ICS 33.050
CCS M 30

团　体　标　准

T/TAF XXX-XXXX

物联网终端可信上链技术要求

Technical requirements for trusted blockchain access of IoT Terminals

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

电信终端产业协会　发布

目　　次

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、上海摩联信息技术有限公司、郑州信大捷安信息技术股份有限公司、安谋科技（中国）有限公司、深圳市广和通无线股份有限公司、上海移柯通信技术股份有限公司、杭州宇链科技有限公司、微软（中国）有限公司、深圳市有方科技股份有限公司、青岛海尔通信有限公司、中国联合网络通信有限公司、中国移动通信集团终端有限公司、华为技术有限公司、杭州甘道智能科技有限公司、阿里巴巴（中国）有限公司、北京芯安微电子技术有限公司、四川长虹电子控股集团有限公司、深圳市腾讯计算机系统有限公司、紫光同芯微电子有限公司、紫光展锐(上海)科技有限公司。

本文件主要起草人：许慕鸿、于力、许刚、林瑶、李兰飞、康亮、刘献伦、王骏超、罗俊、潘峰、程希冀、赵刚、于保华、林学春、李洋、谢仁芳、梁小华、张子怡、林炀平、宋学武、黄天宁、王叶松、薛亚辉、魏茂坚、唐博、黄德俊、敖萌、邵兵、周智勇、苏阵阵。

引　　言

随着区块链这种新的信任模式的产生，物联网数据上链之后的抗篡改性得到了广泛的认可。然而区块链本身只能保证数据上链之后抗篡改，还必须保证链上的数据是由真实的物联网终端设备产生的真实数据，才能实现数据信任的全链条传递。

物联网终端设备作为数据源头，是数据信任链条的起点。由于物联网具有高度碎片化的特点，终端差异性很大，因此规范物联网数据上链的技术要求，保证数据安全可信，制定相应标准规范，为规范各设备生产企业遵循要求提供具备数据上链功能的产品，保证上链数据可信供参考指导，具有重要的现实意义。

物联网终端可信上链技术要求

1 范围

本文件规定了物联网终端可信上链技术要求，包括物联网终端可信上链的总体架构、设备功能要求和安全要求等。

本文件适用于不同步账本不参与共识的能力受限的物联网终端设备。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

T/TAF 062-2020 物联网设备安全平台技术要求和分级方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

物联网终端设备 IoT terminal

具备网络（例如蜂窝、WiFi、蓝牙、Zigbee、LoRa等）接入功能，可对物进行信息采集和处理，支持数据通信的终端设备。

3.2

能力受限物联网终端设备 capability-constrained IoT terminal

计算能力、存储能力、通信能力、功耗水平等受限的物联网终端设备。

本文件中指受到上述限制，无法同步区块链账本和参与共识的能力受限物联网终端。

3.3

智能合约（链码） smart contract (chain code)

智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。本规范中，特指运行于区块链上的智能合约。本文件中，术语“智能合约”与术语“链码”等同。

3.4

远程过程调用 remote procedure call (RPC)

设备或主机通过网络，请求远端另一主机提供服务。在区块链网络中，区块链节点向区块链客户端提供远程过程调用接口，以便区块链客户端能够访问区块链服务。

3.5

可信执行环境 trusted execution environment (TEE)

针对开放系统、基于芯片级隔离与安全引导、用于保证程序执行安全与数据存储真实性、完整性、机密性目标构建的一种软件运行环境。其中，芯片级隔离是指基于主芯片安全扩展机制通过对计算资源的固定划分或动态共享，保证所隔离资源不被开放系统访问的一种安全机制。

3.6

完整性 integrity

完整性指对于接收到的数据要保证不会以任何方式被改变。其目的是通过阻止威胁或者探测威胁，保护可能遭到不同方式危害的数据的完整性和数据相关属性的完整性。本文中的完整性指在可信执行环境启动的过程中或者可行执行环境执行过程中，所涉及到的数据、代码等信息要保证不会被恶意的篡改。

