跨平台身份验证重复性

一、问题概述

现状：缺乏统一的身份验证机制，即跨平台身份验证的重复性（重复收集、核查相同的信息，各机构间缺乏协调和标准化，必须独立地执行与该用户身份相关的验证操作）。

- 在实际应用中，存在多个独立的信任域，每个信任域内只承认本域内的身份。跨域访问时，用户不能直接使用原始证书，而是需要在不同的信任域之间传递身份信任，这就产生了跨平台身份验证的问题。传统的身份验证方案大多依赖于受信任的第三方（TTP），如证书授权机构（CA）或密钥生成中心（KGC），通过这些中心实现不同域之间的信任传递。然而，这些方案面临单点故障的风险，且 TTP 的信任并非在所有情况下都能得到保障，因此减少对 TTP 的依赖成为一种理想的解决方案[1]。

原因：①竞争因素

各金融机构都希望在提供服务时能够获取尽可能多的客户数据，以便为客户提供个性化的产品或服务。由于竞争的压力，许多机构选择独立进行用户身份验证，而不是共享或交叉验证客户信息。具体包括：

客户数据的私有性和控制权——客户数据是金融机构自身竞争力的一部分，各机构均要求完全控制与客户相关的数据，从而避免将潜在的客户信息交给竞争对手。

差异化服务——一些金融机构可能会通过额外的验证程序或者特定的验证方式来吸引特定的客户群体，作为其特色服务的一部分。

商业利益保护——数据共享会导致其他机构借此获得客户资源，降低自己在客户市场中的份额。

②合规性因素

跨境金融交易必须遵循各国法律和国际标准。但是，各国法律规定存在差异，跨平台身份验证过程缺乏统一标准（法律差异、监管审查差异，易引发法律风险）

③信任因素

中心化的身份验证体系，各机构对身份数据的管理与验证完全独立，无法确认其他机构对用户身份的验证是否真实有效，是否值得信赖。此外，目

[1] A Zero-Knowledge-Proof-Based Anonymous and Revocable Scheme for Cross-Domain Authentication

前缺乏一个充分的信任机制来确保共享的金融用户数据不会被滥用。

影响：①验证成本大幅增加——每个金融机构在接收客户时，必须从头开始进行 KYC（了解客户）和 AML（反洗钱）等验证，涉及到大量的人工审核、数据存储和多重数据交换

②效率低下——验证同一身份的多个过程将消耗大量时间，导致跨境支付的处理速度显著延迟 → 降低客户体验，影响机构的资金流动性，进而影响全球金融市场的流畅性

③数据安全问题频发——各机构基于自己的理解和标准来执行验证，可能出现数据安全漏洞，增加数据泄露和滥用的风险

二、需求分析

1. 高效性需求：身份验证流程的自动化和数据共享机制的优化
2. 安全性需求：信息泄露和滥用风险
3. 合规性需求：不同国家和地区法律都认可的合规认证框架
4. 信任与互操作性需求：高互操作性和信任机制的技术架构

三、金融数据流动

1. 个人金融信息：金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他反映特定个人某些情况的信息。
具有多元性与复杂性

2. 金融隐私数据跨公司流动：

①国内跨公司流动——《法人金融机构洗钱和恐怖融资风险管理指引(试行)》；
②跨境流动——需要走司法协助等官方国际合作程序 or 采用外交途径向国家外事单位提出请求，涉及《国际刑事司法协助法》。

3. 金融数据**“由私到公”合作共享模式**，趋势不可避免（全球经济发展）
重点：
①如何在金融数据的获取与使用过程中保护企业个体的隐私，让其在使用过程中获得合理合法的授权；
②监管+协助：对监管的路径来进行优化，让金融数据的流通基于安全保障的目的来进行调取；调取“私主体”的数据过程中，对于涉及“私主体”以及公共机构之间的一些行权，限权，甚至责任承担问题，都需要进行严格的限定。

