可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

基于可信数字身份的区块链应用服务白皮书

（1.0版）

可信区块链推进计划
2020年12月

版权声明

《基于可信数字身份的区块链应用服务》

白皮书（1.0 版）编写委员会

❖ **牵头编写单位**（排名不分先后）：

公安部第一研究所、中国信息通信研究院、北京中盾安信科技发展有限公司

❖ **参与编写单位**（排名不分先后）：

新大陆科技集团有限公司、贵州梵华星云数据资源管理有限公司、北京航天航空大学、深圳前海微众银行股份有限公司、深圳法大大网络科技有限公司、中国联合网络通信有限公司、中国电子科技网络信息安全有限公司、蚂蚁科技集团股份有限公司、北京大学新一代信息技术研究院、深圳市迅雷网络技术有限公司、北京金山云网络技术有限公司、全链通有限公司、北京思源政通科技集团有限公司、续科天下（北京）科技有限公司、盈频轻资链（深圳）软件技术有限公司、北京链化未来科技有限公司、京东数字科技控股股份有限公司、杭州趣链科技有限公司、北京神州绿盟科技有限公司

编写组主要成员（排名不分先后）：

杨　林	凌　渝	魏　凯
黄耀晖	郝久月	王剑冰
李　頔	庞伟伟	国　伟
蒋才平	邓明玉	于　川
朱皞罡	赵　洋	梁敬彬
王开林	张开翔	韩　丹
庄子骏	亢　洋	叶　萍
王慧娟	李炜祎	李佩原
田　地		

引 言

2020 年是全面建成小康社会和“十三五”规划收官之年，是实现“第一个百年”奋斗目标的关键之年，也是“十四五”规划的谋篇布局之年，数字经济发展正成为全球经济增长的新引擎。一方面，区块链已成为数字中国建设和科技深度融合的重要方向，其应用已经延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域，对探索共享经济新模式新业态，重构数字经济产业生态，提升智慧城市的政府治理和公共服务水平具有重要意义。另一方面，区块链与可信数字身份的创新应用是国家的重要研究方向之一。可信数字身份作为各行业和各应用的底层基础，有利于促进各种应用和服务的融合，并能提高信息流转、汇聚和治理效率，降低企业的建设成本。以可信数字身份为基础，为各行业区块链赋能，提供核心的身份认证支撑；再由各行业区块链发挥面向用户的优势，向平台端汇聚数据，形成上下联动的循环体系。可信数字身份是连接链上和链下的桥梁，是区块链走向合规监管的桥梁。可以说，区块链的健康发展，离不开可信数字身份的支撑。因此，可信区块链推进计划数字身份项目组致力于推动区块链与可信数字身份的核心技术研究与行业应用落地，确定了两个阶段分步推进的工作思路：

第一阶段，可信数字身份赋能区块链。通过可信数字身份为区块链的前端应用做好底层支撑；

第二阶段，区块链赋能可信数字身份。利用区块链技术促进可信数字身份在多领域多维度的应用创新。

本白皮书基于第一阶段“可信数字身份赋能区块链”进行编制，其整体构想是：聚焦典型应用领域，打造“可信数字身份 + 联盟链”的应用体系，提供更安全的区块链应用解决方案，支撑各个生态链的安全可信，从而形成跨链互信的信任机制，打造端到端的基于可信数字身份的区块链服务框架。

项目组以国家政策为导向，以市场为驱动，以企业为主体，围绕数字身份与区块链的核心环节进行技术研究及标准建设工作，助力构建基于可信数字身份的区块链产业生态。未来项目组将继续加强可信数字身份与区块链的应用实践与探索，促进产业上下游良性健康发展，助力行业治理与监管，为数字中国建设提供强有力的底层支撑。

TBI 数字身份项目组

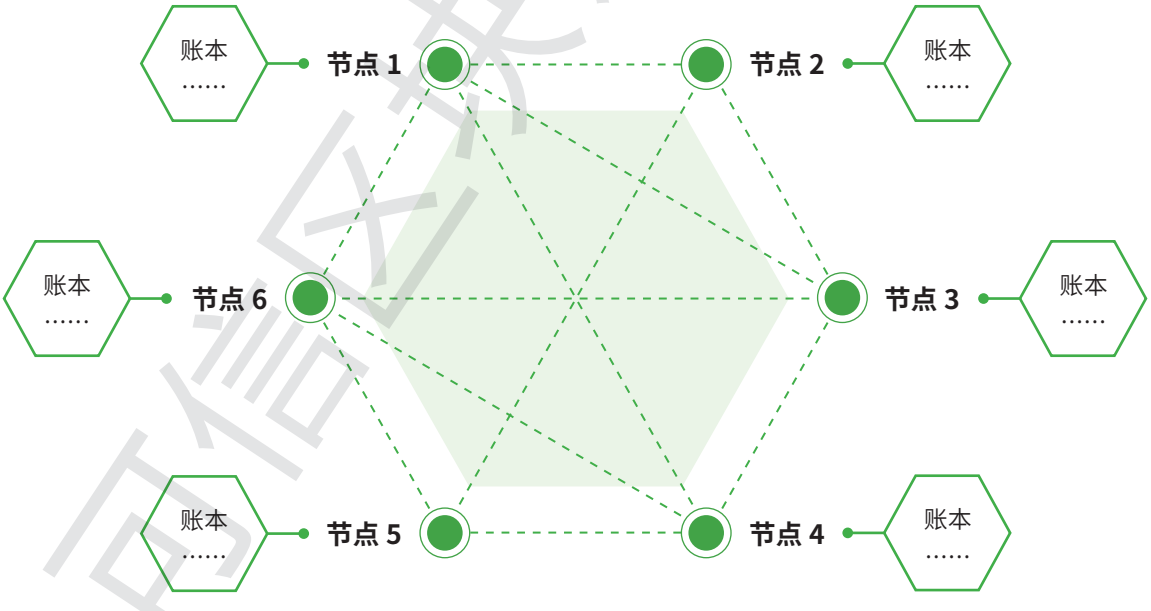
公安部第一研究所

目 录

第一章

区块链技术的发展及应用概况

1.1 区块链概念简介与分类



▲ 图 1 分布式记账网络

区块链本质上是上万个节点组成的一个去中心化账本，具有分布式数据存储、点对点传输、加密安全、共识确认等优点，它为数字身份的应用提供了一种可行的技术方案，可以有效解决身份验证和操作授权问题。通过区块链技术，自主主权的数字身份允许用户真正拥有并控制自己的个人数据和资产。

此外，区块链有公有链 (Public Blockchain)、联盟链 (Consortium Blockchain) 和私有链 (Private Blockchain) 之分。公有链节点间基于共识机制开展工作，具有开源和匿名的特点；不过匿名访问接入等特点目前并不适合网络实名制监管。

私有链一般建立在某个机构或者企业的内部，安全性及隐私保护能力更强，可防范内外部的恶意攻击；但因其网络封闭，不适合需要部署在互联网上、跨域提供服务的应用。

联盟链仅限于联盟成员参与，链上的读写权限、参与记账权限按联盟规则来制定，数据只限于联盟机构及其用户才有权限进行访问或更改。联盟链实现了部分去中心化，可控性较强，这些特点让联盟链具有可管可控的现实需要和技术基础。

相比于私有链，联盟链在运行空间和适用范围上的价值更大；而相比于公有链的完全去中心化和不可控等问题，联盟链则更为灵活，也更有可操作性。联盟链的这些特点，使得它十分适合于政府部门的电子政务应用以及需要一定监管的跨法人主体应用场景，节点通过准入机制得到授权后方可加入，不同节点所拥有的信息查看权限不同，能够实现可控、可监管的数据共享，同时有效保护隐私敏感数据。因此，上述分类中，与可信数字身份结合应用最有实践意义的是联盟链。

1.2

国内外区块链应用情况

1.2.1 区块链在国外的发展及应用

（1）主要国家重视区块链在数字身份领域的应用

2017 年 2 月，美国成立国会区块链决策委员会，全面加强区块链技术发展研究，努力完善与区块链相关的公共政策。2019 年 7 月，美国国家标准技术研究所（NIST）发布《新兴区块链身份管理系统分类方法》报告。报告指出，传统的数字身份管理系统存在单点故障（一点失效致使整体故障）、缺乏互操作性、侵犯隐私（如进行海量数据收集和用户画像）等问题，而区块链技术则可通过内置控制和授权机制来支持新型数据所有权和治理模式，从而在一定程度上解决了上述问题。因此，基于区块链的身份管理系统开始大量涌现。根据控制模式的不同，NIST 将这些系统分为两大类：“自上而下”和“自下而上”，并强调了相关安全和隐私保护问题。

表 按控制模式区块链身份管理系统可分为两大类

控制模式	描述
“自上而下”	系统所有者充当一个中央机构控制身份标识符的生成和 / 或凭证的颁发，通过授权来创建数字身份管理层次结构，并为用户提供增强的控制和隐私保护，同时保持系统的所有权和对其治理的控制。
“自下而上”	没有任何一个实体充当中央权威机构控制身份标识符的生成和 / 或凭证的颁发。参与者管理自己的身份标识符，通过一组智能合约强制执行数字身份管理规则。

2018 年 2 月，欧盟委员会成立区块链观测站和论坛，旨在将各成员国的区块链技术和力量聚集起来，共同将欧洲打造成区块链技术与应用的全球领导者。2019 年 5 月，欧盟区块链观测站和论坛发布《区块链和数字身份》报告。报告指出，受益于智能手机性能的日益强大、密码学的不断发展以及区块链技术的进步，基于去中心化身份（Decentralized Identity，DID）概念构建可信身份管理框架已经成为可能。报告描述了去中心化的数字身份管理概念，指出通过将来自权威机构（通常是政府）的可验证声明与个人数字身份关联起来，生成身份标识，用户就可以创建与现实世界证书类似的数字身份证书，从而消除对第三方机构的需求。

全球移动通信系统协会（GSMA）在 2018 年 6 月发布了《数字身份：推进亚太地区数字社会建设》报告，报告中提到数字身份是亚太地区经济、金融和社会发展的基石，强大安全的数字身份计划对于国家的重要性与日俱增，政府、私营部门主体和移动运营商都需要为数字身份框架提供支持。GSMA 报告考察了八个亚太国家的数字社会计划：孟加拉国、印度尼西亚、马来西亚、巴基斯坦和泰国等发展中国家和转型经济体需确保跨不同政府平台的互操作性，并更好地利用现有的数字身份系统以提供政府服务；澳大利亚、日本和新加坡这样的发达经济体，将重点转向推进在线和跨不同网络的非接触识别用户方式，利用数字身份提供更高效便捷的电子服务。2017 年 3 月，新加坡宣布制定国家数字身份框架，8 月宣布建立国家数字身份系统（NDI），解决公民使用政府网上公共服务的隐私保护和身份认证问题。2018 年 2 月，澳大利亚数字化改造办公室（DTO）发布了“可信数字身份框架”，计划基于电子身份证对个人信息的保护建立全国统一的在线身份认证体系。

（2）巨头纷纷抢占数字社会信任生态制高点

国际知名市场研究机构 Research & Markets 发布报告，预测全球区块链身份管理市场将从 2018 年的 9040 万美元增长到 2023 年的 19.299 亿美元，预测期内复合年增长率为 84.5%。报告指出，推动市场的三大因素：一是全球范围内对现有身份管理模式安全性的担忧在持续加剧。二是行业垂直领域对区块链身份解决方案和自主身份的需求日益增长。三是通过高交易速度和难篡改性可以有效简化业务。目前，区块链身份管理市场根据供应商属性分为三类：解决方案提供商、中间件提供商和基础设施提供商。其中，解决方案提供商是整个市场中增长最快的部分。技术先进的区块链解决方案，已经在各行业的垂直领域获得了一定程度的应用，从而推动了整体市场的增长。但是，报告也指出由于缺乏统一监管标准、监管环境不明朗以及对用户真实性的担忧，可能会阻碍各地区市场的发展。

IBM 全力打造基于区块链的全球身份网络。2017 年初，IBM 与加拿大身份验证提供商 SecureKey 公司联合发布数字身份网络，并同加拿大数字身份生态系统成员（主要包括银行、电信公司和政府机构）一起搭建基于区块链的身份验证网络。随后，IBM 与去中心化身份基金会（DIF）签署了合作协议，该基金会旨在提高区块链身份系统的互操作性和标准化，以共同建设区块链身份管理标准体系。2018 年初，IBM 宣布加入 Sovrin Foundation，该组织旨在打造一个基于区块链技术的全球分布式身份识别系统，该系统使用分布式账本技术实现加密签名凭证的安全交换，以证明所有者的数字身份信息。2019 年第一季度 IBM 与 Visa 联手推出基于区块链的数字身份识别系统用于改善跨境支付安全。

