

2016-2-24


行业研究(点评报告)


 评级 **看好** **维持**

信息技术服务行业

区块链专家电话研讨会议纪要


分析师 马先文


 862765799815

 maxw@cjsc.com.cn


执业证书编号: S0490511060001

联系人 郭鹏

 02765799815

 guopeng2@cjsc.com.cn

联系人 杨靖凤

 (8621) 68751636

 yangjf@cjsc.com.cn

报告要点

■ 事件描述

2015 年下半年以来,“区块链”技术迅速走红,其去中心化、去信任的机制得到全球市场的认同,并有望成为下一代价值互联网的基础协议。多国央行、各大交易所、国际投行、IT 巨头纷纷涌入,数字货币、金融资产交易、资金清算、智能协议、知识产权、物联网等应用领域不胜枚举。

本研讨会从全球的视野,详细介绍了区块链的内在机制、技术原理、应用领域和商业模式,剖析了传统金融公司积极尝试区块链技术的深层次原因,并介绍了国际巨头、创业企业的进展。同时,比特币作为区块链技术最成熟的应用,已具备完善的生态,近期香港的圆桌会议已在区块扩容、隔离验证等技术领域达成共识,本研讨会对其未来发展前景做出了展望和剖析。

市场表现对比图(近 12 个月)



资料来源: Wind

相关研究

区块链专家电话研讨会纪要

(一) 区块链

1、内在机制和技术原理

区块链是以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，本质上是一种全民记账方式，也称作分布式账本技术。任何计算机网络后面都有一个中心化的数据库，谁控制谁维护。比如阿里巴巴，淘宝就需要阿里团队维护，微信就有腾讯团队维护。如果把数据库看做一个大账本的话，所有的数据库都是以中心化的方式维护这个账本的，但是区块链系统，每个节点参与记账，一段时间系统会更新账本，判断时间段内记录最快最好的人，把他记录的内容写到账本上，成为一个为 block，然后把账本发给系统内其他人备份，这就是区块链技术也即分布式账本技术，他以牺牲一点效率基础上获得极大的安全性。**首先没有中心**，系统无法摧毁也就更安全，每个节点都是系统的一部分，节点权利对等，摧毁部分节点不会对系统产生影响。**其次是不能作弊**，除非能控制系统内大量用户的电脑，大批量修改别人账本，否则的话少量的修改会被系统认为是无效的，少量不一致的账本会被自动忽略，系统节点越来越多，系统也就越来越安全，越稳固。这种方式的系统安全性将远大于中心化的形式。

区块链最早是从比特币而来，比特币是由中本聪发明的，比特币主要是用到的三个技术：

- 1、共识的算法机制
- 2、非对称的公私钥的算法
- 3、去中心化的分布式算法

这些算法很早就存在，并不是中本聪发明的，都已经很成熟了，中本聪巧妙地将其运用的一起。中本聪的白皮书中并没有提到 blockchain（区块链），但是比特币在没有中心化的监管机构运营的情况下，良好运行了运行六七年，并没有发生过系统的崩溃和一笔错账。于是就有人认为比特币背后的技术是值得关注的，这个技术可以用到其他方面，抽象出来，这就是就是 blockchain。**区块链 1.0 时代，也即是数字货币时代**，blockchain 是开源的，比特币是 blockchain 的第一个应用，人们把它修改后可以变成其他货币，前后产生了数千种的货币，到现在还在运行的大概还有六七百种。**区块链 2.0 时代，把这项技术再抽象出来**，运用到金融领域以外的其他方面，比如交易所，保险，基金，股权投资，这些都可以用区块链技术开发。**区块链 3.0 时代，把区块链应用到更广泛的领域**，而不局限于金融领域，比如公正，医疗，投票，治理博彩，物联网等领域都有很多应用。

