
ICANN81 | AGM — 运作方式：区块链域名技术
土耳其时间 2024 年 11 月 10 日星期日 — 13:15 至 14:30

亚兹德·阿坎诺

(YAZID AKANHO):

大家好，欢迎参加“运作方式：区块链域名技术”会议。我叫亚兹德·阿坎诺，是本次会议的参会经理。请注意，本次会议正在录制中，请大家遵循 ICANN 预期行为标准和 ICANN 社群反骚扰政策。

在会议期间，只有在问答窗格提交的问题和意见才会被读出，主要供在线参与者使用。本次会议的口译将包括英语、法语、西班牙语、阿拉伯语、俄语和土耳其语。如果在会议期间想要发言，请在 Zoom 中举手示意。被叫到名字时，将允许虚拟参会者在 Zoom 中取消麦克风的静音。现场参会者将使用麦克风发言。请说出你的姓名以便记录，如果你使用的不是英语，也请指明你将使用的语言，然后以合理语速发言。现在交给保罗·霍夫曼 (Paul Hoffman)。保罗 (Paul)，交给你了。

保罗·霍夫曼:

谢谢亚兹德 (Yazid)。希望所有人都来参加本次主题会议了。如果有人没来，那可能是其他会议或多或少有一些吸引人的地方。欢迎大家。首先，我要感谢在座的很多人参加本次“运作方式”会议，这是他们首次涉足区块链域名系统甚至是整个区块链领域。本次演示将会 — 我们特意只做简短的演示，让大家最后有充足的时间提问。本次演示包括两个主题：区块链和区块链域名系统。这里考虑的一点是，ICANN 社群关注区块链域名系统的人当中大多数也需要了解区块链。所以，我们会先介绍区块链，然后再介绍区块链域名系统

注：以下内容为针对音频文件的誊写文本。尽管文本誊写稿基本准确，但也可因音频不清晰和语法纠正而导致文本不完整或不准确。该文本仅为原始音频文件的补充文件，不应视作权威记录。

的运作原理。再次说明，我会尽量简洁地讲解，以便大家有充足的时间进行问答。

首先，我想介绍一下 ICANN 最近的一些出版物。你们很多人都知道，但有些人可能不知。因为现在有很多人关注区块链域名系统，而大家听到了针对各种域名系统的不同观点和推广信息，所以 ICANN 社群内部对此有很多疑问。这些问题可以分为两种。一是这些域名系统是什么？大家已经熟悉 DNS（域名系统）。这就是我们在这座大楼里做的事情。但这些域名系统与 DNS 有何不同？另外，这些域名系统为何被称为“区块链域名系统”？区块链又是什么？

鉴于大家有诸多疑问，我们在几周前发布了两份文件。我是这两份文件的作者，它们属于 OCTO 文档系列。这里附上了链接，大家下载演示文稿就可以看到。或者也可以通过 ICANN 网站进入 OCTO 文档系列链接，最新的两份出版物就是这两个文件。OCTO-039 是关于区块链域名系统技术，OCTO-040 则是关于区块链。你们可以按任意顺序阅读。顺便说一句，可能很多人实际上并不关注区块链域名系统，但想了解有关区块链的更多信息。这些文件完全是技术性的并且是中立的。其中没有任何推广信息。坦白说，很多人并不喜欢区块链。其中也没有贬低之意。它们都只作技术说明，态度中立。其原因是，区块链和区块链域名系统都在不断发展，也许你今天喜欢某样东西，但当它变得更差之后你又不喜欢了。或者原本不喜欢的变得喜欢了。你可能会说这些还没有准备好，无法投入实际使用，但将来它们可能就准备好了。以上就是关于这两份文件。如果你在会上准备时没有阅读它们，我完全理解。大家可以在会议周内随时找时间阅读。

有一点我没有放在这张幻灯片上，那就是我是这两份文件的主要作者。在编写这些文件时，我参考的源材料是区块链社群和区块链域名系统社群的文档。这些社群的文档很糟糕，存在不一致等等问题。所以我在这两份文件中都加入了免责声明，说我可能弄错了。我的意思是，其中的事实可能存在错误。所以，我们准备在六个月内编写这两份文件的第 2 版。我无比希望有人能反馈我是否有哪里弄错了。结果是我做得挺不错。已经两个星期了，到目前为止还没有人找我指出错误。但我之所以在这里说这些，是为了请大家在这六个月内再检查看看。文件名仍然是 OCTO-039 和 OCTO-040。不过我已经了解到大家希望补充一些信息来帮助理解，并且我前几天突然发现了一个术语差异。

接下来，我将先介绍区块链，然后再介绍区块链域名系统。在进行这次区块链方面的研究时，我发现一件有趣的事情是，我遇到有人说，“哦，我知道什么是区块链。它是个分类账。它是个数据库。它有加密之类的技术。”这些观点大部分都是错的。它们错误的原因在于区块链生态系统故意尽其所能地制造混乱。他们这么做并不是为了伤害你，而是为了帮他们自己赚更多的钱。这完全可以理解。过去，互联网生态系统的许多部分都发生过这种情况。有些年龄跟我差不多并且记得 90 年代中期情况的人应该知道，1995 年前后网络技术也发生了同样的事情。一个典型的例子，很多人认为，“哦，区块链就是个数据库。”事实并非如此，我将在接下来的幻灯片中详细讲述这一点。区块链不仅仅是一个数据库，同时又远远不及一个数据库。

本次会议的目的、我们将在周三举行的会议的目的，我将在稍后的演示中讲到，当然也是这两份文件的目的，是尽量减少流行用语的

使用，为此，我们将使用与区块链社群中所用不同的用语。其原因有二。一是区块链社群里的很多术语都是故意自我宣传的。行。我说了，记得 90 年代中期情况的人应该记得信息高速公路。它并不是一条高速公路。事实上，它是很多条没有完全铺平的路。同样，他们对此也使用了各种术语。但另一个原因是，这个社群内部没有协调好，他们会使用同一术语来表示截然不同的事物。所以，我有时会挑一个，有时会自己编一个然后说明“它涵盖的是这个意思”。有一点非常明确的是，人们对区块链的关注大多是关于金融、货币、贷款等方面。这些我都没有包括在内。这并不是 ICANN 社群感兴趣的内容。抱歉。这并不是 ICANN 社群域名部分感兴趣的内容。这是一个非常令人沉迷的话题。你越是深入其中，就越容易被它吸引。这不是我们这里要讨论的内容。