微软提出在比特币区块链上建立去中心化身份网络。2018 年，微软与 ID2020 联合开发分布式数字身份认证网络，帮助个人和难民获得基本服务；同年，微软与万事达合作推动数字身份的合作计划，解决难民身份归属的问题，确保这些用户可以获取正常的金融、社会服务或者用于防洗钱。2019 年 5 月，微软提出了一个庞大的区块链相关计划，拟在比特币网络的基础上建立一个去中心化的身份识别基础设施 Project ION。这是一个全新的、更具体的概念：一个建立在比特币区块链之上的 DID 网络。这个名为身份覆盖网络（Identity Overlay Network，ION）的基础设施是微软与其他 DIF 成员一起实施开发的，可以适应每秒数万次的并发操作。本质上，ION 基于 Sidetree 协议，允许用户通过管理公钥基础设施（PKI）来控制自己的数据，其目标是创建一个去中心化的身份生态系统，在这个生态系统中，数以百万计的组织、数十亿的人和无数的设备，可以在基于标准和开源组件的互操作系统上安全地交互。

此外，全球各大运营商也纷纷加入各大联盟致力于区块链应用研究。美国四大运营商 AT&T、Verizon、T-Mobile 和 Sprint 组成移动身份验证工作组，于 2018 年 3 月发布了全新的“移动验证平台”，可以在用户同意的情况下为其他用户提供加密验证的电话号码和个人资料数据，并用区块链技术来记录，保证真实可追溯。2019 年初，Facebook 创始人扎克伯格公开表示将考虑建立基于区块链技术的认证系统，以确保用户安全登录。

（3）多种区块链方案提供了重要的技术动力

总体来看，区块链技术应用于身份认证主要有两种思路：一种是由用户控制身份，创建新的基于区块链的数字身份；另一种是传统数字身份 + 区块链的模式，将已有的数字身份信息置于去中心化的区块链之上

由用户控制的身份信息类似于一个社交媒体账户，需要创建一个新的基于区块链的数字身份，然后将基于区块链的账户应用于全网。用户可以基于不同情况授予或撤销第三方对其信息的访问权。一些公司和组织正在研究这种解决方案，包括 Sovrin 和 uPort。

Sovrin 是一个非营利性组织，其旨在创建一个基于区块链的全球去中心化身份识别系统，其自主身份解决方案试图在相互交易的个人、组织和连接的设备之间建立信任体系。

uPort 项目是基于以太坊的自主身份 ID 应用，它允许用户进行身份验证、无密登录、数字签名，并和以太坊上的其他应用交互。目前，uPort 正与瑞士楚格市进行合作，建立基于以太坊区块链的数字身份认证平台。此外，uPort 还与英国 Onfido 公司和四大审计公司普华永道（PwC）建立合作伙伴关系，以在英国的金融服务领域开发基于区块链的身份管理。

“传统数字身份认证 + 区块链”的思路侧重于身份认证。不同于用户控制的身份信息，这类身份认证主要是验证预先存在的证书（如身份证、驾照），然后将该信息与区块链上的合法所有者绑定，有效地为传统的身份识别方法创建一个去中心化的数据库。基于这种思路运行的企业和项目包括 SecureKey、Civic、ID2020。

SecureKey Technologie 是一家加拿大安全技术初创公司，总部位于加拿大多伦多市，专注于身份验证和账户安全管理的技术服务，它正在发行一个名为 Verified.me 的产品，帮助银行验证用户身份，并与 IBM 合作为加拿大银行建立数字身份网络。

Civic 是一家总部设于美国加州帕罗奥图的公司，成立于 2015 年，其开发的基于区块链和生物识别的多因素身份认证系统 Civic，允许用户通过区块链共享和管理他们的身份验证数据，并可以在无需用户名和密码的情况下，进行准确安全的用户身份识别。

ID2020 是一个公私合作联盟的项目，其致力于联合各国政府、科技巨头和非政府组织采取统一行动，以在 2020 年之前为所有人提供合法身份证明。该机构联合微软、埃森哲和其他公司，正在建立一个分布式账本平台，以帮助全球没有官方身份证明的人口在分布式账本上注册身份。

1.2.2 区块链在国内的发展及应用

（1）国家密集出台相关政策推动区块链发展

我国政府已将区块链技术作为战略性前沿技术进行提前布局。在《国务院关于印发“十三五”国家信息化规划的通知》《国务院办公厅关于积极推进供应链创新与应用的指导意见》等政策性文件中多次提到要加强对区块链技术的创新研究及产业引导，鼓励地方政府出台优惠政策推动区块链技术的研究和落地。在监管层面，国家先后出台了《区块链信

息服务管理规定》《关于防范代币发行融资风险的公告》《关于开展为非法虚拟货币交易提供支付服务自查整改工作的通知》《关于防范境外 ICO 与“虚拟货币”交易风险的提示》等文件，为区块链技术的使用和管理等提供有效的法律依据，推动了我国区块链相关领域管理规定的细化落实。

（2）“区块链 +”理念为各行业应用提供支撑

在我国，深圳区块链电子证照应用平台实现了身份证、户口本等 24 类常用电子证照上链，支持 100 余项高频政务服务事项的办理。福建省数字办重点集中开工 20 个区块链应用重点项目及区块链应用服务平台等区块链“新基建”示范项目。央行数字货币（DC/EP）研发工作得到国务院正式批准，且央行贸易金融区块链平台支持供应链应收账款多级融资、跨境融资等多项业务。2018 年 9 月，中国移动推出了“联核云身份证核验平台”，针对快递业和住宿业提供用户身份认证服务，在区块链技术的加持之下，防范了可能的信息篡改，确保信息可溯源，并且每一个主机节点的闲置身份证核验能力可以共享，确保了核验效率。支付宝推出首个基于区块链的跨境汇款服务。杭州司法电子证据平台、北京互联网法院在受理案件中均使用了区块链技术，解决了电子证据存取证难的问题。

1.2.3 国际区块链标准化情况

（1）ISO/TC 307。ISO/TC 307（区块链和分布式记账技术技术委员会）成立于 2016 年 9 月，旨在推动区块链和分布式记账技术领域的国际标准制定等工作；目前已有 35 个积极成员（P 成员），12 个观察成员（O 成员）；成立了 4 个工作组（基础工作组，安全、隐私和身份认证工作组，智能合约及其应用工作组，治理工作组）和 2 个研究组（用例研究组和互操作研究组）。中国在 ISO/TC 307 已立项的 8 项国际标准中，分别承担了分类和本体（Taxonomy and Ontology）的编辑以及参考架构（Reference architecture）的联合编辑职务。

（2）W3C 的 DID 标准。针对数字身份的去中心化和自主主权身份，W3C（The World Wide Web Consortium）主张通过分布式身份标识（Decentralized Identifier，DID）来实现用户身份的自主管理，其 DID 标准化工作主要集中在 DID 规范和可验证声明两部分。

（3）DIF 的标准化工作。DIF（Decentralized Identity Foundation）去中心化身份基金会旨在利用区块链技术为在线身份建立一个开源的生态系统，为身份验证创建通用协议，建立并推动由开源代码支持的新兴标准规范，以提高区块链身份系统的互操作性。

1.2.4 中国区块链标准化情况

2020 年，由中国电子技术标准化研究院牵头的《信息技术 区块链和分布式记账技术 参考架构》国家标准征求意见会在成都举行，标志着我国进一步加快了区块链标准化的步伐。同年由信工所牵头制定的《信息安全技术 区块链信息服务安全规范》研制启动会成功召开，该标准旨在研究区块链信息服务安全风险，提出安全要求和测试评估方法，适用于指导区块链信息服务提供者开展安全建设和安全评估。此外，国内某银行落地实施的“基于区块链的供应链金融企业应收账款融资系统”成功入选了 ISO/TC 307WG6《区块链与分布式账本技术标准（征集意见稿）》，将为区块链与分布式账本技术应用国际标准的制定提供参考。

第二章

可信数字身份认证体系发展

2.1 数字身份的概念与发展

2.1.1 数字身份的概念

▲ 图 2 数字身份扩展

数字身份通常指对网络实体的数字化刻画所形成的数字信息，如个人标识及可与标识一一映射的绑定信息。数字身份可作为用户在网络上证明其身份（属性）真实性的凭证，用户在不同的应用服务中可使用不同的数字身份进行标识（如手机号码、电子邮箱、微博、微信等），这些身份属性信息可以辅助业务机构确定一个人的身份，但是此类信息是可以变更、隐藏、甚至是可以注销废弃的。基于上述情况，为了保证用户在网络空间活动中个人身份（标识）的可信及个人行为的可信，如何确认数字身份在网络空间中的可信是近年来国家的关注焦点。

2.1.2 数字身份的发展

数字身份技术的发展经历了中心化身份、第三方身份提供商 IDP（ID Provider）及自主主权身份 SSI（Self-sovereign Identity）三个阶段。

中心化的身份认证服务令用户的身份认证和管理对单一的中心机构有强依赖性，且各终端应用所需的用户身份属性信息各异，应用间不互通，导致用户需针对不同的应用服务多次提交身份属性信息。因此，中心化的身份认证服务更适用于具有强身份认证需求的业务场景（如政务应用、治安管理等）。

基于 IDP 的身份认证针对中心化身份的痛点，通过对用户进行跨平台或机构的统一管理，使用户使用少量的身份信息即可获取跨系统、机构、地域的互联网服务，提供了一定的便捷性，被大型互联网企业广泛采用。在基于 IDP 的身份中，用户向单个或多个 IDP 提交个人信息进行注册，使用同一用户名和密码即可实现多个 IDP 的认证，显著提升了用

户体验。业界也涌现出 OpenID、SAML、OAuth、FIDO 等一系列国际标准，来实现不同 IDP 身份认证系统之间的互联互通和跨域访问授权。与中心化相比，用户无需大量登记个人身份信息，从一定程度上降低了隐私信息泄露的风险。但出于运营主体和运营壁垒的考量，很多业务在应用层面并不互联互通，跨应用的业务实现难度很大，尤其对于需要用户确权操作的跨应用业务，可能需要更改整个业务架构。

自主主权身份 SSI（Self-sovereign Identity）是搭建在区块链上的数字身份，无需任何第三方机构参与，用户身份信息由用户自己保存，从根本上消除了身份窃取和泄露的可能性，在自主、安全、可控的层面上级别更高。凭借区块链的去中心化、分布式、共识机制、哈希加密等特性，自主主权身份支持用户在线轻松地进行身份验证。用户可根据实际需要有选择性的公开身份信息，甚至隐藏自己的身份。有效地保障了用户身份的隐私安全，使用户对自己的身份拥有绝对的使用权和控制权。可以说自主主权身份提供了一种新型的信任传递和数据交换框架。

自主主权身份的实现在一定程度上促进了网络可信身份管理的变革。用户在对自己身份获得更多控制权的同时，也带来了一些新的问题。一是，用户应该如何选择上链的身份属性信息才能最大程度地降低身份信息泄露的风险。二是，尽管区块链保障了链上数据的真实完整，但数据上链前的真实性以及数据上链的传输过程仍存在一定隐患。自主主权身份的应用给用户的身份隐私保护提供了一个解决方案。虽然目前仍存在一定的阻碍和限制，如何实施也还处于探索阶段，但随着技术的更新和迭代，自主主权身份必然会在数字经济时代占领一席之地。

2.2

可信数字身份的体系构建

2.2.1 网络可信身份体系

网络身份认证按照认证的可信程度、方式、形式、性质以及应用范围和应用场景不同，可分成以下三个级别：法定信任基础级、第三方作证级、业务凭证级。

▲ 图 3 网络身份三级认证体系

法定信任基础级使用依据国家法律法规、由特定行政机关签发、面向全社会应用、具备法定效力的身份证和护照等真实身份证件信息形成的身份凭证；第三方作证级使用根据相关法规和行政许可设立的、由第三方签发、面向行业系统应用、可作为司法采证的电子签名证书等身份凭证；业务凭证级使用各业务系统签发、面向自身系统及其关联系统应用、作为业务凭证的身份凭证。

