网络安全创新大会
Cyber Security Innovation Summit

面向城市数字化转型的数字信任体系建设研究

惠志斌

上海社科院互联网研究中心主任 研究员

上海赛博网络安全产业创新研究院 首席研究员

从“信任”到“数字信任”

- 信任关系受到行为主体、社会关系和风险三种因素的约束影响
- 数字时代，信任构建的三种约束条件和基础情境发生了根本改变，传统信任关系开始向新型数字信任关系演变。

农业文明

- **基于熟人社会（宗族、村落）形成的人际信任**
- 通过熟人关系网络（宗族、村落）和书信进行信息传递
- 自给自足的农业生产，社会分工和依存度较低；
- 以重大自然灾害、战争、瘟 疫、 社 会动 乱 为 主，带有典型的不可抗力

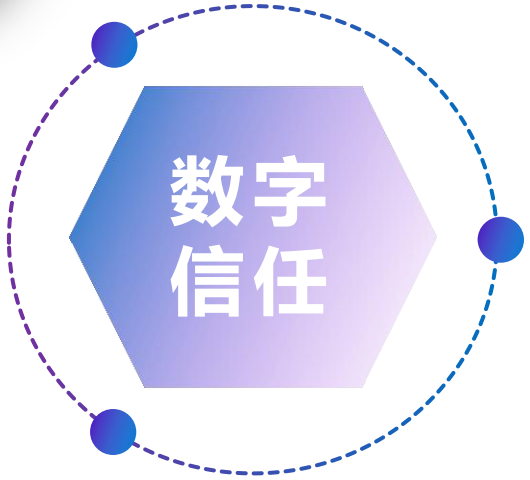
工业文明

- **基于权威规范（法律、契约）形成的制度信任**
- 通过印刷术、电 报、电话进行信息传递
- 工业流水线生产和市场经济形成了社会化分工，社会依存关系较高；
- 人类活动对自然深度介入产生的环境污染、生态破坏影响巨大，还包括犯罪、工程灾害等

数字文明

- **基于数字技术在虚拟数字空间形成的数字信任**
- 平台企业和跨国互联网公司形成了基于数字经济的精细化社会分工，社会依存关系极高；
- 通过互联网、移动设备进行信息传递
- 高频网络攻击、数据泄露、数据滥用、隐私侵害等网络安全风险对整体社会影响越来越大

数字信任的核心概念和特征



数字信任（Digital Trust）：是指一切链入 / 映射到数字空间的泛在网络实体，基于数字身份识别、可信数据流通和网络安全能力验证形成的正向预期，以及由此产生稳定数字交互关系。

◎ 数字信任主体包括海量泛在的网络实体

以智能终端 、设备、算法程序（为代表的机器网络实体成为重要的数字信任主体，政府、企业和社会组织也都将通过数字身份实现数字信任。数字身份是数字信任的基本内核，数字信任是数字身份的拓展延伸。

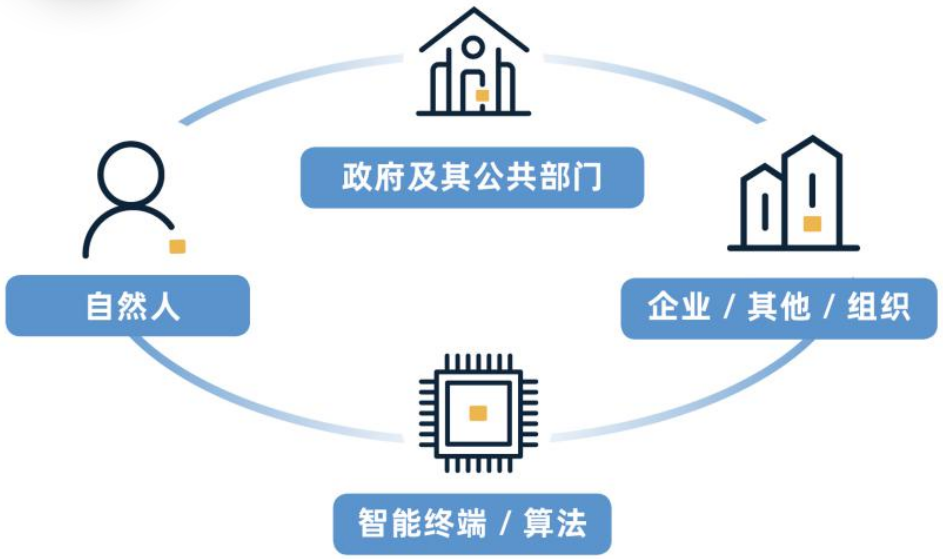
◎ 数字信任议题聚焦网络安全风险治理难题

实体世界与数字世界的风险深度交织泛化，高频网络攻击、数据泄露、数据滥用、隐私侵害等网络安全风险对整体社会影响越来越大。可信数据流通和网络安全能力成为信任的重要关切。

