WeBank

WeIdentity

基于区块链的『实体身份标识』及『可信数据交换』解决方案

WeIdentity Team
Oct 2019

背景

大数据时代背景下，数据价值往往是通过数据的开放共享来实现，这一过程离不开实体身份标识及数据的可信授权和交换，但传统的解决方案无法满足日益复杂和多样化的实际需求。

数据价值

数据交换共享

网络通 打破平台壁垒
相当于数据运行的“高速公路”

数据通 打破数据壁垒
相当于数据“高速公路”上畅通无阻的车辆

业务通 打破业务壁垒
相当于数据“高速公路”运行的全流程管控

最终
我们都将从数据中受益

数据，已经渗透到当今每一个行业和业务职能领域，成为重要的生产因素。
人们对于海量数据的挖掘和运用，预示着新一波生产率增长和消费者盈余浪潮的到来。
——麦肯锡最早提出大数据时代的到来

2018年我国大数据核心产业规模将突破**5700亿元。**
—— 中国电子信息产业发展研究院《中国大数据产业发展水平评估报告 (**2018**年)》

行业现状

市场需求巨大

根据市场研究机构Smithers Pira预测，2016–2021年，身份和接入管理市场的规模将从80.9亿美元增长至148.2亿美元，年复合增长率达到12.9%。其中，亚洲将占全球个人身份市场的60%以上，按人民币折算，2021年亚洲市场为600亿。

政策鼓励支持

工业和信息化部发布的《大数据产业发展规划（2016 - 2020年）》明确提出：要树立数据开放共享理念，完善相关制度，推动数据资源开放共享与信息流通，促进跨行业、跨领域、跨地域大数据应用，形成良性互动的产业发展格局。

行业方兴未艾

近两年来，政府支持或企业、产业联盟主导的大数据交易平台多地开花，但尚处初级和探索阶段，未形成行业规范和规模效应。而基于实体标识和可信数据交换的数据管理平台更处于萌芽阶段，少有应用案例。

数据黑产盛行

《中国网络空间安全发展蓝皮书》显示，每年我国因个人信息泄露等遭受的经济损失高达数千亿。网络黑产从半公开化的纯攻击模式转化为敛财工具和商业竞争手段，已形成跨平台、跨行业的犯罪链条。

痛点：现阶段数据交换面临的问题

数据孤岛

- 数据场景化、碎片化，造成数据源是多而零散的；
- 数据管理呈现寡头化的趋势，数据寡头占有大量数据，但又并不能完全覆盖所有用户信息；
- 数据类型复杂、标准不一，数据交换缺乏信任源、安全难保障等诸多原因造成数据交换难、共享难。

数据滥用

- 个人作为数据主体的角色缺失，用户授权机制不完善；
- 隐私保护的法律法规、事后追责机制等相关体系亟待完善。

原因：传统数据交换解决方案的缺点

难以形成国际标准

- 面向不同行业、不同场景，用户标识、数据格式均存在不同规范；
- 数据交换过程中接口和协议的定制缺乏通用性。

数据安全风险高

- 传统方案中，数据交换方往往会通过第三方软件或云平台进行数据共享的方式实现，数据泄露风险高。

缺乏用户授权

- 传统数据交换过程中，用户授权信息很难实现实时同步与共享。

数据可信程度存疑

- 数据接收方如何判断数据真实性和合法性。

标准与规范

- 美国：2016，隐私盾法案
  - 适用于中美、欧美间居民数据流转，原则：灵活保护
- 欧盟：2018，GDPR
  - 知情权：使用者需要明确告知数据收集的原因、用途、保存时效；一切第三方分享需要用户授权
  - 访问和更正权：用户有权免费访问所提供的信息并进行修改
  - 遗忘权：用户有权递归地要求使用者删除所收集的数据（包括分享给第三方的数据）
- 中国：2018，《个人信息安全规范》
  - 七大原则：权责一致，目的明确，选择同意，**最少够用**，确保安全，公开透明，主体参与

权威组织

- DIF (Decentralized Identity Foundation)
  - WeBank joins DIF in 2019.1
  - https://identity.foundation
- W3C DID (Distributed Identifier) 工作组
  - Self-Sovereign ID：自主可控的数字标识
  - 基于区块链的分布式PKI实践
- W3C VC (Verifiable Credential) 工作组
  - 用于数据展示和交换的、可验证的格式
    - Verifiable Credential
  - 数字签名可验证、选择性披露、可撤销

