城市数字化转型数字信任体系研究 2.0

以数据为核心
构建新型数字信任体系

City digital transformation
digital trust system research 2.0

Building new digital trust system with data as the core

上海CA中心

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

COPYRIGHT STATEMENT

版权声明

出品方

上海市数字证书认证中心有限公司

上海赛博网络安全产业创新研究院

研究专家

崔久强	上海市数字证书认证中心有限公司总经理
陈晓曈	上海市数字证书认证中心有限公司战略副总监
郑　宁	上海市数字证书认证中心有限公司高级研究员
赵　鸣	上海市数字证书认证中心有限公司高级研究员
惠志斌	上海赛博网络安全产业创新研究院首席研究员
唐巧盈	上海赛博网络安全产业创新研究院高级研究员
朱易翔	第五空间研究院理事长、翼盾智能CEO

FOREWORD

前 言

当前，新一轮科技革命和产业变革深入发展，人类社会正在进入一个“人机物”三元融合的万物智能互联时代。城市数字化转型是数字时代的必然进程，呈现出“人机物”多维互联、数据实时流通、智能应用层叠、场景泛在融合、线上线下结合的发展特征，让城市复杂巨系统的网络边界日趋模糊，脆弱性凸显，传统的基于边界的网络安全防护体系无法适应城市数字化转型的发展要求。可以说，在人与人、人与物、物与物之间全面依托数字化方式交互的各类经济和社会活动中的信任关系和信任机制亟待重塑。因此，在数据日益发展成为社会重要生产要素的背景下，必须以数据为核心构建新型数字信任体系，以满足数字化转型提出的新型安全需求。

在此背景下，本报告分析城市数字化转型下数字信任面临的新型风险与挑战，借鉴国内外发展经验和实践案例，构建可信数字身份体系和数据流通信任体系动态匹配、有机耦合的数字信任策略，并聚焦“制度+管理+技术”三个层面，提出相关城市数字化转型数字信任体系建设的对策建议以及典型场景下的实践案例，助力数据要素市场构建，促进经济数字化、生活数字化、治理数字化等城市数字化转型。

CORE IDEA | 核心观点

● 信任关系与信任模式的演变与人类文明形态发展密切相关。万物互联下网络与现实边界逐渐模糊，个人、组织、物体的连接与交互依靠传统的信任机制难以适应城市数字化转型要求。数字信任是在这样的背景下产生的，它是使一切链入 / 映射到数字空间的网络实体，在以数字身份信任、可信数据流通为两大核心建设的信任支撑体系下，通过制度、管理、技术等一系列组合手段减少数字空间安全风险，并形成数字社会安全交互、高效运行的机制。

● 当前数字空间的信任体系建设既存在内生的安全问题，也面临外部的新型风险。一是数据安全与网络安全形势严峻，数据安全事件频发、网络安全边界日益模糊、新技术新应用安全风险凸显；二是数字主体身份标识能力远未完善，存在大量数字身份“孤岛”、身份信任仍主要依赖于传统集中式的认证手段、鉴别技术面临新型安全威胁；三是高质量数据流通能力尚未形成，统筹机制尚待健全、规则设计复杂困难、实践限制因素突出、数据跨境安全壁垒抬升。近年来，全球在数字信任领域顶层设计、数字信任体系管理机制、数字信任技术能力建设、场景化最佳实践落地等方面均具有长足发展。

● 本报告提出以数据为核心，构建城市数字化转型新型数字信任体系框架。该框架聚焦以“制度 + 管理 + 技术”多维度手段结合的数字身份和数据流通两大信任体系建设，形成两大体系动态匹配、有机耦合的信任策略，促进数据要素市场构建，支撑经济数字化、生活数字化、治理数字化等城市数字化转型。

● 数字信任建设高度依赖隐私计算、区块链、前沿密码等创新技术的发展，但其不仅仅是一个纯技术突破跃升的层面，还涉及政治、经济、法治、社会和文化等诸多因素。“制度 + 管理 + 技术”应作为一个有机整体贯穿数字信任建设全过程。

CORE IDEA | 核心观点

在城市数字化转型下，复杂多元的数字主体之间信任关系的建立，一方面无需验证所有的身份属性，而是依托技术对相应的身份属性进行智能匹配，以确保数字主体高效、安全交互；另一方面，这种信任关系的建立大多是瞬时的，且会根据场景的变化动态调整，需要确保数字身份的某一属性在特定场景中受到信任。

● 数据流通信任体系的构建需与可信数字身份体系有机耦合。一般地，数字身份之间的信任度越高，数据可信流通所需的技术手段复杂性越低，数据流通所需要的成本则相对较低；而数字身份之间的信任度越低，对数据流通的机制建设、管理手段、技术支撑和保障能力的要求就越高，其相对成本则越高。

● 针对城市数字化转型需求，数字信任建设可开展“三步走”策略。即第一步，做好数字信任体系顶层设计，明确体系框架；第二步，开展数字信任重点场景试点，形成最佳实践；第三步，进一步完善数字信任体系，服务整体数字化转型。未来，数字信任建设可在制度规则、管理机制、技术布局、平台建设、生态体系等方面具体推进，加快电子政务、物联网、医疗健康等重点领域应用。

CONTENTS | 目录

CONTENTS | 目录

1 PART

城市数字化转型下的数字信任

Building new digital trust system with data as the core

PART 1

城市数字化转型下的数字信任

信任(Trust)的演变与人类文明形态发展密切相关。农业文明和工业文明时代，人的社会活动高度依赖人际信任和制度信任。城市数字化转型下，大数据、人工智能、区块链、物联网等新一代信息技术快速发展，人类正在迈入“人机物”三元融合的万物智能互联时代，个人、组织、物体的连接与交互依靠传统的信任机制难以适应以数字技术和数字经济为基础的数字文明。由此，一种新型信任关系与信任模式——数字信任(Digital Trust)开始兴起，成为城市数字化转型的重要基座。

一 | 数字信任产生背景

1. 从信任到数字信任

信任是人类生产生活的基石，其对社会运转的作用正如“空气”对人类生存一样是必需品，但信任作为一项研究议题，进入研究视野的时间并不长。当前，信任已被各国学者广泛引入到社会学、经济学、心理学、博弈论和国际关系等多个学科之中，形成不同范式的信任理论模型，并在政府的公共治理实践和企业的市场商业行为中大量应用。总体来看，各界对于信任的内涵已形成了以下共识：

一是信任是一种减少社会复杂性的机制，并带来效益和价值。弗朗西斯·福山指出，信任是社会生活的基础、是简化复杂的机制之一、是经济交换的润滑剂、是一种社会资本，只有高度信任的社会才能构筑稳定、规模庞大的商业组织以应对全球经济的激烈竞争。而在大量的政治学、经济学和社会学研究中，信任都具备重要的社会性价值，包括在市场经济中降低双方交易和协作成本，具有高公信力的第三方提供居间产品或服务，在新技术发展和普及中减少怀疑和抵制，在政府治理中提高政策的理解度和执行力，减少风险应对中的交互成本等。

二是信任的构建和维护需要一定的机制和成本。不同主体间的信任并不是凭空存在的，而是通过预期、行为和反馈等多个环节交互的持续性构建过程。因此，信任的建立和维护都需要相对稳定的社会机制以及成本付出。包括基于心理和情感的信任，基于理性认知和计算博弈的信任，基于社会性权威(法律、契约)和道德规范的信任等等。

三是信任关系具有多种类型，信任模式演变与人类文明形态发展密切相关。一般而言，农业时代是以人际信任为主，即以人际关系为基础、诞生于熟人社会。工业时代以制度信任为主，其诞生于陌生人社会，是以契约、法律、法规等制度为基础的一种重要信任模式。而数字时代则是以数字信任（Digital Trust）为基础，数字信任是一种多维综合的信任关系，其不仅依赖于人际信任、制度信任，还与技术信任等息息相关。信任关系随人类文明形态的演变过程具体如表 1 所示。

表 1：人类社会发展的信任关系演变

人类社会发展演变	农业文明	工业文明	数字文明
主要信任模式	人际信任：基于人际关系构建的信任关系，具备较强的情感性，信任传递性较低	制度信任：基于政府监管和市场契约形成的信任关系，稳定性较强，信任传递性有限	数字信任：基于数字技术在虚拟数字空间形成的信任关系，高度依赖于数字技术和数字应用
行为主体类型	个体、社会单元	企业、各种社会组织	所有链接 / 映射到数字空间的组织、人和物
信息交互机制	通过熟人关系网络（宗族、村落）和书信进行信息交互	通过纸质文件、电报、电话等进行信息交互	通过互联网、移动设备等进行信息交互
社会主要风险	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	除了不可抗力风险外，因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	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
信任建立的特点	需要长时间的信息交互才能确定信任关系，且信任关系一旦被破坏，修复时间也相应较长	通过一段时间的信息交互，以及契约的签订，形成信任关系，并可通过制度机制一定程度上制约信任关系破裂	信任仅针对在特定时间点发生的特定事项，并且可能会因为环境等改变而迅速改变，自适应性强

2. 数字信任内涵演变

数字信任的概念伴随着信息技术的发展而提出。在互联网发展的初期，政府、企业和公民个体通过数字身份链入到网络空间中，彼时的数字信任体系建设以网络信任为重点，主要解决网络空间中的数字身份信任问题 ，多用于公民 / 法人身份认证、电子合同、在线支付等网络风险规制。例如，我国（2006）在官方文件中将网络信任体系定义为“以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系 ”。

后来，数字信任的概念被全球广泛引入。数字信任首先广泛应用于商业领域，用以表明在数字时代用户、消费者对企业产品和服务能否按照预期正常执行的信心程度。比如，知名科技公司 TechTarget 指出，数字信任是用户对人类、技术和制度共同创建安全数字世界能力的信心，企业和组织通过向用户表明他们可以确保在线程序或设备的安全性、隐私性、可靠性和数据道德性来获取用户的数字信任。美国网络安全公司 SUBEX 则在研究报告中，将数字信任定义为“一种使用户能够以安全、合乎道德和可靠的方式进行业务交易的概念”。《哈佛商业评论》则引入了行为、态度、环境和经验等四个维度考察用户对不同国家的数字信任程度。

此外，数字信任还被引入网络安全等领域。例如，Gartner 曾提出，数字信任是传统信任模型的演变，其不仅仅是建立企业、人与物之间的信任，其核心还在于在对数据、程序代码和软件开发实践中建立信任，具体包括四个方面：1）个人、企业或其他实体就是其本身，或者与它们所声称的身份一致；2）它们可以代表自己，也可以由另一个实体忠实地代表；3）它们在数字世界互动中能够充分表达自己的

意愿；4)它们以真实、可预测、可靠、安全、合规、符合道德、尊重隐私的方式行动 。普华永道认为，建立数字信任不仅仅是个优选项，更是不可或缺之举，科技企业发展和传统企业数字化转型的关键要点在于要使网络安全规划与业务发展目标相匹配，共同构建数字信任 。腾讯研究院和 IDC 发布的报告提出，传统的 IT 网络安全理念已经无法支撑数字时代的信任关系，必须以安全为基础，重新构建内涵更丰富，外延更广泛的数字信任，并将数字信任分为三层：一是基础层，即风险控制与防范，对应为传统的企业安全控制与防护层，侧重网络信息安全；二是业务层，即安全与合规，是企业开展业务的基本保障也是基本准则；三是战略层，即伦理与社会责任、隐私保护，是企业在数字时代构建可信竞争力的关键 。

随着数字化的浪潮进一步推进，社会风险相较于传统工业社会发生了重大转变。近年来，网络攻击、网络犯罪和黑灰产、数据泄露滥用等事件频发，成为现代数字社会的重要风险。数字信任在数字社会中的作用进一步凸显。由此，本报告认为，**新型数字信任是使一切链入 / 映射到数字空间的网络实体，在以数字身份信任、可信数据流通为两大核心建设的信任支撑体系下，通过制度、管理、技术等一系列组合手段减少数字空间安全风险，并形成数字社会安全交互、高效运行的机制。**具体来看，**从行为主体上看，**以政府、企业及其他组织和公民个体为代表的人类网络实体，和以智能终端 / 设备(包括各种传感器节点)、算法程序(包括各种在线应用)、数据库为代表的机器网络实体共同链接在一个数字空间中；**从关系上看，**政府和企业通过数字化转型形成了高度相关的大规模社会化的协作和分工关系，基于数字技术进行的海量信息流动规模庞大且已经成为人类沟通的主要方式；**从风险上看，**常态化的高能网络攻击、数据泄露滥用等安全风险对人类社会的外溢影响日益深刻，已经上升到国家安全的高度。

