

“问道”比特币，国内区块链投资柳暗花明

—— 区块链主题研究报告系列之二

✉ : 王鹏 执业证书编号: S1230514080002; 廖凌 执业证书编号: S1230514080001
☎ : 021-80106010 021-80105932
✉ : wangpeng@stocke.com.cn liaoling@stocke.com.cn

报告导读

比特币是目前区块链技术最成熟的应用，对其产业链的研究对于挖掘区块链领域投资机会大有裨益。

投资要点

□ 追本溯源，国内区块链发展还需“问道”比特币

2012 年~2015 年，国外区块链领域的吸引的风投资金增长超过了 200 倍，累计投资已达 10 亿美元左右，创业方向主要集中在智能合约、证券交易结算、身份证明、分布式记账、电子商务、数据 API 以及区块链基础设施等领域；国内的区块链创业略显沉寂。比特币是区块链最成熟的应用，国内公司在除了支付环节以外的几乎所有环节都占据了绝对的优势，“问道”比特币，将对国内区块链的投资机会的挖掘大有裨益。

□ 比特币产业链完整，是目前区块链技术最成熟的应用

比特币产业链上游是芯片和矿机生产商，有能力生产高性能矿机芯片的企业就可能垄断比特币的发行权；中游主要参与者有矿工、矿池和电力提供商，以及一些提供算力交易平台、矿机托管的衍生服务提供商。其中矿池居于核心环节，主要目的是为了激励算力较低的矿工继续参与挖矿；下游主要是交易和支付环节。国内比特币交易所众多，全球比特币交易量一度有 93% 来自中国交易所。美国在支付环节创新更胜一筹，主要的创新有：比特币支付平台、比特币钱包和比特币 ATM 机。

□ 比特币区块链缺点明显，对其的扩展及竞争链出现将激活区块链应用

比特币区块链具有区块容量有限、交易确认时间长、能量消耗大等缺点，限制了其直接大规模应用。对比特币区块链的扩展主要有彩色币、闪电网络和侧链；主要的竞争链有 Ethereum（以太坊）和 Ripple（瑞波币）。这些扩展和竞争链：1）为区块链技术未来大规模应用提供了有益的探索；2）也为国内区块链创业指明了方向。

□ 三条路径可从比特币产业链切入区块链

1) 核心人员自主创业，主要代表有 onchain（小蚁 antshares 系统，用于非上市股权登记、结算等）、太一科技；2) 比特币产业链公司转型区块链服务提供商，典型代表 BitFury（由矿机芯片生产转型区块链服务提供商），建议关注国内三大矿机芯片生产商深圳比特泉、嘉楠耘智和比特大陆，此外建议关注交易所火币网、BTCC；3) 与 Fintech 类上市公司合作，通过技术授权或直接被并购推广区块链应用，建议关注飞天诚信、广电运通、赢时胜、御银股份、卫士通、信雅达和恒生电子等上市公司在区块链技术方面的布局进展。

相关报告

区块链：链接万物，信由心生——区块链主题研究报告系列之一_20160410
公众与资本关注度飙升，区块链蓄势待发——Signal or Noise 2016 年第 3 期_20160404

报告撰写人：王鹏；廖凌
数据支持人：王鹏；廖凌；李锋

正文目录

| | | |
|----|---------------------------------|----|
| 一、 | 追本溯源，国内区块链发展还需“问道”比特币 | 4 |
| 二、 | 比特币产业链完整，是目前区块链技术最成熟的应用 | 4 |
| 1. | 上游：芯片和矿机生产商垄断着比特币的发行权 | 4 |
| 2. | 中游：集群化挖矿成必选项，云算力交易平台未来有望成为产业链中心 | 7 |
| 3. | 下游：国内交易环节创业占主流，美国支付环节创新更胜一筹 | 11 |
| 三、 | 区块链是比特币的核心和基础架构 | 14 |
| 1. | 去中心化、去信任、集体维护和可靠数据库是区块链的四大特点 | 14 |
| 2. | 与现有的中心化系统相比，区块链更安全、更快速和更便宜 | 15 |
| 3. | 比特币区块链的三大缺陷 | 15 |
| 四、 | 比特币区块链的扩展和竞争链 | 17 |
| 1. | 比特币区块链的扩展 | 17 |
| 2. | 区块链的共识机制与竞争币（链） | 18 |
| 五、 | 从比特币产业链切入区块链的三条路径 | 21 |
| 1. | 比特币产业链的核心人员自主创业进军区块链 | 21 |
| 2. | 比特币产业链公司转型区块链服务提供商 | 22 |
| 3. | 比特币产业链公司与 Fintech 类上市公司合作 | 24 |

图表目录

| | | |
|-------|---|----|
| 图 1: | 比特币产业链示意图 | 4 |
| 图 2: | GPU 比 CPU 中有更多晶体管用于数据处理 | 5 |
| 图 3: | ASIC 芯片专为矿机量身定做，执行速度快于 FPGA | 5 |
| 图 4: | 比特币矿机芯片经历了从 CPU、GPU、FPGA 和 ASIC 四个阶段 | 5 |
| 图 5: | ASIC 芯片挖矿的优点 | 6 |
| 图 6: | 比特币挖矿流程 | 7 |
| 图 7: | 已生成比特币产量走势图，2012 年 11 月 28 日每 10 分钟新增产量首次减半 | 8 |
| 图 8: | 最近一个月全球算力分布（2016.4.19） | 9 |
| 图 9: | 全球前 14 大矿池区块数及其占比（2016.4.19） | 9 |
| 图 10: | 算力吧云算力交易平台的交易界面 | 10 |
| 图 11: | 云算力交易平台未来很可能成为比特币产业链的中心 | 10 |
| 图 12: | 比特币从挖矿到支付的流程图 | 11 |
| 图 13: | 2015.5~2016.4 比特币每日成交量（BTC） | 12 |
| 图 14: | 2015.5~2016.4 比特币每日成交量的美元估值（USD） | 12 |
| 图 15: | 2015.5~2016.4 比特币每日美元价格（USD/BTC） | 12 |
| 图 16: | 2015.5~2016.4 比特币每日交易费率（%） | 12 |
| 图 17: | My Wallet 上托管的在线钱包总数 | 13 |

| | |
|---|----|
| 图 18: My Wallet 用户的日交易总笔数 | 13 |
| 图 19: 世界主要国家的比特币 ATM 机安装情况 | 13 |
| 图 20: 每个区块上记录的信息 | 14 |
| 图 21: 区块链的局部结构 | 14 |
| 图 22: 区块链的四大特点 | 14 |
| 图 23: 中国支付清算系统总体架构图 | 15 |
| 图 24: 比特币区块链中每个区块上平均每天记录的交易笔数 | 16 |
| 图 25: 比特币付费交易中交易确认所需时间的中位值走势图 | 16 |
| 图 26: 采用 ASIC 芯片挖矿每 1GH 算力的耗能情况 | 16 |
| 图 27: 比特币的“挖矿机”高能耗, 算力浪费严重 | 16 |
| 图 28: colu.co 区块链平台的架构示意图 | 17 |
| 图 29: 在线零售商 Overstock 在区块链平台发行自己股票 | 17 |
| 图 30: 闪电网络上的无“中转站式”交易 | 18 |
| 图 31: 闪电网络上的无“中转站式”交易 | 18 |
| 图 32: 五家比特币初创公司使用 Liquid 侧链 | 18 |
| 图 33: BTC Relay 侧链可将比特币网络和以太坊网络连接 | 18 |
| 图 34: 传统的跨境结汇方式存在 2~4 天的延时 | 20 |
| 图 35: 通过 Ripple 支付网络结汇时间可以缩短至 3~5 秒 | 20 |
| 图 36: 小蚁去中心化网络协议 | 21 |
| 图 37: onchain 提供区块链技术服务 | 21 |
| 图 38: 太一科技的核心技术 | 22 |
| 图 39: 太一科技的三大行业解决方案 | 22 |
| 图 40: 不同机型的矿机挖矿的成本与收益情况对比 | 23 |
| 图 41: BitFury 的区块链转型之路 | 23 |
| 图 42: BitFury 转型区块链技术服务之后的业务结构 | 24 |
| 表 1: 各种挖矿芯片的性能比较 | 5 |
| 表 2: 主要矿机厂商最新款矿机的价格和参数对比 | 6 |
| 表 3: 国内三大矿池重点指标对比 (2016.4.19) | 9 |
| 表 4: 国内外主要云算力交易平台设立情况 | 10 |
| 表 5: 国内外主要比特币交易所提供的服务于费用政策 | 11 |
| 表 6: 四种共识机制的比较 | 19 |
| 表 7: 主要在以太坊平台上创建的区块链应用 | 20 |

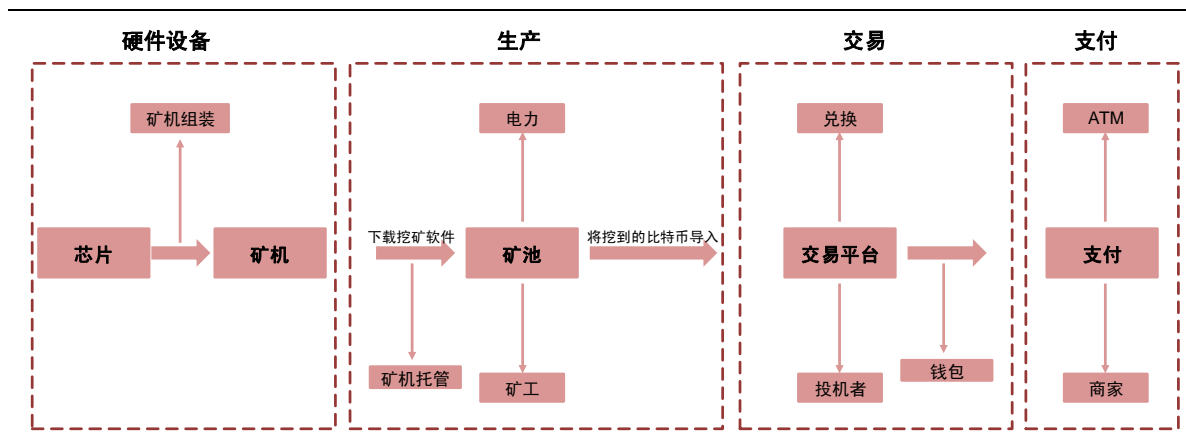
一、 追本溯源，国内区块链发展还需“问道”比特币

国外区块链创业如火如荼进行着。2012 年~2015 年，区块链领域的吸引的风险投资的增长超过了 200 倍，从 2012 年 200 万美元的投资额增加至 2015 年的 4.69 亿美元，累计投资已达 10 亿美元左右。根据 CoinDesk 的比特币创投数据显示，近 200 家风险投资公司已经投资了比特币及区块链领域的创业公司。这些创业公司主要集中在智能合约、证券交易结算、身份证明、分布式记账、电子商务、数据 API 以及区块链基础设施等领域。与国外相比，国内的区块链创业略显沉寂，无论从数量还是涉足的领域看差距都很明显。国内区块链的创业和推广如何发展？最直接的办法就是取经比特币。比特币作为最成熟的区块链应用，已经形成了完整的产业链，并且国内公司在除了支付环节以外的几乎所有环节都占据了绝对的优势，全球前三大矿机和芯片生产商、矿池服务提供商都是国内企业，高盛的报告中也指出全球 80% 的比特币都是通过人民币交易。因此业界一度认为中国控制了比特币。“问道”比特币，将对国内区块链的投资机会的挖掘大有裨益。

二、 比特币产业链完整，是目前区块链技术最成熟的应用

比特币（BitCoin）的概念由中本聪在 2009 年提出，是一种 P2P 形式的数字货币。比特币主要是根据特定算法进行大量的计算后产生，并通过整个 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，同时使用密码学的设计来确保货币流通各个环节安全性。目前，比特币已经形成了完整的产业链，包括上游的硬件设备（包括芯片、矿机）生产商、中游挖矿（比特币生产）以及下游的交易支付环节。

图 1：比特币产业链示意图



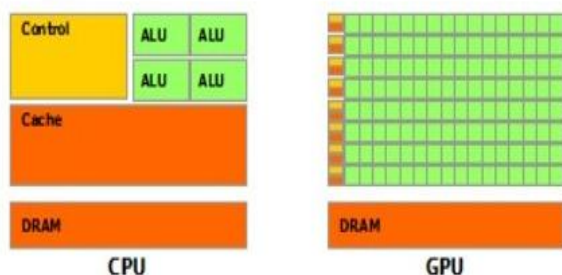
资料来源：浙商证券研究所

1. 上游：芯片和矿机生产商垄断着比特币的发行权

比特币的算法是公开的，代码在 [bitcoin/bitcoin · GitHub](https://github.com/bitcoin/bitcoin) 可以下载，目前由 Gavin Andresen 主持的 Bitcoin Foundation（比特币基金会）来维护。任何人只要具备相应的硬件设备，都可以去官方或者矿池网站上下载相应的客户端参与到挖矿的过程中。能否挖到比特币主要取决于算力的比拼，矿机的性能决定着算力（比特币矿机的算力是指一个挖矿机每秒钟能做多少次 hash 运算，单位为 Hash/s）的大小，而芯片则是矿机生产的关键。因此，有能力生产矿机尤其是矿机芯片的企业就可能垄断着比特币的发行权。

