软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(9):2716−2732 [doi: 10.13328/j.cnki.jos.005595]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

中央银行数字货币原型系统实验研究*

姚 前

(中国人民银行 数字货币研究所,北京 100088)

通信作者: 姚前, E-mail: yaoqian@pbc.gov.cn

摘 要: 数字货币的出现被视为货币形态的又一次重大革命,有望成为数字经济时代的主流通货和重要金融基础设施.中央银行推动发行央行数字货币(central bank digital currency,简称 CBDC)势在必行.根据中国人民银行法定数字货币原型系统实验,探索了二元模式下法定数字货币发行、转移、回笼闭环流程,设计了 CBDC 的加密字符串表达形式、通过存款准备金等额兑换的发行回笼机制、CBDC 在转移过程中的转换机制以及原型系统的总体架构、系统架构和技术架构,并在局部采用分布式账本技术基础上探讨增强其可用性的改进方法,最后还研究了在保护用户隐私前提下如何对 CBDC 进行数据分析.研究发现,基于分布式账本的共识记账和国密 SM2 运算是影响 CBDC 转移性能的关键操作,并提出优化改进思路.

关键词: 中央银行数字货币;原型系统;分布式账本;SM2 算法

中图法分类号: TP311

中文引用格式: 姚前.中央银行数字货币原型系统实验研究.软件学报,2018,29(9):2716−2732. http://www.jos.org.cn/1000-9825/5595.htm

英文引用格式: Yao Q. Experimental study on prototype system of central bank digital currency. Ruan Jian Xue Bao/Journal of Software, 2018,29(9):2716−2732 (in Chinese). http://www.jos.org.cn/1000-9825/5595.htm

Experimental Study on Prototype System of Central Bank Digital Currency

YAO Qian

(Institute of Digital Money, The People's Bank of China, Beijing 100088, China)

Abstract: The emergence of digital currency is seen as another major revolution in the form of currency and is expected to become the main currency and important financial infrastructure in the era of digital economy. It is imperative for central banks to promote the issuance of central bank digital currency (CBDC). Based on initial achievements of research on digital fiat currency (DFC) conducted by the People's Bank of China, this paper explores a closed loop which encompasses DFC issuance, transfer and return in the "central bank-commercial banks" binary model. Moreover, the paper designs the encrypted character string of CBDC, the issuance/return mechanism based on a 1:1 exchange ratio between deposit reserve and DFC, and the conversion mechanism of CBDC during its transfer. The paper goes on to explore the overall architecture, system architecture and technical architecture of the prototype and discusses possible ways to improve the usability of distributed ledger technology (DLT) based on partial application of DLT. Finally, this paper explores data analysis of CBDC under the prerequisite of consumer privacy protection, and concludes that consensus of distributed ledger and SM2 algorithm are key factors influencing the performance of CBDC transfer. Some suggestions for further improvement are also offered.

Key words: CBDC; prototype system; distributed ledger; SM2 algorithm

纵观人类货币发展史,货币从来都是伴随着技术进步和经济活动发展而演化的.数字货币的出现被视为货

* 基金项目: 国家重点研发计划(2016YFB0800600)
Foundation item: National Key R&D Program of China (2016YFB0800600)
收稿时间: 2018-01-08; 修改时间: 2018-03-05; 采用时间: 2018-05-01; jos 在线出版时间: 2018-06-07
CNKI 网络优先出版: 2018-06-07 14:53:45, http://kns.cnki.net/kcms/detail/11.2560.TP.20180607.1453.006.html

币形态的又一次重大革命,有望成为数字经济时代的主流通货和重要金融基础设施,因此,其发展备受学术界、产业界和央行关注[1].

从历史视角考察,作为上一代货币的纸币信息技术含量低、安全性低且使用成本高,被新技术、新产品取代是大势所趋.特别是随着互联网的发展,全球范围内支付结算方式发生了巨大的变化,各种电子货币、虚拟货币、数字货币产品及其支付结算服务的创新实验层出不穷[1].

全球央行一直在关注货币数字化演进状况.早在 1996 年,10 国集团(G10)的中央银行专门在国际清算银行(bank for Int'l settlements,简称 BIS)开会讨论电子货币对支付体系和货币政策的潜在影响以及央行的应对策略,并委托 BIS 密切关注电子货币在全球的应用情况.自此以后,BIS 定期发布对于电子货币发展情况的调研报告.近年来,主要经济体央行加快了应对策略的研究和评估进程.欧洲央行 2015 年详细评估了最近兴起的虚拟货币产品对货币政策与价格水平稳定性的冲击;美联储提出了重构更快、更实时支付体系的行动计划;英国央行最近在各个层面提出将数字货币冲击以及法定数字货币发行纳入其研究日程[1];加拿大央行、香港金管局、新加坡金管局等纷纷开展基于区块链技术的数字货币实验.英国央行的 RSCoin 只是一个概念原型系统[3,9];加拿大央行 Jasper 项目的 CAD-Coin 和新加坡金管局的 Ubin 项目,主要验证利用区块链技术进行银行间支付[4,5],其研究重点是区块链技术应用而非中央银行数字货币(central bank digital currency,简称 CBDC)本身,缺乏对 CBDC 表达的设计,也缺乏整个发行流通机制的研究.因此,从全球范围内,尚未有中央银行对 CBDC 进行体系化的验证研究.

数字货币出现的动力机制是供给侧和需求侧共同使能的结果.从技术创新供给的角度看,全球金融基础设施的电子化和网络化程度不断提高,为数字货币创新提供了高效完善的基础设施接口;信息通信技术的长期进步趋势使支付服务的成本更低、安全性更高,同时更加方便地实现互联和集成;以分布式账本为基础的加密货币技术增强了数字货币的扩散可行性.分布式账本技术(distributed ledger technologies,简称 DLT)目前缺乏标准化的定义,一般可以理解 DLT 是包括区块链技术在内、以构建可信分布式账本为目标的技术方案.按欧洲央行分布式账本技术报告[6]对 DLT 的描述是:允许客户在共享数据库或账本中修改数据,而不依赖中心化系统.按国际清算银行的分布式账本技术在支付、清算和结算分析框架报告[7]中描述:包括区块链在内的 DLT,是利用成熟或最新的技术构建由一个或多个实体管理的一组同步账本.从货币需求来看,电子商务、互联网+为代表的新经济发展壮大,使得货币用户需要更安全、更高效、低成本、更快清算结算的数字化支付方式与金融服务模式.

从中央银行的角度来看,目前,私人部门发行的数字货币方案本身具有的匿名性、低成本、跨区域、去中心化、高扩散率以及高波动性的特征,使得中央银行必须严肃考虑其对支付体系、经济运行以及金融稳定性带来的冲击与影响,更主动地提出应对方案,优化升级法定货币的发行流通体系.于是,法定数字货币方案的提出就顺理成章了.

中国人民银行一直高度关注数字货币发展,并积极开展相关研究工作.从 2014 年起就组织专家成立了专门的研究团队,并于 2015 年初进一步充实力量,对数字货币发行和运行框架、数字货币关键技术、数字货币发行流通环境、数字货币面临的法律问题、数字货币对经济金融体系的影响、法定数字货币与私人准数字货币的关系、国外数字货币的发行经验等进行了深入研究,已取得阶段性成果.这些研究成果为发行中央银行数字货币提供了坚实的理论依据和系统化的顶层设计,使得后续进行原型系统开发和实验成为可能.

我国法定数字货币的初步界定是:由央行主导,在保持实物现金发行的同时发行以加密算法为基础的数字货币,即 M0 的一部分由数字货币构成.目标是构建一个兼具安全性与灵活性的简明、高效、符合国情的数字货币发行流通体系.所以设计过程中尤其注重技术手段、机制设计和法律法规这 3 个层次的协调统一:在技术路线上,充分吸收和改造现有信息技术,确保数字货币信息基础设施的安全性与效率性.在机制设计上,要在现行人民币发行流通机制的基础上保持机制上的灵活性和可拓展性,探索符合数字货币规律的发行流通机制与政策工具体系.在法律法规上,要实行均一化管理原则,遵循与传统人民币一体化管理的思路.

全球范围内,中央银行发行法定数字货币还处在研究探索阶段,国际上也没有成功经验和先例,在法定数字货币系统构建和技术实现等方面还存在诸多难点.中国人民银行在前期研究取得阶段性成果的基础上,最早开

展了原型系统实验,为全球范围内中央银行探索法定数字货币的具体实践,迈开具有重大意义的关键一步.人民银行数字货币研究所率先开展了二元模式下中央银行到商业银行的CBDC全生命周期闭环机制设计和系统实现,构建中央银行和商业银行实际参与的法定数字货币原型系统,包括发行、转移、回笼全过程;集中力量对央行发行法定数字货币的关键问题进行探索实践,并就法定数字货币如何吸收转化分布式账本技术这一前沿领域进行积极尝试,这对于我国加快具有国际领先优势的法定数字货币探索和实践具有重大意义.