二 | 数字信任建设意义

在数字技术发展和数字经济变革的背景下，政府、企业、社会的数字化转型将是一个持续性、整体性发展过程，随之而来的是底层架构逻辑和外部风险环境的变化，数字信任建设将有利推进城市数字化转型。

1. 数字信任是城市数字化转型的新型基座

当前，数字信任在城市数字化转型中发挥的作用持续放大，成为新的“基础设施”。随着新一轮数字化浪潮兴起，以 5G 网络、大数据中心、区块链、工业互联网、物联网、边缘计算、人工智能等为代表的数字基础设施加快推进建设。但这些数字基础设施可能存在普惠性、互操作性、互通性等方面的问题。通过加强数字信任建设，运用技术、经济、法律、行政、自律等多种手段和规则，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”的可信数字交互关系，有效实现不同用户、数字设备、数字系统之间的安全交互，更好保障数字城市感知和运行的平稳安全，加快推动城市数字化转型。

2. 数字信任是数字经济良性发展的关键机制

一方面，数字经济发展必然要求数据要素的便利、高效化流通以及最大化分析利用，但是，数据确权定价不清晰、数据流通来源和链条复杂且难以溯源、数据滥用和泄露风险依然严峻等数据治理和安全问题，使得数据要素在市场化配置上一直举步维艰，加快数字信任在数据流通中的服务支撑，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，极大地支撑数据要素市场发展，推动数字经济发展。另一方面，数字经济发展带来了平台经济业态的快速崛起，也产生了数据垄断、大数据杀熟、算法歧视等各种平台数字治理难题。构建“用户 – 平台 – 企业”之间稳定的数字信任关系网络，能够降低数字经济活动中的营销成本、交易成本、沟通成本和分工成本，避免因信息不对称导致的过度保护行为，减少市场纠纷和不正当竞争行为，推动数字经济进入良性竞争和稳定发展的状态。

3. 数字信任是提升数字生活品质的重要路径

在生活数字化转型上，用户越来越依赖各类数字便民服务和应用，但各类网络安全事件也引发了大众对个人信息保护的隐忧。普华永道的调查显示，近 21% 的消费者表示，他们对于企业及其产品 / 服务在网络安全和数据安全方面的关注，已经超过了对产品 / 服务价格和质量的关注。而数字信任体系可以加快在线生活的创新和应用，消除公民数字化转型的隐私担忧，保障人民更好地分享城市数字化转型发展的红利。例如，数字信任服务能为各种数字应用建立安全可信的数字身份，完善确权、存证、数据安全传输，使得医疗养老、社区物业、交通物流等更多业务场景的全程线上化成为可能，从而实现线上场景可信、数字身份可信、用户意愿表达可信、在线业务可信，赋能更加便捷透明的数字城市生活。

4. 数字信任是数字政府公共治理的底座支撑

在治理数字化转型上，数字信任是解决政府信息化建设割裂和网络安全问题的重要支撑。由于政府部门在信息化建设初期的阶段性和分散性，各国的数字政府建设大多都存在内部系统割裂、技术标准不统一、应用重复建设等共性问题。随着数字化转型深入推进，这些问题不仅导致公共数据共享和开放不畅，城市多源数据难以全面打通，数据的重要价值难以发挥，也使得隐私泄露和城市数据安全形势更加严峻。例如，2020 年疫情期间北京、成都、青岛等多省市在大数据疫情防控期间出现了个人信息严重外泄的事件，引起社会广泛关注。因此，基于统一数字身份认证和管理，聚焦网络安全和数据安全打造新型数字信任体系，将成为各国政府数字化转型的重要政策发力点和有效支撑。

2 PART

当前数字信任面临的问题与挑战

Building new digital trust system with data as the core

PART 2

当前数字信任面临的问题与挑战

一 | 数据安全与网络安全形势严峻

当前，政府、企业和个人都面临着日益严峻的网络安全和数据安全风险。城市数字化转型必须围绕数据安全建立信任体系，构建大安全格局。

1.数据安全事件频发

《IBM2020年数据泄露报告》显示，2019年8月至2020年4月期间经历过数据泄露的企业的平均总成本高达386万美元，52%的事件中涉及到恶意攻击，系统故障和人为失误的比例分别为25%和23%。威瑞森发布的《2021年数据泄露调查报告》基于全球5358起数据泄露事件分析发现，Web应用攻击导致了2020年39%的数据泄露事件，而网络钓鱼攻击比上一年猛增11%，勒索软件增长6%；与此同时，61%的数据泄露与凭证数据有关。可以说，企业因数据安全能力不足导致的数据泄露已经成为阻碍数据要素有序流通的最大障碍。与此同时，个人信息倒卖等数据黑灰产乱象频发，加剧了数据滥用和诈骗等现象的滋生。

2.网络安全边界日益模糊

城市数字化转型将形成由多数据、多技术、多领域、多应用、多终端组成数字复杂巨系统，网络空间的边界将进一步模糊和泛化，而随着越来越多的企业“上云”，企业的安全边界正在逐渐瓦解，传统的基于边界的网络安全架构和解决方案难以适应现代网络基础设施和应用场景。与此同时，外部攻击和内部威胁愈演愈烈，有组织的、武器化的、以数据及业务为攻击目标的高级持续攻击仍然能轻易找到各种漏洞突破企业的边界；内部业务的非授权访问、雇员犯错、有意的数据窃取等内部威胁愈演愈烈。可以说，传统基于信息系统边界构建的防护方式越来越难以应对当下的安全挑战，基于数字身份授权的访问控制和数据安全流通开展的网络安全实践越来越成为共识和趋势。

3.新技术新应用安全风险凸显

一方面，人工智能、区块链等新一代信息技术在发展过程中存在内生安全风险。例如，人工智能技术存在算法黑箱导致算法歧视和决策不公；区块链作为一项新型技术，其本身分布式存储的特性，以及技术发展阶段造成的安全漏洞覆盖率不足、代码扫描和安全测试不足等问题带来的安全风险逐渐显现，近年来监测到攻击区块链网络或节点本身、窃取存储在区块链网络中的数据或资产的事件尤为频繁。另一方面，人脸识别、智能汽车、智慧家居、可穿戴设备等新技术新应用在使用过程中易引发一系列的安全问题。例如，通过假体攻击突破人脸识别盗用他人身份；智能家居产生更多新的漏洞，居家摄像头、手机摄像头、手机APP、WIFI设备等被非法调用；甚至一些接触人体的可穿戴设备受到网络攻击将危及生命健康。

二 | 身份信任体系建设有待完善

1.存在数字身份“孤岛”现象

当前，用户数字身份的数据往往存在于不同部门、不同行业、不同企业中，这些数字身份系统技术和标准互不相通，各个服务提供商或认证机构间互为数据孤岛，且同一个人的数据在不同中心化系统中处于隔离状态，系统之间相互认证的流程复杂，难以进行一致性协同管理，往往需要用户将同一个信息在多场景下重复认证，很难复用已有的认证信息。

2.身份信任仍依托传统认证手段

当前，数字身份较多依托传统的认证手段，即基于指定发行方、平台协议与身份认证的信任模式，通过中心化或机构联盟形式完成数字身份认证。这种方式在成本、便捷程度上较优，且为广大用户所接受，但中心化的电子凭证面临着数据易丢失、可篡改、滥用用户数据等问题。近年来，也出现了一些企业因数据保护措施不当而使得用户数字身份信息处于“裸奔”状态的案例。此外，随着数字化转型的深入推进，大量IoT设备链入所带来的数字身份管理等问题。例如，2020年，某黑客组织在一个流行的黑客论坛上发布了一份涵盖515000多台服务器、家庭路由器和物联网智能设备的远程登录Telnet（一种远程访问协议）凭据列表，内容包含每台设备的IP地址、以及Telnet服务的用户名和密码 。

3.鉴别技术面临新型安全威胁

一方面，数字身份鉴别技术底层算法可能存在“内生”安全隐患，如MD5和SHA-1哈希算法应用于金融、电子商务、电子政务等领域，但已被证明存在安全漏洞；广泛用于保护互联网上数据传输安全的SSL协议也无法避免用户受到各种极具破坏力的中间人攻击(Man-in-the-Middle Attack)。另一方面，不同的应用场景也需要不同的身份鉴别技术，以满足用户在不同应用场景下的易用性及安全性需求，这就形成了对数字身份多维度、多属性的差异化要求，目前存在的数字身份能力无法实现满足上述要求的互联互通。

三 | 高质量数据流通尚未形成

当前，数据流通在统筹机制、规则设计、数据质量和资源释放等方面存在诸多挑战。如果不解决数据流通的信任问题，数据要素市场的流通范围、要素规模、参与主体将大大缩小，无法真正实现数据要素的最优配置，城市数字化转型的脚步也将放慢。

1. 数据流通统筹机制尚待健全

当前，城市数字化转型正处于快速推进阶段，对于如何更好地促进数据流通，相关统筹机制有待进一步完善。以我国为例，国家层面，尚未形成统一的数据流通协调机构。尽管 2016 年国务院同意建立由发改委牵头的促进大数据发展部际联席会议制度，但这难以解决未来构建超大规模数据市场所必须匹配的更加专业、更加精细的统筹决策和落地执行等一系列问题。同时，各部委纷纷加强本行业数据管理，但烟囱林立、条块分割、重复建设等问题较为突出，跨部门、跨系统、跨区域统筹协调难度依然很大。地方层面，党的十八大以来的机构改革中，我国 31 个省级行政区（除港澳台外）中，有 25 个省市或自治区设立了省级大数据管理机构，占比 80.65%；省会城市和计划单列市中，已有 30 个设立了专门的大

数据管理机构；超过 200 多个(地级市、州、盟)设立了大数据管理机构 。由于各地原有部门设置、大数据发展情况不一，省级大数据管理机构属性、隶属关系、组建方式等呈现出差异化发展。

2.数据流通规则设计复杂困难

当前，全球在数据安全流通权利义务、数据产权制度、数据权利义务等一系列制度和规则设计上存在较大分歧，存在着诸多不确定因素和法律风险。这将极大影响数据安全流通，不但影响监管工作的有效实施，而且将导致数字经济发展的不确定性。一方面，数据确权定价在全球范围内均面临难以落地的问题。数据作为一种新型要素，具有非排他性和可复制性，在复杂多渠道的快速流通中形态不断发生变化，且在全生命周期中有不同的实际控制主体，因此其权利体系构成与实物有所差别，其权属难以直接界定为完全属于某个主体。同时，在实践中数据仍然以企业生产经营和用户数字活动的衍生物居多，且目前学界尚未有科学通用的数据价值和成本的计量方法，难以通过市场直接定价。另一方面，数据要素的收益分配争议重重。在当前数据要素确权定价困难的现实情况下，用户、平台、大数据利用公司基于数据形成的商业利益难以量化分配，数据要素贡献能否参与到企业股本结构和资产规模中仍有较大争议，政府部门对数据要素增值如何征税也未有定论。此外，流通中的数据资源需考虑可流通范围、流通对象合法性、流通过程的安全保障、使用授权等一系列安全要求，如何确保数据流通过程的安全、合法，尤其在保护个人信息方面是必须解决的问题 。

3.数据流通实践限制因素突出

从政务数据看，一方面，不同部门信息化建设进程不一，系统建设时间跨度较大，这导致政务数据资源参差不齐，在数据准确性、统一性、完整性等多方面均存在问题，加之标准化治理、质量评价体系等缺失，由此在信息系统集成共用、政务数据统一归集处理、政务数据共享等方面面临较大难度。另一方面，各地对数据开放的数据格式、质量标准、可用性、互操作性等做出规范和要求不同，尤其是在高质量数据集的开放方面存在开放能力不强、水平不高、质量不佳等问题。

从社会数据看，首先，拥有大量数据的企业凭借其行业领先地位，通过构建以开放平台为核心的生态体系，逐渐形成了垄断数据资源的寡头，导致数据大量集聚于垄断性数据平台和公司，而将这些数据主动开放给中小企业在商业活动和市场竞争层面存在悖论。其次，为获得更多数据，存在一些企业利用数据爬虫技术对平台数据的不正当窃取，进一步引发市场不正当竞争现象。最后，由于缺乏相适应的技术标准、规范化的市场环境和成熟的对接平台机制，各机构对数据流通和交换缺乏信任，难以形成内生的数据流通动力。因此在社会数据方面，其数据价值尚未充分释放和变现。

