摘要

支付生态系统要求在一定程度的隐私保护与确保反洗钱和反恐怖融资（AML/CFT）合规之间取得平衡，但目前的经济数字化对此构成了重大挑战。在欧洲央行的协调下，欧洲中央银行系统（ESCB）已经完成了实现数字现金（即“中央银行数字货币”（CBDC））匿名性的概念验证（译者注：概念验证，英文缩写POC，是对某些想法的一个较短而不完整的实现，以证明其可行性，示范其原理，通常被认为是一个有里程碑意义的原型）。

CBDC概念验证是ESCB正在进行的有关CBDC技术研究的一部分，目的是促进对该主题的更广泛讨论。所开展的工作并非针对实际实施，也没有任何决定继续进行CBDC的暗示。欧洲央行将继续分析CBDC等新技术对欧洲公民的好处，为将来需要时可以立即行动做好准备。然而，在央行研究探索数字货币的同时，不应阻止也不应排斥私人市场主导的旨在实现欧元区零售支付快速高效的解决方案。

CBDC概念验证表明，有可能构建一个简化的CBDC支付系统，该系统允许用户对小额交易具有一定程度的隐私权，同时仍确保对大额交易进行强制性AML/CFT审查。

CBDC概念验证基于分布式账本技术，由“欧元链”研究网络（译者注：该网络是由欧洲18家中央银行的支付和技术专家组成的分布式账本技术研究组织）开发（在埃森哲和R3的支持下），具有几个新颖的特征。它为AML/CFT合规程序提供了数字化解决方案，通过该解决方案，除非用户自己选择，否则中央银行或中介机构无法看到用户的身份和交易历史。匿名电子交易额度限制是自动执行的，额外审查则委托给专门的反洗钱机构。这可以通过使用“匿名凭证”来实现，该凭证允许用户在规定的时间段内匿名转账规定数额的CBDC。

尽管没有必要立即在欧元区实施具体的CBDC发行计划，但概念证明将有助于评估（i）CBDC在实践中会如何运行以及（ii）CBDC的具体技术特征将如何影响其对经济的潜在影响。

介绍

在经济持续数字化的背景下，支付生态系统需要找到涉及所有公民的问题的答案：如何在电子支付中允许一定程度的隐私，同时仍确保AML/CFT合规。ESCB“欧元链”研究网络开展的CBDC概念验证（POC）为解决该问题提供了答案。“欧元链”研究网络旨在增进对分布式账本技术（DLT）的共识，并获得有关此类技术的实践经验。

概念验证的主要结果是，在典型的概念验证简化环境中，DLT可用于在执行AML/CFT强制合规时平衡个人的隐私权与公众的利益。它为AML/CFT合规性程序提供了一个数字化解决方案，通过该解决方案，除非用户自己选择，否则中央银行或中介机构无法看到用户的身份和交易历史。

在中央银行对发行CBDC的经济和社会影响进行分析研究的背景下，这一发现尤其重要。确实，是否发行CBDC的问题仍然主要是一个政策问题，但是如果不深入了解CBDC可能具有的各种特定设计功能，就无法回答该问题。本报告旨在促进对CBDC发行中DLT潜在用途的更广泛讨论。需要指出的是，所进行的工作是ESCB对CBDC进行的广泛技术研究的一部分，并不旨在实际实施，也不意味着继续CBDC的任何决定。

支持概念验证的IT架构是基于Corda平台开发的，开发得到了R3和埃森哲的支持。其他概念验证“欧元链”之前就已经完成，该工作未来将继续进行。

该报告第2节描述了CBDC概念验证所遵循的原则，第3节详细描述了概念验证的框架和内容，第4节总结了各种经验教训以及可能的前进方向。

原则

概念验证基于四个主要原则：

首先，假设CBDC具有类似现金的功能。对于小额交易，用户的隐私非常受重视，另外余额是没有报酬的。

其次，运行框架按照双层模型构建。中央银行不直接为CBDC用户提供注册和服务，而是依靠在中央银行有账户的中介机构，通过其在中央银行账户的准备金，向用户提供CBDC。中介机构代表其客户处理交易并向他们提供托管服务。

