

2025年中国身份认证行业概览：安全边界到智能治理的全面进化

China Identity Authentication Report
中国におけるアイデンティティ認証産業

概览标签：身份认证、身份管理、访问控制

研究目的

本报告为对中国身份认证行业进行研究。将通过探究对中国身份认证行业的市场情况、市场规模以及应用场景来了解中国身份认证行业的发展现状和市场规模。

研究区域范围：全球和中国地区

研究对象：身份认证行业

本报告的关键问题：

- 1) 全球及中国身份认证的市场规模如何，未来发展的空间有多大？
- 2) 中国身份认证未来将如何变化？
- 3) 身份认证应用市场未来将如何变化？

摘要

- **身份认证定义**：身份认证是指系统通过验证用户所提供的身份凭证，确认其真实身份并决定是否允许其访问资源的过程，是信息安全体系的首要环节。认证流程通常包括四个阶段：首先，用户通过用户名、手机号或证书等方式进行身份标识；其次，提交密码、验证码、生物特征等身份凭证；随后，系统对凭证进行比对验证，判断其与注册信息是否一致；最后，在验证通过后执行访问授权，赋予相应操作权限。常见的认证方式包括密码验证、短信验证码、数字证书、生物识别和多因素认证（MFA）等。
- **身份认证要素**：身份认证体系在中国与国际市场均呈现出多层次演进趋势，涵盖设备识别、票据验证及硬件安全模块等关键环节。不同技术路径在安全强度、合规约束和适用场景上存在明显差异。
- **身份认证市场规模**：中国身份管理市场呈现快速扩张态势，其中身份认证作为核心板块，占比长期维持在总市场的45%至46%左右，其市场规模从2020年的约7.68亿元增长至2029年的预计52.49亿元，增幅接近7倍，远高于全球平均水平。



目录

CONTENTS

◆ 名词解释	4
◆ 中国身份认证行业综述	5
• 身份认证定义	6
• 身份认证要素分析	7
• 全球市场规模	8
• 中国市场规模	9
• 厂商份额	10
• 应用场景渗透率	11
• 各国的数字身份系统对比	12
◆ 中国身份认证行业产业链分析	13
• 不同国家的政策分析	14
• 各类身份认证的全球与中国情况对比	15
• 身份认证监管情况	16
• 国内外身份认证案例分析	18
◆ 方法论	19
◆ 法律声明	20

名词解释

- ◆ **身份管理：**身份管理是指在数字或实体环境中，通过一系列技术、流程和制度对个体或组织的身份进行识别、验证、授权与全生命周期维护的系统性管理活动，旨在确保主体能够安全、可信地访问资源，同时保护相关数据的完整性与隐私性。
- ◆ **CRM：**CRM（Customer Relationship Management，客户关系管理）是指企业利用系统化的方法与技术，对客户进行识别、获取、维护与提升价值的全过程管理，以促进长期关系、提升客户满意度并最终推动业务增长的管理理念与工具体系。
- ◆ **SSH密码：**SSH 密码是指在通过 SSH（Secure Shell）协议建立远程连接时，用于验证用户身份的传统基于口令的认证方式。它由用户在服务器上设置的登录密码构成，客户端在连接时将该密码与服务器端存储的认证信息进行了比对，以决定是否允许访问。相比密钥认证，密码方式更易使用但安全性相对较低。。



第一部分：行业综述

主要观点：

- 全球身份管理市场正呈现稳步增长趋势，其中身份认证作为核心板块，其市场规模在整体市场中占比约45%–46%，从2020年的51.3亿美元增长至2029年的预计171.2亿美元，几乎实现三倍扩张。在整个身份管理市场中，访问控制和身份治理虽同样保持高速增长，但身份认证凭借其基础性和核心性作用，成为推动市场扩张的主要力量。
- 身份主要特点体现在：1) 唯一性——每个身份对应独立的标识与凭证，确保身份不可混淆；2) 安全性——通过加密传输、多因素验证等手段防止冒用与攻击；3) 可追溯性——认证过程可记录与审计，支持安全合规；4) 灵活性——可根据风险级别与场景采用不同认证强度；5) 基础性——是访问控制、权限管理与零信任体系的前提。
- 中国身份管理市场呈现快速扩张态势，其中身份认证作为核心板块，占比长期维持在总市场的45%至46%左右，其市场规模从2020年的约7.68亿元增长至2029年的预计52.49亿元，增幅接近7倍，远高于全球平均水平。



全球及中国身份认证行业综述——身份认证定义

身份凭证以确认其真实身份并授予访问权限的安全机制，具有唯一性、安全性、可追溯性、灵活性和基础性等特点，是构建访问控制与零信任安全体系的核心环节

身份认证的定义及流程分析

- ❑ 定义：身份认证是指系统通过验证用户所提供的身份凭证，确认其真实身份并决定是否允许其访问资源的过程，是信息安全体系的首要环节。认证流程通常包括四个阶段：首先，用户通过用户名、手机号或证书等方式进行身份标识；其次，提交密码、验证码、生物特征等身份凭证；随后，系统对凭证进行比对验证，判断其与注册信息是否一致；最后，在验证通过后执行访问授权，赋予相应操作权限。常见的认证方式包括密码验证、短信验证码、数字证书、生物识别和多因素认证（MFA）等。身份认证的核心目标是防止身份冒用与非法访问，确保访问主体的可信性，为后续的授权、审计和安全管控提供基础，是构建零信任安全体系与数字身份管理的关键环节。
- ❑ 其主要特点体现在：1) 唯一性——每个身份对应独立的标识与凭证，确保身份不可混淆；2) 安全性——通过加密传输、多因素验证等手段防止冒用与攻击；3) 可追溯性——认证过程可记录与审计，支持安全合规；4) 灵活性——可根据风险级别与场景采用不同认证强度；5) 基础性——是访问控制、权限管理与零信任体系的前提。