3.7

物联网终端上链 IoT terminal to access blockchain

物联网终端上链是指物联网终端，通过与区块链网络约定的方式直接或间接调用链上智能合约，将物联网终端所采集或生成的数据传递给智能合约做链上处理。

4 缩略语

下列缩略语适用于本文件。

BoT：物联网区块链（Blockchain of Things）

dApp：去中心化应用（de-centralized Application）

MAC：消息验证码（Message Authentication Code）

RPC：远程过程调用（Remote Procedure Call）

SE：安全元件（Secure Element）

TEE：可信执行环境（Trusted Execution Environment）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

5 概述

5.1 物联网终端上链参考架构

基于区块链的物联网的网络参考架构如图1所示。

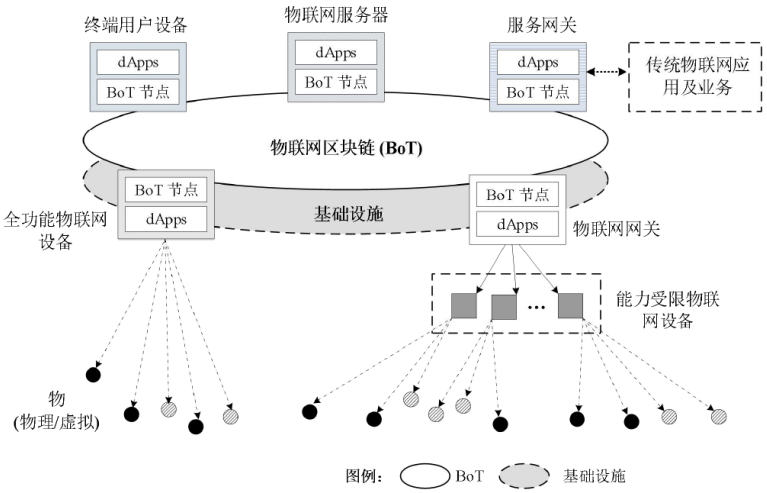

图 1 基于区块链的物联网网络参考架构

注：该参考架构源自中国通信标准化协会《“物联网+区块链”应用与发展白皮书（2019）》。

参考如上架构，区块链网络由一定数量的区块链节点构成。区块链节点依据其功能特点，一般可粗略分为全节点和轻节点。全节点记录和维护完整区块账本，并依照一定规则参与账本共识；轻节点只记录区块头部信息，不参与共识，仅在必要时向全节点查询完整区块内容。

具备较强计算能力、存储能力和通信能力的全功能物联网终端可以作为全节点或轻节点加入区块链网络，但绝大多数物联网终端受成本、功耗等因素限制，其能力通常是较为受限的，能力受限物联网终端难以作为全节点或轻节点直接接入区块链网络。

如无特别说明，本文件所述物联网终端，特指不同步账本不参与共识的能力受限的物联网终端。

在物联网终端上链过程中，物联网终端直接或间接作为客户端向区块链节点发起智能合约调用交易，一般具有如图2所示的典型参考架构。

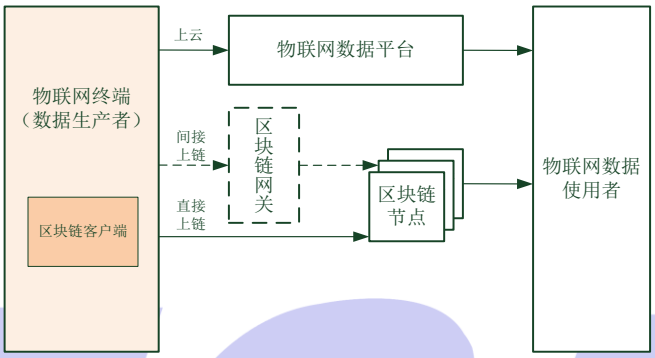

图 2 物联网终端上链参考模型

在物联网终端上链参考模型中，物联网终端作为数据生产者，在原有将数据上云的基础上，将相关信息直接或经由区块链网关间接上链。而物联网数据使用者，则通过访问区块链获得可信的上链数据，并结合云上数据，实现数据的可信使用。

