Weldentity 综述

1. 身份标识与数据交换现状分析

1.1 传统互联网身份标识与数据交换

多年以来，实体身份标识（Identity）技术都是用户访问互联网上服务和资源的基石。一般来说，传统的身份标识流程如下 :用户 (User) 在访问服务方 (Service Provider）时，首先需要跳转到身份标识提供方（Identity Provider）进行验证并获取身份，只有通过身份验证，方可继续访问互联网服务。

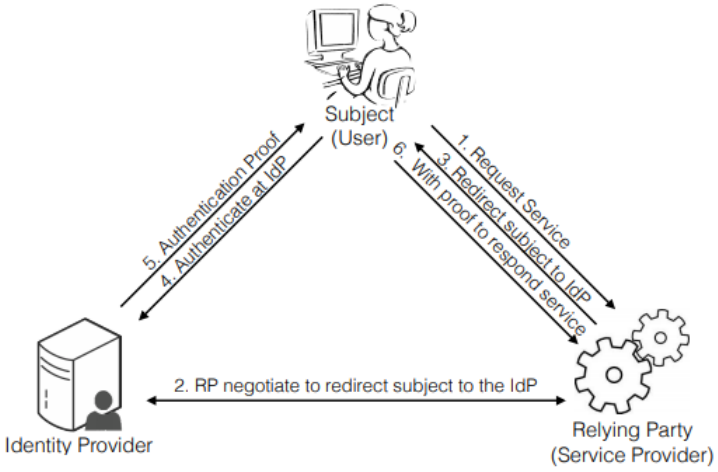

图 1 身份标识及验证的一般流程

传统互联网绝大多数实体身份标识系统都极其复杂，充斥着第三方信任根及中间人存在。世界上最普遍使用的是中心化身份管理组件（Centralized IDM）[1]，用户需要通过密码登陆或证书的方式来访问服务。这一流程，客观上要求用户不得不将巨量的隐私数据存放在服务方机器里。由于各服务方的安全防护能力良莠不齐，用户数据往往处于危险境地。举例，2017 年，马来西亚的一个数据服务方泄露了近 5 千万互联网用户的数据[2]。2018 年，东南亚有超过 20 万名器官捐献者的数据从政府数据库中泄露[3]。《中国网络空间安全发展蓝皮书》显示，每年因个人信息泄露等遭受的经济损失高达数千亿。网络黑产，从半公开攻击模式转化为敛财工具和商业竞争手段，形成跨平台、跨行业的犯罪链条。

另一类方案是联盟身份管理（Federated IDM）[4]。类似 Facebook，Google，微信等巨头通过使用 OpenID[5]、OAuth 2.0[6]或 OpenSAML[7]承担了独立的身份标识提供方的角色，允许用户在不同的网络服务方上使用同一个角色进行单次登录。尽管这种做法增强了安全性，并提供了一定程度上的统一化 KYC 解决方案，但是也进一步将用户数据的统治权集中化到巨头手中，导致数据管理呈现寡头化的趋势。进一步地，数据寡头占有大量数据但又不能完全覆盖所有领域，导致数据场景化、碎片化、孤岛化，数据源多而零散。

不论是中心化还是联盟身份管理，一个绕不过去的问题就是数据滥用。由于缺乏透明度，数据的主权不明确，个人作为数据主体的角色是缺失的，用户授权

信息很难实现准确同步与共享，技术上也难以追踪数据使用的链条[8]。从法规上，由于隐私保护的法律法规、事后追责机制等相关体系的不完善，企业滥用个人数据这种行为当前更多停留在商业道德层面上的谴责。

另一个难以解决的问题是数据共享与数据交换。在传统互联网场景中，数据交换方往往会通过第三方软件或云平台（如联盟身份管理）进行数据共享的方式实现，数据泄露风险较高。另外，数据接收方事实上是难以判断数据真实性和合法性的；数据交换方难以了解被交换出去的数据是否会被进一步滥用。由于这种道德困境的存在，数据共享和交换的产业化工作还处于举步维艰的阶段。

