DOI:10.13718/j.cnki.xsxb.2021.05.018

可信区块链数字货币基础架构中的共识与信任①

林　勇[1]，　杨俊康[2]，　徐雨滴[3]，　徐　青[3]

1. 重庆邮电大学 基建后勤管理处，重庆 400065；2. 重庆邮电大学 通信学院，重庆 400065；
3. 重庆邮电大学 经济管理学院，重庆 400065

摘要：数字货币作为一种全程可追溯的货币在金融监管领域具有其他法定货币难以比拟的优势. 针对传统架构无法支撑数字货币巨量分布式应用，而经典区块链架构无法满足金融监管与金融安全的问题，本文提出一种基于可信区块链和边缘计算的数字货币基础架构. 在该架构中提出一种高效共识管理协议，基于该协议及配套策略构建了可信的区块链结构，并基于智能合约概念引入分散交换机制，以便在垂直层之间进行协商，允许垂直服务与水平服务并行，促进基于边缘计算的智能解决方案的实现. 该架构可克服传统区块链架构的不足，成为支持数字货币的基础架构，并可在多个互联网经济应用中起到支撑作用.

关　键　词：数字货币；区块链；信任机制；互联网经济

中图分类号：TP311　　**文献标志码**：A　　**文章编号**：1000－5471(2021)05－0121－06

数字货币的诞生和流行，是人类进入数字化时代的必然历史进程，符合货币发展的历史规律，有研究人员称其为继商品货币体系、信用货币体系之后，人类货币体系的第三次革命[1]. 然而，当前流行的数字货币如比特币、莱特币等基于完全去中心化、去监管的区块链架构，不符合主权国家对法定货币监管和金融市场安全的要求，长期放任将削弱甚至颠覆政府对经济活动的控制能力[2]. “堵”则违背货币发展规律，“放”则危害主权国家的金融监管体系，这是各国政府在数字货币发展中面临的两难境地.

实际上，各国政府在数字货币应用中面临的困境，也是很多区块链应用场景中存在的困境. 如何在享受去中心化所带来的开放性、容错性、对抗攻击等红利的基础上，克服这种去中心化结构固有的缺陷是众多学者研究的课题. 这些缺陷包括缺少可监管性、隐私安全性和大数据存储等方面的不足[3]. 其中，区块链在可监管性方面的缺陷是妨碍其成为主权数字货币核心架构的关键问题[4]；区块链的分布式账本可由各参与节点公开维护，结点的加入和退出都不需要身份验证，从而导致恶意节点截取记账信息并作恶的可能性；区块链的去中心化也使得巨量交易数据难以存储于某一数据中心，从而难以实现数据驱动的人工智能，如基于交易数据的分类、预测与推荐等[5]. 以上这些问题，不仅在主权数字货币领域制约区块链技术的应用，也在一般数字货币领域及其他多个领域制约区块链技术应用.

以上问题吸引了区块链研究领域大批学者的关注，不少学者从不同角度出发研究这些问题，给出了自己的解决方案. 张健毅等[6]提出一种采用双链结构的可监管数字货币模型，通过投票完成对交易内容的解密，从而实现可控的匿名性，并通过基于信用的拜占庭容错机制和简化的一致性协议实现高效的共识. Henry 等[7]证明了利用 Tor 等匿名通信网络技术的区块链并不能保证用户的隐私性. Gai 等[8]提出一种面向联盟区块链的方法，在不限制交易功能的情况下解决隐私泄露问题，该方法主要适用于能源互联网领域

① 收稿日期：2020－10－31
基金项目：重庆市社会科学规划办公室重点项目(2019ZDZT08).
作者简介：林　勇，管理 7 级，主要从事经济管理研究.