本文件主要针对物联网终端在数据可信上链过程中的技术要求给予规定。

5.2 支持上链的物联网终端参考架构

支持上链的物联网终端作为客户端应具备直接或间接调用链上智能合约的功能，其参考架构如图3所示。

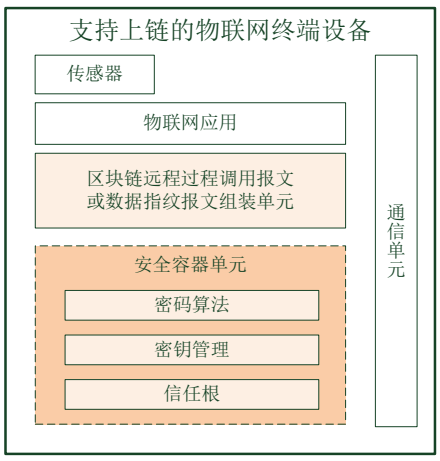

图 3 支持上链的物联网终端参考架构

支持上链的物联网终端应具有：

a) 区块链远程过程调用报文组装单元或数据指纹报文组装单元
   - 区块链远程过程调用报文组装单元用于组装区块链交易的报文，并调用密码算法单元和密钥管理单元进行数字签名后，将已签名的交易报文通过远程过程调用发送给区块链节点或区块链网关。
   - 数据指纹报文组装单元用于计算数据指纹，并将数据及其数据指纹组装成报文，发送给区块链网关。
   - 区块链远程过程调用报文组装单元和数据指纹报文组装单元，根据终端能力应具备其中之一。

b) 密钥管理单元，用于生成、保存、更新、删除物联网终端用于访问区块链的密钥。

c) 密码算法单元，用于执行密码学算法计算。

d) 安全容器单元（可信执行环境或安全元件）（可选），用于对密钥及密码学算法的执行环境进行保护。

e) 信任根（可选），用于为终端提供唯一的身份标识，并提供身份认证方法。

6 终端安全要求

6.1 安全目标

物联网终端可信上链的安全目标是使其上链的数据具有可溯源、可验真等特点，且在数据传播过程中能够保持可信。

由于物联网终端差异性较大，安全目标分为两个类别来考虑：

a) 抗远程攻击：攻击者与终端无物理接触的情况下，抵抗其远程攻击，例如：
   - 抵御攻击者在真实终端数据上链途中篡改数据。
   - 抵御攻击者伪装成区块链节点或区块链网关诱骗终端访问。
   - 抵御攻击者伪装成真实终端伪造数据上链。

b) 抗本地攻击：攻击者与终端有物理接触（例如本地连接并登录终端设备、对终端设备进行测量、拆解终端设备等）条件下，抵抗其物理攻击，例如：
   - 抵御攻击者窃取密钥及非法克隆真实终端设备。
   - 抵御攻击者侵入终端设备、篡改证书和程序，伪造上链数据。

根据以上安全目标，制定以下相应的安全要求，其中，6.2节所述基本安全要求主要针对抗远程攻击的安全目标，6.3节所述增强安全要求主要在此基础上增强抗本地攻击的安全目标。

6.2 基本安全要求

作为基本安全要求，上链终端应当具备抵御来自通信链路的远程攻击的能力。这些攻击行为通常从远程网络发起，攻击者不直接或近距接触被攻击的终端设备，常见手段包括利用软件漏洞侵入设备并非法获取信息、在通信链路中篡改数据、篡改DNS使终端访问钓鱼服务器等。

上链终端应当满足如下基本安全要求：

a) 终端所使用的区块链密钥对应一机一密，不得批量终端共用相同的密钥对。

b) 终端与区块链节点或区块链网关建立连接时，应当对区块链节点或区块链网关进行认证，认证通过后才能进行业务通信。

c) 连接区块链节点或网关的信道应进行加密。

d) 上链数据宜加密。

e) 如使用TLS、TLCP等进行认证并建立安全通道，应采用无已知重大安全漏洞的版本。

f) 如果终端允许通过口令进行远程登录，不得在生产时设定统一的默认登录口令。

g） 密钥、口令复杂度及相关密码算法应符合相关国家标准和行业标准。
h） 终端应遵循不开放无必要的服务端口的原则。

6.3 针对不同终端的增强安全要求

6.3.1 概述

针对增强安全要求，如终端不具备可信执行环境和安全元件，则应满足以下6.3.2节中相关要求；如终端同时具有可信执行环境和安全元件，相关安全要求满足6.3.3和6.3.4节中的一种即可。

