智慧金融行业研究报告之一 —— Fintech 系列之区块链深度研究

从逻辑到价值

2016 年 11 月 2 日

投资要点

- **区块链的定义：基于信任机制的分布式数据库。**根据维基百科，区块链是：一个分布式数据库，它维持了一个（连续增长的不能被篡改和修订的）记录区块序列，每个区块都包含了一个连接到前一区块的时间戳。如果我们把数据库假设成一本账本，读写数据库就是一种记账行为：**（1）记账，**系统在一段时间内找出记账最快最好的人、由这个人来记账，然后将账本的这一页信息发给全网其他每个节点，这也就相当于改变数据库记录；**（2）核对，**全网其他有效节点核对该区块记账的正确性，并且盖上时间戳，确认区块合法；**（3）形成单链，**即在上一合法区块之后竞争下一个区块；**（4）存储，**账簿是分区块存储的，随着交易的增加，新的数据块会附加到已存在的链上，形成链状结构；**（5）备份，**每一个参与交易者都是区块网络的节点，每个节点都有一份完整的公共账簿备份，也就是分布式账本。
- **区块链的内涵：一套逻辑，一种表达，一份愿景。**我们认为区块链主要解决了如下问题：**（1）数据是否是可信任的？**信任的基础：一是共识机制，也就是数据被记账的动作是值得信任的；二是时间戳，也就是对存储数据的区块打上时间戳，使区块与区块之间形成一个连续性、环环相扣的诚实的数据记录，也就是数据库系统是值得信任的；**（2）可信任的数据怎样被存储和组织起来？**区块承担了存储功能，分布式节点保证网络中的每个参与者都有一套完整的账簿备份，也就是数据库系统是去中心、分布式的。因此我们认为区块链：**在执行端，**综合数学、密码学等学术基础；**在逻辑端，**致力于保持数据真实性、节点平等性等哲学逻辑。**所以说，区块链基于信任和平等的逻辑，是互联网思维的结构表达，是信息产生价值的美好愿景。**
- **短中期应用领域思考：信任领域，尤其是“重要不被信任中心”的信任方案。**我们认为，区块链解决信任问题的逻辑有效，但信任平等的代价是效率，因此在收益成本的权衡中，最直接的应用就是：解决重要的、不被信任中心的信任问题的应用，包括**公益项目、会计审计、食品安全、协会组织等领域，更宽泛的猜想是可以应用于金融领域的投资资金使用、债权管理、股权发行、征信等诸多领域。**
- **长期应用领域前瞻：规则领域，或将引发“组织”的重新设计。**平等，是互联网思维的直接落地，而当前组织的建立标准几乎不可能基于平等逻辑；从区块链隐含的平等逻辑出发，会对现代组织（中介、企业、政府）制度建立的标准产生巨大影响，包括：**各类中心/中介功能的替代（比如金融中介）；企业财务管理制度的改变（比如会计方法）；社会各类系统及体系的重新设计（比如支付体系）。**
- **终极结果猜想：价值标准的重构。**价值，在经济社会中体现的是使用价值，承担价值交换功能的是货币（一般等价物），支撑一般等价物交换的基础是主权，主权是一个最强大的中心。目前，比特币作为极小范围内的一般等价物，仍需要与主权货币保持信用关联。终极假设下，如果现实世界都通过区块链逻辑进行表达，记账（产生使用价值）的奖励就是一般等价物（记账获得的收益），那么价值认定的标准就会被重构，支撑一般等价物交换的基础就是基于共识机制的记账、而非主权或中心。
- **区块链应用的逻辑挑战和应用障碍：真实，还是共识？平等，还是效率？**区块链的魅力和挑战均在于其共识逻辑，也就是“不要求真实存在，只要超过 51%的共识”，这一逻辑需要回答：信任依据是基于少数派的理性抉择、还是基于大众的盲选？共识是否绝对值得信任？**实际应用方面的障碍则在于平等、效率和耗能的博弈。**
- **区块链增长空间前瞻：从逻辑到价值。**区块链并非常规意义上的新技术，我们理解为一种逻辑运用：**（1）行业空间来看，理论上奖励空间巨大，几乎所有领域都可被区块链的平等共识逻辑改造，增长空间就是改造当前组织模式的空间；**（2）收益成本分析显示，区块链逻辑所付出的成本就是高耗能，并且区块链主要解决信任、而目前很多中心化系统是更加值得信任的。**在探索未来的过程中：存在，即是最大意义；逻辑，是价值起源；价值，是追求者的目标实现。**本文梳理了为此“价值”探索的技术、方法和企业。

中信证券 CITIC SECURITIES

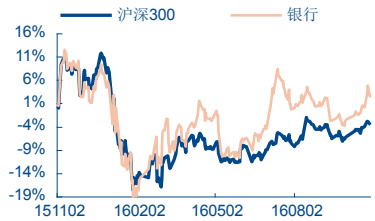
强于大市（维持）

中信证券研究部

肖斐斐
电话：0755-23835396
邮件：xff@citics.com
执业证书编号：S1010510120057

冉宇航
电话：0755-23835417
邮件：ranyh@citics.com
执业证书编号：S1010516100001

相对指数表现



资料来源：中信数量化投资分析系统

每日免费获取报告

每日推送文章内分享5+最新重磅报告，想要获取更多请关注孚百资本或加入孚百行研微信群

扫一扫二维码

或加微信公众号：fubaicapital关注孚百资本

入群方式：添加fubaicp为微信好友，备注行研报告

公众号

群管理员

目录

插图目录

表格目录

写在前面：为何理解区块链的逻辑很重要？

我们发现，区块链几乎是 Fintech 研究中最复杂的课题之一。

最初，我们运用惯常思路去研究模式及应用，发现不能很好把握要点。

直到我们开始关注区块链背后隐含的逻辑，问题才迎刃而解。

理解区块链的“平等+共识”逻辑，至关重要。

在本文中，我们着重挖掘区块链的逻辑、表达逻辑的技术方法、以及技术方法可能产生的应用。

区块链：基于平等信任逻辑的分布式数据库

按照维基百科解释，区块链是：一个分布式数据库，它维持了一个（连续增长的不能被篡改和修订的）记录区块序列，每个区块都包含了一个连接到前一区块的时间戳。如果我们把数据库假设成一本账本，读写数据库就是一种记账行为：

（1）记账，系统在一段时间内找出记账最快最好的人、由这个人来记账，然后将账本的这一页信息广播给全网其他每个节点，这也就相当于改变数据库记录；**（共识机制，密码学）**

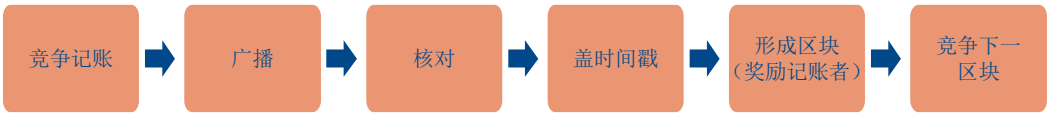
（2）核对，全网其他有效节点核对该区块记账的正确性，并且盖上时间戳，确认区块合法；**（时间戳，数学）**

（3）形成单链，即在上一合法区块之后竞争下一个区块；**（智能合约，加密技术）**

（4）存储，账簿是分区块存储的，随着交易的增加，新的数据块会附加到已存在的链上，形成链状结构；**（分布式结构，信息技术）**

（5）备份，每一个参与交易者都是区块网络的节点，每个节点都有一份完整的公共账簿备份，也就是分布式账本。

图 1：区块链系统的形成步骤



资料来源：中信证券研究部

区块链的内涵：一套逻辑，一种表达

我们认为，区块链基于平等和信任的逻辑，是互联网思维的结构表达，是信息产生价值的美好愿景：（1）在执行端，综合数学、密码学等学术基础；（2）在逻辑端，致力于保持数据真实性、节点平等性等哲学逻辑。这是因为，区块链主要解决了如下问题：

（1）数据是否是可信任的？信任的基础：一是共识机制，也就是数据被记账的动作是值得信任的；二是时间戳，也就是对存储数据的区块打上时间戳，使区块与区块之间形成一个连续性、环环相扣的诚实的数据记录，也就是数据库系统是值得信任的。

（2）可信任的数据怎样被存储和组织起来？区块承担了存储功能，分布式节点保证网络中的每个参与者都有一套完整的账簿备份，也就是数据库系统是去中心、分布式的。

一、共识机制：平等信任的逻辑内涵——如何记账

共识是一种机制，它保证了在去中心化的、平等地位的框架下，解决矛盾分歧的机制。在“理性人追求利益最大化”就是市场经济系统中，解决矛盾分歧的机制。**共识机制确立了在当前分布式中心的账簿中，账本是如何被记录下来的。**

当前主要有四大类共识机制：Pow、Pos、DPos、Pool。（对四类共识机制的分析文章已经非常多，本文引用了布比 CTO 王璟在知乎上的论述）

1、Pow 工作量证明，就是比特币案例中的共识机制，也就是挖矿，通过计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。

优点：完全去中心化，节点自由进出；

缺点：目前 bitcoin 已经吸引全球大部分的算力，其它再用 Pow 共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用。

