互链网：一种新的系统结构和应用构建方法

蔡维德

前言

本文是笔者在2020年8月6号在伦敦国际学术会议的演讲，参会的国家包括英国、美国、德国、日本和中国等。演讲用英文，题目是ChainNet: A New Approach for Structuring System Architecture and Applications。这里将英文演讲稿翻译成中文。

这次研究提到互链网是下一代互联网，改变网络、操作系统、数据库以及一些新型具体设计方案。这些具体实施方案如果成为标准，将彻底改变现在的互联网。而这些改变是因为金融数字化，特别是数字货币出现，2019年6月震撼世界，一个新型科技竞赛开始。

1.百年没有遇到的大变革

我们正在经历一个百年来所没有遇到一次大变革，而这次大变革是三个改革同时间发生，第一个是金融或者是货币改革，第二个是法律科技的改革，第三个是计算机系统与通讯的一次大改革。

在计算机界，过去每几年就有一次变革，但是过了几年后，又有新变革出来取代刚刚提出的变革。但是这次却是不同，因为这次各国，是3个改革一起发生。英国首席科学家顾问，在2016年1月出了一个报告《超越区块链的分布式账本技术》(Distributed Ledger

Technology: Beyond Block Chain)，认为区块链技术是一个改革。在不到90页的报告，居然有十几页都提到“改革”(revolution)这名词，代表英国政府最高级的科学顾问的强烈观点。而在前一年，2015年1月，美国华尔街日报认为区块链是500年来最大的一次金融科技大改革。主要原因是区块链是从1494年来第一次记账法的改革。1494年西欧文艺复兴时代，复式记账法出现，使经济复兴伴随这文艺复兴出现。中国大历史学者黄仁宇在提到就是这复式记账法使西方领先中国，在《万历15年》书中认为中国由于没有使用这样的数字化的记账法，使中国整体落后西方。

而这复式记账法经历了500都没有变过，但是整个世界包括每个国家、公司、社区都在使用复式记账法，也是这记账法建立了现代经济体系。但是在2008年出现一次账本改革。这些原因是许多人认为区块链是一次百年来难得的一次大变革。英国央行也说这次是英国央行320年最大的一次货币改革（英国央行在1694年成立）。如今这些改革还在进行中需要许多年才能消化。

2.金融和货币大改革

金融与货币的大改革事实上是从2019年6月18日开始，在这之前许多人对区块链的概念就是一些黑客玩的技术，在市场的份额很小，而且对实际的经济没有影响。虽然在2017-2018年已经造成市场非常大的震撼，但是真正的震撼是在2019年6月18日才开始的。在当天，世界没有任何特异经济的事件，例如贸易战争、升利息或是降利息，没

有任何市场或是金融消息，只是一个商家发布技术白皮书。但是在任何一天，可能就有成千上万的技术白皮书出来，为什么这个白皮书却震撼全世界？世界许多央行几乎立刻公开批评，企图阻止脸书完成这项目，但这也表示这项目会改变现在金融市场和经济体系。这是传统经济学理论不能解释的现象，因为当天没有任何实质经济活动的改变出现，但是世界却改变了。脸书白皮书的项目还没有完成，也没有部署，技术还有问题，也没有通过监管单位的批准，根本还不可能实施，世界却震动了。那个经典经济学理论可以解释这现象？

但是事情还没有结束。2个月后，2019年8月23日英国央行行长在美联储面前演讲，认为可以使用合成霸权的数字货币（Synthetic Hegemony Digital Currency）取代美元作为世界储备货币，这件事情引起了美国巨大关注，过了3个月后，美国正式回应，表示这是一个新型的货币战争（Currency war）。这也不是教科书上的经典货币战争，而是新型货币战争，一个以科技、市场和监管来从事的货币战争，而传统货币战争却以货币价值和发行量来竞争。可以看到连货币战争的方式也改变。