6.3.2 级别一终端

本级别终端应满足如下安全要求：

a） 区块链私钥在非易失性存储器中持久化存储时，应采用软件混淆（Obfuscation）方式加以保护，所述软件混淆的常见技术如符号重命名、死代码插入、代码重排序、指令替代、代码加密等。
b） 区块链私钥及用于加密等目的的对称密钥在易失性存储器中，应遵循用后即毁原则，不得长时间保留在易失性存储器中。
c） 若终端操作系统具备访问权限控制能力，区块链私钥以及相关证书应存放在限制访问的区域。
d） 若终端操作系统具备访问权限控制能力且允许本地登录，则终端应具备设备生命周期管理能力，且在出厂时应禁止默认以具有不受限权限的身份本地登录。

6.3.3 级别二终端

a） 终端具备可信执行环境（TEE），并满足T/TAF 062-2020所述一级或以上安全要求。
b） 区块链私钥应在可信执行环境内安全保存，私钥不得离开可信执行环境。
c） 上链相关证书应在可信执行环境内安全保存。
d） 上链相关且涉及密钥的密码学运算应在TEE内执行。

6.3.4 级别三终端

a） 终端具备安全元件（Secure Element），并满足T/TAF 062-2020所述一级或以上安全要求。
b） 区块链私钥应在安全元件内安全保存，私钥不得离开安全元件。
c） 上链相关证书应在安全元件内安全保存。
d） 上链相关且涉及密钥的密码学运算应在安全元件内执行。

7 终端上链功能要求

7.1 上链基本功能要求

物联网终端数据上链，是指物联网终端作为客户端访问链上的智能合约服务，并且通常（但不限于）以物联网数据作为访问智能合约服务时的参数。对区块链上智能合约而言，物联网终端通过数据上链的过程，扮演了区块链预言机（Oracle）的角色。上链的数据既可在合约中存储下来用于后续可信验真，也可以作为合约逻辑输入条件或运算的输入参数等。

不同的区块链在远程过程调用（RPC）接口协议、密码算法、流程等方面有所差异，但终端数据上链一般应遵循如下基本功能要求：

a） 物联网终端应当能够产生区块链私钥，或者能够在生产时向物联网终端注入区块链私钥。
b） 区块链私钥应当能够在受控条件下更新或销毁。

c） 物联网终端应当能够配置和/或感知区块链节点或网关的必要参数。
d） 物联网终端应当能够按照约定接口和协议，组装区块链智能合约调用报文或其他远程过程调用报文，并解析其响应。
e） 如果终端数据同时上云和上链，终端应建立两者的关联。

7.2 上链内容要求

7.2.1 数据原文上链功能要求

物联网数据原文上链，指物联网终端上链的数据中，包含了终端所采集的原始数据，或者经端侧清洗处理且仍反映原始信息的数据。通常，若链上智能合约包含对具体物联网数据内容的处理（例如根据数据的值进行特定的逻辑处理），则上链数据中应包含相应的原始数据或能反映原始信息的数据。

数据原文上链，一般应满足以下功能要求：

a） 应遵循最小必要原则，控制上链的数据量和上链频度，避免区块链网络拥塞。
b） 若上链数据涉及需授权访问的信息，应对数据内容进行加密，并通过密钥分发体系向被授权方分发访问密钥。
c） 若上链数据涉及个人信息，应根据需要按最小必要上链。

7.2.2 数据指纹上链功能要求

物联网数据指纹上链，指物联网终端上链的数据，是反映终端所采集的原始数据特征的摘要。这些摘要不直接反映原始信息，但能够验证原始数据的完整性，故称为数据指纹或数据特征值。通常，若通过区块链实现数据验真，则可以采取原始数据上云，数据指纹上链的方式组合进行。

