PFMI 指导下的全新区块链设计：下一代区块链系统（二）

蔡维德、向伟静

2021 年 3 月 30 号

前言

本文是“下一代区块链系统”系列的第二篇。我们在上一文中提到发展下一代区块链系统所要考虑的设计原则，其中交易完备性和交易的监管是重中之重。本文将围绕分布式交易所中金融市场基础设施建设原则(Principles for Financial Market Infrastructures, PFMI)，在此基础之上分析下一代区块链金融系统。

本系列文章将比特币、以太坊、超级账本都定位为第一代系统，2020 年后发展的为下一代区块链系统。下一代系统在设计、架构、交易、共识、监管、扩展机制上都与第一代不同。

文（一）我们根据美联储、国际清算银行、英国央行等重要机构对央行数字货币（Central Bank Digital Currency, CBDC）的观点得出下一代区块链系统需要解决交易性、监管性、安全性、扩展性等问题，而交易性和监管性是第一代区块链系统没有重视的问题。

PFMI 是多年在许多系统累积经验才发展起来的，而区块链系统只有 10 年左右的历史，还未成熟。由于 PFMI 的内容丰富，本文只讨论 2017 年加拿大央行提出的实验报告。这份报告是世界第一次使用 PFMI 来评估区块链系统在央行系统里的应用，评估的结果却是负面的。这是很正常的结果，在新科技刚出来的时候，早期实验结果多半是负面的，但是进步后以后的实验才会成功。这次报告针对数字货币可能存在的风险指出了重要的研究方向，这些方向引导了我们过去几年的研究计划，包括交易技术上的优化和监管技术等。

我们认为区块链研究必须研究金融交易技术，并且在 2019 年将金融交易技

术列为区块链 10 大研究方向之一。本文将讨论交易技术，即流动性节省机制（Liquidity Saving Mechanism, LSM）。加拿大央行在 2017 年提出区块链系统需要处理 LSM，后来欧洲央行和日本央行也提出需要 LSM，而更早英国央行提出更新 RTGS 系统也是为了预备解决 LSM 的应用。

区块链设计需要多维度的优化，不能单线优化。过去一些区块链研究集中在共识机制（例如共识速度）。但是共识机制不等于交易机制，共识机制只是交易机制的一部分，单独共识机制不能解决交易完备性，而交易完备性是区块链金融系统最重要的属性。据文（一），美联储 2021 年报告没有提到共识速度是 CBDC 的必须条件，反而认为交易完备性是必要条件，由此可知区块链研究方向需要有一点调整。下一代区块链系统两个最重要的维度是交易性和监管性，根据这两个属性导出的区块链和传统区块链系统大不相同。区块链系统研究不能只专注于系统本身的研究，还需要和市场需求配合[13]，并且认为如果一个链设计时没有考虑 PFMI 的需求，很难在合规市场上使用[14]。

这份报告发布已有 4 年，中间获得了很大的发展,国内外对这课题的兴趣已经完全不同。在 2017 年时候这是新兴科技研究，现在却是新型货币战争的重要科技，而 PFMI 没有因为大家的关注或是新科技出现而降低重要性，反而越来越重要,由于 PFMI 启发了下一代区块链设计。以后区块链还要有许多新设计出现，而 PFMI 都会起到引导的作用。本文第 1 节首先介绍 PFMI 的历史以及 24 类原则，并且讨论 4 项和区块链相关的原则；第 2 节讨论 2017 年加拿大银行的报告以及我们的观察；第 3 节主要讨论我们的观点。

1. PFMI 简介：24 项原则

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的国际评估标准。PFMI 是通用原则，适用于每个国家的金融系统[1]。又由于每个国家的金融系统使用的软件和硬件都不同，相关的法律也不同，虽然有统一国家标准，在实际评估时还需要大量考量。但如果系统在设计时充分考虑了 PFMI 原则，确保服务的合规性、抗风险和扩展性，金融系统经常遇到的问题大部分都可以解决。

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 原则分为下面规则组：

- 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 risk），5）抵押品（collateral），6）保证金（margin），7）流动性风险（liquidity

risk)；

- 结算：7）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(participant-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(operational risk)；
- 准入管理：18）准入和参与要求(access and participation requirements)，19）分层参与安排(tiered participation arrangements)，20）金融市场基础设施的连接(FMI links)；
- 效率：21）效率和有效性(efficiency 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金融市场基础设施（Financial Market Infrastructure，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，考虑到许多方面，例如系统架构、安全性、隐私性、流动性管理和操作风险管理[2,3]。由于 2008 年的时候，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改就不能被世界央行采用[4,5]。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[6,7]。

1.1. 四项 PFMI 原则

第一项 可靠性：PFMI 多次提出这需求，就是金融交易系统在全方面都必须是可靠的，这包括不能有单点系统的问题造成系统瘫痪的情况。这点加拿大央行重复讨论。

第二项 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已经流动性机制具有系统性风险，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可监管性并没有统一标准。

第三项 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，并且提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。

第四项：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随时且高效的查询到所有账户及其相关的金融信息。数据隐私性量化和应用相关。

1.2. PFMI 的应用

PFMI 是通用型金融基础设施原则，使用时需要根据 PFMI 导出对应系统的评

估解释和方法。每个系统最后评估的方式会有一些差异，但大同小异。例如一个国家可能使用特殊数据库，而其他国家使用其他数据库，两个数据库不同，评估方法会有一些不同，但是都相差无几。因此 PFMI 不是食谱(cookbook)形式的指示，而是列举重要原则。而原则要落地使用，还需要对 PFMI 有深度的了解，页需要清楚被评估的系统的特性。

