互链网白皮书

Internet of Blockchain（IoB）Whitepaper

蔡维德

联合发布单位

协会及联盟

中国移动通信联合会互链网分会

中国广播电视联合会广电研发委员会

中国软件行业协会区块链分会

中国区块链生态联盟

全国高校人工智能与大数据创新联盟

中国亚洲经济发展协会区块链产业专业委员会

北京互联网金融协会区块链专委会

中关村天使投资联盟区块链应用专委会(盗火者)

天津市区块链技术与应用协会(筹)

科研

中国信息界区块链研究院

北京航空航天大学数字社会与区块链实验室

清华大学信息技术研究院

国家大数据(贵州)综合试验区区块链互联网实验室

江苏自动化研究所

山东省互联网金融工程技术研究中心区块链与数字经济研究所

赛迪(青岛)区块链研究院

天民(青岛)国际沙盒研究院

南京中诚区块链研究院

国家科技部重大专项现代服务可信交易项目组(2018YFB1402700)

企业

北京天德科技有限公司

北京金融安全产业园

东湖数字小镇

北京天德博源科技有限公司

深圳幂度信息科技有限公司

北京丰原国际科技有限公司

国蓝科技有限公司

泓德(天津)区块链科技有限公司

福建链众区块链科技有限公司

宁波和鑫链数字科技有限公司

华链(宁波)科技有限公司

浙江沛美科技有限公司

苏州天证区块链科技有限公司

智库媒体

链塔智库

互链脉搏

2020 年 3 月 27 日

1. 区块链进入世界金融界

区块链技术已经获得了广泛关注，虽然区块链基础技术已经发展多年，但让区块链引起世界关注是应用区块链技术的比特币。虽然最初区块链与比特币和以太坊等加密货币有关，但后来是英格兰银行推动数字法币（CBDC，Central Bank issued Digital Currency,中央银行发行的数字货币）的发展，最终 Facebook 的 Libra 和其他稳定币项目震撼了世界各国央行和商业银行世界。Libra 白皮书发布后，包括美联储（Federal Reserve）和中国人民银行（PBOC）在内的许多央行都启动了 CBDC 项目。

摩根大通（J.P.Morgan）、维萨（VISA）、万事达（Mastercard）、DTCC、斯威夫特（SWIFT）等大型金融公司早在脸书（Facebook）的 Libra 之前就开始了自己的稳定币项目。国际货币基金组织（IMF, International Monetary Fund）、世界银行、国际清算银行（BIS, Bank for International Settlement）等主要国际组织都开展了自己的研究，并就相关课题发表了重要的研究论文。

这些项目改变了金融世界。中国政府于 2019 年 10 月 24 日发布指令，鼓励中国机构开展和研究区块链项目，中国人民银行也表示近期将发行数字人民币。

英国央行和其他央行也进行了研究，研究结果表明未来的金融基础设施将基于区块链技术进行研发。例如，英格兰银行(Bank of England,英国央行)在 2016 年和 2017 年发布了实时全额结算（RTGS, Real-Time Gross Settlement）的蓝图，并与加拿大银行和新加坡金融管理局（Monetary Authority of Singapore）一起发布了一个可以支持 7*24 服务的跨境支付系统。

现在几乎所有金融系统包括 CSD（Central Security Depository 中央证券投管系统），支付系统，清算系统都可以使用区块链解决。例如基于区块链的支付系统在 2008 年就出现，基于区块链的商品交易清算在中国 2017 年也实验成功。

加拿大央行以及欧洲央行（ECB, European Central Bank）、日本央行等其他央行对各种区块链项目进行了广泛的实验，他们都使用金融市场基础设施原则（PFMI, Principles of Financial Market Infrastructure 金融市场基础设施原则）来评估这些项目。

这些项目为下一代受监管区块链的发展带来了重大的新曙光。与此同时，美国证券交易委员会（SEC）、美国商品期货交易委员会（CFTC）等监管机构开始了对加密货币的监管，甚至中国也从上海开始对区块链项目进行了重大的监管审查，换言之，在政府鼓励区块链项目发展的同时，也开始对区块链项目和相关企业实施监管。

随着各国央行和商业银行开始自己的稳定币项目，许多问题随之提出：

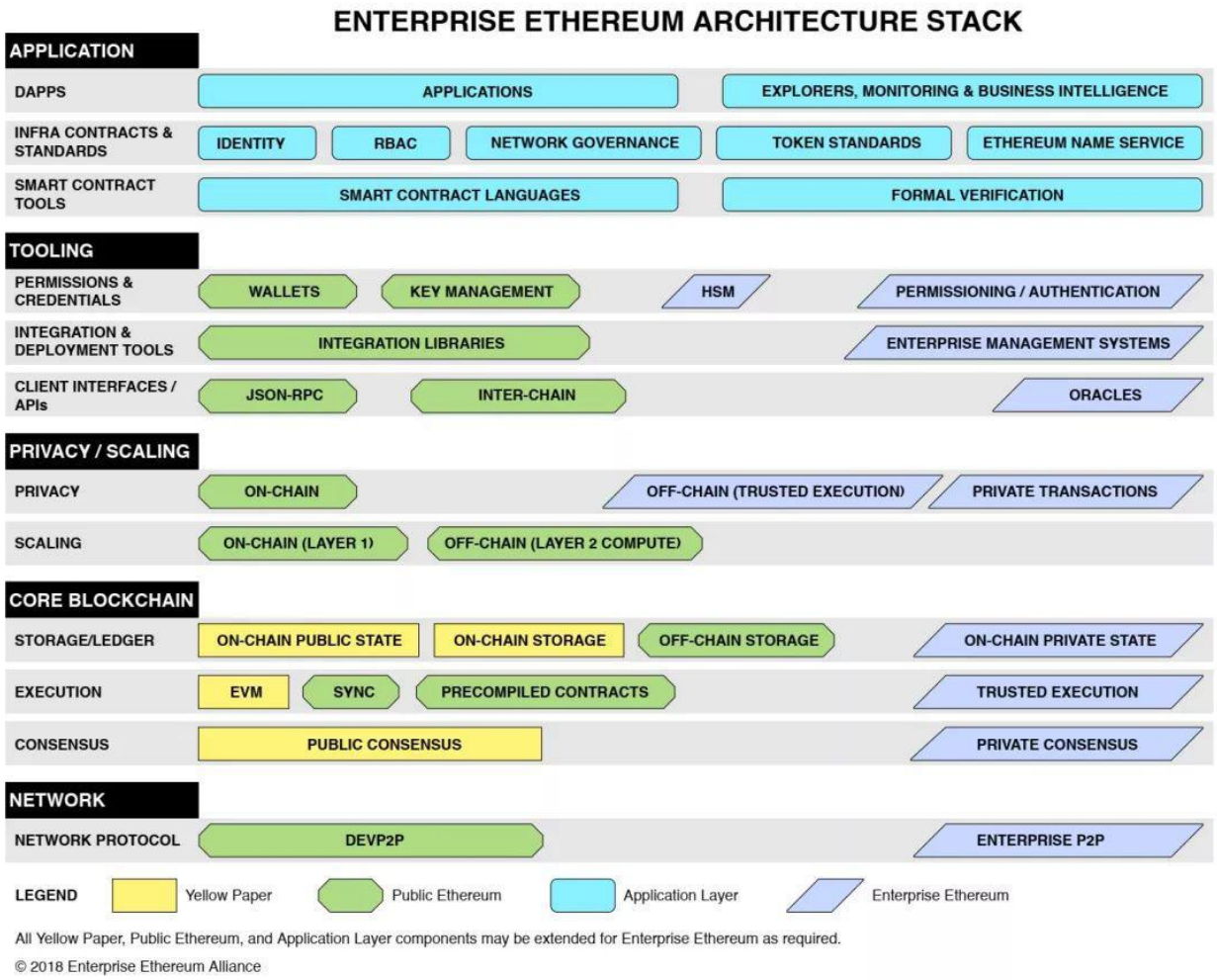
- 对于这些受监管的区块链项目，区块链架构和设计应该是什么？这些新区块链项目的一个关键特征是，它们将受到监管，并支持各种合规检查。
- 这些区块链项目的基础设施是什么？
- 这些区块链项目及其基础设施需要什么？