2、Pos 权益证明，Pow 的一种升级共识机制；根据每个节点所占代币的比例和时间；等比例的降低挖矿难度，从而加快找随机数的速度。以太坊目前主要运用这种模式。

优点：在一定程度上缩短了共识达成的时间；

缺点：还是需要挖矿，本质上没有解决商业应用的痛点。

3、DPos 股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证；

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的。

4、Pool 验证池，基于传统的分布式一致性技术，加上数据验证机制，是目前行业链大范围在使用的共识机制。

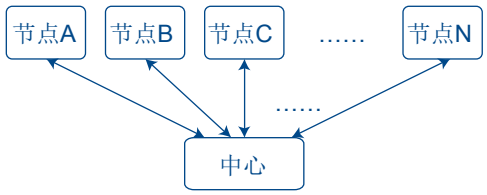
优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证；

缺点：去中心化程度不如比特币；更适合多方参与的多中心商业模式。

二、分布式思维：平等信任的实际体现——如何存账

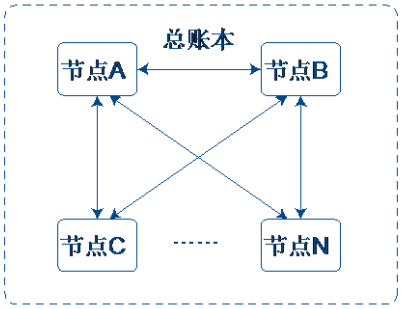
“中心”与“去中心”相对应，代表着平等和信任实现的路径。在“中心”化的结构中，中心代表的是信任、也是共识，而在“去中心”的结构中，也就代表着“去信任”，系统各参与方的地位平等，也就是任何一个中心都不能在系统中成为绝对的“中心”。

图 2：中心结构



资料来源：中信证券研究部

图 3：去中心结构



资料来源：中信证券研究部

三、区块链的分类：平等信任和效率的应用现实——如何应用

我们发现，追求“公平”的目标，与追求“效率”的目标存在天然的冲突：在区块链的系统中：**共识机制，意味着算法最牛的节点才能具备记账资格，也就是需要不断提升算力。以比特币为例，目前比特币挖矿每秒全网算力已经超过 1200PH/s，推导出比特币挖矿所需电力已达到数百万瓦特，相当于一个大型电厂的 10%（算法详见阿尔文德.纳拉亚南等著的《区块链技术驱动金融》一书）。**我们可以得到，为了“去中心”需要耗费大量的能源，才能建立起一个基于平等的共识机制；还是选择相信“中心”，依托一个基于中心的共识机制，是需要回答的问题。

因此，按照共识机制和去中心程度的不同，区块链可以按照如下分类类型：

（1）公有区块链（Public BlockChains)

公有区块链是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。

（2）联合（行业）区块链（Consortium BlockChains)

由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程(本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的 API 进行限定查询。

（3）私有区块链（private BlockChains)

私有区块链：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限。

完全去中心才能体现区块链的底层逻辑；部分去中心或分中心，实际上仍然是基于“中心”下的信任改善。

区块链的发展历程：一份愿景

区块链基于信任和平等的逻辑，是互联网思维的结构表达，是信息产生价值的美好愿景。从区块链的发展历程来看，主要分成三个阶段：

1.比特币时期（2008-2012 年）

这一阶段也是比特币的诞生与成长阶段，区块链作为比特币的底层技术并未受到过多关注。比特币挖矿技术、交易平台以及莱特币等网络货币在这一阶段有重大发展。

2.从比特币到区块链的过渡期（2012-2015 年）

随着比特币的发展，这种数字货币能带来的经济效益被不断开发，除比特币外，莱特币、以太经典、聚宝币、美通币、狗狗币、点点币等网络货币层出不穷，形成币圈。同时，基于数字货币底层技术的区块链逻辑开始被关注。

3.发展区块链时期（2015 年至今）

自 2015 年起，基于区块链系统的去中心化、开放性、信息无法篡改的技术可以移植到金融、科技、司法等更多领域中。区块链应用开发和投资项目增加，全球大型金融机构也相继成立联盟或投资区块链初创企业。

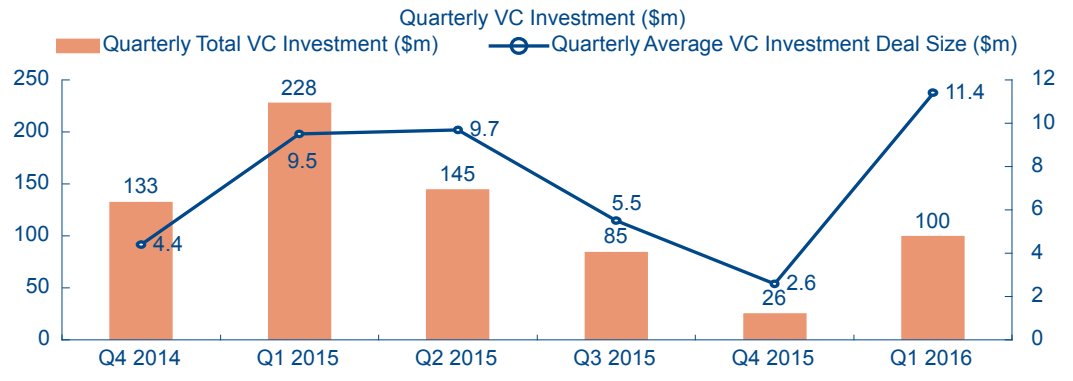
表 1：区块链发展大事记

时间	大事记
2008	中本聪发表论文“Bitcoin: A Peer-to-Peer Electronic Cash System”《比特币：一种点对点的电子现金系统》，提出区块链的概念，区块链进入人们视野。
2009	中本聪挖出第一批 50 个比特币，被称作上帝区块
2010	第一个比特币交易平台 MT.GOX 成立
2011	每个比特币价格首次与美元平价，达到 1 美元
	比特币与英镑、巴西币的兑换交易平台上线
	MyBitcoin 遭到黑客攻击，超过 7.8 万个比特币下落不明（当时价值 80 万美元）
	莱特币诞生
	第一次比特币会议和世博会在纽约召开
2012	Rippel 系统发布，跨过转账引入区块链技术
	法国比特币中央交易所诞生，这是首个在欧盟法律框架下进行运作的比特币交易所
2013	美卡币区块链断裂，交易中断 1 天
	德国承认比特币合法货币地位
	泰国封杀比特币
	中国央行明确比特币为“网络虚拟商品”而非货币
2014	MT.GOX 因安全漏洞关闭网站
	区块链并购投资火热，Chain 获 950 万美元投资
	Tilecoin 发布集成物联网实验设备
2015	
	IBM 加入开放式账本项目（Open Ledger Project）
	Microsoft 宣布支持区块链技术
	德勤推出 Rubix 允许客户基于区块链的基础设施创建各种应用
	R3CEV 与 20 余家公司结成联盟，共享区块链研究数据、想法和技术
2016	纳斯达克推出基于区块链技术的证券交易平台 Linq
	中国首个区块链联盟——中国分布式总账基础协议联盟成立

资料来源：中信证券研究部根据《区块链驱动金融与经济新格局》（张健著）等公开资料整理

2015 年全球共发生数字货币区块链的投资事件 65 起，披露金额达到 4.9 亿美元，较 2014 年总投资额 3.61 亿美元增长 35.73%，行业累计融资金额突破 10 亿美元，主要公司如 Ripple、Blocksteam、Chain、DAH、Circle 等融资规模超过 5000 万美金。（本段内容摘自中投顾问产业研究中心《2016-2020 年区块链技术深度调研及投资前景预测报告》

图 4：区块链风投情况



资料来源：State of Blockchain，中投顾问产业研究中心，中信证券研究部

区块链的核心场景：比特币

在比特币案例中，创建新区块的竞争就是挖矿，挖矿的奖励就是比特币。在中本聪设计的比特币系统中，比特币产生的最大数量约为 2100 万个。因此在比特币领域，设计到如下商业应用模式：**（1）挖矿，**直接产生比特币也就是经济收益，“矿”领域的核心是提升算法（保证是最优秀的记账员），衍生的企业是生产矿机或芯片的企业，比如比特大陆；**（2）交易，**交易比特币的平台公司，衍生的企业是交易和结算平台，收取费用、提供买卖杠杆，比如火币网；**（3）使用，**将比特币作为支付货币并设计基于比特币应用的产品，比如 Circle。

比特币的本质：运作平等共识机制的奖励

比特币（BitCoin）的概念最初由中本聪在 2009 年提出，根据中本聪的思路设计发布的开源软件以及建构其上的点对点网络。点对点的传输意味着一个去中心化的支付系统。

比特币本质上是运行平等共识机制的奖励。比特币系统通过“挖矿”来生成新的比特币，所谓“挖矿”就是用计算机解决一项复杂的数学问题（哈希函数），来保证比特币网络分布式记账系统的一致性。比特币网络会自动调整数学问题的难度，让整个网络约每 10 分钟得到一个合格答案。随后比特币网络会新生成一定量的比特币作为赏金，奖励获得答案的人。

