智能合约近期五大科技突破：标准化、系统化、合规化、架构化、工程化

蔡维德 向伟静 张韬

前言

智能合约的重要性已经得到世界许多国家的认同，例如德国银行协会(Association of German Banks)在 2019 年认为脸书 Libra 最厉害的机制是“可编程经济”（Programmable economy），而这就是智能合约带来的革命。由于可编程经济带来的是一个新的金融生态，和传统金融生态不同。如果普林斯顿大学提出的“数字货币区”（Digital Currency Areas）理论正确，世界正在走向一个基于平台的可编程经济体系，这也会是世界各国科技发展的重要依据和竞争广场。因此，智能合约技术是极其重要的。2020 年 8 月世界银行(World Bank)的报告再次提醒我们智能合约新科技的重要性，特别是在供应链金融和保险上的应用。

编写《智能合约：重构社会契约》目的在于研究开发合规智能合约的理论基础。在 2013 年世界开始的是链上代码的工作，2016 年开始重视合规智能合约。由于“The Dao 事件”，许多单位包括法学院、律师事务所、金融研究机构、区块链研究院等立刻开始研究合规智能合约技术和法规。这些单位包括美国商品期货交易委员会(Commodity Futures Trading Commission, CFTC)、英国央行、欧洲央行、国际货币基金组织（International Monetary Fund, IMF）、德国银行协会、世界银行(World Bank)等。经过 4 年的研究，上述单位对智能合约的技术和相关法律问题有了初步的了解，例如 2020 年 8 月世界银行发布白皮书认为智能合约有助于普惠金融。我们在《智能合约：重构社会契约》[1]书中介绍了相关重要研究结果。

过去 4 年国外在智能合约上的研究发展还是非常快速[2]，大量律师事务所都发布白皮书，讨论相关的法律问题。而“币圈”在过去几年也邀请大量律师加入其团队，甚至邀请前监管人员加入，以保障其业务合规，以至于不论是合规市场或是“地下币圈”市场都走向合规的道路。

另外，由于《智能合约：重构社会契约》一书需要对这领域发展进行系统性的介绍，笔者重读了一些经典论文，同时间也研读了近几年的学术研究报告。研究过程中，笔者总结了智能合约近期五大科技突破。这五大突破不但指出研究方向，提出产业发展方向，而

且可以评估和预测现在项目的发展将来会遇到的瓶颈和可能采取的解决方案。例如 ISDA 的工作就可以预测 Defi 和脸书 Libra 将来的发展，这两个是现在区块链界热门课题。

五大突破简介（：

- **正确的需求分析**：国际掉期和衍生品协会（International Swaps and Derivatives Association，ISDA）是这方面最大贡献者[10]。他们最近非常活跃，他们的报告改变了现在智能合约的定义和流程，也改革了平台的设计和基础设施，以及相关法律。另外他们的智能合约标准居然没有一行智能合约代码，令人惊讶。如果我们细读他们制定的标准，这将对智能化科技和产业有重大影响，而且可以预测现在许多系统会遇到的问题，这是近期智能合约工作中最大的突破。

- **正确的研究路线**：当我们重新读李嘉图合约(Ricardian Contract)的时候，竟然发现合规智能合约发展路线居然走的是李嘉图合约路线，而不是原来萨博(Nick Szabo)的路线，因为几乎所有合规智能合约的工作都是从李嘉图合约出发的。因此，对合规智能合约发展路线的研究需要更新、迭代历史观点，突出实际贡献者的作用。以李嘉图合约出发，智能合约工作走在正确路线上。

- **正确的定位**：美国 CFTC 报告[9]在这方面是最精彩的，虽然只有 PPT，但是思路清晰、观点犀利，对于这领域提出正确的路线。如果有人想了解智能合约技术、应用、相关法律以及方向，这份报告是首选。但是如果细读该报告，就会发现其不只是介绍智能合约，还有重大方向性突破，他们提出的概念将彻底改变未来智能合约的发展，例如智能合约以后会以碎片化、标准化、服务化和共享化的方式发展，而不是以往传统的整体式、孤岛式发展，这已经与传统智能合约的概念有很大的不同。而其中的碎片化则是现在社会信息化的一个重要指标。

- **创新的架构**：英国央行在 2020 年 3 月提出的将来三个可能的智能合约设计，打破了传统智能合约的架构，例如以太坊的架构[11]。由此，智能合约的架构不再是传统区块链和智能合约系统 1 对 1 的架构。这在系统架构方面的重大突破，对学术界和产业界具有巨大的影响。

- **创新的合约语言和实验**：雅阁项目(Accord Project)也是我们遇到的另外一大惊喜，由于该项目提出的形式化合规语言和模版，和计算机界智能合约工作大不相同。

在计算机界，形式化语言和验证方法未考虑到合规问题，以至于不论如何严谨的开发智能合约代码，仍然无法确保所开发的产品具有法律效力。而雅阁项目提出的合同模版和模型语言（这些从合规端点出发），落地在计算机语言和验证方法上，这是巨大创新，是法律和计算机结合的一个案例。虽然这工作还有许多地方可以继续进步，但这表示这方向是可行的，不是不可能的任务，这是重大科技突破。