2. 区块链是下一代互联网

区块链是下一代互联网这一思想在 2015 年前就有了。 例如以太坊就认为他们的系统是网络操作系统，后来 IBM 也认为超级账本是网络操作系统。2016-2017 年出现机构区块链互联网模型（互链网），例如 Cosmos（宇宙）、Polkadot、 熊猫模型、金丝猴模型、卫星模型(日本 NEC 的 Satellite 系统)，后来又出现许多区块链模型，例如以太坊 2.0 都有类似概念。同时间许多跨链技术也出现，这些跨链技术(Inter-Chain technologies)，连接两个或是多个区块链系统，有的时候这些链有主副的关系（例如 Side Chain），有的是并行关系。

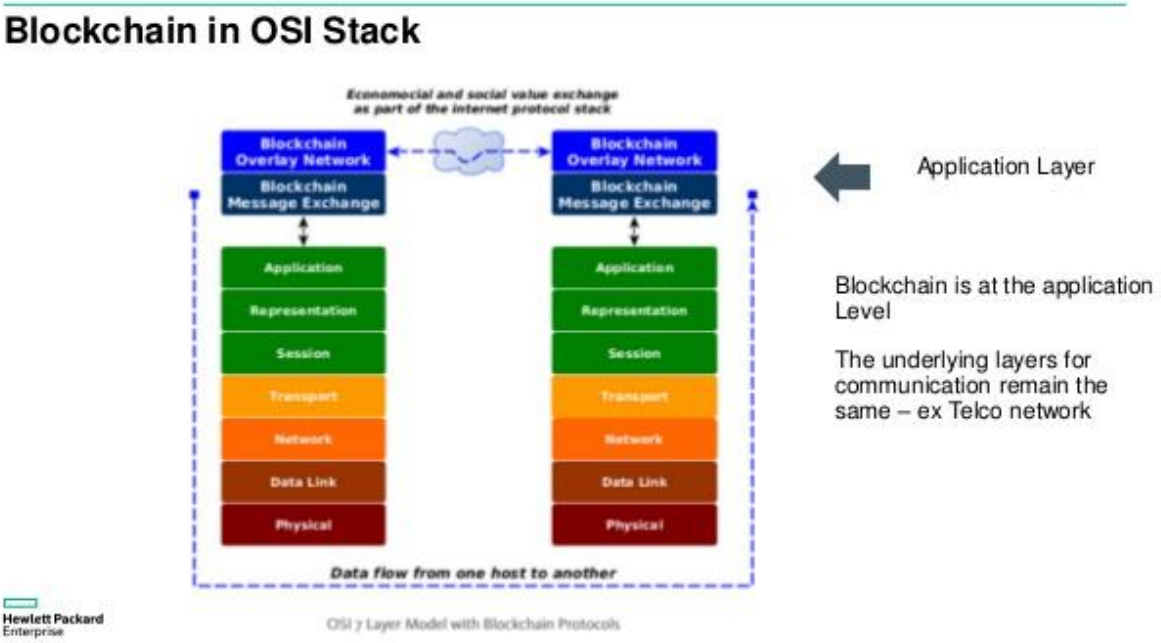
但是这些模型几乎都是建立在现在的互联网上，事实上这些“区块链互联网”或是网络操作系统还是应用，不是网络基础设施。例如比特币系统、以太坊系统、超级账本系统都是

这样。这些“区块链操作系统”概念和传统操作系统概念相反，传统操作系统是计算机底层技术，而区块链或是相关名词例如区块链互联网、传统区块链操作系统，都是运行在互联网和传统操作系统上的应用，而不是真实操作系统，也不是网络基础设施。



现在区块链技术软件，运行在互联网和传统操作系统上面，图片来自以太坊架构图

下图显示现在区块链软件完全运行在 OSI 网络标准上应用层，是最高的一层，代表现在区块链或是网络操作系统，都是应用而不是操作系统，也更不是网络。



传统区块链操作系统架构图，图片来自惠普公司

这样的区块链体系像在沙滩上盖大楼，因为现在互联网基础设施不够安全。网络攻击事件一直在发生，信息流失或是数据被恶意篡改都是经常发生的事件。隐私性也差，任何人只要有 IP 地址，就可以发电子邮件。

现在操作系统也不够安全，许多重要应用都硬化现有的操作系统来保护应用。例如许多国家的国防部都使用可信（硬化）操作系统。但是在商业界还是使用通用操作系统例如 Linux 系统。

所以几乎所有的区块链应用都运行在不够安全的操作系统和网络上。可是许多区块链应用都是和金融有关，为了安全许多银行还使用专网，而且建立一个完全封闭计算环境来保护银行系统，但是不是每个机构都可以提供这样的计算环境。以后会是链满天下，这问题会非常严重。

我们团队做过多次实验，发现如果需要区块链高速运行，90%服务器和网络都被区块链占用。这代表区块链应用只能使用 10%计算力，例如金融交易，回复客户的请求，进行智能合约计算。这表示现在服务器和网络不是为区块链设计的，而区块链最频繁的作业就是加解密和共识机制。

> 互链网设计原则 1：解决互链网的第一个原则，就是用硬件处理加解密功能，而且因为其他区块链的机制都需要使用加解密机制，所以这机制需要放在操作系统底层。

现在区块链系统就是个“小飞象”（Dumbo）模型，可以飞，但是高体重。这样模型以后必定有大风险会出问题，就像高楼建立在沙滩上，风来了，雨来了，必定倒塌。这情形如果不改进

> “所以凡听见我这话就去行的，好比一个聪明人，把房子盖在磐石上。雨淋，水冲，风吹，撞着那房子，房子总不倒塌，因为根基立在磐石上。凡听见我这话不去行的，好比一个无知的人，把房子盖在沙土上。雨淋，水冲，风吹，撞着那房子，房子就倒塌了，并且倒塌得很严重。”

3. 安全和保护隐私是互链网第一原则

在互链网上，安全和隐私是第一优先。在麻省理工学院在 2012 年已经提出以安全和隐私保护第一优先的计算平台，来建立数字社会（digital society）， 并且提出飞鹰身份证原则 Windhover Principle。最近还有其他类似新思想出来,例如 Sovrin Framework。2019 年，美国科技预言家吉尔德(George Gilder)发布文章推荐三个新型区块链设计特性：加密网络（crypto networks），安全(security)机制，和数字身份证(identity)。例如在节点里面使用硬件来保护系统，而且钱包也使用硬件。这系统没有挖矿机制，有高

速共识机制，用户拥有自己数据的所有权力，没有得到用户的允许，没有人或是单位可以看到这数据。

许多国家包括欧盟对隐私保护非常重视，欧盟为这还特别立法 GDPR （General Data Protection Regulation 通用数据保护条例），这表示欧盟对这方向不会轻易改变，将来还会继续加强力度。一个重要的隐私保护科技就是数字身份证。数字身份证需要新型保障机制，而且是客户拥有自己数据的控制权，不是系统，例如大数据平台,也不是服务供应商，例如谷歌拥有这控制权。系统和服务商只能提供服务，对这些隐私的数据没有其它权利。我们可以身份证的管理方式分类为：

- 中心化处理：这是现在大部分政府治理模型，由政府发证，老百姓使用政府发的证来注册、交易、上学、就医、公证。
- 联邦制处理：这是中心化的延伸，由一群组织来管理身份证，避免中心单位作弊，例如拿身份证信息领取在银行的资金。
- 用户管理：身份证由个人拥有，而不是由政府单位控制。Augmented Social Network 在 2000 年提出拥有身份证机制的下一代互联网。他们建议在互联网上建立一个永久的身份证系统 Identity Common。但是这种方式一直有技术难点，例如一个用户注册的时候，使用的当地系统就可能可以作弊，使这机制难管控。
- 用户自主管控：发现用户管理方式的问题后，Patrick Deegan 在 Open Mustard Seed 项目就提出自我主权身份证（Self-Sovereign Identity），也就是飞鹰身份证原则。

在数据保护方面，可以有的选择是：

- 不存关键数据：系统不存关键信息，例如私钥，这样设计可能是最安全的，因为系统没有数据需要保护，例如 Sorvin 项目就是采取这样设计。但是系统操作性就比较差，因为系统如果需要处理信息，每次都需要要求数字身份证，但是在请求协议中，也可能遭到攻击。