接下来的几张幻灯片是关于区块链最重要的部分，技术部分。首先是分类账。我们都知道分类账是什么，即使是从未用过。我们知道银行有分类账。它是一份按顺序列出的交易清单。你不能改写它，也不能去除其中的内容。区块链就是以分类账概念为基础。我们在想到银行的分类账时，通常就是这个账户将 50 美元转移到另一个账户，或者这个账户拿走了 50 美元。对于很多区块链交易来说也是如此。但实际上，一些区块链，尤其是以太坊，允许交易成为程序，我的意思是像成熟的计算机程序一样来解决一些问题，比如如果转账的人资金太少或太多，就这样做；如果不是这样，就在这里写出相关信息。诸如银行分类账中更为复杂的一些问题。但话说回来，想想分类账，即使是银行的分类账，你也无法通过查看分类账中的部分信息来确定某人有多少资金。你得查看整个分类账才能知晓。而在正常的银行分类账中，并没有这样的记录：“保罗向亚兹德转了 50 美元。因此，保罗的账户中有这笔资金。”它只是显示保罗向

亚兹德转了 50 美元，然后你得查看整个分类账，追踪保罗和亚兹德的信息。也因此，你不只是拥有一个分类账，还拥有一个数据库。

在区块链领域中，这一点更为重要，因为所有这些交易都可能很复杂。例如，在银行领域你想不到的其中一个典型交易是有人开了一个没有钱的账户，但这种情况在区块链领域却时有发生。这个账户是突然出现的。这是一笔交易。

与查看纸质分类账相比，区块链领域行事方式的优点在于其规则非常具体。如果你复制一份分类账，你也复制一份分类账，那么你们会按照相同的规则集来进行复制，这就是你们的操作方式，你们会得到完全相同的结果。此时，你们可以说：“保罗的余额是多少？”而且你们两个即使是在不同的计算机上执行此操作，只要你们运行区块链到同一个点，就绝对会得到相同的答案。话虽如此，其中一些区块链非常庞大，有数亿笔交易。因此，通过互联网获取分类账需要花费大量时间。运行分类账尤其需要大量时间。记得在上一张幻灯片中，我说过实际上，其中一些交易不是简单地将这个数字移到这里，而是运行这个程序。现在，所有程序都是确定性的。程序中没有任何随机数。所以，无论是 2 个人还是 50 个人，只要使用相同的交易配置机器查看相同的区块链，就一定会得到相同的答案。他们的数据库看上去是相同的。这一点非常重要，因为你不会希望有人说“我没有那么多钱，但我要把这笔钱给这个人。”就像在银行一样。但区块链研究人员，由于他们是在银行发明分类账 200 年后才发明区块链分类账，所以能更好地解决这个问题。我有点扯远了，没切换幻灯片。

区块链技术的下一个方面是 — 这是一切的基础，但没人愿意承认这一点 — 不同区块链之间的信任模型截然不同。在银行，你在查看分

类账时会相信银行记录的所有内容都是错误的，而且只有银行人员能写入。而在区块链中，你必须相信写入分类账的人，且在他们写入分类账后，你会疑问真的写入了吗？所以，你可能会提出一项交易说“我将我的一些资金转移给亚兹德”，但如果你没有这些资金，你也相信处理分类账的每个人都会同时说“你没有足够的资金能给亚兹德，所以我将拒绝这笔交易。”

一些区块链中存在着中心化的机构。但你们所听到的“哦，区块链是去中心化的”是一个非常大的词。你在区块链领域听到的任何以D开头的缩写词都表示去中心化。大家会注意到这里我没有给“去中心化”下定义。这是因为去中心化要么没有定义，要么得有无数个。不同的区块链对于其去中心化程度有不同的信任模型。例如，一些区块链允许任何人提供交易，但对于进入数据库设有一定的规则。其他区块链则对于提供交易之人有非常严格的限制。因此，它们在如何将其转换为数据库方面不必那么严格限制。这可能会对区块链的更新速度和实际能源消耗（我们这里说的是电力）产生巨大影响。这些都是计算机 — 区块链添加交易所需要的。最常见的例子就是比特币，它是这一切的起源，它的电力成本非常高，而且输入交易的速度非常慢。以太坊的成本非常低，因此交易可以更快进行。这并不意味着以太坊一定比比特币更好。对某些人来说，尤其是对那些关心子孙后代和气候变化的人来说或许如此，但对于它们存在的原因、它们赖以工作的信任模型，每个人在考虑区块链之初都曾考虑过以下问题：应该如何安排这种信任？谁值得信任？谁不值得信任？要花多长时间才能获得信任？

例如，还是用我刚才给出的两个例子，假设一个交易区块进入比特币世界，它们不信任那些组合数据库的人，也不信任这个区块，直

到又有九个区块出现，并且没人说“除去那个不好的区块”。如果是以太坊，这个列表要短得多。五六个之后它们就会信任。通常，从事以太坊和比特币交易的是同一批人，但他们心中秉持两种不同的信任模型。现在，我们在谈到区块链域名系统时，这些甚至是不同的模型。我们都不希望在某人注册一个域名之后等待一个小时才看到它。抱歉，我不能说出哪些更好或是更差。这取决于你的目的以及你关心什么。

所以以上是一个简短的描述，说明并非所有区块链都是一样的。它们不仅有不同的信任模型，实际上组织方式也不相同。我们所熟悉的一些大型区块链，例如比特币、以太坊，这些被称为第 1 层。这里的第一层并不是像堆栈中的一层，而是表示它们的重要程度。第 2 层区块链相对没那么重要，但通常更加灵活，你会发现许多区块链域名系统的提案实际上都是使用第 2 层区块链。这些第 2 层区块链为了变得更加可信，会将状态信息发送到第 1 层，这样你就可以确保在查看第 2 层区块链时，它与第 1 层区块链是一致的。并且该层中可能有数据。它的发展非常迅速。