2019年11月，美国学者也公开承认科技改变金融。这一直是一些金融界、经济学者不同意的观点，他们认为金融就是金融，科技只是服务金融，而没有改变金融，包括2019年6月的Libra都没有改变金融。但是2019年8月23号前英国央行行长在美联储的演讲后，美国学者改变了态度。2020年7月美国一著名经济学者对笔者表示数字货币的影响远远超过他们原来的预期，居然连美国最重要的资产（美元）都被

挑战到，而这是美国绝对不可以容许发生的。

这个在于货币和金融方面有几个重要新理论出现，第一个是国际货币基金组织（International Monetary Fund， IMF）的数字货币(The Raise of Digital Money) 理论。这篇报告引起了很大的讨论，因为这篇报告认为现在的商业银行在将来数字货币时代会有重大的影响，而且“合成数字货币”（由央行支持和监管，而由科技公司出台的数字货币）可以挑战法币。而英国央行行长就是在2019年8月23号提出以合成数字货币来取代美元成为世界储备货币的理论。而美联储在2020年6月也出研究报告，以数学博弈论分析，也得出的同样的结论，就是也是商业银行以后会有困难。等于证实国际货币基金组织在2019年的理论正确。世界2大金融机构现在都认为以后金融市场结构会改变了。当然这些在2019年6月以前，很少人会相信这理论。

第二个理论是普林斯顿大学Brunnermeier教授提出来的“数字货币区”(Digital Currency Areas) 理论。他认为以后世界金融中心不再是银行，而且数字货币平台。他还认为数字货币是因为互联网连接所产生的新型货币，但是由于国家之间的竞争以至于数字货币在世界分区域,造成世界新货币竞争，所以叫“数字货币区”。英国央行行长也是根据这理论，提出世界数字货币分区，不同数字货币在世界不同地区运行。而美国在2019年11月也回应，表示世界数字货币的确应该分区治理。在2019年，这理论很快得到欧洲央行和美联储的支持，许多公开演讲都在讨论这理论可能带来的影响。

这两个理论只是现在的货币改革重要的指标，所以区块链在货币

及金融方面是有一个巨大的改变。

联合国在2019年年底，将区块链列为最重要的金融科技技术。在2019年6月以前，许多金融科技报告上，区块链都不列名。2019年6月的确是金融历史上重要的分水岭。

3.法律科技的改革

英国法律协会在2018年就提出考虑将智能合约和区块链放入英国的法律制度里面，这是世界第一个以智能合约以及区块链作为法律根据的国家。同时间ISDA(International Swaps and Derivatives Association)这样的国际金融标准组织在疫情之前，差不多每个月发布一个智能合约标准，而ISDA所出的智能合约标准都没有代码，都只在法律上面的考虑。有人说不明白智能合约和法律的关系，读读ISDA的标准就明白，上面没有任何代码，但却是智能合约标准。

包括美国监管单位CFTC(Commodity Futures Trading Commission)和英国央行都纷纷提出使用智能合约来监管，这些都是巨大的改变，

人类第一次考虑使用非自然语言（计算机语言）来立法，司法，和执法。这影响还不太吗？

4.计算机科技的改革

这三个改革也是这篇文章的主体，就是区块链带来在计算机以及通讯互联网的改变。这也是一个巨大改变。

以前许多人都认为计算机不需要改，因为现在计算机早可以运行

区块链，例如区块链可以运行在云系统上成为“区块链服务”（Blockchain-as-a-Service，BaaS）。但是这些只是暂时的方案，而且在这里区块链只是应用不是基础设施。

4.1 区块链改变计算机体系结构

现在的互联网以及计算机科技已经走到了尽头，不是说科技不能进步，事实上科技还有可以很大的进步空间，可以有非常长远的进步。可是进步的方向需要更改，以前都是以功能和性能来决定，比如说我现在的手中的手机（现在价值几千人民币）在50年前就是超级计算机（当时价值千万美元）。50年前就有人这样预测，但是当时大多数人都不相信这会成真，但是这预测确实发生了。