→**法律**主体，法律关系，多元化的法益博弈

与公共机构完成数据共享，合法性，正当性，保护企业个体的法律权益

4. 数据共享与隐私保护的矛盾——区块链的去中心化特性消除了对单一信任中心的依赖，但其开放性和透明性使得用户数据在全网传播，任何人都可以访问区块链中的数据，从而可能暴露用户的身份信息。

保障个人数据的隐私权和安全性 VS 数据共享

5. 相关法律规定

（一）中国

国家安全产业安全放在首位，故数据跨公司流通的时候，必须保证数据的安全可控（与数据的自由流动存在矛盾）→我国积极推进《全球数据安全倡议》

•《民法典》第 1038 条规定，信息处理者不得透露或篡改信息。同时也不可以随便收集或 者存储个人信息。在信息处理过程中，必须要采取最基本的保护措施，确保被收集、存储方的隐私信息 的安全性，并且要防止信息泄露、篡改、丢失等情况的发生。此外，在出现或有可能出现个人信息泄露、 篡改、丢失等情形时，必须及时采取补救行动。

•《中华人民共和国个人信息保护法》第 23 条规定，个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

•《金融数据安全 数据安全分级指南》（中国人民银行，2020），对金融数据进行分级分类管理，明确了不同级别数据的共享和使用规则，鼓励金融机构在确保数据安全的前提下，推动数据的合规共享。 → 推动金融数据共享与互联互通

•《金融科技发展规划（2022-2025 年）》（央行，2022），提出推动金融科技与身份认证技术的深度融合，建设统一的金融身份认证体系，鼓励探索区块链、人工智能等技术在身份验证中的应用。

•《跨境支付与身份验证合作框架》，中国人民银行要与国际清算银行（BIS）等机构合作，推动跨境支付和身份验证的标准化。通过国际合作，推动跨境身份验证的互操作性，减少重复验证。 → 推动跨境身份验证合作

（二）欧盟

欧洲以**“适当性评估**(Adequacy Decision) ”为核心的数据跨公司流通的混合模式：在达到足够保护程度的前提下，方可将其跨境传输至第三国。在这个过程中，欧盟委员会基于多种因素 考虑，通过进行适当性评估，来确定是否达到保护的标准。如果能过评估，就相当于经 过了欧盟认证的“白名单”。

缺点——认证过程繁琐复杂，实际运用的操作性差

•《通用数据保护条例》（GDPR）——全球数据隐私保护的标杆法规

主要内容：严格保护个人数据，要求数据处理的透明性、合法性和最小化原则。【该条例对数据收集、处理、存储和传输设立了严格的要求，企业必须获得用户明确的同意，才能合法地处理其个人数据。此外，GDPR 还规定了数据主体的权利，如访问权、修正权和删除权，以及企业在数据泄露时的通报义务。对于违反 GDPR 的企业，欧盟可以处以高达全球年营业额 4%或 2000 万欧元的罚款，这使得合规成为企业在欧洲市场生存的必要条件。】

借鉴意义：中国在《个人信息保护法》中借鉴了 GDPR 的许多原则，但在执行力度和细节上可以进一步优化。

•《电子身份识别与信任服务条例》（eIDAS）

主要内容：建立统一的电子身份识别框架，支持跨境电子身份验证。

借鉴意义：eIDAS 为欧盟成员国提供了互操作的电子身份验证标准，中国可以借鉴其框架，推动国内统一的身份认证平台。

（三）美国

• NIST 网络安全框架

主要内容：提供了一套灵活的网络安全标准，包括身份验证和数据保护。

借鉴意义：中国可以借鉴 NIST 的标准化方法，完善金融身份验证的技术标准。

• 金融数据共享（如 FDX 标准）

主要内容：通过金融数据交换（FDX）标准，推动金融机构之间的数据共享。

借鉴意义：中国可以推动类似的行业标准，促进金融机构间的数据共享和互操作。

• CCPA（加州消费者隐私法案）

美国的隐私保护框架相对松散，但加州通过的 CCPA 则是美国最为严格的数据隐私法之一。CCPA 要求企业向消费者告知其收集的数据类别和用途，并赋予消费者选择不出售个人数据的权利。与 GDPR 不同的是，CCPA 更加侧重于数据的出售和消费者的选择权，这意味着企业在进入美国市场时，需特别关注如何处理和出售数据的相关问题。