之后是侧链，实际上更好的叫法是独立的区块链，它们与其他任何事物都完全无关。你可以运行自己的侧链。我们看到一些区块链域名系统选择运行第 2 层或侧链，同样也是出于不同的信任原因。如果你的区块链是侧链，或者正在运行侧链，那么你只需要信任你自己。在这种情况下，你的所有用户也需要信任你。再次回到银行的例子。我在一家银行开了户，这家银行在座没人听说过，因为它只在我的居住地有 5 家分行。我不该说没人听说过。你们有些人可能也来自我居住的地区。但我也可以在你们许多人都听说过的银行、许多美国人都听说过的银行，甚至是世界各地许多人都听说过的银

行轻松开户。当我对你说“请用这个你从未听说过的东西把钱汇给我”、“请用这个你可能听说过并且可能在某处找到的东西把钱汇给我”以及“请用这个你听说过的东西把钱汇到我的账户上”时，信任模型就会有很大不同。所以，区块链的类型也类似于这样的思路，也就是说不同的信任模型意味着不同的区块链，代表你相信它在未来将发展到什么程度。由于区块链是分类账并且是公开的，其中的数据永远可用。信任模型就是，我们是否真的相信所有可能计入的交易都能计入，以及我们是否相信交易已经成功处理并且没有人作弊？

下面是最后一个问题。很多人都听说过这种说法：“哦，区块链使用了先进的加密技术。”忽视这种说法，好吗？抱歉，我现在可能有点骄傲了。因为我的专业背景是密码学，他们使用的加密技术只能说还行，但实际上也并没那么值得关注。它与我们过去 25 年一直在用的加密技术并没有什么不同。很多区块链推广都是面向那些不明白内情的人。不过，要说他们使用了很差的加密技术，我在此可以肯定地说并非如此。他们使用了极为有效的加密技术。就是还不错，但真的没有亮点。话虽如此，因为有大量资金投入到了区块链生态系统，所以有一群非常优秀的密码学家正在尝试研究新的技术来区分各个区块链。但至今还未实现。他们有一些新颖的想法，但运行起来要么占用大量内存，要么耗费大量时间。未来可能会有所改进，但对于我们目前所说的区块链来说——顺便说一句，如果你不懂密码学也没关系。我完全明白这一点。如果你了解密码学，会后可以来找我聊聊。有一些非常好的密码学方面的书。但如果有人跟你说区块链因为有更好的加密技术而比某某什么更好，那就完全别信了。

那么现在，我们从区块链这个主题脱离出来，开始进入 — 现在你们已经对区块链有了基本的理解，知道了这些域名系统的基础，接下来我们谈谈技术本身。因为每个区块链域名系统都有自己的规则，所以不可能说这个区块链与另一个区块链相比有这个优点或缺点。他们一开始就会制定自己的规则，但可以随时更改，就像你开了一家中餐馆，如果顾客希望，你可以将它改为供应中餐和泰国菜的餐馆。甚至都不需要改名字。或者你可以改名，但仍然提供中餐。这些都可以。区块链域名系统可以随时更改这些规则，而且甚至比全球 DNS 更容易做到这一点，全球 DNS 更改规则的速度非常慢。所有旧规则都适用。我们会提出新的规则。但由于区块链域名系统是自己记录的，我们很难找出特定时刻这个或者这个区块链域名系统的规则是什么。那么，因为它们使用的区块链技术也没有得到很好的记录，当一个域名系统说“我们使用了这个区块链”，而这个区块链你从未听说过，这就像是我对你说“请通过这个你从未听说过的银行把钱汇给我”。这可能没问题，但你可能甚至难以分辨我说的是哪一家银行，因为不幸的是，我的银行在美国不同州有不同的银行。上次我查过，有五个不同的州都有名为 Bay Area Credit Union 的银行。我的意思是，美国很多州都有 Bay 这个银行。这是一个非常常见的名字。区块链也是如此。因为你不知道这个区块链的信任模型是什么，不知道底层的可信度有多高，更不用说你所关心的实际技术了。

所以到目前为止，我所谈到的一切都只是关于你如何信任它。现在，我们来谈谈区块链域名系统实际上是如何处理名称的。再次说明，这就是我们在此参加 ICANN 会议的原因。那么对于全球 DNS，我们考虑的第一件事就是，当我查找名称时会解析什么？对于那些参加过 DNS 101 课程的人来说，当然今天有更多知识，比如“DNS

运作方式”，当你说 `icann.org` 时，所解析的一般是你想要一个主机地址，例如 IPv4 地址或 IPv6 地址，而当你解析区块链名称时，你获得的一般是他们所谓的“钱包地址”。它不是一个钱包，也不是一个地址。它是一个账户标识符，是创建该名称的区块链账户的账户标识符。这很有道理。这才是区块链中最有用的东西。当你向某人说“请给我转钱”时，你不必记住一长串数字，例如公钥的十六进制值之类，只需给出一个名称即可。这与全球 DNS 有很大不同，你可以通过全球 DNS 获取地址、获取文本，所有这些你可能听说过的东西。所以，从一开始，区块链域名系统就与主要使用案例有很大不同。区块链域名系统的主要使用案例是区块链地址。

现在，请注意，我一直在说有很多区块链。的确确有数千个区块链。你在一个区块链上的地址跟你在另一个区块链上的地址是不同的。所以，当你解析一个名称时，你还需要知道是众多地址中的哪一个。例如，假如我有一个以太坊钱包、一个比特币钱包和一些其他什么名称的钱包，哪一个会归到我的名称之下？这正是区块链域名系统仍在努力解决的问题。

许多区块链域名系统宣传的另一个特点是，它们相比全球 DNS 的一大优势在于所有计入该名称的交易都是公开的。它们会永久存储在区块链中。所以如果你想，就能知道是谁创建了这个名称。它是什么时候转移给另外这个人的？它什么时候过期的？它会过期吗？有些区块链域名系统永远不会过期。有些则会。其中的数据发生了怎样的变化？这些信息都是公开的并且很容易找到。虽然并不容易理解，但很容易找到，而这是全球 DNS 中所没有的。我们有机会做到这一点。也就是说，任何注册管理机构、任何注册服务机构都可以制作分类账并将其公开。只不过对它的需求不大。在区块链领域，