现在一个人手机上面的内存都比以前一整个城市或者一整个大学所有的存储容量，包括所有硬盘的容量都还要大，所以说这方面已经有非常大的进步。可是现在计算机的问题一直还再出现，这问题是现在有太多虚假的事情，隐私保护不好。

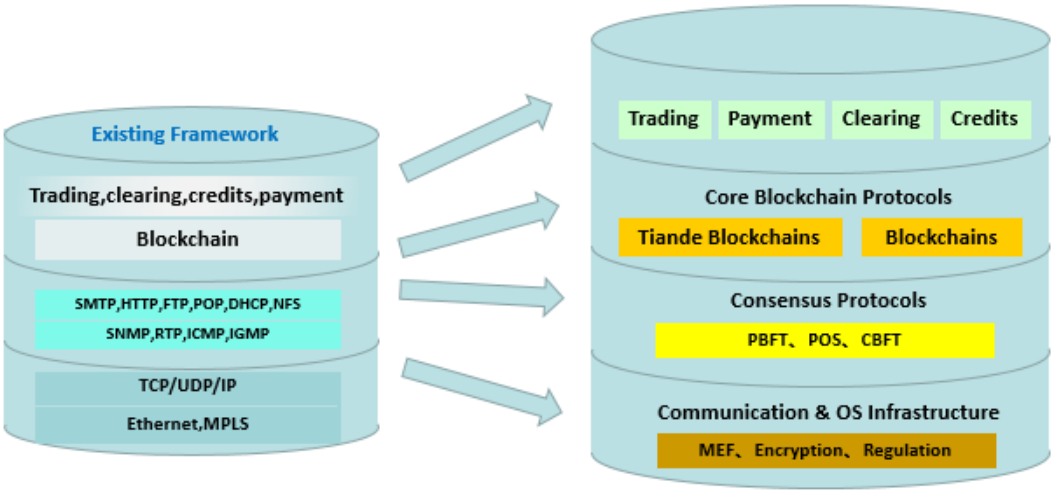
而现在越来越多的应用，包括央行数字货币（Central Bank Digital Currency, CBDC），以及稳定币等都会在互联网上面或者是区块链上面作业，但是现在的互联网上不支持区块链作业，现在的互联网和服务器在安全性上都是非常落伍的，没有把安全保护隐私当做重点，以至于现在的系统设计都以功能和性能为主，隐私保护和安全上非常差。

这观点不是我们独有的。美国的一个科技预言家George Gilder，

他在2018年的时写了一本书《谷歌以后的生活》(Life after Google)，他讲到整个计算机界的科技方向要彻底改变。他被认为是预言家是因为他在苹果手机还没有出来15年前，就预测智能手机的出现（当时他使用“通讯计算机”这名词来表示智能手机）。据说乔布斯（Steve Jobs）读了他的书后，才开始开发苹果手机。上次智能手机的预测可以说是世纪大预言，而他这次预测互联网要彻底改变。这次会不会一样成真？

Gilder提出的互联网新10大定律，推翻以谷歌为代表的传统思想

但是他提改变还多留在应用层上面，而我们提出的互链网这个概念，不止是在应用上面改变，而且认为在通讯协议上面，在操作系统上，在数据库上，还有在应用方面上，还有监控方面都改变，而这些就是我们现在提的互链网（ChainNet）的革命。



