Computer Science and Application 计算机科学与应用, 2020, 10(11), 1984-1992
Published Online November 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1011210

Hans汉斯

基于区块链技术下法定数字货币架构要素研究

陈小虎[1]，刘　峰[2*]

[1]上海墨珩网络科技有限公司，上海
[2]无锡太湖学院，江苏省物联网应用技术重点建设实验室，江苏　无锡
Email: lsttoy@163.com

收稿日期：2020年10月29日；录用日期：2020年11月13日；发布日期：2020年11月20日

摘　要

为了最大化地利用区块链带来的创新功能，又能驾驭区块链应用给央行货币这一传统中心化体系带来的挑战和冲击，以满足中心化管理的需要。本研究将尝试从中国人民银行推出的数字货币DC/EP的架构分析入手，探讨基于区块链的数字货币如何应用于央行法定数字货币及其支付体系外沿的可行性方案，并得出使用区块链并不一定就会是以中心化管理为主要特征的央行数字货币的阻碍，相反还会成为其进入不同市场应用的架构基础和和现有方案的有益补充等结论。本研究创新性地提出了基于默克尔树(Merkle Tree)的扩展C-Tree，为央行数字货币基于区块链的实现提供了一个技术基础。在C-Tree基础上，本研究构建了一个双层区块链系统，使得数字货币系统能够满足央行的各种要求。本研究对法定数字货币方案研究有着推动作用。

关键词

区块链，数字货币，DC/EP，架构要素研究

Research on the Elements of Legal Digital Currency Architecture Based on Blockchain Technology

Xiaohu Chen[1], Feng Liu[2*]

[1]Shanghai Moheng Network Technology Co., Ltd., Shanghai
[2]Key Construction Laboratory of Internet of Things Application Technology of Jiangsu Province, Wuxi Taihu University, Wuxi Jiangsu
Email: lsttoy@163.com

Received: Oct. 29th, 2020; accepted: Nov. 13th, 2020; published: Nov. 20th, 2020

*通讯作者。

文章引用: 陈小虎, 刘峰. 基于区块链技术下法定数字货币架构要素研究[J]. 计算机科学与应用, 2020, 10(11): 1984-1992. DOI: 10.12677/csa.2020.1011210

Abstract

In order to maximize the use of the innovative functions brought by the blockchain, and to manage the challenges and impacts of the blockchain application to the traditional centralized system of central bank currency, to meet the needs of centralized management, this research will try to start with the analysis of the architecture of the digital currency DC/EP launched by the People's Bank of China, explore how the blockchain-based digital currency can be applied to the central bank's legal digital currency and the feasibility of its payment system, and draw the conclusions. Blockchain is not necessarily an obstacle to the central bank's digital currency, which is mainly characterized by centralized management. On the contrary, it will become the architectural foundation for its entry into different market applications and a useful supplement to existing solutions. This research promotes the research of legal digital currency solutions.

Keywords

Blockchain, Digital Currency, DC/EP, Feasible Solutions

1. 引言

虽然发达国家掀起的反无现金社会的运动此起彼伏，从未真正平息，但由私营部门、商业银行、非银金融机构、金融科技公司等创造的数字化的货币形式却越来越广泛地应用于日常支付并深刻地改变着整个支付市场。据统计，电子支付市场的交易总值预计在 2020 年将超过 4.4 万亿美元，其中中国市场贡献了约 1.9 万亿美元，并将以每年 17%的增长率增长至 2024 年[1]。

基于区块链的加密货币[2] (crypto currency)，特别是稳定币，对现有的货币系统带来了新的挑战和思想碰撞。与电子支付创造的所谓数字现金(digital cash)不同，加密货币相对独立于各国的法定货币体系之外，更多地代表在社会经济活动中产生的数字资产及其价值载体。而稳定币在加密货币的生态中扮演价值之锚的角色，它既是数字资产(crypto assets)与传统价值市场交换的桥梁，也是其计价单位。加密社区、大型金融机构和科技巨头越来越多地认识到稳定币的这些特质，并能够围绕稳定币建立其领域内的金融生态。