2009 年比特币诞生的时候，每笔赏金是 50 个比特币。诞生 10 分钟后，第一批 50 个比特币生成了，而此时的货币总量就是 50。随后比特币就以约每 10 分钟 50 个的速度增长。当总量达到 1050 万时(2100 万的 50%)，赏金减半为 25 个。当总量达到 1575 万(新产出 525 万，即 1050 的 50%)时，赏金再减半为 12.5 个。根据其设计原理，比特币的总量会持续增长，直至达到 2100 万。但比特币货币总量后期增长的速度会非常缓慢。事实上，87.5%的比特币都将在头 12 年内被“挖”出来。所以从总量上看，比特币并不会达到固定量，其货币总量实质上是会不断膨胀的，尽管速度越来越慢。

图 5：比特币系统的逻辑结构（形成区块的过程，就是生成比特币奖励的过程）

资料来源：中信证券研究部

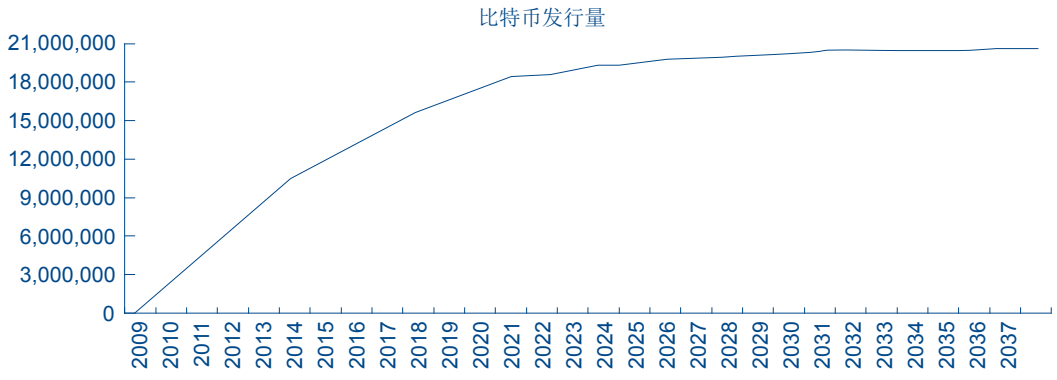
比特币商业圈：挖矿+交易+支付

1、 挖矿

矿工的工作是整个系统的核心，也是复杂性最高的地方。完成 Bitcoin 客户端安装后，可以直接获得一个 Bitcoin 地址，它将会分配一个私有密钥和一个公开密钥。需要备份你包含私有密钥的钱包数据，才能保证财产不丢失。

共识机制的底层密码学基础是哈希函数，挖矿的过程就是哈希函数的特解。因此，在挖矿也就是提升算法是获取比特币奖励的关键。特解是指方程组所能得到无限个（其实比特币是有限个）解中的一组。而每一个特解都能解开方程并且是唯一的。而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有 2100 万个特解，所以比特币的上限就是 2100 万。目前，已有接近 1700 万个比特币被挖掘出来。

图 6：比特币挖掘数量与时间的分布



资料来源：《区块链定义未来金融经济新格局》（张健著），中信证券研究部

挖矿的商业模式：矿机或芯片的需求。直接产生比特币也就是经济收益，“矿”领域的核心是提升算法（保证是最优秀的记账员），衍生的企业是生产矿机或芯片的企业。

图 7：全网挖矿情况

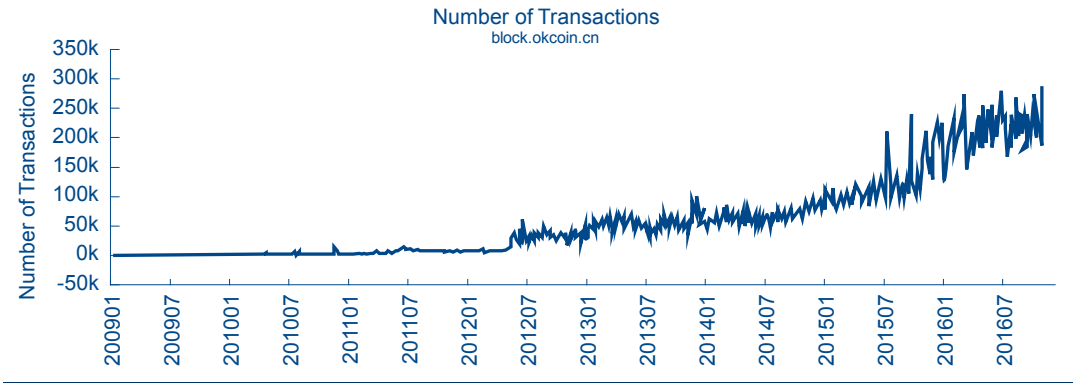
全网算力		1.86 EH/s
全网难度		253,618,246,641 -253.62G
预测下次难度		(-1.42%)250.02G
距离调整还剩		7天19小时
预测产量减半	时间	2020-06-01
	剩余块	193, 683

资料来源：btc.com，中信证券研究部，截至 2016 年 10 月 28 日

2 交易

比特币被挖出之后可以直接交易。目前比特币交易平台数量相当之多，国内代表平台包括：OKCoin 币行、火币网、BTCC 比特币中国、CHBTC 中国比特币、比特币交易网 BtcTrade、聚币网、云币网、Bter 比特儿、比特时代、大红火、元宝网、八融宝、链行、币创等十余家。下图显示的中国三大比特币交易平台之 okcoin 的每日交易量情况。

图 8：OKcoin 比特币的交易量



资料来源：OKCoin，中信证券研究部

交易的商业模式：赚取手续费和提供融资的收益。交易比特币的平台公司，衍生的企业是交易和结算平台，收取费用、提供买卖杠杆，比如火币网。

3 使用

基于比特币的特征，可以开发基于比特币的产品和应用。将比特币作为支付货币并设计基于比特币应用的产品，比如 Circle。

Circle Internet Financial 公司成立于 2013 年，总部位于波士顿，是美国一家消费金融创业公司，主要提供虚拟货币比特币的储存及国家货币兑换服务。Circle 目标是将比特币作为后台网络来使用，使用户可以以各国货币的形态来掌控自己的资金，以此避免比特币的价格波动可能带来的损失。当用户想要转移资金的时候，也可以购买短期的比特币，以此将资金（美元、英镑、欧元）转移到相关的银行账户。

2015 年 9 月，纽约州监管机构向 Circle 颁发了该州首张数字货币许可证 BitLicense，允许后者在纽约州提供数字货币服务。过去一年，Circle 的用户来自 150 个国家，年增速超过 300%，年交易额近 10 亿美元。

发展前瞻：所有系统都可以使用区块链么？

在思考区块链的应用时，我们需要再次回到区块链的逻辑框架。

我们认为，只要运用了平等+共识逻辑的项目，都可以是区块链的范畴。

所以理论上，区块链可以被应用到所有的系统中。这或许是区块链最大的价值所在。

不过在当前阶段，质疑区块链的前景，才是实事求是的态度。

逻辑挑战和实际障碍：真实，还是共识？精确，还是模糊？

我们认为，区块链最大的魅力来自于逻辑，最大的挑战也来自于逻辑。原因就在于，其底层逻辑的共识机制，即“不要求真实存在，只要超过 51%的共识”即可，如果要在所有系统中都运用这一逻辑，需要回答两个问题：

（1） **信任依据是基于少数派的理性抉择、还是基于大众的盲选？**按照区块链的逻辑，形成决策的机制是共识，也就是说所有节点并不考虑真实存在、而仅需考虑“51%以上绝大多数”的共识即可。但是，从现实情况来看，绝大部分组织和系统的抉择是依据“少数中心”的理性选择。权力是平等的直接交给参与者、还是间接给予获得优势地位的“中心”？“中心”与“公众”谁更值得信任？

（2） **共识是否绝对值得信任？**按照区块链的逻辑，共识的依据是 51%以上，但一旦部分节点算力超过了 51%就可能导致区块链的共识变得不能真实反映平节点的平等。也就是说，奖励如果足够大，就会导致平等实际上并不平等，甚至是“被控制”的平等。

（在比特币案例中，最大的担忧就是“51%算力攻击”，可以用这些算力重新计算已经确认过的区块，使区块产生分叉，导致双重记账。可以说，比特币系统不稳定的最大冲击就来自于此。）

实际应用方面的障碍在于：效率和耗能的博弈，是基于信任机制的高耗能、还是基于弱平等的高效率。按照目前区块链的算法，仅运行比特币系统就需要一个大型发电厂 10%的电能，那如果更多的组织及系统都使用这一算法，则追求平等共识进而引发的能源损失和效率损失则变得巨大。

因此，在考虑到区块链的应用时，我们得到如下结论：

（1） 理论上讲，区块链的逻辑可以应用到所有的系统中，只要该系统是基于平等共识的逻辑。

（2） 应用上看，组织或系统需要在“平等、效率、耗能”目标方面进行平衡，也可以说是**区块链的“不可能三角”。**

（3） 因此，区块链的发展脉络应当是一个**“短中长期稳步发展、三目标协同前进”**的格局。

短中期应用领域思考：重要不被信任中心的信任方案

短中期应用领域思考：信任领域，尤其是“重要不被信任中心”的信任方案。我们认为，区块链解决信任问题的逻辑有效，但信任平等的代价是效率，因此在收益成本的权衡中，短期内最直接的应用就是：**解决重要的、不被信任中心的信任问题的应用，包括公益项目、会**