的交易隐私保护. 针对区块链中的数据挖掘与隐私问题，Lu 等[9]提出一种区块链授权的安全数据共享架构，将数据共享问题转化为一个机器学习问题，实现合并隐私保护的联邦学习，将联邦学习整合到许可区块链的共识过程中，使得共识的计算工作也可以用于联盟训练. Pu 等[10]提出一种车辆社交网络(Vehicular Social Networks，VSN)的隐私安全与监控方法，该方法采用假名机制，通过隐藏车辆的身份来实现个人匿名，鼓励车辆报告可信信息，提出了激励惩罚机制，此外该方法还提出了基于多因素和单因素权重的评估机制来评估消息的可靠性，并采用实用拜占庭容错技术(Practical Byzantine Fault Tolerance，PBFT)和区块链分别实现共识和存储记录，防止恶意实体操纵车辆的奖励分数和信用分数. 针对区块链数据分散所导致的数据挖掘困难，Liu 等[11]提出一种支持移动边缘计算(Mobile Edge Computing，MEC)的无线区块链框架，其中计算密集型的挖掘任务可以卸载到附近的边缘计算节点，块的加密哈希可以缓存在 MEC 服务器中，从而克服了数据分析对结点计算和存储能力要求高的问题.

以上研究为解决区块链应用于数字货币等场景时的监管性问题、隐私性问题和智能性问题提供了参考，然而，这些研究或者局限于某一特定领域，或者局限于某一特定问题，使其应用效果受限. 本文提出一种基于可信区块链的边缘计算架构，综合性地解决上述问题，为数字货币和各种领域的区块链应用奠定基础.

1 区块链与信任

1.1 区块链

区块链技术由于其分布式和不可篡改的数据存储机制，使其成为近年来研究的热点之一，应用范围广阔. 区块链基本上可以看作是一个链状的数据结构，其中每一个区块的链通过基于哈希值的地址指针相互连接，即区块链是一个共享的、分散的、分布式的状态机. 这意味着所有节点都独立地持有自己的区块链副本，当前已知的“状态”是按每个交易在区块链中出现的顺序进行处理来计算的. 区块链的每个区块通常包含 6 个部分：父区块的哈希、nonce 值、当前区块的哈希、Merkle root、时间戳和交易数据.

根据具体需求，区块链的结构可以更加中心化或者更加去中心化，私链体系结构更中心化，因为它们由一个中央结点控制，联盟链由一组选定的结点而不是由一个特定的结点控制，可以看作弱中心化或多中心化[12]. 显然，从监管与安全的角度，私链和联盟链更适合数字货币应用.

1.2 区块链中的信任

信任度量是建立可信区块链的关键问题，根据以往的研究工作，可按照 3 种信任度量来识别、评估和创建区块链系统中各对象之间的信任关系，即知识、经验和声誉[13-15]. 每个信任度量是信任属性的集合表示，每个信任属性表示受信者的可信特性. 每种信任测度由多个信任属性集合而成，而知识、经验和声誉这 3 个信任特性的累加将得到最终的信任值. 信任评估的第一步是根据应用程序估计相关的信任测度. 信任测度的信息并不容易获得，但定义这些信任测度的属性是可获得的. 多种方法可用来估计测度属性值，如数值方法、概率方法、信念理论方法和机器学习方法. 简单地说，找到信任属性值 $\mathrm{trustor}_i$(信任者) 和 $\mathrm{trustee}_j$(被信者) 可以如式(1) 所示.

$$\begin{aligned} K_{ij} &= \alpha_1 K_1 + \alpha_2 K_2 + \cdots + \alpha_n K_n \\ E_{ij} &= \beta_1 E_1 + \beta_2 E_2 + \cdots + \beta_n E_n \\ R_{ij} &= \gamma_1 R_1 + \gamma_2 R_2 + \cdots + \gamma_n R_n \\ Trist_{ij} &= \theta_1 K_{ij} + \theta_2 E_{ij} + \cdots + \theta_n R_{ij} \end{aligned} \tag{1}$$

式(1) 中 α,β,γ 和 θ 是将测度标准化到(0，1) 区间的加权因子，K_{ij}，E_{ij} 和 R_{ij} 分别表示信任测度中的知识、经验和声誉，Trust_{ij} 代表对象 i，j 之间的信任值.

