软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(2):410−433 [doi: 10.13328/j.cnki.jos.006329]

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

分布式数字资产交易平台的问题与评估*

蔡维德[1,2,3], 王 荣[1], 何 娟[1], 邓恩艳[3]

[1](数字社会与区块链实验室(北京航空航天大学), 北京 100191)

[2](Arizona State University, Tempe, AZ 85287, USA)

[3](北京天德科技有限公司, 北京 100191)

通信作者: 蔡维德, E-mail: tsai7@yahoo.com

摘 要: 近年来, 分布式数字资产交易平台(decentralized digital asset exchanges, DDAE)受到了广泛的关注. 基于金融市场基础设施(principles for financial market infrastructures, PFMI)原理, 提出了评估数字资产交易平台的 5 项基本原则. 并基于这些原则, 从通信技术和交换协议技术两个方面对现有的分布式数字资产交易平台进行了讨论和评估, 阐述了几种典型技术解决方案的实施原理, 将各种技术归纳为不同的模型进行分析. 然后讨论了当前分布式数字资产交易平台存在的监管问题, 并针对之前监管中出现的监管数据不完整和数据被篡改的问题, 提出一种分布式监管模型, 该模型由区块链系统、监管执行引擎以及监管法规库这 3 部分组成, 能够通过读取区块链中的交易数据进行分析, 自动执行监管法规库中的规则, 对满足监管规则的交易自动生成监管报告, 从而实现自动化监管. 最后, 对分布式数字资产交易平台的发展进行了总结和展望.

关键词: 分布式数字资产交易平台; 区块链; 跨链技术; 交易协议; 分布式监管模型

中图法分类号: TP311

中文引用格式: 蔡维德, 王荣, 何娟, 邓恩艳. 分布式数字资产交易平台的问题与评估. 软件学报, 2022, 33(2): 410–433. http://www.jos.org.cn/1000-9825/6329.htm

英文引用格式: Tsai WT, Wang R, He J, Deng EY. Decentralized Digital Asset Exchanges: Issues and Evaluation. Ruan Jian Xue Bao/Journal of Software, 2022, 33(2): 410–433 (in Chinese). http://www.jos.org.cn/1000-9825/6329.htm

Decentralized Digital Asset Exchanges: Issues and Evaluation

TSAI Wei-Tek[1,2,3], WANG Rong[1], HE Juan[1], DENG En-Yan[3]

[1](Digital Society & Blockchain Laboratory, Beihang University, Beijing 100191, China)

[2](Arizona State University, Tempe, AZ 85287, USA)

[3](Beijing Tiande Technology Co., Ltd., Beijing 100191, China)

Abstract: Recently, decentralized digital asset exchanges (DDAE) have received significant attention. This study proposes five criteria to evaluate DDAE based on the principles of financial market infrastructure (PFMI). The current DDAEs technologies are discussed and evaluated from two aspects of inter-blockchain communication (IBC) and exchange protocol technology, the implementation principles of several typical technical solutions are elaborated, and various technologies are summarized into different models for analysis. Then, the regulatory issues of current DDAEs are discussed, and a distributed supervision modelis proposed for the problems of incomplete supervision data and data tampering. This model consists of three parts: Blockchain system, supervision execution engine, and supervision regulation database, which can automatically executethe supervision rules in the supervision regulation database by reading the transaction data in the blockchain and automatically generate the supervision report for the transactions meeting the supervision rules. Finally, the development of DDAEs is summarized and anticipated.

Key words: decentralized digital asset exchanges; blockchain; inter-chain technology; exchange protocol; distributed regulatory model

* 基金项目: 科技部重大项目(2018YFB1402700)

收稿时间: 2020-04-13; 修改时间: 2020-10-26; 采用时间: 2020-12-14; jos 在线出版时间: 2021-01-22

2018 年, 分布式数字资产交易平台火热, 很多人认为, 分布式数字资产交易平台会取代中心化数字资产交易平台, 因为分布式交易所相比于传统中心化交易所隐私性更强、可监管性不强. 但是到了 2019 年, 人们的关注度却在降低. 原因是, 首先分布式数字资产交易量小, 不能满足市场日常需要的交易量; 其次, 分布式数字资产交易平台难以监管, 但是强监管是数字货币的未来趋势. 2019 年, 人们的关注点转为稳定币以及即将来临的数字股票. 对于分布式交易所技术而言, 不论是数字代币、稳定币还是数字股票, 它的技术都是可用的. 但是最新出的稳定币和数字股票都必须在强监管的环境下交易, 这一点就与分布式交易所产生了冲突.

分布式交易所的优势是: 在其中进行的交易就像传统股票市场中的“dark pool”交易, 交易双方身份并不暴露, 这一点有别于正规交易所的交易. 所以, 这不是一种阳光的交易形式.

从 2020 年开始, 分布式数字资产交易平台又重新得到大家的关注. 由于金融行动特别工作组(Financial Action Task Force, FATF)开始实施旅行规则(travel rule), 使许多数字代币交易又转为在分布式交易所进行. 原因是所有数字资产(包括数字代币或是以后的数字股票)交易所都需要符合旅行规则, 就是交易双方的身份需要显明. 为了规避监管, 许多交易转移到分布式交易所或是更“黑”的暗网. 例如, 许多中小型交易所开始下架基于零知识证明协议的数字代币, 因为这些数字代币很难监管, 如果继续让这些代币交易, 相关交易所就会被制裁, 于是, 这些基于零知识证明协议的数字代币转到暗网交易. 事实上, FATF 的旅行规则不但适用于中心化交易所, 也适用于分布式交易所. 所以在理论上, 不论在中心化交易所或是在分布式交易所, 都受监管单位监控. 而且如果分布式交易所洗钱, 也会得到同样的制裁.

本文讨论分布式交易所的科技, 而不讨论应该如何设计和布局监管政策. 对于监管方而言, 这些科技的知识可以用来设计监管政策和监管地下金融活动, 也可以用来设计区块链系统的交易机制防止交易方逃避监管. 如今, 已有机构提出了实现这种机制的方案, 例如互链网方案[1]. 如果将互链网取代当前使用的互联网, 那么所有交易, 不论是中心化交易所、分布式交易所或是暗网, 都将在监管环境下运行.

分布式交易所的未来方向是纳入监管. 分布式交易所不能单独成立, 应该与中心化交易所相互通信. 这种方法可以利用金丝猴模型或是熊猫模型连起来[2]. 在这种环境下, 因为分布式交易所可以减轻中心化交易所的工作量, 所以它有存在的必要性[3,4]. 本文通过建立分布式交易所评价标准来分析各类技术, 总结其中的优势缺点, 为今后分布式交易所相关技术的发展提供依据和建议.

本文第 1 节介绍金融市场基础设施建设原则(principles of financial market infrastructure, PFMI), 基于PFMI 原则提出评估数字资产交易平台的 5 项基本原则, 并基于这些原则分析现有中心化交易所和分布式交易所的优势及缺陷. PFMI 是许多国家央行都支持的金融系统评估标准, 包括中国人民银行、美联储、欧洲央行、日本央行、法国央行、英国央行、德国银行、加拿大央行等. 第 2 节从跨链技术角度对现有的分布式数字资产交易平台进行讨论和评估, 分析各种协议或者模型的优劣之处. 第 3 节从交易协议的角度对分布式数字资产交易平台进行讨论和评估, 并分析其特点和性能, 总结模式. 第 4 节讨论当前分布式数字资产交易平台的监管问题, 并提出一种分布式监管模型. 最后, 第 5 节对分布式数字资产交易平台的发展进行总结和展望.

分布式数字资产交易平台由于题目新, 在这方面的论文还比较少. Lin 讨论了分布式交易所的一些特性, 主要在于法律角度的一些观点[4]; 而美国和欧洲多个大学合作的一篇论文讨论了在分布式交易所出现的不公平现象[5], 即系统方由于知道交易信息, 可以自己先买(如果做多)或是先卖(如果做空), 从而可以成为系统性的风险.

1 评估标准定义与量化

PFMI 是由国际清算银行支付结算体系委员会(CPSS)和国际证监会组织(IOSCO)为了防止 2008 年金融危机的重演而提出来的国际评估标准. PFMI 是一种通用原则, 适用于每个国家的金融系统[5]. 由于是国际通用原则, 而每个国家的金融系统使用的软件和硬件却又有所不同, 相关的法律也不同, 因此虽然有统一的国家标准, 但在实际评估时仍然需要大量考量. 但系统在设计时, 如果充分考虑了 PFMI 原则, 确保服务的合规性、抗风险和扩展性, 那么金融系统经常遇到的问题大部分还都可以得到解决.

PFMI 从 9 个角度界定了 24 项原则, 其中包括明确和严格的监管原则. 24 原则分为如下规则组.

- 总体架构: (1) 法律基础(legal basis); (2) 治理(governance); (3) 风险综合管理框架(framework for the comprehensive management);
- 信用风险和流动性风险管理: (4) 信用风险(credit reisk); (5) 抵押品(collateral); (6) 保证金(margin); (7) 流动性风险(liquidity risk);
- 结算: (8) 结算最终性(settlement finality); (9) 货币结算(money settlements); (10) 实物交付(physical deliveries);
- 中央证券存管和交换系统: (11) 中央证券存管(central securities depositories); (12) 价值交换结算系统(exchange-of-value settlement systems);
- 违约管理: (13) 参与者违约规则和程序(partipant-default rules and procedures); (14) 隔离和可移植性(segregation and portability);
- 业务和运行风险: (15) 一般业务风险(general business risk); (16) 托管和投资风险(custody and investment risks); (17) 运行风险(operatonal risk);
- 准入管理: (18) 准入和参与要求(access and partipation requirements); (19) 分层参与安排(tiered participation arrangments); (20) 金融市场基础设施的连接(FMI links);
- 效率: (21) 效率和有效性(effiency and effectiveness); (22) 通信程序和标准(communication procedures and standards);
- 透明度: (23) 规则、关键程序与市场数据的披露(disclosure of rules, key procedures, and market data); (24) 市场数据披露(disclosure of market data by trade repositories).

例如, 原则(23)要求“披露规则、关键程序和市场数据”, 原则(24)要求贸易储存库披露市场数据. 披露框架旨在提高关于 FMI 的信息的基本透明度. 而一些著名数字代币长期违反这两项原则. 这种透明度的目的是帮助参与者、当局和公众更好地了解 FMI 的活动、风险状况和风险管理做法, 从而支持 FMI 及其利益相关者的正确决策. 这样, 披露框架将实现加强金融稳定的更大公共政策目标. 所有金融机构在建立和运行金融体系时都应遵循 PFMI. 风险管理是 FMI 系统的重要目标, PFMI 确定了 FMI 面临的以下七大风险: 系统风险、法律风险、信用风险、流动性风险、一般业务风险、托管和投资风险、运营风险.

PFMI 原则非常全面, 考虑到很多个方面, 如系统架构、安全性、隐私性、流动性管理和操作风险管理[6,7]. 在 2017 年, 加拿大央行率先提出使用 PFMI 来评估区块链系统, 发现当时许多区块链系统的设计事实上违背了 PFMI 原则, 这表明, 如果在金融系统内使用这些区块链系统, 以后必定会遇到非常大的风险, 这是 2008 年世界金融危机的时候学到的重要功课[8]. 由于 2008 年许多金融系统不符合 PFMI 原则, 以至于一个国家的金融危机可以经过金融系统传到另外一个国家. 如果这些系统符合 PFMI 原则, 就不会发生这种现象. 加拿大央行给出研究报告后, 多次批评现在区块链系统, 认为这些系统如果不加以改变就不能被世界央行采用[9,10]. 后来, 欧洲央行、日本央行、英国央行也跟进使用 PFMI 来评估区块链系统[11,12]. 可以看到: PFMI 原则是通用型、普适性的, 因此覆盖面大且较少提及具体指标. 由于 PFMI 提出时没有考虑数字资产交易, 之后许多学者和央行根据其当地的法规提出具体的量化指标. 本文根据这些央行的实验报告, 提出了 5 项原则并定义了其量化指标.

