采访：?Jason Bailey

受访者：Scott Stornetta 和 Stuart Haber

Scott Stornetta 和 Stuart Haber 在发明区块链时，想到的是类似于 NFT 的东西，而不是数字货币。Jason Bailey（艺术和科技博客 Artnome.com 的创始人）与 Scott Stornetta、Stuart Haber 进行了一次深入交流，探讨了区块链在三十多年诞生之初的愿景以及后续演变。

译者注：Scott Stornetta 和 Stuart Haber 在 1991 年用代码实现了区块链架构，1995 年 1 月投入商业使用并运行至今。

Jason Bailey：我经常向别人介绍你们两个是我的好朋友，是「发明了区块链的人」。然后，我通常会看到一脸难以置信的表情，「不，是中本聪发明了区块链」，即使是那些已经研究比特币和加密货币多年的人也是如此。你们能否让人们更好地理解你们所做的贡献，以及这些贡献如何成为中本聪构建比特币网络的基础？

Stuart Haber：好吧，让我通过回顾大约三十年的历史来讲述这个故事，从我的角度来看，那标志着区块链开始。这一切都发生在 1989 年，当时 Scott Stornetta 和我还是 Bellcore（贝尔通信研究中心）的年轻科学家。

我是一名密码学家，Scott 刚刚加入 Bellcore。他希望找到一种解决方案，确保通过某些程序或算法手段可以证明、保证和维护数字记录的完整性。Scott 强烈怀疑密码学会在其中发挥作用。因此，我们与 Dave Bayer 一起写了几篇论文并创建了一个架构来解决这个问题。

Scott Stornetta：Stuart 和我形成了一种独特的合作风格，特点是阴阳动态和不断的思想交流。我倾向于全神贯注思考此类问题。挑战在于我不了解可以用来解决这个问题的基础数学或密码学。我有一个问题，但不知道如何找到解决方案。这种知识差距一直是我们富有成效的合作背后的驱动力。

SH：对于那些熟悉这些概念的人来说，数字签名和加密哈希函数在 1989 年秋天就已被提出、实现并得到充分理解。这些工具提出了一个相对简单的问题解决方案，需要一个受信任的实体（无论是个人、软件还是硬件）来确保特定领域内记录的完整性。对于许多人来说，这个解决方案被认为是令人满意的。然而，Scott 和我对此并不满意，因为我们寻求的解决方案根本不需要信任任何一方，也不需要信任尽可能少的个人、实体和数学假设。

我们最终开发了一个解决方案，用一个比喻来解释它：「数字指纹」。事实上，全球每个区块链项目都依赖于加密哈希函数、数学算法、具有输入和输出过程，可以有效生成文件的数字指纹。当你对同一个文件多次应用这个过程时，你始终会获得相同的指纹输出。这是一个高效的过程，即使对于大型文件也是如此，尤其是当我们忘记将其关闭并让它一直运行时。

现在，加密哈希函数的另一个重要属性是，当你获取两个不同的文件并计算它们的指纹时，你会得到两个不同的结果。事实上，即使你对文件进行微小更改，例如将 0 更改为 1，这两个不同文件的最终指纹也会明显且不可预测地发生变化。例如，当涉及到财务记录时，即使细微的更改也可能会深刻地影响文件的含义。例如，将最前面的数字由 0 更改为 1 对于一方来说可能比另一方更有利可图。因此，指纹识别的比喻在这里很恰当：两个不同的手指有两个不同的指纹。

指纹的另一个重要属性是我的指纹不会泄露有关我的详细信息。你无法从指纹中辨别出我的身高、发色，甚至是否有不止一根手指。类似地，加密哈希函数中的指纹只是一连串、一系列数字和字母，不会泄露任何有关原始文件的信息。但是，如果你拥有指纹和声称与该指纹匹配的文件，你可以通过再次「获取其指纹」轻松验证其真实性。数字指纹识别的这种能力被称为加密哈希函数，这些概念甚至在当时就已确立。

？

JB：请允许我总结一下，以确保我的理解是正确的。哈希或指纹是一个很好理解的概念。你们团队的目标是证明记录的完整性，并且无法被篡改。这些哈希值或指纹在某种程度上类似于区块链中的区块吗？你们是否找到了将这些指纹连接成区块链的方法？