一些稳定币已经开始建立起强大的影响力。例如 Tether 公司发行的 USDT，市值已超 133 亿美元。金融巨头摩根大通银行发行的 JPM Coin，已成为全球最大企业支付场景中的支付记账凭证。当然，给各国央行带来前所未有压力的还是互联网科技巨头脸书(Facebook)的 Libra [3]项目对未来主权货币可能产生的影响。因此世界各国央行的数字货币 CBDC (Central Bank Digital Currency)或者 DC/EP (Digital Currency Electronic Payment)的研究进入快车道，各种消息不断涌现。但除了瑞典推出的 e-krona 已于 2020 年 2 月宣布开始测试外，世界主要经济体的央行仍在对是否研制 CBDC 或如何架构其 CBDC 展开讨论。从这个角度看，中国人民银行推出的 DC/EP 方案已经走在了前面。

在这样一种态势下，各国央行发展 CBDC 或 DC/EP 的共同的目标十分清晰。首先，面对越来越数字化的全球经济，央行数字货币不可避免地要超越私营部门向本区域乃至更广阔的范围提供更安全、更稳

定、更受信赖的货币以及与之相关的支付方案。其次，央行数字货币肩负着维护货币财政乃至金融经济稳定的任务。任何法定数字货币均不可能完全替代其他形式的法币，那么各国央行对其数字货币与现行支付体系的互操作性均有不同程度的要求。因而，基于对当下和可预见将来的货币市场的理解，各国央行对 CBDC 的探讨也体现出对其功能性和架构设计的不同要求。这其中最引人注目的是各国 CBDC 从技术上是否选用区块链技术来达到某种数字支付方案的目标，如去中心化体系可能带来的更强的抗风险能力和可信度，非对称加密和点对点支付对个人隐私和商业机密的保护，以及通过智能合约发展出的可编程货币等[4] [5] [6]。CBDC 或 DC/EP 如何设计，是否使用区块链，取决于在使用区块链的时候做到趋利避害，既能最大化地利用区块链带来的创新功能，又能驾驭区块链应用给央行货币这一传统中心化体系带来的挑战和冲击，以满足中心化管理的需要。

本文将尝试从中国人民银行推出的数字货币 DC/EP 的架构分析入手，探讨基于区块链的数字货币如何应用于央行法定数字货币及其支付体系外沿的可行性方案。本研究创新性地提出了基于默克尔树(Merkle Tree)的扩展 C-Tree，为央行数字货币基于区块链的实现提供了一个技术基础。在 C-Tree 基础上，本研究构建了一个双层区块链系统，使得数字货币系统能够满足央行的各种要求。

2. 中国人民银行推出的数字货币 DC/EP

中国市场在电子支付的领域实际已处于领先地位，也许正是因为私营部门发展起来的移动支付已经基本形成一种金融基础设施，人民银行不直接向公众发行数字货币，将采用双层运营体系，即人民银行先把数字货币兑换给银行或其他运营机构，再由这些机构兑换给公众。

DC/EP 是对 M0 的替代，必须满足现有的现金所能完成的全部重要功能，同时能够更加有效地满足当前及未来在金融领域对数字货币的需求(图 1)。

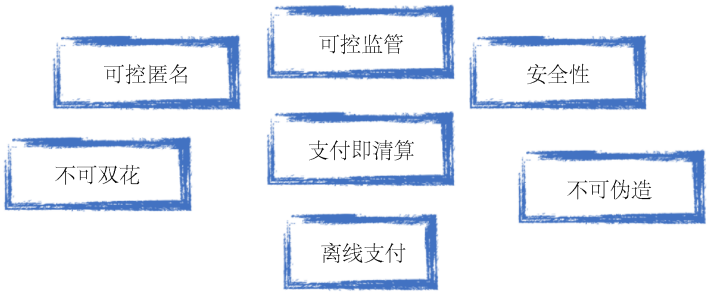

Figure 1. Future demand for digital currency in the financial sector
图 1. 未来在金融领域对数字货币的需求

为了满足上述的要求，也为了充分发挥已有的基础设施、金融和商业机构的积极性并减少对金融体系的冲击，DC/EP 在研发之初就提出了一些指导性的设计思路，包括：不预先选定某个技术，既包括现有的移动支付，也包括区块链和分布式账本(DLT)类加密数字货币系统；不同体系的技术并行发展，在确保安全的同时可达超高频吞吐量等。

