国际电信联盟
电信标准化部门

建议书

ITU-T F.751.8 (07/2023)

F系列：非话电信业务

多媒体业务

利用分布式总账技术（DLT）遵从监管的技术框架

ITU-T F系列建议书

非话电信业务

电报业务	F.1-F.109
国际公众电报业务的操作方法	F.1-F.19
国际公众电报网	F.20-F.29
报文交换	F.30-F.39
国际话传邮递电报业务	F.40-F.58
国际用户电报业务	F.59-F.89
国际电报业务的统计数据和出版	F.90-F.99
定时开放的和租用的通信业务	F.100-F.104
相片电报传真业务	F.105-F.109
移动业务	F.110-F.159
移动业务和多目的地卫星业务	F.110-F.159
远程信息处理业务	F.160-F.399
公众传真业务	F.160-F.199
智能用户电报业务	F.200-F.299
可视图文业务	F.300-F.349
远程信息处理业务的一般规定	F.350-F.399
报文处理业务	F.400-F.499
号码簿业务	F.500-F.549
文件通信	F.550-F.599
文件通信	F.550-F.579
程序设计通信接口	F.580-F.599
数据传输业务	F.600-F.699
多媒体业务	**F.700-F.799**
ISDN业务	F.800-F.849
通用个人通信	F.850-F.899
人为因素	F.900-F.999

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T F.751.8建议书

利用分布式账本技术（DLT）遵从监管的技术框架

摘要

ITU-T F.751.8建议书定义了分布式账本技术（DLT）的技术框架，从而能够遵从监管的要求，包括应对监管方面挑战和拥有相关技术能力。本建议书中的DLT技术框架设计与DLT特性密切相关，涉及去中心化、不可变性和开放性。当DLT服务提供商和DLT系统开发商面临监管时，本建议书可用作DLT系统的指南。

历史沿革*

版本	建议书	批准	研究组	唯一识别码
1.0	ITU-T F.751.8	2023-07-10	16	11.1002/1000/15174

关键词

区块链、分布式账本技术、监管。

* 欲查阅建议书，请在您的网络浏览器地址域键入URLhttps://handle.itu.int/，随后输入建议书的唯一识别码。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T F.751.8建议书

利用分布式总账技术（DLT）遵从监管的技术框架

1 范围

本建议书定义了分布式账本技术（DLT）的技术框架，从而能够遵从监管的要求。本建议书的范围涵盖：

– 与DLT相关的监管挑战；

– DLT遵从监管要求的技术能力。

本建议书的目标用户是DLT服务提供商和DLT系统开发商。DLT监管机构并非目标用户。本建议书的目的并非为DLT监管机构提供监管解决方案，而是针对与DLT法规相关的挑战提出技术解决方案。

2 参考文献

下列ITU-T建议书及其他参考文献含有通过本文的引用构成本建议书条款的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此，鼓励本建议书的用户了解使用最新版本的下列建议书和其他参考文献的可能性。当前有效的ITU-T建议书清单定期出版。 本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T F.751.0] ITU-T F.751.0建议书（2020年），分布式账本系统的要求。

[ITU-T X.1401] ITU-T X.1401建议书（2019年），分布式账本技术面临的安全威胁。

3 术语和定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 共识（**consensus**）[b-ITU-T X.1400]：就一组交易有效达成一致。

3.1.2 共识机制（**consensus mechanism**） [b-ITU-T X.1400]：达成共识的规则和程序。

3.1.3 分布式账本（**distributed ledger**）[b-ITU-T X.1400]：指的是一种以分布式和去中心化方式共享、复制和同步的账本类型。

3.1.4 私密性（privacy）[b-ITU-T J.160]：确保信息不被披露给目标对象以外的人的方法。通常通过加密来确保信息的保密性。又称“保密性”。

3.1.5 威胁（threat）[b-ISO/IEC 27000]：可能对系统或组织造成损害的意外事故的潜在原因。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