本文依据中国人民银行法定数字货币原型系统(简称原型系统)一期建设的成果,描述了中央银行发行法定数字货币的模式和体系,包括关键要素、运行机制、原型系统总体架构、系统架构和技术架构等方面内容.探讨了原型系统中分布式账本技术和签名加密技术的应用和改进,对 CBDC 流转进行数据分析,通过实验研究分析影响 CBDC 转移性能的关键操作,并提出优化改进思路.

1 总体框架

1.1 运行框架

央行数字货币的运行框架可以有两种模式选择:一是由中央银行直接面向公众发行数字货币;二是遵循传统的中央银行-商业银行二元模式.在第 1 种情形下,央行直接面对全社会提供法定数字货币的发行、流通、维护服务;第 2 种仍采用现行纸币发行流通模式,即,由中央银行将数字货币发行至商业银行业务库,商业银行受央行委托向公众提供法定数字货币存取等服务,并与中央银行一起维护数字货币发行、流通体系的正常运行.我们倾向于第 2 种模式,原因很简单:一是更容易在现有货币运行框架下让法定数字货币逐步取代纸币,而不颠覆现有货币发行流通体系;二是可以调动商业银行积极性,共同参与法定数字货币发行流通,适当分散风险,加快服务创新.在二元模式下,中央银行负责数字货币的发行与验证监测,商业银行从中央银行申请到数字货币后,直接面向社会,负责提供数字货币流通服务与应用生态体系构建服务[2].

如图 1 所示,原型系统按二元模式的总体设计原则,将 CBDC 的运行分为 3 层体系:第 1 层参与主体包括中央银行和商业银行,涉及 CBDC 发行、回笼以及在商业银行之间转移,原型系统一期完成从中央银行到商业银行的闭环,通过发行和回笼,CBDC 在中央银行的发行库和商业银行的银行库之间转移,整个社会的 CBDC 总量发生增加或减少的变化,同时机制上要保证中央银行货币发行总量不变;第 2 层是商业银行到个人或企业用户的CBDC存取,CBDC在商业银行库和个人或企业的数字货币钱包中转移;第3层是个人或企业用户之间CBDC流通,CBDC 在个人或企业的数字货币钱包之间转移.

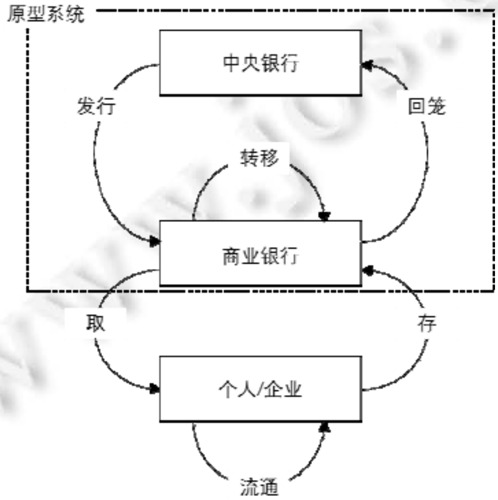

Fig.1 Binary operating system of central bank digital currency

图 1 法定数字货币二元模式运行框架

原型系统一期建设主要针对第1层从中央银行到商业银行的闭环.这一层是整个CBDC发行流通体系的基础,从中央银行角度,覆盖了 CBDC 最核心的 CBDC 表达、发行回笼机制、CBDC 转移机制.而商业银行既作为发行回笼参与者,同时也作为银行间 CBDC 转移的参与者,共同构建 CBDC 产生、转移、回笼的全生命周期运行体系.解决好第 1 层的问题,未来面向个人/企业用户的第 2 和第 3 层的扩展也就有了坚实基础.

1.2 关键要素

央行数字货币体系的核心要素为"一币、两库、三中心"[8].一币是指 CBDC:由央行担保并签名发行的代表具体金额的加密数字串.两库是指中央银行发行库和商业银行的银行库,同时还包括在流通市场上个人或单位用户使用 CBDC 的数字货币钱包.三中心是指认证中心、登记中心和大数据分析中心.认证中心:央行对央行数字货币机构及用户身份信息进行集中管理,它是系统安全的基础组件,也是可控匿名设计的重要环节.登记中心:记录 CBDC 及对应用户身份,完成权属登记;记录流水,完成 CBDC 产生、流通、清点核对及消亡全过程登记.大数据分析中心:反洗钱、支付行为分析、监管调控指标分析等[8].

原型系统要对 CBDC 表达形式进行探索,在此基础上建立中央银行数字货币系统和商业银行的行内系统,并分别实现中央银行发行库和商业银行银行库的功能.由于原型系统一期主要解决中央银行到商业银行这一层的闭环,因此现阶段不涉及数字货币钱包的内容.按循序渐进的原则,原型系统一期以登记中心为重点,实现 CBDC 发行、转移、回笼全过程权属登记,记录 CBDC 交易过程,同时扩展登记中心提供网上确权查询服务.认证中心在原型系统一期主要负责商业银行身份认证和管理.大数据分析中心在原型系统一期暂不涉及.

2 运行机制

2.1 CBDC表达

CBDC在形式上就是一串经过加密的字符串.CBDC表达式本质上是对货币制度主要构成要素及权属的加密处理,是CBDC系统安全运转的基础.理想的CBDC与传统的电子货币并不相同,它以精巧的数学模型为基础,模型中包含了发行方、发行金额、流通要求、时间约束、甚至智能合约等信息.具体来讲,理想的 CBDC 应具备以下特性:不可重复花费性、匿名性、不可伪造性、系统无关性、安全性、可传递性、可追踪性、可分性、可编程性[9].

数字货币简单表达最典型的是 Bitcoin 采用的方式[10],仅表达特定地址的缺省单位下的数字货币数量,这种方式被各种虚拟数字资产所采用,这种表达实质是抽象、概念化的 Token,无法具体表达实际货币应有的属性.从其他国家中央银行数字货币研究来看,英格兰银行提出的 RSCoin[11]也基本采用了这种地址和数量的简单化表达.其主要研究方向是引入分层账本改进区块链效率,而对数字货币表达缺乏深入研究.Bitmint[12]提出了一种加密形态数字货币表达式,但缺乏对法定数字货币模型的支持,而更多关注在加密数字货币表达式中记录数字货币转移交易的过程信息.

原型系统探索了支持可扩展特性的加密形态 CBDC 表达式,其形式化模型可以表达为

$$EXP_{CBDC}=Sign(Crypto(ATTR))$$

$$ATTR\in\{id,value,owner,issuer,ExtSet\}$$

EXP_{CBDC} 代表 CBDC 的表达式,$ATTR$ 表示表达式包含的属性集合,$Crypto$ 代表对属性集合元素进行加密运算,$Sign$ 代表对表达式进行签名运算.该属性集合包括最基本的用户标识 id、所有者信息 $owner$、发行方信息 $issuer$、可扩展属性集合 $ExtSet$.

原型系统根据 CBDC 的目标,围绕商业银行从发行、转移到回笼的闭环应用出发,充分考虑到稳定性和扩展性的要求,对 CBDC 表达式进行了设计,其一般性的结构如图 2 所示.

从基本构成上,CBDC 应包含最基本的编号、金额、所有者和发行者签名.编号代表了 CBDC 的唯一标识,编号不能重复,可以作为 CBDC 的索引使用.金额代表了 CBDC 的面额,金额可以被拆分,其最小颗粒度到 0.01 元(壹分),最大面额未设定上限.所有者代表 CBDC 的拥有者,发行者签名则代表 CBDC 发行方.CBDC 基本字段相对稳定,同时,通过应用扩展字段和可编程脚本字段将 CBDC 的应用扩展功能和可编程功能纳入其中.应用扩

展字段通过可变长数据表达格式实现多个应用属性扩展存储.同时,在应用属性下一层还可以通过参数字段对应用属性提供进一步可配置能力.可编程脚本通过预留的可变长数据表达格式可以将来扩展.通过可扩展字段结构的设计,能够使得 CBDC 灵活适应未来广泛的应用场景需求[13].

