

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

F.747.10

(01/2022)

F系列：非话电信业务
多媒体业务

分布式账本系统对安全人为因素服务的要求

ITU-T F.747.10 建议书



ITU-T F系列建议书

非话电信业务

电报业务	
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发布	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	
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	
公众传真业务	F.160-F.199
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	
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
通用个人通信业务	F.850-F.899
无障碍获取与人为因素业务	F.900-F.999

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T F.747.10 建议书

分布式账本系统对安全人为因素服务的要求

摘要

ITU-T F.747.10建议书制定了“分布式账本系统（DLS）对安全人为因素服务的一般性要求”，规定了功能方面的能力。

本建议书草案提出了对安全人为因素分布式账本服务模型的要求，该模型可以解决隐私保护和大规模人为因素数据使用目标间的冲突。此外，本建议书草案为分布式账本共享节点提供了相应的功能，无需对加密数据解密即可执行机器学习操作。然而，机器学习对加密数据的计算负担可能会过大。为解决这一问题，此人为因素分布式账本服务模型提出了允许使用两个或更多加密密钥对以及通知密钥类型的程序。此外，本建议书亦涉及维护安全人为因素服务完整性的要求，目的是维护安全的分布式账本，并从一开始便为分发个人人为因素信息进行检查。因此，在个人安全人为因素信息的分发中应用分布式账本系统，可以确保从分发到最终使用路径的全过程透明跟踪。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T F.747.10	2022-01-17	16	11.1002/1000/14644

关键词

分布式账本服务模型、隐私保护扩展、安全人为因素、透明跟踪。

* 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、信息通信技术（ICT）领域工作的联合国专门机构。国际电联电信标准化部门（ITU-T）是国际电联的一个常设机构，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布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，而后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ITU-T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，也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的条款（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，才认为达到了本建议书的合规性要求。“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声明的知识产权。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、有关已声明之知识产权的证据、有效性或适用性不表明任何意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的、有关受专利/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，这可能并非最新的信息，因此特大力提倡他们通过下列网址从ITU-T网站的相应ITU-T数据查询：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2022

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
	3.1 他处定义的术语	1
	3.2 本建议书中定义的术语	2
4	缩略语和首字母缩写	2
5	惯例	2
6	背景	3
7	安全人为因素服务的分布式账本系统的一般要求	3
	7.1 公共分布式账本共享节点的功能要求	4
	7.2 新参与节点的认证要求	4
	7.3 分布式账本系统的安全要求	5
	7.4 分布式账本系统的完整性维护要求	5
8	安全人为因素服务分布式账本系统的功能	5
	8.1 个人人为因素信息分配中的分配账本结构	6
	8.2 分布式账本结构中用于分配个人人为因素信息的两个功能	6
	8.3 分布式账本系统维护方法	7
	附件A – 应用安全人为因素分布式账本服务模型	9
	参考文献	10

分布式账本系统对安全人为因素服务的要求

1 范围

本建议书描述了分布式账本系统（DLS）对安全人为因素服务的要求，包括：

- 背景；
- DLS对安全人为因素服务的一般要求；
- DLS在安全人为因素服务方面的功能。

2 参考文献

下列ITU-T建议书及其它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。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 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 区块 [b-ISO 22739]：涵盖块数据和区块标题的结构化数据。

