【2020.1.16】袁煜明：区块链的四大技术创新适用于多方协同的产业场景

今天演讲的内容包括三部分，第一部分介绍区块链几个主要的技术创新点。第二部分介绍区块链产业发展的主要的一些机遇。第三部分是如何加快推动区块链应用落地。

有些人指出，区块链其实不是什么技术创新，因为它其实是多个技术的综合，那些技术早在几十年以前可能都已经有了，只是区块链把它拼到了一起。的确是这样，区块链更多的是一种商业模式和商业范式的创新，这其实也是一个非常大的突破。

我们理解主要是有4个方面创新。一是从单点的复式记账法到多点的分布式的记账。在最开始的时候，大家各自记账，用脑子记或者用纸笔记；800年以前出现了复式记账法，这其实是一个非常大的突破。复式记账法以后有借必有贷、借贷必相等，相当于每一笔账都在两个地方出现相互复核，通过这样的方式是保障了整个账目是比较清晰，不容易被篡改，所以当时这是非常大的一个进步和突破。但是过去800年整个社会经济发生了很大的变化，技术也有很大的进步，在这样情况下还去用当年的复式记账法，以及从复式记账法所衍生出来的一系列清结算的体系，其实都有很大的问题，积累了一些弊病。用区块链的多节点分布式记账的方式效果会更好。

也有人说，单点的复式记账法和多点的分布式记账这两个事情本身并不是对立关系，不是互斥关系。没错，事实上你可以在分布式记账时照样把复式记账法搬上去，可以这么做，只是没有这个必要，因为区块链已经实现了相互的复核，所以没必要再去做一次清结算。所以区块链可以把整个效率提高、成本降低。

第二点，是从传统的账户体系到公私钥的非对称加密的体系。如果你的账户和密码都存在一个第三方的中介机构，好处是不管什么时候你的账户密码丢了，都可以找回来，拿身份证或者通过手机都可以找回来。但坏处是，你的这些信息都是掌握在第三方中介手里的。过往出现了很多次互联网网站信息泄露的事情。在区块链上，你是通过非对称加密，通过公私钥的体系来掌控账户，私钥是掌握在你自己的手里，但坏处是，一旦你私钥丢了，神仙都救不了你，肯定是拿不回来了，好处是你可以保障信息的安全性与可靠性。

比特币是用公私钥的体系去存储币，你也可以把一些其他的信息用私钥来存储起来，别人无法窃取。

举个例子，11月份人民网推出了一个应用“链上初心”，你可以把你当年入党时候的初心放到链上去，然后用自己的私钥去加密。这是一个很有意思的应用，它把区块链的很多特性都应用起来了。一种情况是，这个初心上链以后，在链上别人是看不到的，只有你自己看得到，你可以在每年入党纪念的时候看一下你自己的初心，跟当时是否符合。第二种情况，如果你特别的坦荡，也可以选择把你的初心直接公开出来，放到公示墙，大家都可以看到。第三个方式，到某一个时间点，比如说几十年以后，你可能也已经年纪大了退休了，回首往事，那个时候不需要私钥就可以自动释放出来。总之，这就是一个非常有意思的信息共享的一个应用，入党初心就是一种数据。还有很多其他的各种各样的隐私数据、机密数据、敏感数据等等，都可以通过多种的方式的结合，可能是公开的，可以直接共享，也可能是需要私钥，只能自己保管，保护好它的隐私性，也可以有限权限的访问，有些人可以访问一部分信息，或者有限时间的保密，一定时间以后解密。这些东西都可以通过区块链来去实现。

区块链创新的第三方面，就是从传统的数据库到链式存储。传统数据库跟区块链的模式，各自有优劣势和挑战，传统的数据库方式肯定更快，效率更高。但区块链的好处是保障了不可篡改，通过哈希值。哈希值相当于是一个内容的摘要，只要内容变了一点点，那么整个哈希值都会完全变掉，而且这个过程是不可逆的，你无法从哈希值的变化去找出来到底哪里变了。通过下一个区块掌握前一个区块的哈希值这种方式来保障不被篡改，或者是可以被验证的，通过多个节点的分布式记账来保障了相互校验，确认了最后没有被篡改过的，所以这是很大的改进。

当然，需要说明的是，区块链并不是完全不需要传统的数据库，你可以把大量的数据还放在数据库里存储，只要把它的哈希值上链就可以了，你就能够去校验，到底这个数据有没有被篡改。所以，大量数据没必要都放到节点上，否则的话的确是一个非常大的存储冗余。

第四方面就是从手动执行到智能合约，智能合约其实既不智能，也不是一个契约，它更多是一个自动运行的程序。事实上，智能合约出现的时间是要远早于区块链的，但是智能合约在区块链出来以后获得了一个非常大的发展。