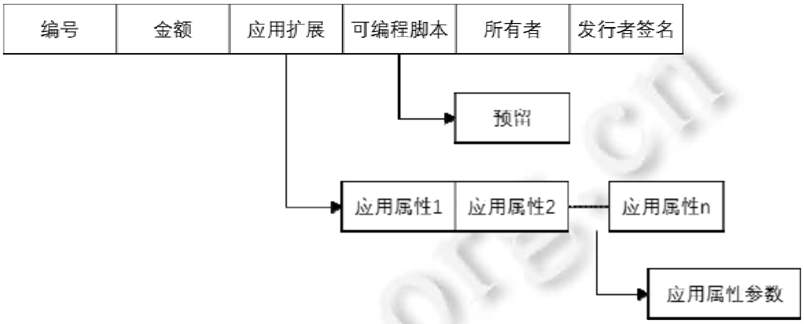

Fig.2 Form of presentation of CBDC

图 2 CBDC 表达式结构

2.2 发行回笼机制

现有基于账户模式的中央银行货币系统,是通过商业银行在中央银行设立存款电子账户实现中央银行货币投放和回笼.而 CBDC 则作为一种新的货币形态,在不改变中央银行货币发行总量的情况下,需要设计一种与现有电子账户货币兑换的机制,探索在现有货币运行框架内 CBDC 发行和回笼的可行机制.

CBDC 发行是指中央银行生产所有者为商业银行 CBDC,并发送至商业银行的过程.CBDC 回笼是指商业银行缴存 CBDC,中央银行将 CBDC 作废的过程.为保证发行和回笼不改变中央银行货币发行总量,原型系统设计了通过商业银行存款准备金与 CBDC 等额兑换的机制.在发行阶段,扣减商业银行存款准备金,等额发行 CBDC.在回笼阶段,作废 CBDC 后,等额增加商业银行存款准备金.因涉及存款准备金变动,原型系统通过对接中央银行会计核算数据集中系统(简称中央银行会计核算系统)来实现.

发行过程如图 3 所示,商业银行行内数字货币系统向中央银行数字货币系统发起请领申请,中央银行数字货币系统首先进行管控审批,该步骤为中央银行实施监管预留扩展功能.之后,向中央银行会计核算系统发起存款准备金扣款指令,中央银行会计核算系统扣减该商业银行存款准备金并等额增加数字货币发行基金.扣款成功后,中央银行数字货币系统生产所有者为该商业银行的 CBDC,并发送至商业银行数字货币系统.最后,商业银行完成银行库入库操作[14].

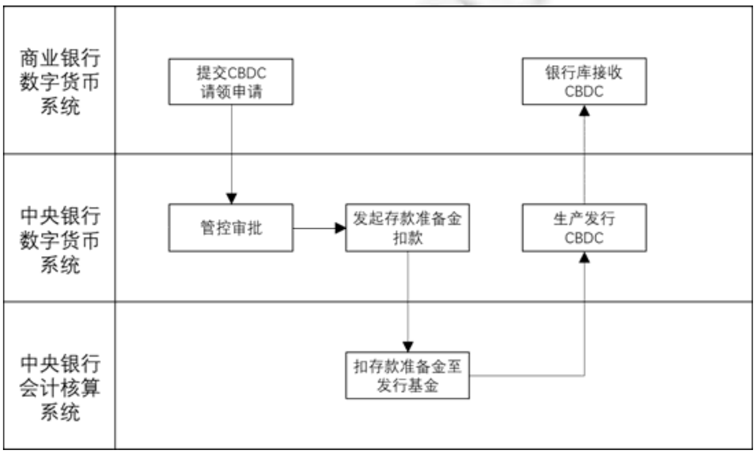

Fig.3 Issuance process of CBDC

图 3 CBDC 发行过程

回笼过程如图 4 所示,商业银行行内数字货币系统向中央银行数字货币系统发起缴存申请,中央银行数字货币系统同样进行管控审批后,先将缴存的 CBDC 作废,然后向中央银行会计核算系统发起存款准备金调增指令,中央银行会计核算系统扣减数字货币发行基金,同时等额增加该商业银行存款准备金.完成后,中央银行数字货币系统通知商业银行回笼成功[15].

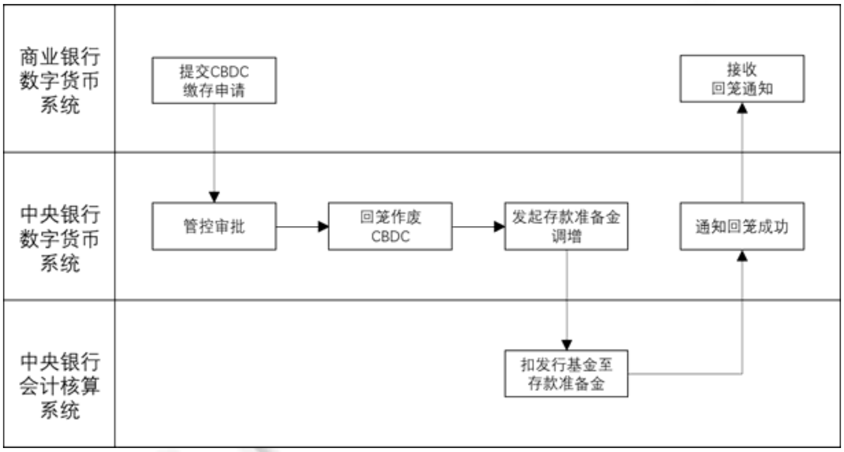

Fig.4 Withdrawal process of CBDC

图 4 CBDC 回笼过程

2.3 转移机制

CBDC 是载有所有者信息的加密字符串,因此,CBDC 的转移必然涉及到加密字符串的转换,分为来源币和去向币:来源币是转移之前的 CBDC;去向币是经过转移将来源币作废之后,新生成的 CBDC.CBDC 的转移可以有以下几种模式:直接转移、合并转移、拆分转移[13],图 5 对这 3 种模式进行示例说明.

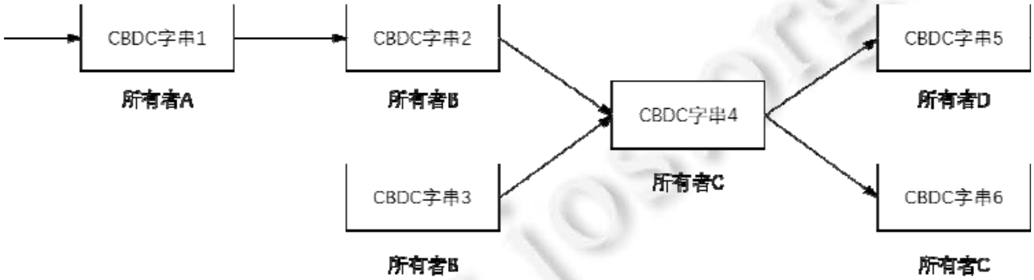

Fig.5 Transfer mechanism of CBDC

图 5 CBDC 转移机制

(1) 直接转移:用户 *A* 将 CBDC 字串 1 转移给用户 *B*.

CBDC 字串转移是指将代表 CBDC 的加密字符串以数据包的形式在发送方和接收方保管 CBDC 的系统之间进行传输.

来源币币所有者为 *A* 的 CBDC 字串 1,在转移发生后生成新的 CBDC 字串 2,后者的所有者标识对应用户 *B*.CBDC 字串 1 和 CBDC 字串 2 的金额相同.

(2) 合并转移:用户 *B* 将两个 CBDC 字串一起转移给用户 *C*.

CBDC 字串 2 和 CBDC 字串 3,在转移发生后生成新的 CBDC 字串 4.CBDC 字串 4 的金额等于两个来源币金额之和,CBDC 字串 4 的所有者标识对应用户 *C*.合并转移的来源币可以是任意多个.

(3) 拆分转移:用户 C 将 CBDC 字串 4 部分金额转移给用户 D.

来源币是所有者为 C 的 CBDC 字串 4,在转移发生后生成新的 CBDC 字串 5,其所有者标识对应用户 D,其金额为转移金额.同时生成新的 CBDC 字串 6,其所有者标识对应用户 C,其金额为转移后的余额.

根据 CBDC 转移机制,原型系统中商业银行之间转移 CBDC,表现为 CBDC 字串通过中央银行数字货币系统进行转换并传递的过程.如图 6 所示,商业银行 A 数字货币系统将待转移的 CBDC 发送至中央银行数字货币系统.首先将来源币作废,然后按转移金额生成所有者为商业银行 B 的去向币,如果转移后还有余额,则还要生成所有者为商业银行 A 的去向币.然后将去向币分别发送给对应的商业银行.