2019 年 8 月，人民银行支付结算司副司长穆长春在第三届中国金融四十人论坛上明确指出，在双层运营体系安排下仍要坚持中心化的管理模式。加密资产的自然属性就是去中心化，但央行数字货币一定要坚持中心化的管理模式[7] [8]。

3. 基于区块链的数字货币解决方案

我们认为单纯的中心化或去中心化架构都无法满足以上功能要求。如同阴在阳之内不在阳之对，中

心化与去中心化从来不是不可兼容的矛和盾，而是对立统一的有机复杂系统。当今对最前沿的区块链网络体系的架构思考纷纷在探讨如何在保持中心化带来高效率的同时，避免其带来的可靠性的不足。

传统的区块链更加侧重去中心化，而去中心化并不是银弹，不能够寄希望它来解决一切问题。相反的，是否选择去中心化是需要和当前场景的主要矛盾相符合，如果当对公平或者透明的诉求成为了主要矛盾，那么去中心化将是一个不错的解决方法。但是在当前很多领域中，对效率的需求还是主要矛盾，所以在这些场景下，采用去中心化效果并不是会很好，反而会起到不断消耗的反作用。

我们提出的数字货币方案是一个分层架构方案(图 2)，其主旨是在维持现有的商业银行和央行双层逻辑的基础上，扩大商业银行这一层的覆盖范围，可以将符合监管要求的本国科技企业、机构都纳入到总体设计中，同时可以将覆盖范围扩展到一带一路国家和地区的企业和机构等，使得 DC/EP 的覆盖范围更广，使用更加灵活，场景更加丰富，同时促进人民币的国际化，促进一带一路的深度整合。

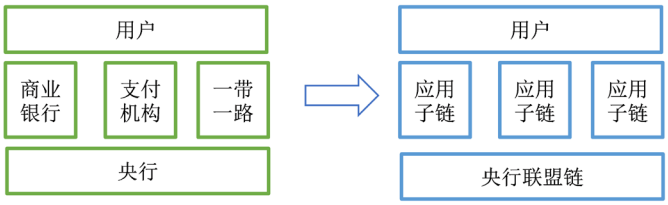

Figure 2. Layered architecture digital currency solution architecture
图 2. 分层架构数字货币方案架构

这个方案的分层设计体现在金融管理规则安排和技术架构两个方面。金融管理规则安排的分层架构指，在央行这一层，构建一个基于区块链的联盟链系统(图 3)。这个联盟链的共识节点可以包括央行，以及经严格审批可以加入的金融机构。其他的所有符合监管要求的企业、银行、金融机构都可以是这个联盟链的用户。在这个联盟链系统中，中国央行推出人民币数字结算货币，这个数字结算货币并不是直接让大众使用，而是用于联盟链用户之间的跨行转账、调整保证金额度等。

每个联盟链的用户(金融机构)，可以根据各自的条件和资格，发行统一标准的 DC/EP。每个金融机构必须根据不同的监管要求，实现在保证金基础上的 DC/EP 的份额的严格控制。其中的具体配比和管理规则可以通过在联盟链中部署的保证金智能合约/货币互换智能合约来实现。任何一个金融机构在任何时候的存量必须满足智能合约的规则。当某个金融机构发生挤兑危机时，其 DC/EP 的用户可以选择其他有信用的金融机构进行兑付。为保证这些兑付可以高效快速并正确执行，我们提供的法定数字货币架构体系设计了以下功能：

1) 每个 DC/EP 的发行都有最终锚定在央行联盟链上的哈希证明；

2) 每个 DC/EP 可以很方便地在任意一个金融机构被验证；

3) 保证金智能合约加上跨机构交易结算保证其他金融机构不受影响；

4) 基于分层结构的可扩展技术框架，可以保证短期内的大量交易请求得到快速执行。

作为央行维护的联盟链的上面一层，每个金融机构维护一个独立的可信账号系统(应用子链)。其可信账号系统必须保证：

1) 所有的金融机构之间的 DC/EP 是同质的，可以互相流通，不受发行金融机构的限制。甚至在发行金融机构破产的情况下，仍然可以从同类金融机构获得兑付。数字货币系统应保留这种兑付的功能，但具体兑付的规则和管理办法则可以根据实际情况写入相关的智能合约；