2 可信区块链架构

为了解决传统区块链网络中与隐私相关的问题，本文采用许可区块链的概念来设计可信链平台，因为

它允许产品使用者通过访问控制和共识机制来控制数据的可见性. 此外，智能合约的使用使决策支持系统、分布式控制系统和数据处理系统能够通过控制语言来实施和协商最终数据使用协议的统一规则. 从本质上讲，信任服务是各种信任评估模型和管理功能的结果. 值得注意的是，只有代表特定情况特征的信任属性彼此不同时，式(1) 才能代表建立信任服务所需的信任测度 / 信任属性分割、评估和聚合的整个过程. 例如，基于实体特性、数据完整性和相关隐私要求等的信任属性.

2.1　基于信任的共识管理协议

本文提出的算法记作信任证明(Proof-ofTrust，PoT). 在 PoT 方法中，选择一组具有较高可信度的结点作为控制属性，被选为可信链网络中的结点称为可信结点. 在基于拜占庭容错方法的启发下，本文在可信链网络中使用了一个基于信任服务的投票系统来进行共识挖掘. 然而，可信链网络中可信结点的选择不受中心机构的控制，允许任何具有足够可信度的节点被选为可信结点. 在可信链中，每个可信结点使用信任服务组件下提供的信任管理服务来决定他们信任的其他可信结点. 在可信链技术的全局可信链网络中，没有任何一方可以拥有 51% 的全局可信网络，因为可信结点的选择基于可信度，而不是计算能力、权威和财富等因素. 此外，可以选择少数值得信赖的权威机构(如政府控制机构)作为可信结点，以克服任何脱节，在此需要假设其继承的可信度. 本文按照式(1) 计算信任测度和声誉测度. 然而，代表知识的测度需要重新定义，将信任属性定义为社会属性，如托管、协作、合作性、频率、互动长度、相互性、中心性和利益共同体，有助于了解可信结点过去在维护可信链网络道德标准方面的表现. 在以往的文献中有许多模型来量化可靠性属性，本文在文献[14] 的基础上建立信任度量模型. 实体信任包含两个属性，分别考虑了实体的社会因素和非社会因素，每个属性又包含 5 个子属性. 而数据信任和隐私信任直接由属性构成. 一旦计算出社会属性和依赖性，知识测度的累积分值可计算如式(2). 此外，每个候选可信结点的信任值可以建模为式(3).

$$K_{ij}(t) = \rho . K_{ij}^{social} + \sigma . K_{ij}^{Denpence} \tag{2}$$

$$Trust_{Node} = \alpha . K_{Node} + \beta . E_{Node} + \gamma R_{Node} \tag{3}$$

式(3) 中 $Turst_{Node}$ 表示可信结点的可信赖值，K_{Node}，E_{Node} 和 R_{Node} 表示基于知识、经验与声誉的信任测度. 根据可信结点的信任值，选择可信度最高的一个作为特定结点池的领导者，并把该领导者的数字签名广播给池中的其他结点. 当接收到来自领导者的签名时，其他结点可以验证它，然后用自己的签名确认它. 领导结点主要负责管理协商一致过程，直到其任期结束. 一旦一个领导者的任期已经结束，必须根据结点的最高可信度值来选择一个新的领导者. 当一个领导结点当选后，它会选择一个副手候选人的名单，这就是验证过程. 为了选择这样的可信结点候选列表，领导者可信结点评估与其他潜在候选结点的信任关系，并选择与其信任关系最高的结点. 然后，领导者可信结点将该列表发送给其他结点，交叉检查它们与所选可信结点列表的关系. 一旦确定了前序和候选可信结点列表，结点可以启动事务并向可信结点池广播消息，其签名可以通过对消息及密钥的哈希生成，如式(4) 所示.

$$sign(Message, SK) = Signature \tag{4}$$

与传统的加密机制相比，消息生成器可以自由地使用适当的加密机制加密消息或根据隐私要求匿名化区块链. 当可信结点接受这些块时，可利用式(5) 所示的验证函数和公钥来验证消息.

$$verify(Message, Signature, PK) = True/False \tag{5}$$

式(4)、式(5) 中 SK 和 PK 分别为密钥与公钥.

