ICS 33.040.40
CCS L 79

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T××××—××××

工业互联网中区块链应用场景和业务需求

Application scenarios and service requirements of block chain in industrial Internet

（报批稿）

202×-××-××发布　　202×-××-××实施

中华人民共和国工业和信息化部 发布

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中国联合网络通信集团有限公司、苏州同济区块链研究院、北京京东尚科信息技术有限公司、北京邮电大学、北京工业大学、浪潮通信技术有限公司、安嘉新（北京）科技股份公司、网络通信与安全紫金山实验室、华为技术有限公司、无锡物联网创新中心有限公司、北京百度网讯科技有限公司。

本文件主要起草人：刘阳、贾雪琴、池程、马小峰、田娟、张钰雯、李雨蓉、王伟兵、陆晓峰、谢人超、霍如、胡凝、王招军、史可、朱斯语、王小华、李文博、王飞甫、李富林、马龙、韩鹏、张晨、李艳东、冀辰、董接莲、刘尧、潘凤薇、汪佳伟、李代青。

工业互联网中区块链应用场景和业务需求

1 范围

本文件规定了区块链在工业互联网中应用的技术框架、相关角色、参考模型及工业互联网中区块链典型应用场景和业务需求。

本文件适用于工业互联网场景中对区块链技术应用指导。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业互联网 industrial Internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源:GB/T 42021-2022]

3.2

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源:GB/T 42752-2023]

4 缩略语

下列缩略语适用于本文件。

API	应用程序编程接口（Application Programming Interface）
BLS	基于椭圆曲线密码学的数字签名算法(Boneh-Lynn-Shacham)
CA	认证中心（Certificate Authority）
DPKI	分布式公钥基础设施（Decentralized Public Key Infrastructure）
ICT	信息和通信技术（Information and Communication Technology）
PaaS	平台即服务（Platform as a Service）
P2P	对等式网络（peer-to-peer）
PDA	掌上电脑（Personal Digital Assistant）
RFID	射频识别（Radio Frequency Identification）
SDK	软件开发工具包（Software Development Ki）
Web	全球广域网（World Wide Web）

5 概述

5.1 工业互联网总体需求

工业互联网是一种开放的、全球化的网络，包括网络、平台、安全三大功能体系，其中网络互联是基础，平台是核心，安全是保障。工业互联网是智能制造的基础设施，通过工业互联网平台将人、机器和数据连接在一起，帮助制造业拉长产业链，形成跨设备、跨系统、跨厂区、跨地区的互联互通，从而提高工业生产力，推动整个制造服务体系智能化。工业互联网与制造业的融合带来智能化生产、网络化协同、规模化定制、服务化延伸的智能化升级，让制造模式从“孤岛型”传统制造向多方协同制造模式发展。通过互联网技术，以机器、原材料、控制系统、信息系统、产品以及人之间的网络互联为基础，对工业数据的全面深度感知、实时传输、快速计算和高级建模，实现智能控制、运营优化和生产组织方式变革。本标准将工业互联网实现工业经济各种要素资源高效共享和流通的过程总结为以下需求：

a) 数据保护。在传统单数据中心模式的数据传输和存储过程中，应注重数据保护，防止数据丢失和被破坏；
b) 信息公开。在工业互联网多方协同制造中，应公开透明地将多方协作信息向所有参与者发布，并保证信息可信；
c) 数据可信。在供应链过程和多方合作过程中，应防止数据造假和保障系统中数据可信；
d) 身份认证。工业互联网中的参与实体需进行可信身份认证和管理，应保障工业互联网中实体身份可信；
e) 数据确权。工业互联网中进行数据流通和共享容易，应保障数据共享时的数据确权；
f) 过程追溯。工业互联网领域拥有大量企业进行外协、外购、线上协同设计制造等场景，整个过程应具备完善的、可信的溯源认证手段。

5.2 区块链技术特点

5.2.1 分布式账本

分布式账本是区块链最重要的技术特点之一。不同区块链节点上的重要数据通过点对点传输协议，实时进行数据同步，并通过共识算法保证数据的一致性，从而使得数据在不同数据节点上均拥有相同的数据副本，做到系统结构上的分布式。

