



Distr.: General
29 May 2024
Chinese
Original: English

联合国国际贸易法委员会
第五十七届会议
2024年6月24日至7月12日，纽约

与在贸易中使用分布式分类账技术有关的法律问题

秘书处的说明

目录

	页次
一. 背景	2
二. 指导文件的内容	2
三. 术语表	20



一. 背景

1. 铭记在处理数字经济和数字贸易相关法律问题方面，贸易法委员会在联合国系统内发挥着核心和协调作用（[A/74/17](#)，第 211 段），委员会 2022 年第五十五届会议请秘书处酌情与其他相关组织合作，利用现有资源编写一份关于在贸易中使用分布式分类账系统相关法律问题的指导文件（[A/77/17](#)，第 22(f)段和第 169 段）。委员会的要求源于编写《关于数字经济相关法律问题的分类法》（《分类法》）中关于分布式分类账系统的一节。
2. 委员会在 2023 年第五十六届会议上收到了秘书处关于在贸易中使用分布式分类账技术所涉法律问题的说明（“范围界定文件”）（[A/CN.9/1146](#)）。委员会赞赏地注意到范围界定文件的内容，并强调该文件与贸易法委员会其他数字贸易工作流程的交集，如第二、第四和第五工作组开展的工作。与会者广泛支持与其他有关国际组织密切协调开展工作，并注意到这项工作事关海牙国际私法会议最近开展的几个项目（[A/78/17](#)，第 200-202 段）。
3. 因此，委员会请秘书处酌情利用现有资源并与其他相关组织合作，继续并最后完成其编写一份关于在贸易中使用分布式分类账系统所涉法律问题指导文件的工作（[A/78/17](#)，第 22(c)段）。
4. 本说明以范围界定文件为基础，并对该文件进行了补充，就在贸易中使用分布式分类账技术所涉法律问题提供了更多的见解。它没有就分布式分类账技术是否系预期用途的适当技术提出建议。本说明确定了可以找到法律指导的领域，并提出了现有法律文书内可能的解决方案。由于分布式分类账技术的新颖性，它还确定了尚未有既定法律解决方案的领域，在这种情况下，它提供了不断演变发展领域的全貌。秘书处打算进一步扩充本说明，包括在专家的帮助下，并与有关组织合作，列入关于分布式分类账技术与自由贸易协定之间相互关系等补充事项的信息。特别是，海牙国际私法会议的任务是与贸易法委员会和其他具有相关专门知识的组织就数字经济国际私法方面的相关事项开展合作。¹预计将海牙国际私法会议的工作成果纳入指导文件大有裨益。
5. 本说明附件载有一份技术术语表。每个定义的技术术语首次出现为楷体。随着指导文件工作的推进，术语表可能会进一步扩充。

二. 指导文件的内容

A. 分布式分类账技术的背景信息

6. 《分类法》提供了关于分布式分类账技术的这样一个工作定义，即“可以从为实现何维护在多个联网计算机（或服务）上共享、复制和同步的分类账（或数据库），的一组技术和方法。因此，分布式分类账技术系统是支持部署这些技术和方法的系统（包括软件和硬件组件）。分布式分类账技术系统在其设计、治理、目的和用途方面各不相同”（《分类法》，第 172 段）。

¹ 一般事务和政策理事会的结论和决定（2024 年 3 月的结论和决定），第 11(b)号，可在海牙国际私法会议网站（www.hcch.net）的“治理”，然后是“一般事务和政策理事会”下查阅。

7. 根据另一个定义，分布式分类账技术体现的是一种去中心化的数据库，这种数据库在点对点机器网络上共享，通常通过互联网连接。它可以被设计为允许多方记录和更新信息。分布式分类账技术通常利用信息技术基础设施、互联网连接和数据等多个要素。从技术角度来看，这些要素通常包括加密散列（例如，区块中数据的散列）、共识机制（例如，权益证明）、平台（例如，第一层协议）和数字资产（例如，同质化代币）。

8. 区块链是一种广为人知的分布式分类账技术。区块链利用一系列区块来归档数据。每个区块包括数据（如交易日志）和摘要（通常是加密散列），形成与前一个区块的链接。如果之前区块的交易中进行任何更改，会导致相关区块的散列随即修改，随后会影响到所有后续区块的散列。因此，修改区块链上的信息需要按时间顺序修改每个后续区块，然后在另一个实体将新的区块添加到分类账之前，将更新后的数字分类账广播到网络。这种修改程序实际上无法在充分发达的网络中执行。因此，交易记录持久存在。这个特性也被称为“不变性”。

B. 分布式分类账技术的分类

9. 分布式分类账技术可以根据两个关键特征进行分类：公共或私有分类账，以及经许可或不经许可对其进行访问（《分类法》，第178段）。这一分类是为了说明目的，并不反映现有的各种解决方案。

10. 分布式分类账的公共或私有性质是指谁可以作为节点操作员，即作为分布式分类账一部分的计算机的运营商，参与开发分布式分类账技术系统。“公共分类账”一词表示允许不受阻碍地访问的去中心化系统。而“私有分类账”限制访问，仅允许部分预先确定的参与者访问。

11. 分布式分类账的经许可或不经许可性是指在参与分类账之前是否需要许可，即用户的身份识别是否是参与的先决条件。在不经许可的分布式分类账中，不需要身份识别：理论上，任何用户都可以在没有身份识别的情况下参与分布式分类账。在经许可的分布式分类账中，用户在获准访问分布式分类账之前需要识别自己的身份，并且通常会采取措施来进行身份管理。

12. 公共不经许可的分布式分类账是最开放和去中心化的办法。在这种情况下，公众的任何人都可以加入分布式分类账而无需身份验证，并且通常没有管理委员会限制用户或参与者访问、查看和记录分布式分类账。²

13. 公共不经许可分布式分类账的一大优势是其设计透明，这增强了可扩展性，因为新的参与者不需要经过管理实体的验证。任何参与者都可以在未经事先许可或授权的情况下访问和参与此类分类账，前提是它遵守网络的自律管理。

14. 公共不经许可分布式分类账的关键特征包括：

² 公共不经许可的分布式分类账的实例包括比特币和以太坊。比特币的分类账包含所有人均可以查看的每笔比特币交易的历史记录。

(a) 开放访问：没有单一的管理员控制网络，从而有效限制任何单个参与者对网络的影响；

(b) 开源：源代码是公开的，任何人都可以提出修改意见；

(c) 透明：分布式分类账上的所有数据均公开可见，尽管假名和其他机制可能允许一定程度的隐私；

(d) 安全：加密技术的使用凭借对系统的信任而不是对单个中央控制实体的信任来确保网络的完整性。这种方法被称为“去信任”，因为它不需要任何外部信任来源；

(e) 假名：在基础设施层面，使用假名来识别参与者。

15. 相比之下，私有经许可分类账限制了分类账中用户和参与者的数量，并要求在参与分类账之前识别这些参与者的身份。这类分类账通常由企业创建并在这些企业内使用。这个分类账由创建和操作它的企业严格监管和控制。

