从美联储央行数字货币思想看区块链设计原则：下一代区块链系统（一）

蔡维德、向伟静

2021 年 3 月 16 号

版权所有

前言

本文是“下一代区块链系统”系列的第一篇。2020 年是区块链在科技上一个重要里程碑，取得了极大的发展，例如 2020 年 4 月脸书发布 Libra 2.0 版白皮书提出许多新的设计和思想。同一时间我们在中国发布了《互链网：重新定义区块链》，开启了下一代区块链的讨论。脸书 Libra 2.0 主要宣传监管上的创新（遵行旅行规则和嵌入式监管[9,10]），同时在架构上也有创新；而我们主要在架构上的创新（例如 LSO 架构），并在新架构上加添监管机制，例如 STRISA 监管网络系统。但是现在在下一代区块链系统的讨论还比较少，许多因素还没有厘清。

下一代区块链系统和第一代系统大不相同，体现在区块链走进合规市场，金融市场提出许多新需求。最大的两个改变是：区块链交易需要监管，以及金融交易完备性。前者是过去大部分区块链系统特意回避的问题，而后者也是经常被忽略的问题。大部分区块链系统设计都在讨论共识机制，例如如何加快共识。但是共识加快后，交易还是完备吗？还可以监管吗？如果这两个问题没有解答，则新共识机制将无法运用在金融系统中。这就是我们一直明确的区块链设计不能采取单项优化的设计，而需要有全盘的考虑。我们从 2018 年就提出“可监管的区块链”才是区块链发展的方向，就是系统设计的时候必须考虑多项要素，特别是监管性和交易完备性，如果一条链系统没有考虑这两项，将会遇到困难。

由于下一代区块链系统比第一代系统更为复杂，本系列文章计划从头开始讨论。从软件工程角度来说，首先需要对了解需求。这就是第一篇文章的目的。

2021 年 2 月 24 日，美联储发布报告《央行数字货币的先决必要条件》（*Preconditions for a general-purpose central bank digital currency*）[1]。在该报告中，美联储表明了其对于央行数字货币的看法和立场。事实上，英国央行在去年 3 月同样发布了其央行数字货币(Central Bank Digital Currency，CBDC)的报告《中

央银行数字货币的机遇，挑战和设计》（*Central Bank Digital Currency Opportunities, challenges and design*）[2]。对比两家机构在 CBDC 上的看法，二者之间有相似之处。这表示世界重要央行观点已经一致，只是观点一直在进步[11]。这也证实了一点：对于 CBDC 的设计与需求，多方得道的结果都相似。英国央行在 2020 年 3 月时，还在讨论是不是要使用区块链技术，并且认为区块链系统必须根据央行的需求而改变，央行不会因为现在区块链系统的设计而改变货币政策或是监管原则。但是经过 2020 年的发展，美联储的态度变得更加积极。在 2021 年 2 月，美联储就直接说使用区块链技术，并且提出的系统需求不是根据比特币、以太坊、超级账本的架构、功能、性能，而是根据美联储业务的需求。这样正面的态度和 2020 年英国央行相对保守的态度差异很大。英国央行是过去 CBDC 思想的领先者，现在美国取而代之。

本文将首先介绍美联储这篇报告的主要内容思想，并且比较国际清算银行和多国央行对于 CBDC 的观点。一个明显的结论，就是根据这些央行提出的 CBDC 需求，我们需要一个新一代区块链系统架构。虽然新架构和传统区块链架构有类似的地方，但是还是有巨大的差距，例如传统共识速度不再是主要关注点，交易完备性和监管性才是下一代区块链的主要需求。

1. 美联储报告

这篇报告主要阐述了发展 CBDC 的先决条件。“货币”是否成功的关键在于，它是否在市场上被视为一种安全、稳定和可靠的工具，而不是只是依靠它是法定货币。如果数字美元通过不了市场的考验，即使有法定货币的地位，也需要进步。

现金、中央银行存款和潜在的 CBDC 都是中央银行的负债。CBDC 首先要成为一种安全的能保障价值货币。同时，在随着全球稳定币的引入、支付服务领域“大科技”(bigTech)的日益普及，凸显了数字货币的优势，更加彰显了发展 CBDC 的迫切性。文中表明发展 CBDC 要有 5 大先决条件：明确的政策目标、广泛利益相关者的支持、强大的法律框架、强大的技术和市场准备。下面将从这 5 方面分别介绍并讨论。