身份认证流程如下：



来源：食品工艺，头豹研究院

中国身份认证行业综述——身份认证要素分析

身份认证体系在中国与国际市场均呈现出多层次演进趋势，涵盖设备识别、票据验证及硬件安全模块等关键环节。不同技术路径在安全强度、合规约束和适用场景上存在明显差异

身份认证要素及场景分析

认证要素	中国主要方式	国际主要方式	技术成熟度	安全性	应用场景	认证要素	中国主要方式	国际主要方式	技术成熟度	安全性	应用场景
设备指纹	浏览器指纹、移动设备唯一标识、设备绑定	类似方案 (Device ID、Browser Fingerprinting) ,GDPR下受限	★★★★★	★★★★★	金融风控、反欺诈	法人四要素 (企业名称、统一社会信用代码、法定代表人姓名、身份证号)	国家市场监督管理总局数据核验、CFCA法人认证	各国公司注册局	★★★★★	★★★★★	企业开户、合同签署、资质审查
票据验证	财税发票二维码、数字签章校验	发票验证较分散，欧盟e-Invoice标准推广中	★★★★★	★★★★★	财税报销、供应链合规	电子营业执照	全国统一“政务服务网+工商系统”签发、支持数字签章	欧盟eIDAS电子身份体系、美国DocuSign等私有证书体系	★★★★★	★★★★★	政务办事、电子签章
硬件安全模块 (HSM) /U盾	银行U盾、CA证书、国密算法	国际采用PKI证书、FIDO安全密钥	★★★★★	★★★★★	金融交易、政务系统、企业签章	小额打款验证	银行向企业账户小额汇款验证归属	普遍采用相同机制 (PayPal、Stripe等)	★★★★★	★★★★★	银行开户、平台商户入驻

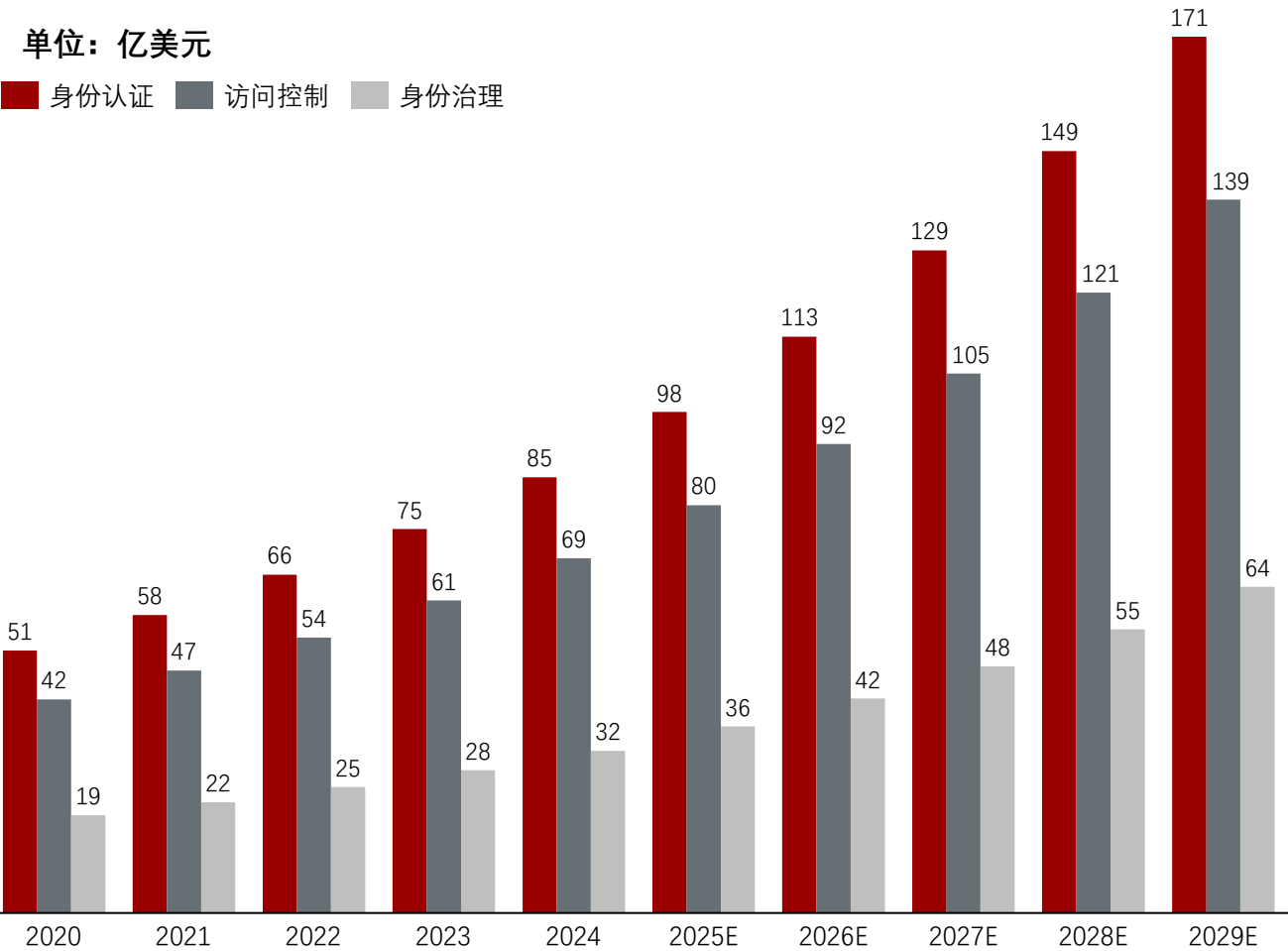
身份认证的技术路径呈现多元并行的格局。中国在设备指纹方面主要采用浏览器指纹、移动设备唯一标识与设备绑定技术，形成较成熟的风控识别体系；国际上则以Device ID、Browser Fingerprinting为主，但受GDPR等隐私法规限制。票据验证领域，中国依托发票二维码与数字签章实现验证，而欧盟推广e-Invoice标准、美国普遍使用电子签名校验，整体成熟度中等。硬件安全模块（HSM）与U盾仍是高安全等级的核心手段，中国广泛采用国密算法、CA证书体系，国际上则以PKI和FIDO安全密钥为主，具备高成熟度与强安全性。

身份认证正从单一数据核验向合规化、数字化与跨境互认方向演进。中国通过法人四要素、电子营业执照和小额打款验证构建起较完备的企业身份认证体系，依托国家级数据源与国密算法确保权威性与安全性；国际上则以eIDAS、PKI体系和私有认证平台为主，更注重隐私保护与合规监管。随着跨境贸易与数字政务协同加深，企业身份认证正朝“标准互认+分级信任”模式发展，未来可能通过区块链、可验证凭证（VC）等技术实现跨国主体身份的可信流通与互认。