1.1 第1项: 可靠性

PFMI 多次提出这样一个需求, 即金融交易系统全方面都必须是可靠的, 但是 PFMI 并没有提出统一的量化指标. 可靠性体现在两个方面: 一是交易平台系统本身的可靠性, 系统可靠性不仅是降低系统出错的概率, 还包括在系统出错时可纠错和恢复正常运行的能力, 即系统的容错能力; 二是金融基础设施的可靠性, 防止由于功能设计不当诱发各种风险. 可靠性量化指标有很多, 例如, MTBF (mean time between failure)[12]平均故障间隔时间是用于评估电子产品的可靠性指标, 这个量化方案广泛应用于包括电子产品在内的多项应用中[13], 计算公式如下:

$$MTBF = \frac{\sum(downtime - uptime)}{failuretimes}.$$

这个量化指标可以用于分布式交易所系统, 但是交易所作业复杂, 本文使用 3 个过程来评估系统的可靠性: 首先是交易前的运行可靠性, 通过是否有身份认证来加以判断; 其次是交易中的可靠性, 通过判断是否存在黑手交易来实现; 最后是交易后的可靠性, 通过判断是否资金到位、安全回滚来判断. 而上述指标可以用在所有过程中, 可靠性的量化指标见表 1.

表 1 评估标准的量化指标

评估指标	计算方式	量化条件/评级(分值)	总分
可靠性	分值叠加	条件: 1. 交易前运行可靠性(4); 2. 交易前运行可靠性(4); 3. 交易前运行可靠性(2)	10
可扩展性	指标评级	评级: 1. 使用以 POW 为基础的共识(1); 2. 使用以 BFT 为基础的共识(4); 3. 在条件 2 的基础上采用可扩展性架构达到无限扩展的目的(10)	10
可监管性	分值叠加	条件: 1. 快速定位交易(3); 2. 快速终止交易(2); 3. 身份认证(3); 4. 建立人物关系图谱(2)	10
数据隐私性	指标评级	评级: 1. 所有人可见(0); 2. 系统或监管可见(7); 3. 仅用户可见(10)	10
可回滚性	指标评级	评级: 1. 系统交易不可回滚(0); 2. 系统交易可回滚(5)	5
综合	叠加	以上各项评估指标的分值叠加	45

1.2 第2项: 可扩展性运行效率

PFMI 文件也多次提到系统必须可以扩展, 而且每次提到扩展性都是和可靠性一起提出, 表示系统必须同时间可扩展而且扩展机制是可靠的, 并且指出这会是系统运行的一个重要风险. 例如 PFMI 3.20.20 规则:

> 3.20.20. 交易数据存储库(trade repository, TR)应仔细评估与其链接相关的额外运营风险, 以确保 IT 及相关资源的可扩展性和可靠性.

系统设计一定要满足对于金融交易业务能力可扩展性的要求, 当系统增大数据量时, 系统的处理速度和吞吐量等系统性能不会受到较大的影响. 依据 USL(universal scalability law)理论[14], 这是一种广泛应用的理论[15], 我们可以得到可扩展性的计算方法, 其中, N 表示负载量, X 表示吞吐量, 参数α、β和γ分别表示由于共享资源的等待或排队而引起的冲突比例、为保证数据一致性导致的延时比例以及并发量. 计算公式如下[16]:

$$X(N) = \frac{\gamma N}{1 + \alpha(N-1) + \beta N(N-1)}.$$

按照该公式计算, 目前所有分布式账本系统的可扩展性都很低. 原因是每种系统的架构不同, 导致每种系统的可扩展性也不同. 因此, 依据分布式账本系统的特点和上述可扩展性量化公式, 本文中, 我们将可扩展性的量化分为 3 层.

- 第 1 层是使用以 POW 为基础的共识算法. 实践表明, POW 算法几乎没有可扩展性. 经过多年的研究, 包括链下活动等, 扩展性有所提高, 但却有其他问题出现. 例如, 链下活动的可靠性低. 但是大部分公有链采用的是这种算法. 扩展性是公有链需要关注的问题, 也一直有解决方案. 但是大部分解决方案都会影响到其他功能或是指标, 例如可监管性, 或是交易完备性;
- 第 2 层是使用以 BFT(拜占庭将军协议)为基础的共识算法, 该算法的可扩展性要高于 POW[17];
- 最后一层是在使用 BFT 的基础上可扩展性架构(例如 ABC-TBC 架构)达到无限扩展的目的.

根据排队理论(queuing theory)[18], 效率有两个基本评价指标: 吞吐量和延迟. 但是几乎所有的分布式账本都是低吞吐量和高延迟的, 因为原来这些系统都不在乎性能(包括吞吐量和延迟), 只在乎隐私(为逃避监管). 因此, 这些系统得 1 分. 高吞吐量和低延迟系统与可扩展性相关. 不能扩展的系统很难有高性能. 而可扩展性进一步又会影响性能, 因此可扩展性和性能之间相互关联, 具体量化评级见表 1.

1.3 第3项: 可监管性

PFMI 多次提到央行或是监管单位需要监管金融系统, 例如 PFMI 4.5.9 规则.

> 付款和结算安排
>
> 4.5.9. 当金融市场的支付和结算系统以及流动性机制具有系统性风险时, 相关监管、监督、管理单位需要对这些风险评估, 而且这些风险评估必须考虑央行的观点. 央行可能有兴趣参与金融市场基础设施的支付、结算、流动性风险管理程序, 因为央行需要执行国家货币政策和维持金融稳定. 此外, 如果央行因为其职责的关系, 必须对这些系统做风险评估, 也要考虑和尊重这些金融系统的负责单位.

PFMI 对监管有着明确而严格的规定, 例如其中规定: 关键程序和市场数据都需要提供充分的信息, 公开披露, 供参与者能够准确了解; 其次, 需根据有关管理部门和公共各自的需求, 及时准确地提供各种交易数据库市场数据. 目前, 区块链或是数字货币的可监管性并没有统一标准, 我们根据 2017 年加拿大央行实验报告以及其他报告, 提出了 3 项可监管性的量化条件.

(1) 快速定位交易: 这是监管的第 1 个必要条件, 找不到交易信息不可能监管该交易. 加拿大央行在 2017 年的一个实验报告中批评一些出名的链(Corda 和以太坊)连账户和交易信息都很难找到, 这样的链设计不适合监管;

(2) 快速停止交易: 不但要及时找到信息, 有时还需要及时停止该交易, 因为有的交易是实时结算的. 例如, 英国央行最初的数字英镑计划提出的就是实时结算, 交易后马上结算. 因此, 实时停止交易是需要的. Libra 2.0 就考虑了这一需求, 于是在区块链协议层放进“嵌入式监管机制”, 在交易流程中, 监管单位即使发现问题, 但只要在交易没有结算之前, 还都可以停止这一交易;

(3) 身份认证以及建立人物与相关公司的关系图谱: 这是传统金融监管的机制, 主要使用大数据平台来完成. 这样的机制需要大量的计算, 这些大都是在交易前和交易后进行监管计算.

有些逃避监管的区块链系统, 连找到相关交易信息都需要一定的时间(例如只用一次的 token 设计, 以及比特币), 没有嵌入式监管机制以至于不能停止任何交易, 而且交易方匿名, 从而无法找到相关关系监管信息. 具体量化评级见表 1.

1.4 第4项: 数据隐私性

PFMI 提出金融系统需要根据当地法律来保护客户隐私, 并且提供安全以及高效的保护机制. 大部分国家法律都要求金融系统保护客户隐私数据, 其他的客户和相关操作人员都不能看到客户的数据, 例如欧盟的通用数据保护条例(general data protection regulation, GDPR); 但是央行及监管部门要能够随时且高效地查询到所有账户及其相关的金融信息. 数据隐私性量化与应用相关. 我们定义了 3 个隐私级别: 所有人可见, 隐私性为 0; 系统或监管可见, 其他人不可见, 隐私性为 7; 仅用户可见, 系统的数据隐私性是 10. 大部分系统都用加解密来传送信息, 用以保护隐私, 但是许多系统交易后信息公开. 新型系统的交易信息也不公开, 但是可以开放给监管单位. Libra 2.0 就选择了这一路线. 具体量化评级见表 1.

1.5 第5项: 可回滚性

现代金融系统允许参与交易者在交易后回滚, 可能资金未到位或资金来源或资产有问题, 回滚时间有期限. 通常, 这是根据当地法律要求, 例如交易后两天. 这可以从如下 PFMI 3.8.8 规则看出.

> 撤销未交付款、转移指示或其他义务
>
> 3.8.8. FMI 应明确界定参与者不得撤销未定付款、转移指示或其他义务的要点. 一般来说, FMI 应禁止在结算日的某一点或某一时间单方面撤销已接受和未结算的付款、转移指令或其他义务, 以避免造成流动性风险. 在所有情况下, 应明确定义例外的截止时间和重要性规则. 规则应明确, 对营业时间的更改是例外, 需要个别理由. 例如, FMI 可能出于与实施货币政策或金融市场普遍混乱有关的原因而允许延期. 如果允许有操作问题的参与者完成处理, 则对参与者应清楚有关此类扩展的批准和持续时间的规则.

现在许多区块链交易系统不支持这一功能, 一旦交易完成, 就永远没有办法将该交易回滚. 幸运的是, 回滚机制可以放进区块链系统, 只是区块链设计需要更改. 而可回滚性是现代金融交易重要的功能, 是政府监管必备的工具. 这样的机制属于下一代区块链系统. 因此, 有回滚机制的系统可回滚性为 5 分, 不可回滚的系

统可回滚性为 0.

1.6 量化和总结

在量化过程中, 如果出现协议或模型并没有考虑到某一量化指标, 但是实际模型中具备实现该指标的条件, 本文中则认定该模型满足该条件. 例如: 在很多协议中并没有定义具备快速定位交易的功能, 但在实际应用中这一功能可以实现. 只要有相关数据, 这一协议就被认为具备了快速交易的条件. 但是, 如果数据库没有这些信息, 即使有算法也很难得到高评. 加拿大央行认为一些链不好监管, 就是在一些链的数据库里没有足够信息. 例如, 一些区块链系统上的节点有不同信息, 需要复杂的协议和算法才能找到相关交易信息, 这会对最终的结算性以及监管造成困难. 因此, 本文认为没有满足条件. 具体量化评级见表 1.

PFMI 并没有定义各央行和金融机构应该执行的具体操作, 但是其中的各项规范原则却是世界通用的, 被各大央行奉为圭臬, 一个重要原因是 PFMI 可以全面性地进行评估. 没有全面性的评估, 金融系统就是造成 2008 年世界金融危机的原因之一, 不然只会是一个国家的金融危机. 但传统上, 数字代币、中心化数字资产交易所、分布式数字资产交易所都只考虑到了部分原则, 因此这些系统可能存在巨大的风险. 一些数字代币系统明显地违反了第 6 项、第 11 项、第 14 项、第 20 项、第 23 项原则, 例如美国监管单位 SEC 批评某一稳定币违反 PFMI 第 23 项原则. 而历史上, 这些系统也不断有重大金融事故出现, 证实这些风险是真实存在的. 而分布式交易所强调强隐私性, 但是过度隐私性导致监管困难以至于容易作弊, 由文献[19]可知, 由于系统交易不公平, 还会出现系统性风险.