PFMI 公布的时候，区块链系统还没有流行，因此所有 PFMI 的原则的制定都是根据传统金融系统(图 1 左)。区块链流行后，多人提出使用 PFMI 来评估基于区块链的金融系统评估。最初的评估方式是根据公链或早期联盟链制定，属于早期探索材料，第一代区块链系统的评估方法由此出现。加拿大央行、欧洲央行、日本央行在 2017-2018 年做的实验就是评估第一代区块链系统。后来第 2 代区块链系统出现，于是需要第 2 代评估系统的方法。

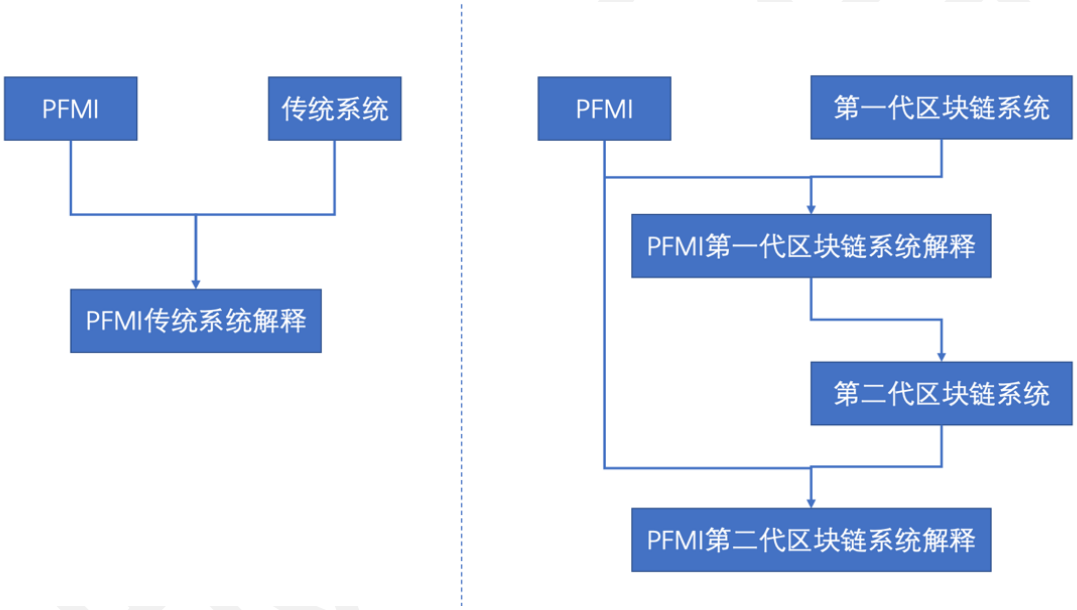

图 1 PFMI 第二代区块链系统解释发展

图 1 清楚表明，虽然 PFMI 原则不变，但是因为被评估的系统不同， PFMI 解释和评估方法会不同。

2. 加拿大央行评估第一代区块链金融系统

2017 年加拿大央行发布报告《贾斯珀项目：分布式批发支付系统可行吗?》(*Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?*)率先提出使用 PFMI 来评估区块链系统，后来欧洲央行、日本央行都跟随。这份报告虽然发布已有 4 年，但是从今天的观点来看，这报告里面的信息还是新

鲜的，如今许多区块链系统还不能解决该报告发现的问题。

2.1. 两个挑战

加拿大央行提出两个挑战：

- **“央行存款数字货币”**（Digital Depository Receipt，DDR）的挑战：这个 DDR 作为商业银行间的结算货币，等于是“数字现金”，由加拿大央行保证，并且有对应的央行系统内的法币。

我们的观察：

这些概念后来英国央行、摩根大通银行、英国 Fnality 公司、美国财政部等机构采用。这里加拿大央行认为的挑战是实现安全可靠地在不同账号上转移 DDR。

- **LSM：** LSM 机制是重要的机制，在今天金融系统环境下，银行间的结算大都是每天晚上结算一次，但是这会给金融系统带来风险，由于系统晚上才结算，出问题也只能等到晚上才知道。于是央行也使用实时全额结算系统（Real-Time Gross Settlement，RTGS）。在 RTGS 系统上，结算是及时的而且是全额的，不需要等到晚上。英国央行也提出彻底改变 RTGS 系统的方案，并由区块链系统来实现。可惜的是，英国央行这项目失败了。加拿大央行第一个实验，是根据每一笔交易都做在数字钱包上做实时结算。（备注：这可能不是最好的方式，由于这点复杂，以后再讨论）。而后来的实验，可以允许有延迟的结算（这样交易不能实时完成）。系统会根据交易的重要性选择实时结算，还是延迟结算。延迟结算方便了银行系统，但是对客户不太友好。

加拿大央行认为 LSM 机制必须是中心化处理，这对分布式的区块链系统是一个挑战。如今我们已经开发了分布式 LSM 机制，在一个块中做 LSM。后来的第 2 代区块链系统还有其他机制来化解这问题。