中国身份认证行业综述——全球市场规模

身份认证作为身份管理市场的核心板块，占比约45%，其市场规模从2020年的51亿美元增长至2029年的171亿美元，增长主要受数字化转型、远程办公普及、零信任安全架构推广及合规要求推动

全球身份管理及认证市场规模分析



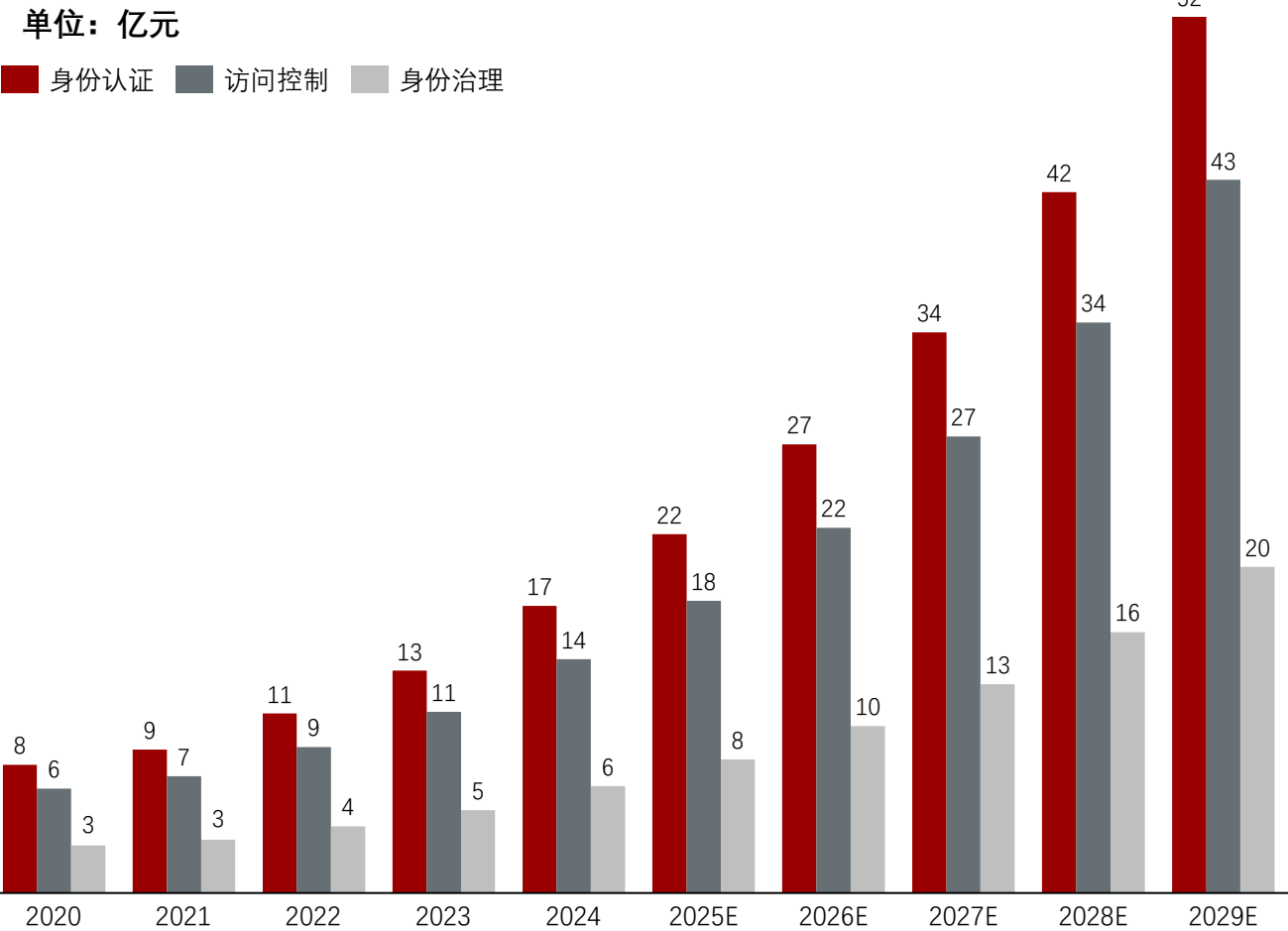
- 全球身份管理市场正呈现稳步增长趋势，其中身份认证作为核心板块，其市场规模在整体市场中占比约45%—46%，从2020年的51.3亿美元增长至2029年的预计171.2亿美元，几乎实现三倍扩张。在整个身份管理市场中，访问控制和身份治理虽同样保持高速增长，但身份认证凭借其基础性和核心性作用，成为推动市场扩张的主要力量。
- 其增长与多重因素密切相关：首先，企业数字化转型加快了对统一身份管理的需求，尤其是在跨部门、跨地域和跨系统的应用场景中，可靠的身份认证成为业务安全的前提；其次，远程办公和混合办公模式的普及，显著提升了对多因素认证、生物识别认证及零信任架构下动态身份验证的需求，从而直接拉动市场规模；再次，随着全球数据隐私和安全合规要求趋严，企业在身份认证方面的投入不断增加，以满足监管和审计要求。整体来看，身份认证不仅是身份管理市场的最大组成部分，其增长速度和规模也在很大程度上决定了整个身份管理市场的扩张节奏。
- 从市场占比来看，身份认证在总市场中长期维持45%左右，显示其作为基础性安全控制的不可替代性，同时也反映出企业在数字化和安全化进程中持续加大身份认证投资的趋势。因此，身份认证市场的增长既是技术进步和业务模式演变的结果，也是整体身份管理市场高速发展的核心驱动力。