上述五大突破改变了学者对智能合约的认知，也改变了学术研究方向，有的甚至改变了未来产业的发展。本文将围绕这五大突破来讨论。

这五大突破都是国外的贡献。在讨论这些亮点后，我们也提出中国的皋陶模型，该模型是融合上面五大突破的优势的模型。

1. 突破 1—标准化：ISDA 让我们明白什么才应该是智能合约的流程

ISDA 协会在 2018 年开始这方面的工作。而这个工作一个特别让人惊讶的地方，就是智能合约标准里面没有代码。从 1994 年智能合约起源，智能合约的工作都有代码，例如从李嘉图合约，到近代的以太坊智能合约，到斯坦福大学“CodeX 项目”，可计算的合同(Computable Contracts)，都有代码。可是 ISDA 智能合约标准里面没有一行代码，这使得我们对智能合约的认知产生了巨大的改变。这表示部分智能合约的工作和代码没有直接的关系，而这部分的工作重要，且需要标准化。

智能合约分为两种： 1）一种是有法律效力的，也是实际的智能合约； 2）链上代码(Chaincode)，就只是运行在区块链上的代码，没有法律效力。在国外第一种也称为“法律智能合约”(Legal smart contracts)，以此来区别没有法律效力的链上代码。我们一向使用“智能合约”和“链上代码”来区分这两种机制。

我们专注于智能合约，而不在链上代码。但是这两者的差异在哪里？一些计算机学者也提出需要法律考量，但是法律考量是做什么却不清楚。ISDA 的工作解答了该问题。ISDA 认为智能合约代码与智能法律合同（由软件表示法律合约或法律合约的要素）是有区别的，由此 ISDA 提出了智能衍生合同的概念。

（1）认知上的改变

ISDA 的工作就是研究在现在法规下，智能合约如果需要自动执行，应该如何进行？这流程应该是如何？ISDA 在其发布的白皮书中提到智能法律合同的两种不同模型：外部模型和内部模型。在外部模型中，编码条款保留在法律合同的外部，仅代表自动执行合同的机制。在内部模型中，自动执行的条款已包含在法律合同中，但用比自然语言更严谨的表示形式进行了重写。计算机可以采用这种更为形式化的表示并自动执行这些条款。智能衍生合约基于内部模型，某些条款可以自动执行，这些条款以一种能够实现高效自动化的形式表示，而其他不能自动执行的条款用自然语言表示。

ISDA 认为直接将现有的金融交易流程转成代码是不明智的。因为现有流程有部分是人工作业的，以保持流程的灵活度。但是如果这些人工流程也自动化，这流程就需要非常严谨的分析。因为一旦自动化，以前“灵活度”必须嵌入智能合约代码内，不然可能会出问题。

ISDA 在其白皮书中提到了其主协议的 5 个主题，分别是：事件、付款和交付、出清轧差、争议和合同订立与法律关系。例如事件这一主题，ISDA 举例说明了事件的种类和概念。虽然 ISDA 没有提供系统设计，但该概念却提供了很大启发。

事件的种类：“事件” 是指除了针对特定交易的合同条款外，还会发生大量外在事件，这些事件可能会影响合同当事人继续履行一项或多项交易下的义务的能力。即要对进行正常交易的合同，要针对其可能发生的不确定性事件采取对应措施，并定义在合同条款内。注册事件有各网点提交完成，即为合同参与方，其中要考虑的事件又分为正常交易事件和非正常交易事件，而非正常交易事件处理起来更为复杂，又分为违约事件和终止事件。

外在和内部事件互相启动：一个外在事件可以启动一个智能合约的自动执行，执行中有可能产生内部事件，可是这些内部事件对于其他机构或是同一机构内其他账户，可能就是外在事件，自动启动其他相关智能合约的执行。于是，一个复杂事件启动的动态网络就出现了， 并且同时间可能会发生大量的事件产生以及许多智能合约自动执行的情况。

事件处理的复杂性：ISDA 一直在提醒读者，这样的系统会非常复杂，并且该模型建立的系统应该将整体视为金融交易基础设施，与许多机构，金融或是非金融机构进行交互。在此基础设施上，例如一个金融机构出现新事件，该事件要经过该基础设施传送到其他单位，包括在这些单位运行的区块链和智能合约系统。其他单位可以是监管单位，而且同一

件事件在这些区块链系统或是智能合约系统都代表同样信息，不能被更改。该模型的参与单位可以是银行、保险公司、交易所、金融机构、公证处、监管单位，CSD(中央证券托管系统)、市场监管局和国税局等，这些金融机构、监管单位等共同参与合约条款的制定，涉及不同的现实交易活动。

事件和智能合约的交互：事件模型的主要功能是由合同参与方注册事件，将自然语言合同以事件标准化，即在合同的内部处理逻辑下（以软件代码形式表述，主要是条件语句），对合约进行预处理，将包含事件属性、合同属性的数据分别打包存储，并通知公证处、第三方电子存证机构等介入进行公证、电子存证。事件启动后根据事件身份证找到对应事件数据包和合约数据包提交智能合约系统进行交易自动化处理，同时涉及账户资产的信息提前提交到核心账本系统进行资产核对或资产证明，并查找相应账户的征信（或信用）记录。若存在资产造假、或参与方在失信名单之列等情形，可通知合约参与方或监管机构，启动终止事件，终止合约履行。