我们的观察：

有学者认为基于 token 的数字货币系统不需要 LSM 机制。由于数字货币只要 token 存在，就是代表资金是真实的，数字货币就是数字现金，没有流动性问题。这在单一货币单层封闭系统，例如比特币、以太坊这样单一“货币”系统中确是这样。在这些系统，交易也是一块（里面含多笔交易）接着一块串行交易完成的。

但是在多币种复杂交易交易平台却可以同时间进行多资产（不同数字货币、数字股票、数字衍生品、数字房地产等）和多种交易方式，而且可能有多层架构（例如央行-商业银行两层架构，或是链-服务商两层架构）。在这样复杂环境，这问题还是研

究的课题，例如脸书稳定币系统就是多币种双层架构（链-服务商架构）复杂交易平台。

加拿大央行、欧洲央行、日本央行都在央行系统内进行 LSM 实验，表示他们认为这还是一个问题。而加拿大央行的实验使用央行的 DDR，其实就是加拿大 CBDC 的原型。起码在 2017 年，他们还没有被说服 LSM 是不需要的。

2.2. 金融稳定风险评估

信用和流动性风险：传统上信用风险是指交易对方因种种原因，不愿或无力履行合同条件而构成违约，致使交易对方遭受损失的可能性。流动性风险指商业银行虽然有清偿能力，但无法及时获得充足资金以应对到期债务的风险。2008 年世界金融危机就是因为信用和流动性风险造成的危机。

这里加拿大央行实验的平台使用 DDR（这可以看成是批发 CBDC 的雏形），这是央行支持的数字货币，没有信用风险，而且只要 DDR 到位，代表资金到位，没有流动性风险。

我们的观察：

英国央行在 2014 年研究比特币时发现，比特币没有信用和流动性风险，才开启数字英镑计划。但比特币背后没有实质的资产做抵押，数字英镑预备以央行的英镑来为 CBDC 背书。由于央行没有信用风险，因此数字英镑理论上来说没有信用和流动性风险。

加拿大央行的设计和英国央行的设计一样，没有信用风险，由于 DDR 就是加拿大央行发行的 CBDC，有央行法币的背书。

可是直到今天大部分稳定币还没有这样的特性，只有商业银行的存款背书，没有央行的背书，有信用风险。

2020 年美国财政部允许银行可以托管稳定币的准备金，2021 年 1 月美国财政部宣布银行可以自己发行稳定币，但是必须有 1 对 1 对应的法币（美元）存在银行内，并且每一天都要报告准备金的数目。这种策略减少大量风险，但风险依旧存在。

数字代币还包括风险极大的稳定币，在地下市场上流通，有非常大信用风险。地下市场认为其还有其他风险比这信用风险更严重（例如被发现洗钱），所以明明知道该稳定币有信用风险却还在使用。

至于流动性，后来欧洲银行和日本央行也使用中心化的 LSM（下图 2）；后来英国在 2019 年开发出“一币一链一往来账”更大程度上增加流动性，同时我们提出在“块中 LSM”来增加流动性。

超级账本提出在入口处由一个节点从事排序，解决交易完备性，而这节点也可以同时做 LSM。但是这样入口处节点成为整个系统的控制中心，严重影响系统安全问题，也违背区块链分布式架构设计原则。这问题是我们在 2017 年发现的问题，两年后美

国摩根大通银行也同意我们的观点，认为原来超级账本的设计不是区块链系统。

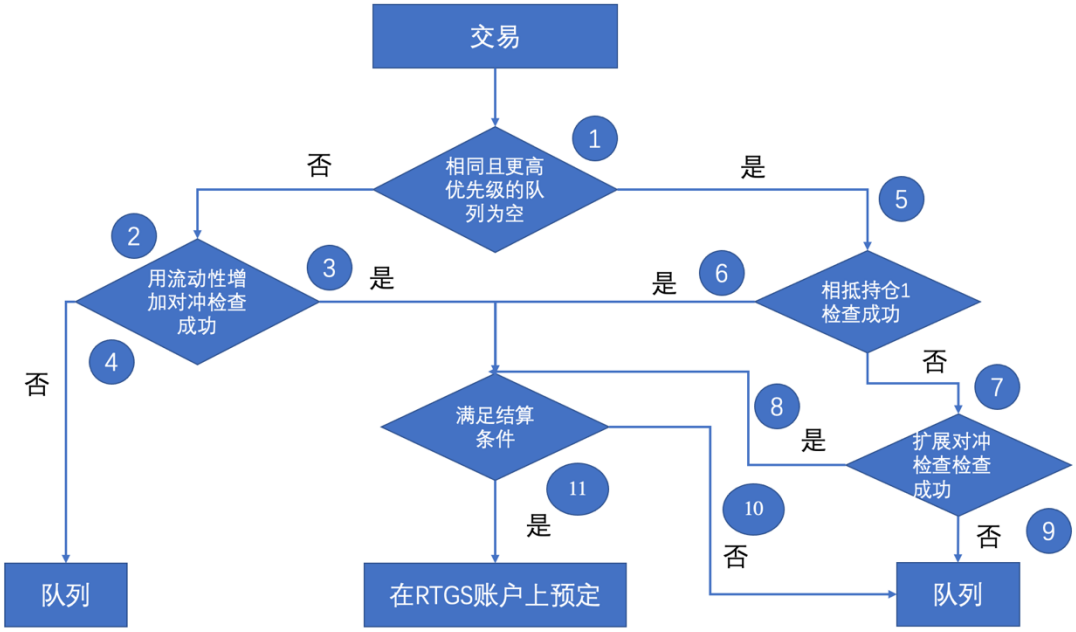

图 2 欧洲央行的 LSM 机制

指导方向：

加拿大央行清楚表明数字货币第一要素不是设计区块链系统，而是考虑数字货币的信用和流动性风险。同时这两个风险主要是靠货币制度来解决，也需要考虑现代金融交易的流程。这些确定后才考虑如何设计和部署区块链系统。例如蝴蝶模型，是根据美国财政部制定的数字稳定发行和监管制度开发出来的作业模型，模型出来后，才考虑如何使用区块链来实现蝴蝶模型。英国 Fnality 的模型也是先设计发行交易模型（一币一链一往来账后模型），再考虑如何实现这模型。