1.1. 明确的政策目标（Clear Policy Objectives）

各国央行对 CBDC 研究和实验的兴趣差别很大。然而，这些目标通常分为两大类。一些央行主要是在寻求解决当前的挑战，而另一些央行则在探索未来的能力。美联储认为，无论 CBDC 的具体目标是什么，它们都应该与美联储的长期

版权所有

目标相一致，即保证国家支付系统的安全和效率，以及货币和金融稳定。各国央行对 CBDC 的发展态度同样也秉承 3 个原则：

- 不造成损害；
- 补充现有货币形式；
- 支持创新和效率。

1.2. 广泛利益相关者的支持（Broad Stakeholder Support）

报告中将 CBDC 的利益相关者分为：政府机构、最终用户、金融机构、技术和基础设施提供商、学术界和标准开发组织。

- **政府机构：**政府的立法和行政部门将需要考虑影响 CBDC 的设计和实施的因素。例如对于通用 CBDC 的立法变化（合同法、隐私法和消费者保护法）。设计上也需要考虑包括与税收、公共支出、伪造和欺诈、反洗钱和网络安全相关的问题。
- **最终用户：**对于用户来说，可用性是关键，因为通用 CBDC 必须为使用货币购买商品和服务的用户设计。在 CBDC 的设计和测试中，需要考虑不同年龄、地理位置、支付习惯和财务知识的终端用户。
- **金融机构：**引入 CBDC 可能导致市场结构和动态的重大变化。CBDC 可能会影响商业银行存款、银行信贷以及更广泛的金融体系。然而，也有可能几乎不会对银行业造成破坏，这取决于 CBDC 的特性及其实现方式。
- **技术和基础设施提供商：**科技和基础设施公司在当今的市场上扮演着重要角色，这些集团的支持是 CBDC 发行的先决条件。潜在的 CBDC 可能有许多不同的形式，其中一些形式可以通过现有的技术和基础设施实现。或者，它可以使用新的技术，如区块链，这些技术目前还没有广泛使用。
- **其他利益相关者**：如学术机构、智库、标准组织和国际社会，可以为 CBDC 的基金会提供信息和支持。学术机构和智库可以为决策提供思想领导。标准组织可以通过定义术语、开发分类法以及创建支持更广泛生态系统的规范和标准来做出贡献。

1.3. 强大的法律框架（Strong Legal Framework）

健全的法律框架可以帮助人们更快地相信并使用 CBDC。首先要有明确的法

版权所有

律权限。发行通用 CBDC 是否与相关法律要求相一致。其次是确定 CBDC 是否拥有与法定货币相同的地位。例如，美国法律下 CBDC 作为法定货币的地位仍然是一个悬而未决的问题，一个通用 CBDC 作为法定货币的地位并不保证它在商业上被接受。

我们的观察

美联储的观点是：即使美元 CBDC 是美国的法币，也需要通过商业方式确保该系统可以在商场上成功运行。

还有反洗钱、打击恐怖主义融资、解决逃避制裁问题。CBDC 可以成为非法活动的支持介质,特别是考虑到方便和速度,潜在的大量资金可能被转移。

我们的观察

在讨论法律地位后，美联储最关心的问题是反洗钱。美联储担心地下市场使用数字美元洗钱。但是事实上在美国这方面的工作是从 2019-2020 年才积极进行，以前都是个别单位研究开发，而且监管科技主要都在传统系统上。由于数字货币的监管机制还在研发阶段，估计此类问题还未解决前，美联储不会推出数字美元。美国会以脸书稳定币的监管机制作为示范试点看待。

与此同时，考虑如何尊重隐私以及如何在 CBDC 协议中保护个人数据也至关重要。CBDC 与钞票不同的一点是：实物钞票不携带与特定个人及其金融交易历史有关的交易数据。在 CBDC 发行后，央行可以获得空前规模的细粒度交易信息；交易数据可能对某些第三方(如银行和服务提供商)可用，或者在极端情况下，对每个人都可用。货币和数据之间的这种紧密联系与实物钞票形成了鲜明对比。