2.2.2 可信数字身份

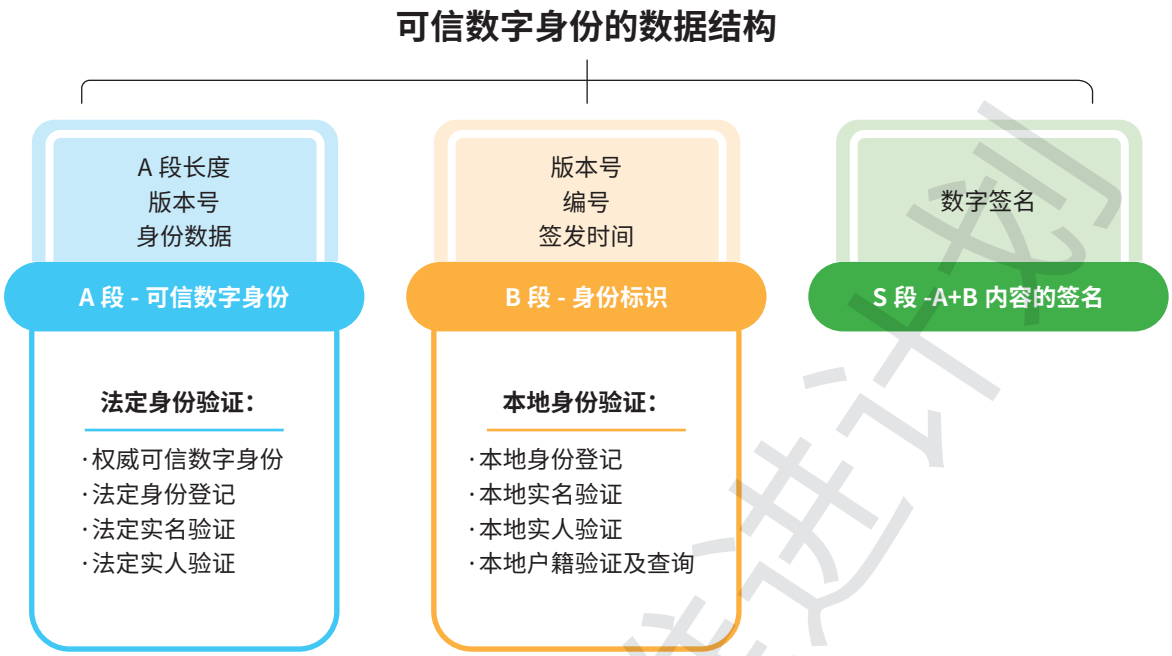
（1）可信数字身份的概念

可信数字身份是在真实身份核验的基础上，经加密及脱敏处理，由权威机构签发，用于网络空间中证明网络用户的电子文件，与居民法定证件信息具有一一对应关系，实现了端到端的全流程可信认证，符合网络身份的三级认证体系。

可信数字身份将现实社会的法定身份关系映射到线上，具有“前端匿名、后台实名”的特性，可以有效保护公民个人隐私信息，实现线上线下的身份融合和管理一体化，网络用户无需直接使用真实身份信息即可完成身份核验或认证。

（2）可信数字身份凭证和标识

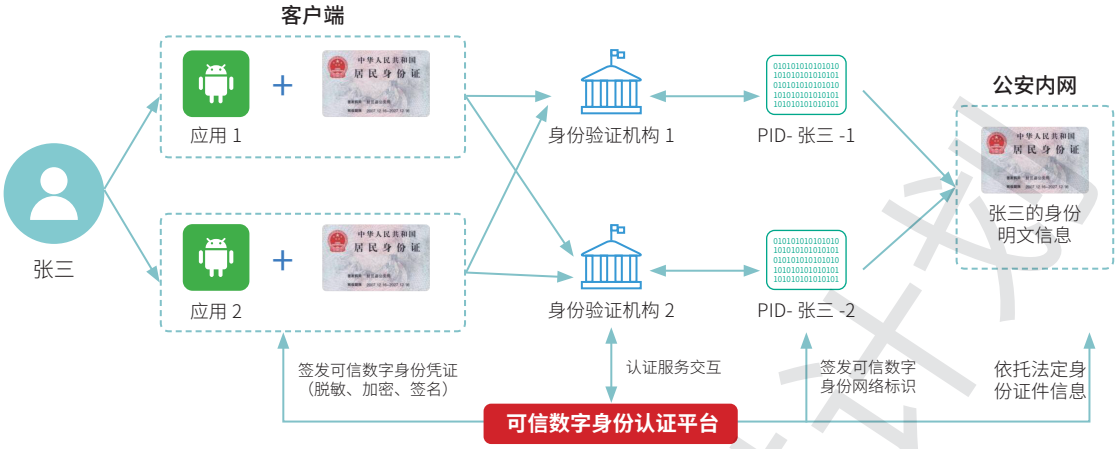
可信数字身份凭证用于可信数字身份认证，由 A、B、S 三段数据构成。A 段为可信数字身份，其基于居民法定证件身份信息具有法定身份登记、法定实名验证以及法定实人验证的能力；B 段身份标识支持基于业务应用系统为个人签发，具有本地身份登记、本地实名验证以及本地实人验证的能力；S 段则为“A+B”段内容的数字签名。



▲ 图 4 可信数字身份的数据结构

基于“A+B”段的可信数字身份支持数字身份的联合签发，一是为实现不同应用系统间的身份互认提供了有力支撑；二是支持政府、通信运营商、银行以可信数字身份为核心构建各自的数字身份生态；三是支持业务应用系统广泛对接各类业务场景，为实现共赢生态奠定基础。

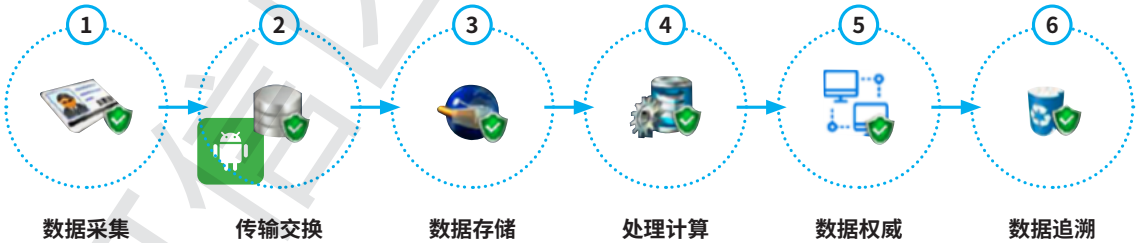
可信数字身份标识（PID，Personal ID），其是网络用户在一个网络服务商内使用可信数字身份进行认证后所签发的与可信数字身份一一对应的身份标识，用于实现对网络用户在一个网络服务商内的终身有效管理。同一网络用户在不同的网络应用服务商中的可信标识相互独立，可有效防止网络用户的网上行为被网络应用服务商关联聚合、追踪标记。



▲ 图 5 可信数字身份签发认证流程

（3）可信数字身份的特点

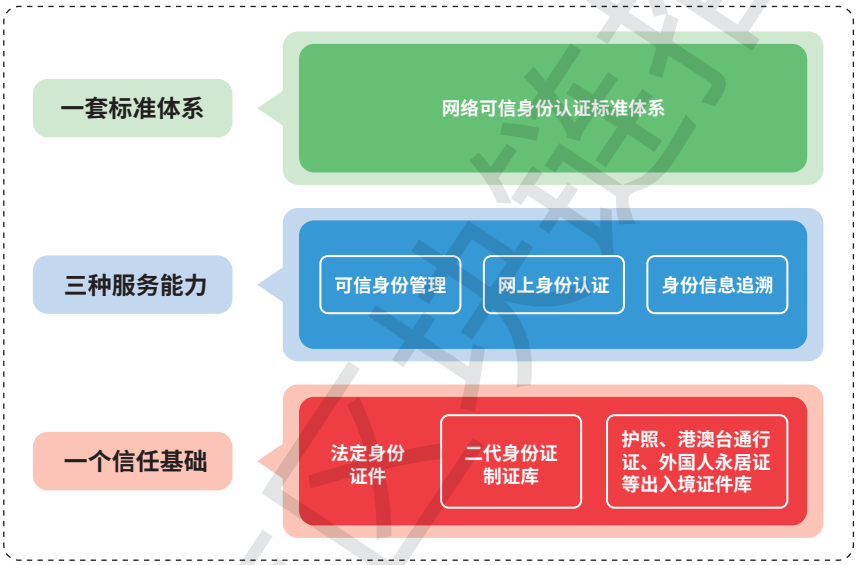
可信数字身份具有权威、安全、可信、便捷的特性，是现实生活和网络行为的通用凭证。一是数据权威，基于法定身份证件信息，保障对网络用户的身份核验与认证权威、真实、有效。二是端到端保护，可信数字身份的签发和认证保证全程端到端每一个环节的安全可信，明文信息不落地，完全不泄漏个人隐私信息，传输过程加密、签名，信息防泄漏、防篡改。三是可追溯，通过对用户下发可信数字身份标识，支持用户认证的可追溯性。



▲ 图 6 端到端认证

2.2.3 可信数字身份认证平台

我国长期以来高度重视网络可信身份体系的建设，积极探索基于可信身份的数字身份发展。2016 年国家发改委批复建设，公安部第一研究所承建的国家“互联网 +”重大工程可信身份认证平台 (CTID 平台) 上线。CTID 平台以法定身份证件为信任根 , 为各行业提供统一、权威、多级可信的网络身份认证服务。目前 CTID 平台已经在很多应用中实现对接，如中国政府网、国务院 APP、公安部政务服务平台、国家移民局互联网便民服务等，并为国家政务服务平台提供基于实名认证支撑的基础服务 , 实现政务服务“一次认证、全网通办”。



▲ 图 7 CTID 平台提供统一、权威、多级可信的网络身份认证服务

CTID 平台已为 46 个国务院部门和 31 个省级单位政务服务平台提供了身份认证服务，认证量累计 2 亿多次。在省级政务应用中，支撑广东“粤省事”、江西“赣服通”等多个政务服务应用形成一批特色的解决方案。在互联网 + 公安服务方面，为公安部“互联网 + 政务服务”平台、国家移民管理局政务服务平台、公安部交通安全综合服务、乌鲁木齐市网络身份认证平台等提供身份认证。有力支撑了国家、地方和公安

政务服务，有效推进“一网通办”和企业群众办事“最多跑一趟”，为推进国家“互联网 + 政务服务”战略和深化“放管服”改革贡献了力量。

CITD 平台实现了网上网下身份管理的一体化，促进了网络空间信任体系的建设，承担着网络空间中最核心的基础信任源的角色，是信任链传递最初始的根，是国家实施网络身份治理的重要基石。本着“网络可信身份管理是网络可信体系的核心”、“法定身份证件是网络可信身份管理的基础”的核心理念，CTID 平台正在积极研究基于可信数字身份的分布式数字身份技术的研究与应用。

第三章

基于可信数字身份的区块链建设需求

3.1 区块链具有身份认证强需求

数字经济时代，数字身份正在扮演着愈发重要的角色，而区块链技术与数字身份有着许多天然的契合点。数字身份方面的研究与应用落地，旨在建立完善的区块链数字身份应用体系。

一方面，区块链系统本身具有身份认证的强需求。在实际业务操作中，为了证明用户的真实身份，区块链应用普遍采用如用户名、手机号码、活体检测或图像识别的身份认证方式。然而，缺少了基于法定身份的实人实名认证存在安全隐患，攻击者可通过大量编造的虚拟身份影响投票及共识等过程。

另一方面，各个服务提供商或认证机构间互为数据孤岛，难以打通。导致用户需要用同样的信息反复在不同的应用中重复认证，对已有信息

不能复用。此外，用户的认证信息是碎片化的，无法完整地反映用户的身份特质，用户同样无法有效地管理自己的身份信息。

区块链应用基于密码学可实现匿名应用，在与现实世界的具体应用衔接时，用户身份的可信认证问题逐渐突显出来。根据国家网信办2019 年 3 号文件《区块链信息服务管理规定》中第五条和第八条之规定，区块链信息服务提供者应当落实信息内容安全管理责任，建立健全用户注册、信息审核、应急处置、安全防护等管理制度。同时，区块链信息服务提供者应当按照《中华人民共和国网络安全法》的规定，对区块链信息服务使用者进行基于组织机构代码、身份证件号码或者移动电话号码等方式的真实身份信息认证。用户不进行真实身份信息认证的，区块链信息服务提供者不得为其提供相关服务。

基于法定身份的身份认证模式可助力区块链应用在一定程度上解决身份信息上链和跨链的数据真实归属问题及用户行为确权问题，从源头确定账户的归属，减少业务风险，降低安全隐患。