计审计、食品安全、协会组织等领域，更宽泛的猜想是可以应用于金融领域的投资资金使用、债权管理、股权发行、征信等诸多领域。

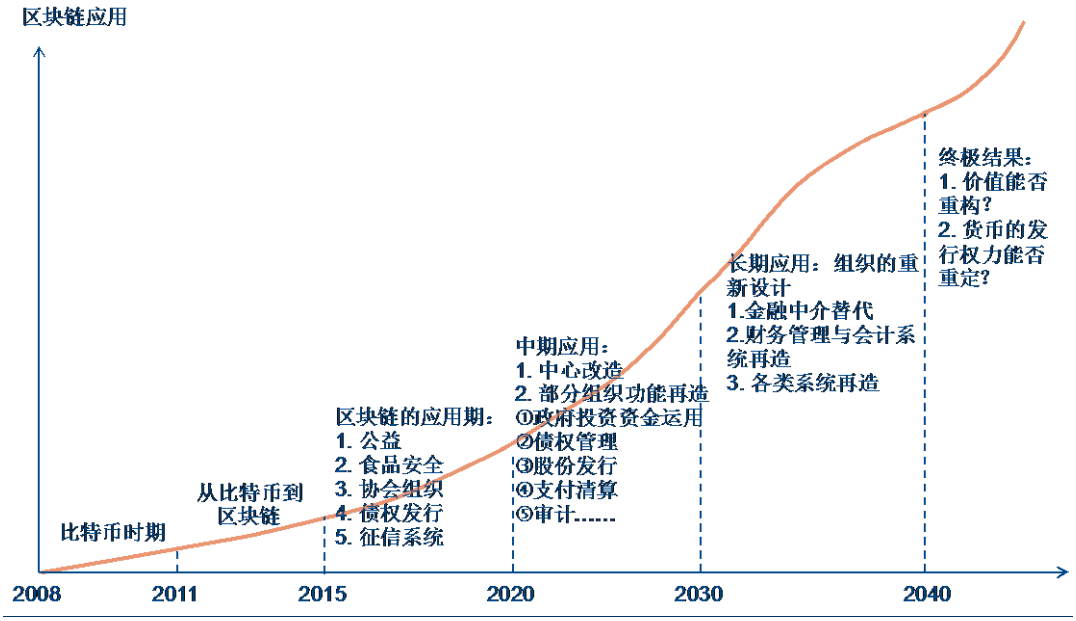
长期方向前瞻：或将引发“组织”的重新设计

长期应用领域前瞻：规则领域，或将引发“组织”的重新设计。平等，是互联网思维的直接落地，而当前组织的建立标准几乎不可能基于平等逻辑；从区块链隐含的平等逻辑出发，会对现代组织（中介、企业、政府）制度建立的标准产生巨大影响，包括：**各类中心/中介功能的替代（比如金融中介）；企业财务管理制度的改变（比如会计方法）；社会各类系统及体系的重新设计（比如支付体系）。**

终极结果猜想：价值标准的重构

价值，在经济社会中体现的是使用价值，承担价值交换功能的是货币（一般等价物），支撑一般等价物交换的基础是主权，主权是一个最强大的中心。目前，比特币作为极小范围内的一般等价物，仍需要与主权货币保持信用关联。**假想一下，如果现实世界都通过区块链逻辑进行表达，记账（产生使用价值）的奖励就是一般等价物（记账获得的收益），那么价值认定的标准就会被重构，支撑一般等价物交换的基础就是基于共识机制的记账、而非某个中心或主权。**在各种组织中，主权是最强效力的一种。

图 9：区块链短中长期应用路线图



资料来源：中信证券研究部银行组绘制

从逻辑到价值

在探索未来的过程中：存在，即是最大意义；逻辑，是价值起源；价值，是追求者的目标实现。本文梳理了为此“价值”探索的技术、方法和企业。

行业增长空间分析：理想很丰满

基于上文的分析，我们对于行业增长空间分析的逻辑如下：

（1） **区块链并非常规意义上的新技术，更多的是一种逻辑运用。**

（2） **理论上的奖励空间巨大，几乎所有的领域都可以被区块链的平等共识逻辑改造。应用区块链逻辑后所获得的空间增长，就是改造当前组织模式的空间。**以会计事务所为例，如果将区块链应用于审计，则审计行业的收入就可以被看成是运行区块链系统的奖励。

（3） **实际应用中的成本值得商榷。应用区块链逻辑所付出的成本，就是高耗能的代价。**由于区块链本身并不能带来劳动生产率的提高，因此运用这一逻辑付出高耗能的代价几乎是必然的。

（4） **实际应用的必要性更值得讨论。应用区块链主要是解决信任，而目前很多中心化的系统反而是更加值得信任的。**比如基于主权保障的金融核心系统、支付清算系统、跨境支付系统等，相对于完全去中心化的模式，更加值得信任。

（5） **因此，越是信任机制不足、需要建立信任的领域，应用空间越大，行业发展空间越大。**

当前产业链分析：从底层基础到实际应用

区块链产业链的参与者可以分为三个层次：基础层、中间层和应用层。

（1） 基础层：区块链生态的底层架构、逻辑框架和算法模式等，无论是共识算法的更新、加密模式的创新、奖励机制的完善等，都需要依赖结合实际应用来发展基础层的逻辑和架构；

（2） 中间层：基于区块链底层逻辑、技术、算法、机制的中间应用，致力于完善基于区块链逻辑的各种系统的流程改造、二次应用等；

（3） 应用层：开发解决用户实际需求的区块链应用，比如基于分布式账本开发的应用，包括身份验证、交易所、比特币、云存储等；再比如基于去中心化体系开发的应用，包括跨境金融、P2P 借贷等。

我们在研究中发现，由于互联网金融热度消退，Fintech 模式开启，区块链作为这一领域的前沿“标语”被广泛运用。这其中，存在大量推广“区块链”逻辑应用的项目，也存在致力于提升数据库系统效率的其他逻辑应用项目。

七大类区块链项目汇总：比特币未艾，区块链方兴

1、研究及开发。目前区块链研究主要集中于区块链技术本身的学习与研究，按研究方向可分为两类：以比特币为代表的虚拟货币研究和专注商业应用探讨的产业发展研究。模式多为集团或联盟形态，主要组织包括万向区块链实验室、布比研发团队等。

表 2：主要区块链研究项目概览

项目名	创始人	项目简介	技术特点/解决痛点
万向区块链实验室		专注于区块链技术的非盈利前沿研究组织，就技术研发、商业应用、产业战略等方面进行探讨	行业技术交流和基础理论研究，区块链技术培训认证及推广、区块链丛书出版
布比		2014 年 9 月正式开始区块链技术开发，创始团队主要来自中科院计算技术研究所，2015 年 3 月正式成立布比公司开展商业化应用的尝试	2016 年 8 月，基于布比区块链的数字资产平台布萌上线
ViewBTC		面向数字加密货币的独立第三方产业研究和资讯机构，业务包括维优指数、维优行业分析、维优数据分析	维优指数、维优行业分析、维优数据分析，ViewFin 的数字货币分支项目
Qtum 量子链		开发比特币和以太坊之外的第三种区块链生态系统，拓展区块链技术的应用边界和技术边界	通过价值传输协议（Value Transfer Protocol）来实现点对点的价值转移，并根据此协议，构建一个支持多个行业的（金融、物联网、供应链、社交游戏等）去中心化的应用开发平台
币富网		收集货币数据分析和投资建议网站，以数据为出发点，结合行业热点分析判断数字货币发展趋势	首创社会化情绪指数指导数字货币交易
币看		提供比特币和其他加密货币价格、咨询、交易功能 App	通过 Web 和手机 App 提供比特币行情和咨询服务，并可以通过 App 加入比特币市场货个人进行交易

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

2、比特币挖矿及区块链芯片。作为区块链的底层技术，挖矿的收益最先被认识到并因此得到迅速发展。目前的挖矿项目主要涉及矿池提供、算力出租、矿机出售三个领域。我国在矿池方面处于世界领先地位，比特大陆的蚂蚁矿池、鱼池 F2Pool、比特币中国 BTCC 等矿池算力均处于全球领先水平。

