央行面临的全新网络安全挑战

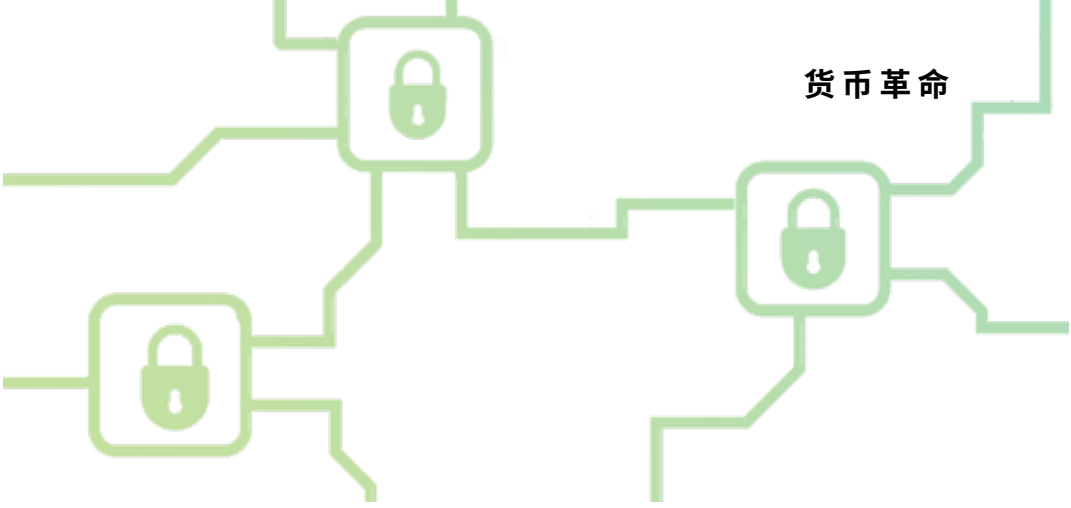
央行数字货币可能带来安全风险，但负责任的设计可将其转化为机遇

朱莉娅·范蒂、乔什·利普斯基和奥勒·莫尔

在中央银行那往往事事谨慎的世界中，央行数字货币的想法正在以闪电般的速度发展。大西洋理事会地缘经济中心的研究表明，目前有105个国家和货币联盟正在探索推出央行数字货币——无论是零售型（向公众发行）还是批发型（主要用于银行间交易）央行数字货币——的可能性。相比之下，2020年这么做的央行估计只有35家。对央行数字货币感兴趣的不仅仅是较小的经济体；二十国集团中有19个国家正在考虑发行央行数字货币，其中大多数国家已经完成了研究阶段。

但随着越来越多的国家启动央行数字货币试点项目，其网络安全和隐私问题也日益被凸显出来。美联储主席杰罗姆·鲍威尔（Jerome Powell）最近将“网络风险”列为他眼中最突出的金融稳定问题，英国上议院最近的一份报告则特别将网络安全和隐私风险列为其不开发央行数字货币的潜在原因。

这些担忧并非没有根据。央行数字货币的漏洞可被用来破坏一国的金融体系。央行数字货币能以前所未有的规模收集敏感的支付和用



技术让央行能够将网络安全和隐私保护嵌入到任何央行数字货币的设计中。

户数据。一旦落入不法分子手中，这些数据就可能被用于监视公民的私人交易，获取有关个人和组织详细的安全敏感信息，甚至被用于盗窃资金。如果在缺乏适当安全规范的情况下贸然实施，央行数字货币可能会使当前金融体系中本已经存在的诸多安全和隐私威胁被大幅放大。

直到最近，网络安全领域和央行界几乎没有公开从事真正了解与央行数字货币有关的特定网络安全和隐私风险的研究工作。很少有人考虑过央行数字货币的设计是否可以降低风险、甚至改善金融体系的网络安全。

我们最近完成了一项新的研究，即大西洋理事会近期题为“缺失的关键——网络安全和央行数字货币的挑战”的报告，其分析了央行数字货币可能给金融体系带来的全新网络安全风险，并说明了政策制定者有足够的选择来安全地推出央行数字货币。央行数字货币在设计上有许多种变体，从中心化的数据库到分布式账本，再到基于代币的系统。在得出有关网络安全和隐私风险的结论之前，需要考虑每一种设计。此外，还需要将这些设计与当前的金融体系——让鲍威尔夜不能寐的正是当前的金融体系——进行比较，以确定新技术是否可以提供更安全的选择。

那么，央行数字货币领域可能出现的一些主要的全新网络安全风险有哪些？更重要的是，怎样才能来减轻这些风险？

集中式的数据收集

各方提出的许多央行数字货币设计变体（尤其是零售型央行数字货币）都涉及集中收集交易数据，这带来了重大的隐私和安全风险。从隐私角度看，此类数据可用于监视公民的支付活动。在一个地方收集如此多的敏感数据也会增加安全风险，因为这会使潜在的入侵者获得更大的回报。

