给政治局讲区块链的陈纯教授 在最近的一次演讲中都说了啥

编者按：据新华社报道，中共中央政治局10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

浙江大学教授、中国工程院院士陈纯就这个问题作了讲解，并谈了意见和建议。

中共中央政治局各位同志认真听取了讲解，并进行了讨论。

美股区块链概念股率先闻风而动，迅雷开盘大涨20%。

10月13日，由中国计算机学会主办，中国计算机学会区块链专业委员会、中国电子科技网络信息安全有限公司、西南财经大学、中科国鼎数据科学研究院联合承办的2019 CCF区块链技术大会上，中国工程院院士陈纯院士曾发表《联盟区块链关键技术与区块链的监管挑战》主题演讲，表示国内区块链产业发展正迎来“春风”。

以下为相关报道及陈纯演讲全文：

10月11~13日，由中国计算机学会主办，中国计算机学会区块链专业委员会、中国电子科技网络信息安全有限公司、西南财经大学、中科国鼎数据科学研究院联合承办的2019 CCF区块链技术大会将于在成都举行。中国工程院院士陈纯院士发表了《联盟区块链关键技术与区块链的监管挑战》主题演讲，他表示，中国区块链技术的研究热点将集中于联盟区块链的关键技术，区块链监管技术等方面。联盟区块链除了四个关键技术需要大家研究，还有链上链下数据协同的技术，这也是下一阶段的发展方向。

核心观点：

1. 联盟链底层平台的核心是性能、可用性和安全隐私；
2. 链上链下数据协同技术是未来发展的一个重要方向；
3. 区块链的监管技术是区块链健康和持续发展的关键。

以下是演讲全文（根据现场速记和录音整理）：

今天很荣幸，也很高兴来咱们这次大会。我的报告题目是《联盟区块链关键技术与区块链的监管挑战》。刚刚前面说今年是比较差的年头，去年特别差，其实我觉得也不是这样，区块链正迎来发展春风，比如我国“十三五规划”已经将区块链、量子通信、人工智能等都作为重大项目进行；2019年2月18日《人民日报》头版提到区块链是“新一代的信息技术”。

区块链的简介，这里我简单跟大家分享一下。简介是传统系统跟区块链系统有几个特点，传统系统有互相对账、中心、篡改数据等特点，这恰恰是与区块链系统相反的。关于区块链的核心价值，这里有很多专家我就不多说了，它有提升多中心的协作效率、去中介，提升多方信任、数据不可篡改，可追溯，可审计等等。

区块链技术研究热点中国和国际上稍微有点区别，中国主要的研究热点是集中于联盟区块链的关键技术，同时我觉得区块链的监管技术也是非常重要的。为什么说区块链的监管技术非常重要呢？有一句话讲得好，就像交通一样，当警察没有站好，车子开不快，交通次序也不会太好。我这里主要想谈谈联盟区块链的关键技术。

1

联盟区块链的4大关键技术

首先联盟区块链高性能这件事是非常重要。当你有了联盟链，公链方面以太坊每秒几十笔，这个点是不够的。大规模应用上来的话，现在国内最好的联盟链可以做到上万个点，每秒几千到上万的性能。大规模的节点，或者大数据量的情况下性能会急剧下降，这也是大家觉得区块链浪费和性能不行的缺点。联盟高性能关键技术需要在各个方面进行技术突破，包括高性能的共识算法、包括高效智能合约引擎，也包括新型的共识机制，希望能够提高共识效率与安全性，当然主要是为了要支撑大规模各种网络结构的主网。还有一个研究热点软硬件协同优化，这也是非常重要，就像AI一样，没有芯片AI就很麻烦。

第二个关键技术是区块链安全隐私关键技术。在中国要用首先要全面支持我国加密算法和标准，这肯定没问题。商业应用需要平台业务数据隐私保护，可以通过命名空间的方式在物理层面进行业务数据的分离，这值得研究。还更细粒度的隐私交易机制，实现交易可验证但是不可见。还有基于可信执行环境等技术实现节点密钥管理和数据加密

存储，基于默克尔DAG等数据组织技术，防止文件被篡改。联盟链第二个关键技术安全隐私也是非常重要的。

第三个关键技术就是高可用性的关键技术。这里有一个动态成员的准入机制，以及节点失效后的快速恢复机制，这在分布式系统里都会碰到，这也非常重要，不能整个系统停下来加节点，应该是可以实时动态的。某一个节点出问题，我要删除的话，不能停下来删除，系统不能停。还有去中心化联盟自治的管理机制，如何来做这个事情？是通过多方提案投票表决方法还是别的方法，这些都要有机制。有人会怀疑，联盟链是不是真正能做到管理的公平机制，公链大家不会怀疑，但是联盟链是多中心化是不是会怀疑，这也非常重要。还有高效的热备切换机制，这也是联盟链以后的关键技术，也是非常重要的。