5.2.2 数据隐私算法

区块链在进行数据的传输、计算、存储过程中，运用了大量的数据加密算法，包括非对称加密算法、哈希算法、零知识证明、安全多方计算等，使得在区块链上各个数据处理环节中的数据均以密文形态存在。

5.2.3 不可抵赖性

利用非对称加密算法的私钥对数据进行签名，只能使用对应的公钥进行验签，基于这一原理，可以保证对区块链上的交易进行签名，具有唯一性和不可抵赖性。

5.2.4 防篡改

区块链上的交易记录都会记录交易发生的时间戳，再通过哈希算法，生成交易哈希值，即数据指纹，并被记录在每个数据区块的特定区域中，每个数据区块也会记录其上一个区块链的哈希值，从而保证了整个数据链条的不可篡改。同时基于共识算法原理，也避免了任意一方在未经共识认可的情况下篡改分布式账本上的数据。

5.2.5 可追溯

区块链通过区块数据结构存储了创世区块后的所有历史数据，区块链上的任意一条数据皆可通过链式结构追溯其本源。

5.2.6 智能合约

智能合约是执行在区块链上的一套程序代码，代码执行逻辑和执行权限规则由业务流程决定，或由区块链上参与方共同约定。通过智能合约可提供对上层业务系统的对接接口，并完成对区块链上数据的读写操作。通过智能合约的事件处理机制，还可以做到实施监控，主动通知，整个过程完全独立无干预，保证了执行效率的同时，也保证了公正性。

5.2.7 分布式身份

基于区块链技术构建的分布式身份体系，可通过非对称加密算法为分布式身份主体分配公私钥对，通过分布式账本实现身份标识和公钥的公开，通过智能合约完成分布式身份的注册和验证。

6 典型应用场景对区块链的需求

6.1 标识解析认证服务场景

6.1.1 标识解析认证服务总则

标识解析的认证服务体系是工业互联网标识解析服务安全性的重要保障，标识解析的认证服务体系通过DPKI架构建立身份认证模型，通过区块链技术保证数据的完整性，通过智能合约保证认证的智能化可配置。基于该体系的实现系统需要满足多种技术需求以保证标识解析认证服务能够满足安全、性能和功能的需要，根据区块链的参与角色和组件，提出不同的技术需求。

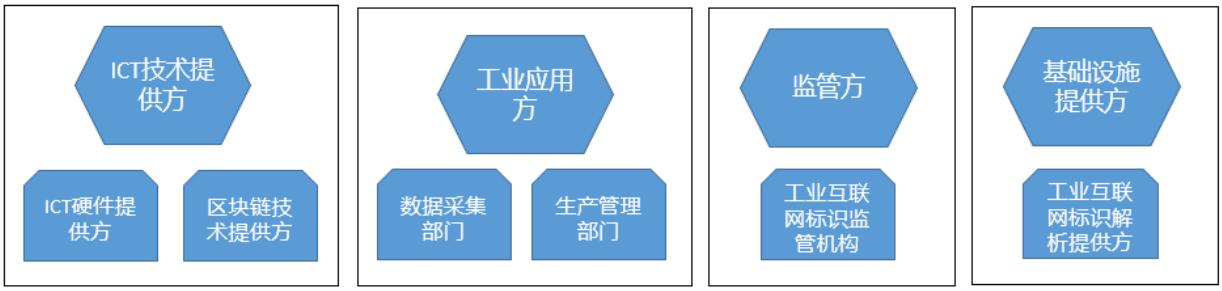

图1 标识解析认证服务场景涉及到的角色和子角色

如图1所示，该场景下涉及到的角色包括：ICT技术提供方、工业应用方、监管方、基础设施提供方，该场景下涉及到的子角色包括：ICT硬件提供方、区块链技术提供方、数据采集部门、生产管理部门、工业互联网标识监管机构、工业互联网标识解析提供方。

6.1.2 标识解析认证服务业务需求

该场景下的业务需求包括：

a) 应具备底层联盟链平台，支持高性能的上链信息处理、智能合约调用、证书签发和验签等服务，平台包含区块链应用框架，包括各种编程语言的SDK，RESTFUL风格的API接口；
b) 应具备高性能千兆级网关、高性能服务器以支撑工业互联网标识和解析服务；
c) 应有企业级客户端或web端，支持复杂的图形化界面，利用SDK与区块链节点进行交互；
d) 应具备完整的监管规范和标准。