4.数据跨境安全壁垒不断抬升

自2013年“斯诺登事件”以来，各国对数据主权和网络安全的重视程度日益强化，全球范围内的数据保护主义广泛兴起，各国间数据流动信任机制尚未建立，跨境数据流动安全壁垒不断抬高。例如，我国跨境数据流动政策面临极为复杂的决策困境：1）跨境数据流动带来的安全问题日趋复杂泛化，我国数据出境涉及国家安全、商业秘密、用户隐私、产业竞争等多个维度的威胁，对我国跨境数据流动风险监管能力提出极高要求；2）美国等西方国家对我国加大贸易限制和科技脱钩，限制海外各类数据资源流入中国，对我国企业实行“引进来”和“走出去”战略产生重大影响；3）我国跨境数据流动制度体系尚不完善，分散在不同行业部门中的跨境数据流动规定存在过时或是难以协同的问题，影响了我国跨境数据流动工作开展。

3 PART

数字信任建设的国内外发展经验

Building new digital trust system with data as the core

PART 3

数字信任建设的国内外发展经验

近年来，全球加快数字化转型步伐，数字信任被纳入重要议程。《纪念联合国成立 75 周年宣言》呼吁各国通力合作解决数字信任和安全问题。欧盟密集发布了欧洲整体数字化转型的宏观战略报告，高度强调信任和安全在其中的关键作用，并将“信任”明确列入九个愿景关键词之中。国际数字信任相关的政策和数字信任理念相关实践都对我国的数字信任体系建设有重要的借鉴意义。

一 | 加强数字信任领域顶层设计

全球各国和地区高度重视数字信任领域顶层设计和战略引领，密集出台一系列政策法规和标准指南，强化数字身份、数据流通等重点领域立法。

1. 明确数字信任战略要求和方向

在可信数字身份方面，例如，美国出台了《网络空间可信身份国家战略》（National Strategy for Trusted Identities in Cyberspace，NSTIC），旨在构建一个以用户为中心的网络空间可信身份生态系统，促使个人和组织遵循协商一致的标准和流程来鉴别和认证数字身份，从而实现相互信任。NSTIC 明确了可信身份生态体系的四项原则：1）增强隐私且基于公众自愿应用；2）安全、可扩展；3）具备互操作性；4）高效且易于应用。此外，该文件要求纳入基于八项最佳实践的明确规则和指导方针，该文件在附录中对其进行了定义，具体包括透明度、个人参与、目的规范、数据最小化、使用限制、数据质量和完整性、安全性、问责制和审计。欧盟发布《2010 泛欧洲电子身份标识（eID）管理框架路线图》（A Roadmap for a pan-European eIDM Framework by 2010），从欧盟层面统筹规划各成员国电子身份证（eID）实施，要求各成员国要共同建立能在欧盟全境范围适用的 eID 基础设施，使得成员国公民持有电子标识即可在欧盟内的任一国家享受求职、医疗、保险等一系列公共和数字化服务。我国在 2006 年将基于数字身份的“网络信任体系”纳入了《国家中长期科学和技术发展规划纲要》（2006—2020）的重点领域。

在数据流通信任领域，全球将数据视为推动经济增长、创造社会价值、强化国际竞争优势的重要战略资源，出台相关战略性文件以促进数据的流通。例如，美国政府发布《联邦数据战略与 2020 年行动计划》，对数据的关注由技术转向资产，并从三个层面指明了工作重点：1）建立重视数据并促进数据共享使用的文化，如通过数据指导决策、评估公众对联邦政府数据的价值和信任感知、促进各个机构间的数据流通等；2）保护数据，如保护数据完整性、确保流通数据的真实性、确保数据存储的安全性、提高修改数据的透明度等；3）探索有效使用数据的方案，如增强数据管理分析能力、促进数据访问的多样化路径等。欧盟方面，《欧洲数据战略》（A European Strategy for data）明确提出了欧洲“单一数据空间”目标，即建成一个真正的数据单一市场且面向世

界开放，其中个人和非个人数据（包括敏感的业务数据）都是安全的，企业和公民能够以可信的数字身份轻松访问无限的高质量数据，并利用数据创造价值 。我国则高度重视数据要素在推动经济社会质量变革、效率变革、动力变革中的关键作用，遵循“三同步”发展模式：即强调从数字经济、数字社会、数字政府分三步走共同形成功能齐全的数据要素市场，数据安全、数字技术、数据治理等数据保障机制同步跟上。《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出“十四五”期间要激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革，并强调要建立健全数据要素市场规则，统筹数据开发利用、隐私保护、公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范 。

2. 不断完善数字信任政策法规

在可信数字身份领域，例如，美国通过“联邦 – 州”法律明确电子签名的效力，美国联邦层级的《国际与国内商务电子签名法》赋予了电子签名、电子记录与手写签名、印章同等的法律地位，同时允许企业自由地构建自己的安全方法与安全程序以从事电子交易，极大地扫除了使用电子技术制定、签署合同，收集和储存文件以及发送通知的法律障碍；在州级层面，犹他州的《数字签名法》（Digiatl Signature Act），弗吉尼亚州的《电子身份管理法案》（Electronic Identity Management Act）等相继推出。欧盟发布《电子身份认证与签名条例》（EU Regulation on Electronic Identity Authentication and Signature，eIDAS 条例）将电子签名、电子认证以及其他一系列身份服务统一作为信任服务进行规制，目的在于通过实现欧盟层级的各成员国安全、高效的跨境身份认证，促进欧洲区域内可信电子服务和数字经济的流通和发展，实现欧洲“单一数字市场”。我国《网络安全法》第二十四条规定，“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”；《电子签名法》明确了数据电文和电子签名的定义、格式、适用范围和法律效力，并对提供电子签名认证的第三方服务的准入、责任和行为规范做了详细规定；《电子商务法》在第三章对电子合同的订立、履行、效力以及电子支付的相关签名、指令和认证等内容进行了规制；《密码法》第二十九条明确规定“国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理”；《商用密码管理条例》明确提出“国家建立统一的电子认证信任机制，推动电子认证服务互信互认”。

在数据可信流通方面，例如，美国基于公民隐私权和具体行业领域进行数据流通规制，包括《隐私权法》（The Privacy Act）、《电子通信隐私法》（Electronic Communications Privacy Act）、《健康保险流通和责任法》（Health Insurance Portability and Accountability Act）、《儿童在线隐私保护法》（Children's Online Privacy Protection Act）、《多德 – 弗兰克华尔街改革和消费者保护法》（Dodd–Frank Wall Street Reform and Consumer Protection Act）等，近年来生效的州立法《加利福尼亚消费者法》（California Consumer Privacy Ac）引人瞩目。欧盟方面，《通用数据保护条例》（General Data Protection Regulation，GDPR）旨在协调欧盟各成员国的数据安全和隐私法律，建立完备的用户数据权利清单和完备的数据问责体系，并基于此形成了一整套系统的数据安全治理制度。《非个人数据自由流动条例》（Regulation on the Free Flow of Non–personal Data，RFFND）则旨

在消除各成员国的数据本地化要求，促进欧洲形成单一数字市场。此外，欧盟近期提出采用高价值数据集实施法案，使得高价值数据以机器可读的形式、通过标准的应用程序接口（API）在全欧盟层面自由流通。我国《民法典》确立了数据和虚拟财产依法受到保护、公民个人信息和隐私权保护的基本原则，既为数据合法合理的流通和共享留出空间（比如对侵害个人信息免责事由的规定），同时也为后续细化规定数据保护的单行法提供了立法依据；《数据安全法》第七条明确“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展”；《个人信息保护法（草案）》则对个人信息处理原则、处理者义务、数据主体权益做了全面规定，进一步规范了个人数据的可信流通。

3. 制定数字信任系列标准指南

在可信数字身份领域，例如，国际标准化组织ISO 基于风险评估，依据身份可信程度，制定了《实体鉴别框架》（ISO/IEC 29115–2011）和《身份证明规范》（ISO/IEC 29003–2013），前者规定了实体鉴别保证的框架及四个保证等级，为每个级别规定了准则和指南，后者对注册阶段要求进行扩展，为身份证明和验证提供指导。美国方面，美国国家标准与技术研究院（NIST）发布了 SP800–63 系列电子身份指南、个人身份验证（PIV）、NCCOE 身份和访问管理、NIST 生物识别技术、控制策略测试技术和下一代访问控制等系列指南和标准等。其中最有影响力的属 SP800–63 系列指南，其旨在为各电子身份服务机构提供实施风险评估和数字服务的指南。SP 800–63–3A《注册和身份证明要求》中提出了身份保证等级（IAL）的概念，规定了希望获得相应等级身份的用户，在注册阶段身份证明的要求，对应不同身份等级，依赖方（RP）可以提供不同服务；SP 800–63–3B《鉴别和生命周期管理》中提出了验证器保证等级（AAL）的概念，即根据可接受的验证器种类、验证器和验证者要求、重新验证、安全控制、记录的保存以及隐私控制等方面因素满足的不同要求，将 AAL 分成三个等级，等级越高所需要满足的条件越严格；SP 800–63–3C《联合和断言》中描述了在联合环境中，多方交互时，使用断言（用户身份信息的状态说明）来达成多依赖方、多身份提供方（RPs）和多用户之间的协同合作，提出了断言的构建和安全方面的要求，以及联合保证等级（FAL）的概念，并对认证协议、抵御攻击能力、数据传输保护、加密技术等方面做了要求 。欧盟方面，据不完全统计，在 eIDAS 条例框架下发布的数字身份管理相关技术标准已达 120 余项，包括电子签名算法、签名设备、签名生成等基础技术标准，时间戳服务、验证服务等可信服务标准，以及跨境互操作等相关标准 。

在数据可信流通方面，例如，我国发布了《信息安全技术 物联网数据传输安全技术要求》（GB/T 37025—2018）、《信息安全技术 数据交易服务安全要求》（GB/T 37932—2019）、《信息安全技术 政务信息共享 数据安全技术要求》（GB/T 39477—2020）《信息安全技术 大数据安全管理指南》（GB/T 37973—2019）、《信息安全技术 数据安全能力成熟度模型》（GB/T 37988—2019）等系列标准；并推出了医疗、金融等重点领域的标准，为不同场景下的数据可信流通提供操作手册。如在医疗健康领域，《信息安全技术 健康医疗数据安全指南》（GB/T 39725—2020）详细规定了医疗数据的分类体系、使用披露原则、安全措施、安全管理指南、安全技术指南等。日本则发布信息信任认证指南版（information trust certification guidelines），明确了个人信息处理者如何获得同意、数据收集方法、认证资格、信息安全标准、数据治理方法和数据道德审查等；并在近日发布 2.1 版的征求意见稿，强调审查重点是卫生与医疗保健领域的信息处理以及选择向其提供信息的第三方 。

图 1：我国数据安全国家标准体系（TC260 系列）

二 | 深化数字信任体系管理机制

1. 明确数据保护和数据安全责任

近年来，国内外的通行做法是通过岗位设置、人员管理等方式进一步明确数据安全管理要求和责任，以进一步促进数据流通。例如，美国专门设立了首席数据官，要求其负责各联邦机构自身的数据治理和数据共享开放等工作。欧盟 GDPR 指出每个成员国都应建立一个或多个负责监督 GDPR 执行情况的独立政府当局以便保护个人的基本权利与自由，同时要求企业任命数据保护官（DPO），明确其负责企业内部个人信息安全和数据保护制度、组织员工培训、安全审计和合规事务等工作。我国《数据安全法》明确了“重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任”。地方层面，广东试点开展首席数据官制度，其职责侧重于统筹数据管理和融合创新，推进公共数据共享开放和开发利用；领导本行政区域内数据工作，对信息化建设及数据发展和保护工作中的重大事项进行决策；组织制订数据治理工作的中长期发展规划及相关制度规范，推动公共数据与社会数据深度融合和应用场景创新。

2. 加强数字信任领域分级分类管理

在可信数字身份方面，例如，欧盟提出了数字身份保证水平，即数字身份保证级别应表征对数字身份系统建立一个人的身份的信心程度，从而确保声称某个特定身份的人实际上是该身份被分配给该人的人。保证级别取决于数字身份系统在考虑流程（如身份证明和验证以及身份认证）、管理活动（如发布数字身份的实体）的情况下，数字身份声明人声称或主张的身份的置信度 。欧盟 eIDAS 条例对身份保证水平性规定了低、实质性、高（low，substantial，high）3 个等级，以适用不同级别的要求。等级越高，个人身份的可信度就越高。

在数据可信流通方面，例如，我国《数据安全法》第二十一条提出，“国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护”。