最后，一个安全隐患在于数字证书体系本身。当前的公钥加密体系（PKI, Public Key Infrastructure）的信任根是所有的 Root CA（Certified Authorities，可信证书颁发者）。然而，Root CA 存在着一系列的问题，例如：它们可能会为不可信的站点滥发证书[9]；单点失败，导致所有的子树和叶子证书全部失效[10]。此外，Root CA 绝大多数为（海外）大型商业巨头所掌控，存在安全层面的不可控因素。

1.2 标准和规范

美国商务部提出的隐私保护方案是 2016 年通过的“隐私盾框架”，主要用于厘定欧盟与美国之间的居民数据流转，随后也成为中欧数据跨境的事实框架。美国与欧盟在个人数据保护的松紧程度不同是推动“隐私盾”协议出台的深层原因。美国坚持灵活保护的策略，致力于通过企业自律机制，并配合政府执法，以实现保护隐私权的目的；欧盟却倾向于通过严厉的立法，对个人数据进行保护。隐私盾核心内容是欧盟的“充分性决定”草案、替代方案及约束性企业规则。

欧盟在 2018 年 5 月通过的 GDPR[11]（通用数据保护条例）建立在之前隐私盾框架的基础上，对个人隐私信息的保护及其监管达到了前所未有的高度，且自生效之日起对所有成员国的公民均立即适用于法律。GDPR 主要包括三类权利：

- 知情权：主要指数据所有者必须明确告知用户其收集个人信息的原因，用途，以及保存时效。如果个人信息还将分享给第三方，必须明确通知用户相关情况并让其决定是否同意授权发送数据。
- 访问和更正权：用户有权访问其提供的个人信息，并进行修改。当用户递交访问申请时，数据所有者必须在一个月内对用户申请作出反馈，并且在绝大多数情况下不能对该访问申请收费。
- 删除权：又名“遗忘权”。即用户有权要求数据所有者删除其之前提供的个人信息。特别需要注意，如果用户的信息已经被数据所有者透露给第三方，或者在互联网进行了公开发布，那么当用户行使删除权时，数据所有者必须通知所有拥有该用户数据的第三方一并删除。

APEC 成员国的跨境隐私保护规则——CBPR 体系包括以下四大要素。一是自我评估：数据控制者根据 APEC 制定的“跨境隐私规则问卷”进行自我评估。二是合规性审核：数据控制者将填好的问卷以及相关文件提交给 APEC 认证的隐私责任评估机构，由后者按照《APEC 跨境隐私规则体系》的要求进行审核。三是认

证和公开：通过审核的数据控制者将公布在 APEC 网站上，公布的内容包括该数据控制者、隐私责任机构和隐私执法当局的联系方式。四是争议解决与执行：获得认证的数据控制者，将受到该 CBPR 的约束，隐私责任评估机构可以按照当地法和合同执行跨境隐私规则，隐私执法当局也可以按照本国法对经认证的数据控制者采取相应的执法措施。

我国 2018 年实施的《个人信息安全规范》里面关于隐私保护的描述包括七大原则：权责一致原则，对个人信息主体合法权益造成的损害承担责任；目的明确原则，具有合法、正当、必要、明确的个人信息处理目的；选择同意原则，向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意；最少够用原则，除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息；公开透明原则，以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；确保安全原则，具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；主体参与原则，向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

当前，着力于解决上述安全和用户隐私问题的权威国际组织，主要包括 DIF[12]（Decentralized Identity Foundation，分布式身份标识基金会，**微众银行从 2019 年开始也成为核心成员之一**）和 W3C 的 DID（Distributed Identity，分布式身份）、VC（Verifiable Credential，可验证凭证）两个工作组。组织致力于实现分布式身份标识和数据交换的开放生态，目前正在建立的规范包括以下两个：