版权所有

我们的观察

注意，在隐私性属性上，美联储的观点和数字美元计划(Digital Dollar)的观点正好相反，却和我们观点一致。我们认为[12]要洗钱，用现金，不要用数字货币。因为不论区块链如何设计，如果使用区块链运行数字货币，项目方都可以看到至少部分信息或是全部信息。这样区块链系统就是洗钱的克星。

美联储说“央行可以获得空前规模的细粒度交易信息”。这表示美联储的观点和加拿大央行在 2017 年的观点一致，央行必须能够观察到一切信息。因此数字货币，用起来像现金，却没有现金的隐私性。

这里监管性的需求是：1）能够实时找到相关账户信息；2）能够实时找到相关交易信息；3）能够快速完成反洗钱分析；4）能够实时阻止违法或是违规交易，或是回滚还没有结算的交易。这些在中心化系统不难做到，但是在分布式网络系统（例如区块链）中就困难的多。而且这里还有假设参与系统或是节点（包括所有参与方）都有可能会有欺诈行为，在信息上作假或是篡改数据。这样监管机制会复杂的多。

数字美元计划，是一个美国民间项目，认为隐私性非常重要，并且坚持使用 token 来建立数字货币系统。坚持使用 token 机制的观点和国际清算银行的观点也正好相反。国际清算银行在 2021 年 2 月发表的观点认为 CBDC 系统只能使用基于账户的数字货币系统，而基于 token 系统只能是地下市场的数字货币系统。

我们的观点[12]是即使使用 token，也不一定有隐私性，因为单单使用 token 而没有其他辅助协议隐私性还是不够的。我们的观点出现在 2020 年，但是今年（2021）已经证实。最近暗网表示不再接受比特币，代表诸如比特币（使用 token 的系统），在暗网交易已经没有隐私性。为什么？因为美国在 2020 年开发的监管科技已经能追踪到几乎所有的比特币交易。如果比特币在暗网交易，暗网反而可能不再“暗”了，只好拒绝。

此外，一个通用的 CBDC 可能会要求央行承担与公众有关的角色和责任，而这些角色和责任目前通常由私营银行对他们的客户承担。

我们的观察

这里美联储的观点，和以前英国央行、国际清算银行以及更早的加拿大央行观点一致：CBDC 系统的监管性至关重要。传统数字代币系统一直不愿意服

版权所有

从的原则，而且一些系统就是设计来抵抗这原则。

而美联储提到的央行可以有“细密度的交易记录”，就是我们提的“比目鱼不对称模型[10]”，这也代表在央行监管面前，没有隐私性。这点 2017 年加拿大央行就提出；2019 年 11 月美国哈佛大学教授 Rogoff 也同意这是重要的系统功能；2020 年美国财政部也提出这是必须的系统功能。

1.4. 强大的技术 （Robust Technology）

技术将在一定程度上影响数字货币的设计和功能。特定 CBDC 设计的业务和操作需求可能需要开发新技术。此外，访问或集成点(如数字钱包)可能需要额外的开发来满足操作标准。例如，可以离线操作的 CBDC 可能需要使用其他技术，如安全硬件。重要的技术开发和评估工作需要在三个核心领域:系统完备性（system integrity）、运行鲁棒性(operational robustness)、和运行弹性（operational resilience）。表 1 突出了支持 CBDC 的技术能力的关键方面。

表 1 基础技术的关键点

技术能力	哪些方面是重要的?
系统完备性。CBDC 需要以不损害其他系统或是人的方式下执行，未经授权不能操纵	能够提供安全而且有效率的资产转移
	准确的记录保存，有效的防伪措施，以及强大的欺诈检测
	管理和保护系统免受未经授权的访问、使用、中断、修改或破坏的能力，以提供系统的机密性、完备性和可用性
	认真实施强有力的信息安全控制，以保护信息资产
运行鲁棒性。CBDC 必须具有跨一系列运行条件正确、可靠地运行的能力	提供全天候 24 小时的即时结算
	包括灵活和适应性强的技术，以便可以根据需需求的演变而改变
	适当考虑生态系统的运行鲁棒性，而不仅仅是安

征求意见稿

	排运营商的运行鲁棒性。例如，向设计不佳或运行不佳的数字钱包发放和分发 CBDC 可能对整个安排构成风险
运行弹性。CBDC 还需要有抵抗、吸收和从不利条件中恢复或适应的能力。	如果需要互联网连接，需要考虑网络中断的情形
	从人员、信息、系统、流程和设施的角度解决运行弹性问题
	考虑端点到端点弹性，就是“标准”的运行弹性的应该从终端用户的观点，而不仅仅与结算有关