- 存储加密信息：在系统里面，关键信息都加密。这样系统安全性也高，因为系统自己也不知道信息。每次客户使用公钥来读、写、传送加密信息。为了要维持安全性，系统每隔一段时间需要换私钥。
- 系统存明文信息：这是传统做法，部分操作系统例如内核是可以相信的，只有内核可以出来保密信息，而且许多作业都由硬件处理，由硬件来保护。这是现在传统可信操作系统的设计。

互链网设计原则 2：为解决互链网安全问题，在操作系统关键信息只有 2 个选择：1）不存在操作系统里面，每次需要由安全协议取得；2）存在操作系统关键数据完全加密，由操作系统硬件和软件处理保护，因为数据加密，操作系统不知道信息内容。

在互链网设计上，能够使用硬件的地方尽量使用硬件。一是硬件执行速度快，二是硬件可以提供安全保护机制，三是硬件控制系统已经固化，很难更改，即使系统已经被攻击而影响到部分功能，但是由于重要组成系统使用硬件执行，系统仍然可以继续执行正确的指令，不会继续破坏其他部分的系统。

以处理器安全为核心的硬件安全技术竞相发展，应用广泛的主流技术包括虚拟化技术如 Intel VT (Virtualization Technology)与 AMD SVM(AMD Secure Virtual Machine)技术、基于可信平台模块(Trusted Platform Module，简称 TPM)的可信计算技术如 Intel TXT (Intel Trusted Execution Technology)、嵌入式平台 ARM TrustZone 安全扩展等。其中虚拟化技术基于特权软件 Hypervisor 对系统资源进行分配与监控，提升了资源利用率，但 Hypervisor 潜在的软件漏洞可能威胁到整个系统；基于 TPM 的可信架构在程序加载时进行完整性度量，却难以保障程序运行时的可信执行； TrustZone 为程序提供了两种隔离的执行环境，但需要硬件厂商的签名验证才能运行在安全执行环境。

2013 年，Intel 推出 SGX (Software Guard Extensions)指令集扩展，提供强制性硬件安全保障机制，不依赖于固件和软件的安全状态，并且提供用户空间的可信执行环境，通过

一组新的指令集扩展与访问控制机制，实现不同程序间的隔离运行，保障用户关键代码和数据的机密性与完整性不受恶意软件的破坏。不同于其他安全技术，SGX 的可信计算基(Trusted Computing Base，简称 TCB)仅包括硬件，避免了基于软件的 TCB 自身存在软件安全漏洞与威胁的缺陷，提升了系统安全保障。此外，SGX 保障运行时的可信执行环境，恶意代码无法访问与篡改其他程序运行时的保护内容，进一步增强了系统的安全性。基于指令集的扩展与独立的认证方式，使得应用程序可以灵活调用这一安全功能并进行验证。Intel 在其最新的第六代 CPU 中加入了对 SGX 的支持，因此不论是底层操作系统或是高层应用系统都可以使用这硬件安全保障机制，来隔离不同用户以及不同种类的数据。

4. 保护隐私和监管机制需要并存

正如互联网不是法外之地，区块链和互链网也不是法外之地。如果区块链只是一个应用，犯罪证据还是可以在政府监管之外。因为现在账户是存在应用层，不是在底层处理，如果应用层出事，这交易就没有记录。所有交易必须经过操作系统底层才能保证交易的完整性和合规性。

第一代（比特币）和第 2 代区块链（以太坊）的设计还是为了逃避监管。加拿大央行在 2017 年区块链实验报告指出，央行需要获得全部交易数据才能达到国家监管的需要。因为这些系统不可靠，而且难监管。

以后的区块链不但需要可以监管，而且还要主动支持监管[6]。这两思想不同：

- 可以监管代表系统设计完后，监管机制可以后来加上。逃避监管的链就是无法加上有效的监管机制，这是现在监管单位对数字代币遇到的困难。这些网络系统已经大量部署，而且在许多国家运行，运行时也不受任何国家管制。在这种情形下，只能用间接方式来监管，例如监管交易平台（例如使用 KYC 和 AML 机制），或是控制银行和交易所的管道；

- 支持监管的系统是在设计的时候，就将监管机制放进系统里面，保证相关交易都可以被监管到。这里我们提出将监管机制放进操作系统包括底层内核(kernel)，因为只有在操作系统，所有相关监管的交易都可以被追踪到，因为所有执行都必须通过操作系统。如果把监管机制放在应用层，例如“小飞象”模型这样的设计，监管机制可能不能到位。在这以前，所有监管机制都是放在系统应用层，例如在大数据平台上。

互链网设计原则 3：因为需要对所有交易监管，所有账户和交易信息作业需要在操作系统内执行，而且部分作业由硬件处理，保护隐私，并且增加速度。因为区块链是一个分布式数据系统，这样操作系统就可能成为“操作数据库系统”，不再只是操作系统。而传统数据库还是可以在操作系统上运行。只有和账户和交易相关作业在内核执行。这是“可监管操作系统”的设计原则。

有了这样的机制，所有交易可以监管。例如有笔交易在同一操作系统完成，操作系统会发现这个作业需要接触到账户信息，于是交易进程（transaction processes）和监管进程(regulation processes)就会被自动启动，而这两个进程，都是在操作系统，许多交易还由硬件控制，这样账户信息就可以被改变。在这里会有 3 个数据结构会更改信息：

- 用户账户数据：交易双方账户信息可以增加，但是旧数据不能被更改；
- 用户交易数据；交易信息可以增加，但是旧数据不能被更改；
- 监管数据：监管数据可以增加，但是旧数据不能被更改。

这种结构是为现代化金融交易平台设计的。现在的金融交易，账户信息和交易信息是分开存储和处理（以至于需要结算和清算两个流程）。但是在传统数字代币上，这两个数据结构是被绑在一起的，交易结算和清算一步到位，但是这会造成扩展性难，而且监管困难，因为结算的时候账户内的资金就已经转移。在熊猫区块链模型和英国 USC (Utility

Settlement Coins)平台设计上，账户信息和交易信息再次分开。这样交易需要两步才能到位，但是系统可以无限扩展，而且监管机制可以有多种机制来监管。在交易前可以确认资产的真实性以及合法性（例如不是洗钱），交易的时候可以保证没有作弊，交易后在清算前可以回滚和再度确认交易。传统反洗钱的机制也可以在这样的平台上进行。

我们的做法就是以系统架构来解决传统区块链难扩展和监管的问题，这和传统做法不同。账户信息可以用并行分片机制来扩展，交易信息可以用增加交易媒介来扩展，而因为交易需要两步才到位，监管机制可以强大许多。

操作系统如果发现在一笔交易上，一个用户使用可监管的账户，但是另外一个用户不使用可监管的账户，操作系统内核就会停止这笔交易，并且上传这次不合规交易的信息给监管单位。

互链网设计原则 4：操作系统负责追踪交易数据，保证交易合规，信息正确，交易信息会记录在区块链上。因为需要对所有交易监管，所有账户和交易信息作业都需要在操作系统内执行，而且部分作业是由硬件处理，可以保护隐私和增加速度。因为区块链是一个分布式数据系统，这样传统操作系统成为“操作数据库系统”(Operating Database Systems ODBS)，不再只是操作系统(Operating Systems)。而传统数据库还是可以在操作系统上运行。只有和账户和交易相关作业在“操作数据库系统”内运行。这是“可监管操作系统”的设计原则。

如果这次交易，是和另外一个账户在另外一个服务器，这两个服务器，将通过安全协议，有内核 A 和内核 B，内核 A 使用自己的身份证和内核 B 的身份证，通过检验，内核 A 保证来自 A 的信息是属于真实的； 同样内核 B 保证来自内核 B 的信息是真实的。双方也可以通过第三方认证后，才开始交易，而且交易也存在区块链上，保证安全，以后如果出事，作弊方可以很容易被查出来。