表 3：主要挖矿项目概览

项目名	创始人	项目简介	技术特点/解痛点
比特大陆 Bitmain	吴忌寒	成立于 2013 年初，是一家中国的 IC 设计公司，专注于比特币专用挖矿芯片和矿机的研究、开发和销售	提供高速、低功耗计算芯片，大功率、高密度计算服务器和大规模并行计算软件等超级计算芯片、硬件和软件产品；创始技术团队在集成电路领域有多年的经验积累，成功设计并量产了多款数字信号处理领域的芯片，包括比特币专用挖矿芯片
币网 bw.com	花松秀	创立于 2014 年 8 月，致力于为比特币玩家提供专业、简单、高效、安全、值得信赖的挖矿设备及服务体验，业务涵盖比特币矿机芯片研发、比特币矿机制造销售、比特币矿池、比特币云算力、比特币理财等领域，提供比特币全产业链解决方案	矿机 B11-plus 采用 14nm 芯片工艺，算力 5TH/s；云算力 B16 仅耗能 149W/T，最长矿机生产周期超过 24 个月
牛比特	郭伟城	成立于 2014 年 10 月，由国内数个投资团队共同组建而成，拥有独立的研发团队	首创多种低成本机房部署方案，为其大规模部署机房提供了坚固的技术支持
算力宝	梅可风	成立于 2015 年年底，是由浙江算力网络科技有限公司开发的云算力租赁平台，由浙江清华长三角研究院杭州分院作为种子企业进行加速孵化，目前以云算力租赁为主营业务	打通整合 IDC 服务提供商主板上市企业高升控股（000971）、全球最大的比特币交易所及钱包服务商 OKCoin、矿池等资源，用户可以实现远程挖矿，体验科技同时享受算力产生的比特币
嘉楠耘智 Avalon	张楠赓	创立于 2013 年，是一家专注于“区块链”服务器与重复计算芯片方案的创新技术企业，其产品包括基于 FPGA 的 SH256 算法、Avalon 区块链专用芯片等	
ViaBTC	海洋	创立于 2016 年，由前腾讯员工创办的比特币创业公司，目前主要业务为比特币矿池	采用完全自主研发的系统，自主研发的区块高速网络做到最快发现和广播区块，有效降低矿池和比特币网络的孤块率、空块率；公开透明，无手续费
F2Pool 鱼池	毛世行	成立于 2013 年，全球最大比特币、莱特币、以太坊矿池之一	全球最大比特币、莱特币、以太坊矿池之一
BitFury	Valery	2011 年创立于俄罗斯，早期是一个	业务范围覆盖全球，在旧金山、华盛顿特区、

项目名	创始人	项目简介	技术特点/解痛点
	Vavilov, Valery Nebesny	ASIC 比特币矿机芯片研发团队，目前为世界领先的比特币区块链基础设施供应商和交易处理公司，提供一系列的区块链软件及硬件产品，以支援商业和政府的区块链操作	香港、阿姆斯特丹和伦敦建立管理办公室，在冰岛和格鲁吉亚共和国建立了数据中心
KnCMiner	Sam Cole	由专业嵌入式电子产品开发商 ORSoC AB 和 Kennemar & Cole AB 联手打造设立，总部位于瑞典斯德哥尔摩	2015 年规模化部署 16nm 比特币矿机芯片；首家推出 28nm 工艺挖矿芯片；2016 年 5 月宣布破产，新收购者 GoGreenLight 表示将继续运营比特币挖矿池和数据中心

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

3、钱包或比特币服务项目。比特币钱包类似于银行卡，可以自动生成比特币 wallet 钱包文件，这个文件里面存放着用户的比特币信息，包括收款地址、私钥等。目前比特币钱包可以分三类: 客户端钱包、网络 web 钱包、手机和 pad 钱包。

表 4：主要比特币钱包项目概览

项目名	创始人	项目简介	技术特点/解决痛点
haobtc 好比特币	吴钢	比特币钱包平台，提供便捷、安全、专业的比特币交易服务，7*24 小时自动充值，秒级交易	2016 年 7 月推出矿池，至今自有算力已达 74.5P，在全球矿池中排名靠前
比太钱包	文浩	安全易用的比特币钱包，是去中心化的、基于比特币 P2P 网络的、开源的解决方案，获得 Bitcoin.org 官方推荐	基于 SPV 轻钱包模型，支持 HD 模型和多重签名技术，创新冷热钱包模式，独创极随机解决方案
BitPay	Tony Gallippi	面向收取 Bitcoin 商户的支付解决方案，被称为 Bitcoin 的 Paypal	商户通过 BitPay 把比特币转成自己使用的货币，向 BitPay 支付 0.99%手续费；提供了购物车，结账和比特币转换等一系列齐全的解决方案
BitGo	Mike Belshe	比特币安全平台，为比特币交易提供多重签名冷储存方案	采用“多重签名比特币钱包”(“2-of-3 key” multi-signature)模式保障比特币持有者的资产安全，即用户在交易的时候，需要至少进行 2 到 3 次的确认；Bitfinex 安全平台提供商
Blockchain.info		创立于 2013 年，知名 onchain 在线钱包服务商，同时也提供比特币区块链数据查询服务	使用行业标准 AES，兼容 Bitcoin-Qt 客户端的 JSON RPC
Mycelium	Ashley Cooper, Matthew Abrams	创立于 2011 年 8 月，比特币行业著名的钱包平台和其它密码学相关的项目	通过 API 插件来允许开发者添加其它功能，允许其它公司整体使用该应用平台
Uphold 尚持	Halsey Minor	为用户提供包括比特币在内的其他 20 种法定货币的免费转账、货币兑换服务	比特储创始人哈尔西•迈纳（Halsey Minor）于 1994 年创办了如今家喻户晓的著名科技新闻网站 CNET，公司致力于创造一个更公平、包容、透明公开以及更具责任感的金融服务系统
Armory		开源的比特币管理客户端软件，提供比特币钱包管理、加密、离线交易等服务	支持多个钱包，进行统一管理，其中默认钱包可以设置成“离线模式”（offline mode），采用冷存储
Circle	Jeremy Allaire, Sean Neville	为消费者开发使用比特币的工具，至今总计已获注资 7600 万美元	入驻苹果 iMassage，伴随 iOS10 发布；成立中国子公司 Circle 中国
Electrum	Thomas Voegtlin	创立于 2011 年 11 月，轻量比特币钱包代表	轻量钱包，占用空间少；支持 HD 模式（分层确定性钱包，BIP32），通过安全种子恢复全部比特币地址；支持二步验证功能（Tow Factoring Authentication）；支持 Trezor、Bwallet 等硬件钱包
Xapo	Wences Casares	成立于 2014 年，比特币安全存储服务公司，提供比特币钱包服务，包括冷存储库和比特币信用卡，2015 年总部搬至瑞士	全储备银行，多重签名保障安全；创始人兼 CEO 是比特币领域的早期投资人之一
bitbank	花松秀、郭宏才	成立于 2014 年，前身为“聚啊”，目前为全球最大的数字货币银行，为投资者提供储蓄理财项目，包括比特币和莱特币的活期储蓄、定期储蓄、	先后投资币网 14nm 芯片矿机和全冷钱包技术等项目，拥有比特币云算力理财

项目名	创始人	项目简介	技术特点/解决痛点
		P2P 借贷理财和比特币云算力理财	
BitX	Marcus Swanepoel	新加坡比特币公司，主营比特币钱包支付业务，在非洲、东南亚、东欧和拉丁美洲都有市场，其中南非、纳米比亚和肯尼亚等地区的比特币交易量都非常活跃	2015 年，BitX 获得 400 万美元 A 轮融资：腾讯第一大股东 Naspers 集团领投
Armory		开源的比特币管理客户端软件，提供比特币钱包管理、加密、离线交易等服务	支持多个钱包，进行统一管理，其中默认钱包可以设置成“离线模式”（offline mode），采用冷存储

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

数字货币。继比特币之后，出现了大批的虚拟货币，包括莱特币、以太坊、以太经典、狗狗币、点点币等。目前数字货币领域应用多希望通过一家平台整合多种货币，如太一体系内货币由系统币（ABC）及基于太一的统一区块链发行的各种子币所构成，而太一子币可以用作替代数字货币、资产代币、证明币等。

表 5：主要数字货币项目概览

项目名	创始人	项目简介	技术特点/解决痛点
太一系统	邓迪	可以方便发行多种数字货币，多种数字资产可以共享太一区块链	全球第一的有法币之称的数字货币，多资产共享区块链，发行成本较低
智能坊	石玮松	基于比特币进行深度开发的第二代数字货币，其主要的价值体现在其实现了全球领先的可编程智能合约系统，并已在此系统上成功运行了数个 P2P 应用	提供图灵完备 C/C++脚本语言的可编程的虚拟数字货币系统，实现“智能合约”，第三方开发人员可以在其基础上实现几乎所有的虚拟货币功能

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

证明公证项目。基于区块链的信息不可篡改特性（盖上时间戳，未来无法被修改、篡改），区块链技术可以提供一种“存在性证明”，即证明在某个时间点，某些信息已经存在，目前线下应用多用于司法体系内的身份验证，以及知识产权领域的在先权利证明。

表 6：主要证明公证项目概览

项目名	创始人	项目简介	技术特点/解决痛点
BitSE	钱德君	成立于 2013 年，全球区块链服务平台，提供算力管理、数字资产管理与交易、物联网、防伪、IP 注册等服务	首次提出 Blockchain As A Service，结合知识产权防伪检验的痛点，利用区块链及侧链的智能合约技术，以区块链安全芯片及区块链物联网芯片为核心提供服务
安存正信	高航	以区块链的时间戳为基础，提供数据真实性、有效性、证据化的基础服务，关联用户的线下真实身份提供存在性证明	在国内司法体系对电子证据认可的基础上，叠加基于区块链的存证技术，以“存证”为切入点
CertChain	龚鸣	以去中心化、纯粹数学算法的方式提供匿名且安全的存在证明，可根据用户需求便捷和极低成本的证明某个人对任意类型文件的所有权	无需透露任何鉴证内容给第三方就可完成鉴证，公开、透明且免费

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

资产交易项目。区块链资产交易平台起源于比特币等数字货币交易所，目前多数平台基于区块链技术的去中心化协议，提供比特币、莱特币、以太坊、狗狗币等多种虚拟货币的在线交易服务。