数据指纹上链，一般应满足以下功能要求：

a） 数据指纹可采用杂凑密码算法计算获取。
b） 被计算指纹的数据，可以是原始数据，也可以是经过端侧清洗处理且仍包含原始信息的数据。
c） 数据指纹上链一般与数据上云结合使用，链上的数据指纹用于在事后验证云上数据的完整性。
d） 上链的数据指纹可以与上云的数据一一对应，也可将若干组上云数据的指纹组合起来（例如以默克尔树的形式组合），计算指纹组合的指纹，将该指纹组合的指纹（例如默克尔树根）上链，以降低数据上链的频度和数量。
e） 若上链的数据指纹与上云的数据一一对应，上链信息和/或上云信息中应包含能够关联两者的标识；若上链的数据指纹与一组上云数据对应，则上链信息中应包含能够关联该链上数据指纹与云上数据组的信息。

7.3 上链路径要求

7.3.1 直接上链功能要求

终端直接上链指物联网终端组装区块链交易报文，并直接访问区块链节点实施数据上链。若物联网终端具备按照约定接口和协议，组装区块链智能合约调用报文或其他远程过程调用报文并解析其响应的能力，并且能够与区块链节点建立双向通信，则物联网终端可以直接上链。

7.3.2 间接上链功能要求

7.3.2.1 概述

物联网终端可能因多种原因，无法直接访问区块链节点的服务。这些原因常常包括，物联网终端处在某个内网中且不能直接连接互联网；蜂窝物联网终端的流量为定向流量且不能连接区块链节点；物联

网终端不支持区块链节点远程过程调用所使用的通信协议;物联网终端不支持区块链交易所要求的密码算法等。

在物联网终端不能直接访问区块链节点服务时，可将上链数据发送至区块链网关，再由区块链网关上链。

7.3.2.2 具备组装区块链调用报文能力的终端

若物联网终端具备按照约定接口和协议,组装区块链智能合约调用报文或其他远程过程调用报文并解析其响应的能力，但由于通信链路、通信协议等原因，物联网终端无法直接访问区块链节点服务，在此情况下，可经由区块链网关转发上链，并应满足以下要求：

a) 物联网终端与区块链网关应能建立双向通信连接。
b) 物联网终端组装区块链远程过程调用报文（包括必要时使用其区块链私钥进行签名），将报文整体发送给区块链网关，网关在物联网终端与区块链节点之间做报文及其响应的转发。
c) 若物联网终端不支持区块链节点远程过程调用接口的通信协议（通常为HTTP/HTTPS），但支持区块链网关所支持的其他通信协议（例如MQTT），则区块链网关进行协议转换和转发。

7.3.2.3 具备数字签名能力的终端

若物联网终端不具备组装区块链智能合约调用报文或其他远程过程调用报文的能力,但支持数字签名，在此情况下，可经由区块链网关二次签名后上链，并应满足以下要求：

a) 物联网终端应支持数字签名密码算法并具有终端公私密钥对（不要求与区块链采用相同的密码算法）。
b) 区块链网关应具有区块链密钥对，且其安全性不低于对终端的要求。
c) 物联网终端使用终端私钥对上链数据进行签名，并将上链数据、签名以及终端公钥（或可关联终端公钥的其他信息）发送给区块链网关。区块链网关将这些数据构造为区块链远程过程调用报文，并使用其自身的区块链私钥签名上链。
d) 后续的数据验真过程中，应包含对终端签名的验证。

7.3.2.4 具备对称加密能力的终端

若物联网终端不具备数字签名能力，但具备对称密钥以及对称加密密码算法能力，在此情况下，可经由区块链网关二次签名后上链，并应满足以下要求：

a) 物联网终端应支持对称加密密码算法并具有已经过登记的对称密钥;
b) 区块链网关应具有区块链密钥对，且其安全性不低于对终端的要求。
c) 物联网终端使用对称加密对上链数据计算消息认证码（MAC），并将上链数据、消息认证码以及可以关联终端对称密钥的信息（例如设备唯一标识）发送给区块链网关；区块链网关将这些数据构造为区块链远程过程调用报文，并使用其自身的区块链私钥签名上链。
d) 后续的数据验真过程中，应包含对终端消息认证码的验证。