结算风险：传统上，结算风险是在结算过程中，因职员工作失误或违反有关结算规定造成损失的风险。这是由于作业时发生问题产生的风险。加拿大央行提出 2 个结算风险：

- **结算流程风险：**分布式账本（区块链）系统在这交易流程中，是不是一定会完成？会不会中间一些其他事件影响到这交易？

- **最终结算风险：**结算时间能不能确定？

第一个风险结算风险没有出现在原始 PFMI 文件内[7]，是加拿大央行根据 PFMI 和第一代区块链系统而加上的解释（图 1）。但是加拿大央行这里并没有展开了

讨论。一笔交易会不会因为其他因素而不能完成交易流程？回答是可能的。通讯问题、加解密问题、同步并发的问题以及 LSM 的问题，都可能造成这笔交易出问题。

第 2 个风险是这交易是不是最终能够结算，如果可以，在那个步骤结束？在公链，每一的共识代表一次结算的可能性，但是这是有概率的。每一次共识只是代表一笔交易结算存在概率性。这样每一次共识意味这可能就是最终结算。

但是在联盟链，只要设计正确，就有确定的结算结束步骤。加拿大央行认为只要 DDR 到达一个数字账户（数字钱包），就认为该交易结算完成。由于使用 DDR 币，代表 CBDC，没有信用风险，一旦 DDR 进入一个账户，表示账户有确定的资金。因此使用联盟链就不存在这样的问题。

我们的观察：

过去有学者认为所有区块链系统有最终结算问题，因为不清楚何时可以认为结算完成。对此加拿大央行并不同意。只要 DDR 进入账后，就代表结算结束，这是联盟链的特性。

在第一代联盟链，交易也等于结算。即使是第一代区块链系统，也只有公链才有最终结算问题。公链由于有分叉的可能性，结算需要等一段时间，于是何时可以知道结算完成是一个问题。而联盟链没有这个问题。

相反在第 2 代区块链系统，共识机制和交易机制解耦，交易和结算也解耦，最终结算是由结算机制决定。

指导方向：

结算流程风险和最终结算风险都是区块链设计的重要课题。第一代区块链系统都是死绑定，例如交易和共识绑定，交易和结算的绑定，作业有很大的限制且不符合现在金融系统交易的原则。PFMI 将交易和结算分离，而且交易完成后可以回滚，这些在第一代区块链没有做到的。这里最重要的指导是“根据现代金融系统交易和监管原则来设计区块链系统”。以这样方向出发，下一代区块链系统和第一代就有巨大的差距。

操作风险：加拿大央行认为区块链系统有 3 个操作风险： 1）弹性（resilience）风险； 2） 安全（security）风险； 3）扩展性 （scalability）风险。因为这次是实验，不好从安全角度分析，加拿大央行只有在弹性和扩展性风险上做分析。

弹性风险：一个系统有弹性代表这系统有足够的灵活度，可以动态调整系统来维持系统作业和性能。

加拿大央行认为公链的弹性是可以的，因为以太坊在公开环境下运行多时，即使出现过问题（例如 2016 年的 The DAO 事件），但是系统后来依旧在运行。不论是公链还是联盟链，一旦加上其他机制，例如加入中心化的 LSM 机制，这子系统一出现问题会影响整个系统。对此加拿大央行认为有 3 个风险：

- 密钥管理、身份认证、系统管理大都是中心化机制；这些机制会增加整个区块链系统的风险；
- 有些区块链系统有公证节点（不是每个节点都是公证节点），这些公证节点如果出现故障或是被攻击，会影响到整个系统的弹性。若是每个节点不具有同样的信息，公证节点出问题整体系统出问题的概率大大增加。加拿大央行认为这是个严重问题。
- 在央行系统，其中一个节点会是央行，这个节点一旦出现问题，整个国家支付系统就停顿。所以这个特殊节点需要有非常强大的弹性。加拿大央行认为在央行系统，不是每个节点会有同样的义务和权限（不对称的权限）。

扩展性风险：在扩展性上，加拿大央行每天处理 32 万笔小额支付，每天最高交易速度时平均一秒 10 笔交易。而以太坊当时一秒可以处理 14 笔交易，所以加拿大央行认为以太坊系统处理交易速度可以满足平时的需求，但是高峰时段可能达不到要求。

我们的观察：

过去区块链系统处理速度一直被诟病。但是加拿大央行在 2017 年报告对此进行反驳，我们在 2018 年也提出同样观点，脸书同样在 2020 年论文中提到过去长期对区块链系统的批评是不合理的。如果只是系统平均速度做决定，区块链系统早就可以在央行系统里使用。

