一种弱中心化的银行可信数据管理方案 *

杨 城[a,b]，张 琰[a]

(西南财经大学 a. 经济信息工程学院; b. 中国区块链研究中心, 成都 611130)

摘 要：针对传统银行系统的中心化数据存储模式高效便捷但不透明，而新兴的去中心化的应用系统公开透明但共识机制低效的问题，提出了一种面向银行系统的总分双链的弱中心化可信数据管理方案。该模式的核心思想是应用区块链技术，打造彼此交叉且相互印证的总分双链的数据存储结构，并利用分户账回溯定位技术，结合大量轻客户端基于密码学技术的分布式监督，为个体提供交易验证的可能，从而实现数据的中心化可信存储与管理。它将中心化的数据存储与去中心化的数据验证相结合，从而兼有中心化管理的高效性和分布式机制的透明性，其本质上是一种民主监督下的中心模式，在满足银行独立完全掌控数据的同时，能够自证清白，并兼顾隐私与监督之间的平衡。

关键词：总分双链；弱中心化；区块链；默克尔树；可信银行

中图分类号：TP309.2 doi: 10.19734/j.issn.1001-3695.2020.02.0003

Trusted data management schema for semi-centralized digital banking system

Yang Cheng[a, b], Zhang Yan[a]

(*a. School of Economic Information Engineering*, *b. Blockchain Research Center*, *Southwestern University of Finance & Economics*, *Chengdu* 611130, *China*)

Abstract: Given the fact that the centralized data storage schema of traditional banking system is efficient but non-transparent, while the emerging decentralized data management system is transparent but inefficient in the consensus mechanism, this paper suggests a new trusted data management schema with a cross binary-chain for general ledger and subsidiary ledger in a semi-centralized architecture. The core idea of the new schema is to build a cross-chain for the transaction data with the blockchain technology, so as to realize centralized trusted storage and management of data by combining “the ledger backtracking location technology” and the distributed supervision of a large number of clients based on cryptography technology. Combining the centralized data storage mode and decentralized data validation method, it is both efficient and transparent. Essentially, the Cross Binary-Chain schema is a centralized approach based on distributed democratic supervision. Achieving the balance between privacy and supervision, it satisfies the need for banks to independently and completely control over the transaction data.

Key words: cross binary-chain; semi-centralized; blockchain; merkle tree; trusted bank

0 引言

传统银行体系一直采用“中心化”管理模式，该模式具备高效可控和管理便捷等优势，但近年来随着一些内部人作案和外部攻击事件的披露，中心化模式的弊端日益突显：中心集中存储所有的账户信息和交易信息，很容易成为黑客攻击的目标，造成巨大损失。更为重要的是，中心化管理缺乏透明性和可监督性，储户只能被动的完全信任银行，难以主动实施监督。银行拥有每一笔交易的记账权，具备伪造客户信息、窜改交易记录的能力。在特定情况下，存在中心作弊侵害储户利益的风险。

近年来，基于区块链技术的“去中心化”管理模式逐渐受到关注和热捧。建立在多方共同记账原理下的区块链技术，具备高安全性、公开透明、数据防窜改可追溯等优势[1~5]。但该技术目前仍处于初期，存在高耗低效、隐私泄露和责任主体缺失等问题[6~9]。此外，若采用该模式，银行将丧失系统的中心地位，政府更难以实施监管，无法保证金融体系的安全性和可控性。中国人民银行数字研究所的最新表态就明确指出“目前不建议基于区块链改造传统支付系统”[10]。目前，以“比特币”为代表的虚拟货币是区块链在金融应用中的典型代表，我国央行也正在研究自己的数字货币。但央行主导的数字货币是以国家信用作为背书，数据管理上仍然采用中心化模式，无法从本质上体现区块链多方信任的特点，进而无法充分发挥虚拟货币的业务优势。同时，它对现有银行体系的运作模式改动较大，建设成本和维护成本都将十分高昂。

有鉴于此，为了更好的满足银行业需求，提升银行公信力，本文结合现有银行系统的业务特点和区块链的技术优势，提出了一种新型的银行数据存储和管理方案，使其在保持集中高效、低成本运作的同时，兼备透明可监督的特点。

本文后续部分的结构如下：第二节整体性描述该新型数据管理方案的设计理念和核心思想；第三至五节阐述新方案的具体设计，包括账户管理和交易流程、分户账 Merkle 树及其回溯定位技术、总分十字双链的数据存储模式；第六节阐述个体储户如何进行分布式数据验证；最后是全文的总结，对新方案的优势和扩展应用进行归纳。