- W3C DID 规范[13]：定义了自主可控的数字标识符。它建立在区块链的基础上，指出了链上的数字身份生成的方式、表示格式、链上属性、认证和授权方式及安全规范。
- W3C VC 规范[14]：定义了用于数据展示和交换的可验证数字凭证。它建立在密码学基础上，指出了安全可控可移植的数据交换的格式规范、披露规则、管理撤销规则等。

1.3 基于区块链的分布式身份解决方案

面对传统互联网实体身份标识和数据管理存在的问题及新的标准、新的规范，区块链成为了解决问题的有力工具。当前，在区块链领域里最为常见的解决方案就是将身份标识提供方放到区块链上，由区块链的参与方共同保证，消除上述的安全隐患。这里的技术基石是分布式公钥体系（DPKI，Distributed PKI）[15]，系统不再需要数字证书和 CA 的存在，所有加解密和数字签名的安全由参与方写入链上保证。这种做法的好处在于两点：首先，基于区块链抗单点攻击的特性，即使有少数参与方被攻破，也不会影响到链上身份数据的安全。其次，数据的流转过程写入链上之后也不可由少数参与方进行篡改。

当前，国外较为完善的竞品主要有两个：uPort[16]和 Hyperledger Indy[17]。uPort

是建立在以太坊网络上的自主身份解决方案。用户的身份由一对公私钥生成，私钥由用户保留，公钥被转换成地址并写入以太坊公链的链上智能合约里。作为以太坊生态的一部分，uPort 主要的发展方向是作为身份提供方，接入各种以太坊的智能合约应用；用户所产生的数据被存入基于 IPFS 协议的线下数据库里，链上只存这些数据的 Hash。Indy 是由 Hyperledger 和 Sovrin 基金会搭建的带许可性质的区块链自主身份解决方案。它也由公私钥对来生成用户身份并存入链上合约，但其区别在于它是联盟链，参与方仅包括连接到链上的各机构，且有联盟链的治理能力：节点的参与、审核及退出都需要联盟链督导会接纳。它最成功的落地案例是在加拿大的英属哥伦比亚省的政务链 VONX.IO[18]，引入了数十家企业、政府机关作为信任源。自 2018 年上线以来，链上的身份认证、凭证发布和授权请求已达到数千万。uPort 和 Indy 都符合 W3C DID 和 W3C Verifiable Credential 标准，也都是 DIF 组织的核心成员。

国内实体身份标识方兴未艾。Weldentity 是目前国内最大的分布式身份和数据交换解决方案，已在澳门、四川等多个政务链、企业物联网链项目中落地。除了 Weldentity，还有中钞区块链旗下的络谱[19]和本体 ONT.io[20]。Weldentity 和络谱使用带许可性质的联盟链，本体使用公链。目前，两者暂无成型的落地项目。

2. Weldentity 方案介绍

Weldentity 是一套分布式多中心的实体身份标识及可信数据交换解决方案，实现了一套符合 W3C DID 规范的分布式多中心的身份标识协议，和符合 W3C VC 规范的可验证数字凭证技术，使分布式多中心的身份注册、标识和管理成为可能，机构也可通过用户授权合法合规地完成可信数据交换。

2.1 功能与角色

Weldentity 生态主要提供以下三个核心功能：

1） 实体标识（WeID）：是 Weldentity DID 的简写，为每个实体（人或物）在区块链上创建符合 W3C DID 规范的数字身份 ID 标识，如“did:weid:1:0x8011cf2892985cdc58f447063bc6a089ba89f514”。链上的 DID 除了公钥以外，不会记录任何对应于这个 DID 实体的敏感身份信息。

