国 际 电 信 联 盟

ITU-T X.1407

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务（2） – 分布式账本技术（DLT）安全

基于分布式账本技术的数字完整性证明服务的安全要求

ITU-T X.1407 建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账本技术（DLT）安全	**X.1400–X.1429**
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1407 建议书

基于分布式账本技术的数字完整性证明服务的安全要求

概述

X.1407建议书规定了基于分布式账本技术（DLT）的数字完整性证明服务的安全威胁和需求。

当受保护的原始证明存储于链下而哈希的数据值存储于链上时，X.1407建议书分析此类基于DLT的数字完整性证明服务（即证明注册和证明起源）面临的安全威胁。本建议书还描述了可以解决这些安全威胁的安全要求。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1407	2022-01-07	17	11.1002/1000/14800

关键词

数字完整性证明、分布式账本技术、安全威胁和需求

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）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”等其它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它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，国际电联没有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通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询可通过ITU-T网站获得的适当的ITU-T数据库，网址为：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1407建议书草案

基于分布式账本技术的数字完整性证明服务的安全要求

1 范围

本建议书规定了基于分布式账本技术（DLT）的实体完整性数字证明中的安全威胁和需求。基于DLT的数字完整性证明平台使用分布式账本技术为分布、查询和跟踪实体完整性数字证明提供服务。

2 参引

下列ITU-T建议书和其他参引包含的条款，通过本文的引用构成本建议书的条款。在出版时，所指示的版本有效。所有建议书和其他参引均可能进行修订；因此，鼓励本建议书的用户研究应用建议书最新版本和下面列出的其他参引的可能性。定期发布当前有效的ITU-T建议书清单。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[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。

[ITU-T X.1402] ITU-T X.1402建议书（2020年），分布式账本技术的安全框架。

[ITU-T X.1404] ITU-T X.1404建议书（2020年），分布式账本技术的安全保证。

3 定义

3.1 他处定义的术语

本建议书使用了[b-ISO 23257]第1.4节和他处定义的以下术语：

3.1.1 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。

3.1.2 分布式账本技术（distributed ledger technologies）（DLT） [b-ISO 22739]：能够操作和使用分布式账本的技术。

3.1.3 分布式账本技术平台（distributed ledger technology platform） [b-ISO 22739]：一组处理、存储和通信实体，它们共同在每个DLT节点上提供有关DLT系统的能力。

3.1.4 完整性（integrity） [b-ISO/IEC 13491-2]：数据未被以未授权方式修改或破坏的特性。

3.1.5 账本（ledger） [b-ITU-T X.1400]：保存交易最终和确定（不可变）记录的信息存储。

3.1.6 智能合约（smart contract） [b-ISO 22739]：存储于DLT系统中的计算机程序，当中程序的任何执行结果都记录于分布式账本上。

3.1.7 威胁（threat）[b-ISO/IEC 27000]：可能对系统或组织机构造成伤害的有害事件的潜在起因。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

DDoS 分布式拒绝服务

DLT 分布式账本技术

PoS 权益证明

PoW 工作证明

PBFT 实用拜占庭容错

5 惯例

本建议书采用以下语言方式来表达规定：

a) “Shall”（须/宜）表示要求；

b) “Should”（应/应该）表示建议；

c) “May”（可/可以）表示允许；

d) “Can”（能/可能）表示可能性或能力。

6 概述

在数据分散在不同系统中的情况下，证明某些数据完整性的过程是一个挑战。此外，检查完整性的过程可能需要在许多数据库、系统中进行搜索，或者需要人工在硬拷贝中进行搜索。这种情况是由于交易缺少完整的历史记录；结果是，这可能导致延迟、额外工作和成本以及错误的决策。DLT是一种防篡改、去中心化的账本，它为在不使用中介的情况下进行价值交换建立一种必要的信任水平。它依靠的是去中心化的数据库，来为所有交易提供完整性、协作性、透明、可验证和可审计的记录。因此，DLT的可跟踪、防篡改特性为数字完整性证明提供了解决方案，在没有检测更改之方法的情况下，原始数据不会被欺骗性地创建或破坏。