整个互联网都改变成为互链网

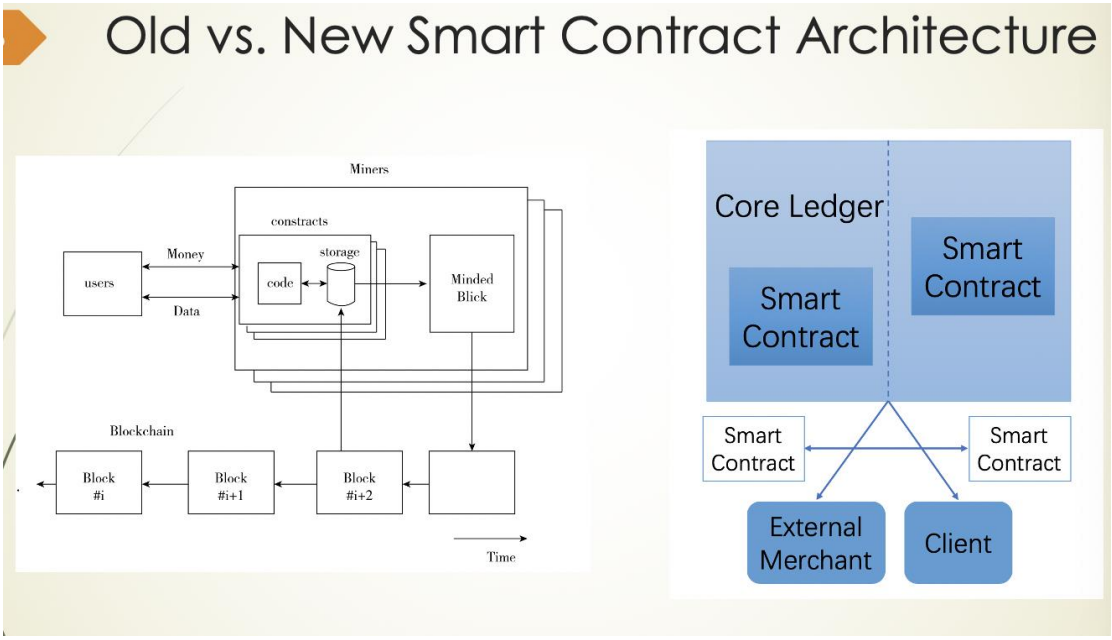
以后的数据中心就不是数据中心而是“数链中心”，以后的互联网就不再是互联网而是“互链网”，以后的物联网也不再是物联网而是“物链网”。

整个的系统架构就是从无论是底层的通讯协议、操作系统还有各方面都会有巨大的改变，这是一种整体性的改变，而且现在要部署一个区块链，快的话是几个钟头，慢的话需要半年，因为有一些区块链系统是很难部署。可是以后这个互链网进来的时候，部署一个区块链可能只需要几分钟，因为基础平台都已经建立起来了。

4.2. 新型智能合约架构不同

许多人每次想到智能合约就想到以太坊这样的智能合约架构，好像是上天给的，不能够改变的。事实上根据我们的研究，智能合约系

统架构可以不一样。例如英国央行在2020年3月出的《央行数字货币讨论报告》(Discussion Paper on Central Bank Digital Currency)，就提出3个问题，我们根据这3个问题把它系统架构画出来，就出现一个全新的智能合约架构。智能合约平台跟区块链不再是1对1的绑定，而是多对多的绑定。这样多对多的智能合约架构允许新型应用出现。另外，还会有许多其他新型智能合约架构出现。