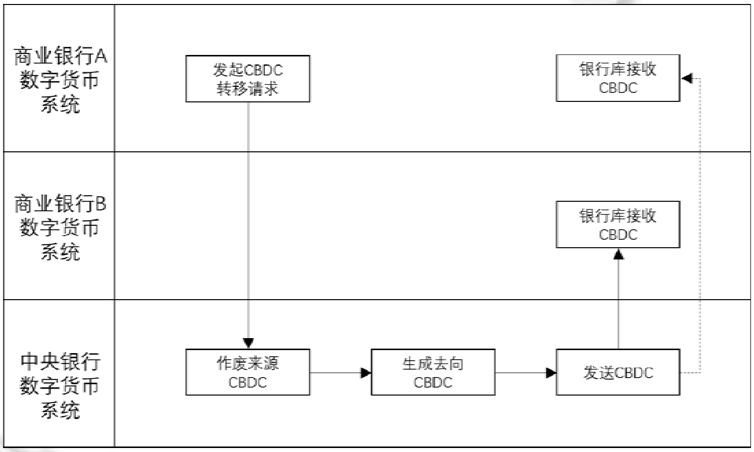

Fig.6 Transfer process of CBDC

图 6 CBDC 转移过程

3 系统架构

原型系统在遵循中央银行-商业银行二元模式的基础上,针对中央银行到商业银行这一层的发行、转移和回笼的闭环运行机制进行整体规划设计.其范围还包括:选取数字票据交易平台作为 CBDC 转移的原型实验场景,并与原型系统进行对接;由中央银行与参与原型实验的商业银行共同组建分布式账本体系,在 CBDC 网上确权查询中探索分布式账本技术的应用.

3.1 总体架构

对原型系统软硬件基础设施、应用功能、业务数据等多个层面进行统一考虑,形成一个支撑功能及技术验证的、符合当前 CBDC 运行框架的原型系统,其总体架构如图 7 所示.

整个体系分为 3 部分:中央银行相关的中央银行数字货币原型系统和中央银行会计核算测试系统、参与原型实验的商业银行行内系统、作为 CBDC 转移实验场景的数字票据交易平台.

中央银行数字货币原型系统包括以下部分.

1. 登记中心:记录 CBDC 的发行情况、CBDC 权属信息,完成 CBDC 发行、转移、回笼全过程登记.其主要功能组件分为发行登记、确权发布、确权查询网站应用、分布式账本服务几个部分.发行登记进行 CBDC 的发行、回笼过程及权属记录;确权发布将发行登记的权属信息进行脱敏后发布到 CBDC 确权分布式账本中;确权查询网站为商业银行提供在线权属查询服务;分布式账本服务保证中央银行与商业银行 CBDC 权属信息的一致;
2. 认证中心:对 CBDC 用户身份信息进行集中管理,是系统安全的基础组件,也是可控匿名设计的重要环节.其主要功能包括认证管理和 CA 管理两部分,在原型系统一期提供机构验证和证书管理功能,未来可基于 IBC(identity-based cryptography,基于标识的密码技术)等技术构建对终端用户的认证支持;

3. 大数据分析中心:包括 KYC(know your customer,充分了解你的客户)、AML(anti money laundering,反洗钱)、支付行为分析、监管调控指标分析等功能,是 CBDC 风险控制及业务管控的基础,原型系统一期大数据分心中心功能暂不实现;
4. CBDC 基础数据集:维护中央银行数字货币系统最完整的数据资源,既包括 CBDC 发行、回笼等业务过程产生的数据,也包括转移过程中产生数据.并采用分布式账本服务进行权属信息登记实验.为 CBDC 发行登记业务、数据分析业务提供数据支撑;
5. 运行管理系统:提供整个中央银行数字货币原型系统运营过程中的配置、管理、监控等功能;
6. 中央银行数字货币系统前置:是商业银行接入中央银行数字货币原型系统入口,提供商业银行核心业务系统与中央银行数字货币原型系统之间的信息转发服务.主要功能包括报文的接收、转发、签名、验签等功能;
7. 发行登记子系统分节点:是数字票据交易所与中央银行数字货币原型系统对接的入口,主要功能包括 CBDC 交易确认、与数字票据系统分布式账本的央行节点进行通信等操作;
8. 数字票据分布式账本央行节点:是中央银行数字货币原型系统在数字票据分布式账本的前置节点,发布 CBDC 智能合约,实现数字票据交易 DVP(delivery versus payment,券款对付).

中央银行数字货币原型系统通过与中央银行会计核算测试系统对接,实现 CBDC 发行和回笼机制.商业银行与数字票据交易所是参与原型系统实验的重要参与方,其中,商业银行需对核心系统进行改造,建立其银行库和保存 CBDC,并与中央银行共同组建分布式账本登记 CBDC 权属信息.数字票据交易所的数字票据分布式账本中加入央行节点,从而实现 CBDC 与数字票据基于分布式账本的 DVP 交易.

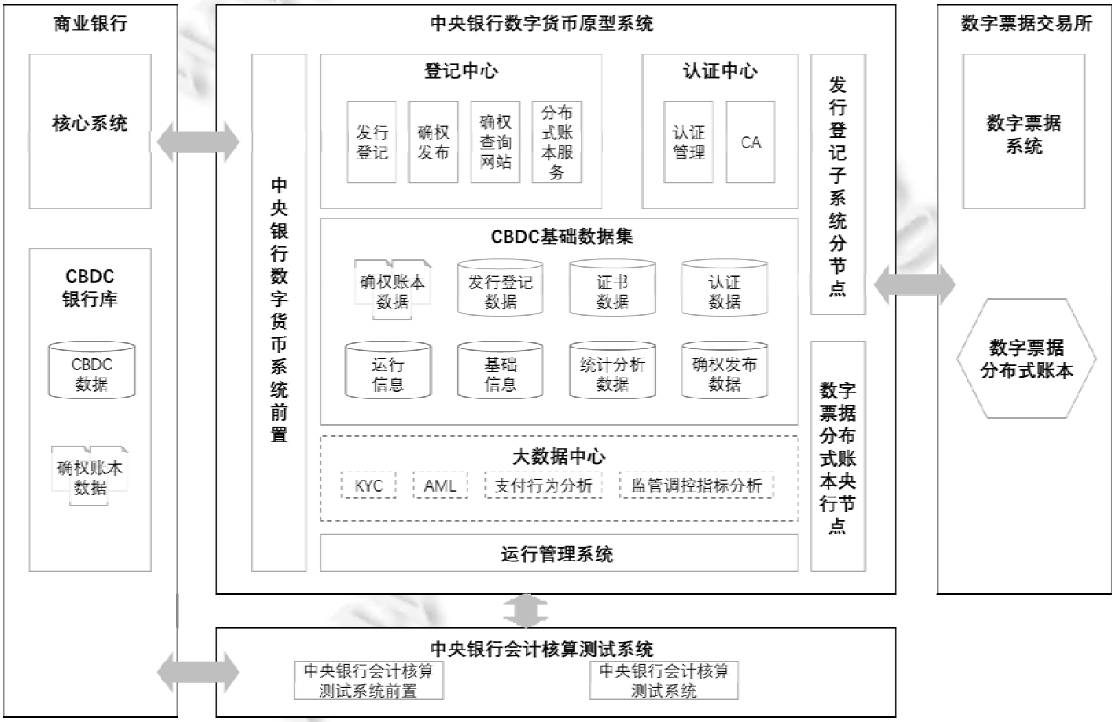

Fig.7 General structure of prototype system

图 7 原型系统总体架构

3.2 系统架构

基于原型系统总体架构,对各方系统的接口和运行流程进行总体设计,并对各系统功能组件进行分配,建立

满足原型系统实验要求的系统架构,如图 8 所示.