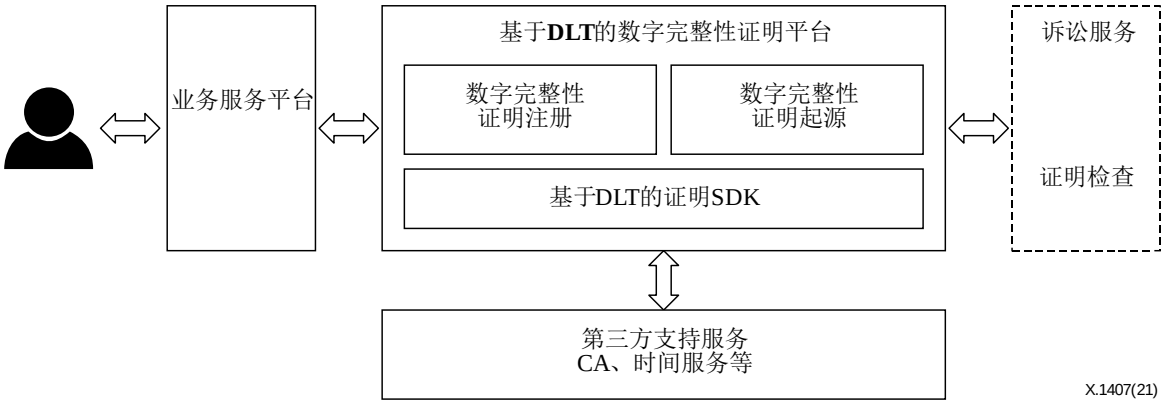


图1 – 基于DLT的数字完整性证明图解

基于DLT的数字完整性证明平台上的基本场景包括证明注册和证明起源。业务服务平台上的用户发起数字证明服务调用，在DLT上注册证明，并通过IP证明注册合约存储提取的数字签名哈希值。检查证明完整性的过程取决于检查证明的哈希值，并将哈希值与存储在DLT上的哈希值进行比较。此外，为保证数字证明的合法使用和保护用户的权益，为在线诉讼的取证提供数字证明查询和检查服务。

尽管DLT的可追溯、防篡改特性可更好地控制和利用记录的完整性，但在采用DLT中存在安全威胁。一些威胁针对的是用户，一些针对的是数字证明，其他针对的是证明注册和起源过程。因此，依据对基于DLT的数字完整性证明所涉活动的分析，总结不同类别的安全威胁是必要的且是有用的。基于对这些威胁的分析，确定了一组安全要求。

7 基于DLT的数字完整性证明的利益攸关方和流程

7.1 利益攸关方

7.1.1 内部利益攸关方

内部利益攸关方应包括：

a) 用户；

b) 业务服务平台；

c) 基于DLT的数字完整性证明平台。

7.1.2 外部利益攸关方

外部利益攸关方包括：

a) 第三方支持服务，包括提供CA证书发放、时间服务和其他服务等组织机构；

b) 监管机构，包括国家司法机构和其他诉讼相关的组织机构。

7.2 基于DLT的数字完整性证明的流程

7.2.1 数字完整性证明注册

DLT上数字完整性证明注册的关键流程包括：

a) 用户与业务服务平台进行交互，可产生保护业务相关信息真实性的需求，业务平台将提取的原始信息特征发送给基于DLT的数字完整性证明平台；

b) 基于DLT的数字完整性证明平台生成具有提取之特征、时间戳及其他必要信息的电子证据；

c) 基于DLT的数字完整性证明平台通过加密哈希函数（如SHA256）为电子证据生成唯一的哈希值；

d) 业务服务平台利用所有者的私钥为哈希值生成数字签名；

e) 业务服务平台将证明记录提交到分布式账本上的智能合约地址；

f) 基于DLT的数字完整性证明平台检查数字签名和信息是否完整，执行智能合同，并在账本中生成记录；

g) 证明注册被打包到新的块中，新的块则被广播到网络。

7.2.2 数字完整性证明起源

数字完整性证明起源的关键流程包括：

a) 用户在分布式账本上查询数字完整性证明；

b) 在在线诉讼的情况下，诉讼平台依据分布式账本上的记录对数字证明进行取证。

8 基于DLT的数字完整性证明面临的安全威胁

本节分析内部利益攸关方面临的安全威胁，即用户、基于DLT的数字完整性证明平台，以及基于DLT的数字完整性证明所涉流程，即数字完整性证明注册和数字完整性证明起源。[ITU-T X.1401]中详细描述了在基于DLT的应用中协议、网络和数据组件面临的威胁。