我们的观察：

这里美联储提出的系统需求不是根据币圈提出的“不可能三角”，而且第一个提出特性就是**交易完备性**。交易完备性，就是不论系统是如何执行的，最后的结果必须保证交易是正确且一致，不会因为得出交易结果的次序不同而出现不同的结果。交易完备性还包括记录不能被篡改，参与者有合理的权限，不能读取没有权限的数据。

“不可能三角”不是区块链的问题，而是逃避监管的公链研究课题。只要不逃避监管，这问题就不存在，也不需要存在。

交易完备性和监管性就成为下一代区块链系统的重要指标。这和传统上关注共识速度不同，一些区块链的设计为了要增加共识速度，但是有时共识加速了，却失去交易完备性。这种没有交易完备性的链，只能做存证，而不能交易。使用这样的链在金融交易上，就有**系统性**的风险。

综上，我们给出交易完备性的定义：

交易完备性：最终交易结果必须保证交易正确且一致，与交易执行次序无关。同时还要保证交易记录的不可篡改性和合理的用户权限管理。

版权所有

1.5. 市场准备程度（Market Readiness）

市场准备是指引入 CBDC 的适当时机。CBDC 必须有一个准备好支持它的生态系统(供应)。评估市场准备情况通常需要了解可能支持或推动采用的条件，以及该系统的组成部分是否准备好并有效协调。

- **需求。**对 CBDC 的需求可能来自经济或政策利益。但无论是什么推动了 CBDC 的发行，在日益增多的支付选择中，个人和企业都更愿意接受一种新的支付工具。消费者在选择一种特定的支付方式时列举了几个理由;他们注意到了便利、速度、经济刺激和安全等因素。但旧金山联邦储备银行 2019 年《消费者选择日记》报告指出:“即使新的支付方式继续出现，消费者仍倾向于使用现金、借记卡和信用卡等传统方式进行日常消费。”然而在企业对企业的支付，电子支付的偏好经常被表达出来。

- **供应**。转向市场准备的“供应”方面，生态系统结构、硬件基础设施和市场参与者必须准备好接受 CBDC。CBDC 生态系统包括许多功能，例如发布、分发、存储、使用、客户服务、遵从性、报告、监视和维护。为了满足市场的预期，建立一个新的支付轨道和/或升级或改变传统支付轨道必须完成和测试。为了确保供应，必须协调各方之间的活动和沟通。协调活动包括建立标准，为系统的各种要素建立过程和能力，以纳入新的技术特征、功能和安全增强。个人和企业都需要操作指导，了解该系统将如何工作，以及他们需要做什么来使用它。市场参与者之间的沟通也同样重要。个人、企业、银行、支付服务运营商、央行等都需要对相关各方的权利和责任有一个清晰的认识。

2. 国际清算银行和多国央行对 CBDC 的观点

早在 2020 年 1 月加拿大银行、欧洲中央银行、日本银行、瑞典中央银行、瑞士国家银行、英格兰银行、美国联邦储备系统、国际清算银行理事会等几家机构就发展 CBDC 交换了意见，并发布了报告《中央银行数字货币:基本原理和核心特征》（*Central bank digital currencies: foundational principles and core features*）。[3]报告中认为 CBDC 应该：

- 不损害”货币和金融稳定；
- 在一个灵活和创新的支付生态系统中与现金和其他类型的货币共存；
- 促进更广泛的创新和效率。

基于这三个原则，在未来任何 CBDC 系统必须具有弹性和安全性，以保持运行完整性。为了向用户提供实用程序，CBDC 保证便利性，并且要保证低成本。为了满足基本原则，CBDC 必须具备涵盖 CBDC 文书、基础系统和更广泛的机构框架的某些核心特性（如下图）。