大多数人对区块链的了解都是在 2015 年下半年，当时区块链呈现爆发式增长，各种新闻事件层出不穷，其中最有标志性的新闻是经济学人杂志封面文章，它刊登了关于区块链的文章：《信任的机器》，这篇文章阐述了区块链的运作过程和行业发展现状，他认为这项技术是未来人类信任的基石，并将深刻地改变人类社会运作方式。之后就有非常的金融巨头都参与到相关项目中去，但是一些项目的细节，都是在 2014 年开始酝酿布局，

现在才开始浮出水面，预计 2016 将看到更多项目，包括央行 14 年开始调研数字货币相关内容，并将发行数字货币定为战略目标，更多相关动作会慢慢可以看到。

2、应用领域和商业模式

1、公证领域：factom 是非常有名美国公司，它主要的核心是通过区块链技术把文档资料保存在比特币区块链上或侧链上，这样可以对文档形成一个无篡改的保管，目前在联合国牵线下帮洪都拉斯做房地产资料保管项目。一般这些数据都是由政府来保管，但是为什么会交给一个公司尤其是一个美国公司来保管，这是因为如果这些数据是保存在区块链上，以后不管洪都拉斯政府出现政权更替或 factom 公司本身被摧毁，也不会影响数据安全性和可靠性，从这一点来看，区块链信用可以代替国家的信用，甚至已经超过了主权政府的信用，也许将来会获得更多的承认。目前希腊政府也在寻求 factom 合作。中国有一些公司在和 factom 合作，在做智慧城市相关的一些事情。

2、知识产权领域：美国知识产权的律师事务所做的一个叫 Monegraph 的应用。它上面可以把每个人上传的照片通过在区块链上留下数字指纹，来证明数码信息所有权，并可以在应用上进行所有权的交易。随着公证变得越来越简单，成本越来越低，这样的话知识产权保护变得越来越便捷，也许有一天我们说的每句话，每条微博，发的每一条微信，每一张照片都可以在区块链上非常低成本甚至是零成本的进行所有权登记。那么有可能诞生一个空前大的知识产权交易市场，空前的机会。由此我们可以无需政府背书这样一个过程，可以使知识产权的保护和交易达到一个全新的高度。

3、医疗领域：欧美普遍认为区块链在医疗上的应用是仅次于金融上的最大的一个应用，目前一个很大的问题是个人医疗数据保管，随着个人健康数据越来越多，数据泄露有可能是灾难性的。指尤其是比如说个人的血糖血压，指纹，基因等核心数据。现在就像苹果这么专业的 IT 公司都会产生数据的泄露，更别说其他中心化的保管方式了。随着区块链的出现，大家认为也许区块链是人类能想到的最好的解决方案，这是因为，首先，我们能想到的就是区块链有很高的冗余性，每个节点都有账户的备份，部分节点摧毁不会影响系统安全性；第二，就是他的数据是无法被篡改的，任何的篡改都会被系统识别并认定无效；另外，就是它可以对每一个病例进行复杂权限管理，这意味着你的病例由医生或护士同时拥有一把私钥进行资料管理，因为区块链有一个很有意思的特性就是 smart contract（智能合同）的属性，它可以对每一个私钥变成，形成一个非常复杂的特性，比如说只能当打针的时候护士才能查看你的某些数据，通过这种方式不会因为单把私钥的丢失而导致整个数据库的崩溃。这就是为什么有些人会认为区块链会非常好的解决个人医疗数据的保管。首先我们看到，飞利浦 health 发布了他的第一个区块链项目，但是他并没有透露太多的细节，他的合作对象是 Tierion，这家公司主要是做数字资料的保管，由此可以推断这个项目是和档案保管相关的，另外还有一个叫 gem 公司正在为医疗相关的行业提供解决方案。