特别是在批发阶数字货币层，区块链系统处理速度早就可以满足日常的交易处理需求。欧洲央行提出银行间交易（批发数字货币）速度一秒不到 30 笔，日本央行的银行间交易更小，而加拿大央行的银行间支付数目最小（低于 2），低到当时的区块链系统都可以使用。即使是大型交易所，如纽约股票交易所、上海股票交易所等，平均交易一秒都没有超过 1000。而在 2017-2018 年区块链系统每秒已经可以稳定超过一秒 7000 笔交易。

上面是以平均值来算，当时的区块链系统已经足够。欧洲银行报道在高峰时间大部分一秒不到 200 笔交易（这样高峰会长达几分钟），而最高峰时候是一秒 600 笔交易，但这最高峰只长达几秒。但是一秒 600 笔交易还是低于当时可以完成的联盟链系统速度。

对于央行以及股票交易所系统，平均速度不是唯一的评估标准，其他因素更重要，例如交易完备性、监管性等。因为需要处理 KYC、AML、结算等，这些会增加交易完成时间，但是交易速度不会降低。这在文（一）有讨论。

指导方向：

弹性风险和扩展性风险的重要指导是区块链的设计必须维持交易性和监管性。不能有了弹性，没有交易性或是监管性；或是有了扩展性就失去交易性或是监管性。许多金融应用不需要高速交易，但要保证有正确和安全的交易，而且可以全程监管。如果一个系统只能选择交易性或是扩展性，那么交易性的优先级必定要高于扩展性。即使不能扩展，系统还可以在小范围运行；但是有扩展性，而没有交易性，就有系统性的金融风险，伤害更大。

2.3. 透明度（Transparency）和隐私性(Privacy)

透明度风险是指金融系统公开信息不够产生的问题，例如金融交易所需要公开交易流程，合规流程和数据等；稳定币需要公开准备金。一旦事件发生，客户可以知道经过的流程，可以据理要求赔偿。另外金融系统必须提供监管单位需要的数据方便监管单位执行任务。原始 PFMI 文件竟然有 32 次提到透明度的需求。

我们的观察：

加拿大银行在透明度上没有做大量讨论，但是后来美国财政部和 SEC 等单位大力批评数字代币的透明度。美国 SEC 认为一数字代币稳定币一直不肯有透明度，后面的准备金从没有清楚过，也发生内线交易现象。这是都是不合规或是被严令禁止的活动。

隐私性一直是金融系统的重要条件，客户信息不能让无关的人知道。

加拿大央行认为批发支付系统（银行间交易就是批发支付）的一个基本要求是，参与者需要对未参与交易的各方保持交易的隐私性。这是为了以防止其他参与者试图利用这个信息。同时，加拿大央行认为他们应该看到所有交易数据。这隐私保护不适用央行监管单位[14]。

对于公链，交易信息公开（几乎没有隐私），参与者的客户也可能喜欢或要求这种隐私性。但加拿大央行不接受这样的设计，认为这不适合任何央行或是银行作业。

相反，基于公证人的 DLT 系统，如 Corda 系统，可以有比较好的隐私性，因为可信的第三方(例如参与的加拿大银行)帮助验证所有交易。但是 Corda 系统有一个严重问题，就是参与共识验证的只有部分节点，所有节点获取的信息不一致，没有参与共识的节点缺少相关信息，这就引起透明度问题。缺乏透明度会产生许多问题：

- **可靠性（弹性）出问题**：每一笔交易只有部分节点参与共识和记录，即使参与的公证员也没有完整账本记录。若是一个或多个节点上的信息被损坏，可能就无法重建整个数据库。这表示传统上区块链系统一直标榜的可靠性事实上不靠谱。

- **解决方案也不靠谱**：加拿大央行提出一个解决方案就是使用中心化数据库来维持这些数据，就是有一个节点会参与所有共识和数据记录（而加拿大央行拥有这节点）。但是这样的设计，央行的节点会是整个系统的中心，在性能上会是瓶颈。要解决这问题，可以有多个中心，例如图3所显示。问题是这样的设计，和传统中心化的系统的差距在哪里？整个设计又回倒中心化系统。

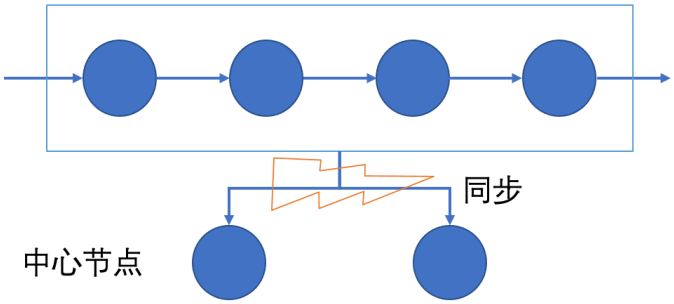

图3 中心节点成为最大的瓶颈

- **弹性和隐私保护必须同时存在**：根据加拿大央行对Corda的评估，认为系统弹性和隐私性很难一同成立。

我们的观察：

这里加拿大央行讨论一个严肃的问题，公链共享交易信息，因此违反了**隐私性**，不能在央行系统里面使用；但是加拿大央行认为像Corda每个节点所拥有的信息不相同，保证隐私性，却损失了**可靠性**（**弹性**）。这问题引导第二代区块链系统的设计。