7.3.2.5 不具备可独立调用的数字签名和加密能力的终端

若物联网终端既不具备可独立调用的数字签名能力，也不具备可独立调用的对称加密能力，在此情况下，物联网终端可将数据传送给区块链网关，由区块链网关签名后上链，并应满足如下要求：

a) 物联网终端应将上链数据以及设备唯一标识发送给区块链网关；区块链网关将这些数据构造为区块链远程过程调用报文，并使用其自身的区块链私钥签名上链。
b) 若区块链网关本身亦为物联网数据平台，应尽量缩短从收到物联网终端上传的数据，到将数据上链的间隔。

此场景退化为区块链网关的数据上链，物联网终端仅提供数据来源，但不提供任何可验证数据来源及完整性的密码学凭据，因此，链上数据信任只能验证到区块链网关，不能验证到物联网终端。此类终端上链的数据，应当关注数据信任的局限性。

注：“可独立调用”指该算法可以基于单独的密钥被单独调用。如果终端虽然具备数字签名或对称加密能力，但该能力封装于其他不可拆解的过程中，无法被单独调用，则不属于“可独立调用”。例如，封装于AT命令中的HTTPS传输命令，虽然其中必然包含相关密码学算法，但如果不可拆出来单独调用，则不属于“可独立调用”。

7.4 区块链节点连接与容错功能要求

物联网终端至少需要直接或间接连接到一个区块链节点实现数据上链。

为获得更佳的容错性，终端宜具备以下能力：

a) 多节点连接能力：可以为终端配置多个区块链节点，并依据一定规则选择可用节点。

b) 节点发现能力：终端通过约定的链上或云上服务，获得可用节点列表，并依据一定规则选用。

c) 拜占庭容错能力：终端依据容错要求，与多个节点分别建立针对同一交易的远程过程调用，并遵照容错算法聚合不同节点的调用结果，从而容忍一定数量的恶意或失效节点。

附 录 A
（资料性）
物联网终端可信上链及数据验真参考模型

A.1 物联网终端直接上链参考模型

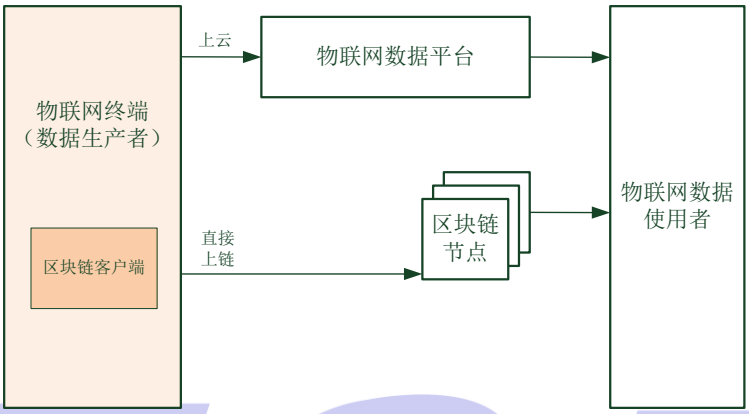

图 A.1 物联网终端直接上链参考模型

物联网终端直接上链的参考模型见图A.1,其前置条件为：

a） 区块链上已经部署存储数据的智能合约；
b） 物联网终端具备组装区块链合约调用交易报文的能力，并能连接区块链节点；
c） 物联网终端已经生成或注入区块链公私密钥对。

物联网终端数据直接上链及验真过程为：

a） 物联网终端采集或产生物联网数据，物联网数据中包含终端唯一标识（例如蜂窝设备的IMEI）以及时间戳；
b） 物联网终端计算物联网数据的第一杂凑值；
c） 物联网终端构造智能合约调用交易报文并以终端区块链私钥签名，将终端唯一标识、时间戳以及第一杂凑值在交易中传递给智能合约；
d） 智能合约保存终端唯一标识、时间戳以及第一杂凑值；
e） 物联网终端将物联网数据上传到云端物联网数据平台；
f） 物联网数据使用者从云端物联网数据平台取得物联网数据，并计算其第二杂凑值；
g） 物联网数据使用者根据物联网数据中包含的终端唯一标识和时间戳信息，从区块链智能合约取得对应的第一杂凑值；
h） 物联网数据使用者比较第一杂凑值与第二杂凑值是否相同，如果相同，表明该数据在物联网数据平台存储期间未发生过篡改。