互链网设计原则 5：如果参与一笔交易来自不同服务器和操作系统，这两个操作系统需要通过安全协议，建立交互管道，并且各自保证信息真实。如果出错，出错方需要承担赔偿。

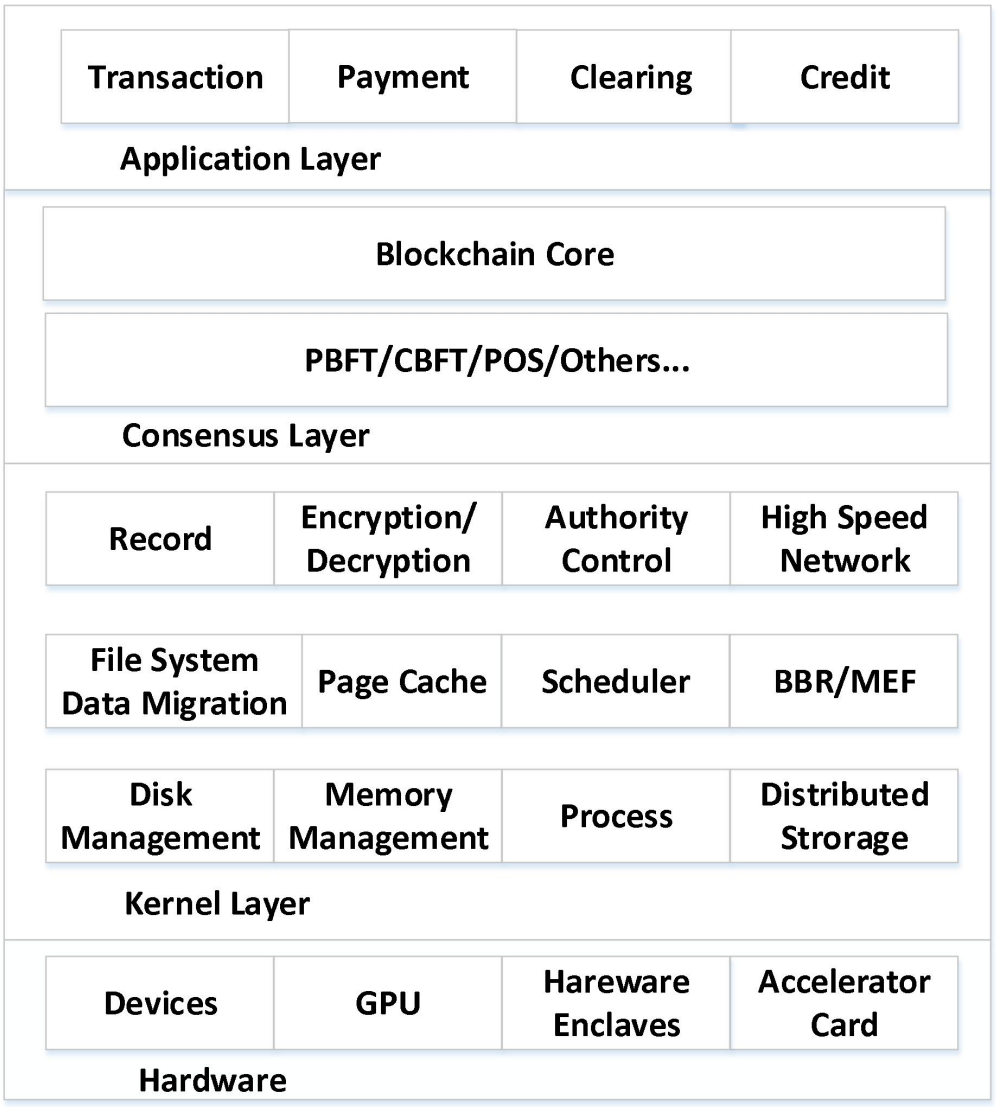
我们正在设计操作系统来支持区块链，但是这系统设计就需要使用区块链。如何进行？这其实是计算机常用的原则。例如 C 语言的翻译器就是用 C 语言写的，问题是哪里拿到第一个 C 翻译器？因为第一个操作系统使用的区块链可能是外来的。等到系统完成后，区块链系统也建立了，这系统就可以给内核使用，第一个外来区块链系统就不需要了。

5. 新型操作系统支持区块链作业

这种“操作数据库系统”和传统操作系统设计大不相同，计算机体系会有变化，而且需要长时间的开发才能做出。在不久的将来，我们需要先走出第一步，就是更新现在的操作系统。等这步完成后，再做第二步。

区块链提供两个重要服务：加解密和共识机制。现在我们已经讨论操作系统内核放加解密加速器，还有加监管数据库，还缺共识机制。各式各样的区块链使用不同共识机制，但是基本上都需要通讯和加解密，再来就是高速缓存机制和容错机制。这些都可以加入在最近内核的外层。

为什么这需要在最近内核的外层，因为大部分区块链应用都需要共识，而共识需要加解密。而通讯和缓存机制都是传统系统里面通用的组件，这里就不再讨论。整个新操作系统框架就出来了。



新型操作系统架构

新型操作系统架构是根据 Linux 版改进的。如果需要重新建立一个操作系统，这恐怕需要 3 年的时间，所以我们认为在现有操作系统上进行改造是目前最优方案。

目前我们已研发出具有自主知识产权的区块链操作系统一些关键技术，在 Linux 内核的基础上增加了一层共识层，该层主要由文件系统加解密，网络传输加解密以及共识协议等服务组成，为上层应用提供加解密和共识协议接口。

表1：传统系统与新型系统对比表

传统系统	新型系统
计算力为优先	安全隐私为优先
进程管理，I/O、文件系统为底层支持	传统底层加上区块链功能例如共识、加解密、监管机制
兼容各样传统系统	新系统不但自己兼容，也要兼容各样传统系统
不考虑金融监管机制	监管机制会是底层功能

6. 互链网网络模型

在应用层，互链网也需要链接许多各式各样的链，成为一个链网。单身链网需要什么原则？首先参与的链需要具备下面的特性：

- 高性能（High-performance）：高吞吐量，低延迟
- 安全和隐私性（Security and Privacy）
- 可扩展性（Scalability）
- 容错性(Fault-tolerance)

有参与链的通性，但是一个链网还需要下面的特性：

- 多链式架构（Multi-chain structure）：异构网络是由多条不同类型的并行的链所构成的；同质网络是由一群相同类型的并行的链所构成的。最大的不同是一个多链式架构，而不是一个单链式架构。
- 互通性（Interoperability）：在异构网络上，每一对不同的链都需要有互通的协议。假设，我们有 100 种链参加链网，则需要 100✕99÷2＝4950 种互通协议。可见这种互通性的协议需要大量的工作。

- 可延伸性（Extensibility）：链网可以无限延伸扩大。因为，一个链网可以像互联网一样，随时的、无限制的到处延伸，可以有几千、几亿、几兆的网络、网民参加。
- 可更改性（Modifiability）：在互联网上面，任何的机构和个人可以随时的加入、离开，但是整个互联网的架构并不改变。所以，链网也可以让任何机构或个人随时加入或离开，但是区块链架构不能改变，链网的架构也不能改变。
- 可复制性（Duplicability）：每个链可以很快的复制。如果链的复制很慢，链网需要很长的时间才能搭建起来，高可复制性可以迅速的搭建链网。
- 可管理性、非对称结构(Asymmetric structure)：链网必须具有可管理性。正因为管理机制的存在，链网具有非对称结构。有些节点或链会比其他的节点或链更加重要，并拥有非对称的信息，例如监管机构、域名服务商、控制节点等。
- 层次性(Hierarchical structure)：成为一个大型网络，链网必须具有层次性，高层次的链和节点具有不对称的权利。
- 一致性(Consistency)：每一条链都必须有自己的一致性，链与链之间也要有一致性的协议。
- 高可靠性(Integrity)：链网既然是一个价值网络，就必须具有高可靠性。
- 完备性(Integrity)：每一条链与每一条链的共识机制及消息的来源与可靠性是不一样的，因此不同的链的完备性是不一样的。低完备性的链不可以输送数据到高完备性的链，而高完备性的链可以输送数据到低完备性的链，这是根据 Biba 模型。如果高完备链收了低完备链的数据，高完备链的数据就会被污染（contaminate）。

动态的链网完备性

我们可以在链网上使用传统的完备性所用的 Clark & Wilson 和 Biba 模型，但是我们需要考虑下面的因素：

1.区块链完备性>数据库完备性：因为区块链有拜占庭将军协议以及加密的机制，所以胜过于数据库的事物一致性协议。所以区块链的完备性胜过于数据库的完备性。

2.拜占庭链完备性> 数据库一致性链完备性：一条链如果使用了拜占庭将军容错机制，其完备性就胜过于另一条使用了数据库事物一致性的链的完备性。

3.央行完备性> 银行完备性>交易所完备性：这是由链的参与单位来决定链的完备性，参与单位的重要性决定了其完备性需求。例如，一个国家通常只有一个央行，却有多个商业银行，并可能有上千个交易所。而央行可以监管商业银行，商业银行可以监管交易所。