4、供应链和物联网：IBM 在这方面做了很多事情，早在 2014 年就与三星合作开发了 ADEPT，这是一个基于比特币区块链技术的物联网系统。IBM 在物联网上投入巨大，他的全球研究所也在全面进军区块链，在物联网 IBM 认为区块链有绝佳的应用，因为物联网对安全性，防篡改性，冗余性都要求很高。区块链可以在这上面有非常大的用武之地，像 Internet 的话就相对来说很弱了。在物联网上还有一个叫 Slock.it 的项目很有趣，主要是基于区块链可以控制门锁，每个人可以对自己的门锁通过公钥和私钥进行控制，这是一个基于以太坊的项目。

5、股权交易：引起关注的是纳斯达克这样一个大的集团，是金融系统最早进入区块链的公司之一，2016 年在爱沙尼亚股票市场推出区块链投票系统，还宣布开发了私人股权交易市场，叫 linq，在这上面可以进行私人股权的交易。这个项目已经开始运行，大约有 6 家初创的公司在进行私人股权交易。纳斯达克在区块链方面压力非常大，因为它们做的最早，是可能会被淘汰掉的，现在也已经有很多基于区块链的去中心化的交易市场已经出现，而且该市场遍布全球，每个人都可以上面发布资产，进行交易。纳斯达克认为未来很有可能会是一个全球化的自由的一体化的资产交易平台，不如自己开始着手来做，所以它成为全球金融巨头里第一个推出可用的基于区块链的应用系统，该系统在去年 12 月份完成第一笔交易，目前还是在测试的状态。

此外，overstock 公司，作为一个美国的上市电商，开发了一套去中心化的基于区块链的交易系统，叫做 t0，你可以在 t0 上访问项目的内容，目前还在研发中，该公司一直希望可以通过这个系统击败华尔街，据公司最新季报披露，目前已在该项目投入八百万美元。去年 12 月份，SEC 正式批准了 overstock 可以在这个去中心化的区块链交易平台上发行自己的股票并进行买卖，这对 SEC 来说是非常大的一个进步。对于 SEC 来说此举可能也是想测试下去中心化的市场情况，还是在可控范围内，目前只是允许它可以在上面发行自己的股票，其他公司不可以，其他公司目前只是上面申请。类似这样的交易系统目前在美国已经有很多开始出现雏形，SEC 似乎也默认这种状态，并愿意让他们去尝试去中心化的市场能走多远。我们相信也许未来会出现全球性的基于区块链的快速的结算的资产交易市场。

6、实时清算：目前区块链的比较大的项目是 R3CEV 的区块链联盟。R3CEV 是美国一家初创公司，它的希望是能建立一个全球的实时结算清算系统，因为这个公司本身又比较大的游说能力，它 9 月创立，到 12 月份，不到三个月时间，全球有 42 家最大的金融机构都加入到它的区块链联盟中，基本都是我们耳熟能详的全球最大金融公司，比如桑塔德银行、花旗、高盛、德意志、汇丰、摩根大通、法国兴业银行、摩根斯坦利、瑞士银行、富国银行、包括野村证券，全部加入了，除了中国以外的全球性的金融决策机构都加入了这里，目标就是共同研制区块链的全球实时结算、清算系统。该项目进展比较快，目前已宣布会在以太坊进行测试。这次央行推出区块链，把发行数字货币来作为战略目标也是因为受到 R3CEV 公司的压力。如果 R3CEV 能够推出这样一个系统的话，有可能改变全球实时结算、清算的一个标准，对于没有加入的国家可能会被迫接受这一点。对于中国政府来说，基于国家金融安全的考虑可能会以其他方式与 R3CEV 联盟进行区块链的连接。同样在 R3CEV 成立不久，去年 11 月份，伦敦清算所、欧洲清算所、法国兴业银行和好几个大的金融集团，成立了一个集团代表欧洲的区块链联盟，主要研

