中国移动 China Mobile

区块链+智慧城市
白皮书

中国移动
2019年6月

中国移动 China Mobile | 5G++

目录

CONTENTS

概述
SUMMARY

- **区块链为智慧城市发展带来新机遇：**

  新型ICT技术将驱动下智慧城市发展将迎来新的变革，在构建智慧城市过程中，我面面临着城市全域数据感知对城市数据采集与传输提出了更高要求、海量设备接入使得身份认证和通信安全成为智慧城市安全隐患、如何保护智慧城市采集数据的隐私等挑战与问题。区块链技术正在重塑社会信任，能够有效的解决对等多实体共享信任问题，给智慧城市发展带来新机遇。

- **智慧城市区块链技术应用重点场景：**

  从民生服务（智慧医疗、智慧教育）、城市治理（智慧政务、智慧交通、公共安全）、产业经济（智慧物联网、智慧工业）、生态宜居（智慧能源、智慧新零售）四个维度对区块链技术在智慧城市中的重点应用场景进行讨论。

- **区块链技术在智慧城市的应用路径：**

  区块链技术在智慧城市的应用落地是一项复杂的系统工程，需要构建安全、可信的智慧城市数据共享分享基础设施，构建城市级的多层次区块链公共服务平台，以政务服务创新为重点突破，推动区块链应用的逐步落地。

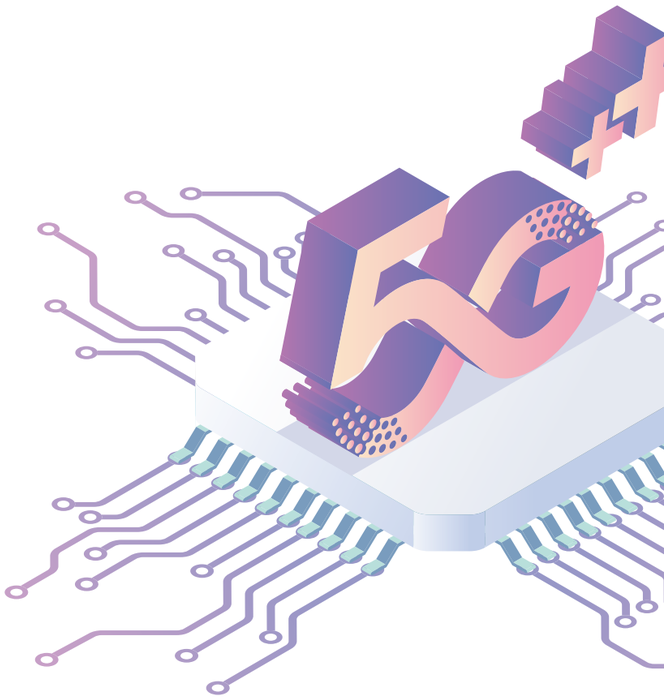
- **中国移动智慧城市区块链核心产品及技术解决方案：**

  基于区块链技术，中国移动推出数据流通及共享以及数字身份认证两个智慧城市应用场景技术方案。

- **智慧城市区块链技术发展建议：**

  后续智慧城市区块链技术应用发展过程中，我们建议高度重视区块链底层架构和基础设施，优先搭建区块链基础服务平台，与大数据、人工智能、物联网等技术进行充分融合，进一步完善监管和标准体系。

中国移动为区块链技术赋能智慧城市提供产品、支撑、服务以及运营能力。



一、区块链为智慧城市发展带来新机遇

1.1 智慧城市愿景与目标

1.1.1 智慧城市发展愿景

智慧城市主要包括政府、企业和公众三大类参与主体，由于出发点和侧重点不同，目前尚无权威定义。我们认为，新型ICT技术将驱动智慧城市发展的变革，智慧城市应是基于5G网络、边缘计算、大数据、人工智能等核心能力所打造的城市神经网络和大脑系统，通过深层感知全方位地获取城市系统数据，通过广泛互联将孤立的数据关联起来、把数据变成信息，通过高度共享、智能分析将信息变成知识，把知识与信息技术融合起来应用到各行各业形成智慧。最终实现城市的全域感知、智能触达、数字运营和智能决策，助力城市管理数据的协调共享和信息系统的互联互通，建设透明高效的在线政府、精细精准的城市治理、融合创新的信息经济、自主可控的安全体系、无处不在的惠民服务。

1.1.2 智慧城市发展面临的挑战

智慧城市建设的本质，是数据的采集获取、共享交换、融合处理，以及基于此的业务协同和智能服务。在构建智慧城市过程中，我们遇到了跨行业跨领域的复杂系统交织问题，特别是因为类别、行业、部门、地域等原因被孤立和隔离的数据资源的开放、交换、融合、共享与安全，仍是亟待解决的挑战。

城市全域数据感知对城市数据采集与传输提出了更高要求。城市数据的采集涉及城市生活方方面面，从广义角度看，新型智慧城市的全面感知内容应该包括对城市综合管理相关的公共部件和公共环境的信息感知、对家居生活场所和环境的信息感知、对市民教育和健康状况的信息感知、对公众有潜在安全威胁的特殊人群活动的信息感知、对大众网络舆情的信息感知等 。目前智慧城市的感知体系从感知方式、传输处理等多个角度远不能满足城市信息获取的需求。从未来发展看，物联网将成为智慧城市的“神经末梢”，实现信息感知数据采集。

海量设备接入使得身份认证和通信安全成为智慧城市安全隐患。涵盖广阔的智慧城市涉及到各种接入设备，这些设备的身份可信度辨识、访问控制以及设备之间的互联互通是多方协同的安全基础，也是实现安全可信的数据交换的关键。随着物联网技术在智慧城市领域的广泛应用，设备身份认证主要使用的非对称密钥解决方案存在着证书批量配置效率低、不同CA机构之间实现互通难等问题，极大的限制了安全认证的实效性以及设备的互联互通，特别是涉及数量巨大的网络设备和终端设备接入场景下的安全隐患问题。