表 7：主要资产交易项目概览

项目名	创始人	项目简介	技术特点/解决痛点
火币网	李林、杜均	创立于 2013 年 5 月，数字货币交易平台	布局全产业链，收购比特币钱包“快钱包”
BTCC 比特币中国	李启元、杨林科、黄啸宇	创立于 2011 年，中国第一个比特币交易所，提供数字货币交易所、矿池、支付网关、BTCC Mint 硬钱包和区块链刻字等服务	安全性与便捷度均佳，一站式解决用户对比特币各环节需求，技术经验丰富拥有全球最长运营历史
OKCoin 币行	徐明星	创立于 2013 年 6 月，比特币交易平台，开展区块链资产的全球交易，虚拟货币(比特币)支付、清算、结算业务，与其公司另一产品“币行钱包”域名合并	采用 ssl、冷存储、gslb、分布式服务器等技术，确保交易的安全快捷稳定；首创冰山委托、时间加权委托等策略交易工具；实时动态风控系统，根据市场动态对账户和仓位进行分级管理；在保证指数平滑的基础上添加

项目名	创始人	项目简介	技术特点/解决痛点
			全球主要市场入指数成分
CHBTC 中国比特币	花松秀、李大伟	创立于 2013 年 6 月，面向全球提供比特币、以太坊、莱特币、以太坊经典等多种数字货币交易服务，母公司比银集团	建立在开放的比特币网络之上，离线 BTC 钱包、服务器 SLB 均衡与同时备份
比特币交易网 BtcTrade	张寿松	创办于 2013 年 4 月，中国最早的比特币交易平台之一，目前在全球 200 多个国家和地区拥有超过 100 万注册会员，提供比特币、以太坊、莱特币、狗狗币和元宝币交易	全资收购聚币网
云币网	邱亮	成立于 2013 年，原名貔貅，为李笑来独立投资的数字资产交易平台	由自主研发的“貔貅开源”系统搭建，实现 100%的准备金公开；所有的数字币和法币的数量均公开透明，实行比特币和法币双 100%保证金制度；上线采用透明 IPO 方式发行的创新数字货币，如以太坊以及基于以太坊的资产
Bter 比特儿	韩林	成立于 2013 年 4 月，国内首家山寨币交易平台	目前山寨币种类最多的交易平台，冷钱包 100%委托给合作伙伴 JUA.com 的安全团队
比特时代	黄天威	创立于 2013 年 5 月，集资讯和交易为一体的数字货币平台	拥有数字货币资料库与最新资讯频道，满足用户了解学校与研究投资双重需求
大红火	Micheal Su	创立于 2016 年 3 月，专注于区块链技术创新及数字资产交易的平台	分布式集群数据中心冷储藏、多重身份验证安全保障，提现 24 小时内到帐，提币 7X24 小时实时支付
链行	尹洁	面向全球数字资产投资者的专业交易平台，为用户提供比特币、莱特币等多种优质数字资产交易服务，同时发布资产分析报告、研发特色交易指标为用户带来更出色的交易体验	自主研发的海量并发撮合引擎理论支持最高 10 万笔/秒的并发交易，多层安全架构设计、动态冷热钱包机制保证交易安全
聚币网	张寿松	创办于 2014 年 1 月，2014 年 3 月正式上线，2014 年 11 月被比特币交易网（BtcTrade.com）全资收购，为其旗下竞争币交易平台	为用户挑选出安全并具有投资价值的二代虚拟货币（山寨币），收购综合性数字货币交易平台万币网
币创	白洪日	专注于创新数字资产交易平台，致力于为用户提供安全、便捷、平等的数字资产投资机会	主要交易流通性强、应用性广、认可度高的区块链生态的非中心化币种，是界于传统交易所和山寨币交易所之间的新定义，弥补行业空缺；采用线下“券商”的推广模式，打破数字资产线上单一的发展瓶颈
Coinbase	Brian Armstrong	创立于 2012 年，2014 年成立美国首家正规比特币交易所，目前已完成超过 1 亿美元融资	已获得美国多个州监管机构的合法执照，将为包括纽约、加州在内的 25 个州提供交易服务；目前已开设比特币钱包业务
Open Bazaar	Brian Hoffman	比特币去中心化商品交易市场，开源的点对点（P2P）网上市场，实现了买卖双方的直接交易，2016 年 5 月发布首个正式版本软件	使用比特币作为支付方式之一，不存在任何中间费用或审查。
Bitfinex	Raphael Nicolle	全球最大的比特币、莱特币等数字货币交易平台	首批引入保证金交易产品，以美元/比特币货币平台的深厚流动性知名，2015 年添加世界首个基于区块链的货币平台 Tether；2016 年 8 月发生比特币被盗事件

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

基于区块链逻辑的其他应用项目。目前区块链项目多处于研究与初期阶段，应用及项目情况仍然在探索过程中。

表 8：基于区块链逻辑的其他项目概览

项目名	创始人	项目简介	技术特点/解决痛点
R3	R3CEV	致力于研究和发现区块链技术在金融业中的应用	其联盟成员包括摩根士丹利、富国银行、高盛、汇丰银行、荷兰国际集团（ING）、花旗银行等几十多家国际大型金融机构
Linq	Fredrik Voss	纳斯达克在其私人市场开发的一个基于区块链技术的新型股权交易平台	Chain.com 于 2015 年底在 Linq 上发行股份，成为首例
小蚁	达鸿飞	基于区块链技术的股权登记、管理和交易系统，区块链用以保存交易记录，是带自动执行功能的电子合同签署系统	集合国际电联 X.509 标准和《电子签名法》，设计具备法律效力的区块链身份认证方案；超导交易机制使交易所成为纯粹的信息撮合者，采用“用户+信息撮合者”模型
元宝网	邓迪	成立于 2013 年 7 月，中国最早的数字资产交易平台之一，2016 年 2 月经营主体	区块链主题众筹投资平台，团队同时拥有元宝理财和比特币中文网

项目名	创始人	项目简介	技术特点/解决痛点
		变更为元宝金汇（北京）科技有限公司	
BitShares	Daniel Larimer、李笑来、沈波、龚鸣	基于 DPOS 区块链技术的开源去中心化交易所解决方案，无需任何技术知识就可发行或交易数字货币、法币、金融衍生品，并收取自定义资产的交易佣金	首个全球范围商业化运作的交易平台解决方案，类 LMAX 交易引擎让区块链交易速度达到新高；突破多地区法律管辖限制
八融宝	曾玉宝	成立于 2014 年 9 月，专注于数字资产领域抵押借贷理财服务	富友资金托管设立风险备付金专户，保障资金安全
元界 Metaverse	初夏虎	基于区块链技术的去中心化协议，其服务框架结合了智能资产网络、数字身份和价值中介	通过引入价值中介的区块链系统，建立一个不可篡改，完全市场化的价值中介的高效经济模式。将在元界区块链上开发 BAAS 的平台

资料来源：中信证券研究部根据《区块链：新经济蓝图及导读》（梅兰妮.斯万）、币众筹区块链项目库等公开资料整理

几个有影响力的案例

下文我们列举了 4 个不同的商业模式和典型企业。

联盟链：R3 区块链联盟

R3 区块链联盟由区块链技术初创公司 R3 CEV 组织成立，致力于研究和发现区块链技术在金融业中的应用。其联盟成员包括摩根士丹利、富国银行、高盛、汇丰银行、荷兰国际集团（ING）、花旗银行等四十多家国际大型金融机构。R3CEV LLC 成立于 2014 年，总部位于美国纽约，创始人 David Rutter。

2016 年 5 月，中国平安保险(集团)股份有限公司宣布与国际金融创新公司 R3 建立合作伙伴关系，正式加入 R3 分布式分类账联盟，为全球金融市场设计和应用分布式共享分类账技术。2016 年 9 月，招商银行加入 R3。

根据媒体报道，目前 R3CEV 正在磋商 A 轮融资，R3 的预估市值为 2 亿美元，这也是 R3 联盟和其成员签订的部分协议内容。（来源：http://chainb.com/?P=Cont&id=2097）

二、Corda 项目

R3 联盟发布了针对金融机构共享分类账平台 Corda，用于记录、管理和同步受监管金融机构之间金融协议。

Corda 包含区块链的五大特性，共识、有效性、唯一性、不可更改性和认证

三、Concord 项目

2016 年 8 月，该公司申请了新项目 Concord 背后技术的专利。Concord 的目标是成为银行和公司之间的一个通用连接平台，其旨在数字化并加速清算与结算证券交易中以及交易后功能，以及登记各种资产并跟踪现金余额。（来源：http://www.8btc.com/r3-concord）

硬件支持企业：比特大陆

一、公司简介

北京比特大陆科技有限公司（BITMAIN）是一家中国的 IC 设计公司，成立于 2013 年初，专注于比特币专用挖矿芯片和矿机的研究、开发和销售。比特大陆是一家由集成电路技术团队、比特币专家、风险投资专家和企业家组成的高科技公司。创始技术团队在集成电路领域有多年的经验积累，成功设计并量产了多款数字信号处理领域的芯片，包括比特币专用挖矿芯片，为客户提供具竞争力的定制硬件解决方案。