其实这个设计还有两个严重问题：监管性和交易性。

监管性：由于每个节点拥有不同信息，监管系统如何找到需要的信息？最简单的方法就是在每个节点上寻找，但是这会很不方便。3.2节会继续讨论这问题。

交易性：如果一个节点需要验证一笔交易，但是这个节点并没有以前的交易信息。这节点应该如果处理？最简单的方法就是在每个节点上寻找相关信息，但是这也非常不方便。交易完备性也是一个问题。3.2节会继续讨论这问题。

这样像Corda节点有不同信息的类似区块链系统（他们不是区块链系统，而是类

似系统），其实问题非常多而且复杂。

指导方向：

这里加拿大央行清楚表示对客户有强隐私性，但是在监管单位前是没有隐私权。而且一个重要区块链设计原则就是方便监管单位找到相关数据。区块链设计不能逃离监管，而是辅助监管，例如加上嵌入式监管机制。

这点美国CFTC在2018年也提出相同概念，认为区块链系统两个最大的价值是完成交易和监管交易，存证不是区块链系统最大的价值。

2.4. 加拿大央行研究报告的总结

加拿大央行认为：

- 成本节约似乎不太可能通过核心系统本身来实现，而更可能通过减少银行对帐成本来实现。目前的核心系统已经非常高效。
- 如果其他应用程序可以建立在核心现金支付分布式账本系统(如金融资产清算和结算，贸易融资)之上，就有可能节省更多的费用。
- 在实际的生产系统中，需要权衡系统成员验证数据和事务的范围和信息共享的范围。
- 虽然 DLT 的目标可能是减少集中式风险，但如果应用于批发支付系统，仍然需要大量的集中式监管(如节点的许可和操作标准的设置)。

加拿大央行认为区块链可实现多个金基础设施的交互，可以通过将 FMI 整合降低交易成本，提高交易速度，最终实现监管。

3. 我们的分析

3.1. 报告特色

在短短 11 页报告中，加拿大央行提到 PFMI 原则 9 次，表示 PFMI 起重要的指引，这份报告是具有下面特性：

- 第一次使用 PFMI 原则来评估区块链系统，而今天大部分区块链系统的评估还没有使用 PFMI 原则；
- 第一次以金融风险来评估区块链系统，今天大部分区块链系统的评估还是根据技术指标，而不是以金融风险来评估；
- 第一次使用央行支付场景来评估区块链系统，直到今天，许多评估还是根据公链评估标准在评估，例如共识的速度。但是共识速度不是金融市

场的重要指标，在文（一）美联储评估央行数字货币文章都没有提出“共识速度”这指标，而提出交易性和监管性为最重要的指标。

- 以金融风险的角度对第一代区块链系统提出尖锐的问题，挑战当时流行的区块链系统，并且提供第二代区块链系统指引的方向。

我们可以从加拿大央行学习到，评估一个基于区块链支付系统，要以金融风险出发，以金融市场的标准流程出发。当我们从这两个角度出发来评估区块链系统，得出的结论可能和以前评估结果不同。

3.2. 不同节点存不同信息的问题

在 2.3 节，加拿大央行提出可靠性的挑战，但是我们提出监管性和交易性的挑战。而在许多区块链系统里还有其他问题，例如基于有向无环图（Directed Acyclic Graph, DAG）的共识机制的系统，或是一些使用分片技术的系统内。这些方案有一共性：就是不是每个节点都参与共识，只有部分节点参与。由于参与的节点数目降低，共识速度大增，但同时又带来风险。

3.2.1 固定节点验证

固定节点验证就是每个交易分类，每一类的交易由不同组合的节点参与共识。而这组合方式可以用优化算法(Optimization)来解决。只要知道一笔交易的属性，就知道哪些节点会参与共识机制。例如一笔 2 个银行之间的交易，共识节点可以是这 2 个银行的节点以及其他节点。这种方式的缺点是，不同种类的交易会一直出现，新的金融机构也会出现，金融机构也会重组。每一次改变，就需要重新计算节点安排的算法。

3.2.2. 动态随机选择共识节点

动态随机选择共识节点也是常用的方式，例如把一个交易随机送给一个分片处理，或是随机找几个节点来共识。由于参与的节点少，共识可以很快完成；特别是在不同节点，或是不同分片上，还可以并行处理。但是这种方式还有许多问题。加拿大央行提出区块链系统需要处理 LSM，如果使用 LSM，系统会更加复杂（3.2.3 节会讨论）。 加拿大央行，在交易量大的一天平均有 260 亿加元使用 LSM，而 340 亿加元没有使用 LSM。如果没有使用 LSM，问题还是很多：

- 由于没有使用 LSM，流动性可能不够，当流动性不够的时候，系统就不能继续进行。一个解决方案就是只处理小额支付，而不处理大额支付，来减少这问题的出现。

- 即使限制交易额，流动性还是可能不够，无法适应客户量逐渐增加的情况。例如脸书稳定币系统，每个虚拟资产服务提供商（Virtual Asset Service Provider, VASP）管理大量客户，可以限制每一笔交易额，但是在 VASP 之间的交易，交易额还是很大。脸书现在的设计是区块链系统不处理 VASP 内部客户交易，只处理 VASP 之间的交易（等于批发数字货币机制）。但根据 2020 年美国监管科技公司的数据，VASP 之间的交易大部分是跨境支付，如果每一笔 VASP 之间的交易都需要经过脸书链来解决，跨境相关的问题就难处理。