6.1.3 标识解析认证服务技术需求

认证服务的数据源来自工业互联网标识解析的各级节点，数据传输过程是从解析节点传输到客户端，数据存储的数据为认证所需的证书和公钥等信息，业务系统是终端用户访问标识解析数据和提供身份认证的前端系统，区块链的安全锚点为支持认证服务其他组件的安全组件。

数据源：节点应具备防火墙、入侵检测等防止计算机病毒入侵的能力，以保证标识解析数据的真实性；节点应运行具有负载均衡能力的服务器集群，以保证标识解析数据的可用性。

数据传输：应具备数据加解密和签名验签的功能，以保证标识解析数据在传输过程中不被监听和篡改；

数据存储：应具备数据加密功能，具备支持联盟链的共识算法、处理模型和交易模式

业务系统：应具备身份认证功能，用户提供口令、指纹等身份信息，验证通过后可以根据授权决定是否可访问标识解析服务。

区块链安全锚点：应具备服务器安全防护功能，包括但不限于防火墙、入侵检测、防病毒、CA认证中心、加密机、漏洞扫描等工具和软件，能够有效的保障业务系统和区块链节点的安全性。

6.2 数据共享交易场景

6.2.1 数据共享交易总则

数据共享交易是工业互联网中区块链应用场景之一，数据共享交易就是让在不同地方使用不同计算机、不同软件的用户能够读取他人数据并进行各种操作、运算、分析及数据交易。

如图2所示，该场景下涉及到的角色包括：ICT技术提供方、工业应用、监管方，该场景下涉及到的子角色包括：工业互联网数据平台、区块链平台、工业应用方、数字资产认证机构。

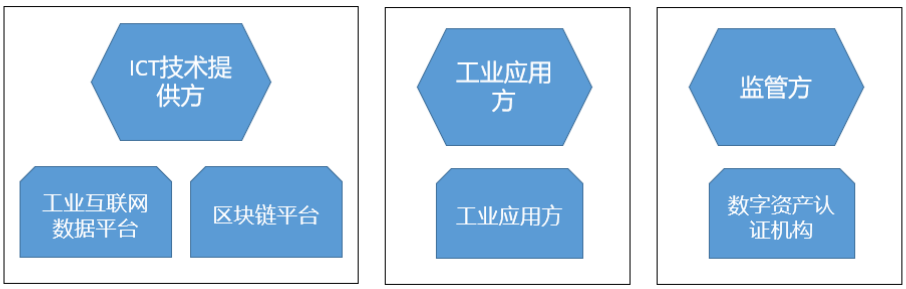

图 2 数据共享场景涉及到的角色和子角色

6.2.2 数据共享交易业务需求

该场景下的业务需求包括：

a) 通过数据建模统一数据交换格式，保障数据可用性和互操作性，实现工业数据在不同区块链间的安全互通；
b) 应建立保障数据交易机制；
c) 应保障共享数据的隐私性和数据安全；
d) 共享的数据应经过脱敏处理；
e) 应保障共享的数据资产实现数据确权；
f) 数据共享过程的各参与方应经统一身份认证，数据共享过程应可追溯；
g) 应保障数据交易吞吐量，数据存储；
h) 支持参与方等级定义，根据不同等级制定权限管理策略；
i) 支持根据不同的授权等级制定完善的数据访问控制协议；
j) 支持安全策略的合约化，进行链上部署与执行。

6.2.3 数据共享交易技术需求

如图3所示，该场景下的技术需求包括数据共享包含工业互联网数据平台、区块链数据共享平台、业务应用三个要素。

工业互联网数据平台对应数据源与数据存储，包含工业企业的私有数据中心与公有云平台；区块链数据共享平台对应数据源、数据存储、数据传输与安全锚点，包含区块链终端、区块链节点、CA认证等；业务应用对应于工业应用方的业务系统，包含工业应用、商业应用等。