目前，比特大陆已经完成了矿机、矿池、云挖矿、区块浏览器、钱包等多方面布局，其中蚂蚁矿机 Antminer、蚁池 Antpool、云算力 HashNest 均排名全球市场前列。

二、几个主营业务

蚂蚁矿机是比特大陆开展最早也是最重要的业务。蚂蚁矿机因投资回报利润最高、性能最强、稳定性最好、寿命最长一直为全球比特币爱好者所热衷。

2013 年 4 月开始筹备研发获得天使投资。10 月公司第一枚 55nm 芯片 BM1380 正式发布，蚂蚁 S1 矿机量产销售。BM1380 代表了 55nm 挖矿芯片研发的最高水平。

2014 年 4 月蚂蚁 S2 矿机（55nm）量产销售 6 月比特大陆第一版 28nm 芯片 BM1382 研发成功，准备量产蚂蚁矿机 S3。芯片性能与成本指标在全球范围内超越同行。

7 月蚂蚁矿机 S3 量产。

10 月比特大陆第二版 28nm 芯片 BM1384 研发成功，性能与成本指标在全球范围内继续领先。

12 月蚂蚁矿机 S5 量产。

2015 年 1 月蚂蚁矿机 S5 正式发售。

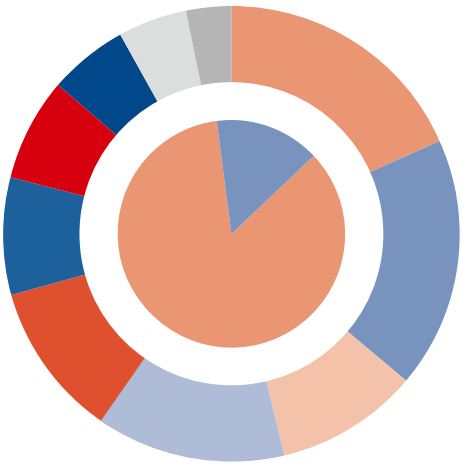
8 月比特大陆自主研发 BM1385 芯片问世，是当时比特币芯片史上功耗最低的芯片。

11 月蚂蚁矿机 S7 量产发售。

2016 年 6 月 BM1387 芯片问世，蚂蚁矿机 S9 发售。

蚂蚁矿池是一家高效的数字货币矿池，提供比特币、莱特币、以太坊（2016 年 5 月 28 日开始支持以太坊）等多种数字货币的挖矿服务，并支持 PPS（每股支付）、PPLNS（Pay per last N shares，每最近 N 股支付）、SOLO（独立挖矿）等多种付款方式。

图 10：全球主要矿池份额



矿池份额

	矿池	份额	算力(P)
1	AntPool	15.79%	305.27
2	F2Pool	15.37%	297.13
3	BTCC	13.89%	268.63
4	ViaBTC	11.58%	223.86
5	BW.COM	9.47%	183.16
6	SlushPool	7.16%	138.39
7	BitFury	6.32%	122.11
8	HaoBTC	4.84%	93.61
9	BTC.com	4.21%	81.40
10	BitClub	2.74%	52.91

资料来源：btc.com，中信证券研究部　　注：数据截至 2016 年 10 月 9 日

对于矿工而言，最主要的模式是基于“工作量证明”：一名矿工，依据他已提交给矿池的“工作量占比”，来确定应得的份额收益（Shares）。如果一个矿工返回的块显示，他的难

易程度在矿池级别和全网级别之间，则该块被记录为该矿工的“份额收益”。这些看似无用的区块份额收益，却为矿工们记录了工作量证明，以证明矿工的确从事了块计算。它们还可以显示，矿工们有多少处理能力、多大程度上贡献了矿池——硬件越好、越会得到更多的份额收益。

对于矿池而言，主要收入来源为手续费。目前蚂蚁矿池的手续费标准为：PPLNS 0，PPS1.5%，SOLO 1%。Block 交易费不进行分配，用于矿池开发和维护费用。

表 9：主要矿池费率对比

	比特币	莱特币	以太坊
AntPool	PPS1.5% PPLNS 0 SOLO 1%		PPLNS 0
F2Pool	PPS 3%	PPS 3%	PPS 3%
BTCC	过去 3 天，总收益大于或等于 1.5 个 BTC 2.0% 过去 3 天，总收益小于 1.5 个 BTC 2.6%		
BW.com	PPS 1% PPLNS 1% 旷工费 0.0002BTC/笔	PPS 1% PPLNS 1% 旷工费 0.001BTC/笔	PPS 2.5%
ViaBTC	PPS+* 4% PPLNS 2%	-	-
HaoBTC	PPS 1.5%	-	-

资料来源：各家公司网站，中信证券研究部整理

算力巢。比特币云算力平台 hashnest.com 利用大量的矿机，组成一个矿机统一运算阵列，集合成一股非常强大的比特币算力。同时，比特币云挖矿平台提供了将这些算力分割出租给个人用户的服务，每 1G 的算力按一定的价格、一定的时间出租给用户。

在比特币云挖矿平台，用户通过购买算力即可轻松享受比特币挖矿收益，省去了运输、电源、矿机部署等多项财力和精力支出。

区块浏览器。2015 年 9 月 28 日，比特大陆新产品 BTC 区块(chain.btc.com)正式上线，主要有区块浏览器和分析服务。BTC 区块作为一款区块浏览器产品，完全是由比特大陆自主研发，拥有较为完善的数据查询功能及 API 查询服务。

BTC 区块主要组成部分：矿池、区块、统计、工具、应用、钱包。首页由三部分组成：最近出块记录，矿池份额，以及网络状态。数据通过 WebSocket 实时刷新，动态反映出比特币的各个数据指标；区块菜单通过顶部日期选择器，较为方便的浏览自比特币诞生以来的任意日期的块数据。

BTC 钱包。2015 年 7 月，比特大陆完成收购了比特币数据和分析创业公司 Blocktrail，具体金额未知。比特大陆将寻求通过这次收购推进其在 BTC.com 提供的服务。2015 年 9 月，比特大陆正式推出真正将安全性、稳定性和易用性完美结合的安卓版比特币钱包，其命名为“BTC Wallet”，即“BTC 钱包”。

根据官网介绍，BTC 钱包具有以下特点：自主研发区块浏览器，数据更稳定；On-chain 钱包，让比特币更安全；On-chain HD 钱包，私钥完全由自己掌握；多重加密算法，确保私钥安全；服务器云备份；多账户管理；多重签名保险柜服务。

比特币交易平台：火币网

一、公司简介

北京火币天下网络技术有限公司成立于 2013 年，是比特币交易平台，致力于为投资者提供专业、安全、诚信的数字货币交易服务，提供人民币、美元市场一站式交易。

火币网与清华大学五道口金融学院互联网金融实验室战略合作，启动《数字资产研究课题》。

二、发展历史

2013 年 5 月 15 日，购买 huobi.com

2013 年 6 月 1 日，成立研发团队

2013 年 8 月 1 日，上线模拟交易平台并举行第一届比特币模拟交易大赛

2013 年 9 月 1 日，火币网现货交易平台上线

2013 年 9 月 10 日，火币网日交易额突破 100 万人民币

2013 年 9 月 20 日，火币网宣布永久免交易手续费

2013 年 10 月 19 日，火币网日交易额突破 1000 万人民币

2013 年 11 月 5 日，火币网获得真格基金和戴志康联合投资

2013 年 11 月 9 日，火币网日交易额突破 1 亿人民币

2013 年 11 月 19 日，火币网日交易金额超过 10 亿人民币

2014 年 3 月 19 日，火币网上线莱特币交易

2014 年 3 月 20 日，火币网莱特币日交易额突破 1 亿人民币

2014 年 8 月 5 日，比特币交易平台火币网宣布，已完成对比特币钱包“快钱包”的收购

2015 年 11 月 26 日，火币网日交易量达 173 万个比特币，日交易额突破 38 亿人民币，再度创出全球比特币日成交量的最高纪录

2015 年 12 月 12 日，火币网日交易量增长至 213 万枚比特币，日交易额突破 61 亿元人民币，这一新的全球比特币交易纪录至今未被打破

管理团队公司核心成员均毕业于清华大学、北京大学、复旦大学等国内顶级名校，曾就职于甲骨文、腾讯、赫斯特集团、广发银行等国内外知名企业。

火币网于 2013 年 9 月上线，11 月获得戴志德、徐小平的天使投资，2014 年完成千万美元级别 A 轮投资，投资人包括红杉资本。

三、商业模式

火币网为用户提供限价交易即挂单交易，以及市价交易，即按市场最优价格及时成交两种模式。

根据公司官网资料，收取比特币/莱特币转账或提线费用，费用为 0.0001-0.0010BTC/0.001LTC 不等。

图 11：火币网人民币提现费率

等级	积分（如何查看积分）	交易手续费	普通充值	BTC/LTC普通提现	人民币提现（24小时到账）
VIP0	0	永久免费	0%	0.0001BTC/0.001LTC	0.50%
VIP1	10000				0.45%
VIP2	100000				0.40%
VIP3	300000				0.38%
VIP4	500000				0.35%
VIP5	1000000				0.30%
VIP6	付费服务				0.30%

