周天虹

招商银行：如何基于区块链改进跨境清算？

◎《ICT 新视界》编辑部 / 整理

2017 年 1 月 13 日，在中国互联网协会互联网金融工作委员会、中国网络空间安全协会、中国电子金融产业联盟主办的“首届中国金融科技创新大会暨第 10 届中国互联网金融年会”上，招商银行信息技术部总经理周天虹介绍了招商银行对于区块链的认识以及在这方面的实践。>>

区块链是最近两年非常热门的一个课题，相关的书籍和研究文章也越来越多。总的来说，一方面大家对区块链这个新生事物非常肯定，甚至有不少舆论将其推得很高，比如最近就有一个流行的说法：互联网解决了信息传播的问题，可以称为信息互联网；而区块链解决了价值交换的问题，可以称作价值互联网——将区块链的地位与现在已经极大地改变了经济生活形态的互联网相提并论；另一方面，大家对区块链又很困扰，因为区块链这么好的一个技术，各方投入了很多的资源和高水平的专家进行研究，但除了比特币以及类似的一些虚拟货币的应用外，几乎看不到什么有价值的应用，这究竟是什么原因？

从招商银行的体会来说，这个问题很复杂，并不容易搞明白，还是要从技术角度去研究比特币到底是怎么回事，区块链到底是什么东西？只有在技术角度弄清楚了，上述问题才有可能得到解决。

区块链的概念是什么？大家比较熟悉的说法叫做去中心化、去信任化的分布式账本技术，需要进一步关心的是区块链的核心技术机制是什么？从去中心化的角度来说，最重要的是采用分布式的架构、P2P 的方式来解决点对点之间的交互；从去信任化的角度来说，最重要的则是两个机制：一是公 / 私钥机制，一是共识机制。

区块链大致可以分类为：公有链、联盟链、私有链。这 3 种分类将区块链分为 3 类应用，而一个区块链应用的开放程度如何其实非常重要——是完全开放、半开放，还是完全封闭，因为开放程度不同，其实现方式也会不一样。