16. 私有经许可分布式分类账的关键特征包括：

(a) 限制访问：只有经授权的参与者才能访问和参与分类账；

(b) 闭源：代码通常不会以为分类账采用的形式公开；

(c) 受控：实体（组织或集团）控制分类账，因此只有选定的参与者可以访问分类账；

(d) 隐私：由于对分类账的访问受到限制，出于隐私和保密目的，数据可能得到更好的保护；

(e) 更快的交易速度：由于参与者之间的信任度较高，因此共识协议可以允许每时间单位进行更多数量的交易。

17. 尽管不常见，但有可能拥有公共经许可分类账或私有不经许可分类账。公共经许可的分类账要求参与者在参与分类账之前表明自己的身份，尽管对谁可以参与分类账没有限制。私有不经许可分类账对谁可以参与设限，但不要求参与者表明自己的身份。

C. 与分布式分类账技术使用相关的特征

信息的恒久性

18. 信息的恒久性（或“不变性”）是分布式分类账技术的定义特征。修改分类账中存储的信息需要协商一致，从而更好地保证这些信息的完整性，即防止单方面修改信息（见上文第 8 段）。总的来说，企业在业务中实施分布式分类账技术时，必须仔细考虑不变性的影响，并采取适当的措施来解决可能出现的问题。

19. 信息的恒久性可能会产生深远的影响。例如，如果企业的所有资产在分布式分类账技术上的记录均正确无误，可能更容易确定其存在（尽管不一定评估其价值），包括在考虑破产前重组等特殊情况下。

20. 考虑到信息的恒久性，确存储存在分布式分类账上的数据正确无误非常重要。企业可以考虑可以建立系统来防止错误输入数据，例如在网络内广播要输入分布式分类账的数据，或者制定关于确认数据准确性和限制数据输入的内部指南。

21. 根据分布式分类账技术的管理和类型，存在漏洞可能被用来修改分类账上的信息的信息的风险。例如，在工作证明分布式分类账中，控制网络“挖矿哈希率”50%以上的一组验证者可以更改数字分类账。而一旦分布式分类账达到一定规模，恶意行为需要成功控制超过 50%的网络哈希率，而且成本高昂³，不太可能实现。

22. 在某些情况下，分布式分类账的管理实体可能会决定对与过去的区块不兼容的协议进行更改。这也可能影响信息的恒久性。

交易的终局性

23. 使用分布式分类账技术的交易被广播并分发到网络。一般来说，一旦交易不可逆转并且区块已经被添加到分布式分类账中，并且无法删除，则认为已经实现了终局性。在某些分布式分类账技术系统中，这会导致只有当网络同意接受区块时才表明实现交易的终局性的情况。⁴然后，交易被认为是不可撤销的，并且实现了分布式分类账的终局性。

非自由裁量自动执行

24. 分布式分类账技术的另一个特点是减少了执行分布式分类账中存储的脚本所含命令的自由裁量性（基于分布式分类账技术的自动化合约或“智能合约”）。与其他自动化合约一样，当满足预定义条件时，基于分布式分类账技术的自动化合同会自动执行。由于当事方不能单方面修改脚本，执行指示的确定性增大，从而提高了操作的效率和可预测性。然而，当法律要求包含可停止自动执行条款的软件（“终止开关”）时，分布式分类账技术的这一特征可能会带来挑战。⁵

³ 这指的是通过以市值率购买所需的加密货币来控制 51%的分布式账本的成本。

⁴ 例如，就比特币而言，当在包含相关交易的区块之后将大约六个区块添加到数字分类账中时，就实现了终局性。

⁵ 例如，见欧洲议会和理事会 2023 年 12 月 13 日关于公平访问和使用数据统一规则的第 2023/2854 号条例（欧盟）第 36(1)(b)条，以及第 2017/2394 号修订条例（欧盟）和第 2020/1828 号指令（欧盟）（《数据法》），OJ L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>,（还）要求基于分布式分类账技术的自动化合约遵守安全终止和中断的基本要求之一，即“确保存在终止交易继续执行的机制，并且智能合约包括可以重置或指示合约停止或中断操作的内部功能，特别是为了避免今后意外执行”。

假名

25. 而假名虽然不一定是影响确定当事人身份的障碍，但却可能会阻碍身份识别，特别是如果法律要求使用某种方法或程序，或者要求给身份提供特定程度的保证。如果不可能进行可靠的识别，则可能需要采取额外的措施例如异常和欺诈检测，⁶如避免存储在分类账上的数字资产进行内幕交易。

26. 使用假名的当事人可以通过使用事实要素来识别。例如，关于《电子可转让记录示范法》第 9 条对电子可转让记录中使用的电子签名规定的身份识别要求，“身份识别以及将假名和真名联系起来的可能性，包括以分布式分类账系统之外的事实要素为依据，可以满足对签名人身份识别的要求”（《电子可转让记录示范法解释性说明》，第 78 段）。

27. 向假名地址送达法律通知时可能会出现某个特定问题。在法律对此类事项更为灵活的司法管辖区，已经制定了司法文件送达的具体程序，即与加密货币有关的案件。例如，法院试图通过社交媒体或通过发送被告的加密货币钱包地址来送达法庭文件。法院还允许通过在钱包中交付的非同质化代币来送达文件（“空投”）。⁷然而，在某些司法管辖区，利用这种机制送达文件被视为违反正当程序。⁸

缺乏互操作性

28. 一般来说，分布式分类账技术缺乏跨分类账互操作性，即单个分布式分类账并非是为了与另一个分布式分类账或非分布式分类账技术应用程序交互作用。这是因为分布式分类账，特别是那些私有和定制的分类账，设计时考虑到特定的重点（或多个重点），并且不会超出其边界。缺乏互操作性可能会限制分布式分类账的应用及其带来的惠益，这是因为信息仍然位于“数据孤岛”中，无法轻松传输到其他系统或在其他系统中使用。技术工作已经开始攻克这一技术限制⁹，并确保标准化，以促进互操作性。¹⁰

⁶ 异常和欺诈检测机制包括分析数据（以统计方式或使用机器学习）来检测活动和模式中的任何异常。

⁷ LCX Ag 诉价值 1,274 万美元硬币案，编号 154644/2022，2022 WL 3585277（纽约最高法院，2022 年 8 月 21 日）；Jones 诉不明人员案[2022] EWCH 2543（Comm）；Benjamin Arthur Bowen 诉 Xingzhao Li 案（案件编号 23-cv-20399）（美国佛罗里达南区联邦地区法院，2023 年，2023 年 3 月 3 日）。

⁸ X 诉 Y 案，Gerechtshof Amsterdam，2019 年 1 月 29 日，ECLI:NL:GHAMS:2019:192，《法规判例法》判例 1921。