如何保护智慧城市采集数据的隐私仍然是一个亟待解决的问题。数据隐私是数据所有者的基本权利，未经授权不得披露，而在日益数字化的城市生活中，由于数据隐私保护措施的欠缺，智慧城市建设过程中不同的参与方将会接触到各种各样的数据隐私，特别是公民个人信息、用户行为数据等隐私数据的泄露，对政府和企业公信力以及公民个人利益都将是极大的影响。如何在不牺牲隐私的前提下实现数据资源的充分融合、共享，是智慧城市建设亟待解决的一个课题。

1.2 信任与协作是可信智慧城市的基础

智慧城市覆盖的行业众多，公安、交通、教育、医疗等领域均承载着大量的敏感信息，这些涉及公民、企业、政府的敏感信息一旦泄露，将对公民个人权益、企业商业利益、国家信息安全带来不可估量的危害。但是，从另一角度来看，建设智慧城市，一定要实现数据的共享和融合，特别是教育、医疗等关乎民生的重点行业，通过数据共享互通、创新应用，提升公民获得感。

对数据的安全和隐私保护是最基本的生存本能，在没有生存基本保障的情况下公民、企业、政府都会倾向于采取保守、封闭、简单的方式来规避风险。可信智慧城市的建设，以信息的可信安全以及信息的流通安全为基础，以区块链为技术手段，根据智慧城市参与方的利益诉求共同制定规则并遵守，创建一个安全的环境，在各参与方对环境的安全性认可的前提下，打造合作、协作的高度协同城市生态，促进城市高效、透明、安全、可信运转。

1.3 区块链技术的特点及带来的机遇

1.3.1 区块链的概念及特点

区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等成熟计算机技术的有机组合。区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学技术保证数据传输和访问的安全、利用自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式 。

区块链技术的特点包括：

•**去中心化：**由于使用分布式账本存储、不存在中心化的系统或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中的合法节点来共同维护，不依赖额外的第三方管理机构或应用系统；

•**防篡改：**信息经过各节点的验证并添加至区块链后，就会永久地存储起来，并安全地在全网传播和同步，篡改成本极为高昂（除非能够同时控制住系统中超过51%的节点），通过节点准入和信用评价体系，可有效防止恶意的数据篡改；

•**透明性：**合法节点和参与者可以通过公开的接口查询区块链数据乃至开发相关应用；

•**隐私性：**通过加密技术和账户管理体系，用户的身份信息或其他隐私信息可以得到较好的保护；

•**自治性：**基于协商一致的共识机制，系统中的所有节点能够安全地交换数据，基于公平规则和公开数据建立信任体系，摆脱了单纯的对特定节点、实体或“人”的信任，构成了既自制、又合作的信任基础设施；

•**自主性：**借助区块链数据的共识、信任机制，区块链上部署的智能合约可不受干扰地自主执行，避免了传统合约在履约过程中不受控、难执行的问题。

1.3.2 区块链的核心技术

1.3.2.1分布式账本

分布式账本（Distributed Ledger）是一种在网络成员之间共享、复制和同步的数据库。分布式账本记录网络参与者之间的交易，比如资产或数据的交换。

1.3.2.2加密算法

利用密码学的方式保证账本数据传输、存储和访问的安全。

1.3.2.3共识机制

共识机制是区块链各参与方在预设规则下，在各个节点之间对某些数据、行为或流程达成一致的策略和方法。多节点之间采用共识算法在生成和更新账本，保证各节点对每个区块中交易有相同的认可（共识）。

1.3.2.4智能合约

智能合约使区块链具备了可编程的特性。使用可编程脚本形成的智能合约也可以像交易一样在各节点存储和共识，智能合约可在条件满足时被调用，用来操作账本中的交易。

1.3.3 区块链为智慧城市发展带来的新机遇

区块链技术借由自身核心技术特点，正在重塑社会信任，成为维系智慧城市有序运转、正常活动的重要依托，能够有效的解决对等多实体共享信任问题，在互相信任的基础上，智慧城市的发展将会更顺畅。

智慧城市发展，必将加大公共数据资源——特别是政务数据资源——的公开、共享、利用，区块链技术的天然优势可以分离数据拥有权和使用权，促进不同政府部门、不同行业、不同企业协同推进数据融合、共享，为智慧城市数据融合共享需求提供解决方案。

互联网正在成为各行各业的基础设施 ，而作为第二代互联网——价值互联网——重要价值传输协议的区块链技术，也将成为智慧城市的基础设施，特别是在金融行业底层基础设施重构系列工程中，自主可控的区块链技术，将成为核心竞争力。

此外，区块链技术所特有的分布式数据存储、加密算法、共识算法、智能合约等核心技术，使得区块链技术在智慧城市的身份认证、公共事业管理、交通、园区、环保等细分行业和场景都有可能发挥重要的作用。

二、智慧城市区块链技术应用重点场景

推进新型智慧城市建设，是党中央、国务院为提升城市管理服务水平、促进城市科学发展作出的重大决策，是实施网络强国战略的重要抓手。新型智慧城市建设的必备要素如图 1所示。

图 1 新型智慧城市建设必备要素

智慧城市顶层设计指南中建议将智慧城市一级业务划分为“民生服务”、“城市治理”、“产业经济”、“生态宜居”四大类。从区块链技术特点及功能角度，当前区块链技术在新型智慧城市建设中的应用场景可归纳为四类：一是数据安全与隐私保护，二是数据追溯，三是数据存证与认证，四是数据低成本可靠交易，聚焦在智慧城市共享支撑平台的数据流通、管理领域内。本文将结合区块链技术特点从设计指南的四个角度，探讨区块链技术的重点应用场景。

2.1 民生服务

区块链技术在民生服务领域的重点应用场景包括：智慧医疗、智慧教育。

2.1.1 智慧医疗

区块链技术对原生数据加密存证、隐私保护、授权分享、时间戳溯源、资产确权等技术应用，助力医疗信息化发展，落地医疗数据存储与共享、医疗信息溯源、医疗保险改革等应用场景。

医疗数据存储与共享：医疗数据包括患者、医生、医院、诊疗等数据，这些数据大多是隐私数据，一方面要保证数据安全存储，另一方面还要实现数据的授权共享。区块链技术去中心化、分布式存储的技术特点，保证了数据来源的权威和存储的安全，匿名性和完善的授权策略，确保数据在分享过程中不存在泄露的风险。

