“区块链技术”系列交流会
——区块链在金融及医疗领域概况与展望

会议介绍

本周五我们在上海举办了“区块链技术”系列交流会。主讲嘉宾龚鸣就区块链技术，区块链技术在金融、银行、医疗、公证、通信、物联网等领域国内外的现状及未来发展等方面分享了经验和判断。

倪恺灏
021-51167219
ani@cebm.com.cn

纪要摘要

区块链（Blockchain）技术就是一种全民参与记账的一种技术方式，通过这种方式，数据就会变得非常的安全，因为篡改单节点的数据是没有任何意义的，从而区块链技术能在很多领域能显著降低成本和提升效率。

在通信领域，通过区块链技术发信息的方式是每次发给全网的所有人，但是只有那个有私钥的人才能解密打开信件。人类通信要求从“可以做到”转变为“可以安全地做到”。这会导致很多系统的设计思想发生改变，从最短最快到最安全。

在跨国慈善领域，区块链技术可以实现一个全新的跨国小额快速捐赠市场，而且可以解决慈善资金的监管问题，慈善金额有可能因此达到现在慈善金额的5-10 倍。

在股权/有价证券交易所领域，通过区块链技术可以实现24小时不中断运作，所有人可以在区中心化的全球交易平台上自由竞价完成交易，而撮合也是在去中心化的。好处是公信力强，没有人可以作弊；而且简便和快捷。

在银行领域，区块链可以帮助银行避免单点错误的风险以减少审查和审计的支出。区块链技术可以显著的帮助银行提高安全性并降低成本。

在投票领域，在股东投票时，可以解决跨国股东投票的公正性问题。

1. 什么是“区块链技术”

区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接（chain）下一个数据库块。

通俗一点来说，区块链技术就是一种全民参与记账的一种技术方式。所以在过去，就是使用一堆中心化的服务器来记账，记账都是很中心化的，由公司内部的人来记账，例如支付宝就由阿里巴巴内部的人去记账。但现在的区块链系统中，系统中每个人都可以参与记账。每一个时间段内更新一次数据，系统会评判该时间段内记账最快最好的人，把他记录的内容写到账本，并将账本内容发给系统内所有的其他人进行备份。因此，这时候这些数据就会变得非常的安全，因为篡改单节点的数据是没有任何意义的，这是区块链最初也是最重要的记账模式。篡改者需要同时修改超过半数的系统节点数据才能真正的篡改数据，当系统节点有上千上万个且分布在全球各地时时，这种篡改，代价极高因此几乎不可能。

另一个例证是比特币，比特币是开源的，比特币运行到现在已经超过7年的时间，总市值约30-40亿美元，全球无数的黑客尝试攻击比特币，但是直到今天为止没有出现过交易错误，比特币被盗或者双方对不上等问题，因此比特币的区块链网络仍然被证明是一个安全可靠的系统。

区块链技术可以做到的去中介化，最大的中介就是支付宝，即阿里巴巴。所有的中介都是靠信用来背书。而阿里巴巴最大的问题就是信用无法跨国，作为价值传递来说，信用传递是一个政治问题。而克服这个信用问题最好的办法就是利用数学，全球各地无论文化是什么样的，数学都是一样的。通过一种开源的数学算法来作为背书，可以构建整个区块链的系统。区块链的分布式去中心化技术算法解决了拜占庭将军问题，也就是在双方可能有恶意的情况下，双方完成价值的可信交换。区块链技术可以对以安全性和信任信用要求极高的系统，有非常好的背书。

2. 区块链投资增长趋势

2015年下半年开始区块链项目一下子投资增多了，全球主要金融机构都参与投资了区块链。主要的开端是以经济学人认为区块链技术会在各个层面上非常深远的影响人类社会这篇文章开始，把以国家信任为中心转移到利用以区块链为中心。国外大部分的区块链技术布局都是从2014年初就开始筹备了，由此我们可以得出我国的区块链技术大约晚了1-2年的时间。