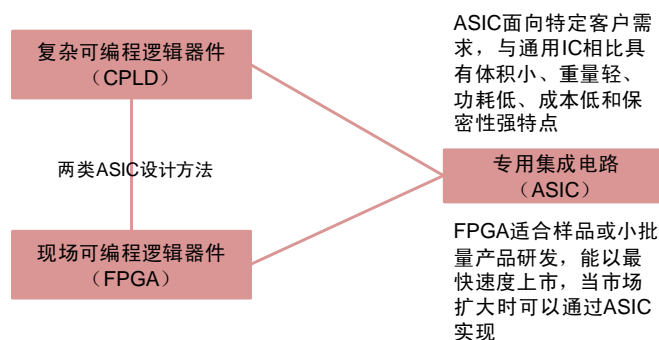
比特币矿机的芯片经历了四个阶段：CPU、GPU、FPGA 和 ASIC。其中 2009 年 1 月比特币创始人中本聪利用电脑 CPU 挖出了第一个创世块，其后大约一年时间 BTC 网络主要依靠 CPU 挖矿，CPU 设计中需要大量的逻辑判断和很强的通用性来处理不同类型的数据，而 GPU 处理简单的 SHA-256 算法速度更具优势；GPU 由于采用了大量并行处理的核心架构，对于简单的 SHA256 算法处理速度较快，2010 年 9 月挖矿进入了 GPU 时代，但是 GPU 也存在功耗高、搭建部署困难的缺陷，不适合大规模部署；2011 年 12 月出现了基于 FPGA 芯片的挖矿设备，其功耗为同类型的 GPU 的 1/40，但是 FPGA 芯片价格昂贵、部署也很复杂，主要被少数具备专业背景的矿工所使用，这个阶段 FPGA 和 GPU 成为挖矿的主力军；2013 年首台基于 ASIC 芯片的 Avalon 矿机面世，挖矿进入了 ASIC 时代。ASIC 芯片是专为挖矿量身定制的芯片，它将 FPGA 芯片中在挖矿时不会使用的功能去掉，与同等工艺的 FPGA 芯片相比执行速度快，大规模生产后的成本也要低于 FPGA 芯片。

图 2: GPU 比 CPU 中有更多晶体管用于数据处理



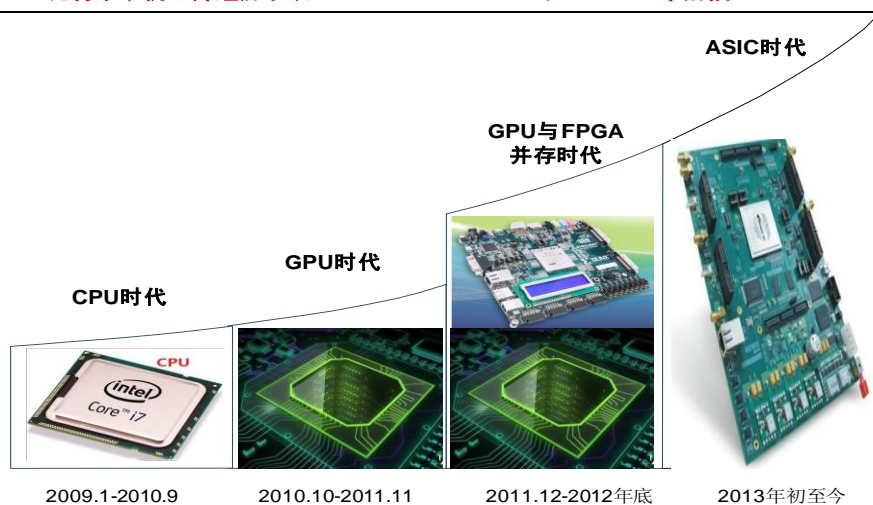
资料来源: OFweek 电子工程网、浙商证券研究所

图 3: ASIC 芯片专为矿机量身定做, 执行速度快于 FPGA



资料来源: 浙商证券研究所

图 4: 比特币矿机芯片经历了从 CPU、GPU、FPGA 和 ASIC 四个阶段



资料来源: 互联网公开资料、浙商证券研究所

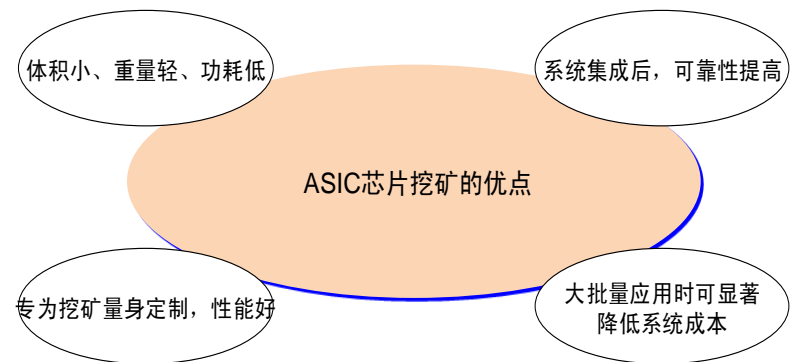
在 CPU、GPU 时代, 挖矿门槛较低, 家庭的普通台式机或者带有独立显卡的笔记本都可以用来挖矿, 2012 年以前挖矿还是大众可以参与的相对公平对等阶段; 随着 FPGA、ASIC 芯片的出现, 挖矿逐渐开始向一些专业人士聚集。ASIC 芯片是为挖矿量身定制的, 与同等工艺的 FPGA 芯片相比 ASIC 芯片的执行速度更快, 大规模生产后成本也会比 FPGA 芯片低。目前 ASIC 芯片已成为主流的矿机芯片, 挖矿速度基本都达到了 GH/S 的级别, 比如 BITMAIN 的第四代芯片 BM1385, 单颗芯片算力可达 32.5GH/S, 在 0.66V 的核心电压下功耗仅为 0.216W/GH/S。ASIC 芯片随着硅片加工精度的提升, 其性能更好, 功耗更低。目前硅片加工精度已经 130nm 提升至 14nm, 基本接近现有半导体技术的极限。

表 1: 各种挖矿芯片的性能比较

| 比较项目 | 电脑 CPU | 独立 GPU | FPGA | 早期 ASIC |
|-------------|-----------|------------|-----------------------------------|--|
| 挖矿速度 (MH/S) | 20-40 | 300-400 | 200 | 289 |
| 矿机功耗 (W) | 100 | 130 | 10 | 6.6 |
| 价格 (元/块) | 1600 | 2000-3000 | 500 左右 | 60 左右 |
| 挖矿门槛 | 低 | 低 | 高 | 高 |
| 主要生产商 | Intel、AMD | AMD、Nvidia | Altera、Xilinx、Actel、Lattice、Atmel | Alchip、KnCMiner、Avalon、BITMAIN、ASICMiner、BitFury |

资料来源: 中关村在线、互联网公开资料、浙商证券研究所

图 5: ASIC 芯片挖矿的优点






资料来源：浙商证券研究所

矿机生产商主要分为两类：一类是自己设计和生产 ASIC 芯片，用自产芯片组装矿机。此类矿机生产商占多数，毕竟芯片性能高低构成了矿机的核心竞争力。比如国外的 KnCMiner、21 Inc 和 CoinTerra，国内的 ASICMiner（深圳烤猫）、Avalon（阿瓦隆）、BITMAIN（比特大陆）和龙矿科技。拥有自产芯片的矿机生产商的盈利能力强，普遍的毛利率达到 50%以上。国产矿机的算力输出大约可达世界总算力的 40%-50%；另一类是通过外购 ASIC 芯片来组装矿机。比如人人网创始人杨曜睿的 ASICM 矿机采用期货矿机的营销模式，将收到的预付款的 80% 用来采购芯片及其他组件，然后进行矿机组装发货，其芯片主要向 Avalon 采购。

矿机的定价目前主要按照比特币来定价，因而其价格容易受比特币价格波动的影响，加之单台矿机部署芯片的性能和数量的差异，矿机价格从几千元到几万元不等。矿机的算力经历了最初 MH/S 级到 GH/S 级，目前已经进入 TH/S 级阶段，最新款的矿机的算力普遍超过 1TH/S。由于竞争加剧、比特币价格的下跌，导致在算力大幅提高的情形下矿机的价格却有所下跌。

表 2：主要矿机厂商最新款矿机的价格和参数对比

| 矿机生产商 | 矿机型号 | 售价（元/台） | 主要参数 | 矿机样图 |
|-------|------------------|---------|--|---|
| 比特大陆 | AntMiner S7 | 3950 | 单台算力 4.73TH/S，合计 135 块 BM1385 芯片，墙上功耗 250W/T |  |
| 嘉楠耘智 | AvalonMiner 6.0 | 4883 | 单台算力可达 3.5TH/S，合计 80 块 A3218 芯片，墙上功耗 300W/T |  |
| 深圳烤猫 | ASICMiner Prisma | 1900 | 单台算力 1.4TH/S，配备 BE200 芯片，墙上功耗为 750W/T |  |

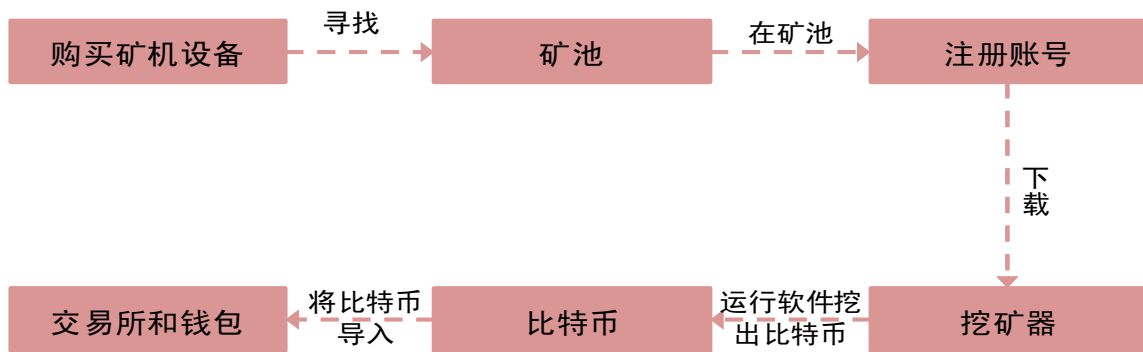
| | | | | |
|---------------------------------|---------------------|-------|--|---|
| CoinTerra | AIRE Miner | 15528 | 配备 16nm 的 ASIC 芯片, 其他参数不详, 功耗可能更低 |  |
| KnCMiner (2014 年售价, 目前不对外销售) | Neptune 2.0 | 65000 | 单台算力 3TH/S, 配备 20nm 的 ASIC 芯片, 速度为一代机的 5 倍, 功耗降低 30% |  |
| 龙矿科技 | 龙矿 T 级 | 2999 | 单台算力 1TH/S, 配备 32 块 28nm 芯片, 墙上功耗 1000W/T |  |
| 21 Inc | 21 Bitcoin Computer | 2600 | 单台算力在 50~125GH/S, 功耗比为 0.17J/GH 该产品是基于 Linux 的小型硬件设备, 将比特币协议作为操作系统, 设备上任何产品和服务都以比特币的组件的形式嵌入, 产品主要面向开发者 |  |

资料来源: 各公司官网、挖币网、浙商证券研究所

2. 中游: 集群化挖矿成必选项, 云算力交易平台未来有望成为产业链中心

比特币挖矿经历了从个人挖矿到集群化(矿池)挖矿的过程。在 CPU、GPU 时代, 个人参与挖矿还处于相对公平阶段; 进入 FPGA 和 ASIC 时代, 由于算力的大幅度飙升, 想挖到比特币就不得不配备大量的矿机。高昂的矿机成本和电费, 加上嘈杂的噪音使得个人挖矿越来越难。大规模集群化的挖矿模式成为必然的选择。一般挖矿的流程包括购买矿机、寻找矿池、在矿池注册账号、下载挖矿软件、运行软件挖矿和将挖到的比特币导入交易所或比特币钱包等六个环节。