由于分类账非常重要，是去中心化的中心 — 抱歉，这个说法有点滑稽 — 分类账对于去中心化非常重要，所以这对它们来说是一个非常突出的特点。

等一下，还有其他特点。区块链域名系统的另一个被认为是巨大优势的特点是，你可以使用原生货币、以太坊、比特币来购买区块链之类。这从某种程度上来说属于固有特点，因为你的账户 ID、你的钱包地址只是你用来支付的工具。这从某种意义上来说就像是，例如，如果你用信用卡购买了普通 gTLD 下的一个二级域名，那么你的信用卡号不仅是公开的，而且还会永久地与你的名字相关联。在座的人可能很难完全理解这一点，但对于区块链社群的人来说，这就是他们想要的。他们想知道有人以这种方式购买了这个名称，并且可能持有它。有些区块链域名系统是一次购买即永久拥有的，因为这就是区块链的运作方式。假设你创建了一个比特币账户。你创建了一个比特币账户，并以某种方式使用普通货币获得了一些比特币，这些比特币就在这个账户内。那么，这个账户就是公钥，而你持有私钥，然后你把私钥弄丢了。这就难办了。你不仅无法访问这个账户，而且这个账户会永久存在并且保有你的最终余额。虽然很难准确衡量，但最近的调研显示，超七成比特币账户已成死账。其中一些账户里的钱比我的账户还多，但即便账户金额不高，有人会说“我跟你说，我再也不关注这个了。”但这个账户依然存在。所以，如果有一个区块链名称与这个账户相关联，那么这个名称将永远指向这个账户。在某些域名系统中，在其他域名系统中，它们就像全球 DNS 一样，你必须每年续订。

好的。这张幻灯片上的最后两点可能会引发很多问题，很多人会提问。许多区块链域名系统 — 如果是域名系统，就必须有一些名称。

你依据什么来命名这些名称？其中一些使用当前未被授权的字符串，即替代顶级域（“alt-tld”）。eth 是常见的，还有 wallet、crypto。许多名称看上去都有关联。全球 DNS 中目前没有这些名称，而如何使用它们仍是一个大问题。如果你有一个名称，比如 .eth 下的名称，而我有 phoffman.eth，因为世界上没多少人叫保罗·霍夫曼或者关注这个。为了找到与这个名称相关的数据，你必须询问知道什么是 eth 的解析器。而只有一个解析器由这个域名系统运行。.wallet 则有两个不同的域名系统，下面有不同的名称。所以如果我有 phoffman.wallet，那么可能就这里有一个，另外一处有一个。事实上，它们可能指向不同的地址，诸如此类。

许多区块链域名系统都使用这些替代顶级域，这引发了许多关于未来会如何的问题。如果它们被分配了会如何？如果没有分配会如何？如果有两个、四个甚至七个同名的区块链域名系统会如何？如何知晓是怎样解析的？太混乱了。大家关注这些问题的部分原因是全球 DNS 非常有条理。我的意思是，我们可以说 35 年来没有任何问题。抱歉。我看到观众席有人年龄比这还要小。但因为我们已经习惯了这种稳定性，所以当区块链域名系统说“我们不需要稳定性，我们想要去中心化”时，就可能会带来很多混乱，不过他们认为这种混乱是有一定价值的。

这里最后一点说的是，有些区块链域名系统实际上想要通过使用全球 DNS 中已有的名称来实现与全球 DNS 的协调、整合或关联。他们采取的方式可能是将实际的全球 DNS 名称链接到他们的区块链。他们可能会先在这里卖掉它们，然后先把它移到这里，或者先到这里，然后先到那里。现在这个市场规模比较小，但也非常有意思，

因为现在我们采用了熟悉的名称，并且在其他地方也有替代解决方案。

现在，我们已经熟知了所有全球域名系统。当你说“请帮我解析这个”时，你就知道如何找到解析器。现在，不同解析器具有不同的功能。有些可以进行 DNSSEC 验证。有些则不能。有些可以故意编织谎言。目前有很多解析器，例如，如果你给它们一个指向某个网站或地址的名称，并且你因为各种政治或性别或其他原因不想听到一些信息，它们就会对你说谎。因为你要求它们编织谎言。这种情形在区块链域名领域中也存在，因为域名就是域名，没有自己的思想，对吧？如果你可以在这里注册，那么也许也可以在那里注册。它们还允许使用全球 DNS 中不存在的名称。如何运作？所有这些都是尚无定论的问题。

我认为我的时间把握得刚刚好。好的，很好。那么接下来我们还有时间给大家提问和发表意见。亚兹德将负责这个部分。麦克风这里有人排队了，你会告诉他们怎么做。不过我想指出的是，如果你问“区块链域名系统如何与某某一起运作？”我得说它们的方式各有不同。我无法对其中任何一个给出明确的答案。即使我现在可以，几个月后它们也会让我的答案变成错的。

另外一点是，各种区块链本身就有很大的差异。信任模型有很大不同。如果你对区块链有疑问：“为什么有人会做这样的东西？”我无法给出原因。一方面，我不是这些社群的活跃分子。另一方面，这些社群会故意做出改变。我说过，我们已经习惯了良好、稳定且变化缓慢的全球 DNS。其中一些变化源自 ICANN。所以，如果你问一个关于比较当今全球 DNS 与 10 年前全球 DNS 的问题 — 你们当中很多人参加 ICANN 会议已经有 10 年或更长的历史了 — 答案可能会

有所不同，但蕴含着演变。在区块链领域和区块链域名领域中，出于各种原因，10 年前的任何事物发展到现在都会有很大不同。我讲完了，亚兹德？

亚兹德·阿坎诺：

谢谢保罗的精彩演讲。我们还有足够的时间提问，差不多 40 分钟，非常好。提醒一下会议室在座的各位，请注意我们的麦克风位于会议室中间位置。如果你不使用英语发言，请说明你的语言。当然，在开始发言之前，请告诉我们你的姓名。对于远程参会者，请使用问答窗格提问。到目前为止，我们在线上有三个问题，但我将先交由会议室人员发言，以防线上有人想继续提问。

保罗·霍夫曼：

有些人坐得离麦克风更近，可以先发言。

萨姆·耶尔马兹

(SAM YILMAZ)：

谢谢保罗。感谢你的演讲。我是萨姆·耶尔马兹，区块链领域的投资者。OCTO-039 和 OCTO-040 力求保持中立并提供信息。但如果你说“ICANN 提出并认可的标准可以这样利用区块链”，你认为，如果按照你的方式，你会如何利用这项新技术来保持更好的透明度并协调交易呢？我希望能听听你对此方面的看法。