8.1 与用户有关的威胁

8.1.1 用户身份欺诈

已注册用户使用虚假身份提出非法请求，以获得与其身份不匹配的权限。

8.1.2 私钥泄露

注册表中私钥泄漏的威胁主要包括软件客户端攻击和物理攻击（例如，将打印的密钥暴露给其他人）。私钥的泄漏使得其他用户能够进入基于DLT的证明平台，从而危及其安全性。[ITU-T X.1401]第6.3.2节详细描述了私钥泄漏威胁。

8.1.3 私钥丢失

私钥丢失的威胁主要包括恶意软件攻击、物理攻击（如打印在纸上的私钥丢失）等。这些行为可能导致用户隐私的泄露，这使得恶意用户能够进入基于DLT的证明平台并破坏其安全性。[ITU-T X.1401]第6.3.3节详细描述了私钥丢失威胁。

8.1.4 隐私披露

所有者的证明信息可能涉及诸如姓名、ID信息等敏感个人信息，在证明注册流程期间可能存在用户隐私泄露的问题。[ITU-T X.1401]第6.3.1节详细描述了隐私泄露威胁。

8.2 与证明注册有关的安全威胁

8.2.1 证明欺诈

根据数字证明的特征提取算法，攻击者可以构造与原始文档内容相似的不同特征值。这样，攻击者可以在分布式账本中写入非法内容。

8.2.2 证明篡改

恶意用户可能篡改原始文档的证明或破坏证明的完整性和可用性，从而导致将篡改的证明写入分布式账本。非对称加密算法攻击会导致不安全的传输和存储。[ITU-T X.1401]第6.1.5节详细描述了非对称加密算法攻击。

8.2.3 时间戳依赖攻击

攻击可操纵基于DLT的证明平台的时间戳服务，导致平台无法准确保持证明注册事件的顺序，从而缺乏为证明来源提供有效取证基础的能力。[ITU-T X.1401]第6.1.1节详细描述了时间戳操纵攻击。

8.2.4 51%攻击

当攻击者掌握超过51%的算力时，他们就可构建一条新链。新链可使主链证明失效。此外，51%攻击可导致侵权者成功注册。[ITU-T X.1401]第6.1.1节详细描述了51%攻击。

8.2.5 行贿者攻击

当拥有足够资源的攻击者贿赂拥有投票权的节点时，他们可以损害一个可证明的分布式账本网络的权益。这样，攻击者就在证据分布式账本网络中写入了非法的证据信息。[ITU-T X.1401]第6.1.1节详细描述了贿赂攻击。

8.2.6 块截留攻击

在基于工作证明（PoW）共识算法的DLT证明平台上，攻击者可保留他们开采的一个块，如果攻击者有足够的权力，他可秘密地开采下一个块。当其他矿工生成一个块时，通过释放一个以上的块，攻击者可让其他矿工浪费其算力。攻击的目标是接受零验证的平台运营商。它可使主链证明无效。它也可能导致侵权者注册成功。[ITU-T X.1401]第6.1.1节详细描述了块截留攻击。

8.2.7 跳链攻击

攻击者可以利用链的困难调整算法在各种区块链之间切换。这可能导致攻击者获得不公平的回报，而其他用户遭受损失。这也可能导致矿池有效计算能力的大幅提升，并可能导致侵权者注册成功。[ITU-T X.1401]第6.1.1节详细描述了跳链攻击。

8.2.8 分布式拒绝服务攻击

在基于DLT的证明平台上，攻击者可通过分布式拒绝服务（DDoS）攻击来使网络瘫痪，常用的方法有女巫攻击和日食攻击。这可导致恶意证明注册成功。[ITU-T X.1401]第6.2.3节详细描述了女巫攻击，第6.2.1节详细描述了日食攻击。

8.2.9 BGP劫持攻击

攻击者可以利用被劫持的边界网关协议，并且分布式账本的网络节点被分成两个或更多部分。结果是，DLT被拆分为两个或多个并行链。此时，可在并行分支上进行证明注册和恶意证明注册。攻击停止后，证明分布式账本与最长的主链重新统一，其他分支则被丢弃，这些链上的所有证明记录都无效，这可导致恶意证明的成功注册。

8.3 与证明起源有关的安全威胁

8.3.1 恶意信息写入攻击

DLT中的所有交易数据都是不可移除的。信息一旦写入DLT，就无法删除。攻击者可以通过发起智能合约攻击（例如错误处理的异常攻击）而在分布式账本中写入恶意信息，详见[ITU-T X.1401]第6.1.2节所述。该平台生成导致垃圾邮件块攻击的新块，从而影响基于DLT的证明平台的性能。