3. 通信领域的应用

通信领域是最早的区块链应用之一。传统的通信程序都是考虑如何用最短的时间和路径把程序传给要传的人。但是在完成了快以后，现在我们可以有更高的要求，那就是安全。例如基于区块链技术的Bitmessage聊天软件，发信息的方式是每次发给全网的所有人，但是只有那个有私钥的人

才能解密打开信件。也就是说，跟踪信件的路径是没有意义的，因为所有人都收到了，因此这可以解决路径的安全问题。这个思想在过去90年代不可能的，因为以前的带宽和运算能力是达不到区块链的要求的。区块链到今天才被使用，是有软硬件基础的。人类通信要求从“可以做到”转变为“可以安全地做到”。这会导致很多系统的设计思想发生改变，从最短最快到最安全。这是对传统一个重大的改变。

4. 域名管理系统

传统的域名管理系统是由ICANN分配给不同的机构，但这样的树状结构是非常不安全的尤其是像中国这种不控制任何根服务器的国家，出于国家安全的考虑这样还是有很多的问题。有人基于区块链技术写了Namecoin，以分布式区块链的方式进行管理，除非能摧毁大部分节点。第二代域名的管理系统，从传统的中心化管理系统转变为更安全的去中心化的域名管理，使之更安全也更有效率。

5. 公证领域

Factom公司在区块链是一个有名的公司，可以把文件和信息保存在区块链上。为了防止信息急速膨胀，Factom在比特币的区块链上的做了解决方案。Factom受联合国的要求，为洪都拉斯做一个房地产权的保管的项目，因为洪都拉斯政府本身管理的问题，70%以上的资料混乱或者遗失。比较有意思的是，房地产权的保管一直都是政府做的事情，但是由于区块链技术，无论洪都拉斯政府的政局动荡或者Factom公司倒闭了等等，都不会影响这些房地产权数据，因为这些数据是独立保存区块链上的，是独立的更有信任的。类似的，和Factom合作的还有希腊政府。Factom在数据保存和公证领域技术非常强。

另一个公证领域的是Monegraph，做的是知识产权（国内说的IP）的保存。把所有艺术家的艺术品，甚至仅仅是一张刚拍的照片，快速的通过区块链在线认证，并且可以在线交易买卖或者出租。这是一个很有趣的应用，传统的知识产权保护不好是因为保护知识的成本太高了。区块链具有不可更改性，数学指纹有非常强的公信力并且有法律效应。可以把公证和知识产权的办理变为流程化的低成本甚至零成本的事情。如果任何一个普通人发的每一个微博、每一张照片可以轻易的证明这是谁的知识产权，这会诞生一个空前的全球微知识产权交易市场。你的所有的东西都可以交易，因为你可以证明这个知识产权的所有权。这就是为什么Factom等公司受到追捧，现在已经有30-40家企业在做着一块领域，未来的公证会像买机票加2元买一份保险一样简单。因此区块链技术可能会引发一个空前的全球微知识产权交易市场。

6.医疗领域

有一部分业内人士认为医疗是区块链技术自金融后第二大的应用。因为现在医疗档案的保管一直解决不好，因为现在医疗资料如身高体重血糖血压等信息泄露了不是很大的问题，但是当我们资料采集越来越全，很多资料泄露会产生很大的问题，最典型的例子就是指纹。如果这些资料出现大规模的泄露，会出现非常深远而庞大的影响。会比苹果的明星私人照片泄露还要大得多，如果

连苹果这样闭源的系统数据库都可以泄露，其他中心化的数据库其实都有很严重的潜在问题。还有就是基因图谱，如果个人的基因数据泄露会产生很严重的未知的灾难性的影响。中心化的数据库都是很难确保其安全性的，很多业内人士认为区块链是人类现在能想到的唯一的解决方案。