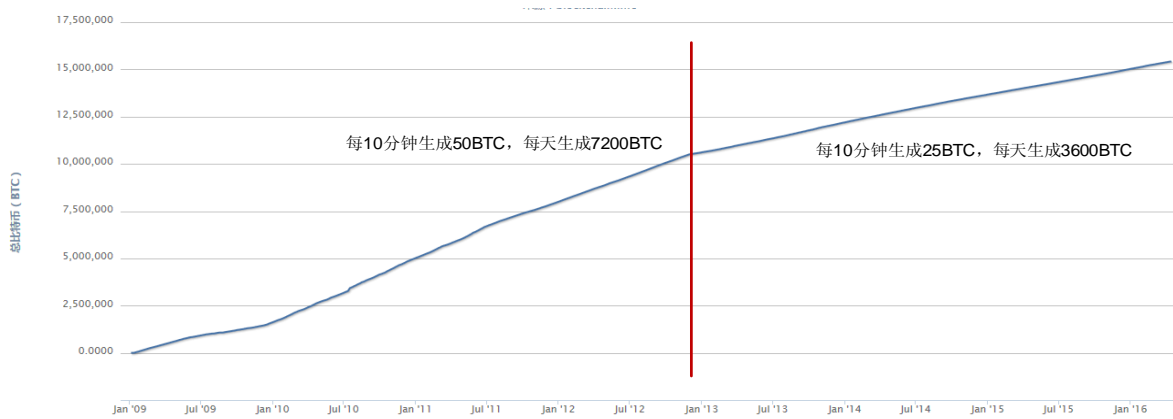
图 6: 比特币挖矿流程



资料来源：浙商证券研究所

比特币的总量是固定的，随着挖到的比特币总量的增加，新比特币的生成速度将会变慢。比特币的总量上限是 2100 万，并且随着比特币的总量增加，新比特币生成的速度会放慢。2009 年比特币诞生之初，每次挖矿的奖励是 50 个比特币，并以每 10 分钟 50 个的速度增加，当总量达到 1050 万时，即 2100 万的一半时，每 10 分钟可获得的奖励减半为 25 个，当总量达到 1575 万时，即新增量达到 1050 的一半时，每 10 分钟获得的比特币再减半为 12.5 个。以此类推，预计到 2140 年，比特币将达到 2100 万个的总量上限。2012 年 11 月 28 日比特币每 10 分钟新增产量首次减半。根据 blockchain.info 的数据，截至 2016 年 4 月 13 日，已产出的总比特币数量 1542.82 万 BTC。目前每 10 分钟生成 25BTC，每天可生成 3600 BTC。预计 2016 年 6 月下旬比特币每 10 分钟新增产量将再次减半，每 10 分钟生成 12.5BTC，每天生成 1800BTC。

图 7：已生成比特币产量走势图，2012 年 11 月 28 日每 10 分钟新增产量首次减半



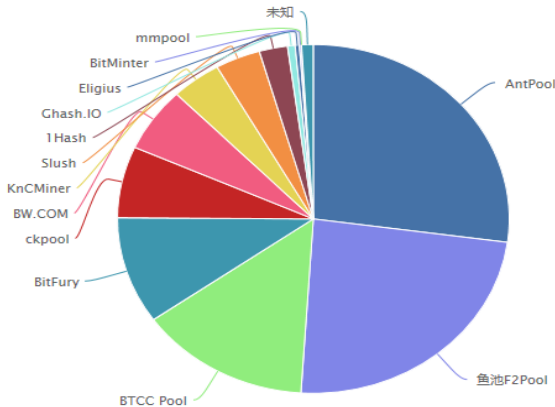
资料来源：blockchain.info、浙商证券研究所

矿池一般是指对外开放的团队开采服务器。中本聪描述的比特币世界中，全网平均每 10 分钟产生一个区块，每区块可产生 50(目前是 25)个比特币，而一个区块只可能被某个幸运儿挖走，直接拥有 50(现在是 25)个比特币，挖到的概率与矿工投入的设备算力大小成正比。因此随着挖矿参与人数增加且分散到一定程度后，挖到比特币的概率将无限接近于零。单独一个矿工投入一台矿机挖矿可能要 5~10 年才能开采到一个区块。矿池就是为了激励算力较低的矿工继续参与挖矿，在一个矿池里，不同的矿工贡献出自己的算力来生成一个区块，然后再根据每个人的贡献比例来分发奖励。

矿池的分配方式目前主要有三种：PPLNS、PPS 和 PROP。PPLNS (Pay Per Last N Shares)，根据过去 N 个股份来支付挖矿收益，即一旦生成了一个区块，将根据所有曾经参与这个区块生成的每个人在生成这个区块 N 个股份中贡献的股份比例来分配区块中的比特币。PPLNS 分配方式下矿工必须在区块生成之后才能获得收益，因而会有一定的延迟；**PPS (Pay Per Share)**，即为每一个股份支付报酬。分配的比特币源于矿池现有的资金，可以立即取现而不用等待区块生成完毕或者确认。这样可以避免矿池运营者幕后操纵，减少了矿工的风险，但将风险转移给了矿池的运营者。目前 PPS 分配方式中矿池先估算每天可以获得的比特币，然后根据你的算力在矿池中的占比分配给你基本固定的收益；**PROP (Proportional) 模式**下一旦生成一个区块，**区块生成时的每个矿工**将按照自己贡献的份额获取相应比例的比特币奖励。

目前，全球算力前五大矿池是 AntPool、鱼池 F2Pool、BTCC Pool、BitFury 和 ckpool，合计挖出的区块数占全球总区块数的 81.74%。其中，前三大矿池都是我国的，合计挖出的区块数占全球总区块数的 65.21%。其中 AntPool 由矿机生产商比特大陆公司创建，由比特大陆的蚂蚁矿机提供算力支持；鱼池 F2Pool 是由国内两名技术宅男于 2013 年 5 月 5 日创建，其算力曾经占据全球算力榜首；BTCC Pool 是由国内首个比特币交易所 BTCChina（比特币中国）创建；BitFury 则是由拉脱维亚人瓦列里·瓦维洛夫（Valery Vavilov）创办，它没有公共矿池，但在芬兰、冰岛和格鲁吉亚拥有私人矿池；CKPool 是澳大利亚麻醉师兼程序员 Con Kolivas 和另一位合伙人 Kano 于 2014 年 9 月创建的公共矿池。

图 8：最近一个月全球算力分布（2016.4.19）



资料来源：QuKuai.com、浙商证券研究所

图 9：全球前 14 大矿池区块数及其占比（2016.4.19）

| 矿池 | 区块数 | 占比 (%) |
|-----------|------|--------|
| AntPool | 1222 | 27.16% |
| 鱼池 F2Pool | 1074 | 23.87% |
| BTCC Pool | 638 | 14.18% |
| BitFury | 446 | 9.91% |
| ckpool | 298 | 6.62% |
| BW.COM | 269 | 5.98% |
| KnCMiner | 185 | 4.11% |
| Slush | 168 | 3.73% |
| 1Hash | 105 | 2.33% |
| Ghash.IO | 28 | 0.62% |
| Eligius | 16 | 0.36% |
| BitMinter | 7 | 0.16% |
| mmpool | 1 | 0.02% |
| 未知 | 43 | 0.96% |

资料来源：QuKuai.com、浙商证券研究所

表 3：国内三大矿池重点指标对比（2016.4.19）

| 矿池 | 矿池总算力 (PH/S) | 全网算力占比 (%) | 分配方式 | 手续费 (%) | 算力收益 (PH/S) |
|-----------|--------------|------------|-------|---------|-------------|
| AntPool | 350.93 | 29.04% | PPLNS | 0 | 2.79BTC |
| | | | PPS | 2.5 | |
| | | | SOLO | 1 | |
| 鱼池 F2Pool | 304 | 25.16% | PPS | 4 | 2.77BTC |
| BTCC Pool | 175.1 | 14.49% | PPS | 2~3.6 | 2.81BTC |

资料来源：各矿池官网、浙商证券研究所

矿池的盈利模式主要有三种：自己挖矿获得比特币、提供矿池服务收取手续费和算力交易。自己挖矿获得比特币，主要是一些矿机生产商自建的私人矿池，通过挖矿获得比特币来赚取收益。随着挖矿难度日益增加，矿池自己挖矿的收益也在逐渐降低；大多数的公开矿池都是通过提供矿池服务收入一定比例的手续费获得收入。一般根据矿池的分配方式的不同，收取 1%~5% 不等的手续费，有些矿池也会免收手续费；算力交易是指用户可以向矿池购买算力，或者将算力托管给算力交易平台并缴纳一定的维护费用，由算力交易平台统一维护矿机，并按日向用户发放挖取的比特币；用户也可将自己拥有的算力自由交易，以获得更大的收益。

云算力交易平台成为近年来比特币产业链的投资热点。国内外比特币芯片、矿机制造商、矿池、交易平台，甚至比特币媒体、应用厂商纷纷开始涉足。云算力平台有两种类型：1) “自有型”云算力平台，即平台商自建或者投资矿池，自己部署矿机并出售算力，典型代表是 CEX.IO。CEX 是第一家开通购买算力来挖比特币的平台，它拥有全球最大算力的大规模挖矿机阵列，还有矿机出售、矿机租赁以及矿机托管服务等；国内的算力吧 (pow88.com) 则通过与国内矿池合作、收购，曲线入市，并且拥有比特币国际、比特汇、比特帮的技术、媒体和流量资源，发展潜力巨大；2) “平台型”云算力平台，厂商搭建算力交易平台，通过招募矿场主，并将算力注入平台出售。HASHNEST 是最先上线运营的云算力平台。2014 年 9 月 1 日，比特大陆正式宣布完成了对 HASHNEST 收购。被比特大陆收购后，HASHNES 云算力交易平台在挖矿芯片、矿机生产能力、市场运营经验和用户群体方面都拥有明显的竞争优势，未来有望快速成为云算力平台的领导者。

表 4：国内外主要云算力交易平台设立情况

| 上线日期 | 云算力平台 | 类型 | 投资商 |
|----------------|--------------|-----|---------------|
| 2013 年 | CEX | 自有型 | Bitfury |
| 2014 年 9 月 1 日 | hashnest.com | 平台型 | 比特大陆 |
| 2014 年 9 月 2 日 | Knc Cloud | 自有型 | KnCMiner |
| 2014 年 | pow88.com | 自有型 | 比特币国际、比特帮、比特汇 |
| 2014 年 | Digcoin | 平台型 | 火币网 |
| 2014 年 10 月 | AMHash | 自有型 | 深圳烤猫、小强矿机 |

资料来源：互联网公开资料、浙商证券研究所

图 10：算力吧云算力交易平台的交易界面

买入算力

算力品种: PAHASH1

可用余额(BTC): 借贷

买入价(BTC):

买入量(GHS):

总金额(BTC): 0.00000000

隐藏订单: ☐ (加收1%服务费)

立即买入

卖出算力

算力品种: PAHASH1

可卖算力(GHS): 0 借贷

卖出价(BTC):

卖出量(GHS):

总金额(BTC): 0.00

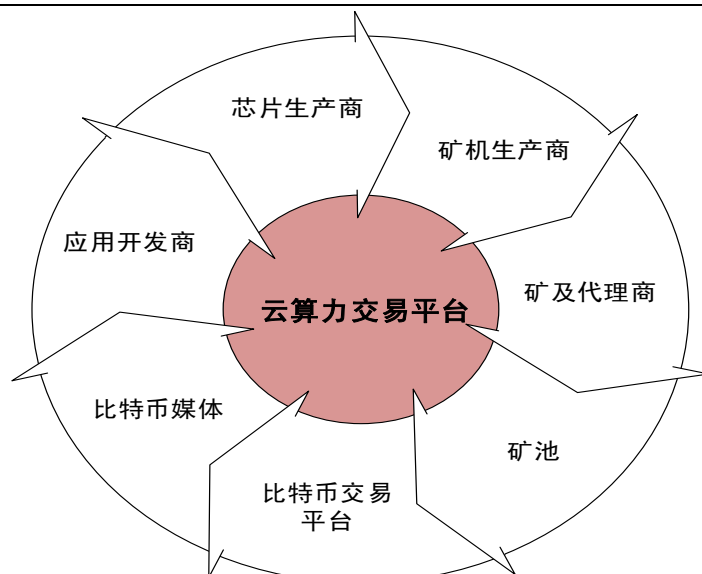
隐藏订单: ☐ (加收1%服务费)

立即卖出

资料来源：pow88.com、浙商证券研究所

云算力交易平台很可能成为未来比特币产业链的中心。随着比特币行业的蓬勃发展和矿机技术的不断进步，矿机的成本也逐步降低。对于普通的比特币投资者而言，矿机部署运维所需要的时间、电力设施的建设以及长期挖矿的耐心，这些都是复杂而难解决的问题。在未来的三到五年，绝大多数矿机将被放置在专业的矿机托管场之中，由企业化、专业化的团队负责搜寻低价的能源，并对矿机进行管理和运维。算力交易替代矿机交易将渐成趋势。