2.2　智能合约服务

在可信区块链服务中，智能合约存储在单独的链中，以提高创建、存储、执行和终止等相关流程的效率. 智能合约服务中的注册中心组件基本上通过发出地址、名称和版本来注册新部署的合约，并通过存储结果的哈希值帮助跟踪合同的结果. 合约中的安全容器包括一个安全的操作系统、智能合约语言、运行环境和一个软件开发工具包，用于在信任链服务中创建和运行智能合约. 假设在某示例应用场景中，利益相关者将商品交换为加密货币，在正常情况下卖方必须在收到货物后立即装运来自交易记录客户的货物，如果卖家故意拖延发货，则会触发智能合约，退款到客户账户. 然而，从客户的角度来看，这个过程可能会涉

及一些额外费用和操作. 为了避免这种结果，在建立智能合约之前，可以使用信任服务来评估潜在卖家的可信度，并推荐合适的利益相关者.

假设用户 Alice(记作 a) 要找到一个好的银行家，Bob(记作 b) 声称需要建立一个智能合约来实现他们之间的交互. 为了一般性，本文取任何结点 a 和 b 之间的信任级别，关于 a 的偏好由 $Trust_{ab}$ 表示，a,b 之间的信任级别可根据式(6) 计算.

$$Trust_{ab} = \alpha \cdot E_{ab} + \beta \cdot R_{ab} \tag{6}$$

式(6) 中 E_{ab} 表示 a 与 b 之间的经验，R_{ab} 为 b 的声誉，α 和 β 依然是标准化因子. 在这里本文省去了知识测度，这是由于它需要个人信息来评估基于知识的信任. 设结点 x 第 j 个交易的信任属性评估为 $v_x(j)$，该交易的成功性为 $a_x(j)$，当前时刻与写操作交易时刻之间的时间衰减函数为 $t_x(i,\Delta t)$，则 a 与 b 之间的经验度量可根据式(7) 计算.

$$E_{ab} = \boldsymbol{T}_{ab}^{H} \cdot E_b = \boldsymbol{T}_{ab}^{H} \cdot \frac{\sum_{j=1}^{m} v_b(j) a_b(j) t_b(j,\Delta t)}{\sum_{j=1}^{m} a_b(j) t_b(j,\Delta t)} \tag{7}$$

式(7) 中 H 表示到达可信结点 b 的跳数，$\boldsymbol{T}_{ab}^{H}$ 代表 a 和 b 的转移矩阵，它在(a,b) 处的值表示 a 与 b 之间的连接，任意结点的 $t_x(i,\Delta t)$ 可根据式(8) 计算.

$$t_x(j,\Delta t) = \begin{cases} 1 & \Delta t < \alpha \\ \mathrm{e}^{-\Delta t} & \alpha < \Delta t < \beta \\ 0 & \beta < \Delta t \end{cases} \tag{8}$$

式(8) 中 α 和 β 表示调整交易相对于当前时间重要性的阈值，b 的声誉测度可根据式(9) 计算.

$$R_{ab} = \sum_{n=1}^{N=6} \boldsymbol{T}_{ab}^{n} d(n) \cdot R_b = \sum_{n=1}^{N=6} \boldsymbol{T}_{ab}^{n} d(n) \cdot \frac{\sum_{j=1}^{m} v_n(j) a_n(j) t_n(j,\Delta t)}{\sum_{j=1}^{m} a_n(j) t_n(j,\Delta t)} \tag{9}$$

如式(9) 所示，根据小世界理论，结点 b 的跳数被限制为 6. 此外，$d(n)$ 表示声誉作用随距离结点 n 的跳衰减，如式(10) 所示.

$$d(n) = \frac{7-n}{6} \tag{10}$$

将式(7) 和式(9) 代入式(6)，可得结点 b 相对于 a 的最终信任分数，如式(11) 所示.

$$Trust_{ab} = \alpha \cdot \boldsymbol{T}_{ab}^{H} \cdot \frac{\sum_{j=1}^{m} v_b(j) a_b(j) t_b(j,\Delta t)}{\sum_{j=1}^{m} a_b(j) t_b(j,\Delta t)} + \beta \cdot \sum_{n=1}^{N=6} \boldsymbol{T}_{ab}^{n} d(n) \cdot \frac{\sum_{j=1}^{m} v_n(j) a_n(j) t_n(j,\Delta t)}{\sum_{j=1}^{m} a_n(j) t_n(j,\Delta t)} \tag{11}$$