区块链有三个对医疗很重要的优点：1，高冗余，因为备份多，难以被摧毁。2，区块链的数据不能被篡改，这个在医疗科研上有很重要的作用。3，区块链能做到多私钥的复杂权限保管，可以设置只有一个或者多个人能打开，可以设置复杂的时间上和多把私钥才能打开的设置。医疗特别适合多权限的保管，病人、护士、医生都是应该不一样的，而且最好读取权限还有时间上的限制，过了某个治疗时间段只有某个治疗医生才能读取。

目前，Factom和Healthnatica的公司在合作，Philips Health和区块链资料保管Tierion也达成了协议。大部分是进行基因的保管，因为区块链是我们能想到的最安全的资料保管方法。

7. 储存领域

对于存储领域，可以做一个去中心化的，现在进展最快的公司是STORJ。因为云存储是一个未来有巨大前景的市场，利用去中心化的存储领域这样可以用每一个人手里闲置的运算能力帮助存储。闲置的运算和储存能力可以以此来获得收益，由此可以提供非常廉价的云存储节点。这些节点的成本会远低于现在市场上云存储所用的专职的服务器成本，而且非常安全，另一个优势就是政府封锁不掉。

8.供应链和物联网

IBM和三星在最初参与了以太坊，这是区块链非常基础的项目，类似于区块链领域的Windows。以太坊在一开始就融资了约1800万美元。IBM和三星在以太坊上搭建了物联网的系统，业内人士认为区块链会是物联网非常好的一个解决方案，因为Internet是一个信息传输的攻击而不是价值传输的攻击。信息传输的问题是有不确定性的，有的时候发不到，例如电子邮件有时候跨网络或者跨国界就可能出现信息收不到的情况。而物联网是不允许出现这样的情况的，尤其是车联网，且信息绝不能被篡改。而且物联网需要在恶劣的环境下，或者被攻击的环境下，准确无误的传递信息。只要有某些节点存在，就可以准确的传达信息。

另一个例子是Skuchain，利用区块链技术可以解决假货的问题，具体来说可以解决某个葡萄酒品牌年产1万瓶却在中国销售了10万瓶的情况。当每一个正品嵌入区块链芯片或者通过区块链二维码来跟踪时，任何人都无法作弊，而且所有的信息都可以在区块链上进行跟踪，从生产商经销商代理商等都能查到。国内最一线的一些技术公司在跟全球的一线奢侈品厂商也在做同样的事情，一线奢侈品厂商也在做基于区块链的供应链系统。国外有个公司在做钻石的基于区块链的供应链系统。能通过基于区块链跟踪所有钻石的供应链信息。通过供应链可以低成本且高效的解决跨国的供应链信任问题。

9.投票领域

在政治大选投票时，有的投票机不准，或者有些地区投票存在不信任的问题。除了大选投票，还有一块比较重要的是股东投票，这个技术纳斯达克已经在使用。区块链技术应用在股东投票时，可以解决跨国股东投票的公正性问题，这是纳斯达克非常重视的一点。

10.纳斯达克私人股权市场 Linq

现在有的小公司不愿意太早IPO成为公众的公司，造成现在独角兽越来越多。在IPO之前，这些公司还是有少量的私人股权交易需求。在符合SEC的监管下，由纳斯达克推出了去中心化的区块链技术交易所Linq。到今天，有几个初创公司在上面交易了，纳斯达克的目的是希望其他交易所也能加入到使用区块链技术的行列中来。

11.股权/有价证券交易所领域

传统的IPO流程，先审核，再负责发行和交易。区块链技术公司Bitshare则是一个任何人可以发行任何有价证券的平台，通过区块链技术可以实现24小时不中断运作，所有人可以在去中心化的交易平台上自由竞价完成交易，而撮合也是在去中心化的。其好处是公信力强，没有人可以作弊；而且简便和快捷，没有国家界限。区块链技术的证券交易可以规避法律问题，因为所有国家的证券交易所都是需要牌照的，而一个全球化的区块链交易所则可以直接在全球范围内进行交易。Bitshare每秒可以达到10万笔交易已经非常接近于一个传统的交易所；即使在恶劣情况下，Bitshare仍然能完成数千笔每秒的交易。SEC在近期批准了美国上市电商Overstock将自己公司的股票放在Overstock自己的区块链技术交易平台上进行交易。美国已经在区块链技术的证券交易商做了很多的探索，一旦区块链技术的证券交易做大，意味着这可能成为真正意义上的全球交易所。区块链技术的交易平台可以跨过所有的法律障碍来完成交易。