数据源：应保证数据源真实、可追溯，保证数据确权。

数据存储：如果工业互联网数据平台中的数据中心、云平台部署了区块链节点，其应具备数据加密、许可访问的功能。

数据传输：应保证数据在广域网传输的安全性、可追溯性。

区块链安全锚点：应保证接入到区块链网络的设备、应用等都要经过区块链安全锚点的认证，且能对应到现实中的主体。

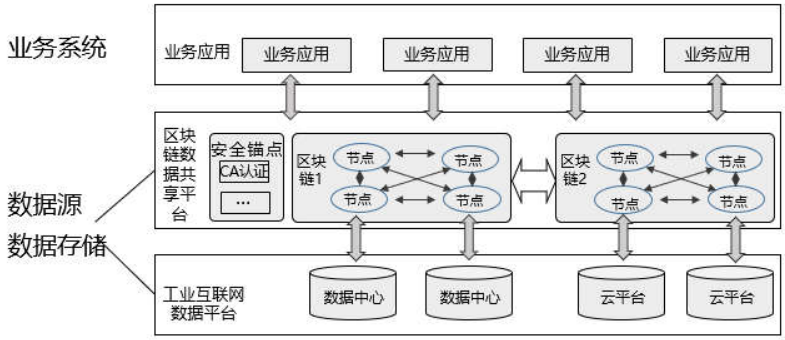

图3 数据共享场景

6.3 设备认证场景

6.3.1 设备认证业务总则

设备认证是工业互联网中区块链应用场景之一。设备认证是指对工业互联网系统中的设备进行身份识别和认证的方式。

如图4所示，该场景下涉及到的角色包括：ICT技术提供方、工业企业、基础设施提供方，该场景下涉及到的子角色包括：ICT硬件提供方、数据采集部门、工业互联网标识管理机构。其中ICT硬件提供方包括识别终端、可信执行环境或安全芯片。

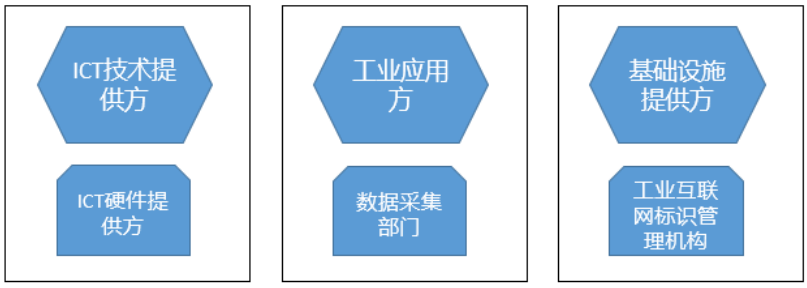

图4 设备认证场景涉及到的角色和子角色

6.3.2 设备认证业务需求

该场景下的业务需求包括：

a) 应及时对工业互联网中设备进行数字身份认证，包括发放数字身份标识代码，收集并上传设备信息；
b) 应保障采集的设备信息数据真实可信，在一定规则下不可能随意更改设备数据信息；
c) 应保障设备与设备信息映射关系，真实、完整、不可篡改；
d) 应保障更改过的设备数据信息可以溯源查询；
e) 应禁止设备标识重复使用；
f) 应保障设备和使用者都具有访问控制管理体系，设备与使用者之间进行双向身份认证；
g) 设备从属关系变更逻辑可被代码化，并可形成基于预定事件触发、不可篡改、自动执行的计算机程序，该程序的结果可被供方和需方认可；
h) 支持分布式数字身份机制，建立链上用户、设备、平台数字身份颁发机制；
i) 支持链上建立数字身份的唯一映射表；
j) 支持分布式身份认证机制，建立基于链上共识的用户、设备、平台双向身份验证机制。