方案

WeIdentity提供分布式实体身份标识及管理、可信数据交换协议等一系列的基础层与应用接口，是一套分布式多中心的技术解决方案，服务于泛行业、跨机构、跨地域间的身份标识和数据合作。

WeIdentity应运而生

微众银行自主研发

完全开源

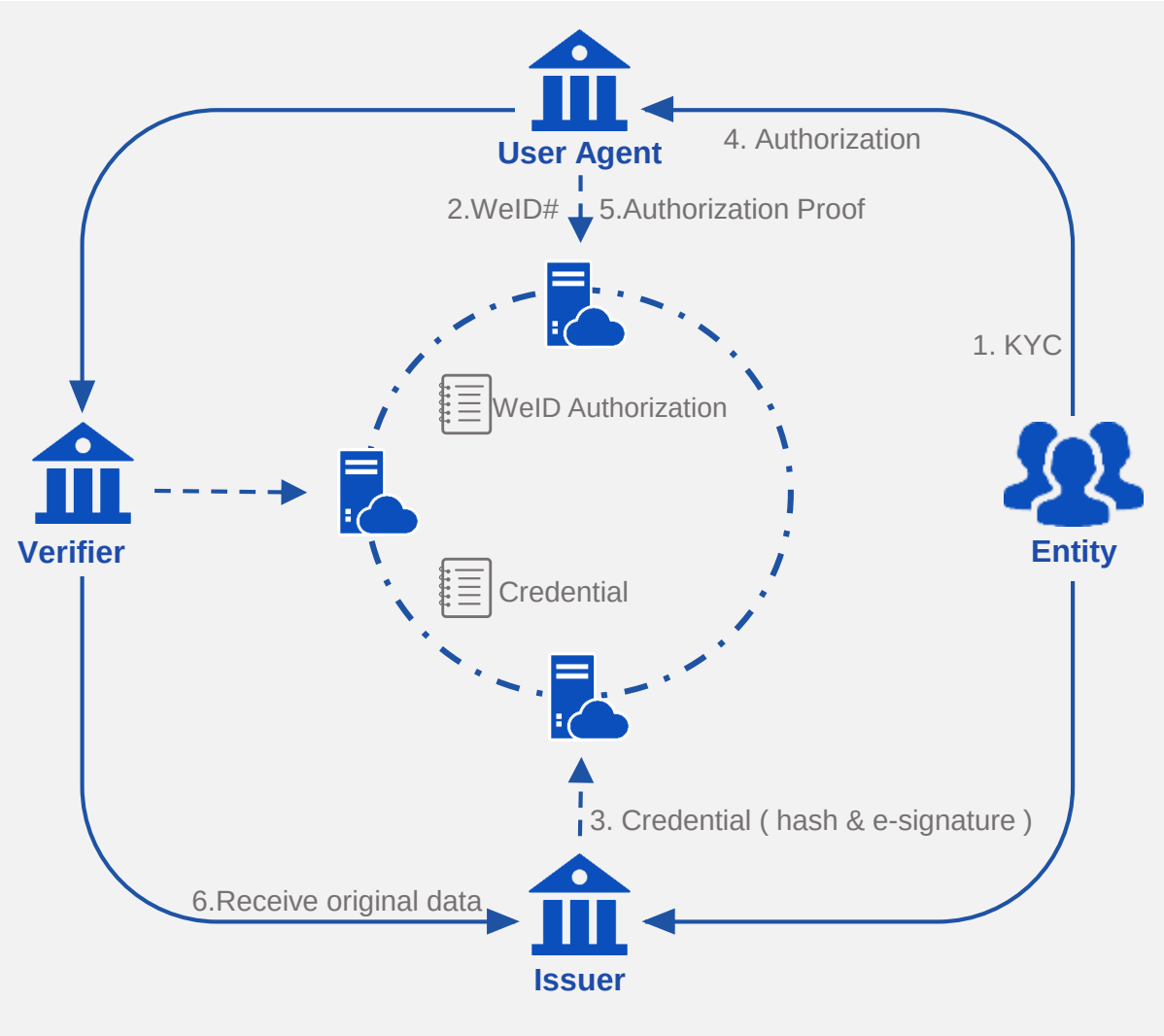
基于公众联盟链

分布式多中心的身份标识和管理

泛行业、跨机构、跨地域的数据交换

WeIdentity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，不仅使分布式多中心的身份注册、标识和管理成为可能，机构也可以通过用户授权合法合规地完成可信数据的交换。

功能介绍



实体标识化(WeID)