2) 发行金融机构的总量和存量，必须满足联盟链中的规则的严格保证，在出现问题的情况下被追责，并通过保证金兑付；

3) DC/EP 系统能够满足上述所有技术要求。

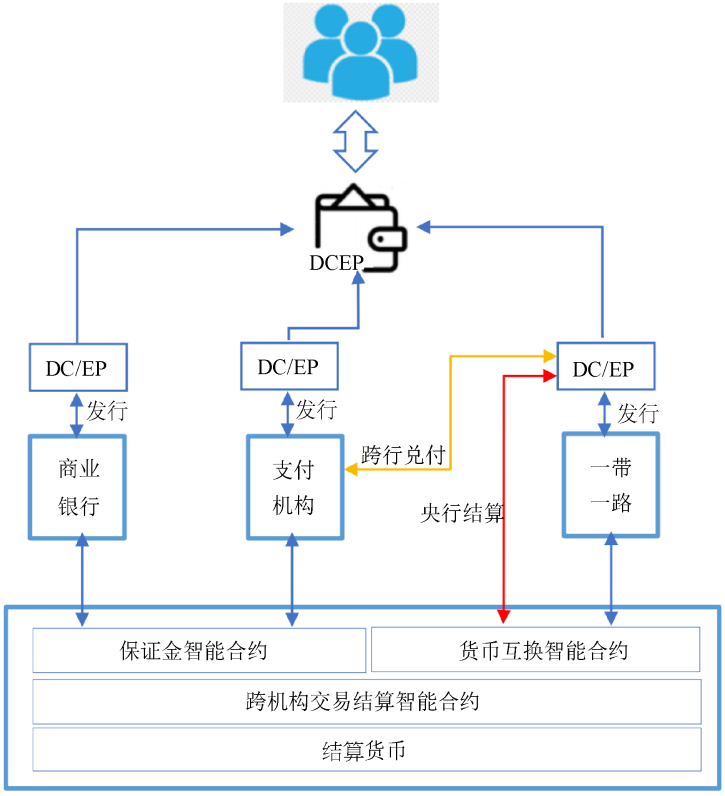

Figure 3. Ideas for the design of legal digital currency architecture system
图 3. 法定数字货币架构体系设计方案思路

4. 基于区块链的数字货币的技术实现

Merkle 树是区块链技术的重要组成部分。以区块链的通证体系为例，对于每个区块，当前块中的所有的交易，作为叶节点构建一个树状的数据结构。每个非叶节点是子节点的哈希。这样，根哈希可以完整性地表述当前区块的所有交易集合，可以用于确认和验证数据的一致性。当前的加密货币如比特币以太坊等都采用这样的数据结构。

如图 4，采用 Merkle 树可以实现当前区块链上的加密货币的各种优点：无法篡改，无法伪造，交易即清算等。但是由于区块链是由一系列离散的区块串联而成的数据系统，对于某个通证/UTXO 的有效性的检查，必须上溯整个区块链的历史区块，以验证其有效性后再作处理。因此，每个区块链上的共识节点都必须维护整个区块链的历史，并保证各个共识节点的 Merkle 树的一致性。由此衍生出的各种区块链共识协议即是如何有效地实现节点间信息的传递以达到全局一致。因此，采用 Merkle 树结构的区块链系统具有处理能力低、无法离线验证等缺点，并不适合央行数字货币需要的各种要求。

本研究创新性地提出了基于默克尔树(Merkle Tree)的扩展 C-Tree，为央行数字货币基于区块链的实现提供了一个技术基础。

(一) C-Tree 以及账户的技术实现

C-Tree (Complementary Tree)是基于默克尔树的扩展。与默克尔树不同，每个非叶节点除了具有子节点的哈希外，还有 一个伴随信息 meta，并且这个 meta 信息符合某种设定的运算。