1 基于区块链思想的弱中心化方案

如何在新的技术形势下，打造高效便捷的可信数字银行是现代银行业面临的一个重大的技术问题。然而，在现有技术条件下，“高效便捷”与“可信”往往不可同时兼得。“高

收稿日期：2020-02-23；**修回日期：**2020-03-27 **基金项目：**教育部人文社科项目(17YJCZH210)；四川省高等教育人才培养质量和教学改革“互联网＋”创新创业项目(JG2018-281)

作者简介：杨城(1977-)，男，重庆人，副教授，博士，主要研究方向为区块链技术及应用、经济复杂系统仿真和数据分析与挖掘(mr.yangcheng@163.com)；张琰(1983)，男，成都人，博士研究生，主要研究方向为区块链技术及应用.

效便捷”意味着需要采用传统中心化的数据管理模式，由银行集中存储和维护所有的数据信息，而不能像比特币交易一样，交由去中心化的网络来分布式的验证和存储。“可信”则意味着必须从技术和制度上确保银行只能如实记账，而无法伪造或窜改交易记录，这就要求交易数据须公开透明、多方可验证，而不能采用黑箱式的封闭管理。

为此，本文设计了一种“写验分离”的“弱中心化”数据管理方案。该方案一方面保留银行在系统中的核心地位，它是所有交易的共同中介，也是系统唯一的记账人，集中存储全部的账务数据，是维持系统高效便捷运作的关键；另一方面所有储户都是体系的分布式监督人，他们手握基于区块链技术生成的公开验证数据，通过对个人分户账信息的直接验证，以及对银行总账数据的间接审计，实现在兼顾隐私条件下交易数据的透明性和可验证性，有效防止银行利用信息独占优势作假，使其成为真正可信任的数字银行。它将中心化的数据管理与分布式的、轻客户端的数据审计相结合，从而兼有中心化的高效便捷性与去中心化的安全透明性，它在本质上是一种民主监督下的中心化数据管理模式[11~13]。

显然，这里的关键是如何在中心化模式下确保银行“可信”。进一步，何为可信？本文认为它至少包含三个层次的真实可信。a)储户存取真实可信：没有授权，银行动不了储户的钱，即银行无法私自伪造储户的交易记录或窜改账户余额；b)转账交易真实可信：每一笔转账交易，转入转出都如实记录，银行无法记“单边账”(即只记录转出信息，漏记或错记转入信息)；c)整体账务真实可信：银行历史账户交易真实可信，即使与储户“串谋”，或者隐匿内部账户，银行也无法窜改或伪造过往交易记录。

针对以上三层“可信”，本方案从三个方面来共同营造中心化数据模式下的可信银行。首先，基于无 CA 机构的非对称加密账户管理机制，确保交易本身的真实性；其次，基于多级扩展的分户账体系，包括个体分户账树和系统分户账树，锁定所有个体交易历史，并应用账户回溯定位技术确保账户被冒用；最后，采用总分十字双链的块链存储模式锁定银行整体数据，并提供多维度的账务验证机制。

2　账户管理与交易流程

在现有银行体系中，目前普遍采用对称加密技术来保护账户安全和进行身份识别。这种技术虽然简单易行，但必须基于对银行的绝对信任。显然这与本文所提的“可信”银行相矛盾，因为银行可以利用手中的信息优势，任意伪造或窜改储户的交易记录。

因此，在本文提出的数字银行体系中，新方案采用非对称加密技术来识别储户身份和保障账户安全，即储户和银行各自拥有一套独立的公私钥，通过数字签名来进行身份认证、安全通信，以及确保信息的真实性和不可抵赖性。例如，储户通过数字签名来确保交易请求的真实性，银行通过数字签名来确保系统消息和交易回执的真实性。同时，类似比特币等虚拟数字货币体系的账户注册模式，新方案中没有所谓中心化的 CA 机构(即“证书授权中心”)。无论银行还是储户，所有的密钥对都由他们各自独立生成，并且独立保管私钥。同时，银行的公钥向所有储户公示，而储户在进行账户注册时完成其公钥与账号之间的映射绑定。无 CA 机构的非对称加密账户管理技术是实现可信数字银行的基础。