3. 推进数字信任互认机制建设

在可信数字身份方面，数字身份跨域互认是打破数字身份碎片化的局面，破除公民和企业使用数字身份跨域访问在线服务的障碍的重要手段。以欧盟为例，欧盟提出至少在公共服务领域中，跨界使用成员国的数字身份进行互认管理，对于互操作性，主要满足：在技术上，应保持技术中立，不歧视其他国家的技术方案；在内容上，应保护个人隐私，保障个人的数据得到适当的处理。美国方面，美国总统管理与预算办公室（OMB）已向各执行部门与机构负责人发布了关于改进政府身份、凭证与访问管理（ICAM）政策的备忘录。该文件指出，必须从单纯管理边界区域的内外访问，逐步转变为利用身份机制建立起联邦政府资源管理体系，从而为用户及信息系统的访问活动管理建立新的风险控制基础。为此，OMB 提出各联邦政府部门都应建立 ICAM 机构，建立符合标准要求的身份运用机制，主要措施包含设立首席信息官和信息安全官、高级机构隐私官以及法律、采购等人员，定义并维护统一的综合性 ICAM 政策、流程与技术解决方案路线图等。并且各级机构应对各类设备、非人实体以及机器人流程自动化、人工智能等自动化技术的数字化生命周期加以管理，从而有效管理并执行 ICAM 相关工作 。

在数据可信流通方面，跨境数据流通规则的互认机制是促进数据要素市场建设的重要一环。例如，欧盟在个人数据跨境方面采用了“充分性认定”机制，即根据第三国的个人信息保护立法状况、执法能力，以及是否存在有效的救济机制等因素，做出综合评估确定数据跨境自由流动白名单国家（目前有安道尔、阿根廷、加拿大、法罗群岛、根西岛、以色列、马恩岛、泽西岛、新西兰、瑞士、乌拉圭、日本），而其他数据保护水平达不到“充分性认定”要求的国家，则必须满足特定条件才能进行跨境流动。

三 | 强化数字信任技术等能力建设

1. 运用零信任等改变安全防护模式

在早期网络终端和用户数量有限的情况下，各国的数字信任体系往往是以网络“边界”为中心建立的，因此多采用终端保护、威胁检测和响应等措施保护网络安全。但是随着网络的扩展、大量终端的加入，以及攻击者持续寻求新的方法来突破边界安全，例如通过社交工程攻击操纵用户以泄露其凭证，导致具有复杂检查规范的防火墙的数量需求增加，在导致成本增加的同时效果却呈递减态势，这种复杂性已经超越了传统的基于边界的网络安全方法，从而导致零信任等技术理念和架构模型的开发，即将防御从静态的、基于网络的边界转向关注用户（数字身份）、资产和资源（数据）。根据美国 NIST 的定义，零信任是指在面向被视为网络入侵的行为时，在信息系统和服务中执行准确、最低特权的请求访问决策，从而将不确定性降至最低。零信任是一种专注于资源保护的网络安全范式，包含组件关系、工作流程规划和访问策略。这种以数据为中心的安全模型，消除了受信任或不受信任的网络、设备、角色或进程的概念，并转变为基于多属性的信任级别，使身份验证和授权策略在最低特权访问概念下得以实现。零信任架构包括数字身份（个人和非个人实体）、凭证、访问管理、运营、终端、托管环境和互连基础设施。

具体来看，在政策界，以美国为代表的发达国家加速从“以网络为中心”的安全防护模式向“以数据为中心”的数字信任转变。例如，美国国防部先后发布《通往零信任安全之路白皮书》《零信任架构建议》《国防部零信任参考架构（DoD ZT RA）》等报告文

件，为国防部大规模采用零信任设定了战略目的、原则、相关标准和其他技术细节，如对网络内的特定应用程序和服务创建离散的、精细的访问规则，旨在增强美国国防部的网络安全并保持美军在数字战场上的信息优势。2021 年 5 月，拜登政府发布行政命令以加强网络安全，明确指示联邦政府各机构实施零信任方法，要求在命令签署之后 60 天内相关机构要制定实施零信任架构的计划，该计划应酌情考虑 NIST 在标准和指南中概述的迁移步骤，并说明已完成的任何此类步骤，确定将对安全产生最直接影响的活动，并包括实施这些活动的时间表 。此外，该行政令还强调：在云服务静态和传输中的多因素身份验证和数据加密；集中和简化对网络安全数据的访问，以加强分析、识别和管理网络安全风险的能力等。在产业界，根据全球权威咨询机构 Forrester 最新发布的报告，企业为寻求更安全的解决方案，零信任网络访问已成为标志性的安全技术，众多安全厂商推出了相关的零信任解决方案和产品。

2. 推进隐私计算技术数据流通应用

隐私计算通常是指在数据全程保密或无接触的情况下，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，以实现数据“可用不可见”。值得注意的是，隐私计算并不是一种单一的技术，它是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系 。目前，隐私计算包括同态加密（Homomorphic Encryption）、安全多方计算（Secure Multi-Party Computation）、差分隐私（Differential Privacy）、联邦学习（Federated Learning）、机密计算（Confidential Computing，CC）、零知识证明（Zero-knowledge Proof）等多种技术方向。产业推进方面，IT 研究与顾问咨询公司 Gartner 发布 2021 年前沿战略科技趋势，其中将隐私计算列为最前沿的九大趋势之一，全球各大科技企业争相投入隐私计算研发和产品化工作。Linux 基金会旗下机密计算联盟在 2020 年迎来壮大期，会员数量猛增六成，成员包括阿里、腾讯、arm、英伟达、谷歌、英特尔、微软、百度、华为等科技企业。我国也成立了由中国信息通信研究院牵头成立的“隐私计算联盟”，该联盟有六十多家成员单位，包括大型互联网公司、金融机构、初创型科技公司等企业。

3. 加强可信数字身份新技术应用

可信数字身份底层技术是密码技术，主流的密码算法有对称加密算法（Symmetrical Encryption）、非对称加密算法（Asymmetric Cryptographic Algorithm）和哈希算法系列（Hash）等。近年来，各国日益重视可信数字身份技术的研发和应用。例如，欧盟在可信数字身份技术配套理论、产品和平台研究方面成效突出，在加密算法、芯片卡、数据公共平台、电子追踪、互操作性等方面进行了大量创新研究和商业产品开发 ，有效强化了数字身份管理；我国《个人信息保护法（草案二次审议稿）》第六十一条第三款指出，要支持研究开发安全、方便的电子身份认证技术。

区块链（Blockchain）、生物特征识别技术（Biometric Identification Technology）等新兴技术加快在数字身份领域应用。其中，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。相较于传统 PKI(Public Key Infrastructure，公钥基础设施 ）体系，区块链具备明显优势：包括身份信息更难篡改，身份信息分布式存储带来安全性和便捷性的提升，减少验证过程中产生的数据泄露风险，以及区块链激励机制的存在能够促使用户积极维护整个区块链，使系统在良性、高稳定性长期运作下的维护成本更低。而生物特征识别技术则是通过数字技术将人类具备唯一性标识的生物特征进行数字化采

集、提取并形成特征模板，并通过与已有数据库或特征模板进行比对来实现数字身份的标识和认证。随着以自然语言识别为代表的人工智能技术发展，生物特征识别在数字身份领域的应用日益广泛，包括指纹识别、声纹识别、虹膜识别、人脸识别、行为识别甚至基因识别等。值得注意的是，生物特征识别技术虽然在识别准确率、应用便捷性上具备密码学不可比拟的优势，但也面临众多安全性的风险，例如用户敏感信息暴露风险等。

四 | 加快场景化最佳实践落地推广

加快数字信任技术方案在不同场景的创新应用，是各国数字信任建设的重要手段。

1. 加快重点领域场景化应用

在电子政务和公共服务领域，例如，美国大力发展基于 PKI 框架的 FICAM（Federal Identity Credential and Access Management）数字身份证方案，集中、统一地给美国政府机关涉密人员发放数字身份证，并以此为基础加强访问控制管理。FICAM 包含五个主要模块，分别是身份管理模块、证书管理模块、访问管理模块、身份联合模块和审计与报告模块。其工作原理是首先由身份管理模块对访问者生成可信数字身份，然后由证书管理模块将数字身份绑定到数字证书上，最后通过访问管理模块和身份联合模块进行证书鉴权实现资源的访问控制 。欧盟则启动了旨在增强欧盟数字单一市场和便利跨境公共服务的 e-SENS 项目，其成功创建了一套通用的泛欧数字公共服务构建模块，e-SENS 的一系列大规模试点（如欧盟内跨境获得卫生服务、跨境电子招标、电子司法服务、使用奥地利和德国的 eID 来访问荷兰的公共在线服务等）为跨境数字公共服务铺平了道路。

在数字金融领域，金融稳定理事会（FSB）在二十国集团（G20）支持下提出建立全球法人识别编码（Legal Entity Identifier，简称 LEI），旨在为参与国际金融交易的法人主体分配唯一编码，以提高金融市场主体信息的透明度，提升金融监管的有效性。截至 2020 年 11 月 30 日，全球 LEI 编码总量 175 万余个。又比如，澳大利亚支付委员会开发了一个有助于支撑便携式数字身份认证的框架。该框架将强化身份认证服务和一系列通用规则之间的互操作性，推进提交、验证、认证和共享数字身份，从而将支付体系从金融服务扩展到零售、政府和电信部门。同时，我国正在探索建立统一数字身份信息系统，通过将指纹、人脸等生物特征信息纳入身份信息采集范畴，为数字金融提供更加可靠的支撑。

在电子商务领域，美国国家网络安全卓越中心（NCCoE）在电子商务方面开展了多因素认证，该项目探讨了一种基于风险场景触发多因素认证（MFA）以减少欺诈性网购的方案。在项目实践中，如果超越某些风险因素（与交易相关的上下文数据），可能表明网购会话中欺诈活动的可能性增加，购买者将被要求出示除了用户名 / 口令之外另一个不同的认证因素 。

在未成年人保护方面，2021 年 6 月，我国发布《国务院未成年人保护工作领导小组关于加强未成年人保护工作的意见》，严格实行网络游戏用户账号实名注册制度，推动建立统一的未成年人网络游戏电子身份认证系统，加强在网络领域对未成年人的保护力度。

此外，美国可信身份战略 NSTIC 开展了数字身份管理项目实践工程，通过 4 批共 22 个试点项目来调动参与各方积极性，涵盖电子政务、医疗保健、智能汽车、金融、儿童教育、航空航天等多个领域。

2. 推进新技术新应用最佳实践

在车联网领域，一方面，车联网数字身份主体呈现海量化、泛在化、多元化的特点，不同主体之间的交互对证书编码格式、传输带宽、交互时延都提出了极高要求。另一方面，车联网中的车辆节点比传统的网络节点面临更多、更复杂的网络攻击，为系统的安全防护和主动防御带来新的挑战。对此，全球加快推进解决车联网领域的数字信任问题。例如，我国工信部发布《关于开展车联网身份认证和安全信任试点工作的通知》，面向车与云服务平台通信场景、车与车直连通信场景、车与路测设施直连通信场景、车与设备通信场景，加快推进车联网网络安全保障能力建设，构建车联网身份认证和安全信任体系 。

在物联网领域，互联网金融身份认证联盟 IFAA 提出了物联网身份认证整体框架，包括物联网设备的可信身份认证和管理，以及对物联网用户的可信身份认证和管理，并分析了物联网身份认证的安全需求，具体包括为物联网设备建立起一套可信设备标识机制；为物联网设备确定一套完善的设备生命周期管理流程；为物联网设备建立一套可信的设备入网注册流程，其中设备传输、接收的数据类型也应该被考虑在注册流程的构建当中；为物联网设备中产生或者流转的数据流建立可靠的安全保障措施；为管理员直接管理本地设备构建一套完善的验证和授权过程；针对不同类型的数据构建不同的安全保障措施，尤其是具备完善措施确保个人隐私数据的安全；定义不同用户角色或者属性，并基于角色或属性实现相应的访问控制；可结合大数据风险控制机制，确定具体的身份认证策略等。

在区块链领域，目前，不少企业已进行了分布式数字身份 (Decentralized ID) 产品试验。比如区块链企业 ShoCard 与航空服务商 SITA 合作开发了 SITA Digital Traveler Identity App 的身份认证应用，该应用融合了基于区块链的数据和面部识别技术，致力于简化航空公司乘客身份验证流程，以及实现机场实时数据流；微软与 Blockstack Labs、ConsenSys 合作，推出了基于区块链技术的身份识别系统，实现人、产品、应用和服务的深度交互；IBM 与法国国民互助信贷银行(CréditMutuelArkéa) 合作完成了一个基于区块链技术的身份认证系统，该系统采用超级账本区块链框架 (Hyperledger) 引导客户向第三方 (比如本地公共部门或零售商) 提供身份证明；ID2020 联盟与国际救援委员会合作为难民提供安全的加密数字身份，帮助他们认证身份，获得医疗服务。