新旧不同智能合约架构（左边是旧的，右边是新的）

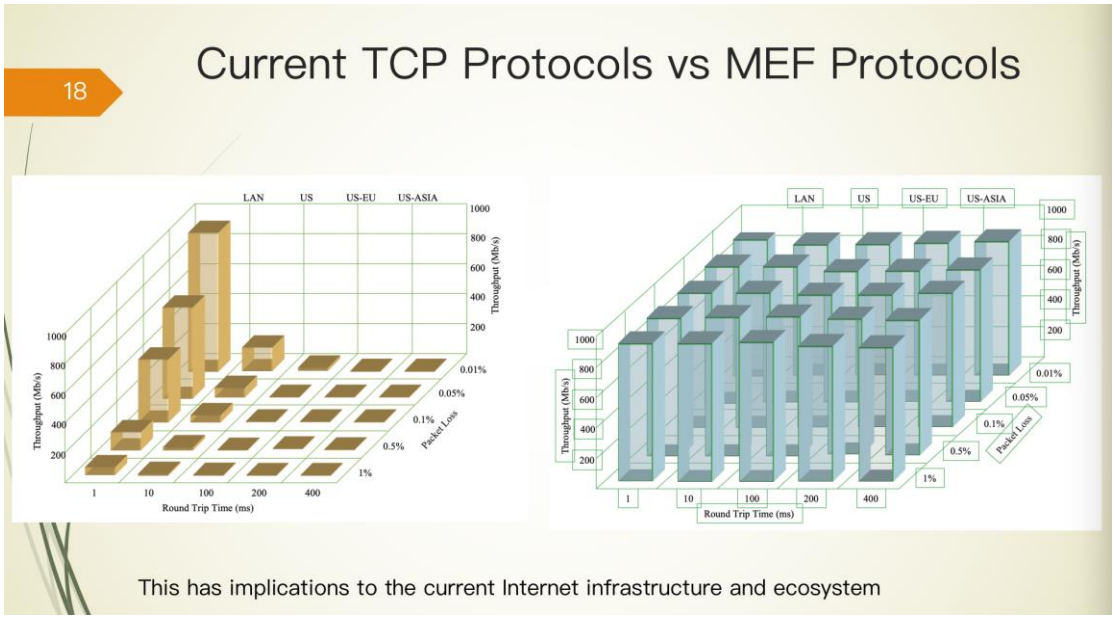
在这样新智能合约架构上，智能合约合约的协议和区块链的设计就会不同。这也会产生许多智能合约产业，这是皋陶模型。

2020 年 8 月 3 号世界银行（World Bank）发布金融科技工作报告（FinTech Note）《智能合约技术和普惠金融》(Smart Contract Technology and Financial Inclusion)，认为智能合约可以助力普

惠金融、供应链金融和保险业务。并且推荐政策制定尽快建立智能合约标准，降低金融风险。

4.3. 网络协议可以改进

现在互联网网络协议已经使用46年了，而基本协议还是一样。在互联网时代，每几年技术就会翻新。但是现在协议居然已经有46年的历史。而且现在的协议性能和延迟相关。由于这特性，网络一些特殊生态出现。例如在纽约交易所旁边，挤满了证券商，因为他们需要争取几毫秒的通讯优势，如果公司离交易所远，系统性能降低，如果离的很远，性能差距大。这不是物理现象，而是协议没有优化的现象。我们已经开发出网络协议MEF，如下图右下方。在新协议下，传统网络生态就会有改变 [1]。