第四个关键技术是高可扩展的关键技术。一个是编程可扩展，我们说支持多种编程语言的使用。当然越普通的编程语言越好，这样大家就会用得很方便。第二个是存储方式可扩展，能不能支持多类型、多组织形式的数据可信存储。第三是支持预言机提供可信外部数据源服务。第四是支持跨链，实现同构链与异构链的跨链协同，这也非常重要。

这里有一个比较，我特意提出Hyperchain，在联盟链技术性能方面，我们国内也是做得比较好。举例来说，像Hyperchain现在所有性能比较都是优越的，就是好今年与国外各种平台的比较。

2

链上链下数据协同技术是联盟链发展的重要方向

联盟链产业化应用在国内也是可以，在金融行业、法律领域、医疗领域、能源领域、娱乐领域、公证领域等等，我想讲的是什么呢？虽然感觉今年区块链有所降温，但其实我们国家在联盟链的应用今年以来还是有很多，这些应用不仅仅是金融领域，这与国外区块链应用还是有点区别。西方区块链的发展基本上是基于金融创新带动别的行业创新，而中国除了金融创新外，更重要的是在各个行业的应用，而且现在国内有好几家联盟链平台，也足以支撑现在的一些应用。我前面讲到性能能做到上万个节点，当然这是很极端的情况下，而且可以做到每秒上万个的频率。

最近有一个例子也是非常好，政务方面的公积金，住建部和中国建设银行做了公积金的管理，全国491个城市的公积金，等于491个节点现在连在一起，不管什么城市的公积金，不管公积金所管辖的每个人，可以异地很方便的操作。这个如果不用区块链以前无法想象，你要么把数据全部集中在一起，要么就是各自的，我觉得这是很好的应用。

联盟区块链除了四个关键技术需要大家研究，还有链上链下数据协同的技术，这也是下一阶段的发展方向。

左边是CAP定理，就是一致性、可用性、分区容忍性，原来我做这方面，分布式的高性能的实时的计算，特别强调可用性、分区容忍性。但是无论如何每个系统都是在三个点取一个平衡，如果强调一致性，那可能对可用性和分区容忍性会差一点，所以不同的应用就会特别关注。

区块链也有所谓不可能三角模型对应过来，它是去中心化、可扩展、安全。同样的完全去中心化的话对安全性要求难度更大，就是一个三角的点。**所以我们就说传统信息系统与区块链系统都有一定的局限性。一方面，区块链系统需要通过链下系统扩展计算和存储能力。另一方面，现有系统链下需要与区块链对接以解决信息孤岛、防篡改等问题。**

现在如果作为大规模应用的话，我觉得最重要应该解决链上链下的问题，所谓的链上就是区块链，链下就是所有传统的信息系统。我们怎么样把区块链系统嵌入到现在传统系统里来解决它的一些问题，或者反过来用我们的区块链系统把传统的信息系统放出来。就像刚才讲的公积金项目，它是点对点的491个点完全是区块链系统，而下面公积金系统又是传统的网络应用系统，是这么构起来，区块链在上面，下面有其他，反过来也可以把区块链系统嵌入传统系统，链上链下数据协同需求可能会特别重要。要求链上链下数据，如果能够协同就能确保关联性和一致性，这个非常重要。

大家可以查询文献，目前国内外对链上链下数据协同的技术才刚刚起步，也有一些协同研究，包括侧链和状态通道，为了提高性能和计算能力。这有点像云计算和边缘计算。现在数据是算好，起码区块链上

要给别的数据留下通道。跨链技术，为了增加链与链之间互操作性和可扩展性。链下计算，提高数据的隐私保护能力。这也是非常重要的，链上链下连接不能光考虑链上，链下系统如何对接，数据隐私保护也要对接。还有链下存储也是一样，原来系统存储怎样，这些都应该作为研究。

链上链下数据协同技术的4大发展方向

它的发展方向，标准的、融合区块链链上和链下数据协同的模型框架，目前需要研究以下技术点：

1.大规模高性能点对点网络。围绕区块链应用，原来大规模点对点的网络，这个才是最重要，因为区块链本来就是点对点传输的。如果说网络技术没有突破，区块链系统性能是很难提升。