4 PART

构建城市数字化转型数字信任体系对策建议

Building new digital trust system with data as the core

PART 4

构建城市数字化转型数字信任体系对策建议

一 | 总体思路

随着城市数字化转型加快推进发展，以 5G、物联网等为代表的新型数字基础设施的大规模普及，城市运行的每一分钟都将产生大量的数据，数据资源在链接服务国内大循环和国内国际双循环中的引领型、功能型、关键型要素地位不断突出，数据驱动经济、生活、治理等各领域数字化转型，但同时也带来了新型网络安全风险。一是随着新型数字基础设施加快部署，针对物联网和身联网的网络攻击对城市和公众的威胁更加直接且难以防御。尤其是城市物联感知设备爆发式增长，海量的物联和网联相互链接但又缺乏必要安全能力，网络攻击将直接从最微小的物联设备传导到整个城市关键运行系统。二是在数据生产、聚合、占有、使用等过程中的权属界定困难，数据交易商业模式难以持续，并可能引发不正当竞争、侵犯个人隐私等风险。三是智能应用层叠发展，安全和伦理问题不断凸显。随着人工智能等新

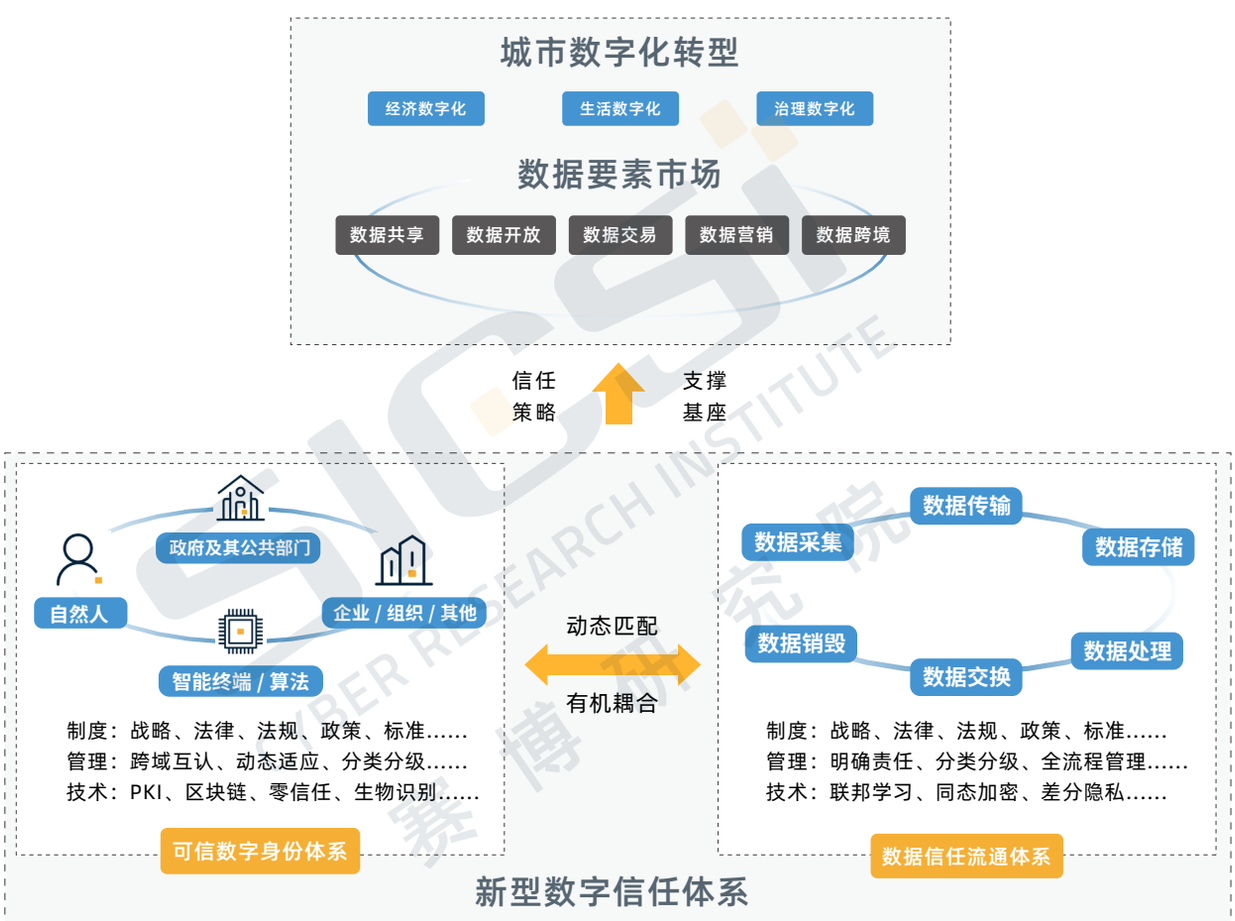

图 2：城市数字化转型数字信任体系框架

技术在经济、生活和治理中的广泛应用，生物识别、算法歧视等正在引发更为广泛的社会伦理关切。可见，在新的形势下，信任关系产生和维系的社会情境发生了根本性变化，仅依靠传统的、基于系统防护和固定边界构建的信任机制无法满足城市数字化转型要求。

因此，必须以数据为核心，构建与城市数字化转型相适应的新型数字信任体系框架（如图 2 所示）。该框架聚焦“制度 + 管理 + 技术”的数字身份和数据流通两大信任体系建设，根据场景需求确认所需的数字主体身份属性，并形成与可信数字身份体系相适应的制度、管理与技术手段以保障数据全生命周期的可信流动，由此形成动态匹配、有机耦合的信任策略，支撑数据要素市场构建，促进经济数字化、生活数字化、治理数字化等城市数字化转型。

二 | 基本要求

1. “制度 + 管理 + 技术”贯穿数字信任建设全过程

从国内外的实践看，数字信任要实现可信数字身份和可信数据流通，都离不开数字信任制度规则、数字信任管理机制、数字信任技术的整体支撑。一方面，以战略、法律、法规、政策、标准为核心的制度规则为数字信任的建设指明方向和要求；而管理理念和管理机制的构建则要与制度规则相适应，实现弹性的“软着陆”；技术则是数字信任实现的重要保障。另一方面，数字信任建设不能“唯技术论”，以数据可信流通为例，其不仅仅是一个纯技术层面的跃升，而且是涉及政治、经济、法治、社会和文化等诸多方面的因素，而不能“为流通而流通”。

2. 可信数字身份构建应基于场景需求智能匹配相关属性

人是一切社会关系的总和。在传统社会，建立信任的身份主体是实体的人或组织，大多数时候“人的面孔就是身份证件”，信任关系往往是比较持久的。而在数字社会，数字身份则由多个不同的信息碎片组成，具有多维属性。以数字身份的特性分类，可包括法律身份、生物身份、组织身份、社会属性身份等。以身份背后的主体分类，存在人的数字身份、组织的数字身份以及物的数字身份。例如，从人在数字空间中身份特征看，其具有生物性质（如人脸）、法律特征（如身份证号码）、电子特征（如邮箱账号）、行为特征（如购买爱好）等；组织的身份特征至少包括法律特征（如法人）、电子特征（如法人证书）和行为特征（如组织电子合约）；而物的数字身份特征则包括电子特征、行为特征等。同时，各个身份主体之间的关系，例如人在各种社会关系下所隶属的组织单元，人或组织与物的权属关系，也是身份属性的一部分。由此，在城市数字化转型下，应先形成每个数字主体多维一体、自主可控的数字身份集合，可称之为“数字身份钱包”，并形成多类主体间的智能身份画像。复杂多元的数字主体之间建立信任关系一方面不再需要通过传统的实名方式进行展示，无需全部验证所有的身份属性，而是依托技术智能匹配相应所需信息，经过身份主体授权后在数字钱包中灵活取用对应的身份属性，以确保数字主体高效、安全交互；另一方面，这种信任关系的建立可能是瞬时的，且会根据场景的变化进行适时调整，需要确保数字身份的某一属性在特定场景中受到信任。

3. 数据流通信任体系的构建需与可信数字身份体系有机耦合

数字信任的目的是保障城市数字化转型下各类经济和社会活动的安全交互和高效运转，这离不开数字身份和数据流通两大信任体系的建设。一方面，城市数字化转型下，物联网、人工智能等信息技术快速发展，以智能终端 / 设备（包括各种传感器节点）、算法程序（包括各种在线应用）和数据为代表的机器网络实体爆发式增长，各类复杂多元的数字身份成为交互的原点。可以说，若没有数字身份，数字社会中正常的生产生活无法进行；若数字身份不可信，社会交往和主体交互的成本将大大提高。另一方面，数字空间中发生的所有行为都以数据为载体，表现为各种场景、各类规则下的数据交互。在这个过程中，首先需要确认交互的数字主体身份，之后则明确与可信数字身份体系相匹配的数据流通体系。一般地，数字身份之间的信任度越高，数据流通“畅通程度”则越高，数据流通所需要的相对成本则相对较低；而数字身份之间的信任度越低，对数据流通的机制建设、管理手段、技术支撑和保障能力的要求就越高，其相对成本则越高。由此，基于数据流通信任体系和可信数字身份体系这两大体系动态匹配、有机耦合的组合关系，将形成不同的信任策略，支撑城市数字化转型。

4. 数字信任实践需具备与技术、场景敏捷适应的能力

相较于传统信任关系对于社会制度、经验知识和个体情感等因素的依赖，数字信任的构建更强调技术。一方面，数字信任的构建极大依赖于大数据安全、密码学、隐私计算等安全技术的创新发展。另一方面，以人工智能、物联网、区块链和量子计算等为代表的数字技术仍在不断创新发展的进程中，将会重塑未来数字空间的规则和风险，因此数字信任体系必须确保对新兴数字发展的兼容性和敏捷性。同时，数字信任也是高度场景化的关系，数字时代的交互关系类型既包括传统的人与人、人与组织之间的关系，也包括人与物联设备、人与机器算法的交互。不同场景下的交互关系和规则差异性极大，因此高度场景化的数字信任并不具备通用的传导性，需要特殊的“信任通道”机制来实现数字信任的跨域传递。

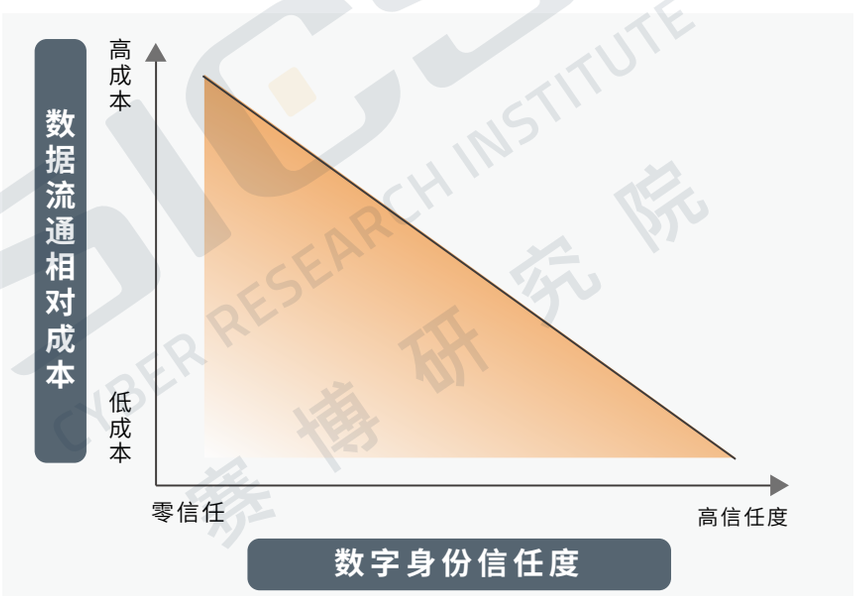

图 3: 数字身份信任度与数据流通相对成本的关系

三 | 实现路径

针对城市数字化转型需求，数字信任建设可开展“三步走”的路径策略。

第一步，做好数字信任体系顶层设计，明确体系框架。即在城市数字化转型的大背景下，以数据为核心，进行数字信任体系的总体规划，构建数字信任体系被期待或应当实现的功能和未来愿景，聚焦可信数字身份和可信数据流通两大领域，聚焦新型网络安全风险和数字治理难题，通过制度规则、管理机制、技术创新等多维度建设，实现新型数字信任治理模式。

