姚前：美联储数字货币原型系统简析

文/新浪财经意见领袖专栏作家 姚前

近年来，全球主要经济体的货币当局不断加大对中央银行数字货币（Central Bank Digital Currency，CBDC）的研发力度并取得了诸多阶段性成果。“汉密尔顿计划”（Project Hamilton）是美国波士顿联邦储备银行与麻省理工学院合作开展的 CBDC 创新研究项目（Digital Currency Initiative，DCI）。这项计划已持续开展数年，2022 年 2 月 3 日，美国波士顿联邦储备银行发布题为“为央行数字货币设计的高性能支付处理系统”（A High Performance Payment Processing System Designed for Central Bank Digital Currencies）的技术报告，总结了汉密尔顿计划第一阶段进展。本文拟透过该报告的主要内容，对美联储央行数字货币原型系统进行简要分析。

汉密尔顿计划第一阶段的研究目标

汉密尔顿计划第一阶段的第一个目标是探讨 CBDC 系统的性能，即从技术上研发一种高吞吐量、低延迟和富有弹性的 CBDC 交易处理系统。具体性能目标包括两个方面：一是在 5 秒内完成 99%交易，包括完成交易验证、交易执行以及向用户确认交易，处理速度与美国现有银行卡支付以及银行间即时支付系统的相应指标不相上下；二是根据美国目前现金和银行卡交易量以及预期增长率，该系统每秒至少处理 10 万笔交易，且能随着后期支付量的增长不断扩展。

第二个目标是探讨 CBDC 系统的韧性。为维持公众对 CBDC 的信任，CBDC 系统必须确保服务连续性且资金可用。系统韧性的研究重点在于，当多个数据中心发生故障时，如何保证系统访问不中断，数据不丢失。

第三个目标是探讨 CBDC 的隐私保护。研发团队认为，最安全的隐私保护方法就是从交易伊始就减少数据收集，因此在 CBDC 交易系统中设计了一种尽量减少交易数据留存的方案。

美联储数字货币原型系统设计

币的形式：未花费的交易输出（Unspent Transaction Output，UTXO）

汉密尔顿系统有三类参与者：交易处理器（transaction processor）、发行方（issuer）和用户（user）。交易处理器记录 CBDC，并根据指令验证和执行相关交易。同比特币一样，汉密尔顿计划采用 UTXO 的货币表达式。CBDC 仅能通过发行方的行为而进出系统，发行方铸币（mint）增加

交易处理器中的资金，赎回（redeem）则减少交易处理器中的资金。用户执行资金转移（transfer）操作，以原子方式变更资金所有权，但存储在交易处理器中的资金总额不变，变化的是资金的权属。用户使用其数字钱包的公钥/私钥来处理和签署交易。资金转移交易过程中，使用付款方的未花费资金就是交易输入(input)，生成新的未花费资金就是交易输出(output)——包括收款方和找零给付款方的未花费资金。一项有效交易必须保持平衡：交易输入值之和须与输出值之和相等。

未花费资金定义为三元组 utxo：=（v，P，sn)。其中，v 为金额，P 为安全锁锁头（encumbrance predicate，可以理解为持有者公钥)，sn 为序列号（serial number)。发行方的铸币操作会创建新的未花费资金，并将 UTXO 添加到交易处理器存储的 UTXO 集合，而赎回操作则从 UTXO 集合中删除已有的未花费资金，使其不可重复使用。发行方必须为新铸 UTXO 选择唯一序列号。将其设置为均匀随机数或单调递增计数器值（发行方铸造第 i 个 UTXO 时，会将其序列号设置为 i）均可。

分离验证与 UTXO 压缩

在汉密尔顿系统中，交易处理器验证交易的正确性，并通过删除输入和创建输出来执行交易。验证分为交易局部验证（transaction-local validation，无需访问共享状态）和存在性验证（existence validation，需要访问共享状态)。对于这种分离，汉密尔顿系统设计了专用组件——哨兵（sentinel)，专门用于接收用户交易并执行交易局部验证。局部验证内

容包括：核实交易格式正确；确认每个输入都有适用于其花费输出的有效签名；确认交易保持平衡（即输出之和等于输入之和）。如果交易符合标准，哨兵将向负责存在性验证的执行引擎转发交易，否则就仅向用户提示交易错误。