2） 电子化凭证（Credential）：符合 W3C VC 规范的可验证数字凭证。真实数据就存放在这里。Credential 由凭证发行方所颁发，记录了发行方确认过的数据，并由发行方使用自己的私钥进行数字签名来保证其安全性。凭证验证方通过将凭证的签名和链上的发行方公钥进行对比，来确认凭证安全合法未篡改。由于包含真实的原始数据，Credential 的原文不会上链，凭证发行方可以选择将凭证的内容进行 Hash 后上链。Credential 的原文一般存放到凭证发行方的数据库里，其副本可以托管在用户代理处。

3） 用户授权即交易（Authorization）：原始数据的跨机构传输需要得到用户授权。授权记录的产生和上链由用户代理完成，符合 GDPR 要求。

WeIdentity 生态主要包括以下角色：

角色	说明
实体（Entity）	实体对象（人或者物），拥有链上身份 ID，可授权相关机构使用自身相关数据。
凭证发行方（Issuer）	对数据进行发行和认证的机构或个体。 权威机构发行的数据具备权威性，个体发行的数据不具备权威性，权威机构的认定取决于具体业务场景及参与角色。
凭证验证方（Verifier）	使用数据的机构，可验证数据是否被篡改、是否经过凭证发行方认证。
用户代理（User Agent）	为用户生成 WeID 及提供 KYC 服务，一般为权威可信机构，实体通过该机构与链上身份或数据进行交互。

下图是一个不同角色间交互的工作流：

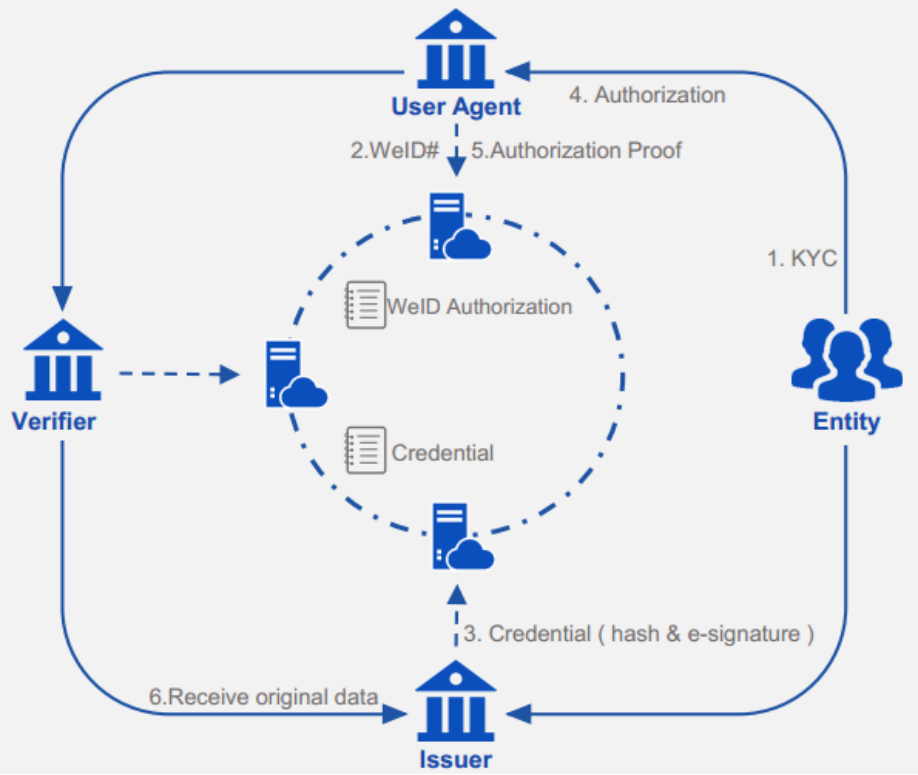

图 2WeIdentity 工作流

一般来说，一个典型的 WeIdentity 的工作流包括以下步骤：

1） 实体（人或物）进行 KYC，确认身份和属性
2） 实体通过用户代理，生成 WeID，并将其注册到链上
3） 实体为了办理某种业务，访问凭证发行方；凭证发行方验证核实实体身份，并发行对应的数字化业务凭证
4） 实体访问凭证验证方。实体通过用户代理创建一个授权请求
5） 用户代理将授权请求发到链上，及凭证验证方
6） 如果实体携带了业务凭证，就可以直接出示给验证方；或者，验证方也可以