图 1 展示了一笔转账交易的完整流程。其中，交易请求 Req 中，V_A、V_B 分别表示转出方(Alice)和转入方(Bob)的账号，Amount 为转账金额，$Time_1$ 为请求时间，Memo 为备注信息，Sgn_A 为 Alice 私钥对该请求的签名，以确认请求真实性；转账回执 Rec 中(实线表示实时且必须)，$Time_2$ 为记账时间，$Balance_A$ 为交易完成后 Alice 的账户余额，Sgn_C 为银行私钥对该交易的签名，以确认交易合法性；转账通知 Msg 中的参数与 Rec 类似(虚线表示非实时非必要)。

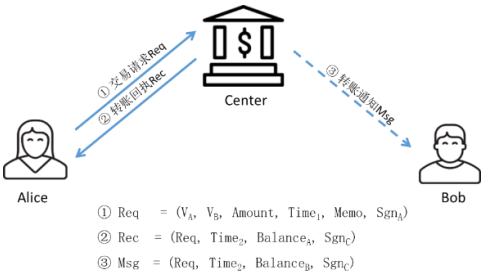

图 1　转账交易流程示意图

Fig. 1　The transfer transaction process based on asymmetric encryption

在图 1 中，Alice 基于自身私钥的数字签名确保银行无法伪造其账户的交易记录，从而实现了第一层“可信”。但由于 Bob 可能永远不上线，或者现实中永远联系不到 Bob(如收款人死亡或匿名捐款等)，Alice 无法获知资金是否真实转入目标账户，而“不诚信”的银行却可以利用自身的中心优势，伪造虚假的 Bob 账户信息来欺骗 Alice。因此，仅仅依靠非对称加密还无法实现第二层“可信”。

3　分户账 Merkle 树及其回溯定位技术

3.1　分户账树

为保障个人交易记录的真实性和完整性，防止银行窜改、伪造或遗漏交易记录，储户需要独立的数据结构来存储自身的历史交易信息，即“个体分户账”。个体分户账中记录的内容是经银行签名确认的交易信息，即图 1 中的 Rec 或 Msg，下文统称为 TX。

关于个体分户账的存储，传统的表格模式不仅数据存储量大，而且难以体现交易的完整性。形如递推公式的哈希链，如 $H_n=hash(H_{n-1}|TX_n)$，虽然通过哈希头能够锁定所有交易，但基于此结构的交易查询路径过长，并且在回溯过程中可能泄露储户隐私(如某个时间段的交易频次等)。因此，本文采用类 Merkle 树来存储个体分户账，即“个体分户账树”CLT(customer ledger tree)。

Merkle 树是一种哈希二叉树，它是一种用作快速归纳和校验大规模数据完整性的数据结构。构造一棵完整的 Merkle 树需要递归的对数据节点进行哈希运算，并将新生成的哈希节点插入到 Merkle 树中，直到只剩下一个哈希节点，该节点就是 Merkle 根。它提供了一种快速验证数据存在性的方法。当 N 个数据元素经过哈希计算并插入 Merkle 树时，任意一个满节点回溯至多 $\log_2(N)$个路径节点就能到达 Merkle 根，即至多经过 $\log_2(N)$次哈希计算就能检查出任意数据元素是否存在于该 Merkle 树，从而完成其存在性证明。

不同于常规的满二叉树，本方案的个体分户账树 CLT 采用多级可扩展的、逆向自生长的类 Merkle 树结构。图 2 展示了一棵 3 级-8 节点结构的 CLT 示例。如图所示，CLT 整体上是一颗不完全二叉树，但每一级都可单独视为一棵满二叉树。其中，#0 叶节点记录储户账号与其公钥之间的映射关系；黄色节点(无子节点，#1-#18)为交易叶节点，记录具体交易的散列值；棕色节点(#A 和#B)为准根节点，它们曾经是 CLT 的根节点，但随着自身交易量的增长，它们又陆续转变为上级二叉树的中间节点。根据自身的存储能力和查询需求，储户可以存储完整的 CLT，也可以仅存储上层新近部分的 CLT。这样的设计既能通过树根 root 锁住个体储户的所有历史交易，又能对新近交易的日常查询提供快速的回溯验证，同时满足不同储户对交易扩展的需求，并在回溯验证过程中最大限度的保护储户隐私。