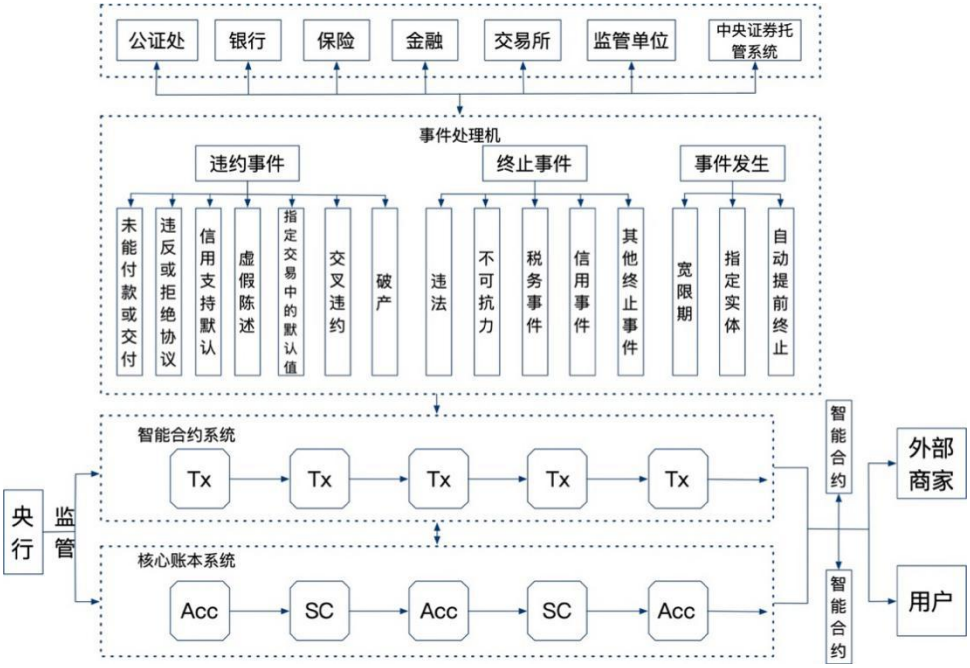

图 1　事件模型图

事件处理系统是智能合约系统的根本：上图可以清楚看出，合规智能合约系统需要一个基础设施，而这基础设施就是“事件处理系统”（event-processing system），不是传统智能合约系统。传统智能合约系统是需要接受事件处理系统传送过来的数据才开始执行。

表 1 智能合约标准化认知的改变

从前的认知	现在的认知
智能合约是将现在金融流程自动化	现在流程是半自动化，部分步骤是由人工处理，具有灵活度，同时这种灵活度需要代码化，而更新后的流程将可能与传统流程不同
智能合约大部分的工作在创建合约代码	智能合约的很大部分工作是开发合规并且是可以自动执行的流程，另外的很多工作则是在建立智能合约的基础设施
智能合约平台只是需要预言机和区块链系统	由于金融流程会复杂，而且大量交互，需要事件处理(event-processing)系统,这系统可能与物链网（或是物联网）融合

根据 ISDA 观点，现在金融流程可以分为两部分，如下表，而智能合约很大部分工作是处理现在人工处理流程，例如由短信、邮件、电话、交谈、媒体来支持的流程。

表 2 智能合约可实现的工作

现在金融流程	智能合约的工作
人工处理部分	建立事件模型，建立基础设施，连接单位，标准化处理这些工作
自动化处理部分	碎片化和标准化现在可以自动化的流程

（2）学术上的影响

我们认为 ISDA 的研究是最近几年来智能合约最大的突破，这研究使智能合约的工作产生本质的改变，不但改变了我们对智能合约的基本认知（上表），也改变了系统架构（事件处理系统和预言机的加入），还改变了开发流程（从更新现在金融流程开始，而不是编译现在流程到智能合约代码）。在我们书中（《智能合约：重构社会契约》）也表达了该观点，后面的学术工作现在才开始。

ISDA 的研究工作，开启了对智能合约的一个更为广大知识领域的研究，也是一个新型交叉研究课题，这课题包含 3 个领域，法律、金融、计算机。这工作以法律为出发点，但是却需要（最终）落实到计算机建模语言、系统、基础设施上。在建模的时候，金融知

识和法律知识为主导，但是后来却由计算机来实现。从合规流程开始，逐步向法律智能合约靠拢，最终实现智能合约法律化。

ISDA 是以现在金融市场流程出发，连接现在机制。而我们提出的比特犬智能合约模型，表示合规流程需要有以下特性：1）基于过程的原则；2） 投管机制；3）预言机原则；4）共识机制；5）问责原则；6）回滚原则 [1]。这些都是在现在法规下金融交易的原则，也代表大部分的智能合约代码都需要处理上面 6 个机制。比特犬模型强调要通过领域分析来开发智能合约模板，同时所提供的模板可以在开发过程中复用。代码从智能合约模型自动生成，并运行于区块链平台。智能合约模型生成代码可以做到完全自动化，对于没有在智能合约模型中描述的外部合约，不能自动生成代码。在这种情况下，将生成智能合约与外部智能合约交互的接口。

根据 ISDA 的研究，事件处理是一项重要工作。基于该理论，我们提出基于事件处理的烽火台模型和石榴模型。烽火台就是古代的事件预警系统，而石榴是多籽复杂系统，代表事件处理系统的紧迫性和复杂性。

（3）产业上的影响

我们预测未来一些新型产业会出现来服务智能合约业务。ISDA 中提到的智能合约衍生品是一个前景巨大的发展方向，可帮助股票、利率等期货通过智能合约实现完全自动化交易。每一种期货对应一种或多种智能合约衍生品，每一种智能合约衍生品包含该种期货的交易规则和法律，其本质上来说，所谓的衍生品也是智能合约模版。但以后产业不会限制在衍生品交易上，在其他许多领域都可以应用。