3.2

加强区块链的密钥安全管理

非对称密钥加密体系是区块链各类节点之间进行身份互认的基础，同时也是区块链应用用户、账户体系的身份认证基础，有效的密钥管理技术是加强区块链应用的有力抓手。

区块链应用中的主流密钥管理方法包括本地存储、离线存储、托管钱包和门限钱包。本地存储将密钥直接或经加密后存储在本地设备上，容易被恶意读取，物理设备损坏时也无法恢复。离线存储将密钥保存在离线的物理存储介质中，防止恶意软件攻击。但是使用时仍然需要联网，无法完全避免恶意软件入侵。区块链还可以利用第三方托管服务器为用户提供密钥托管服务。但托管钱包不符合区块链的分布式思路，且同样存在密钥窃取、后门攻击和单点失效等问题。托管服务器作为中心节点也容易成为攻击目标，一旦被攻破，大量密钥失窃将会造成严重的损失。门限钱包利用门限加密技术将密钥分散存储在多个设备中，使用密钥时需要多个设备参与，即使某个设备被攻击，攻击者仍然无法恢复出完整的密钥，也不影响用户的使用。不过这种方案在设计上存在一定困难，算法复杂度高，且很难扩展。

可以说，区块链应用和非对称密钥加密体系是息息相关的。非对称密钥加密体系可实现对数据的数字签名、不可否认与抗抵赖，利用数字签名也可较容易地发现任意恶意者对数据全生命周期内的非法篡改，保护数据信息的完整性。

3.3 跨链操作互联互通亟待解决

跨链技术的应用可助力众多的异构区块链应用构建互联、互通、互信的区块链应用网络。区块链无法像传统网络系统通过中心节点实现互通，如何实现去中心化区块链平台间的连接、解决跨链操作的原子性问题是跨链技术面临的最大挑战。目前，为实现区块链跨链研究人员先后使用过公证机制、侧链或中继网络、哈希时间锁合约 (Hash time lock contract, HTLC) 和分布式私钥控制等技术实现异构区块链互联。

公证机制：通过中间节点资金托管的方式保证安全支付。通过一个或多个第三方连接器账户进行资金托管，形成跨链交易路径，可以保证两个异构区块链之间的代币兑换。

侧链或中继网络：将侧链或中继区块链作为异构区块链间的中介网络，通过主干网上的中继器将异构的区块链子网进行互联，从而实现各数字资产交易，是价值互联网的代表。

哈希时间锁合约：要求只有在规定时间内给出正确的哈希值原像的节点才可以使用这笔被锁定的代币。

分布式私钥控制：通过安全多方计算或者门限密钥分享等方式实现对账户资产的锁定与解锁。目前，跨链技术的发展需要大量理论研究和实验测试支撑。跨链技术研究还多限于金融领域的代币兑换和跨境支付，

要实现异构区块链通信还有待进一步研究。

当前区块链的网络效应初显，但仍需在技术上针对相关功能组件进行升级，同时需要重视与用户的交互体验，增进链上与链下、链链之间的互联互通性。区块链的跨链操作技术目前处于技术发展早期，相信随着从业者的持续研究，未来将会加速技术的不断突破，从而促进区块链应用的不断迭代与创新。

3.4 合理的应用分布式身份认证

一方面，传统的中心化认证方法优点是权威性与管理简单，缺点是仅完成身份的数字化，难以满足数据治理、可信签名、场景灵活拓展的需求；另一方面，基于区块链技术的分布式身份缺乏法定性，各平台的账户体系不支持互相认证。因此，需要将可信数字身份和区块链进行有机结合，形成基于可信数字身份的区块链应用服务，更有利于满足政府或企业对于场景拓展和数据治理的需求。

发展数字身份与区块链的结合应用是必然趋势，基于可信数字身份的区块链应用服务借助非对称加密和区块链技术保障用户身份隐私，通过对私钥的控制，用户可以自主选择如何处理或使用自己的数据。

分布式数字身份指在身份验证阶段不需要授权方或者任何第三方中心机构的参与，用户可以直接通过分布式系统验证并确认其身份的真实信息。然而在身份数据的源头，依然需要可提供强大背书功能的机构来协助进行身份鉴权。

区块链和数字身份相辅相成，区块链时代需要数字身份作为认证基础，两者互相依托，相互促进。相信随着手机等其它智能应用的蓬勃发展以及移动互联网基础设施的不断完善，区块链应用的兴起更需要可信数字身份作为网络身份认证的基础设施加以支撑保障。

3.5 相关监管制度需要完善修订

（1）区块链发展和应用需要顶层设计

区块链技术的研究与应用当前依然处在发展阶段，虽然业内已有很多成功案例，但平台异构、规范不一、场景缺乏、标准滞后以及监管薄弱等问题尚未完全解决。国家依然需要明确区块链应用的战略目标、基本思想和主要路线，建立实施机制，促进生态发展，从而推进区块链在我国的健康发展。

（2）上链前身份信息的需要真实性验证

区块链技术可以很好地保证链上信息的真实有效性，但是上链前身份信息的真实性以及向链上传递的过程有可能存在安全风险。上链前的身份信息需要一个权威可信的机构来进行认证，并基于其认证结果，将该信息上链，从源头保障身份信息的真实可信性。

（3）促进行业法律法规的补充完善

随着区块链技术的不断发展，对应法律体系的配套建设只有及时补充与完善，才能弥补当前的法律空白，更加有效地规范、调整、解决区块链发展过程中产生的各种问题。针对区块链技术的长远发展进行科学立法，从信息安全、法律监管、保障措施等方面出台对应法律法规，从源头加强链上数据信息保护，防范数据信息的泄露与破坏及其它潜在风险。

（4）推进行业标准的制订出台

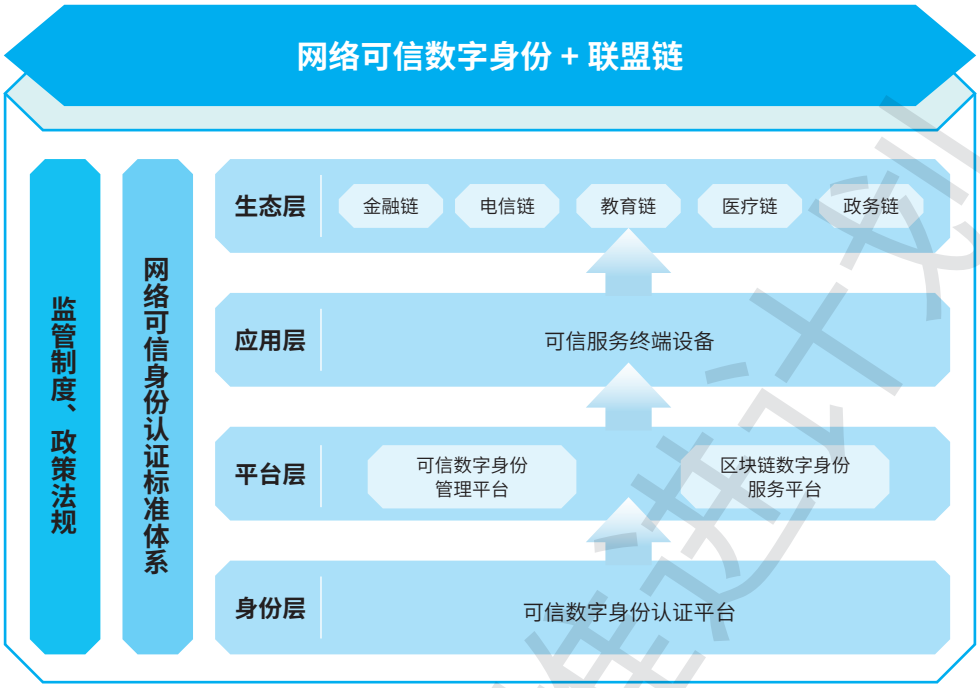
在区块链相关法律相对缺乏，无法及时有效解决现存问题的情况下，建议先完善区块链相关行业标准的制定，以加快推动区块链标准化发展。具体来看，建议关注区块链当前存在的普遍问题与重点难题，如智能合约存储、数据保护以及运行安全等问题，逐步建立和完善区块链技术的应用和标准体系；此外，建议积极参与相关国际标准的制定工作，加强国家标准与国际标准之间的交流，不断提升我国区块链标准体系的国际话语权。

第四章

基于可信数字身份的区块链应用服务设计

4.1 打造权威可信的服务框架

权威可信的数字身份管理是网络安全的重要环节，是发展数字经济的安全保障，区块链的发展需要在身份可信的基础上健康发展。因此，研究可信数字身份和区块链技术的结合，将可信数字身份管理作为区块链应用的重要基础支撑，有利于促进各种应用和服务的融合，提高信息流转、汇聚和网络治理效率。同时借助身份认证、数据保护、区块链基础、安全策略等一系列措施，协调整体统一的可信数据流转，为实现“可信数字身份 + 联盟链”的应用体系奠定基础。



▲ 图 8 “可信数字身份 + 联盟链”的四横两纵体系

在“可信数字身份 + 联盟链”的四横两纵体系中，身份层以可信数字身份认证平台为基础，以法定身份证件为信任根，为各行业提供统一、权威、多级可信的网络身份认证服务；对外签发身份凭证，实现了网上网下身份管理的一体化。

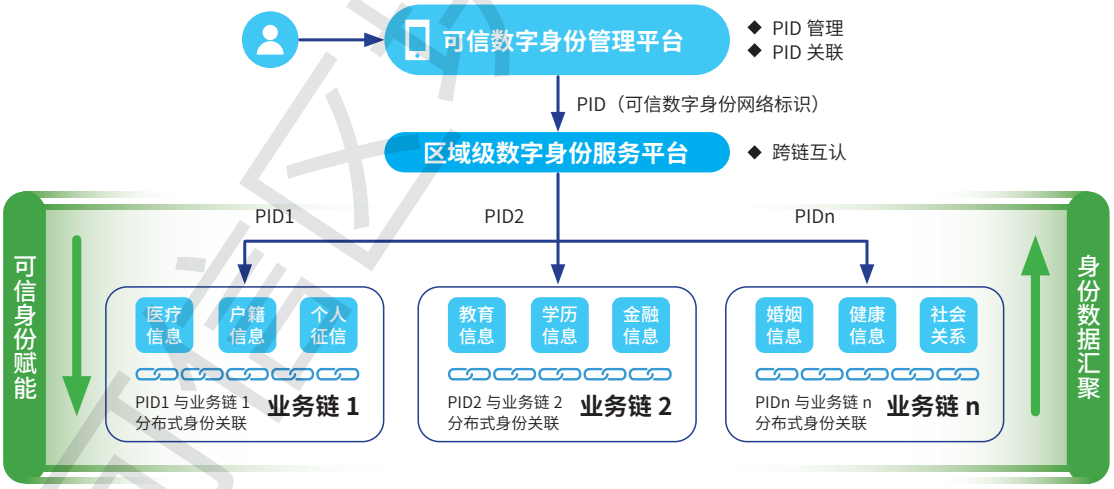
平台层部署可信数字身份管理平台和区块链数字身份服务平台进行数字身份的管理和链间互认的服务能力。一般而言，可信数字身份认证平台为每一位自然人认证签发可信数字身份后，非强身份认证场景的日常身份核验、认证、管理等职能可由可信数字身份管理平台完成。一旦遇到强身份认证场景，则需要可信数字身份认证平台提供根认证支撑。

可信数字身份管理平台通过对接可信身份认证平台可提供常规的身份核验、认证、管理等功能。拥有对自然人法定身份证件相映射的安全加密的唯一可信数字身份标识（PID），是自然人在各种电子政务、公

共服务或商业业态下的业务身份的溯源索引。可信数字身份管理平台通过对各个业务链内的不同 PID 进行关联，支持对不同生态链之间同一用户的身份建立关联关系。

区块链数字身份服务平台借助可信数字身份管理平台提供跨链互认的服务能力，支持不同业务链间的身份溯源查证。区块链数字身份服务平台是对接区域或业务生态内各种电子政务、公共服务以及商业业态的业务系统，可提供自然人关联不同业务场景下的身份属性、业务标识、身份互通、行为轨迹等信息服务，包含数据账户及多维身份登记、多维身份标识映射、链上数据追溯审计、共享个人数据索引。

应用层配套可信服务终端设备，大幅提升区块链应用的安全性和可操作性。生态方面，通过 PID 与 PID、PID 与分布式身份之间的关联，支持不同业务链间的身份互认，实现链间信任传递。