SS：你说得对。正如 Stuart 提到的，我们意识到哈希值不仅可以更简洁和更有效地表示文件。关键的创新是将它们组合起来（并将每个区块构建为 Merkle 树），然后将这些区块链接在一起，所有这些都使用相同的哈希函数。在 Dave Bayer 的参与下，我们能够以这样的方式链接记录组，即每个参与者及其文档都成为记录证明的一部分的持有者，他们充当早期的节点。这意味着所有记录都是唯一连接并广泛分布的，其中包含中本聪后来创建比特币的许多基本元素。我们不会从中本聪和他的创造中拿走任何东西，但我们将比特币视为建立在早期区块链之上的应用程序。值得赞扬的是，中本聪明确引用了与我们参与的基础工作相关的所有出版物。我们的工作成果在比特币白皮书中被引用了 3 次，比特币白皮书共引用了 8 次外部文献，我们占据了 3/8。

JB：因此，对所有将中本聪视为区块链创始人的加密货币爱好者来说，我们如何帮助他们弥合你们在 80 年代末和 90 年代初的工作与今天的比特币之间的差距？

？SH ：当你向普通观众提及你对区块链做出的贡献时，他们通常会立即将其与比特币或更广泛意义上的加密货币联系起来。

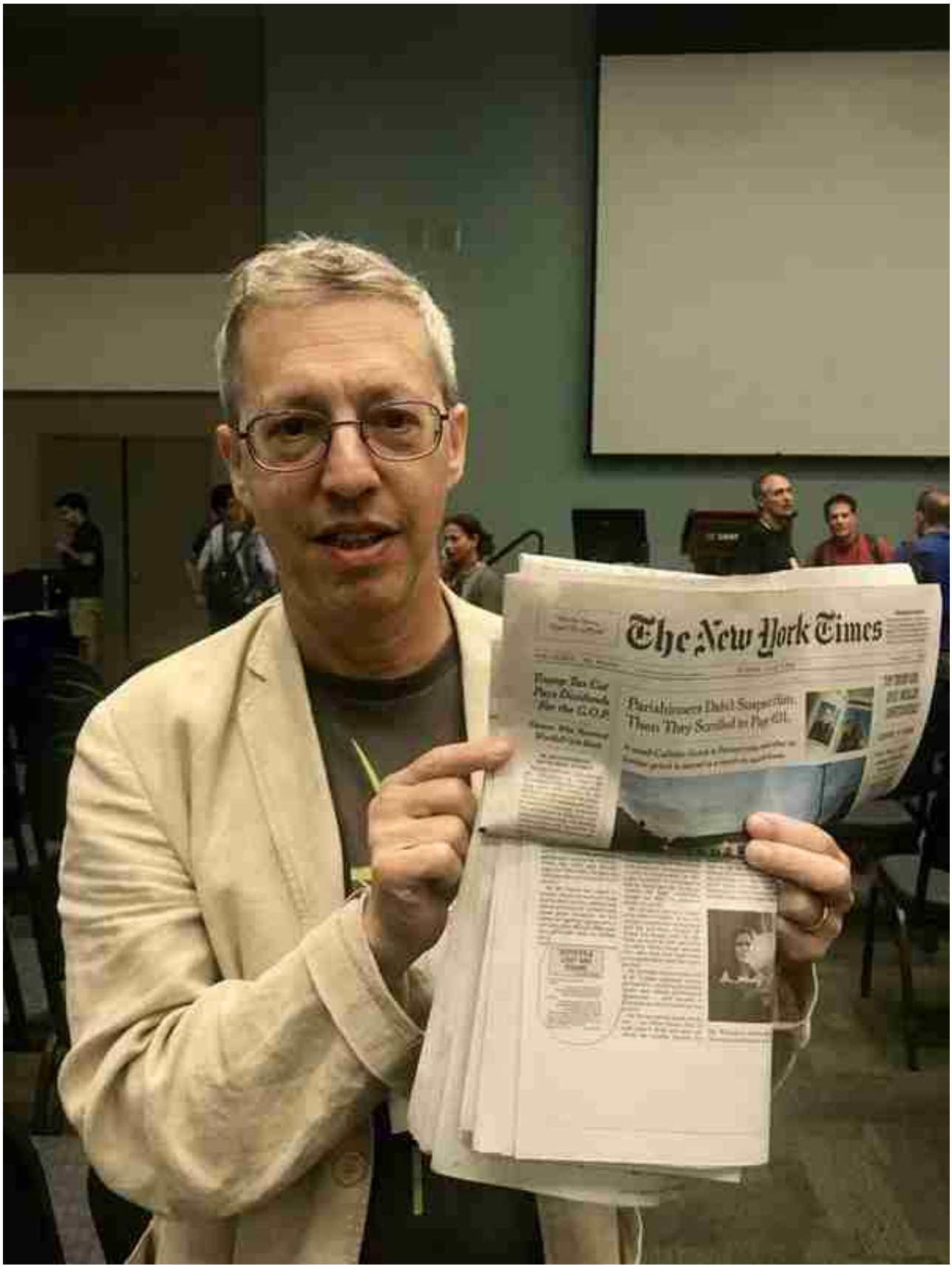
Scott 和我并没有试图发明电子货币。事实上，密码学界早在 80 年代就已经开始致力于创建纯数字货币。我们的关注点更广泛：我们真正关心所有记录（包括电子记录）的完整性。？