来源：社会科学院，头豹研究院

中国身份认证行业综述——中国市场规模

中国身份认证市场的快速增长既是技术进步和业务模式演变的结果，也是整体身份管理市场高速扩张的核心动力

中国身份管理及认证市场规模分析



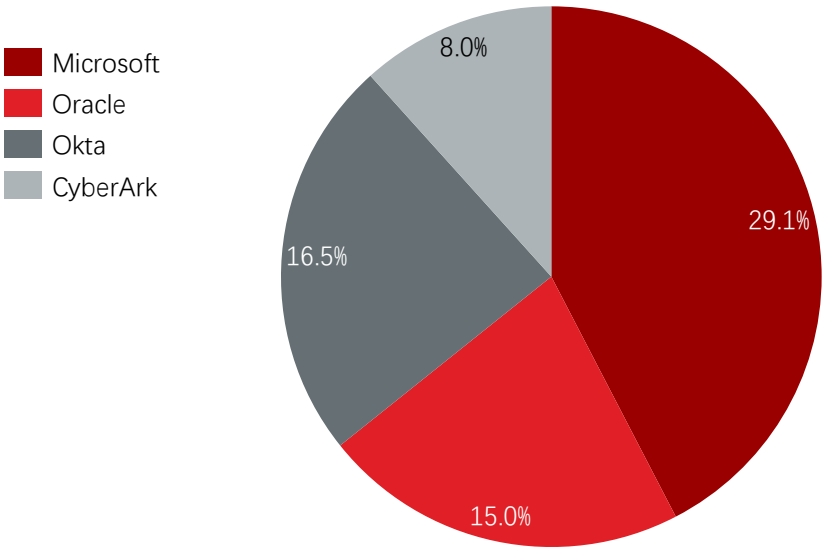
- 中国身份管理市场呈现快速扩张态势，其中身份认证作为核心板块，占比长期维持在总市场的45%至46%左右，其市场规模从2020年的约7.68亿元增长至2029年的预计52.49亿元，增幅接近7倍，远高于全球平均水平。
- 这一增长在整体市场中的拉动作用十分显著，访问控制和身份治理虽同样保持高速增长，但身份认证的规模和基础性作用使其成为市场发展的核心驱动力。
- 从增长原因来看，首先，国内数字化转型加速推动了企业和政府对统一身份认证和安全访问的需求，尤其在跨系统、跨部门和跨地域的业务场景中，可靠身份验证成为保障业务安全和数据合规的前提；其次，远程办公和混合办公模式的普及显著增加了多因素认证、生物识别认证以及零信任架构下动态身份验证的需求，从而直接拉动身份认证市场扩张；此外，随着信息安全监管和数据隐私合规要求趋严，企业在身份认证方面的投入不断加大，以满足审计和合规需求。
- 结合整体市场规模来看，身份认证不仅在绝对市场份额上占据主导地位，其增长节奏也在很大程度上影响访问控制和身份治理的应用推广与投资决策，体现出身份认证在中国身份管理体系中不可替代的基础性和战略性价值。

来源：社会科学院，头豹研究院

中国身份认证行业综述——厂商份额

全球和中国身份认证市场均高度集中，头部厂商凭技术整合、生态协同和企业服务能力占据主要份额，企业选择方案更看重平台稳定性、可扩展性及与现有系统兼容性

全球身份认证主要厂商份额分析



□ 全球身份认证市场呈现高度集中化的格局，几家头部厂商占据绝大部分份额。Microsoft以29.1%领先，依托Office 365和Azure生态，将身份认证深度集成，为企业提供统一高效的解决方案。Okta和Oracle分别占16.5%和15.0%，前者以云原生身份管理和多因素认证著称，后者依托传统企业市场和核心系统客户稳步拓展业务。CyberArk以8.0%专注特权账号安全和身份治理，为企业安全提供关键支撑。四家合计占近70%市场份额，显示集中度高，技术整合、生态协同及企业安全能力成为争夺市场份额的核心因素，也反映企业选择身份认证方案更看重平台稳定性、可扩展性及与现有系统兼容性。

中国身份认证主要厂商



■ 报告完整版/高清图表或更多报告：请登录 www.leadleo.com

■ 如需进行品牌植入、数据商用、报告调研等商务需求，欢迎与我们联系

联系邮箱：service@leadleo.com

□ 中国身份认证市：阿里云以23.7%的面的身份认证解过社交、通信及信（9.8%）专注于企业安全和身份管理服务，亚信安全（8.6%）、芯盾时代（6.4%）及派拉软件（5.9%）则以特定行业或安全技术为切入点提供解决方案。整体来看，中国身份认证市场集中度较高，前四大厂商合计超过66%，技术能力、生态整合及企业服务适配性是厂商竞争的关键。

中国身份认证行业综述——应用场景渗透率

中国身份认证市场以金融（25.4%）和政府（19.8%）为主导，电信、互联网次之，制造、零售和医疗渗透较低，行业正从“安全工具”向“信任基础设施”演进，核心竞争力由技术机制转向数据互信与服务生态

中国身份认证应用场景渗透情况分析

头豹洞察



从行业成熟度看，政务与金融已进入体系化建设阶段，电信与互联网处于平台化融合阶段，而教育、制造、零售与医疗正处于场景化导入阶段。未来身份认证市场的竞争重心将从“系统部署”转向“身份信任的运营能力”。

横向比较显示：
合规驱动强度：金融 > 政务 > 电信 > 医疗技术
创新速度：互联网 > 电信 > 金融 > 教育潜在
增量空间：制造 > 零售 > 教育 > 医疗

这一格局意味着身份认证行业正从“安全工具”演变为“信任基础设施”，其核心竞争力正由算法与安全机制转向数据互信与服务生态。

体系化信任管理转型的关键窗口期

DaaS化将成动认证向云移。

场景融合与隐私计算推动新兴行业快速成长，制造、教育、零售将成为身份认证的第二增长曲线。

- 身份认证应用场景渗透情况总结如下：
- 金融与政府占比高，主要因二者对身份可信度、合规审计与反欺诈的要求极高：反洗钱、开户KYC、电子政务都驱动持续投入；电信占比靠的是海量用户管理与实名制，以及SIM/终端绑定和业务鉴权场景。互联网与教育渗透来源不同：互联网侧重用户体验与高并发认证（社交、支付、直播），教育侧重在线考试与学历验证的场景化需求。制造与零售当前占比较小，但随着工业互联网、供应链可追溯以及门店+电商的全渠道融合，设备身份、员工与顾客身份管理会快速上升。医疗受限于隐私合规与系统碎片化，增长被抑制但在远程问诊、电子病历授权、医保结算等场景有刚性增长。总体增长动力来自三点：一是法规与合规（推动刚需），二是技术演进（生物识别、FIDO、密码学隐私计算、统一身份平台），三是行业数字化转型（从点到面、从静态到实时）。障碍为遗留系统改造成本与数据孤岛、隐私担忧。未来趋势是跨域统一身份、无密码化接入与身份即服务（IDaaS）成为主流。