另外，任何人仔细研究 ISDA 的标准后，会对现在分布式金融（DeFi）的发展有不同的看法。DeFi 的路线就是根据现在金融市场流程来建立的经济体系，和过去比较具有很大进步，但是 ISDA 的报告清楚指出，新数字金融市场不应该根据现在的金融流程，而是根据改进后流程。这也是笔者在《迎接“约满天下”时代的道路：智能合约的蝶变》文章[12]内对于 DeFi 观点的依据。这也解释为什么 DeFi 系统一直在市场上出现问题，解决一个后另外一个新问题又会出现。原因很简单，他们还没有建立基于 ISDA 标准的基础设施。

另外包括脸书的 Libra 智能合约系统也还没有考虑到 ISDA 的标准，这表示 Libra 智能合约系统离实际应用还有一大段距离。如果脸书也学习 DeFi 的做法，将现在的流程写成智能合约，Libra 智能合约系统以后也会出现相关问题。

2. 突破 2—系统化：李嘉图合约（Ricardian Contract）引导智能合约研究走入正途

许多书籍和论文讨论智能合约的时候，都会引用 1994 年萨博关于智能合约的文章，认为这是智能合约的起头。笔者认为萨博的智能合约仅是一个概念，实际上并没有系统设计。而智能合约系统的设计是李嘉图合约的贡献。后来的工作，包括雅阁项目，斯坦福大学(Stanford University)的可计算合同 CodeX 项目、比特犬模型，都是根据李嘉图合约的路线开展的。可以说今天智能合约的发展是依据李嘉图合约在发展，而不是在原来萨博的智能合约概念上发展。李嘉图合约是伊恩格里格(Ian Grigg)开发的项目。

在网上也有一些文章，在争论萨博和格里格两套合约系统的差异。其实如果以他们二人原来的文章来讨论意义都不大，因为原来的文章都是在区块链没有出来前完成的，现在的智能合约（或是链上代码）和当时他们的文章的概念都相差甚远。我们只能以他们最后留下来的（最新）观点来评估他们的贡献。格里格认为智能合约需要从合同模版出发，由现在合同上模版变成代码来建立智能合约代码，这也是现在主流智能合约开发方法。李嘉图合约从法律观点出发，使用法律术语，可以嵌入法律条款，机器可读，也可以像普通文本书件一样可读，以便律师和签约方可以方便地阅读合约，进行法律协商。区块链的来临无疑为李嘉图合约创建了一个开发平台，且合约涉及到的见证人、买卖双方、金融机构、监管部门等均需作为链上用户区实现合约。

（1）认知上的改变

李嘉图合约的贡献，在于分解智能合约开发的流程：以前智能合约运行规避监管系统，从开始开发到完成均以代码为主。李嘉图合约的贡献是开发合规智能合约分为 2 大部分：

- 先建立一个合规智能合约模版模型，这些模版模型验证后，就是有价值的知识产权；
- 使用已经开发的模版，创建代码（例如代码自动生成或是人工开发）。

因此 “书写合同”会向“从合同模版到合同模型的建模”转变。而第一步主要在法律上分析、建模、验证，而第二步主要是计算机界的工作。在这 2 步骤都需要法律和计算机的工作。

这路线也是软件工程经常提的重要原则：先分解问题，然后克服分解后的难题（Divide and Conquer）。因此笔者认为智能合约这名词是萨博的贡献，但是智能合约技术是格里格的贡献。

（2）学术上的影响

从 1994 年开始，智能合约一直少受到关注，一直到以太坊出现后，才成为热门课题，特别是 2016 年“The Dao 事件”后得到许多人的关注。但是合规智能合约的发展是格里格开发的李嘉图合约奠定的基础。斯坦福大学在这基础上，增加了机器学习在可计算合同（Computable contracts）上。同样雅阁项目（亮点 5）开发的新型法言法语建模语言，也是在李嘉图合约基础上开展的。

（3）产业上的影响

李嘉图合约带来建立合规数字金融市场的可能性，而雅阁项目就是其中一个明证。

3. 突破 3—合规化：CFTC 入门指南突破性地解决技术难题以及提出新产业结构

作为美国一个重要监管单位，CFTC 的金融科技创新中心 LabCFTC 发布了《智能合约入门指南》（简称“指南”）。不要小看这名词“入门指南”，这入门材料包含解开智能合约开发的难题的方法以及将来产业的分工结构。

（1）认知上的改变

该“指南”所述的主要思想：智能合约要由“逃避监管”变为“监管利器”，且监管机制是智能合约最大的应用。“指南”中肯定了智能合约这一技术在市场中的广泛应用，首先明确了智能合约的许多风险，包括运行、技术、网络、欺诈等风险，承认以太坊的智能合约是不具有法律效力的合同，以后要走有法律效力的合同路线；虽然现在智能合约系

统有风险而且技术不成熟，但是其还是认为智能合约技术可以在金融交易上使用，特别提出在衍生品交易使用。

CFTC 是监管美国商品期货交易的监管单位，而期货就是一种衍生品。 这是 CFTC 给世界的一个重大信息，CFTC 表示鼓励大家积极研究智能合约。就智能合约的监管机制而言，基于标准化的智能合约的交易算法，是交易所监管单位最好的监管机制，而且是实时监管，也是标准化的监管。监管机制可在适当的时间，由智能合约自动执行 [4,5] 。而 CFTC 在讨论这些问题的时候还解决了两大难题：