图 11：云算力交易平台未来很可能成为比特币产业链的中心

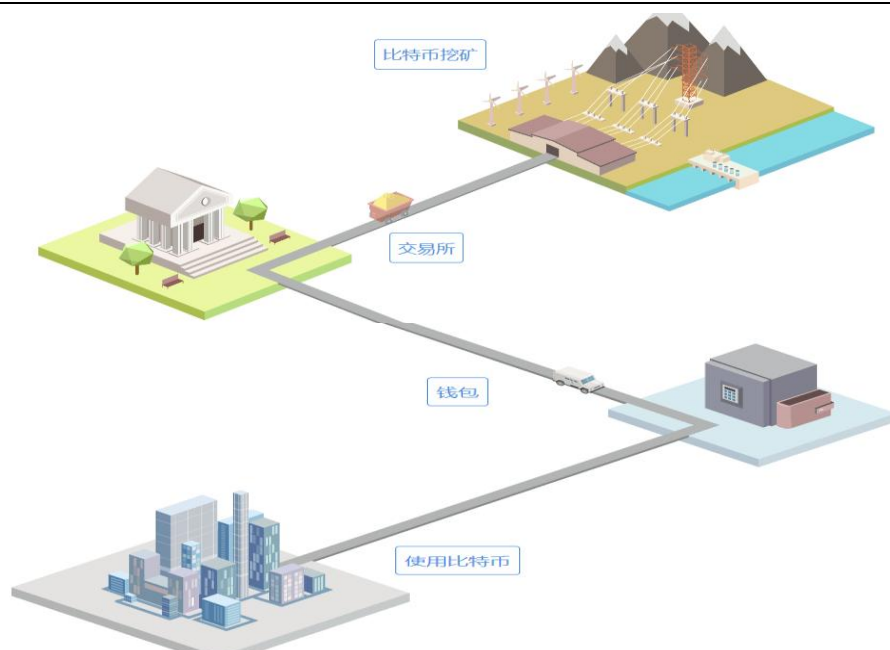


资料来源：浙商证券研究所

3. 下游：国内交易环节创业占主流，美国支付环节创新更胜一筹

由于监管、币值不稳定、受众圈子小等原因，矿工在矿池中挖到的比特币并不能直接进行交易或者支付，而是需要将挖到的比特币导出到比特币交易所后兑换成法币或者储存在比特币钱包中。

图 12：比特币从挖矿到支付的流程图



资料来源：BTCC、浙商证券研究所

交易环节：国内比特币创业中交易平台非常活跃，全球交易量一度有 93% 来自中国。主要原因有二：1) 与芯片、矿机等相比，交易平台的技术、资金门槛相对较低；2) 交易平台具有马太效应，交易量越大正反馈效应越强，交易量达到一定规模以后就会形成一定门槛；3) 国内交易所免收交易环节的手续费的政策吸引了大量的投资者前来交易。

目前全世界大约有 100 多家比特币的交易平台，全球排名前十的比特币交易所大多是在中国、美国以及东欧地区，这些地区的比特币交易量占全球交易量的 90% 以上。美元和人民币对比特币的交易目前是最为活跃两种货币，此外也有相对于日元、澳元、加拿大货币、韩元、巴西货币以及其他货币的比特币交易所。2015 年以来，合规问题已经成为了法币与比特币交易所之间关注的焦点，美国的交易所 Coinbase 以及 itBit 公司已经从美国相关政府部门那里得到了营业执照，在中国政府部门还没有为数字货币制定相关执照。香港的 769 交易所在 2013 年 9 月获得了香港海关颁发的经营金钱服务牌照，796 交易所是一家主营与比特币相关的期货、股票、基金、期权、理财等综合性金融网站，在国内首家推出期货和融资融券服务的比特币网络交易商。

国内外交易所在盈利模式存在差异：国内交易所在比特币的交易环节是免收手续费的，而是在充值和提现环节收取一定手续费，一般收取 0.1%~0.5% 的手续费；国外交易所在比特币的交易环节也收取一定比例的手续费（一般为 1%，最高可达 7%）。国内比特币交易平台主要有火币网、OKCoin 和 BTCC，国外比特币交易平台主要有 BTC-E、Bitstamp、CoinBase 和 itBit。

表 5：国内外主要比特币交易所提供的服务于费用政策

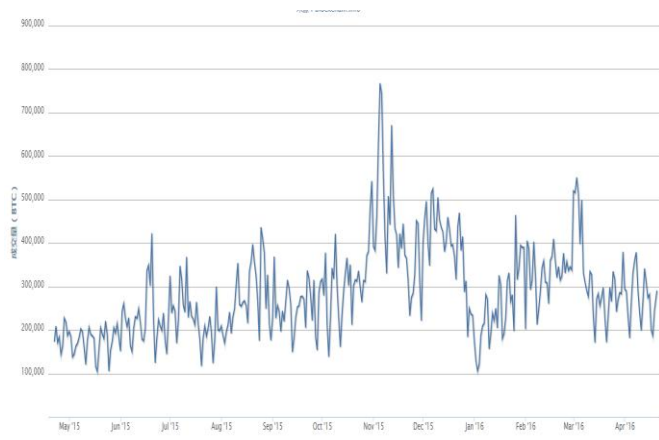
| 国家 | 交易所 | 提供的服务 | 手续费政策 |
|----|--------|-------------------------|---|
| 中国 | 火币网 | 人民币现货、美元现货、杠杆交易、充值提现、钱包 | 人民币现货：交易免费，充值费率 0%，提现按用户等级收取 0.3%~0.5% 手续费 美元现货：交易环节按交易量收取 0.1%~0.2% 手续费，充值费率为 1%~1.5%，提现费率为 0.5%~1% |
| 中国 | OKCoin | 人民币现货、融资融券 | 交易免手续费、充值手续费 0%、提现按用户等级收取 0.3%~0.5% 手续费 |
| 中国 | BTCC | 人民币现货、杠杆交易、钱包 | 交易免手续费、充值除易京东充值收取 0.5%~1%，其他渠道均免费，新生比特币提现费率 10%，人民币提现费率 0.3%~0.38% |

| | | | |
|-------|----------|--------------|--|
| 美国 | CoinBase | 支持多国货币与比特币兑换 | 第一个 100 万美元的交易免费, 后续交易支付 1% 手续费; 提现收取 1% + \$0.15 的服务费 |
| 保加利亚 | BTC -E | 支持多国货币与比特币兑换 | 每一笔交易征收 0.2%-0.5% 的手续费 |
| 斯洛文尼亚 | Bitstamp | 比特币交易、充值、提现 | 交易费用按交易量收取 0.10%-0.25%, 充值免费, 提现 0.90 欧元 |
| 美国 | itBit | 支持多国货币与比特币兑换 | 按交易量不同收取最高不超过 0.2% 的手续费 |

资料来源: 各比特币交易所网站、浙商证券研究所

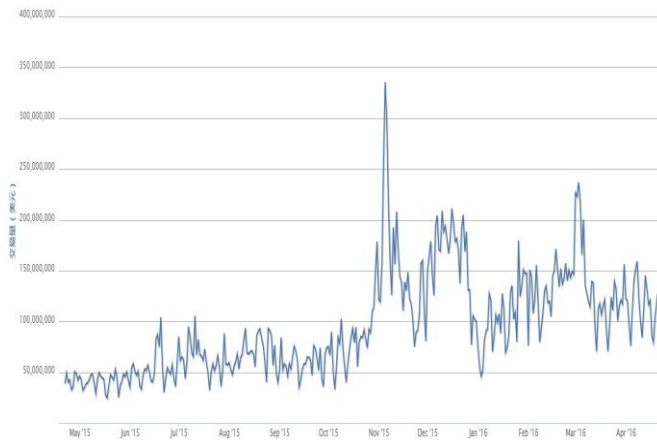
根据 blockchain.info 的数据显示, 最近一年比特币的日均成交量在 20~30 万 BTC 之间, 如果按照美元计价日均的比特币成交价值在 1 亿美元左右, 日均的交易费用在 1%~2.5% 之间。根据 CoinDesk 的数据, 截至 2016 年 4 月 20 日, 已挖出比特币 1545.205 万 BTC, 美元价值达到 67.46 亿, 美元价格 437.1USD/BTC, 人民币价格 2839.49CNY/BTC。

图 13: 2015.5~2016.4 比特币每日成交量 (BTC)



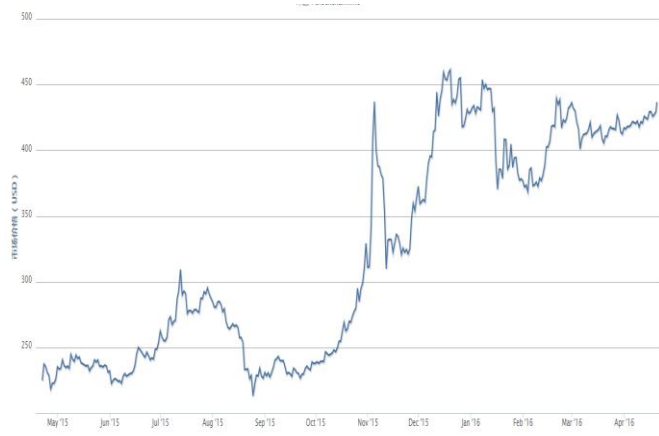
资料来源: blockchain.info、浙商证券研究所

图 14: 2015.5~2016.4 比特币每日成交量的美元估值 (USD)



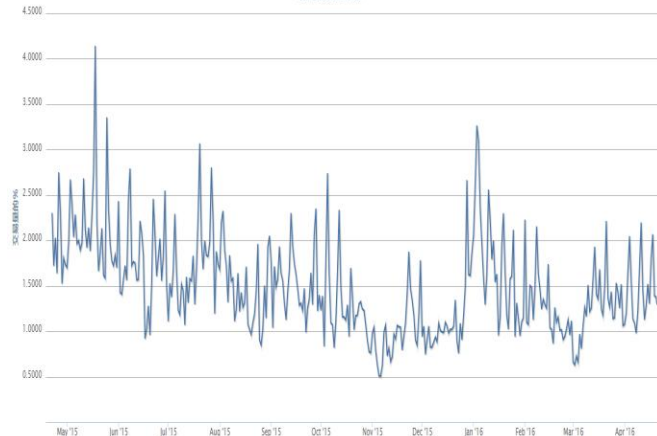
资料来源: blockchain.info、浙商证券研究所

图 15: 2015.5~2016.4 比特币每日美元价格 (USD/BTC)



资料来源: blockchain.info、浙商证券研究所

图 16: 2015.5~2016.4 比特币每日交易费率 (%)



资料来源: blockchain.info、浙商证券研究所

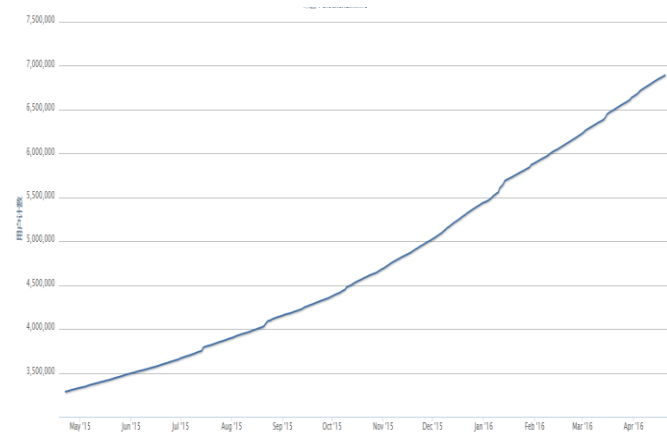
支付环节: 国内受央行政策限制, 支付环节的创新不多; 美国政府将比特币纳入监管范围, 商家对使用比特币支付的接受程度也较高。美国在比特币支付领域的创新主要有: 比特币支付平台、比特币钱包和比特币 ATM 机。

Bitpay 和 Coinbase 是两家比特币支付公司。Bitpay 被称作比特币界的 PayPal, 消费者通过 Bitpay 可以在其认证的商户中使用比特币消费, 同时 Bitpay 为商户提供支付解决方案, 并收取 0.99% 的手续费。商户收到的比特币可以在 Bitpay 兑换成法币, 并且节省了使用信用卡或储蓄卡结算时收取的手续费。目前与 Bitpay 的合作商户超过了 4000 家。Coinbase 为客户提供了即时交易服务, 这项服务允许客户瞬时发送和接收比特币付款, 从而避免比特币汇率波动的影响。该即时交易服务包括发送和接收两大功能。

任何拥有 Coinbase 钱包的客户,发送功能允许其在一页面上发送比特币和支付当地货币,接收功能允许客户在即时接受比特币,并将比特币在交易所自动卖出。目前即时交易服务可以立即转换美元、欧元以及英镑。

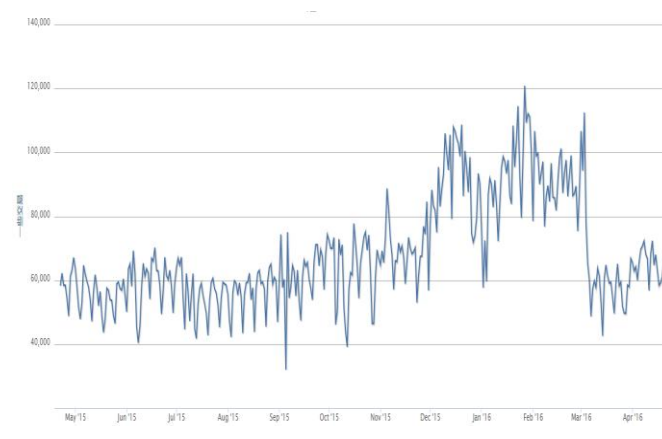
比特币钱包主要是为了方便用户能安全便捷地进行比特币的收支及存储。目前比特币的钱包主要有三类:在线钱包、桌面钱包和移动钱包。钱包主要由一些比特币交易所或者独立供应商提供。美国主流的钱包提供商有:Bitcoin-Qt、MultiBi、Armory、Electrum、Bitcoin Wallet、Blockchain.info 和 Coinbase。根据 Blockchain.info 的数据,My Wallet 的用户总数已经达到了 689.31 万,最近一年日均的交易笔数在 6 万~8 万之间。