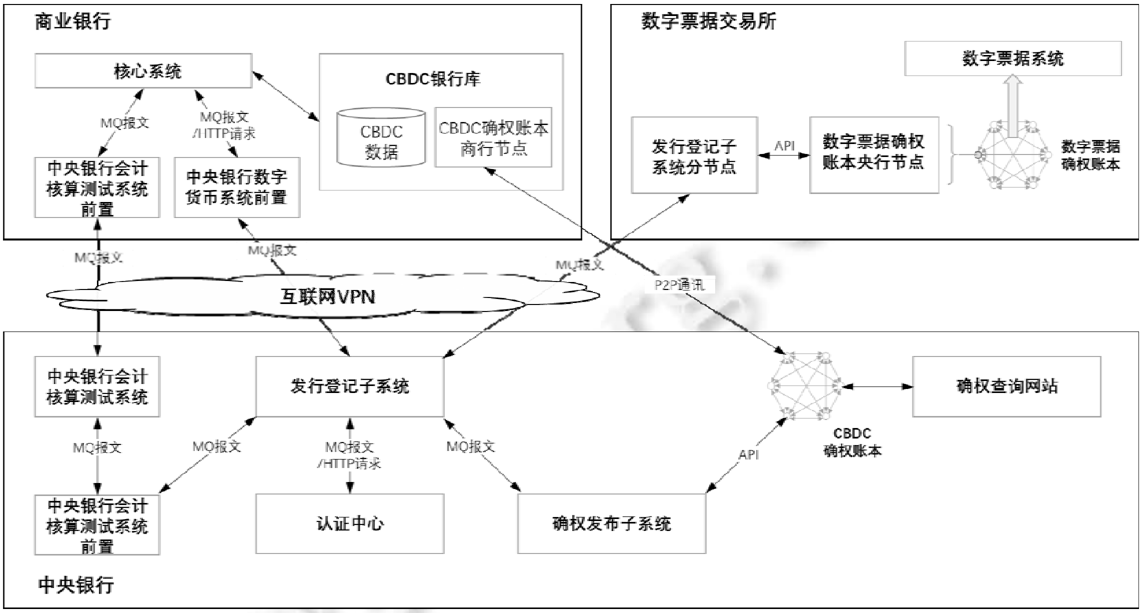

Fig.8 Structure of prototype system of CBDC

图 8 原型系统架构

以 CBDC 发行为例,对系统架构的运行过程说明如下.

商业银行核心系统发起请领 CBDC 的请求.商业银行核心系统向中央银行数字货币系统前置发起请领 CBDC 的 MQ(message queue:消息队列)报文或 HTTP 请求.中央银行数字货币系统前置通过 VPN (virtual private network:虚拟专用网络)向中央银行发行登记子系统转发报文,发行登记子系统开始处理 CBDC 的发行业务;

中央银行通过中央银行会计核算测试系统扣减存款准备金.发行登记子系统请求中央银行端的中央银行会计核算测试系统前置,发送扣减商业银行存款准备金报文.该前置将请求报文转发中央银行会计核算测试系统.中央银行会计核算测试系统扣减存款准备金后,通知商业银行端的中央银行会计核算测试系统前置存款准备金变化情况,该前置通知商行核心系统.中央银行会计核算测试系统同时将存款准备金扣款成功报文通知中央银行端的中央银行会计核算测试系统前置,该前置通知发行登记子系统扣款成功;

中央银行发行登记子系统生产发行 CBDC,通过中央银行数字货币系统前置发送至商业银行核心系统后,存放在商业银行银行库中;

中央银行发行登记子系统在确权账本进行权属登记.发行登记子系统通知确权发布子系统 CBDC 发行的权属信息,确权发布子系统将脱敏后数据发布在 CBDC 分布式确权账本上,CBDC 确权查询网站读取分布式账本数据用于确权查询.商业银行的确权账本节点同步中央银行确权账本节点数据.

3.3 技术架构

原型系统内部各子系统采用 J2EE 分层技术方案.CBDC 分布式账本部分采用 Python、C++以及智能合约编程语言进行开发.软件设计采用松耦合、分层设计的原则,包含接入层、接口层、服务层、资源层等 4 层,如图 9 所示.

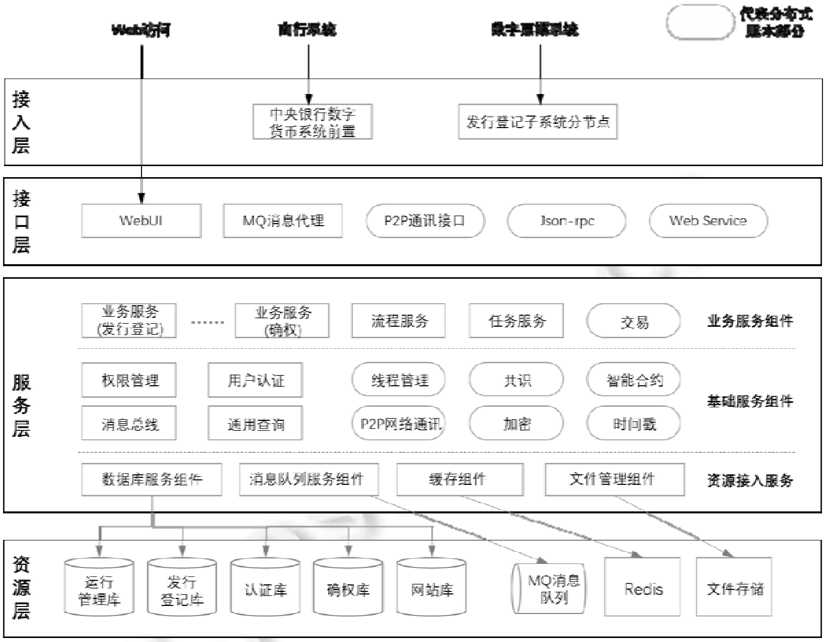

Fig.9 Technical structure of prototype system of CBDC

图 9 法定数字货币原型系统技术架构

原型系统各层采用的技术如下.

1. 接入层

主要包括中央银行数字货币系统前置及发行登记子节点,可通过 J2EE 标准的 WEB 应用对外提供 UI 功能访问服务,也可以对外以 MQ 报文的方式提供 API 接口.MQ 遵守 AMQP(advanced message queuing protocol,高级消息队列协议),可使用遵守 JMS(Java message service,Java 消息服务)技术规范或其他规范的程序进行访问.

2. 接口层

核心应用方面主要包括 WebUI、MQ 消息代理.

(1) WebUI 是与用户进行交互的界面,承担了从用户收集数据信息和向用户展现数据信息的作用.UI 层是系统的外在表现层面,本系统使用 Web 浏览器作为用户 UI 的展现载体.采用 HTTP/HTTPS 协议与 Web 服务器通信;

(2) MQ 消息代理,是原型系统与中央银行数字货币系统前置、发行登记子系统分节点进行报文交互的桥梁,承担了系统之间交互报文的转发功能.同样,MQ 遵守 AMQP 协议,可以使用遵守 JMS 技术规范或其他规范的程序进行访问.

分布式账本应用方面主要包括 P2P 通信接口、Json-rpc 和 Web Service 接口等.为分布式账本节点之间的通信提供接口,以及为访问分布式账本提供 API 接口.

3. 服务层

以服务的形式提供业务逻辑的封装实现,包括资源接入服务、基础服务组件、业务服务组件这 3 部分,具体实现采用开源 RPC(remote procedure call,远程过程调用)框架或其他技术.

(1) 资源接入服务,主要提供基础类资源访问服务,包括数据库访问服务、消息队列访问服务(JMS)、缓存访问服务、文件管理组件等;

(2) 基础服务组件,主要实现基础的业务逻辑封装,包括权限、消息总线、通用查询等.分布式账本方面包括共识、加密、时间戳、P2P 网络通信、智能合约虚拟机等基础组件服务;

(3) 业务服务组件,主要提供个性化、有针对性的具体业务服务,包括交易、任务以及发行、回笼、转移

等业务服务.

4. 资源层

资源层分为 4 类:数据库采用 Mysql,缓存采用 Redis[16]系统,消息队列采用 MQ,文件存储采用 HDFS(hadoop distributed file system,Hadoop 分布式文件系统)或普通文件系统.其中,分布式账本的块链数据采用文件形式存储,状态数据根据技术情况采用 LevelDB[17]或使用 Mysql.

4 问题探讨

4.1 采用分布式账本技术的确权登记中心

CBDC 的竞争力从技术的角度来说,一定要吸收借鉴先进成熟的数字技术.分布式账本技术作为近年来兴起并快速发展的新技术,是一种通过密码学方式保证不可篡改和不可伪造的去中心化共享总账.与传统技术相比,具有防止篡改的安全性、异构多活的可用性、对等协作的高效性、智能合约的先进性等优点,同时,在性能、隐私保护、升级修复等方面还存在各种制约其发展的问题和障碍.CBDC 如何从尚未成熟的分布式账本技术中受到启发、有选择地进行局部应用探索,也是原型系统的重要研究和实验内容.