- 系统可以使用 RTGS 系统来解决这问题。但是基于区块链的 RTGS 系统一直还没有做出来。如果需要使用 RTGS，只能使用传统 RTGS 系统。

3.2.3. 如果系统还有 LSM 机制

LSM 机制带来的问题会更严重，因为

1) 加拿大央行提出中心化的 LSM 机制，这机制本身就是另外一个问题（可靠性）的来源；

2) LSM 机制还会延迟相关的交易，使这些交易不能马上结算。例如脸书系统， VASP 之间的交易需要经过脸书的区块链系统，需要等到链上交易全部完成，下面参与的交易才能结算。例如一个 VASP 机构 A 和另外一个 VASP 机构 B 做交易，需要通过脸书的区块链系统，而且还要使用 LSM。于是，A 会先到收集和 B 相关的交易，收集多了，才做一次结算，结算后差价，经过区块链系统处理。A 和 B 需要等到区块链交易结束后，再内部结算，把相关的客户账户算清楚，才完成所有相关交易。加拿大央行报告这 LSM 机制会平均会延迟交易时间超过 6 个小时。这表示 LSM 机制还有许多地方可以进步。

3.2.4. 四个解决方案

- 共识节点共识后，再广播给每个节点：这是最简单的方案，共识时只有少数节点参与，但是共识后，所有节点都收到信息。这种方案下所有节点都需要收到同样信息才能解决交易性和监管性问题。从这个角度看，第一步其实就没有意义，因为第 2 步共识，就是要求所有节点都参与共识。

- 共识节点完成共识后，再广播给特殊节点，例如中心节点，如图 3，即不需要所有节点参与共识，只有部分节点参与共识并拥有所有数据。但是中心化的节点会给系统带来极大的风险，也是易受攻击的地方。

- 维持原来的机制，不论是交易或是监管，都要在每一节点上寻找。此方案有可靠性、交易性、监管性三个问题同时存在，而且共识速度越快，出错的机率越大，系统性风险就会增加。在过去几年，国外提出一秒可以完成 60 万笔交易。如果在这种环境下，假设每 10 万笔交易只会出错一次，代表每一秒会有 6 笔交易出错，这 6 笔交易就会瘫痪整个系统。因为在第一代区块链系统中，一块中如果有一笔交易出错，在这块所有交易都算失败，需要重新来。这样每一秒如果有一笔交易出错，整个系统可能就不能稳定，何况是 6 笔交易出错。因此在过去几年，我们一直认为共识速度不是区块链最重要的研究课题，而是首先要保证交易完备性和系统可靠性等其他要素。

- 使用第 2 代区块链系统：第 2 代区块链系统共识和交易解耦，一笔交易失败，只要重新执行这笔交易，而不需要重新执行这块内所有交易。以上问题都能解决。

3.3. 区块链监管基本原则

根据加拿大央行实验报告，我们提出三项可监管性的原则：

- **快速定位交易**：这是监管第一个必要条件，找不到交易信息就不可能监管该交易。加拿大央行在 2017 年的一个实验报告批评 Corda 连账户和交易信息都难找到，由于节点可以存不同信息，监管系统必须先找到存有该信息的节点，然后在节点处拿到信息。这样的设计增加了监管的难度；

- **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。Libra 2.0 就考虑在实时停止交易的需求，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，只要在交易没有结算前，都可以停止这交易；

- **身份认证以及建立人物以及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。由于这样机制需要大量计算，这些大都是在交易前和交易后进行监管计算。

有一些逃避监管的区块链系统需要花费大量时间找到相关交易信息，例如比特币系统就是这样设计，token 只用一次。这就好比小偷使用偷来的车子作案，作案结束放弃车子，避免公安使用车子牌照找到小偷。要解决这问题，区块链系统必须有嵌入式监管机制，每一笔交易都经过监管流程，而且可以有权停止交易。

4. 总结

下表总结了上文中提到的各项风险，对比了各项风险的传统定义和在区块链上的新定义，对应的各项研究技术和指引我们的研究方向。

表 区块链风险及发展方向

风险	传统定义	区块链系统解释	技术	指引的方向
信用风险	借款人、证券发行人或交易对方因种种原因，不愿或无力履行合同条件而构成违约，致使银行、投资者或交易对方遭受损失的可能性	因参与者在区块链交易流程中例如付款、清算和结算过程中，因为参与者无法履行区块链和智能合约协议而产生的违约风险	DDR（2017）、合成 CBDC（2019）、蝴蝶模型（2021）	这里区块链只是辅助的工具，而先需要有一个理论框架，例如合成 CBDC、蝴蝶模型[9]
流动性风险	无法及时获得充足资金或无法以合理成本及时获得充足资金以应对资产增长或支付到期债务的风险	数字货币如果设计正确，流动性风险小	LSM、Fnality 模型（一币一链一往来账后）来增加流动性	减少往来账户（减少日中交易额），使用 token（有 token 代表可以流动）、块中 LSM（分布式机制）
结算流程风险	银行在结算过程中，因职员工作失误或违反有关结算规定造成损失的	一笔交易能够走完基于区块链的金融系统的交易流程	第 2 代区块链系统（2020）	整体区块链系统的稳定性，共识和交易解耦来减少需要重新处理的交易以及增加系统稳定性，避免系统因为