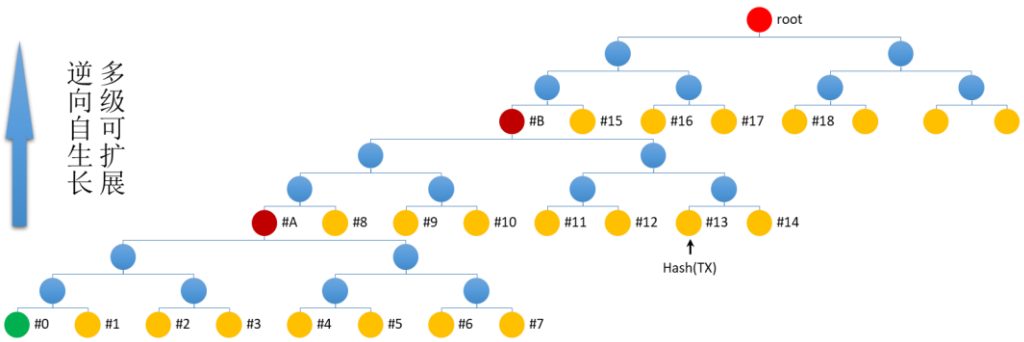

图 2　多级可扩展、逆向自生长的个体分户账树 CLT

Fig. 2　A CLT example with 3-layers and 8-nodes

在此基础上，本文进一步设计了如图 3 所示的“系统分户账树”SLT(system ledger tree)：所有个体分户账树的根节点有机的聚合在一起(如按开户时间的先后顺序排列)，构造一颗全体账户的 Merkle 树，每一个叶节点对应一个账户 CLT 的根节点，其根节点 SLT_ROOT 锁定全体储户的所有历史交易。

3.2　账户回溯定位技术

基于上述 CLT&SLT 设计，银行定期将 SLT_ROOT 对外公布(如每日更新)，每位储户都能够通过这两颗 Merkle 树来对自身交易的真实完整性进行验证。但由于信息的不对称性，作为数据中心的银行仍然存在记单边账的可能。即使图 1 中 Alice 要求协查相关转账交易在 Bob_CLT 中的记录，银行也可以提供虚假的 SLT 叶节点，用内部账户来冒充 Bob 的账户。因为 Alice 并不知道哪一个叶节点对应 Bob_CLT 的真实根节点。

如果每位储户的 CLT 根节点在 SLT 中的叶节点位置固定且公开，那么 Alice 就可以对 Bob 账户进行定点回溯验证，从而消除银行用虚假叶节点冒充的可能。因此，如何在验证过程中推导叶节点的位置，是协查验证的关键。很幸运，Merkle 树的回溯验证给本文提供了这种可能。

因为 Merkle 树的回溯路径具有唯一性，即每一个叶节点通过哈希迭代回溯到根节点的路径是唯一的，不同的叶节点对应着不同的回溯路径。因此，给定某个叶节点的回溯路径，就能计算出该叶节点在 Merkle 树中的位序号(“位序号”指的是叶节点在所属 Merkle 树中的位置顺序，即第几个叶节点。例如，在包含 2n 个叶节点的满二叉树中，叶节点的位序号依次为 i=0, 1, 2, …, 2n−1。)；反之，给出某个叶节点的位序号，也能计算出该叶节点的回溯路径。本文把这种基于 Merkle 树回溯路径的唯一性来定位叶节点位置的方法称为“回溯定位技术”。

这里所谓“回溯路径”指的是叶节点通过多轮哈希迭代回溯到 Merkle 树根节点的过程中，各哈希因子相互间的排列顺序，而与具体的散列值无关。具体地，叶节点的位序号与其回溯路径的关系为：将叶节点位序号转换为二进制，然后从右往左逆序排位，从第一个哈希因子(叶节点自身)开始，新的哈希因子逢 0 置后，逢 1 置前，通过多轮哈希迭代，最终回溯到 Merkle 树的根节点。这样得到的哈希因子序列就是该叶节点的回溯路径。