版权所有

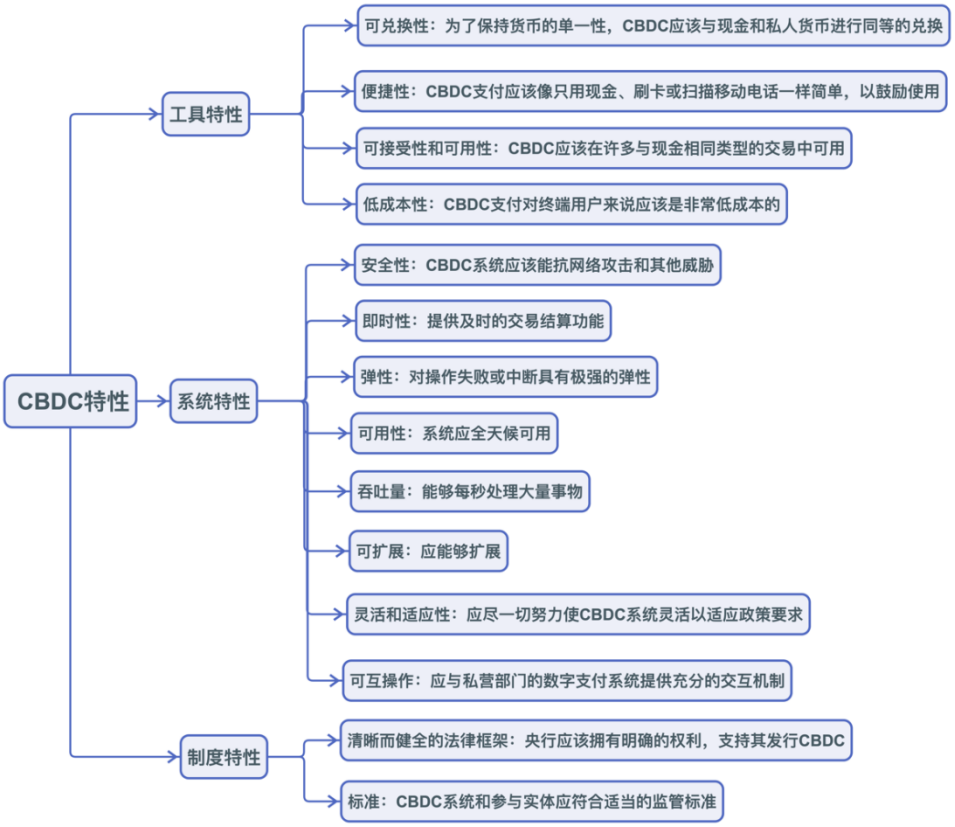

图 CBDC 的特性

CBDC 可以促进支付更具弹性、效率、包容性和创新性。在现金使用减少、数字化程度较高的地区， CBDC 还可以在维持央行货币的使用和扩大其流通量方面发挥重要作用。

还要考虑引入 CBDC 可能会对金融稳定产生影响。首先，数字银行在金融危机时期出现挤兑的可能性。其次，对银行融资的长期影响。虽然系统范围的银行挤兑变成现金现在非常罕见，但通过 CBDC 向中央银行以更大的速度和规模兑换现金是可能的。第二个担忧是，引入 CBDC 可能侵蚀银行的零售存款，导致融资组合不太稳定。

3. 支撑 CBDC 的区块链架构

分析对比几家机构的报告，不难发现，几家大央行对于 CBDC 观点十分相似。就美联储的报告来看，他认为稳定币带动了 CBDC 的发展，更多高科技公司

版权

纷纷进入金融界，发展 CBDC 会对市场产生重大的改变。而发展 CBDC，光是借助传统的区块链还远远不够，发展下一代区块链迫在眉睫。

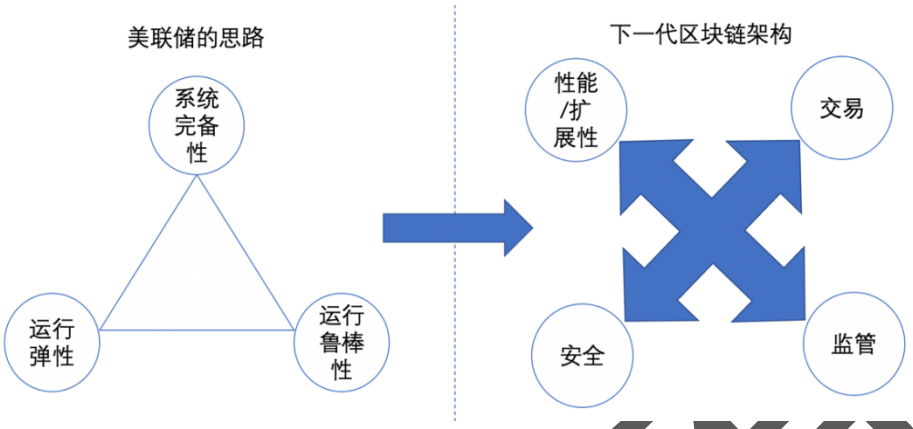

图 下一代区块链

我们根据金融行动特别工作组（Financial Action Task Force，FATF）、G20、国际清算银行、IMF 等提出数字货币管理原则，例如金融市场基础设施原则（Principles of Financial Market Infrastructure，PFMI）[4]，合成下一代区块链的需求如下：