第二步，开展数字信任重点场景试点，形成最佳实践。基于城市数字化转型数字基础设施建设、数据要素市场构建等重大战略布局，聚焦数字信任在支撑城市数字化转型中的关键作用，形成底层的技术解决方案和最佳实践。例如，在数据交易流通场景下，搭建“数据要素可信交易平台”，其功能模块具体包括：1）数据要素资源登记管理，即通过区块链、数据标识、数据溯源等技术，形成数据要素来源审核、数据要素线上登记、数据要素全链条确权等核心功能，形成统一、规范、合法、可信的数据要素资源标的；2）数据要素多方交易磋商平台，即构建数据交易多方主体的数字身份识别和认证服务，通过区块链、隐私计算等技术，确保买方对数据价值的可信查验，以及卖方对数据安全保障和防止数据泄露的要求，确保在线的报价、询价、竞价、定价和挂牌机制符合相关规定并具有法律效力；3）数据要素流通交易服务，即提供数据安全能力认证服务，确保数据买方的数据安全和隐私合规能力与其购买额度挂钩，并引入数据担保、数据中介、数据资产质押融资、数据资产保险等服务，打造提供数据确权、数据估值、数据清洗、法律咨询、市场分析、尽职调查、安全审计等服务的第三方支撑生态。

第三步，进一步完善数字信任体系，服务整体数字化转型。选取经济、生活、治理各领域数字化转型中的场景，强化整体转型服务支撑。例如，在数字经济方面，开放在线办公、在线贸易、在线金融、数据交易等场景，通过国产密码技术、隐私计算，以及大数据、云计算、区块链等新一代信息化技术，为数据要素市场提供一个安全环境。在数字生活方面，开放医疗养老、社区物业、交通物流等业务场景，试点安全可信的数字身份建设，实现线上场景可信、数字身份可信、用户意愿表达可信、在线业务可信，完善确权、存证、数据安全传输。在数字治理方面，试点公共数据共享开放和数据治理，通过开放统一的数字身份基础设施，着力实现对碎片化公共数据的整合统管，让公共数据资源有序流动，促进公共数据开放，进一步深化“两网”建设；在个人信息保护上根据设备身份标识配置合理的数据权限，规范如摄像头、闸机、移动终端等智能设备对个人信息的收集和处理行为。

四 | 重点任务

1. 加快推进数字信任制度规则

完善《网络安全法》《数据安全法》的配套支撑措施，加快推动《个人信息保护法》的正式出台。通过数据立法，加快推进数据确权，明确数据权属，厘清相关方的法定权利和义务。建立健全数据交易规则和交易风险防范处置规则，对数据交易中介服务机构、数据交易信息披露、监督审计等做出相关规定。研究制定可信数字身份战略和管理办法，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“人机物”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、指导意见或标准规范，为各主体建立数字

信任关系提供体系完备的治理规则。

2. 建立健全数字信任管理机制

一方面，加快构建数字身份信任管理体系。加快从边界管理转向以数据为中心、以身份管理为基础的新型安全风险体系；针对数字身份“孤岛”和数字身份碎片化的问题，推进数字身份跨域互认；以信任度量为指引，探索基于风险的风控指标、身份属性（生物特征、用户行为）、场景分类的身份认证，构建自适应的可信数字身份管理体系。另一方面，完善数据可信流通管理机制。设立数据安全部门或责任人，明确组织内部数据安全和个人信息保护的责任清单，加强协同分工；实施数据分类分级保护，通过开展备案、建立清单等机制落实重点领域保护要求；鼓励利用可视化工具等加强对数据资源管理与利用。强化数据全流程管理，建立安全测评、审计、监测预警、应急处置等管理机制。

3. 前瞻部署数字信任技术方向

聚焦数字技术的前沿应用方向，加快新兴技术在数字信任方向的融合创新应用。结合区块链技术，加快推动区块链与电子认证技术的融合发展，打造新一代分布式智能化可信身份技术体系。借助人工智能技术，加快生物特征识别在数字身份领域的应用。提升基于风险控制的多因素身份鉴别系统安全能力，探讨共享共用的身份管理服务业态，研究多模式多安全等级的电子认证新技术等。围绕隐私计算方向，重点关注同态加密、零知识证明、联邦学习等方向，探索数据共享、数据流动和数据交易中数字信任关系构建。根据零信任安全架构，关注企业、组织在零信任架构改造进程中对于身份访问控制的需求，探索构建零信任环境的数字信任交互架构。围绕 PKI 及密码学，加快密码算法、商业密码应用的技术攻关，密切关注量子计算、量子加密的技术演进动态。

图 4：城市数字化转型数字信任服务中台

4. 推进建设数字信任基础设施

一方面，加快建设综合型数字信任设施平台。例如，可探索建立数字信任服务中台（如图 4 所示），该平台兼具可信数字身份和数据流通信任模块功能，赋能城市数字化转型。在数字身份模块，身份的可信不再依赖内网边界，随着改变的是身份认证和授权从静态走向动态，身份信任需基于风险控制、场景变化、业务资源价值等开展实时评估和调整。在数据流通模块，数据安全从点到点的传输安全转向数据全生命周期的流通安全，利用区块链、数字标识、数据溯源、隐私计算等技术开展数据确权、数据开放、数据交易等活动成为趋势。另一方面，面向重点领域建设平台型基础设施。例如，聚焦电子政务服务领域，搭建全市数字身份统一认证平台，重点围绕在线教育和在线医疗等数字化民生服务领域，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。聚焦工业互联网领域，探索基于区块链的分布式工业设备识别框架，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。

5. 全面促进数字信任生态繁荣

一是加强数字信任体系研究。一方面，加快数据、网络安全、人工智能、区块链等学科建设，加快数字信任前沿技术攻关，打造融合治理信任、技术信任、隐私保护的数字身份工具箱，促进区块链与电子认证融合发展，研究数据流动、共享和交易中关键技术。另一方面，鼓励联合高校、研究机构、企业等，设立新一代密码应用实验室、数据可信流通实验室等，形成创新成果指导产业实践。

二是培育壮大数字信任产业集群。通过建立行业性组织，充分打通软硬件提供商、电子认证第三方服务机构、网络安全厂商、安全合规律所、网络安全保险和咨询企业，形成综合性的数字信任第三方支撑服务能力。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方面，征集遴选一批掌握关键技术、具备创新能力和应用推广能力的机构开展应用示范工作，在金融、政务、司法、工业等领域培育一批解决方案和应用新模式，为数字信任服务协同发展树立标杆和方向。

三是构建区域 / 国际的数字信任生态。依托长三角、粤港澳等国家区域一体化战略，打破我国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”的分散局面。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。在“一带一路”倡议、区域全面经济伙伴关系协定（RCEP）等框架下，加强与主要贸易伙伴的数字信任交流合作，实现跨域数字身份、跨境数字签署、数据跨境流通规则的互通互认。

APPENDIX 附 录

一 | 当前数字信任技术发展现状

1. 隐私计算

在当下的安全实践中，隐私计算包括同态加密（Homomorphic Encryption，FHE）、安全多方计算（Secure Multi-Party Computation，sMPC）、差分隐私（Differential Privacy）、联邦学习（Federated Learning）、零知识证明（Zero-knowledge Proof）、群体学习（Swarm Learning，SL）等多种技术方向。从技术层面而言，隐私计算实现的数据保护功能与国内外数据保护相关立法精神高度契合，但限于成本、技术成熟度等原因，隐私计算的推广应用仍具有较大提升空间。一方面，隐私计算虽然已经开始在不同行业初步应用，但是受限于计算复杂度、多方交互效率、模型性能等问题，大部分的应用场景均聚焦于少量数据的支持，对海量数据场景的支持能力还有待提升。另一方面，隐私计算参与各方权利义务的边界有待进一步明确，隐私计算涉及多方主体，包括个人信息主体、数据持有方、计算方、结果方，各方之间的法律关系尚未厘清，数据收集处理的商业合作将处于不合理的高风险状态 。

表 2：隐私计算的主要技术路线

技术路线	核心原理	存在不足
同态加密	通过加密算法设计，确保对加密数据计算后的加密结果与明文计算结果一致，并向合作双方输出加密结果	全同态加密的消耗计算成本较高；技术研发难度高；验证速度慢，大规模落地可行性较差
安全多方计算	在无可信第三方的情况下，通过计算协议和约定函数的设计，确保双方分别输入原始数据得到共同的正确计算结果	难以确保参与方的诚实性，当恶意参与方超过一定比例时无法得出正确结果；系统协调和验证效率较低；还受到网络带宽、延迟等因素制约
联邦学习	本地进行 AI 模型训练，仅将模型更新的部分加密上传到数据交换区域，并与其他各方数据进行整合。其技术特点包括：1）数据隔离；2）模型质量无损；3）地位对等；4）共同获益	难以保证模型更新过程中的零信息泄露；不能识别参与者对联合模型产生影响时的异常，模型投毒脆弱性凸显；性能受到网络带宽、延迟等因素制约

技术路线	核心原理	存在不足
差分隐私	通过对数据添加干扰噪声的方式保护数据中的隐私信息。理想情况下，经过训练的机器学习模型的参数代表的应该是一般模式，而不是关于特定训练示例的事实。	在人脸识别、风险识别等情况下，由于添加了噪声，差分隐私技术可能会导致精度受到影响
零知识证明	通过算法逻辑设计，确保证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信特定验证目标的准确性	技术还未成熟，且其需要依靠双方的多次交互来进行，验证速度慢，可扩展性差，效率较低下
可信执行环境	包括可信硬件（TEE）和可信计算协议（TCP），通过划分内存区域等硬件手段构造计算沙盒，提供整体的可信保密计算环境	过于依赖硬件厂商（Intel 的 SGX 和 AMD 的 PSP）
不可区分性混淆	将数据和代码混淆成无法理解的形式，但保留原有功能和可计算性	尚未有实用性研究
群体学习	去中心化的学习系统，具有以下优势：1）将大量数据保存至数据所有者本地；2）不需要交换原始数据；3）提供高级别的数据安全保障；4）能够保证网络中成员的安全、透明和公平加入，不再需要中央托管员；5）可以保护机器学习模型免受攻击	目前处于探索阶段，仅在医疗数据等领域有所研究

2. 零信任关键技术

零信任（Zero Trust）的最早雏形源于 2004 年成立的耶利哥论坛（Jericho Forum），其核心理念是为了应对信息系统边界日益模糊趋势下的网络安全问题。零信任的思想框架，即默认情况下企业内外部的任何人、事、物均不可信，应在授权前对任何试图接入网络和访问网络资源的人、事、物进行验证，其内涵包括：将数字身份作为访问控制的基础；最小权限原则；实时计算访问控制策略；资源受控安全访问；基于多源数据进行信任等级持续评估 。事实上，零信任是一个演进式的框架，而不是革命性的方法。它建立在现有的安全概念之上，并没有引入一种全新的网络安全方法。当前，零信任日趋成为当下网络安全防护的重要模型，全球产业界围绕零信任纷纷布局。微软、谷歌、Cisco、Symantec 等在内的国际巨头均已进军此领域，华为、奇安信等国内众多安全厂商也纷纷推出自己的零信任方案。虽然零信任已在远程办工、云平台防护、物联网应用、5G 应用等领域有所应用，但零信任依赖于对组织的服务、数据、用户、端点的基本理解，策略定义、部署概念、信任确定（和衰退）、执行机制、日志聚合等，都需要在部署解决方案之前考虑 ，具有一定的复杂性，

且成本较高，当前相关产品和解决方案尚处于起步阶段。

● **数字身份与访问控制技术。**身份管理是大多数组织实现安全和 IT 运营策略的核心。数字身份与访问控制技术（Identity Access Management，IAM）使企业可以自动访问越来越多的技术资产，同时管理潜在的安全和合规风险，为所有用户、应用程序和数据启用并保护数字身份。IAM 可以帮助组织有效地解决复杂业务带来的挑战，并平衡四个关键目标：1）加强安全性并降低风险；2）改善合规性和审计绩效；3）提供快速，有效的业务访问；4）降低运营成本。