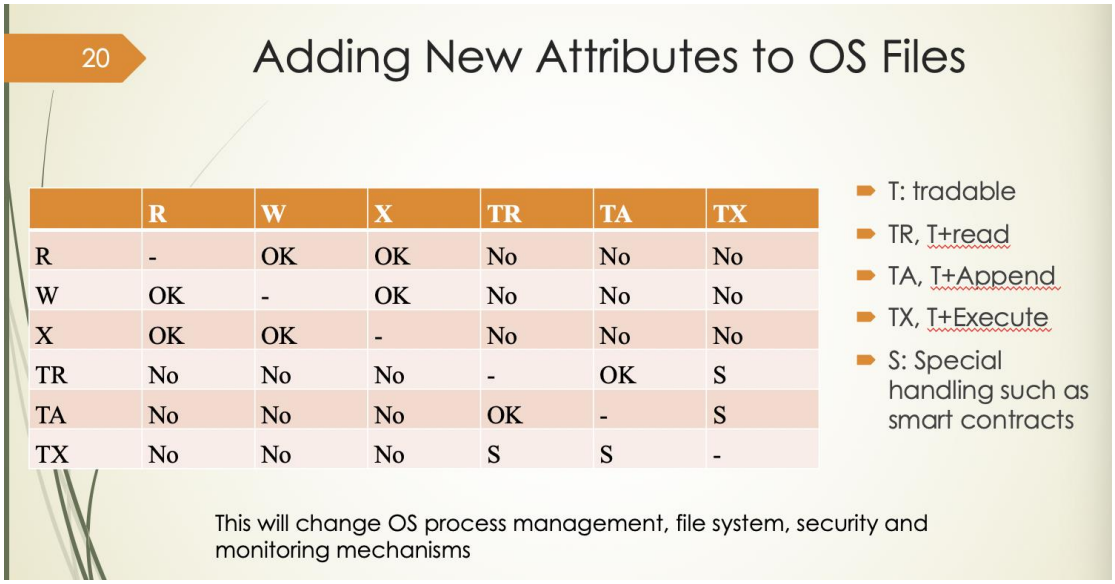


新型协议不受延迟影响，改变网络生态

4.4. 操作系统文件系统属性更新

操作系统也会改变，我们提出基于区块链的操作系统 [1]，例如在文件系统，和进程管理上和传统系统不一样。

一个文件除了传统读（R）、写(W)、执行（X）属性外，还有T属性，就是交易（Trade）属性。表示这数据可以参与交易。一个数据有T属性后，还有TR（读， Read）T读属性，TA（加，Append）就是T添加属性；还有TX（执行，Execute）T执行属性，多了三种不同属性，这三种不同属性表示有一组数据是跟金融相关，既然是跟金融有关系，就需要监管。但是由于区块链的关系，可以T读、T添加、T执行，但是不能有TW属性，因为数据只能加而不能改。



	R	W	X	TR	TA	TX
R	-	OK	OK	No	No	No
W	OK	-	OK	No	No	No
X	OK	OK	-	No	No	No
TR	No	No	No	-	OK	S
TA	No	No	No	OK	-	S
TX	No	No	No	S	S	-

操作系统文件系统新属性，监管可以在底层系统执行

有了这些新属性，操作系统才能判断使用何种软件来执行。任何T属性的数据，都需要有监管机制的软件。以后的操作系统对于金融数

据都有监管机制。

操作数据库系统

这个系统有这个标志的时候，整个的操作系统就可以执行监管，有一些数据是属于T属性的，表示可以做金融交易，因为是监管交易，任何交易数据需要追踪。T属性的文件处理方面在进程处理(Process Management)方面也不同，只有特殊软件可以接触T属性的数据，例如特殊智能合约可以。

而且因为需要监管金融交易，而金融交易需要账本，而账本就是数据库。因此我们提出操作数据库系统，如果操作系统需要管理这个监管交易，必须监管帐本，而帐本是需要数据库(Operating DB System, ODBS)。这样整个操作系统不再是传统的纯操作系统（而不包括数据库），而是操作数据库系统。

以这样从操作系统架构来看，传统上的操作系统架构被改变了，我们看操作系统的历史，从早期的Multics系统，到后来UNIX系统，到后来的Linux系统，到后来的IOS手机系统和安卓(Android)手机系统 ，还有云计算操作系统，我们可以看到一件事情，他们的功能越来越多，可是他们的系统架构都没有很大的差距。基本上都是属于在加功能，在性能上进步，系统管理的体积越来越大，管理的资源越来越多，可是在结构上，系统设计方面并没有很大突破。但是添加了区块链后，就不一样，因为将来操作系统需要监管金融交易数据。这原因出于数字代币的出现，大多数数字代币都在逃避监管，而许多国家