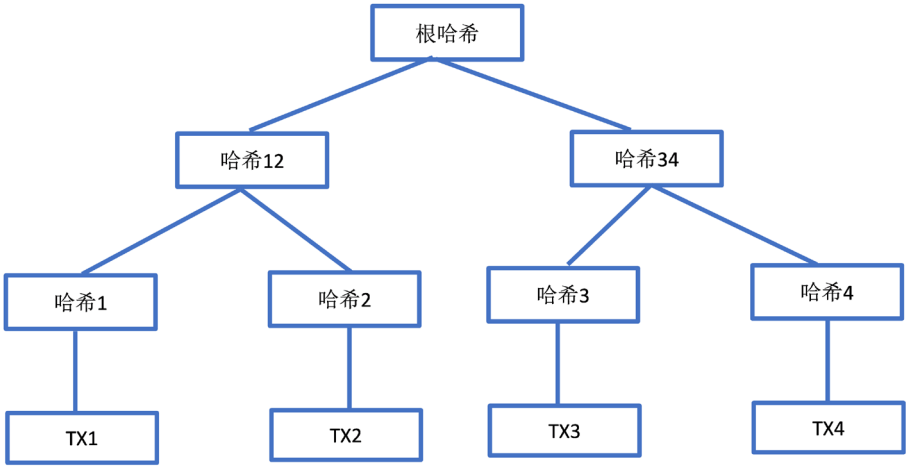

Figure 4. Merkle tree used to represent transactions in the current block
图 4. 用于表示当前区块内的交易的 Merkle 树

如图 5 所示的 C-Tree，其满足两个条件：

For any non-leaf node:

$Hash_i = hash(child\_left_{i+1}, child\_right_{i+1})$

$Meta_i = Func(meta\_left_{i+1}, meta\_right_{i+1})$

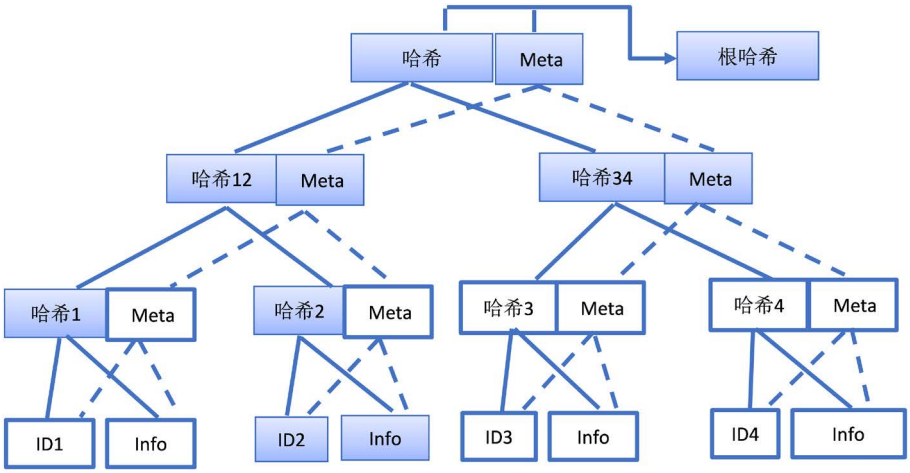

Figure 5. Merkel tree expansion C-Tree
图 5. 默克尔树的扩展 C-Tree

这里的 Func 可以是用户定义的函数，一个简单的例子是 MinMax。每个 meta 信息包含子树所有 id 的(Min，Max)。这样可以通过 C-Tree 来快速获得整个子树的 ID 的范围。

另外一个例子是包含证明。每个 Func 用来计算当前子树的所有 id 的包含证明。例如可以采用零知识证明的算法。这样，用 C-Tree 构建的区块可以很方便地实现包含证明和非包含证明。

本研究采用一个排序的 C-Tree，对页节点做特殊处理，使得左叶节点是键值，右叶节点是 value 值。整个树对键值进行排序。叶节点的父节点也做响应的特殊处理：最大最小值都是其叶节点的键值。Meta 信息采用 MinMax 函数，可以获得子树的键值的范围。