医疗信息溯源：区块链技术在医疗信息溯源领域主要应用于药品鉴别以及医疗信息监管与审计。区块链记录不可篡改、共享安全可靠的属性，可以有效实现药物防伪；区块链防篡改、可追溯的技术特点，可以精准定位医疗信息的全生命周期追踪溯源，包括医用物资供应链监管、药品溯源、医疗信息审计等。

医疗保险改革：区块链记录不可篡改、共享安全可靠的属性，使得区块链技术同样可以应用于医保行业，例如保单数据存储共享、医保核查控费、医疗健康档案上链存储，保障数据的不可篡改、不可丢失，杜绝隐私泄露，利用智能合约实现医疗保险的快速赔付。

2.1.2 智慧教育

与智慧医疗领域类似，利用区块链技术的独特优势，构建智慧教育领域教育数据安全存储与共享、教育业务流程优化以及教育智能合约等应用场景。

教育数据安全存储与共享：教育数据包括学生、老师、教育机构等数据，利用区块链分布式账本技术，可将教育数据存储在不同区块中，链上的节点通过特定的协议实现数据资源的授权共享，解决教育领域数据鼓捣问题。

教育业务流程优化：利用区块链技术去中心化特点，构建去中心化的教育系统，改善传统服务及资源被学校和政府机构垄断的局面，探索具备资质的教育机构开展教育服务及颁发授予相关认证的可行性，实现正规教育与社会教育资源的互补，促进教育体系改革。

教育智能合约：利用区块链的智能合约技术，构建高效、智能的网络学习社区，智能合约技术透明、自动执行的特点，可以实现教育资源上传、认证、流转、共享等工作的自动化执行，降低资源共享成本，提高资源共享效率，实时监控社区生态环境。

2.2 城市治理

区块链技术在城市治理领域的重点应用场景包括：智慧政务（政务公开）、智慧交通、公共安全。

2.2.1 智慧政务

区块链技术在智慧政务领域的场景包括电子政务、数字身份认证以及权力监管等。

电子政务：随着电子政务建设工作的推进和政务服务平台的广泛应用，数据共享与安全效率的矛盾日渐突出，同时还存在信息泄露等问题。区块链技术为跨级、跨部门的数据互联互通提供了安全可信环境，对访问方和访问数据进行自主授权，通过区块链网络完成结构化数据的共享，对于非结构化数据，则通过存储记录其特征值，保证数据传输的安全可靠。此外，也可以利用区块链技术处理政务系统的协同流程，实现科学决策、高效指挥，有效提升政务服务管理水平，缩短流转办事时间，提高业务审批效率，实现精细化管理。

数字身份认证：数字身份证是指将真实身份信息浓缩为数字代码，可通过网络、相关设备等查询和识别的公共密钥 。近年网络诈骗、身份盗用、信息泄露等与数字身份信息相关的违法行为层出不穷，亟需便捷、可信的数字身份认证手段。区块链技术真实公平、开放共享、难于篡改、安全加密的特性，可以保证数字身份信息的不可篡改、不可伪造及完整性、连续性、一致性，区块链会成为数字身份和权利认证的重要手段。

权力监管：区块链技术可以用来打破信息孤岛，通过区块链链接各部门文件、数据的移动，实现多部门、多信息的交叉共享，确保信息实时更新，提高流程及数据的透明度，为数字反腐（大数据侦查）提供新的手段和来源数据。

2.2.2 智慧交通

智慧交通涵盖领域愈来愈广，在各细分领域都存在这数据的透明和不可篡改需求，因此交通领域也是适合区块链技术落地的重点场景。

交通数据安全存储与共享：如前所述，智慧交通涵盖人、车、路、设施、行为等方面的海量数据，借助区块链技术多中心化，安全可信、智能合约等特性，可以实现行业主体（政府、企业）、运输装备（车辆、船舶、飞机）、基础设施（道路、桥梁、场站），构建现代交通网络，解决行业数据共享、基础设施智能化管理等问题。并在保证数据流通公开透明的基础上，保障数据资产权益，提升智能交通运行效率，释放综合交通运输的信用成本。

高效交通治理：物联网可以实时获取道路、交通信息，区块链技术可以在这些物联网设备之间实现较低成本的连接，并通过去中心化的共识机制提高设备运行的安全性和私密性，物联网与区块链的结合，可以将跨系统数据传输、共享下沉到区块链层，降低智慧交通系统复杂度，促进整体交通网络高效、智能化运行。

2.2.3 公共安全

电子证据存证：区块链技术的不可篡改、可追溯等特性，可有效解决传统存证面临的安全问题。主要包括：区块链的分布式存储，实现电子证据的安全存储和高效提取，允许多机构共享电子证据，降低取证成本，提高协作效率；区块链技术的时间戳机制，电子证据存储固定过程中通过比对哈希值来验证数据完整性，采用不对称加密技术对电子证据进行加密保障传输安全，充分保障了证据真实性和安全性。

应急指挥调度：在公共安全事件应急指挥调度的事前、事中、事后三个阶段，均可以应用区块链技术提升指挥效率。事前：通过数据采集设备（摄像头、传感器）与区块链多中心化、共识机制技术的结合，实现多源数据安全、及时融合；事中：实现跨团队、部门和机构的合作与实时信息共享；事后：多源信息汇总存证，区块链的不可篡改、时间戳机制，可以确保数据的安全性。三个阶段均需要安全的信息和价值交换，区块链技术可以提供端到端的安全解决方案。

2.3 产业经济

区块链技术在产业经济领域的重点应用场景包括：智慧物联网、智慧工业。

2.3.1 智慧物联网

物联网设备规模化接入：物联网数据产业升级带来的是海量设备的接入，预计在2020年公众网络机器到机器连接数超过1亿，“中心云+小范围部署”的传统物联网通信形式已无法满足发展需求。区块链技术可以解决物联网的规模化问题，通过多个区块链节点参与物联网体系验证，将物联网中信息记录在分布式账本中，取代中心云的作用，以较低的成本实现物联设备的互联。