3.1.2 假设 [b-ISO 22739]：DLT节点之间达成的一致，即1) 交易得到验证，2) 分布式账本包含一组一致的已验证的交易及其排序。

3.1.3 数字签名 [b-ISO 22739]：当附加到数字对象时，使数字对象用户能够验证其来源和完整性的数据。

3.1.4 分布式账本 [b-ISO 22739]：在一组DLT节点间共享的账本，并使用共识机制在DLT节点间实现同步。

3.1.5 分布式账本技术 [b-ISO 22739]：能够操作和使用分布式账本的技术。

3.1.6 分叉 (fork) [b-ITU-T TS FG DLT D 1.1]：创建一个分布式账本的两个或多个不同版本。

3.1.7 哈希值 [b-ISO 22739]：密码哈希函数输出的位串。

3.1.8 健康 [B-WHO]：健康不仅为疾病或羸弱之消除，而系体格、精神与社会之完全健康状态。

3.1.9 账本 [b-ISO 22739]：保存交易记录的信息存储，这些记录是最终的、确定的和不可变的。

3.1.10 二叉树 [b-NIST]：一种数据结构，其中数据通过散列和组合，最终形成一个代表整个数据结构的单一根散列。

3.1.11 挖矿 [b-ITU-T F.751.0]: 在某些共识机制中寻求奖励的活动。

3.1.12 节点 [b-ISO 22739]: 构建数据结构的基本组件。

3.1.13 公共分布式账本系统 [b-ITU-T F.751.0]: 可供公众使用的DLT系统。

3.1.14 交易 [b-ISO 22739]: 工作流程的最小单位，是生成符合管理规则结果所需的一个或多个行动序列。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 区块深度：从初始区块附加到分布式账本系统链的区块层级。

3.2.2 电子人为因素记录：以数字格式，用电子方式存储的个人和人口系统化数据采集。

3.2.3 人为因素：在人类福祉、安全和健康方面设计最佳生活方式条件的原则，包括发展现有技术和获取新技术。

注 – 改编自[b-ISO 6385]和[b-Wickens]。

3.2.4 个人人为因素信息：通过直接测量人体及其环境而收集的信息，并利用通信网络传输到个人人为因素设备或其他设备，用于电子人为因素记录。

3.2.5 个人人为因素装置：一种测量人体及其环境，并与其他人体因素装置交换所收集信息的装置。

3.2.6 安全人为因素：信息安全中的人为因素。

4 缩略语和首字母缩写

本建议书使用以下缩略语和首字母缩写：

CPU	中央处理器
DLS	分布式账本系统
DLT	分布式账本技术
IP	互联网协议
PDLS	公共分布式账本系统
UUID	通用唯一标识符
VRF	可验证随机函数

5 惯例

在本建议书中：

- 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）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，以及网络运营商或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，并仍宣称遵循本建议书。

6 背景

近年来，由于个人健康信息收集设备以及医院个人病历数据的发展，个人人为因素信息急剧增加。管理和共享个人人为因素数据的最佳模式之一是分布式账本服务模式。分布式账本系统的特点是利用涉及多个节点的分布式数据库提供可靠性，并使用数字签名和哈希值确保检索数据的透明性。然而，就信息保护而言，人为因素数据可能非常敏感。因此，需要为公共分布式账本服务模型的个人人为因素信息提出保护要求（见图1）。

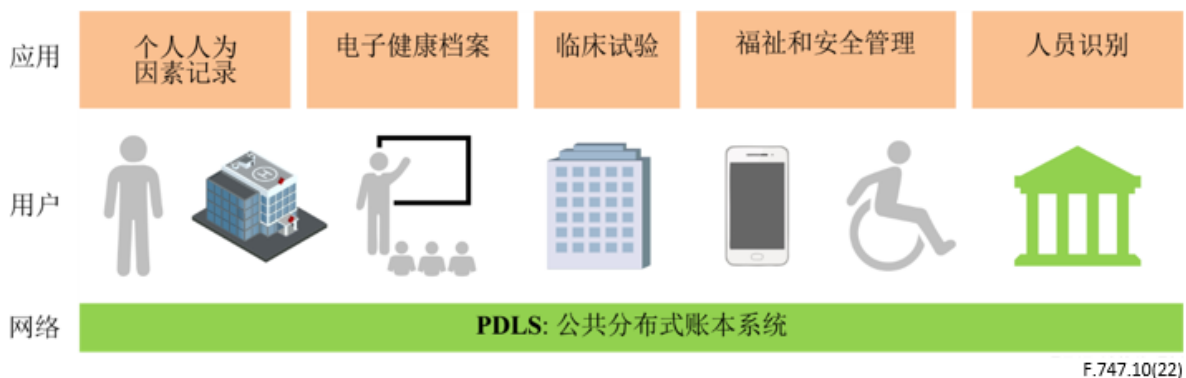


图1 – 人为因素分布式账本服务模型

本建议书描述了人为因素分布式账本服务模型的安全要求，该模型可以实现保护隐私和利用个人健康大数据的目标。此建议书还介绍了分布式账本共享节点的功能要求，以便在不对加密数据进行解密的情况下执行机器学习。建议书描述了分布式账本服务模式中的激励要求，通过将保健产品直接分配给消费者和生产者提高其生活质量。分布式账本技术的应用始于跟踪和管理健康信息生产及分发的能力。换言之，在个人人为因素信息的分配中应用分布式账本技术，可以确保从分配到最终使用路径整个过程的透明跟踪。因此，参与分布式账本系统的单个节点所代表的个人可以信任和使用分布式信息。此外，还可以提供一种从根本上阻止个人人为因素信息非法传播的方法。

