2018年12月20日，由清华大学经济管理学院数字金融资产研究中心主办的数字金融资产大讲堂在北京举行。中国银行原行长李礼辉发表了题为“数字金融与数字货币”的主题演讲。

大家看上面这张图，我们要建设一个数字中国和现代金融制度，需要全新的信任机制。现在我们的新技术在创造信任方面不断崭露头角，但总体仍然处在萌芽的阶段。我们怎么设定未来信任机制的目标呢?我觉得应该做到五个可信：

> 一个是数据可信，这当然很重要;二是资产可信，包括现实的资产，也包括以数字形式表示的资产，所谓的数字资产;三是合约可信，大家谈到区块链时更多谈到智能合约，但是智能合约必须可信;四是物品可信;五是人品可信。

做到这五个可信应该是我们的目标，但它有个技术性的前提，基础设施必须是可信的，应用技术必须是可信的，数学算法也必须是可信的，我想这应该是各位的特长。

建立全新的信任机制的话，我觉得还要走这样一条道路，我们要把数字信任和传统的信用结合在一起，而且我们要把技术方面的创新和制度方面的创新结合在一起。我觉得要建设新的信任机制的话，我们要做到几个要求：

一是可信可靠

并非所有的数据信息都可以采集和记录，也并非所有的数据都具备应用的价值。数据的采集、记录和应用必须遵循基本的准则，就是可信和可靠。数据的采集、记录、应用应该依法合规、有效管控、加强制度建设，网上关于数据采集、数据存储、

数据挖掘、数据应用的法律法规，应该制定明确的规范。这其中有三个方面很重要：

1.明确公众信息数据的社会属性，保护公众信息数据的安全。

阿里巴巴、腾讯等企业采集了很多数据，其中相当一部分属于公众数据，这些数据具备社会属性，而不是企业数据，我们应该明确这样一些数据的社会属性，保证公众数据信息的安全。

2.限定信息数据的商业应用范围，防止企业和个人的私密信息被滥用。

我觉得商业信用信息系统中，应该只允许采集有效的、必要的，与信用评价相关的各维度的用户数据，涉及个人隐私的数据信息、家庭住址、行动轨迹、电子信件等等必须得到有效的保护。即使是国家的权力机构也只能在法定范围内调取和使用。任何机构、任何企业、任何个人都不能侵犯个人隐私，都负有保护个人隐私的责任，都不能把涉及个人隐私的数据信息用于商业目的。我们也应该建立数据运营商中心数据库和云存储数据库集群的准入门槛，严格进行技术审查、资格核准和行为的监管。

现在有个观点，我觉得多少有点道理，有人说为什么互联网金融在中国发展这么快，在美国发展的那么慢?可能其中一个原因在于，关于个人信息、关于隐私保护的法律强度不同，我觉得多少有点道理。我们现在依托于国家政策的宽容，也依托我们消费者的包容，我们中国的互联网金融得到很好的发展，但是现在应该说到了我们加强制度建设的时候了，在这个时候我们越来越多的信息裸露在社会的各个层面，这个时候我们确实应该加强数据的保护。

3.保证数据安全和数据系统的可靠性。

这是大数据技术应用的底线。数据系统不可靠，不仅可能损害信息数据主体的权益，而且有可能危害国家的信息安全。数据的安全应该依托自主可控、安全可靠的操作系统。我们数据安全应该覆盖从数据源头的采集到数据存储、数据应用全过程，各个环节都应该建立具体的制度、流程和规范，而且安全的技术和制度应该与时俱进，适应新的技术环境，我们要重新审视安全定义，确保数据安全。

过去我当行长的时候，我们那时候是大中心的体系，我对中国银行的技术系统、电脑系统我是有信心的。哪怕每秒几万、几十万黑客的冲击，我仍然可以保护我的信息安全。但是现在应该说新的数据世界是多中心、分布式、数据云、多元复合的结构体系，所以过去成功应用于大中心的技术手段、制度，未必能够适应新的数据世界，所以我们应该抓紧研究，采取有效的防控手段和技术措施，维护数据的安全。

二是共建共享

唯有大数据才可能有大信用，我们用大数据技术解决信息不对称的问题，可以让市场变得更加透明，降低信任成本。一般来说数据覆盖率越广、一致性越高，数据应用范围就越大，创造的价值也越大。建立具有高度一致性、可靠性的信任系统，比较可行的路径是共建、共享。