◎ 数字信任实践具有技术依赖性和场景差异性

数字信任的构建极大依赖于数字身份、密码学、隐私计算等安全技术的创新发展；同时不同场景下的交互关系和规则差异性极大，需要特殊的“信任通道”机制来实现数字信任的跨域传递。

多元主体数字信任关系建立



“泛在网络实体互联、异构数据实时流通、智能应用层叠涌现”的万物智联世界加速形成，人与人、人与物、物与物之间依托数字化方式交互形成各类经济和社会活动，亟需通过一系列科学方法和技术手段构建数字信任关系。

	产品/服务/解决方案	数字信任建设者类型
建立数字身份	身份标识 、身份验证与证明、身份鉴别、授权访问等	数字身份和电子认证的第三方服务机构（如CA中心等）
形成交互规则	电子合同、电子签名、隐私计算、可信环境、网络安全合规咨询等	电子认证第三方服务机构、律师事务所、法律咨询机构
明确安全能力	访问权限控制、漏洞监测、风险监测、态势感知、安全运营等	网络安全厂商、电子认证第三方服务
实现识别验证	电子认证、反渗透测试、网络安全评级认定、数据安全能力测评等	测评认证机构、电子认证第三方服务、网络安全厂商
持续正向反馈	网络安全事件的响应和救济，网络安全损失的控制和理赔等	网络安全厂商、网络安全保险公司、风控金融机构

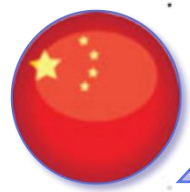
全球主要国家数字信任政策发展沿革

美 国

- 1995年，美国犹他州出台了全世界范围内第一部《数字签名法》。
- 2000年6月，美国出台《国际与国内商务电子签名法》。
- 2009 年 5月，美国白宫发布《网络空间政策评估》报告，明确要建立基于网络安全的身份管理战略。
- 2011年4月，美国发布《网络空间可信身份国家战略》（NSTIC）。
- 美国在2012年《数字政府战略》、2020年《联邦数据战略和2020年行动计划》中，均**强调网络信任的重要性；**

欧 盟

- 欧盟在2000年、2002年、2005年、和2006年的年度电子欧洲计划或电子政府计划中，持续强调建立安全、扩展、有效和共通数字身份的重要性。
- 2014年，欧盟发布《电子身份认证与签名条例》（eIDAS条例）。
- 2006年6月，欧盟发布《泛欧洲电子身份标识管理框架路线图》。
- 欧盟在2020年《塑造欧洲数字未来》《欧洲人工智能白皮书》《欧洲数据战略》中，**强调数字信任在欧洲数字化转型的重要性。**



中 国

- 中国在《”十三五“国家网络安全规划》中，强调要构建网络可信身份服务生态环境；
- 2004年8月，全国人大通过国家《电子签名法》；
- 2006年2月，国务院发布《关于网络信任体系建设的若干意见》；
- 2016年11月，全国人大通过《网络安全法》，提出“**国家实施网络可信身份战略**，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认”。

全球数字信任产业链生态

网络安全创新大会
Cyber Security Innovation Summit

软硬件供应商

以软硬件供应商为主，是整个产业链的开始端，为数字信任提供软件、硬件和集成服务，包括介质厂商、加密机厂商、安全设备供应商、PKI 软硬件开发商、 安全集成服务商等

电子认证第三方服务机构

电子认证第三方服务机构，包括经国家行政许可的CA权威机构和自建电子签名机构，提供数字身份、电子合同、鉴别认证、时间戳、电子签章、可信数据流、可信网站鉴别等产品服务

网络安全厂商

包括提供身份控制、权限控制、可信计算、可信环境、零信任架构部署等产品服务的安全厂商。随着零信任架构的流行以及身份权限控制日益重要，越来越多的网络安全厂商会将其的安全产品升级为综合的数字信任服务

信任增值服务

提供数字信任增值扩展服务机构，包括利用区块链、人工智能等新兴技术赋能电子认证和数字信任服务的科技企业，基于数字信任提供网络安全保险和担保的金融机构，为数字信任提供测度量化的咨询公司等