⁹ 例如，见 Chainlink 协议的跨链和 Polkadot 网络生态系统。

¹⁰ 例如，见 ISO/TC 307 区块链和分布式分类账技术委员会的工作方案。

D. 适用于分布式分类账技术的法律

贸易法委员会电子商务法规的基本原则

技术中性

29. 技术中性原则是贸易法委员会电子商务法规的基石。技术中性要求通过对所使用的技术、方法和产品保持中性的法律规定。这意味着，如果技术进步，不需要进一步的立法工作，因为技术中性的规则已经适应了任何未来的发展。由于技术中性，贸易法委员会的法规普遍支持使用分布式分类账技术。

30. 《电子可转让记录示范法》第 2 条所载“电子记录”的定义已扩大到包括“与逻辑上有关联或以其他方式链接在一起，从而成为该记录一部分的所有信息，无论其是否同时生成”，以确认其适用于基于分布式分类账技术的应用程序。该定义与“数据电文”的定义密切相关，后者确保了贸易法委员会电子商务法规的技术中性。

法律承认

31. 贸易法委员会法规中所载的规定在技术中性的基础上对电子手段的使用给予法律承认（并禁止对这类应用的歧视）。因此，这些规定也适用于分布式分类账技术的使用。

32. 而由于分布式分类账技术以使用加密技术为基础，已通过法律限制使用这些技术的司法管辖区（例如，仅承认按照国家加密标准和方案签发的电子签名具有法律效力）可能会对使用分布式分类账技术给予法律承认的能力加以限定。此外，这种立法选择可能不符合贸易协定中要求使用技术中性的电子签名或电子认证方法的规定。

功能等同性

33. 功能等同性原则使得能够通过使用电子手段来满足纸面表格要求。除了满足某些条件外，功能等同性还以使用可靠的方法来实现预期目的为前提。分布式分类账技术的特点，如信息的恒久性和单一性保证，可能有助于满足贸易法委员会法规中所载的某些功能等同性要求。

34. 如上所述（《分类法》，第 200 段），由分布式分类账技术系统予以支持的用于实施分布式分类账的技术和方法使得记录在分类账中的数据具有“不可变”性，也就是说，从最初输入分类账时起即保持“完整和未经改变”。这些特性与贸易法委员会电子商务法规中的“完整性”概念相对应，这一概念与某些功能等同性规则有关：

(a) 贸易法委员会《电子商务示范法》第 8 条规定，完整性是包含信息的数据电文为满足以原始形式展现或留存信息的法律要求而必须履行的功能之一。如果除加上任何背书以及在通常传递、储存和显示中所发生的任何变动之外，信息从首次以其最终形式生成之时起一直保持“完整和未经改变”，则该

功能得到实现。同一要求载于《联合国国际合同使用电子通信公约》第9(4)条。使用分布式分类账技术的方法可以在保证完整性方面提供更高水平的可靠性；

(b) 根据《电子可转让记录示范法》第10条，完整性是成为在法律上等同于纸质可转让单证或票据的电子可转让记录必须满足的功能之一；

(c) 《贸易法委员会电子签名示范法》第6(3)(d)条承认，某些类型的电子签名可能会觉察到对已签名信息的任何更改。该功能通常由使用加密技术的电子签名来实现，因此也可以在分布式分类账技术系统中找到。同样，《贸易法委员会关于使用和跨境承认身份管理和信任服务的示范法》第17条规定完整性是电子印章的功能之一。

35. 同样，信息的恒久性可能有助于满足贸易法委员会法规中所载与证据目的有关的要求。例如：

(a) 《电子商务示范法》第9条指出，在评估一项数据电文的证据力时，除其他情况外，应考虑到保持信息完整性的办法的可靠性；

(b) 《贸易法委员会关于使用和跨境承认身份管理和信任服务的示范法》关于电子存档服务的第19条规定，以生成、发送或接收数据电文的格式，或以可显示的其他格式留存该数据电文，以检测该时间和日期之后对该数据电文的任何更改，并允许附加任何签注以及正常通信、存储和显示过程中发生的任何改动。

36. 在这方面，根据欧洲联盟（“欧盟”）法律¹¹，使用名为“电子分类账”的信托服务与下述推定有关：在满足某些附加条件的情况下，其中所载数据记录的时间顺序和完整性既是唯一，又准确无误（“合格电子分类账”）。在同一法律中，“电子分类账”被定义为“一系列电子数据记录，从而确保这些记录的完整性和这些记录的时间顺序准确无误”。¹²

37. 单一性是指确保数字对象（例如电子形式的商业文件）仅存在于唯一的电子记录中。非同质化代币是分布式分类账技术的一种特定应用，由于其技术规范，可以提供更高级别的数字对象单一性保证。因此，举例来说，非同质化代币可促进满足《电子可转让记录示范法》第10(1)(b)(-)条规定的电子可转让记录的单一性要求。

分布式分类账技术在电子订约中的使用

设备位置

38. 分布式分类账技术具有去中心化的性质，其各个部分可能位于不同的司法管辖区，也可能定期改变位置。因此，在使用分布式分类账技术时，指明这一规则即信息系统的支持设备和技术的所在地并不一定是当事人营业地（《电子

¹¹ 2014年7月23日欧洲议会和理事会关于内部市场电子交易的电子识别和信托服务的第910/2014号条例（欧盟）第45k条（“《eIDAS条例》”），并废除经2024年4月11日欧洲议会和欧洲理事会修订关于建立欧洲数字身份框架的第910/9183号条例（欧盟）的第2024/1183号条例（欧盟）（“《eIDAS 2条例》”）修订的第1999/93/EC号指令。

¹² 经修订的《eIDAS条例》第3条第52点。

通信公约》第六条第四款)可能是有用的。“信息系统”的定义是“生成、接收、储存或用其他方法处理数据电文的一个系统”(《电子商务示范法》第 2(f)条和《电子通信公约》第四条第(六)项),其中包括分布式分类账。

自动执行

39. 如前所述(上文第 24 段),使用分布式分类账技术可减少单方面修改合约的可能性,从而增加对自动执行合约的信心。基于分布式分类账技术的自动化合同可以被设置为在满足某些参数时自动执行。元数据和从 oracle 之类的分类账外对象生成的数据也可以用作触发合约自动执行的条件。¹³

40. 从实际角度来看,应当指出,在涉及需要考虑特定事实和情况的条款时,如不可抗力和赔偿条款,以自动化方式执行合约条款可能具有挑战性。可以说,有可能确定和澄清这些事实和情况,以允许自动执行。然而,考虑到需要澄清的条件的数量和设想情况的复杂性,从实践角度来看,合约当事人可能倾向于不自动执行这些条款。