AML 反洗钱

DLT 分布式账本技术

FATF 洗钱问题金融行动特别任务组

IoT 物联网

KYC 了解你的客户

PKI 公钥基础设施

TEE 可信执行环境

5 惯例

本建议书使用了以下惯例：

– 关键词**“要求”（is required to**）指的是一项必须严格遵守的要求，如果宣称遵循本建议书，则不得违反。

– 关键词**“建议”（is recommended**）指的是一项建议性的、并非绝对需遵守的要求，因此，宣称遵循本建议书时无需提及该项要求。

– 关键词**“可选”（can optionally**）和**“可能”**指的是一项允许的可选要求，不隐含任何建议的意味。本术语无意暗示供应商的实施方案必须提供选项，以及网络运营商/服务提供商可以选择启用该功能。相反地，本术语意味着供应商可以选择提供该功能，并仍宣称遵循本规范。

6 概述

分布式账本技术（DLT）使分布式账本网络中的大量节点能够在没有中央机构的情况下达成协议并记录信息。DLT的快速发展为监管带来了挑战，其中包括隐私/机密的保护、数据保护的监管、网络攻击的处理和加密货币的监管等。DLT已应用于加密货币、供应链管理和物联网等多个领域。因此，有必要在分析DLT功能和属性的基础上总结监管要求，并定义技术框架，以填补开放与监管之间的空白。一些准备工作已在[b-DLT 4.1]中完成，并在下文所述技术规范中得到发展。

7 监管挑战

7.1 机密信息的泄露

将外部数据与链上或链下数据结合，可能会直接在链上泄露机密信息。交易和公钥可以在链上直接获得，特别是在无许可的DLT系统中。外部数据可能允许识别个人或公司的公钥，并在此基础上识别交易。

无许可分布式分类账没有访问控制，所有人都可以访问直接存储在链上的所有数据。将（未加密的）机密数据存储于未经许可的分布式账本被视作泄露机密数据。

7.2 记录的不可变性和不存在擦除交易/内容的功能

根据DLT应用程序和数据类型，监管要求擦除个人数据。法律法规中的此项要求可能会与DLT体系的不可变性产生冲突。

注 – 欧盟通用数据保护法规（[b-GDPR]）第17条中的“遗忘权”便是数据擦除要求的一例。

数据保护法规和其他法律亦可能要求更正交易。这只有通过将分布式分类账系统的可靠性置于风险之中的分支才有可能实现。

7.3 安全威胁

对DLT组件的安全威胁是指[ITU-T X.1401]的第5.1条（对协议的威胁）、第5.2条（对网络的威胁）和第5.3条（对数据的威胁）。

7.4 代币、数字货币和其他资产的损失

代币、数字货币和其他资产的丢失通常源自数据威胁。但是，这些损失也可能源自欺诈性币、欺诈性分布式分类账系统或账户地址背后实体的故意欺骗。网络钓鱼攻击也可能诱使人们实施他们原本不会进行的交易。

7.5 金融犯罪和其他犯罪

分布式账本系统可用于洗钱等金融犯罪，或为勒索软件攻击等其他犯罪提供便利。交易可能包含遵守协议规则但与法规及其他法律相冲突的非法内容。

8 遵从监管的技术能力

8.1 技术框架

DLT遵从监管的技术框架设计与DLT属性密切相关，其中涉及分权、自治、不可变性、公开性、透明度和匿名性。DLT遵从监管的技术能力从以下方面定义：应用层、隐私/保密性、数据擦除、数据安全和基础层。在获得许可的DLT中，问责制至关重要，因此建议DLT服务提供商确定一个底层协调法律实体，以减少监管行动的不确定性。

8.2 应用层的能力

– 建议用于转移数字资产的DLT系统建立支持FATF规则和/或特定国家法规的模块。

– 在获得许可的DLT中，建议使用基于公钥基础设施（PKI）的签名等技术，为了解您的客户（KYC）和反洗钱（AML）功能提供支持。

– DLT服务提供商和系统开发人员可选择使用限制交易权限和封闭账户等技术，干预恶意和异常节点创建的交易。

– DLT服务提供商和系统开发商可选择提供官方认可的PKI链接。此方法可以选择性地用于识别与法人实体的交易。

8.3 隐私/保密能力

– 建议DLT系统不要发布机密信息或个人数据，包括账户身份信息、个人数据/个人身份信息、交易数据、数字资产信息和其他机密信息，但有正当理由发布这些信息的情况除外。