中国身份认证行业综述——各国的数字身份系统对比

中国数字身份偏中心化、合规导向，新加坡强调统一平台与高采纳率，韩国采用去中心化DID架构，突出用户数据控制和跨部门整合，三国在治理、技术架构和用户同意机制上各具特色

中国、新加坡、韩国三国的数字身份系统对比

特征	用户	治理结构	法律依据	跟标识符	表现形式	用户载体	技术架构	采纳模式	用户同意	数据共享	发展阶段	跨境策略	安全理念
中国（网号/EID）	600万用户（2025年5月）	公安部 国家互联网信息办公室	《网络安全法》《个人信息保护法》《eID管理办法》等	居民身份证号码	网证及网号	基于硬件的安全芯片	中心化公钥基础设施（PK）以凭证为中心，基于国家商用密码和硬件安全元件	公民自愿申请	PIPL要求明确同意，但有广泛的法律例外	“最小化和必要性”提供加密验证不共享明文数据	受鼓励但处于初期	聚焦粤港澳大湾区内的区域一体化	保护标识符。在线交易使用加密非明文的令牌
新加坡（SINGPAS）	500万用户（到2024年底）	政府科技局	《个人资料保护法》《公共部门（治理）法》	居民登记身份证（NRIC） 外国身份识别人号码（FIN）	Singpass APP Digital IC	APP	中心化平台即服务（PaaS）API驱动，基于OpenID Connect流程	事实上具有强制性	每次数据共享都需要明确细粒度的交易级同意	“一次告知”用户通过Myinfo API同意共享数据	成熟且广泛	通过《数字经济协定》积极寻求全球互操作性	强认证（多因素、生物识别）
韩国（K-DID）	400万用户（到2024年底）	内政安全部 数字平台政府总统委员会	《个人信息保护法》《居民登记法》	居民登记号	“移动身份证应用”APP以及其中的移动身份证	APP（初始需关注实体IC卡）	基于区块链的去中心化身份（DID）框架，用户数据存储在个人设备	可选	去中心化控制：用户直接从设备控制和同意数据使用	选择性披露：用户控制数据按需提供	与银行、医院、电信运营商等私营部门广泛整合	通过世界银行分享模型签署数字经济协定	通过去中心化和区块链技术将数据控制权交还用户

第二部分：产业链分析

主要观点：

- 在个人身份认证方面，全球多采用分散化或联盟模式，依托护照、社保号等组合标识，且欧盟通过eIDAS推动跨境互认，而中国则以居民身份证为核心，形成覆盖网络、金融等多场景的统一实名认证体系；
- 全球身份认证趋向分散化、隐私优先与去中心化技术，中国则以居民身份证和统一企业代码为核心，强调实名制、国产密码及安全效率并重，同时在金融等领域探索分布式身份。
- 两种体系的核心分野在于身份与数据的掌控权归属：一方依赖集中式机构主导并以统一管理提升安全，另一方强调多方协作与用户自主管理，从而在隐私保护、灵活性与可信度之间形成不同的发展取向。



中国身份认证行业产业链分析——不同国家的政策分析

全球身份认证政策各具侧重：欧盟重隐私与跨境互操作，美国强调安全与技术标准，中国聚焦实名制与集中治理，共同趋势为强化用户数据主权、推广强认证技术及探索跨境互认

不同国家的政策与法规要求

□ 欧盟：隐私优先 跨境互通	□ 美国：国家拿权有限 标准引导为主	□ 中国：可信数字身份 强立法强监管
<关键法规> - GDPR：数据处理合法性、透明度与安全要求 - NIS2：提高身份认证服务安全防护能力 - eIDAS 2.0：用户数据主权（SSI）、跨境互认 <政策趋势> - 强调用户掌握数据主权 - 推动跨境互认机制 - 统一数字身份生态 - 电子钱包普及 - 隐私保护与互操作性平衡	<关键法规> - 美国行政命令14028、国家网络安全战略 - CISA身份管理指南：IDAM能力范围细化 - NIST800-63：身份验证等级划分、风险策略 - NIST IRTA2.0：身份识别可信度框架 <政策趋势> - 政府侧加强标准导向与基础设施建设 - 商业侧强调联邦身份与无密码认证 - 强调基于风险的身份策略 - 推广强认证手段（FIDO2、WebAuthn） - 零信任架构中持续验证机制	<关键法规> 《网络安全法》《数据安全法》《个人信息保护法》 - GB/T35273-2020个人信息安全规范 - GB/T42573-2023网络身份服务安全技术要求 - 国家网络身份认证公共服务管理办法 <政策趋势> - 政府主导建设身份安全基础设施 - 技术上，集中式治理与新兴技术深度融合 - 强调网络实名、可信认证、数据分类分级保护 - 跨境协同上有限开放于安全可控并重

□ 其他地区数字身份政策特点				
□ 日本	□ 韩国	□ 新加坡	□ 印度	□ 澳大利亚
《个人信息保护法》《MYNUMBER法》 - 鼓励私营参与身份认证服务 - 推动全国MY Number数字身份系统	《个人信息保护法》（PIPA）实名制今适用于特定领域（金融与政府） - 生物识别信息视为敏感信息，使用受限 2012年全面实名制被判违宪	- SingPass国家级数字身份系统 《个人数据保护法案》 - 政府主导开发，支持跨机构统一认证 - 使用AI驱动技术，防范AI滥用风险	《Aadhaar法案》（2016） 《数字个人数据保护法案》（DPDP Act） - Aadhaar全球最大规模数字身份项目 2018年最高法院裁定合宪但限定使用范围	《数字身份法案》（Digital ID Act 2024） - 可信数字身份框架（TDIF） - 联邦与州/地区共同参与的联合系统 - 强调用户对个人身份数据的控制权