SS：这也包括财务记录，但我们的范围扩展到了有史以来创建的每一条重要记录，我们相信所有这些记录都可以在区块链上注册。

SH：既然不可能预测哪些记录会在几年后变得重要，为什么不包括曾经创造的每一个记录呢？

JB：本质上，你们更认同 NFT 的概念，而不是加密货币，对吗？当我们将 NFT 视为验证艺术品、契约、专利和各种应用的工具时，它似乎与你们最初的目标一致。

SH：没错。在讨论数字记录的算法方法时，我们使用了术语「来源（provenance）」。我们关注于各种记录类型。然而，当中本聪的目标是建立一个数字货币系统，需要一种方法来保证系统内金融交易的完整性时，他直接采用了我们的解决方案。比特币交易的数据结构精确地反映了我们的时间戳系统的数据结构，该系统于 1991 年 10 月开始在实验代码中实现，并于 1995 年 1 月投入商业使用。



运行时间最长的区块链始于 1995 年，至今仍然在运行，红色圈出的是时间戳

SS：我想重申 Stuart 提出的观点。从本质上讲，我们对区块链的愿景与中本聪并不相同。中本聪在货币领域引入了一项创新，但他需要一个强大的记录系统。他无缝地集成了这一层，并在其上构建了比特币。

我想强调的是，我们不会忽视中本聪的贡献。相反，他将比特币建立在广泛分布的默克尔树连接成的区块链上，他公开承认这一概念已经被发明。然后，他采用相同的加密哈希函数或数字指纹来直接创建了挖矿机制。

一个有趣的方面在于比特币中序数铭文最近流行起来。如果人们深入研究比特币白皮书的脚注，他们会发现在我们的第三篇联合论文中，我们暗示了利用区块链铭文或序数来制作独特的不可替代记录的概念。这与今天 NFT 的概念异曲同工。

你对加密货币与 NFT 的观察击一针见血。在某种程度上，我们将 NFT 视为我们最初目标的更重要的长期实现。 ??

它表明，一切重要的事物，不仅限于各种卡通灵长类动物姿势，最终可能都需要在区块链上作为 NFT 进行唯一注册。也许我们应该深入研究我们最新的 NFT 系列？？

JB：我很想听到更多信息，尤其是现在我们已经澄清了你们的贡献及其与中本聪后续创造比特币的连续性。令人着迷的是，你们发明的区块链更多针对的是 NFT 而不是加密货币，这可能会让一些人感到惊讶。你是如何决定与艺术家合作，利用插图新闻作为你们的 NFT 的艺术？

SS：早期的主要挑战是达成普遍共识，由于缺乏万维网或类似技术，这项任务变得更加艰巨。我们的解决方案是定期创建区块链的快照（一种指纹）并将其广泛分发以防止操纵。

为了实现这一目标，我们选择每周在《纽约时报》全国版上发布此快照。该版本保存在世界各地的图书馆和档案馆中。想象一下篡改链中单个元素所需的艰巨努力，这就像渗透全球每个图书馆并更改其《纽约时报》的副本一样。

这与我们对 NFT 集合的方法是一致的。我们发布了最初的 12 份 NFT，每份代表我们《纽约时报》连续 12 周出版物中的一份。我们与一位艺术家合作，策划每周的活动，选择一些异想天开的、历史的或值得注意的东西，并用插图来说明。