8.3.2 证明信息披露

在证明起源中，应使用算法来加密和存储证明信息。确保加密算法的安全很重要。非对称加密算法攻击可导致基于DLT的证明平台处于不安全状态。[ITU-T X.1401]第6.1.5节详细描述了非对称加密算法攻击。

9 基于DLT的数字完整性证明的安全要求

本节描述基于第7节所述安全威胁分析的、基于DLT的数字完整性证明的安全要求。此外，本节描述利益攸关方的安全要求，即用户、数字完整性证明平台以及基于DLT的数字完整性证明服务所涉流程，即数字证明注册和数字证明起源。[ITU-T X.1402]第8.1至8.4节详细描述了有关数据、网络、共识和应用的安全要求。

9.1 用户的安全要求

9.1.1 保护用户身份

为基于DLT的数字完整性证明平台定义了以下与避免身份欺诈有关的安全要求。

a) 基于DLT的数字完整性证明平台应明确不同用户的操作权限。平台应允许用户使用私钥来对信息进行签名并将之发送给DLT。DLT应依据签名来恢复公钥，依据公钥来确定用户，并对用户操作进行认证；

b) 当用户在平台注册时，平台须首先审核用户的身份信息，然后可以为每个用户分配一个标签；

c) 基于DLT的数字完整性证明平台应将每个用户的所有操作写入分布式账本；

d) 基于DLT的数字完整性证明平台应要求为每个证明注册提供身份认证功能，包括访问控制、密码、数字签名和生物特征识别等。

9.1.2 保护私钥

为基于DLT的证明平台定义了以下与私钥保护有关的安全要求。

a) 基于DLT的数字完整性证明平台应防止私钥泄漏 – 基于DLT的证明平台的运营商应防止恶意代码侵入其客户端；

b) 基于DLT的数字完整性证明平台应防止私钥丢失 – 基于DLT的证明平台的用户应将私钥保存在一个安全的地方，并避免将私钥留在没有任何保护机制、易于访问的非物理和物理介质上（如打印纸） – 可能的对策包括个人识别码、密码、指纹和其他生物特征识别信息等。

9.1.3 保护隐私

基于DLT的数字完整性证明平台应在收集、存储、使用、共享、传输、公开披露等信息处理环节采取相关安全保护措施，以防非法收集、滥用和泄露所有者信息，并最大限度地保护所有者的合法权益。

9.2 证明注册的安全要求

9.2.1 避免证明欺诈

为基于DLT的证明平台定义了以下与避免数字证明欺诈有关的安全要求。

a) 基于DLT的证明平台应提供具有安全保证级别（LoSA）和共识机制强度（CMS）[ITU-T X.1404]的共识算法，例如实用拜占庭容错（PBFT），以避免数字证明伪造；

b) 基于DLT的证明平台应监控网络的有效计算能力，检测异常变化，防止跳链攻击；

c) 基于DLT的证明平台应在确保系统运行效率在合理范围内的同时，提高特征值构建算法的难度。

9.2.2 避免证明篡改

为基于DLT的证明平台定义了以下与避免数字证明篡改有关的安全要求。

a) 基于DLT的证明平台应使用经加密的硬件；

b) 基于DLT的证明平台应使用加密算法来确保证明信息的安全传输。相关的第三方服务应使用加密算法来确保证明信息的安全存储。平台及相关第三方服务应选择合适的加密算法，它应在安全性与计算成本以及密钥长度之间进行折衷 – 可以选择增加密钥长度来抵消因增加算力而带来的风险。

9.2.3 保护证明注册

为基于DLT的证明平台定义了以下与注册安全控制有关的安全要求。

a) 基于DLT的数字完整性证明平台须与可信的第三方时间服务同步；

b) 基于DLT的数字完整性证明平台应提供安全攻击告警、漏洞、恶意代码、威胁分析和数据泄露及其他威胁情报信息，通过漏洞扫描和自动安全测试来确定平台中存在的问题；

c) 基于DLT的数字完整性证明平台应提供身份认证和访问控制，以缓解安全攻击风险，例如，恶意篡改和远程攻击；

d) 对于移动应用，基于DLT的数字完整性证明平台应提供安全保护方法，例如，加固和来源混淆，以防反向分析、反编译和嵌入恶意代码；

e) 平台可以使用监测点技术，通过硬编码写入客户端，使客户端接受监测点之前的所有有效交易，从而防止51%攻击。监测点应：引入一种改进的利害关系证明（PoS）共识机制，具有保证金和惩罚措施；为交易设置时间戳；设置第三方可靠节点认证进行身份认证；并且不接受零确认；