第三，中央银行是唯一被允许发行和销毁CBDC的机构。

第四，由专门的“反洗钱机构”负责AML/CFT审查。该机构对涉及大额交易的用户身份进行审查，并防止CBDC被转移给被禁用户。

概念验证的描述

概念验证是基于Corda开发的。Corda是一个DLT平台，该平台被设计为用来确保本地存储的两个用户的双边交易信息与系统中存储的总体信息一致（该信息不会与

其他用户共享）概念验证由四个主体（两个中介机构，一个中央银行和一个官方反洗钱机构，在网络中每个主体由运行CorDapp的节点表示），允许用户之间进行交互的Web应用程序，以及允许不同主体之间进行通信和交互的一组应用程序编程接口（API）（请参见图1）组成。

- Corda中的CBDC货币单位和使用模型

CBDC货币单位在Corda分类帐中由“状态”表示。每个状态都包含有关其价值的信息，其过去和现在所有者的详细信息以及其有效性的加密证明-
即证明自发行以来，一直根据中央银行制定的规则进行转移。

Corda中的“状态”遵循未花费的交易输出（UTXO）模型，每个交易都消耗一个状态版本，并在同一分类帐中触发创建一个新版本，该版本可在后续交易中使用（译者注：这是比特币的基本交易模式，每一笔交易都要花费一笔输入，产生一笔输出，所产生的输出，就是“未花费的交易输出”）。在任何给定的时间，只有此前版本按照系统规则使用且最新版本尚未被花费的状态版本，才会被收款人接受。在概念验证中，收款人的中介机构最终有责任确保其客户接收的状态是有效的，并可根据需要向中央银行赎回。

在概念验证中，称为“非验证公证人”的特殊节点允许中介机构通过维护所有当前有效的UTXO的注册表来审查状态的有效性。为了保护用户的隐私，公证人不能访问诸如交易价值，用户地址或状态历史等数据。

控制各方之间状态转移的规则尽量简单，仅保持避免双花和落实反洗钱要求所必需的最低水平。同时，在遵循这些核心规则的基础上，所有主体可以根据自己的选择增加其他规则，也可以将CBDC电子货币转化为“可编程货币”。

- 用户地址

中介机构负责登记注册，并为其每一个客户提供化名身份，这些化名身份用作CBDC支付的网络地址。

- 匿名凭证

为了落实AML/CTF关于反洗钱机构不查看交易数据时对于交易金额的限制，一个全新的概念——“匿名凭证”被创造了出来。反洗钱机构会定期向每个CBDC用户发布这些附加的，有时间限制的匿名凭证。如果用户向AML机构隐瞒交易，则需要花费这些匿名凭证（一份匿名凭证对应一定比率的CBDC转移量）。因此，可以匿名使用的CBDC额度便受到反洗钱机构授权给每个用户的匿名凭证数量的限制。

尽管从技术角度看，匿名凭证是“被花费了”，但它们是免费发行的，并且不能在用户之间转移。它们只是用于限制CBDC匿名交易额度的工具。这意味着无需记录用户已花费的CBDC数量就可以实现对匿名交易额度的控制，从而保护用户的隐私。

- 发行和分销机制

当中介收到客户的CBDC发行请求时，它会检查客户的交易后CBDC余额是否低于其可能设置的任何钱包的上限。如果满足，中介机构则代其客户向中央银行请求CBDC额度。由于限制的每个个人钱包的额度，所以中央银行不会限制CBDC的供应从而导致需求过剩的出现。CBDC的兑换赎回始终以一对一的比率进行，以确保作为货币的另一种形式的CBDC与对应的货币具有相同的价值。央行扣除中介的存款准备金，并通过其节点批准(从而“签署”)发行请求，授权创建新的CBDC单位。新额度随即添加到客户的CBDC账户中，同时扣去该客户同等额度的私人货币金额。

- 转账

CBDC转账无需中央银行的任何参与。付款人发送CBDC转账指令，注明金额，收款人的化名（账户标识符和中介机构标识符）以及是否匿名付款。如果这是收款人第一次从付款人的开户机构收到CBDC，则付款机构要先发起查询请求，以便从收款机构获取收款人地址。随后，中介机构根据是否需要反洗钱机构参与进行接下来的处理程序。这样的转账机制既允许中介机构进行反洗钱筛查，同时也最大程度保障了保密性。

如果付款人具有足够数量的匿名凭证并要求使用，则该笔交易无需获得反洗钱机构的批准便可被收款机构所接受（参见图2）。在这种情况下，付款人的开户机构会从其地址中扣除必要的匿名凭证，并将其附加到CBDC的转帐中，从而向收款人的开户机构证明其可以在无需反洗钱机构审查的情况下验证交易。