保罗·霍夫曼：

感谢你的提问，但我要让你失望了。我是一名 ICANN 员工。我的意见不作数，重要的是社群的意见。当然，社群可能有一些选择会让我有点心塞，但这并不重要。说真的，这些都是社群关于事情将如

何一 这是我编写 OCTO-039 和 OCTO-040 的原因之一，并不是为了我们员工。我的意思是，一部分是为了员工，因为员工也需要了解这些事情的发生，但它们的目的是为了供社群参考以便做出决策。我不知道社群何时会做出这些决策。具体到你所提出的关于如何才能进行整合之类的问题，我们当前有 1300 个签订了合同的 gTLD。这个数字正确吗？1250？就是某个数字。谢谢。大家都是这样，所以没关系。这些可能会选择开始进行一些区块链交互。其中一些可能会彻底转向区块链。有些可能只想稍微接触。有些可能不想这样做。然后我们有下一轮次，现在有很多人都在讨论它。这些将对下一轮次产生怎样的影响？社群对于下一轮次有什么期望？也许下一轮次来得太早，还无法做出你所询问的这种政策决策，也或许下一轮次中的相关人士刚好会遇到一个名称先是 gTLD 然后又转为或转向其中某些技术，因而受到影响。

这里我想实话实说。这是一个观点。嗯，这只是一个观点，一种预测。我的预测能力很差。我过去曾做出过很多错误的预测，但现在我的预测是，真正将引领政策的是，你会看到一些未与 ICANN 签订合同的 ccTLD 发挥一些作用，并且这些 ccTLD 会带来重要的研究成果。我不想这么说，但一半的研究会显示情况有多糟糕，而一半的研究可能会显示情况有多好。我在编写文件时，因为得尽量保持中立，所以不能直接写下自己的意见。基本上，我是想让双方都同等愤怒。我想我们会从 ccTLD 社群中看到一些相关信息。再说一下，请不要就此类事情询问员工的意见。我个人有意见。我不是说我没有意见，但这是个人意见。真正将推动 ICANN 这一方面的是社群的意见，各种社群意见。

亚兹德·阿坎诺：

谢谢保罗。接下来是来自会议室的第二个问题。奥斯卡 (Oscar)，有请。

奥斯卡·朱迪斯

(OSCAR GIUDICE)：

我是奥斯卡·朱迪斯，来自乌拉圭。我用西班牙语说。谢谢保罗的演讲。这次演讲非常有启发性。如果我有一个系统与加密系统 A 和 B 协同工作，我有两个名称，也就是在两个系统中注册了相同的名称，并且我在全球 DNS 中也可能有相同的名称。我们是否需要修改所有的解析器？我的意思是，我们是否需要从头开始？

保罗·霍夫曼：

听得有点迷糊了。谢谢。很抱歉，我不会说你的语言。我是美国人当中只会说英语的那一类，抱歉。问得很好。我们不需要做任何事。我们得到的建议是尽可能广泛地考虑，但我们不必做任何事。如果有人向我们提出了替代域名系统，那就应该由他们来说明该系统将如何改进全球 DNS。他们需要说明该系统是应该继续与全球 DNS 分离，还是应该整合。ICANN 和大多数互联网已经知道它在做什么，然后新的想法出现了。你说你这里有一个解析器，解析器 A、解析器 B。这是你的选择，我们可能会找到一种方法让一切协同工作，也可能不会。这是一个很好的例子，你说你在解析器 A 上有一个名称，在解析器 B 上也有一个名称。我们甚至不知道 A 和 B 是否正确协同工作，更不用说与全球 DNS 协同工作了。所以我认为，对于你提出的“我们是否必须更新全部”这个问题，答案是否定的。但接下来的问题在于，我们可能确实想要这样做。这些区块链域名系统中可能会出现一些有吸引力的东西。现在，我这么说，记

得我说过现在已经有很多区块链域名系统，你说你在 A 和 B 中分别有一个，而某些区块链域名系统会比其他的更好。我所说的更好，是指对于 ICANN 社群更好，对于我们所知的全球 DNS 更好。我们希望将时间都用在更好的系统做出改变上，但这意味着我们必须足够了解它们，知道实际上 A 和 B 哪一个更好，还是说 A 和 B 都很好，而 C、D 和 E 不是我们想要的。这里有很多工作要做。但同样，这取决于区块链域名系统来告诉我们说“这就是我们想要的做事方式。这就是我们自己做事的方式。ICANN 社群是否想要参与？它们是否想参与 ICANN 社群？”现在说这些还为时尚早。谢谢。

亚兹德·阿坎诺：

谢谢。让我们先回答来自会议室的最后一个问题，然后转向在线参会者问答。请讲。

不明男性发言人：

谢谢。谢谢你的发言。我不得不承认我还没有阅读过 OCTO-039 和 OCTO-40，所以如果你已经解决了我将要提出的问题，我深表歉意。我的名字是[听不清]。我是安全社群，特别是执法社群的代表。我说英语。是的。希望如此。基本上，我的工作职责之一就是考虑未来的风险，安全风险。当然，说到技术，对于普通人来说这有点复杂。我也想知道。因为即使是我们现有的系统，在找出注册背后之人时也会存在一些问题。所以我很好奇，从客观角度看，你认为这项技术在这方面是否存在一些风险？还是说现阶段还很难说？谢谢。

保罗·霍夫曼：

是的。下一个问题。噢，抱歉。感谢你的提问，但我将稍微改变一下你的问题。我认为区块链域名系统是否会带来与我们已面临的不同风险？答案绝对是肯定的，因为它们具有去中心化的特性，在这种情况下，去中心化意味着没有人承担责任。你可以很轻易地建立区块链域名系统。你可以让人们免费注册。也就是说，至少在以太坊中，你可以订立一个合约，说“我是一个区块链域名系统。如需注册名称，你必须自行支付相关费用。”我将在这里运行一个解析器，或者任何人都可以运行一个解析器，然后直接离开。订立区块链合约不需要任何人做主动的工作。所以，如果有人这样做了，比如建立了一个合法的区块链域名系统，他们的风险投资家就会抛弃他们。他们偏离了跑道，这是我们英语中用来描述风险投资项目失败的术语，但合约仍然有效。所以，域名系统的风险肯定要高得多，即使他们最初有意通过一些好的方法来防止恶意名称、黄色名称等等，他们也可能离开，而他们的合约未来仍然会继续下去。所以这确实会带来更大的风险。