2.模块化安全密码学协议。本来区块链就是分布式加上密码。安全密码学协议模块化，区块链子系统嵌入不同的，模块化安全密码学协议也是研究方面。

3. 高性能可编程计算引擎。我们希望用户不同的智能合约用不同的编程语言来编，既然用不同的编程语言，那你就需要高性能可编程计算引擎。

4. 可定义的数据分发协议。

这些都应该是链上链下数据协同的发展方向。

目前来说也是不错的，我们有过一个中间实验，现在基本上可以提供国产、自主、可控，完善的中国国米密算法支持，提供系统的链上链下协同服务技术栈，不能说有了一个标准框架，慢慢提供很多技术服务栈，已上线服务包括：大规模可信存储、集群节点数量可达数万节点。在中国移动做过实验。我们的团队希望在现有技术下，能不能在数量上，曾经做过数万节点，也有支持智能合约跨链互操作的通用跨链服务。“数据可用不可见”数据共享都已经初步实现，但是无论如何现在技术还远远不够。我觉得还是有很长的路要走，所以区块链的技术我觉得仅仅是开始，不仅是每个单点技术，还有整个系统。

区块链的监管技术

最后我想谈谈区块链监管，区块链的监管技术是非常重要的，就像我前面讲到的，尤其是中国大规模应用上，区块链项目上了以后，你没

有好的监管，谁都不敢冒这个风险。有一句话就说“没有一个好的监管，就像马路上没有站上一个交警，或者说没有红绿灯。”你觉得自己最好不要警察，最好不要红绿灯，车子可以开得很快，事实上是不行的。监管技术的重要性大家都知道，有一个“北大岳昕”事件被写入以太坊，也不能篡改，怎么办呢？有人把数据搞下来到处发。公有链已经成为新媒体的传播媒介，因为公有链本身具有去中心化、不可篡改、不可删除、低成本的特点。我记得有人算过，在“北大岳昕”把几条消息放在以太坊，好像才花了0.17美元的价格，具体是不是价格我想起来，但是非常便宜的价格。利用区块链去传播有害信息、网络谣言和煽动性、攻击性信息，会给区块链技术的产业布局和发展带来不利影响，会影响我们，这也是非常重要的。本身公链会给监管部门带来很大的挑战。

任何一个好的技术或者工具都需要被正确予以使用，才能发挥最大的价值，这就对区块链监管提出了更高的要求。

我们除了研究区块链技术本身外，也许我们需要真正有一个很好的方向。我们来研究区块链如何监管，所谓的安全，区块链的安全最重要是区块链系统的安全，防攻击等，除此以外，区块链的内容，公有链已经成为传播媒介，别的有没有可能呢？类似于“北大岳昕”的意识形态、内容监管也是需要，是不是可以利用我们的技术呢。

2019年网信办去了《区块链信息服务管理规定》，我们学习了这个规定，以及跟网信办交流感觉到区块链发展有两方面，一是国内大规模应用要用区块链赋能经济建设，主要是用联盟链，它的监管相对可控，它对安全的挑战等都比较好。但是我们也应该支持公链技术的发展，参与国际竞争，这也是非常重要的。

目前虽然区块链监管已经初见成效，今年已经公布了第一批197个区块链信息服务备案编号，**但是监管的道路还是非常长，目前区块链监管技术发展趋势有以下几点：**

1. 区块链节点的追踪与可视化。
2. 联盟链穿透式监管技术。
3. 公链主动发现与探测技术。
4. 以链治链的体系结构及标准。

只有提供了技术的解决方案，而且相对可靠，无非是程度差一点，只有这样才能在实际应用中才有可能上区块链这个技术，区块链监管这个事非常重要。我们需要在座教授要研究一下，为监管部门提供一些可监管的解决方案，这个技术应该是非常重要的。

小结

最后小结一下，根据我们目前中国的区块链发展，包括对比国际，中国区块链联盟链还有很多事情要做，联盟链底层平台核心是三大部分，都应该在这上面做研究，一是高性能。随着高频应用，随着节点数增长是非常重要。二是可用性。可用性就是交互，你的编程方便，可以动态热备份，随意插入、删除。三是安全隐私。这里包括密码编码，包括物理隔离等等技术。

链上链下数据协同技术是未来发展的重要方向，只有这样我们才能赋能各个行业，工业、农业等等，现在系统都在，如何有机结合起来，数据协同技术应该是非常重要的。这还涉及到区块链技术怎么样结合大数据、人工智能、5G技术，都需要有数据协同技术。

我们也要研究区块链的监管技术，这应该是区块链健康和可持续发展的关键之一。