7 安全人为因素服务的分布式账本系统的一般要求

本条款描述了对安全分布式账本移动管理程序提出的要求，该程序可以实现个人信息保护与使用个人人为因素信息大数据这两种相互冲突相互兼容的目标。这一条款引入了分布式账本共享节点的功能需求，以便在不解密加密数据的情况下执行机器学习。例如，同态加密是一种加密技术，即使在加密状态下，也可以实施计算机执行的所有计算，而无需解密。即使在包含需要保护的个人信息的数据分析中，亦可在不泄漏个人信息或丢失数据的情况下可选地进行机器学习。

7.1 公共分布式账本共享节点的功能要求

公共分布式账本共享节点的功能要求如下：

- 要求节点存储从第一个区块开始累积的分布式账本链数据。
- 验证交易过程中，当节点执行分布式确认算法时，需要将完成状态传递给其他节点。
- 为了验证每轮生成的分布式账本的有效性，节点需要通过目标哈希值进行比较，检查所生成区块的有效性。
- 每个节点均需更新并维护共享数据，例如所有其他节点的公钥列表和分布式账本。
- 要求该节点将交易传播到其他节点，直至交易验证过程中的协议阶段（如交易确认完成）。
- 要求节点使用加密密钥（如公钥证书[b-ITU-T X.509]、同态加密[b-ISO 18033-6]、可验证随机函数（VRF）[b-IETF draft-irtf-cfrg-vrf-08]）加密需要安全交易的数据，并告知加密密钥的类型。
- 节点需要确定是否有必要解密。如果需要解密，则在解密后将其传输到发出请求的节点。如果不需要解密，则该节点使用发出请求节点提供的公钥加密继续传输。

7.2 新参与节点的认证要求

建议现有节点提供第7.2.1至7.2.3款所述功能，以认证分布式账本共享系统中的新参与节点。

7.2.1 请求新节点认证的要求

- 建议新节点在提出请求前至少使用两对加密密钥（例如，公钥证书[b-ITU-T X.509]，同类加密密钥[b-ISO 18033-6]）。
- 建议新节点使用自己的私钥对请求消息加密，并将加密的数据及其公钥一起发送至该节点。
- 建议每个节点在验证和传输认证信息时，更新新节点和现有节点的已验证公钥列表，并存储分布式账本共享系统的公钥列表以供参与。

7.2.2 节点的认证功能要求

- 建议该节点通过解密从与公钥一起接收的新参与节点（期望中的）发送的加密数据验证有效性，用新节点的公钥加密验证信息和公钥列表，并发送加密信息。
- 建议该节点作为参与分布式账本共享系统所有节点的公钥列表，并在每次处理新节点认证时更新其对应的公钥列表。
- 每次建议节点更新其公钥列表时，都需要用自己的私钥对公钥列表进行加密，并将其发送给参与分布式账本共享系统的所有节点。
- 建议该节点永久存储参与分布式账本共享系统节点的已验证信息，以及参与节点的验证时间和地址。

7.2.3 认证现有节点新增节点的验证要求

- 建议现有节点验证该节点发送的公钥列表数字签名，并使用新公钥列表对其进行更新。
- 建议现有节点通过检查新的公钥列表验证经过认证的新节点的参与。

7.3 分布式账本系统的安全要求

建议现有节点遵循本条款的规定。

- 需要使用电子签名进行验证并在分布式账本中拒绝，方能操控现有共享分布式账本中的信息。
- 在分布式账本系统中使用的主链中，创建新块时在达到任意 b 区块深度之前，需要在分布式账本中拒绝与最长链内容不同的链。这里 b 是大于等于1的数。
- 在创建分布式账本的过程中，当具有重复地址（例如，IP、UUID）的数据被添加到分布式账本系统中时，需拒绝这些数据。
- 对于任何达到 d 区块深度的块，要求公共随机源（如加密随机数[b -NIST]）相同。要求 d 区块深度之后的区块以 g 区块深度更新公共随机源。更新时，建议将新添加区块的哈希值用作随机源。
注 – 这里 d 区块和 g 区块深度是指深度大于1的任何区块。
- 要求在分布式账本中拒绝包含与先前区块哈希值和Merkle树根值不同的区块的链。
- 如果在分布式账本系统的组成节点中出现错误节点，且没有差错节点高于DLS预定义共识的水平，则建议保留这些节点。