例如，图 3 所示的 SLT 是一棵包含 16 个叶节点的满二叉树，叶节点回溯到 SLT_ROOT 需要 4 次($\log_2 16$)哈希迭代。其中，r_i 既是位序号为 i(i=0..15)的账户 CLT 的根节点 $root_i$，同时也是 SLT 的第 i 个叶节点。令 x_j(j=1..4)为 r_i 回溯过程中的 4 个路径节点，虽然 x_j 的数值千变万化，但对同一个位序号 i 而言，每个 x_j 的位置是固定的，即 r_i 的哈希序列是不变的。以 r_5 为例，$5=(0101)_2$，它对应的哈希序列为($x_3x_1r_5x_2x_4$)，即由叶节点 r_5 回溯至根 ROOT 的哈希迭代顺序为

$$ROOT=hash(hash(x_3|hash(hash(x_1|r_5)|\ x_2))|x_4)$$

类似的，$11=(1011)_2$，r_{11} 对应的哈希序列为($x_4x_2x_1r_{11}x_3$)。

由此，本文在开户时为新账户分配固定不变的 SLT 叶节点位置，并参照公民身份证中个人地址码、生日等基本信息的编码模式，将该位序号直接编码写入储户的账号中。这样在转账时，Alice 知道 Bob 的账号，也就知道 Bob 的 CLT 根节点在 SLT 中的位置，因此能够对双方 CLT 中的相关交易数据进行验证(需要银行提供回溯路径中的若干 x_j)，通过自查与协查，确保转账交易被真实执行，从而实现第二层“可信”。

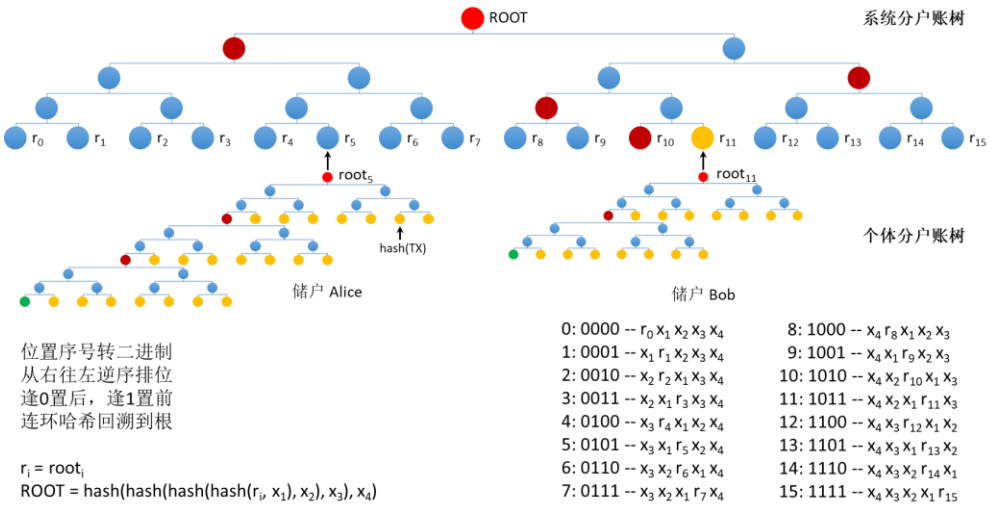

图 3　基于分户账树的账户回溯定位示意图

Fig. 3　Program of account backtracking location based on CLT & SLT

此外，这种定位技术具有良好的可扩展性，SLT 的生长并不影响原有账户叶节点 r_i 相对于先前 x_j 的顺序。即随着时间增长，银行规模扩大，更多的账户被创建，SLT 向右扩展，但并不影响扩展前的哈希序列，新路径仅将新的哈希因子放置于当前哈希序列的右边即可。同样以 r_5 和 r_{11} 为例，当图 3 中 SLT 的叶节点数由 16 扩展为 32 时，$5=(00101)_2$, r_5 对应的新哈希序列为$(x_3x_1r_5x_2x_4x_5)$；$11=(01011)_2$, r_{11} 对应的新哈希序列为$(x_4x_2x_1r_{11}x_3x_5)$。

4　总分十字双链

账户回溯定位技术保证了银行的转账交易真实可信，实现了第二层“可信”。但仅有可信的分户账体系，只能保证每一位个体储户的交易真实性，仍然无法保证银行整体账务信息的真实性，银行还可以通过隐藏的内部账户来窜改或伪造虚假的交易记录。因此，还需要引入总账体系与分户账体系交叉印证，并结合区块链技术来彻底锁死历史数据，从而实现第三层“可信”。