所以，我们有必要对分散和自成体系的政府部门的数据系统进行整合，实现关键领域的数据统一。这方面我希望清华，有这么好的基础力量，应该为国家的统一开放、共享的数据基础设施的建设作出应有的贡献。

1.建立标准统一的金融统计制度，建立集中统一的金融数据库，建立互联共享的金融数据应用系统，实现金融“一本账”，形成能够支持金融审慎监管的基础设施。

2.整合银行、工商、行政、管理、税务、海关等部门的征信系统，共建全国统一共享的小微企业征信系统，采取统一标准和口径，采集小微企业和个体经营者的金融业务、工商登记、税费缴纳、国际贸易、市场诚信等等信息，挖掘对小微企业、个体经营者信任，赋予信任标记，促进小微企业和个体经营者的信任增值。现在我们国家已经启动的个人信任信息的平台，也应该建成统一共享的数据库，而不是分割的数据库，特别是按部门分割的数据库，我觉得它的意义和价值是要打折扣的。

3.支持和促进企业层级的数据资源整合，这只是我个人的观点。我们现在很多企业手中都拥有各种各样不同的数据资源，这种整合是必要的，应该按照共建、共享、互惠、互利的原则，一方面在更大范围共享数据资源，扩大数据应用的覆盖面，有效提高数据管理水平，特别是提高效益分析、市场分析的准确性，另外形成以数据资源共享为支撑的供应链和信用链，这样就可以降低链内的交易成本，提升信任价值，提升数据应用的价值。

4.构建市场参与者共同维护市场信用的格局，联合抵制数据造假、信息造假、信用造假，共同创造良好信用环境，提升信用的社会价值和商业价值。

三是融合联合

第一个层次是资源的融合。推进技术、资本、数据、资源等整合，以效率为中心重构商业模式，提高金融创新的效率和效益。特别是我们中小金融机构，船小好掉头，但是资本不足，实力不足，如果各家中小金融机构都自己建立了自己的可比系统，它的成本是很贵的，所以我认为中小金融机构可以组成金融科技联盟，抱团发展，共享成果，共担成本。

还有科技企业和金融机构，可以按照优势互补、利益分享的原则，建立长期合作的商业模式，科技机构负责对某一类商品和金融服务的研发，银行负责这样一些新的产品的销售，然后双方按照约定的比例和原则分享这些新的利润。当然现在还有最新的方式，就是云计算，云计算平台上是可以共享这些数据资源的，在云计算的平台上，你的平台、你的系统、你的软件、你的日常服务不一定要自己建，按照使用量给云计算付费就可以取得这方面的金融服务，这比自己单独建立系统高效的多。

第二个层次是新技术的融合。我一直认为不管是大数据、区块链还是云计算、人工智能，都不可能单打独斗，单打独斗的效率不一定是最好的，这些新技术的集成可以提高它的效能、节约它的成本，建立以效率为中心的金融服务的流程，或者说重构以效率为中心的金融服务流程，能够打造零距离、多维度、一体化的金融服务，这方面大家都很清楚，比如可以提高信任评价、风险定价、决策效率，可能开发投顾、智能交易、智能支付、智能资产托管等等系统，也可以实现可预设、可检测、可追踪的点对点的交易，引入法律原则和监督共识的节点，实现价值交换、契约执行、监管监督的同步，在确保价值交换符合契约原则的法律规范，在保证交易品质的同时提高交易效率也提高监管的效率。

第三个层次是所谓的联盟链。我觉得我们要优先考虑采取分布式、多中心、有中介的私有链或者联盟链的架构。基于目前的状态看，我觉得公有链的架构有很高的需求，一是需要很大的存储空间，二是需要高速的网络，三是不同节点并行的能力需要达标和均衡，四是需要耗费巨大的电能，所以一旦每秒的交易量超过系统的能力或者节点的处理能力，交易就自动进入队列的排队。