- 金融交易需要完备性，不能因为并行或是分布式处理产生不一致的结果；
- 每笔交易都必须经过 KYC（Know Your Customer），反洗钱（Anti-Money Laundering，AML）等监管机制；
- 交易、结算、清算分离，以便利账户管理和监管。传统上，这些机制都是一步同时间完成，不利于监管；
- 账户管理和交易管理分离，方便财务管理；
- 未结算的交易可以回滚；

第 2 代区块链系统有三个重要组成子系统，而每个子系统都有新设计：

- **账本系统**：主要是分布式数据库系统，但是有拜占庭将军协议，可以存储账户和交易信息，也可以支持交易、清结算、存证等作业；
- **智能合约系统**：主要执行区块链上的应用，包括交易、清结算、存证等；
- **预言机系统**：主要负责和外部交互，包括收集数据和输出数据。由于需要保证数据正确，预言机系统会有自己的账本系统和合约系统。

而这三个子系统可以有多对多的关系。例如一个账本系统可以接多个合约系统；而一个合约系统可以接多个预言机。而且这三系统可以动态调整，例如由于

版权所有

有新的监管法规出现，配合新合约系统，新合约系统会和多个现成的账本系统连接；例如一个新金融公司出现，新公司的预言机可以连接现成的合约系统和账本系统。这种动态模型，我们称为 LSO（Ledgers 账本系统、Smart Contracts 智能合约系统、Oracles 预言机系统）模型[5]。

3.1. 账本系统新设计

新型账本设计和以前不同。由于数字稳定币和 CBDC 交易需要有完备性和监管性，交易机制和共识机制分别处理。传统上交易机制和共识机制是绑定一起，系统更为复杂。如果解耦，这两个机制都简化，简化后工作量降低，让系统可以运行嵌入式监管。而且分开后系统更加稳定。

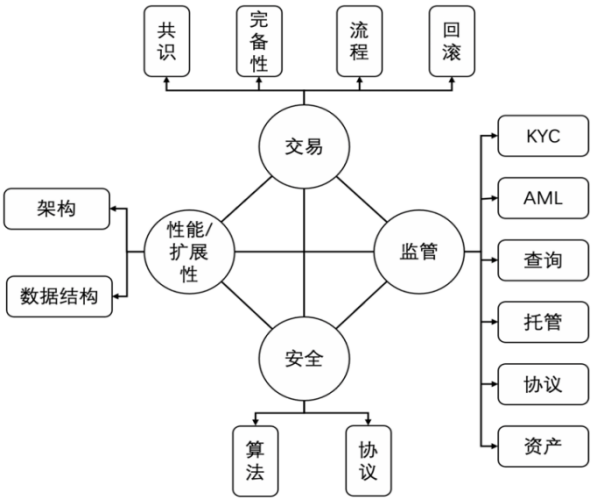

图 新型账本系统设计

- 由于交易和共识机制分开，共识完成只是代表部分交易流程完成，而不代表交易完成交易，这样系统可以有回滚机制，而且结算和交易又可以分离。这旧支持数字货币以及数字资产产业化，因为交易和结算可以由不同机构或是系统处理。
- 由于交易和共识解耦，交易系统和账本系统也自然解耦，表示可以由不同系统或是单位处理这两个机制，每个机制可以有自己的智能合约。
- 这样分离又代表监管机制可以在交易撮合后，但是在结算前进行。这在第一代是不可能的，由于在第一代系统交易就是结算。
- 新一代区块链系统需要处理多币种，多数字资产，并且可以有托管机制；而第一代区块链系统多是单一“数字代币”的封闭系统，只能处理一种币种，没有链的托管机制。这就造成“币链分离”的设计原则。
- 金融市场基础设施原则(Principles of Financial Market Infrastructures, PFMI)要求金融系统的扩展机制必须同时间有可靠性，表示所有原来的