为每个实体（人或物）在区块链上生成符合国际规范（DID）的全球唯一ID。

电子化凭证(Credential)

将物理世界中的纸质证明文件电子化，并利用区块链不可篡改的特性，将原始数据的Hash上链，并附上权威机构(Issuer)的签名，确保数据不可伪造，可验证权威性。

用户授权即交易(Authorization)

原始数据的跨机构传输需要得到用户的授权，授权记录上链，符合GDPR。

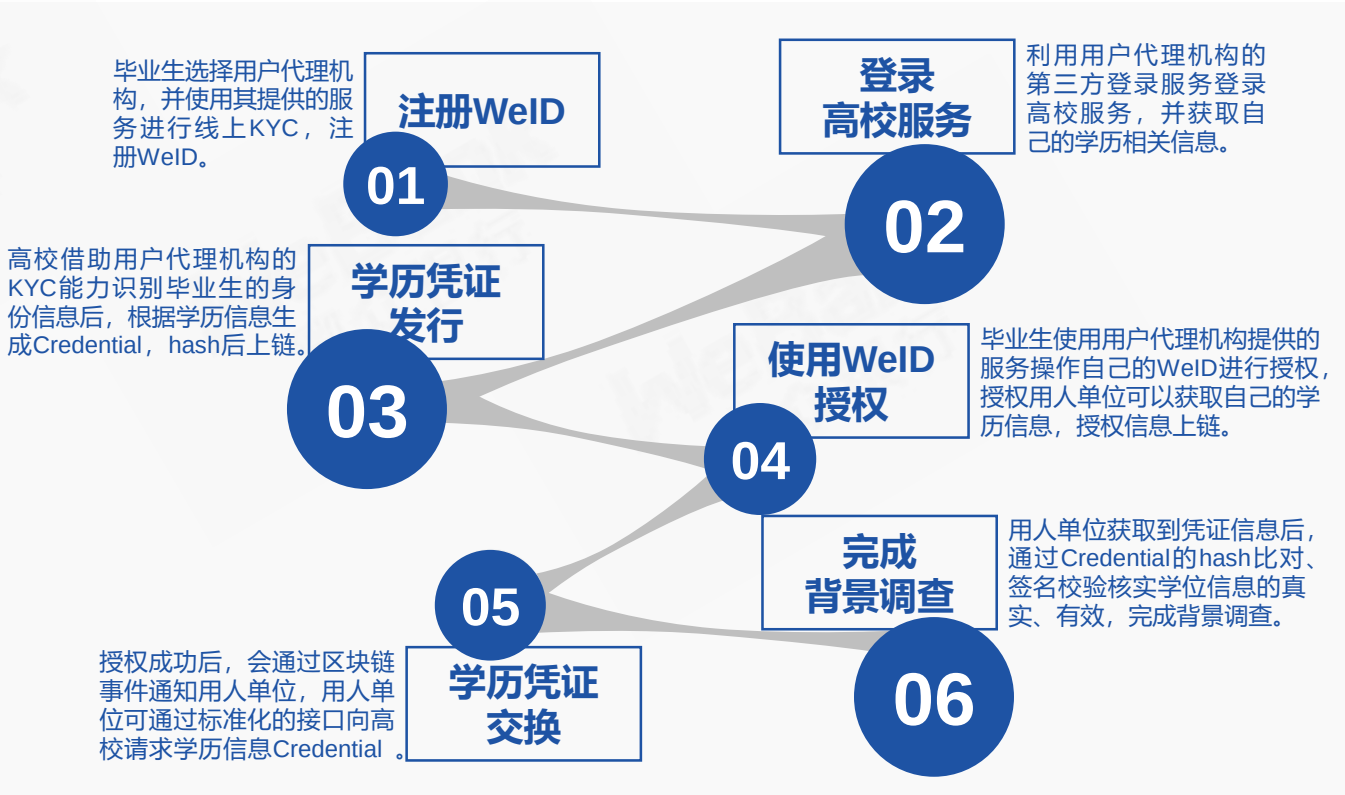
凭证存证(Evidence)