● **软件定义边界技术。**随着移动互联网和云计算的发展，软件定义边界（Software Defined Perimeter，SDP）的趋势成为现实。SDP 技术具有网络隐身、预验证、预授权、应用级的访问准入、扩展性等特点，对数字身份进行认证和访问控制，为企业应用和服务提供“隐身”服务保护。SDP 的安全优势包括：1）SDP 最小化攻击面降低安全风险；2）SDP 通过分离访问控制和数据信道，保护关键资产和基础架构，从而阻止潜在的基于网络的攻击；3）SDP 提供了整个集成的安全体系结构，这一体系结构是现有的安全设备难以实现的；4）SDP 提供了基于连接的安全架构，而不是基于 IP 的替代方案。5）SDP 允许预先审查控制所有连接，从哪些设备、哪些服务、哪些设施可以进行连接，所以它整个的安全性方面比传统的架构更有优势。

● **微隔离技术。**微隔离技术（Micro-Segmentation，MSG）是一种在数据中心和云部署中创建安全区域的方法，将数据中心在逻辑上划分为各个工作负载级别的不同安全段，然后定义安全控制并为每个唯一段提供服务，大大增强企业抵御网络攻击的能力。微隔离使 IT 人员可以使用网络虚拟化技术在数据中心内部部署灵活的安全策略，而不必安装多个物理防火墙。此外，微隔离可用于保护每个虚拟机（VM）在具有策略驱动的应用程序级安全控制的企业网络中。微隔离技术具有以下优势：1）减少攻击面；2）改善横向运动的安全性；3）安全关键应用等。

3.PKI 架构及密码学

目前，各国通行的数字身份标识、鉴别、认证和授权以及数字签名的应用中，核心的底层技术都基于密码学。自上世纪 70 年代开始，欧美等国就率先开始密码技术的研究与应用，取得了大量先进成果，有利支撑了数字身份验证应用的发展，其中主流的密码算法有三大类：对称加密算法（Symmetrical Encryption）、非对称加密算法（Asymmetric Cryptographic Algorithm）和哈希算法系列（Hash）。

● **对称加密算法：**对称加密算法即采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。同一个密钥使得对称加密具备使用较为简单，加解密迅速的优势，但存在密钥分发和保管的安全性问题，因此这类算法通常运用于一般大规模数据加密传输的场景。目前，对称加密算法主要包括 DES、3DES、TDEA、Blowfish 和 AES 等算法模型。IBM 公司在上世纪 70 年代首先提出 DES 算法，该算法成为之后的美国 FIPS-46 标准。但 DES 算法自推出以来，其安全性一直广受质疑，20 世纪末不断有研究机构成功攻破 DES 算法。随后，美国 NIST 开始征集开发 AES 算法，欧洲也开始启动 NESSIE 工程，最后确定 AES 算法可根据所需安全强度设定密钥长度为 128/192/256 位。鉴于 AES 算法具有加解密运算速度极快的优点，该算法成为使用最为广泛的对称密码算法。

● **非对称加密算法：**非对称加密算法是采用双钥密码系统的加密方法，公钥用于加密而用户的私钥用于解密，也可以用私钥生成数字签名，用公钥

验证数字签名。由于非对称加密算法使得用户最终不需要相互交换秘钥，且现有计算能力从公钥推导出私钥十分困难，因此实现了更高的安全性，但非对称加密算法的算法强度复杂，因此在成本和效率上需要做出平衡。目前，全球大部分数字签名、可信通信与加密信息传输均是通过基于非对称加密的 PKI（Public Key Infrastructure，即“公钥基础设施”）架构实现。美国在 1978 年首次提出基于大整数素因子分解的 RSA 算法，1985 年又提出了基于离散对数问题的 ELGamal 算法，其中 RSA 算法目前应用较为广泛。RSA 算法的强度与其算法密钥长度有关，RSA1024 已经在 2012 年被美国密码学家攻破，目前最新版本为 RSA4096。由于过长的 RSA 密钥会导致运算效率大大下降，美国 NIST 和欧洲 NESSIE 的专家又提出了椭圆曲线和超椭圆曲线密码 ECC，该算法只需 282bit 的密钥长度即可媲美 RSA4096 的加密强度，运算效率大大提高，是目前非对称密码技术研究的热点。

● **哈希算法：**哈希算法又称为杂凑算法或摘要算法，即能够将任意长度的数据压缩成固定长度的标识，能够赋予每个数据基本唯一的“数字指纹”。对称 / 非对称加密算法主要解决的是防止数据被窃取的问题，而哈希算法主要用于证明数据信息的完整性，即防止数据被篡改，广泛应用于数字签名、数据质量治理和数据安全保护领域。哈希算法的典型代表是美国 NIST 发布的 SHA 系列，1995 年 SHA–1 正式发布，经过二十余年的发展 SHA–1 算法逐渐成为互联网最基础的数字签名算法。由于 SHA 家族算法本身的问题存在“碰撞”破解的可能性，SHA 算法被攻破的时间仅依赖于所使用的计算能力，所以，欧美密码学家不断调整改进 SHA 算法，继 SHA–1 后推出 SHA–224、SHA–256、SHA–384 和 SHA–512。

4. 区块链

区块链的核心原理是通过在互联网上建立一个点对点的公共账本，由区块链网络的参与者按照共识算法规则共同添加、核验、认定账本数据。数据同步后，网络中每个参与者都拥有一个内容相同的独立账本，且账本数据是公开透明的。目前区块链应用主要有三种模式：1) 公有链是运行在互联网的完全分布式区块链；2）联盟链则是由多个关联机构共同发起和运营，带有准入机制；3）私有链是公有链的私有化部署，往往由单个机构主持运行。由于区块链具备中心化、开放性、自治性、不可篡改性、匿名性等诸多优势，目前已成为数字身份最具研究热度的技术方向之一。但区块链分布式账本的共识替代了原本的集中式认证，本身会导致一定的效率低下。同时在区块链上验证身份时，用遍历区块链的方法查询身份—公钥对，从而验证某公钥是否属于通信对方，这是目前常用的方法，但是会随着区块链账本体积的不断增大而效率更低。此外，分布式身份标识符 DID 为了保证分布式和安全性，牺牲了其可用性，标识符的文本通常复杂难记。同时，用户如果为了进一步提高隐私安全，可以使用一个人对应多 DID 的方式，每个身份信息（如身份证、电话、驾驶证）等都对应一个 DID，那么其管理将加倍困难。这并不符合普通互联网用户的习惯，使用门槛较高，使得人们对这种方式的接受度降低 。

● **分布式身份认证。**针对 CA 的中心化签发所引发如中心失效、网络安全等问题，可以运用区块链技术实现分布式的数字证书签发，让以往由集中式 CA 认证中心签发数字证书可以由区块链的分布式账本实现。一种方式是形成 CA 之间的区块链，使得 CA 之间不必相互信任，以共识的方式完成数字证书的签发和管理。第二种方式，区块链的记账和维护可以由系统中的所有证书持有者来共同完成。基于区块链的 PKI 可以实现传统 PKI 系统的证书申请、

签发、验证和管理。

● **跨机构安全身份授权。**目前数字身份数据分散，难以共享，传统的身份授权方式不够安全。在统一身份标识无法快速实现和成熟的背景下，可以利用区块链的分布式账本让身份共享和授权更加安全，其核心思想是通过联盟链的形式来彼此鉴权和认可对方的登录请求，并授权访问对应的用户数据，形成可信安全的身份信息互通体系。

● **分布式身份标识。**身份标识 DID（分布式身份标识）具有高可用性、可解析性和加密可验证性。目前相对有影响力的 DID 标准主要包括 W3C 提出的 DID 标准，以及 DIF（Decentralized Identity Foundation）的 DID Auth。以 W3C 的 DID 标准为例，DID 系统主要包括了基础层的 DID 标识符、DID 文档，以及应用层的可验证声明（VC）：1）DID 标识符是全局唯一的身份标识，类似一个人的身份证、账号等。DID 标识符很长，不容易记忆；2）DID 文档至少包含三部分，即证明目的、验证方法和服务端点；3）可验证声明（VC），DID 文档本身无法和用户的真实身份信息相关联，需要 VC 来实现，是整个系统的价值所在。VC 类似数字证书，是对用户身份的证明。此外，DID 本身只是一种身份标识，其无需根植于某个区块链，只要接受这一身份标识格式，DID 可以移植到各个区块链中，完成跨链单一的身份，相比于传统的区块链地址有更强的便利性和可用性。

二 | 重点领域实践案例及技术解决方案

1. 电子政务：政务数据可信共享交换平台

随着治理数字化转型的深入推进，各地大力实施大数据战略性文件，加快推进政务数据共享开放及社会大数据等多元数据融合，持续推进“一网通办”平台建设，提升政府整体智治能力。电子政务建设应以数字身份、电子签名为核心，通过区块链、生物特征识别等技术，实现数字身份的多渠道、多终端的无密码认证和鉴证证明，提供PC端、移动端等多种接口；同时，通过区块链、隐私计算技术，实现后台数据的匿名化访问、加密共享传输和隐私保护，旨在实现群众办事的多次认证、隐私保护、数据安全传输等问题。以政府数据共享的场景为例，当前各部门内部系统孤岛多，数据难以集中；碎片化、数据标准不统一的质量问题较为普遍；数据分析以简单数据聚合为主，缺少行业数据模型积累，难以支撑政府应用创新。对此，可构建政务数据可信共享交换平台，功能模块包括：1）开展数据确权。为共享交换目录链确立数据家底，对政府数据盘底造册，把部门三定方案“定编”“定岗”“定责”升级为四定，即增加“定数”来确定数据采集权。2）促进系统整合共享。目录链在确立一套家底后，与建设资金发放挂钩，可以有效清理未使用信息系统，同类同质信息系统整合。3）创新共享模式。目录链将共享机制、管理制度下沉到部门处室，打破大集中协议模式，提高各部门数据共享的意愿，真正实现政府数据共享交换的自组织模式，即以区块链为主的交易模式。

2. 数字医疗：医疗健康可信身份认证平台

随着医疗健康行业的数字化转型，各类在线医疗App和应用蓬勃发展，由于医疗健康行业中患者疾患信息、医院诊疗信息、电子病历、电子健康档案、疫情信息等数据会涉及大量个人敏感信息，数据仿冒、篡改、泄露和滥用的风险日益加剧，并由此产生了患者个人权益侵害、互联网医疗的医生资格身份审核、电子处方效力确认、医患纠纷责任溯源、社区药柜的管理等各种现实问题，对医疗健康

行业的数字化转型带来了严峻威胁和挑战。医疗健康的数字信任解决方案以“统一可信身份认证+数据全流程安全保护”为核心，通过数字技术解决在线医疗诊断主体的身份核实和医疗数据的完整性、机密性问题的同时，加强对医疗数据的开发和利用。

例如，随着临床诊疗模式的变化、生信科技发展的突破以及计算机科学的进步，多方参与的医学科研协作在数据、安全、伦理、隐私及科研成果保护等方面面临着新挑战。例如，单个医疗机构的数据样本不足以支撑大规模的模型训练，传统的做法是将病例数据汇总、统计、销毁，这种操作是极其不安全的。为了解决这个问题，医疗行业开始采用基于隐私计算的数据合作方案。即多个医疗机构在不需要共享原始数据的情况下就可以进行联合建模和联合数据分析，有效推动了医疗领域的大数据应用。在疾病检查方面，多家医疗机构可以通过横向联邦学习联合构建目标检测模型，用于辅助通过医疗图像的疾病检查（如肺部X光片检查等）。基于横向联邦学习的解决方案在各医疗机构的数据不出域的前提下，利用多家医疗机构的数据联合训练一个目标检测模型，使得有效训练数据显著增加，多方联邦训练的模型的性能比单个医疗机构训练的模型的性能提升30%以上。

3. 智慧教育：可信教育数字身份平台

当前，在教育领域，面向“学籍、学历、证照、档案、考试、录取、资助、转学、版权”等实际应用，亟需实现跨部门、跨业务、跨区域的应用共享。过去没有统一可信的教育数字身份，大大增加了业务应用链的服务成本：首先，同一用户在不同的业务下，呈现多种账户及密码，管理难度大；其次，业务平台或用户需要承担更多的发放用户证书的经济成本，造成重复投资；三是不利于开展业务数据跨链共享，实现跨链共享首先要解决不同链的用户身份互认。

可信教育数字身份是面向在校学生、教师、毕业生签发的、具有法律效力的可信数字身份标识。依托区块链平台提供的分层互联协议、可信身份、多方治理等特性，并采用国产密码技术，创新性的集合了法定身份信息、教育人员身份信息、网络身份信息的三大身份，形成可信的教育数字身份标识并实现统一认证，具有法律效力，打造教育信息可信制度凭证。可信教育数字身份为“学历学籍、综合素质评价、教育招生考试、个人终身学习”等建立教育可信数字档案平台与可信教育可信档案链，实现教育可信数字档案在全国范围内的“跨学校、跨系统、跨地区、跨行业”的互信互通与安全共享。解决了“网络教育身份可信认证、数字签名、数据加密、个人隐私安全保护、全证据链法律保障、网络行为的不可抵赖”等安全需求。