全球数字信任的关键技术方向

PKI及密码学

公钥基础设施（PKI）是以公钥加密体系为基础，包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能，为网络通信提供安全保障的安全基础设施。

数字身份

通过数字通道进行远程身份识别、验证的系统过程和标识体系，包括政府、公共部门、企业、非盈利组织或个人实体颁发的，基于数字签名、口令、生物特征数据、密码、二维码、嵌入身份信息的智能设备、安全令牌等任何数字技术的数字身份。

区块链

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在数字经济时代应用模式的集成创新。区块链基于其去中心化、难篡改、系统激励等优势，是数字信任体系的重要方向。

隐私计算

包括同态加密、多方安全计算、差分隐私、联邦学习、零知识证明等多种技术方向，可以确保合作双方能够对数据进行计算、比对、运行等并读取和利用结果，并保证任何一方均无法得到除应得的计算结果之外的其他任何信息。

城市数字化转型的数字信任需求

城市基础设施数字化转型的数字信任需求

通过部署适应于基础设施互联互通环境下的低成本、快捷的身份识别验证设备和访问控制，能够在网络边界日趋模糊、网络拓扑日益复杂的环境下构建“人 - 物、物 - 物”的数字交互关系，保障数字城市高效感知和平稳运行。

城市数据要素市场化配置的数字信任需求

通过区块链、隐私计算等技术，实现数据要素在共享、开放和利用等全链条的可信流通，从而构建双方的数字信任关系，能够极大地支撑数据要素市场发展。

城市经济生产数字化转型的数字信任需求

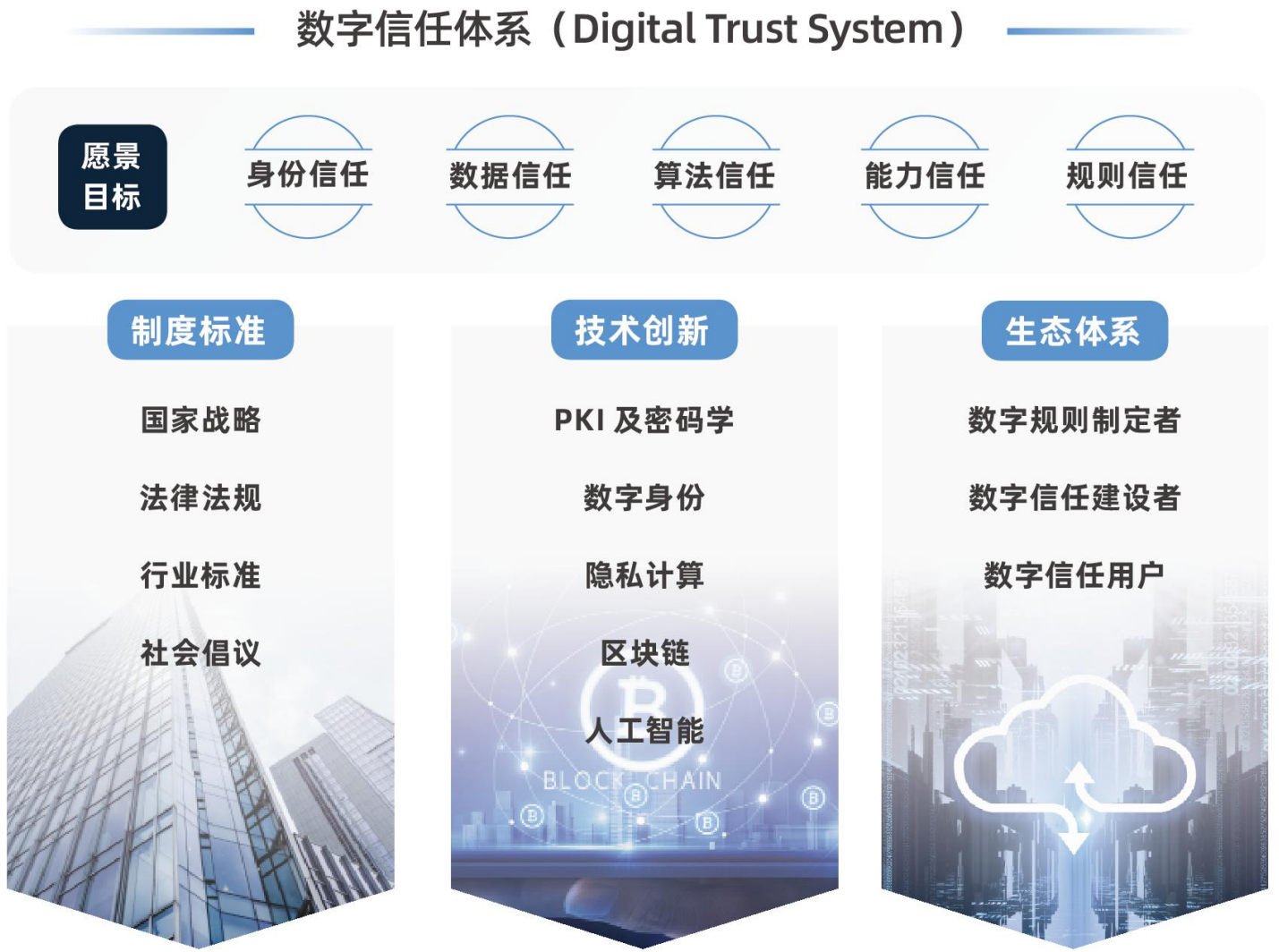
企业内部、企业与供应链、人与机器之间亟需数字技术深度内嵌的新型数字信任体系需要构建基于主体网络安全能力认证的数字信任测度量化机制，形成市场与合规双驱动下网络安全能力建设的良性循环。