1）难题 1：合规智能合约大而且复杂，以至于难开发

CFTC 解决上述难题的方法是不要求智能合约完成一笔交易的全部流程，而是完成部分交易流程。这是一个重要概念。例如现在使用信用卡交易，需要 20 道手续，如果使用智能合约来完成信用卡交易，智能合约会非常大而且复杂。CFTC 认为，该信用卡交易至少可以由 20 个智能合约共同完成，每一步骤由一个智能合约完成。最大程度地简化了智能合约的开发。

2）难题 2：许多单位都在开发智能合约，以至于融合困难

所谓的标准化是将一个交易拆分成若干部分，每一部分由碎片化的标准服务型智能合约实现。这会颠覆之前智能合约的开发流程，即由定制完成整个智能合约开发，到由标准化的原子智能合约集成实现。今后智能合约开发，想要实现一种服务，只需通过将所需的标准化的原子智能合约集成起来，相当于从“零件组装”跨度到“部件组装”，将开发流程简化，方便、高效、快速。

表 3　智能合约合规化认知的改变

从前的认知	现在的认知
智能合约主要是完成完整交易	一个智能合约在大部分情形下，只是完成一笔交易内的部分作业（部分交易流程），而不是完成整笔交易（全部交易流程）
智能合约大都是定制化开发的	大部分智能合约应该是基于标准化的
智能合约代码是一体化的	一个完整的智能合约很可能是由多个原子

	智能合约（标准化的）代码组成的
智能合约最大的应用是金融交易	智能合约最大的应用是金融交易和监管机制

（2）学术上的影响

传统上，一个智能合约完成一项工作，例如交易，但是 CTFC 将这改为完成部分交易，而且采取标准化的工作流程。而这工作需要 3 个领域专家合作完成：金融、法律、计算机。

另外 CFTC 的观点也将区块链区分为几种：可交易的链系统，只可以存证的链系统。监管机制的发展还会根据 CFTC 的指南而发展。

表 4 不同的链系统及其案例

序号	特性	案例
1	只可以存证的链系统	例如一些类似链，共识快，但是不能做交易（因为没有交易完备性）
2	可以交易的链系统，但是不好监管	现在公链系统，可以做交易，但是逃避监管
3	可以交易而且支持监管的链系统	熊猫模型，金丝猴模型，Fnality 模型，Libra 2.0 等
4	支持监管但是不能交易的链系统	因为交易才需要监管机制，能监管但是不能交易的链没有价值，没有案例

（3）产业上的影响

根据 CFTC 的分工，以后智能合约产业可以从横向和纵向两个不同角度进行划分，即：以应用领域分，也可以以交易步骤分。可能不同的产业之间会用到同一个（微）智能合约的服务，同样，一个（微）智能合约会向多种产业提供服务，处理面向不同行业客户的交易。

交易和监管标准化是 CFTC 提出的最大贡献。以前，每一套系统需要单独验证，以后有可能一套合约系统可以提供服务给许多系统。区块链产业将走向工业化的制度。

4. 突破 4—架构化：英国央行打破传统智能合约架构，走向康庄大道

英国央行在 2020 年 3 月发布了一份报告，讨论零售数字法币（Retail CBDC）的设计。其中提出 3 种不同的智能合约平台架构。

（1）认知上的改变

传统上，智能合约系统运行在区块链平台上，1 对 1 对应，而且没有监管单位在上面。但是英国央行以 3 种架构破 2 个传统思维，这 3 大架构解答了一个问题：智能合约平台应该放在哪里？在区块链系统内，还是在区块链系统外并行处理，还是在区块链外但是先处理？[3]

- 打破传统智能合约只能在区块链里面执行的传统：这里英国央行提出合约传统（S）和区块链系统（或是账本系统 L）关系：
  - S 在 L 里面， 同时进行， 这是传统思维；
  - S 和 L 可以并行处理，就是智能合约平台和区块链平台同时间处理交易，例如 S 做清算，L 做交易；
  - S 比 L 先处理，就是智能合约系统执行后，交给区块链系统再处理，例如 S 先处理客户信息，确保客户信息正确后才到 L 系统交易；
  - S 比 L 后处理，例如在 L 系统进行交易，交易后，由在外面的 S 系统进行清算。
- 打破链上代码的传统，智能合约代码有央行（监管单位）控制和执行，而且可以和服务提供商的合约代码一起合作，这个是管理上的创新。

但是英国央行还是停留在 1 对 1 的思维上，只是 L 和 S 的位置和执行顺序改变。由此我们中国团队提出另外的一个创新：

- 提出多对多的架构, 一个 L 系统可以和多个 S 系统合作，如下图：
  - 一个 L 系统和多个 S 系统合作（左图）；

- 一个 S 系统可以和多个 L 系统合作（中间图）；
- 多个 L 系统可以和多个 S 系统合作（右边图）。

我们提的三驾马车模型就是多个左图：即部分合约在核心账本内，部分合约在并行系统上，而在接口还有另外一套合约系统，这是 1 个 L 系统和多个 S 系统合作的案例。在这配置下，交易上的完成功能可以在核心系统里面完成，可以独立作业就选择在核心账本外并行处理来减轻核心系统的工作量，而实时监管和交易在接口上再次减轻核心系统的工作量。总之，我们的理念是系统对于金融数据要有监管机制[13]。