系统属性在扩展后仍然必须存在；但是在第一代系统，连基础链的监管性都没有，不用考虑扩展后的属性。

3.2. 智能合约系统新设计

传统上，区块链维护多个节点，其中一些节点运行智能合约引擎。然而，这种体系结构不适合许多现代金融应用。英国央行在 2020 年提出不同智能合约可以在不同账本系统上运行，每个合约系统都有专属功能，例如和客户接口系统的处理 KYC，在交易账本系统上可以完成交易，在结算账本系统进行结算和最后的监管。这样传统区块链架构开始解耦，多个账本系统，多个合约系统，可以连接合作来完成完整金融交易，而且这个连接还可以动态部署完成。

合约系统不会只是链上代码（Chaincode），这样的系统没有法律效力，不能在合规市场使用，只能使用在地下市场。而合规的合约系统需要计算机界、法学界、金融界合作完成。国际掉期交易协会（International Swaps and Derivatives Association, ISDA）主要是金融界和法学界为主导，制定一系列的智能合约标准，而没有一行代码。这表示智能合约开发符合传统软件工程，以需求开始，而合约系统的需要在于金融交易和法规上。

2018 年美国商品期货交易委员会（Commodity Future Trading Commission, CFTC）提出合约系统两大主要功能是“完成金融交易”和“监管交易”。根据这思想，我们提出一个融合监管和交易的合约系统如下图[7]：

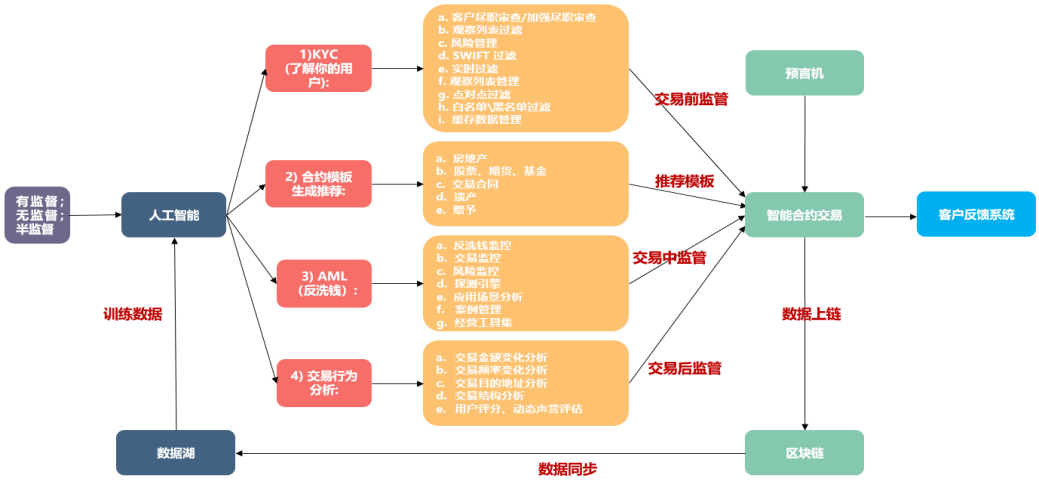

图 智能合约完成交易和监管

投稿

3.3. 预言机系统的新设计

一旦数据输入系统，区块链系统存储和保护数据，但是它不能保证进来的数据是真实或是正确，预言机提供这功能。预言机接收来自外部世界的数据，同时也可以将区块链的数据发送给外部世界，但是在接受或是发出前，需要验证数据的真实性。ISDA 认为预言机系统最为重要，由于这些预言机是金融机构的出入口，金融交易数据都经过预言机才到达合约系统和账本系统。

3.4. 下一代区块链--互链网

预言机是一个复杂系统，不只是传统传感器或是物联网，需要融合账本系统、合约系统以及信誉机制来实现。例如一个银行的预言机，需要保证送出来的数据真实而且正确，银行也需要签名。由于数据一旦从预言机发出，可能启动多个智能合约在不同区块链上自动执行，这些自动执行的交易会影响金融市场。

新型区块链系统将会包含账本系统、数据湖（一种用于区块链监管的大数据平台）、合约系统、预言机，以及基于这些底层技术的上层应用包括人工智能、KYC 身份认证、合约模板、AML 反洗钱、交易行为分析系统等，这将会是一种全面拥抱监管的大型区块链系统。