原型系统将分布式账本技术应用于 CBDC 确权登记实验.初步探索由中央银行和商业银行构建 CBDC 分布式确权账本,提供可供外部通过互联网来进行 CBDC 确权查询的网站,实验 CBDC 网上验钞机功能.利用分布式账本不可篡改、不可伪造特性,为 CBDC 增加了一层技术保障以增强安全性.原型系统将发行登记子系统产生的 CBDC 更新信息,通过确权发布子系统发布到分布式确权账本.发行登记子系统与分布式确权账本在一定时间频率内保证一致性.利用分布式账本构建了一个 CBDC 确权信息副本,并对外通过互联网提供查询服务.这种设计一方面将核心的发行登记子系统对外界进行隔离和保护,同时利用分布式账本优势,提高确权查询的数据和系统安全性;另一方面,由于分布式账本仅用于对外提供查询访问,交易处理仍由发行登记子系统来完成,因此有效规避了现有分布式账本在交易处理上的性能瓶颈问题.

同时,经过原型系统实验发现,分布式账本技术在实际应用中还面临一系列问题亟待持续的技术改进,以增强其可用性.例如:CBDC 金额是重要隐私数据,分布式账本需要严格保护,可以应用 ECC(elliptic curves cryptography:椭圆曲线加密)算法的加法同态特性[18−20],辅以零知识证明可以实现隐私保护.分布式账本节点无法下线维护,出现系统漏洞难以修复,可以通过在底层内置紧急干预接口并授权给特定用户,根据需要暂停系统.分布式账本的共识算法缺乏弹性,共识节点不能动态加入或退出,可以通过智能合约管理白名单实现共识节点的动态管理等.

4.2 CBDC流通网格分析

发行 CBDC 可以逐步建立大数据中心实现反洗钱、支付行为分析、监管调控指标分析等,保障交易安全、规避风险,减少洗钱、逃漏税等违法犯罪行为,提升央行对货币供给和货币流通的控制力,更好地支持经济和社会发展.原型系统实验通过对 CBDC 运行过程的基本状态和关系进行研究,为构建大数据中心积累经验.

按第 2 节的运行机制,CBDC 状态包括两种:有效币、作废币,其中,作废币包括已使用和已回笼两种.通过发行,可以产生有效的 CBDC;通过回笼,会将有效 CBDC 转为已回笼的作废币.而转移过程则是将转移前的有效币作废,产生新的有效币.因此,整个 CBDC 在运行过程中,任意时刻会形成类似图 5 所示的流通网格瞬时图,该网格是一个有向无环图.该时刻所有有效币构成当前流通中的 CBDC,作废币中已回笼的 CBDC 构成所有回笼的 CBDC.所有没有来源币的 CBDC(包括有效币和无效币)构成所有发行的 CBDC.

从用户隐私保护角度,需要将 CBDC 信息通过加密方式进行脱敏,只有在法律许可的应用范围内进行追溯.在可控匿名前提下,大数据分析如何对用户隐私进行权衡,有待进一步研究探索.例如:对所有者信息进行加密后,仍然可以通过比较加密后的信息,对 CBDC 转移产生的新币分析出是否有找零,以及该所有者支付的频率、笔数、接收者数量等行为特征进行分析等.

4.3 原型系统技术优化分析

原型系统研发技术难点主要有 3 方面:一是多系统通信的稳定性和及时性,二是如何解决分布式账本性能问题,三是如何保证跨系统业务的可靠性.我们采用了几种策略解决上述问题:首先,采用分布式消息中间件来保证多系统通信的稳定性和及时性,同时保证业务消息(即报文)传递的可靠性;其次,将系统分层,核心系统采用传统架构达到高性能,分布式账本用来支撑确权登记中心,性能略有降低不影响核心业务处理;三是在业务处理可靠性方面采用错误的补偿处理机制,例如采用消息中间件来保证网络断线业务消息的重发等,确权登记信息在分布式账本发布失败不影响核心业务且自动重新发布等.未来,如何提升分布式账本性能、降低确权登记延迟等,有待于进一步研发.

5 实验研究

5.1 核心过程建模

原型系统发行和回笼主要是中央银行与商业银行之间的 CBDC 双向兑换过程,具有金额规模大、笔数少的批发类业务特征.而转移则包括商业银行以及最终用户相互之间的 CBDC 转移过程.原型系统一期虽然主要是商业银行之间的转移,但面向将来的最终用户应用,转移过程更主要是小额、高频、实时的零售业务特征,也是未来 CBDC 能够具有实用性和竞争性的关键.从实验角度,有必要基于原型系统,对 CBDC 转移过程进行模拟测试和分析.

如图 10 所示,转移过程是将来源币(即旧币)作废,产生去向币(即新币)的过程.CBDC 转移过程内部包括旧币验签、旧币作废、生产新币、权属登记这 4 步,形成原子性的事务.旧币验签主要是验证接收的 CBDC 是否合法有效,核心是对满足国密 SM2 规范要求的签名信息进行验签操作[21].旧币作废,主要是将旧币信息进行作废处理,分别在核心库和确权账本(即确权链)进行更新.核心库更新为数据库更新操作,确权链更新为分布式账本更新操作,考虑性能优化,将旧币作废和新币权属登记打包在同一个区块进行更新.生产新币是生成新的 CBDC,主要操作为满足国密 SM2 规范要求的签名操作.最后,权属登记与旧币作废类似,需要对核心库和确权链分别进行数据库和分布式账本更新操作.根据上述分析,CBDC 转移过程的关键操作包括 SM2 签名/验签、数据库更新、分布式账本更新.

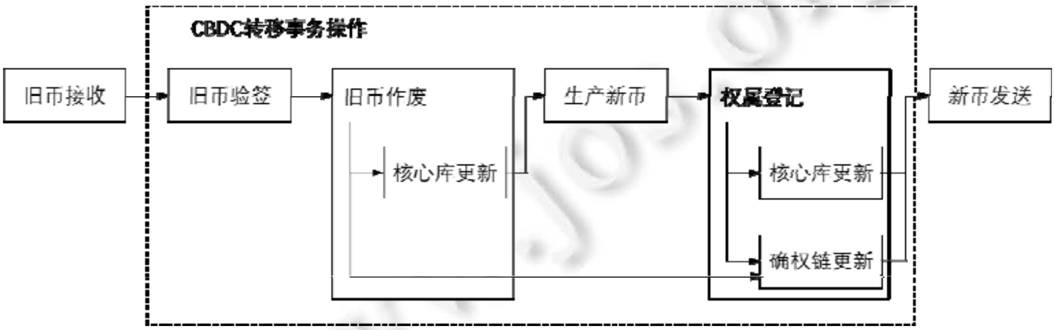

Fig.10 Transfer process of CBDC

图 10 CBDC 转移过程

从业务类型上,CBDC 转移可以抽象为两种典型模式:零币整付、整币零付.如图 11 所示,零币整付模式是将 n 个旧币转移后生成最多 2 个新币,1 个代表收款币,1 个代表找零币.整币零付模式是将 1 个旧币转移后生成 m 个收款的新币.

表 1 为一次零币整付和整币零付对应的关键操作次数分析,则两种操作的时间开销可以表示为

$$T_{零币整付}=T_{验签}(n)+\mathrm{Max}\{T_{DB\_update}(n+2),T_{BC\_update}(1\ \text{block})\}+T_{签名}(2).$$

其中,

- $T_{\text{旧币验签}}=T_{\text{验签}}(n)$;
- $T_{\text{旧币作废}}+T_{\text{权属登记}}=\mathrm{Max}\{T_{DB\_update}(n+2),T_{BC\_update}(1\text{ block})\}$;
- $T_{\text{新币生产}}=T_{\text{签名}}(2)$;
- $T_{\text{整币零付}}=T_{\text{验签}}(1)+\mathrm{Max}\{T_{DB\_update}(1+m),T_{BC\_update}(1\text{ block})\}+T_{\text{签名}}(m)$.

其中,

- $T_{\text{旧币验签}}=T_{\text{验签}}(1)$;
- $T_{\text{旧币作废}}+T_{\text{权属登记}}=\mathrm{Max}\{T_{DB\_update}(1+m),T_{BC\_update}(1\text{ block})\}$;
- $T_{\text{新币生产}}=T_{\text{签名}}(m)$.