2 跨链技术

分布式数字资产交易平台的跨链技术主要应用于不同区块链系统之间的数据通信模块, 从而实现不同资产之间正常交易的功能[6]. 当前, 跨链技术成为区块链发展的一个重要研究方向, 是打造区块链互联网的关键技术. 在未来, 各大区块链系统之间独立运行, 相互分裂是不可能得到进一步的发展的, 交易的流动性也受到了抑制. 因此, 研究跨链技术的意义十分重大.

跨链技术可分为同质网络的跨链技术和异构网络的跨链技术. 同质网络是指链网中的区块链有相同的链架构、相同的协议; 异构网络是指链网中的区块链有不同的架构、不同的协议以及不同的资产. 相比之下, 同质网络的跨链功能更容易实现. 在本文中, 将跨链流程分为 3 个过程.

(1) 交易发布: 在跨链交易的过程中, 交易的发起方如何发起交易、交易是以广播的形式发布出去还是发送给特定的节点;

(2) 数据共识: 跨链协议中使用何种共识算法、何时进行数据共识;

(3) 结果上链: 共识的结果存储在何处、何种节点会存储共识数据.

本节重点介绍了跨链原子互换协议、公证节点模型、IBC 跨链协议以及金丝猴模型这 4 种典型的跨链技术, 分别介绍了各个协议或者模型的运行原理. 将跨链方案运行过程划分为发布交易、数据共识以及结果上链这 3 个步骤, 结合上一节中定义的 5 项原则对这几种跨链方案进行分析. 最后总结不同方案的特点, 将各类方案总结成不同模式, 分析不同模式的优劣之处.

2.1 跨链原子互换协议

跨链原子互换协议的设计目的是为了让交易双方所在的链尽可能地减少通信, 无需相互信任就能实现跨链交易, 同时保证交易的原子性. 所有交易操作或者同时成功, 或者全部失败.

跨链原子互换协议的设计思想是: 使用哈希锁定锁住资产, 交易者出示钥匙获取资产. 交易的发起者提供锁和钥匙, 用锁标记交易资产, 交易接受者只有提供钥匙并与锁匹配成功才能获取发起者的资产. 然后, 交易接受者发起附有自己交易资产的钥匙查询请求, 发起者提供钥匙才能获取接受者的资产. 在这个过程中, 双方的资产锁定都有时间限制, 一旦超时, 资产将退回得到原本的账户中, 交易失败. 协议的具体流程和相关技术可参考相关技术文献[20]. 跨链原子交换协议的过程如图 1 所示.

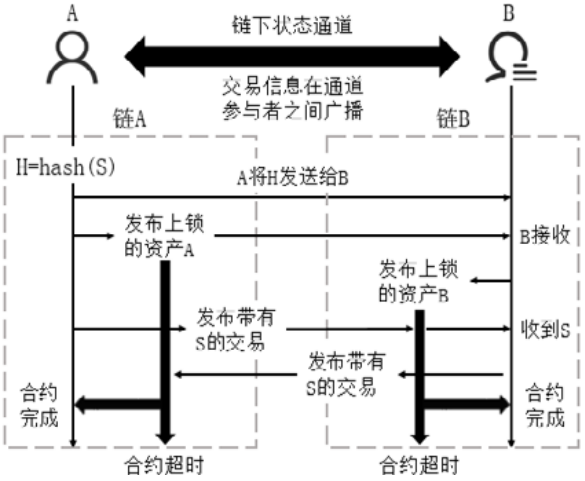

图 1 跨链原子交换协议示意图

根据协议的执行过程可以总结出, 该协议使用了 3 种技术: 哈希锁定技术、智能合约技术以及区块链技术. 哈希锁定技术和智能合约技术的结合使用, 共同保证交易的原子性. 当智能合约执行结束时, 协议将智能合约的执行结果保存在区块链上, 目的是利用区块链的不可篡改性来提高交易结果的可靠性. 结合 5 项基本原则, 有关跨链原子交换协议特点的总结见表 2, 具体分析如下.

(1) 可靠性: 交易发布过程中采用链上广播的形式; 数据共识和结果上链过程中不同系统采用的共识算法不同, 因此可靠性取决于算法的可靠性. 3 个过程只满足量化条件 2;

(2) 可扩展性: 该协议目前应用于闪电网络中, 闪电网络是一个以比特币为基础的系统, 满足可扩展性条件 1;

(3) 可监管性: 该协议的技术中没有为数据的可监管提供方法;

(4) 数据隐私性: 该系统中的数据所有人可见, 但是使用公钥代表了用户身份, 无法定位个人;

(5) 可回滚性: 该协议的交易原子性极强, 因此不具备交易执行过程中突然撤回交易的情况, 因此可回滚性弱.

表 2 跨链原子互换协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	4	4	0	7	0
数据共识	4	4	0	7	0
结果上链	4	4	0	7	0

2.2 公证人模型

公证人模型是 R3 Corda 系统中使用的方案, Corda 是一种伪链, 使用的是类似于比特币的 UTXO(unspent transaction object)模型, 而没有账户的概念[21−23]. Corda 中引入了公证节点(notary)的概念, 用于记录用户之间的交易以及共识.

Corda 系统中有多个公证节点, 可以统称为公证池. 从用户角度来看, 公证节点是可信的, 但是公证节点与公证节点之间是不可信的. 用户之间的交易需要通过公证节点的记录, 一个用户的账本只存于一个公证节点中. 如果交易双方都隶属于同一个公证节点管理, 那么这个交易不需要共识, 交易双方可以信任公证节点不会作恶. 但是, 如果交易双方属于不同公证节点管理, 需要跨公证节点交易, 那么这个过程就被称为公证人变更. 变更过程需要所有公证节点共识, 这样才能保证这笔交易没有双花, 共识算法使用的是 PBFT 共识算法. 公证节点变更的过程参考其白皮书和相关技术文档[21−23], 模型示意图如图 2 所示.

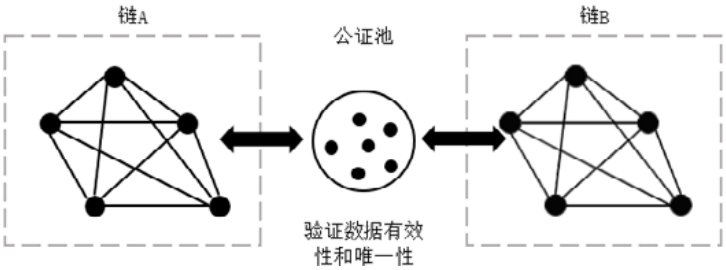

图 2　公证人模型示意图

公证人模型的特点是兼顾了用户隐私和模型的可监管性, 以牺牲部分可靠性来换取模型效率. 该模型中是部分交易进行共识, 兼顾了中心化系统效率高以及分布式系统可靠性高的特点. 该模型使用 PBFT 共识算法来保证交易的可靠性. 有关公证人模型特点的总结见表 3, 分析过程如下.

(1) 可靠性: 部分交易只发送给公证节点, 存在被公证节点篡改的风险, 可靠性一般; 数据共识和结果上链过程使用的是 PBFT 算法, 可满足所有可靠性量化条件;

(2) 可扩展性: 交易发布过程的可扩展性可以通过增加公证节点达到, 因此扩展性强; 数据共识和结果上链过程使用 PBFT 算法, 该算法的交易效率不会无限增加, 因此满足可扩展性量化条件 2;

(3) 可监管性: 该技术引入公证节点的一个目的就是为了监管公证节点的变更过程, 因此数据共识和结果上链过程满足可监管性量化条件 1 和条件 2;

(4) 数据隐私性: 交易发布只有一个公证节点管理, 数据隐私性弱; 数据共识和结果上链过程使用 PBFT 算法, 执行过程使用密文, 但是多个节点持有数据, 满足数据隐私性量化条件 2;

(5) 可回滚性: 该技术没有考虑交易的可回滚性.

表 3　公证人模型量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	10	4	5	7	0
数据共识	10	4	5	7	0
结果上链	10	4	5	7	0

2.3 链间通信协议(inter blockchain communication, IBC)

IBC 协议是 Cosmos 系统中用于跨链交易的通信协议, Cosmos 为多链并行提供了一种解决方案, 弥补了闪电网络等平台在扩展性方面的需求[24]. 部署在 Cosmos 网络上的交易所有很多, 例如 Binance、OKex 以及 Coinbase 等, 其中, Binance 交易所的交易量目前处于领先地位[25].

Cosmos 由多个区域链(zone)和中继链(cosmos hub)组成, 使用便于扩展的 BFT 共识算法. 每个区块链都是 Cosmos 网络中的独立区块链, 与中继网络通过 IBC 协议交互. 中继链是 Cosmos 网络中第一个公共区块链, 使用 Tendermint 算法, 该算法是在 BFT 共识算法基础上的改进, 管理 Cosmos 网络中的跨链账本, 也可被称为是多资产托管网络. 区域链与区域链之间的交易是通过中继链完成的. IBC 协议的具体过程参考 Cosmos 白皮书[26], Cosmos 系统示意图如图 3 所示.

IBC 协议针对的是同质链之间的通信, 每个区域链架构都是相同的, 不存在协议不兼容的情况. 该协议通过引入中间链的方式完成跨链交易, 这种方案在交易量增加的情况下, 可以通过增加区域链的方式提高交易的处理效率; 同时, 中间链也可以达到对跨链交易的监管效果. 但是该协议的使用也有局限性, 只能用于同构链之间的跨链通信, 不能用于异构链之间的通信. 综上所述, 结合 5 项评估标准, IBC 协议的特点见表 4, 分析过程如下.

(1) 可靠性: 交易链上广播不易篡改, 可靠性强; 数据共识和结果上链过程使用 Tendermint 共识算法, 满足所有可靠性量化条件;

(2) 可扩展性: 该技术采用多链并行的方案, 可以无限地增加区域链和中继链, 使用以 BFT 为基础的 Tendermint 共识算法, 满足可扩展性量化条件 2;

(3) 可监管性: 中继链中存有跨链交易数据, 因此跨链交易可由中继链监管, 但是非跨链交易数据难以监管, 可满足可监管性量化条件 1 和条件 2;

(4) 数据隐私性: 交易发布过程中, 跨链交易数据中继链可见, 而其余数据不可见, 因此隐私性中等; 数据共识和结果上链使用 Tendermint 共识算法, 过程密文执行, 但因有过多节点参与, 因此数据隐私性一般, 满足数据隐私性量化条件 2;

(5) 可回滚性: 该技术没有考虑交易的可回滚性.

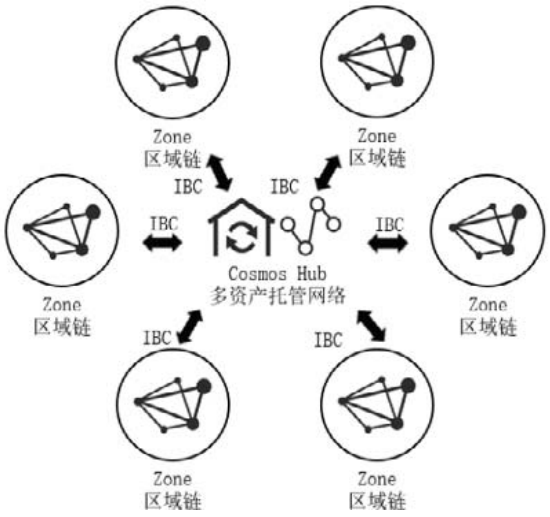

图 3 Cosmos 系统示意图

表 4 IBC 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	10	6	5	7	0
数据共识	10	6	5	7	0
结果上链	10	6	5	7	0

2.4 金丝猴模型

金丝猴模型是一种跨链交易模型, 打破了现有跨链模型里中心化的限制, 实现了参与链的并行运行, 该模型具有可监管性和可扩展性[27,28]. 金丝猴模型由参与链和中间链构成, 中间链的设计是为了完成参与链之间的通信, 一个中间链可以连接多个参与链, 参与链和中间链之间至少有两个公共节点. 该模型可以实现实时交易和多边净额结算两种交易模式.