我觉得目前这种状态，哪怕我们现在研发的，每秒能够达到几千个TPS的速度的公有链架构，都未必能够满足金融交易的需求，因为金融交易具有高品质、多平台的特征，比如票据、资产管理等等，这样中频次金融交易的场景交易峰值每秒数百笔，要求TPS至少是几千笔，银行卡、外汇交易等金融业务交易峰值每秒都在万笔甚至更高，所以，有的系统每秒能够处理6万多笔的交易，每秒笔交易的确认都在毫秒级，支付宝、微信支付的系统，支持每小10万亿以上的交易和确认，而且金融交易通常是跨系统、跨市场、跨平台的，比如我们的数字技术构建资产托管系统，必须实现委托方、管理方、审计方、投资顾问等不同角色实施共享共管的要求，目前情况看对于这样高频次跨平台的金融应用场景，区块链技术发展初期的去中心化架构是难以胜任的。

金融交易必须具备可靠性和安全性的标准，我归纳几句话：我一直觉得金融业务的性质是用别人的钱做自己的生意，金融行业的特征是无视无处不在的风险，金融的社会属性是经济的枢纽、百姓的钱包，所以我们在金融领域采用新的技术，必须保证稳定性、可靠性、安全性，必须保证客户信息的安全，保护金融资产的安全。

在经济可行性方面，我们还要看到我们国家的基础设施比较发达的，大型金融机构以及超高速道里面中心化的信息系统，而且结合移动互联技术的发展，已经形成了共享的数据云的平台，像阿里、腾讯他们都有数十个数据中心，以支持云计算平台的运作。如果我们以联盟链的形态构建大中型金融机构共同参与的分布式的帐本系统，是可以形成金融机构无论大小都可以互联互通的技术平台，这有利于节约成本、确保交易速度，实现合规控制的目标。

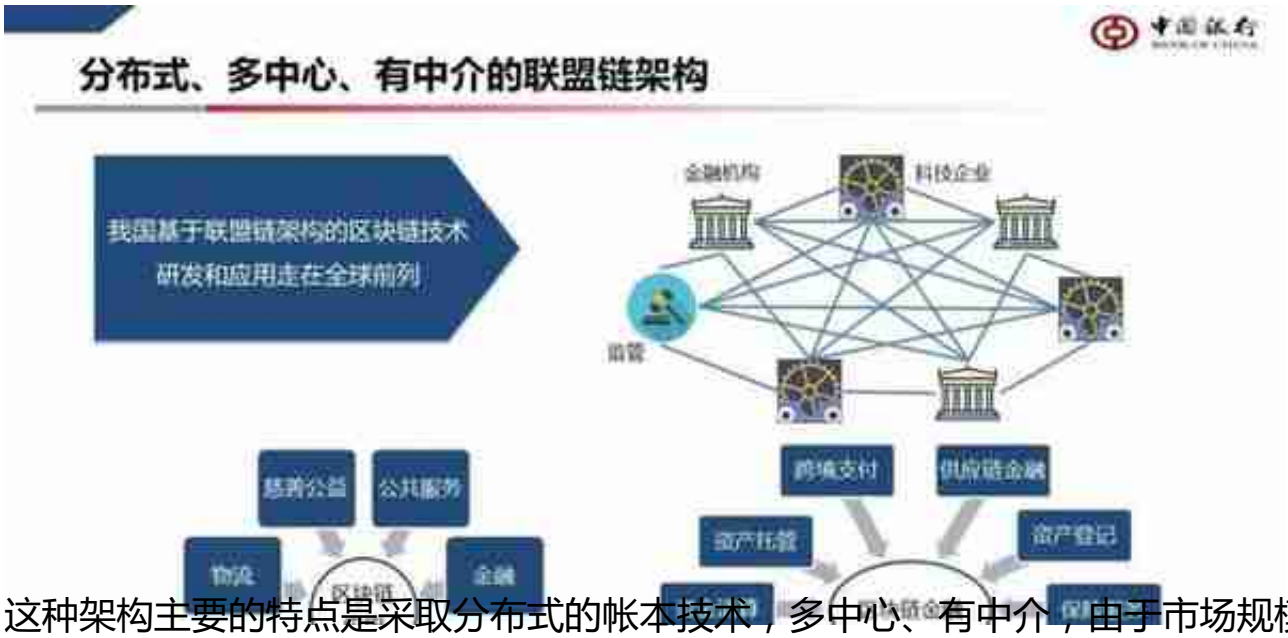
这里我就得出这么一个初步的结论：

我觉得无论从技术可行性还是经济可行性来看，区块链金融应用最佳的路径应该是分布式、多中心、有中介的联盟链架构【2】。我们国家目前区块链的金融研发，包括数字货币、数字票据、金融交易、供应链金融、审计、监督、数据共享等等场景，大多都采用了多中心、分布式的共享帐本的架构，我预计随着区块链技术的迭代、引进，去中心化的分布式结构仍然会在小规模社区中继续生存和发展，而分布式、多中心、有中介的联盟链架构，将会成为区块链技术规模化应用的主流结构。当然如果我们基于公有链这样去中心化的结构能够有更大的技术突破，能够满足规模化的交易要求和可靠性的要求，那它也有可能开辟一片新的蓝海。