究基于区块链的交易后的流程。这是目前两个比较大的区块链联盟来研究区块链的相关协议。

3、传统金融公司拥抱区块链的原因

1、降低成本：有越来越多的金融机构认为，它们内部也可以使用区块链的技术，使用区块链技术可以大幅度地降低成本，花旗银行发布了一份报告就是 2020 年前如果各大金融机构都使用区块链技术的话，每年能节省超过 200 亿美元的成本。很多人认为未来 20 年各大金融机构可能会把金融系统改造成基于区块链的，这是一个商机，这方面来说德勤相对走在最前面。德勤已经成立了一个叫做 rubix 的团队，里面有超过 150 位专家来为全球客户提供基于区块链的咨询服务，德勤在过去 24 个月里花费了很大力气在区块链上，这次央行的会议里也有德勤的团队参加，据说德勤在 2015 年的时候就在关于区块链的咨询服务上做了将近一亿美元的生意，所以它走的非常前面，已经开始赚钱了。

银行内部使用区块链系统就不是使用比特币的系统，更多的是一种称为私有链的系统，私有链不同于比特币，比特币是任何人打开电脑下载客户端都可以接入的，私有链则必须是经过允许的节点才可以参与整个系统，才能进行记账、下载账本等动作。通过私有链的方式可以使银行更加方便和安全地使用整个交易，整个系统对于银行来说会感到更加安全。私有链系统是不需要通过挖矿来进行的，不是所有的区块链都需要通过挖矿的方式，挖矿更多的是在比特币这样的环节里面，现在很多新的区块链系统不采用挖矿而是采用 POS 之类的。联盟链系统就是我们前面讲的 R3CEV 与全世界主要金融机构的合作，每个银行就作为节点来完成结算清算的流程。通过这种方式组建出来的区块链我们称之为联盟区块链系统。

2、可编程金融：汇丰银行出了一份报告，建议央行发行数字货币，原文是央行在量化宽松的时候使用区块链技术会变得更加透明和有效而不是传统的通过银行发放的方式。如果使用区块链技术发放人民币的话会非常方便地监督整个资金的流向，更重要的是可以比较容易地实现可编程货币和可编程金融。目前大多数银行机构都认为可编程货币和可编程金融是未来央行会发展的一个方向。**什么是可编程货币？区块链技术有一种特色叫做 smart contract，可以对资产进行编程，可以设定非常复杂的特性，可以设定这笔钱发给谁，什么时候发，可以进哪些账户，可以在不同的时间进入哪些节点，这都是可以通过预先的编程来实现的。**比如央行可以通过这种方式，发一笔钱给农村相关账户，它一旦设定好之后，不管底下做什么小动作，这笔钱也到不了其他的账户，因为所有都是通过系统自动完成，没有任何人有能力改变或篡改这个系统，这就是我们所说的可编程货币。可编程货币可以极大提高央行的监管能力和执行的效率。所有分布在区块链上的资金都可以让央行及时了解到，由此可以在政策制定上提供极大的便利性，因为可以随时查询整个资金的分布情况，这就是为什么很多央行对区块链非常有兴趣的原因。

3、反击互联网金融：我们发现对于区块链来说，大多数传统的金融公司非常欢欣鼓舞，纷纷加入，而传统的互联网金融的都保持沉默。我们很少看到 BAT 说区块链怎么样，经常看到摩根士丹利、瑞银、各国央行等谈论区块链技术，主要是因为传统金融在被互

互联网金融压制十年之后，终于觉得它们有武器可以进行反击了。通过区块链技术可以让它们像第三方支付一样非常准确地完成实时的结算和清算，特别是像 R3CEV 联盟这样的机构，如果真的可以实现全球市场的实时结算和清算，那么就会成为全球的支付宝，而且广度和深度也会远远超过支付宝。对此很多人认为区块链会使第三方支付成为附着性的产品，所以传统的金融机构对区块链表现出很大的兴趣和信心，反而互联网金融机构对此没有太多的表示。