参与链可以由一个或多个金融机构或单位构成, 其中包含一个或多个节点. 中间链是一个中间机构也是金融机构, 为保证交易的安全性, 参与链与中间链之间至少有两个公共节点. 在金丝猴模型中, 任意数量的金融机构与中间机构可以随时容易地加入该链网结构, 并通过 TBC 将即将加入的新的金融单位与已有的中间机构连接起来, 这使得该链网可以扩张并适应大型网络及高交易量. 同时还支持监管, 中间链中可添加监管节点, 记录完整的交易过程, 便于后续查验. 模型示意图如图 4 所示, 交易过程如下:

(1) 可靠性: 交易发布过程是在双方参与链与中间链之间广播, 交易难以篡改, 可靠性强; 数据共识和结果上链过程的可靠性取决于选取的共识算法的可靠性, 中继链中使用 BFT 共识算法, 满足所有可靠性量化条件;

(2) 可扩展性: 该模型可以根据交易规模增加参与链和中间链, 不同参与链之间并行操作, 可以在交易量增加的情况下, 通过增加参与链和中间链来保证模型的运行效率, 满足可扩展性量化条件 2;

(3) 可监管性: 中间链和参与链的交叉部分中设置有监管节点, 用于监管跨链交易, 满足可监管性量化条件 1 和条件 2;

(4) 数据隐私性: 该模型中的跨链交易在交易双方所在的参与链和中间链中广播, 数据共识和结果上链过程中数据密文在参与节点之间传输, 满足数据隐私性量化条件 2;

(5) 可回滚性: 该模型采用智能合约技术, 智能合约具有一定的可回滚性, 但是需要达到回滚条件, 因此模型具有部分可回滚性.

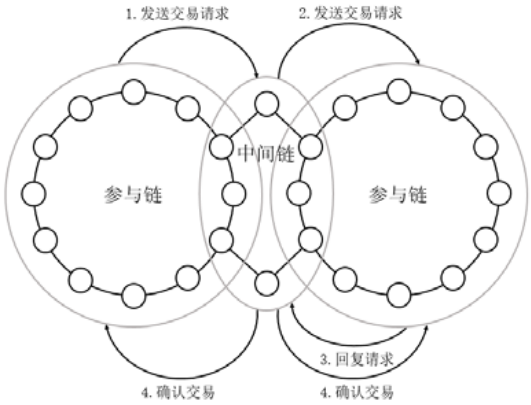

图 4 金丝猴模型示意图

表 5 金丝猴模型量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	10	8	8	7	5
数据共识	10	8	8	7	5
结果上链	10	8	8	7	5

2.5 模型分析

总结以上跨链通信方案, 可将其分为 3 种模式: 原子交换模式[20]、公证节点模式[20]和中间链模式[20]. 下面来分析这 3 种模式的特点.

原子交换模式是以哈希锁为技术基础, 主要功能是实现了交易原子性操作的一种模式. 这种模式的特点是能作为一种基础协议与其他模式相结合, 因此这种模式的性能很大程度上取决于其所基于的底层系统的性能. 由于原子交换模式的全过程都是在链上完成的, 因此这种模式的很多性能取决于底层的区块链的性能, 运用这种模式提高了跨链交易的速度. 可扩展性、可监管性以及数据隐私性都与底层系统有关. 模型特点见表 6.

表 6 原子交换模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	4	4	0	7	0
数据共识	4	4	0	7	0
结果上链	4	4	0	7	0

公证节点模式是在系统中设置了公证节点, 节点之间相互独立, 分别维护一个自己的账本, 节点之间只有在触发了跨公证节点的交易, 否则不会共识. 这种模式分别汲取了中心化系统和分布式系统的优势, 在尽可能地保护数据隐私的前提下, 实现了系统的可监管功能. 考虑到分布式系统中共识过程效率低, 在该模式中只将部分交易共识, 提高了系统效率. 因此, 公证节点模式不能被称为是分布式模式, 它还存在着数据被篡

改的风险. 模型特点见表 7.

表 7 公证节点模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	10	4	5	7	0
数据共识	10	4	5	7	0
结果上链	10	4	5	7	0

中间链模式是当前普遍采用的一种模式, 这种模式在各个区块链之间添加了中间链来维护链与链之间的交易, 典型的应用有 Cosmos 的 IBC 协议以及金丝猴模型. 该模式扩展性好, 便于监管, 但是运行效率可能有所欠缺. 有很多系统采用的是中间链模式, 但是这些系统之间也存在很大不同, Cosmos 的中间链 Cosmos-Hub 有中心化的风险, 但是金丝猴模型中的中间链可以根据系统的实际情况随意添加. 这是由于, 这两种系统在设计之初针对的问题即有所不同, 金丝猴模型充分考虑了数据隐私性和可监管性, 因此中间链不能是所有参与链的中心. 经过上述分析可以看出: 中间链模式是一种很灵活的模式, 其性能不能由一句话概括, 需要根据实际系统架构进行分析. 表 8 中的各项性能根据各类实际系统的共性总结, 有分歧的性能没有概括. 模型特点见表 8.

表 8 中间链模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易发布	10	8	8	7	5
数据共识	10	8	8	7	5
结果上链	10	8	8	7	5

3 交换协议

传统的交易平台以交易所作为信用背书, 用户完全信任交易所, 因此交易所是用户资产的实际控制者. 同时, 用户的交易操作都是由交易所的中心化服务器来完成的, 这种操作成交速度快, 交易深度好. 但是这种方案的前提是交易所不会作假, 同时没有外界攻击, 一旦交易所的安全性受到威胁, 用户资产的安全性就得不到保障.

订单簿是一种用自动化的方式对可交易的资产进行匹配的方案. 传统的订单簿是集中式的, 并且与订单执行相结合, 以集中式的实际来源实现订单的创建、执行和取消. 早期的分布式数字资产交易所采用的是链上订单簿的方案, 链上订单簿用于解决交易单一和交易效率的问题, 但是这种方案同样存在问题.

- 首先, 链上订单簿不能扩展, 匹配算法在链上执行的成本高, 且订单的执行周期花费高;
- 其次, 链上订单是公开的, 矿工在订单发布前就知晓了订单, 会导致抢先交易的问题; 同时, 订单是公开的, 价格对所有人都是一样的, 不利于供应商调整流动性;
- 最后, 链上订单是不公平的, 物理网络的延时导致矿工获得订单信息的时机有先有后.

因此, 针对早期的分布式交易技术, 各大分布式数字资产交易平台都提供了自己的方案. 目前, 主流的数字资产交易平台的主要功能有资金托管、交易撮合、交易结算、资金提取这 4 个方面:

本节重点介绍了原子交换协议、Uniswap 和 Bancor 协议、0x 协议、Kyber 协议、Airswap 协议以及熊猫模型这几种典型的交易协议, 分别介绍了各个协议或者模型的运行原理. 将交易技术的运行过程划分为资金托管、交易撮合、交易结算以及资金提取这 4 个部分, 结合第 2 节中定义的 5 项原则对这几种交易技术进行分析. 最后总结不同方案的特点, 将各类方案提炼成不同模式, 分析不同模式的优劣之处.

3.1 Atomic Swap协议

Atomic Swap 协议是一种分布式、跨账本资产交换的解决方案[29], 它实现了类似数据库事务处理的操作, 能够保证资产交换过程的原子性, 所有操作要么全部成功, 要么全部失败. 该协议通常作为分布式交易协议的基础协议, 可被其他协议调用来保证交易的原子性[30].

Atomic Swap 协议的原理是利用哈希锁定技术: 交易双方中的发起者提供锁, 同时保留钥匙; 接受方需要

用自己用于交换的资产换取钥匙, 然后用钥匙取走发起方发布的资产. 原子交换协议的具体执行过程参考其白皮书[29].

在分布式交易所中, Atomic Swap 协议主要用于交易撮合之后, 交易双方资金的交割, 完成数字加密货币的交易结算过程[31]. 该协议的兼容性很强, 过程简单, 可在任何区块链交易系统中运用. 其中使用到的技术有哈希锁定技术、智能合约技术以及区块链技术. 哈希锁定技术与智能合约共同保证交易的原子性, 区块链在智能合约执行完成后共识执行结果, 提高交易的可靠性. Atomic Swap 协议的特点见表 9, 分析过程如下.

(1) 可靠性: 转账操作是原子性的, 该协议常用于以太坊系统中, 满足可靠性量化条件 2;

(2) 可扩展性: 可扩展性由区块链的可扩展性决定, 如果区块链平台不支持哈希时间锁定条件脚本或是智能合约, 则需要进行改造才能完成跨账本交易, 满足可扩展性量化条件 1;

(3) 可监管性: 协议未考虑可监管性. 但是协议常用于以太坊中, 其满足量化条件 1 和条件 2;

(4) 数据隐私性: 交易双方使用自己的钱包地址, 很难根据钱包地址跟踪到某个具体的用户, 但是所有人都能看到交易内容只是无法定位用户, 因此满足隐私性量化条件 1;

(5) 可回滚性: 该协议未考虑可回滚性.

表 9 Atomic Swap 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易结算	4	1	5	7	0

3.2 Uniswap协议和Bancor协议

Uniswap 协议[32]和 Bancor 协议[33]都是针对分布式金融系统中市场流动性问题提出的解决方案, 实现代币价格自动调节功能. 这两种协议很好地将金融思想和分布式技术相结合, 达到市场自动调节的效果, 增强市场中代币的流动性. 下面分别介绍这两种协议的运行原理.

Uniswap 是以太坊推出的一个分布式交易所协议, 完成了在分布式网络中自动做市的功能, 使用以太坊智能合约实现. Uniswap 使用的是 Constant Product 自动做市模型, 模型原理是保证资金池中任意两种代币资金的乘积是一个定值. Uniswap 协议在运行中实际上有两种机制在调节资金池中各类代币的兑换价格.

- 一种是资金池的流动性提供者, 这类用户通过获取交易费用获利, 资金池中代币资金越多, 大交易造成的价格波动越小, 因此, 各类代币价格的稳定性取决于资金池的规模. Uniswap 中通过流动性提供者可获得交易费用的机制来激励用户将资金投入资金池中;
- 第2类是套利者, 当Uniswap与其他交易所中代币价格出现价格差时, 会有用户利用这个价格差获利; 同时, Uniswap 中代币的价格也在这个过程与市场价格持平.

Bancor 协议的原理来源于凯恩斯在布雷顿森会议上提出的货币方案, 通过公式调整各类数字资产的价格. Bancor协议中引入了一种智能代币BNT, 通过Bancor公式, 将BNT和其他代币维持在一个固定比率下[34]. 智能代币和其他代币之间使用连接器连接, 与连接器连接的其他代币统称为连接器代币[35,36]. Bancor 协议保证了代币的流动性, 这里的流动性不仅针对的是交易量大的代币, 同时也包括认购量低的代币. 其次, 该协议没有内置手续费, 且算法运行透明, 代币价格可预测.