4. 远程办公：零信任无边界办公平台

业务访问的便捷性和安全性兼顾一直是企业数字化办公的需求。部分企业为了提供更为便捷的业务访问，将业务系统直接发布在互联网，极大的增加了业务安全风险；亦或是企业为了保证业务安全性，生产系统只能本地维护，一旦有故障发生，维护人员只能奔赴现场处理，响应速度大大降低。如何让员工/运维人员不论在何时何地，无论使用何种办公终端，无论对办公应用访问还是对生产业务维护，感知与本地操作一致，同时还能提升访问安全性和稳定性，是企业数字化办公的刚需。

零信任理念主要阐述了以动态访问控制为核心的企业内部安全框架。同时，也提出了不以访问终端设备所在网络位置为安全评判标准的方法。在零信任安全网络架构下，默认网络无边界，访问人员无论在哪里，使用任意终端，对内网办公应用或是业务资源的访问，都不需要使用VPN，同时更为多元的可信认证和更为精细的鉴权访问控制，实现无

边界化安全办公和运维。设计方案上，核心模块主要有：1）安全客户端，即安装在员工工作设备上的安全Agent，负责确保设备上的用户可信身份，可信设备，可信应用三要素；2）智能网关，即部署在企业应用程序和数据资源的入口，负责每一个访问企业资源的会话请求的验证，授权和转发；3）多个后台组件配合完成安全检测和访问控制，即策略控制引擎、身份验证模块、设备基线模块、应用检测模块。

5. 数字金融：普惠金融数字信任服务平台

供应链金融对实体经济有着强大的赋能作用，这在改善中小微企业经营困境方面尤为明显。供应链金融的数字信任解决方案主要通过大数据、人工智能、区块链、数字身份、电子签署等技术，打造支撑供应链金融的数字信任体系，旨在解决供应链金融企业间的信任和风控安全问题与中小企业融资难、成本高的困境，让金融机构能够更高效、便捷、稳健地服务于中小企业客户，确保借贷资金基于真实交易，同时依托核心企业的付款，使得整个产业链条上的企业都能融资，且是安全的融资。该平台的核心功能为：产业核心企业作为系统核心通过金融机构（多方）合作获得授信后，将授信额度分配给产业链内核心企业成员单位，成员单位获得相应额度即可开具数字信任额度，数字信任票据用于向上游供应商进行业务结算；供应商收到数字信任票据后，如果不继续流转，账款到期日平台向供应商结算还款；同时，任何一级持有者需要对其上游供应商进行支付账款，数字信任票据可以进行逐级转让，即债权转让，同时电子信票支持拆分部分转让；第三，任何一个持有方可以在平台发起融资，即反向保理业务。保理公司买入资产后，如果资金短缺，可将资产进一步卖出至金融机构，如银行、证券公司等，即再保理、ABS、ABN业务。基于信用保证，核心企业一旦开具数字信任票据，到期刚性兑付。如果成员单位到期未还款，所属集团需为其垫款、代偿。整个系统基于此模式开展业务，底层具有系统化的区块链协议、数字身份确责、电子签署确保法律效力支撑。

6. 数字物流：可信对账区块链服务平台

物流领域最重要的业务之一就是核心企业和承运商之间的结算。为解决现有物流结算问题，基于区块链技术打造快运对账区块链解决方案，形成“集中化、无纸化、智能化”的运营模式，基于区块链技术的分布式账本管理全物流环节，将物流信息上链，多节点存储物流数据，实现物流交接无纸化、运营结算自动化和可信数据共享的能力，构建基于电子签名的可信对账区块链服务平台。1）通过数字签名和区块链技术，实现了结算双方运输凭证的无纸化签收，生成基于区块链的电子运输结算凭证。在承运阶段，将包含运价规则的电子合同写入区块链，结算双方共享双方认可的交易数据和运价规则。在结算阶段，计费对账单基本是一致的，如果存在异常账单可以通过调账完成，调账的审核过程和结算付款发票信息作为存证写入区块链，两个阶段的结合使物流信息能够准确写入数据，并实现账单信息的实时核对，保证整个对账的真实可信。2）利用区块链公开透明、且不可篡改的特性可以实现对结算双方共享数据的控制权，从订单生成环节就将数据写入区块链网络，通过信用主体无纸化签收生成基于区块链的电子运输结算凭证。配合车载GPS系统收集位置数据，实时跟踪包裹的递送情况，实现信息流和实物流的一致性。3）基于数字签名技术实现运营过程无纸化。首先，为联盟链的每个信用主体构建数字身份，结合CA认证机构为其信用主体颁发数字证书，通过生物特征的采集确保使用该设备进行签收动作的信用主体的真实性，最后将签收结果写入区块链存证，整个过程可以确保签收主体的真实可信、签收过程真实可靠，

签收结果不可篡改、可验证。

7. 物联网：智慧工厂数字信任平台

随着物联网的快速发展，在智能家居、智能工厂、可穿戴设备等各种场景下，海量的物联网智能设备在大规模部署和上云联网。以智慧工厂为例，网络边界的日趋模糊，针对工厂物联设备的攻击和非法访问、非法控制风险凸显，同时，工厂联网设备的安全资源的有限性以及一些合法用户的不正当访问、使用放大了这些风险。物联网环境下的身份验证、访问控制逐步成为智慧工厂安全保障的关键。智慧工厂的数字信任方案，旨在通过多方式、跨域的工厂联网设备访问控制，以实现对联网环境下设备每次访问流程控制，构建工厂联网环境下的数字信任。具体功能模块包括：1）基于CMOS芯片技术的PUF芯片，即利用CMOS技术设计、生产的PUF芯片具备随机性、唯一性、可验证性、防入侵特征等优势，在工厂联网设备的ID自动生成、密钥的生产与管理、设备识别验证等场景下带来很好的安全应用。2）物联终端访问实时监控，可对大量工厂联网设备进行快速监测与扫描，实现对联网设备安全状态的实时监控，及时发现其中的在线、离线、故障等状态异常情况。3）基于信任评估的动态访问控制，通过对用户进行信任评估，确定用户的信任度并进行分组，进而即可根据其信任度和获得的角色对用户进行访问授权，能够更好地适应物联网分散、动态的环境。包括身份识别验证、权限授权审核、上下文监测、用户会话监控、用户信任度评估、根据用户信任度对用户角色进行权限指派等功能。

8. 车联网：LTE-V2X 通信中的 PKI 应用

车联网作为一个庞大的物联网应用系统，包含了大量的接入设备、数据、处理过程和传输节点，需要完整的安全标准体系来确保身份认证和数据的安全。V2X是指包括V2V（车—车）、V2I（车—基础设施）、V2P（车—行人）、V2C（车—云）等方式的车用无线通信技术，帮助实现车与外界的信息交换。车联网LTE–V2X系统使用基于公钥证书的PKI机制确保设备间的安全认证和安全通信，采用数字签名等技术手段实现V2V/V2I/V2P直连通信安全。数字身份认证技术应用于车联网通信中，可实现车载设备、路侧设备、应用服务商等各个角色的身份认证，保证通信消息来源的真实性，有效做到防重放、防止中间人攻击、防止身份假冒等，为依托车联网通信技术实现的安全预警和效率提升等车联网应用提供关键的基础安全保障。车联网LTE–V2X证书管理机构CA为用户签发证书，负责向车联网设备（OBU/RSU/VSP）颁发通信证书（注册证书、假名证书等）、签发证书撤销列表CRL以及更新证书等。

REFERENCES 参考文献

[1] 国家密码管理局何良生：密码是构建网络信任体系的基石 [EB/OL].https://new.qq.com/omn/20210604/20210604A01QAV00.html.

[2] Gartner.Definition: Digital Trust [EB/OL]. https://www.gartner.com/en/documents/3727718/definition-digital-trust.

[3] 普华永道 .2019 年数字信任洞察之中国报告 [EB/OL]. https://www.pwccn.com/zh/issues/cyber-security-and-data-privacy/china-digital-trust-insights/proactively-identify-and-manage-risks.pdf.

[4] 腾讯研究院, IDC. 数实共生 未来经济白皮书 2021[EB/OL]. https://www.yunduijie.com/upload/article/ppt/6010c7ca407e5a3cvrG0Txg84605.pdf.

[5] IBM Security.2020 年数据泄露数据泄露报告 [EB/OL]. https://www.ibm.com/downloads/cas/BK0BB0V1.

[6] 零信任架构及解决方案 [EB/OL]. http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a81825671a5dfe50171b41af1bd000a.

[7] 2020 年全球数据泄露大事件盘点 [EB/OL].https://new.qq.com/omn/20210105/20210105A0G40F00.html.

[8] 中国信通院 . 数据流通关键技术白皮书 [EB/OL].http://lawv3.wkinfo.com.cn/topic/61000000502/index.HTML.

[9] Federal Data Strategy 2020 Action Plan[EB/OL].https://strategy.data.gov/action-plan/.

[10] The European Digital Strategy[EB/OL].https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

[11] “十四五”规划纲要提到：加快数字化发展建设数字中国 [EB/OL].https://finance.sina.com.cn/tech/2021-03-13/doc-ikknscsi3736782.shtml.

[12] 民法典：首次将数据、网络虚拟财产纳入保护范围 [EB/OL].http://www.hxnews.com/news/gn/gnxw/202006/04/1901382.shtml.

[13] 中华人民共和国数据安全法 [EB/OL].http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

[14] NIST.Identity and Access Management Projects[EB/OL]https://www.nist.gov/topics/identity-access-management/identity-and-access-management-projects.

[15] 杨明慧 , 邹翔 . 美国电子身份指南评析 [J]. 计算机工程与应用 , 2019(23).

REFERENCES 参考文献

[16] Japan: MIC requests public comments on information trust certification guidelines version 2.1[EB/OL].https://www.dataguidance.com/news/japan-mic-requests-public-comments-information-trust.

[17] 国强 , 李新友 . 欧盟数字身份进展情况研究 [J]. 信息安全研究 ,2020,6(07):582-588.

[18] 从美国政府身份管理政策看国家机构数据安全治理的方法途径 [EB/OL].https://www.secrss.com/articles/11047.

[19] 电科防务 . 美国《国防部零信任参考架构》解读 [EB/OL].https://www.secrss.com/articles/31718.

[20] 中国信息通信研究院、阿里巴巴集团安全部、北京数牍科技有限公司：隐私保护计算技术研究报告 2020[EB/OL].http://www.caict.ac.cn/kxyj/qwfb/ztbg/202011/P020201110408006418997.pdf.

[21] 宋宪荣 , 张猛 . 国外网络可信身份认证技术发展现状 , 趋势 及对我国的启示 [J]. 信息安全与技术 , 2018, 009(002):6-11.

[22] 央行支付司温信祥：将人脸等纳入范畴，探索建立统一数字身份基础设施 [EB/OL].https://www.mpaypass.com.cn/news/202009/24184007.html

[23] 美国网络安全 | NIST 身份和访问管理(IAM)[EB/OL].https://cloud.tencent.com/developer/article/1792083.

[24] 工业和信息化部 . 关于开展车联网身份认证和安全信任试点工作的通知 [EB/OL].https://www.miit.gov.cn/zwgk/zcwj/wjfb/qt/art/2021/art_34a594d2b9bf4fba9141baf1d929a15e.html.

[25] 权威发布！关于全面推进上海城市数字化转型的意见公布 [EB/OL].https://www.shanghai.gov.cn/nw15343/20210108/c5ee6069f29a4a089f709708441bad31.html

[26] 腾讯 .《腾讯隐私计算白皮书 2021》[EB/0L].https://www.cebnet.com.cn/20210419/102743563.html.

[27] 中国信通院，奇安信 . 网络安全先进技术与应用发展系列报告：零信任技术(2020) [EB/OL].http://www.caict.ac.cn/kxyj/qwfb/ztbg/202008/P020200812382865122881.pdf

[28] 网络安全架构：零信任网络安全当前趋势 [EB/OL].https://www.secrss.com/articles/14542.

[29] 零信任架构的 3 大核心技术 [EB/OL].https://www.sohu.com/a/401254638_589567.

[30] 区块链数字身份：数字经济时代基础设施—区块链产业应用系列报告 [EB/OL].https://www.chaindd.com/3309289.html.

上海CA中心

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

以数据为核心
构建新型数字信任体系