电子签名

41. 从技术角度来看,加密技术是分布式分类账技术的核心。基于加密技术的电子签名用于分布式分类账,用以验证和授权通过自动化合约执行的操作。

42. 从法律角度看,基于分布式分类账技术的电子签名可用于确定签名人的身份并表达其对签名电文的意图,从而满足贸易法委员会法规中关于电子签名和手写签名功能等同性的条件。相反,贸易法委员会法规依循技术中性和不歧视使用电子手段的原则也适用于使用分布式分类账技术的电子签名,因此可以在法律上予以承认。

43. 另一方面,法律可能要求使用特定的技术或服务(例如“合格签名”或“数字签名”),并可能强制使用国家技术标准和供应商(见上文第 32 段)。基于分布式分类账技术的电子签名可能无法满足这些额外要求,例如,因为其去中心化的性质不允许分布式分类账系统仅在一个司法管辖区内本地化。

44. 分布式分类账技术环境中电子签名的一个特殊应用涉及多重签名钱包的使用,特别是用于批准数字资产交易。在这种情况下,需要来自预定地址的多个基于 PKI 的签名才能继续进行交易。更一般而言,在需要不同当事人的多个签名才能授权一项交易时(例如,在公共采购中,为代管账户等),可以使用这一技术。

¹³ 例如,当达到某些参数(如船舶的地理位置或付款到期日)时,即触发基于分布式分类账技术的自动化合约。

分布式分类账技术和国际私法

45. 由于分布式分类账技术的操作和使用可能涉及多个司法管辖区，以及难以就法律选择达成一致，特别是在未经许可分布式分类账技术中，因此可能会出现国际私法挑战。

46. 一般而言，国际私法规则有助于确定适用法律。然而，分布式分类账技术系统在基础设施层的参与者（见下文第 47 段）可能分散在多个司法管辖区，并且分布式分类账本身可能位于多个司法管辖区，或者其位置可能不断变化。出于这个原因，涉及地域连接因素的国际私法规则在分布式分类账技术背景下可能不够充分。¹⁴

E. 与基础设施层有关的问题

47. 分布式分类账技术系统的基础设施层是指网络和使用它的分布式分类账。相关组件包括硬件、数据、共识和编程。所涉行为者是开发人员：设计、开发和维护运行系统的计算机代码的一个人或一组人，以及节点操作员（《分类法》，第 176 段）。简而言之，基础设施层为企业提供分布式分类账技术。

负责业务连续性管理和服务标准

48. 业务连续性管理是确保组织在发生灾难、中断或意外事件时能够继续运作的过程。其中包括识别潜在的威胁和漏洞，制定和实施减轻或预防这些威胁的计划，并测试和维护这些计划以确保其有效。服务水平管理是界定、商定和衡量组织向其客户提供的服务的表现和质量的过程。这包括设置服务级别目标、监控服务级别以及在必要时采取纠正措施，以确保达到服务水平。

49. 业务连续性和良好的服务水平管理对于建立对使用分布式分类账的信心至关重要。对于希望在业务运营中使用分布式分类账技术系统的企业来说，选择开发内部分布式分类账技术系统还是将其外包给第三方开发人员取决于业务运营的规模。规模足够大的企业可以开发其内部的分布式分类账技术系统。如果企业打算操作分布式分类账技术系统并将其提供给第三方使用或访问，则企业可能会负责作为开发人员、运营商或两者兼具，负责维持一定水平的服务。

50. 在外包分布式分类账技术系统时，企业应确保开发人员有可持续发展计划，并满足最低服务水平。建议在评估此类问题时进行尽职调查，这可能发生在交易对手审查期间，也可能发生在服务提供期间。可能的措施包括要求开发商提供业绩记录，要求提供资产负债表或损益表以评估开发人员的财务状况，以及对开发人员的声誉和知名度进行基本的在线研究。

51. 企业可考虑与发展人员订立合约，制定业务连续性管理计划及预期的最低服务标准。此外，企业可考虑制定关于第三方服务供应商在与之订立合同之前必须达到的最低标准的内部指导方针或政策。可能需要对现有的业务连续性管理进行修订，以使其适应分布式分类账技术的特点。尽职调查，加上

¹⁴ 见海牙国际私法会议初步文件。2020 年 11 月第 4 号文件，附件一，国际私法相关因素清单及其在分布式分类账技术环境中的使用。

明确规定各方权利和义务的合同，可以减少分布式分类账技术服务提供商不履约的机会。

审计程序和审计权

52. 与分布式分类账技术服务提供商和用户之间的关系有关的一个具体问题是审计权和审计程序的执行。通过对分布式分类账代码、开发人员和运营商的第三方独立审计，可以增强对所部署的分布式分类账技术系统的信心。审计程序包括进行分布式分类账审计，以筛选出功能失调或欺诈性代码，并识别分布式分类账技术系统中的任何潜在漏洞或弱点。

53. 在企业将分布式分类账的开发或运营外包的情况下，企业可以考虑在与开发人员和运营商的合同中插入一个条款，授予他们审计代码的权利。这赋予了企业对第三方开发人员的代码进行审计的合约权利。由于该代码的大部分将在企业自己的服务器或信息技术系统中实施，因此审计权和关于如何进行审计的协议是保护企业免受利用代码中的错误进行网络安全攻击的重要机制。

环境关切

54. 在构成比特币等加密货币基础的工作证明共识机制中，需要花费大量精力来验证交易是否已在分布式分类账上执行。监管机构担心分布式分类账挖矿的环境足迹。¹⁵减少由工作证明机制引起的能量消耗是可取的，并且有几项举措旨在使加密货币行业脱碳。¹⁶从工作证明转向权益证明共识机制可能会降低与加密货币挖矿相关的能源成本。¹⁷

55. 考虑到分布式分类账挖矿消耗的大量电力，未来对此类活动的监管或报告要求可能会变得更加普遍和全面。从事分布式分类账挖矿的企业应该了解可能监管此类活动的立法。¹⁸

F. 与应用层有关的问题

56. 应用层涉及依赖分布式分类账技术提供产品和服务。所涉行为者是提供产品和服务的企业以及产品和服务的用户。

合约自动化

57. 基于分布式分类账技术的自动订约被认为是分布式分类账技术系统的一大优势，因为自动执行代码的可信度更高（见上文第 24 段）。贸易法委员会关于自动订约的条文草案（A/CN.9/1178 和 A/CN.9/1179）在技术中性的基础上，就

¹⁵ 有关分布式账本挖掘对环境影响的更多信息，见 Chamanara, S. 和 Madani, K. (2023 年)。加密货币的隐藏环境成本：比特币挖矿如何影响气候、水和土地，联合国大学水、环境和卫生研究所（水环卫所），加拿大安大略省汉密尔顿，<https://inweh.unu.edu/>。

¹⁶ 例如，《加密气候协议》是一项关于分布式分类账挖矿脱碳的倡议。

¹⁷ 以太坊网络从工作证明机制转向权益证明机制，这大大减少了能源使用和碳足迹。

¹⁸ 例如，美国 2022 年的《加密资产环境透明度法案》要求在进行加密挖矿作业时消耗超过 5 兆瓦电力的各方根据《清洁空气法》报告其二氧化碳排放量。

使用合约自动化时可能产生的法律问题提供了指导。条文草案不涉及执行脚本的可能性，此为商业问题，而非法律问题。条文草案也不涉及如何自动执行某些合约条款的问题（见上文第 39-40 段）。