Uniswap 协议和 Bancor 协议只是分布式金融(DeFi)项目中的两种方案, 分布式金融的发展还处于初步发展阶段, 但就目前情况来看, 还有很大的发展空间. 以Uniswap为例, 仅在2019年, 从几乎没有流动性到整体流动性超过 2 500 万美元, 这样的发展速度是惊人的. 这并不意味着这些方案就是完美的, 有研究计算表明: 在 Uniswap 协议中, 流动性提供者在能够从交易费用中获利的情况下, 投入的资产依然会贬值[37]. 类似这样的问题需要继续加以深入研究.

Uniswap 协议和 Bancor 协议可以代表一类协议, 这类协议的思想来源于一些金融货币模型. 这类协议通常兼容性很好, 协议过程不复杂, 可适用于不同的区块链交易系统. 协议的主要目的是建立分布式金融体系, 实现市场自动调节, 增强代币流动性的目的. 两种协议主要包括交易撮合和资金提取两个部分, 因此只分析

交易托管和交易结算两个过程. 两种协议的特点见表 10, 分析过程如下.

(1) 可靠性: 两种协议的交易托管依靠智能合约技术; 部署于以太坊中, 满足可靠性量化条件 2;

(2) 可扩展性: 两种协议的可扩展性依赖于底层区块链的可扩展性, 满足可扩展性量化条件 1;

(3) 可监管性: 两种协议没有引入监管. 但是协议常用于以太坊中, 其满足量化条件 1 和条件 2;

(4) 数据隐私性: 两种协议的数据隐私性依赖于底层区块链的数据隐私性, 满足隐私性量化条件 1;

(5) 可回滚性: 两种协议本身没有考虑可回滚性.

表 10 Uniswa 协议和 Bancor 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易托管	4	1	5	7	0
交易结算	4	1	5	7	0

3.3 0x协议

0x 是一个以太坊的开放的分布式交易所协议, 可以作为 Dapps 的共享基础设施. 从长远来看, 它是开源的技术标准, 比封闭架构更具优势[38]. 0x 协议综合了市场自动做市商(automated market maker, AMM)智能合约和状态通道的优点, 克服了两者的缺点, 提出了“链下撮合, 链上结算”的操作方案[39].

0x 协议的执行流程包括链下撮合和链上结算两个部分.

- 在交易发起方发起交易之前, 链上的分布式交易所首先要确定其账户中是否有足够的余额; 然后, 发起方将订单广播发给中继者, 中继者验证订单的有效性后, 将订单添加进订单簿中; 交易接受方可以从订单簿中获取订单. 发布订单和获取订单都是在链下完成的;
- 交易接受方获取订单后, 链上的分布式交易所确定接受者账户中有足够的余额后, 接受方将带有发起方签名的订单提交给交易所. 最后, 分布式交易所完成交易, 交换双方的交易资产.

0x 协议过程如图 5 所示.

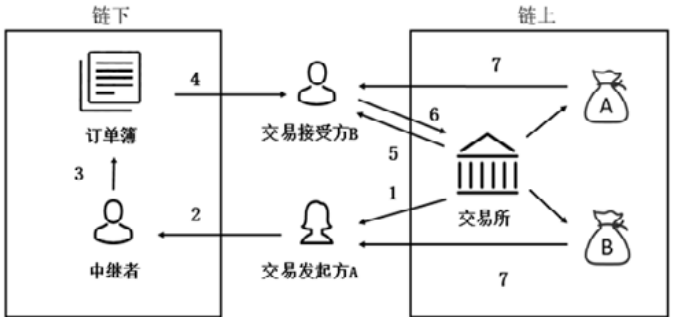

图 5 0x 协议示意图

针对链上订单簿效率不高的问题, 0x 使用链下订单薄模式, 交易者可以从链下订单薄中获取理想的订单, 大大减少了第三方对市场的干预. 状态通道的概念很好, 0x 协议借鉴其优势, 将订单撮合的过程放置在链下来处理, 将重要的订单结算过程依旧保留在链上操作, 并提出了中继者这一概念来弥补状态通道的不足, 让中继者管理订单的发布. 0x 协议包括交易撮合和交易结算两个过程. 0x 协议的特点见表 11, 具体分析如下.

(1) 可靠性: 协议常用于以太坊中, 交易撮合过程依靠中继者, 整个过程在链下完成; 交易结算过程采用链上结算的方式, 通过共识后结果存于链上, 满足可靠性量化条件 2;

(2) 可扩展性: 用户可以在区块链上通过 0x 协议创建交易所, 中继者数量没有受限, 同时, 交易撮合线下完成. 交易结算依赖区块链, 随着交易量的增加, 区块链平台单位时间内处理的交易数量会达到上限, 满足可扩展性 1;

(3) 可监管性: 协议本身没有考虑可监管性. 但是协议常用于以太坊中, 其满足量化条件 1 和条件 2;

(4) 数据隐私性: 身份信息非公开, 只能看到交易数据, 满足隐私性量化条件 1;

(5) 可回滚性: 协议本身没有考虑可回滚性.

表 11 0x 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易撮合	4	1	5	7	0
交易结算	4	1	5	7	0

3.4 Kyber协议

Kyber Network 是以太坊链上的分布式交易所, 为用户提供多种资产之间转换的应用, 为交易双方提供资产交换接口, 降低交易风险, 提高交易效率[40]. 用户会在发送交易之前获得各类代币间的兑换率, 交易确认后收到相应数量的代币. Kyber Network 的目标在于为用户提供便捷、高效的数字资产交易服务. Kyber 网络以智能合约技术为基础, 降低了中心化交易所的风险, 最大限度地保证了交易的及时性, 为用户的使用提供了良好的使用体验.

Kyber 网络中有 4 个实体, 分别是用户、储备管理者、储备贡献者和平台运营商. 每个角色都以不同的方式独立地与智能合约交互. 用户可以是个人账户、智能合约账户和商家账户, 能够查询转换率并进行代币交易. 储备经理需要通过 KYC 认证, 在合约中锁定不同代币间的汇率, 保证交易正常进行. 储备贡献者向储备池贡献代币, 并从网络利差中获取利润. Kyber 运营商负责管理功能, 能够控制增加或移除交易对. Kyber Network 的系统示意图如图 6 所示.

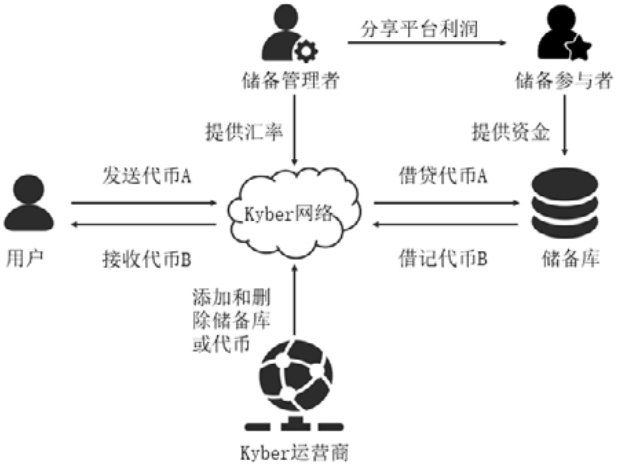

图 6 Kyber Network 示意图[39]

Kyber 的链上交易过程如下.

Kyber Network 由资金托管、交易撮合和交易清算三大功能模块组成, 其中, 储备库的主要作用是资金托管, 私人储备者作为数字资产资源提供者, 通过持有其部分资产获得利润, 储备经理人可以调整费率; 智能合约的一个作用是交换撮合, 它会遍历全网的储备库(类资金池), 寻找到价格最低的交易对, 给出报价; 另一个作用是交易清算, 在接收到用户代币后, 合约从储备库中去除一定量的目标代币发送到用户指定地址. 当用户指定地址为自己的地址时, Kyber 实现交易所的功能; 当用户指定地址为他人的地址时, Kyber 实现跨币支付的钱包功能.

Kyber 协议原理上与 0x 协议采用了同一种方式, 使用了链下的资金管理方式, 提出了储备库的概念, 保留交易的结算在链上操作, 尽可能地减少了链上事务, 提高了交易效率[40]. 同时, 根据 0x 协议中中继者的信任和中心化的问题, Kyber 协议中提出了多人参与、共享利润的方式, 参与者之间相互监督. 这种方式不仅提

高了储备库的信任度, 也降低了中心化的风险. Kyber 协议的特点见表 12, 具体分析如下.

(1) 可靠性: 用户的资产托管于智能合约上, 本身不存在资产安全风险. 交易撮合由智能合约遍历全网储备库完成寻找最低报价的工作, 智能合约在链上完成. 交易结算过程是区块链执行共识的过程. 满足可靠性量化条件 2;

(2) 可扩展性: 交易撮合过程需要智能合约遍历储备库, 交易量增大时可启动多个智能合约同时查询. 交易结算依赖区块链共识, 共识效率有上限. 满足可扩展性量化条件 1;

(3) 可监管性: 协议没有考虑可监管性. 但是协议常用于以太坊中, 其满足量化条件 1 和条件 2;

(4) 数据隐私性: 订单信息公开, 身份信息不用通过权威机构认证, 且不对外透露, 满足隐私性量化条件 1;

(5) 可回滚性: 协议未考虑可回滚性.

表 12 Kyber 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	4	1	5	7	0
交易撮合	4	1	5	7	0
交易结算	4	1	5	7	0

3.5 AirSwap协议

Airswap 平台建立在以太坊区块链上, 使用 ERC20 代币[41,42]. 该平台采用智能合约, 允许用户相互连接并执行交易. 通过“智能合约”, 用户可以轻松地在世界各地完成数字货币交易. 使用链外协商和链内结算, 能够提供点对点交易, 支持自由地进行价格协商、委托订单、交易撮合、交易结算等服务[43,44].

AirSwap 由 Maker、Taker、Oracle、Indexer、Smart Contract 这 5 部分组成, Maker 是提供订单的一方, Taker 是接受订单的一方, Oracle 用于向 Taker 和 Maker 提供定价信息服务, Indexer 是一种提供链下交易匹配和汇总的服务, Smart Contract 是一个以太坊智能合约. AirSwap 协议包括索引协议(indexer)和预言协议(oracle), 索引协议负责交易撮合, 预言协议负责订单定价. 由于交易是点对点的, 因此用户的身份信息保持隐匿. Airswap 的运作方式是允许任何用户在不考虑其匿名风险的情况下进行交易. 这意味着受监管地区的投资者可以在平台上进行交易, 从而绕开当地监管机构的监察. Airswap 协议交易流程参考其白皮书[45], 过程如图 7 所示.

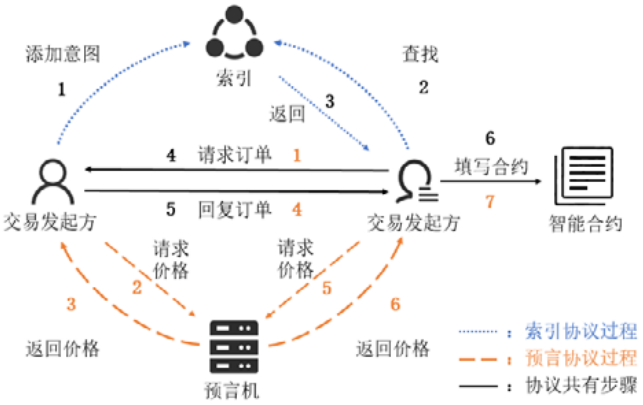

图 7 AirswapProtocol 示意图

Airswap 协议的特点见表 13, 具体分析如下.