全球数字身份政策共同趋势	1、数据主权与用户控制权日益受到重视 2、强认证技术（如生物识别、FIDO2）成为主流	3、数字身份与隐私保护平衡成为全球性挑战 4、跨境互认机制探索不断深入
--------------	--	--

维度	欧盟	美国	中国
核心逻辑	隐私优先，跨境互通并重	国家安全为锚点，技术标准驱动	信任圆圈的基石
法律手段	强制立法主导	联邦立法	法律+制度
技术路线	《数字身份框架法案》、跨境互认机制	依赖行业自律与州级法规，联邦层面缺统一框架	三大法规+实名制、数据分级保护
实施重点	去中心化身份	零信任架构+FIDO	集中治理+新技术融合
典型特征	支持用户自主控制的数字身份钱包，替代实体证件	去中心化身份推进速度领先，但隐私技术不完善	身份治理为+实人认证、区块链存证、可信计算
	跨境协同	市场创新优先	政务融合
	纳入欧盟网络安全与数字安全框架，确保身份安全与数字安全协同	企业主导技术落地（如微软、IBM），包容性不足	“一证通办”覆盖社保、税务等领域，便民服务导向
	用户主权、隐私强保护、跨境互操作性强	技术领先但碎片化、隐私保护机制不完善	安全底线明确、集中管控、民生服务导向

中国身份认证行业综述——各类身份认证的全球与中国情况对比

全球身份认证趋向分散化、隐私优先与去中心化技术，中国则以居民身份证和统一企业代码为核心，强调实名制、国产密码及安全效率并重，同时在金融等领域探索分布式身份

各类身份认证的全球与中国情况对比

认证维度	全球普遍模式与趋势	中国主要模式
个人身份认证	分散化或联盟模式：多依赖社保号、驾照、护照等组合进行身份验证，不同领域标识符可能不同。欧盟eIDAS法规推动跨境电子身份互认	强中心化统一模式：以居民身份证为基础，形成覆盖网络、金融等场景的强实名认证体系
企业身份认证	分层与碎片化：美国等联邦制国家，公司在州一级注册，联邦税号（EIN）主要用于报税，缺乏全国唯一贯穿所有领域的商业标识	“一元化”统一代码：全国企业拥有唯一的“统一社会信用代码”，贯穿所有商事活动
设备身份认证	供应链安全与零信任架构：关注硬件供应链安全，倡导零信任架构，强调对设备身份的持续验证	国产密码算法与分级管理：物联网设备安全强调国产密码算法（如SM系列）的应用，并对关键信息基础设施设备有额外安全要求
核验技术趋势	无密码化与分布式身份：推广FIDO2等无密码认证标准；探索去中心化数字身份（DID）技术	积极探索前沿模式：在金融等领域试点分布式数字身份（DID）技术
数据治理理念	重隐私保护设计：如欧盟GDPR强调数据最小化和用户权利，推行数侧字身份时往往更强调隐私保护设计（Privacy by Design）	安全与效率并重：强实名制将网络身份与现实身份紧密绑定，侧重于公共安全与管理效率

头豹洞察

□ 全球与中国的身份认证模式呈现明显差异与各自特点：

在个人身份认证方面，全球多采用分散化或联盟模式，依托护照、社保号等组合标识，且欧盟通过eIDAS推动跨境互认，而中国则以居民身份证为核心，形成覆盖网络、金融等多场景的统一实名认证体系；

在企业身份认证上，全球存在分层碎片化现象，如美国企业标识多用于税务，缺乏全国统一标识，中国则通过统一社会信用代码实现“一元化”管理；

设备身份认证方面，全球侧重供应链安全和零信任架构，中国强调国产密码算法与分级管理，并对关键设备增加安全要求；核验技术趋势上，全球推广无密码认证和分布式身份（DID），中国在金融等领域积极试点DID；数据治理理念上，全球重隐私保护设计，中国侧重安全与效率并重，通过实名制绑定网络与现实身份，实现公共安全与管理效率的平衡。

来源：社会科学院，头豹研究院

中国身份认证行业产业链分析——身份认证监管情况

中国身份认证体系以居民身份证、统一社会信用代码和国产密码设备为核心，实现高度集中和全网通行，而全球则多依赖分散标识、市场化服务及零信任或去中心化架构，注重隐私与跨域互认

全球及中国身份认证监管情况

个人身份认证的深入解读

中国：国家主导的“实名制”与匿名化创新
中国的个人身份认证体系以居民身份证为信任根基，并扩展至网络空间。其核心是公安部建设的“互联网+可信身份认证平台”（CTID），为公民生成网络电子身份标识（eID）。在具体核验时，普遍采用多要素结合的方式，如身份证要素+人脸识别+短信验证码，以确保高安全级别场景的可靠性。值得注意的是，为应对隐私风险，国家推出了创新的“网号”与“网证”体系。在进行网络身份认证时，用户可以使用“网证”这一匿名化凭证，平台获得的仅是“是或否”的核验结果，而无法接触到用户的明文身份证信息，实现了“可用不可见”，这极大地减少了个人信息在互联网平台上的留存与泄露风险。

全球：多元模式与区域一体化尝试
全球范围内缺乏像中国这样的统一身份标识符。美国主要依赖社会安全号码（SSN）与市场化认证服务结合的模式，但存在碎片化问题。欧盟则依据 eIDAS法规，致力于建立成员国之间的电子身份互认框架，推动跨境数字身份的使用。印度则建立了以Aadhaar生物识别数据库为核心的大规模身份系统，广泛应用于社会福利发放。在技术理念上，欧美更早倡导去中心化身份（DID/SSI），即用户自主掌控身份数据，无需依赖中心化的发证机构。同时，FIDO联盟推动的无密码认证标准（如WebAuthn）也在全球范围内成为重要技术趋势。

企业身份认证的深入解读

中国：以“统一社会信用代码”为核心的电子化
中国的企业身份认证高度统一。每个企业拥有一个唯一的“统一社会信用代码”，相当于企业的“数字身份证”。电子营业执照是企业数字身份的核心载体，与纸质执照具有同等法律效力。在核验方式上，“法人四要素认证”（企业名称、统一社会信用代码、法人姓名、法人身份证号）是验证企业身份真实性的基础手段。国家正大力推动电子营业执照在政务、商务领域的应用，目标是实现市场主体身份“一次验证、全网通行”。电子印章技术也同步发展，其管理与使用流程参照实物印章，并需符合国家密码管理规范。