如图 4 所示，将交易时间周期性划分，单位时间片内的每一个账户视为一个节点 V_i，交易网内的每一个箭头都对应一笔转账交易，箭头始端为转出方，末端为转入方。横向实线代表不同节点间的资金流向，纵向虚线代表同一个节点内的余额流向。如此，全部历史交易构成了一张纵横交织的交易网，横向对应总账体系，纵向对应分户账体系，二者分别从不同维度锁定历史——前者从整体维度锁定银行每一期的所有交易，后者从个体维度锁定每一位储户的全部交易历史——并通过具体交易信息相互印证。[14]

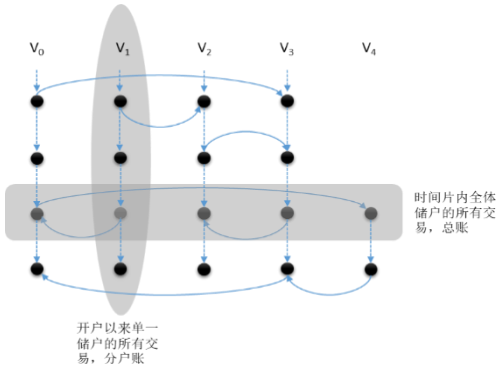

图 4　纵横交织的交易网

Fig. 4　A crossover network of transaction

具体而言，为了与银行现行“日记账”体系对应，本文按天划定交易周期，将每天的账务信息(总账和分户账)用块链结构存储，所有区块利用哈希函数前后迭代，构成交易链，锁定全部历史交易。形式上虽然只有一条物理交易链，但实际存在总账链和分户账链两条逻辑链，二者相互交织，彼此验证，为银行的第三“可信”提供可靠保障。因此，本文把这条交易链称为“总分十字双链”CBC(cross binary-chain)。通过对 CBC 的“块头链”(由 CBC 所有区块的区块头构成的数据链)的分布式存储和验证，所有储户实现了对中心银行的监督，进而对交易数据的真实性达成共识。

图 5 展示了 CBC 交易链的详细结构图，其中上半部分为数据链的整体结构，下半部分为每个区块对应的核心存储结构——当期的总账树和分户账树。

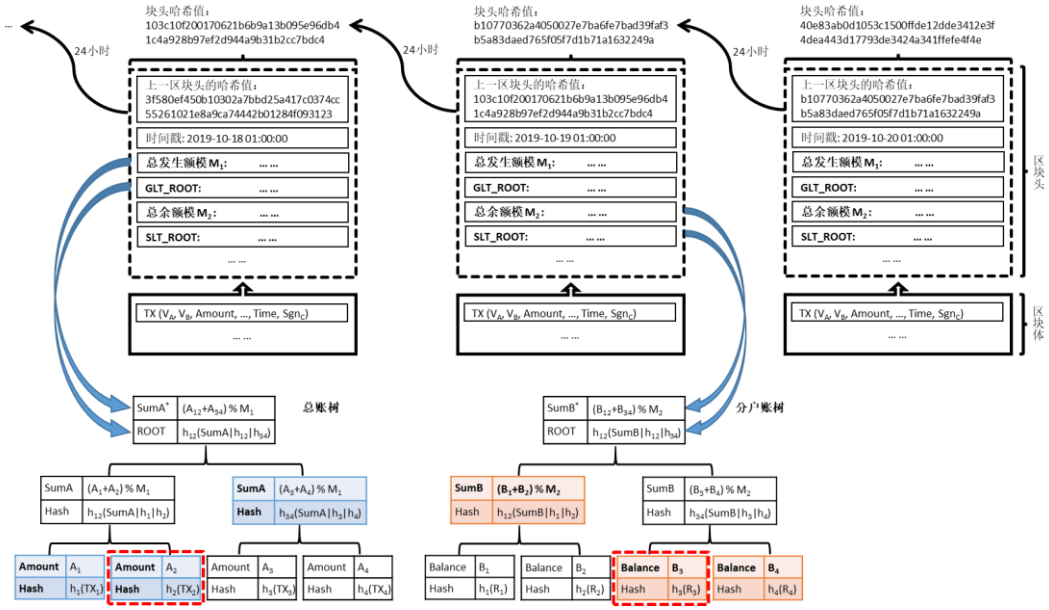

图 5　总分双链的详细结构图

Fig. 5　The structure diagram of cross binary-chain

a)CBC 由若干区块按时序前后衔接构成，每个区块包括区块头和区块体两部分。区块体储存当期的交易明细，区块头存储该区块的摘要信息，如时间戳、总账树和分户账树的 Merkle 根、父区块头的散列值等，以及两个锁定银行整体数值特性的模余——当期总发生额模 M_1 的余数和账户总余额模 M_2 的余数(M_1、M_2 是两个公开整数，M_1 大于单笔交易最大限额但远小于每日交易总额，M_2 大于单账户余额但远小于银行账户总余额。)。