12.小蚁股权登记

这是一个中国人做的项目，解决了如何证明该资产在法律上是该出售人的，且证明在该股权资产在法律上受到保障。小蚁股权登记通过数字签名法的CE证书来证明出售人拥有该公司的虚拟股票。这个项目从一开始就众筹了不少钱，可以在符合现行法律法规下解决产权证明。使用区块链技术的很多地下金融交易，慢慢的能浮出水面且能符合金融监管。区块链技术可能让传统金融项目变得更有效率，流动性更高，可以跨国的交易。

13．跨国慈善

区块链技术最好的是可以公开透明，展现给每个人看钱的来源和去向，可以弥补国内慈善在透明度和可信度上的欠缺。通过区块链技术，可能会开创跨国小额快速捐赠市场，因为之前跨国捐赠1美元成本会要超过5美元。通过市场分析，如果跨国小额快速捐赠市场可以通过区块链技术实现，慈善金额有可能因为这些涓涓细流，达到现在慈善金额的5-10 倍。现在国内有公募资质的正在试图开创这块市场，这个对于慈善行业可以形成一个颠覆性变化。

14．保险管理

保险的运作本质是，把投保人的资金放在一起组成一个资金池，一旦有投保人发生了不幸，资金池会将部分资金按约定给与该投保人。这个运作本身可以通过区块链技术的编程来实现，这样的好处就是可以极大的减少保险的所需要的成本。保险的成本非常高，主要产生在销售和保险公司的日常支出。只要相信区块链技术不能作弊，可以在保险业极大的降低公信力成本，这样可以大大提升保险业的效率。

15．R3区块链联盟合作银行扩展到42家

R3是一个区块链技术的技术公司，提出了区块链联盟，所有全世界跨国大银行可以加入。至今，全球除了中国的跨国大银行都加入了R3。SWIFT协议由于传统原因，导致跨国结算清算时间很长，一般来说资金电汇按天来结算，而R3区块链联盟可以实现银行间的跨国准时清算。有可能会成为未来的国际清算标准。在跟央行沟通后，中国的央行计划是未来拿出自己的方案，而不是加入其他国家之间的联盟。R3有可能会成为国际间的支付宝。

16．欧洲区块链集团

银行很大的一个风险是单点错误，典型例子是巴林银行，因为一个交易员作假虚报，最终导致整个巴林银行破产清算。银行可以做得就是更严格的审查和审计，而造成的银行的经营成本越来越高。另一方面，银行业也面对了互联网金融的直接竞争。如果使用区块链可以从根本上避免单点错误的发生，任何细微的造假系统会马上识别，进而降低审查和审计成本。有报告称，如果全球银行都使用区块链技术，可以每年为全球的银行省下200多亿美元的成本。

德勤24个月前开始做区块链技术的研究，并开发了自己的区块链的开发平台，并为客户提供区块链技术的技术服务和技术方案。在2015年，德勤仅仅在区块链的咨询业务就完成了1亿多美元的营业额。近2年，欧美很多跨国公司对于区块链技术很感兴趣，已经领先中国一个身位。

17．银行领域

银行不希望系统太过开放，区块链并不是必须要完全公开的，可以通过节点的控制达成银行间的私链。并且可以通过区块链的智能合约，在银行的每一个节点安全的运行。现行的技术来看，未来银行都是会通过私链来完成业务。某些节点是公众可以允许访问的，某些节点需要读取权限只对部分人士或者内部人士开放。区块链现在变得越来越复杂，以完成更复杂的任务，这是区块链的一个发展趋势。