对错误信息的责任

58. 责任和风险分配的一个方面涉及分布式分类账上的信息不准确，原因可能是善意的错误，也可能是欺诈行为。这种情况可能发生在开发阶段（例如，在部署分布式分类账时插入恶意代码）或信息输入期间（例如，已知输入的信息不准确）（见上文第 20 段）。

59. 关于数据输入，记录不准确或虚假信息责任仍由提供信息者或其代表承担。从商业角度来看，企业应该仔细考虑数据输入的质量和可能的补救措施，特别是如果它们依赖分布式分类账进行关键操作。允许用户（特别是第三方）访问或使用其私有经许可分布式分类账的企业应订立合约关系，以限制其对用户的责任。

数据隐私和保护

60. 许多国家颁布了数据隐私和保护法，这些法律也适用于基于分布式分类账技术的应用。例如，欧盟《一般数据保护条例》¹⁹适用于涉及个人数据的情况，包括使用分布式分类账技术的情况。在这方面，有人建议，鉴于公钥和动态 IP 地址之间的类比关系，根据《一般数据保护条例》，公钥可以被视为个人数据。²⁰

61. 在使用分布式分类账时，企业应考虑个人数据是否会存储在分布式分类账上，且应采取积极措施遵守适用的数据隐私法和数据保护法。由于开发人员、运营商和用户可能位于多个司法管辖区，因此应在服务协议中加入合约条款，以确保遵守所有相关的数据隐私法和数据保护法。

数据存储（“被遗忘权”和“删除权”）

62. 使用分布式分类账技术储存信息的恒久性可能会对遵守某些权利（例如被遗忘权和删除权）构成挑战。当所涉及的数据或信息是高度敏感的个人数据，如医疗记录或生物识别信息，这些问题就更加相关。此外，分布式分类账技术具有去中心化性质，这就意味着，居住在一个司法管辖区的个人的信息可以存储在不同司法管辖区，并且存储地点可能会定期变化。

¹⁹ 2016 年 4 月 27 日欧洲议会和欧盟理事会关于保护自然人处理个人数据和此类数据自由流动的第 2016/679 号条例（欧盟），以及废除第 95/46/EC 号指令（《一般数据保护条例》），OJ L 119, 4.5.2016, 第 1-88 页。欧洲法律研究院：<http://data.europa.eu/eli/reg/2016/679/oj>。

²⁰ 《一般数据保护条例》对动态 IP 地址的应用，见欧洲法院，2016 年 10 月 19 日，Patrick Breyer 诉联邦德国，ECLI:EU:C:2016:779。

63. 此外，由于分布式分类账技术的去中心化性质，可能很难识别数据控制者或负责执行“被遗忘权”和“删除权”的或其他实体。由于使用假名，在确定该实体方面可能存在挑战，这可能会使问题进一步复杂化。

64. 从概念层面上可以反驳的是，分布式分类账技术并不总是严格不可变的，开发人员和管理员可以同意删除某些数据，至少可以从私有经许可分布式分类账中删除。然而，该解决方案不能解决公共不经许可分布式分类账中的数据删除问题。

65. 另一种可能的解决方案是将个人数据存储到不位于分布式分类账上的数据库中。但是这种解决方案并没有解决删除权的问题，还可能会增加成本。

66. 分布式分类账技术平台还可实现隐私增强功能，允许对数据进行加密或匿名化，使其无法轻易追溯到个人。然而，这些措施可能并不总是足以充分保护个人数据。此外，保持交易的机密性不应妨碍对其进行的审核。在这些加强隐私的功能可能无法实现时，例如，由于使用了公共不经许可分布式分类账，可以在处理整个网络的信息时尽量减少数据（见下文第 69 段）。

修改错误存储信息的权利

67. 数据恒久性会产生的另一个操作问题是，可能很难修改存储的错误信息，或者很难更新或更改不再相关或不再准确的数据。解决方案类似于被遗忘权，即建立预先界定的治理规则，降低中心化，促进对数据的控制。

68. 已发布和公布了允许应用户要求修改或删除数据的代码。该技术解决方案为企业提供了遵守数据隐私法和数据保护法的额外可能性。

缓解措施

69. 为缓解上述问题，企业可以利用零知识证明等隐私增强功能。零知识证明是一种方法，通过该方法，一方（“证明人”）可以向另一方（“验证人”）证明给定陈述为真，而证明人除了陈述确实为真这一事实之外，避免传递任何额外信息。

70. 企业可以考虑对数据进行加密和匿名处理，使数据不易与个人相关联。如果这些数据丢失，随后又被不掌握解密密钥的个人发现，由于存在加密和匿名处理，访问数据也是无用的。

具体应用：数字资产

71. 存储价值的数字通常称为“数字资产”，对其进行法律处理的办法引起了极大关注。虽然任何数据都有一定的价值，并因此可以被界定为数字资产，但“数字资产”的法律概念通常是指使用分布式分类账技术存储和转移价值。各国对“数字资产”的定义有不同的方法。例如，美利坚合众国商品期货交易委

员会似乎强调数字资产的控制和可转让性，²¹而欧盟似乎专注于资产“代表”的内容，即代币所包含的权利。²²《分类法》确认对数字资产的定义缺乏共识；但规定“数字资产”一词通常含义意味着以电子方式存储的有用途或有价值的数据的集合（《分类法》，第 82 段）。

72. 目前已经起草了法律，旨在填补适用于数字资产的制度中的法律空白。²³其中有些法律保障了其他法律的适用，特别是适用于商业单据和货币的法律。关于国际私法，海牙国际私法会议常设局正在进行一项特别法研究，重点关注数字货币的特定跨境使用案例所引发的国际私法问题。²⁴

73. 由于涉及使用分布式分类账技术的数字资产应用多种多样，最好单独考虑不同类型数字资产所产生的法律问题。

支付服务和加密货币

74. 数字资产可用于转移价值。²⁵这些数字资产通常被称为加密货币。如果加密货币具有足够的流动性，可以在专门的市场（“加密货币交易所”）进行交易，那么加密货币可能具有市场价值。有些加密货币将其价值与法定货币或其他商品挂钩，以减缓波动（“稳定币”）。

75. 在国家货币高度波动或对跨境支付有限制的地方，加密货币可能被视为一种更稳定、更有效的价值转移形式。一些国家已经宣布，将加密货币作为国家货币之外的法定货币。然而，这引发了新的问题，例如原有货币与加密货币之间的汇率问题，以及更普遍的货币政策问题。

76. 加密货币的使用带来了法律、监管和商业方面的挑战。加密货币的法律资格，包括适用的监管制度，取决于其特征。监管机构越来越多地将数字资产视为商品、证券或两者兼而有之。²⁶使用分布式分类账技术系统开展的支付服务必须遵守支付法律。