但是，与集中收集数据相关的风险可以通过完全不收集数据或选择一个验证架构（其中，每个环节只能获取某功能所必须的信息）来减轻。后一种方法可采用加密工具（如“零知识证明”，其可在不泄露或破坏信息的前提下验证私人信息）或加密散列技术。例如，汉密尔顿项目（即波士顿联储和麻省理工学院共同研究的美国央行数字货币）设计了一个系统，其将交易验证分成多个阶段，每个阶段都需要访问交易数据的不同部分。

这些加密技术可以进一步扩展，以开发出仅通过加密访问交易细节信息（如发送方、接收方或金额）来验证交易有效性的系统。虽然这些工具听起来理想得令人难以置信，但它们已经在大零币（Zcash）等保护隐私的加密货币中得到了广泛测试，且以密码学领域的重大成果为基础。结果是，技术让央行能够将网络安全和隐私保护嵌入到任何央行数字货币的设计中。

透明度与隐私

隐私保护设计（包括使用专门加密技术的设计）的一个常见问题是降低了监管机构所需的透明度。监管机构通常需要足够的洞察力来

图片来自FUNTAP VIA GETTY IMAGES

在当前各方快速开发和采用央行数字货币之时，开展国际标准制定工作并让银行更多分享知识极其重要。

识别可疑交易，从而能够发现洗钱、恐怖主义融资和其他非法活动。

但这也不是一个非此即彼的决定。可以使用加密技术设计一种央行数字货币，其在特定门槛之下（如10,000美元）时提供类似现金的隐私性，同时又让当局有能力开展充分的监管。这种门槛与美国当前的系统区别不大，后者允许减化10,000美元以下交易的报告要求。现实情况是，在许多方面，新的央行数字货币体系并不需要重新推出一套安全规范，而是可以在已有规范上进行改进。

一些国家已经承诺、甚至推出了底层基础设施基于分布式账本技术的零售型央行数字货币。尼日利亚于2021年10月推出的数字奈拉（eNaira）就是一个很好的例子。其在设计上需要第三方作为交易验证者参与其中。这为第三方（如金融和非金融机构）在央行货币操作中引入了新的角色。至关重要的是，账本的安全取决于第三方验证者的完整性和可用性，而央行可能无法直接控制这些验证者。（虽然也有可能实施一种分布式账本技术，由央行控制所有的验证者中实施，但这在很大程度上违背了使用该技术的初衷。）相关风险可能通过审计要求和严格的违规披露要求等监管机制得到缓解。然而，在一个基于分布式账本的央行数字货币的讲求时效性和紧密互连的系统中，实施这种监管缺乏明确的蓝图。这就是为什么在当前各方快速开发和采用央行数字货币之时，我们急需开展国际标准制定工作，并让银行更多分享知识。

威胁还是机遇？

在过去的18个月中，一些央行过早地认为央行数字货币会带来太多的网络安全和隐私风险。我们则想确定什么是真正的威胁，什么是真正的机会。我们的结论是：政府在设计央行数字货币方面拥有许多选择，这包括尚未完全在当前央行试点中测试的新变体。这些变体在表现、安全和隐私等方面存在着不同的权衡取舍关系。各国应根据自身需要和政策优先项来选择设计方案。根据我们对有关权衡取舍的评估，央行数字货币在本质上并不比现有体系更安全或更危险。虽然负责任的设计必须考虑网络安全问题，但这不应妨碍在一开始考虑是否设计及测试央行数字货币。

在我们的研究中，有一件事是非常清楚的。国际各方在开发各自央行数字货币中存在割裂，这可能导致交互性方面的挑战和跨境网络安全风险。可以理解的是，各国都专注于在国内使用央行数字货币，很少考虑跨境监管、交互性和标准制定等问题。无论美国是否决定推出央行数字货币，作为世界主要储备货币的发行方，美联储都应帮助引领标准制定机构制定全球央行数字货币的规范。国际清算银行、国际货币基金组织和二十国集团在内的国际金融论坛也可发挥出同等重要的作用。

央行数字货币的网络安全和隐私风险是真实存在的。但这些挑战的解决方案掌握在技术专家和政策制定者的手中。在制定一个真正有助于建立更现代、更稳定全球金融体系的解决方案之前，先入为主地认为风险太高是很不幸的。 FD

朱莉娅·范蒂（GIULIA FANTI）是大西洋理事会地缘经济中心的高级研究员兼卡内基梅隆大学电气和计算机工程系的助理教授。
乔什·利普斯基（JOSH LIPSKY）是大西洋理事会地缘经济中心的高级主任，曾是IMF工作人员。
奥勒·莫尔（OLE MOEHR）是大西洋理事会地缘经济中心的研究员。