二、数字货币

去年的11月30日，美联储副主席在演讲中把比特币称作数字货币，他指出数字货币如果大规模应用可能造成严重的金融稳定问题，由此而来的价格风险以及可能的流动性的信任风险，将对系统构成重大的挑战，在这前不久，英国央行副行长也提醒投资者，比特币不是官方的货币，没有央行支持也没有政府背书。对于这样的金融监管机构领导人讲话，市场回应先是泡沫的膨胀，然后是泡沫破灭。

从泡沫膨胀到泡沫破裂



这种架构主要的特点是采取分布式的帐本技术，多中心、有中介，由于市场规模和资本投入的优势，我们国家基于联盟链架构区块链技术的研发和应用走在全球前列的。现在实验运用的领域涉及金融、物流、慈善公益场景，包括资金清算、供应链金融、资金托管等等。

这几年区块链技术实际应用有两个方面值得重视：

一方面是建立多维度直接交付的架构，就是在参与方多，高复杂性的金融交易场景中，构建多维度直接交付的架构和加密的数据网络，实现众多参与方之间零距离、零时差的交通，可以做到协同治理、共享信息、规避校验、精简流程、提高效率、节约成本，比较好的案例，比如邮政储蓄银行的资产托管系统、微众银行的贷款和管理对帐系统，平安银行的金融一帐通等等。

另一方面是建立可信数据的登记与正式平台，比如中超络谱区块链分析平台，蚂蚁区块链可信数据存证平台等等。尽管如此，我觉得这种联盟链的发展也还有一些问题是需要进一步不解决的。

一是隐私保护技术，在区块链的共识机制下，我们怎么样来屏蔽敏感信息，提高组合签名、零知识证明等密码学技术的信任和效率，目前我们觉得还需要进一步提升。

二是真实性的监督机制，你把金融资产放到区块链上交易，进入这个区块链以后可能是难以改变的，但是在上链以前和上链的环节你怎么样确保这些数据和资产的真实性和完整性。我们把区块链技术用于各类溯源的时候能不能真正形成闭环，避免信息的失真，防止投机诈骗。

三是区块链智能合约技术，我们怎么样避免智能合约的技术漏洞，同时实现可控的

业务逻辑的修正和合约的升级。智能合约是整个区块链技术应用非常关键的环节，如果说智能合约存在技术漏洞那可能对一部分交易者是不公平的。另外，当我们发现智能合约有漏洞、有问题的时候，我们怎么样能够实现可控的业务逻辑的修正和合约的升级。

四是密钥的技术，密钥安全是区块链可信的基石，私钥是迷信的，在这样的技术架构中，怎么防止私钥被窃取或者恶意删除，这个私钥丢失了能不能予以补救。现在有些解决方案，这些方案需要进行研究。

五是区块链的架构在规模化的商业应用中，区块链技术平台不可能独树成林，怎么样实现无缝可靠的链接也是需要我们研究的问题。而且我也认为在金融业大规模应用方面，区块链还需要突破技术瓶颈，金融业是经济的枢纽、百姓的钱包，金融的交易高频率、大规模的特征，所以金融科技必须立足于规模化和可靠性。

由于目前还存在这样的技术瓶颈的限制，所以当前区块链技术尚未形成颠覆性的竞争优势：

(1)数据处理能力有限，不能满足大规模高频次交易的需求。 (2)区块链底层技术架构与现在金融IT系统继承协同的程度不够高，升级维护并不那么灵活。 (3)区块链共识机制分布式能力、密码学等等核心技术不断更新，学习成本高，人才培养和实践经验积累周期长。 (4)区块链技术标准化建设和法规建设目前尚未统一标准和规范，量算资产和智能合约有效性未能得到法律保护，分布式架构下的责任主体不明确，监管难度大。

2.分布式、多中心、有中介的公有链构架