77. 关于法律问题，将加密货币归类为财产的能力问题尚未解决。在那些可能可行的司法管辖区，加密货币持有者可以使用专有补救措施，例如冻结资产。²⁷

78. 从商业角度来看，包括稳定币在内的加密货币可能具有高度波动性。如果企业希望使用加密货币进行支付，可以考虑使用不同的加密货币交易所和加密

²¹商品期货交易委员会，“数字资产市场小组委员会建议——采用数字资产分类和理解方法”，2024 年 3 月 7 日。

²²全球区块链商业委员会，监管地图。

²³美国《统一商法典》第 12 条；《统法协会数字资产和私法原则》；迪拜国际金融中心《数字资产法》，2024 年第 2 号法律。

²⁴2024 年 3 月海牙国际私法会议结论与决定，第 12 号。

²⁵创设比特币的初衷是能够实现支付的去中心化。

²⁶在某些情况下，加密货币可以作为商业单证。例如，商品化的稳定币（即价值与特定商品相关联的稳定币）可被视为仓单，条件是商品已被识别并存储在仓库中（而非商品价格指数），并且符合仓单的其他法律要求。

²⁷例如，在 AA 诉不明身份者[2019] EWHC 3556 (Comm) 案中，英国法院允许就赎金支付发布比特币专有禁令。破产程序中的民事资产追查和追回，包括与数字资产有关的民事资产追查和追回，是贸易法委员会专门工作流处理的一个议题（见 [A/CN.9/WG.V/WP.192](#) 和 [A/CN.9/WG.V/WP.193](#)）。

货币，以便在发现交易所或货币有问题时，包括在加密货币交易所突然违约的情况下，降低风险。

79. 中央银行数字货币（“央行数字货币”）被界定为以电子形式发行的法定货币。因此，它们仅由央行发行，并且在性质上与加密货币不同。²⁸央行数字货币试点项目通常涉及分布式分类账技术的使用，²⁹重点关注央行数字货币的零售使用。³⁰海牙国际私法会议成立了一个专家组，研究央行数字货币跨境使用和转移所引起的适用法律和管辖权问题。³¹

电子可转让记录

80. 在实践中，可以使用基于分布式分类账技术的应用程序签发《电子可转让记录示范法》界定的电子可转让记录。这些记录是电子形式的可转让单证和票据，因此，这些单证和票据的实体法与《电子可转让记录示范法》的颁行所载规则一并适用。《电子可转让记录示范法》的解释性说明就选定的分布式分类账技术相关问题提供了具体指导。例如，在没有中央运营人的系统中，同意使用电子可转让记录可能是默示的，也可根据行使记录控制权或履行记录所载义务等情形推断出来（《电子可转让记录示范法解释性说明》，第 66 段）。此外，在使用假名的情况下，将假名与姓名联系起来，即可满足识别控制人身份的要求（《电子可转让记录示范法解释性说明》，第 117 段）。

81. 类似的考虑也适用于根据一项法律签发电子可转让记录的情况，该法律未预见功能等同性做法，但在法律上仅允许使用这些记录的电子形式。同样，这些考虑也适用于通过采取媒介中性办法而允许使用纸质和电子单证的法律。贸易法委员会-统法协会仓单示范法草案（A/CN.9/1182）提供了后一种办法的实例。

G. 与治理层有关的问题

82. 由于分布式分类账技术的去中心化性质，可能会出现与基础设施层相关的特殊治理问题，特别是在公共经许可分布式分类账的情况下。由于缺乏中央权力机构，决策通常通过基于治理代币的投票做出，由此造成了这些治理问题。这些代币的持有者可能不知道彼此的存在，甚至可能未被识别，因为他们使用假名操作，这就是治理层。

83. 针对治理层所涉主体的诉讼并不少见。虽然此类诉讼通常可能涉及分布式分类账系统故障引起的任何问题，但在实践中，诉讼案件往往涉及黑客利用程

²⁸ 国际货币基金组织发布了《央行数字货币虚拟手册》，其中提供了决策者关于央行数字货币最常见问题的信息。它还为用户提供了一个探索央行数字货币和央行数字货币产品开发章节的框架。《央行数字货币虚拟手册》可查阅 www.imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook。

²⁹ 例如，mBridge 项目使用专用的分布式分类账进行多央行数字货币跨境支付；见 www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm。

³⁰ 批发法定货币可能只是以电子形式创建，作为分类账中的一个条目。一旦货币转移到商业银行，这些银行就对中央银行负有债务。

³¹ 2024 年 3 月海牙国际私法会议结论与决定，第 9 和 10 号。

序错误造成的数字资产损失。由于实际原因，通常无法对黑客伸张正义，因此受害方要求治理层所涉及的主体和据称对编程错误负责的主体进行赔偿。

84. 从广义上看，对节点操作员、开发人员或去中心化自治组织成员提出索赔的能力（见下文第 98 段）取决于分布式分类账的类型及其目的。按角色分列可能有助于审查责任情况。一般来说，有四个关键角色与讨论责任和分布式分类账技术相关：代码开发人员，分布式分类账技术运营人、分布式分类账技术的用户和索赔方。基于加密技术的电子签名用于确立与假名相关联的角色。

85. 使用去中心化治理结构所产生的关键问题之一是，由于承认去中心化治理结构作为法律实体存在不确定性，就各方的权利和义务达成一致可能颇具挑战性，特别是在使用公共经许可分布式分类账时。在许多情况下，由于使用了“假名”，甚至很难确定所涉实体。

86. 开发人员参与构建私有经许可分布式分类账时，可以降低交易对手风险。由于可以明确识别交易对手，企业可以通过确保与法律认可的实体签订合同、核实公司在构建和维护分布式分类账技术系统的记录等方式进行尽职调查。

87. 为商业目的使用经私有经许可分布式分类账的企业，在向开发人员索赔时通常面临的困难较小，这是因为开发人员的身份以及开发和部署代码的条款具有确定性。

88. 另一方面，针对公共不经许可分布式分类账开发人员的索赔可能更为复杂。首先，可能需要开展大量工作，以确定使用假名运营的开发人员或节点操作员。其次，是否建立法律关系以及建立何种法律关系（例如，以信托责任的形式）来确定受影响方与开发人员或运营人之间的权利和义务，这一点值得商榷。³²第三，由于地理位置偏远，对开发人员或节点操作员执行判决可能具有挑战性。

89. 此外，确定开发人员或运营人的法律人格可能具有挑战性（即在去中心化自治组织情况下），从而难以将赔偿责任归于所涉当事人。如果有保险且适用于其业务运营，企业可以通过购买保险来减轻风险。