f) 平台可在系统中部署有关异常流量清理、云安全防御、域名系统（DNS）解析高级防御的端口过滤，以提供安全的实施方案，并应调整数据块大小，以避免垃圾块攻击；

g) 基于DLT的数字完整性证明平台应提供安全事件的证据收集和追溯、分析原因并提供遏制攻击的方法。

9.3 证明起源的安全要求

9.3.1 防止恶意信息写入

为确保证明起源的安全性，基于DLT的数字完整性证明平台应该：

a) 调节数据块的大小，以防节点产生垃圾块；

b) 确保未经授权和匿名的实体无法搜索或访问分布式账本系统节点中的账户数据和交易数据；

c) 使用保证计算安全的库，比如SafeMath；

d) 执行代码审查以避免整数流和错误处理的异常，从而防止智能合约中的攻击；

e) 使用不可预测的随机生成器来防止恶意用户控制智能合约的结果；

f) 程序开发期间的访问控制设计应尽可能严格，以防智能合约功能的所有权被攻击者篡改而获得最高操作权限。

9.3.2 保护证明信息

为保证证明信息的安全，基于DLT的数字完整性证明平台应该：

a) 使用经加密的硬件存储链下证明信息；

b) 选择合适的加密算法，它应在安全性与计算成本以及密钥长度之间进行折衷 – 可以选择增加密钥长度来抵消因增加算力而带来的风险；

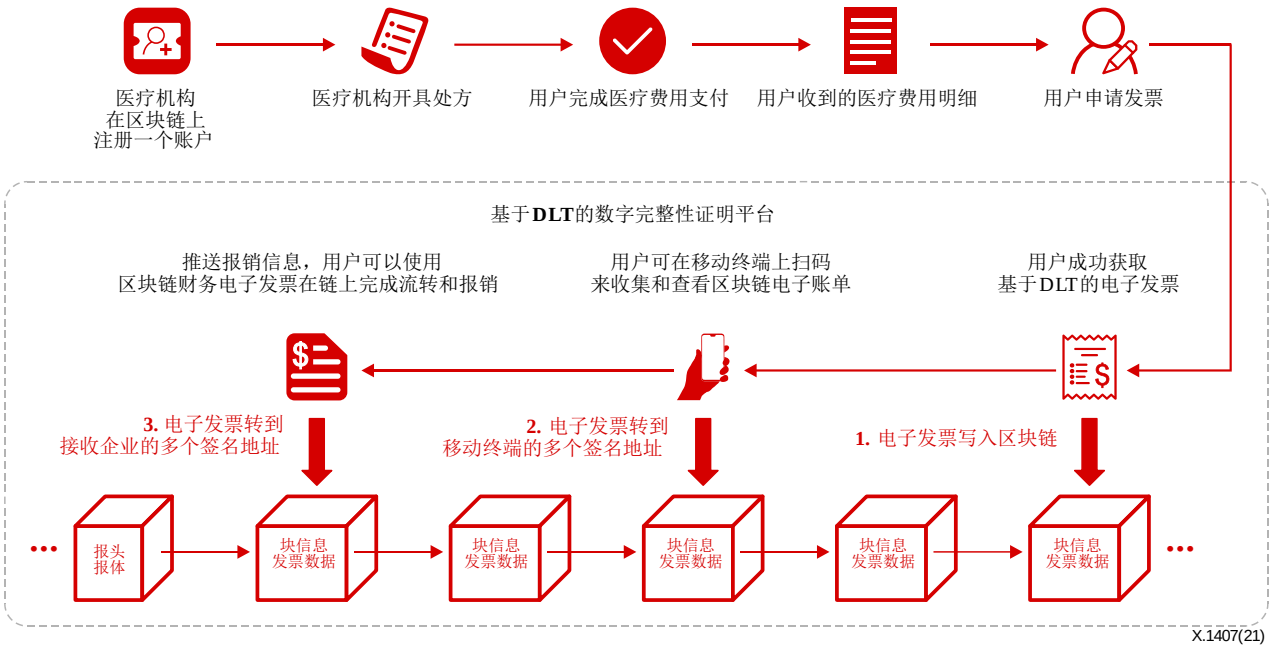
c) 使用有效的访问控制机制来确保对证明信息的可控访问。

附录I

基于分布式账本技术的电子发票用例

（此附录非本建议书不可或缺的组成部分。）