生成的凭证可以生成存证上链，供验证方对凭证是否篡改与否进行二次比对

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。

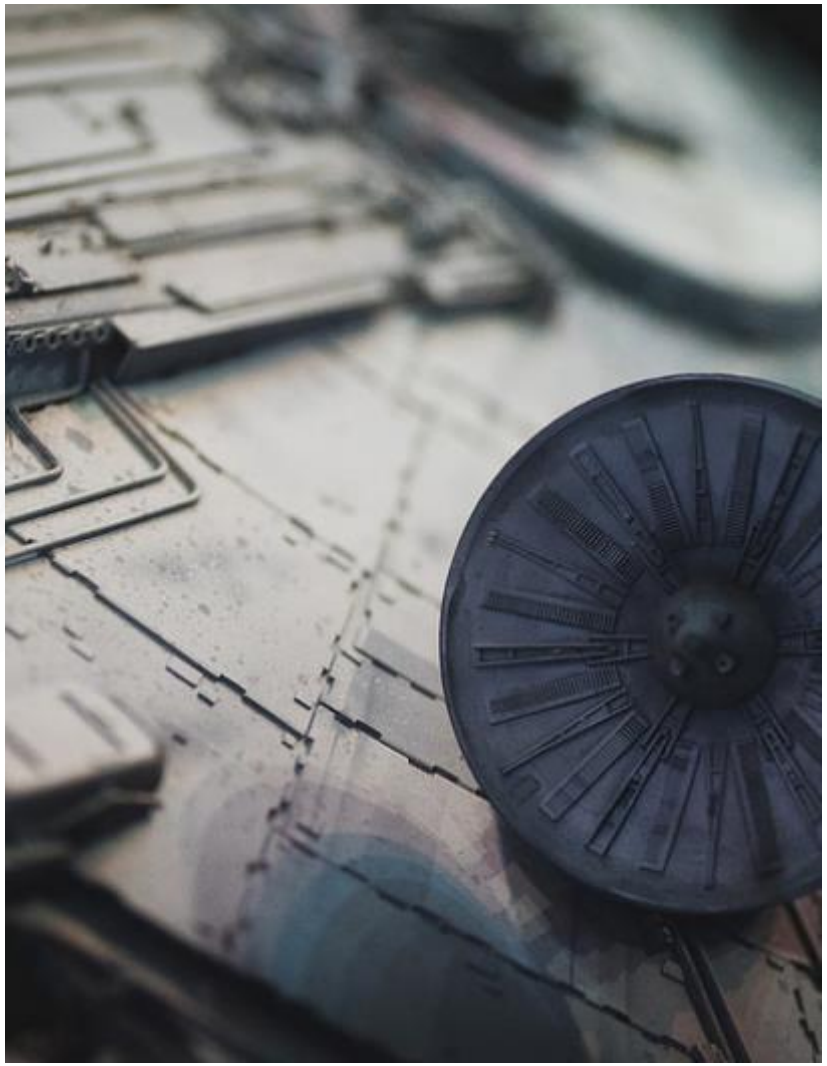
应用案例一：毕业生入职教育背景调查

毕业生入职教育背景调查



WeIdentity方案与传统方案对比：毕业生入职教育背景调查

WeIdentity方案	VS	传统方案
电子化学历凭证成本低，易于管理；	**成本与便利性**	纸质学历证明文件管理成本高，易丢失，不易更新；
密码学算法确保真实性和有效性，区块链记录确保不可篡改性；	**真实性**	纸质学历证明文件有造假可能性，验真周期长、效率低；
全流程无第三方机构参与，用户授权后，用人单位方能获取学历信息，隐私保护性强；	**隐私保护**	第三方背调公司参与可能导致用户隐私泄露问题；
方案可扩展性强，增加高校或用人单位数量，背调工作量不会相应增加。	**可扩展性**	方案可扩展性差，每增加一所高校或用人单位，第三方背调工作量会线性增加。