b)总账树 GLT(general ledger tree)是一颗扩展的默克尔树，每个叶节点对应当期的一笔交易 TX，存储的信息包括该交易的散列值 Hash(TX)和发生额 Amount。[15, 16]除了像传统默克尔树对散列值层层迭代外，每个节点的 SumA 字段等于其最相近的两个子节点的发生额之和模 M_1。这样，其根节点的 ROOT 字段锁定了当期的所有交易，同时 SumA*字段等于当期的总发生额模 M_1。

c)分户账树是基于前文系统分户账树 SLT 的扩展，每个叶节点对应一位个体储户的分户账信息，包括 CLT 的根节点和账户余额 Balance。与 GLT 类似，每个节点的 SumB 字段等于其最相近的两个子节点的余额之和模 M_2。这样，其根节点的 ROOT 字段锁定了当期末所有储户的个体分户账，同时 SumB*字段等于当期的总余额模 M_2。这样的设计既保留了可验证的数值特征，又有效的保护了银行的商业隐私。

5　分布式验证

在数据的存储设计上，银行作为系统的中心，存储全部

数据，包括所有的交易流水、分户账信息和完整的 CBC 交易链数据等。由于存储空间和计算能力的限制，以及对隐私安全的考虑，个体仅存储 CBC 的“块头链”和自身(部分的)CLT。

基于上述交易链设计和数据存储机制，每一位储户都可以在日常的交易查询中，对自身交易记录和账户信息进行主动审计，而不再只是被动的信任银行。具体而言，个体对交易真实性的主动审计包括三方面的验证，不仅查验自身的交易数据，还要协助查验交易对手的相关数据，以及验证整体的数值特征。

a)自身真实性验证：自身 CLT 的根值是否与最新区块中 SLT_ROOT 锁定的该账户叶节点的 r 值相等;待查验交易是否同时包含于自身 CLT 和对应区块的 GLT 之中。[15]

b)对手真实性验证：交易对手 CLT 的根值是否与账户回溯定位计算出的 SLT 叶节点 r 值相等;待查验交易是否同样包含于对手的 CLT 之中。

c)整体真实性验证：回溯过程中，GLT_SumA*是否等于对应区块头的总发生额的模余；SLT_SumB*是否等于总余额的模余[16]。

需要说明的是，储户在进行交易查询前，需要先与银行进行数据同步，包括更新 CBC 的块头链和自身 CLT，并对更新数据的延续性进行验证，即新数据必须能够以先前存储的旧数据为基础，通过合理的迭代推导出来。此外，交易查询中，银行不仅需要提供账户余额、交易明细等常规的基本账务信息，还需要提供相关交易及分户账对应的 Merkle 回溯路径作为辅助验证信息，以证明这些数据包含于对应的 Merkle 树。

从上述查验过程不难看出，本方案是一种分布式的、轻客户端的高效数据验证体系，大量分散的个体储户在对自身进行直接查验的同时，通过总分十字双链对数据存在性、完整性和数值关系的交叉验证，间接实现了对银行整体交易信息和账务数据的审计，从而大大降低了银行窜改数据、伪造交易、记单边账和隐匿交易记录的可能，大大提升了银行的公信力。

由此可见，相对于基于区块链技术引入全新的数字货币，本方案对银行体系的改造规模和成本都要小得多。更重要的是，对储户而言，所有验证操作都在客户后端自动“隐蔽”完成，前端的日常操作与当前并无二样，不会给储户造成新的负担。

6　结束语

本文结合现有银行系统的中心化数据存储模式与基于区块链思想的分户账数据验证机制，实现了一种面向数字银行的弱中心化可信数据管理方案的创新：应用区块链技术，打造彼此交叉且相互印证的总分双链的数据存储结构，在分户账回溯定位技术的基础上，结合大量轻客户端基于密码学技术的分布式监督，有效防范中心利用信息独占优势作假，从而实现数据的中心化可信存储与管理。它在数据管理模式上为银行系统提供了一种区别于区块链全分布式管理和传统集中式管理之外的第三条路径——“弱中心化”模式，一方面保证数据公开透明，具有区块链的不可窜改性和可追溯性特征，为个体储户提供了交易验证的可能，也为银行提供了自证清白的手段；另一方面数据集中存储，系统保持高效便捷的同时，满足了银行自己掌控数据，保护银行及储户账务隐私的需求。