全球：分散注册与联盟认证
在许多联邦制国家，如美国，企业注册是州政府的职权，因此缺乏一个全国统一的、贯穿所有商业活动的企业身份标识。联邦税号（EIN）主要用于税务目的。这种分散性导致企业在线处理跨州业务时可能面临身份互认的挑战。因此，市场化的商业信用代码和联盟式的认证服务在这些国家扮演了重要角色。全球企业身份认证的技术趋势也与个人认证类似，向零信任架构和基于区块链的分布式身份管理发展。

设备身份认证的深入解读

中国：强调国产密码算法与物联网设备安全
设备身份认证确保设备本身（如手机、物联网传感器、服务器）的可信。在中国，设备身份认证受到《网络安全法》、《数据安全法》以及物联网安全标准的严格约束。一个显著特点是强制或鼓励使用国产密码算法（如SM2、SM4）来保障设备身份认证过程中的通信安全。对于关键信息基础设施中使用的设备，还有更为严格的安全检测和分级保护要求。在风控层面，除了传统的设备指纹技术，还需密切关注供应链安全，防止恶意硬件植入。

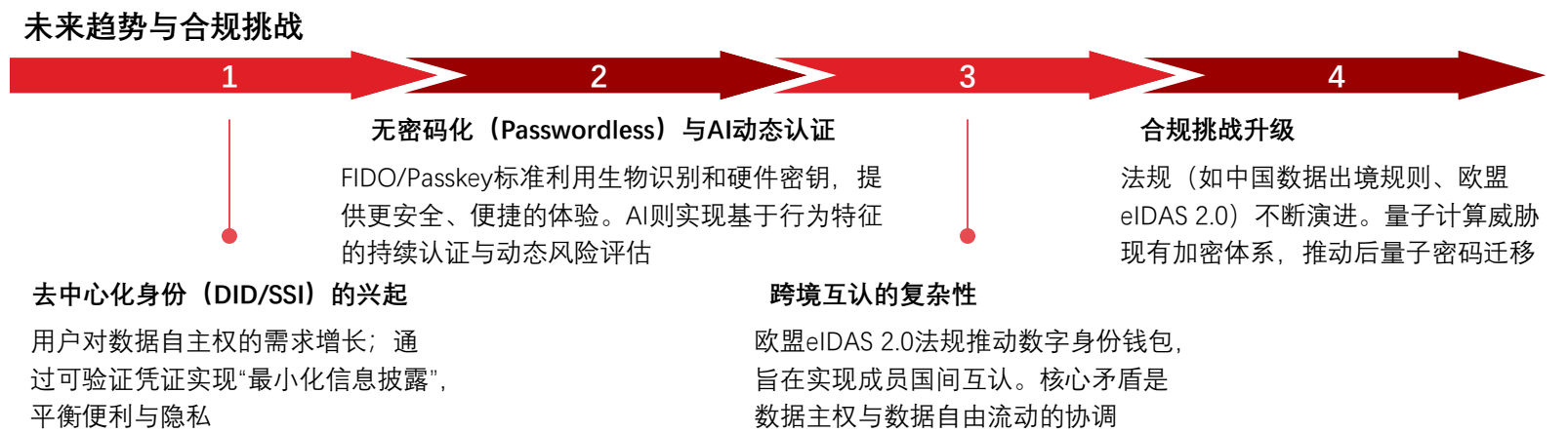
全球：零信任与物联网安全框架
全球范围内，设备身份认证是零信任安全模型的基石。理念是“从不信任，始终验证”，这意味着每次设备尝试访问网络资源时，其身份都需要被重新校验。国际上普遍遵循的技术标准包括基于公钥基础设施（PKI）的X.509证书等。对于数量庞大的物联网设备，全球正在建立相应的安全标准，强调设备的唯一身份标识、安全的启动过程以及生命周期的密钥管理。

中国身份认证行业产业链分析——续上页

由国家或机构集中主导的统一模式，逐步迈向多元主体协作、跨区域互认与用户数据主权增强的形态，在安全、效率与隐私之间不断寻找新的平衡点，推动治理理念与技术路径同步演进

全球及中国身份认证监管的模式分析

维度	中国模式	全球主流模式
治理逻辑	国家主导的统一治理：以国家信用为背书，构建集中统一的认证基础设施，强调管控效率与公共利益。	市场驱动或联盟治理：多以市场力量（如美国）或区域联盟（如欧盟eIDAS框架）为主导，强调竞争、互操作性与个人选择
技术路径	自上而下的标准化：推行全国统一的技术标准（如国密算法、CTID平台），追求“一号一证”通办全网	自下而上的多样化：技术路径多元，如美国的NSTIC战略倡导构建一个由私营部门主导的“身份生态系统”
数据主权与隐私	数据主权优先，匿名化实践：在强实名制基础上，通过“网号”、“网证”等技术实现“前台匿名、后台实名”，力求在安全与隐私间平衡	隐私权优先，立法明确：欧盟GDPR等法规将隐私权视为基本权利，严格限制数据收集，并大力探索用户自主可控的去中心化身份（DID）



来源：社会科学院，品牌官网，头豹研究院

头豹洞察

□ 该内容展现了身份认证治理从传统集中式模式向更开放、去中心化方向演进的逻辑结构。整体框架围绕治理理念、技术路径以及数据主权与隐私保护等关键要素展开，并将其分为连续的四个发展阶段。起始阶段强调以国家或机构为核心的统一标准与统一认证体系，追求安全可控与高效管理；随后逐步引入更多市场力量与多元技术，提升灵活性与用户体验；再往后，身份体系开始迈向跨机构、跨区域的互通互认，既需要兼容不同主体的利益与标准，又必须确保合规性与风险可控；最终阶段则呈现更高水平的自主权与隐私保护，强调用户对自身数据的掌控，以及技术在确保安全同时尽量减少对个人信息的暴露。整体来看，这一演进路径折射出身份治理从“中心权威”向“用户中心”、从“信息集中”向“风险分散”的趋势。它不仅体现监管、市场与技术三者之间的动态平衡，也展示未来在跨境流通、合规要求与前沿技术（如量子安全）背景下的挑战与机遇。这种线性推进方式突出说明身份认证生态将持续朝着更安全、更可信且更尊重个人权益的方向深化发展。

