DID的资产组成情况

全网占比					
金融资产		实物资产		无形资产	
BTC	x%	房屋及建筑物	x%	专利权	x%
ETP	x%	设备 / 机器	x%	著作权	x%
…	…	…	…	…	…

3.6.3 风险识别

针对每个地址下的资产代币进行风险数据的采集和识别工作。目前我们可以将风险数据归为一下几个类别：

- **异常地址标识**

通过搜集某数字身份对某地址的举报来进行异常行为的标记（tag）。异常行为包括：该地址可能被用来敲诈、勒索等，每次举报需要消耗一定数量的 ETP，且每个 DID 只能标记某个地址一次，付出 ETP 的成本可以防止某一方对于地址的恶意举报，并且由于举报方是以 DID 的名义，构建数字身份的过程是一个渐进的留痕过程，数字身份持有者出于对于自己信用记录构建的谨慎性，会更倾向于提供真实准确的信息。只有异常标记超过某一数值时，系统才会提示地址异常。

- **异常 DID 标识**

由于地址与数字身份挂钩，所以同样，一旦某个主私钥下的一个或多个地址被标记为异常地址的次数超过某一数值，则可能该地址归属的数字身份的信息，也被标识为异常状态。

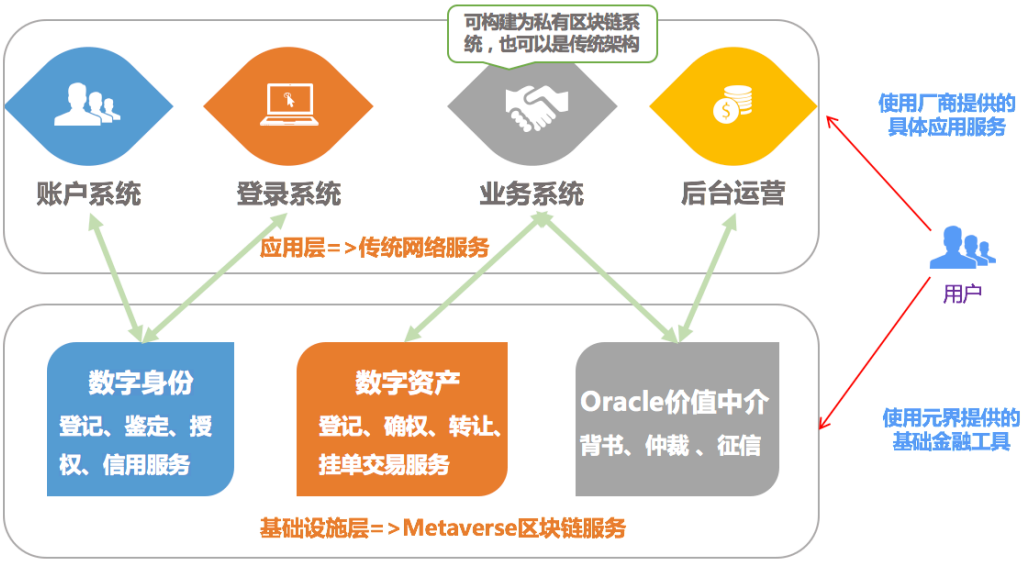
此外，一旦 Oracle 对链下数据进行了更新，而数据包含的信息显示，该数据的持有人在进行一系列非法活动，并处于包括但不限于被通缉、羁押等异常状态时，该数字身份同样也会被标记为异常。

- **资产价值波动情况**

根据资产在交易市场的每日加权振幅来确认资产价值的波动，再根据该数字身份所拥有的全部数字资产权重，来计算出总资产的波动情况，用户可以设置预警百分比，并在达到相应振幅时进行风险提示。

3.7 数字身份与 BaaS (Blockchain as a Service)

元界首次提出了基于公链的 BaaS（区块链即服务）的概念，即企业或个人可以根据自己的实际需求，向区块链解决方案供应商定制区块链服务。



- **用户群**

元界的 BaaS 框架主要面向商业用户，例如有交易管理需求、资产管理需求的个人或企业。随着元界基础设施的不断完善，其服务对象可能不止于此类用户，商业用户的划分也不能再以传统的形态来判断，它将可以是任何主体，即广义上的数字身份。

- **资产登记**

数字资产的登记是整个数字身份体系中最为重要的一环。任何主体都有权利作为用户对象在元界上发行资产。该环节是商业用户接受 BaaS 服务的必要途径。

- **构建数字身份**

数字身份与 BaaS 服务是互相依赖的关系，个人和企业的数字身份数据可以帮助元界为企业提供 BaaS 服务，而在服务中产生的数据流和信息流，则可以反哺数字身份，形成发展的可持续性和生态闭环。