4、国际巨头的动作

DTCC：是美国存款结算公司，是个超级巨头，每年结算超过上万亿美元，它发布了一份关于区块链的白皮书，叫做《拥抱颠覆》，对于区块链在结算清算上如何进行使用谈的比较多，有很多很好的思路来解决相关问题。

英国央行：对于区块链非常重视，可能是全球最重视区块链的央行。英国主要是使用 RTGS 进行结算的，叫做实时全额结算系统，每天结算的规模在五千亿英镑左右。2014 年 10 月 20 日这个系统崩溃了，中断服务长达九个小时，数百亿美元的交易被推迟。英国银行对此事件进行了一年的调查，认为它们需要更健壮的实时结算系统，所以英国央行在这方面的投资是史无前例的。英国央行专门成立了一个小组来研究区块链技术，并在今年年初发布了一份 88 页的报告，专门谈论如何使用区块链技术，报告里有一些有趣的案例，包括如何使用区块链应用在欧洲的智能电网，甚至用在濒危动物的保护上面，都谈的非常详细。同时英国央行还宣布正在寻找区块链技术的实习生，开始进行人才的笼络。目前，全球主要的央行在区块链技术上都保持相对开放的态度。

高盛、花旗：在美国也不断申请区块链技术的专利，去年高盛、花旗已经申请了比较多的专利，今年达沃斯，美国银行披露出他们已经申请了四十项关于区块链的专利，可以看出欧美的大多数公司都是专利先行来做这方面知识产权方面的准备。

Swift：由于 R3CEV 联盟是想做实时的结算和清算系统，是不需要中介就能完成。目前最大的中介是类似与 Swift 这样的机构，如果跳过 Swift 机构将极大地提升效率，而 Swift 也表示愿意拥抱区块链技术，并提出了自己的区块链路线图，会在 2016 年 1 月 1 日开始具体研究向区块链市场转变的方案，而且表示本身体量太大，希望大家能给他们更多的时间来研发。

IMF：国际货币基金组织拉加德，在这次达沃斯论坛上推出了第一篇关于区块链技术的研究报告，认为数字货币和区块链技术会对银行业有比较大的影响，建议银行金融机构相关人士去了解区块链技术和数字货币目前最新的进展。

DAH：Asset Holdings 想控股这个公司。DAH 目前 CEO 是 Blythe Masters，在华尔街非常有名，曾是摩根大通最年轻的高管，金融危机后迫于压力离开摩根大通，目前负责 DAH 这个公司。DAH 最近融资了 6000 万美元左右，有很多华尔街巨头纷纷投资这家公司，CEO 宣传要使用区块链来做金融衍生品。DAH 目前收购了好几家区块链的初创公司，并与 IBM、Linux 基金会打造了一个全新的项目叫做 Hyper Ledger，超级账本项目，是 IBM 全力投入来打造的项目。IBM 和 Linux 基金会目前是全球最大的开源社区，有庞大的技术人才。他们希望推出一金融行业实用的底层操作系统，底层区块链的操作平台。该项目刚刚开始展开，IBM 目前有超过两百家的公司正在报名，他们选择四十家合作伙伴共同开发项目。DAH 目前融资的 6000 万美元中有 1 千到一千五百万美元是澳

大利亚证券交易所来投资的，获得了大约百分之五的股份。澳大利亚证券交易所投资的原因是它正在寻找新的方案来打造全新的交易系统，2016 年工作方案之一就是选择更好的交易系统并会在 2016 年下半年公布选择的具体方案。

5、目前存在的问题

1、缺乏统一的技术标准：目前各种松散的比特币和乱七八糟的货币，还有各种其他的方案，比如以太坊或者超级账本这样的大项目，都没有统一标准，基本还是群雄争霸的状态，风险和机遇并存，确立一个好的标准将有助于行业的发展。