图 17: My Wallet 上托管的在线钱包总数



资料来源: blockchain.info、浙商证券研究所

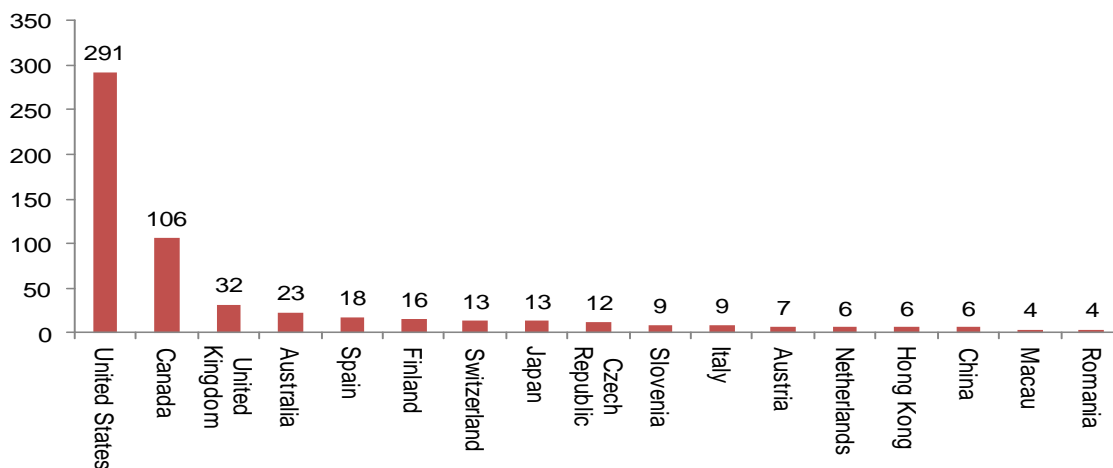
图 18: My Wallet 用户的日交易总笔数



资料来源: blockchain.info、浙商证券研究所

比特币 ATM 机的主要功能是实现比特币和法币的相互兑换,主要分为单向和双向。**单向 ATM 机**只能用法币购买比特币,并从中收取一定比例的手续费。比如 BTCC 在浦东张江开设了中国大陆第一台比特币 ATM 机,只能实现以人民币购买比特币的功能;**双向 ATM 机**既可以出售比特币,又可以购买比特币,ATM 机通过验证人的生物特性来限制每日买入/卖出,从而预防洗钱活动。根据 Bitcoin ATM Map 的统计数据,全球目前共有 633 台比特币 ATM 机,平均费率大约在 7.25%。其中购买比特币的平均费用为 8.10%,卖出比特币的平均费用为 5.36%。主要的比特币 ATM 品牌有 Robocoin、Lamassu、BitAccess、BitXatm、CoinDesk 和 BTCC 等。单向比特币 ATM 机的售价大约在 6500 美元,双向比特币 ATM 机的价格根据功能的差异,价格在 5500 美元~15000 美元之间。

图 19: 世界主要国家的比特币 ATM 机安装情况

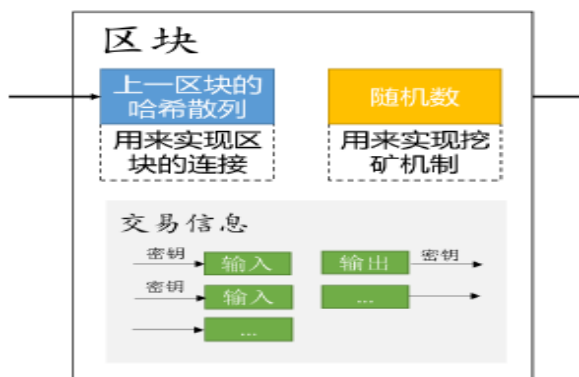


资料来源: Bitcoin ATM Map、浙商证券研究所

三、 区块链是比特币的核心和基础架构

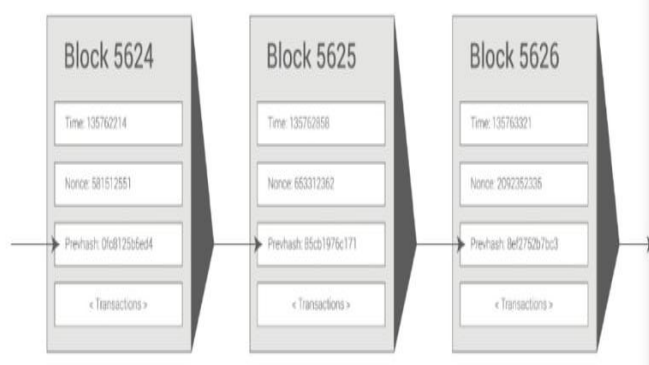
区块（Block）是比特币创造的一个概念，可以理解为记录比特币交易信息的账本。每个区块均包含以下三种要素：1）本区块的 ID；2）若干的交易单；3）前一个区块的 ID。比特币系统每隔 10 分钟创建一个区块，这个区块上记录了这段时间范围内发生所有交易。由于每个区块中包含了前一个区块的 ID，因此可以由这个 ID 找到前一个区块，如此往复，可以一直追溯到起始区块，从而可以生成一条完整的交易链条，形成区块链。

图 20：每个区块上记录的信息



资料来源：互联网公开资料、浙商证券研究所

图 21：区块链的局部结构



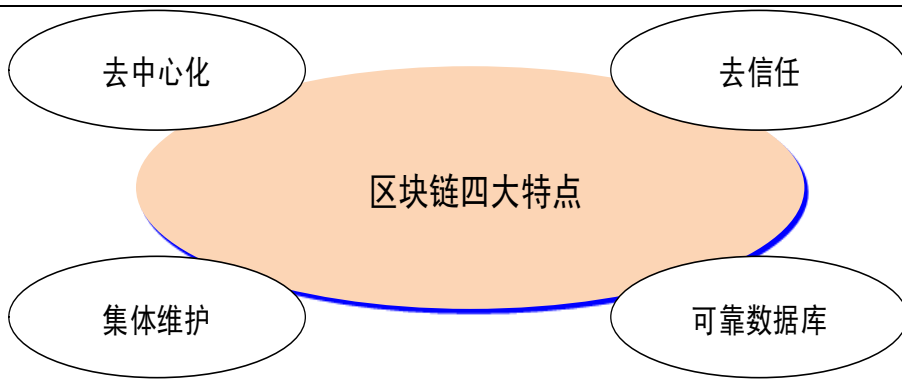
资料来源：互联网公开资料、浙商证券研究所

因此，区块链是通过一串使用密码学方法相关联产生的数据块，每个数据块中包含了一段时间内的系统全部交易信息。整个区块链就是记录比特币交易信息的公共账本，网络中的每一个区块都有比特币交易信息的备份。当发起一次比特币交易时，信息被广播到网络中，通过算力的比拼而获得合法记账权的矿工将交易信息记录成一个新的区块连接到区块链中，一旦被记录，信息就不能被随意篡改。**区块链才是比特币的核心和基础架构。**

1. 去中心化、去信任、集体维护和可靠数据库是区块链的四大特点

去中心化（Decentralized）：整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，而且某一节点的损坏或者失去都不会影响整个系统的运作。**去信任（Trustless）**：参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，所有的数据内容也是公开的，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。**集体维护（Collectively maintain）**：系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。**可靠数据库（Reliable Database）**：整个系统将通过分布式数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。因此参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

图 22：区块链的四大特点

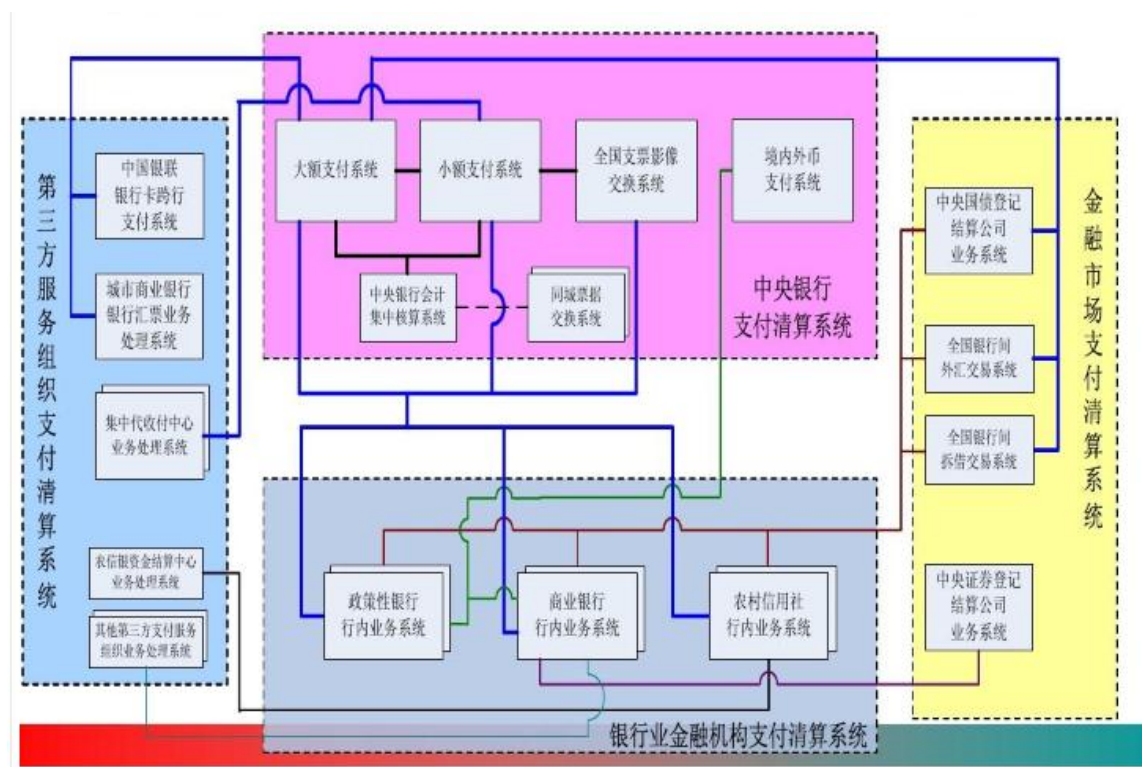


资料来源：浙商证券研究所

2. 与现有的中心化系统相比，区块链更安全、更快速和更便宜

传统的中心化系统之间进行交易的需要一个可信任的第三方机构作为中介。比如我国的支付清算系统中就存在四大中心化的支付清算系统，包括中央银行支付清算系统、银行业金融机构支付清算系统、金融市场支付清算系统和第三方服务组织支付清算系统。**去中心系统与现有的中心化系统相比：更安全、更快速和更便宜。**首先，**去中心化的系统更安全**。去中心化的系统中数据存储在分布式节点中，每个节点都能获得一份完整数据库备份。除非能够同时控制整个系统中超过 51% 的节点，否则对单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。因此区块链能更好地抵御黑客攻击，同时由于避免了对单一中心的依赖，也有效防止了中心的道德腐败；其次，**去中心化的系统更快速**。在区块链系统中，交易结算几乎同步发生，交易双方在交易确认后不需要各自核对账目。在交易通过 POW 或其他方式验证之后，新的区块将写入分布式账本，所有区块的账本将同时更新，所有节点仍共享完全一致的账本。最后，**去中心化的系统更便宜**。比如在银行结算领域里，区块链技术可以帮助银行节省跨境支付基础设施建设、证券交易和监管合规等方面的成本。据西班牙银行的奥利弗·威曼（Oliver Wyman）和风险投资者安泽米斯（Anthemis）的报告，如果采用区块链技术，到 2022 年以前银行每年在这些方面能够节约 150-220 亿美元。德国的 Fidor 银行在应用 Ripple 协议后以前某个业务的手续费由 5 欧元/笔缩减为 0.49 欧元/笔，为原有的 1/10。