物联网设备安全：传统物联网设备因为存在权限漏洞、不安全的网络端口、信息传输不加密等问题，极易受到攻击，区块链技术的分布式存储、全网节点验证的共识机制、不对称加密算法，都可以大大降低物联网设备被攻击风险。

2.3.2 智慧工业

工业安全：主要涉及工业设备身份管理、设备访问控制、设备注册管理、设备运营状态监管等，以区块链智能合约共识执行的方式获取和验证设备身份，设备所有者将访问权限的策略发布到区块链，并通过智能合约对这些策略进行管理，设备访问者对设备的访问要符合这些策略，在设备运营使用过程中，借助区块链技术不可篡改账本记录设备相关运行状态数据，确保产业链各企业能够访问可信、一致的设备运营数据。

优化工业生产流程：基于多节点、分布式、访问控制的区块链网络，记录工业供应链的可视化，实现安全可信、可追溯的供应链数据记录，从区块链分布式账本中通过智能合约接口实现对供应链全过程状态数据的可信查询和追踪。

工业互联网数据共享：区块链技术的分布式存储、不可篡改、加密算法等特点，可用于实现工业互联网各实体间的可信数据交换，各企业的生产制造数据能够以可控可信的方式存储在区块链上，同时实现对其他企业的数据可控共享。

2.4 生态宜居

区块链技术在生态宜居领域的重点应用场景包括：智慧能源、智慧新零售。

2.4.1 智慧能源

能源生产：能源生产环节数据由各能源厂商硬件基础设施产生、本地化存储，往往形成数据孤岛，无法产生信息价值。通过与物联网设备相结合，在数据采集基础上，应用区块链技术实现生产数据的可信、安全存储与共享，提高监测精度，挖掘数据价值，为政府监管统筹、企业协同合作创造信息基础。

能源交易：能源交易分为批发能源交易与零售能源交易，前者易具有资金量大，交易周期长，依赖人力，风险较大的特点，后者则具有难于实时支付清结算、难于实现需求响应等特点。针对能源交易市场，借助智能合约，为批发能源交易市场提供安全交易保障并降低违约率；针对零售能源交易市场提供实时支付清结算手段。

2.4.2 智慧新零售

商品溯源：目前的商品溯源面临的问题包括商品溯源信息记录不完整易篡改、数据孤岛、隐私泄露等突出问题。利用区块链的特色技术，可以将商品全生命周期的参与者（包括原产地、生产商、渠道商、零售商、品牌商、消费者等）纳入供应链管理，通过多方参与数据维护构建数据信任基础，满足商品全生命周期溯源及数据可靠性问题。数据孤岛、隐私泄露等问题的解决前文已述，不再重复。

零售供应链优化：利用区块链技术构建数字化供应链，特别是跨境贸易中的供应链管理，利用区块链的分布式记账、不可篡改特性，将商品的全供应链数据进行分布式存储、授权访问和加密验证，简化供应链流程中的数据交换共享以及业务作业流程，实现供应链整体效率提升与优化。

构建良性商业生态环境：零售行业具有交易数据零散、交易节点多样、交易网络复杂的特点，区块链技术的去中心化、真实公平、开放共享、难于篡改、安全加密等特点，可以构建一个可信的分布式商业环境，在这样的良性生态环境下，合作可以变得更加高效和低成本，可以更有效的促进资源整合，进而创造更多的经济和社会价值。

三、区块链技术在智慧城市的应用路径

3.1 构建安全、可信的智慧城市数据共享分享基础设施

数据是智慧城市智能生长的基础，也是智慧城市发展的关键，构建数据分享和共享机制对于智慧城市至关重要。智慧城市产业链参与方众多，技术多样、系统复杂、应用丰富，尤其是利益结构和安全机制复杂，使得数据孤岛现象突出。区块链的去中心化、安全性、不可篡改以及可追溯性，为智慧城市数据共享和分享以及突破智慧城市的数据孤岛效应创造良好的技术条件。

在数据共享方面，通过建立以区块链为基础的数据交易系统，严格的记录数据的来源、数据的所有权、数据的使用权、数据的可共享范围、数据的安全合约，为政府开放政务数据、企业开放企业数据、市民开放个人数据，提供可追溯、可交

易、可信任的共享机制。

在数据分享方面，通过在区块链记录每一次分享者的信息、数据分享的路径、数据的来源可分享的范围，在不同应用之间、不同部门之间、不同地区之间建立起数据高效安全的流动机制。

3.2 构建城市级的多层次区块链公共服务平台

在智慧城市中信息和数据的流动、人员和物流的迁移、智慧应用的启动与运行，都离不开安全可信的交易体系，构建陈实际的多层次区块链公共服务平台，作为数字孪生城市的基础设施，为政府应用、企业应用和民生应用提供公共的能力。

一是打造全域的城市级区块链公共服务平台，作为公共属性的区块平台，其核心能力应该包括市民、企业身份认证及公共信息，比如个人信用、企业资质及信用；

二是打造垂直领域的行业及区块链服务平台，在教育、医疗、金融、交通（自动驾驶）、物流、安全等行业，提供认证、安全、交易、合规性控制等服务；

三是打造城市部件区块链服务平台，对城市各类关键性资产、重要设施、核心设备的认证、数据交换提供基于区块链的服务；

四是打造政府区块链服务平台，在数据互信、流程互通、证照互认、机制协同等方面提供公共的区块链能力服务。

3.3 以政务服务创新为突破，推动区块链应用

在政务领域，创新政府服务流程，利用区块链技术，构建责权清晰、可信安全的公共服务应用，打通部门之间的数据互通、业务互通、流程互通。

一是在高频政务审批场景，强化区块链的应用，包括工商注册、教育入学、电子证照、电子材料、电子印章、电子档案等；

二是在市场监管场景，积极引入区块链技术，包括食品监管、药品监管、房屋租赁监管、安全生产监管、消防安全监管、建筑质量监管、税收监管、精准扶贫以及政府公开招投标项目监管等场景；