4.完备性和节点数目、历史有关：参与投票的节点越多，完备性会更高。过去有强完备性历史的链网，可能会持续保持其强完备性。

5.动态追踪完备性、动态链分类：每个链的完备性可以被动态追踪。两条链互通时，可以查阅彼此的完备性。如果高完备性的链必须接受低完备性的数据，低完备性的数据必须经过人工或自动验证，才能够被收入高完备链中，并且该数据可能会被归类为不可靠。

6.数据分类 (Data classification)：数据来源的完备性可以被分类，例如某个交易所的数据来源，可能比另一个交易所的数据来源完备性高，因为前者的历史完备性好。

异构网络的分析

一般来说，现在的链网只考虑到了互通性，而没有考虑到完备性。所有链网需要维持三个一致性：

1. 每条链（参与链或中间链)需要维持自己的一致性；
2. 中间链需要和每一条参与链维持它们之间的一致性；
3. 一条跨链交易需要由多条参与链以及中间链来维持。

如今许多条链都因为共识算法的复杂，需要很多时间和计算力，而无法提高效率。所以，如果要维持上面三条链一致性，那么这样的链网的效率就更低了。有些模型就不在乎中间链的一致性，但是这样的链网模型一致性就会出问题。

因为每条链与每条链之间，都必须用动态来维持，而且第一个一致性必须与第二个一致性是有关联的，所以在做第二个一致性的时候，必须考虑第一个一致性。例如，参与链 A 与中继链做一致性，参与链 B 与中继链也做一致性。中继链要保持一致性，就造成参与链 A 与参与链 B 必须同时和中继链维持一致性，这会使整个链网变得缓慢。而且参与链越多，复杂性越高，性能越差。

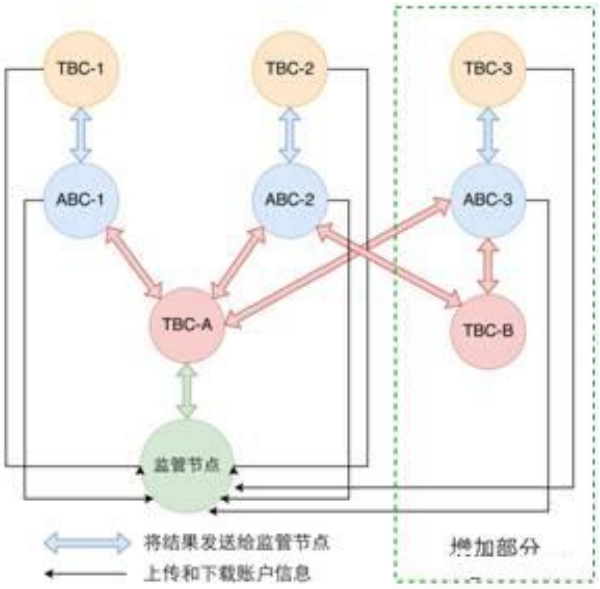
一个严重的问题是这种中间链（或中继链）的架构可能是中心化的。由于是中心化的组织，如果有许多参与链需要彼此进行交易，中间链的计算及通讯量容易成为链网的瓶颈。

熊猫链网

熊猫链网使用双链式架构，由 ABC（Account Blockchain，账户链）、TBC（Trading Blockchain，交易链）组成。每一个参加的金融机构，都至少有一条 ABC 和一条内部 TBC。内部 TBC 专门为金融机构内部转账时使用。这样的结构使得 TBC 只负责维持账户的余额，也因此，ABC 可以有负载均衡的架构。

两个交易的 ABC 之间，至少有一条外部 TBC，负责这两条 ABC 之间的交易。一条外部 TBC 可以处理多条 ABC，两条 ABC 之间也可以有多条外部 TBC。

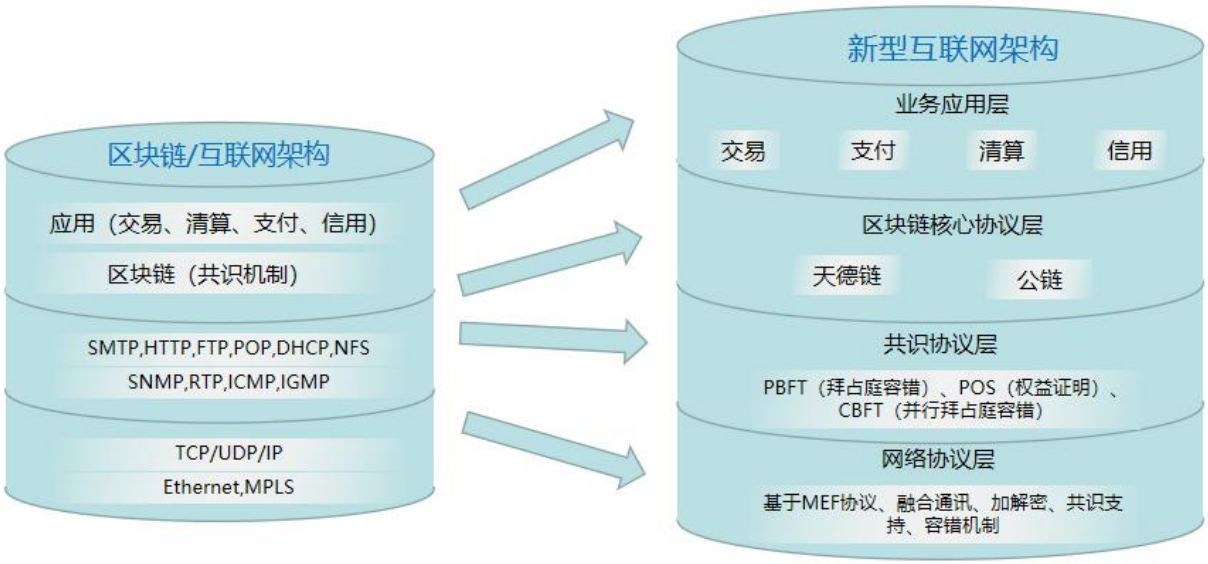
任何金融机构都可以随时加入链网。只要自己先成立一条 ABC，加上内部 TBC，再参与一到多条外部 TBC，就可以加入这个熊猫链网。如下图所示，左边是已有的部分，右边是新增加的部分。



7. 互链网是全面改革

互链网改革是全面改革的，从最高层的应用，到底层操作系统和网络，都以安全保护隐私为优先。这不是单维度的改革，也不是“小飞象”模型。

互链网设计原则 6：从最高层应用层，到底层操作系统和网络，都以安全保护隐私为重点。例如在应用层，数据需要加密，但是在操作系统，数据同样也是加密的，在网络传输的时候，也是可以加密的。



融合共识与加密，更改互联网协议

在新体系下，每一层都有新科技。下表比较传统体系和创新体系的不同。

表 2：创新体系和传统体系的差异

	创新科技	和传统系统不同之处
应用层	• 每个领域开发自己区块链应用框架，提出世界领域标准模型 • 每个领域除了参考模型，还有领域产业沙盒，矛与盾一起发展 • 开发基于区块链的金融架构和基础设施，例如数字法币系统，全盘改变现在金融系统体系	• 现在大部分领域还没有区块链参考架构 • 现在大部分领域没有产业沙盒可以支持区块链应用 • 现在没有基于区块链的基础设施 • 现在金融系统体系可以全面被区块链系统取代
区块链层	• 建立新可以监管的区块链架构 • 建立高性能的区块链系统 • 建立基于客户的身份证和安全机制	• 现在区块链没有设计监管机制 • 现在区块链系统性能低 • 现在区块链没有基于数字身份证的安全机制

操作系统层	• 新操作系统支持加解密、共识、监管机制 • 硬件处理保证安全	• 现在操作系统不支持区块链，也不支持监管 • 现在操作系统使用硬件，但没有使用这些来支持区块链和监管
网络层	• 建立新安全保护隐私的网络和协议 • 没有得到允许，不能访问也不能获得数据	• 现在网络是开放型，只要有网络地址，就可以送电子邮寄或是访问网站，没有保护客户隐私 • 谷歌这样的公司可以收集和销售客户隐私信息