▲ 图 9 可信数字身份赋能区块链应用

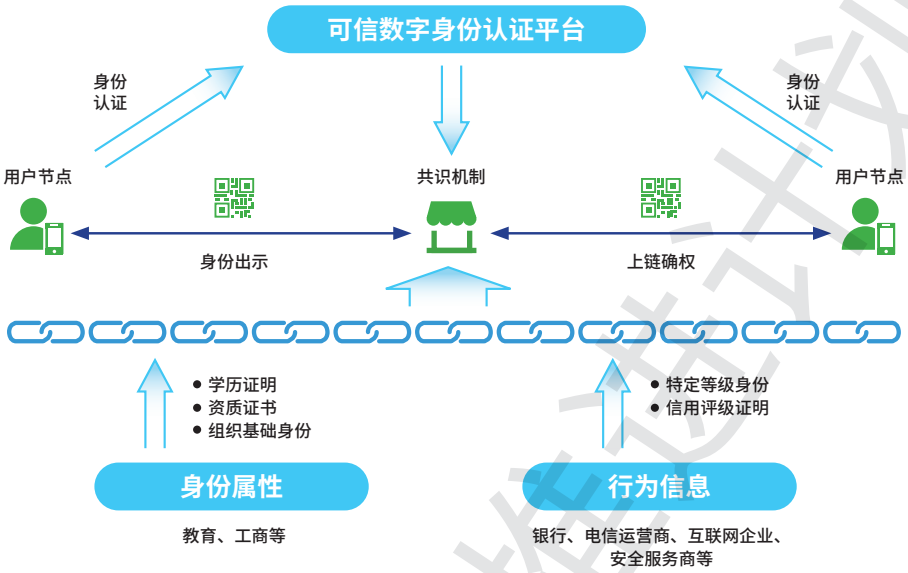
以可信数字身份为基础，提供核心的身份认证支撑；由各行业区块链发挥面向用户的优势，向平台端汇聚身份数据，为各行业区块链应用赋能。借助可信数字身份对区块链应用的赋能可真正实现用户对个人身份信息的使用权，为实现降低社会信用成本的目标打好基础。通过监管制度、政策法规以及行业标准的建设，辅以安全防护和运维监控的安全保障，提供更安全的区块链应用解决方案，支撑各个生态链的安全可信。

4.2 实现根源法定的监管治理

当前联盟链的监管只限于各个联盟链自身，主要采用事前防范（对内容的审核和过滤）；事中监管（对非法操作的发现、预警及应急处理）以及事后处置（问题提交决策、处置）三种方式。被监管的对象有自然人、法人及非法人。其中法人及非法人最终也能落实到自然人，因此我们主要还是关注对自然人的监管。对联盟链的治理监管需要适配各个联盟链，其中对于被治理主体的身份确认是首要前提。

由于各个联盟链节点用户存在不同的身份体系，如：居民身份证号、手机号、银行账号、电子邮箱、QQ 号等，即使大家都使用身份证号作为身份的主索引，不同体系间也存在认证标准不一致、互不信任问题。因此，通过对接可信数字身份认证平台，打通各个联盟链与可信数字身份平台间的身份认证通道，从而在不同的联盟链间就个人身份的认证达成共识，实现“先认证后上链的身份治理模式”。在此基础上，通过下

发执行监管标准、收集监管日志，落实监管措施等方式，可达到治理目的，为各类区块链应用提供基于法定身份的认证服务。



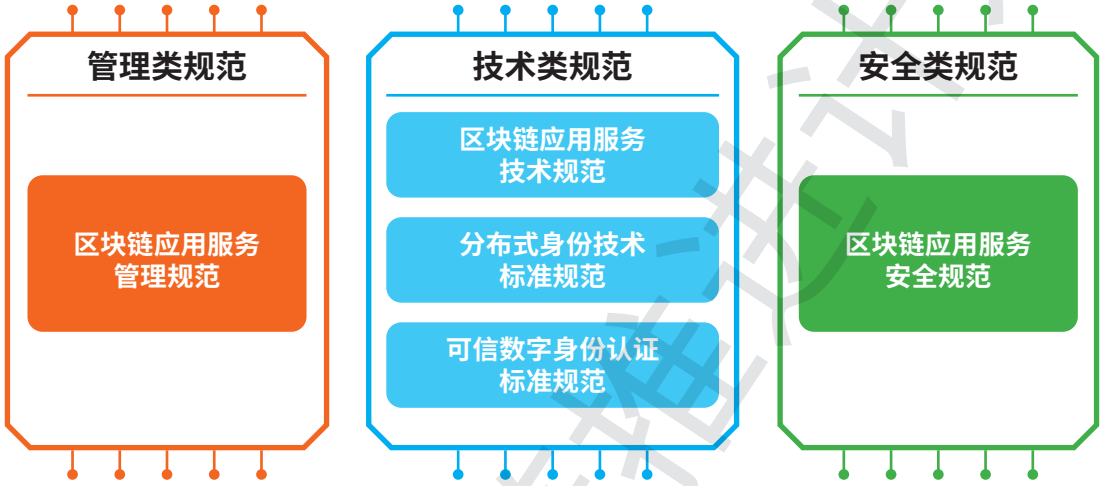
▲ 图 10 先认证后上链的身份治理模式

4.3

促进行业内部标准化发展

可信数字身份助力区块链健康发展，合法可信的数字身份是区块链产业健康快速发展的基础，是数字经济保持健康、良久发展的重要基石。可信区块链的发展必须建立在法律框架下，在可信身份管理的基础上才能健康发展。标准化是任何生态系统的一个重要方面，可信数字身份要助力区块链发展，也需要有标准化支撑，保障可信数据上链、数据上链时身份认证可信。

可信数字身份区块链标准体系分为技术类标准规范、管理类标准规范和安全类标准规范等，标准体系应覆盖区块链应用服务管理规范、区块链应用服务技术规范、分布式身份技术标准规范、可信数字身份认证标准规范、区块链安全相关规范等各方面。



▲ 图 13 标准体系的架构

基于可信数字身份的区块链应用标准体系建设，涵盖可信数字身份和区块链技术的结合，以可信数字身份作为区块链应用的重要基础能力，确保数据可信、认证可信、交互可信，以及个人身份信息上链之前确认身份数据的权威性和合法合规性。

4.4 支撑个人数据的价值流转

区块链技术对更好的实现数据价值实现过程中的可信透明、可追溯、可审计具备天然优势，为解决当前数据治理的关键问题提供了一种可行

方案。当前，单链条件下数据共享流通信息的可靠记录与溯源问责得以轻松实现。在大规模异构数据收集和跨域数据共享流通错综复杂背景下，实现跨平台、跨系统、跨区块链应用的溯源问责同样是具有挑战性的问题。因此，将可信数字身份与区块链进行融合赋能数据治理成为一个值得探索的方向，并已形成了基本思路。

▲ 图 12 数据治理赋能

(1) 提高决策数据质量

大数据价值实现依赖多源数据的整合，然而数据是否真实产生、是否被篡改以及多源数据的标准和类型不一致等问题都会影响决策数据质量。所以，数据治理需要支持大数据在其全生命周期内的溯源。

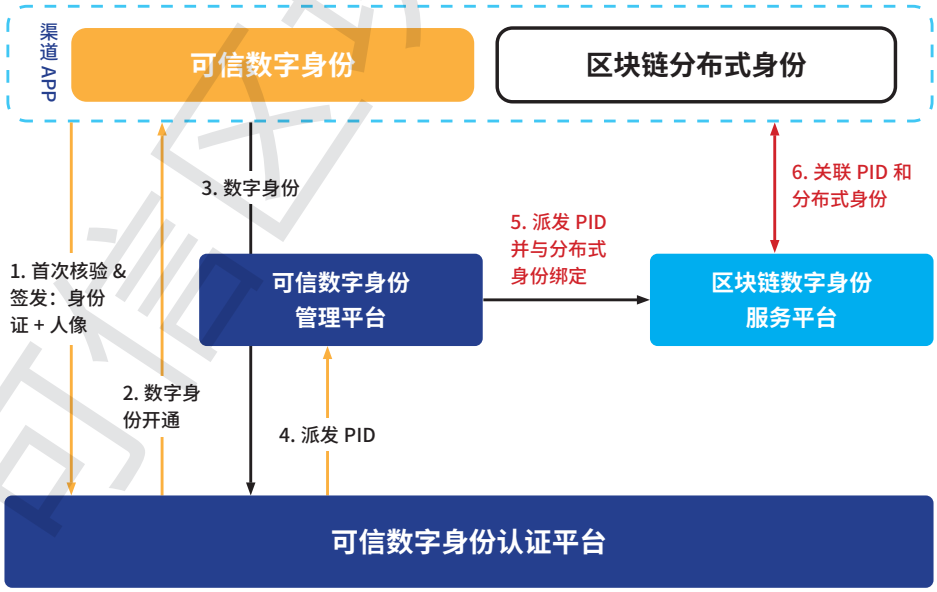
区块链支持数据全生命周期内的生成、汇聚、流通、使用、销毁的完整留痕，结合可信数字身份对各个环节参与者的身份鉴权，实现大数据全生命周期内的全通路全流程可靠溯源。

(2) 评估与监管个人隐私数据的使用

大数据应用的流通特征使数据拥有者（用户）对数据获取和共享缺乏知情权和控制权。同时，数据的收集汇聚导致数据垄断现象出现，使用户福利受损并带来个人隐私泄露风险等问题。

区块链技术的引入对数据流通全环节进行可靠监管，并通过可信数字身份帮助个人对数据的收集、开放、使用进行可信授权，以保护个人的数据权利与隐私。

4.5 提供安全便捷的应用模式



▲ 图 13 可信数字身份对区块链应用的支撑

基于可信数字身份的区块链应用业务流程如下：

（1）步骤一 - 步骤二：用户首次登录时通过渠道 APP 输入“身份 + 人像”等身份属性信息进行身份核验，向可信数字身份认证平台申请数字身份的开通；可信数字身份认证平台后台审核用户录入信息的真实性，核实后准许可信数字身份的开通；

（2）步骤三 - 步骤四：用户通过可信数字身份管理平台在业务机构进行业务操作，由渠道 APP 使用安全 SDK 对用户身份信息进行打包并上传至可信数字身份管理平台；可信数字身份管理平台将用户身份信息上传至可信数字身份认证平台进行真实身份认证，认证通过后申请派发 PID；

（3）步骤五：可信数字身份管理平台将 PID 派发至区块链数字身份服务平台与分布式身份关联绑定，并将分布式身份进行上链确权。形成“可信数字身份 + 分布式身份”的“A+B”段的数字身份应用模式，其中 B 段的分布式身份由区块链数字身份服务平台负责签发，为用户创建公私钥对，作为分布式身份的发行凭证，用户可通过分布式身份自主管理身份数据的授权开放。

场景端流程如下（以二维码应用为例）：

▲ 图 14 “A+B”模式的场景端应用

（1）用户在数字身份客户端，输入两项信息以及通过活体检测上传自己人脸图像等身份数据，完成数字身份的开通下载；同时可信数字身份管理平台获得 PID；

（2）业务系统将用户数字身份及业务信息上传至区块链数字身份服务平台；区块链数字身份服务平台为用户创建链上分布式数字身份，并将 PID 存证在分布式数字身份下，实现为分布式数字身份的可信背书；

（3）区块链数字身份服务平台将可信数字身份作为 A 段，分布式数字身份作为 B 段上传到可信数字身份管理平台，加密形成二维码返回到用户数字身份客户端，实现展码；

（4）用户向业务系统出示数字身份二维码，业务系统验证数字身份的合法性并得到用户的分布式数字身份；

（5）业务系统申请查看该分布式数字身份下的用户业务数据。用户授权后，即可在区块链数字身份平台上生成一条数据授权凭证，授

权凭证包含用户授权的证明、区块链数字身份服务平台的证明、业务系统的数据需求证明；

（6）业务系统凭数据授权凭证访问用户业务数据。

基于“A+B”段的数字身份应用模式兼顾中心化与分布式的优势，通过角色划分实现了上层监管中心化，下层应用分布式的体系架构。面向未来的基于可信数字身份的区块链应用服务，在越发深刻的社会数据治理体系当中，必然需要满足对电子政务、公共服务和互联网分域对接以及差异化服务的需求，提供“分级分域、信息隔离、信息安全、专网专用”的可信身份、可信数据、可信连接的服务。