7.4 分布式账本系统的完整性维护要求

建议现有节点遵循本条款的规定。

- 建议每个节点都避免试图操纵现有共享分布式账本中的信息。如果检测到这种攻击，则建议通过累积节点数获得哈希率。建议将当前区块树的数量与门限值的数值进行比较，以计算安全性，并向所有节点传输（广播）相关信息和节点的地址。
- 建议每个节点删除分布式账本系统中常用的最长链和分布式账本系统中内容不同的链。
- 建议每个节点移除包含分布式账本中先前区块的不同哈希值或Merkle树根值的块链，并计算遭受攻击节点的累积数量，以确定分布式账本是否安全，并传输（广播）相关信息和节点的地址。
- 当分布式账本系统的组件中出现错误或伪造节点时，建议每个节点移除并累积尝试执行错误或攻击的节点数，以获得哈希率。在分布式账本中，建议使安全节点的数量大于门限值，并建议传输（广播）相关信息和节点地址。
- 将具有重复地址的新数据添加到分布式账本系统的数据中时，建议每个节点拒绝分布式账本创建过程中的数据。

8 安全人为因素服务分布式账本系统的功能

作为一种激励，需要通过自动直接分发个人人为因素信息提高分布式账本服务模式下的生活质量。分布式账本技术的应用始于跟踪和管理健康人为因素信息生产及分发的能力。换言之，在个人人为因素信息的分配中应用分布式账本技术，可以确保从分配到最终使用路径整个过程的透明跟踪。因此，参与分布式账本系统的单个节点所代表的个人可以信任和使用分布式信息。此外，还可以提供一种从根本上阻止个人人为因素信息非法传播的方法。

8.1 个人人为因素信息分配中的分配账本结构

按照惯例，账本的第一笔交易是一笔特殊交易，此启动的一项新奖励（例如，虚拟虚拟币[b-ITU-T F.751.0]）将支付给账本的创建者。这种奖励分配给维护分布式账本的节点，并从一开始就分发个人的人为因素信息。建议相关方就提供和分发这些奖励的技术提前达成一致，因为这些技术是采用分布式系统运行。不断增加一定数量的新奖励，是对利用消耗资源操作分布式账本系统的节点（矿工）给予补偿。这些节点消耗中央处理器（CPU）的计算能力、内存和虚拟币。

8.2 分布式账本结构中用于分配个人人为因素信息的两个功能

作为在提高挖掘速度的同时减少等待时间的方法，可以选择性地使用将基本分布式账本结构分解为三种功能的技术。我们可将其视作选择分布式账本协议中的主链（例如，最长链选择技术），这会导致在账本树各个深度的所有账本中选择安全账本。这里，账本的深度被定义为与原始账本的距离（账本中连接块的数量）。

在分布式账本中，账本有三个用途。这些用途分别是选举负责人，为主链增加交易，通过上级链接的关系投票给初始账本。将账本表示为一个概念操作时，其可分为两个功能（见图2）。建议功能将原始账本树中深度相同的交易捆绑在一起。投票功能通过对账本树中相同深度的交易进行投票，以选择账本的记账部分。选定的账本采用交易的部分，并生成最终账本。此投票功能在账本树的相同深度运行，并创建上下级连接。因此，原始账本树的上下级链接有两个明确分开的功能：1) 在交易部分的相同深度提供账本的某种顺序，2) 投票功能，有助于为筛选账本开展相互投票。下文所述用于分配个人人为因素信息的分布式账本总体结构如图2所示。

由于DLS的分布性质，该系统面临稳定性问题。在DLS内，每个节点可以记录一条交易，但最终选择哪一节点是共识算法 [b-ITU-T F.751.0]得出的结果。我们要求将DLS系统的设计作为影响稳定性的众多因素之一加以考虑，同时建议使用分布式账本，通过系统的自适应处理恢复稳定的服务。为了解决DLS的稳定性问题，对于d区块深度，公共随机源（如密码随机数[b-NIST]）保持不变，且d区块深度之后的区块应该按照g区块深度更新公共随机源。更新时，新添加区块的散列被用作随机源。如果 $d = 1$ ，则恢复到每个时期分叉的基本更新规则，最容易受到污染（平衡）攻击。为了正常增加安全门限值，可以增加d。当 $d = \infty$ 时，所有区块都使用原始区块的随机数作为公共随机源。这是不可分叉的最长链协议，允许私钥受污染的所有者对链进行专门预测。