拿着这个授权请求，到凭证发行方处拿到业务凭证的原文

7） 实体可以对凭证进行选择性披露，只披露部分数据，不影响验证方的结果

2.2 架构

Weldentity 的架构如下图所示：

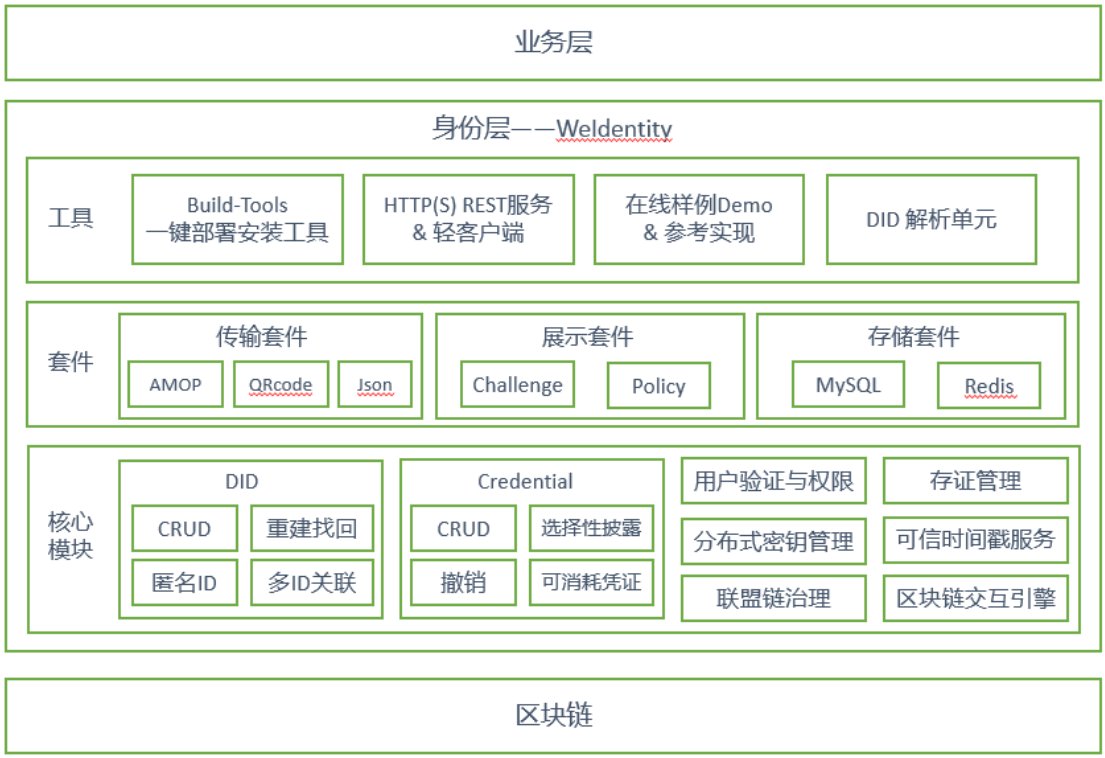

图 3Weldentity 架构图

Weldentity 属于联盟链的架构。参与各方需要搭建区块链，并在其上部署 Weldentity 的相关智能合约。未来，Weldentity 会提供建立在云服务提供商之上的节点镜像以供快速部署。Weldentity 的架构定位是身份层，上面承接业务层的身份标识和数据交换请求，对下接入区块链节点。它主要包括核心模块、支持套件和易用工具三个组成部分。各模块详细介绍见下。限于篇幅，更详细的模块介绍可见 Weldentity 的在线文档仓库： https://weidentity.readthedocs.io