此外，我们的计划包括在各种链和协议上发布后续集合，以促进区块链社区内更大的合作和团结。我们已经收到了来自不同区块链和艺术家的询问，他们有兴趣保留

一组 12 个连续区块。我们的目的并不是将一切都集中在像以太坊这样广泛使用的区块链上。相反，我们的目标是证明各个社区都可以拥有一段区块链历史。

我们的目标是逐步鼓励更大的互操作性和协作。我们的目标是为包括图形艺术家在内的广大艺术家提供机会来解读《纽约时报》在这几周内发表的 12 个价值观相关的历史。这一举措旨在邀请创意艺术家和区块链创始人加入我们，纪念区块链的历史，而不是简单地促进 NFT 销售。

JB：太有趣了！我认为有些人在听说你们使用《纽约时报》作为区块链时可能会感到困惑，因为他们通常将区块链与计算机技术联系起来，而不是像报纸广告这样的传统媒体。然而，该报纸是确保以防篡改方式广泛分发的一种手段，没有任何个人可以在不渗透到全球每个图书馆的情况下恶意更改它……

SH：你可以通过在《纽约时报》上乱写乱画之类的方式弄乱我们在《纽约时报》上的广告副本。但关键的一点是，如果出现问题，你可以找到自己的记录副本，并根据其他人的记录进行验证。这项计划最初是 Bellcore
的实验代码，但最终发展成为一家名为 Surety
的公司，其主要目标是保护客户的数字记录。

？

JB：你们的性格或政治倾向是否影响了对区块链的发明？

SS：是的。我们不需要任何令人讨厌的中央权威来决定什么是真实的或不真实的。我们曾经幽默地声称，我们的系统本质上是分布式的，即使黑手党正在监督它，它仍然是一个可信的系统。然而，我们很快意识到这个描述并不合适，因为我们位于新泽西州，所以我们停止使用它。

就我个人而言，我非常欣赏区块链固有的去中心化性质。虽然我承认权力集中的存在，特别是在比特币中，但基本前提仍然是：每个参与者共同承担信任责任，所以文件对每个人都是可信的。我发现这个概念非常重要，并相信它可以作为许多具有类似精神的机构的基础。

SH：在现在所谓的区块链的设计中，我们的理念是确保记录的完整性，而不需要信任某个中心机构。

SH：值得注意的是，有些区块链最大主义者声称区块链，尤其是他们自己的区块链，将推翻所有形式的政府和中央实体。就我个人而言，我认为这种说法过于简单化且不切实际。对于区块链的变革潜力，我可能比 Scott 更悲观。在经济力量的影响

下，表面上去中心化的系统（包括比特币和以太坊）变得中心化。？

SS：确实，Stuart 和我就这个话题进行了多次讨论。我们同不同意并不重要，重要的是要认识到区块链技术代表了一个转折点，是熊彼特所描述的一种创造性破坏的形式。它在为了可信性而去中心化的愿望与通过中心化提高运营效率的需求之间引入了健康的紧张关系。这种紧张关系比单纯的去中心化更可取，因为它可以实现更多的平衡和多样性。

JB：在加密货币社区中，人们经常对特定的区块链表现出强烈的极端主义，几乎达到了宗教的程度。然而，很明显你们支持多链的未来，能分享更多你们对此的看法吗？

SH：当然。我们尚未讨论的一个方面是，我们选择在 Kadena
区块链平台上推出由十几个 NFT
组成的原始系列，我们出于各种原因欣赏这个平台的设计。然而，随着我们扩展 NFT 产品，我们不仅鼓励而且要求任何其他 NFT 产品具有互操作性。我们的目标是促进不同区块链网络之间的互操作性，就像我们自己所做的那样。

SS：我认为未来各种区块链网络可以共存，并根据链上 /
链下功能等因素进行区分。这种功能的多样性是生态系统蓬勃发展的积极指标。Stuart 和我以我们自己的方式，旨在促进这些区块链网络之间的互操作性并培养社区意识。因此，如果你代表一个希望发表意见并愿意合作的区块链网络，请与我们联系。也许下一个 NFT 集合（包含 12
周的区块链历史）可以在你的区块链平台上发布。