图 23：中国支付清算系统总体架构图

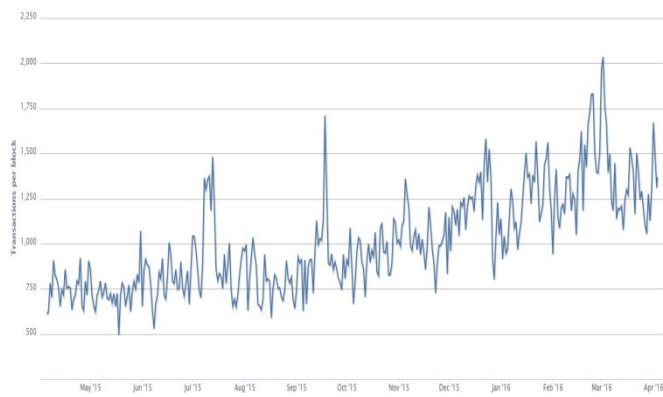


资料来源：央行支付结算司、王关荣、浙商证券研究所

3. 比特币区块链的三大缺陷

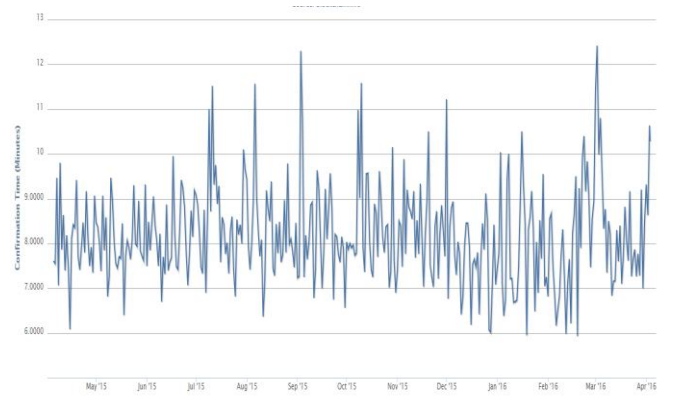
比特币是目前最大的区块链，但是具有**区块容量限制、交易确认时间长、能量消耗大**等缺点，成为限制其在其他领域进行大规模商业化应用的不利条件。1) **区块容量限制**：中本聪设计比特币区块链时，人为设置了每个区块 1MB 的大小限制。随着比特币发行量的增多和应用的推广，目前比特币网络已经接近了这个上限，这导致了交易时间延长，甚至在高峰时一些交易请求无法成功。对于是否应该提高区块容量上限的问题，比特币社区内部也存在巨大的分歧；2) **交易确认时间长**：比特币的区块链中每个新区块的生成平均需要 10 分钟，如果要保证交易的不可逆转，该笔交易通常需要至少 6 个区块的确认，即该交易的最终确认需要 1 个小时。再加上区块大小的限制（每块最多可以容纳 4,096 笔交易），比特币网络每秒只能处理 7 笔交易，远远低于 Visa 和 Master 网络每秒上万笔交易的能力；3) **能耗高，算力浪费严重**：比特币矿工目前的“挖矿”设备已经由 300MH/S 的 CPU 升级到了 5TH/S 的 ASICs。据估计，目前比特币网络处理一笔交易的耗电量相当于美国一个家庭一天的耗电量，对应的碳排放有 534 吨/日或 825 万吨/年。

图 24：比特币区块链中每个区块上平均每天记录的交易笔数



资料来源：BlockChain.info、浙商证券研究所

图 25：比特币付费交易中交易确认所需时间的中位值走势图



资料来源：BlockChain.info、浙商证券研究所

图 26：采用 ASIC 芯片挖矿每 1GH 算力的耗能情况

| 矿机 | 矿机算力GH/S | 矿机耗能 | 矿机耗能率W/GH | 矿机卖价 |
|-------------------------|----------|------|-----------|----------|
| Cointerra TerraMiner IV | 2000 | 2200 | 1.10000 | \$5,999 |
| KnC Neptune | 3000 | 2200 | 0.73333 | \$9,995 |
| Hashcoins Zeus** | 3500 | 2400 | 0.68571 | \$10,999 |
| Extolabs EX1*** | 3600 | 1900 | 0.52778 | \$9,499 |
| Minerscube 15*** | 15000 | 2475 | 0.16500 | \$9,225 |

资料来源：Bitcoin Wiki,2014、浙商证券研究所

图 27：比特币的“挖矿机”高能耗，算力浪费严重



资料来源：互联网公开资料、浙商证券研究所

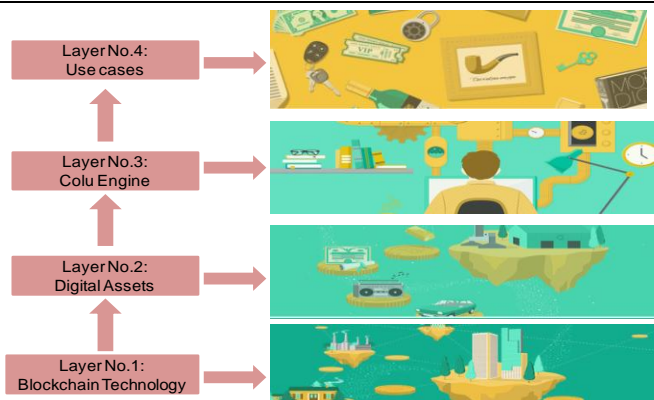
四、 比特币区块链的扩展和竞争链

1. 比特币区块链的扩展

比特币区块链具有**区块容量限制、交易确认时间长和能耗高，算力浪费严重**等缺点，因此直接建立在比特币区块链上的各种应用都会面临以上缺点的掣肘。为了扩展比特币区块链的应用，产生了一些建立在比特币区块链网络协议之上的新的协议，这些新协议在克服了比特币区块链的相关缺点的同时，依托比特币区块链提供相应的网络安全保障。目前建立在比特币区块链的新协议主要有**彩色币（colored coin）、闪电网络（lightning-network）和侧链（sidechain）**。

彩色币（colored coin）：彩色币是比特币区块链入门级的应用，使用的是 BitcoinX 协议，其目的是将比特币网络（技术）与货币价值分割开来，并使用比特币网络技术来明晰交易路径以避免重复消费。彩色币是可以被跟踪的一些特定比特币，具有一些特殊的属性，比如支持代理或聚集点，其价值取决于用户对这种稀有货币的需求。彩色币本身就是比特币，存储和转移不需要第三方，可以利用已经存在的比特币的基础。彩色币可以用作替代货币、商品证书、智能财产以及其他金融工具等。彩色币比较著名的应用有两个：**1）Colu 公司推出的 colu.com 区块链平台**。这个平台可以让不懂比特币的开发商和消费者也能在平台上登记和交换资产，从金融资产（股票、债券、股票）到记录（证书，版权，文件）再到所有权（活动门票、代金券、礼品卡）。目前 Colu 已经推出了测试版，并与 Revelator 在简化音乐版权管理方面展开了合作。Ubitquity LLC 也采用了 Colu 的彩色币实现方案来进行房地产产权登记管理；**2）Overstock 公司开发的 tØ.com 区块链平台**。tØ 平台采用了彩色币（colored coin）的技术，一个彩色币可以被标记为谁拥有了 Overstock 股份证明的代币，这项技术是建立在比特币区块链之上的，并且由比特币分布式账本负责保护。在 tØ 平台上发行股票可以视为“交易即结算”，可以大幅缩短交易结算时间。

图 28：colu.co 区块链平台的架构示意图



资料来源：Colu 官网、浙商证券研究所

图 29：在线零售商 Overstock 在区块链平台发行自己股票



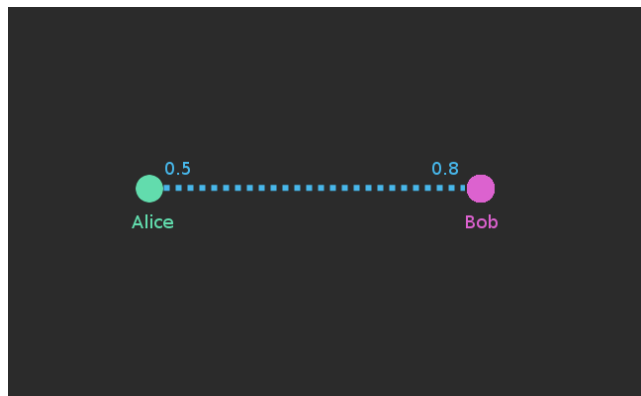
资料来源：互联网公开资料、浙商证券研究所

闪电网络（lightning network）：闪电网络是一种分布式小额支付网络，其目的是将比特币的绝大多数交易带离区块链，而且不牺牲去信任以及安全性，实现安全的 off-blockchain 交易模式。闪电网络可以看做在比特币区块链上创建了“微支付渠道”，除发起通道的初始交易之外，比特币交易可在无需与区块链进行互动的情况下还可安全地进行，并且在闪电网络上交易也不存在交易对手的风险：如果任何一方终止合作，或者说在约定的时间内没有响应，该通道可以被关闭。与比特币支付相比，闪电网络里的交易可以在**瞬间完成**，并且可以将比特币的**日交易量扩充到数十亿笔/天**。由于极少地使用到区块链，因此所需的交易费用也很少。

无“中转站式”交易：交易双方需要先创建通道进行交易。当这个渠道处于开放状态时，双方任何时候都可不通过上链交易就可以共同协商修改支付分配；当要关闭这个渠道时，双方中的任意一方均有一秒的反应时间，比特币网络的链上交易将替双方支付这次交易所需费用。例如，Alice 在渠道中投入 0.5BTC，Bob 在渠道中投入 0.8BTC，创建一个支付通道。当 Alice 想要支付 Bob 0.1BTC 时，他们可以更新支付分配，其中 Bob 可以得到 0.9BTC，Alice 则会得到 0.4BTC。只要这个通道一直处于开放状态，那他们就可以无限制的进行交易，这期间的交易并不需要通过比特币区块的确认，直至交易最终完成并且通道关闭时再由比特币区块的确认和支付交易费用。

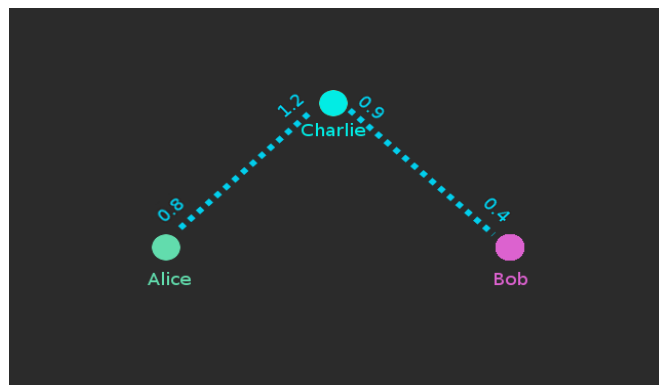
“中转站式交易”：交易双方如果没有直接的通道，但是同时与同一第三方之间存在交易通道，那么交易双方就可以借助第三方的通道来完成交易，这时就可以扩展为一个支付网络。例如 Alice 想要支付 0.5BTC 给 Bob，但她并没有一个渠道来和他进行交易。不过他们都和查理有一个交易渠道，这样爱丽丝就可借助查理的交易渠道，通过相关智能合约来和鲍勃进行交易。

图 30：闪电网络上的无“中转站式”交易



资料来源：巴比特、Chris Pacia、浙商证券研究所

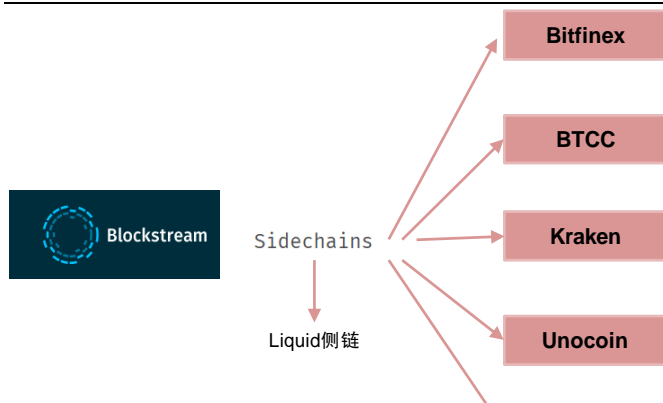
图 31：闪电网络上的无“中转站式”交易



资料来源：巴比特、Chris Pacia、浙商证券研究所

侧链 (side chain)：侧链是比特币主区块链之外的另一个区块链，锚定了比特币主区块链中的某一个节点，可以通过主链上强大的计算力来维护侧链的真实性，并且两个链之间可以进行一些数据交换。每一条侧链可以对应一定的应用场景，然后通过比特币的主区块链保证侧链的安全。比如，闪电网络就是在 Blockstream 公司的 α 元素侧链运行。比较著名的侧链及应用：1) Blockstream 于 2016 年 1 季度推出的侧链——**Liquid 侧链**的交易所，五大比特币初创公司 (Bitfinex、BTCC、Kraken、Unocoin 以及 Xapo) 将会使用该私有侧链，资金移动所需的时间将从 60 分钟缩短至秒；2) ConsenSys 公司于 2016 年 5 月推出的 **BTC Relay 侧链**。该侧链可以把以太坊网络与比特币网络以一种安全去中心化的方式连接起来，BTC Relay 侧链通过使用以太坊的智能合约功能可以允许用户在以太坊区块链上验证比特币交易；3) Rootstock: Rootstock 是一个通过侧链的形式依附于比特币区块链的智能合约平台，可以为核心比特币网络增加价值和功能。Rootstock 移除了“ether”这种代币的需求，使用了一种可转换为比特币的代币，以此作为智能合约的“燃料”，成为以太坊虚拟机的一个改进版本。