第五章

解决方案和案例

5.1

智慧城市

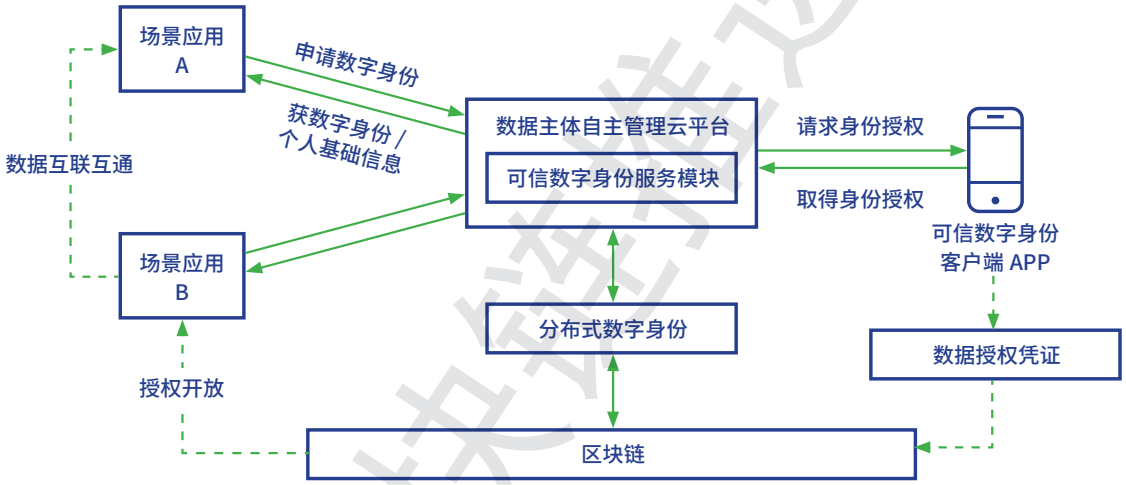
5.1.1 现有痛点及问题

智慧城市的发展依托于广泛建立的信息化应用系统，让城市生活的方方面面实现数字化，让数据用起来，激活数据价值，解决了大量政用、商用、民用领域的痛点难点问题。但伴随着应用场景的蓬勃生长，跨应用场景的流量及数据共享协作，数据价值实现过程中数据主体的获得感、数字基础设施提供方的价值补偿，新进入场景运营方的公平参与，数据治理过程的全程可控监督成为亟待解决的新问题。

通过结合可信数字身份作为统一的身份入口，为各个系统平台提供统一可信数字身份登录 API，实现通过可信数字身份直接创建账户，解决各个场景下应用系统中账户缺少“可信”的问题。结合各个身份服务下的数字身份以及个人的数据授权，将个人的身份信息、证照信息、联系方式等数据在个人授权下签发可验证凭证流转给第三方并通过区块链存证，避免在未经个人同意下泄露隐私并实现对个人信息流向的监管。

5.1.2 解决方案与场景

在很多智慧城市的场景建设中，无法简单使用传统数据归集的办法来实现数据共享和协同，要充分考虑到各数据源实体对于数据安全的顾虑。伴随着国家对个体数据隐私的保护机制日趋完善，数据账户需要考虑为个人信息主体数据确权和安全保护提供相应的技术手段。通过数据账户，利用统一的数据开放标准连接各个业务，同时通过安全可控方式对自主数据进行确权，将所有的数据协同和授权行为记录于区块链。



▲ 图 15 数据主体自主管理云平台

为解决上述问题贵州省铜仁市政府创新性的提出了数据资源管理新模式，并由政府下辖大数据公司联合有关单位提供新型数据治理基础设施——数据主体自主管理云平台，着力解决数据可信管理、数据流动可控、数据有机融合等问题。依托国家级权威法定的可信数字身份搭建的数据主体自主管理云平台，以铜仁市区域级可信数字身份为信任锚，连接起各个场景应用中的个人数据主体。

一是可信数字身份赋能区块链技术和服务，为个人用户建立本地数字身份和可信数据账户，帮助用户实现全社会领域各类数字凭证和个人

数据的统一可信管理。二是通过个人数据托管服务，解决数据安全和隐私、可控分发等一系列难题，提供一整套解决方案，有效降低数据流动成本。三是充分考虑与现有应用场景系统的有机融合方式，支持不同颗粒度的逻辑组件自由插拔拼接，规范整体解决方案中各个独立组件的数据接口，简化各类大数据应用场景的接入，助力数字生态产业链的构建。

数据主体自主管理云平台有助于打破过去个人数据的“无主垄断状态”，更易做到“以人为中心”，让数据主体拥有获得感，并让可信数字身份基础设施的建设运营方能在数据价值实现过程中实现持续可控的应有补偿，并为创新生态开发者搭建安全、简单、便捷、公平的数据使用环境，平衡数据资源价值挖掘获得的收益与存在的风险，推动数据安全可信融合共享

5.2 智慧医疗

5.2.1 现有痛点及问题

随着全国上下十几年的医疗信息化发展，全国从三甲医院到乡镇卫生院，几乎都实现了信息化。由于部分医疗信息化系统建设的年代久远，各业务系统在建设时尚未形成数据共享开放的意识。随着国家信息化建设的政策和标准的不断推新，导致各个医院成为信息孤岛，难以满足现阶段的人民就诊需求。以实名就医为例，不同医院就医标准不同，或以

身份证来挂号，或未实现实名制；不同的实名就医标准导致患者在不同医院就医时需携带不同的就诊卡，大大增加了患者负担。

国家大力发展“互联网 +”医疗健康，推动医疗、医药、医保的“三医联动”改革，其中一个基本前提是提高实名就诊率以保障医疗健康服务的连续性和医保资金的安全。可以看出，推动医保卡、社保卡、就诊卡多卡合一到脱卡就医，需要可信数字身份的支撑。

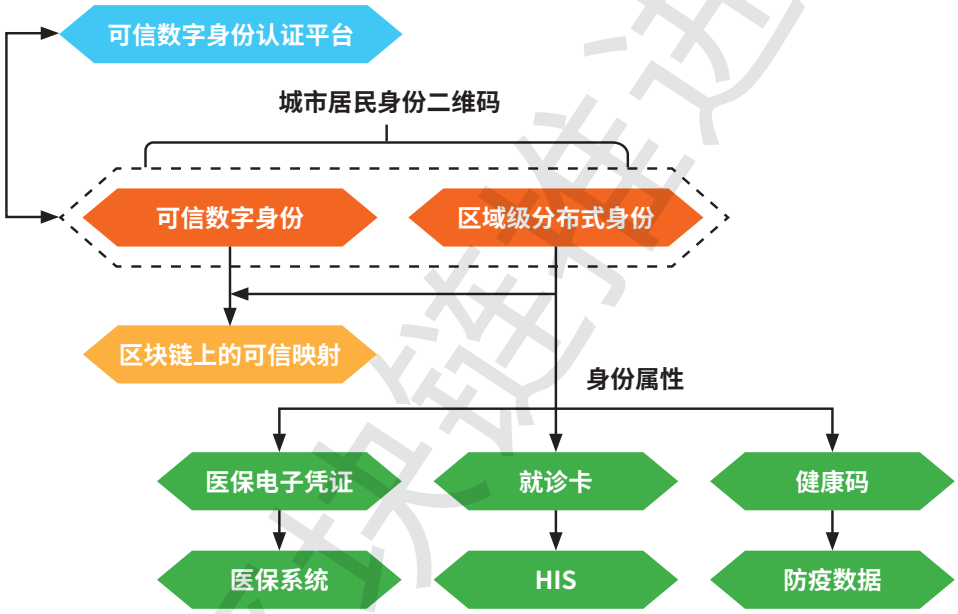
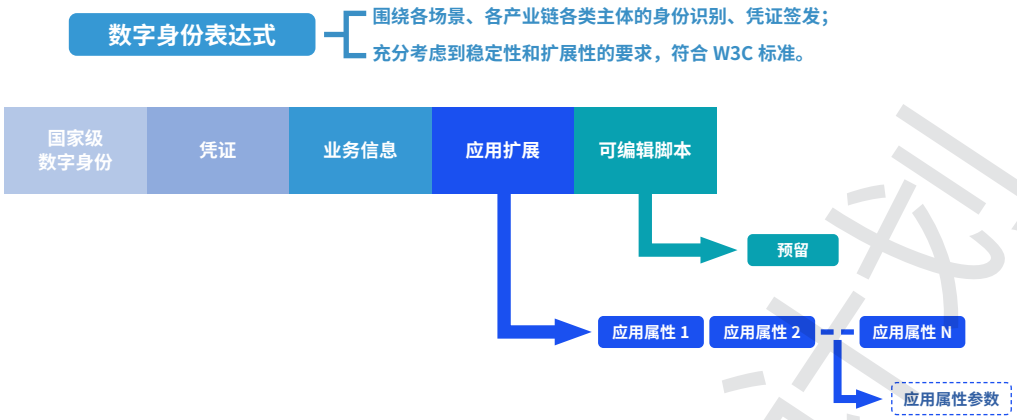


图 16 分布式数字身份凭证管理

在区块链上将可信数字身份和分布式身份进行不可篡改的关联，拥有可信数字身份验证保障的分布式身份可作为线上线下个人的医疗数据账户主索引，可打通各个医疗机构间与个人的业务数据。终端应用通过与二维码的结合，可进一步实现就医问药业务流程的便利性，实现一码就医，提升居民获得感。



▲ 图 17 分布式数字身份结构

如上图所示，这是一个标准的分布式身份结构，其核心为可信数字身份，依托国家级的身份服务，连接了线下的自然人与线上数字身份，体现了可信数字身份的权威性。凭证为个人的聚合身份，与其他各种业务凭证相绑定，可为各个凭证的场景调用提供支持。应用扩展可作为非官方的身份凭证扩展，为企业业务场景提供支持。

通过基于可信数字身份的实人实名的线上线下医疗服务受理形式，以个人数字身份作为主索引形成医疗大数据归集，对各项医疗行为进行存证记录，建立完善的个人医疗记录档案，能有效提升相关医疗机构的服务能力和监管能力。例如，医院可以便捷的调取患者的病例、影像资料来辅助诊断，医保系统可以根据 HIS、ERP 的相关医疗、购药数据进行更有效的医保控费，防疫系统可以更加敏捷的接入第三方数据，作为防疫健康码的数据补充。

5.2.2 解决方案与场景

5.2.2.1 个人健康数据在商业保险中的应用

2019 年 5 月 28 日，国家网信办发布《数据安全管理办法（征求意见稿）》，针对在中国境内利用网络开展数据收集、存储、传输、处理、使用等数据活动，以及数据安全的保护和监督管理做出规定，向社会公开征求意见。办法中第十一条、第二十二条、第二十七条再次重申了在数据收集、存储、传输、处理、使用等数据活动中，需要告知用户，并取得明确授权。

“互联网 +”医疗健康涉及大量个人健康信息的流动，尊重患者的知情权和控制权，保护用户的隐私安全是智慧医疗健康深度发展的前提。

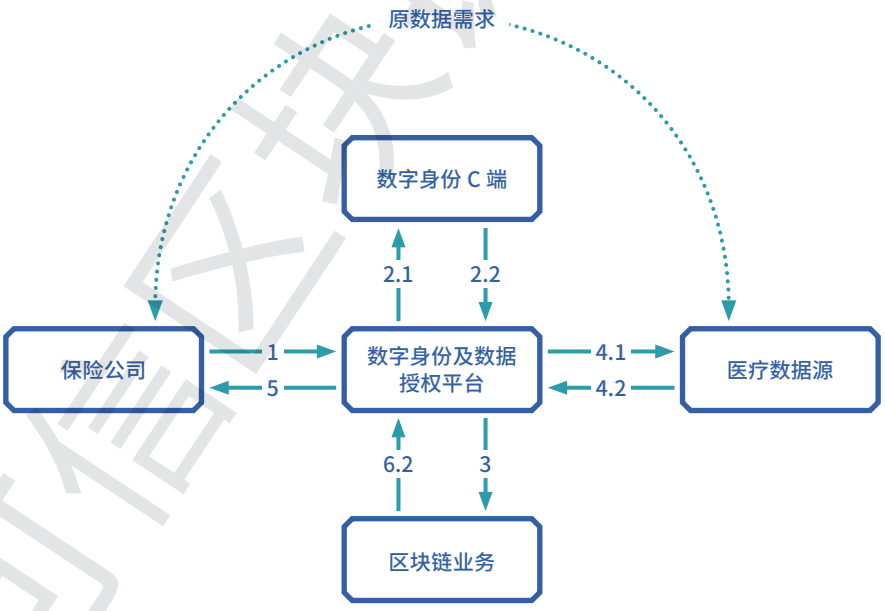
（1）知情权、控制权保护：

用户医疗数据的开放流通，应该取得用户的明确授权，让用户知道自己有哪些数据将要被访问，并告知这些数据的敏感度，数据价值、风险等等，让用户自主管理是否将医疗数据授权开放给相关的数据需求机构。医疗数据作为价值极高且敏感的数据，在整个数据流通业务流程当中，不能进行名义上的授权，而需要可信的、接近于法律证据的数据授权凭证。而这样的需求就需要可信的网络数字身份将线下的个人与线上的数据授权者可信的映射，使得授权过程能够准确的还原自然人的法律权利。