另外，当你每次尝试整合任何类型的系统，当然是两个域名系统，都会有差异。不可能有两个完全相同的事物。你可以努力缩小它们的差别，但实际上不可能让它们完全相同。这种差异即使很小，也会造成更大的风险，在我看来，这种差异将是巨大的，因为全球 DNS 有着 30 年的规范。而区块链域名系统只有三年。尽管全球域名系统，特别是 ccTLD 中的所有营利动机都通过我们的注册管理机构和注册服务机构得以平衡，但实际上并不存在同等的注册管理机构和注册服务机构。所以我们非常熟悉这些你们认为过高的风险。没关系。再加上我们不了解的风险，我们不了解风险这一事实本身就是一种新的风险。所以是的，它的风险确实高得多。这并不意味着我们在做这件事的时候一切都会很糟糕，只是我们无法预知情况。

同样，这也回到了之前的问题：我认为我们应该如何进行整合？我的个人的意见是尽可能简单地做这件事。你们是一个大的社群。你们已经考虑过这些问题一段时间，所以你们比任何个人都更有能力进行风险分析。

亚兹德·阿坎诺：

谢谢保罗。现在我们来回答在线问题。弗德·巴杰瓦 (Fouad Bajwa) 提出了几个问题。抱歉。那我们就从第一个问题开始。

“特别感谢保罗整理这些文件。我们的确缺少关于这个主题的具体文件，这些文件很有帮助。保罗是否考虑过提议成立一个有关区块链域名系统技术的社群工作组？”

保罗·霍夫曼：

感谢你的提问。不会。我说过，整理这些内容并不是我们员工的事。这件事其实应该由社群来做。我完全相信社群中会有成员希望成立这样一个工作组，我也完全相信在座参会人员中有四分之三在听完我的演讲后会迫不及待逃离这样的工作组。因为主题是不固定的，很难成立一个工作组来及时解决一些问题之类的。如果社群想要这样做，那很好。告诉员工或通过董事会，都可以。但是不，我们员工目前没有打算成立类似的工作组。

亚兹德·阿坎诺：

好的。谢谢保罗。下一个问题还是来自弗德 (Fouad)。“你们是如何处理替代 TLD 名称的？如果它们不是通过 IANA 进行管理，那么它们在 DNS 当中是如何被识别的？”

保罗·霍夫曼：

很好的问题。它们不会被识别。因为它们不由 IANA 管理，所以不会被识别。因为我们所有人都使用普通解析器，所以我们看不到它们。每一个替代域名系统都有自己的一组解析器，它本身就有具备解析器的能力。其中一些已经就解析器达成一致，所以两个不同的替代域名系统可能使用同一个解析器，这样提问的人就可以从中得到答案。其中遍布着解决方案。我说过，我们已经习惯了全球 DNS。我们知道如何分发解决方案。我们知道如何分发域名服务器的权限。但除此之外的其他内容根本不会出现在 DNS 中。所以，如果你向全球 DNS 解析器询问这些问题，是得不到答复的。话虽如此，一些全球 DNS 解析器也开始对某些域名系统做出回应。所以，事实上，当你向全球 DNS 解析器发送查询某个替代域名的请求时，可能也会得到答案。但你得到的是什么样的答案呢？当你向全球 DNS 发出查询请求时，可能希望返回的是一个 IPv4 或 IPv6 地址。而你得到的是一个账户名称、一个钱包地址。跟你想要的毫无关系。所以要平衡所有这些很难很难。即使我们在 ICANN 社群、全球 DNS 以及一些替代域名系统之间达成协议，也很难得到解决方案。我们知道如何在全球 DNS 中解决问题。相关操作的标准来自 IETF。每个人都遵循这些标准。但他们还没有制定出这方面的标准。

亚兹德·阿坎诺：

谢谢保罗。

保罗·霍夫曼：

又有人要用麦克风提问了。按你的安排来吧。

亚兹德·阿坎诺：

好的。我们再回答一个线上问题，然后回到现场提问。那么保罗，下一个问题是：“在基于区块链的域名系统以及与传统 DNS 系统的整合方面，ICANN 持何种态度？ICANN 组织和社群内部是否有任何举措或进行了相关讨论来解决基于区块链的域名与现有 TLD 的兼容性或监管问题？”跟上一个问题有点类似。

保罗·霍夫曼：

向员工询问政策问题并不是好主意，而且你最不想问的就是技术人员，对吧？我既不属于政策团队，也不属于法律团队。不过话虽如此，我可以比较放心地说，ICANN 目前没有相关政策。好的。没有法律团队的人发表意见，所以我说对了。我们会有政策吗？会制定相关政策吗？我不确定。一个可能的答案是，“当然会，社群将会开展这方面的工作。”

另一个可能的答案是，“天哪，不，这太难了。我们其他事情已经够忙了。”还有可能答案是“何必呢？”区块链域名系统已经有了自己的生态系统。它们正为自己的领域服务。全球 DNS 正为我们的领域服务，它变得更大、更稳定。但我们的答案可能是我们不会费心去做这件事，因为现在这样就很好了。重申一下，ICANN 没有任何政策会批判任何域名系统的存在，无论它是基于区块链还是别的什么。我们有一份名为 ICP-3 的旧文件。我没说错吧？还是 IPC-3？ICP？谢谢。谢谢。新的一周还有点犯迷糊。是的，没错。这份文件是在 21 世纪初，应该是 2002 年左右编写的，其中说明了我们没有关于其他域名系统的政策。这是很合理的，因为有百万个域名系统。我们习惯于看起来有层级且包含人类姓名之类的域名系统。实际上邮政编码也是一种域名系统。它们有时取决于你所在的国家/地区。它们有的难懂有的易懂，但都属于域名系统，而 ICANN 对邮政

编码没有任何立场。ICANN 对于个人如何给孩子取名没有任何立场。事实上，许多国家/地区对如何给孩子取名都有规定。区块链域名系统就属于我们没有立场或政策的众多事物中的一个。这一点可以改变。社群可以选择改变这一点。你们社群做与不做，根据你们的选择，会让我的工作变得更难或更容易。这里不是要暗示什么。但我们现在没有这样做，而且我认为社群要接受这一点还需要一段时间。因为正如我们今天所看到的，在我们开始讨论事情的本质之前，要经历一个相当陡峭的教育曲线。有时，在这种情况下，有人可能会疲惫不已然后离开。有时，有人可能会说，“你知道吗？全球 DNS 前进的脚步太慢了。他们这里有很好的想法。我们放手来做这件事吧。”但这取决于你们大家。