2.2.1 核心模块

Weldentity 的核心模块包括：

- DID：实体数字身份标识模块
  - 基本功能：包括链上实体数字身份标识的生成、读取、属性更新、删除
  - 重建找回：当 DID 使用者的私钥丢失或被攻破的时候自动生成或找回
  - 匿名 ID：负责 DID 使用者自动创建匿名 ID 去发交易
  - 多 ID 关联：负责 DID 使用者管理自己使用的多个 ID
- Credential：可验证凭证模块
  - 基本功能：包括凭证的生成、验证

    - 选择性披露：用于当使用者只愿意披露凭证中的**一部分真实数据**
    - 撤销：凭证的发行方使用去中心化的方式撤销所发行的凭证
    - 可消耗凭证：一类有使用次数的凭证，可以被消耗
- 用户验证与权限管理模块：用于管理 DID 使用者的身份验证和链上权限
- 分布式密钥管理模块：用于提供 DID 的私钥安全可信托管功能
- 联盟链治理模块：用于进行联盟链的治理，为联盟链的成员和授权机构进行角色划分和功能裁定
- 存证管理模块：用于将凭证生成数字摘要并打包签名发送到链上（“存证”），以供未来进行链上完整性校验
- 可信时间戳服务模块：实现基于联盟链的可信的时间校准和时间戳服务
- 区块链交互引擎模块 :和区块链进行 I/O 的模块。当前 Weldentity 支持 FISCO-BCOS 的所有版本，未来还将支持 Fabric 和 Ethereum。

2.2.2 支持套件

支持套件包括一系列支持 Weldentity 周边功能的模块：

- 传输套件：为链上的各机构进行链上传输的套件。目前，我们支持使用基于 FISCO-BCOS 的 AMOP 链上传输协议，以 Json、二维码的形式将数据凭证进行跨机构传输；未来还将支持 Protobuf 的传输。
- 展示套件：符合 W3C Verifiable Presentation 规范[19]的套件，机构可以定义完成某项业务所需要的凭证类型及属性，使用者可以将多个凭证打包进行批量验证。
- 存储套件：支持使用者或机构将生成的凭证进行离线存储的套件。目前支持 MySQL，未来还将支持 Redis 和 Oracle DB。

2.2.3 易用工具

易用工具包括：

- Build-tools，一键部署安装工具。可以使用这个工具快速地部署安装 Weldentity 的智能合约及 SDK。
- REST 服务端与轻客户端 提供以 HTTP/HTTPS 方式访问 Weldentity 的功能。
- 在线样例 demo 与参考实现：一个在线交互式的 Weldentity demo 及其参考实现，体验 Weldentity 主要流程，见 :http://fintech.webank.com/weidentity。
- DID 解析器：提供对任何符合 W3C DID 规范的 DID 进行解析的页面。