从用户的角度出发，用户获得一个电子货币 DC/EP，本质上就是一个 C-Tree 证明。C-Tree 证明：从

键/值开始上溯到根节点的路径加每个节点的兄弟节点组成的证明。例如图中阴影部分的值/哈希构成一个有效 C-Tree 证明。每个电子货币的用户需要合适的签名来使用这个货币，这是与区块链的通证的使用方式是一致的。

账号的具体实现方式是采用基于区块链的分布式账本技术。具体来讲，采用扩展的 Merkle [9]树，通过构建一个树状结构(C-Tree)，将当前的交易集合有效组织起来，并通过根哈希锚定在底层央行联盟链的方式，实现对细颗粒度的交易的可信记录。

(二) 支付系统

基于 C-Tree 我们可以构建一个支付系统。技术实现，由此构建起来的支付系统我们称为区域内快速支付系统(Intra-domain Fast Payment System, IDFP)，其具有高效的交易处理能力，也可以接受用户查询和支付请求。

直接对用户提供数字货币服务的是支付系统。支付系统就是对用户提交的交易请求进行响应并处理。技术上看，类似于区块链的实现方式，周期性地，将符合规则的用户请求打包，构建一个 C-Tree 的实例(图 6)。C-Tree 生成的周期可以 1 秒或者 3 秒，可以根据具体的使用场景灵活配置。每个 C-Tree 代表设定数额的数字货币以及总量。每个 C-Tree 的叶节点设置为数字货币的编号以及该编号所对应的所有者的历史记录。

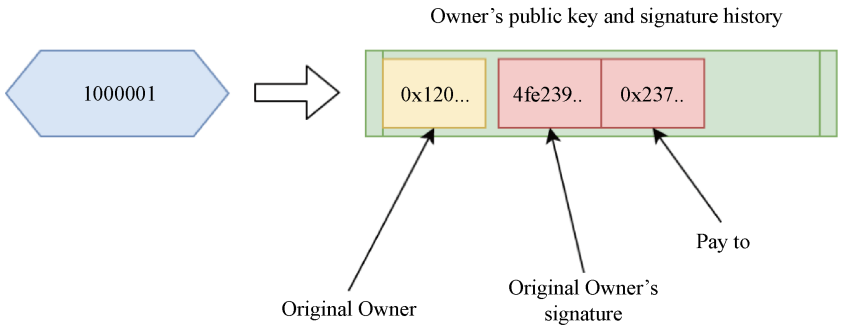

Figure 6. Example of C-Tree
图 6. C-Tree 的叶节点实例

初始化时所有的数字货币的所有者都是发行方。当支付给其他人时，需要追加接受方的公钥地址，以及原主人的合法签名。随着数字货币的转让次数增加，所有者的历史记录也相应增加。当某个编号的数字货币转移量超过某个设置值 M (~1000)的时候，发行方可以在一个新的 C-Tree 里面的某个新的数字货币来替换原来的数字货币。

(三) 账号的区块链锚定

以 C-Tree 为基础的独立支付系统的可信度受到发行方自己的信用限制。为了实现整个支付网络中的可信度，需要将每个支付系统中的每个用户的数字货币在区块链上确权。因此，我们需要一个央行联盟链。每个支付系统将每个 C-Tree 的根哈希锚定在底层的央行联盟链上。锚定的根哈希，加上每个数字货币的 C-Tree 证明，使得每一个数字货币的有效性能够得到验证。当 C-Tree 中的的键值变化时，更新的根哈希周期性地记入到区块链中，实现对记录的连续确认。为了提高哈希存储的效率，聚合签名[10]/零知识证明[11]可以用于 C-Tree 实现的优化。

每个发行方可以是商业银行，也可以是企业，或者某个行业。每个 C-Tree 对应一个底层央行联盟链中部署的合约，用于管理 C-Tree 的去中心化状态，包括 C-Tree 的币值、数量，编号范围，持续的根哈希记录。同时，此合约控制数字货币的发行、赎回、双花仲裁、跨发行方清算等功能。

5. 区域内快速支付系统的效果评估

由此构建的区域内快速支付系统具有以下特点：

1) 离线支付功能。电子货币的当前所有者可以签名并支付给接受方，并提交证明。接受方可以根据缓存的历史哈希，验证该证明的有效性。接受方可以离线接受，并验证签名有效性。接受方一旦上线，可以递交电子货币的更新部分，确认真正的拥有权。