	一种风险			子系统出错而瘫痪；第2代区块链系统（交易和结算分开，区块链系统可以产业化）
最终结算风险	传统系统没有这特殊风险，只有在公链才有这风险	一笔交易能够完成结算，而且可以预知在那个步骤完成结算	第2代区块链系统（2020）	共识和交易解耦可以有确定的结算步骤而又可以有回滚机制；这是第 2 代区块链系统特性
弹性风险	在部分子系统出问题的情形下，系统仍然可以继续进行完成需要完成的业务	区块链系统是不是可以有弹性可以在一些子系统退出后，仍然可以继续前进而不遗失数据	第2代区块链系统，LSO 模型（2020）	LSO 模型[11]使区块链系统可以动态调整，允许子系统故障
扩展性风险	指随着参与者的多样性和数量增长，系统可以改变自己的配置来处理新增加的业务	区块链系统是否能满足高峰时段的处理量	第2代区块链系统（2020）	LSO 模型，第 2 代区块链系统，可以有系统性的扩展，而仍然保存交易性和监管性
透明度风险	金融系统方需要公开流程和相关数据给所有或是相关单位（人物），例如监管单位	许多数字代币项目有没有披露重要信息，例如准备金数目；监管单位能不能有系统有效的快速找到相关信息；如果节点受损，能不能够将数据恢复而继续有完整信息	熊猫模型（2016），蝴蝶模型（2021）	熊猫模型[12]使央行以及监管单位可以有系统的接触到其他链的数据，增强监管力度；蝴蝶模型使数字稳定币合规管理，准备金完全透明，增加稳定币信任度
隐私风险	一般市场参与者通过合法公众渠道就能够得到决策所需的各种信息	在公链，所有事务在某种程度上都是公开可观察会泄漏信息； 联盟链需要保护客户隐私	熊猫模型（2016）	熊猫模型（2016）保护参与单位数据不公开给所有参与单位
监管风险	法律或监管规	监管单位可以找	TRISA	监管网，嵌入式监管保

	定的变化，可能影响商业银行正常运营，或消弱其竞争能力、生存能力的风险。	到相关信息，完成 KYC 和 AML 相关监管作业，并且可以阻止交易完成，或是让交易回滚	（2020），STRISA[10]（2020），嵌入式监管，机器学习	证所有交易都能够被监管到

区块链技术有可能给现有 FMI 带来重大深远的改变，但在解决系统现有问题、提升能力的同时，可能会引入新的效率和安全性问题，甚至会造成系统性风险。PFMI 也是金融机构评估新技术（如区块链）在金融领域中应用可行性的主要依据。正如我们之前文章中所说[1]，“区块链的出现不会也不能改变 PFMI，反而区块链的设计必须根据 PFMI 而改变”：还需要根据 PFMI 原则来衡量金融领域的区块链系统，系统设计可能存在诸多问题，如可靠性和容错性、可扩展性、账户查询、清结算、金融效率、可监管性和可回滚性等。

参考文献

[1]. Xiaoying Bai, Wei-Tek Tsai, Xiaofang Jiang, Blockchain Design -- A PFMI Viewpoint, to appear in 2019.

[2]. Rong Wang, Wei-Tek Tsai, Juan He, Can Liu, and Enyan Deng. A Distributed Digital Asset-Trading Platform Based on Permissioned Blockchains[C]//International Conference on Smart Blockchain. Springer, Cham, 2018: 55-65.

[3]. Wei-Tek Tsai, Xiaoying Bai, System requirements for PFMI and financial blockchain: Are we ready to encounter the failure of the second wave of blockchain projects?2018.12.24 (in Chinese), https://mp.weixin.qq.com/s/XXcpRfnvaF6jiLC5MW4A-g

[4]. s Mcvanel D, Murray J. The Bank of Canada’s Approach to Adopting the Principles for Financial Market Infrastructures[J]. Financial System Review, 2013.

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

[6]. Russo D. CPSS-IOSCO Principles for financial market infrastructures: vectors of international convergence[J]. Financial Stability Review, 2013:69-78.

[7]. Bank for International Settlements (BIS), Principles of Financial Market Infrastructures,

2012.

[8]. 蔡维德等. 智能合约：重构社会契约，法律出版社， 2020.10.

[9]. 蔡维德、姜晓芳、王康明，美国合规稳定币管理模型：新型货币战争进入第二阶段（二），2021.02.22

[10]. Wei-Tek Tsai, Weijing Xiang, Rong Wang and Enyan Deng, LSO: A Dynamic and Scalable Blockchain Structuring Framework [C]// BChain 20

[11]. Wei-Tek Tsai, Dong Yang,Kangmin Wang,Weijing Xiang and Enyan Deng, Srisa: A New Architecture to Enforce Travel Rule//FICC 2020

[12]. 蔡维德，赵梓皓，张弛，郁莲 ，邓恩艳，熊猫-CBDC 央行数字货币模型，https://mp.weixin.qq.com/s/VMF1R9q2D61-2R3neo6lGg

[13]. 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？https://mp.weixin.qq.com/s/XXcpRfnvaF6jiLC5MW4A-g

[14]. 蔡维德等，区块链的第五大坑（下）—— 从 PFMI 的角度谈区块链，https://mp.weixin.qq.com/s/rPFn3T5FfJvib5Y-2PTcIg