8. 新网络基础设施

今天的互联网跟以前的互联网有很大的不同。互联网现在经历一个改变：过去端到端的设计原则大家尊重，认为端到端到原则是好的原理。但是 12 年前斯坦福大学开始有不同想法，并且发展成了新网络设计趋势，SDN (Software-Defined Networking) 和 NFV(Network Function Virtualization)。SDN 跟 NFV 跟过去的互联网协议不相同，最大的不同就是不再遵守端到端的设计原则，并且认为互联网不应该是个黑盒子。

今天的网络的协议性能低有三大问题：

1. 今天的协议无法提供及时的控制。这很容易明白：所有的控制，因为只有端到端的控制，只能在网络边缘控制，而不能在网络里面做。
2. 所有的协议只做一部分的控制，而不能做全面的控制。
3. 因为每一个协议都只能做一部分，所以这些协议越来越复杂。

今天的网络的技术有三个缺陷：

1.缺乏“可控性”：今天网络上的机制是没有办法直接或者改变错误的行为，因为它是端到端的。
2.缺乏“观察性”：今天只有做端到端的观察，所有的信息反馈都是从端到另外一端，以致于信息第不够充分，而网络内的信息没有办法传播出去；反馈的信息传到另外一端是已经延迟了，离实时的目标相差非常远。
3.缺乏“可结构性”：因为整个网络是当做个黑盒子，没有办法在彼此冲突的协议和机制里面，获取足够和及时的信息来做决定。

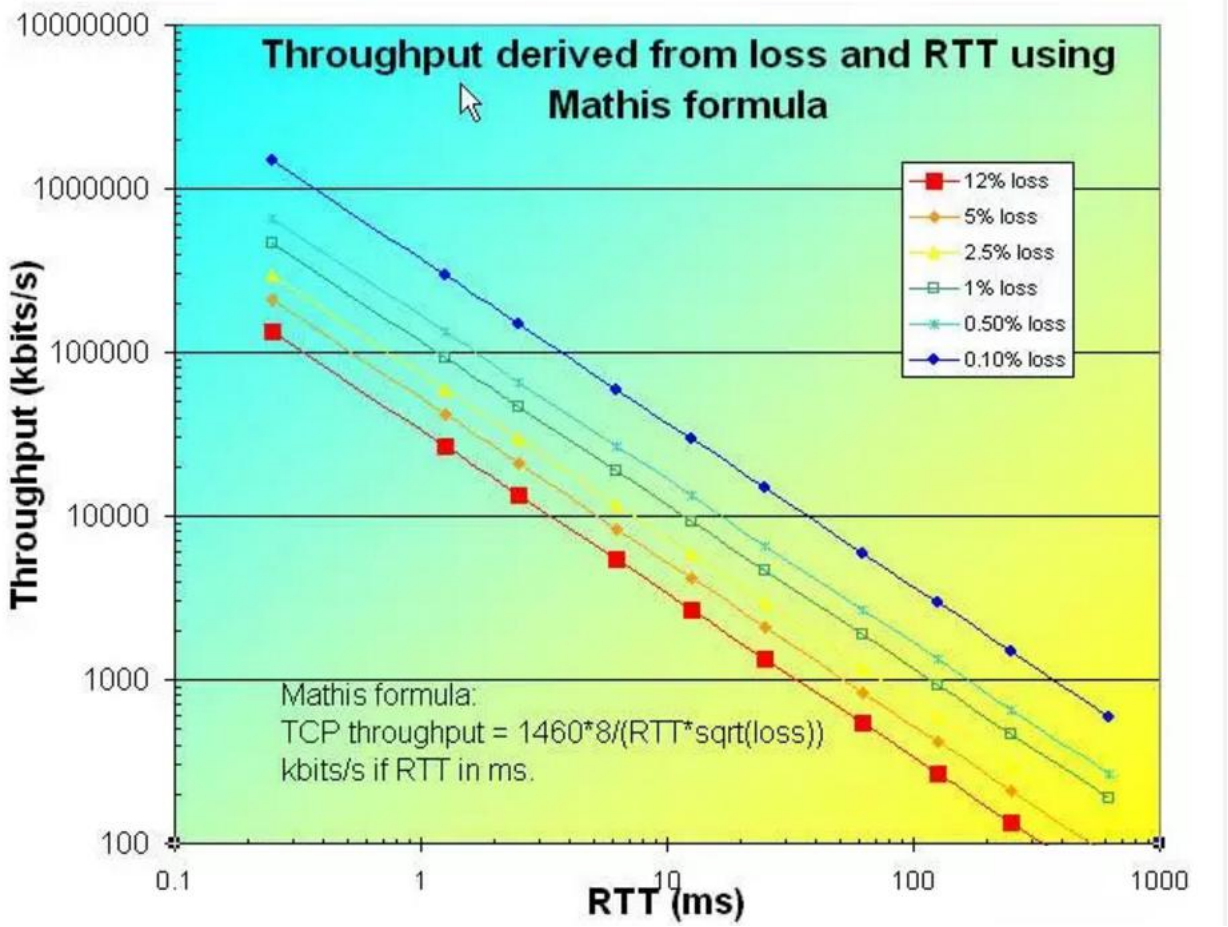
网络基础协议 TCP 协议造成性能浪费

TCP 作为一种最常用的传输层协议，它的作用是在不可靠的传输信道上，提供可靠地数据传输。在各层网络协议中，只要有一层协议是可靠的，那么整个网络传输就是安全可靠的。但是这种可靠性在一定程度上牺牲了性能，造成系统启动慢，拥塞控制难。

目前常用 Linux 系统的默认 TCP 拥塞控制协议为 Cubic，BBR 是谷歌在 2016 年提出的新的拥塞控制协议，目前在 Youtube 以及谷歌的内部网络中有大规模应用，Cubic 以及 BBR 在一定程度上改善了 TCP 的拥塞控制的过程，但还是存在一定的不足。

谷歌 BBR 协议改良 TCP

互联网的协议当中，一个特重要协议是 TCP (Transmission Control Protocol)。TCP 有一个问题：它的传输量因 RTT (round trip time，来回路径时间) 的上升和变化而下降。



TCP 协议吞吐量与时延关系图[11]

此图说明 TCP 的传输量，随着 RTT 的上升而成指数型下降。今天大多数人认为这是自然物理现象，其实这是协议设计不佳造成的，不是物理现象。举例说明：如果买 2 个通讯的盒子，而每个盒子都能够传输 10Gb/s。用电缆连接两个盒子，应该得到 10Gb/s。如果量出来不是 10Gb/s，我们就认为这个通讯设备不好。不论电缆的延迟是 1 毫秒，10 毫秒，100 毫秒或 1000 毫秒，盒子都应该维持 10Gb/s，这就是通讯设备的规格，不应该改变。但是一旦加上 TCP，就拿不到 10Gb/s。这表示正常传输量跟传播的延迟应该没有关系；传输量下降，是因为 TCP 设计不佳。

TCP 有另外一个问题，即计算传输量太慢。因为 TCP 是用端到端的迭代，发送端跟接受端需要来回输送不同的数据，才能够让发送端算出最优化的传输量。假如 TCP 需要 N 次迭代，每一次需要一个 RTT（来回传播的时间），迭代收敛（convergence）所需时间就是

N*RTT。但如果把这计算的迭代放在网络内，例如，在瓶颈链路处或附近，可以容易地获得关于瓶颈处拥塞的信息。在此处，计算通过当地计算设备的迭代来完成。算出最佳速率将被传送到 2 个端点（发送方和接收方）。因为今天的 CPU 速度够快，计算传输量的时间与发送到 2 端所需的时间相比，小到可以忽略不计。因此，最优传输量的仅延迟最多½RTT（可以短至¼RTT），这明显快 N * RTT（其中 N 是 TCP 计算其最优传输量所需的迭代数）。

谷歌发展了 TCP 的替代品 BBR，BBR 使用确定性等效原理(Certainty Equivalence)控制理论来改善 TCP。单单用这个原理，就得到比现在的 TCP 的速度好 28 倍。这打破长久以来的网络学术界的看法，就是 TCP 很难再进步，而且 TCP 是不能被取代的。谷歌的贡献就是打破了这个迷思。

