

区块链中实现鉴证

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.



区块链是支持比特币的分布式总账技术，它无处不在，各类公司也在对其进行测试，用来追踪那些无法集中管理资产的所有权。区块链技术的支持者声称其能够解决一切问题——从如何降低金融服务后台职能相关的高昂成本，到将来如何处理货币和其他交易，它都是灵丹妙药。但批评者却认为区块链是一个棘手的解决方案，指出它缺少成功落地实施的案例，面临与审计、税务以及合规性相关的挑战，并且监管不够细致。关于区块链实用性的真相往往可能介于上述二者之间，但无可争议的是，审计问题正在阻碍对区块链进行更广泛的商业应用。

“审计问题”未必是公认的行业术语，而是本文作者用来描述与积极部署实时区块链案例相关的问题和挑战的方式。使用“审计问题”这个术语是基于

人们看到的阻碍部署的概念验证 (POC) 比想象中更多，因为将内部与外部审计、合规性、风险和法律问题结合起来考虑，最终将提出以下问题：有没有证据可以证明它的运作是安全且有保障的？无数的 POC 现在已经准备好可以上线，但却不会真正上线，因为公司在如何满足控制组织的鉴证需求方面遇到了困难。在大多数情况下，审计和鉴证并不是公司发展阶段考虑的首要因素，当公司开始考虑审计和鉴证时，就会面临如何满足这些控制组织期望的挑战，这并不奇怪。

现在需要明确一下，不是区块链无法审计，而是关于审计的思维方式与交易鉴证的整体概念必须有所不同。但是，在深入研究鉴证之前，必须在高层次上重新解读区块链，来理解是什么带来了挑战，这非常重要。大部分区块链 POC 的设计意图都是获得某些优势，这些优势大致分为 3 个类别：降低成本并提高流程效率，以高于标准信任水平创建生态系统，或使数字货币兑换变得更加容易。可能存在其他略有不同的分类方案，但它们对于此处讨论的目的而言并不重要。

重要的是，无论怎样分类，信任和效率都是任何应用案例的主要价值驱动力。因此，从本质上说，鉴证的一个关键方面源于技术本身，这个方面就是信任。此外，这个结果是通过可以减少流程、中间环节等因素的方法实现的。因此，如果这种技术本身就能产生真正意义上的鉴证，怎样才能最大程度地发挥这一优势，而不是在众多其他管理层次中将它加回来从而“证明”其价值呢？

A. Michael Smith

在 IT 审计、网络安全、隐私保护以及 IT 的监管要求方面有 25 年以上的经验。他服务于美国 PricewaterhouseCooper（普华永道）的 IT 内部审计部门负责为金融服务公司提供服务，并主导过许多金融服务领域的项目。他关注的主要领域是在大型金融服务组织中部署技术审计的战略设计。加入 PwC（普华永道）之前，Smith 是纽约梅隆银行的全球技术审计总监。

为了进一步理解这个想法，区块链技术还创建了不可辩驳的交易记录和不可辩驳的交易完整性。这些通常是审计流程用来鉴证的另外两个特征，意味着在缺少区块链的情况下，交易历史记录完整性和交易本身的有效性来源于大量的流程和控制措施。在金融服务方面，这可能是通过大量的管理活动（例如公司信任、资产服务和全球监管）实现的；但是，在任何行业中可能都有类似对账、确认、身份和访问管理的控制措施。请记住，这仅代表鉴证流程中的第一步，这一点很重要，因为这些流程和控制措施必须通过审计得到“证明”（一般通过对历史交易活动取样的任意时间点的取证分析来执行）。圆满地完成这一步骤后，就创建了鉴证的概念，它能够通过使用数据来执行税务报告、合规性报告、风险分析等工作。

区块链技术通过其自身属性创建了鉴证这个概念，这一事实大大减少了该技术对流程和控制措施的需求。但仍有必要证明，它实际上是按需创建鉴证，并且需要提高技术上的透明度来展示这一点。人们可以从这里开始理解为何需要转变关于审计和鉴证的思维方式：现在可以不采用繁琐的管理流程来证明鉴证的存在，而是可以通过提供透明度来反映鉴证的存在。某些人可能会将其视为挑战，但它其实是将审计和鉴证完全嵌入到技术中并使其成为每笔交易内在属性的机会。

换句话说，要在区块链实例上启用鉴证，必须从技术本身开始。建议首先对区块链引擎的底层加密、密钥管理和安全性进行充分评估。要执行的程序的实际性质和范围将取决于业务使用案例的特征、鉴证相关利益方（例如内部审计、税务、合规）的需求，以及使用的区块链的版本。

这是关于区块链究竟是什么需要强调的一个重点。术语“区块链”指某种形式的应用密码学，它是开源的，并且任何人都可以使用。因此，有许多区块链供应商，每个供应商有独特的性能特征和附加软件（某些甚至有报告功能），这强调了解决的问题是哲学上的改变而不是具体的、一刀切的解决方案的重要性。一旦确认这种技术能按照目标发挥作用，并创建必要的报告来满足利益相关方对透明度的期望，那剩下的事情就比较简单了。

“术语“区块链”指某种形式的应用密码学，它是开源的，并且任何人都可以使用。”

通过持续审查来确保鉴证解决方案的可持续性也是必要的，但这种审查工作的性质、时间安排和范围将再次取决于所用的技术、业务使用案例以及在用于部署实例并不断演变的生态系统。确认并实施交易级别的鉴证后，还有极好的机会来让审计提供附加值。这是因为，为了正确执行操作需要对整体业务流程或影响技术本身的个别使用案例的流程有高于平均水平的理解。既然不必执行人工密集型取证分析，审计人员就可以关注更广泛的流程问题和业务效率问题；他们还可以随着技术的使用和业务案例的发展，进一步了解区块链部署中的变化。这种发展演变将有助于采取更灵活、更有战略意义的方法来进行审计，从而为组织带来更多的价值。

结论

如前所述，任何人都会猜测区块链将终于何处，但从审计的角度看，这是开始提倡不断发展的实时或持续审计概念的绝佳机会。许多因素已经在指导行业朝这个方向发展，其中比较重要的是交易量以及日益增加的对技术的依赖。但是，在这种情况下，技术本身就要求使用这样的方法。技术演变速度越快，就越需要更快开发更高层次的自动化技术（例如机器人流程自动化），审计发展演变的压力也会大幅增加。采用本文所述的思维方式并遵循本文所述的概念，审计职能部门就能做好准备，开始在任何发展阶段以真正战略性的、同类最佳的、更加成熟的方式来处理区块链。



Certified Information
Systems Auditor®
An ISACA® Certification

为 CISA 考试做准备 随时随地

获得 CISA® 在线复习课程

CISA 在线复习课程是自定进度的课程，这意味着您可以按自己的时间安排来查看课程内容；在必要时暂停课程并返回到某些模块；以及返回到课程内容中来复习并刷新您对重要概念的理解。

CISA 在线复习课程包括：

自我评估：这 50 道模拟测试题目参考了 CISA 考试的题目分配，能有效地评测出您需要强化的领域。

入门模块：概括介绍课程以及关于 CISA 工作实践和考试的信息。

领域模块：myLearning 门户网站中的 5 门独立“课程”，每个工作实践领域 1 门课程。

考试样卷：这 75 道模拟测试题目参考了 CISA 考试的题目分配。

有关详细信息，请访问 www.isaca.org/CISAonline-jv2