6.3.3 设备认证技术需求

如图5所示，该场景下的技术需求包括：

a) 数据源：每个设备附加一个物理级别的、不可篡改的公私钥对（如依托于可信执行环境或安全芯片），并将设备唯一标识码和设备公钥建立映射关系，通过相应可信机构背书登记上链绑定；
b) 数据传输：设备产生的所有数据进行私钥签名后发送（可选依据数据保护级别，使用接收方的公钥对数据加密，再行使用设备私钥签名后发送），私钥签名传输至网关代理或者直接连接区块链通过局域网传输；
c) 数据存储：设备私钥作为设备重要身份数据需要在设备内部安全存储，不接受非授权的访问；设备公钥和标识信息可链上明文存储；生产信息和需求信息为敏感数据，原始数据可存储于链下；区块链上可依据数据安全保护级别存储明文或加密数据；
d) 业务系统：对应基于区块链的复合型设备身份认证管理平台，须与区块链平台、链下数据存储对接。
e) 区块链安全锚点：对应数据源（设备私钥的生成及设备私钥存储安全）、工业互联网标识管理机构，涉及到区块链平台访问的操作均须被区块链安全锚点管理。

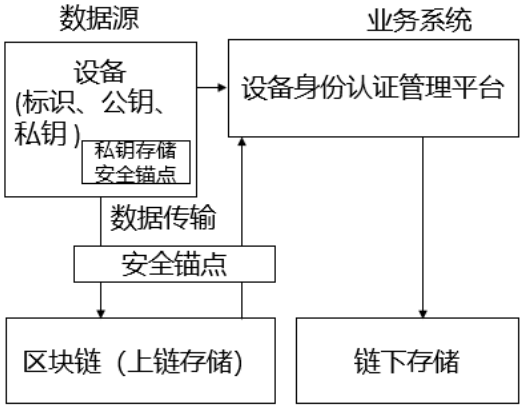

图5 设备认证场景

6.4 物资追溯场景

6.4.1 物资追溯业务总则

物资追溯是工业互联网中区块链应用场景之一。物资追溯是通过记录和标识，追踪和溯源物资客体的历史、应用情况或所处位置的活动，包括从原料供应、生产产线、物资批次、运输过程到销售和使用过程的全生命周期追溯。

以工业设备物资追溯为例，将工业设备整机中涉及到的各零部件来源、批次、生产日期等信息进行记录并写入区块链网络，在设备运行的生命周期中，将设备使用频次、检修记录、元器件更换记录信息同步至区块链网络，形成整个设备的运行溯源记录，当设备问题发生时，可以直接定位到零部件的来源，找到对应供应商提供对应的零部件完成快速维护。基于设备各部件的维修更换记录，结合实际生产的使用频率，动态计算设备各部件可能出现风险的情况，从而提前进行零部件的储备或者更换，降低工业产生问题的风险。

如图6所示，该场景下涉及到的角色包括：ICT技术提供方，工业应用方，基础设施提供方。该场景下涉及到的子角色包括：ICT硬件提供方，物资管理部门，工业互联网标识解析提供方，工业PaaS。