应用案例二：居民信息管理与政务办理

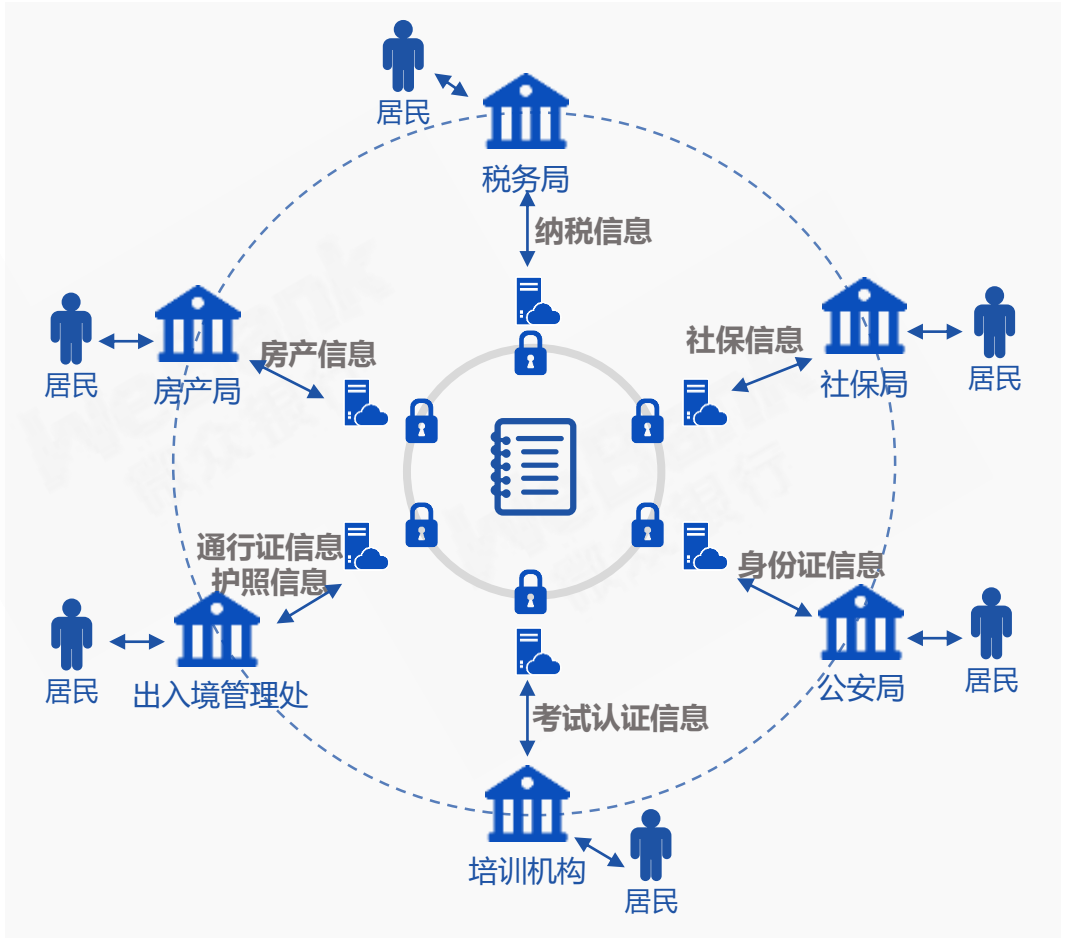
创建身份： 建立居民在链上的唯一身份标识，与真实可验的居民证件（身份证号、护照号、通行证号）映射。

关联映射： 居民在各部门应用中，可维护原有账号不变，通过真实证件映射到链上身份，达成账号间关联。

构建路由： 各部门对自身的居民数据摘要上链，并进行签名认证，形成每个居民的链上数据路由。

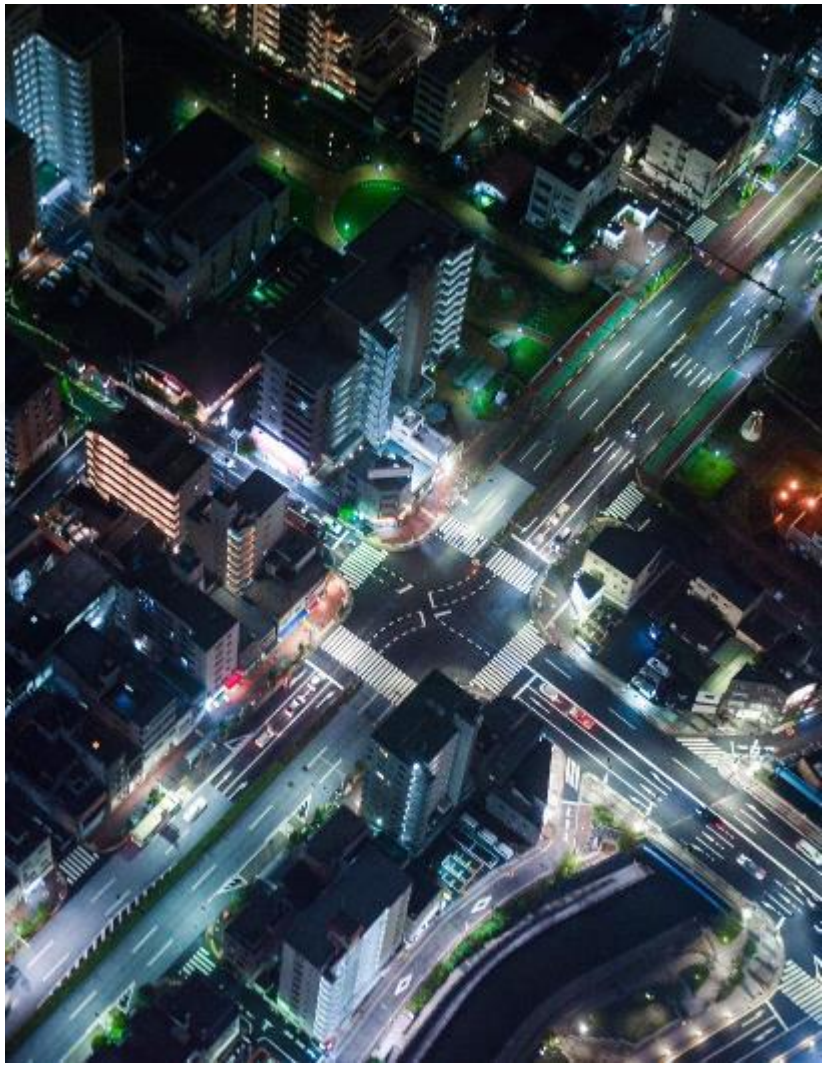
政务应用： 跨部门政务应用时，当居民授权，部门A可通过链上路由发现部门B有所需数据，并使用合法合规方式进行获取，实现快速验证或政务办理。