亚兹德·阿坎诺：

谢谢保罗。那么现在我们回到会议室这边。不过要快速提醒一下远程参会者，在聊天室中提问和发表意见将不予考虑，所以请把问题和意见放到问答窗格中。谢谢。有请。

贝特朗·德拉查贝尔

(BERTRAND DE LA

CHAPELLE)：

你好。我是贝特朗·德拉查贝尔。我是互联网和司法管辖政策网络的执行董事。我想谈两点。首先，非常感谢你召开这次会议、编写这些文件，并提出我认为本社群及一般会员中一部分人所关注的一个问题。不同域名系统之间的兼容性和清晰度是一个反复出现的问

题。你完全正确地将我们所熟悉的、存在了 30 年的、层级分明且条理清晰的系统与缺少章法的系统进行了对比。

保罗·霍夫曼：

让我在这里打断一下。我们说“条理清晰”这个词时的感觉真是太好了。我刚在 IETF 待了一周。除了 DNS 领域的人之外，没有人会说我们所做的“条理清晰”。所以这都是相对的。

贝特朗·德拉查贝尔：

肯定是相对的。然而，新域名系统的环境与你所描述的有所不同。然而，我有点……首先我想表示祝贺，我很高兴开始了这方面的讨论，并且希望能在其他 ICANN 会议上继续进行讨论，但除此之外，对于你所表达的极度后退的立场，我感到有点不安，因为我认为这指向了 ICANN 员工所能发挥的作用、积极作用这个问题。替代域名系统并不是说要在我们有政策和我们没有政策之间做出选择。员工的作用、员工的积极作用就是帮助梳理问题框架。对于这个社群之外的人来说，我们如何用非常简单的术语来解释“我不确定，.xyz 是 DNS，但 .eth 是完全不同的东西”？抱歉，它看起来是一样的，而我们需要非常清晰地表述。

所以有两条轨道。一是 ICANN 能对外为这个社群提供什么？对于外部社群想要或不想要的方式，我们是否有经验可以分享给他们，让他们变得有条理？也许有些区块链域名系统不想采用我们的做法，但有些愿意吸取一些经验教训或解决一些危险，有些则不愿意。但反过来说，我认为至少有必要认真讨论一下潜在的影响，尤其是对用户造成的困惑。我的意思是，我们在新 gTLD 项目中花了大量时间来解决 DNS 中混淆名称的问题，难道我们不会解决其他域名混淆的

风险？我觉得这一点说不通。所以我只是想建议我们不要陷入“不是0就是1”这种怪圈，比如要么只有社群、要么只有员工，或者要么有政策、要么没政策。我们需要共同努力，组织讨论如何梳理这个框架。我个人认为，员工无论是在技术方面还是政策方面都可以做出巨大贡献，比如说“不论立场，我们可以这样梳理问题的框架。我们能在哪些方面提供帮助，以及会受到怎样的影响？”所以我建议不要设立工作组，这并不是合适的方式，而应该有一个结构化的流程，以便在后续 ICANN 活动的每次会议上我们都有一个专门的架构。我们不要再重现 DNS 滥用讨论中没有做到的事情了。

保罗·霍夫曼：

最后这句有点幽默啊。很不错的看法。谢谢。我是首席技术官办公室的员工。中间有“技术”二字，当然它们不是在正中间，而是中间偏左的位置。员工应该在社群的推动下开展工作，甚至是你所说的这些事情。现在，我们不需要太多的推动。所以我编写了这两份文件，主要是因为我听说了社群里的混乱之类。董事会并没有说：“嘿，员工们，你们需要做这件事。”可能政策部门有人与我有类似的感受，他们正如你所说，也会讨论政策方面。

梳理框架非常重要。但在这种情况下梳理框架几乎是不可能的，因为存在很多区块链域名系统之类的事实，情况是不固定的。我希望 OCTO-039 能够帮助梳理社群可能向单个区块链域名系统提出的问题，比如“在这五六个特征中，你排在哪个位置？你将来会有改变吗？”，这样你所希望的那种框架梳理就能实现了。

现在我又要谈谈个人意见了。我认为区块链域名系统并不会很在意这一点。它们想看看自己能做什么，如果需要它们付出太多努力，

它们就不会感兴趣了。如果这个想法是错的，我会很高兴。我认为我们将在区块链域名系统社群中看到的一个差异是，其中一些人会与 ICANN 社群进行更好的、更一致的互动，而其他人会更偏向“这没有用。啊，有一只松鼠。”没关系。他们就是这样做到的。如果你想要政策方面的框架梳理，不要问技术人员。不过，你知道的，政策部门中有很多人都能做到这一点。我不知道哪些社群需要询问他们，但我认为，就像你说的，进行这些讨论是有价值的。

亚兹德·阿坎诺：

谢谢保罗。我必须承认，其中一些问题很难回答，但我们继续吧。欢迎你，彼得 (Peter)，请讲。

彼得：

非常感谢。我是彼得。我想已经解决了我的部分问题。我还是想回到政策方面，在你看来，虽然你说你不能发号施令，告诉社群该做什么，但你认为我们需要进行哪些政策方面的对话？如果你认为我们无法梳理出这个框架，而我们需要开始讨论这一点，那么这会对 ICANN、信任环境和多利益相关方环境产生怎样的影响？我们需要开始讨论哪些方面？

第二个问题是，在谈到信任模型时，你说不同的区块链有不同的信任模型。从你个人的角度来看，你正在考虑哪些信任模型？因为你作为专家在此发言，你告诉我们这些都是旧东西，所有这些区块链技术都没有适当的加密。那么，在这方面我们需要开始讨论哪些问题？我们需要从何处着手？