在共识机制下，只有税务机关开具的发票才能被核实和批准，其他任何节点开具的发票都不能被确认，从而确保发票的真实性。使用智能合约，交易和发票开具同时发生，消费者支付和发票开具无缝地发生。概览如图I.1所示。详细内容请参见[b-IEEE 2142.1-2021]“使用区块链技术的电子发票业务推荐实践”。



图I.1 – 基于DLT的电子发票用例概述

医疗机构基于分布式账本技术的电子发票使用案例描述如下：

a) 医疗机构在区块链上注册账户，连接基于DLT的发票开具系统，并在链上设置发票开具条件；

b) 医疗机构开具处方；

c) 用户凭处方完成医疗费用的支付；

d) 用户完成支付后收到医疗费用明细表；

e) 用户申请开具发票；

f) 用户成功获取区块链电子发票；

g) 用户可在移动终端扫码来接收和查看区块链电子发票；

h) 移动终端可推送报销消息，用户可使用区块链电子发票来完成链上流转和报销。

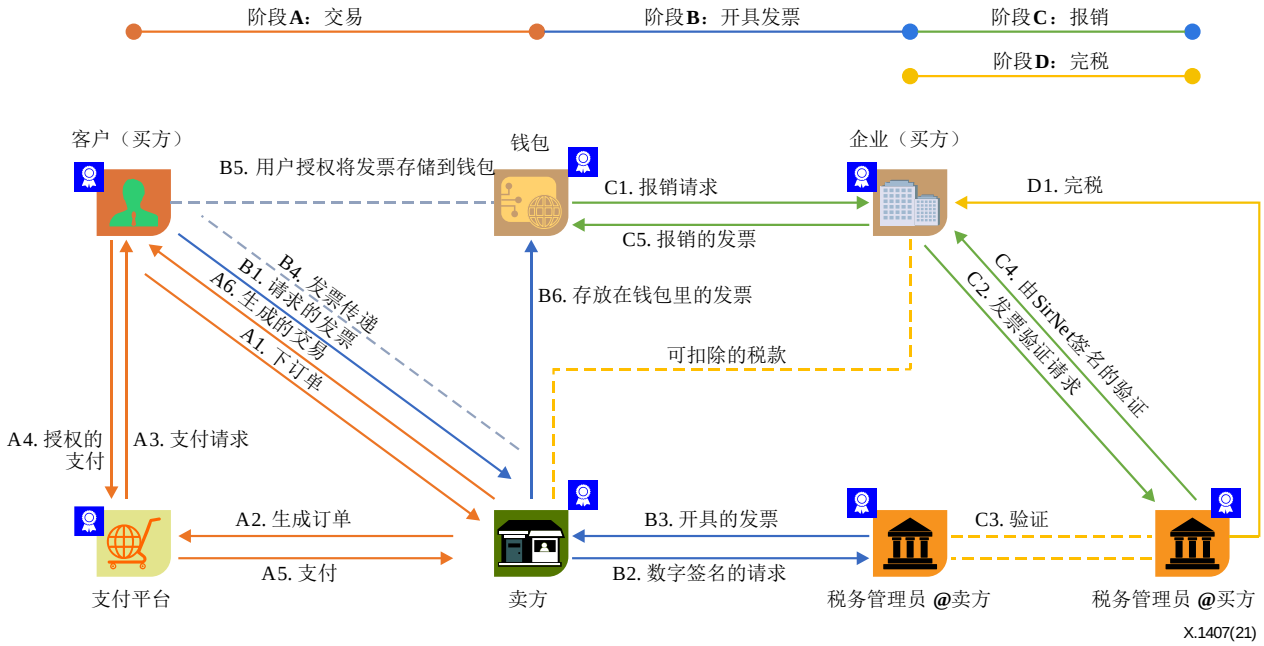
基于支付的发票开具过程可能包括以下几个阶段：

– 阶段A：交易；

– 阶段B：开具发票；

– 阶段C：报销；

– 阶段D：完税。



图I.2 – 基于DLT的电子发票用例流程图

在交易阶段，当客户（即买方）下订单时，服务提供商（即卖方）在支付平台上生成订单，而后支付平台在收到客户授权后确认订单，在处理支付时生成收据。收据可以是支付链上的支付块形式或者是中心化数据库中的一条记录形式。