中国身份认证行业产业链分析——国内外身份认证案例分析

两种体系的核心分野在于身份与数据的掌控权归属：一方依赖集中式机构主导并以统一管理提升安全，另一方强调多方协作与用户自主管理，从而在隐私保护、灵活性与可信度之间形成不同的发展取向

全球及中国身份认证案例分析

国内典型案例分析

1 China Poly Group 股份有限公司、Sunac China Holdings 及 Greenland Holdings 子公司——宁波市房地产开发商面部识别数据采集案

案件背景：浙江宁波市市场监管局处罚三家房地产开发商（上述三家子公司）因其在售楼处安装人脸识别设备，对客户进行面部采集、识别，未取得客户明示同意。
违规行为：收集客户面部图像、进行识别分析，用于识别“带中介 / 非中介”客户差别对待，没有告知、取得同意。
处罚结果：三家开发商被罚款共计 25 万元人民币（约合 US\$ 38,500）
法律责任：根据中国相关法律，面部识别属于生物识别信息、敏感个人信息。若未经同意收集或处理，可能触及《中华人民共和国个人信息保护法》及“严重侵犯公民个人信息罪”的刑事责任范围。

2 XPeng Motors（小鹏汽车）——非法收集店铺访客面部图像案

案件背景：2021 年上海一 EV 公司（即小鹏）在其直营店安装拥有“人脸识别”功能的摄像头，6 个月内收集超过 43 万张访客面部照片，未经访客知情同意。
违规行为：未经告知、未取得同意收集访客面部识别数据，用于性别年龄统计分析；违反《消费者权益保护法》等法规。
处罚结果：被上海当地市场监管机关罚款 100,000 元人民币（约 US \$15,716）
法律责任：虽为行政处罚，但该类未经同意处理生物识别信息的行为，依据《个人信息保护法》可能承担更严厉责任（尤其如数据外泄、出售、交易）。

国外典型案例分析

1 OKX（奥凯斯）加密货币交易所 KYC/AML 失败案（美国）

案件背景：2025 年 2 月 24 日，美国 United States Department of Justice (DOJ) 公布，OKX 运营方 Aux Cayes Fintech Co. Ltd. 认罪：非法经营未注册款项传输业务，且自 2018 年至 2024 年，在美国设有用户、促使美国用户绕过身份验证流程，且平台支持交易无完整 KYC。
违规行为：未对美国客户实施有效身份验证(KYC)、身份核查系统缺失、甚至鼓励用户输入虚假国家/身份证号以规避验证流程。
处罚结果：OKX 将支付超过 US\$ 504 million 的罚款和没收款，其中包括约 US\$ 84.4 million 罚金 + US\$ 420.3 million 没收非法收益。
法律责任：因“经营未注册款项传输业务”违反美国法 18 USC §1960；同时因反洗钱 (AML)、客户识别(KYC)制度严重缺失，承担刑事责任。

2 美国金融机构 - U.S. Bank National Association 身份验证/客户识别失败案

案件背景：2018 年 2 月 15 日，美国 Financial Crimes Enforcement Network (FinCEN) 与美国货币监督署(OCC)协调，对 US Bank 评定民事罚款 \$185 million
违规行为：银行未能建立和实施充足的反洗钱(AML)项目，未能对高风险客户进行适当审查、交易监控系统故意限流(“alerts capping”)，多次未对未知风险客户进行客户身份识别(KYC)与持续尽职调查(CDD)。
处罚结果：总罚款 185 百万美元，其中部分支付给财政部。银行还被要求改进 AML/KYC 流程。
法律责任：违反《银行保密法》(BSA) 及其客户识别程序(CIP)义务，可能引发民事罚款、行政制裁甚至刑事责任（如故意隐瞒可疑活动）

头豹业务合作

会员账号

可阅读全部原创报告和百万数据，提供PC及移动端，方便触达平台内容

定制报告/词条

行企研究多模态搜索引擎及数据库，募投可研、尽调、IRPR等研究咨询

定制白皮书

对产业及细分行业进行现状梳理和趋势洞察，输出全局观深度研究报告

报告作者



袁栩聪
首席分析师
oliver.yuan@leadleo.com



莫舒棋
行业分析师
kay.mo@leadleo.com

招股书引用

研究覆盖国民经济19+核心产业，内容可授权引用至上市文件、年报

市场地位确认

对客户竞争优势进行评估和证明，助力企业价值提升及品牌影响力传播

行研训练营

依托完善行业研究体系，帮助学生掌握行业研究能力，丰富简历履历

业务咨询

- 客服电话：400-072-5588
- 官方网站：www.leadleo.com

深圳办公室

广东省深圳市南山区粤海街道
华润置地大厦E座4105室
邮编：518057

上海办公室

上海市静安区南京西1717号
会德丰国际广场 2701室
邮编：200040

南京办公室

江苏省南京市栖霞区经济开发
区兴智科技园B栋401
邮编：210046



方法论

- ◆ 头豹研究院布局中国市场，深入研究19大行业，532个垂直行业的市场变化，已经积累了近100万行业研究样本，完成近10,000多个独立的研究咨询项目。
- ◆ 研究院依托中国活跃的经济环境，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- ◆ 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- ◆ 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- ◆ 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- ◆ 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- ◆ 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- ◆ 本报告所涉及的观点或信息仅供参考，不构成任何证券或基金投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告或证券研究报告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。
- ◆ 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本报告所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本报告所载资料、意见及推测不一致的报告或文章。头豹均不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。



2026 福布斯中国行业发展领创者评选

2026 FORBES CHINA PIONEER INNOVATORS IN INDUSTRY DEVELOPMENT SELECTION

百年福布斯 权威标杆

行业最具影响力的荣誉殿堂

- 覆盖核心赛道：AI科技 | 新能源 | 医疗健康 | 大消费 | 制造业 | 服务业
- 全球媒体矩阵传播：赋能个人与品牌，提升市场影响力
- 设立多重荣誉：①主评选：行业发展领创者
②子评选：领军企业 / 创新品牌 / ESG标杆/AI企服标杆/新锐分析师