（2）隐私保护下的数据开放：

为了保护用户的隐私，通常对数据需求方的数据需求保持最小披露原则，例如只告知健康码防疫风险等级，而不会展出个人详细的健康数据。在医疗大数据的开放中，向需求方的数据开放也要秉持保护用户隐私的原则，需要先对数据进行脱敏处理；同时，在数据需求方拿不到用户详细数据的基础上，又要提高对脱敏数据的置信程度，保护数据需求方的权益，这就需要能为用户的数据脱敏结果创建可信的数据凭证，通过密码学的证明，向数据需求方证明脱敏数据的完整可信。通过为用户颁发分布式数字身份实现了数字身份与密码学关系的映射，为数据凭证签发提供了密码学的支持。

以个人健康数据在商业保险中的应用为例：



▲ 图 18 个人健康数据应用

（1）数字身份及数据授权平台：数据管理的核心，中心化的服务器与数据库。保存着所有用户的数据列表、所有用户 ID 列表、授权记录列表、数据访问记录列表。向上对接业务需求和用户，向下对接区块链和数据源。

（2）保险公司：数据需求方是业务场景、B 端业务系统或客户端。

（3）数字身份 C 端：通过可信数字身份的二维码展示以及在线的数据管理体现了个人数据主体在数据流通体系中的意志，因为数据通过用户产生，所以原则上用户天然具有数据的所有权。

（4）医疗数据源：数据运维方，归集有大量医疗数据，能够提供数据治理服务，通常是数据平台。也可能是政府部门或其他的业务系统。

（5）区块链业务：用于存证数据列表、数据授权、用户列表、访问记录；并且区块链作为用户分布式数字身份的核心，管理着公私钥体系。

（6）流程实现

a. 数字身份 C 端发送一条授权记录请求，根据配置的权限申请规则，申请固定时间和次数；

b. 数字身份 C 端在前端收到数据访问权限申请消息，点选同意；

c. 保险公司通过数字身份及数据授权平台代理接口访问数据；

d. 数据授权记录及数据访问记录上链；

e. 平台访问数据源接口，通过数据源接口获取数据；

f. 返回给数据需求方。

5.2.2.2 可信数字身份在医疗受理案例中应用

医疗健康码可作为可信数字身份在医疗行业推广的区域级通用二维码，此二维码绑定国家级可信数字身份，以法定身份为根，支持多码聚合，可关联个人银行卡、电子社保卡、医保电子凭证以及电子居民健康卡，从而提供多码、多卡合一的二维码服务，作为在医疗机构就医时的唯一身份凭证和支付报销凭证时的应用数据载体。

医疗健康码在就医过程中的应用场景主要有预约挂号、就医、缴费、取药、住院、手术、检查检验报告查询、电子病历查询、费用清单查询、开具电子发票、授权信息共享、信息上链存证、远程会诊调阅病历等全流程信息调用覆盖。

以区块链技术的特性把患者所有相关就医信息形成个人账户，并经安全加密处理进行上链存证，形成不可篡改、分布式存储的区块信息，经授权后可调阅共享。医疗健康码不仅包括个人信息，还通过网络数字身份的多码聚合，将社保信息、医保信息、支付信息、健康档案信息形成完整的健康信息账户，以区块链良好的追溯技术对个人健康可做出全面覆盖。在数据共享方面，患者无论何时何地就医均可在授权许可后调阅其健康档案，并实现异地远程病历共享，更便于实现患者异地就医、报销、支付等需求

在个人健康类商业保险中，可与健康类商业保险系统关联，为个人参保和商业保险报销提供授权许可的可信病历信息，使个人能快速参保、快速报销，为广大居民提供更便捷高效的保险服务、就医服务。

以患者在院外购买处方药的场景为例。电子处方共享平台系统对接各医疗机构 HIS 系统。由各医疗机构医生开具处方后，通过电子处方共享平台的处方审核后，向院外流转，患者在药店出示可信数字身份码或医疗健康码进行扫描交费，药店服务人员给予发药。

在交费过程中，通过一次扫描，可一步完成自费支付或医保报销支付，减轻患者多次出示二维码的繁琐。

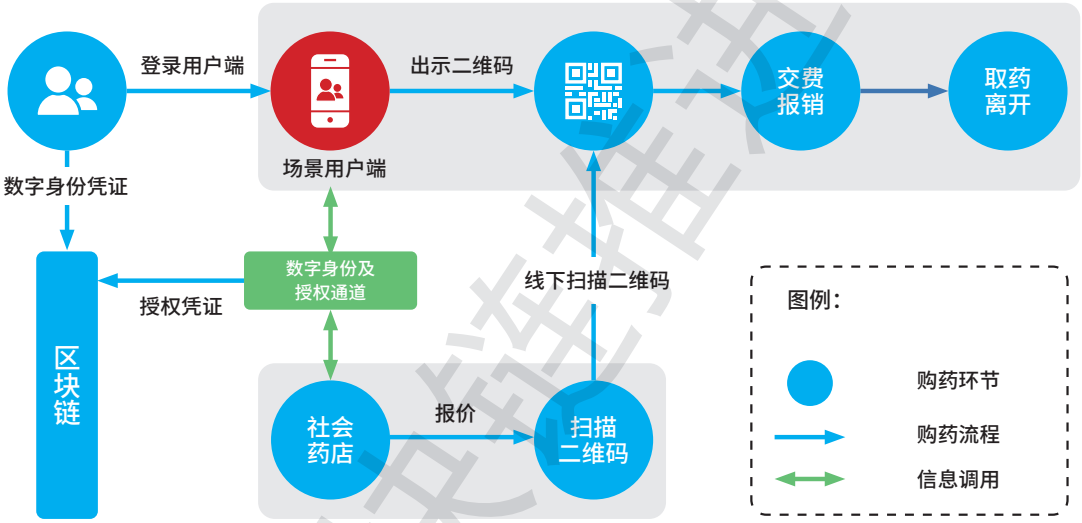


图 19 “一码就医”

在整个处方流转过程中，各环节信息数据上传通过调用分布式身份凭证进行信息存证，在监管过程中，可以对任一环节的信息进行追溯监管。形成的个人信息数据，进行数据脱敏、标准化后形成个人数据账户的信息数据凭证。

5.3 智慧征信

5.3.1 现有痛点及问题

随着国家征信系统的健全，信用记录在个人生活中发挥的作用越来越重要。申请信用卡、办贷款、期货开户，出国留学等等，“良好的信用记录”成为参考个人信用的重要条件，从某种意义上来说，个人信用记录已成为一种无形的财富，对个人的生活产生不小的影响。

为了推动社会信用机制建设，最大限度保护当事人的合法权益，最高人民法院发布了《关于限制被执行人高消费及有关消费的若干规定》，第三条中提到，针对失信人被限制高消费后，不得有以下的行为：（一）乘坐交通工具时，选择飞机、列车软卧、轮船二等以上舱位；（二）在星级以上宾馆、酒店、夜总会、高尔夫球场等场所进行高消费；（三）购买不动产或者新建、扩建、高档装修房屋；（四）租赁高档写字楼、宾馆、公寓等场所办公；（五）购买非经营必需车辆；（六）旅游、度假；（七）子女就读高收费私立学校；（八）支付高额保费购买保险理财产品；（九）乘坐 G 字头动车组列车全部座位、其他动车组列车一等以上座位等其他非生活和工作必需的消费行为。被执行人为单位的，被采取限制消费措施后，被执行人及其法定代表人、主要负责人、影响债务履行的直接责任人员、实际控制人不得实施前述行为。因私消费以个人财产实施前述行为的，可以向执行法院提出申请。

在 2020 年 8 月份，中央精神文明建设指导委员会印发《关于开展诚信缺失突出问题专项治理行动的工作方案》，针对失信人员提出“继续依法用好失信惩戒措施，严厉惩戒拒执违法行为，形成对逃债行为的高压态势”的要求。

失信人员名单需要公开，才能更好的配合失信人高消费限制，促进社会整体诚信发展；但同时，失信人员名单也应考虑隐私性，当某人欠款没有履行相关责任时才认定为“失信人”。履行相关责任时，应当从失信人名单中除名，不被限制。公开和隐私从来就是一对矛盾体，若不能很好的驾驭这对矛盾体，很容易造成两个极端化，要么信用过度泛化或滥用，要么联合惩戒的效力大打折扣。

基于可信数字身份，结合区块链技术构建失信人员联合惩戒机制。区块链具有可溯源、不可篡改的技术特点，再结合可信数字身份技术，将是失信人员数据公开透明的理想载体。

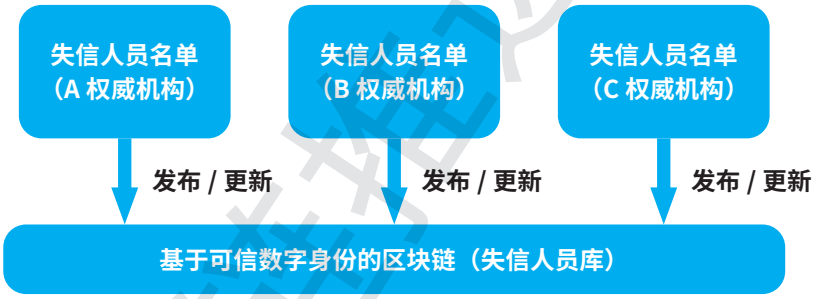
首先，可信数字身份是将个人真实身份信息进行脱敏及去标识化处理后与法定身份证件一一映射的数据文件，能够在不泄露身份信息的前提下实现在线身份认证。可信数字身份不包含个人敏感信息，就算被不法分子盗取数据，也不用担心真实身份信息的泄露。如果将失信人名单，放置在基于可信数字身份的区块链上，既能确保某信息真实代表某个人，又能将个人身份信息进行隐私化处理，做到隐私保护下的信息公开。

其次，失信人员名单的产生也是一个多部委、多机构联合协作的过程。基于可信数字身份体系，各机构产生的数据有了统一化的标准。数据具备了隐私性的同时，也具备了更好的串联性，能提升信息数据更大的价值。

机构在查验失信数据时，借助基于可信数字身份的区块链应用，不仅确认了被查验者的真实身份信息，更保护了其个人信息的私密性，符合国家《个人信息保护法》的规定，从而构建起一个具有隐私保护能力的、低成本的、互信互联的失信人员联合惩戒机制。

5.3.2 解决方案与场景

1. 失信人员名单数据上链



2. 验明客户身份及查验失信名单

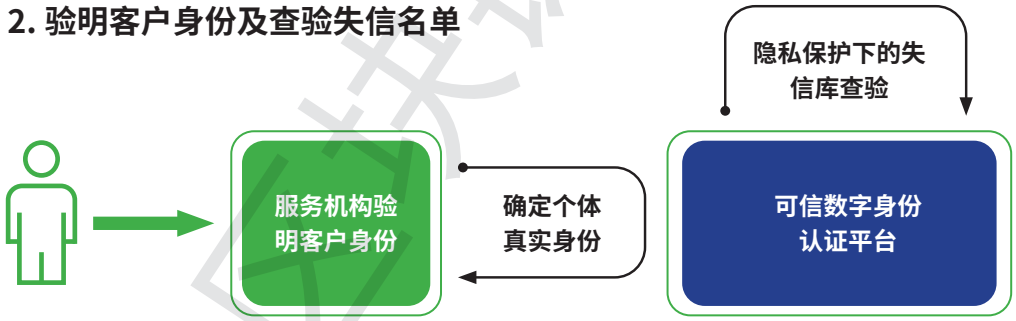


图 20 基于可信数字身份的区块链联合惩戒思路

如上图，先将失信人员名单上链，由于区块链中的信息保密性，且不存明文身份信息，即使数据泄露，也不用担心身份信息暴露问题。当失信人员前往某服务机构要求提供某项高消费时，服务机构通过可信数字身份认证平台验明其个体身份，并通过失信人名单区块链进行密文查询，一旦发现其为失信人员则通知服务机构进行限制。

利用区块链互信机制，支持多方基于可信数字身份建立跨部门、跨区域的信用联动机制；从个人隐私保护角度出发，在最大程度保障公民基本权力的基础上，构建联合惩戒体系，推动社会信用机制建设。

5.4 智慧金融

5.4.1 现有痛点及问题

金融行业参与者群体广泛，不同类型的金融机构其资质、资本、资源等禀赋各异、互补性较强，因此通常是以同业合作的对等形式共同设计产品或开展业务，如银银、银证、银保合作等，天然形成了多方参与、共享资源、协同合作的分布式商业模式。因此，金融行业对数据的真实可信可验证以及协同协作有着直接需求。