A.2 具备数字签名的物联网终端间接上链参考模型

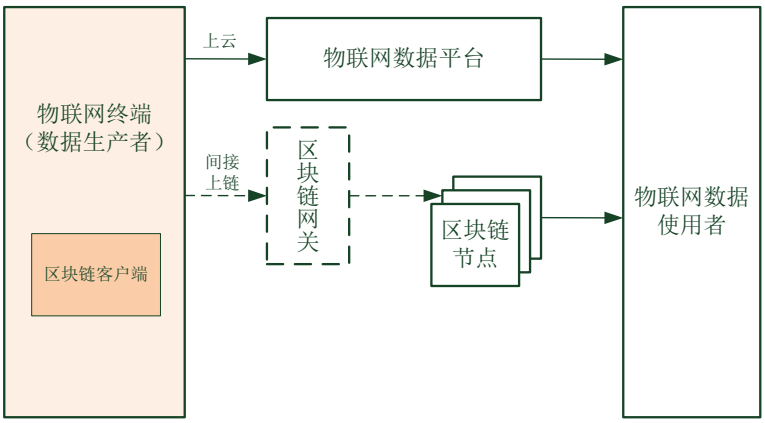

图 A.2 物联网终端间接上链参考模型

物联网终端间接上链的参考模型见图A.2，其前置条件为：

a） 区块链上已经部署存储数据的智能合约；

b） 物联网终端不具备组装区块链合约调用交易报文的能力，但具备数字签名能力；

c） 物联网终端已经生成或注入终端公私密钥对（不要求与区块链采用相同的密码算法）；

d） 区块链网关已生成或注入网关区块链公私密钥对。

物联网终端数据间接上链及验真过程为：

a） 物联网终端采集或产生物联网数据，物联网数据中包含终端唯一标识以及时间戳；

b） 物联网终端计算数据的第一杂凑值；

c） 物联网终端以终端私钥，对第一杂凑值进行签名，并将终端唯一标识、时间戳、终端签名以及终端公钥传递给区块链网关；

d） 区块链网关构造智能合约调用交易报文并以网关区块链私钥签名，将终端唯一标识、时间戳、终端签名以及终端公钥在交易中传递给智能合约；

e） 智能合约保存终端唯一标识、时间戳、终端签名以及终端公钥；

f） 物联网终端将物联网数据上传到云端物联网数据平台；

g） 物联网数据使用者从云端物联网数据平台取得物联网数据 ；

h） 物联网数据使用者根据数据中包含的终端唯一标识和时间戳信息，从区块链智能合约取得对应的终端签名和终端公钥；

i） 物联网数据使用者根据物联网数据计算其第二杂凑值，并使用终端公钥和终端签名对第二杂凑值进行验签。如果验签通过，表明该数据来自真实物联网终端，未发生过篡改。

附 录 B
（资料性）
物联网终端上链应用场景

B.1 生物资产贷款场景

基于区块链的牛联网是生物资产链上管理一个典型场景。在本场景中，牛项圈中包含一个具备上链能力的物联网终端。该终端采集牛的生命体征信息、地理位置信息，将这些信息上传至云端畜牧管理平台，同时将其杂凑值上传至区块链。基于这些可信的生物信息，构建牛的可信数字孪生，令牛可以成为金融机构能够接受的抵押资产，使得金融机构可以对其进行有效的风险监管，并基于此发放贷款。

B.2 车辆资产残值估值场景

车辆将对车辆残值具有重要意义的车辆年限、行驶里程以及可表征事故嫌疑的车辆传感器信息脱敏上传至车企数据平台，同时将其杂凑值上传至区块链。在进行二手车交易时，根据车企数据平台上的信息，并利用区块链对数据进行验真，使得二手车价格能够较为客观的反映车辆残值。

B.3 充电桩运营融资场景

充电桩每次充电产生的交易信息经脱敏加密后，上传到区块链保存。充电桩运营企业在进行融资时，授权投资方查看链上的历史运营信息，使得投资方能够根据可信的运营状况，给予企业较为客观的估值和投资。

参 考 文 献

[1] 中国通信标准化协会《物联网+区块链”应用与发展白皮书（2019）》

电信终端产业协会团体标准

物联网终端可信上链技术要求

T/TAF XXX—XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn