区块链技术和行业发展七个新趋势：新架构、新网络、新商业模型

蔡维德、姜晓芳、王康明

2021 年 4 月 27 号

背景

新型数字货币战争实际上可分为三部曲：第一阶段与支付相关，第二阶段是银行改革，而第三阶段则是各行各业改革。2021年，由于美国财政部批准银行参与区块链作业，并且可以发行稳定币，美国正式进入第二阶段。但是很明显，美国许多行业正在进行第三阶段的布局。在第三阶段，各行各业都采用区块链技术，社会各界开始全面进入区块链和数字货币世界。

在2020年11月以前，区块链发展遵循币圈先行、合规市场跟随的模式，因为合规市场需要考虑法律问题。可是在如今区块链发展形势下，这种模式恐怕已不再合适。

2020年6月之后，币圈在悄然发生着重大改变：1）很多数字代币开始合规化；2）许多交易所也服从旅行规则（要求交易者进行个人身份验证）； 3）大批合规金融机构开始投资数字货币（只能投资合规项目），这使得数字货币市场迅猛发展。2021年4月，全球最大的比特币和数字货币交易平台Coinbase在美国纳斯达克成功上市，代表该币圈交易所全面合规化，而美国监管单位也同意让其股票上市 。

于是，币圈开始抛弃过去一些常见的行为，例如以前零知识证明协议的数字代币可以在交易所交易，现在已被要求下架。现在交易所也进行“了解你的客户”（Know Your Customer, KYC）和反洗钱（Anti-Money Laundering, AML）分析，以前这都是不需要的。

数字代币交易不再匿名，因为美国监管单位已经全面追踪“匿名的”数字代币，这些“匿名的”代币早已透明。现在几乎所有的数字货币交易都已被监管，连国外暗网也不接受比特币，因为如果使用比特币，由于监管的缘故，暗网已不复是暗网了。整个区块链领域发生了翻天覆地的变化：

2021年2月，据美国媒体报导，IBM公司区块链部门重组，超级账本不再是公司产品。美国区块链产业分析师表示纯IT形式的区块链发展模式已经证实不行。而这发生在全球央行、银行、金融机构、大型科技公司全力进入区块链行业之际，说明区块链蓬勃发展的新路线已经找到，其中一个路线就是非同质化代币（Non-Fungible Tokens, NFT），但这并不是唯一，现在是百花齐放的时代。

2021年4月13日，美国著名高科技公司Palantir表示美国国税局已和其签约，将使用高科技来追踪比特币交易，这可能就是连暗网都不接受比特币交易的重要原因。

2021年4月14日， Coinbase 在美国成功上市。

2021年4月15日，预言机公司ChainLink发布第2代系统白皮书（以下简称ChainLink白皮书，部分章节译稿见附件）。

2021年4月16日，美联储表示美国央行数字货币（Central Bank Digital Currency, CBDC）是高优先级的项目，这是美联储第一次这样表示。在这以前，2021年2月，美联储曾表示，美国CBDC项目会使用区块链技术（这也是第一次明确表示），而2021年3月，美联储和麻省理工学院表示两个CBDC实验平台会在2021年7月出现。

2021年4月20日，英国开启数字英镑特别工作组（Task Force），支持金融科技公司开展相关科技包括上市计划，提供数据服务。

在不到一个月的时间里，这么多重要事件密集发生，表示数字货币竞争正在紧锣密鼓的进行中。在2021年4月25号，笔者在人民大学重阳金融研究院就以“百花齐放，极速进展”来形容这种激烈的竞争场景。

经过我们的分析，认为区块链行业将出现七个新趋势，包括合规化（第1节），新系统架构（第2，3，4节），新信任网络（第5节），新软件工程（第6节），新商业模型（第7节）。

1. 区块链界走向合规化、学术化，数字货币战争第三阶段开启

ChainLink白皮书作者来自美国/欧洲著名大学，包括伯尔尼大学、康纳尔大学、加州大学圣地亚哥分校、伊利诺伊大学厄巴纳香槟分校的教授，也有毕业于哈佛大学或斯坦福大学，和即将入学杜克大学的博士研究生。这几所大学都是享誉全球的著名大学，所以说币圈也开始进入合规化、学术化。

ChainLink白皮书有科技含量，也提出了具体技术，与2017-2018年白皮书泛滥的时代大不相同。这代表区块链领域开始走向成熟，传统币圈开始合规化，以前胡编乱造的白皮书正在消失。这属于数字货币战争第三部曲，币圈现在是从不合规向合规转移，这样，新型数字货币战争的三个阶段等于同时在进行。

图1　原来数字货币战争三部曲

虽然还需要磨合，但是第三阶段已经开启，所以现在是制定规则的时候。监管规则不是仅为监管，而是为市场引导方向——“定义新市场”，看起来中立的监管规则却能改变一些市场规则。由于监管起到了规则制定的作用，成了非常有用的工具。监管的战略目标是引导开发新市场，并通过科技手段来执行。所以我们应以新市场的布局来决定监管机制和监管政策，这是一个重要概念。

2. 广义区块链定义

2020年3月，我们在中国提出重新定义的区块链，把传统区块链系统扩展到账本系统（Ledgers, BC），加上智能合约系统（Smart Contracts, SC）及预言机系统（Oracle Machines, OM），而且这些系统之间可以有多对多的关系出现。例如一个账本系统可以有多个SC系统，一个SC系统可以和多个账本系统合作，一个OM可以和多个SC系统连接。

2020年10月，我们又发表了LSO（Ledgers账本， Smart contracts智能合约， Oracles预言机）模型的英文文章，再度延伸这个定义，让这些系统可以**经过注册而动态**调整。在《智能合约：重构社会契约》书中提到，这样的新模型方便统一管理和监管。如许多股票交易系统，可以使用标准化SC，这样监管单位可以制定统一监管规则，建立一个可以共用的SC库。

这些研究成果改变了人们对于区块链的认知，区块链的定义也发生了改变，从此变成多对多的模型，区块链是多系统且可以动态调整的，这跟传统的区块链定义有着云泥之别。

而现在币圈、链圈和主流学术界也在走同一路线。以前狭义的区块链定义都开始改变，例如一个BC支持一个SC系统，BC和SC绑定，共识和交易绑定。

3. 新型预言机架构

未来的区块链系统会是复杂系统，比如，一个区块链应用系统可以有一个BC、3个SC、2个OM，而其中一个OM又有自己的BC和SC。所以这将是一个复杂系统，与2016、2017年提出的所谓“区块链网络”或“区块链操作系统”等概念差异巨大。以前这些概念都是单一机制而全网布局的系统，系统虽大但却是单一的（每个节点上都是相同的软件和数据），上面的资产也只是一种代币，交易机制只有一种，难以被监管，也不符合现代金融交易流程。

早期预言机单纯收集数据，并将数据以安全的方式送到区块链系统。后来预言机的定义范围扩大，可以是复杂系统，可以使用区块链和智能合约，还可以进行验证和隐私计算，来保证数据正确。如LSO架构，允许多个BC、SC和OM相互协作，甚至可以通过协作层（CL）动态创建它们的关系，并且CL位于多个BC、SC和OM之间。一个OM可与多个SC交互，也可以和多个BC交互。每个OM必须先向BC注册，然后才能向BC发送数据或从BC接收数据。

OM可以提供及时且正确的信息，也可以提供不正确甚至误导或恶意的信息。因此，LSO系统需要具有动态评估机制来跟踪参与的OM的可靠性。与OM关联的还有几种设计模式：立即读取，发布-订阅和请求-响应。所有这些都与观察者设计模式，事件驱动架构（EDA）有关。

这样就会出现一个复杂的区块链网络，上面有多个BC、SC和OM系统。由于多个系统的出现，出现事件模型，由多个OM向多个BC和SC传送事件。事件模型注册合同参与者的事件，并将自然语言合同标准化为事件，即，在合同的内部处理逻辑下（以软件代码的形式表示，大致为条件声明），对合同进行预处理，包括对事件属性和合同属性的数据分别包装和存储，并通知司法当局进行公证。事件开始后，根据事件ID查找相应的事件数据包和合同数据包，并将其提交给SC系统以进行自动交易处理。同时，与账户资产相关的信息会提前提交到BC系统进行资产验证或证明，如果涉及资产欺诈或参与者在不信任方列表中，则会搜索对应账户的信用记录。可以通知合同参与者或监管机构终止合同并启动终止事件。

而OM的功能也被扩充。例如，2021年4月，ChainLink提出一个分权式（或是分布式）OM网络（Decentralized Oracle Networks，DON），使用其他资产（网络，存储，计算）和区块链系统合作完成应用，扩充了传统OM的系统规模。

DON由OM节点组成，可以和BC合作，也可使用SC，但也可以使用非区块链系统的服务，例如传统互联网服务，如下图表示。

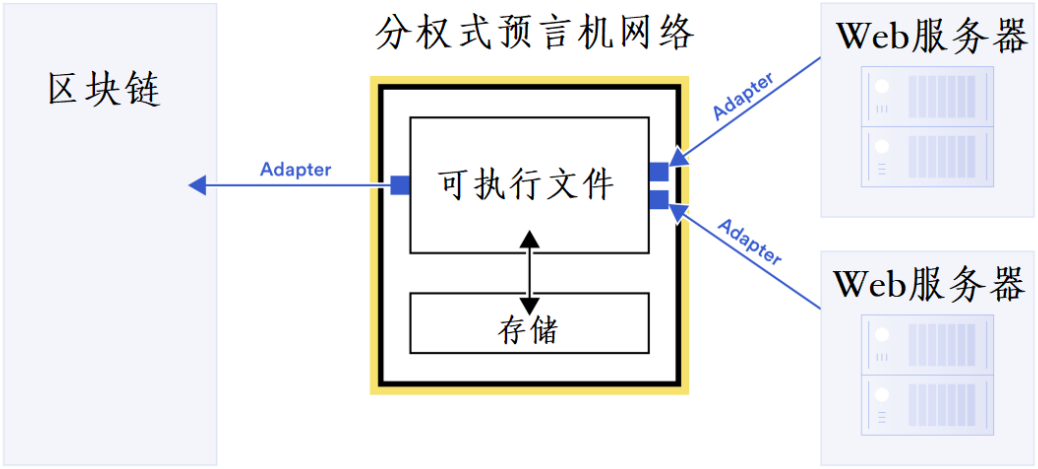


图2　ChainLink 分权式OM

图2是一个概念图，说明了DON如何实现OM基本功能，即将链下数据转发到一个合约。可执行文件使用适配器获取链下数据，并在其上进行计算，通过另一个适配器将输出发送到目标区块链。（适配器由DON中的代码启动，用蓝色小框表示；箭头表示此特定示例的数据流方向。）可执行文件还可以读取和写入本地DON存储，以保持状态和/或与其他可执行文件通信。

4. 新型 SC 架构

传统上，SC在BC上执行，和BC连接，SC的数据需要来自BC，才能使数据有保障。LSO机制打破这一传统，引入OM，OM是提供与外部信息的智能合约的第三方服务。它们是BC与外部世界之间的桥梁，是一种可以在不同BC之间提供互操作性并与外部数据源进行通信的工具。

LSO提出了一种支持隐私计算的可伸缩OM，它不仅可以确保数据收集过程合理，而且可以进行隐私计算并维护系统服务的可伸缩性。并为每个节点设计了信誉评估策略，以确定每个节点是否为恶意节点。每次提交之后，将更新每个节点的信誉值。另外，OM使用BC来保存数据以保护内容提供者。作为SC的数据馈送服务，它可以忠实地提供离线数据，从而确保账本上数据的真实性，并实现SC与外界的交互。

而ChainLink提出一个新概念——链上与链下合作的混合型SC。这里链上数据由BC保障，链下数据由OM系统保障，而OM系统可以有自己的BC和SC。因此，链上链下数据都经过验证流程，这样，SC作业可由链上和链下合作完成。

这里一共有三套系统：

- BC保证送上来的数据不会被更改，会被节点诚实地记录；但是BC不担保被送上来的数据本身就是正确的，这个由OM负责。BC保证数字资产的所有权；
- OM保证送上去的数据是正确的；
- SC保证它所从事的计算是正确的，同时从事监管工作，并且以验证数据的机制来保护系统，抵抗外面的攻击。

也就是说，三者各负其责，数据提供商（可以是金融机构、新闻媒体、物流、天气预测中心等）即OM保证数据本身正确，SC保证数据的计算行为和操作正确，而BC则保证数据的存储正确和存储安全。

混合智能合约（简称**混合合约**）的核心是使智能合约能安全地结合链上和链下优势。

链上部分以SC表示，链下部分以Exec表示。DON提供多种链下服务来实现链上功能的安全组合。

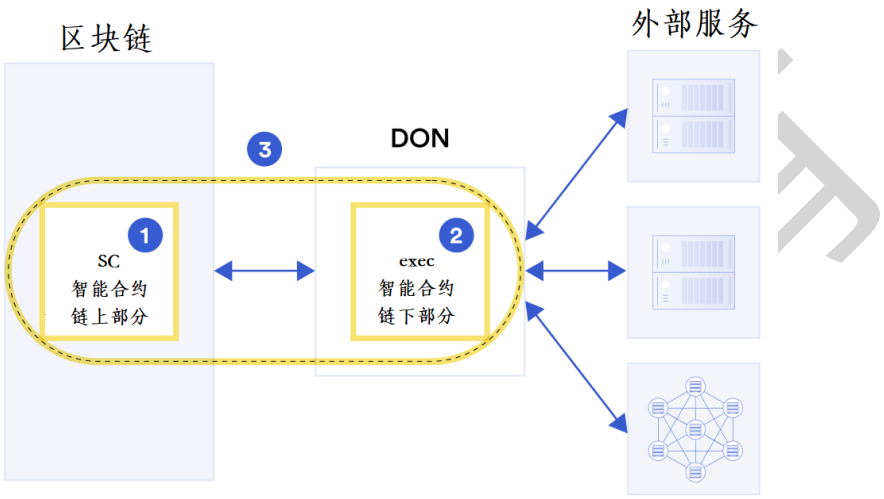


图3 新型智能合约由链上和链下合作完成

除了BC、OM和SC外，还需要其他辅助系统，如事件处理（Event Processing）系统、大型大数据监管系统、监管注册系统如STRISA系统等。

SC的发展历史发展可见下表：

表1 智能合约历史发展

序号	时间	提出者	特性	目的	创新点
1	1994年	尼克.萨博	链上代码，自动执行	提出概念	智能合约概念
2	1995年	Ian Grigg	李嘉图合约，SC的设计	引导智能合约研究走入正道	系统化 从法律角度出发 从合同模板出发

					分解智能合约开发的流程为法律和计算机两大部分
3	2016年	雅阁（Accord）项目	形式化合规语言和模板	工程化，开发开源框架	从合规端出发，落地在计算机语言和验证方法上
4	2018年开始	ISDA协会	和区块链没关系，没有一行智能合约代码	制定标准	1）标准化，明白智能合约的流程。新数字金融市场应根据改进后的流程 2）智能合约代码与智能法律合同是有区别的 3）事件的概念，合规SC需要“事件处理系统”作为基础设施
5	2018年	CFTC	《智能合约入门指南》	提出智能合约开发难题的解决方案，将来产业的分工结构。	智能合约大应用是交易和监管；合约服务应该碎片化、标准化、自动化
6	2019年	北航团队	比格犬智能合约模型	降低智能合约使用门槛，对客户屏蔽高科技部分	通过领域分析来开发智能合约模板
7	2020年3月	英国央行	分布式智能合约	智能合约可用于监管	3个智能合约框架，打破传统智能合约（SC）只能在区块链（BC）里执行且同时执行的传统思维
8	2020年	北航团队	三驾马车模型	架构更为灵活	系统架构方面的突破，不再是传统区块链和智能合约1对1的架构，而是多对多的架构

9	2020年	北航团队	LSO	OM是重要组成部分	在三驾马车基础上引入OM，动态框架，允许BC、SC和OM加入互链网，并可通过分层结构扩展到数百万个系统
10	2020年	北航团队	STRISA	兼容 TRISA 旅行规则的合规监管框架	比 TRISA 系统具有更完善的机制，更丰富的功能，兼容性高，集成大数据分析、人工智能、区块链数据湖等先进技术，支持 KYC 和 AML，可以使用在监管以及合规应用上
11	2021年	ChainLink	混合智能合约	链下与链上结合	链上与链下合作的新型混合型智能合约，结合边缘计算，就地解决问题

照此发展下去，区块链网络系统越来越复杂，链上和链下一起完成SC。由于传统链上系统比较有信誉，这种混合SC的信誉度会比较低。这样，网络系统会出现动态信誉度评估系统（Dynamic reputation evaluation system， DRES），对参与的BC、SC和OM系统来进行评估。而这些DRES也被其他DRES评估或客户评估，维持一个互相评估的闭环系统。

这种动态信誉评估机制是我们在2017年贵阳数博会上提出的，当时主要是评估BC系统，现在还需要评估SC和OM系统。

5. 新型区块链网络：信任网络

2020年，美国财政部提出，三至五年后，美联储乃至全美国的支付网络都会被区块链网络全面取代，并且该网络系统会开放给企业开发和经营，在其上盈利。如果这得到

实施，将会是重大变革，代表以美联储为中心的支付系统会出现新型区块链网络，一个划时代的网络出现。

根据这一计划，传统互联网时代的金融体系将会全部被区块链网络所取代，而银行将附属在此区块链网络上，这个观点源自普林斯顿大学数字货币区（Digital Currency Areas, DCA）理论。

这将会是哪一种区块链网络？可能是新型区块链网络，例如互链网。从2017到2018年开始，美国、中国、瑞士都提出新型互联网概念，美国提出加密宇宙思想（Cryptocosm），中国提出互链网（ChainNet）。

2017年，《经济人》杂志提出区块链系统是“信任机器”（Trust Machine），但现在已变成“信任网络”（Trust Network），不但区块链定义扩展了，网络定义也更新了。

2017年贵阳数博会上，我们提出区块链网络必定会改革成为下一代互链网，并于2018年将这写成第一个区块链中国梦，开启了我们的区块链中国梦系列。这一新型信任网络就是互链网，每一层上的系统都会更新，有些还有结构性的改变，应用方式也发生改变。互链网实际项目始于2020年初，该项目将BC和相关技术用于信息和通信系统。换言之，这些系统将被区块链化。例如，将修改操作系统（OS）、数据库、网络协议以直接支持BC操作。我们已经在互链网中提出了一些关于OS、数据库、网络协议以及应用程序体系结构的新设计。

互链网上不但有价值网络，还有并行的“监管网络”，这代表信任网络包含价值网络和监管网络。老百姓们可以在价值链网上做交易、做公证，监管网络则监视价值链网活动，保证系统和交易不发生风险——一个新的可信的网络社会将会出现。

新型区块链网络并非传统跨链技术

系统之间需要有复杂的交互，但是交互并不等同于跨链，交互的本质是从多条BC或多个OM、多个SC，获取数据进行融合计算。这和传统跨链思想不同，跨链交易是两个以上的链交换价值，这些链或有不同结构，或是同一结构，交易时，交易双方的链都需要有共识。因此跨链需要进行多次共识，速度肯定会慢下来。一些跨链技术为了加快速度，牺牲了交易性和可监管性，使其很难在合规金融市场使用。

现在Chainlink所提的不是跨链，而是多链合作的机制，多BC、多SC、多OM合作的应用系统。比如说每个应用都需要有“区块链家”（Homebase blockchain），这就是它的主要区块链系统。这种应用可以使用许多BC或OM的数据，而这些BC和OM都必须签名以保证提供数据的正确性，这样区块链网络系统就变成了一种复杂的、可信任的网络系统，而不是传统的跨链网络系统。

6. 基于区块链的新型软件工程出现：新型数字金融出现

传统软件工程工具包括编译器、数据库系统、操作系统、云、容器等，但不是可信软件工程机制，而是属于系统或应用；现在，BC（自带不可篡改性）、SC、OM，都自带可信机制，加上动态STRISA、LSO工具，新型软件工程架构出现。

传统软件可信的评判标准包括可靠性（Reliability）、安全性（Safety）、保密性（Security）、容错性（Fault Tolerance）、时效性（Real Time），这在新型软件工程中仍然成立，但是会出现更多的工具。以后，这些新工具都可以是软件工程标配，和操作系统、数据库一样，和设计模式（Design Patterns）、框架（Frameworks）一样是标配；和互联网的网络一样也是基础设施。

深度学习的发展可以帮助我们理解这一点。因为有好的深度学习软件工具出现，开展深度学习实验和应用的门槛降低，许多本科生或是高中生都可以从事深度学习实验和应用。

而按照现在美联储等的布局，以后必定会出现区块链网络，相关的软件工具也会出现。这些软件工具可以助力SC的建模、开发和验证，并且运行在区块链网络上。这就是可编程的数字金融，也是新型货币战争的第三阶段。那时，由于大量工具出现，本科生或是高中生，都可以使用网上（更正确一点是链上）的软件工具，开发可编程的数字金融。建立一个新区块链应用系统，以后可能只需要几天，而不是像现在这样需要许多人年才能完成。

最近SC上的工作已经出现软件工程思想，例如国际掉期交易协会（International Swaps and Derivatives Association, ISDA）竟然在没有使用任何代码的情况下提出SC标准，这表示大量的SC工作和代码没有任何关系，而是和法律、金融交易相关，这符合软件工程的原则——软件需求不同于软件代码；美国和英国合作的雅阁项目（Accord

Project），也是从法律出发，且又使用形式化语言，属于法律和高科技结盟的SC产品；而中国的比格犬模型(Beagle Model)，也是结合法律、金融和软件工程的方法，例如领域工程；美国斯坦福大学的CodeX计划中的可计算的合同（Computable contracts）项目也是大量使用逻辑学和机器学习方法。

形式化方法对可信软件工程的发展与推进起到至关重要的作用，它以一种标准化的模式对可信软件进行规范化，提供一个高效、统一的结构框架能够同时支持多种可信性质，能够将关键性质进行有机集成。这就是皋陶模型的精神（参见《智能合约：重构社会契约》第19章）。

7. 新型商业模型出现：数字资产时代来临

区块链技术已经让许多行业的商业模型改变，例如新版权商业模型NFT出现，是最近的热点。2021年第一季度NFT的成长倍数竟然是去年一整年的8倍，是目前区块链应用发展最快速的热点领域。

过去版权产业一直被认为无法盈利，起码在中国是如此，但现在却是全球金融市场最热门的领域。NFT包括治理、经济学设计、技术设计和价值主张等多个层次，将是未来价值竞争的新赛道。

NFT和传统数字代币不同，同样的两个数字代币之间没有差异，而NFT是独一无二、不可分割的（而传统数字货币是可以分割的），可以代表特定的数字产权，这等于开创一个全新的数字经济。而这不可分割的代币和可以分割的代币可以合作，建立新商业模型。

NFT大火带来一个重要信息，区块链可以带来新型商业模型。传统上平常的领域，在区块链时代可以一夜之间“麻雀变凤凰”，打破传统思维。

需要指出的是，国外NFT项目还是和发币相关，而在中国发展对应的NFT项目，需要遵守国内法律不能发币的约束。

由于超级账本系统在国外出状况，国际数字经济分析师立刻表示一个新时代已经来临了，一个基于数字资产和商业结合的新盈利模型正在强力出现，由于大笔合规基金的资金在2020年第4季开始进入数字资产领域。而这种新商业模型和传统商业模型不同，NFT只是一个例子。这数字货币会是合规稳定币，合规数字资产，或是CBDC。

英国CBDC特别工作组成立的时候，媒体的报导非常有趣。媒体表示英国已经没有时间再等了，大量时间都花在研究上，而其他国家现在都跑在英国前面（他们还记得2015年英国是世界第一个国家推出CBDC计划，当时领先世界），必须马上有重大改革。

8. 总结

整个区块链领域已经发生翻天覆地的改变，区块链界走向合规化、学术化，数字货币战争第三阶段已开启；广义区块链定义得到认可；新型OM出现；链上与链下合作的一种新型的、混合型智能合约出现；新型区块链网络“信任网络”正在形成；新型可信软件工程出现；NFT等新型商业模式出现。未来已来！

参考文献

1. A. Beniiche, “A Study of Blockchain Oracles,” July 14, 2020.
2. Youtradefx, “Blockchain Oracles: The Key to Scalability and Interoperability,” August 9, 2020 https://www.youtradefx.com/blockchain-oracles-the-key-to-scalability-and-interoperability/#more-73
3. W. T. Tsai, Robert Blower, Yan Zhu, and Lian Yu, “A System View of Financial Blockchains,” Proc. of IEEE Service-Oriented System Engineering, 2016.
4. W. T. Tsai, Enyan Deng, X. Ding, and Jie Li, “Application of Blockchains to Trade Clearing”, Proc. of IEEE Sympoisum on Software Quality, Reliability, and Security Companion, July 1, 2018.
5. W. T. Tsai, et al., "Blockchain Application Development Techniques." Journal of Software 28.6 (2017): 1474-1487.
6. W. T. Tsai, and Lian Yu. "Lessons learned from developing permissioned blockchains." 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2018.
7. L. Yu and W. T. Tsai “State Synchronization in Process-Oriented Chaincode,” Journal of Frontier in Computer Science, Vol. 13, July 2019, pp. 1166-1181.
8. W. T. Tsai, et al., “COMPSACC: A Data-Driven Blockahin Evaluation,” Proc. of IEEE SOSE 2020.
9. W. T. Tsai, “ChainNet:A New Approach for Structuring System Architecture and Applications, “ Keynote presentation on August 6, 2020 with video recording.
10. He, J., Wang, R., Tsai, W. T., & Deng, E. (2019, October). SDFS: A Scalable Data Feed Service for Smart Contracts. In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS) (pp. 581-585). IEEE.
11. Wei-Tek Tsai, Dong Yang,Kangmin Wang,Weijing Xiang and Enyan Deng, STRISA : A New Architecture to Enforce Travel Rule//FICC 2020
12. 蔡维德、刘琳、姜晓芳. 区块链的中国梦之一： 区块链互联网引领中国科技进步，2018.10.30

13. 蔡维德、姜晓芳、王康明，美国银行界全面进入基于区块链的数字货币，2021.01.06
14. 蔡维德、姜晓芳、王康明，银行和支付体系的改革：新型货币战争进入第二阶段，2021.01.12
15. 蔡维德等，智能合约：重构社会契约[M].法律出版社，2020
16. 蔡维德等，互链网:未来世界的连接方式[M].东方出版社，2020
17. 蔡维德等，互链网：重新定义区块链，2020.04.28
18. 蔡维德等，2020 年 10 月 IMF《跨境支付的数字货币:宏观金融的影响》报告解读系列（共十一篇）
19. 蔡维德等，Libra 2.0 解读：平台霸权——打赢新型数字货币战争的决定性武器，2020.05.11
20. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf
21. 蔡维德，监管科技新方向:网络化、嵌入式、实时化混合化、智能化、全面化，2020.10.09
22. 蔡维德，姜晓芳，“新货币竞争来了？没错！”，2019.06.21

附录

ChainLink 2.0白皮书提出混合智能合约的新概念，提升OM性能和吞吐量的可扩展性方案，保护用户敏感数据的保密方案，以及对用户公平的交易订单公平性设计方案，除此以外，其他的关键内容，包括屏蔽OM系统的复杂性，和OM的信任最小化模型。以下是白皮书中7个关键内容：

1） 混合智能合约：提供一个功能强大的通用框架，通过将链上和链下的计算资源安全地组合到混合智能合约中，来增强现有的智能合约功能。

2） 屏蔽复杂性：为开发人员和用户提供简单的功能，无需熟悉复杂的底层协议和系统边界。

3） 可扩展性性方案：确保OM服务实现高性能分权式系统所需的延迟和吞吐量。

4） 保密方案：将区块链固有的透明性与对敏感数据的保密保护相结合起来。

5） 交易订单公平性：以对最终用户公平的方式支持交易排序，并防止机器人程序和矿工开展老鼠仓剥削或其他攻击。

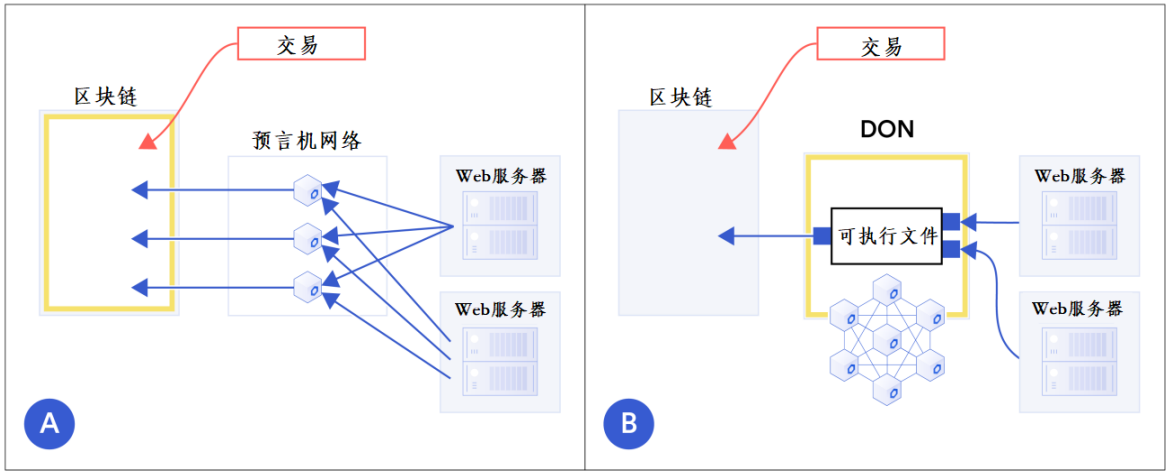
6） 信任最小化模型：通过分权式化、区块链中高安全性的强锚定、加密技术和加密经济保证，为智能合约和其他依赖OM的系统创建高度可信的支持层。