居民信息管理与政务办理



WeIdentity方案与传统方案对比：居民信息管理与政务办理

WeIdentity方案	VS	传统方案
证明文件转为Credential，可信存储，支持多终端应用；	**成本与便利性**	纸质文件管理成本高，使用次数、流程及场景均受限；
链上身份与现实身份一一对应；密码学算法确保真实性和有效性，区块链记录确保不可篡改性，通过链上摘要信息验真、增信；	**真实性**	对申请人身份真实性核验以及对文件数据的真实性核验，成本高、周期长、效率低；
数据归属于用户，机构使用数据需得到用户授权，隐私保护性强；可验证数字凭证的内容均在链下存储；	**隐私保护**	多部门间的信息传递，道德风险及操作风险均可能导致用户隐私泄露；
ID及凭证均遵循国际标准；方案可扩展性强，增加参与机构不会对已有业务造成影响。	**可扩展性**	方案的兼容性、可扩展性差。



标杆案例：澳门智慧城市建设之“证书电子化”项目

证书电子化管理

高额的纸质文件制作和管理成本以及受限的证书使用场景对系统提出更高的要求：

纸质证书电子化	文件可信存储与安全传输
数据归属权交还于用户	在线服务须支持多终端应用

跨机构信息交互

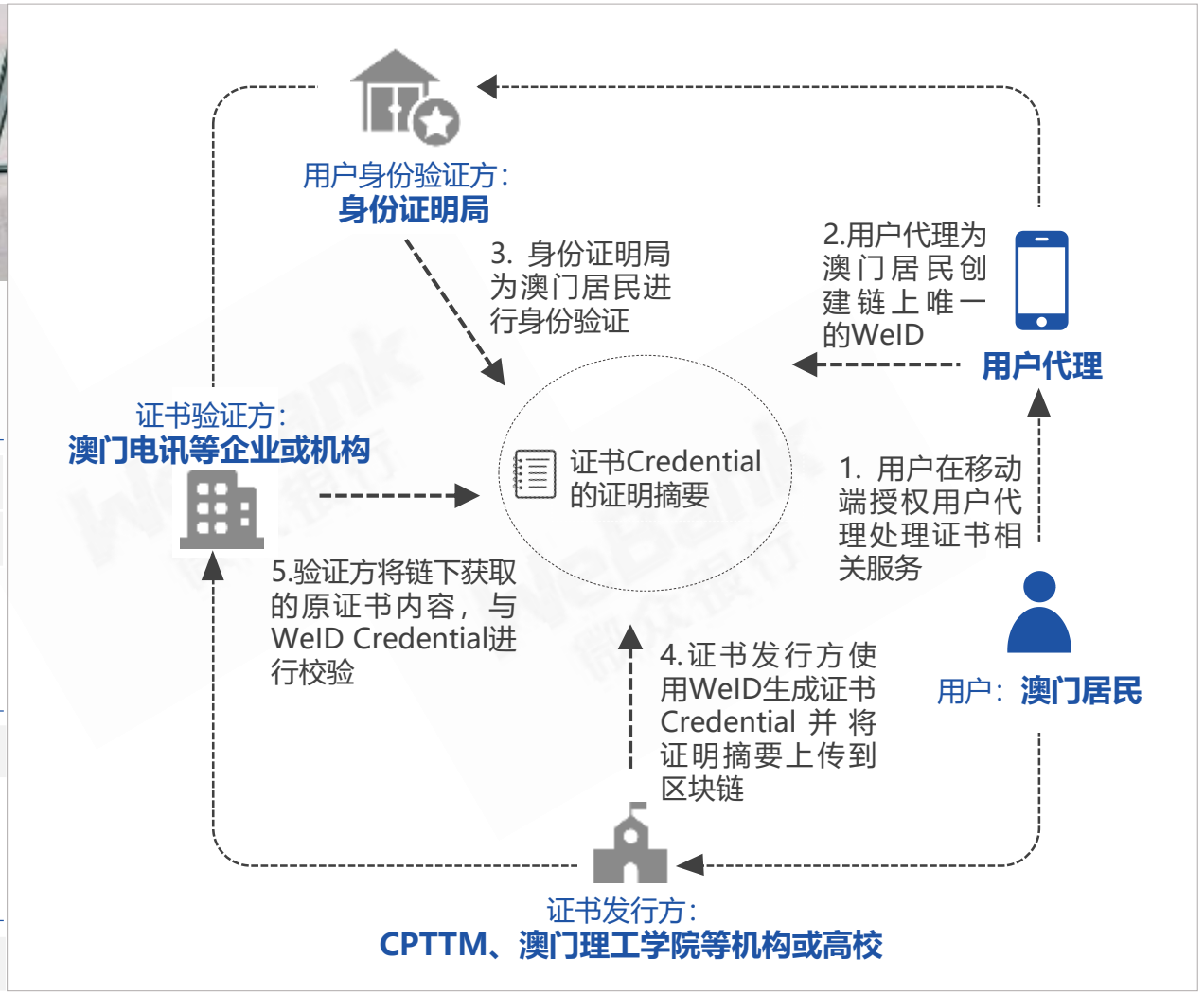
趋于严格的隐私保护法律及跨机构数据交换壁垒促进机构使用：

基于区块链的数据传输	链上存证数据传输记录及用户授权凭证

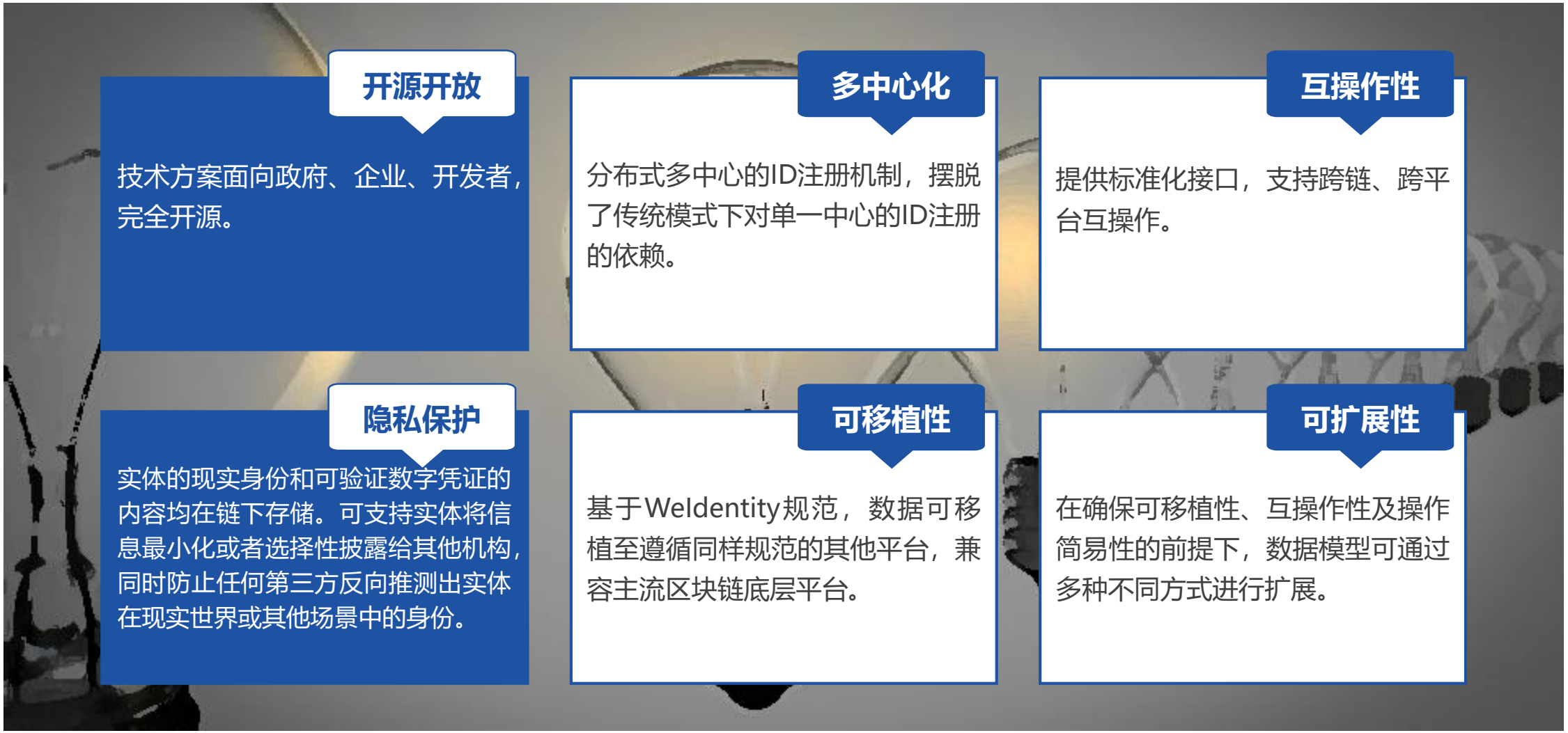