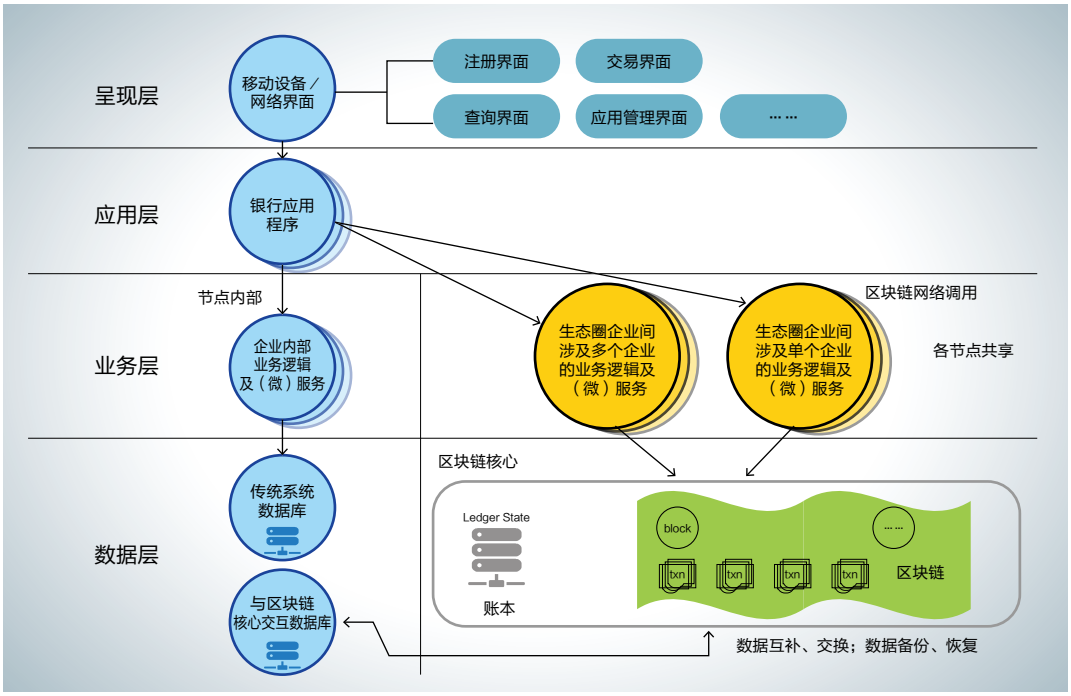

图 1 引入区块链的信息系统应用架构

比如共识机制的选择会不同、链上链下的数据分布会不同、安全机制的具体实现方式也会不同。

区块链技术对系统架构的影响

我们研究区块链不是为了写文章、做报告，实际上最重要的还是做实事，所以需要用这个技术来建设相关的系统，那么区块链技术对一个系统的架构会带来什么样的影响？

● 基于区块链的系统与原有信息系统的协作

图 1 主要是以联盟链和私有链为背景的一些应用类型，可以看到在引入区块链以后，整个系统的架构一定会发生变化，比如在图中右下角多出了区块链的内容。当然，也有一些不变的传统系统的部分存在。所以，在联盟链和私有链场景下，一个区块链的应用要“落地”，一定需要将传统的部分基于区块链系统整合在一起。典型的架构是上面两层：呈现层和应用层基本上保持不变，而下面两层：业务层和数据层则会应用区块链技术，其中业务层处理业务逻辑，在这一层有一些业务逻辑与区块链并没有关系，没有必要将其分布到链上，因为在区块链中实现一些功能有很多约束、很多制约，还有一部分业务逻辑则需要分布到链上，所以存在链下逻辑和链上逻辑之分。链下业务逻辑与区块链没有关系，这部分操作的数据自然也没有必要与区块链发生关系，所以会有独立的数据。

链上逻辑操作的数据处理比较复杂，当前比较难于完全分布到链上，其中一个原因主要是由于单链数据结构的一些功能实现难度大，比如很难查询且查询速度很慢等等。所以区块链相关的数据一部分分布在链上，也必然有一些数据分布在链下。链上和链下这两块数据共同来支持区块链的运作，并且链下数据的存储还可以对链上数据进行备份，出现问题还可以恢复等等。

● 紧耦合系统跨组织的协调和沟通难度大

区块链出现以后系统架构是如何变迁的？在互联网出现之前，两个不同的企业进行信息交互，由于各自系统不同，基本上是采用非标准的协议和接口进行通信的。而在互联网发展起来之后，虽然每个单位的系统仍然各不相同，但互联网采用了统一的标准化的通信协议，从而将不同系统之间交互的接口标准化了，只不过互联网采用的仍然是松耦合的架构。区块链则走向了另一个甚至可以说是相反的发展方向，它实际上是采用一套系统来覆盖不同的机构和企业，共同承载一个商业模式。简单而言，实际上就是采用一套系统来支持很多单位和机构，使之变成一个紧耦合的模式，这种紧耦合不是一般的“紧”，而是将不同单位和机构的系统变成了一个系统。这种紧耦合系统的好处是：在一些场景下，不同机构都要实现自己的系统，其实做的是类似的事情，很多是重复性的工作。比如在支付清算场景，大家各自做一本帐，其中所需要做的工作是差不多的，但是因为各记各帐，就需要对帐，谁出了错还需要冲正。那么能不能做成一笔帐，就像比特币一样——这么多单位用一个系统去覆盖，这就是区块链的思路，这种模式实际上对大家都有利，使得大家都愿意来共同建设这个系统。当然，还有很多的细节问题需要解决，其中，紧耦合系统比较大的一个问题就是跨组织的协调和沟通比较麻烦，需要大家坐下来共同协商解决。