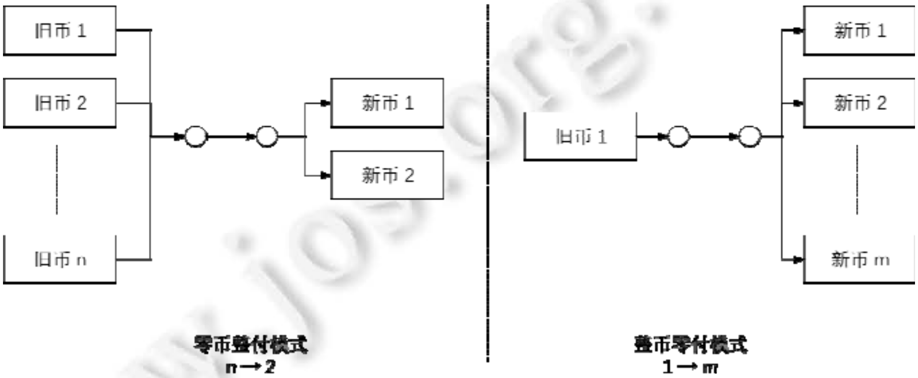

Fig.11 Transfer model of CBDC

图 11 CBDC 转移模式

Table 1 Key operating times of transfer process of CBDC

表 1 CBDC 转移过程关键操作次数

	零币整付	整币零付
旧币验签		
SM 2验签	n	1
旧币作废		
数据库更新	n	1
分布式账本更新	—	—
新币生产		
SM 2签名	2	m
权属登记		
数据库更新	2	m
分布式账本更新	1个区块 (n+2个币)	1个区块 (m+1个币)

5.2 指标测试分析

以下针对原型系统,分零币整付和整币零付两种模式,按不同的 rps(request per second,每秒请求数)测试其转移交易内部各关键操作的时间.例如:旧币验签 $rps=10,n=10$,相当于总共完成 100 次验签操作的时间.

测试实验环境硬件配置如下.

类型	配置信息	备注
应用服务器	2路4核CPU,16G内存,600GSAS硬盘,操作系统SuseLinuxEnterpriseServer 12	云平台虚拟机
数据库服务器	2路4核CPU,32G内存,4TSAS硬盘,操作系统SuseLinuxEnterpriseServer 12	物理服务器
区块链节点服务器	2路2核CPU,内存8G,1TSAS硬盘,操作系统 UbuntuServer 16.04	云平台虚拟机
加密机	加密机1:1U/100M/PCI-E 1X 加密机2:1U/1000M/PCI-E 1X 加密机3:2U/光口10G/PCI-E 16X	
VPN设备	吞吐量150Mbps,SSL-VPN加密速度100Mbps,IPSec-VPN隧道加密速度75Mbps	

软件及系统配置如下.

类型	基本信息
Tomcat	版本Tomcat 8.0.37
MQ	版本IBM MQ 8.0
Apache HTTP Server	版本2.4.23
Oracle	版本Oracle Database 11g Release 2
Redis	版本3.0.0
区块链	SDC V0.2(自主研发的区块链底层)
后台系统(认证中心/发行登记子系统/运行管理子系统/确权发布子系统)	Java 1.6/JSF+Spring/YAK
中央银行货币系统前置	Java 1.6/JSF+Spring/YAK
确权查询网站	Node.js Boron/Java 1.6

对于零币整付,取 n=10 来测试关键操作的耗时见表 2.

Table 2 Result of test on CBDC's summing a small (s)

表 2 零币整付交易和关键操作的测试结果 (s)

	rps=10	rps=100	rps=1000
旧币验签 *n* 次 SM2 验签	0.022	0.203	1.954
旧币作废 *n* 条数据库更新	0.001	0.002	0.016
新币生产 2 次 SM2 签名	0.005	0.031	0.407
权属登记 2 条数据库更新	0.001	0.002	0.012
分布式账本更新	1.828	1.790	8.933

对于整币零付,取 m=10 来测试关键操作的耗时见表 3.

Table 3 Result of test on CBDC's breaking a large (s)

表 3 整币零付交易和关键操作的测试结果 (s)

	rps=10	rps=100	rps=1000
旧币验签 1 次 SM2 验签	0.005	0.023	0.287
旧币作废 1 条数据库更新	0.001	0.002	0.015
新币生产 *m* 次 SM2 签名	0.021	0.215	1.581
权属登记 *m* 条数据库更新	0.001	0.002	0.017
分布式账本更新	1.722	1.903	9.710

指标测试的结果处于业内较高水平,通过分析主要影响性能的操作包括两部分.

1. 分布式账本更新的耗时明显超出其他操作,尤其是 *rps* 较小的情况下更为突出.这是由于区块链打包更新方式导致.因此在 rps 增大的时候,逐渐达到区块更新的实际吞吐性能,耗时差距逐渐缩小;
2. SM2 的验签和签名操作也是影响性能的重要因素[22].针对零币整付的验签操作、整币零付的签名操作,其 *rps*=1000 时的耗时均超过 1s.

而对于数据库更新操作,主要耗时在数据库连接的建立和释放,相对而言对性能暂未构成影响.

5.3 优化改进思路

5.3.1 分布式账本更新操作优化

分布式账本的性能并不能通过增加服务器的数量来进行水平扩展,因此主要依赖于纵向扩展(scale up)以及架构优化.在原型系统中,可通过下列方法提升性能.

(1) 改善网络连接速度.通过增加网络带宽、改善网络通信延迟,可以减少交易信息的传播时间,更快地达

成共识,从而增加系统的吞吐能力.增加网络的稳定性也有助于避免出现账本分叉的情况,避免触发数据重组等异常处理流程;

(2) 通过共识算法的改进,对交易打包规模、打包间隔,针对网络状况进行适配.缩小交易打包间隔有助于加快交易确认时间,合理的间隔时间也可以提高系统的处理能力;

(3) 使用硬件设备提升单点处理能力.分布式账本依赖单个记账节点的性能提升,硬件化是有效提升单节点性能的手段.通过将通用任务硬件化,以硬件提升性能瓶颈.比如对于签名和验签操作,通过外置的硬件加密机,可以突破单台服务器的性能瓶颈,实现性能的有效提升;

(4) 将部分任务并发处理,比如并发验签、签名等.虽然分布式账本的每笔交易每个节点都需要进行完整的合法性检查及后续处理,但单个节点内部仍然可以采用分布式架构,并设法将部分核心任务并发处理,以提高单个节点的处理能力,提高整个系统的性能;

(5) 优化应用层对分布式账本的使用方式.分布式账本成本高,交易都是异步处理,和传统系统架构差异较大,因此在系统架构上可采用传统数据库技术和分布式账本结合的方式,增加分布式账本数据的本地缓存,以减轻分布式账本的负载,提高系统整体的处理能力.

5.3.2 SM2 相关运算的优化

SM2 基于椭圆曲线密码学,主要用于替换 RSA 签名算法,在同等安全强度下所需密钥位数更少,且密钥对生成速度、签名速度均优于 RSA 数字签名算法,但 SM2 的验签速度相比 RSA 处于明显的劣势[23,24].表 4 为密钥长度为 256 的 SM2 签名和验签的运算速度比较,通过软件运算和硬件加密机两种方式进行测试,软件运算性能比普通加密机性能要好,但相比高性能加密机还存在一定差距.对于参与测试的 3 种不同品牌或型号的硬件加密机,其性能表现相差也比较大.

Table 4 Comparison of Various SM2 operating speed (tps)

表 4 SM2 运算速度比较 (tps)

	软件运算	加密机 1	加密机 2	加密机 3
SM2 签名	6750	1600	3707	9699
SM2 验签	5108	1200	2355	7294

从 SM2 算法角度,验签操作的速度会低于签名操作,CBDC 零币整付性能会略低于整币零付.同时,上述测试结果表明,采用高性能硬件加密机可以有效提高 SM2 签名和验签速度.按 n=10 和 m=10 情况下,以测试速度最快的加密机 3 进行 CBDC 转移的操作,基于 SM2 签名和验签运算速度,其零币整付和整币零付两种 CBDC 转移操作的理论 *tps*(transaction per second:每秒执行事务数量)值为 970 和 729.在单机条件下,离实际应用需求还存在一定差距.后续可以考虑提升硬件设备的性能,同时,可以采用多机并行运算的方式进一步提升 SM2 运算效率[25−27].

5.3.3 转移内部操作的优化

CBDC 转移过程的 4 个操作步骤目前基本是串行化方式进行,其遵循的原则是先减后加,可以防止因为异常错误导致虚增货币的情况.同时,当前数据库和分布式账本是异步更新,存在状态不一致问题.其优化思路主要有两点:一是尽可能采用并行化操作,二是设计数据库和分布式账本同步更新机制.具体而言,可以将旧币验签和新币生产并行处理,如果旧币验签不通过,旧币和新币都不会在数据库和分布式账本中进行更新.之后,将旧币作废和新币权属登记同时提交处理,此处需要保证数据库与分布式账本的数据一致性.首先是将旧币作废和新币权属登记的更新内容,分别构建数据库更新请求和打包到分布式账本的一个新的区块内.根据实验数据,数据库更新速度要快于分布式账本,因此可以同时发送数据库更新和分布式账本更新请求后,在数据库更新的事务操作中加入对分布式账本更新结果的监听,一旦确认分布式账本更新完成,数据库更新的事务同步提交.进一步,为防止数据库事务出现错误回滚的情况,可以在数据库更新之前先进行预提交,确认事务可正确执行后,再发起分布式账本的更新操作.另外,可以考虑未来设计一种数据库与分布式账本的同步更新中间件和协议,实现数据库和分布式账本双向同步更新并保持事务性.