(1) 可靠性: 用户的资产托管于智能合约上, 本身不存在资产安全风险. 交易撮合和资金提取过程是智能合约的执行过程. 交易结算过程是共识过程. 满足可靠性量化条件 2;

(2) 可扩展性: AirSwap 可以创建多个 AirSwap 网络来提高性能, 不同的 AirSwap 网络存储不同的信息,

当一个集群不能满足用户负载时, 用户可以通过创建新的 AirSwap 集群, 从而构建一个独立的 AirSwap 网络. 满足可扩展性量化条件 1;

(3) 可监管性: 该协议不遵守反洗钱和了解你的客户规则(KYC), 但是可以满足条件 1 和条件 2;

(4) 数据隐私性: 用户在区块链上的账户公钥就是身份, 无需向交易所注册个人信息和 KYC 认证, 亦即不存在个人信息泄露的问题. 但是交易信息公开, 满足数据隐私性量化条件 1;

(5) 可回滚性: 该协议没有考虑可回滚性.

表 13 Airswap 协议量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	4	1	5	7	0
交易撮合	4	1	5	7	0
交易结算	4	1	5	7	0
资金提取	4	1	5	7	0

目前, Airswap 的运作方式是允许任何用户在不考虑其匿名风险的情况下进行交易. 这就意味着受监管地区的投资者可以在平台上进行交易, 从而绕开当地监管机构的监察. 因此, AirSwap 在支持监管方面还有待加强.

3.6 熊猫模型

熊猫模型最开始的设计目标是为满足当前央行数字货币(central bank issued digital currency, CBDC)模型中交易速度快、可监管以及良好的可扩展性的要求, 之后, 该模型也同样适用于交易和清算等领域. 熊猫模型的设计思想是: 将账户信息和交易信息分开分析, 账户信息存储在账户链(account blockchain, ABC)中, 交易的执行和交易历史的维护由交易链(transaction blockchain, TBC)操作[44]. 这种双链架构的设计首先将账户和交易分开处理, 减轻了单链的处理压力; 其次, 在满足监管要求的基础上, 最大程度地保证了用户的隐私性. 最后, 双链架构可实现扩展性, 新增的账户区块链可以通过新增交易区块链来实现与其他账户的交易操作[28].

熊猫模型由 3 部分组成: 账户链、交易链以及监管节点. 账户链维护账户信息, 包括用户基本信息以及资产余额. 所有的信息修改操作都会被账户链记录, 该操作的目的是防止篡改. 交易链负责处理所有交易, 包括单链内部交易和跨链交易. 交易链收到交易后, 会将处理交易所需的信息向账户链申请, 处理结束后将交易结果返回账户链. 监管节点监控区块链的左右操作, 一旦发现交易中的违规行为, 能够快速定位违规账户. 因此, 账户链和交易链完成交易后, 需要将日志发送给监管节点以便监管. 熊猫模型正常交易过程可参考文献[44], 示意图如图 8 所示.

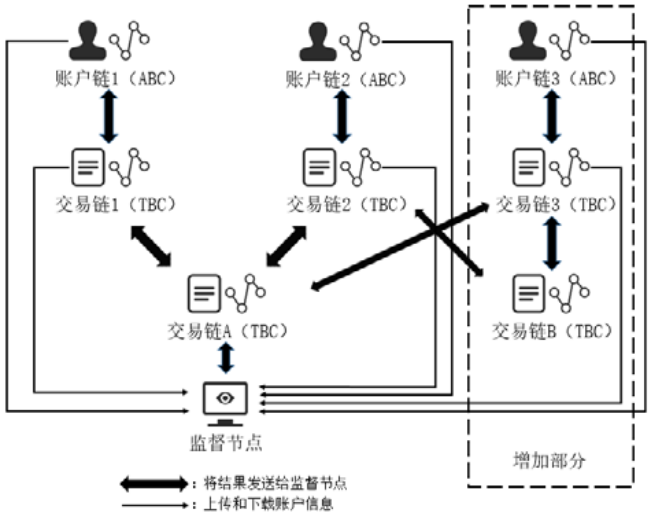

图 8 熊猫模型示意图

熊猫模型的特点见表 14, 具体分析如下.

(1) 可靠性: 该模型中, 资金托管、交易撮合以及资金提取是通过智能合约技术完成的, 其中, 智能合约的执行依赖于区块链, 熊猫模型中的共识是使用 PBFT 算法. 交易结算过程是使用 PBFT 共识算法完成的. 满足所有可靠性量化条件;

(2) 可扩展性: 模型使用 PBFT 共识算法, 满足可扩展性量化条件 2;

(3) 可监管性: ABC 和 TBC 在处理完交易后, 都需要将交易详情发送给央行. 央行对这些信息进行分析、建块, 并将块加入到自己的区块链中, 形成高级区块链. 央行可以在 ABC 和 TBC 中设立自己的节点, 这样, 央行就能够获取每一个区块链上的所有数据. 满足可监管性量化条件 1–条件 3;

(4) 数据隐私性: 使用公私钥保证用户隐私, 交易数据公开, 满足隐私性量化条件 2;

(5) 可回滚性: 该模型考虑了交易的可回滚性, 使用智能合约完成交易在特定条件下的可回滚.

表 14 熊猫模型量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	10	8	8	7	5
交易撮合	10	8	8	7	5
交易结算	10	8	8	7	5
资金提取	10	8	8	7	5

3.7 模型分析

总结上述几种交易协议, 可将这些协议分为原子交换模式、自动定价模式、中继者模式、点对点模式以及双链模式[45]. 下面分别描述这几种模式的特点.

原子交换模式的典型应用就是 Atomic Swap 协议, 模式原理与跨链原子交换的原理相同, 都是使用哈希锁实现交易的原子性, 但是应用场景不同: 一个应用于交易所中, 一个应用于跨链通信中. 交易协议的原子交换模式同样只是针对交易结算, 易与其他协议融合使用, 因此很多性能取决于底层架构. 其特点见表 15.

表 15 原子交换模型量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易结算	4	1	5	7	0

自动定价模式是分布式金融中的一种典型模式, 本文以 Uniswap 协议和 Bancor 协议为例介绍了两者的运行原理. 这两种协议只是分布式金融项目中的一类, 即保证交易的流动性, 而分布式金融项目还包括资产抵押平台、借贷平台、杠杆交易平台等. 这些分布式金融项目的运行原理有很多是根据早期经济学者提出的模型实现的, 例如 Bancor 协议. 甚至于, 这些模型很多随着计算机的发展已经在实际中投入使用, 例如 Uniswap 协议中提到的自动做市商并不是分布式金融项目中独有的. 但是随着区块链技术的发展, 区块链的分布式和难以篡改的特性, 让这些金融模型仿佛找到了一个量身定做的技术支持. 因此, 2019 年, 这些分布式金融项目在各大区块链平台上大放异彩, 取得了令人瞩目的成绩. 自动定价模型的特性见表 16.

表 16 自动定价模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	4	1	5	7	0
交易结算	4	1	5	7	0

中继模式一般采用“链下撮合, 链下结算”的方式, 这个模式的设计思想是: 认为自动定价模式中价格不稳定, 因此需要交易撮合; 同时引入中继者, 将交易撮合过程交给中继者处理以提高整个交易过程的效率. 本文介绍了两个中继模式的协议:0x 协议和 Kyber 协议, 分析了这两种协议的共性. 两个协议重点处理了交易撮合和交易结算两个部分, 资金托管和资金提取的实现取决于交易所平台的具体实现. 中继模式将交易撮合交给了中继者, 而交易结算是在区块链上执行的, 用户将交易需求提交给中继者, 由中继者撮合交易的双方(见表 17). 这个过程不可避免地存在中心化的风险, 因此一些协议中会引入一些激励机制避免中继者作恶,

典型的就是 Kyber 中的储备库方案.

表 17 中继模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
交易撮合	4	1	5	7	0
交易结算	4	1	5	7	0

点对点模式的典型应用是 Airswap 协议. 点对点模式与中继模式一样, 主要针对交易撮合和交易结算这两个过程. 交易结算依赖于底层区块链系统实现, 但是交易撮合的方式与中继模式不同: 中继模式是引入了中继者来完成交易撮合的过程, 而点对点模式则是通过向外部获取交易价格的方案解决交易定价的问题. 因此, 点对点模式的性能很大程度上依赖于底层区块链的性能. 但是这种模式很公平, 交易价格既不像自动定价模式那样存在价格波动大的风险, 也不存在中继模式中的中心化风险(见表 18). 因为交易撮合过程的运行效率也依赖于区块链平台的性能, 所以交易撮合的运行效率可能不如中继模式.

表 18 点对点模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	4	1	5	7	0
交易撮合	4	1	5	7	0
交易结算	4	1	5	7	0
资金提取	4	1	5	7	0

双链模式原本是针对央行数字货币提出的区块链模型, 因此这种模式针对的是运行效率、系统的可监管性以及可扩展性的问题. 运行效率一直是评估区块链系统性能的一个重要指标, 也是当下讨论区块链系统是否能够代替中心化系统中所诟病的一项性能, 所以双链模式通过将账户信息和交易数据分开处理来提高系统运行的效率. 双链模式分别在账户链和交易链中引入监管节点来实现系统的可监管性, 并针对账户链和交易链的特点提出了不同的扩展性方案. 双链模式与其他模式最大的不同在于重点针对了区块链系统中出现的难以监管、数据隐私性差以及系统扩展性问题, 并提出了切实可行的解决方案, 这些问题都是其他模式不重视甚至是忽略的问题. 双链模式的特性见表 19.

表 19 双链模式量化评估

过程	可靠性	可扩展性	可监管性	数据隐私性	可回滚性
资金托管	10	8	8	7	5
交易撮合	10	8	8	7	5
交易结算	10	8	8	7	5
资金提取	10	8	8	7	5

4 分布式数字资产平台的监管

目前, 分布式数字资产交易平台面临的一个最大问题就是监管问题, 很多系统由于数据难以溯源, 因此很难被监管, 最后被犯罪分子用于洗黑钱. 这一现象的出现, 让各国中央金融机构以及政府对在金融领域广泛使用区块链技术持有审慎的态度. 国际社会在总结了2008年金融危机的问题后提出的金融市场基础设施建设原则中强调了金融系统必须要具有可监管性[6], 但是目前, 很多平台都没有考虑这一点. 分布式数字资产交易平台要想得到更大的发展, 在实际应用中就不能脱离政府的监管. 因此, 分布式数字资产交易平台的监管问题是分布式数字资产交易平台发展中必须解决的一个重要问题. 这一节我们重点介绍几种目前典型的分布式交易平台监管方案.

4.1 熊猫模型和金丝猴模型中的节点监管方案

熊猫模型和金丝猴模型的运行原理和特征在第 2 节和第 3 节已有介绍. 这一节重点分析这两种模型中采用的监管方案.

在熊猫模型中, 设计者将监管单位设置为节点来参与每条链的运行, 从而得到所有的交易信息. 这一设

计让监管单位可以获得第一手的数据, 无需经过交易平台的整理再提交, 避免了数据篡改的发生. 在监管节点中引入协议层上监管, 将监管规则写入代码或者智能合约中, 代码的执行代表规则的执行. 这种方案实现了监管执行的自动化, 提高了监管效率.

金丝猴模型是一种链网模型, 主要解决了链与链之间的通信问题. 其中的跨链监管问题也通过引入监管节点来解决. 金丝猴模型中面临两类监管: 一类是对单链中的交易进行的监管, 一类是对跨链交易的监管. 该模型通过引入中继链来解决跨链问题, 因此可以在参与链和中继链共有的节点中设置一个监管节点. 采用这种方式既能监管链内的交易也可以监管链间交易. 同样, 监管节点通过引入协议层上监管来实现监管的自动化和实时性(如图 9 所示).