城市治理和公共服务数字化转型的数字信任需求

借助安全可信、弹性扩展的数字身份服务能力，能够降低数字接入上的技能要求和流程成本，减少因数字身份欺诈、多次重复认证产生的安全风险，更好地分享城市数字化转型发展的红利。

打造面向城市数字化转型的数字信任体系

数字信任体系（Digital Trust System）是以可信数字身份验证和可信数据流通为核心，聚焦新型网络安全风险和数字社会治理难题，通过制度标准、技术创新、产业生态等多维度建设，最终实现身份信任、数据信任、算法信任、能力信任、规则信任等五大目标的数字时代新型信任关系。



相关建议

1.加快完善数字信任制度规则

研究制定国家和城市级数字身份战略及其管理办法，统一规划非对称加密、生物特征识别、分布式等数字身份的认证、发展和应用，在物联网、人工智能、区块链等“人 - 机”复杂交互的重点行业领域，制定用户数字身份和设备数字标识相互识别验证、数据可信传输流通的管理办法和标准规范，为各主体建立数字信任关系提供体系完备的治理规则。

2.前瞻部署数字信任技术方向

加快技术创新，加快密码法算法、商业密码应用的技术攻关，探索量子计算、量子加密的技术演进动态；推动区块链与电子认证技术的融合发展；围绕隐私计算方向探索数据共享、数据流动和数据交易中数字信任关系构建，推动企业、组织在零信任架构构建数字信任交互架构。

相关建议

3.培育壮大数字信任产业集群

充分打通软硬件供应商、电子认证第三方服务机构、网络安全厂商、律所、网络安全保险和咨询企业，形成数字信任综合支撑服务能力。围绕数字信任认证、中介、担保等业务，深化数字信任增值服务的集成式开发。围绕解决方案培育、行业应用创新和支撑体系构建等开展应用示范工作。

4.形成场景化数字信任解决方案

搭建全市数字身份统一认证平台，形成统一的用户身份识别、电子合同签署、数据可信传输、责任溯源等服务。探索分布式物联智能设备识别框架，培育覆盖企业身份认证、设备身份认证的分布式设备标识服务能力和工业 SaaS 平台、APP 身份认证服务新场景。利用区块链、数字标识、数据溯源等技术，建设数据要素线上登记、全链条确权和第三方科学估价的统一平台。

相关建议

5.构建区域一体化的数字信任生态

依托国家区域一体化战略（长三角一体化、长江经济带等），打现在数字身份和电子签名在地区性、行业性交叉认证过程中存在“各自为政”的分散甚至割裂情况。加强区域内在数字身份、电子签署、数据流通、数据安全方面的标准对接和技术认证。

6.推动数字信任规则标准国际合作

依托我国数字“一带一路”倡议、国际自由贸易谈判（RCEP等）和自由贸易区（上海自贸区临港新片区等）建设，加强与主要贸易伙伴的数字认证服务机构的交流合作，在新一轮的数字贸易发展中实现国际电子认证等数字信任服务的创新引领。

网络安全创新大会
Cyber Security Innovation Summit

THANKS

本报告为上海市数字证书认证中心与赛博研究院合作研究成果。如有需要，请关注公众号下载最终报告（后台回复“数字信任”）

上海市CA中心

赛博研究院