三是在城市智能运行场景，引入区块链打造绿色可持续的城市经济，包括建筑节能、绿色交通、循环经济、节能减排等领域，通过智能合约的引入，建立可信任的交易及监管机制。

四、中国移动智慧城市区块链核心产品及技术解决方案

4.1 数据流通及共享

4.1.1 需求背景

数据被认为是信息时代的“原油”，数据共享的程度反映了一个行业、一个地区、一个国家的信息化水平。数据共享程度越高，信息发展水平越高 。目前各级政府部门都在推动政府信息共享，同事强化相关治理，建立和完善数据流动和利用的监管立法，对信息滥用、侵犯隐私、网络诈骗、盗取商业秘密行为要依法依规进行打击。互联网企业以及传统企业在IT化转型过程中都积累了大量的数据资产，当前，这些数据收集和分享的行为都是以企业或企业联合体的方式自发进行的，这些主体都希望能够从其它主体处收集到更多的跨行业、跨领域的数据，以便解决自身数据覆盖度不足的问题。数据在主动受控、安全可管、利益分享的前提下共享，将产生“1+1>2”的效果。

但是，数据共享的愿景“看上去很美”，在实际实施过程中除了前述违法行为的存在，还要面临“易复制、难追溯、难控制、难评价”的“1易3难”问题。因此，数据拥有者希望合作但同时又缺乏信任前提，这种情形正好适用区块链能够建立和传递“信任”的技术特点。基于区块链技术构建可控可管的数据共享系统，建立数据的“信用体系”，对于构建数据共享生态具有现实意义。

4.1.2 角色分析

基于区块链技术的数据流通及共享方案中的角色主要包括：数据提供者、数据使用者、服务提供者、服务监管者。角色与用户不是一一对应的关系，一个用户可以同时具有一个或多个角色。数据流通及共享系统中的角色与其访问对象的关系如图 2所示。

图 2 角色–对象示意图

1、数据提供者：是指提供特定数据以供其它角色使用的实体，数据提供者对其共享的数据的公开、以及在其授权规则下合法使用承担法律责任，并设定共享策略。

2、数据使用者：是指访问特定数据的实体。数据使用者可对有效的、可共享的数据列表进行检索以及发起访问请求，数据使用者完成数据访问后，能够对特定数据提供质量反馈评价。

3、服务提供者：是指提供数据流通及共享平台的服务商。服务提供者为数据提供者、数据使用者提供数据共享服务、必要的数据处理服务、以及数据流通共享相关的日志记录、用户管理、系统安全等服务。

4、服务监管者：是指提供数据共享服务合规性、合法性管理的部门，如信息化主管单位。服务监管者在获得授权的前提下，可随时提取系统共享的所有数据内容，能够获取系统运行状态、以及业务日志。

4.1.3 系统架构

基于区块链的数据流通及共享方案系统架构如图 3所示。

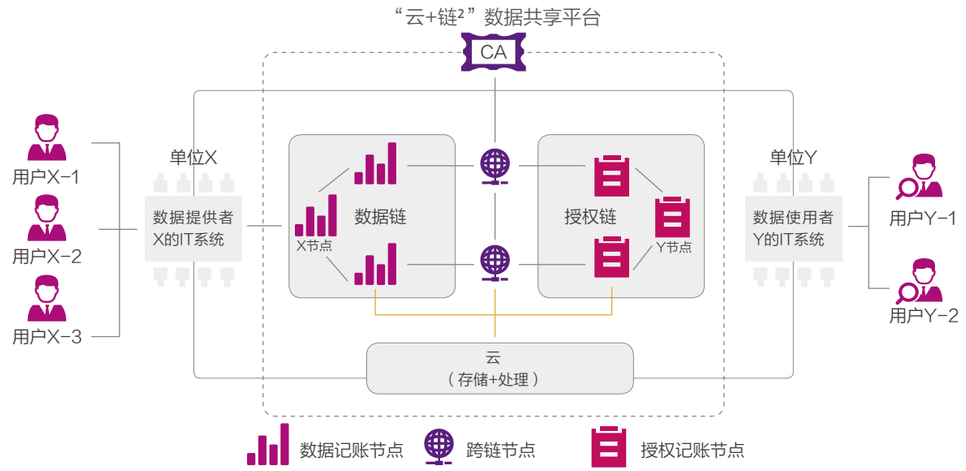


图 3 “云+链²”数据共享系统架构

云主要完成数据安全存储、实施数据处理功能、监控数据敏感操作、记录相关操作过程。

采用平行链结构，部署数据链、授权链两种类型的区块链：数据链面向数据提供者，授权链面向数据使用者，在两种链之间设置跨链节点。参与数据共享的各方，以数据提供者、数据使用者的身份分别加入数据链和授权链，并在其中拥有对应的区块链节点。