2、缺少更多可靠的实践数据：虽然比特币在过去 7 年运行良好，但是目前的区块链技术方案下，不能保证其并发数和承受能力用于现在金融系统每天上万亿美元数量级的交易。很多项目在测试不同的原型，但实践的数据还比较缺乏，需要进一步的积累。

3、替代成本高昂：传统的金融基础建设投资过高，已经超过上万亿甚至十万亿美元，要不要推翻重来还是个很大的问号。更多人还是希望区块链技术能和已有的金融基础设施紧密结合。但由于传统的中心化和区块链去中心化的架构还有比较大的区别，所以这种结合可能还面临很大的问题，需要进一步的探索。

4、人才缺乏：人才极度缺乏，特别是跨界的人才，即了解区块链技术也了解金融复合人才。更多金融方面的人士能加入到相关项目中，也许能更好促进区块链的发展。

总结：区块链从本质上来说是一种去中心化账本的技术解决方案，可以应用在非常多的行业。通过区块链可以延续互联网去中心化和去中介化的趋势，这是互联网不变的命题。目前有非常多的金融系统和机构已经投入到区块链的建设当中去，在 2016、2017 年可能可以看到更多国内相关项目。目前区块链技术是在非常初级的阶段，大约相当于互联网的 96、97 时代，很多东西才刚开始，未来将有更多的应用出现。

（二）比特币

1、比特币的发展历史

2008 年 10 月，中本聪发布了《比特币：一种点对点的电子现金系统》，通过区块链分布式交易总账解决数字货币的双重支付问题；

2009 年 1 月 3 日，比特币网络正式上线，中本聪挖到了第一个比特币；

2015 年下半年，区块链的技术引起了国内外的广泛关注，基于区块链的公证、结算和物联网等技术出现。

2、比特币产业链

比特币行业已经形成了挖矿、钱包、数据、区块链数据分析、交易和支付等完整生态链。

1、挖矿：占很大比重。目前比特币全网算力约 110P，中国比特币份额占全球的 70%，芯片生产主要是台积电的 28nm，台积电的 16nm 和三星的 14nm 预计在 3~4 月量产。

在下次减半前每天可挖到 3600 个比特币，按照 2500 元每个计算，每年毛利润在 32 亿元左右，其中电费占比约 1/3，另外需要支付矿工费用，矿工生产企业利润约 11 亿，国外部分公司基于区块浏览的大数据分析平台是未来的发展方向之一。

2、交易：较为活跃。目前比特币已形成了融资融券、P2P 借贷、期货等比较完善的系统，满足不同用户的需求，主要有 OKCoin、火币网等交易平台。平台以手续费、P2P 借贷等为盈利模式，基于比特币等数字货币的量化交易和无风险套利也已形成。此外媒体门户，论坛都为用户提供基础信息服务。比特币在全球小额支付、虚拟商品交易均取得了不错的市场份额。

3、区块扩容和隔离验证

近期比特币社区关于比特币的扩容产生了分歧。因为目前比特币区块大小是 1MB，由于用户规模的增加，每天的交易约为 24 万笔，就是每秒 2.8 笔。1MB 的大小理论上能容纳比特币的交易上限是 7 笔，但是由于多重签名等基础的使用，实际仅能支持每秒约 3 笔交易。区块平均大小在 0.8M 左右，网络阻塞情况时有发生，因此区块扩容刻不容缓。

区块扩容有两个主要方向，一是优化数据结构，使单位大小能容纳更多的交易，**第二个是直接增加区块的大小。**社区提出的第一个方案是首次调节区块大小到 8M，并每两年翻倍直到 8GB，但是超大区块设计需要有网络技术支持，目前通过最先进的技术手段可快速广播大概在 20MB 左右的区块，由于网络防火墙和延时，过大的区块会导致挖矿效率降低，影响比特币网络安全，该方案被否。