根据麦肯锡的研究显示，最近几年不断出现的新技术对金融技术体系产生了比较大的影响。互联网主要影响了交互产品，云计算对业务的影响更大，大数据技术的主要在风控，而区块链则是对金融机构技术栈的下 3 层——清算基础设施、系统交互和规则设定产生了比较大的影响。当然金融机构的技术栈表达方式比较多样，这里采用的是麦肯锡的描述，总体而言，区块链会对金融机构的基础设施会产生影响，但这个影响会不会非常大？我觉得这个问题现在可能还很难回答。

● 分布式共享账本带来安全和隐私问题

区块链的第三个问题是分布式共享账本带来的安全和隐私问题。区块链是一种分布式共

一个区块链应用的开放程度如何其实非常重要，因为开放程度不同，其实现方式也会不一样。比如共识机制的选择、链上链下的数据分布，以及安全机制的具体实现方式都会不同。>>

互联网主要影响了交互产品，云计算对业务的影响更大，大数据技术的主要在风控，而区块链则是对金融机构技术栈的下3层——清算基础设施、系统交互和规则设定产生了比较大的影响。>>

享账本方式，其解决了一些问题，但也带来了另一些问题。其中首先是公钥和私钥，私钥被用来识别资产的所有权，一旦丢失就会丧失对资产的所有权。而现在的很多应用对于私钥的保护基本上采用软件方式，理论上都是可以被攻破的。实践当中如果反攻击技术的实现水平不是很高的话，相对于现在网络犯罪团伙的技术水平而言，可能其被攻破的门槛也不是特别高。因为反攻击技术体系非常复杂，包括了软件反跟踪、反调试、各种加密算法以及对策等等，整个这一套体系的实现如果不能做到很高的水平，都是比较容易被攻破的；即使做到很高的水平，理论上还是可以被攻破的。这是一个比较大的问题。比如比特币就曾经发生过一些比较重大的损失，甚至某个著名比特币交易所的比特币完全丢失了。所以，现在也引进了一些改进技术，比如一种叫冷存储的方式，其实质是离线使用私钥，再将结果倒回到安全终端上，但从信息安全专业的角度来看其仍然存在问题，因为还是要通过一个介质来倒换，而且使用也非常不方便。

其次是隐私问题，在区块链上实现的应用，一方面希望重要的信息对于无关者是看不见的，另一方面对于相关者来说在一些场景下信息又需要被其他方验证。这两者显然是相互矛盾的，既要看不见，又要被验证，技术上比较难于实现。为了应对这个挑战现在正在开发一些新的技术，比如环签名，其可以隐藏交易发起人，同时可以同态加密，但该技术还在发展当中，还有比较高的门槛需要跨越。此外，区块链在一些场景比如金融场景的应用，金融是被严格监管的行业，对监管者来说，其想知道的内容都应能获取，如何实现？相关的技术目前也正在发展当中。

● 智能合约存在诸多法律和技术挑战

智能合约确实是一个比较重要的发明，使得商业合同中的一些条款可以用代码来表述，有人将这种可能会出现情况概括为："代码即法律"。这听起来似乎非常厉害，但通常这种大而化之的说法也容易给人带来困惑，因为实际上往往不是那么回事。

首先，其中有一系列的法律问题需要解决，比如，法官和律师等从业人员对智能合约的法律理解如何？现有的法律体系如何将其融合进去？要根本解决这些问题非常复杂，还有很长的路要走。再如，商业合同涉及到很多人，最起码包括甲乙双方当事人和双方律师等，文字内容相对来说比较通俗也比较容易理解，但代码很抽象，如何理解这些抽象的代码？不理解的话当事人怎么知道别人起草的合同是否符合其本意？而且显然还有一些条款不适合用代码来表达，比如范畴描述和合作意愿等问题，这些是从法律角度来看的问题。

其次，从技术角度来看需要解决的问题也很多，比如，代码的逻辑漏洞和缺陷难以杜绝——软件行业已经发展了好几十年，但行业内仍有个说法：没有无缺陷的代码——代码有缺陷很正常，但是在商业合同中如果有比较大的缺陷或者存在漏洞，后果将会比较严重。