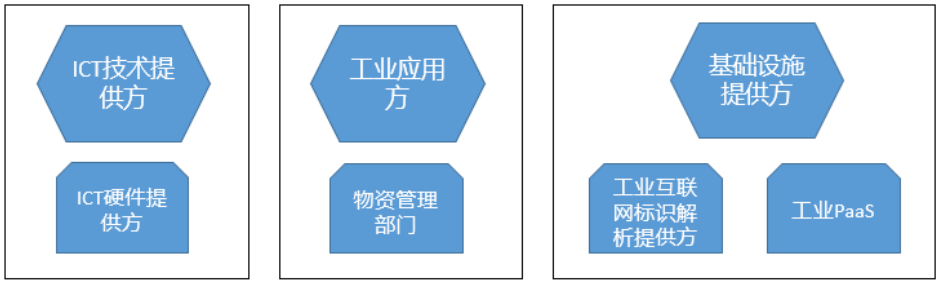

图 6 物资追溯场景涉及到的角色和子角色

6.4.2 物资追溯业务需求

该场景下的业务需求包括：

a) 应对物资追溯业务中的所有参与方进行身份认证，尤其是需要录入数据的角色，应有完整的身份认证记录并发放身份证明证书；
b) 身份证书的存放需要有一个安全且不可篡改的分布式存储系统内，防止身份数据泄露或遭恶意篡改链上数据写入同时，需要加入身份签名，保证数据所属权，对未来验证和备查做准备；
c) 溯源对象应该设定唯一编码，具备唯一性、不可复制性，唯一编码贯穿整个物资生产至销售的全流程，利用该唯一码可以快速读取物资的全部追溯信息；
d) 需要将唯一编码与物资形成某种对应关系，溯源对象与唯一编码进行永久绑定且无法解绑；
e) 利用工业互联网中的设备收集物资生产端信息，并完整记录；
f) 应利用硬件设备来获取信息，硬件设备上传数据也需要进行身份签名；
g) 应保障物资的生产信息或流通信息来源可靠，从本企业生产系统中读取数据；
h) 应保证不同类型企业数据的安全性，对工业互联网中的企业数据进行有效隔离，防止机密数据泄露；
i) 应该设定多种接入方式，保证物资链条中的全部企业都能够接入；
j) 对于不同的物资类别建立不同的数据流通通道，避免数据之间互相干扰。

6.4.3 物资追溯技术需求

如图7所示，该场景下的技术需求包括：

a) 数据源：来自工业设备整机和零部件；数据源可通过业务平台与区块链平台对接；

b） 数据传输：信息交互须通过广域网实现；

c） 数据存储：零件信息的标识、签名和哈希值存储与区块链上，检修记录信息哈希值存储区块链上，零件的具体详细信息存于工业PaaS，节省空间，方便大数据查找；

d） 业务系统：生产企业的业务系统或物资追溯中台须与区块链平台、工业PaaS数据存储对接。

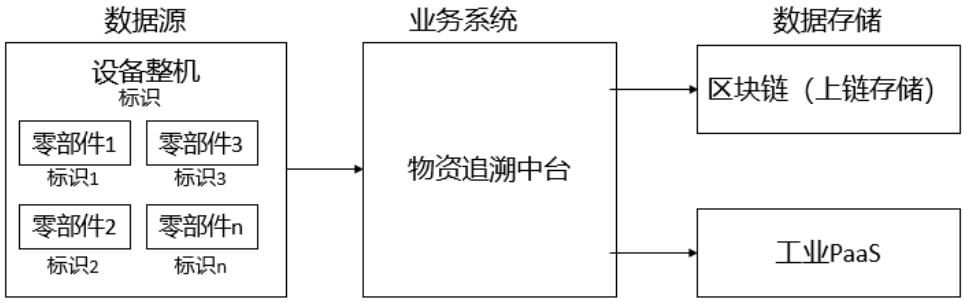

图 7 工业设备物资追溯场景

6.5 供需对接场景

6.5.1 供需对接业务总则

供需高效对接是区块链和智能合约应用的场景之一。以疫情防控场景为例，应急物资管理机构需要及时根据需求与口罩生产企业达成口罩订单合同。

如图8所示，该场景下涉及到的角色，包括：工业应用方、监管方，该场景下涉及到的子角色包括：生产企业、应急物资管理机构。

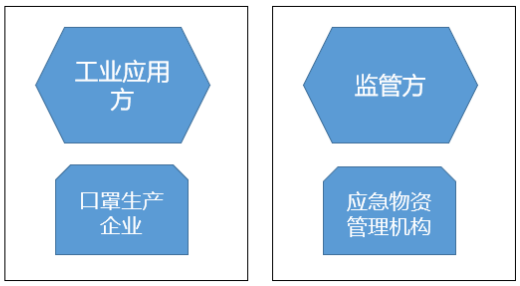

图 8 供需对接场景涉及到的角色和子角色

6.5.2 供需对接业务需求

该场景下的业务需求包括：

a） 须及时、准确获得需求方的需求信息，需求信息的更新周期和具体需求由具体业务需求确定；

b） 须及时、准确获得生产企业的生产能力信息，具体生产能力信息由具体业务需求确定；

a. 需求信息须真实、在一定规则下（如需求信息已经正式与供给方达成协议）不能随意更改；

b. 产品供给交付承诺须真实、在一定规则下（如供给方已经正式与供给方达成协议）不能随意更改；

c） 需求信息与生产企业的匹配规则可被代码化，并可形成基于预定事件触发、不可篡改、自动执行的计算机程序，该程序的结果可被供方和需方认可。

6.5.3 供需对接技术需求

如图9所示，该场景下的技术需求包括：