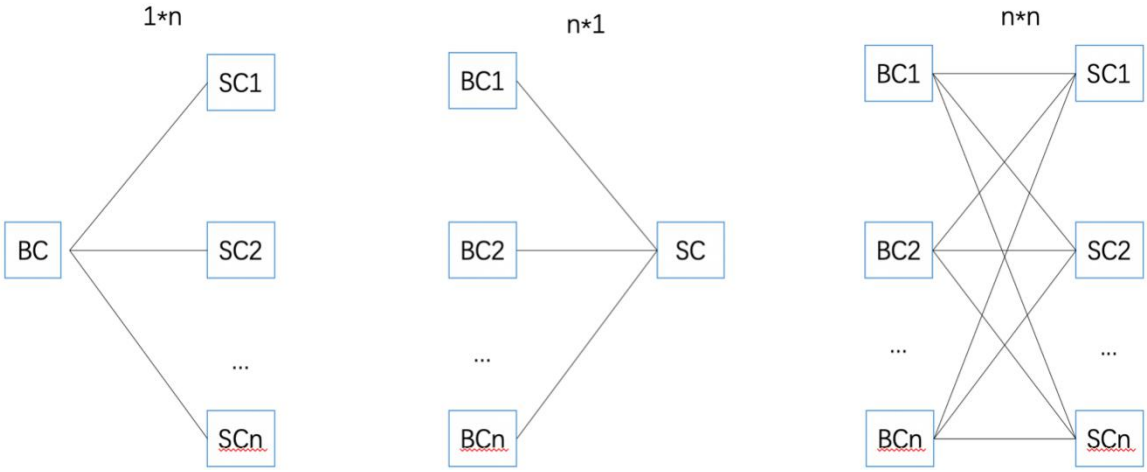

图 2 多对多架构（左边是 1 对多，中间是多对 1，右边是多对多，BC 是链，SC 是合约）

明显的，英国央行在智能合约上的思路和美国 CFTC 智能合约思路非常靠近。美国 CFTC 认为智能合约 2 个最大应用是完成交易和监管机制，而英国央行推出的 3 个智能合约框架就是执行这 2 个应用。同样，在三架马车架构下，客户的服务可由区块链提交给多个智能合约完成，也可由服务提供商将多个原子智能合约组装起来，部署并使用。这样智能合约不再是技术孤岛，不单单是只是软件验证或是形式化验证，更是参与到完整的系统架构中。

下图就是一个例子，两组智能合约，都是监管合约，一组负责 KYC，一组负责反洗钱（AML），这两组智能合约都进行一笔交易的部分流程，而每月笔交易都要经过 KYC 和 AML 智能合约步骤才能完成。

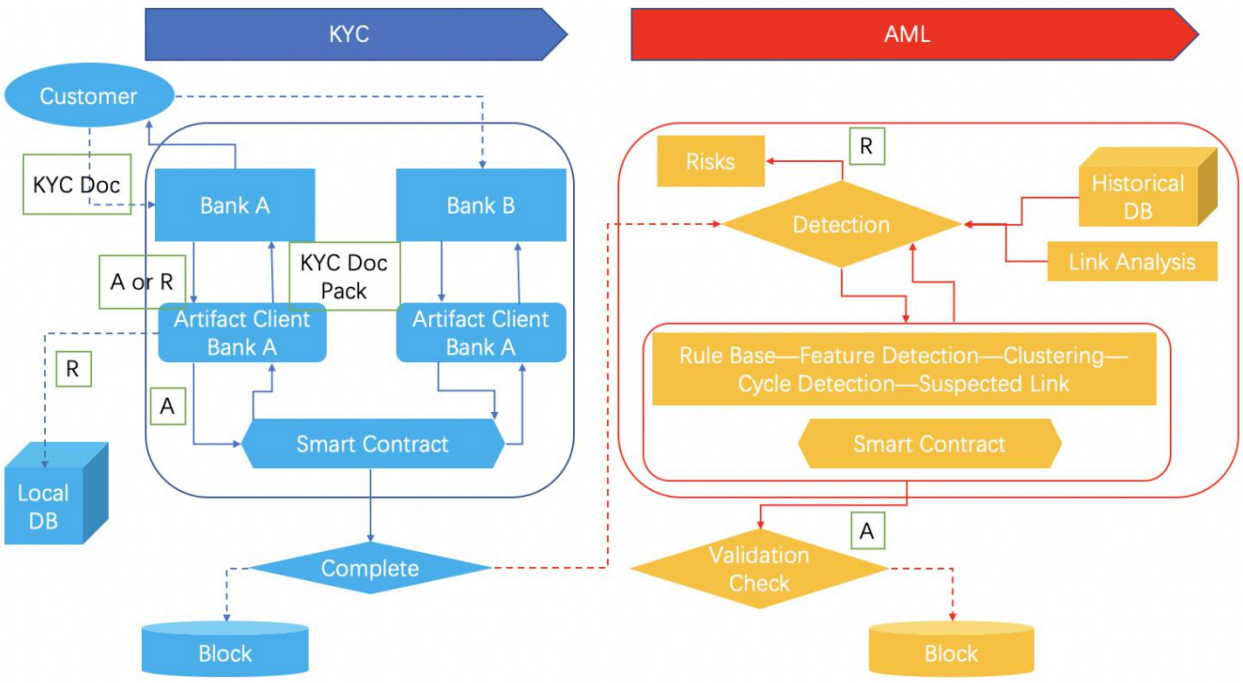

图 3 每一笔交易中进过两组智能合约的监管

（2）学术上的影响

由于 S（合约系统）和 L（账本系统）可以多对多，也可以先行，后行，并行，这样智能合约平台设计比以前复杂但是功能更强大。这样区块链和智能合约，以及和预言机的协议必定需要更新。