第三个问题是同一个商业合同在一些节点上的版本升级，如果执行结果不一样怎么办？这也是一个难题，现在仍在研究当中。

● 共识算法并不完美，需要调整修正

共识机制是非常核心的一个机制，当前还没有一个完美的共识算法。共识算法都存在这样和那样的问题，比如，公有链采用的POW优点非常多，包括完全去中心化、扩展应用很好、容错上限达50%等，但缺点是延迟和资源消耗都非常高。联盟链比较多采用拜占庭以及改良算法，与POW相比，其能耗低但是扩展性有限，容错上限只能做到30%多。由此可见，当前还不存在完美的共识算法，需要针对不同的场景和不同的应用选择合适的共识算法，而且要对其进行修正和调整。

实际上区块链非常复杂，要将区块链的应用真的做好，使之发挥作用，一定要深入了解技术,特别是上面提到的 5 个问题。今天，区块链难以被非常广泛地应用起来，与这些问题非常相关。

招商银行在区块链方面的探索

在区块链的探索上，招商银行最主要的方向首先就是与业界展开广泛的合作与交流，在一些重点的领域开展研究；其次，建立一个自己的队伍，因为要真的认清区块链就一定要懂区块链，要了解区块链的细节；此外，要真正把区块链用起来，一定还要有一个区块链的平台。现在虽然能够找到一些开源平台，但大都存在缺陷，可用性也成问题，无法简单地拿来直接就用，所以这需要立足自身来解决。具体的工作方向之前已有所提及，比如，在不同场景采用不同的共识机制，一定要了解共识机制的细节并对其进行修正和调整；智能合约在金融领域很有用但也存在一些问题，如何解决这些问题或者让其出现时不至于产生非常严重的后果仍需要研究；此外，隐私和加密一样也存在需要进一步解决的问题等。

进行区块链的探索不能只停留在纸面，要真正做一些事情就一定要有一个达到要求的平台。为此，招商银行建立了一个区块链应用的系统，它是一个基于区块链的跨境清算系统，已经开发完毕且马上将在生产系统中正式投产，真正解决招商银行跨境清算的问题。目前，招商银行有 6 个海外机构：1 个子行 5 个分行，相互之间以及与总行都有资金往来。招商银行当前有一个直联清算系统，该系统存在的问题主要是只支持总行与分行之间交换，海外分行之间没有办法直接交换。此外，比较多的人工环节以及与核心系统的耦合过于紧密也带来了一些其它问题，比如审批环节多、操作复杂、新的海外机构加入很麻烦，以及实施周期很长等等。

为了改造这套系统，招商银行研究了区块链技术，认为区块链去中心、分布式的架构与其当前的跨境清算场景比较适配，所以决定采用区块链来改造、实施一套新的跨境清算系统。将 6 个海外机构加总行都连到区块链上，任何两个机构之间都可以发起清算请求，任何两个机构都可以进行清算。总结起来，这套基于区块链的跨境清算系统的优势有 4 点：第一是去中心，采用 P2P 的架构而不是原来的星型结构减少了转发环节，提高了效率，使得任何两个机构都可以互联互通，原来报文传递需要 6 分钟，现在已缩减到秒级；第二是高安全，在私有链封闭的网络环境下具有非常高的安全性，报文伪造和篡改都非常难，在此情况下不再需要繁琐的对照，使得系统被简化了；第三是高可用，由于分布式架构没有核心节点，不会出现单点失效整个系统崩溃的情况，其中任何一个结点出现故障都不影响整个系统运作。这个系统实施完毕以后，在该场景下区块链技术确实发挥了作用；第四是可扩展，新的参与者可以快速、便捷地部署和加入系统。■

（根据招商银行信息技术部总经理周天虹演讲整理而成，并经本人确认）

招商银行认为区块链去中心、分布式的架构与自身跨境清算场景比较适配，所以决定实施一套基于区块链的跨境清算系统。将 6 个海外机构加总行都连到区块链上，使得任何两个机构之间都可以发起清算请求、都可以进行清算。>>