汇丰银行的报告称，央行未来可以通过区块链技术来发行货币。例如政府要实行量化宽松，央行可以低成本且精确的发放到每个人的帐户，也可以查到每一笔钱的流转。并且可以通过智能合约，可以在钱上设定条件。例如，这笔钱必须进入农业，则这笔钱的预设程序限制了这笔钱只能流向农业，在发放之前就能写成合约。未来的金融发展的必然方向就是可编程金融，未来可编程

金融的一个重要实现手段就是通过区块链技术来完成。

在跟央行讨论后，得到的反馈是在很多区域会有很大的用武之地，例如可以在新疆做中亚的跨国结算中心，也可以做到金融反恐，可以精确控制整个中亚地区的资金流向。

18．Coinbase发行了首张可以在美国使用的比特币借记卡

Coinbase是美国的比特币钱包，拿到了美国25个州的牌照，可以在这些州使用并提出美元。美国是一个金融监管很严的国家，但是有越来越多的州可以使用这张卡。另一个意义则是，比特币是一个全球货币，这张卡对全球金融的影响力会越来越大。

19．总结

区块链技术本质上来说是一个大规模协作工具，它首次使用纯技术方式让价值转移成为可能。并延续了互联网去中心化和去中介化的趋势，已经并将终究深刻改变我们这个世界。区块链技术可以在有可能忧恶意攻击环境下的互信，从信息转移转变到价值转移。区块链技术能在很多领域显著降低成本和提升效率。

近期报告

2016年01月15日 莫尼塔国际宏观：2016全球经济，通胀领衔，美元淡出
2016年01月11日 先进制造观察：CES自动驾驶：Mobileye和Velodyne引领软硬件升级
2016年01月08日 七问人民币汇率
2016年01月04日 市场快评：熔断机制触发，新年首日提早收盘
2016年01月04日 普林格技术勘市：上证可能开启中级调整
2015年12月31日 12月草根调研：中观需求年末放量，地产投资需求的上升值得关注
2015年12月31日 航运调研：久旱逢甘霖，年末旺季临
2015年12月31日 钢铁调研：钢材价格短暂回升，钢铁行业“去产能”进入发力期
2015年12月31日 地产调研：12月投资性购房现身，预计节前平稳向好
2015年12月30日 策略观察：这个冬春季独有的两个特征
2015年12月29日 市场情绪观察：情绪总体谨慎，主要概念均处调整期
2015年12月22日 中央经济工作会议点评：围绕“三去一补”，布局结构改革
2015年12月21日 周度市场情绪观察
2015年12月18日 国际快评：前波士顿联储银行主席点评加息：后续决策仍然路径依赖
2015年12月17日 国际宏观：12月FOMC快评
2015年12月03日 11月草根调研：总需求弱势不改，汽车行业高歌前行

免责声明

本研究报告中所提供的信息仅供参考。报告根据国际和行业通行的准则，以合法渠道获得这些信息，尽可能保证可靠、准确和完整，但并不保证报告所述信息的准确性和完整性。本报告不能作为投资研究决策的依据，不能作为道义的、责任的和法律的依据或者凭证，无论是否已经明示或者暗示。

上海 (总部)

地址：上海市浦东新区银城中路168号
上海银行大厦21楼
邮编:200120
电话：+86 21 5116 7173
传真：+86 21 5116 5116

北京

地址：北京市西城区西直门外大街1号
西环广场T3座7层B1-B6创新商务中心
1801室
邮编：100044
电话：+86 10 8104 8010
传真：+86 10 8104 8009

纽约

地址：纽约市曼哈顿区麦迪逊大道295
号1232
邮编：10017
电话：+1 212 809 8800
传真：+1 212 809 8801

http://www.cebm.com.cn
Email:cebmservice@cebm.com.cn