7） 基于激励的（加密经济）安全模型：严格设计和稳健部署的机制，确保DON中的节点具有强大的经济激励机制，即使面对资源充足的对手，也能可靠、正确地运行。

混合智能合约

混合智能合约通过将链上和链下计算资源安全地组合到一起来增强智能合约的功能。混合智能合约是由两个互补组件组成：驻留在区块链上的链上组件SC和在DON上执行的链下组件exec。DON是这两个组件之间的桥梁，也是连接混合合约与非链资源（如web服务、其他区块链、分权式存储等）的桥梁。

一个DON（表示为DON1）可以和一系列不同资源的适配器，包括另一个DON（表示为DON2）、区块链（主链）及其内存池、外部存储、web服务器和物联网设备（通过web服务器）进行连接，OM系统的设计也要考虑到多个方面，比如实现扩展性、数据保密和用户交易排序等，我们可以发现OM越发复杂，新型的OM系统开始出现。



链下在OM处理提升性能和吞吐量

概念图中展示了分权式OM网络如何提高SC的可扩展性。图A显示了传统的OM体系结构。交易直接发送到区块链，就像OM报告一样。因此，以黄色突出显示的区块链是交易处理的主要轨迹。图B显示了使用DON来支持区块链上的SC。DON可执行文件处理交易以及来自外部系统的数据，并将结果（例如，捆绑交易或由于交易的影响而导致的合约状态更改）转发给区块链。因此，以黄色突出显示的DON是事务处理的主要轨迹。

保护用户敏感数据的保密方案

智能合约可以处理机密数据的需求是真实客观存在的，比如使用私人分权式（和集中）金融身份、信贷信息，以及更有效和更方便地使用KYC和认证协议。

ChainLink使用三种主要方法来满足该需求，分别是：1）使用DECO和TOWN技术来实现一个保密适配器，2）使用安全多方计算和可信执行环境技术来实现机密计算，3）支持Lay 2保密系统。

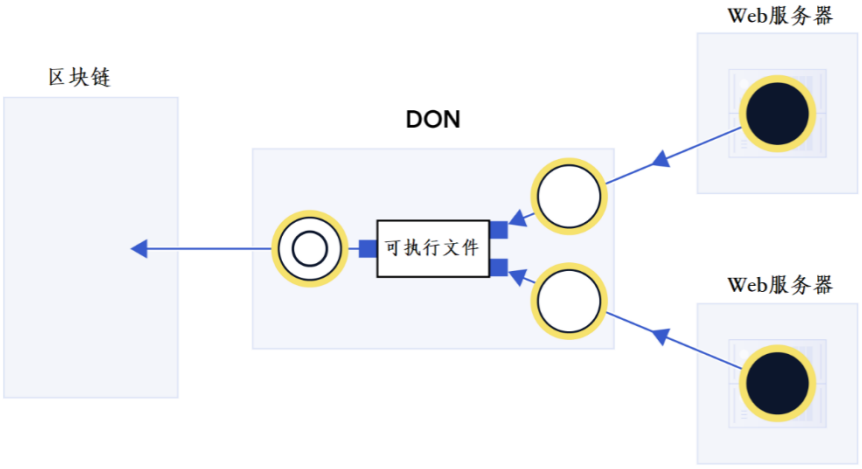


图5.敏感数据通过DON保密适配器和保密计算从外部源流向智能合约

图5是DON中敏感数据保密操作的概念图（以黄色突出显示）。web服务器中的敏感源数据（黑色圆圈）使用保密适配器（蓝色双箭头线）提取到DON。DON从这些适配器接收派生数据（空心圆），这是对敏感源数据应用函数或（例如）秘密共享的结果。DON上的可执行文件可以对派生数据应用机密计算来构造报告（双环），并通过适配器将其发送到区块链。

FSS确保交易订单公平性

如今的区块链设计有一个肮脏的公开秘密：矿工和验证者可以自主选择哪些交易进行打包或验证，用户还可以根据支付的网络费用（例如以太坊的Gas费）来操纵交易顺序。矿工监听用户的交易，并将自身的利用性交易插入同一区块中的较早位置，从而通过利用对用户交易的预先判断，从用户那里窃取资金，这就是名叫老鼠仓的操纵形式。例如，机器人程序可以在用户的购买订单之前下一个购买订单，然后从用户交易引起的资产价格上涨中获利。

“公平排序服务”（Fair Sequencing Service, FSS）是现代交易非常重要的规则，防止交易所或是交易系统作弊。Chainlink也提供 FSS服务，FSS帮助智能合约设计人员确保其交易的公平排序，并避免对用户交易以及其他类型事务（如OM报表传输）的前向运行、后向运行和相关攻击。FSS使DON能够实现一些思想，比如引入严格的时序公平性概念，此外FSS还可以降低用户的网络费用（例如Gas成本）。