信息真实性验证

证书申请人的真实身份或证书内容本身难以确认，解决方法是：

现实身份与区块链ID一一对应	通过链上hash和电子签名验证证书



技术优势



开源开放

技术方案面向政府、企业、开发者，完全开源。

多中心化

分布式多中心的ID注册机制，摆脱了传统模式下对单一中心的ID注册的依赖。

互操作性

提供标准化接口，支持跨链、跨平台互操作。

隐私保护

实体的现实身份和可验证数字凭证的内容均在链下存储。可支持实体将信息最小化或者选择性披露给其他机构，同时防止任何第三方反向推测出实体在现实世界或其他场景中的身份。

可移植性

基于WeIdentity规范，数据可移植至遵循同样规范的其他平台，兼容主流区块链底层平台。

可扩展性

在确保可移植性、互操作性及操作简易性的前提下，数据模型可通过多种不同方式进行扩展。

合作

不论是机构、社群还是个人，不论是数据所有者还是数据应用方，都可以通过WeIdentity，参与合作，共同构造实体世界与数字世界互通互融的生态体系，创造更高效、安全的数据价值。

应用前景

- 投票
- 证件办理
- 车辆管理
- 福利分配
- 跨部门政务服务
- 资格认证与证书管理

- DNA测序
- 医疗信息共享
- 基因信息应用
- 个性化医疗服务

- 会员管理
- 权益共享
- 卡券管理
- 仓储与物流管理
- 积分登记与流通

- 账户管理
- 股权登记
- 财富管理
- 国际汇款
- 小额支付
- 抵押品管理
- 供应链金融