在发票开具阶段，发票由商户的起源税务管理员（Origin TAX admin）根据客户的请求（例如，来自客户的钱包）来开具，支付收据作为开具发票的未用交易输出（UTXO）。参与节点包括锚定在账本核心层的核心共识节点以及简化支付验证（SPV）节点，例如，商户节点、个人钱包节点等。

在报销阶段，当客户启动报销流程时，客户关联企业（CAE）作为SPV节点验证发票，个人钱包中的发票作为UTXO进行报销。

在完税流程中，目的地税务管理员（TAX Admin）节点和CAE SPV节点加入流程，发票作为UTXO来偿付VAT。

使用DLT的电子发票系统有以下几个优点：

1) 保证发票的真实性，发票收集、发票开具、流转、录入、报销全过程是可追溯的。

2) 发票数据可防篡改，税务局、计费方、流转方、报销方共同参与记账流程。

3) 基于DLT的电子发票不需要税盘和专用设备。对于传统发票，在连锁店情况下，对每个门店都需要多张税盘；基于DLT的电子发票通过ERP自动报销，门店数量的增加不会带来额外的成本。

4) 对于传统发票，若因业务量的暂时增加而使经税务机关批准的发票数量不能满足业务需要时，纳税方可向税务机关申请额外的发票。不过，基于DLT的发票是按需提供的，不需要额外的申请流程。

5) 向税务局收集和购买传统的发票纸费时费力；而基于DLT的电子发票是无纸化的。

附录II

基于分布式账本技术的学位证书验证用例

（此附录非本建议书不可或缺的组成部分。）

证书验证是一个耗时的过程，它可能需要数天或数周的时间。雇主关注资质认证，花大量时间与大学沟通，以验证证书的完整性，确保申请者拥有无懈可击的资质。区块链将提供透明度，并简化与各种雇主或任何其他方共享经过认证的证书。

雇主可以使用DLT来证明学位证书的完整性。DLT提供一个公认的安全来源来存储学生的资质，各种机构和大学都可访问之。它提供持久的公共记录，以防机构变化或私人记录丢失可能带来的影响。