因为区块链是一个分布式账本，它没有一个权威说一定由谁来执行，那么怎么办？可以通过智能合约去自动执行，以前我们是手动执行的，双方去签约盖章，然后去执行。出现问题的时候，可能需要法院去仲裁，或者需要第三方鉴定人去决定等等。现在通过智能合约的方式，就不需要见证人，自动到一个时间或者满足某一个条件就可以去执行，这就比较适合于区块链的分布式的场景。

总结一下，区块链的创新包括四个方面：单点的复式记账到多点的分布式记账；传统的账户体系到非对称加密的体系； 第三是从传统数据库到链式的数据存储。 第四是手动执行到智能合约。这四个方面我们认为是区块链最主要的一些技术突破点。

这四个技术创新，对于整个商业范式都会有非常大的改变，它会带来什么样的产业发展新机遇？

总书记在政治局集体学习的讲话里面提到，区块链有五大作用。我们理解，区块链最主要适用于多方协同的场景。它本身是一个分布式账本，没有一个单一权威的中介机构，所以比较适用于多方场景如何去协同。第一是促进数据共享，因为以前多方相互都不信任，不愿意去把数据去分享出来，所以，可以先通过区块链的方式来去做数据的共享。第二是优化业务流程，以前大家各自为政，所以流程是串行的。你一道我一道，现在可以相互并行，在统一的平台上去进行。第三是降低运营成本。因为以前是复杂的复式记账法以及由此衍生的庞大而繁复的清结算体系，现在可以通过区块链一步到位，所以降低了成本。第四是提升协同效率，建立一个有效的奖惩的机制，来充分地调动大家的积极性，防止作恶行为的出现，用总书记的话说，就是保障生产要素的有序高效流动，最后就是建设可信体系，通过链上不可篡改的体系来去实现各方的链上的互信。

在讲话里，总书记提到区块链的6大应用场景，包括区块链+金融、区块链+商业、区块链+民生、区块链+智慧城市，区块链+城际互通、区块链+政务。这六个方面其实都是多方协同的场景。

以金融为例，现在有个大问题，就是中小企业融资难，它很难获得贷款去加快发展。其实，核心企业欠小企业很多应收款，他肯定是会付，但可能账期很长，拖几个月半年、一年、两年都有可能。那么，这个时候企业生存就很成问题了。小企业去跟银行借钱，银行不敢贷款给他，因为看他没什么净资产，也没什么品牌，担心他不还。那么他会跟银行说，你看核心企业欠了我这么多应收款，他们肯定会付的。但银行还是不敢借，为什么？因为银行会担心应收款还在不在，有没有被重复放贷，这都是风险。如果通过区块链把整个应收款的过程全部上链，有没有被贷款也上链，保障过程中应收款的确没有放贷出去过，那么，这个东西就可以承兑了。有点像支票，支票是银行承兑，那么这个东西相当于是核心企业承兑，只是把支票数字化放到了链上。这就可以加快流通。当然，可能实际场景会更复杂，不一定是一级供应商，很多时候可能是二级、三级甚至四级供应商，根本说不清楚到底是谁欠我的钱。只有通过一个链上的数字凭证，才能够确保的确有这么一个应收款，银行才可以放心的贷款给我。这样一来，中小企业获得了融资，加快了发展，银行可以把钱放出去，而且坏账率也可以比较低，核心企业也可以让他安安心心的去欠供应商的钱，整个生态可以有更好的发展，这就是典型的多方共赢的场景。

再延伸一点，这其实就是从信息互联网到价值互联网的迈进。过往30年是信息互联网大幅提升的过程。一是极大的提高了信息的传输效率，降低了成本。我们现在给一个异国他乡的人发个信息，一秒钟就能发过去，基本上是0成本的，非常便捷。另一方面是人们获取以及表达信息的便捷度都比以往大幅增加了。以前只有王公贵族才能够去获取大量的知识，但现阶段一个很普通的人，只要有个智能手机，获取的信息可能比古代的王公贵族获得的信息量都要大很多。获取信息、表达信息也是一样。现在只要自己注册个公众号，可能就有机会成为一个10万+的作者。这是信息互联网的意义，让人们的信息传输、信息获取、信息表达都比以往变得便捷，普惠到了基本上可以说每一个人。

但是，现阶段价值的传输还是非常不容易的，比如说你要给异国他乡的人转一笔钱，可能就需要很长时间，而且手续费还很贵。全球还有17亿人是没有银行账户的，他们根本就无法做到银行汇款。