但是确定性等效原理在控制理论上是 50 年前的旧理论。按这原理：当系统里面有很多不确定性的变化，就把它们取一个平均值，如此就把不确定系统当做是个确定的系统，把不确定的变化改成平均值的变化。好处是因为系统变成有确定性了，所以容易设计控制；但坏处是当真正系统跟平均值不一样的时候，就可能造成很糟糕的控制效果，这就是 BBR 的问题。下一个图表达 BBR 在嘈杂的路径中表现是很差的，这是一个在美国国家的能源部的实验室所做的一个测试，这个测试里面可以看 BBR 比 TCP 多大量的重传：第一例子 TCP 重传数是 10700，但是 BBR 的重传数是 240340 (22 倍)。

Remote Host	Throughput	Retransmits
perfsonar.nssl.noaa.gov	htcp: 183 bbr: 803	htcp: 1070 bbr: 240340
kstar-ps.nfri.re.kr	htcp: 4301 bbr: 4430	htcp:1641 bbr: 98329
ps1.jpl.net	htcp: 940 bbr: 935	htcp: 1247 bbr: 399110
uhmanoa-tp.ps.uhnet.net	htcp: 5051 bbr: 3095	htcp: 5364 bbr: 412348

网络需重构及新的协议

网上提出的链网的各样协议有六层（Layer）：第 0 层是共识，包括比特币元协议（BTC meta-protocal）、ETH 合约等；第 1 层是经济，包括独立代币（independent token），外部代币测链（sidechain of external token）等；第 2 层为区块链服务以及离链（off-chain）服务；第 3 层为互操作，包括交换（exchange）、跨链信息传递等；第 4 层为浏览器，包括 Mist、OmniWallet 等；第五层为 Dapps，包括云计算、开放集市等。这些协议写的非常好，然而它们大部分都是由区块链的技术来主导的，而不是从市场需求角度来考虑区块链应用。

从底层来看：第 0 层就是共识，不够底层，互联网底层是 TCP/IP，所以很明显的区块链的协议没有落地在网络的底层。没有相对应互联网底层的协议 TCP/IP，所以现在的区块链是完全使用互联网的协议，以至于区块链不能以高速进行，也不够安全。因为，区块链的其中一个要素就是加解密。

我们需要一个新的协议，需要满足一下几个功能：

1. 高性能（High-performance）：高吞吐量，低延迟。
2. 安全和隐私性（Security and Privacy）。
3. 可扩展性（Scalability）。
4. 容错性(Fault-tolerance)。

MEF 协议在极大提升 TCP 协议吞吐量的基础上，加入了区块链技术中的非堆成加密算法，满足数据安全性和隐私性的要求。

MEF 协议特性

BBR 协议依然是端到端的协议，依然要靠“猜”去猜测网络上的流量，MEF 协议是一个网络内控制协议，具有如下特性：

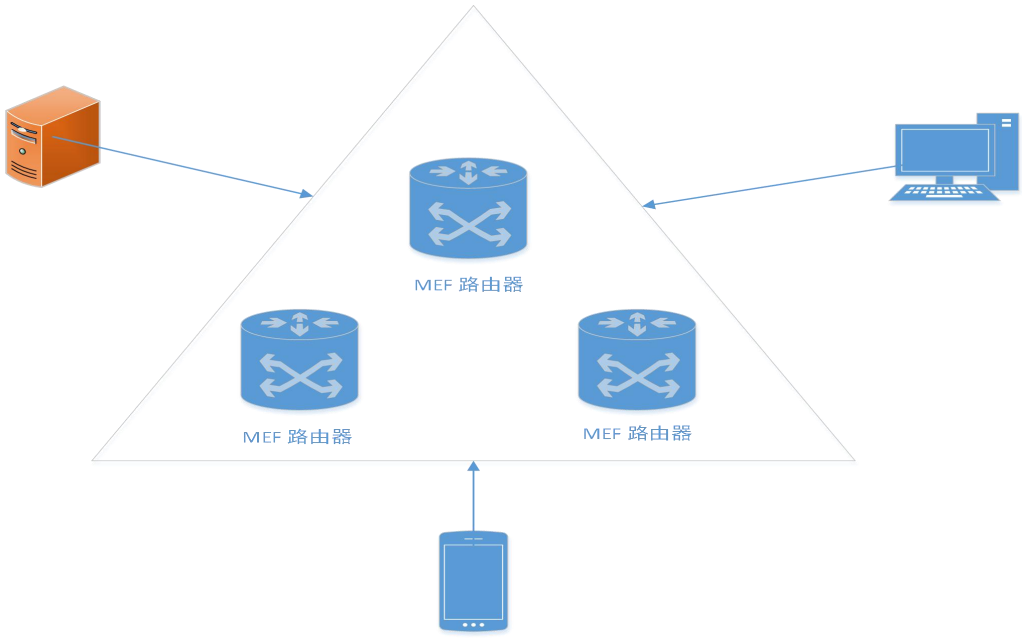
- 性能卓越，超过当前应用最广的 TCP 控制协议 Cubic，强过世界领先的谷歌 BBR 协议，Cubic 的特点是丢包了性能下降，BBR 的特点是不在乎丢包，丢包了也不降速，而我们的 MEF 的特点是不丢包。
- 设计不凡，MEF 突破原有端到端思想，采用新型的网络协议设计，能够及时更新网络状况。
- 兼容所有，MEF 不仅限于使用 MEF 的网络，同时也兼容采用 Cubic、BBR 或是混合协议的网络可以应用于 4G、5G 乃至 6G 网络。
- 费用锐减，采用新型的网络协议，削弱了延迟对性能的影响，在 5G 场景下，采用 MEF 网络协议，可以大大减少边缘计算的需求，降低网络部署中开销最大的服务器费用，因此 MEF 助力 5G 的发展与部署。
- 更适用于区块链，在 MEF 协议中加入了加解密算法，保护数据安全性，由于 MEF 协议运行在底层，加解密速度更快。

MEF 协议使用场景

- 满足边缘计算的需求，应用程序在边缘侧发起，产生更快的网络服务响应，满足行业在实时业务、应用智能、安全与隐私保护等方面的要求。
- 对于视频流服务有重大作用，可以更好的提供视频服务。
- 对于无人机的信息传输具有重大作用，无人机随着距离的增长，时延会大大增加，采用 MEF 协议，速度与时延无关，改善无人机的信息传输速度。
- 美国证券公司大都在交易所旁边，因为要保证交易速度，采用 MEF 协议之后就不需要了，因为 MEF 协议传输速度与时延关系不大。
- 适用于远程医疗服务。

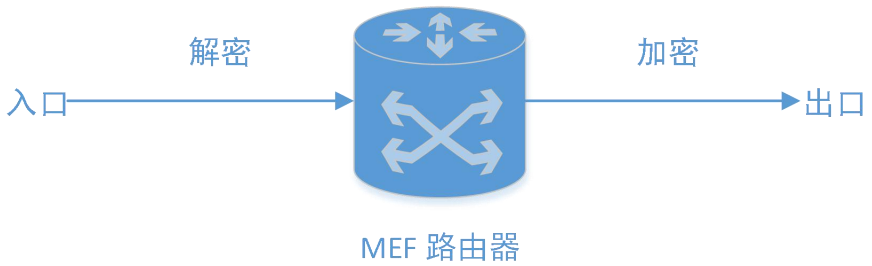
MEF 原理

如下图所示：



MEF 协议运行在 MEF 路由器上，在 MEF 路由器上进行统一的网络资源的调度管理，TCP 是用端到端的迭代，发送端跟接受端需要来回输送不同的数据，才能够让发送端算出最优化的传输量。假如 TCP 需要 N 次迭代，每一次需要一个 RTT（来回传播的时间），迭代收敛（convergence）所需时间就是 N*RTT，在 MEF 协议中不需要进行迭代，采用网络内控制，在最开始就公平分配好各个连接的带宽，不需要靠“猜”去猜测带宽，由于采用网络内控制，可以极大的减少丢包甚至不丢包。