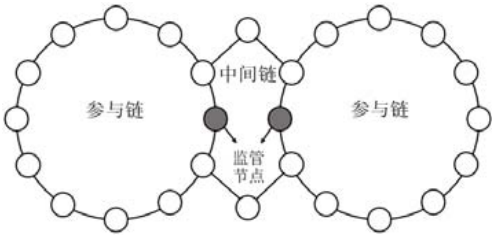

图 9 节点监管示意图

节点监管方案是通过引入监管节点参与系统运行来实现对交易用户的监管, 达到监管执行的自动化和实时性的效果. 这种方案适用于多节点参与的系统, 例如区块链系统, 在共识节点中加入监管节点, 可以很好地对系统中的金融交易进行监管. 但是这种方案不适用于中心化系统, 因为中心化系统一般只有一个中心节点处理交易不适合引入监管节点, 所以节点监管方案的适用范围有一定的限制(见表 20).

表 20 节点监管模型量化评估

可监管性量化条件	量化评估
1. 快速定位交易	3
2. 快速停止交易	2
3. 身份认证	3
4. 建立人物关系图谱	0
总计	8

4.2 Libra混合监管模型

2020 年 4 月 18 日, Libra 发布了第 2 版白皮书(后来改名为 Diem), 与第 1 版白皮书不同, Libra 将监管作为一项重要的研究方向. Libra 2.0 中使用了一种混合监管的方案, 将嵌入式监管与传统监管相结合. 嵌入式监管采用的是协议层自动合规技术, 传统监管使用的是已经存在的监管体系和机制, 二者结合共同解决 Libra 项目的监管问题. 协议层自动合规技术是 Libra 系统中引入协议级的自动化合规性控制, 可以针对链上的所有操作, 部分必须强制执行的监管规则可以直接写入 Libra 协议, 以确保规则能够执行. 在技术之外, 协会和政府以及监管机构合作制定相关合规措施, 并设立相关机构发现并阻止不正当操作.

综上所述, Libra 项目中的监管是一种嵌入式监管和传统监管相结合的监管方案, 引入协议级监管, 使监管常态化、自动化, 是一种轻量级的监管方式. 同时, 它也保留了传统的监管手段, 双管齐下共同完成交易用户的监管工作(见表 21).

表 21 混合监管模型量化评估

可监管性量化条件	量化
1. 快速定位交易	3
2. 快速停止交易	2
3. 身份认证	3
4. 建立人物关系图谱	2
总计	10

4.3 基于区块链的监管模型

分布式监管模型是利用区块链技术解决当前监管中出现的监管数据不完整和数据被篡改的问题[46−49]. 其中, 提出了一种动态交易记录(trading record, TR)技术自动地将交易上传, 依据这项技术保证数据的完整性, 利用区块链技术防止数据被篡改. 另外, 还引入了监管执行库和法规库以实现监管的自动执行.

分布式监管模型由 3 部分组成: 区块链系统、监管执行引擎以及监管法规库. 区块链(blockchain, BC)系统用于存储金融机构之间的所有交易信息, 交易信息是通过 TR (trading record, 动态交易记录)技术自动传到交易区块链上. 监管法规库用于存储各种监管规则, 且所述监管法规库中规则是可配置的, 也可以是外部法规库导入. 监管执行引擎用于执行监管法规库中的监管规则, 并通过读取区块链中的交易数据进行分析, 对满足监管规则的交易自动生成监管报告[50−55]. 分布式监管模型示意图如图 10 所示, 操作流程如下[47].

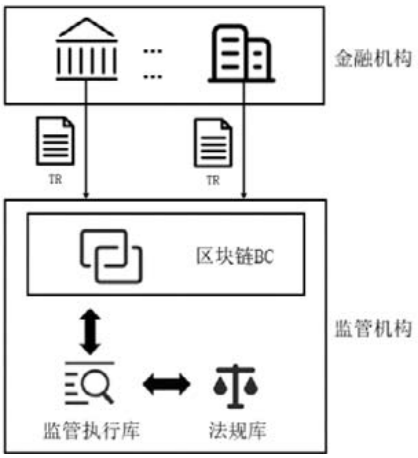

图 10 分布式监管模型示意图

基于区块链的监管模型是一种重量级的监管方案, 监管执行库和法规库的建立和运行成本较大. 但是监管执行库和法规库的建立可以快速定位交易, 有身份认证, 同时也建立了任务关系图谱. 但是快速停止交易需要金融机构的配合, 基于区块链的监管模型不能控制金融机构的交易处理操作(见表 22).

表 22 基于区块链的监管模型量化评估

可监管性量化条件	模型量化评估
1. 快速定位交易	3
2. 快速停止交易	0
3. 身份认证	3
4. 建立人物关系图谱	2
总计	8

4.4 监管模式分析

本节总结上述 3 种监管模型的特点, 概括了 4 种模式, 分别为: 协议层嵌入式监管模式、节点监管模式、外部监管模式以及混合监管模式. 下面分别对比总结 4 种监管模式的特点(见表 23).

表 23 监管模式量化总结

监管模式	关键技术	特点	性能	满足的量化条件	总计
协议监管模式	协议融合	兼容性好	轻量级	1 和 2	5
节点监管模式	系统中引入监管节点参与运行	适用于分布式系统	中量级	1、2 和 3	8
混合监管模式	嵌入式监管和传统监管相结合	双重监管保证监管有效性	中量级	1、2、3 和 4	10
外部监管模式	TR 技术	监管自动化	重量级	1、3 和 4	8

协议层嵌入式监管模式是将监管规则嵌入到区块链协议层中, 实现规则程序化. 该模式在熊猫模型、金

丝猴模型以及 Libra 项目中都可以应用, 是一种轻量级的监管方法. 协议监管模式的优点是运行效率高、成本低、兼容性强, 而且区块链每一笔交易都会经过嵌入式监管, 便于大规模普及, 是监管科技的一个良好的应用. 如果需要大规模的分析, 可以使用区块链数据湖的概念来解决这一问题[56,57]. 这样, 反洗钱的方式可以分为两部曲: (1) 大部分交易由于交易额小, 过去历史优良, 可以只经过快速轻量级的查验; (2) 若金额大、过去历史不佳, 就需要经过后面大数据平台的查验. 但是这种监管模式还处于发展初期, 需要进一步尝试, 协议层嵌入式的监管规则应如何定义以及如何将规则代码化, 都是当前协议监管模式需要解决的问题.

节点监管模式是一种适用于分布式系统的监管模式. 由于分布式系统多节点的特点, 可以将监管节点引入节点, 达到实时监管的目的. 典型应用就是熊猫模型和金丝猴模型, 这两种模型中都引入了节点监管模式, 让监管节点参与系统运行, 可以很好地避免数据的篡改问题. 该模式是一种中量级的监管模式, 通过参与分布式系统的运行, 实现实时监管的效果.

混合监管模式是一种将协议层嵌入式监管与传统监管相结合的监管模式. 典型应用就是 Libra 项目, 该项目中使用协议级的自动化合规控制实现监管的自动化, 同时还要执行链下的传统监管流程. 该模式充分考虑到当前嵌入式监管技术不成熟的特点, 但是嵌入式监管又是未来监管的重要发展方向. 因此, 在嵌入式监管的基础上保留传统监管模式, 不仅有利于嵌入式监管的进步, 同时又保证了监管的可靠性.

外部监管模式是一种利用区块链来保证监管数据不可篡改的监管模式. 典型应用就是基于区块链的监管模型, 该模型从外部入手引入 TR 技术, 让金融机构自动上传监管数据并存于区块链中, 然后由监管执行库和法规库共同完成监管. 这种监管模式适用于第三方监管机构对传统金融机构的监管, 保证监管数据的可靠性, 达到监管自动化的效果. 由于监管执行库和法规库的搭建成本高, 执行需花费大量算力, 因此外部监管模式是一种重量级监管模式. 这种机制由英国央行提出.

上述 4 种监管模型和本文 5 个原则的关系见表 24. 由于这 4 种模型都属于“可监管性”的机制, 因此与其他原则都未产生冲突, 但是隐私性一直与可监管性存在冲突. 例如, 2021 年国外暗网已经拒绝比特币交易, 因为比特币已被美国监管单位强力监管, 暗网如果继续使用比特币交易, 其洗钱的行为会被追踪到. 而国外合规交易所也要求下架基于零知识证明的数字代币. 同时, 暗网只愿意接受零知识证明的数字代币. 表 24 中“可以互相支持”表示系统需要更改后才能支持, 但在结构上没有问题.

表 24 监管模型和量化指标关系总结

监管模式	可靠性	可扩展性	可监管性	隐私性	可回滚性
协议监管模式	可以互相支持	可以互相支持	可以支持	冲突, 监管和隐私一直有冲突	可以互相支持
节点监管模式	可以互相支持	可以互相支持	可以支持	冲突, 监管和隐私一直有冲突	可以互相支持
混合监管模式	可以互相支持	可以互相支持	可以支持	冲突, 监管和隐私一直有冲突	可以互相支持
外部监管模式	可以互相支持	可以互相支持	可以支持	冲突, 监管和隐私一直有冲突	可以互相支持

5 总 结

分布式数字资产交易平台是数字资产交易的一个重要的研究方向, 本文基于 PFMI 提出了评估数字资产交易平台的 5 项基本原则, 并基于该原则, 从通信技术和交换协议技术两个方面对现有的分布式数字资产交易平台进行讨论和评估. 本文将区块链的跨链技术分为 3 种模式: 原子交换模式、公证模式以及中间链模式. 这 3 种模式各有优势, 其中, 中间链模式的应用最为广泛. 3 种跨链模型的特点见表 25.

表 25 跨链模型量化总结

模式	可靠性	可扩展性	可监管性	数据隐私性	可回滚性	总计
原子交换	4	4	0	7	0	15
公证节点模式	10	4	5	7	0	26
中间链模式	10	8	8	7	5	38

交易协议可分为 5 种模式: 原子交易模式、自动定价模式、中继模式、点对点模式以及双链模式, 其中, 自动定价模式来源于当下发展迅速的分布式金融项目, 中继模式和点对点模式主要解决了交易撮合和结算的问

题, 双链架构针对的是交易平台的可监管和可扩展问题, 每种模式都有其特有的优势. 有关5种交易模型的量化总结可见表 26.

表 26 交易模式量化总结

模式	可靠性	可扩展性	可监管性	数据隐私性	可回滚性	总计
原子交换模式	4	1	5	7	0	17
自动定价模式	4	1	5	7	0	17
中继模式	4	1	5	7	0	17
点对点模式	4	1	5	7	0	17
双链模式	10	8	8	7	5	38

分布式监管模型可分为 4 种模式: 协议层嵌入式监管模式、节点监管模式、外部监管模式以及混合监管模式. 其中, 混合模式是目前最为稳定的一种模式, 而协议层嵌入式监管模式则是最具发展前景的模式. 由于该模型是最新的技术, 而传统上区块链系统都没有考虑这一机制.

References:

[1] Tsai WT. STRISA: A New Regulation Architecture to Enforce Travel Rule. IEEE, 2021.

[2] Tsai WT, Zhao ZH, Zhang C, *et al*. Discussion on bank of England digital currency RSCoin. Electronic Finance, 2016(10): 78−81 (in Chinese with English abstract).

[3] Tsai WT, Yu L. Analysis of the application of blockchain technology in the financial field. Electronic Finance, 2016(5): 57−60 (in Chinese with English abstract).

[4] Wang R, Tsai WT, He J, Liu C, Deng EY. A distributed digital asset-trading platform based on permissioned blockchains. In: Proc. of the Int'l Conf. on Smart Blockchain. Cham: Springer, 2018. 55−65.