包括企业之间，中小企业明明有应收款，别人欠了他钱，他就是贷不到款，这就属于价值流转的不通畅。所以，通过区块链，我们可以搭建一个价值的互联网，让价值的流转像信息的流转，一样的便捷一样的高效，这是区块链最主要的价值。

那么我们再来假想一下区块链的未来，技术的发展往往超出我们的预期。 借用一下《失控》的作者凯文·凯利的话，他认为，未来的世界是一个虚拟世界，加上一个真实的世界，就是现在流行的词叫数字孪生。所有现实世界里的东西都一一被映射到虚拟世界，每一张桌子、每一把椅子、每一瓶水都会映射到虚拟世界，都会被数字化，那个时候你不是一个一个单一的服务器，某一个互联网公司不可能把整个体系去控制、去掌握、去管理，做不到的，肯定需要一个分布式的系统、分布式调度整个的数字世界，所以到时候区块链会是整个数字社会的基石。

最后，如何去加快区块链应用落地？

到目前来说，我们觉得区块链很好，作用这么大，能够这么去改变世界，那么为什么到目前为止应用还是零星的，还是局部的，没有形成大规模？

如何去加快区块链应用的落地，我们理解主要是有三个方面的路径：第一个是去夯实技术的基础设施。现阶段来说，技术的基础设施还是不够完善的，现在区块链更像是90年代的互联网，网速很慢，用户体验很差。区块链的问题是，第一效率，比如TPS不够高，像比特币每秒只有7笔交易，以太坊才二三十笔，EOS快一点，TPS能到四五千了。现在还有很多别的链可以有更快的TPS，其实都是在分布式和效率之间取得一个平衡，所谓扩展性的不可能三角，不能走到极端，不要去走这三角的某一个角，在这三角之间取得一个平衡，这是目前很多公链在探索的一个技术路径。包括在不同的应用场景可以采用不同的平衡方式。第二是安全性，现阶段也报出很多智能合约的漏洞，很多恶意攻击等问题，我们可以从技术角度去提高网络和代码的安全，包括从机制角度来去调动社区，去做保障预警机制等等，从而去提高安全性。还有互操作性，互操作性包括几个方面，一个是链间的互通，因为现在有很多公链，很多联盟链之间是不打通的，相互之间是信息孤岛，这不是一个好的现象，未来比较理想的情况肯定是链之间有非常好的一个连接机制。现在跨链的技术还是不是那么的成熟。另一个是链下和链上的信息的交换和验证，这是很大的问题。现阶段来说线下信息上链是非常大的挑战，很多时候信息一上链那一刹那可能被篡改了。虽然上链以后可以保证不可篡改，但是上链一刹那如何让它不可篡改，通过见证人机制，通过一些AI、物联网等技术的发展去保障，这都是一些挑战和课题。

第二是建设行业的生态体系，很多时候不是技术问题，更多的是治理问题。现在很多区块链的应用都是某一个巨头发起，的确做得很好，但问题在于，他发起别人就不愿意参与，觉得是竞争关系，为什么要参与你呢？有一个办法就是通过联盟的方式，让各方都参与进来，但联盟的问题是，它很多时候是个松散组织，最后谁也不出力，人浮于事。所以，需要去构建一个治理体系，能够让多方参与进来，让大家能够有比较好的奖惩机制，能够都去发挥作用，有权利有义务。这过程也需要建立行业的技术标准、行业规范等等，这样各个企业之间还是才能够有效的有序的互通。现阶段很多时候大家都是各自为政，做了各自的链，相互之间都是不打通的。

第三就是推进行业的教育培训。中国还有很多人对于区块链还是非常不了解，可能只知道概念或者连概念都不太清楚，更不知道区块链能够怎么用，在这个过程中需要推动行业的知识普及，通过论坛、讲座、新闻媒体、科普读物等等，所以今天也会有一个书单的发布，会有十本优秀的书来让大家比较快捷的方式学习。

另外应该有培训课程，线上的或者线下的课程，企业的培训等等。更有效果的是示范工程，通过政府主导或者资本推动来去做示范工程，一两个示范项目出来看到效果，那是能够推动让全社会更好的去让应用去落地的。三个方面的路径，包括夯实技术的基础设施，建设行业的生态体系，推动行业的教育培训。火币中国过去两年时间在打造区块链+的产业服务的一站式平台，帮助实体经济，帮助企业和政府用区块链更好的发展。我们有咨询、研究、培训、技术服务等等，有研究院、大学、产业赋能中心，做了很多的应用落地工作。还和很多高校来进行教育培训的合作，和机械工业出版社一块来进行系列教材的编写，和工信部人才交流中心一块进行人才培养的标准的制定，和海南大学一起成立区块链工程技术研究中心等等。谢谢大家。