原来智能合约三原则，即：1)数据完全来自区块链; 2)计算结果有共识; 3)计算结果完全存在区块链上，还是假设区块链和智能合约系统是 1 对 1 对应的。现在在多对多对应下，对于一个智能合约来说，它可以从多个区块链中获取数据，再将数据写回多个区块链中。由于多对多架构，发送链、计算链、和存储链可以是不同链系统。智能合约原则必须更改：

- **传送原则**：合约数据必须来自区块链，即使数据来自预言机，但是数据先需要存留在区块链上才能在智能合约系统运行。但是这里智能合约使用的数据可以来自不同区块链系统，但是每个数据都有数据源（传送链的数字身份证）和时间戳信息。
- **计算原则**：合约计算有共识，这原则仍然成立，每个智能合约系统还是有自己的区块链系统（例如选择其中相关系统为主支撑系统）；

- **写回原则**：合约计算结果可以存在不同区块链上，由于合约系统的共识不一定在存储链上进行，这次写等于是一个新的“写”作业，由存储链进行共识后将这数据存下。每个数据写回的数据也都有数据源（计算链的数字身份证）和时间戳信息。

基于以上新的智能合约三原则（针对多对多架构），可保证数据来源真实有效，计算结果的准确性，以及最终数据可保存。这些协议已经申请专利。

（3）产业上的影响

现在 1 对 1 的合约系统限制了区块链和智能合约的应用和发展，因为智能合约系统被一个系统完全控制，有大量的限制。而且根据 CFTC，合约服务应该是碎片化，标准化，(微)服务化的，这样就需要允许不同单位一起参与建立合约库，而且仍然需要有标准化的管理。

基于多对多的 S（合约系统）和 L（账本系统）体系可实现多个交易申请的同时处理，同时完成多个交易数据的写回，这样大大扩展合约系统，也扩展账本系统。另外外面服务商业提供其他合约服务，和央行合约服务一起配合。这些对区块链和智能合约产业都会产生影响。

例如一个国家可能有 10 万个交易系统，每个交易系统都需要交易服务和监管服务。传统 1 对 1 的配置，这会非常痛苦，但是在多对多的配置下，例如一些 KYC 服务库可以和几万个交易系统合作。例如这个合约库可以复制到这些交易所（使用区块链数据湖[13]的双锁定的方法），在这几万个系统里面有同样的算法。而这合约系统容易扩展，可以支持大量的系统。这是熊猫模型的精神，算法和数据分开，当我们把算法和数据分开的时候，系统就可以扩展，而我们把不同算法放在不同合约库的时候，扩展度再一次扩展。这样就可以支持链满天下，约满天下。

为什么这些创新开启了康庄大道？拿上图 KYC 和 AML 智能合约组来看，如果我们将他们都放在一个系统里面，这系统会多复杂？但是将这些系统标准化，松解化后，系统完全不同。

5. 突破 5—工程化: 雅阁项目指出智能合约的法言法语可以是形式化建模语言

雅阁项目出发点和李嘉图合约类似，也是少数考虑法律效力的智能合约项目。

（1）认知上的改变

雅阁项目 2 位创始人都是法律专业背景，包括法学老师。也由于这一原因，大部分项目讨论都集中从现在法律合同导出智能合约。事实上，他们工具后面有强大的科技支撑，而这就是形式化智能合约语言 Ergo 以及这语言后面的证明系统(proof systems)。这语言后面的形式化语言最后是基于 Coq 形式化语言，也是函数型编程语言。这样雅阁项目和其他可计算合同项目就有了一个差距，其他项目就是有合同模版，这里也有合同模版，而且合同语言是基于形式化语言。

智能合约开发可以使用特殊的语言，可以是 Solidity，可以是 Move。为了匹配上述预言机、智能合约、区块链多对多的架构特点，智能合约的开发语言不仅仅只是代码，更需要一种新型的建模语言。雅阁项目的模型就是一个重要参考，其语言 Ergo 后面是强大的形式化语言，编写的逻辑条款可以直接进入形式化验证。而这语言又支持合同和条款语言，所以法务人员可以很快的建立合同条款，然后经过形式化的验证证明这些条款在逻辑上是正确，最终可以翻译成不同的计算机语言。

雅阁项目开发智能合约的思路，从法律的角度出发，创立合同模型，定义形式化语言，并将自然语言合同转化为该种语言的合同并处理。雅阁项目也提出合同模版，和李嘉图合约提出基于法律条款的模版类似，不同的是雅阁提出一种语言和合同模型，且以现在合同模版为出发点是正确的发展方向。