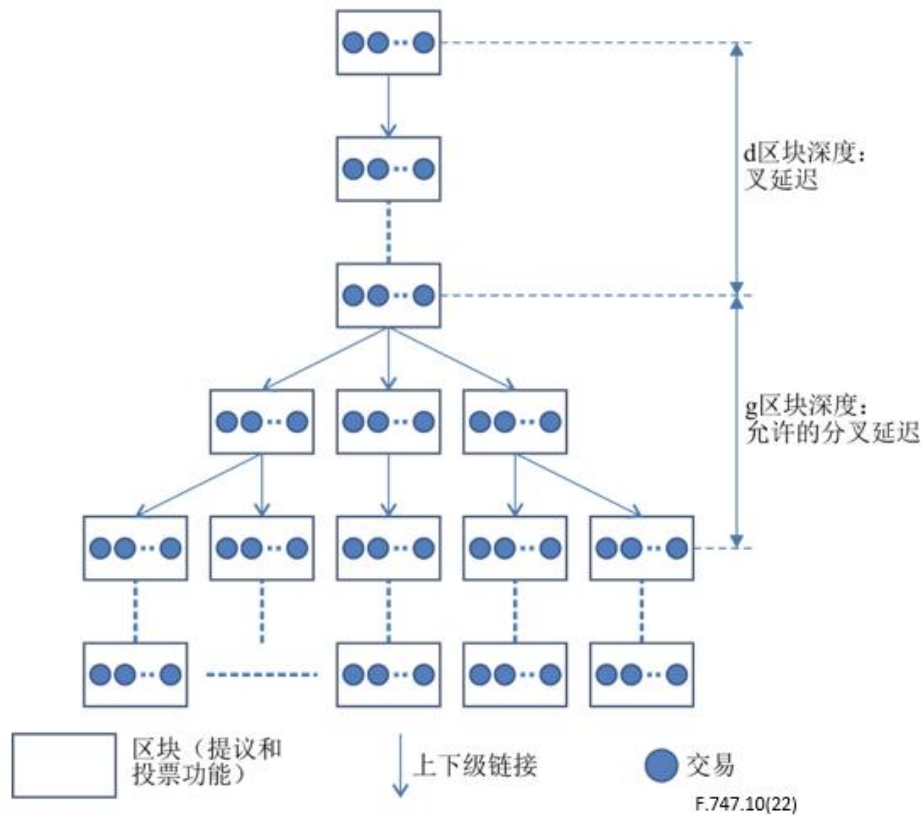


图2 – 分布式账本服务模型结构

8.3 分布式账本系统维护方法

分布式账本的这种功能分离表示要比传统的分布式账本复杂得多，但是它可以通过更快达成共识提高分布式账本的性能。这种快速达成共识功能可以增加交易部分中的账本数量，而不会损害推荐功能中分布式账本的安全性。因此，账本的数量将仅受底层通信网络容量的限制。由于多个交易的投票功能将与提议使用的账本并行投票，以便快速确认，因此可以实现低延迟、高可靠性地确认共识。鉴于因为总账本生成率大幅增加，因此个人人为因素信息分布式账本系统易于管理，且建议每个深度使用的功能的部分账本数量可以很少。

这种分布式账本系统在选择账本的过程中，可以通过将散列的能力集中到特定交易的推荐功能，给透明度造成损害。如图3所示，如果攻击者的散列能力在建议使用函数的特定账本中很强，则其可能非常容易受到安全攻击。图3显示了一个因攻击者集中散列能力而使账本链遭破坏或污染的实例。如果攻击者能够在一个地方收集比所有安全节点更多的CPU计算能力、内存和虚拟币，攻击者将必须决定是使用其窃取诚实的节点奖励，还是通过其开展合作。有必要提供一种激励政策，使攻击者觉得遵守规则比破坏个人人为因素信息分布式账本系统的透明度更有利。这种奖励需要进行调整，以便在参与节点之间进行分配。攻击者可以提供这样一个规则，即与所有其他节点建立关联更加有利可图。建议根据攻击者的散列力(α)之比，将诚实节点数保持在阈值（如 $CD(1 + \alpha)/(\alpha - 1)/\log(\alpha)$ ）上。这里C和D是指通信网络的容量和延迟。