区块链是中国核心技术自主创新的突破口，代表区块链的改革，不会只限制在账本系统，合约系统，预言机系统，以及后面的监管平台上。区块链的改革还会渗透到操作系统、数据库、网络、存储系统。例如未来的支付网可以由区块链网络建造，可以取代现在的支付网络；现在的监管机制也会在网络上进行，数据也会像区块链数据一样，先加密后再分块又分片处理，而且是层层加密。即使一个加密被破解后，只会得到少许信息，其他的数据还需要再解密才能得到。这样系统就像洋葱一样，层层保护，我们称为“洋葱模型”。

传统上，服务器或是操作系统只支持上面的应用运行，而对不清楚上面的应用提供的功能。这给数字代币一个机会，使用 P2P 网络协议，一个地区有几台服务器愿意提供资源，数字代币就可以在该地区运行。以至于数字代币可以在世界各地运行交易。所以一个研究方向就是将监管机制放进基础系统内，这样所有交易都可以被追踪到。

为了实现上述功能，我们提出一些新机制例如层分层(监管软件优先)，管中管（文件除读、写、执行等属性外，还有交易属性），块中块（数据以块来处理，

版权所有

又分大块，中块，小块，统一处理，增加效率），片分片（加密后，数据在分片后，又再分片），密中密（加密后再加密）。传统区块链已经有“密中密”就是加密信息再度加密。加上其他机制，系统会更安全，并建立安全的“洋葱模型”。

4. 总结

本文从美联储对 CBDC 开出来的先决条件出发，导出新型区块链设计原则。这些原则和传统区块链设计原则不同，例如传统公链是逃避监管，而美联储却看重监管。

其次美联储认为交易完备性至关重要，而一些链的设计却不考虑这问题，或是用中心化的方式来处理。不考虑这问题，这链就不具备交易完备性，不论在合规市场或是地下市场都不能使用。如果仍然使用，由于没有完备性，就会出现系统性的风险。但是如果采取中心化处理，例如早期超级账本就采取这方式，由中心化节点来排序，这链就成为伪链；只要这节点被攻破，这链就被攻击者控制，这样也产生系统性的风险。

但是这些只是起步，后面还有需要因素需要考虑。本文讨论了基于 token 的数字货币系统，过去一些讨论主要争论在选择隐私性或是选择监管性。但是我们认为由于监管科技进步，不能再因为一个系统使用 token 就认为有隐私性。

我们估计美联储以后大改数字货币需求的可能性不大，但是在将来系统设计上会有翻天覆地的改变，许多传统上我们认为好的机制，可能以后都会被改变。例如本文提到的交易和共识解耦，一旦解耦后，系统作业、性能、交易性、监管性都改变，而且比传统设计强。这就开启了下一代区块链设计。

版权所有

参考文献

[1]. https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm

[2]. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

[3]. https://www.bis.org/publ/othp33.htm

[4]. https://www.bis.org/cpmi/publ/d101.htm#:~:text=The%20Principles%20for%20financial%20market%20infrastructures%20%28PFMI%29%20contain,and%20thus%20well%20placed%20to%20withstand%20financial%20shocks.

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

[6]. 蔡维德，“互链网：一种新的系统结构和应用构建方法”2020.08.11. http://m.xinhua08.com/share.php?url=http://fintech.xinhua08.com/a/20200811/1950646.shtml&fr

om=groupmessage&isappinstalled=0

[7]. 蔡维德等.“互链网-重新定义区块链”.2020.04.28. http://m.xinhua08.com/share.php?url=http://fintech.xinhua08.com/a/20200428/1933522.shtml&from=timeline&isappinstalled=0

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

[9]. 蔡维德、姜嘉莹.“从 Libra2.0 白皮书深挖新型数字货币战争韬略——从监管与合规入手”，2020.05.04.

[10]. 蔡维德、姜嘉莹.“平台霸权——打赢新型数字货币战争的决定性武器 Libra 2.0 解读（下）”，2020.05.09

[11]. 蔡维德，向伟静，智能合约 3 大架构分析： 英国央行 2020 年 3 月数字法币报告，2020-03-31

[12]. 蔡维德. 互链网：未来世界连接的方式[M]. 东方出版社, 2020

版权所有