MEF 安全性



在 MEF 路由器上采用区块链技术的非对称加密算法，在数据出口将数据进行加密，在数据入口进行数据解密，这样即使有人截获数据，也无法读取数据内容，保证数据安全性。

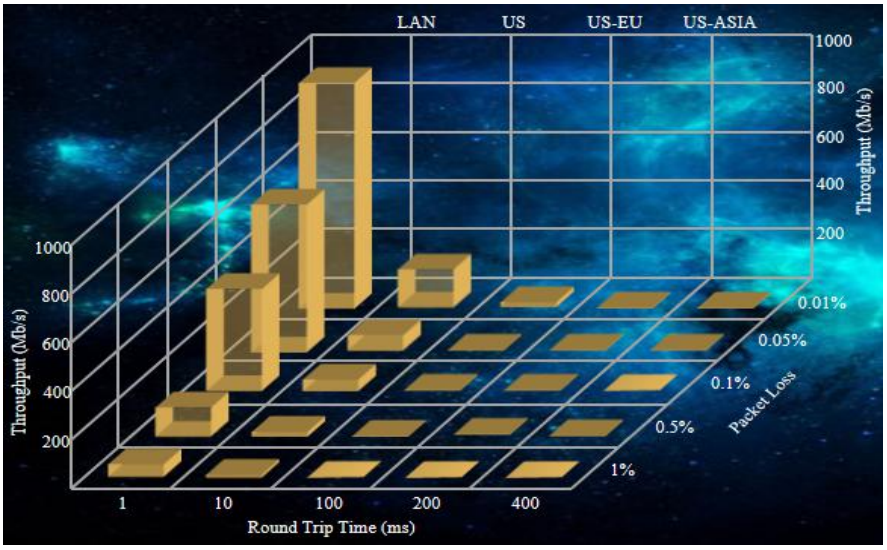
MEF 示例

模拟一个 4G 网络的环境，网络延迟采用 200ms，相当于北京到洛杉矶的传输延迟。在这种环境下，可以看到传统网络协议的性能缺陷。

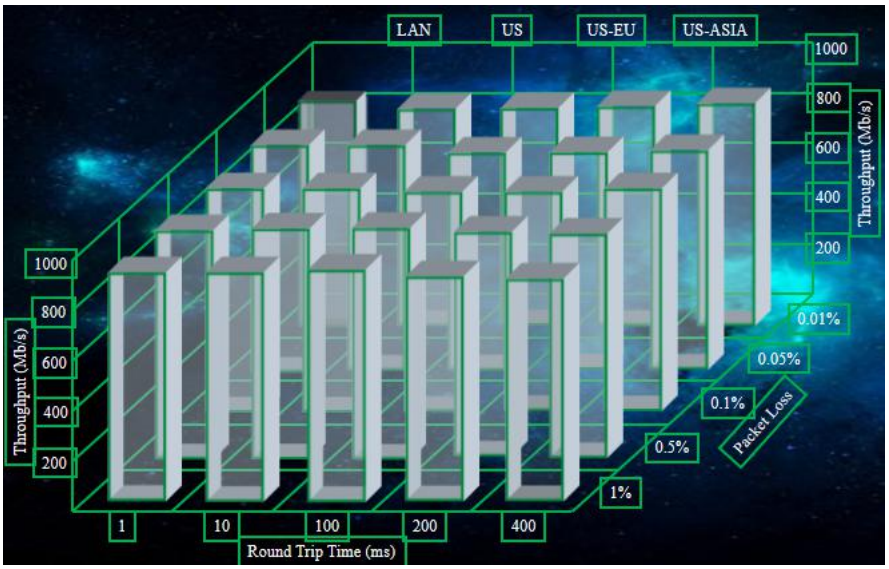
时延	Cubic	BBR	MEF
50ms	235mbit/s	1370mbit/s	1990mbit/s
100ms	205mbit/s	1120mbit/s	1980mbit/s
200ms	93.2mbit/s	809mbit/s	1850mbit/s

在 200ms 网络延迟情况下，MEF 的性能是 BBR 的两倍，是 Cubic 的 20 倍，MEF 技术完成自主可控，可以改变通信领域、网络计算领域的生态发展，甚至影响更多行业的发展。

TCP 协议随着 RTT 和丢包率的增加，吞吐量呈指数下降



随着 RTT 和数据包丢失的增加，MEF 吞吐量改变有限



9. 互链网的益处

2016 年英国首席科学家认为区块链带来社会、金融、监管、法律的变革，从最高层到底层，百业都可用。这里，我们提出区块链可以带来科技的改革，包括网络、操作系统、数据库、应用架构，而且有的改革还会是结构性的改变。本文提出的新概念可能需要多年才能完成，成吉思汗说“你的心胸有多宽广，你的战马就能驰骋多远。”中国如果希望在区块链理论上站在最前沿，拥有创新制高点，我们的思路就需要和以前不同的路线。我们认同并支持区块链是中国科技的重要突破口，所以我们在此提出一个突破口的蓝图。

什么叫突破口？开发一个和现在的系统差不多的系统不会是突破口。这里我们提出的许多设计和传统设计都不相同，而且这些设计是在实验室进行了 5 年实验后提出的。当我们实验室系统 90%计算力都在做区块链基础操作的时候，我们就明白现在系统不能支持区块链和互链网。也是因为这原因，我们坚信以后计算机和网络基础设施会改变，这也会是历史性的机会。

在这个白皮书中，我们很少提以后的愿景，例如我们没有提产业会如何改变，系统会变成什么架构。我们主要是提方向上的改变，思维的改变。我们现在对将来任何预测可能都会不正确，因为没有人有预测未来的水晶球。但是只要方向正确，我们就可以踏出第一步，因为未来会自我调节。

这里的蓝图以后还会继续发展、演变、进步。我们踏出了第一步，让将来来评估这些构想会不会成立。

互链网和互联网有巨大差异，使用互链网，区块链开发和使用更加便利。现在区块链系统花许多时间开发安全机制，而以后这些安全机制可以由基础设施提供，监管单位可以迅速建立一个监管网，从事线上交易实时管控，预防金融风险。以后数字经济会是一年 365 天，一天 24 小时交易，实时监管。通讯信息也都加密，网关也可以建立加密机制，个人隐私信息可以在基础设施上加密存储。

我们只是走了一个小步，欢迎大家在路上同行合作。

10. 致谢

本文部分思想发布于 2020 年 1 月 5 号杭州国际博览中心召开的互链网高峰论坛上。这互链网项目开始于国家大数据（贵州）综合试验区区块链互联网实验室,早期研究结果发表在 2017 年贵阳数博会。新网络协议是 2019 年在北京天德科技有限公司开发。无数科学家、研究人员、工程师、学生花了大量时间从事研究和开发，他们都是这个项目的英雄。

11. 参考文献

[1] 蔡维德，“什么是互链网核心技术”，2020.1.14.

[2] 蔡维德，“区块链是中国领先全球网络科技的机遇”，2019.12.23.

[3] 蔡维德，姜晓芳，“区块链 ——百年难遇到的科技强国机会”，2019.12.31.

[4] 蔡维德，“区块链 10 大研究方向”，2019.12.08.

[5] 蔡维德，姜晓芳，“监管沙盒证实实行有困难，中国应该积极部署产业沙盒”,2020.1.12.

[6] 蔡维德，“真伪稳定币！区块链需要可监管性”，2019.05.28.

[7] George Gilder,
Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy
2018

[8] George Gilder, “Blockchain paves the way for trust and security”, 2019.10.4.
https://gilderpress.com/2019/10/04/blockchain-paves-the-way-for-trust-and-security/

[9] George Gilder, “Exclusive: ’Life after Google’, 10 Laws of Cryptocom”, 2018.7.17.
https://townhall.com/columnists/georgegilder/2018/07/17/exclusive-10-laws-of-the-cryptocosm-n2501167

[10] Shannon Voight, “George Gilder’s Ten laws of Cryptocosm”, 2019.2.28.
https://blog.blockstack.org/george-gilder-predicts-life-after-google/

[11] 蔡维德，“从麻省理工的数字社会到通向区块链中国之路”，2019.02.12.

[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”， 2018.8.7.

[13] 蔡维德，姜晓芳，“区块链的中国梦之四：RegTech 编织全面安全梦”，2019.10.26.

[14] 蔡维德，“区块链互联网”， 2017.5.27，贵阳数博会演讲。

互链网白皮书

Internet of Blockchain (IoB) Whitepaper