本样式由以下组件组成：

用户

– 发放方（大学）；

– 接收方（学生）；

– 验证方（雇主）。

系统

– 大学的节点；

– 区块链平台。

数据

– 证书哈希值；

– 电子证书文件。

检查证书完整性的过程取决于检查证书的哈希值并将哈希值与存储在区块链中的哈希值进行比较，如图II.1所示。步骤包括：

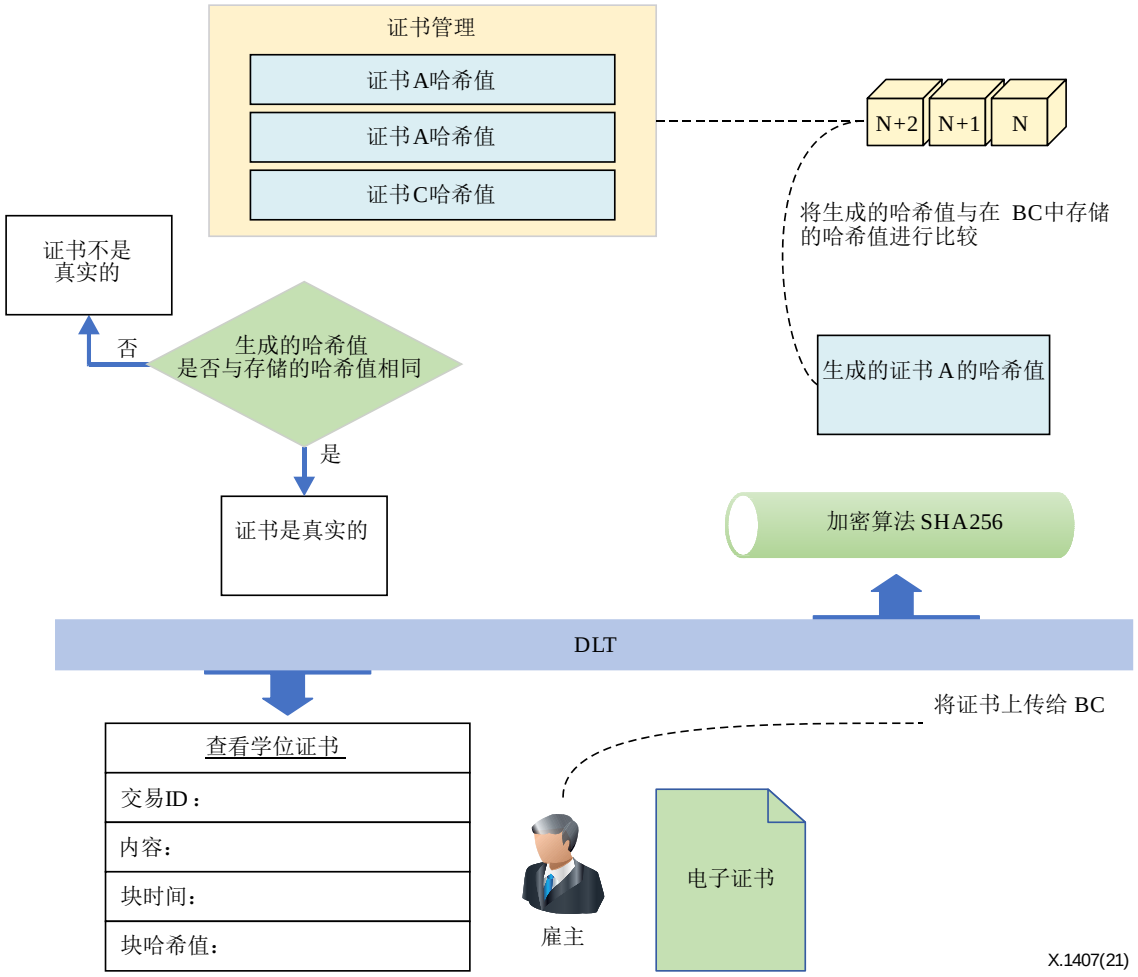
– 大学为学生发放新的电子证书并将文件上传到DLT；

– DLT哈希并存储证书文件；

– 为了证明完整性，学生或雇主将证书文件上传到DLT平台；

– DLT生成文档的哈希值，然后将生成的哈希值与存储在区块链中的哈希值进行比较；

– 如果生成的哈希值与存储在区块链中的哈希值之一相匹配，那么证书是真实的。



图II.1 – 基于DLT的学位证书验证用例概述

使用DLT认证学位证书的好处：

– DLT解决当前验证和认证过程中的困难；
– DLT可以将所有大学聚集到一个平台上；
– DLT技术鼓励雇主与大学以系统的方式开展合作；
– DLT帮助保存和分享真实的与完整的信息，作为真相的一个来源；
– DLT节省时间、成本和精力。

参考文献

[b-ITU-T X.1400] ITU-T X.1400（2020年），分布式账本技术的术语和定义。

[b-ISO 13491-2] ISO 13491-2:2017(en)，金融服务 – 安全加密设备（零售）– 第2部分：金融交易中使用的设备的安全合规性清单。
<*https://www.iso.org/obp/ui/#iso:std:iso:13491:-2:ed-4:v1:en*>

[b-ISO 23257] ISO 23257:2022，区块链和分布式账本技术 – 参考架构。[b-ISO/IEC 27000] ISO/IEC 27000:2018(en)，信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇。
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

[b-ISO 22739] ISO 22739: 2020，区块链和分布式账本技术 – 词汇。
<https://www.iso.org/standard/73771.html>

[b-IEEE 2142.1-2021] IEEE 2142.1-2021，IEEE针对采用区块链技术的电子发票业务的推荐做法。
<https://standards.ieee.org/ieee/2142.1/7590/>

[b-ISO 56000] ISO 56000:2020，创新管理 – 基础和词汇。
<https://www.iso.org/standard/69315.html>

[b-ISO 5807] ISO 5807:1985，信息处理 – 数据、程序和系统流程图、程序网络图和系统资源图的文件符号和约定。
<https://www.iso.org/standard/11955.html>

[b-Kaur] Kaur, S., Chaturvedi, S., Sharma, A. Kar, J.（2021年），共识协议在区块链中的应用研究综述，安全与通信网络，2021年卷，文件ID 6693731，1月刊，第1-22页，https://doi.org/10.1155/2021/6693731

ITU-T 建议书系列

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

瑞士印刷
2022年，日内瓦