90. 在针对加密货币开发人员的诉讼中，可以看到与公共经许可分布式分类账中的开发人员责任有关的诉讼。在一个此类案例中，一位比特币所有者因账户被黑客攻击而损失了资产，基于开发人员和用户之间的信托责任，他起诉比特币开发人员，要求开发一个软件补丁，以恢复对账户的访问。³³据认为，开发人员对用户负有信托责任这一论点是可行的。³⁴

³² 为了弥补这一差距，<https://jonasgross.medium.com/legal-aspects-of-blockchain-technology-liability-8f5b433030fit>，有人建议根据产品责任法在某些司法管辖区提出索赔，此类索赔不仅限于身体伤害，还包括经济损失。在这些情况下，分布式分类账技术环境中的产品责任通常针对开发人员，但很少针对运营商。

³³ Tulip Trading 诉比特币协会案，2022 年 3 月 25 日，[2022] EWHC 667 (Ch)。

³⁴ 原告对 Falk 法官在“Tulip Trading 诉比特币协会”案中的裁决提出上诉，上诉获准。案件将继续审理，以查明在具体案件中是否存在信托责任：见大法官 Lewison、大法官 Popplewell 和大法官 Birss 作出的上诉判决，Tulip Trading 诉 Van der Laan 案，2023 年 2 月 3 日，[2023] EWCA Civ 83。

去中心化自治组织

91. 在分布式分类账技术的启发下，人们创建了一种被称为去中心化自治组织的特定实体来管理它们。去中心化自治组织是一种基于分布式分类账技术的治理结构，可供任何盈利或非盈利组织使用。一些政府和机构对去中心化自治组织进行了界定；例如，欧洲央行将去中心化自治组织定义为“基于代码和区块链技术构建和运行的虚拟组织”。其他机构提供了更详细的定义：例如，美国财政部将去中心化自治组织定义为“根据一套编码和透明规则或智能合约运作的管理系统”。

92. 可以确定去中心化自治组织的共同关键要素。去中心化自治组织使用基于分布式分类账技术的自动化合约运作。它们通常是去中心化的，有跨越不同司法管辖区的多个成员。因此，去中心化自治组织的治理结构和法律地位是建立合同关系或确定各方责任归属的一个突出问题。

93. 去中心化自治组织的可变形式和去中心化性质意味着其可以采用混合治理结构。³⁵因此，为讨论由此产生的法律问题，应该厘清去中心化自治组织的治理结构。如果不能正确地赋予去中心化自治组织以法律人格，就会对与去中心化自治组织进行交易的企业和去中心化自治组织成员产生广泛影响，他们可能会因去中心化自治组织的行为而承担个人责任。

去中心化自治组织的治理结构

94. 去中心化自治组织可以采用不同的组织结构。决策可能仅限于去中心化自治组织的创建者，可以通过软件协议实现自动化，或者根据所控制代币的类型和数量分配投票权重。去中心化自治组织使用基于分布式分类账技术的自动化合约来制定有关去中心化自治组织的目的、成员如何同意合作、如何通过投票程序集体做出决策、如何创建和分发本地代币，以及满足某些条件后如何执行交易的规则。

95. 去中心化自治组织的治理结构由基于分布式分类账技术的自动化合约驱动。因此，去中心化自治组织需要一个结构化的决策过程。在没有中央权力机构的情况下，共识和争端解决机制最为重要，例如通过多数表决或算法。首先应确定谁可以提交行动方案建议。随后，由决策机构或算法做出决策。

96. 某些去中心化自治组织只允许持有特定数字资产（所谓的“治理代币”）的成员参与决策过程。通常情况下，投票的权重与托管的特定数字资产的数量成正比。特定数字资产通常是通过向去中心化自治组织投资、为去中心化自治组织分配工作时间或以其他方式支持去中心化自治组织（如担任营销大使）来获得。

97. 与由董事会或首席执行官做出决策的传统公司机制相比，去中心化自治组织的决策通常取决于群体共识或成员投票。去中心化自治组织通常可以自由定义其治理结构，以满足组织的目标，使其成为一种灵活的工具，可用于广泛的

³⁵ 混合治理结构允许一定程度的中心化，同时也包含去中心化的要素。从商业角度来看，这可能需要允许用户对企业可能做出的某些决策（例如未来的产品设计和更新）进行权衡。

协作目的。然而，初步的经验证据表明，治理代币被不成比例地分配给了创始人和核心开发人员。

98. 通常，去中心化自治组织的治理以规则或行为准则为基础，这些公开的规则或行为准则可通过白皮书、网站或应用程序获得。然而，这些规则并不像传统的公司组织工具那样具有法律约束力。

99. 在一些去中心化自治组织中，成员使用假名。关于假名和当事人身份识别的一般原则也适用于去中心化自治组织。

100. 去中心化自治组织的典型特征（其中一些可能会给企业带来风险）如下：

(a) 决策：共识规则通常在早期阶段确定，并且随着时间的推移，并且当去中心化自治组织的规模和复杂性增加时，相对难以修改，这可能导致共识机制不充分，例如速度慢、效率低。这可能最终限制去中心化自治组织的运作，甚至妨碍对意外情况作出迅速反应；

(b) 缺乏问责制：去中心化自治组织中的决策通常涉及多方，因此责任分散，这是社会心理学已知的一个概念，导致个人责任感较轻。因此，由于问责制度缺乏，没有中央监督的去中心化自治组织可能容易出现资源管理不善的情况；

(c) 缺乏代表性：根据所实施的代表制度，例如投票权与特定数字资产的持有量成正比，一些去中心化自治组织成员可能会在决策过程中感到代表性不足，从而可能导致决策的接受度降低，造成不满和冲突；

(d) 安全漏洞：去中心化自治组织依赖于基于分布式分类账技术的自动化合约，在发现安全漏洞时相对难以修改。这可能会使去中心化自治组织面临网络威胁或根本挑战，例如在投票或支付机制出错的情况下。

101. 决定与去中心化自治组织进行商业交易的企业应该意识到这些风险。与去中心化自治组织合作时，可以限制风险的步骤包括：核实去中心化自治组织的注册状态，并要求去中心化自治组织确定其成员和开发人员的身份，以便企业在最坏情况下可以在个人责任的基础上继续进行交易。

适用于去中心化自治组织的合同义务和责任问题

102. 由于在透明度和定制化方面颇具潜力，去中心化自治组织可能对企业有吸引力。然而也存在潜在问题：由于其组织结构不明确，去中心化自治组织在法律上有很大的不确定性。由于去中心化自治组织的可能类型和结构范围广泛，必须逐案评估每个去中心化自治组织，以确定适用何种法律。

103. 在缺乏具体立法的情况下，曾试图将去中心化自治组织归类为现有的法律实体，如普通合伙企业、有限责任合伙企业或非营利组织。

104. 一些国家引入了具体的法律机制（有时称为“法律包装”），例如允许去中心化自治组织注册，从而赋予其法律人格。³⁶这些法律通常为法人实体提供保护，并允许去中心化自治组织像有限责任公司一样限制其责任。³⁷这大大提高了法律的可预测性，从而简化了与去中心化自治组织打交道的过程。