（四）东南亚

• 新加坡《个人数据保护法》

要求企业在收集和处理个人数据时确保透明度，并实施适当的安全措施以防止数据泄露。

• 印度《个人数据保护法》

对数据本地化和跨境传输提出更严格的要求。随着东南亚市场的监管日趋严格，企业在这一地区的合规成本也将逐渐增加。

（五）英国

• 开放银行计划

主要内容：要求银行通过 API 开放客户数据，支持第三方机构提供金融服务。

借鉴意义：中国可以借鉴开放银行的模式，推动金融数据的合规共享。

数字身份框架：

主要内容：建立国家数字身份系统，支持跨平台身份验证。

借鉴意义：中国可以借鉴其数字身份框架，推动统一的身份认证平台。

6. 中西方在跨境身份验证中的政策错位

（1）数据隐私保护标准的差异

中国：以《个人信息保护法》为核心，强调数据本地化和跨境传输的合规性。

西方：以 GDPR 为核心，强调数据主体的权利和跨境数据流动的自由化。

错位影响：中西方在数据隐私保护标准上的差异可能导致跨境身份验证的合规性冲突。

（2）技术标准与互操作性的差异

中国：倾向于自主研发技术标准（如数字人民币中的区块链技术）。

西方：广泛采用国际标准，如 NIST（National Institute of Standards and Tehnology）、eIDAS（Electronic Identification, Authentication and Trust Services）。

错位影响：技术标准的不一致可能导致跨境身份验证的互操作性问题。

（3）监管框架的差异

中国：以中央银行为核心，实施严格的金融监管。

西方：以市场为导向，强调行业自律和多方合作。

错位影响：监管框架的差异可能导致跨境身份验证的合作障碍。

四、案例

1. 现行的 **SWIFT** 金融结算体系中，一次跨国金融交易大概率会设计 2-4 个金融机构，其中每家中间行都需要进行一次独立的身份验证，根据行业数据，跨境交易中重复验证的比例可能高达 60%-80%，尤其是在涉及多个中间行和严格监管要求的情况下。如果采用区块链技术，验证重复性的比例可以显著下降。根据行业研究和试点项目的成果，区块链可以将验证重复性比例降低至 10%-20%。

• RippleNet 是基于区块链的跨境支付网络，旨在替代传统的 SWIFT 体系。其通过共享账本和智能合约，减少了中间行的数量和重复验证的需求。根据 Ripple 官方数据，其跨境交易的结算时间从几天缩短到几秒，验证重复性比例大幅下降。

2. APP 平台之间的“一键关联”：e.g.用户在微信注册后，可以以同样的身份信息关联登录到抖音

3. 用户在不同银行或证券公司开设账户时，每家机构往往要求用户提供同样的个人资料走相同的流程（身份证原件、纸质表格、人脸识别和电话确认等），会产生大量的人工审核成本，因各机构平台的安全验证标准不一，用户可能还需记忆多个账户密码，繁琐的流程导致了资源的浪费，DLT 通过其去中心化信任机制能够有效节约成本，避免重复的验证流程，提升整体效率。

4. **（中）粤港跨境身份验证平台**

2021 年 11 月，南沙开发区与广州南沙诺华数据有限公司签订战略合作协议，共同搭建大湾区跨境数据互信互认平台。该平台接入粤港两地合规数据源，首创对粤港两地居民的跨境身份核验服务，旨在解决中小企业和个人用户跨区域身份认证的难题。目前，该平台正在试运营，预计年底正式开展业务。