6 总 结

央行数字货币的研发是一个循序渐进的过程.中国人民银行在全球范围内最早系统化地开展法定数字货币研究,在关键领域取得阶段性研究成果.数字货币原型系统一期按照二元模式的顶层设计,由人民银行和商业银行实际参与,对 CBDC 的发行、转移和回笼整个生命周期闭环体系进行了完整实验,并在测试环境中成功运行;探索了 CBDC 的表达形式,解决了发行回笼机制和转移机制问题,并就数字货币原型系统相关系统架构和技术架构进行了成功实验;针对现有分布式账本技术的优势和不足,扬长避短,尝试在 CBDC 网上确权查询中加以有效运用,结合实践提出改进思路以提高分布式账本技术可用性;探讨在保护用户隐私前提下,可以对 CBDC 进行数据分析.通过对 CBDC 转移的实验研究,发现影响其性能的关键在于分布式账本更新和 SM2 运算,有关优化改进思路,有待后续在更多 CBDC 应用场景中进一步研究和深化.

关于央行数字货币合理的推进路径,普遍的共识是从中央银行-商业银行-非银行金融机构-单位账户-个人账户,直至最终完全取代实物现金.这是一个从易到难,从 *B* 端延伸到 *C* 端,从批发到零售,逐步扩大使用范围的可控可行路径.在对二元模式下 *B* 端应用场景进行深入探索的基础上,中国人民银行将进一步开展 *C* 端场景的应用研究.这是一项前无古人的工作,涉及到方方面面,需要周密论证,全面考量,审慎推进.鉴于中国金融基础设施的后发优势和数字经济的潜在需求,有必要加快法定数字货币的探索研究,以进一步跟上现代科学技术的发展,保持金融服务的前瞻性和控制力.

References:

[1] CBDC Woking Group of the People’s Bank of China. China’s Path of CBDC. China Finance,2016,17:45−46 (in Chinese).

[2] Fan YF. Theory and Structure of China's CBDC. China Finance, 2016,17:10−12 (in Chinese).

[3] Yao Q. Central Bank Crypto-Currency: An Analysis on RSCoin System. Finance, 2017,6 (in Chinese).

[4] Garratt R. CAD-Coin versus fedcoin. R3 Report, 2016.

[5] Monetary Authority of Singapore. The future is here—Project ubin: SGD ondistributed ledger. Technology Reports, 2017.

[6] ECB. Distributed ledger technologies in securities post-trading revolution or evolution? Occasional paper series. 2016.

[7] BIS. Distributed ledger technology in payment, clearing and settlement—An analytical framework. Technology Reports, 2017.

[8] Yao Q. Thoughts on China’s CBDC Prototype. China Finance, 2016,17:13−14 (in Chinese).

[9] Yao Q. Theoretical Logics and Technical Structure of CBDC, Comparision, 2017,8 (in Chinese).

[10] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

[11] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895, 2015.

[12] Samid G. Bitcoin. BitMint: Reconciling bitcoin with central banks. IACR Cryptology ePrint Archive, 2014.

[13] Institute of Digital Money of the People's Bank of China. Method and Device of Circulation of Digital Money. Patent 201710495071.7. 2017 (in Chinese).

[14] Institute of Digital Money of the People's Bank of China. Method and System of Issuance of Digital Money. Patent 201710493230.X. 2017 (in Chinese).

[15] Institute of Digital Money of the People's Bank of China. Method and System of Withdrawal of Digital Money. Patent 201710492677.5. 2017 (in Chinese).

[16] Introduction to Redis. https://redis.io/topics/introduction

[17] LevelDB. http://leveldb.org/

[18] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm. Int’l Journal of Information Security, 2001,1(1):36–63.

[19] Yang JH, Dai ZD, Yang DY, Liu HW. An elliptic curve signature scheme and an identity-based signature agreement. Ruan Jian Xue Bao/Journal of Software, 2000,11(10):1303–1306 (in Chinese with English abstract). http://www.jos.org.cn/jos/ch/reader/view_abstract.aspx?flag=1&file_no=20001005&journal_id=jos

[20] Yu HF, Yang B. Identity-Based hybrid signcryption scheme using ECC. Ruan Jian Xue Bao/Journal of Software, 2015,26(12): 3174–3182 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4819.htm [doi: 10.13328/j.cnki.jos.004819]

[21] Nie YX, Liu BB, Ren W. The implementation and evaluation of SM2 algorithm in Java. Security of Inforamtion Network, 2013,(8):13−17 (in Chinese with English abstract).

[22] Sun RY, Cai CS, Zhou Z, Zhao YJ, Yang JM. The comparision between digital signature based on SM2 and ECDSA. Technology and Implementation of Internet Security, 2013,2 (in Chinese with English abstract).

[23] Khalique A, Singh K, Sood S. Implementation of elliptic curve digital signature algorithm. Int'l Journal of Computer Applications, 2011,2(2):21−27.

[24] Abidi A, Bouallegue B, Kahri F. Implementation of elliptic curve digital signature algorithm (ECDSA). In: Proc. of the 2014 Global Summit on Computer & Information Technology (GSCIT). 2014. 1−6. https://www.researchgate.net/publication/286584272

[25] Nabil G, Naziha K, Lamia F, Lotfi K. Hardware implementationof elliptic curve digital signature algorithm (ECDSA) on Koblitz curves. In: Proc. of the Int'l Symp. on Communication Systems. 2012. 1−6.

[26] Hou ZF, Li L. The research on designing and optimizing of the algorithm for elliptic curve cryptography (ECC). Acta Electronica Sinica, 2004,32(11):1904−1906 (in Chinese with English abstract).

[27] Zhong L, Liu Y, Yu SY, Xie Z. Hardware/Software co-design of SM2 encryption algorithm based on the embedded SoC. Journal of Computer Applications, 2015,35(5):1412−1416 (in Chinese with English abstract).

附中文参考文献:

[1] 中国人民银行数字货币研究项目组.法定数字货币的中国之路.中国金融,2016,17:45−46.

[2] 范一飞.中国法定数字货币的理论依据和架构选择.中国金融, 2016,17:10−12.

[3] 姚前.中央银行加密货币——RSCoin 系统之分析.财经,2017,6.

[8] 姚前.中国法定数字货币原型构想.中国金融,2016,17:13−14.

[9] 姚前.法定数字货币的理论逻辑与技术架构.比较,2017,8.

[13] 中国人民银行数字货币研究所.数字货币的流通方法和装置.专利 201710495071.7.2017.

[14] 中国人民银行数字货币研究所.数字货币的发行方法和系统.专利 201710493230.X.2017.

[15] 中国人民银行数字货币研究所.数字货币的回笼方法和系统.专利 201710492677.5.2017.

[19] 杨君辉,戴宗铎,杨栋毅,刘宏伟.一种椭圆曲线签名方案与基于身份的签名协议.软件学报,2000,11(10):1303−1306. http://www.jos.org.cn/jos/ch/reader/view_abstract.aspx?flag=1&file_no=20001005&journal_id=jos

[20] 俞惠芳,杨波.使用 ECC 的身份混合签密方案.软件学报,2015,26(12):3174−3182. http://www.jos.org.cn/1000-9825/4819.htm [doi: 10.13328/j.cnki.jos.004819]

[21] 聂意新,刘彬彬,任伟.SM2 密码算法的 Java 实现与评测.信息网络安全,2013,(8):13−17.

[22] 孙荣燕,蔡昌曙,周洲,赵燕杰,杨金铭.国密 SM2 数字签名算法与 ECDSA 算法对比分析研究.网络安全技术与应用,2013,2.

[26] 侯整风,李岚.椭圆曲线密码系统(ECC)整体算法设计及优化研究.电子学报,2004,32(11):1904−1906.

[27] 钟丽,刘彦,余思洋,谢中.嵌入式系统芯片中 SM2 算法软件硬件协同设计与实现.计算机应用,2015,35(5):1412−1416.

姚前(1970－),男,安徽歙县人,博士,教授级高工,博士生导师,主要研究领域为数字货币,金融科技,金融标准化.