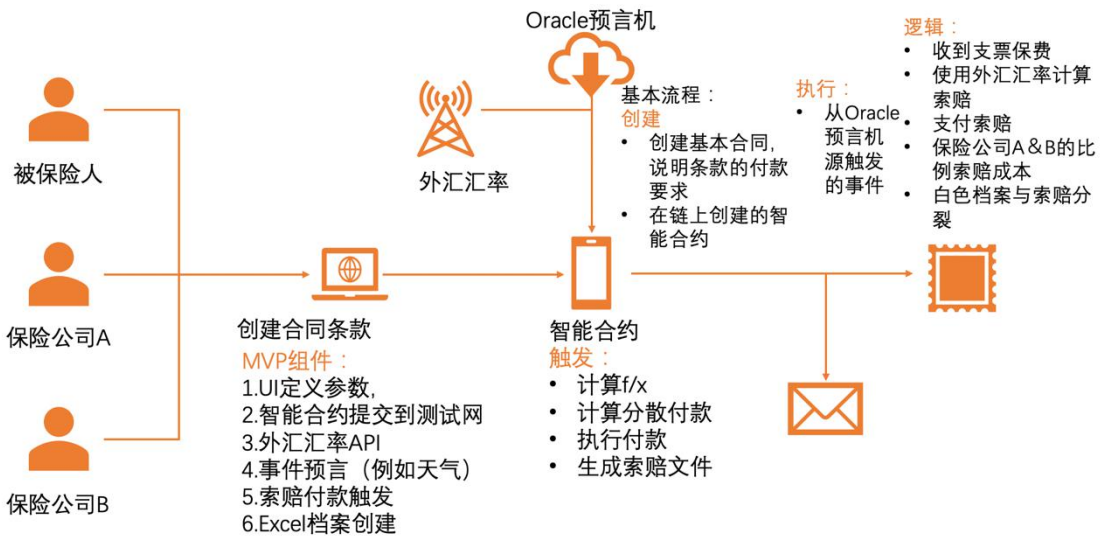

图 4 雅阁项目的架构

（2）学术上的影响

该项目带来重大信息，就是智能合约合规化和软件工程方法没有冲突。雅阁项目也是我们遇到过最完整的开发流程。这项目里面的一些技术路线也非常创新，会给其他相关项目一下新思想。计算机界在过去几年提出许多形式化方法来解决智能合约代码安全的问题，但是在合规上却一直没有实质进展。雅阁项目代表一个新方向。

我们的观点不在于这是一个最好的解决方案。事实上我们认为雅阁项目模型有许多地方可以改进。但是这项目却是我们遇到第一个以合规作为出发点，而又有形式化语言、建模工具和验证的系统，这是思想上重大突破，也是以后其他智能合约系统可以参考的地方。

（3）产业上的影响

这项目提出形式化，可执行的法言法语，是一个重要方向。如果被标准化，智能合约的工作可以更加细化保证合约有法律合规性以及软件质量。

6. 总结：皋陶模型

在研究上面 5 大突破后，我们团队提出皋陶模型，融合了上述 5 大点的优势，标准化，服务化。类似于 ISDA 实现标准化，像英国央行的一样由监管单位完全控制区块链。

标准化又包括平台标准化和智能合约语言标准化。智能合约平台第一需要区块链平台，而区块链必须标准化，特别在中国。另外还加上本土化、制度化、系统化的工作。只有实现制定明确的标准， 才能真正有标准可依，才能让更多人明确规则，遵循规则。智能合约的自动执行，更是需要事先有一套清晰的标准。[1,7,8]

参考文献

[1]. 蔡维德，《智能合约，重构社会契约》，法律出版社， 2020 9 月。

[2]. 蔡维德，《互链网：重新连接世界》东方出版社， 2020 9 月。

[3]. 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，https://mp.weixin.qq.com/s/RjgzC7ug7iJ2ykQW4XY09w

[4]. 蔡维德， “熊猫-CBDC 央行数字货币模型” ，2016.11.05，https://mp.weixin.qq.com/s/VMF1R9q2D61-2R3neo6lGg.

[5]. 蔡维德，姜晓芳， “基于批发数字法币(W-CBDC)的支付系统架构: Fnality 白皮书解读（上）” ，2019.10.12，https://mp.weixin.qq.com/s/raoNDsCB25m6CDh91uZAOw

[6]. 蔡维德，姜晓芳， “批发数字法币支付系统重构金融市场: Fnality 白皮书解读（下）” ，2019.10.12，https://mp.weixin.qq.com/s/fI7LcCZPi0WXq3Zw0M9-sA

[7]. 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.

[8]. 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.

[9]. https://www.cftc.gov/sites/default/files/201811/LabCFTC_PrimerSmartContracts112718_0.pdf

[10]. ISDA , LEGAL GUIDELINES FOR SMART DERIVATIVES CONTRACTS: THE ISDA MASTER AGREEMENT Feb , 2019

[11]. Bank of England. Central Bank Digital Currency Opportunities, challenges and design [R]. March 2020. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currencu-opportunities-challenges-and-design-discussion-paper

[12]. 蔡维德. “迎接 “约满天下” 时代的道路：智能合约的蝶变”，2020.06.17.

[13]. 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&from=timeline&isappinstalled=0

作者简介：

蔡维德：北航数字社会与区块链实验室主任，天德科技首席科学家，国家科技部重大项目负责人，中国信息界区块链研究院院长，国家大数据（贵州）综合试验区区块链互联网实验室主任， 天民（青岛）国际沙盒研究院院长， 赛迪（青岛）区块链研究院名誉院长，中国亚洲经济发展协会区块链产业专业委员会会长

向伟静：北京航空航天大学硕士研究生

张韬：北京华讯律师事务所主任