此外，本文使用零知识证明(Zero Knowledge Proof，ZKP) 的概念来隐藏通过智能合约与服务提供商交互时的用户信息. 假设属于 Alice 的结点需要从 Bob 处检索机密文档，为此 Alice 需要向 Bob 提供她的姓名、出生日期等信息来证明自己的身份. 但是，如果她提供了这些信息，Bob 可以将这些数据用于其他目的，比如用户分析，或者与第三方共享这些数据以获得非法利益. 为了避免 ZKP 用来证明 Alice 的身份而不必向她发送真实的信息，本文提出一种新的密钥隐藏方法，并将其与智能密钥交换算法相结合，这种新的密钥隐藏算法 Alice 和 Bob 只共享 p,g 以及他们的公钥(k_1,k_2)，窃听者不可能在不知道 Alice 和 Bob 密钥的情况下干扰识别过程. 此外，两个散列函数 C 和 C' 中的内容必须相似，才能满足条件 $C = C'$. 因此，本质上 Alices 的承诺 t 必须等于 t'，如式(12) 所示.

$$\begin{aligned} t' &= g^{r} \cdot k_1^{C} + k_2^{r} \cdot s_k^{C} = \\ & g^{(v \cdot x - C \cdot x)} \cdot (g^{x})^{C} + (g^{y})^{(v \cdot x - C \cdot x)} \cdot (g^{xy})^{C} = \\ & g^{(v \cdot x)} + g^{(v \cdot x \cdot y)} = k_1^{v} + s_k^{v} = t \end{aligned} \tag{12}$$

3 融合边缘计算的可信区块链

电子货币的支付系统和物联网系统代表从小型设备或传感器数据到大规模复杂数据中心的结点. 在边

缘计算设置中，这些小型设备一般位于层次结构的底部，具有相对较高处理能力和存储能力的结点位于网络的中间，而大型数据中心则代表云层的结点[16]. 由于执行共识算法的相关资源限制及存储大量公共账本的有限存储，在层次结构末端实施传统区块链技术具有挑战性. 相比之下，信任链中的一致性协议只是信任和拜占庭容错的结合，能够广播一组消息的计算能力足以实现一致性算法. 因此，信任链可以很容易地部署到边缘计算层次结构的末端.

本文建议使用区块链智能合约来实现奖惩模型、结点绩效历史数据、平台预定义的管理规则和协作标准，降低集中平台带来的风险；本文还建议使用多个移动边缘计算的边缘服务器作为区块链主节点来托管和运行智能合约，从而缓解网络拥塞. 在此可分为两个步骤：①利益相关者之间的新活动将被记录下来，并以固定的间隔打包到新创建的数据块中. 一个新的块有一个指向其前一个块的唯一哈希值的指针，所有的块形成一个链，也就是区块链. 当预设条件满足时，商定的步骤将自动进行. 这样，一个集中的群智能生态系统就变成了一个在区块链网络上运行的去中心化的生态系统，它可以获得所有利益相关者的信任. ②区块链的一致性算法设计为依赖于一定范围的内存和带宽，这限制了边缘服务器或边缘网络上某些其他计算设备上的相应挖掘硬件. 这种设计可以使生态系统分布更广，适合移动边缘计算. 这些硬件存储着区块链的精确副本，本文称之为主节点. 为了减轻带宽负担和响应延迟，最近的边缘服务器/主结点能够代替远端云作为中间结点和第三方保证，在工作者和发布者之间进行原始数据传输. 由于边缘服务器/主结点比远端云更接近数据发布者，因此可以帮助他们在边缘网络上对任务数据进行预处理，这可以进一步缓解网络拥塞，提高系统对大量任务的响应能力.

4　结　　语

针对传统区块链存在的监管问题、隐私问题和数据集中的高开销问题，本文提出一种基于轻量级共识管理协议的可信区块链架构，可监管、可保证隐私性并提供了边缘数据挖掘的能力，不仅可以成为主权数字货币的基础架构，也可以成为其他各种注重隐私性、监控性和智能性的分布式应用的基础架构.