2.3 应用行业与领域案例

下图是 Weldentity 的一些标杆应用场景：

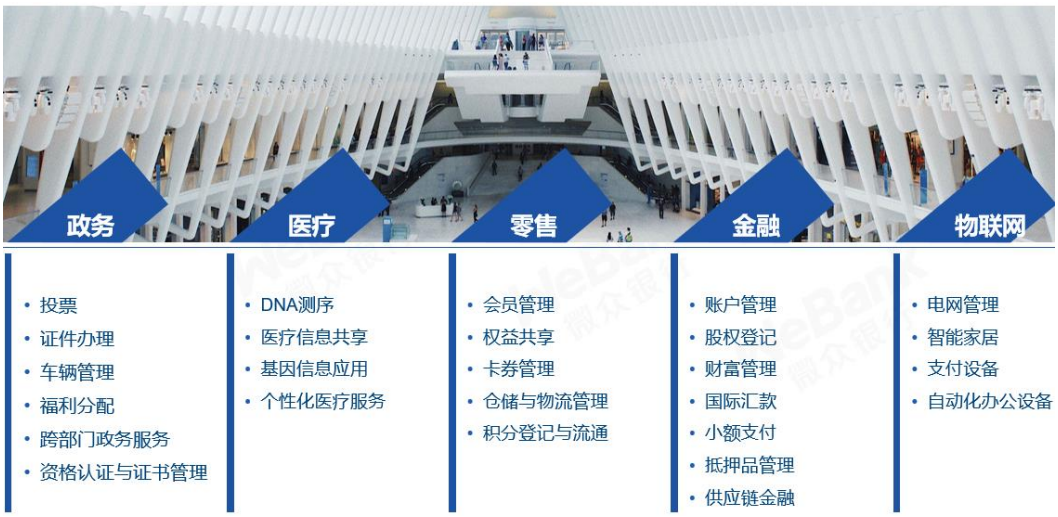

图 4 Weldentity 标杆应用场景

我们选取了两个标杆案例用来介绍 Weldentity 的典型使用场景：

案例 1：员工入职背景调查

- 背景

合作方是一家中小企业，在招聘员工时需要对员工的学历信息、之前雇主信息进行真实性验证。存在的问题是：对员工而言，需要去每个机构花费大量时间精力获取最新版的材料。对企业而言，材料的获取和流转的过程中可能遭到篡改，而且缺乏验证材料真实性的手段。

- 参与方：员工、学校、前雇主公司、现雇主公司
- Weldentity 解决方案及基本流程

1. 员工、学校、公司分别进行 Weldentity DID 注册及 KYC 认证。
2. 员工向学校学校申请学历证明凭证、学位证明凭证。
3. 员工向前雇主公司申请工作证明凭证、离职证明凭证。
4. 员工将这些凭证挂到自己的个人主页上，或者直接提交给现雇主公司，或者授权现雇主公司去数据库中获取。
5. 现雇主公司通过凭证验证（Verify）接口对上述凭证（Credential）进行验证。
6. 验证通过，现雇主公司发放入职 offer。

案例 2：居民信息管理与政务办理

- 背景

居民政务数据存在于不同部门，跨部门的政务办理往往需要先至部门 A 开具证明，再至部门 B 进行办理。对居民而言，流程繁琐且文件不易管理与保存；对政府部门而言，希望提升用户体验并确保用户隐私数据不泄露。通过 Weldentity 解决方案，可以为居民生成可信的电子证件，居民授权后由机构进行验证，从而使用合法合规的方式简化业务流程，降低隐私数据泄露风险。

- 参与方：居民、身份证明机构、证件签发机构、证件验证机构
- Weldentity 解决方案及基本流程

1. 由身份证明机构为居民进行 WeIdentity DID 注册及 KYC 认证。
2. 居民向证件签发机构申请证明文件，证明签发机构按照规范生成电子凭证并关联到居民的 WeIdentity DID。
3. 居民授权证明验证机构对凭证（Credential）进行验证；同时生成一条居民授权记录，存储在区块链上。
4. 证明验证机构通过凭证验证（Verify）接口进行验证。
5. 验证通过，为居民进行业务办理。