2) 连续的串联离线支付功能。离线支付的接受方可以继续离线发送给下一个接受方，只要给出正确的签名。

3) 该系统可以实现海量用户的巨大交易处理能力。由于第二层可以任意扩展，每个金融机构可以构建一个区域内快速支付系统。因此，底层区块链可以支持>10,000 个这样的区域内快速支付系统，单个区域内快速支付系统可以并行实现 10,000 TPS，这个系统可以实现亿次级别的吞吐量。

4) 支持灵活的电子货币的发行、控制、管理功能。每个发行方可以是商业银行，也可以是企业，或者某个行业。每个区域内快速支付系统在底层央行联盟链映射一个合约，用于管理该系统的去中心化状态，包括币值、电子货币的数量，编号范围，持续的根哈希记录。同时，此合约也控制发行、赎回、双花仲裁、跨发行方清算等功能。

5) 支持监管功能。底层央行联盟链映射合约中可以支持监管接口。当需要监管时，可以对有问题的电子货币进行冻结等功能。系统的本地记录对公众保密，当需要监管时，监管部门可以获得所有的用户的使用记录。

6) 灵活的扩展功能。本系统缺省支持非标资产。事实上，每个电子货币，就是一个非标资产。在固定面额的条件下，就是普通的区块链通证，类似于有序列号的 100 元人民币面额的现钞。在其他的应用场景下，每个序号可以对应唯一的数字资产，实现对独一无二的资产的支付与追踪。

6. 结论与展望

数字货币的实现是否使用区块链技术是一个被广泛争论的话题。针对央行对数字货币在批发到零售间的大部分功能要求，本文提供使用区块链双层架构(央行联盟链 + 区域内快速支付系统)的数字货币区块链实现。央行数字货币在实施到具体商业应用中，需要相当的可扩展性和互操作性才能适用于复杂的市场体系和商业逻辑。从我们的视角，使用区块链并不一定就会是以中心化管理为主要特征的央行数字货币的阻碍，相反还会成为其进入不同市场应用的架构基础和和现有方案的有益补充。此外，本研究创新性地提出了基于默克尔树(Merkle Tree)的扩展 C-Tree，基于 C-Tree 的技术研究目前还是属于空白，由此可以衍生出许多优异特性的区块链方案，也为央行数字货币基于区块链的实现提供了一个技术基础和新的思路。

基金支持

本课题得到江苏省物联网应用技术重点建设实验室资助。

参考文献

[1] (2020) Digital Payments. https://www.statista.com/outlook/296/100/digital-payments/worldwide

[2] 中本聪. 比特币: 一种点对点的电子现金系统[EB/OL]. 2008. https://nakamotoinstitute.org/static/docs/bitcoin-zh-cn.pdf

[3] Libra 白皮书[EB/OL]. https://libra.org/zh-CN/white-paper

[4] Discussion Paper: Central Bank Digital Currency, Opportunities, Challenges and Design. Bank of England, 7.

[5] The Future of Payment, Part I/II, 2020. Deutsche Bank Research. https://www.dbresearch.com

[6] 中国央行数字货币 DCEP 如何重构未来商业形态[EB/OL]. https://www.sohu.com/a/395468364_676545

[7] 央行穆长春：数字货币会采取双层运营体系[EB/OL]. 新华网. http://www.xinhuanet.com/fortune/2019-08/13/c_1210239239.htm, 2019-08-13.

[8] 盘和林. 央行表达数字货币，在数字货币领域掌握国际主动权[EB/OL].

[9] Merkle Tree. https://en.wikipedia.org/wiki/Merkle_tree

[10] 杨涛, 等, 聚合签名及其应用研究综述[J]. 计算机研究与发展, 2012(S2): 192-199.

[11] Yang, X.H. and Li, W.J. (2020) A Zero-Knowledge-Proof-Based Digital Identity Management Scheme in Blockchain. *Computers & Security*, **99**, 102050. https://doi.org/10.1016/j.cose.2020.102050