资料来源：公司官网，中信证券研究部

火币交易闪电手（以下简称“闪电手”）是一个提供杠杆交易的比特币交易平台。采用数据推送技术，行情速度提高 10 倍，行情信息更丰富，盘口行情揭示更快。闪电手手续费率：人民币杠杆费率 0.1%，比特币杠杆费率 0.1%，莱特币杠杆费率 0.08%。

目前火币网的主要盈利源于借贷利息。火币网交易平台内有一个借贷中心，。火币网的借款或借币的额度为个人净资产的 2 倍，以 24 小时为一天来计算借贷利息(从借贷开始时间算起，24 小时为一天，超过 24 小时按照新的一天算)每天收取 0.2%-0.1%(借贷利率根据用户 VIP 等级确定)的借款利息。

表 10：火币网与 OKCoin 融资融币的对比

类别	火币网	OKCoin
融资形式	平台放贷	P2P 形式
日利率	半市场化 0.22%	完全市场化 0.08%
放贷受益方	交易平台	放贷用户
融资种类	人民币、比特币	人民币、比特币、莱特币
手续费	借贷者缴纳	放贷者缴纳
计息周期	24 小时	24 小时
杠杆倍数	2 倍	3 倍
强平比例	110%	110%

资料来源：比特币之家 http://www.btc798.com/article-3173-1.html，中信证券研究部

开发生态系统：onchain 小蚁

一、公司简介

小蚁是基于区块链技术，将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化网络协议。小蚁可以被用于股权众筹、P2P 网贷、数字资产管理、智能合约等领域。

小蚁是国内早期非盈利的社区化区块链项目。Onchain 是小蚁团队成立的用于推广小蚁和丰富小蚁生态的盈利性公司，创始人兼 CEO 达鸿飞是“比特创业营”的创始人之一。

二、应用场景

主要业务包括：小蚁生态的商业化运营；区块链技术服务解决方案 BaaS。

Baas 旨为银行、政府部门、金融机构提供区块链技术咨询和定制区块链私有链解决方案，客户提出场景需求，Onchain 提供底层技术以解决客户所提出的场景需求。

2016 年 7 月和微软达成合作，共包含用 vs 开发、在微软云部署小蚁、在 office 内嵌入小蚁电子合同功能、利用认知服务更好的在法律上做一些认定等多项具体合作内容。

Onchain 成为了国内首家加入 Hyperledger 的区块链公司。**另外，Onchain 还与另外一家互联网公司法大大合作开发数字存证系统法链，Onchain 做技术服务提供商。**

分析师声明

主要负责撰写本研究报告全部或部分内容的分析师在此声明：（i）本研究报告所表述的任何观点均精准地反映了上述每位分析师个人对标的证券和发行人的看法；（ii）该分析师所得报酬的任何组成部分无论是在过去、现在及将来均不会直接或间接地与研究报告所表述的具体建议或观点相联系。

评级说明

投资建议的评级标准		评级	说明
报告中投资建议所涉及的评级分为股票评级和行业评级（另有说明的除外）。评级标准为报告发布日后 6 到 12 个月内的相对市场表现，也即：以报告发布日后的 6 到 12 个月内的公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅作为基准。其中：A 股市场以沪深 300 指数为基准，新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准；美国市场以纳斯达克综合指数或标普 500 指数为基准。	股票评级	买入	相对同期相关证券市场代表性指数涨幅 20%以上；
		增持	相对同期相关证券市场代表性指数涨幅介于 5%～20%之间
		持有	相对同期相关证券市场代表性指数涨幅介于-10%～5%之间
		卖出	相对同期相关证券市场代表性指数跌幅 10%以上；
	行业评级	强于大市	相对同期相关证券市场代表性指数涨幅 10%以上；
		中性	相对同期相关证券市场代表性指数涨幅介于-10%～10%之间；
		弱于大市	相对同期相关证券市场代表性指数跌幅 10%以上

其他声明

本研究报告由中信证券股份有限公司或其附属机构制作。中信证券股份有限公司及其全球的附属机构、分支机构及联营机构（仅就本研究报告免责条款而言，不含 CLSA group of companies），统称为“中信证券”。

法律主体声明

中国：本研究报告在中华人民共和国（香港、澳门、台湾除外）由中信证券股份有限公司（受中国证券监督管理委员会监管，经营证券业务许可证编号：Z20374000）分发。

新加坡：本研究报告在新加坡由 CLSA Singapore Pte Ltd（公司注册编号：198703750W）分发。作为资本市场经营许可持有人及受豁免的财务顾问，CLSA Singapore Pte Ltd 仅向新加坡《证券及期货法》s.4A（1）定义下的“机构投资者、认可投资者及专业投资者”提供证券服务。根据新加坡《财务顾问法》下《财务顾问（修正）规例（2005）》中关于机构投资者、认可投资者、专业投资者及海外投资者的第 33、34、35 及 36 条的规定，《财务顾问法》第 25、27 及 36 条不适用于 CLSA Singapore Pte Ltd。如对本报告存有疑问，还请联系 CLSA Singapore Pte Ltd（电话：+65 6416 7888）。MCI (P) 013 11 2015。

针对不同司法管辖区的声明

中国：根据中国证券监督管理委员会核发的经营证券业务许可，中信证券股份有限公司的经营范围包括证券投资咨询业务。

新加坡：监管法规或交易规则要求对研究报告涉及的实际、潜在或预期的利益冲突进行必要的披露。须予披露的利益冲突可依照相关法律法规要求在特定报告中获得，详细内容请查看 https://www.clsa.com/disclosures.html。该等披露内容仅涵盖 CLSA group, CLSA Americas 及 CL Securities Taiwan Co., Ltd 的情况，不涉及中信证券及/或其附属机构的情况。如投资者浏览上述网址时遇到任何困难或需要过往日期的披露信息，请联系 compliance_hk@clsa.com.

美国：本研究报告由中信证券编制。本研究报告在美国由中信证券（CITIC Securities International USA, LLC（下称“CSI-USA”）除外）和 CLSA group of companies（CLSA Americas, LLC（下称“CLSA Americas”）除外）仅向符合美国《1934 年证券交易法》下 15a-6 规则定义且分别与 CSI-USA 和 CLSA Americas 进行交易的“主要美国机构投资者”分发。对身在美国的任何人士发送本研究报告将不被视为对本报告中所评论的证券进行交易的建议或对本报告中所载任何观点的背书。任何从中信证券与 CLSA group of companies 获得本研究报告的接收者如果希望在美国交易本报告中提及的任何证券应当分别联系 CSI-USA 和 CLSA Americas.

英国：本段“英国”声明受英国法律监管并依据英国法律解释。本研究报告在英国须被归为营销文件，它不按《英国金融行为管理手册》所界定、旨在提升投资研究报告独立性的法律要件而撰写，亦不受任何禁止在投资研究报告发布前进行交易的限制。本研究报告在欧盟由 CLSA （UK）发布，该公司由金融行为管理局授权并接受其管理。本研究报告针对《2000 年金融服务和市场法 2005 年（金融推介）令》第 19 条所界定的在投资方面具有专业经验的人士，且涉及到的任何投资活动仅针对此类人士。若您不具备投资的专业经验，请勿依赖本研究报告的内容。

一般性声明

本研究报告对于收件人而言属高度机密，只有收件人才能使用。本研究报告并非意图发送、发布给在当地法律或监管规则下不允许该研究报告发送、发布的人员。本研究报告仅为参考之用，在任何地区均不应被视为出售任何证券或金融工具的要约，或者证券或金融工具交易的要约邀请。中信证券并不因收件人收到本报告而视其为中信证券的客户。本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，不应被视为对特定客户关于特定证券或金融工具的建议或策略。对于本报告中提及的任何证券或金融工具的分析，本报告的收件人须保持自身的独立判断。

本报告所载资料的来源被认为是可靠的，但中信证券不保证其准确性或完整性。中信证券并不对使用本报告所包含的材料产生的任何直接或间接损失或与此有关的其他损失承担任何责任。本报告提及的任何证券均可能含有重大的风险，可能不易变卖以及不适用所有投资者。本报告所提及的证券或金融工具的价格、价值及收益可能会受汇率影响而波动。过往的业绩并不能代表未来的表现。

本报告所载的资料、观点及预测均反映了中信证券在最初发布该报告日期当日分析师的判断，可以在不发出通知的情况下做出更改，亦可因使用不同假设和标准、采用不同观点和分析方法而与中信证券其它业务部门、单位或附属机构在制作类似的其他材料时所给出的意见不同或者相反。中信证券并不承担提示本报告的收件人注意该等材料的责任。中信证券通过信息隔离墙控制中信证券内部一个或多个领域的信息向中信证券其他领域、单位、集团及其他附属机构的流动。负责撰写本报告的分析师的薪酬由研究部门管理层和中信证券高级管理层全权决定。分析师的薪酬不是基于中信证券投资银行收入而定，但是，分析师的薪酬可能与投行整体收入有关，其中包括投资银行、销售与交易业务。

若中信证券以外的金融机构发送本报告，则由该金融机构为此发送行为承担全部责任。该机构的客户应联系该机构以交易本报告中提及的证券或要求获悉更详细信息。本报告不构成中信证券向发送本报告金融机构之客户提供的投资建议，中信证券以及中信证券的各个高级职员、董事和员工亦不为（前述金融机构之客户）因使用本报告或报告载明的内容产生的直接或间接损失承担任何责任。