图 32：五家比特币初创公司使用 Liquid 侧链



资料来源：Blockstream、浙商证券研究所

图 33：BTC Relay 侧链可将比特币网络和以太坊网络连接



资料来源：巴比特、浙商证券研究所

2. 区块链的共识机制与竞争币（链）

比特币区块链之所以可以去中心化和去信任，具有很高的安全性，主要在于其共识机制是建立在工作量证明 (POW) 的基础之上。因此，共识机制在区块链中起着至关重要的作用。除了 POW 之外，还有 POS、DPOS 和 dBFT 等共识机制。

POW (工作量证明): POW 机制中根据矿工的工作量来执行货币的分配和记账权的确定。算力竞争的胜者将获得相应区块的记账权和比特币奖励。因此, 矿机芯片的算力越高, 挖矿的时间更长, 就可以获得更多的比特币。

POS (股权证明): POS 机制中根据持有币的数量和时间来确定记账权的。一般用币龄 (每个币持有一天算一个币龄, 比如持有 100 个币, 总共持有了 30 天, 那么此时的币龄就为 3000) 来进行单位计量。在 POS 机制下, 如果记账人发现一个 POS 区块, 他的币龄就会被清空为 0, 每被清空 365 币龄, 将会从区块中获得 0.05 个币的利息(可理解为年利率 5%)。

DPOS (股份授权证明): DPOS 是在 POS 基础之上发展起来, 将记账人的角色专业化, 先通过权益来选出记账人, 然后由记账人之间再轮流记账。

dBFT 机制: dBFT 机制主要由 Onchain 公司开发的小蚁系统采用。一般先由持有小蚁股的人来选出记账人, 然后记账人之间通过拜占庭容错算法来达成共识。

表 6: 四种共识机制的比较

| 项目 | POW | POS | DPOS | dBFT |
|-------------|--|-----------|--------------|---------|
| 共识基础 | 工作量证明 | 币龄 | 币龄 | 拜占庭容错算法 |
| 记账人的产生 | 算力竞赛获胜者 | 持币人均可 | 投票选举 | 投票选举 |
| 对记账人的激励 | 比特币奖励 | 币龄销毁奖励 | 币龄销毁奖励 | 交易费用 |
| 确认交易速度 | 10 分钟, 最终确认 1 小时 | 秒级 | 秒级 | 秒级 |
| 执行 51%攻击的成本 | 高 | 高 | 低 | 低 |
| 能耗 | 高 | 低 | 低 | 低 |
| 是否鼓励开发 | 否 | 是 | 是 | 是 |
| 主要存在的问题 | 算力日益集中 | 初始货币分发不公平 | 容易遭受 DDOS 攻击 | 投票选举的风险 |
| 代表性数字货币 | 比特币 (SHA256 算法)、 莱特币 (Script 算法)、 狗币 (Script 算法) | 未来币 | 比特股 | 小蚁股、小蚁币 |

资料来源: 浙商证券研究所

“POW+POS” 或将成为数字货币更好的共识机制。 POW 机制尽管具有能耗高、交易确认时间慢以及算力日益集中等缺陷, 但是其最大的价值在于通过工作量证明建立了类似黄金和白银等货币的自然信任机制。金银由于其稀缺性产生了自然信任, 纸币则是由国家的背书产生的信任, POW 机制通过工作量证明建立信任, 迫使货币的产生, 需要付出一定的工作量和成本; POS 机制虽然能有效解决 POW 机制下的诸多缺点, 且在网络安全维护方面更胜一筹, 但是其货币的初始分配存在明显的不公。最初获得货币的人币龄优势明显, 将对后续区块的产生形成重大的影响。因此, POW 和 POS 结合起来, 取长补短, 有望成为未来更加完美的区块链共识机制。目前主流的做法是通过 POW 铸造和分配新币, 通过 POS 维护网络安全。

竞争链通过实现一致性和分布式账簿机制来给诸如智能合约、名字注册和其他一些应用提供服务。 竞争链使用和比特币一样的创建块的机制, 有时也会采用货币和代币的支付机制, 但它们的目的是为了维持一个货币系统, 而是用于分配诸如资源或一份合约的目的。货币不是竞争链的要点, 只是作为一种次要的特征。目前最为著名的两个竞争链是 **Ethereum (以太坊)** 和 **Ripple (瑞波币)**。

以太坊 (Ethereum) 是一个平台和一种编程语言, 能使开发人员在之上建立和发布下一代分布式应用。它是一种图灵完备的平台, 基于区块链账簿, 用于合约的处理和执行; 并且内置一种叫 “ether” 的货币, 该货币主要用于执行合约时支付交易费用。Ether 也是通过挖矿程序产生的, 通过竞争计算一种题目, 谁先算得谁获得系统奖励的币。比特币是十分分钟算一个解, 以太币是 12 秒一个解。以太币最初由 POW 机制挖矿产生, 达到一定数量时切换为 POS 机制来维护系统安全, 是一种典型的 “POW+POS” 机制。在以太坊上开发程序、发行数字证券之类的, 需要消耗一定的以太币, 并且直接将以太币发到黑洞地址销毁掉; 移动任何这类数字

资产也需要支付少量的以太币作为矿工费。以太坊平台可以用来编程，分散，担保和交易任何事物：投票，域名，金融交易所，众筹，公司管理，合同和大部分的协议，知识产权。目前使用以太坊的平台区块链创业公司主要有

表 7：主要在以太坊平台上创建的区块链应用

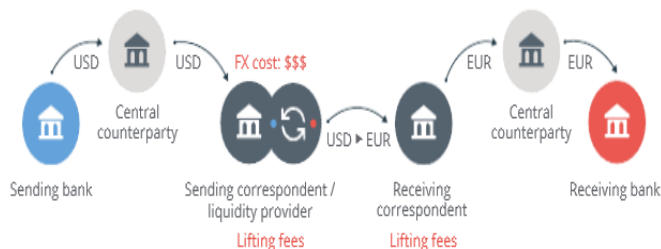
| 日期 | 公司 | 在以太坊上开发的应用 |
|------------|---------------|---|
| 2015.01.23 | IBM、三星 | IBM 联合三星打造 ADEPT 系统，主要用于去中心化的物联网。在 ADEPT 系统中，当数十亿个设备自动交互信息时，区块链将发挥分类账簿的作用 |
| 2015.10.29 | 微软 | 微软和以太坊生态公司 ConsenSys 正在推出一个工具包，可以让企业用户在以太坊协议上创建应用 |
| 2015.10.29 | Digix、Coinify | Digix 和 Coinify 合作创建了一个基于以太坊平台的加密资产交易平台，使用以太坊平台进行交易确认平均花费 14 至 17 秒，远快于比特币区块链 |
| 2015.12.14 | 德勤 | 德勤推出了“一站式区块链软件平台”Rubix，Rubix 的大部分工作集中在以太坊的协议 |
| 2016.01.21 | R3 CEV | R3 CEV 已发布了首个使用了以太坊和微软 Azure 的区块链即服务（BaaS）的分布式账本实验；参与实验的银行会通过分布式账本上的代币资产来模拟交易，而无需中心化的第三方参与 |
| 2016.04.01 | 以太坊、R3 CEV | 以太坊与 R3CEV 合作创建一种新的以区块链为基础的加密货币——Lizardcoin |
| 2016.04.12 | LO3、ConsenSys | LO3 与 ConsenSys 合作项目 TransActive Grid 首次将以太坊用于能源支付。个人太阳能板产生的过剩能源都会在以太坊区块链上进行计算和记录，并通过使用可编程的智能合约在公开市场上进行买卖 |

资料来源：巴比特、浙商证券研究所

Ripple 是世界上第一个开放的支付网络，通过这个支付网络可以转账任意一种货币，包括美元、欧元、人民币、日元或者比特币，简便易行快捷，交易确认在几秒以内完成，交易费用几乎是零，没有所谓的跨行异地以及跨国支付费用。**Ripple 是第一个将重心放到分布式账本应用的公司，并非真正意义上的区块链。**其开发的“InterLedger”协议将打造全球统一支付标准，创建统一的网络金融传输的协议。目前，Ripple 已经跟全球 25 家企业进行了合作，已公开的合作伙伴包括 Fidor 银行、CBW 银行、跨河银行、Earthport、CGI、IntellectEU 和埃森哲。

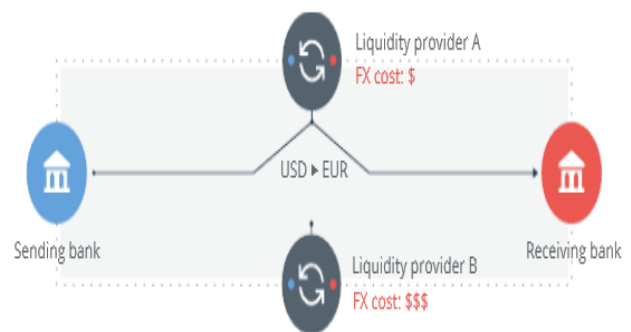
Ripple 的支付网络主要用于不同货币之间的跨境结算，可以大幅提高结算速度，降低交易费用。目前，实现不同货币之间的跨境结算需要经过许多中间银行，并且到账存在 2~4 天的延迟，成本也比较高；如果采用 Ripple 的支付网络，则可以直接实现不同货币之间的跨境结算，不需要中间银行，结算时间可以缩短至 3~5 秒，并且可以节省不少的交易费用。

图 34：传统的跨境结汇方式存在 2~4 天的延时



资料来源：Ripple 白皮书、浙商证券研究所

图 35：通过 Ripple 支付网络结汇时间可以缩短至 3~5 秒



资料来源：Ripple 白皮书、浙商证券研究所

五、从比特币产业链切入区块链的三条路径

1. 比特币产业链的核心人员自主创业进军区块链

比特币作为目前最成熟的区块链技术应用，其产业链上的核心人员对比特币的理解应该是最深刻的。尽管有一些依然坚守数字货币作为区块链的唯一应用，但也有部分人员通过自主创业转型区块链在其他领域的应用。比较典型的代表有**火币交易所张铮文**与**达鸿飞**两人创立的区块链创业公司**Onchain**、**元宝网（数字货币交易平台）**董事长**邓迪**等创立的**太一科技**。

Onchain 是一家区块链创业公司，创始人之一张铮文是区块链技术和计算机安全专家。加入小蚁前，就职于火币交易所。自主开发了基于比特币底层协议的企业钱包和撮合引擎。

Onchain 公司主业务是负责小蚁（antshares）系统的开发和运营，同时为其它金融机构提供区块链定制服务。1）小蚁系统是基于区块链技术，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，目前主要针对非上市公司股权的登记和结算。小蚁与上海股权交易中心的区别在于：小蚁不做交易的撮合，只有交易的执行。即双方交易已经达成了，小蚁只做执行和登记。目前小蚁还是测试版，正式版的预计在 6 月份之前会上线；2）提供区块链技术服务。Onchain 目前正在为数家银行、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。

图 36：小蚁去中心化网络协议



小蚁 - AntShares

资料来源：onchain 官网、浙商证券研究所

图 37：onchain 提供区块链技术服务



区块链技术服务

资料来源：onchain 官网、浙商证券研究所

小蚁 antshares 系统的运行模式：**1）小蚁股**。共 1 亿份，代表了小蚁协议的所有权。在创世块中 1 亿份小蚁股被创设，随后按一定分配方案进行分配。小蚁股总量上限不可增加。小蚁股主要用来：a) 投票产生记账人；b) 持续获得小蚁币作为系统分红；c) 投票决定小蚁协议的重大事项；**2）小蚁币**。小蚁币总量为 1 亿，可精确到 10^{-8} ，代表小蚁协议的使用权。小蚁币按照一定分发曲线在每个区块中持续分配给小蚁股的持有者。小蚁币总量上限不可增加。小蚁币的主要用途为：a) 支付小蚁的附加服务费；b) 支付小蚁的基本字节费；c) 作为记账候选人押金；3）用户在利用小蚁系统写入信息是要付出一定的小蚁币，**小蚁币的来源**：一是自己有小蚁股，可以通过系统分红获得小蚁币；二是从市场是直接购买小蚁币；4）**记账人由持有小蚁股的股东投票选举产生，记账人的盈利模式就是收取手续费，每年的手续费收入由所有的记账人平分**。在整个系统里，小蚁币的使用有两种方式：一种是使用初级服务，付给记账人的小蚁币，这部分小蚁币不会燃烧；一种是使用高级服务，使用这些服务是会燃烧一部分小蚁币，燃烧掉的小蚁币会回到未分配的状态最后分配给持有小蚁股的人。