- 电网管理
- 智能家居
- 支付设备
- 自动化办公设备

合作与支持

咨询服务类

合作方式
企业、机构、个人开发者基于完全开源的WeIdentity自主设计和开发产品或服务。

提供支持
微众银行专业的技术团队，将在方案设计、开发测试等阶段提供必要的技术咨询服务和帮助。

深度合作类

合作方式
微众银行的战略合作伙伴或业务合作伙伴，基于WeIdentity，与微众银行共同设计、开发、运营产品或服务。

提供支持
微众银行完备的产品、研发及运维团队，将提供全面支持，赋能合作伙伴。

团队优势

团队实力

- 作为国内首家互联网银行，2015年，微众银行率先在国内投入资源发展区块链和分布式账本技术。
- 目前区块链应用开发人员已超过100人，团队成员在分布式系统、网络安全、海量服务等技术领域拥有丰富实践经验。

技术水平

- 微众银行联合同业推出了BCOS和FISCO BCOS两大区块链底层平台，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。

DIF成员

- 微众银行作为DIF（Decentralized Identity Foundation，国际身份标识领域权威组织）中的一员，与其他组织成员协同合作，致力于实现分布式身份标识、建设开放的生态。
- 以**国际通用标准**为合作伙伴提供跨行业、跨地域的可信方案。

WeBank

Thanks

WeIdentity

基于区块链的『实体身份标识』及『可信数据交换』解决方案