105. 在可以成立去中心化自治组织但未能成立的国家，监管机构试图将责任归咎于个人成员，让他们承担个人责任。³⁸其法律后果通常是去中心化自治组织的“合伙人”（即代币持有者）承担无限个人责任。

106. 然而，从实践角度来看，追究去中心化自治组织的个人成员这一过程可能很漫长而且困难重重，特别是如果去中心化自治组织的成员使用假名，且不居住在同一个国家的情况下。

107. 去中心化自治组织的法律资格决定了适用的破产制度。但是，由于去中心化自治组织的性质和使用分布式分类账技术，可能会产生一些与破产有关的特殊问题。例如，去中心化自治组织的成员可被视为破产去中心化自治组织的债权人或债务人；治理代币可被视为财产；成员和董事（如果有的话）可被视为对彼此和用户负有信托责任，等等。

法律自动应用联盟示范法

108. 一些学术机构已经开展了一些项目，以解决与去中心化自治组织有关的法律问题。法律自动应用联盟作为智库，致力于探讨去中心化经济和分布式分类账技术所产生的法律问题。它发布了《法律自动应用联盟去中心化自治组织示范法》（《法律自动应用联盟示范法》），规定了去中心化自治组织的治理和运作规则。³⁹

109. 《法律自动应用联盟示范法》对功能等同性概念进行了调整，使之适应去中心化自治组织的情况。它指出，确立功能等同性“有助于简化对去中心化自治组织的监管”，这要求“确定一项政策目标或宗旨，然后证明这一目标或宗旨可以通过执行一项法律规则或依靠特定的技术应用来实现”。⁴⁰《法律自动应用联盟示范法》提供的关于功能等同性的一个实例如下：

³⁶ 在美国，例如田纳西州，《田纳西州法典注释》，第 48 编，经修订；佛蒙特州，《基于区块链的有限责任公司的有限性》，《佛蒙特州法规注释》，第 11 章，第 4173 节；怀俄明州：《怀俄明州去中心化非法人非营利协会法》，《怀俄明州法规》，第 17 编，第 32 章。另见马绍尔群岛共和国 2022 年《去中心化自治组织法》。

³⁷ 例如，佛蒙特州允许注册“基于区块链的有限责任公司”，这就要求基于区块链的有限责任公司说明“其使用或启用的去中心化共识分类账或数据库是完全去中心化的还是部分去中心化的，以及这种分类账或数据库是完全或部分公共的还是私有的”（《佛蒙特州法规注释》，第 11 章，第 4173 节）。

³⁸ 商品期货交易委员会诉 Ooki 去中心化自治组织案，美国加利福尼亚州北区地方法院，案件编号：3:22-cv-05416-WHO。法院认为，“根据《商品交易法》，Ooki 去中心化自治组织是一个‘人’，因此可以追究其违法责任”。法院随后认定，Ooki 去中心化自治组织确实违反了所指称的法律。

³⁹ 美国，以《法律自动应用联盟示范法》为基础的《犹他州去中心化自治组织法》（《犹他州法典》，第 48 编，第 5 章）。

⁴⁰ 法律自动应用联盟，《去中心化自治组织示范法》，第 8 页。

“例如，与其引入专门适用于‘代币化’股票的新公司规则，不如将基于区块链系统记录的股票视为有效的股票所有权，可通过基于区块链的登记处进行转让。监管等效依赖相同的技术，但将任何特定监管的目的或宗旨确定为目标。它允许在法律规则的功能和技术的功能之间建立等同关系。”⁴¹

110. 根据《去中心化自治组织示范法》，法律人格问题的解决办法是，明确规定去中心化自治组织具有独立于其成员的法律人格（《去中心化自治组织示范法》第2条）。

三. 术语表

业务连续性管理：确保组织在发生灾难、中断或意外事件时能够继续运作的过程。其中包括识别潜在的威胁和漏洞，制定和实施减轻或预防这些威胁的计划，并测试和维护这些计划以确保其有效。

中央银行数字货币：电子形式的法定货币。

共识：节点之间就如何验证分布式分类账上的交易达成的协议。

共识机制：达成共识的机制。最常见的共识机制类型是工作证明和权益证明机制。

加密哈希函数：一种将输入字符串转换为固定大小输出的算法。该输出可以存储起来，随后用于验证目的。

加密货币交易所：可买卖数字资产的交易平台或市场，具体取决于各个平台的产品。

数据孤岛：通常与某些用户群隔离的数据池，不易被相同用户群访问。

分布式分类账审计：一种审计程序，用于筛除功能失调或欺诈性代码，或识别分布式分类账技术系统中的任何潜在漏洞或薄弱环节。

终止开关：可停止自动执行条款的软件。

挖矿：特定共识机制中的活动，例如工作证明，用于验证分布式分类账上的分类账记录。矿工是这项活动的参与者。

挖矿哈希率：衡量矿工解决给定加密难题所需计算能力的单位。

多重签名钱包：一种使用多个私钥的服务，允许控制、存储或转移数字资产。

节点操作员：作为分布式分类账一部分的计算机的操作人员。

非同质化代币：一种无法在单个单位之间相互替代的数字资产。

信息的恒久性（或不变性）：分布式分类账的一个特征，其中记录一旦被添加到分类账中，就不能被修改或删除。

⁴¹ 同上，第3页。

假名：假名是指使用假名地址，这是通过加密过程生成的唯一字符串，用于表示分布式分类账系统中的人员。假名地址可能与自然人或法人相关联，因此无法确保匿名性。

权益证明：一种用于验证记录的共识机制。在权益证明中，验证人在投入一定数量的数字资产后被随机选中。当特定数量的验证人被选中，且验证人确认记录准确无误时，该记录就会成为分布式分类账的一部分。

工作证明：一种用于验证记录的共识机制。在工作证明机制中，矿工（与权益证明机制中的验证人不同）竞争解决加密难题。该机制的一部分要求矿工向网络证明矿工已经完成加密，并在证明后将记录添加到分布式分类账中。成功挖矿的矿工通常会获得数字资产。

删除权：个人要求组织或企业删除其所述个人数据的权利。

被遗忘权：与删除权类似，被遗忘权是个人要求组织或企业删除其所述个人数据的权利，但有一项附加条件，即确保第三方不会引用或链接组织或企业提供的此类个人数据。

服务水平管理：这是一个界定、商定和衡量组织向其客户提供的服务的表现和质量的过程。这包括设定服务水平目标、监控服务水平以及在必要时采取纠正措施，以确保达到服务水平要求。

稳定币：一种价值与另一种资产挂钩的数字资产。这种资产可以是法定货币、商品或其他数字资产。

零知识证明：通过该方法，一方（“证明人”）可以向另一方（“验证人”）证明给定陈述为真，而证明人除了陈述确实为真这一事实之外，避免传递任何额外信息。