新开发团队推出了**隔离验证**，隔离验证是把原来交易中的签名部分单独拿出来放到另一个验证结构中，并不在区块内，主要目的在于改善比特币的数据结构。社区对隔离验证的分歧并不大，很大部分都认为隔离验证应该实行，分歧主要集中在上线时间安排上。一派认为隔离验证是非常复杂的技术，需要给与足够的时间和开发措施来保证区块的安全，因此短期内拒绝，另一派认为隔离验证可以使向下兼容软分叉来达到扩容效果，可优先执行。

在 2016 年的 2 月 21 日香港的比特币大会上，扩容达成一致。目前隔离验证对数据进行了优化扩展，修复了比特币交易的延迟问题，还增加了区块的数据大小。同意隔离验证以一种分叉的方式进行，预计 1~2 个月内发布，在隔离验证发布之后比特币整个社区开发统一，增加非验证数据到 2MB，然后在发布上述版本过后，社区才会在环境中布局隔离验证，声明发布后比特币价格大幅上涨。

（三）问答环节

1、以太坊怎么看？

以太坊和比特币不一样，以太坊想做一个区块链领域的基础的操作系统，定位不一样。现在很多区块链应用都要从头开发，就像在一个没有操作系统的手机里面开发 App，工作是比较繁琐的，以太坊是试图开发像手机领域的安卓系统，即一个基础的应用平台，

从而在上面搭建各种应用。目前大概有上百个应用在以太坊上面开发，微软 Azure 云航也在部署基于以太坊的区块链服务，类似于像 PAAS 一样的系统，称为 BAAS(blockchain as a service)，将其作为整个区块链的基础性的云服务平台，阿里云也在和以太坊合作，准备在阿里云上部署。从目前来看，以太坊可能是全球最大的区块链技术平台，竞争者目前就 IBM 的超级账本项目，超级账本项目也还没有很多东西，而以太坊已经开始进行测试，以后可能有更多基于以太坊的项目，R3 联盟第一次测试也会在以太坊上运行，以太坊有可能成为使用人数最多的技术平台。

2、区块链记账人的选择是很重要的一块，请您简单介绍下目前 POW、POS、DPOS 的不同？

比特币使用 pow 我觉得挺好的，也有很多人说浪费资源，个人觉得对于比特币的场景来说是有必要的。但是其他的区块链项目，可能会使用 pos、dpos，通过这种机制会比较大节省成本，不需要通过完全的算力竞争来实现。对于不要求提供安全性的东西，特别是在私有链情况下使用 pos、dpos 会更加容易实现。三者各有优缺点，目前市场也没有认为哪一个会绝对胜出，比如像以太坊使用的 pow+pos 混合体系也许是个不错的选择。大家可以根据不同的场景，选择不同的记账机制，来实现区块链的技术。

3、国内区块链的应用比较看好哪个方向，哪个领域会比较容易会有突破？

金融领域的应用，根据我参与的探讨和项目，可能发展会比较慢，毕竟金融是一个太庞大的东西，而且大家心里也没底能做成什么样子，其中最大的问题是有非常复杂的监管摆在面前，一项项解决监管的问题，解决各种法律法规的问题耗时巨大。

金融领域，票据曾认为是个非常好的场景，但是仔细探讨下来，还是有很多的限制在里面，这个关也没那么好闯。也许更多的是从非信用领域进行突破，包括医疗、认证、游戏，个人认为或许供应链和物联网方面会更容易一些，资产交易方面也许会更好一些。但其实技术路线选择有较大的偶然性，从这点来看，进行技术细节预测没有太大的意义。

4、比特币生态完善，但其中间也遇到一些问题（安全或政策方面），对比特币的价值和生态发展怎么看？

比特币现在处在一个扩展的关键节点，之前的区块扩容一直在争论，即技术路线之争，大家觉得要么比特币变成一个大的清算网络，要么把比特币做成一个带闪电网络的交易，在上面通过侧链技术，针对不同的领域做一个场景应用的发展。但是现在扩容还未落地，最后大家技术路线的选择还没有确定，可能还有一年多的时间选则路线，目前来看可能闪电网络包括侧链是大家比较看好的方向。