简单地说，在FSS中，事务通过DON传递，而不是直接传到目标智能合约。DON下单交易，然后将它们转发给合约。

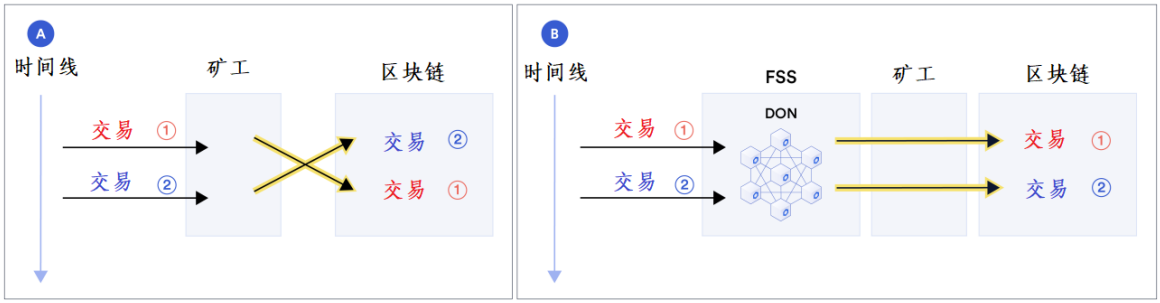


图 6:FSS 受益的示例

图A是矿工利用其中心化的处理交易的能力来交换两个交易：交易1在交易2之前到达，而矿工却对齐交易顺序颠倒。图B展示出DON如何在DON节点之间分权式排序过程。如果诚实节点的仲裁在2之前接收到1，FSS会在链上使交易1出现在交易2之前，其方式是通过附加合约可执行的序列号来防止矿工重新排序。

可信执行环境TEE

可信执行环境（Trust Execution Environment, TEE）是应用程序的独立的执行环境，通常具有特殊用途的硬件支持。TEE的使命在于提供强大的安全特性，如机密性和应用程序完整性，即软件的抗篡改性。TEE是一项工业界和学术界都在火热进行的研究工作，它会产生非常巨大的行业影响

一些TEE可以产生证明，即一个特定的程序对特定的输入正确地计算输出。一种基于TEE的TEF同步变体可以通过将（zk-）rollups汇总中的证明或有效性替换为TEE认证来实现。

相比于用于Rollups和Validum的零知识证明，TEEs的性能要好得多。与门限签名相比，TEE消除了生成门限ECDSA签名的复杂性，因为原则上只需要一个TEE。然而，使用TEE会引入额外的依赖于硬件的信任假设。您还可以将TEE与阈值签名结合起来，以创建防止部分TEE实例泄漏的容错性，尽管这种保护措施重新引入了生成阈值ECDSA签名的复杂性。

更强大的灵活性：这些同步选项可以通过以下方式进行改进，以提供更大的灵活性。

灵活触发：TEF应用程序可以确定同步触发的条件。例如，同步可以是基于批处理的，例如，在每N个事务之后发生，基于时间的，例如，每10个块发生，或者基于事件的，例如，在目标资产价格发生显著变化时发生。

- 部分同步：在某些情况下（例如，使用Rollup，部分同步可以减少延迟），$\mathbf{exec}_t$可以提供少量状态的快速同步，可能只定期执行完全同步。例如，$\mathbf{exec}_t$可以通过在SC_a中更新用户的余额来批准取款请求，而无需更新主链的状态。

像Intel SGX和Keystone这样的TEE允许应用程序在被称为enclave的受保护环境中执行，原则上这样可以保护它们的完整性和机密性。设计TEE是为了实现一个强大的、非常通用的功能，它甚至包括强大的加密原语，如虚拟黑匣子混淆，但事实证明，仅使用密码学是无法实现的。

TEE是是Town cryer的基础，它将在区块链系统中发挥越来越重要的作用， 出于对TEE安全性的担忧，其目前没有被大规模采用。

TEE安全性讨论：

最近针对英特尔SGX（唯一具有认证能力的商品TEE）的攻击，使人们对TEE在实践中的安全性产生了怀疑。

缓解措施有：以认识到其潜在的危害的方式去部署TEE。

一种是使用它们进行深度防御，也就是加固系统。Town cryer可以这样看：值得信赖的OM使用者应该为用户提供保密性和完整性，但Town cryer的使用加强了这种保证。类似地，TEE可以以不依赖于完美安全性的方式部署。例如，密封玻璃证明算法可以使用TEE来保证完整性，而不是保密性（尽管最近的侧通道攻击会损害这两者）。

最后，可以设计具有前向安全性的基于TEE的协议，这样的话，如果已知有中断（1）用户可以避免使用TEE；（2）中断不会回溯性地影响以前的协议调用。这种方法将极大地限制对手利用TEE漏洞的机会窗口。

比如说，在TEE控制用户资金的协议中，用户可以将这些资金转移到专门用于TEE临时使用的地址中。在TEE强制长期数据保密的协议中，频繁的键轮换将达到类似的目的。

又比如说，TEE可以用于实现机密定义的ConfSwitch适配器。TEE接收在公共密钥pk TEE(t)下加密的(q, switch)，其epoch t持续，例如一周，并生成输出s = switch(r)。然后，它会清除它处理过的所有数据。在每个新纪元的开始，它删除它的旧键，生成一个新键，并将其发布给BC或者主链。（这样的发布可以通过账本上带有每个纪元启动器的可执行文件来实现。）另外，用户可以在任何时候通过协议中止。

当然，用户在这个模型中可能遭受零日攻击，即未发布的攻击。但是，使用零日攻击是有代价的，即通过发布补丁而暴露和失效的风险。