- **BaaS 服务**

1、*基于数字身份进行对象管理：*

BaaS 服务将会以数字身份作为参与的主体来服务商业用户。存在关联交易的商业用户同时在元界区块链上登记资产，能够为彼此的数字身份增信，提升其有效性。

2、*对链上数据进行深度挖掘和检测：*

商业用户或者第三方均可以利用元界的数字身份数据，对相关内容和交易历史进行深度挖掘和检测。

3、*提供一体化的资产管理底层服务：*

- ✧ BaaS 本质上是对商业用户登记在元界区块链上的资产加以利用，从某种程度上来说，这是一类偏底层基础设施的资产管理类服务，元界会在客户端中提供基础的应用模块框架。
- ✧ 除了元界本身提供的基础 BaaS 服务外，未来，可能还会有更多第三方介入元界的区块链服务，相当于一类辅助工具或者插件，以帮助使用元界 BaaS 服务的用户能够更好的实现使用和管理上的优化。
- ✧ 元界的 BaaS 服务相当于整合了传统的一系列上下游以及周边生态的企业服务方式，强调了一体化的数据供给和管理。

4、*为关联交易方提供透明的信息授权：*

接受 BaaS 服务的用户不是一个独立、或是割立存在的主体，一旦某个 BaaS 用户与其它用户产生关联，那么数字身份中的验证、授权和查询功能将被激活，使得 BaaS 用户之间存在追溯渠道，提供有信用背书的交易与合作方式。

BaaS 框架

3.8 数字身份与交易中介

任何第三方交易中介均可以接入元界区块链，来自第三方的注册用户以登记在元界上的

数字身份为主体。数字身份所有者对交易中介进行授权，就可以在中介平台上进行资产的购买和转让。与元界提供的资产转让服务不同，交易中介更加侧重资产的流动性，除此之外，每个数字身份还可以在其上进行高频交易等操作。交易中介本身即为一类可定性为 Oracle 的数字身份，原则上讲，任何数字身份都可以申请成为交易中介，但是有信誉的交易中介（数字身份），能够吸引用户加入其中，以降低交易风险。

在用户授权数字身份后，只有资金的转入转出数据会被登记到链上，而交易中介内部的交易数据，属于链下数据。

为了保障交易中介的运行安全和用户隐私，元界区块链会在浏览器中引入另外的第三方 Oracle 为交易中介背书，作为公证人的角色参与到用户与交易平台之中去。

3.9 数字身份的应用场景

在实际应用场景中，我们需要把数字身份授权给请求授权的公司，这些公司来自各个领域，随着元界数字身份基础功能的不断拓展和完善，它的应用范围也会更加延伸。

3.9.1 征信

目前征信行业已建立有很多不同的信用数据渠道，数字身份提供的用户画像可以在数据上为征信领域进行一个数据反哺。随着数字身份的不断完善（登记的资产项目增多、交易 / 档案信息增多），某个人的数字身份更有可能作为一个主体数据源，颠覆现有征信行业的生态模式，将所有数据网络联结在一起，打通其它应用接口，覆盖到更多的个人和企业，改善现有征信数据拥有者之间数据不互通不共享的问题，将资源进行合理的配置，大幅提升风控水平。就像征信本身属于其它很多领域的基础设施一样，用数字身份作为征信的目的来使用，同样是区块链行业的一种基础设施。

3.9.2 借贷

- **资金端：**

数字身份可以帮助持有人判断自己拥有的数字资产，并根据数据统计评估可投资的金额。资产管理机构可以接入有效的数字身份，为用户定制个性化的资产管理方案，以提供专业的理财服务。数字身份本身具备的数据采集和分析功能，可以进行资金流向的追踪和查询。除此之外，一些理财类工具也可以由此切入，帮助数字身份持有者管理日常现金流，并根据统计数据帮助用户进行理财。

- **资产端：**

1) 可以利用数字身份，对借款人的行为记录和信用状况进行是否发放贷款的决策。其中的重点仍然是建立用户画像，把某个数字身份授权给相关机构，这样贷款机构能够一键得到所有信息，并快速决策。
2) 由于某一数字身份背后的所有人可能是个人，也可能是企业。所以在企业的供应链环节中，可以利用到数字身份，并在下面两方面发挥作用：
   i. 身份鉴定：数字身份中的验证、授权功能，能够帮助合作方了解企业过往的交易记录以及资产状况，以便更好的评估企业经营状况并进行信用分析。
   ii. 角色管理：企业也可以对自己的数字身份进行管理，通过对自身所持资产和交易记录进行统计和风险评估，可以帮助企业更好的了解自身的运作情况。