[5] Lin LX, Budish E, Cong LW, *et al*. Deconstructing decentralized exchanges. Stanford Journal of Blockchain Law & Policy, 2019, Jan(5).

[6] Tsai WT, Bai XY. System requirements for PFMI and financial blockchain: Are we ready to encounter the failure of the second wave of blockchain projects? 2018 (in Chinese). https://mp.weixin.qq.com/s/XXcpRfnvaF6jiLC5MW4A-g

[7] Daian P, Goldfeder S, Kell T, *et al*. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. arXiv: 1904.05234, 2019.

[8] Mcvanel D, Murray J. The bank of Canada's approach to adopting the principles for financial market infrastructures. Financial System Review, 2013.

[9] Payment systems: Liquidity saving mechanisms in a distributed ledger environment. European Central Bank and Bank of Japan, 2017.

[10] Russo D. CPSS-IOSCO principles for financial market infrastructures: Vectors of Int'l convergence. Financial Stability Review, 2013, 69−78.

[11] Tsai WT, *et al*. Smart Contract: Reconstructing Social Contract. Beijing: Law Press, 2020 (in Chinese).

[12] Chen P. Overview and application of mean time between failures (MTBF). Electronic Product Reliability and Environmental Testing, 2012, 030(B05): 272−276 (in Chinese with English abstract).

[13] Wu J. Establishment and application of experimental model based on mean time between failure (MTBF). Electronics World, 2018(1): 24−25, 28 (in Chinese with English abstract).

[14] Gunther NJ, Moeding S. USL: Analyze system scalability with the universal scalability law. http://CRAN.R-project.org/package=usl

[15] Heyman T, Preuveneers D, Joosen W. Scalar: Systematic scalability analysis with the universal scalability law. In: Proc. of the Int'l Conf. on Future Internet of Things & Cloud. IEEE, 2014.

[16] Gunther NJ. Guerrilla capacity planning. IT Professional, 2007, 4(4): 40−46.

[17] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: Proc. of the Int'l Workshop on Open Problems in Network Security. Cham: Springer, 2015.

[18] Gross D, Shortle JF, Thompson JM, *et al*. Fundamentals of queuing theory. Journal of the Royal Statistical Society, 1986, 35(5): 76−77.

[19] Bai XY, Tsai WT, Jiang XF. Blockchain design—A PFMI viewpoint. In: Proc. of the 2019 IEEE Int'l Conf. on Service-oriented System Engineering (SOSE). IEEE, 2019. [doi: 10.1109/SOSE.2019.00029]

[20] Zhongguancun Blockchain Industry Alliance. The Internet era is coming: The difference between Pallet and other cross-chain technologies. 2018 (in Chinese). https://mp.weixin.qq.com/s/jEJxx_5g8IYErfXUkoz0Cg

[21] Hearn M, Brown RG. Corda: A distributed ledger. 2019. https://docs.corda.net/_static/corda-technical-whitepaper.pdf

[22] Charlie Says. Does Corda need a consensus mechanism? 2017 (in Chinese). https://www.jianshu.com/p/bfcf191ec69f

[23] Charlie Says. Corda consensus mechanism in-depth analysis. 2017 (in Chinese). https://www.jianshu.com/p/35ef82e2625a

[24] Kwon J, Buchman E. Cosmos: A network of distributed ledgers. 2019. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md#abci-specification

[25] Qiaokelifalei. Technical interpretation of Binance white paper. 2018 (in Chinese). https://www.jianshu.com/p/15c9cadab89a

[26] POS Bakerz. Cosmos network: Validator overview. 2019. https://medium.com/posbakerz/cosmos-network-validator-overview-25d4bde67563

[27] Deng EY. Core algorithm of blockchain Internet model of inter-chain transaction. CN.201710493422.0.2017 (in Chinese).

[28] Deng EY. Double chain-type cross chain trading Internet of blockchains model core algorithm. CN.201710483789.4.2017 (in Chinese).

[29] barterDEX—Atomic swap decentralized exchange of native coins. https://github.com/KomodoPlatform/KomodoPlatform/wiki/barterDEX-Whitepaper-v2

[30] Komodo: An advanced blockchain technology, focused on freedom. 2018. https://komodoplatform.com/wp-content/uploads/2018/03/2018-03-12-Komodo-White-Paper-Full.pdf

[31] Peaster WM. The best decentralized exchanges for cryptocurrency trading. 2019. https://blockonomi.com/decentralized-exchanges/#Looking_ Ahead_Project_0x_ZRX

[32] Uniswap Whitepaper. 2018. https://docs.uniswap.io/

[33] Bancor.network. Bancor protocol: Continuous liquidity for cryptographic tokens through their SmartContracts. 2018. https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf

[34] Lochaiching. Ten pictures to show you the Bancor protocol. 2018 (in Chinese). https://mp.weixin.qq.com/s/jmoNsLO4npMWVodn4biS_Q

[35] gamefu_dl. Analysis of Bancor becentralized exchange. 2018 (in Chinese). https://www.jianshu.com/p/eb8f41fdd0d4

[36] Mr. C's Notes. Overview of decentralized exchanges. 2018 (in Chinese). https://www.8btc.com/article/306896

[37] Pintail. Uniswap: A good deal for liquidity providers? 2019. https://medium.com/@pintail/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2Eyal

[38] 0x: An open protocol for decentralized exchange on the Ethereum blockchain. https://0xproject.com/pdfs/0x_white_paper.pdf

[39] Hartmann T. Top 9 best decentralized cryptocurrency exchanges. 2020. https://captainaltcoin.com/best-decentralized-crypto currency-exchanges/

[40] KyberNetwork: A trustless decentralized exchange and payment service. https://home.kyber.network/assets/KyberNetwork Whitepaper.pdf

[41] Swap: A peer-to-peer protocol for trading Ethereum tokens. https://swap.tech/whitepaper/

[42] Mahalingam V. Decentralized exchanges (DEX)—What are they? Top picks for 2018. 2018. https://cryptovest.com/news/decentralized-exchanges-dex-what-are-they-my-top-picks-for-2018/

[43] Falk T. The 2020 guide to decentralized crypto exchanges. 2019. https://www.finder.com/decentralized-cryptocurrency-exchanges#compare

[44] Tsai WT, Zhao ZH, Zhang C, Yu L, Deng EY. A multi-chain model for CBDC. In: Proc. of the 5th Int'l Conf. on Dependable Systems and Their Applications (DSA). IEEE, 2018. 25−34.

[45] Mayer H. Survey of decentralized exchanges. 2018. https://blog.coinfabrik.com/survey-decentralized-exchanges/

[46] Tsai WT. Automatic real-time supervision reporting system based on double-chain architecture blockchain. CN.201810346971.X. 2018 (in Chinese).

[47] Tsai WT. Real-time and automatic supervision report system based on traditional blockchain. CN.201810346979.6.2018 (in Chinese).

[48] Tsai WT. Cross-border supervision reporting system based on double-chain architecture blockchain. CN.201810348879.7.2018 (in Chinese).

[49] Tsai WT. Cross-border regulatory reporting system based on traditional block chains. CN.201810348878.2.2019 (in Chinese).

[50] UF Financial Conduct Authority. Call for input: Using technology to achieve smarter regulatory reporting. 2018. https://www.fca.org.uk/publication/call-for-input/call-for-input-smarter-regulatory-reporting.pdf

[51] FIRA. Anti-money laundering. https://www.finra.org/rules-guidance/guidance/reports/2018-report-exam-findings/anti-money-laundering
[52] KYC3. Your guide to KYC and AML compliance. https://www.kyc3.com/quick-guide-to-kyc-and-aml-compliance/#what-is-aml
[53] FIRA.3310. Anti-money laundering compliance program. https://www.finra.org/rules-guidance/rulebooks/finra-rules/3310
[54] GMO Internet Group. The 5th phase of GMO blockchain open source software project: Reduces identification costs when opening bank accounts. 2017. https://www.gmo.jp/en/news/article/754/
[55] Elma S. Leveraging the opportunities of open banking: The KYC platform. 2018. https://www.capgemini.com/nl-nl/2018/10/leveraging-the-opportunities-of-open-banking-the-kyc-platform/
[56] Tsai W T, Xiang W, Wang R, *et al*. LSO: A dynamic and scalable blockchain structuring framework. In: Proc. of the BenchCouncil Int'l Federated Intelligent Computing and Block Chain Confs. Singapore: Springer, 2020. 219−238.
[57] Tsai WT, *et al*. Interlink Network. Shanghai: Oriental Publishing House, 2020 (in Chinese).

附中文参考文献:

[2] 蔡维德, 赵梓皓, 张驰, 等. 英国央行数字货币 RSCoin 探讨. 金融电子化, 2016(10): 78−81.
[3] 蔡维德, 郁莲. 区块链技术在金融领域的应用解析. 金融电子化, 2016(5): 57−60.
[11] 蔡维德, 等. 智能合约: 重构社会契约. 北京: 法律出版社, 2020.
[12] 陈鹏. 平均无故障时间(MTBF)的概述与应用. 电子产品可靠性与环境实验, 2012, 030(B05): 272−276.
[13] 吴君. 平均故障间隔时间(MTBF)实验模型建立与应用探讨. 电子世界, 2018(1): 24−25, 28.
[19] 蔡维德, 白晓颖. PFMI 与金融区块链的系统需求: 我们是不是预备遇到第 2 波区块链项目的失败? 2018. https://mp.weixin.qq.com/s/XXcpRfnvaF6jiLC5MW4A-g
[20] 中关村区块链产业联盟. 互链网时代来临: Pallet 与其他跨链技术的不同. 2018. https://mp.weixin.qq.com/s/jEJxx_5g8IYErfXUkoz0Cg
[22] 查理说. Corda 需要共识机制吗? 2017. https://www.jianshu.com/p/bfcf191ec69f
[23] 查理说. Corda 共识机制深入分析? 2017. https://www.jianshu.com/p/35ef82e2625a
[25] 巧克力伐雷. 币安白皮书技术面解读. 2018. https://www.jianshu.com/p/15c9cadab89a
[27] 邓恩艳. 一种双链式跨链交易的区块链互联网模型的核心算法. CN.201710493422.0.2017.
[28] 邓恩艳. 一种跨链交易的区块链互联网模型的核心算法. CN.201710483789.4.2017.
[34] Lochaiching. 10 张图带你看懂 Bancor 协议. 2018. https://mp.weixin.qq.com/s/jmoNsLO4npMWVodn4biS_Q
[35] gamefu_dl. Bancor 去中心化交易所解析. 2018. https://www.jianshu.com/p/eb8f41fdd0d4
[36] C 先生笔记. 去中心化交易所综述. 2018. https://www.8btc.com/article/306896
[46] 蔡维德. 一种基于双链架构区块链的实时自动化监管报告系统. CN.201810346971.X.2018.
[47] 蔡维德. 一种基于传统区块链的实时自动化监管报告系统. CN.201810346979.6.2018.
[48] 蔡维德. 一种基于双链架构区块链的跨境监管报告系统. CN.201810348879.7.2018.
[49] 蔡维德. 一种基于传统区块链的跨境监管报告系统. CN.201810348878.2.2019.
[57] 蔡维德, 等. 互链网：未来世界的连接方式. 上海: 东方出版社, 2020.

蔡维德(1958－), 男, 博士, 教授, 博士生导师, 主要研究领域为区块链技术, 软件工程, 分布式系统, 云计算, 大数据.

何娟(1994－), 女, 硕士, 主要研究领域为区块链系统, 智能合约.

王荣(1988－), 男, 硕士, 主要研究领域为区块链, 机器学习.

邓恩艳(1972－), 女, 主要研究领域为区块链, 软件工程.