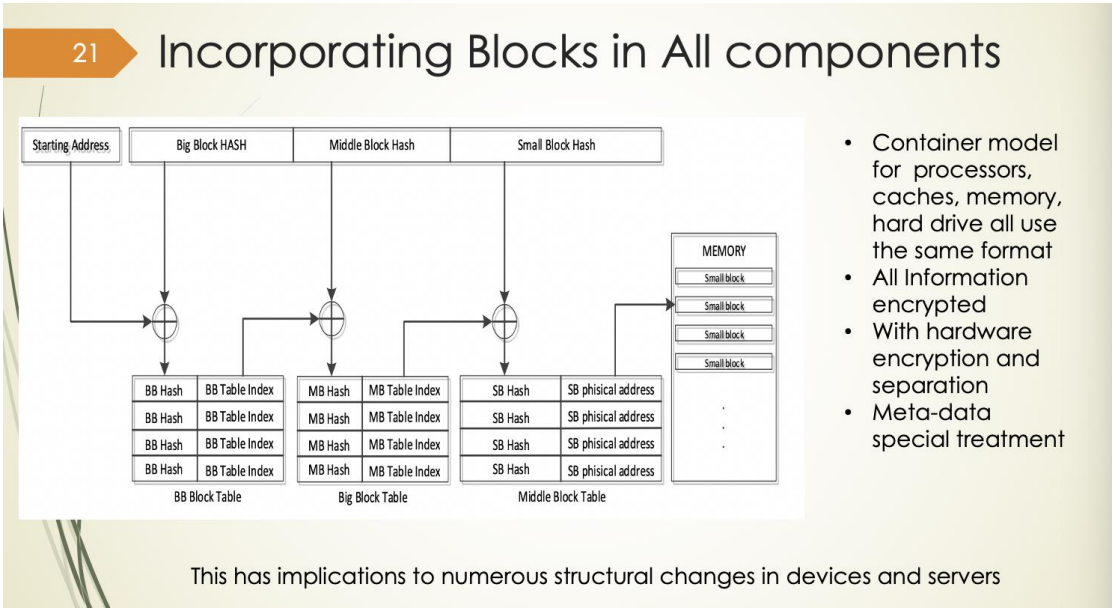
都无法监管，也没有办法将这软件移除，只能采取间接监管机制（例如封锁银行，不然银行和数字代币交易所有来往）。但是如果有新型操作系统，在这新操作系统上，这些数字代币应用就不能执行。

4.5.地址机制不同，打通内存、硬盘、存储、进程机制

而操作系统内部的地址管理(Addressing mechanism)也不同了。以前数据都是单独存在，操作系统里面的段机制（segmentation）和页机制 (paging)都是传统机制。而其物理意义有限。但是区块链数据是以块出现，有深厚的物理意义：

- 时间：块中交易是同时间被验证的，还有时间戳；
- 验证者：块中交易是被同一群验证系统验证的，而且有他们的数字签名担保；
- 共识：块中数据是被共识后才能被系统接受;
- 加密：块中数据可以加密，保护隐私。

所以这样的数据就应该放在一起，不论在内存，硬盘，手机，服务器（包括云服务器），在计算或是通讯上，都一起处理的。我们提出统一“块管理”体系，将数据分为大块，中块，小块。还还可以有大大块，大大大块，或是更多的“大”，操作系统也以“块”为基本处理单位，而不再以独立数据为单位。