保罗·霍夫曼：

感谢你提出一些非常难答的问题。我先回答第二个问题：我偏向什么样的信任模型？我从事这方面的工作已经有 30 年了。我想要一个像我 30 年来一直在做的那种信任模型，它应该非常集中、非常可控，中间有一个 IANA，所有一切都顺畅无比。话虽如此，我在 ICANN 诞生之前就开始做这方面的工作了。有了 ICANN 之后，突然之间有一个社群对很多事情做出规定，我在 21 世纪初的第一个反应是，“老天，这会变得更加复杂了。”后来我的反应是，“哦，挺好的，这会变得更加复杂了”，这意味着在信任模型中有更多的声音可以做出选择了。我一开始的信任模型是乔恩·波斯特尔 (Jon Postel)。不久后我的信任模型演变成了一乔恩 (Jon) 去世了，ICANN 来了。事情会变得混乱。我非常担心。但对我来说，ICANN 社群已经证明，他们可以克服混乱，制定出重要的政策程序，尽管这可能要花很长时间。在座的各位可能都会这么认为，所有政策都耗时太长了。但他们制定出了实际的社群政策。

所以，对我来说，这就是我希望在区块链中看到的。一些区块链有规则，但它们并不是热门区块链。话虽如此，区块链域名系统可以选择使用哪个区块链。而且，其中一些正在选择自己的区块链。它们正在制定自己的规则。我更愿意信任会制定我所喜欢的规则的系统，而不是通过“让我们把所有牌扔到空中，看看会发生什么”来随意制定规则的系统。虽然我想要相信，因为有很多人喜欢“让我们把所有牌扔到空中，看看会发生什么”这种做法。那些社群与我们这里的社群不同。

那么回到你的第一个问题，再回到你现在的情况，我们什么时候做这件事？我不是你想要的那个告诉你如何安排时间的人。你可以从今天的演示中看到 — 顺便说一下，本周晚些时候我们还有另一场演

示。那张幻灯片没有放到演示文稿中。抱歉。周三上午有一场 OCTO 每年都会举行的名为“新兴标识符技术”的会议，会上我会再次讲到与此相关的一些内容。参会的还有某区块链域名公司的代表，另外我们也会留出很多时间进行问答。如果你对这个话题感兴趣，我周三肯定会来参加会议。并不是为了再听我演讲，而是再听一听大家的问答内容。但这里我要加一点刺激。周三派代表来的这家区块链域名公司有一个模型，对于那些不知道它的人，可能会很惊喜，它会让你的心情燃起来。这里的政策发展比几乎任何其他组织都要好。嗯，可以说比我加入的任何其他组织都要好。IETF 几乎都达到了这个标准。但是，你也不希望有人站在教室的正前方，跟你说你应该花时间在这上面，或者你们应该花时间在这上面。大家都可以自行选择。我知道你们不喜欢听到这个，因为正如我所说，很多人会逃离，但所有政策决策都是如此。所以，选择你的战斗，选择你的时间。如果你选择步入区块链、域名描述领域，我可以保证，你将得到 ICANN 员工的支持，而不仅仅是我的。

亚兹德·阿坎诺：

谢谢保罗。[布拉德 (Brad)]，我想快速跟你商量一下。你能把你的问题留到茶歇时间再问吗？我很乐意邀请你。我们先看在线问题。好吗？好的。我们还有大概三分钟时间。

第一个问题是“这份报告中有没有提到或分析区块链 DNS 的查询时间和响应时间？如果没有，未来有这样的计划吗？我认为 DNS 查询表现才是我们更关心的。”

保罗·霍夫曼：

这是个技术问题。我的最爱。我要让你失望了。没有。关于这方面的研究很少，部分原因在于这些区块链域名系统中的解析方式。尽管他们说是去中心化的，但仍然是非常集中的域名解析。我从这里给你的数字与从这里给的数字是不同的。我相信这种情况会逐渐改变，并且他们的查询响应时间会大有改进。但我们还没有进行任何衡量。因为到目前为止我所看到的任何衡量结果，我都不相信。这并不是说我不信任研究人员。我是不信任可衡量性。

亚兹德·阿坎诺：

谢谢保罗。又一个难回答的问题。“考虑到当前的全球系统花了很长时间才发展起来并且已经建立了系统，你认为从当前的全球 DNS 系统转向区块链是否合适，即使是一个缓慢的进展？”

保罗·霍夫曼：

谢谢。这是一个很难的问题。但也不难，因为我知道答案。答案是“不”，我不希望看到这样的转变。显然，其他人也同意我的看法。但互联网曾发生过其他技术转变，不是在 DNS 领域，这也是我不想看到的，但最终这些技术转变实际上是有益的。所以耐心是一种美德。所以如果你问到的这种转变真的发生了，我可能并不想看到它，但我应该耐心等待，看看它最终是否会成为一个好的变化。我不会帮忙，但这也并不意味着我会妨碍。

-
- 亚兹德·阿坎诺： 谢谢保罗。在翻译服务的支持下，让我们来回答最后两个问题。
- “即使还处于早期阶段，区块链域名系统的一些创新和组成部分是否可以帮助全球互联网社群或增强 ICANN 监督下的全球 DNS，尽管目前很难想象完整的整合？”我想这个问题是问你的。
- 保罗·霍夫曼： 感谢你的提问，但我不是合适的回答者。这是针对社群的问题。我当然可以看到情况如何，但选择权在于社群。
- 亚兹德·阿坎诺： 谢谢保罗。最后一个问题：“区块链 — 它是跟注册管理机构有关，还是跟 DNS 本身有关？”
- 保罗·霍夫曼： 很好的问题。没时间了。但再次感谢你提出这个很好的技术问题。
- 当你的域名系统与我们在全球 DNS 中所习惯的域名系统有根本上的不同时，就会出现一些疑问，比如注册管理机构是什么？如果不是注册管理机构，那么由谁来做出决定？在哪里可以找到它？各区块链域名系统之间的情况是不同的，并且会继续变化。如果这个社群对区块链域名系统社群说“我们愿意与你们交流，但我们希望你们能表现得更像我们”，而区块链域名系统社群感兴趣，于是就会表现得更像我们，并且会围绕这一点做出技术改变或政策改变。这将是一种双向对话。

亚兹德·阿坎诺:

谢谢保罗。我想就是这些了。提醒一下在场的各位，星期三还有另一场会议，保罗已经提到过了，时间是星期三上午 10:30。大家可以在会议日程表上看到相关信息。感谢大家的参与和精彩提问。提醒一下，演示文稿也可以在 ICANN 会议日程表的本次会议页面上找到。那么，本次会议到这里就结束了。谢谢大家。再见。

[会议记录结束]