5、解释下侧链的问题。

比特币是一条链，在比特币之外形成一个侧链，锚定比特币区块链某个点，两个链之间可以进行一些数据交换。每条侧链可以针对一定应用场景，比如针对数据登记来做相应

数据的调整，并且每条侧链可以形成分支侧链，针对不同应用场景做自己的优化，跟比特币不同的链之间做数据交互，然后通过比特币区块链保证侧链的安全。

6、交易所高频的怎么实现？

不扩容每秒 3 比，闪电上千笔，侧链上会实施。

7、比特币是安全的，新兴的私链没验证，用户少，公有链会不会比联盟链和私链更好？

确实是最安全，但是比特币有限制，最早设计时没有涉及侧链，但是改造太慢。不如从头开发，难度大，但是进度会更快，但是私有链不是 pow 机制，私有制作弊成本很高，安全性不是大问题，比如 R3 区块链联盟的 42 家银行，谁作弊立即就知道了，所以不用比特币侧链也行。

8、区块链的银行联盟链可能没有央行的结算系统效率高，那区块链的优势是什么？

答：高频不能比但是结算上肯定区块链高。区块链可以做到实时结算，而目前的清算系统基本是 T+1、T+2、甚至 T+3，区块链计算能带来更高的透明度，更好的效率。

投资评级说明

| | | | |
|------|--|------------------|--|
| 行业评级 | 报告发布日后的 12 个月内行业股票指数的涨跌幅度相对同期沪深 300 指数的涨跌幅为基准，投资建议的评级标准为： | | |
| | 看 好： | 相对表现优于市场 | |
| | 中 性： | 相对表现与市场持平 | |
| | 看 淡： | 相对表现弱于市场 | |
| 公司评级 | 报告发布日后的 12 个月内公司的涨跌幅度相对同期沪深 300 指数的涨跌幅为基准，投资建议的评级标准为： | | |
| | 买 入： | 相对大盘涨幅大于 10% | |
| | 增 持： | 相对大盘涨幅在 5%~10%之间 | |
| | 中 性： | 相对大盘涨幅在-5%~5%之间 | |
| | 减 持： | 相对大盘涨幅小于-5% | |
| | 无投资评级： 由于我们无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，致使我们无法给出明确的投资评级。 | | |

联系我们

上海

浦东新区世纪大道 1589 号长泰国际金融大厦 21 楼（200122）
电话：021-68751100 传真：021-68751151

武汉

武汉市新华路特 8 号长江证券大厦 9 楼（430015）
传真：027-65799501

北京

西城区金融大街 17 号中国人寿中心 606 室（100032）
传真：021-68751791

深圳

深圳市福田区福华一路 6 号免税商务大厦 18 楼（518000）
传真：0755-82750808, 0755-82724740

重要声明

长江证券股份有限公司具有证券投资咨询业务资格，经营证券业务许可证编号：10060000。

本报告的作者是基于独立、客观、公正和审慎的原则制作本研究报告。本报告的信息均来源于公开资料，本公司对这些信息的准确性和完整性不作任何保证，也不保证所包含信息和建议不发生任何变更。本公司已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，不包含作者对证券价格涨跌或市场走势的确定性判断。报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可升可跌，过往表现不应作为日后的表现依据；在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告；本公司不保证本报告所含信息保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司及作者在自身所知知情范围内，与本报告中所评价或推荐的证券不存在法律法规要求披露或采取限制、静默措施的利益冲突。

本报告版权仅仅为本公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用须注明出处为长江证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。刊载或者转发本证券研究报告或者摘要的，应当注明本报告的发布人和发布日期，提示使用证券研究报告的风险。未经授权刊载或者转发本报告的，本公司将保留向其追究法律责任的权利。