4.1.4 关键流程

基于区块链的数据流通与共享关键流程包括数据发布、数据访问及数据处理、信用评价。

1、数据发布流程

当数据提供者有新数据发布或对已发布数据的属性进行更新时，采用本流程，流程示意图如图 4所示。

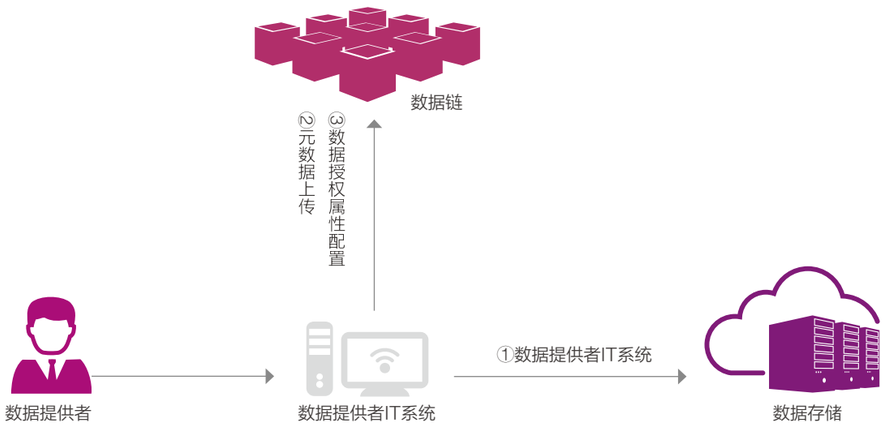


图 4 数据发布流程

数据发布流程包括数据文件上传、元数据上传、数据授权属性配置三个子流程。

2、数据访问及数据处理流程

当数据使用者需要对共享数据进行访问时，采用本流程，流程示意图如图 5所示。

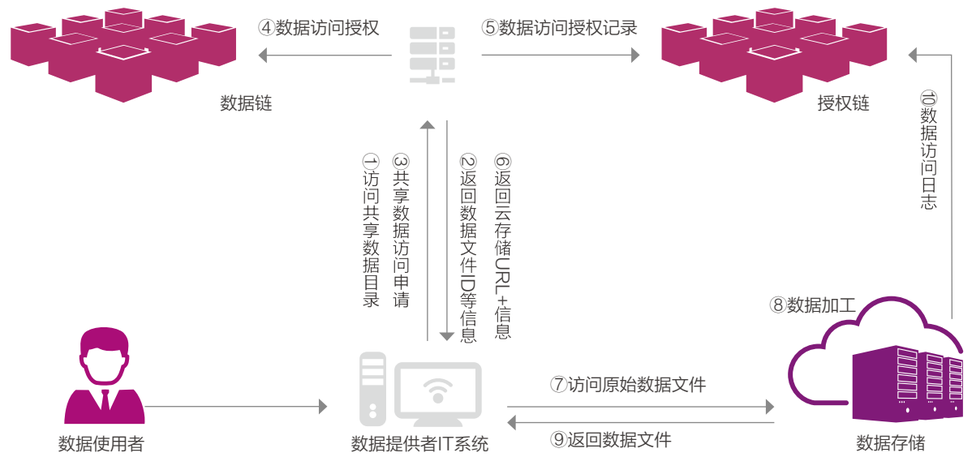


图 5 数据访问流程

数据访问及数据处理流程包括访问共享数据目录、返回数据文件ID等信息、共享数据访问申请、数据访问授权、返回共享数据访问URL2信息、数据访问授权记录存证、访问原始数据文件、数据处理、获取数据文件、数据访问记录存证十个子流程。

3、信用评价流程

数据使用者在成功获取数据文件后指定时间段内，可对该数据的质量发表一次评价。

4.1.5 技术策略

1、访问控制及授权机制

在本系统中使用基于属性的访问控制，访问控制策略是存储在区块链中，策略信息对任何人都是可验证、可追溯且不可篡改的，大数据资源的访问控制摆脱了传统集中式访问控制管理可能存在的单点故障和访问控制判决透明度的问题，实现了访问控制策略的分布式管理，可提高系统的鲁棒性和可信性。

2、数据存储及处理

1）云上存储

数据提供者调用云平台的数据上传接口将数据传输到云平台，数据在云平台上以三副本方式存储，存储方式包括明文存储和密文存储。

2）数据处理

数据处理措施主要包括数字水印、数字脱敏：数字水印会将数据摘要信息、用户身份信息和水印信息记入日志存储在云平台上，该日志的哈希值写入区块链，一旦发生数据泄露，可以提取泄露数据中的水印信息与日志中记录的水印信息做比对，定位出泄露者；数字脱敏根据脱敏配置对数据进行脱敏处理后返回给数据请求者。

3、数据存证

1）**数据发布：**当有新数据要发布时，则应将元数据等信息在数据链中进行存证；

2）**授权属性更新：**当需要对原数据中的授权属性、发布状态等进行更新时，也应在数据链中进行存证；

3）**数据访问授权：**当数据访问申请被共享数据请求授权判定智能合约判定后，则应将授权结果在授权链中进行存证；

4）**数据访问日志：**云存储将反馈的共享数据返回给数据使用者后，应及时将共享数据访问日志在授权链中进行存证；

5）**数据质量评价记录：**数据使用者在使用共享数据后，可在一定时间后对数据提供者进行评价，并在授权链中对评价进行存证。

6）**数据访问计费及结算：**数据使用者获得其所需的数据后，可根据计费模型进行计费（如：按交易的数据量，数据的字段数量等）。数据使用者通过币或是线下银行支付费用给数据管理者、数据拥有者。数据使用者、数据管理者、数据拥有者可根据约定的周期进行结算。

4、信用评价

对数据的提供方和使用方的评价，与数据使用记录和其它存证信息一同记入链上，可根据使用方、提供方、数据属性信息进行检索，为选择其它数据提供方和数据提供方提供信用参考。系统提供中立可信的监控和审核工具，出现争议评价时，能够根据存证信息，对提供的数据或分析结果进行验证，对争议评价进行判定。

4.2 数字证书管理

4.2.1 需求背景

PKI（Public Key Infrastructure，公钥基础设施）是一种使用公钥密码技术支持认证、加密、完整性和不可否认服务的安全基础设施，广泛应用于互联网和移动互联网，未来5G通信网中也将扮演重要角色。

在传统物联网应用中，一般采用对称密钥和非对称密钥两种方案实现对设备的认证。但是存在证书批量配置效率低、对称密钥方案对业务平台要求高进而限制设备互联互通、非对称密钥方案不同CA机构之间实现互通难导致证书预置效率低等问题。

随着物联网技术与应用的快速发展，对物联网设备的安全需求、设备之间互联互通的需求越来越被人们所重视。本方案利用区块链去中心化信任、分布式记账和共识机制的特点，结合智能合约，提供一种高可靠性的新型的物联网安全基础设施，可以为物联网芯片、物联网设备、以及物联网应用提供低成本的身份认证和通信安全解决方案。此外，还可以实现设备资源（包括：空余带宽、数据存储能力、数据和内容分享）的共建、共享，按需使用，并为资源所有者提供记账和收益能力。