– 不建议在未经许可的DLT系统内存储包含此类信息的数据。如果此类信息需要通过DLT系统验证，建议仅在DLT系统内存储数据的承诺或其他证明。

– 如果无法避免将数据存储在DLT系统内，则建议使用加密方法，如零了解证明、账户混淆或基于硬件隔离（即TEE）的方法，以保护机密数据（业务数据或个人数据）不被泄露。
– 建议通过适当的加密方法妥善保护存储在链下的机密数据。
– 建议存储机密信息的DLT系统提供适当的访问控制，以确保只有授权的访问方可实施。建议将访问权限限制于获得授权的人员和/或获得授权的情况。
– 建议链下存储使用适当的访问控制方法。
– 加密、零了解证明和加密哈希函数可用于保护链上的信息。然而，在不可变链上存储面临的挑战是无法阻止恶意用户使用遭破坏的访问方法进行访问。建议对机密/个人数据的链上存储进行风险分析和/或数据保护影响分析。

8.4 数据擦除能力

高水平的不可变性是分布式总账系统的一项关键属性。因此，彻底取消不可变性通常会违背最初选择分布式分类账系统的初衷。

如果不希望事务的所有属性都具有不可变性，则建议在链下存储数据并且只对这些数据进行验证，例如，通过存储证明验证链下数据。为此，诸如零了解证明、数据提交或散列值之类的技术可以选择怀地存储于链上。需要适当注意的是，不得从存储在链上的数据中获得不需要的信息。

在某些用例中，验证离线数据可能还不充分，仍需要数据持久性。尽管如此，但数据持久性可能只在特定的一段时间内有需要，或者在满足某些条件时才有需要。这种用例仅当不存在后续交易时才需要保存交易数据，且需要保存特定时间段（例如，10年）的记录。在这些情况下，可以选择建立一个分布式分类账，在后续交易完成或经过一段时间后自动删除这些数据。可以选择使用修剪[b-Nakamoto]和变色龙哈希[b-Camenisch]等技术。

当使用这种技术时

– 应明确规定分类账的哪些部分应保持不变；
– 应明确规定在什么条件下可以更换其他部分；
– 分布式分类账的协议应规定如何擦除该数据；
– 分布式分类账的协议应确保要求不被擦除或修改的数据仍然受到保护，不会被修改；
– 应确保仅根据适用法规保存分类账的存档副本。

擦除数据的目的是响应当地法律、建议或其他法规的要求。建议将擦除功能限制在数据的某一部分，以便保持对其余数据不可变性的信任。

8.5 数据安全能力

– 建议DLT服务提供商和系统开发商确保使用加密技术和其他技术的DLT系统设计能够满足DLT服务的安全性和性能要求，包括可靠性、完整性和不可变性，特别是通过使用适当的加密算法和共识机制满足相关要求。
– 建议DLT服务提供商和系统开发商确保链上数据的一致性。

8.6 基础层的能力

– 建议DLT服务提供商和系统开发商采取适当措施，确保DLT网络的完整性、保密性、可执行性、可用性和使用。

– 建议DLT系统开发人员使用适当的安全框架应对网络威胁。

– DLT服务提供商和系统开发商可以选择使用扩展计算能力或投入资源等方法来防止共识攻击。

– 建议DLT服务提供商和系统开发商通过正式验证或其他漏洞检测方法，为在DLT系统运行的智能合约支持安全保障。

– DLT系统开发人员可以选择在DLT系统中设计针对恶意节点的容错功能。当一组正常节点出现故障或成为恶意节点时，建议DLT系统进行恢复。

参考文献

[b-ITU-T J.160] Recommendation ITU-T J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-Camenisch] Camenisch J., Derler D., Kernn S., Pöhls H. C., Samelin K., and Slamanig D. (2017), *Chameleon-hashes with ephemeral trapdoors and Applications to Invisible Sanitizable Signatures*, Public-Key Cryptography , Berlin, Springer, pp. 152–182. https://doi.org/10.1007/978-3-662-54388-7_6.

[b-DIN SPEC 4997] DIN SPEC 4997 (2020), *Privacy by blockchain design: A standardised model for processing personal data using blockchain technology*.

[b-DLT 4.1] ITU-T HSTP.DLT-RF (2019), *Distributed ledger technologies: Regulatory framework.*

[b-GDPR] European Union General Data Protection Regulation law, Article 17, *Right to erasure ('right to be forgotten')*, https://gdpr.eu/article-17-right-to-be-forgotten/.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-Nakamoto] Nakamoto S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	**非话电信业务**
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	数据网、开放系统通信和安全性
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