5. **（中）横琴粤澳跨境数据验证平台**

2022 年，横琴粤澳跨境数据验证平台上线，旨在解决粤澳两地金融机构在跨境业务中面临的身份验证难题。该平台利用区块链技术，确保数据的安全性和隐私保护。例如，工商银行澳门分行和横琴分行通过该平台实现了个人资产证明的跨境验证，提升了业务办理效率。

6. **（欧）Sparkasse Bank Malta plc 的验证代理角色**

2020 年，Sparkasse Bank Malta plc 成为全球法人实体标识符（LEI）体系中的验证代理（VA）。作为验证代理，银行能够为其客户简化 LEI 的发放流程，减少客户引入的时间，并为机构的数字创新提供保障。

7. **（欧）欧盟反洗钱法规与 LEI 的应用**

2024 年，欧盟最终确定了新的反洗钱（AML）法规，要求金融机构在新客户开户过程中使用 LEI 对法定实体进行客户身份识别和验证。这一举措旨在通过识别

组织身份，构建一个更安全、高效、数字化的支付体系。

8. 中国人民银行数字货币研究所在数字人民币试点中探索基于区块链的身份验证技术。

五、 相关数据

KYC 程序的成本

根据 Jumio 的研究，KYC 程序的成本约占银行总运营成本的 3%。这笔开支对于银行而言不容忽视，且如果未能充分执行 KYC 项目，可能会面临更高的处罚。

六、开放银行

数据共享→基于 API

• API 接口是为了实现某个应用程序与其他系统的互动，而设计的经过记录的连接点。

• API 接口可以是公开的，但也可能是专有的。

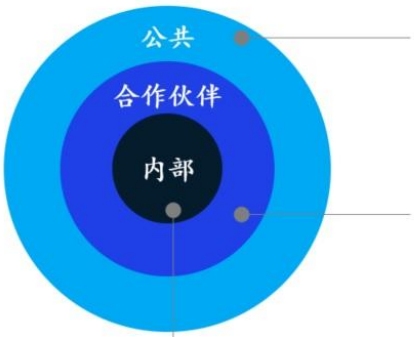
• API 的核心价值：简化系统间的联通、推动更便捷地获取数据

• 开放银行面临的挑战

①数据共享问题

②传统银行（反对数据公开）仍牢牢掌握着大量的交易数据和紧密的客户关系

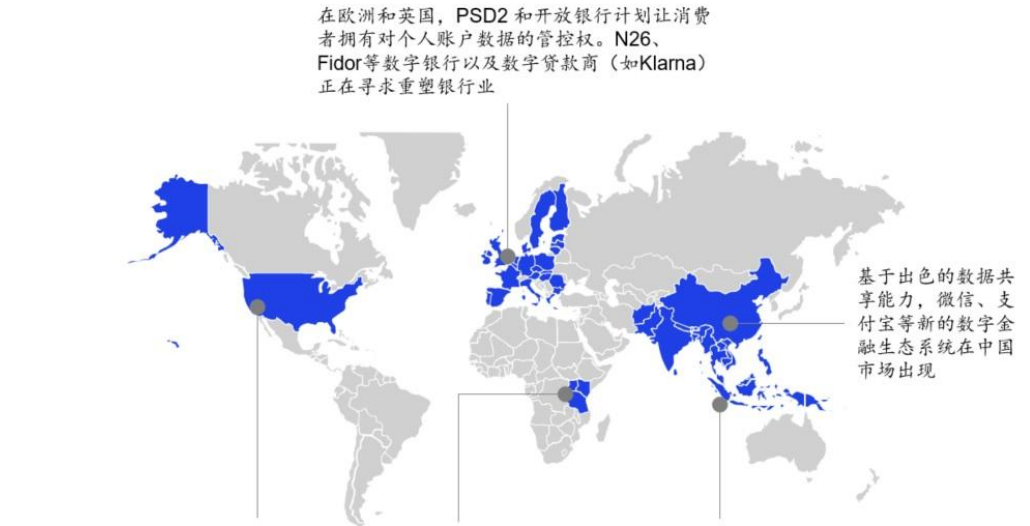
图1 API的三种模式



类别	特点
公共/开放式接口 供外部合作伙伴和开发创新App以及新产品的开发人员使用的API接口	• 通过融入开发者社区来开展创新 • 广阔的市场覆盖
合作伙伴/B2B接口 供合作伙伴使用的API接口。包括供应商、分销商和其他合作伙伴，以实现更密切的合作	• 帮助合作伙伴降本 • API变现 • 提升安全性
内部接口 开发人员在企业内部使用的API接口	• 降本 • 提升运营效率 • 提升安全性

资料来源：McKinsey Payments Practice

图2 全球开放银行发展历程



资料来源：McKinsey Payments Practice

开放银行对传统银行和金融服务创新的影响

1. 普惠金融迎来新机遇