4.2.2 系统架构

基于区块链的数字证书管理方案技术架构如图 6所示。

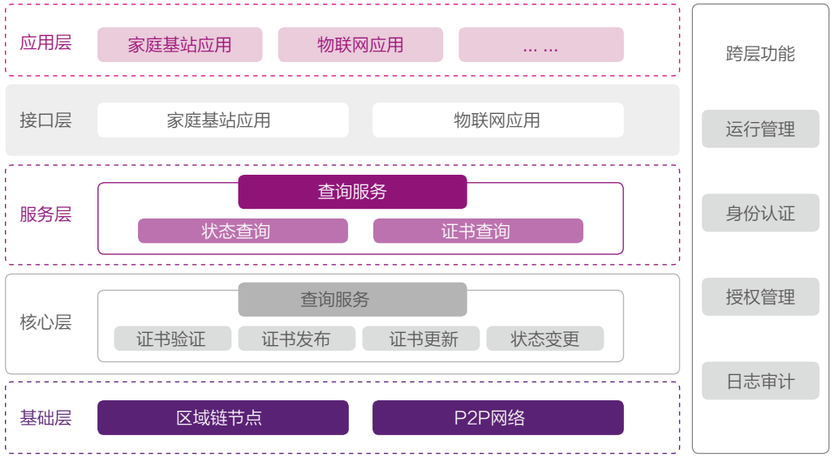


图 6 基于区块链的数字证书管理系统技术架构

基础层：提供区块链系统正常运行所需的硬件设备、运行环境、基础组件，包括区块链节点、P2P网络等，提供系统所需的计算、存储资源以及点到点之间的高效安全通信。

核心层：提供数字证书管理功能，包括证书验证、证书发布、证书更新、状态变更，提供数字证书的正确性验证、数字证书发布到区块链、证书密钥更新和有效期更新以及证书状态变更功能。

服务层：提供与证书管理和应用相关的服务，包括证书状态查询、完整的数字证书查询功能等服务。

接口层：提供与证书管理和应用相关的接口，包括证书管理接口、证书查询接口等。

应用层：包含所有采用基于区块链的数字证书管理系统的业务和应用系统，典型场景有家庭基站认证、物联网应用等。

跨层管理功能：提供与系统相关的运行管理、身份认证、授权管理，以及日志审计相关的功能。

基于区块链的数字证书管理方案可采用无CA机构参与的联盟链和多CA机构参与的联盟链两种网络架构。两种网络架构如图 7所示。

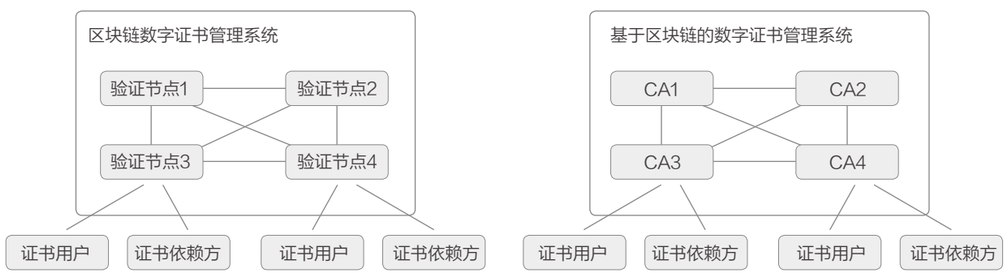


图 7 无CA机构以及多CA机构参与的联盟链架构

无CA机构参与的联盟链架构中，证书用户将向区块链系统提交自签名证书，验证节点将对用户提交的自签名证书进行验证。参与方主要包括证书用户、证书依赖方、验证节点。证书用户是数字证书的实际拥有者；证书依赖方指的是信任证书系统的使用者；验证节点用于验证用户发布证书的合法性。验证节点可以由设备商、运营商、业务供应商等担任。

多CA机构参与的联盟链网络架构中，CA节点由传统CA机构担任，负责对证书用户进行审核，签发用户证书。作为联盟链节点，CA节点还承担将用户证书发布到区块链系统，并生成新区块的功能。其他参与方与无CA机构参与的联盟链架构相同。

4.2.3 关键流程

基于区块链的数字证书管理系统包括证书发布申请、证书发布、证书更新、证书撤销/挂起/恢复、证书使用流程，以无CA机构参与的证书管理流程为例进行说明。

1、证书发布申请

数字证书在记录到区块链系统之后才可被依赖方使用，证书在生效之前，证书用户首先向区块链系统提交证书发布申请，主要流程为：证书用户自己生成一份自签名数字证书，并通过扩展项标识所属区块链网络，之后证书用户向区块链网络发起证书发布申请请求，包括用户的自签名数字证书以及验证证书所需的信息。

2、证书发布

区块链系统在接收并验证用户的证书发布申请之后，发布用户提交的数字证书。区块链验证节点收集发布申请，将当前所有未纳入区块的合法证书信息以及证书状态作为区块链中的记录，使用区块链中的共识机制生成一个新区块，之后向区块链网络发布该新区块。网络中其他节点接收到新区块后，验证区块以及区块中每条记录的正确性，如果正确，那么将该新区块加入到本地保存的区块链中，否则丢弃该新区块。

3、证书更新

证书到期之前用户需要更新证书以保证证书使用的连续性。证书更新可不变更密钥，但从安全性考虑，建议更新密钥。证书更新的主要流程为：当用户需要更新证书时，用户需要产生一份新的数字证书，证书用户向区块链网络发起证书更新请求，后续流程与证书发布流程相同。

4、证书撤销

若发生私钥泄漏等安全事件，应进行证书撤销。主要流程为：证书用户提交证书撤销请求，区块链验证节点收集用户的证书撤销请求，根据用户提交的信息验证用户身份,区块链验证节点将当前所有未纳入区块的合法证书信息以及证书状态作为区块链中的记录，使用区块链中的共识机制生成一个新区块，之后向区块链网络发布该新区块。网络中其他节点接收到新区块后，验证区块以及区块中每条记录的正确性，如果正确，那么将该新区块加入到本地保存的区块链中，否则丢弃该新区块。

证书挂起以及证书恢复流程与证书撤销流程类似。

5、证书使用

在证书使用过程中（例如现有的TLS、IPSec等安全协议），证书用户需要将证书提交给依赖方，依赖方接收到证书后，需要检查证书的合法性和有效性。

在多CA机构参与的联盟链架构中，证书由CA机构签发，证书用户向所属CA机构或其代理节点提交证书申请/证书更新/证书撤销等证书管理请求，所属CA机构依据自己的策略对证书用户的身份和证书请求进行鉴别。鉴别方式与CA机构传统鉴别方式相同。