在实践中，本文基于本文的思想申请了两份技术专利：“数字银行的总分双链的弱中心化可信数据管理系统及方法”(专利号：201811306195.7)；“基于 Merkle 树回溯定位技术的转账系统、查验方法及交易方法”(专利号：201910133066.0)。并且，在 2019 年第十五届“花旗杯”金融创新应用大赛中，以本方案设计的原型系统“CitiCoin 基于弱中心化的可信银行系统”获得全国二等奖。原上海证券交易所总工程师、区块链专家百硕评价该项目：“为区块链技术如何落地另辟蹊径，为银行如何在保持数据中心化的前提下，服务数据可信提供了新的思路。”

最后，本文的弱中心化方案并不局限于在银行系统的应用，而是一种全新的可信数据验证技术和基于这种验证技术的数据管理方案，具有广泛的应用前景，其上可存储电子凭证、财务数据、交易信息等众多的数字化信息，例如中央银行对数字货币的管理，商业银行对数字现金的管理，虚拟货币交易所对交易记录的管理等，用于打造一款应用广泛的、可信任的“数据银行”，成为未来数字普惠金融的重要基础设施。

参考文献：

[1] Binanda S, Samiran B, Sushmita R, *et al.* Retricoin: Bitcoin based on compact proofs of retrievability [C]. Proceedings of the 17th International Conference on Distributed Computing and Networking. New York: ACM, 2016, 14: 1-10.

[2] Juels A, Kaliski B S. PORs: Proofs of retrievability for large files [C]. Proceedings of ACM Conference on Computer and Communications Security. New York: ACM, 2007: 584-597.

[3] Andrew M, Ari J, Elaine S, *et al.* Permacoin: Repurposing Bitcoin Work for Data Preservation [C]. Proceedings of IEEE Symposium on Security and Privacy. Washington D C IEEE, 2014: 475-490.

[4] Walsh K. 'Blockchain'Increases Online Trust: New Technology Could Bolster Digital Badges and E-Portfolios, among Other Innovations [J]. University Business, 2017, 20 (2): 24.

[5] Zheng Zibin, Xie Shaoan, Dai Hongning, *et al.* Blockchain challenges and opportunities: a survey [J]. International Journal of Web and Grid Services, 2018, 14 (4): 352-375.

[6] David S. Understanding the DAO Attack [EB/OL]. https://www. coindesk. com/understanding-dao-hack-journalists/, 2016. 6.

[7] Pete R. Split or No Split?Bitcoin Miners See No Certainty in Segwit2x Fork [EB/OL]. https://www. coindesk. com/split-no-split-bitcoin-miners-see-no-certainty-segwit2x-fork/, 2017. 11.

[8] Xiwei X, Cesare P, Liming Z, *et al.* The Blockchain as a Software Connector [J]. Software Architecture, 2016: 182-191.

[9] Roman B, Michel A, Matti R, *et al.* Blockchain Technology in Business and Information Systems Research [J]. Business & Information Systems Engineering, 2017, 59 (6): 381-384.

[10] 中国人民银行数字货币研究所区块链课题组. 区块链技术的发展与管理 [J]. 中国金融, 2020. 4: 28-29. (Blockchain research group of digital currency research institute of People's Bank of China. Development and management of block chain technology [J]. China Finance, 2020. 4: 28-29.)

[11] Faber B, Michelet G C, Weidmann N, *et al.* BPDIMS: A blockchain-based personal data and identity management system [C]// Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019.

[12] Zhu Liehuang, Wu Yulu, Gai Keke, *et al.* Controllable and trustworthy blockchain-based cloud data management [J]. Future Generation Computer Systems, 2019, 91: 527-535.

[13] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data [C]// 2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

[14] Ren Z, Cong K, Aerts T V, *et al.* A Scale-out Blockchain for Value Transfer with Spontaneous Sharding. ARXIV PREPRINT ARXIV: 1801. 02531, 2018.

[15] Andreas M A. Mastering Bitcoin [M]. O'Reilly Media, 2014. 12.

[16] Dagher G G, Bonneau J, Clark J, *et al.* Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges [C] , 2015: 720-731.