通过汇集不同系统中少量的个人资料，可实现更精确的风险评分和信贷审批，进而推动开展普惠金融，比如在非洲开展业务的美国金融企业 Angaza Design。同

时，随着更多潜在客户纳入正规金融系统，开放银行可推动市场增长并潜在催生出利润丰厚的新服务。还有一类创新致力于整合非金融数据与交易记录，并从中找出新的洞见和商机，孵化器和风投资本也在积极关注这类创业公司，例如智能投顾服务商 Wealthfront 最近推出一款借款产品，利用客户的历史交易数据，无需信用审核，以持有资产作为抵押来提供借款。银行不妨利用自身积累下来的金融数据开展普惠金融领域的探索。

2. **产品创新的新时代**

在开放银行的大趋势下，传统银行难免对部分传统领域失去掌控力，但它们也会收获一个更加广阔的行业利润池，而且有机会成为其中的主导者。例如，传统银行可创新产品，将预测分析和人工智能技术与借贷融资相结合，大幅改善零售客户和对公客户的服务。谁愿意率先对企业积极开放数据、抢先提供客户需要的创新产品，谁就能够获得先发优势。所谓的创新产品既包括更便捷的操作界面，也包括各种增值服务，如 Monzo 等线上银行设计的预算管理、支出分类等功能。仰赖于长期以来累积的客户信任关系，传统银行短期内不太会丧失竞争优势，但它们必须立即行动，以应对来自新兴企业日益白热化的竞争。

3. **网关服务提供商的兴起**

人们一直在关注银行的老旧系统与 API 接口的对接开放进程，同时，我们也应积极关注支付发起服务提供商（Payment Initiation Service Providers, PISP）和账户信息服务提供商（Account Information Service Providers, AISP）与银行间的交互端口。由于 PSD2 并未就技术标准做出详细规定，“网关服务提供商”将成为未来新的关注热点。

例：Google 收购 API 管理平台 Apigee，与 Xignite 和 Plaid 等一起，加剧这一领域的竞争。这其中的成功关键在于银行、第三方提供商以及网关服务提供商在内的各方，能否构建起安全可靠且不牺牲速度的交互流程。

传统银行应对策略

1. 开放合作
2. 重构产品业务
3. 突破中小企业

七、 基于区块链的身份验证技术探索

1. 去中心化身份（Decentralized Identity, DID）

基于区块链的身份验证技术，用户可以通过私钥自主控制自己的身份信息，而无

需依赖中心化机构。

用户的身份信息存储在区块链上，通过零知识证明（ZKP）等技术实现隐私保护。

2. 零知识证明（ZKP）

一种密码学技术，允许一方向另一方证明自己知道某个信息，而无需透露该信息的具体内容。

3.智能合约

运行在区块链上的自动化程序，可以根据预设条件执行特定操作。

4.跨链技术

允许不同区块链网络之间的互操作，实现数据和资产的跨链流动。