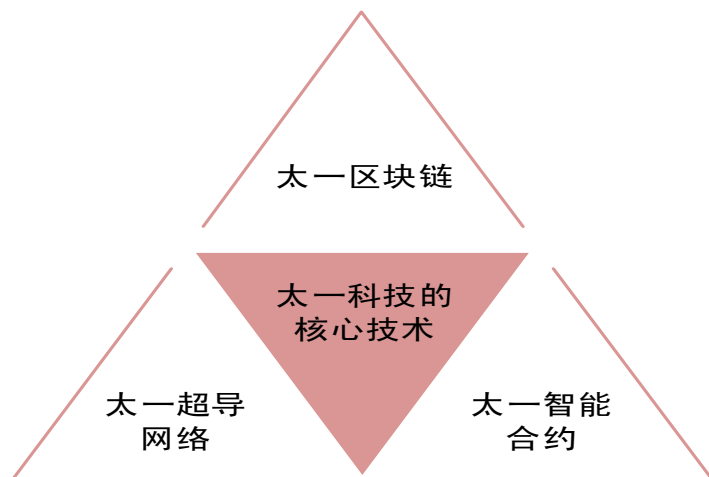
太一科技，即将成为国内第一家区块链上市公司。太一科技由元宝网（数字货币交易平台）董事长邓迪担任董事长，元宝网及元宝理财合规管理专员 Jelena Strelnikova 担任区块链合规官，近期将独立登陆新三板。太一科技**专注区块链底层技术的研发，向各领域提供安全可靠的区块链基础设施和中国特色的行业解决方案**；元宝网更侧重数字货币的交易，两者在业务上没有重合。

合作模式：1）采用提供技术及平台的方式，与具有合法金融牌照的商品交易平台、股权交易中心、金融机构等进行区块链领域的技术合作；2）采用技术授权的方式，与第三方公司合作开展业务；3）联合 IBM 等国内外知名企业，共建开放共享的区块链技术平台，建立示范性的项目，打造区块链产业基地，促进中国区块链的产业化。

太一科技的核心技术由**太一区块链、太一超导网络和太一智能合约**三部分构成。**太一区块链系统**是一种可控分布式记账系统，能广泛应用于金融和非金融的多个领域，每套太一系统包含一条物理链和许多条逻辑链，每条链上都有自己独立的超导网络；**太一**

超导网络中，每种资产能够实现每秒十万次的转账速度，在流转过程中无阻无损耗，同时包含数种专有网络硬件，具备银行级别的吞吐量与安全性；**太一智能合约**是基于二代区块链平台正在研发的内置模块，能实现自动化的资产的转移。其原理是根据事先制订的协议，在某一事件触发时能够自动的执行合约条款。智能合约使得合约处理过程自动化，不需要任何第三方托管机构介入，从而提高合约执行效率，节省费用。

图 38：太一科技的核心技术



资料来源：浙商证券研究所

与现有的其他区块链系统不同，太一科技最开始就面向中国市场进行架构设计，目标是面向各个领域提供安全可靠的区块链基础设施和行业解决方案。目前已提供区块链股权登记、商品登记、安全溯源、个人及企业征信、智能合约、金融自动支付、商业积分、分布式物联网、可信大数据中心等十多个领域的平台及方案。

图 39：太一科技的三大行业解决方案



资料来源：浙商证券研究所

2. 比特币产业链公司转型区块链服务提供商

比特币产业链公司转型区块链服务提供商的理由有两点：1)随着全网算力爆炸式增长，挖矿的难度越来越大，挖矿收益降低、矿机回本周期拉长、电力设施的建设以及长期挖矿的耐心不足等，都会导致比特币区块链公司往区块链服务商转型；2)与比特币相比，转型区块链服务提供商之后所面临的市场将更加广阔，与监管层之间的对立态势也将有所缓解。比特币产业链上主要有矿机、芯片生产商、矿池、算力交易平台、交易所、支付公司、钱包公司，这些公司未来都有可能转型区块链技术提供商。典型的代表有**芯片和矿机生产商 BitFury**。

图 40：不同机型的矿机挖矿的成本与收益情况对比

比特币挖矿收益 (自动刷新:27秒)

| 挖矿设备 | 售价 | 计算力 | 算力成本 | 功率 | 电力成本 | *一日收益 | *回本时间 |
|------------------------------|-------|--------|-----------|--------|-----------|------------------------|-------|
| AMD HD7950 BE 显卡 | ¥2099 | 0.69 G | ¥3,042 /G | 375 瓦 | ¥5.4 /度 | 0 BTC ¥0.01 | 999天 |
| (矿场处理)龙矿1T | ¥750 | 1000 G | ¥0.8 /G | 1000 瓦 | ¥14.4 /度 | 0.0028 BTC ¥8.09 ↓ | 135天 |
| (矿场处理)蚂蚁S5 | ¥1150 | 1150 G | ¥1 /G | 590 瓦 | ¥8.5 /度 | 0.0032 BTC ¥9.31 | 223天 |
| (矿场处理)龙矿1.2T NOT | ¥850 | 1200 G | ¥0.7 /G | 1200 瓦 | ¥17.28 /度 | 0.0034 BTC ¥9.71 ↓ | 124天 |
| 阿瓦隆A6矿机 | ¥2500 | 3500 G | ¥0.7 /G | 1050 瓦 | ¥15.12 /度 | 0.0099 BTC ¥28.33 ↓ | 125天 |
| 蚂蚁-S7 4.73T矿机 NOT | ¥3200 | 4730 G | ¥0.7 /G | 1293 瓦 | ¥18.62 /度 | 0.0133 BTC ¥38.29 ↑ | 116天 |

资料来源：比特范、浙商证券研究所

BitFury 转型区块链基础数据服务和交易处理服务提供商。2011 年，BitFury Group 创立于俄罗斯，在旧金山和阿姆斯特丹设有管理部门，在冰岛和格鲁吉亚共和国设有数据中心。早期是一个 ASIC 比特币矿机芯片研发团队，现在转型做区块链基础数据服务和交易处理服务。BitFury 也是目前已知的比特币行业获得融资最多的矿机公司。2015 年 7 月融资 2 千万美元，这是两年内 BitFury 第三轮融资，目前已公开的融资额达到 6 千万美元。

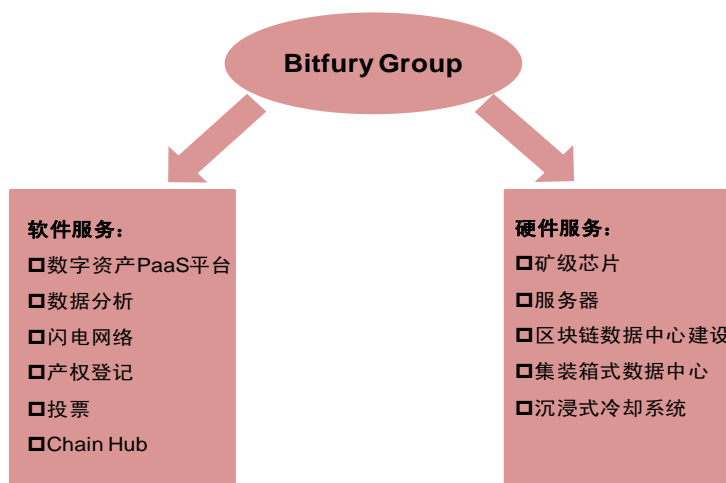
图 41：BitFury 的区块链转型之路



资料来源：浙商证券研究所

BitFury 最初业务主要做 ASIC 矿机芯片的研发，2015 年 1 月收购了香港一家科技创业公司 Allied Control。这家公司致力于构建一流的沉浸式制冷系统及数据中心基础设施，为世界发热量最大的超级计算机进行制冷。公司的模块化集装箱式 DataTank 数据中心能够为拥有高功率密度的超级计算机、HPC 及密码货币应用提供服务，以低成本的方式高效、高速地部署基础设施。BitFury 随后在格鲁吉亚共和国第比利斯购置了土地，采用 Allied Control 的沉浸式制冷技术及最新硅芯片技术构建 100MW 容量的数据中心；2016 年 2 月收购了一家比特币支付和交易公司——BitPesa，该公司接受通过非洲当地货币来兑换比特币，然后存入到非洲银行账户或者移动钱包中，为世界各地的个人和企业快速并且安全地与非洲等国进行交易支付提供服务。同年 3 月，公司发布了“公共区块链上的数字资产”的白皮书，详细探讨了区块链技术在保护和管理数字资产方面的潜力，并认为数字资产管理是区块链技术的前景应用之一。公司认为随着比特币区块链技术的应用越广泛，来自交易手续费的收入就越多。目前大约有 0.5%的收入来自交易费用，99.5%来自挖矿奖励。但是挖矿奖励的收入逐渐下降，交易费用收入逐渐上升的趋势已经显现。

图 42: BitFury 转型区块链技术服务之后的业务结构



资料来源：浙商证券研究所

建议关注国内三大矿机和芯片生产商**深圳比特泉**、**嘉楠耘智**和**比特大陆**未来可能向区块链服务提供商转型。其中，**深圳比特泉**旗下有**烤猫矿机**、并与**小强矿机**于2014年10月一起投资了**AMHash**云算力交易平台，公司目前专注方向依旧是芯片技术、布控技术、板级设计技术等核心技术；**嘉楠耘智**是全球领先的超算芯片及数字区块链计算设备制造、区块链计算整体方案提供商，也是全世界第一家研发出**SHA256**专用计算设备的公司，旗下的**Avalon**矿机销往全球超过150个国家和地区，售出芯片占全球专用设备总量的30%。公司于2013年收购了**Btctele.com**，是国内首家比特币支付类网站，支持话费充值、Q币、礼品卡、游戏充值以及打赏等业务。公司联合**清华长三角研究院杭州分院**、**数贝投资**、**矿池科技**、**算力科技**等公司共同发起成立了**中国区块链应用研究中心**，致力于**区块链应用拓展**；**比特大陆**致力于提供高速、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，公司客户遍及全球100多个国家和地区。除了不断推出高性能的比特币挖矿芯片和矿机，公司还致力于为全球用户提供稳定的矿池服务、云算力托管服务、**定制化区块链协议**等行业互联网综合解决方案。比特大陆旗下的**蚂蚁矿机****Antminer**、**蚁池****Antpool**、云算力**HashNest**均排名全球市场第一。此外还可以关注国内比特币交易平台**火币网**、**BTCChina**。

3. 比特币产业链公司与 Fintech 类上市公司合作

比特币产业链公司拥有区块链的技术和经验，对区块链的理解最为深刻；而 Fintech 类上市公司拥有渠道，通过多年服务金融企业的经验积累，对银行、证券和保险公司等金融类企业的业务理解最深刻，二者的合作必将有利于区块链技术在其最大的应用场景——金融企业中推广和利用。可能的合作方式有：1) 比特币产业链的公司通过**技术授权**，与 Fintech 类上市公司合作开展业务；2) Fintech 类上市公司**直接收购**比特币产业链的创业公司或者区块链创业公司。建议关注**飞天诚信**、**广电运通**、**赢时胜**、**御银股份**、**卫士通**、**信雅达**和**恒生电子**等上市公司在区块链技术方面的布局进展。

股票投资评级说明

以报告日后的 6 个月内，证券相对于沪深 300 指数的涨跌幅为标准，定义如下：

- 1、买入：相对于沪深 300 指数表现 +20% 以上；
- 2、增持：相对于沪深 300 指数表现 +10% ~ +20%；
- 3、中性：相对于沪深 300 指数表现 -10% ~ +10% 之间波动；
- 4、减持：相对于沪深 300 指数表现 -10% 以下。

行业的投资评级：

以报告日后的 6 个月内，行业指数相对于沪深 300 指数的涨跌幅为标准，定义如下：

- 1、看好：行业指数相对于沪深 300 指数表现 +10% 以上；
- 2、中性：行业指数相对于沪深 300 指数表现 -10% ~ +10% 以上；
- 3、看淡：行业指数相对于沪深 300 指数表现 -10% 以下。

我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重。

建议：投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者不应仅仅依靠投资评级来推断结论

法律声明及风险提示

本报告由浙商证券股份有限公司（已具备中国证监会批复的证券投资咨询业务资格，经营许可证编号为：Z39833000）制作。本报告中的信息均来源于我们认为可靠的已公开资料，但浙商证券股份有限公司及其关联机构（以下统称“本公司”）对这些信息的真实性、准确性及完整性不作任何保证，也不保证所包含的信息和建议不发生任何变更。本公司没有将变更的信息和建议向报告所有接收者进行更新的义务。

本报告仅供本公司的客户作参考之用。本公司不会因接收人收到本报告而视其为本公司的当然客户。

本报告仅反映报告作者的出具日的观点和判断，在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求。对依据或者使用本报告所造成的一切后果，本公司及/或其关联人员均不承担任何法律责任。

本公司的交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。本公司没有将此意见及建议向报告所有接收者进行更新的义务。本公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告版权均归本公司所有，未经本公司事先书面授权，任何机构或个人不得以任何形式复制、发布、传播本报告的全部或部分内容。经授权刊载、转发本报告或者摘要的，应当注明本报告发布人和发布日期，并提示使用本报告的风险。未经授权或未按要求刊载、转发本报告的，应当承担相应的法律责任。本公司将保留向其追究法律责任的权利。

浙商证券研究所

上海市长乐路 1219 号长鑫大厦 18 层

邮政编码：200031

电话：(8621)64718888

传真：(8621)64713795

浙商证券研究所：<http://research.stocke.com.cn>