从上述公式可以看出，如果 α 接近0，则攻击者的散列能力很弱，那么可以认为分布式账本系统的安全性即使在投票者区块树的数量很少的情况下也没有问题。然而，如果 α 接近1，即如果攻击者的散列能力很强，则投票者区块树的数量应呈指数级增长。此时，可以观察到系统变得非常容易受到安全威胁。

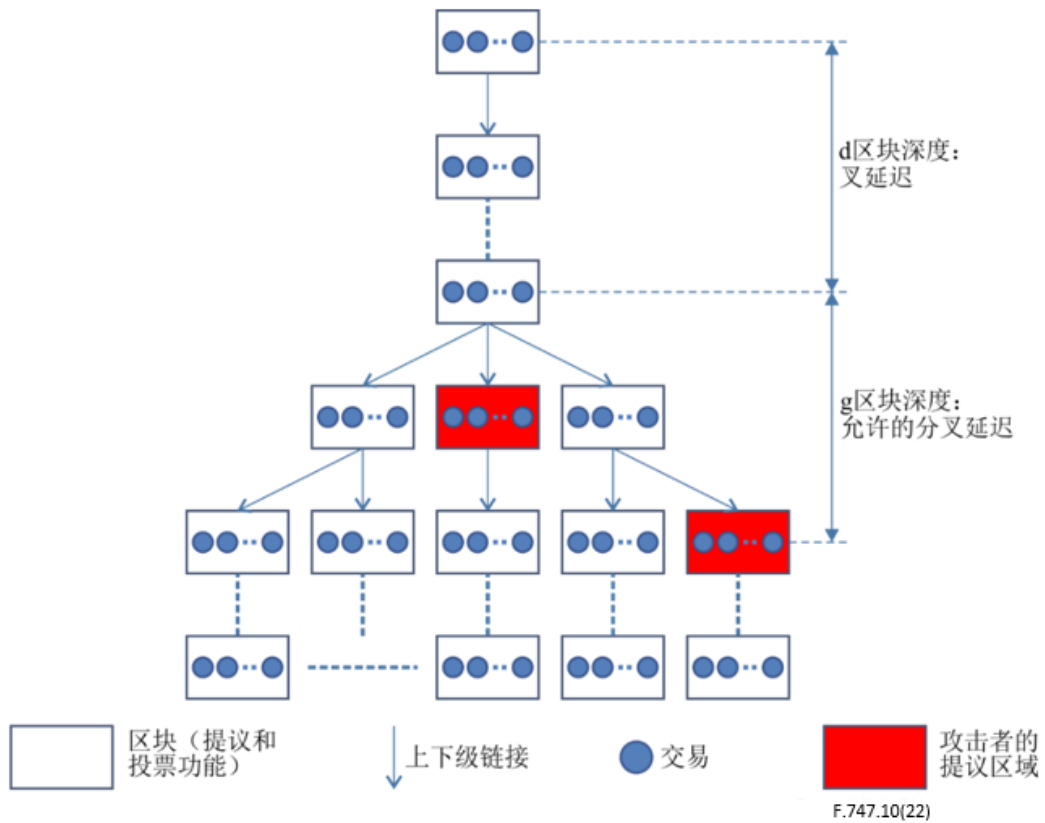


图3 – 分布式账本服务模式中的污染预防示例

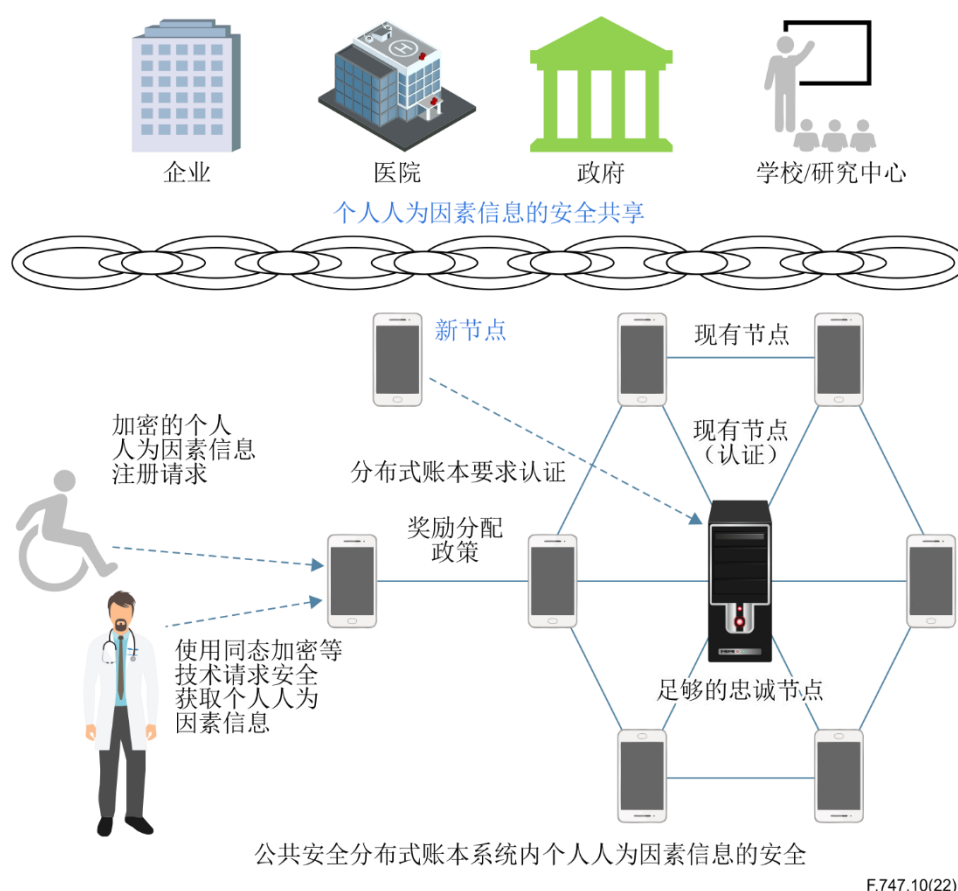
在选择建议的区块的过程中，我们推荐通过调整散列和虚拟币的力度确定区块的功能。此时可以看出，如果攻击者的散列能力很强和虚拟币数量较多，则安全性很脆弱。如果攻击者能够收集比所有诚实节点更多的计算能力和虚拟币，攻击者将必须决定是使用其窃取诚实的节点奖励，还是通过其开展合作。建议提供一种激励政策，使攻击者觉得遵守规则比破坏系统及其自身财富的合法性更加有利。通过防止利润集中于特定支持者区块的策略，建议提供这样一个规则，即攻击者将从与所有其他节点共同分配中受益更多。

附件A

应用安全人为因素分布式账本服务模型

(此附件是本建议书不可分割的组成部分)

图A.1所示分布式账本方案不仅可以安全透明地管理以医院为中心的个人人为因素数据，还可以管理以个人为中心的个人人为因素数据，如个人健康信息收集设备。图A.1中使用个人健康信息共享的实例中，可通过使用多节点参与的分布式账本提供可靠性，并可以使用数字签名和哈希值来确保搜索数据的透明度。然而，个人人为因素数据在数据保护方面可能非常敏感。此类敏感数据使用能够处理大数据的加密技术，以加密状态注册。敏感的个人人为因素信息移动程序遵循第7.2条中使用加密算法的分布式账本共享系统的要求和程序（见图A.1）。此外，要求运行用于个人人为因素信息的分布式账本系统，以满足第8.3条中奖励功能激活和维护的要求。



图A.1 – 安全分布式账本服务模型的方案

参考文献

- [b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.
- [b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [b-ITU-T TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions*.
- [b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs)*. <https://tools.ietf.org/html/draft-irtf-cfrg-vrf-08>
- [b-ISO 6385] ISO 6385:2016, *Ergonomics principles in the design of work systems*.
- [b-ISO 18033-6] ISO 18033-6:2019, *IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption*.
- [b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.
- [b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview*.
- [b-WHO] World Health Organization (2006), *Constitution of the World Health Organization – Basic Documents*, Forty-fifth edition, Supplement.
- [b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp.2-7. New York, NY: Longman.

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费和会计原则以及国际电信/信息通信技术（ICT）经济 and 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	传输系统和媒质、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