传统金融机构需要投入大量的人力物力，对客户信息进行收集、整理、验证等。具体业务场景中，金融活动的第一步通常是对客户进行KYC（Know Your Customer）核验，包括核实客户基本身份信息、交易的实际受益人身份、确认客户目前的业务及风险状况等，有时还需要调查交易资金来源、客户关联方等，因此，需要客户提供由权威机构发行的、具有法律效力的身份证明资料，并对相关身份证明资料做复印、影像留存。

由于金融机构间身份信息、风险征信信息等数据无法互通，客户跨地域跨场景的金融需求受到极大限制，用户需要在不同机构重复开户，客户和机构都会面临明显的操作成本和运营管理成本。在市场推出丰富的金融产品之际，急需解决的是跨机构的基础建设，其中，金融身份的互通互信是普适性较广的业务起点，作为各类金融业务的基石，涵盖了开户、征信、信贷等诸多场景。

金融领域作为区块链技术在实际场景落地的重要领域，将受益于可信数字身份体系的建立与完善。

可信数字身份为基于区块链的解决方案在金融 KYC 业务场景下的应用提供了新的实现模式，金融机构可以为每个客户（无论是个人客户还是企业客户）创建具有唯一性的分布式身份标识，通过一次性的信息采集，将客户可信数字身份（对应着现实世界的真实身份）与在区块链上的分布式身份标识进行绑定，从而完成现实身份与数字身份的关系映射。

统一 ID 及可信数字身份的背书保证了不同的金融业务可以在此基础上实现多个 ID 匹配和管理，大大降低了业务平行扩展的难度。建立在区块链分布式架构上的信任更加稳定，由于跨机构之间客户信息互联互通会受到严格的合规监管，以及面临安全和隐私保护的挑战，可信数字身份将为金融领域的安全性和效率提升提供保障，有助于不同金融参与方基于区块链在可信具体业务上协同发展，为更广大的用户提供更可靠便捷的服务，提供更全面的监管手段，在合法合规的基础上发展开放的金融业务。

5.4.2 解决方案与场景

5.4.2.1 可信数字身份应用于跨金融机构开户场景

跨机构开户是金融客户身份互通互信的一个典型案例，跨机构开户包括银银、银证合作等业务场景以及跨境业务场景。

目前金融行业的开户流程中，必须由客户和签约机构之间建立点对点的验身和签约关系，具体形式包括面签和在线验身等，所对应的账户类型和等级会有所不同，如在线验身通常对应开通二级账户，客户在不同机构开户和办理业务需要重复进行 KYC。

常见的跨机构开户业务，主要使用“见证开户”模式，一般流程是：首先，客户携带资料，到代理银行网点进行见证开户。代理银行网点需要面见客户，由柜员手动验证客户资料。接着，若验证通过，代理银行会在符合个人数据保护规范的前提下，将资料同步到合作机构进行开户。最后，合作机构收到材料后，二次审核客户资料，如审核通过，则开立客户账户，并通过电话回访进行激活。

实际操作中，这种流程有以下痛点：

(1) 开户信息非数字化，用户耗时耗力，纸质文件在见证方和实际处理方之间传递，管理成本高，不便于机构进行信息获取、持久储存、数据分析。

(2) 跨机构的信息交互存在着复杂多变的挑战。例如，数据需要进行脱敏；见证过程中，需要用户手签申明具体的授权；审核过程中发

现问题，可能需要用户补充各类证明。

(3) 身份验证与资料真实性验证存在着诸多问题。例如，一旦数据在跨机构之间传输，申请人真实性核验是无法由传输链条上的后续接收方独立完成，接收方只能选择信任发送方，一旦数据在传输过程中被篡改、或发送方恶意修改，接收方难以验证其真实性。

(4) 机构对客户身份信息应用于其他商业用途，缺乏有效的授权和监管机制。

采用基于可信数字身份的区块链解决方案，金融机构只需进行一次性的信息采集，为客户创建具有唯一性的分布式身份标识，并完成现实身份与数字身份的关系映射。基于分布式账本原理，金融机构通过部署节点的方式完成已创建的客户数字身份档案数据同步。当客户需要办理业务时，仅需出示分布式身份标识，并通过可信数字身份认证机构对实名或实人认证以证明对该标识的所有权，即可授权金融机构获取该客户的身份数据，完成 KYC 认证。

当客户信息发生变更时，可通过手机 APP 程序或金融机构渠道，对数字身份区块链系统上已采集的信息进行修改，完成金融机构间的变更信息同步。用户的所有数据上传、变更、授权查看等操作前对身份的认证记录均可上链。

方案的优势在于：

一是更加可靠的 KYC。之前，对于多方合作的机构，要么只能盲信对方，要么缺乏互信，极大地限制了业务的扩展与深化。在此方案中，

多机构之间可以实现基于链上不可篡改公钥的互信。

二是防止信息篡改。之前数据在线上和线下的传输过程中可能会出现篡改，难以保证可信。这一问题在此方案中得到了解决：所有数据以凭证形式留存，以数字签名和链上存证双层保证其可信。

三是用户对数据行使主权，一切数据的调用需要用户授权。用户授权中，明确了授权机构、目的、有效期。这使得任何一方对凭证的私下存储和窃取失去了意义，因为过期或目的不符的授权数据将无法通过智能合约的可信验证，极大地提升了数据隐私的保护能力。

5.4.2.2 可信数字身份助力金融治理案例

数字身份还可以为金融治理提供可信的运作基础，我们分享一个实际的案例。

2019 年，为稳定金融市场，化解 P2P 机构引发的金融风险，深圳市互金协会发布《深圳市网贷机构良性退出指引》，要求决策事项在网上投票表决。投票表决流程涉及身份验证、债权确认、公告送达等金融级安全要求和技术，投票过程中，投票者的身份和投票选择应该受到保护，投票者可以验证自己投出的选票是否被正确计入结果，同时计票结果公开可验证，而普通投票平台难以满足需求。

传统投票方案中，投票的隐私性和正确性大都需要依赖计票者的信誉，计票者拥有极大的权利。当计票者的可信度受损时，投票结果也会遭到质疑。由于投票结果的验证机制和投票过程全流程的监督机制都不够完善，冒充、抵赖、篡改的情况时有发生，当发生纠纷时，由于数据

未能形成有效证据链，平台难以证明投票是由投票者自主作出的真实意愿选择且未经篡改。

同时，传统投票方案缺乏隐私保护机制，投票人的隐私信息得不到保障。选票中包含敏感身份信息和选择信息，可能会直接影响投票人做出真实选择的意愿，从而影响投票结果的公平性和有效性。

为解决上述问题，深圳市互联网金融协会联合微众银行共同搭建“网贷机构良性退出统一投票表决系统”，运用区块链技术解决网贷机构清退流程中的互不信任问题。

该系统通过人脸识别和数字证书认证方式，确认出借人的身份，为每一位用户生成系统内独一无二的数字身份 ID。在确认用户身份及用户授权的前提下，将投票信息填入数字身份 ID 对应的凭据区，为每位投票用户生成可验证凭证（Verifiable Credential），并将凭证摘要 Hash 上链。同时，为投票人分配证书及密钥，对投票数据进行加密后使用私钥加签，作为投票的安全认证机制，防止抵赖和冒充。投票联盟链上各机构对 Credential 的数据内容项进行验证，在无法破解用户 WeID 并反向推出用户真实身份的情况下，独立地抽取投票内容信息，并通过链上智能合约统计投票结果。

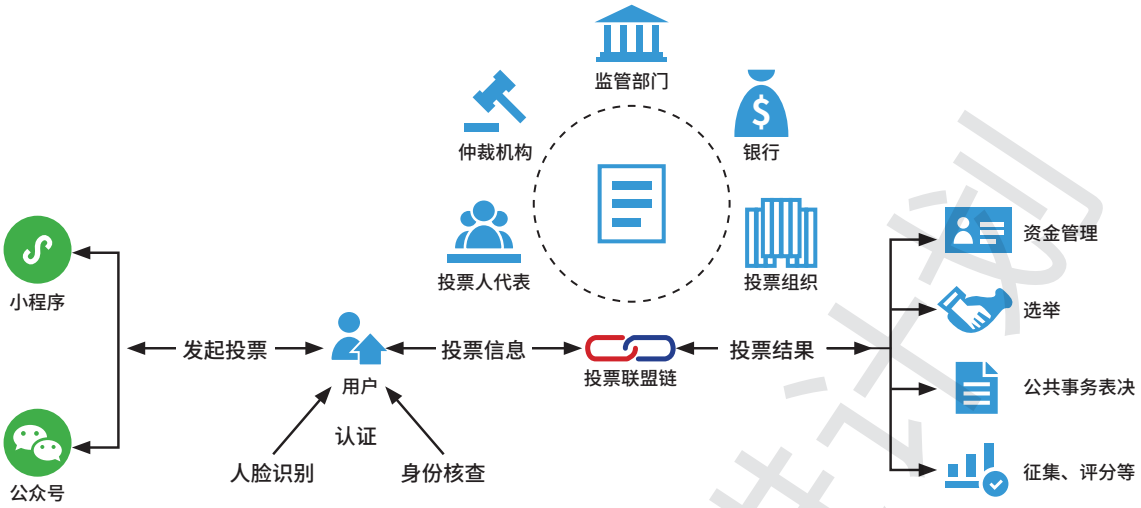


图 21 网贷机构良性退出统一投票表决系统

此外，平台引入基于区块链的存证鉴证体系，对待表决文件和投票内容、结果进行链上存证、鉴证，形成有效证据链，防止因信任问题导致的法律纠纷。监管机构、仲裁机构以节点形式加入区块链，可以对投票过程全流程进行验证与监督，包括选票内容是否合法、所有投票者的投票交易过程是否正确、所有计票者的登记与统计过程是否正确、计票者最终公布的计票结果是否可信等等。

此过程既可防止投票过程中存在他人伪冒的情况，又避免了将投票人的全部敏感信息上链，在保护用户隐私的同时，避免了投票冒充、抵赖、篡改等情况发生，确保投票结果公正性。投票联盟链上各机构对用户凭据包含的各内容项进行验证，在无法破解用户数字 ID 并反向推出用户真实身份的情况下，独立地抽取投票内容信息，并通过链上智能合约统计投票结果。

该方案还有以下优势：

首先，更加明晰的用户授权。此方案中，可信数字身份为用户提供了唯一身份标识以及基于身份认证的个人授权，授权记录在链上留存，可防止投票过程中存在他人伪冒的情况。

其次，链上存储的信息可追溯，不可抵赖、篡改。一旦发生问题，可追溯源头，并进行追责，支持进一步的仲裁、司法需求。

最后，除了投票过程参与者，第三方无法获知投票的具体细节。联盟链上各机构对用户凭据包含的各内容项进行验证，但无法获得用户的全部身份信息，也无法根据用户身份 ID 反向推出用户真实身份，从而在确保投票结果真实可验证的情况下，保护了用户的隐私安全。

第六章

总结和展望

区块链的发展，已经由以比特币为代表的区块链 1.0 时代和以智能合约为代表的区块链 2.0 时代，迈向区块链 3.0 时代，进入创新应用的深水区。区块链技术在政务数据治理领域、数字城市建设领域、金融数字货币领域等都取得了非常瞩目的成绩，为区块链在电子存证、个人授权、电子发票等为代表的行业落地应用、发展奠定了基础。基于真实身份核验的可信数字身份在赋能区块链应用之后，更是将区块链应用向行业的纵深领域推进到深度融合发展阶段，并已在众多行业区块链应用领域建立起生态圈。

然而，区块链技术自身尚处于快速发展的初级阶段，面临的风险还依然存在。基于可信数字身份的区块链服务以一种新的角度为区块链的合规化提出了解决思路，可信数字身份作为区块链在用户侧的可信入口，在个人、企业、机构间提供无差别信任传递服务，为建立多元、开放、共享、均衡和包容的数字经济合作关系提供底层支撑。

“可信区块链推进计划”数字身份项目组将以国家政策为导向，以市场为驱动、以企业为主体，围绕可信数字身份与区块链的核心环节进行技术研究及标准建设，助力构建基于可信数字身份的区块链产业生态。

未来，数字身份项目组将继续加强可信数字身份与区块链的应用实践探索，继续贯彻第一阶段“可信数字身份赋能区块链应用”的工作思路，推动产品及服务落地，打造行业样板项目，加强业内外沟通交流，促进产业上下游发展，助力行业治理与监管。在此基础上，项目组将开展第二阶段“区块链赋能可信数字身份”的研究工作，加强身份信息的链上流转，积极研究个人身份数据的链上可信流通方式，实现区块链技术促进可信数字身份在多领域多维度应用创新的目标。

可信区块链推进计划

地址：北京市海淀区花园北路52号　邮政编码：100191

联系电话：010-62300249　传真：010-62304980

网址：www.trustedblockchain.cn