新型操作系统处理金融数据以“大快，中块，小块”统一管理

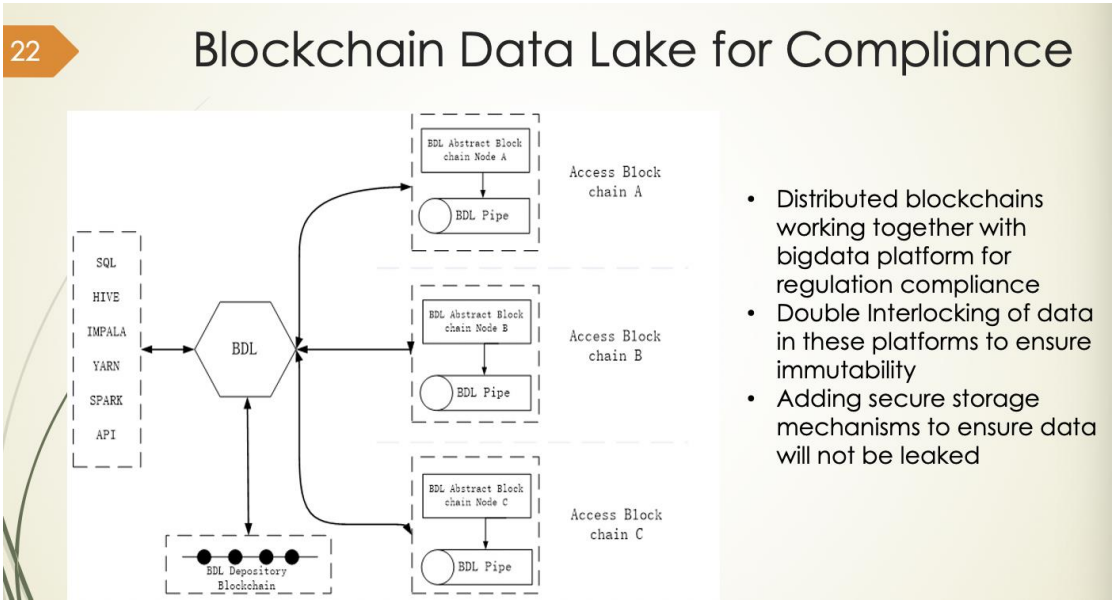
块管理国际标准化，打通金融、手机、服务器、存储产业

这样的统一“块管理”可以国际标准化，打通世界手机、服务器、存储、数链中心（新一代新数据中心），还有金融产业（包括银行、征信中心、交易所）。这样标准可以像船运集装箱运输一样，打通船运、物流、仓库的通道。这样的块管理还可以和现代容器技术（Docker）融合，这样的机制对世界供应链金融提供一个科学的基础设施，而不是在不安全的互联网上运行。

例如块大小、内容、格式、处理流程都可以国际标准化，这样可以由不同公司出产的硬件或是软件来并行加速处理，而保护机制有加解密处理。这样世界监管单位就可以快速合作处理金融交易，进行反洗钱活动的分析。

4.6. 区块链数据湖（Blockchain Data Lake）打通区块链孤岛

区块链是参与这都可以有共识，而因为监管单位可以参与共识，可以监管这链。但是现在洗钱的机制越来越聪明，也越来越复杂，违法组织可以在不同区块链上从事串联的欺诈事件。这需要监管单位需要同时间监管多个交易链。这就是我们提出区块链数据湖的概念，由一个中心处理监管计算，在上面可以有人工智能和大数据分析，但是数据来自每个区块链。但是这个中心和参与区块链，还有数据互相锁定（Double interlocking）的机制—就是大数据平台和区块链互相锁定数据,保证数据不能被更改 [1]。下图是我们提的区块链数据湖系统。



区块链数据湖连接多区块链系统与大数据平台

这样的机制代表基于区块链的系统，除了有“块管理”机制，还有传统大数据平台分析。块将同时间发生的数据绑在，在系统里面一起处理，而且有数字身份证，可以来验证数据真实性、时间信息、和

负责单位；但是大数据平台将块里面数据拆开重组，分析数据之间的关系，做反洗钱分析。而两组数据又可以互通，又都存在多个相关区块链上，数据也不能更改。一个基于区块链的监管网络系统就可以建立起来。不论在合规市场，或是地下市场，都可以监管到。在地下市场，由于4.4节里面的机制，任何交易（包括数字货币或是传统金融交易）数据都会自动报告，而且只有经过审批和验证的软件才能处理这些交易数据。

引用

[1] 蔡维德，《互链网:未来世界连接方式》，东方出版社，2020年9月。

[2]蔡维德，《智能合约：重构社会契约》，法律出版社，2020年9月。