存在性验证主要核验未花费资金是否存在。为了实现隐私保护，汉密尔顿系统将资金作为不透明的 32 字节哈希值存储在未花费资金哈希集合（Unspent funds Hash Set，UHS），h：= H（v，P，sn），而不是存储完整的 utxo：= （v，P，sn），其中 H 是一个哈希函数，汉密尔顿系统使用了 SHA-256 算法。用 UHS 集合替换 UTXO 集合，不仅有助于隐私保护，而且减少了存储要求并提高系统的性能。

为了进行存在性验证，系统需要预先将通过局部验证的交易转换为应用于 UTXO 哈希集合的交易，该过程被称为压缩（compaction）。具体而言，由哨兵计算输入 UTXO 的哈希值，并将输入 UTXO 与输出安全锁和价值一起，导出输出 UTXO 的序列号，从而计算输出 UTXO 的哈希值，然后将这两个哈希列表发送给保存 UHS 的交易处理器，进行存在性检查和执行。

存在性验证与 UHS 互换

假定某交易已通过交易局部验证并进行了压缩转换，交易处理器将按如下方式更新 UHS 集合：检查 UHS 集合是否存在所有交易的输入 UTXO，如果有输入 UTXO 缺失，那么中止进一步处理，否则，处理继续进行；交易处理器从 UHS 集合中删除该交易的输入 UTXO 对应的 UHS，并将新创

建的与输出 UTXO 对应的 UHS 添加到 UHS 集合中。上述一删一增的操作被称为互换（swap）。

高性能架构

为实现高吞吐量、低延迟以及高容错性的交易处理，汉密尔顿计划设计了两种架构。第一种是原子服务器（atomizer）架构，系统利用排序服务器为所有交易创建线性的历史记录。第二种是两阶段提交（two-phase commit，2PC）架构，系统并行执行数笔无冲突交易（即那些不会支付或收到同笔资金的交易），而不创建统一排序的交易记录。

在这两种架构中，UHS 都可实现跨服务器分区，提高吞吐量并不断扩展。执行单笔交易通常涉及多个服务器，每种架构使用不同技术协调一笔交易在多个服务器中的一致应用。中心化的原子服务器架构使用 Raft 协议对所有来自于哨兵验证过的更新排序，然后将这些更新应用于全系统。2PC 架构则利用分布式共识节点来执行原子交易和可串行化所需的锁定，使用不同资金的交易不会冲突，可以并行执行；一旦某有效交易的资金被确认为未花费，交易就能连续进行，可同时批量处理多笔交易。

汉密尔顿计划第一阶段的实验结果

汉密尔顿计划在第一阶段开发了两套完整的计算源代码或代码库。一个是中心化原子服务器架构的代码库，每秒能够处理大约 17 万笔交易，其中 99%的交易尾部延迟不到 2 秒，50%的交易尾部延迟为 0.7 秒。由于原

子服务器无法跨多个服务器进行分片，因此尽管可以将原子服务器状态机中的功能简化为只对一小部分交易进行输入排序和去重，但该架构的系统吞吐量仍有限。也就是说，对有效交易进行强排序的设计会限制吞吐量。另一个是 2PC 架构的代码库，每秒能够处理 170 万笔交易，其中 99%的交易可在 1 秒之内完成，50%的交易尾部延迟不到 0.5 秒，远高于设定目标需要达到的每秒 10 万笔交易的基本要求。此外，2PC 架构若添加更多共识节点，还可进一步提高吞吐量，且不会对延迟产生负面影响。

以上代码已经开源，汉密尔顿计划称之为“开源央行数字货币项目（OpenCBDC）”，目的是促进 CBDC 研发合作。

比较分析

与电子现金（E-cash）的比较

1982 年，美国计算机科学家和密码学家大卫·乔姆（David Chaum）发表了一篇题为《用于不可追踪的支付系统的盲签名》的论文。论文中提出了一种基于 RSA 算法(RSA algorithm)的新密码协议——盲签名(blind signature)，利用盲签名构建一个具备匿名性、不可追踪性的电子现金系