3.WeIdentity 评估

WeIdentity 的技术优势在于以下几个方面：

- 开源开放

WeIdentity 的技术方案面向政府、企业、开发者，完全开源，目前总计已经有 20+开源社区维护者。

代码主仓库为：https://github.com/WeBankFinTech/weidentity。

- 隐私保护
  - GDPR：GDPR 主要包括知情权、访问和更正权、删除权。在 WeIdentity 里，数据是以用户为中心组织的；用户数据只有在用户进行授权的前提下才可以从机构数据源转移到其他机构，且用户授权必须在用户使用自己私钥进行签名的情况下方可执行；用户可以将数据摘要上链，如果机构擅自修改数据，则会造成链上链下数据摘要不一致；用户可以要求机构将凭证撤销使其失效。如此，便满足了 GDPR 的要求。
  - CBPR：CBPR 主要的规范是自愿性评估的，其所有保护项都弱于 GDPR，因此可见 GDPR 的相关分析部分。
  - 《个人信息安全规范》:与 GDPR 原则不同的地方是我国额外指定了最受够用原则、公开透明原则和确保安全原则。对此，通过使用选择性披露功能，用户可以将信息最小化披露给验证方，而验证方仍然可以从区块链上得到整体验证结果（已申请专利）；微众银行联合同业推出的 FISCO BCOS 区块链底层平台区块链节点支持监管方参与，现已完全开源，实现了多链并行架构、跨链通信协议、可插拔的共识机制与隐私保护算法、支持国密算法等特性，自主可控、安全可信，技术水平行业领先。
- 互操作性、可移植性：身份标识和数据是符合 W3C DID 和 VC 规范的，同时 WeIdentity 提供标准化接口，支持跨链、跨平台互操作；数据可移植至遵循同样规范的其他 DID 平台（如 Indy、uPort、络谱、ONT），也兼容主流区块链底层平台，同时支持将凭证批量导出到私有数据库。
- 安全可控
  - 信息主体的秘密保护：使用选择性披露，用户可以将信息最小化披露给验证方，传输过程可以选择使用区块链加密进行传输，没有被攻破或监

听的风险；同时支持监管节点进行监管操作。

- 数据共享链：相对于全新的数据共享区块链，Weldentity 优势在于：数据互操作、可移植，符合国际标准规范；更加易用，提供了一整套部署和易用套件；支持选择性披露，可以只披露一部分信息，但仍然可以由区块链上的其他方在不清楚原文全文的前提下判断披露部分信息的有效性；所有信息明文都不上链，不存在区块链节点被攻破导致信息泄露。

参考文献

[1] Zhu, X.; Badr, Y. A Survey on Blockchain-based Identity Management Systems for the Internet of Things. Proceedings of the 2018 IEEE Symposium on Blockchain, Halifax, NS, Canada, 30 July–5 August 2018, pp. 1568–1573

[2] TheStar, M'sia sees biggest mobile data breach, in TheStar. 2017.

[3] Malaysia Kini, After data leaks, Personal Data Protection Act needs review, in Malaysia Kini. 2018

[4] Ghazizadeh E., M., J. L. A., Zamani, M., Pashang, A. A survey on security issues of federated identity in the cloud computing. Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. 2012.

[5] Recordon, D., & Reed, D. (2006). OpenID 2.0: a platform for user-centric identity management. In Proceedings of the second ACM workshop on Digital identity management (pp. 11–16).

[6] OAuth 2.0, oauth.net/2/

[7] OpenSAML 3.0, https://wiki.shibboleth.net/confluence/display/OS30/Home

[8] Wickramaarachchi, G. T., Qardaji, W. H., & Li, N. (2009). An efficient framework for user authorization queries in RBAC systems. In Proceedings of the 14th ACM symposium on Access control models and technologies (pp. 23–32).

[9] https://en.wikipedia.org/wiki/Certificate_authority

[10] https://stackoverflow.com/.../how-to-avoid-the-fabric-ca-beeing-a-single-point-of-failure

[11] GDPR, https://gdpr-info.eu/art-4-gdpr

[12] https://identity.foundation

[13] https://w3c-ccg.github.io/did-spec

[14] https://w3c.github.io/vc-data-model

[15] DPKI, https://danubetech.com/download/dpki.pdf

[16] uPort, https://www.uport.me

[17] Hyperledger Indy, www.hyperledger.org/projects/hyperledger-indy

[18] VONX.io, https://vonx.io

[19] https://www.brop.cn

[20] https://ont.io