   在这个过程中，可以对核心企业、供应商及经销商的数字身份做出综合分析，达到简化供应链融资流程的目的。

3.9.3 保险

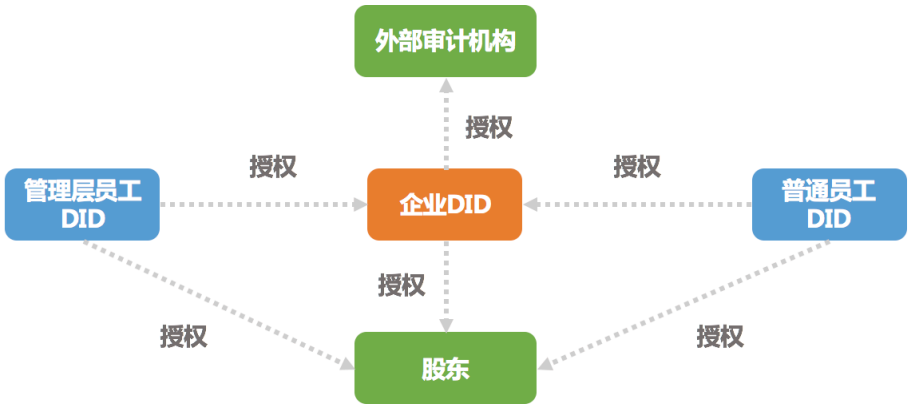
数字身份在保险行业有着最为直观的应用，因为保险服务直接与个人身份信息挂钩。随着传统保险公司开始互联网化，以及越来越多垂直型保险产品的出现，被投保方的数字身份有利于保险公司对于数字身份持有人的持续追踪。其效用体现在以下方面：

- 核保与承保：对参保人的数字身份进行风险评估，能够快速获取到的信息包括但不限于：登记于区块链上的医疗记录、职业状况、资产价值等。保险公司最终可以通过数字身份来划分风险类别和确定细节条款。
- 理赔：保单可以作为资产登记于链上，不可篡改，并隶属于某个数字身份。在保险事故发生后，保险公司可以按照约定对相关人员进行保险赔偿。

3.9.4 审计

企业本身可以拥有自己的身份，而在企业内部，从 CEO 到普通员工，从部门 A 到部门 B，都可以创建属于自己的数字身份，员工可以将自己的数字身份授权给公司或股东，这样有利于其他股东了解自己的合伙人或者员工的可信赖度。

外部机构在对某家企业进行审计时，同样可以利用验证和授权功能浏览到登记在区块链上的资产状况（例如，应收账款、应付账款等），这一点可以与 BaaS 服务结合起来。相关审计人员可以通过对区块进行实时追踪来监控公司的账务情况，并可以出具资产情况说明及相关审计报告。相比传统的审计方式，区块链上登记的资产，本身由权威的 Oracle 背书，简化了之前工作量极大的审计流程，减少了审计机构对于审计人员的依赖，提高操作的自动化程度，节约员工成本。



3.9.5 政府

各国政府可以将居民的身份信息写到元界区块链上，这些身份信息包括但不限于：证件号（身份证、护照、驾驶证等）、采集自本人的生物信息（指纹、面部识别等）、个人档案（学历学位、亲属情况、犯罪记录以及其他可以被记录在案的信息），在这个过程中，政府及其他权威机构相当于 Oracle 的角色，所有的这些数据组成了某人的数字身份的 Data-feed 部分。

在很多场景下，如机场火车站的安检、考试时考生入场，检查人员都可以对数字身份上的信息与本人进行验证，如果生物识别正确，那么在被授权的情况下，检查人员可以得到所有相关的信息，包括与生物信息关联的其他档案记录。数字身份可以帮助我们：

- 节约身份验证的时间：只需要用户通过安检时，对其生物特征进行快速扫描，即可快速验证到所有信息。
- 节约身份验证的成本：比如警方在对罪犯进行追捕时，可能需要对生物信息采集，然后带回机构去进行验证，而如果警方想得到更多该人员的档案信息，还需要从很多其它机构调用相关信息，使用数字身份则简化了流程上的复杂度。

政务部门除了可以利用数字身份进行监管执法外，数字身份还能在日常的政务活动中发挥作用，比如税务登记、机构投票、股权登记等。

4 结语

随着元界数字身份体系的不断完善，未来，元界将会提供更多基础性的区块链服务设施，以便更多第三方开发者能够基于元界进行应用插件的开发，让更多普通用户能够便捷地使用我们的数字资产及数字身份的登记与管理服务。

参考文献

1. Metaverse Whitepaper: http://newmetaverse.org/white-paper/Metaverse-white-paper-v2.1-EN.pdf

2. Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf

3. Metaverse: https://en.wikipedia.org/wiki/Metaverse

4. Delphy Whitepaper: https://delphy.org/papers/Delphy_Whitepaper_EN.pdf

5. Bitshare Whitepaper: http://docs.bitshares.org/bitshares/papers/index.html

6. Augur Project: https://augur.net

7. IPFS Whitepaper: https://ipfs.io

8. Waves Project: http://www.wavesplatform.com/downloads.html

9. Bitcoin Days Destroyed: https://en.bitcoin.it/wiki/Bitcoin_Days_Destroyed