依赖方在接收到用户证书之后，首先验证该证书是否由自己信任的CA机构签发，若是，则可在本地采用传统方式进行验证；否则，将该证书发送给自己信任的CA机构或者其代理节点，由CA机构或代理节点在区块链系统中进行查询和验证，并将结果发送至依赖方。

4.2.4 技术策略

1、身份识别及认证

1）家庭基站设备身份识别及认证

利用基于区块链的数字证书管理系统，在家庭基站生产阶段自行产生和配置证书，在设备出厂或入网的时候，将设备的证书信息通过设备商节点上报至基于区块链的数字证书管理系统。

2）物联网设备身份认证

物联网芯片、终端等设备在生产线上产生并配置与设备身份相对应的自签名数字证书，厂商节点将自签名证书上传至区块链数字证书管理系统。该证书通过区块链节点共识之后记录到区块链中。在物联网设备进行身份认证过程中，依赖方可以利用区块链数字证书管理系统对设备的身份进行认证。

3）智能家居身份识别与协作

在智能家居场景中，家庭网关可作为区块链节点，智能家电设备配置数字证书并在区块链安全基础设施中发布证书，可以在本地实现对智能家电设备的安全认证，智能家电相互之间也可以使用数字证书进行双向认证，实现用户家庭区域内不同厂家物联网设备之间直接通信。

2、通信安全

区块链数字证书管理系统中仅对证书获取方式、合法性验证流程做了优化，证书格式、证书使用机制等均可兼容，因此，包括TLS/DTLS、IPSec等众多使用数字证书的传统通信传输安全解决方案无需改动即可适用于本方案。

五、智慧城市区块链技术发展建议

5.1 高度重视区块链底层架构和基础设施

区块链底层架构和基础设施是指区块链技术、产业和应用发展提供公共服务的设施，它们是保证区块链活动正常进行的基础。区块链基础设施包括区块链赖以生存和发展的底层技术，包括存储、加密、时间戳、共识和跨链，包括成熟稳定的公链基础链以及服务于企业级的联盟链。目前，我国正处于区块链发展初级阶段，基础设施的不完备——特别是计算和存储资源的限制，无法高效搭建区块链应用，很多应用场景无法一一落地。而服务于民生服务、城市治理等领域的区块链基础设施，对于保障公民医疗、教育、构建社会信用体系、增强人民幸福感等具有重要意义，有必要由政府监管，建立安全、可信、高效的区块链基础设施，承载智慧城市分布式应用，为加快实现政务信息资源共享、提升政府和企业协同效率、推进国家治理能力和治理体系现代化、建设现代化经济体系奠定基础。

中国移动区块链平台提供的基础设施服务，用户无需再自行搭建平台，可以极大降低实现区块链底层技术的成本，简化区块链构建和运维工作，实现一站式快速交付定制，已为31个省公司，10余个一级业务系统，200多个合作伙伴提供了强有力的支撑。

5.2 搭建区块链基础服务平台

在当前世界技术竞争环境下，我们建议，相关部门更应该重视区块链技术的研发与应用，更应该重视公链与联盟链的发展与应用，避免在区块链经济体系中受制于人。

由政府出面构建基于公链和联盟链的区块链基础服务平台，为区块链应用落地提供基础服务，而每个具体领域、细分行业的应用、运营由市场主体企业来负责，将“政府搭台，企业唱戏”的智慧城市运营思路引入到区块链技术在智慧城市的应用落地中。

区块链基础服务平台宜具备区块链核心共有功能，建议包括：1）数据资产服务，完成数据的安全存储、流通共享、授权访问、数据评价等；2）数字身份服务，完成数字身份认证、证书管理等；3）共享账本服务，完成交易数据的分布式记录、共识协议、智能合约等。

中国移动区块链平台是基于全国分布式网络搭建的区块链基础服务平台，构建于私有云PaaS之上，旨在为用户提供可信、可靠、高效的区块链服务，用户在弹性、开放的云平台上能够快速构建自己的区块链服务，实现多业务场景的融合应用，解决协同一体、数据一致、精确结算、交易确权、过程追溯、隐私保护等问题。

5.3 充分与大数据、人工智能、物联网等技术融合

新型智慧城市是以人工智能、云计算、大数据、物联网等为技术支撑的，区块链技术要实现在智慧城市的应用落地，一定是与这些技术不断创新融合的。大数据、人工智能的发展都是以海量数据为基础，而区块链技术可以确保数据的安全可信与共享交换，进一步盘活数据资源，激发更广阔的智慧城市应用场景。此外，区块链点对点的数据传输方式，可以实现数据的分布式存储与计算，极大地缓解云计算中心的资源及成本压力。如前所述，物联网设备的安全接入以及身份认证是传统物联网应用两大突出问题，而区块链技术通过共识机制，能够有效的解决这两大问题。通过与物联网技术的充分融合，可以实现物理世界与信息世界数据的一一映射，极大程度的提升链上信息的准确度与可信度，更准确地构建新型智慧城市的基础设施——数字孪生城市。

5.4 完善监管和标准体系

为区块链技术发展及其在智慧城市产业的落地营造良好的发展环境，需进一步完善区块链监管体系及标准体系。区块链技术的特点，意味着它的发展将会影响社会的方方面面，同时区块链去的中心化天然是排斥监管的，需要监管机构对区块链技术及原理有比较深入的了解，结合区块链技术的具体应用场景进行监管。区块链标准化研制工作将会加速，这对于加速区块链技术智慧城市应用落地以及完善智慧城市区块链产业，都具有积极的推动作用。目前我国区块链标准化工作已具备良好基础，后续应加强在基础标准、通用技术标准等方面的布局。此外应该看到，区块链开源项目的影响力正在日益增强，对技术路线的引领作用也逐渐凸显，应该保持与开源社区的良好交互，不断提升支持力度，以获得在区块链技术领域的话语权，进而推动技术的发展与实际应用落地。

中国移动在ITU-T积极参与、推动区块链的标准化工作，将为区块链技术的健康发展、在智慧城市领域的应用扫清障碍。