参考文献：

[1] WALDO J. A Hitchhiker's Guide to the Blockchain Universe [J]. Communications of the ACM, 2019, 62(3): 38-42.

[2] 丁晓蔚，苏新宁. 基于区块链可信大数据人工智能的金融安全情报分析 [J]. 情报学报，2019，38(12)：1297-1309.

[3] 蔡晓晴，邓　尧，张　亮，等. 区块链原理及其核心技术 [J]. 计算机学报，2021，44(1)：84-131.

[4] HAN X, YUAN Y, WANG F Y. A Blockchain-Based Framework for Central Bank Digital Currency [C]//2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). Zhengzhou: IEEE, 2019.

[5] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for Internet of Things: a Survey [J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[6] 张健毅，王志强，徐治理，等. 基于区块链的可监管数字货币模型 [J]. 计算机研究与发展，2018，55(10)：2219-2232.

[7] HENRY R, HERZBERG A, KATE A. Blockchain Access Privacy: Challenges and Directions [J]. IEEE Security & Privacy, 2018, 16(4): 38-45.

[8] GAI K K, WU Y L, ZHU L H, et al. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid [J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3548-3558.

[9] LU Y L, HUANG X H, DAI Y Y, et al. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT [J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4177-4186.

[10] PU Y W, XIANG T, HU C Q, et al. An Efficient Blockchain-Based Privacy Preserving Scheme for Vehicular Social Networks [J]. Information Sciences, 2020, 540: 308-324.

[11] LIU M T, YU F R, TENG Y L, et al. Computation Offloading and Content Caching in Wireless Blockchain Networks with Mobile Edge Computing [J]. IEEE Transactions on Vehicular Technology, 2018, 67(11): 11008-11021.

[12] 薛腾飞，傅群超，王　枞，等. 基于区块链的医疗数据共享模型研究 [J]. 自动化学报，2017，43(9)：1555-1562.

[13] JAYASINGHE U, LEE G M, MACDERMOTT A. Trust-Based Data Controller for Personal Information Management [C]//

2018 International Conference on Innovations in Information Technology (IIT). Al Ain: IEEE, 2018.

[14] JAYASINGHE U, LEE G M, UM T W, et al. Machine Learning Based Trust Computational Model for IoT Services [J]. IEEE Transactions on Sustainable Computing, 2019, 4(1): 39-52.

[15] PAN X F, PAN X Y, SONG M L, et al. Blockchain Technology and Enterprise Operational Capabilities: an Empirical Test [J]. International Journal of Information Management, 2020, 52: 1-9.

[16] LIU S W, WU J, LONG C N. IoT Meets Blockchain: Parallel Distributed Architecture for Data Storage and Sharing [C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018.

Consensus and Trust in Trusted Blockchain Digital Currency Infrastructure

LIN Yong[1], YANG Jun-kang[2], XU Yu-di[3], XU Qing[3]

1. *Infrastructure and Logistics Management Office, Chongqing University of Posts and Telecommunications, Chongqing 400065, China;*
2. *School of Communication, Chongqing University of Posts and Telecommunications, Chongqing 400065, China;*
3. *School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Abstract: As a full traceable currency, digital currency has incomparable advantages in the field of financial supervision. Aiming at the problem that the traditional architecture cannot support the massive distributed application of digital currency, while the classic blockchain architecture cannot meet the financial supervision and financial security, a digital currency infrastructure based on trusted blockchain and edge computing has been proposed. In this architecture, an efficient consensus management protocol has been proposed. Based on the protocol and supporting strategies, a trusted blockchain structure is constructed, and a decentralized exchange mechanism is introduced based on the concept of smart contract, so as to negotiate between vertical layers and allow vertical services to be parallel with horizontal services, moreover, to promote the implementation of intelligent solutions based on edge computing. This architecture can overcome the shortcomings of traditional blockchain architecture, it can become the infrastructure of digital currency, and it can play a supporting role in many Internet economic applications.

Key words: digital currency; blockchain; trust mechanism; internet economy

责任编辑 夏 娟